Practical Scenarios

Network Security All-in-one

ASA Firepower WSA Umbrella VPN ISE Layer 2 Security





Lulu Press, Inc

Redouane MEDDANE 3xCCNP Collaboration, Security and Enterprise

Mastering a topic takes effort Demystifying and Simplifying takes a lot of effort but it is worth it.

Lulu Press, Inc Morrisville, North Carolina

Network Security All-in-one: ASA Firepower WSA VPN ISE Layer 2 Security

Copyright @ 2022 Redouane MEDDANE.

Published by: Lulu Press, Inc Morrisville, North Carolina

All Right Reserved. No portion of this book may be reproduced mechanically, electronically, or by any other means, including photocopying, without the written permission of the publisher.

Description

This book is written for Network engineers working in the Security field and to prepare the CCNP Security exam, it includes Cisco ASA Firewall, ASA with FirePOWER, Firepower Threat Defense FTD, Web Security Appliance, VPN Technologies, Cisco ISE, Cisco Umbrella and Layer 2 Security with practice labs in one book with a simple explanation through 80 Scenarios.

About the Author:

Redouane MEDDANE is 3xCCNP Collaboration, Security and Enterprise certified and he is a published author of some of the most important OSPF Protocol, Security and Collaboration books in the world titled: OSPF Demystified With RFC, Network Security All-in-one, and Dial Plan and Call Routing Demystified on CUCM, Cisco Meeting Server Deploy Implement Maintain Cisco Collaboration Conferencing. He is also a blogger at ipdemystify.com and writes articles about collaboration and security to demystify the most complex topics.

His books are known for their technical depth and accuracy especially the OSPF Demystified With RFC book, which is considered as the best OSPF book in the world and named "One of the best OSPF ebooks of all time" by BookAuthority It gives you a hint at the ability to explain complex topics with remarkable ease.

Table of Contents

Cisco ASA Firewall With FirePOWER Services

Lab 1: Auto NAT and Manual NAT Lab 2: HTTP Inspection Lab 3: FTP Inspection Part-1 Lab 4: FTP Inspection Part-2 Lab 5: TCP normalization Lab 6: Access-list ACL using network object Lab 7: Active/Standby Failover Lab 8: Firewal Transparent mode Lab 9: ASA FirePOWER module installation

Lab 10: URL Filtering with ASA 5506-X FirePOWER

Firepower Threat Defense

Lab 1: FTD Basic Configuration Lab 2: FTD NAT Policy Lab 3: FTD SSL Decryption for Outbound Connection Lab 4: Security Intelligence Lab 5: QoS on Firepower Threat Defense Lab 6: Advanced Malware Protection AMP Lab 7: Network Discovery Policy Lab 8: Intrusion Prevention System IPS Policy Scenario 1 Lab 9: Intrusion Prevention System IPS Policy Scenario 2 Lab 10: Configuration of PBR using FlexConfig on FTD Lab 11: Firepower Threat Defense Failover Active/Standby Lab 12: Pre-Filter Policy on Firepower Threat Defense Lab 13: VPN Site to Site with IKEv2 on Firepower

Cisco Web Security Appliance

- Lab 1: Cisco WSA installation
- Lab 2: Transparent mode with WCCP and Access Policies
- Lab 3: Custom URL Category Configuration
- Lab 4: Configure Application Visibility Control for the Access Policy
- Lab 5: Proxy Authentication using AD Realm
- Lab 6: Identification Profile and Access Policies
- Lab 7: HTTPS Decryption
- Lab 8: Referrer Header Exception
- Lab 9: Application Visibility and Control

Cisco Umbrella

Lab 1: Cisco Umbrella Basic Configuration

Lab 2: Intelligent Proxy and SSL Decryption

Lab 3: IP Layer Enforcement in Cisco Umbrella

Lab 4: Umbrella Active Directory Integration With Roaming Client

VPN Technologies

Lab 1: Static VTI Point-To-Point tunnel

Lab 2: Dynamic VTI Hub and Spoke tunnel

Lab 3: VPN Site-to-Site with dynamic IP

Lab 4: DMVPN Phase 2 using EIGRP

Lab 5: DMVPN Phase 2 using OSPF

Lab 6: DMVPN Phase 3 using EIGRP

Lab 7: DMVPN Phase 3 using OSPF

Lab 8: VPN Site-to-Site between ASA using PKI

Lab 9: Site-to-Site FlexVPN IOS router

Lab 10: GRE VPN over IPsec

Lab 11: Site-to-Site IKEv2 IPsec VPN

Lab 12: Basic VPN AnyConnect Remote Access

Lab 13: VPN AnyConnect authentication using ACS

Lab 14: VPN AnyConnect authentication using ISE

Lab 15: Basic VPN Clientless Remote Access

Lab 16: VPN Clientless authentication using ISE

Cisco Identity Services Engine

Lab 1: Cipher Negotiation TLS Issues

Lab 2: 802.1X With Dynamic VLAN and DACL

Lab 3: Advanced 802.1X Configuration

Lab 4: Guest Access With Self-Registered Portal

Lab 5: Guest Access With Hotspot Portal

Lab 6: Profiling Using DHCP Probe

Lab 7: Basic Device Admin using TACACS From Scenario 1

Lab 8: Advanced Device Admin TACACS Scenario 2

Lab 9: Cisco ISE Integration with F5 BIG-IP

Lab 10: VPN Anyconnect with ISE and Tunnel-Group-Lock

Lab 11: Authorization Policy Based On Profiling Data

Lab 12: Cisco ISE with F5 BIG-IP for Dot1x Load Balancing

Lab 13: Cisco ISE with F5 BIG-IP for Guest Load Balancing

Layer 2 Security

Lab 1: DHCP Snooping IP source guard and ARP inspection

Lab 2: DHCP Snooping and ARP Inspection Part-1 Lab 3: DHCP Snooping and ARP Inspection Part-2 Lab 4: IP source guard Lab 5: ARP Inspection using ARP ACL and "static" keyword Lab 6: Private VLANs PVLANs Lab 7: BPDU Loop Guard Bonus: Comprehensive Security Lab

Network Security All-in-one WorkBook Cisco ASA Firewall And FirePOWER Services

Lab 1: Auto NAT and Manual NAT



Configuration of Basic IP addressing:



ciscoasa# show run interface vlan 1

I interface Vlan1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 ciscoasa# ciscoasa# show run interface vlan 2 I interface Vlan2 nameif outside security-level 0 ip address 209.165.200.1 255.255.254 ciscoasa# ciscoasa# show run interface vlan 3 interface Vlan3 no forward interface Vlan1 nameif DMZ security-level 50 ip address 172.16.1.1 255.255.255.0 ciscoasa#

Affecting of the physical interface to VLAN:

```
ciscoasa# show run interface e0/0
!
interface Ethernet0/0
switchport access vlan 2
ciscoasa#
ciscoasa# show run interface e0/1
!
interface Ethernet0/1
ciscoasa# show run interface e0/2
!
interface Ethernet0/2
switchport access vlan 3
ciscoasa#
```

```
ciscoasa# show run interface e0/0
!
interface Ethernet0/0
switchport access vlan 2
ciscoasa#
ciscoasa# show run interface e0/1
!
interface Ethernet0/1
ciscoasa# show run interface e0/2
!
interface Ethernet0/2
switchport access vlan 3
ciscoasa#
```

By default the echo-reply ICMP is not allowed from a lower security to a higher security, enable ICMP inspection in the policy-map global_policy:

```
ciscoasa(config) # policy-map global_policy
ciscoasa(config-pmap) # class inspection_default
ciscoasa(config-pmap-c) # inspect icmp
```

ciscoasa(config)# policy-map global_policy ciscoasa(config-pmap)# class inspection_default ciscoasa(config-pmap-c)# inspect icmp

Enable access via ASDM:

ciscoasa(config) # username admin password cisco ciscoasa(config) # http server enable ciscoasa(config) # http 192.168.1.0 255.255.255.0 inside

```
ciscoasa(config)# username admin password cisco
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

Auto-nat Configuration:

DMZ Server requires a static translation when routed to the outside interface. The translated ip address is 209.165.200.22:

ciscoasa(config)# object network DMZ-SRV ciscoasa(config-network-object)# host 172.16.1.2 ciscoasa(config-network-object)# nat (DMZ,outside) static 209.165.200.22

ciscoasa(config)# object network DMZ-SRV ciscoasa(config-network-object)# host 172.16.1.2 ciscoasa(config-network-object)# nat (DMZ,outside) static 209.165.200.22

Verify the object network DMZ-SRV:

```
ciscoasa# show run object
object network DMZ-SRV
host 172.16.1.2
ciscoasa#
ciscoasa# show run nat
!
object network DMZ-SRV
nat (DMZ,outside) static 209.165.200.22
ciscoasa#
```

ciscoasa# show run object object network DMZ-SRV host 172.16.1.2

```
ciscoasa#
ciscoasa# show run nat
!
object network DMZ-SRV
nat (DMZ,outside) static 209.165.200.22
ciscoasa#
```

From the DMZ Server connect to the Public Server:

OUTSIDE web Server

WELCOME!

Verification of the NAT translation of the DMZ Server, the auto-nat also called object nat is placed in the Section 2:

ciscoasa# show nat

```
Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source static DMZ-SRV 209.165.200.22
    translate_hits = 4, untranslate_hits = 2
ciscoasa#
```

ciscoasa# show nat

```
Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source static DMZ-SRV 209.165.200.22
translate_hits = 4, untranslate_hits = 2
ciscoasa#
```

The inside network requires PAT when routed to the outside interface, the hosts in the inside network share the same public IP address 209.165.200.20:

ciscoasa(config)# object network INSIDE-NETWORK ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0 ciscoasa(config-network-object)# nat (inside,outside) dynamic 209.165.200.20

```
ciscoasa(config)# object network INSIDE-NETWORK
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic 209.165.200.20
```

Verify the object network INSIDE-NETWORK:

```
ciscoasa# show run object | exc DMZ-SRV|host
object network INSIDE-NETWORK
subnet 192.168.1.0 255.255.255.0
ciscoasa#
ciscoasa# show run nat | exc DMZ-SRV|DMZ
!
object network INSIDE-NETWORK
nat (inside,outside) dynamic 209.165.200.20
ciscoasa#
```

```
ciscoasa# show run object | excDMZ-SRV|host
object network INSIDE-NETWORK
subnet 192.168.1.0 255.255.255.0
ciscoasa#
ciscoasa# show run nat | exc DMZ-SRV|DMZ
!
object network INSIDE-NETWORK
nat (inside,outside) dynamic 209.165.200.20
ciscoasa#
```

From the inside host connect to the Public Server:



OUTSIDE web Server

```
WELCOME!
```

Verify the nat rules:

```
ciscoasa# show nat
Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source static DMZ-SRV 209.165.200.22
translate_hits = 8, untranslate_hits = 2
2 (inside) to (outside) source dynamic INSIDE-NETWORK 209.165.200.20
translate_hits = 3, untranslate_hits = 0
ciscoasa#
```

ciscoasa# show nat

Auto NAT Policies (Section 2) 1 (DMZ) to (outside) source static DMZ-SRV 209.165.200.22 translate_hits = 8, untranslate_hits = 2 2 (inside) to (outside) source dynamic INSIDE-NETWORK 209.165.200.20

```
translate_hits = 3, untranslate_hits = 0
ciscoasa#
```

The show xlate command shown that the inside host with 192.168.1.2 is translated to 209.165.200.20:

```
ciscoasa# show xlate
3 in use, 4 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from DMZ:172.16.1.2 to outside:209.165.200.22
    flags s idle 0:18:08 timeout 0:00:00
TCP PAT from inside:192.168.1.2/4066 to outside:209.165.200.20/41628 flags ri idle 0:00:02 timeout 0:00:30
TCP PAT from inside:192.168.1.2/4065 to outside:209.165.200.20/25933 flags ri idle 0:00:02 timeout 0:00:30
ciscoasa#
```

```
ciscoasa# show xlate
3 in use, 4 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from DMZ:172.16.1.2 to outside:209.165.200.22
flags s idle 0:18:08 timeout 0:00:00
TCP PAT from inside:192.168.1.2/4066 to outside:209.165.200.20/41628 flags ri idle
0:00:02 timeout 0:00:30
TCP PAT from inside:192.168.1.2/4065 to outside:209.165.200.20/25933 flags ri idle
0:00:02 timeout 0:00:30
ciscoasa#
```

Manual-NAT configuration:

For DMZ server, configure a translation that should be used only when the destination is the outside network 209.165.201.0/27 using the translated IP address 209.165.201.23:

```
ciscoasa(config)# object network OUTSIDE-NETWORK
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network DMZ-MANUAL-NAT
ciscoasa(config-network-object)# host 209.165.201.23
ciscoasa(config-network-object)# exit
ciscoasa(config)# nat (DMZ,outside) source static DMZ-SRV DMZ-MANUAL-NAT
destination static OUTSIDE-NETWORK OUTSIDE-NETWORK
```

Verify the Manual NAT configuration:

```
ciscoasa# show run object id OUTSIDE-NETWORK
object network OUTSIDE-NETWORK
subnet 209.165.201.0 255.255.255.224
ciscoasa#
ciscoasa# show run object id DMZ-MANUAL-NAT
object network DMZ-MANUAL-NAT
host 209.165.201.23
ciscoasa#
```

ciscoasa# show run object id OUTSIDE-NETWORK

```
object network OUTSIDE-NETWORK
subnet 209.165.201.0 255.255.255.224
ciscoasa#
ciscoasa# show run object id DMZ-MANUAL-NAT
object network DMZ-MANUAL-NAT
host 209.165.201.23
ciscoasa#
```

ciscoasa‡ show run nat | inc DMZ nat (DMZ,outside) source static DMZ-SRV DMZ-MANUAL-NAT destination static OUTSIDE-NETWORK OUTSIDE-NETWORK ciscoasa‡

ciscoasa# show run nat | inc DMZ nat (DMZ,outside) source static DMZ-SRV DMZ-MANUAL-NAT destination static OUTSIDE-NETWORK OUTSIDE-NETWORK ciscoasa#

The show nat reveals that the Manual NAT configured previously is placed in the section 1, this the default ASA behavior, the Manual NAT is more specific than the auto-nat:

```
ciscoasa# show nat
Manual NAT Policies (Section 1)
1 (DMZ) to (outside) source static DMZ-SRV DMZ-MANUAL-NAT destination static OUTSIDE-NETWORK OUTSIDE-NETWORK
translate_hits = 0, untranslate_hits = 0
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE-NETWORK 209.165.200.20
translate_hits = 5, untranslate_hits = 0
ciscoasa#
```

```
ciscoasa# show nat
Manual NAT Policies (Section 1)
1 (DMZ) to (outside) source static DMZ-SRV DMZ-MANUAL-NAT destination static
OUTSIDE-NETWORK OUTSIDE-NETWORK
translate_hits = 0, untranslate_hits = 0
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE-NETWORK 209.165.200.20
translate_hits = 5, untranslate_hits = 0
ciscoasa#
```

For inside clients, configure a translation that should be used when accessing the DMZ server on TCP port 8080, the inside hosts should use a single IP address 172.16.1.10 and the DMZ Server should see the port 80 instead of 8080:

```
ciscoasa(config)# object network DMZ_PAT
ciscoasa(config-network-object)# host 172.16.1.10
ciscoasa(config-network-object)# exit
ciscoasa(config)# object service HTTP_80
ciscoasa(config-service-object)# service tcp destination eq www
ciscoasa(config-service-object)# exit
ciscoasa(config)# object service HTTP_PROXY_PORT
ciscoasa(config)# object service HTTP_PROXY_PORT
ciscoasa(config)# nat (inside,DMZ) source dynamic INSIDE-NETWORK DMZ_PAT
destination static DMZ-SRV DMZ-SRV service HTTP_PROXY_PORT HTTP_80
```

Verify the configuration of NAT:

```
ciscoasa# show run object id DM2_PAT
object network DM2_PAT
host 172.16.1.10
ciscoasa#
ciscoasa# show run object id HTTP_80
object service HTTP_80
service tcp destination eq www
ciscoasa#
ciscoasa# show run object id HTTP_PROXY_PORT
object service HTTP_PROXY_PORT
service tcp destination eq 8080
ciscoasa#
```

```
ciscoasa# show run object id DMZ_PAT
object network DMZ_PAT
host 172.16.1.10
ciscoasa#
ciscoasa# show run object id HTTP_80
object service HTTP_80
servicetcp destination eq www
ciscoasa#
ciscoasa# show run object id HTTP_PROXY_PORT
object service HTTP_PROXY_PORT
servicetcp destination eq 8080
ciscoasa#
```

ciscoasa# show run nat | inc (inside,DMZ) nat (inside,DMZ) source dynamic INSIDE-NETWORK DMZ_PAT destination static DMZ-SRV DMZ-SRV service HTTP_PROXY_P ORT HTTP_80 ciscoasa#

ciscoasa# show run nat | inc (inside,DMZ)
nat (inside,DMZ) source dynamic INSIDE-NETWORK DMZ_PAT destination static DMZ-SRV
DMZ-SRV service HTTP_PROXY_PORT HTTP_80
ciscoasa#

From the inside host connect to the DMZ Server using the link <u>http://172.16.1.2:8080:</u>

Ор	era	▮ 172.16.1.2:8080 ×								
←	→	C		Ø	172.16.1.	2:8080)			

DMZ web Server

WELCOME!

Verifiy that the NAT translation:

Manual NAT Policies (Section 1)
1 (DMZ) to (outside) source static DMZ-SRV DMZ-MANUAL-NAT destination static OUTSIDE-NETWORK OUTSIDE-NETWORK
translate_hits = 0, untranslate_hits = 0
2 (inside) to (DMZ) source dynamic INSIDE-NETWORK DMZ_PAT destination static DMZ-SRV DMZ-SRV service HTTP_PROXY_PORT HTTP_80
translate_hits = 5, untranslate_hits = 2
Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source static DMZ-SRV 209.165.200.22
translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic INSIDE-NETWORK 209.165.200.20
translate_hits = 6, untranslate_hits = 0

```
ciscoasa# show nat
Manual NAT Policies (Section 1)
1 (DMZ) to (outside) source static DMZ-SRV DMZ-MANUAL-NAT destination static
OUTSIDE-NETWORK OUTSIDE-NETWORK
translate_hits = 0, untranslate_hits = 0
2 (inside) to (DMZ) source dynamic INSIDE-NETWORK DMZ_PAT destination static
DMZ-SRV DMZ-SRV service HTTP_PROXY_PORT HTTP_80
translate_hits = 5, untranslate_hits = 2
Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source static DMZ-SRV 209.165.200.22
translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic INSIDE-NETWORK 209.165.200.20
translate_hits = 6, untranslate_hits = 0
ciscoasa#
```

Verify the translation using the show xlate:



ciscoasa# show xlate
5 in use, 8 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from DMZ:172.16.1.2 to outside:209.165.201.23
flags s idle 0:02:24 timeout 0:00:00
TCP PAT from DMZ:172.16.1.2 80-80 to inside:172.16.1.2 8080-8080
flagssrIT idle 0:00:04 timeout 0:00:00
NAT from DMZ:172.16.1.2 to outside:209.165.200.22
flags s idle 0:03:24 timeout 0:00:00
TCP PAT from inside:192.168.1.2/4167 to DMZ:172.16.1.10/33081 flags ri idle
0:00:04 timeout 0:00:30
TCP PAT from inside:192.168.1.2/4166 to DMZ:172.16.1.10/11414 flags ri idle
0:00:04 timeout 0:00:30
ciscoasa#

Lab 3: FTP Inspection Part-1



FTP inspection between outside PC and the DMZ server requirements. Drop all commands except the get command.

First we configure a static translation for the DMZ Server

```
ciscoasa(config)# object network DMZ-SERVER-PRIV
ciscoasa(config-network-object)# host 192.168.1.10
ciscoasa(config-network-object)# nat (DMZ,outside) static 209.165.201.10
```

ciscoasa(config)# object network DMZ-SERVER-PRIV ciscoasa(config-network-object)# host 192.168.1.10 ciscoasa(config-network-object)# nat (DMZ,outside) static 209.165.201.10

Allow FTP traffic from outside PC to DMZ server:

```
ciscoasa(config)# object-group service FTP-TO-DMZ tcp
ciscoasa(config-service-object-group)# port-object eq ftp
ciscoasa(config-service-object-group)# port-object eq ftp-data
```

ciscoasa(config)# object-group service FTP-TO-DMZ tcp ciscoasa(config-service-object-group)# port-object eq ftp ciscoasa(config-service-object-group)# port-object eq ftp-data

ciscoasa(config)# access-list OUT-TO-DMZ extended permit tcp host 209.165.200.30
object DMZ-SERVER-PRIV object-group FTP-TO-DMZ

ciscoasa(config)# access-group OUT-TO-DMZ in interface outside

ciscoasa(config) # show access-list | incl OUT-TO-DMZ access-list OUT-TO-DMZ; 2 elements; name hash: 0x9c4dc3b4 access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 object DMZ-SERVER-PRIV object-group FTP-TO-DMZ (hitcnt=0) 5a08 access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp (hitcnt=0) 0x9587a5da access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp-data (hitcnt=0) 0x4f70d236

Another method to configure the access-list:

ciscoasa(config)# object-group service FTP-TO-DMZ ciscoasa(config-service-object-group)# service-object tcp eq ftp ciscoasa(config-service-object-group)# service-object tcp eq ftp-data

ciscoasa(config)# object-group service FTP-TO-DMZ
ciscoasa(config-service-object-group)# service-object tcpeq ftp
ciscoasa(config-service-object-group)# service-object tcpeq ftp-data

ciscoasa(config)# access-list OUT-TO-DMZ extended permit object-group FTP-TO-DMZ host 209.165.200.30 object DMZ-SERVER-PRIV

ciscoasa(config)# access-group OUT-TO-DMZ in interface outside

ciscoasa(config) # show access-list | include OUT-TO-DMZ access-list OUT-TO-DMZ; 2 elements; name hash: 0x9c4dc3b4 access-list OUT-TO-DMZ line 1 extended permit object-group FTP-TO-DMZ host 209.165.200.30 object DMZ-SERVER-PRIV (hitcnt=0) access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp (hitcnt=0) 0x9587a5da access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp (hitcnt=0) 0x9587a5da access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp-data (hitcnt=0) 0x4f70d236 ciscoasa(config)#

Or:

ciscoasa(config)# object-group service FTP-TO-DMZ ciscoasa(config-service-object-group)# service-object tcp destination eq ftp ciscoasa(config-service-object-group)# service-object tcp destination eq ftp-data

ciscoasa(config)# access-list OUT-TO-DMZ extended permit object-group FTP-TO-DMZ host 209.165.200.30 object DMZ-SERVER-PRIV

ciscoasa(config)# access-group OUT-TO-DMZ in interface outside

ciscoasa(config) # show access-list | incl OUT-TO-DMZ access-list OUT-TO-DMZ; 2 elements; name hash: 0x9c4dc3b4 access-list OUT-TO-DMZ line 1 extended permit object-group FTP-TO-DMZ host 209.165.200.30 object DMZ-SERVER-PRIV (hitcnt=0) access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp (hitcnt=0) 0x9587a5da access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp (hitcnt=0) 0x9587a5da access-list OUT-TO-DMZ line 1 extended permit tcp host 209.165.200.30 host 192.168.1.10 eq ftp-data (hitcnt=0) 0x4f70d236 ciscoasa(config)#

Creates an access-list named GLOBAL-FTP-DMZ to identify the flow coming from the outside PC to the DMZ server and matches this ACL into the class-map FTP-PROTECTION, then defines a policy-map type inspect FTP named FTP-POLICY and reset with log all command except the get command:

ciscoasa(config)# access-list GLOBAL-FTP-DMZ extended permit tcp any object DMZ-SERVER-PRIV object-group FTP-TO-DMZ

```
ciscoasa(config)# class-map FTP-PROTECTION
ciscoasa(config-cmap)# match access-list GLOBAL-FTP-DMZ
ciscoasa(config-cmap)#
ciscoasa(config-cmap)# policy-map type inspect ftp FTP-POLICY
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# mask-syst-reply
ciscoasa(config-pmap-p)# match request-command appe cdup help rnfr rnto put st$
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# policy-map global_policy
ciscoasa(config-pmap-c)# class FTP-PROTECTION
ciscoasa(config-pmap-c)# inspect ftp strict FTP-POLICY
```

ciscoasa(config)# class-map FTP-PROTECTION ciscoasa(config-cmap)# match access-list GLOBAL-FTP-DMZ

```
ciscoasa(config)# policy-map type inspect ftp FTP-POLICY
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# mask-syst-reply
ciscoasa(config-pmap-p)# match request-command appecdup help rnfrrnto put stou
site dele mkdrmd
ciscoasa(config-pmap-c)# reset log
```

ciscoasa(config)# policy-map global_policy ciscoasa(config-pmap)# class FTP-PROTECTION ciscoasa(config-pmap-c)# inspect ftp strict FTP-POLICY

Verify your configuration:

```
ciscoasa# show run class-map
!
class-map inspection_default
 match default-inspection-traffic
class-map FTP-PROTECTION
 match access-list GLOBAL-FTP-DMZ
!
ciscoasa#
```

```
ciscoasa# show run class-map
```

```
!
class-mapinspection_default
match default-inspection-traffic
class-map FTP-PROTECTION
match access-list GLOBAL-FTP-DMZ
!
ciscoasa#
```

```
ciscoasa# show run policy-map type inspect ftp
!
policy-map type inspect ftp FTP-POLICY
parameters
  mask-banner
  mask-syst-reply
match request-command appe cdup help rnfr rnto put stou site dele mkd rmd
  reset log
!
ciscoasa#
```

```
ciscoasa# show run policy-map type inspect ftp
!
policy-map type inspect ftp FTP-POLICY
parameters
mask-banner
mask-syst-reply
match request-command appecdup help rnfrrnto put stou site dele mkdrmd
reset log
```

Configure an FTP policy to reset and log attempts to access the files with .exe and .txt

Create a regular expression class that include the following parameters:

Create and match a regular expression that matches all .txt files. Create and match a regular expression that matches all .exe files.

```
ciscoasa(config)# regex TXT-FILES "\.txt"
ciscoasa(config)# regex EXE-FILES "\.exe"
ciscoasa(config)#
ciscoasa(config)# class-map type regex match-any DMZ-REGEX
ciscoasa(config-cmap)# match regex TXT-FILES
ciscoasa(config-cmap)# match regex EXE-FILES
```

```
ciscoasa(config)# regex TXT-FILES "\.txt"
ciscoasa(config)# regex EXE-FILES "\.exe"
ciscoasa(config)#
ciscoasa(config)# class-map type regex match-any DMZ-REGEX
ciscoasa(config-cmap)# match regex TXT-FILES
ciscoasa(config-cmap)# match regex EXE-FILES
```

Let's test out regular expression:



Verification:

```
ciscoasa# show run regex
regex TXT-FILES "\.txt"
regex EXE-FILES "\.exe"
ciscoasa#
```

```
ciscoasa# show run regex
regex TXT-FILES "\.txt"
regex EXE-FILES "\.exe"
ciscoasa#
```

```
ciscoasa# show run class-map type regex
!
class-map type regex match-any DMZ-REGEX
match regex TXT-FILES
match regex EXE-FILES
!
ciscoasa#
```

ciscoasa# show run class-map type regex !

```
class-map type regex match-any DMZ-REGEX
match regex TXT-FILES
match regex EXE-FILES
!
```

ciscoasa#

Edit the FTP-POLICY inspection to match the configured regular expression inside the ftp filetype, we should reset and log attempts to access these files.

```
ciscoasa(config)# policy-map type inspec ftp FTP-POLICY
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# match filetype regex class DMZ-REGEX
ciscoasa(config-pmap-c)# reset log
```

```
ciscoasa(config)# policy-map type inspec ftp FTP-POLICY
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# match filetype regex class DMZ-REGEX
ciscoasa(config-pmap-c)# reset log
```

```
ciscoasa# show run policy-map type inspect ftp
!
policy-map type inspect ftp FTP-POLICY
parameters
  mask-banner
  mask-syst-reply
match request-command appe cdup help rnfr rnto put stou site dele mkd rmd
  reset log
match filetype regex class DMZ-REGEX
  reset log
!
ciscoasa#
```

ciscoasa# show run policy-map type inspect ftp
!
policy-map type inspect ftp FTP-POLICY
parameters
mask-banner
mask-syst-reply
match request-command appecdup help rnfrrnto put stou site dele mkdrmd
reset log
matchfiletype regex class DMZ-REGEX
reset log
!
ciscoasa#



ciscoasa# show service-policy global inspect ftp

Global policy: Service-policy: global_policy Class-map: inspection_default Class-map: FTP-PROTECTION Inspect: ftp strict FTP-POLICY, packet 0, drop 0, reset-drop 0 mask-banner enabled mask-syst-reply enabled match request-command appecdup help rnfrrnto put stou site dele mkdrmd reset log, packet 0 matchfiletype regex class DMZ-REGEX reset log, packet 0 ciscoasa#

Verification:

From the outside PC access the DMZ server using the url ftp://209.165.200.10 and try to download the file with .zip, the downloading is successfully:

/ nating in a gostosteorization inneons internet explorer	
) () - (i) ftp://209.165.201.10/	🕶 🗟 🐓 🗙 🕨 Bing
🍃 Favoris 🛛 👍 🖉 Sites suggérés 🔻 🖉 Galerie de composants 👻	
@ Racine FTP à 209.165.201.10	👌 🕶 📓 💌 🖷 💌

Racine FTP à 209.165.201.10

Pour afficher ce site FTP dar	ns l'Explorateur Windows, cliquez sur Page , pu	0% deIOS%20Images%20for%20GNS3.zi	
10/08/2015 12:00 07/20/2015 12:00 07/20/2015 12:00 11/24/2015 03:36 11/24/2015 01:26 07/20/2015 12:00 07/20/2015 12:00 08/30/2015 12:00 07/20/2015 12:00 16 07/20/2015 12:00	Répertoire <u>\$RECYCLE.BIN</u> 6,565,736 <u>ccsetup507.exe</u> 11,128,904 <u>Firefox Setup 39.0.exe</u> 3 <u>ftp ict.txt</u> 0 <u>ftp.txt</u> 56,807,049 <u>GNS3-1.3.7-all-in-one.exe</u> Répertoire <u>Logiciels</u> 454,656 <u>Putty.exe</u> Répertoire <u>System Volume Informatio</u> 88,689,086 <u>Uncompressed IOS images f</u> 4,021,144 <u>USB Disk Security 6.5.0.0</u>	0% deLOS%/20Umages%/2007%/20007%/2007%/2007%/2007%/2007%/2007%/2007%/2007%/2007%/2007%/2007%/2007%/20000000000	Téléchargement de fichiers 25 Voulez-vous ouvrir ou enregistrer ce fichier ? Image: State of the st

The ASA displays a log message to confirm that the access of .zip file is successfully:

Latest A	itest ASDM Syslog Messages 🛛 🖓 🖗									
Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destin	a Description		
<u>4</u> 6	Dec 13 2015	06:26:30	303 <mark>002</mark>	209.165.200.30	49802	192.168.1.10	21	FTP connection from outside: 209. 165. 200. 30/49802 to DMZ: 192. 168. 1. 10/21, user ict Retrieved file /Uncompressed IOS Images for GNS3.zip		
<u>i</u> 6	Dec 13 2015	06:26:30	302013	209.165.200.30	49814	192.168.1.10	53726	Built inbound TCP connection 3388 for outside: 209. 165. 200. 30/49814 (209. 165. 200. 30/49814) to DMZ: 192. 168. 1. 10/53726 (209. 165. 201. 10/53726)		
<u>4</u> 6	Dec 13 2015	06:26:29	302014	209.165.200.30	49813	192.168.1.10	21	Teardown TCP connection 3385 for outside: 209. 165. 200. 30/49813 to DMZ: 192. 168. 1. 10/21 duration 0:00: 11 bytes 242 TCP FINs		
<u>Å</u> 6	Dec 13 2015	06:26:24	106015	209.165.200.30	49789	209.165.201.10	21	Deny TCP (no connection) from 209.165.200.30/49789 to 209.165.201.10/21 flags ACK on interface outside	-	

Try another attempt with .doc file, the result is successful:

3	▼ 🖄 44 ×
🚖 Favoris 🛛 👍 💋 Sites suggérés 🔻 🖉 Galerie de composants 👻	
O Connexion en cours	🖄 👻 🖸

Racine FTP à 209.165.201.10

Pour afficher ce site FT	P dans l'Explorateur Windows, cliquez sur Page, puis sur Ouvrir le sit	e Téléchargement de fichiers
10/08/2015 12:00 07/20/2015 12:00 07/25/2015 12:00 07/25/2015 12:00 07/22/2015 12:00 11/24/2015 03:36 11/24/2015 10:26 07/20/2015 12:00 04/13/2011 12:00 08/30/2015 12:00 07/20/2015 12:00	<pre>Répertoire <u>\$RECYCLE.BIN</u> 6,565,736 ccsetup507.exe 187,965 <u>CDM 2 08 28 Release Info.rtf</u> 41,128,904 Firefox Setup 39.0.exe 53,078,632 FoxitReader708.1216 prom L10N Setup.exe 3 ftp ict.txt 0 ftp.txt 66,807,049 <u>GNS3-1.3.7-all-in-one.exe</u> Répertoire Logiciels 454,656 <u>Putty.exe</u> Répertoire System Volume Information 188,689,086 <u>Uncompressed IOS Images for GNS3.zip</u> 4,021,144 <u>USB Disk Security 6.5.0.0.exe</u></pre>	Voulez-vous ouvrir ou enregistrer ce fichier ? Nom : CDM_2_08_28_Release_Info.rtf Type : Document Microsoft Word 97 - 2003, 183 Ko De : 209.165.201.10 Ouvrir Enregistrer Annuler Volourir Enregistrer Volourir Enregistrer Muler Volourir Es fichiers téléchargés depuis Internet peuvent être utiles, mais ce type de fichier réserte un danger potentiel. Nouvrez ou n'enregistrez ce fichier que si vous êtes sûr de son origine. Quels sort les idees ?

L	itest ASOM Syslog Messages 🛛 🗍 🗗										
S	everity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destin	Description		
4	6	Dec 13 2015	06:32:14	110002	209.165.200.30	49832			Failed to locate egress interface for TCP from outside: 209. 165. 200. 30/49832 to 80. 254. 145. 118/80		
4	6	Dec 13 2015	06:31:54	303002	209.165.200.30	49825	192, 168, 1, 10	21	FTP connection from outside: 209. 165. 200. 30/49825 to DMZ: 192. 168. 1. 10/21, user ict Retrieved file /CDM 2 08 28 Release Info.rtf	-	
4	6	Dec 13 2015	06:31:54	302013	209.165.200.30	49831	192.168.1.10	58886	Built inbound TCP connection 3402 for outside: 209. 165. 200. 30/49831 (209. 165. 200. 30/49831) to DMZ: 192. 168. 1. 10/58886 (209. 165. 201. 10/58886)		
4	6	Dec 13 2015	06:31:54	302014	209.165.200.30	49830	192, 168, 1, 10	21	Teardown TCP connection 3401 for outside: 209. 165. 200. 30/49830 to DMZ: 192. 168. 1. 10/21 duration 0:00: 11 bytes 242 TCP FINs	-	

Try to access the .txt file and the attempt fails:

🚖 Favoris 🛛 🚔 🙋 Sites suggérés 🔻 🙋 Galerie de composants 💌
Signature And the second secon
 Internet Explorer ne peut pas afficher cette page Web Essayez la chose suivante : Diagnostiquer les problèmes de connexion Informations

The ASA displays a log message of the failure:

Latest A	SDM Syslog I	lessages						6 م
Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destin	Description
<u>i</u> 6	Dec 13 2015	06:21:14	302013	209.165.200.30	49764	192.168.1.10	21	Built inbound TCP connection 3345 for outside: 209.165.200.30/49764 (209.165.200.30/49764) to DMZ: 192.168.1.10/21 (209.165.201.10/21)
<u>A</u> 4	Dec 13 2015	06:21:14	507003	209.165.200.30	49760	192, 168, 1, 10	21	tcp flow from outside: 209. 165. 200. 30/49760 to DM2: 192. 168. 1. 10/21 terminated by inspection engine, reason - inspector reset unconditionally.
<u>k</u> 5	Dec 13 2015	06:21:14	303005	209.165.200.30	49760	192.168.1.10	21	Strict FTP inspection matched filetype regex class DMZ-REGEX in policy-map FTP-POLICY, Reset connection from outside: 209.165.200.30/49760 to DMZ: 192.168.1
<mark>Å</mark> 6	Dec 13 2015	06:21:14	302013	209.165.200.30	49763	192, 168, 1, 10	62516	Built inbound TCP connection 3344 for outside: 209.165.200.30/49763 (209.165.200.30/49763) to DMZ: 192.168.1.10/62516 (209.165.201.10/62516)

From the outside PC open the command DOS and access the DMZ server using the FTP command, try to delete a file in the DMZ server, the attempt fails as shown by the following output:



Try to rename a file in the DMZ server, the attempt fails as shown by the following output:



Access ASA to see the log message displayed:

Latest	Latest ASDM Syslog Messages										
Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destin	Description			
<u>i</u> 6	Dec 13 2015	06:47:41	302014	209.165.200.30	49896	192, 168, 1, 10	21	Teardown TCP connection 3728 for outside: 209. 165. 200. 30/49896 to DMZ: 192. 168. 1. 10/21 duration 0:00:59 bytes 362 Flow closed by inspection			
<u>A</u> 4	Dec 13 2015	06:47:41	507003	209.165.200.30	49896	192, 168, 1, 10	21	tcp flow from outside: 209. 165. 200. 30/49896 to DMZ: 192. 168. 1. 10/21 terminated by inspection engine, reason - inspector reset unconditionally.			
<u>k</u> 5	Dec 13 2015	06:47:41	303005	209.165.200.30	49896	192, 168, 1, 10	21	Strict FTP inspection matched request-command appe cdup help rnfr rnto put stou site dele mkd rmd in policy-map FTP-POLICY, Reset connection from outside:209.			
<u>k</u> 6	Dec 13 2015	06:47:05	110002	209.165.200.30	49898			Failed to locate egress interface for TCP from outside:209.165.200.30/49898 to 80.254.145.118/80			

Finally verify the service policy using the show service-policy command:

ciscoasa(config	g-pmap-c)# show service-policy
Global policy:	
Service-poli	cv: global policy
Class-map:	inspection default
Inspect:	dns preset dns map, packet 0, drop 0, reset-drop 0
Inspect:	h323 h225 default h323 map, packet 0, drop 0, reset-drop 0
	tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect:	h323 ras default h323 map, packet 0, drop 0, reset-drop 0
Inspect:	rsh, packet 0, drop 0, reset-drop 0
Inspect:	rtsp, packet 0, drop 0, reset-drop 0
	tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect:	esmtp default esmtp map, packet 0, drop 0, reset-drop 0
Inspect:	sglnet, packet 0, drop 0, reset-drop 0
Inspect:	skinny, packet 0, drop 0, reset-drop 0
1	tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect:	sunrpc, packet 0, drop 0, reset-drop 0
	tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect:	xdmcp, packet 0, drop 0, reset-drop 0
Inspect:	sip , packet 0, drop 0, reset-drop 0
-	tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect:	netbios, packet 0, drop 0, reset-drop 0
Inspect:	tftp, packet 0, drop 0, reset-drop 0
Inspect:	ip-options default ip options map, packet 0, drop 0, reset-drop 0
Inspect:	icmp, packet 0, drop 0, reset-drop 0
Class-map:	WEB-SERVER-PROTECTION
Inspect:	http HTTP-POLICY, packet 0, drop 0, reset-drop 0
Class-map:	FTP-PROTECTION
Inspect:	ftp strict FTP-POLICY, packet 477, drop 0, reset-drop 13
ciscoasa (confi	g-pmap-c)#

Network Security All-in-one WorkBook Firepower Threat Defense

Lab 2: FTD NAT Policy



Configure a static default route for internet access, under devices-Device Management, edit the managed device and go to routing section, click Add Route:

Overview	Analysis	Policies	Device	s Obje	ects AMP Int	elligence						Deploy	A 1	System	Help	▼ ad	min
Device Mana	agement	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates										
FTD-Tra	ining														Save	8 c	ancel
Cisco Firepowe	er Threat De	fense for	VMWare														
Device	Routing	Interfac	es Inli	ne Sets	DHCP												
OSPF															🔘 Add F	Route	-
OSPFv3 RIP			Netwo	rk	Inter	ace	Gateway	Т	unneled	м	letric	Tracked					
Þ 🣁 BGP			▼ IPv4	Routes													
 Static Ro 	oute																
Multica	ast Routing		▼ IPv6	Routes													E

In the interface field, use the logical name outside as the outgoing interface and select anyipv4, any-ipv4 is equivalent to 0.0.0.0/0, the Gateway is the next-hop router 192.0.2.2, and click OK:

Add Static Route Configuration

Type: Inter	ace*	outsid			×	1					
A	vailable Ne	twork	¢ 🔾		:	Selected N	etwork				
	Search					💂 any-ipv	4	6	1		
G	any-ipv4										
6	IPv4-Ber	hchmark-	Tests								
6	IPv4-Link	k-Local									
6	IPv4-Mul	ticast									
6	IPv4-Priv	/ate-10.0	0.0.8								
6	IPv4-Priv	/ate-172	.16.0.0-1								
-	IPv4-Priv	/ate-192	.168.0.0-								
4	IPv4-Priv	ate-All-F	RFC1918								
	Pv6-to-1	Pv4-Rela	ay-Anyca								
Caba	*										
Gate	way*	192.0	.2.2		*	U					
Metrie	C:	1				(1 - 254)					
Tunne	eled:	🔳 (Us	ed only for de	efault Route	e)						
Route	Tracking:				*	\odot					
								_			
							OK	Cance			
FTD-T Cisco Fire	raining power Threat De	fense for VI	۹Ware								
Device	Routing	Interfaces	5 Inline Sets	DHCP							
OSPF											
OSPF	v3		Network	In	terface		Gateway		Tunneled	Metric	Track
Þ 💋 BG	P		▼ IPv4 Routes								
 Static Mu 	c Route Iticast Routing		any-ipv4	ou	tside		192.0.2.2		false	1	
			▼ IPv6 Routes								

? ×

Under devices-NAT, create a new NAT policy named NAT-FTD, select the managed device you want to apply the NAT policy from the Available Devices to Selected Devices:

Overview Analysis	Policies	Devices Obj	jects AMP Intelli	gence		95.		Deploy	e ₁	System	Help 🔻	admin
Device Management	NAT V	PN V QoS	Platform Settings	FlexConfig	Certificates							
											🗿 New	Policy
NAT Policy				De	vice Type		Status					
		Т	here are no polici	es created	. Add a new	Firepower NAT Policy (or) Thr	eat Defense NAT Policy					

ime:	NAT-FTD			
scription:				
rgeted Device	S			
Select device Available De	es to which you want to evices	apply this policy.	Selected Devices	
🔍 Search b	by name or value		FTD-Training	8
FTD-Tr	raining			
		Add to Policy		
		- Foncy		

The NAT policy NAT-FTD is displayed, there are three sections, NAT Rules Before section 1, Auto NAT Rules section 2 and NAT Rules After section 3, FTD supports the same NAT configuration options as the Traditional Firewall ASA, so A NAT rule can be Auto-NAT or Manual NAT, Auto-NAT Rule also called object NAT is commonly used to provide PAT or Port Address Forwarding for inside networks, only the source IP address is translated, optionally, you can translate the source port, NAT Rules Before or Manual NAT is more specific, more flexible and more complex, This rule can match traffic based on source and destination IP address and port as well as source and destination port. This why FTD stores the Manual rule in the section 1 and Auto-NAT in section 2 when you use the show nat command. Note you can configure a Manual Rule after Auto-NAT or NAT Rules After, this the section 3.

In this scenario you will configure an Auto-NAT rule for the 192.168.133.0/26 inside network, so that the users can go to the internet using the IP address outside interface of the FTD, simply configure PAT.

Click Add Rule, in the NAT Rule, select Auto NAT Rule and Type Dynamic to provide Port Address Translation, you have an option to select static if you want your server to be reachable from internet, if you select static you configure static NAT.

N/ Ente	T-FTD er Description										Save	Cancel
Rule	25										Policy	Assignments
能Fi	ter by Device										0	Add Rule
						Original Packet			Translated Packet			
#	Direction	Туре	Source Interface 0	Destination Interface 0	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
• N	AT Rules Before											
▼ A	uto NAT Rules AT Rules After											

While on traditional ASA, you have to use nameif or the logical name in the NAT rules. On FTD, you need to use Security Zones. This is used for matching traffic.

Add NAT Rule

NAT Rule: Type:	Auto NAT Rule	▼ ▼ I Enabl	e			
Interface Objects	Translation PAT I	Pool Advanced				
Available Interface	Objects 🖒		Source Interface Objects (1)		Destination Interface Objects (1)	
Search by name		Add to Source Add to Destination	្ឋូវីភ្លុំ zone_inside	Ĩ	The sone outside	
					ок с	ancel

Translation has two sections. One is Original Packet, which is the conditions to match. The other is Translated Packet, here you see the Translated Source, this is how to translate the original source of the packet. The original packet is also called the Real Address. The Translated Source may be the IP of the egress interface or an object. For example the IP egress interface is the outside IP address of the FTD 192.0.2.1.

Add NAT Rule							? >
NAT Rule:	Auto NAT	Rule 💙					
Type:	Dynamic	~]	e			
Interface Objects	Translation	PAT Pool	Advanced				
Original Packet					Translated Packet		
Original Source:*				× ()	Translated Source:	Address	×
Original Port:	TCP	~					¥ 0
					Translated Port:		
							OK Cancel

In the original Source create and add a Network Object for the inside network 192.168.133.0/26:

? ×

Add NAT Rule								? ×
NAT Rule:	Auto NAT	Rule	•					
Туре:	Dynamic		▼ ☑ Enable		New Network	Objects	? ×	
Interface Objects	Translation	PAT Pool	Advanced		Name:	PAT-INSIDE		
Original Packet					Description:			
Original Source:*				~ O				*
Original Ports		~			Network:	192.168.133.0/26	_	~ O
Original Port.						Format: ipaddr or ipaddr/le	en or	
					Allow Overrides:			
						Save Ca	ncel	
							0	K Cancel

For Translated Source, choose Destination Interface IP and click Save :

Ac	Id NAT R	ule										? ×
N	AT Rule:		Auto N	AT Rule	~							
T	ine.		Dunan			2						
	ype.		Dynam	IC	Enab	le						
In	terface Obj	ects	Translatio	n PAT Po	ool Advanced							
	riginal Pa	cket					Translated	Packet				
0	Driginal Sou	rce:*	PAT	-INSIDE		v ()	Translated S	ource:	Destination Inte	rface IP	~	
0	Original Por	t:	тс	p v					The values sele Interface Object tab will be used	cted for Destin ts in 'Interface	ation Objects'	
							Translated P	ort:				
										OK	Cane	
										UK	Canc	ei
												O (
NA Enter	T-FTD Description										Save	Cance
Rule	5										Policy A	ssignment
and Filte	er by Device					Original Packet		_	Translated Packet			Add Rule
	Direction	Туре	Source	Destination	Original	Original	Original	Translated	Translated	Translated	Options	
			Interface 0	Interface 0	Sources	Destinations	Services	Sources	Destinations	Services		
• NA	T Rules Before											
▼ Au	to NAT Rules	Dun		- zone outride				Interface			Docufaire	28
* NA	T Pulas After	Dyn	20ne_inside	see zone_outside	FATTINGIDE			Threnace			Chstraise	ø 🗊

Deploy the NAT policy :



From CLI, verify the Auto-NAT configuration using the show run nat and the show run object commands:



From the Inside PC, ping the ip address 8.8.8.8, the ping should be successful:



Verify that the ICMP packets are translated using the show nat command, and verify the translate_hits counter increased:

Lab 8: Intrusion Prevention System IPS Policy Scenario 1



Variable sets represent commonly used values in the intrusion rules to identify source and destination IP addresses and ports. To find the Variable sets, navigate to **Objects > Object Management**. Click **Variable Sets** at the right, a default Variable Sets named **Default-Set** is pre-defined, Edit the Default-Set Variable Sets.

Overview Analysis Poli	cies Devices Objects	AMP Intelligence	Deploy 🧕 System Help 🕇 admin
Object Management Int	rusion Rules		
			Add Variable Set
Retwork	^ Name		Description
🥜 Port 🍓 Interface 🧩 Tunnel Zone 😡 Application Filters	Default-Set		This Variable Set is system-provided.
S VLAN Tag			
Time Range			
 Security Intelligence Network Lists and Feeds DNS Lists and Feeds UBL Lists and Feeds 			
Sinkhole	•		Displaying 1 - 1 of 1 rows < < Page 1 of 1 > >

Notice that the values **\$HOME_NET** and **\$EXTERNAL_NET**. These are variables. SNORT uses these variables to represent the protected and the unprotected networks. It's **best practice** to change these values to represent your network. You should create your own Variable Set or than modifying the default set. Edit **EXTERNAL_NET**.

Edit Variable Set Default-Set

Name:	Default-Set			
Description:	This Variable	e Set is system-provi	ided.	
				💿 Add
Variable N	lame	Туре	Value	
Customize	d Variables			
This catego	ory is empty			
Default Va	ariables			
AIM_SERVE	ERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6]	2 76
DNS_SERV	ERS	Network	HOME_NET	Ø76
EXTERNAL	NET	Network	any	Ø96
FILE_DATA	_PORTS	Port	[HTTP_PORTS, 143, 110]	Ø76
FTP_PORTS	;	Port	[21, 2100, 3535]	Ø76
GTP_PORTS	S	Port	[3386, 2123, 2152]	J 🕽 🖥
HOME_NET		Network	any	076
4			· · ·	
			Save	Cancel

From the Available Objects pane click (+) to create a new Network Object.

lame:	EXTERNAL_NET								
ype:	Network	~							
vailable I	Networks 🖒	0		Included	Networks (0)		Excluded Net	vorks (0)	
Search	by name or value			any			none		
any IPv4-P	rivate-All-RFC1918	^							
any-ip	v4								
any-ip	v6								
IPv4-B	Benchmark-Tests								
IPv4-L	ink-Local		Include						
IPv4-M	fulticast	1.00	C. malada						
IPv4-P	Private-10.0.0.0-8	- 11							
IPv4-P	rivate-172.16.0.0-12	- 11							
IPv4-P	rivate-192.168.0.0-16	- 11							
IPv6-I	Pv4-Mapped	- 11							
IPv6-L	ink-Local	- 11							
IPv6-P	rivate-Unique-Local-Addresses	- 11							
IPv6-to	o-IPv4-Relay-Anycast	- 11							
PAT-IN	ISIDE	-		Network	Enter an IP address	bbA	Network Ent	er an IP address	Add
In the Name field enter **Inside-Network**, in the Network field enter **192.168.133.0/24**, your internal network.

New Network	Objects ? >
Name:	Inside-Network
Description:	
Network:	192.168.133.0/26
Allow Overrides	Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)
Allow Overfides:	0
	Save Cancel

Click **Exclude**, the internal network **192.168.133.0/24** should not be considered as an unprotected network. Click **Save**.

t Varial	ble EXTERNAL_NET				?
Name:	EXTERNAL_NET				
Type:	Network	~			
vailable	Networks 🖒	\odot	Included Networks (0)	Excluded Networks (1)	
🔍 INSI		×	any	💭 Inside-Network	6
Inside					
PAT-IN	ISIDE				
			Network Enter an IP address	Add Network Enter an IP address	Add
				Save	Cancel

Edit HOME_NET.

Edit Variable Set Default-Set

iame:	Default-Set			
escription:	This Variable	Set is system-prov	ided.	
			You have unsaved changes	💿 Add
Variable N	ame	Туре	Value	
Customize	d Variables			
EXTERNAL_	NET	Network	!Inside-Network	Ø98
Default Va	riables			
AIM_SERVE	RS	Network	[64.12.31.136/32, 205.188.210.203/32, 6]	296
DNS_SERVE	ERS	Network	HOME_NET	026
FILE_DATA	PORTS	Port	[HTTP_PORTS, 143, 110]	/ 76
FTP_PORTS		Port	[21, 2100, 3535]	/ 76
GTP_PORTS		Port	[3386, 2123, 2152]	2 76
HOME_NET		Network	any	076
HTTP_PORT	s	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,]	2 36
0				E F

From the **Available Networks**, click **Inside-Network**, the network object you created earlier then click **Include**, your internal network should by you protected network. Click **Save**.

Edit Varia	ble HOME_NET									?
Name: Type:	HOME_NET Network	~								
Available	Networks 🖒	٢		Included	Networks (1)		Exclude	d Networks (0)	
🔍 net		×		🚍 Inside	e-Network	5	none			
S EXTER TELNE Truside	INAL_NET T_SERVERS -Network		Include Exclude							
				Network	Enter an IP address	Add	Network	Enter an IP	address	Add
								(Save	Cancel

Review the values **\$HOME_NET** and **\$EXTERNAL_NET** in the Default Variable Sets. Click Save.

? ×

Edit Variable Set Default-Set

Name:	Default-Set			
Description:	This Variable Set i	s system-provi	ded.	
			You have unsaved changes	bhA 💿
Variable N	lame	Туре	Value	
Customize	d Variables			*
EXTERNAL_	NET	Network	Inside-Network	/ 7
HOME_NET		Network	Inside-Network	Ø98
Default Va	riables			
AIM_SERVE	RS	Network	[64.12.31.136/32, 205.188.210.203/32, 6]	/ 76
DNS_SERVE	ERS	Network	HOME_NET	2 36
FILE_DATA	PORTS	Port	[HTTP_PORTS, 143, 110]	Ø76
FTP_PORTS		Port	[21, 2100, 3535]	Ø76
GTP_PORTS	5	Port	[3386, 2123, 2152]	Ø76
HTTP_PORT	s	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,]	Ø98 .
4				Þ
			Save	Cancel

Click **Yes** to confirm the changes.



Navigate to the intrusion policy by clicking **Policies** > **Access Control** > **Intrusion**. Create a policy by clicking **Create Policy**.

Name the policy **IPS-Policy**, and in the **Base Policy** field, choose Balanced **Security and Connectivity**.

Check the **Drop when Inline** check box. Note: if you uncheck this option, the FTD will act as an IDS. Click **Create Policy and Edit Policy**.

Overview Analysis Policies Devices Objects AMP Intel	ligence	Deploy 🍳 System Help 👻 admin v
Access Control > Intrusion Network Discovery Application Detect	ors Correlation Actions •	
	Impo	ort/Export Intrusion Rules Access Control Network Analysis Policy
These are as aslicing defined. Click Consta Deliny to graphs a policy		Compare Policies
There are no policies delined. Click create Policy to create a policy		
Create Intrusion Policy		? %
Policy Information		
Norra *		
Name *	TE2-Folicy	
Description		
Drop when Inline	✓	
Base Policy	Balanced Security and Connectivity V	
* Required	County Delliny County and Edits	alian Canaal
	Create Policy Create and Edit F	Policy Cancel
Overview Analysis Policies Devices Objects AMP Intel	ligence	Deploy 🔍 System Help 🔻 admin
Access Control > Intrusion Network Discovery Application Detect	ors Correlation Actions •	
Edit Policy		
	Loading policy	
	Finalize Rules	

The IPS policy is edited. Click the **Firepower Recommendations** option in the left panel of the window.

Overview Analysis Policies De Access Control + Intrusion Networ	vices Objects AMP Intelligence rk Discovery Application Detectors Correlation Actions •	Deploy	0	System	Help 🔻	admin v
Edit Policy: IPS-Policy						
Policy Information	Policy Information					< Back
Rules Firepower Recommendations Advanced Settings	Name IPS-Policy Description					
Policy Layers	Base Policy Balanced Security and Connectivity ▼ Image: The base policy is up to date (Rule Update 2016-11-29-001-vrt)			Ø	Manage B	ase Policy
	This policy has 8504 enabled rules → 71 rules generate events × 8433 rules drop and generate events				🥟 Mar	age Rules View View
	No recommendations have been generated. Click here to set up Firepower recommendations. Commit Changes Discard Changes					

Click the Generate and Use Recommendations button.

Overview Analysis Policies	Devices Objects AMP Intelligence	Deploy	🛕 System	Help 🔻 a	admin v
Edit Policy: IPS-Policy					
Policy Information	Firepower Recommended Rules Configuration				< Back
Rules	No recommendations have been generated.				
Firepower Recommendations	Include all differences between recommendations and rule states in policy reports				
Advanced Settings	Advanced Settings				
Policy Layers	Generate and Use Recommendations				
	Generate Recommendations				
Overview Analysis Policies Access Control + Intrusion Net Edit Policy: IPS-Policy	Devices Objects AMP Intelligence work Discovery Application Detectors Correlation Actions •	Deploy	▲ ₁ System	Help 🔻 i	admin 🧃
Policy Information	Firepower Recommended Rules Configuration				< Back
Rules	No recommendations have been generated.				
Firepower Recommendations	Include all differences between recommendations and rule states in policy reports				
Advanced Settings	Advanced Settings				
Policy Layers	Generate and Use Recommendations				
	Generate Recommendations				
	Setting Policy to Use Recommendations				

The system informs you with message that the recommendation generation process is Successful. Click ${\rm OK}.$



Overview Analysis Policies De	vices Objects AMP Intelligence	Deploy	0, Sy	stem Help v	admin v
Access Control > Intrusion Networ	k Discovery Application Detectors Correlation Actions •				
Edit Policy: IPS-Policy					
Policy Information	Firepower Recommended Rules Configuration				< Back
Rules	Firepower changed 30823 rule states for 4 hosts		🔍 v	iew Recommend	ed Changes
Firepower Recommendations	Set 4 rules to generate events Set 186 rules to dron and generate events				View
 Advanced Settings 	→ Set 30633 rules to disabled				S View
Policy Layers	Policy is using the recommendations. Click to change recommendations Last generated: 2019 Jul 9 08:52:47				
	Include all differences between recommendations and rule states in policy reports				
	Advanced Settings				
	Do Not Use Recommendations				
	Update Recommendations				

Click **Rule**, you will find a list of intrusion rules that are available on the system.

You can perform a Rule Filter if you want to search and filter an intrusion rule Locate the Rule that identifies an invalid ICMP reply packet.

Perform a string search, based on rule name. The one we are looking for here is undefined packet.

Click show details.



By default the state of the rule is **Disabled**.

There are three states which can be configured for a rule:

1. Generate Events: This option generates events when the rule matches the traffic.

2. Drop and Generate Events: This option generates events and drop traffic when the rule matches the traffic.

3. Disable: This option disables the rule.

Update that and change it to Generate Events.

Overview Analysis Policie	S Devices Objects AMP	Intelligence Deploy	🏮 \rm 🕘 System Help 👻 admin v
Edit Policy: IPS-Polic	Y	electors correlation Actions V	
Policy Information	Rules		< Back
Rules	Rule Configuration	Filter: ICMP reply	× ?
Firepower Recommendations	Rule Content	0 selected rules of 12	
Advanced Settings	Category	⇒ ▼ 0 • 0 • • •	Deline
	app-detect 4	Rule State Event Filtering Dynamic State Alerting Comments	Policy
Policy Layers	blacklist	GID SID Message 🔺	🔿 🕜 🔻 🖸 🔮 🖓
	browser-chrome	1 6128 MALWARE-BACKDOOR dkangel runtime detection - icmp echo reply client-to-server	\rightarrow \rightarrow \wedge
	browser-firefox	1 387 PROTOCOL-ICMP Address Mask Reply undefined code	→ → •
	browser-ie	Lide detaile	
	browser-other	Hue details	
	browser-plugins	(1:409) PROTOCOL-ICMP Echo Reply undefined code	- I I I I I I I I I I I I I I I I I I I
	browser-webkit	Summary This event is generated when a network best generates an ICMP Echo Deply with an invalid or	undefined ICMP Code
	content-replace	Summary This event is generated when a network nost generates an tone but hepry with an invalid of	undernied TCHP Code.
	evoleit kit	Rule State	
	file-executable		
	file-flash	Firepower Recommendation	
		Rule Overhead	
	Classifications	Thresholds (0)	O Add
	Microsoft Vulnerabilities		
	Microsoft Worms	Suppressions (0)	bbA 📀
	Platform Specific		
	Preprocessors	Upnamic State (0)	S Add
	Priority	Alerts (0)	Add SNMP Alert
	Rule Opdate		
Last login on Tuesday, 2019-07-09 at 05	:28:34 AM from 192.168.111.5		սիսիս

Under the State option, select Generate Events and click OK.

Set rule state for "PROTOCOL-ICMP Echo Reply undefined code" ? *

State	Disabled v			
			ОК	Cancel
Set rule s	state for "PROTOCOL-ICM	P Echo Reply	y undefined (code" ? ×
Charles				

State	Generate Events	v	
			ОК
Success		×	
Successful	lly set the rule state for 1 r	rule(s)	
		ОК	

The state now is set to Generate Events.

Overview Analysis Policies	S Devices Objects AMP	ntelligence Deploy	🛛 🌒 System Help 👻 admin v								
Edit Policy: IPS-Polic	Y	tectors Correlation Actions •									
Policy Information	Rules		< Back								
Rules	Rule Configuration	Filter: icon renk									
Firenower Decommendations	Rule Content	Rule Content									
C Advanced Settings	Category										
Advanced Settings	app-detect	Rule State Event Filtering Dynamic State Alerting Comments	Policy								
Policy Layers	blacklist	GID SID Message	⇒ 🌏 🔻 🖸 🕖 🗩								
	browser-chrome	1 6128 MALWARE-BACKDOOR dkangel runtime detection - icmp echo reply client-to-server									
	browser-firefox	1 387 PROTOCOL-ICMP Address Mask Reply undefined code	→ → .								
	browser-ie	Inde stands									
	browser-other	Hide details									
	browser-plugins browser-webkit	(1:409) PROTOCOL-ICMP Echo Reply undefined code									
	content-replace	Summary This event is generated when a network host generates an ICMP Echo Reply with an invalid or	undefined ICMP Code.								
	decoder	Generate Events									
	exploit-kit	Rule State Layer: My Changes									
	file-executable	Firepower Recommendation									
	file-flash	Rule Overhead									
	Classifications		Q								
	Microsoft Vulnerabilities	Thresholds (0)	Add 🔾								
	Microsoft Worms	Suppressions (0)	O Add								
	Platform Specific										
	Preprocessors	Dynamic State (0)	🔘 Add								
	Priority										
	Rule Update	Alerts (0)	Add SNMP Alert .								
			ىلىران								

You can display the documentation about this rule. Very useful to understand the role of the rule.

rule	alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"PROTOCOL-ICMP Echo Reply undefined code"; icode:>0; itype:0; metadata:ruleset community; classtype:misc-activity; sid:409; rev:10; gid:1;)
Summary	This event is generated when a network host generates an ICMP Echo Reply with an invalid or undefined ICMP Code.
Impact	Information-gathering. An ICMP Echo Reply message is sent in response to an ICMP Echo Request message. If the ICMP Echo Reply message reaches the requesting host it indicates that the replying host is alive. Most OS's (operating systems) will accept an ICMP Echo Reply message with an invalid or undefined ICMP code set as a valid ICMP Echo Reply.
Detailed Information	ICMP Type 0 Code 0 is the RFC defined messaging type for ICMP Echo Reply datagrams. This type of message is used to determine if a host is active on the network.
Attack Scenarios	Remote attackers my generate ICMP Echo Reply datagrams with invalid ICMP Codes in an attempt to cause faults in the applications or hosts generating ICMP Echo Requests.
Ease of Attack	Numerous tools and scripts can generate this type of ICMP datagram.
False Positives	None known

You can tune a rule with several options.

You can set thresholds that dictate how often an event is displayed, based on the number of occurrences.

Use the **Threshold option** to configure a count to be more than 3, within 10 seconds for an event to be generated.

Once the number of count has passed 3 then there will be one event generated within 10 seconds

Limit defines the maximum of events per time period that will be generated, if you want to limit, not seen too events within specific time frame.

If you choose threshold, then you will define a number of counts that need to happen within a

time period before an event is generated.

(1:409) PROTOCOL-ICMP Echo Reply undefined code

Summary	This event is generated when a network host generates an ICMP Echo Reply with an invalid or undefined ICMP Code.	
Rule State	➡ Generate Events Layer: My Changes	
Firepower Recommendation		
Rule Overhead	.	
 Thresholds (0) 		O Add
 Suppressions (0) 		O Add
Dynamic State (0)		O Add
Alerts (0)	Add	SNMP Alert

Under the Thresholds section, click Add and enter the following parameters :

Type : Both Tracked By : Source Count : 3 Seconds : 10

Click OK

Set Threshold for "PROTOCOL-ICMP Echo Reply undefined code" ? *

Туре	Both 🔻	
Track By	Source 🔻	
Count	3	
Seconds	10	
Click OK to co	omplete.	OK Cancel
Success	ж	

Success	~
Successfully set the threshold for 1 m	ule(s)
	ок

Dynamic state option, this is the system ability to track the rate of this event count and you can define if the rate of count exceeds a certain value, than you want to change the way the rule will react to the event. It to changes dynamically the Generate Event Action to Drop and Generate Event action based on Specific conditions such as Count of events

Track by rule, means regardless the source or the destination.

The Timeout define the period after which the rule state is reverted.

If the rate of the count of events 10 within 10 seconds is exceeded, FTD starts dropping packets.

In other words we start dropping packets for a timeout 10 seconds before returning to the originale state which is just Generate Event.

Θ	Thresholds (1)				
	Туре	Count	Seconds	Track By	
	Both	3	10	Source	🗒 Delete
ŧ	Suppressions (0)				O Add
⊟	Dynamic State (0)				Obh 🕲
	There are no dynamic s	tates for this rule			
ŧ	Alerts (0)				Add SNMP Alert
ŧ	Comments (0)				🔾 Add
ŧ	Documentation				

Under Dynamic State, click Add and enter the following parameters :

Tracked By : Rule Rate : 10 Count / : 10 Seconds New State : Drop and Generates Events Timeout : 10

Click OK

Add Rate-Based Rule State for "PROTOCOL-ICMP Echo Reply undefined code" ? *

Track By	Destination T		
Network			
Rate	Count /	Seconds	
New State	Drop and Generate Events 🔻		
Timeout			
		ОКС	ancel

Add Rate-Based Rule State for "PROTOCOL-ICMP Echo Reply undefined code" ? *

Track By	Rule 🔻		
Rate	10 Count / 10	Seconds	
New State	Drop and Generate Events 🔻		
Timeout	10		
		OK Cancel	

×

Click **OK** to complete.

Success

for 1 rule(s)
ОК

You should have the following output.

Overview Analysis Policies De Access Control > Intrusion Network	vices Objects AMP k Discovery Application I	Intel Detect	lligence tors C	orrelation	Actions 🔻			Deploy 01	System	Help 🔻	admin v
Edit Policy: IPS-Policy											
Policy Information	Rules										< Back
Rules	Rule Configuration		Filter: io	mp reply							× 7
Firepower Recommendations	Rule Content						1 selected rule of 12				
Advanced Settings	Category app-detect	⇒ Ru	• •	▼ ▼	⊙ ▼ Dynamic Sta	● ▼			Policy		٠
	blacklist browser-chrome		GID 1	SID 6128	Message A MALWARE-BA	CKDOOR dkangel runtime detect	tion - icmp echo reply client-to-server		⇒ 🧐 ⇒ ⇒	70	
	browser-tirefox browser-ie	Hic	1 de details	387	PROTOCOL-IC	MP Address Mask Reply undefine	ed code	K	→ → < [1 of 1 🕽	- ×
	browser-plugins		Туре	/	Count	Seconds	Track By				•
	content-replace		Both		3	10	Source	🗍 Delete			
	decoder	÷	Suppress	sions (0)							O Add
	exploit-kit file-executable	Θ	Dynamic	State (1)							🔾 Add
	file-flash	-	Track B	y Ne	etwork	Rate	New State	Timeout			
	Classifications		Rule			10 Count / 10 Seconds	Drop and Generate Events	10		🗒 Delete	
	Microsoft Vulnerabilities										
	Microsoft Worms	•	Alerts (0)						Add SNI	MP Alert
	Platform Specific	Đ	Commen	its (0)							🔾 Add
	Priority										
	Rule Update	•	Documer	ntation							

Under **My Changes**, you can view the modified rules. Now there is 1 rule with Generate Events.

Click **View** at the left to edit the rule.

Overview Analysis Policies Dev Access Control > Intrusion Network	evices Objects AMP Intelligence Deploy rk Discovery Application Detectors Correlation Actions •	. Ø, System Help v admin v								
Edit Policy: IPS-Policy										
Policy Information	Layer: My Changes < Back									
Rules Firepower Recommendations Advanced Settings	Name My Changes Description									
Policy Layers	Sharing Allow this layer to be used by other policies									
My Changes	Rules (1)	🥔 Manage Rules								
 Firepower Recommendations Balanced Security and Connectivity 	→ 1 rules generate events X 0 rules drop and generate events ⇒ 0 rules disabled	Stew View View								
	Specific Threat Detection © Enabled © Disabled Inherit									
	Intrusion Rule Thresholds Global Rule Thresholding © Enabled © Disabled Inherit									
	W External Responses									
	SNMP Alerting O Enabled O Disabled Inherit									
	Syslog Alerting O Enabled O Disabled Inherit									
	Color legend Above Below									
Overview Analysis Policies Detection Access Control ► Intrusion Network	evices Objects AMP Intelligence Deploy	. ● System Help v admin								
Edit Policy: IPS-Policy										
Policy Information	Rules - Layer: My Changes	< Back								
Rules	Rule Configuration / Filter: State: "Generate Events"	ж ?								
Firepower Recommendations	Rule Content 0 selected rules of 1									
Advanced Settings	$\begin{array}{c} \hline \text{Category} \\ \hline \text{app-detect} \\ \hline \end{array} \Rightarrow \mathbf{v} \overline{\mathbf{v}} \mathbf{v} \overline{\mathbf{v}} \mathbf{v} \overline{\mathbf{v}} \mathbf{v} \\ \hline \end{array}$	Layer: My Changes								
Policy Layers	Rule State Event Filtering Dynamic State Alerting Comments blacklist GID SID Message ▲	⇒ () 7 0 0 .								
My Changes	browser-chrome I 409 PROTOCOL-ICMP Echo Reply undefined code	⇒ ▼ 0								
Rules	browser-firefox									

I< < 1 of 1 > >I

O Add

🔾 Add 🗸

Delete

Click Policy Information in the left panel. From the Policy Information, click Commit Changes.

(1:409) PROTOCOL-ICMP Echo Reply undefined code

-

Count

3

Generate Events

Seconds

10

This event is generated when a network host generates an ICMP Echo Reply with an invalid or undefined ICMP Code

Track By

Source

Hide details Above Below

Firepower Recommendation

Туре

Suppressions (0)

Dynamic State (1)

Summary

Rule State

Rule Overhead

Both

Thresholds (1)

Firepower Recommendations

Balanced Security and Connectivity

browser-ie

browser-other

browser-plugins

browser-webkit content-replace

decoder

exploit-kit

file-flash

file-executable

Classifications

Platform Specific Preprocessors

rity

Rule Update

Microsoft Vulnerabilities

Microsoft Worms

Overview Analysis Policies De Access Control + Intrusion Networ	vices Objects AMP Intelligence	ce Correlation	Actions 🔻					(Deploy	0, S	rstem H	Help 🔻	admin
Edit Policy: IPS-Policy													
Policy Information	Policy Information												< Back
Rules Firepower Recommendations Advanced Settings	Name IPS-Policy Description												
 Policy Layers My Changes Rules 	Base Policy Balanced Security and C O The base policy is up to date (Rule Up	Connectivity 🔻	-001-vrt)								69 M	lanage B	ase Policy
Firepower Recommendations Balanced Security and Connectivity	This policy has 191 enabled rules ⇒ 5 rules generate events X 186 rules drop and generate events											🥜 Man	age Rules View View
	 Firepower changed 30823 rule state ⇒ Set 4 rules to generate events X Set 186 rules to drop and generate events ⇒ Set 30633 rules to disabled Policy is using the recommendations. Click t Last generated: 2019 Jul 9 08:52:47 	es for 4 hosts events to change recomm	nendations							۹, ۱	iew Recon	mmended	d Changes View View View
	This policy contains enabled preprocessor ru	ules. Please read ti	the rule documenta	tion to ensure the pre	Discard	have the cor Changes	rrect settings fo	r these rules					

Click **OK** to complete.

Description of Changes	? :

Committing...



Gathering All Objects

Overview Analysis Policies	Devices Objects AMP Intellige	nce	Deploy 0, System	Help 🔻 admin 🕯
Access Control > Intrusion Netv	vork Discovery Application Detectors	Correlation Actions •		
		1	Import/Export Intrusion Rules Access Control Net	work Analysis Policy
Intrusion Policy	Drop when Inline	Status	Last Modified	
IPS-Policy	Yes	<u>No access control policies use this policy</u> Policy not applied on any devices	2019-07-09 09:12:09 Modified by "admin"	8 🖓 🦉 6

Navigate to the **Policies > Access Control > Intrusion.** Edit the **FTD-ACP-Training** access control policy.

Ove	erview Analy	sis Policie	Devices	Objects A	MP Intellige	ence						De	eploy	9 ₁ Syste	em Help v	admin 1
Acc	ess Control 🕨 A	ccess Contr	ol Network D	Discovery A	Application Dete	ectors Cor	relation	Actions 🔻								
FT Enter	D-ACP-Tra	aining													ave Save	😢 Cancel
Prefi	Iter Policy: Defau	ult Prefilter Polio	æ		SSL Policy	: <u>SSL-FTD</u>			Ide	entity Policy: [None	T= D	nheritance	Settings	Policy Assi	gnments (1)
Ru	les Security I	Intelligence	HTTP Response	Advanced												
尙	Filter by Device								Show Rule	Conflicts 🥹	Add Category	Add Rule	Search F	Rules		5
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicatio	Source Po	Dest Ports	URLs	ISE/SGT Attributes	Action		<u>a</u> 🕁 🎩	
-	Mandatory - FTD	-ACP-Trainin) (1-1)													
1	Internet Access	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	Ū 🗈	A 🛍 📘	o 🥜 E
-	Default - FTD-AC	CP-Training (-)													
The	re are no rules in	this section. Ad	d Rule or Add Cate	egory												
De	ault Action	_	_	_	_	_	_	_	_	_	Intrusion Preven	tion: Balanced Se	curity and	Connectivit	у	👻 \$ 🧾

Click **Add Rule** to add a mandatory rule in the access control policy that will use the **IPS-Policy** intrusion policy.

Name the new Access Control Policy rule **DMZ Access**. Select the default **Allow** action so that the matching traffic can be inspected using an IPS policy. Insert this access control policy rule into the **Mandatory** section and above rule 1.

Under the Available Zones pane, select Zone_inside and click Add to Source. Select Zone_outside and click Add to Destination.

Add Ru	ile											?
Name	DMZ Access				🕑 Ena	bled	Insert	above rule		▼ 1		
Action	Allow			V 🗘 🖓	50							
Zone	Networks	VLAN Tags	🛆 Users	Applications	Ports	URLs	SGT/ISE Attribute	S	_	Inspection	Logging	Comments
Availab	le Zones 🖒				Source	Zones (1	L)		Destinatio	on Zones (1)		
🔍 Sear	rch by name				and zon	e_inside		6	zone_	dmz		6
and zone	e_dmz											
zone	e_inside											
zone	e_outside			Add to Source								
				Add to								
				Destination								
											Add	Cancel

Click the **Inspection** tab. In the Intrusion Policy drop-down box, choose the **IPS-Policy**.

Add Ru	ule											? ;
Name	DMZ Access	5				🕑 Ena	abled	Insert	above rule	¥ 1		
Action	Allow 🗸				r 🗊 🔽	t D						
Zone	es Netwo	rks	VLAN Tags	🔺 Users	Applications	Ports	URLs	SGT/ISE Attributes		Inspection	Logging	Comments
Intrusio	n Policy							Variable Set				
IPS-Po	licy						~	Default Set				× 6
None	-											•
											Add	Cancel

Click the **Logging** tab and enable **Log at Beginning of Connection** and **Log at End of Connection**. Leave the default of sending the events to the **Event Viewer**. Click **Add**.

dd Ru	ile										?
Name	DMZ Access				🕑 Ena	abled	Insert	above rule	¥ 1		
Action	Allow			💌 🤍 🗅 🖉	to 📘						
Zone	s Networks	VLAN Tags	🛆 Users	Applications	Ports	URLs	SGT/ISE Attributes	3	Inspection	Logging	Comment
Log a	at Beginning of Co	onnection									
Log a	at End of Connect	ion									
e Ever	nts:										
Log F	files										
end Co	nnection Events t	:0:									
Even	t Viewer										
Syslo	g Select a Syst	og Alert Configur	ation			× ()					
SNM	P Trap Select an	SNMP Alert Cor	figuration			~ (0				
										Add	Cancel

Click Save.

Ove	Dverview Analysis Policies Devices Objects AMP Intelligence Deploy 0, System Help + admin +														
Acc	ess Control > Access Cor	ntrol Net	work Discovery	Applicat	ion Detectors	Correlation	n Actions	•							
FT Enter	D-ACP-Training											You hav	e unsaved d	hanges 🔡 Save 🛛	🔀 Cancel
Prefi	Iter Policy: Default Prefilter F	Policy			s	SL Policy: Non	ie.			Iden	tity Policy: Nor	ne			
Ru	les Security Intelligence	HTTP Res	sponses Adv	anced								1	nheritance S	ettings 📑 Policy Assig	nments (1)
尙	Filter by Device								Show Rule Cor	nflicts 😡 🖸	Add Category	Add Rule	Search R	ules	3
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source P	Dest Ports	URLs	ISE/SGT Attributes	Action	U 🗅 🔒 🕁 🔳 🗸	•
-	Mandatory - FTD-ACP-Trair	ning (1-2)													
1	DMZ Access	🚠 zone_insid	de 🚠 zone_dmz	Any	Any	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	🤴 🗅 🔏 🖄 🚺	0 e
2	Internet Access	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	🛹 Allow	0 🖪 🖆 🗐 0	6
-	Default - FTD-ACP-Training	(-)													
The	re are no rules in this section.	Add Rule or A	dd Category												
De	fault Action									I	ntrusion Preventi	ion: Balanced Se	curity and C	onnectivity	× \$ 🗾
OV	erview Analysis Poli	cies Devi	res Ohierts		ntelligence							D	enlov 🛛	System Heln 💌	admin a
Acc	ess Control > Access Con	ntrol Net	work Discover	Applicat	ion Detectors	Correlatio	n Actions							1	
															Canaal
FI	D-ACP-Iraining													Save L	
Ente	r Description														
Prefi	Iter Policy: Default Prefilter F	Policy			5	SL Policy: Non	<u>ië</u>			Iden	tity Policy: Nor	ne			
												Te I	nheritance S	ettings 📑 Policy Assig	nments (1)
Ru	les Security Intelligence	e HTTP Res	sponses Adv	anced											
尙	Filter by Device							_	Show Rule Cor	nflicts 😡 🕓	Add Category	Add Rule	Search R	ules	3
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source P	Dest Ports	URLs	ISE/SGT Attributes	Action	U 🗅 🧏 🕁 🔳 🗸	
-	Mandatory - FTD-ACP-Train	ning (1-2)													
1	DMZ Access 🕼 zone_inside 🚠 zone_dmz Any														
2	Internet Access	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	0 🖪 🕾 🖉 0	0 E
-	Default - FTD-ACP-Training	ı (-)													
The	ere are no rules in this section.	Add Rule or A	dd Category												
De	fault Action									I	ntrusion Prevent	ion: Balanced Se	curity and C	onnectivity	¥ \$ 🗾

Deploy the Access Control Policy to the managed device.

Depl	oy Policies Version:2019-07-09 04:17 PM		? >
V	Device	Group	Current Version
	FTD-Training Nat Policy: NAT-FTD Access Control Policy: FTD-ACP-Training Image: State of the policy: DNS-policy Image: Intrusion Policy: IPS-Policy Image: Intrusion Policy: Balanced Security and Connectivity -File Policy: File-policy Image: Prefilter Policy: Default Prefilter Policy Image: Network Discovery Device Configuration (Details)		2019-07-09 03:22 PM
Salari	and devinence 1		
Selec	ed devices: 1		Deploy Cancel

Ove	erview Analysis Polic	cies Device	es Objects	AMP I	ntelligence		- THE	×1				D	eploy 🧯	Sys	tem H	elp v a	admin 🔻
Acc	ess Control > Access Con	trol Netw	ork Discovery	Applicat	ion Detectors	Correlation	Actions •	,									
FT Enter	D-ACP-Training														E Sa	ve	Cancel
Prefi	Iter Policy: Default Prefilter P	olicy			S	SL Policy: None	•			Ide	ntity Policy: Nor	e					
Ru	les Security Intelligence	HTTP Resp	onses Adva	anced								Te 1	inheritance S	ettings	📑 Poli	cy Assignn	nents (1)
尙	Filter by Device								Show Rule Cor	flicts 😡 (Add Category	Add Rule	Search R	ules			24
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source P	Dest Ports	URLs	ISE/SGT Attributes	Action		<u>,</u> 19. 1		
-	Mandatory - FTD-ACP-Train	ing (1-2)															
1	DMZ Access	🚓 zone_inside	🚓 zone_dmz	Any	Any	Any	Any	Any	Any	Any	Any	Any	🖋 Allow	1	0.81	0 🛄 💼	0 E
2	Internet Access	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Ū I) & t	0 🛄 💼	0 E
•	Default - FTD-ACP-Training	(-)															
The	re are no rules in this section.	Add Rule or Add	d Category														
Def	ault Action										Intrusion Preventi	on: Balanced Se	curity and C	onnecti	vity	*	\$ 🔳

From the Kali linux machine, execute the **nping** command to generate an invalid ICMP packet with code 1, choose the count value 11, this value is higher than the count value defined in the Dynamic State created earlier, the destination IP is the DMZ Server 192.168.10.90.

ات ا	
root@kali:-#	~
root@kali:-# sudo npingicmpicmp-type 0icmp-code 1 -c 11delay 0 192.168.10.90	
Starting Nping 0.7.60 (https://nmap.org/nping) at 2019-07-10 00:03 EDT	
SENT (0.0356s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=1] IP [ttl=64 id=190	049
iplen=28]	
SENT (0.0357s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=2] IP [ttl=64 id=190	049
iplen=28]	
SENT (0.0358s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=3] IP [ttl=64 id=190	049
iplen=28]	
SENT (0.0358s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=4] IP [ttl=64 id=190)49
iplen=28]	
SENT (0.0359s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=5] IP [ttl=64 id=190)49
iplen=28]	
SENT (0.0359s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=6] IP [ttl=64 id=190)49
iplen=28]	
SENT (0.0359s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=7] IP [ttl=64 id=190)49
iplen=28]	
SENT (0.0360s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=8] IP [ttl=64 id=190)49
iplen=28]	
SENT (0.0360s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=9] IP [ttl=64 id=190)49
iplen=28]	
SENT (0.0360s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=10] IP [tt=64 id=19	9049
iplen=28]	
SENT (0.0361s) ICMP [192.168.133.40 > 192.168.10.90 Echo reply (type=0/code=1) id=54815 seq=11] IP [ttl=64 id=19	049 -

From the FMC, navigate to the **Analysis > Intrusion > Events** page. Click **Table View of Events**. Your output should look similar to the one that is shown

Overview Analysis Po	Deploy	o s	ystem H	lelp 🔻	admin								
Context Explorer Connect	ions Intrusions Event	s Files v H	Hosts v Users	 Vulnerabilities • 	Correlation •	Custom •	Lookup 🔻	Search					
							Bookmark T	his Page Rep	oort Designer	Dashboard	View Book	marks	Search •
Events By Priority Drilldown of Event, Priority, an No Search Constraints (Edit Searc	and Classification ad Classification > Table View of か	(switch workflow) Events > Packets							2019-0)7-09 22:53	3:10 - 2019	<u>-07-10</u> E	00:05:54 Expanding
Message						▼ Priority		Classifica	tion		Co	unt	
PROTOCOL-ICMP Ed	to Reply undefined code (1:409:10	<u>)</u>				low		Misc Activit	ix.		1		
$ \langle \langle Page 1 of 1 \rangle \rangle $ Disp	playing row 1 of 1 rows												
View	Сору	Delete		Review	Downloa	ad Packets							
View All	Copy All	Delete A	All	Review All	Download	All Packets							

Analyze the following fields including Classification, Application Protocol, Application Risk,

Ingress Interface, Egress Interface, Intrusion Policy, Access Control Policy, Access Control Rule, and so on.

Notice the **Inline Result** field, which means that the packet is dropped.

Overview	Analysis Policies Devices Objects AMP Intelligence Deploy © System Help + admin context Evaluer Connections + Tutrusions + Evants Elles + Hests + Users + Vulnerabilities + Correlation + Custom + Lookun + Search Search Deploy System Help + admin															
Context Ex	xplorer Connect	ons • Intru	sions 🕨 Even	ts Files	 Hosts • 	Users 🔻	Vulnerabilities 🔻	Correla	ation • Cu	stom 🔻	Lookup 🔻	Search				
											Bookmark Th	nis Page R	eport Designer D	ashboard Vie	w Bookmark	s Search 🔻
Events By Priority and Classification (switch workflow) 2019-07-09 22:53:10 - 2019-07-10 00:07. Drildown of Event, Priority, and Classification > Table View of Events > Packets Expand • Search Constraints (Edit Search) Disabled Co Jump to • Expand															10 00:07:13 Expanding abled Colum	
Jump to.	Jump to • • Time × Priority × Impact × Inline × Source IP × Source × Destination × Destination × Source Port / × Destination Port / × SSL Status × VLAN															
	▼ <u>Time</u> ×	Priority ×	Impact ×	Inline × Result	Source IP ×	Count	e × <u>Destinati</u> ry <u>IP</u>	on × j	<u>Country</u>	<u>Sour</u> ICM	<u>rce Port /</u> X <u>P Type</u>	ICMP (ation Port / × Code	SSL Status	×	VLAN × ID
4 🗉	2019-07-10 00:05:0	<u>3 low</u>	2	¥	192.168.13	3.40	192.16	8.10.90		<u>0 (Ec</u>	ho Reply) / icmp	<u>1 / icm</u>	2	🔒 Unknowr	(Unknown)	Q
I< < Page	e 1 of 1 >> Disp	blaying row 1 of 1 i	rows													
	View	Сор	у		Delete		Review		Download Packe	ets)					
	View All	Сору	All		Delete All		Review All	Do	ownload All Pac	kets]					
Overview	Analysis Pol	icies Devices	Objects	AMP In	Itelligence	lisers •	Vulnerabilities -	Correla	tion • Cus	tom •		Search	Deploy	📀 Syste	m Help v	⁄ađmin v
Context Ex	connecti		ions • Event	S Files	Hosts V	Users V	vumerabilities •	Correla	uon • Cus	tom •	LOOKUP V	Search				
<u>x 100</u>	× Application × Risk	Business Relevance	Ingress Security 2	Zone S	gress × Security Zone	Device ×	Ingress × Interface	Egress Interfac	x <u>Intrus</u>	sion ×	Access Contr Policy	ol× A R	ccess Control X ule	Network	<u>Analysis Po</u>	<u>olicy</u> ×
	Medium	Medium	zone inside	2 20	one dmz	FTD-Trainin	g inside	dmz	IPS-Pol	icy	FTD-ACP-Train	ing DI	MZ Access	Balanced S	Security and	Connectivity

From the **Analysis > Intrusions > Events** page, click **Packets** to get detailed information about each event.

The Access Control Policy name, Access Control Rule name, Intrusion Policy name, Intrusion Policy Rule syntax and so on.

Network Security All-in-one WorkBook Web Security Appliance



Lab 2: Transparent mode with WCCP and Access Policies

Common approaches include the following:

WCCP: This is available on many network devices, including the Cisco ASA adaptive security appliances, Cisco IOS routers, and switches. When you specify a WCCP device, you need to configure additional settings on the appliance.

PBR: Routers can redirect HTTP and HTTPS traffic using PBR. However, PBR is implemented in software and therefore can be resource-sensitive.

Layer 4 or 7 Switches: You can use a Layer 4 or Layer 7 switch to redirect traffic to the Cisco WSA. When you specify a Layer 4 switch, you only need to specify that the appliance is connected to an Layer 4 switch when you configure the appliance. You do not need to configure anything else on the appliance.

Choose Network > Transparent Redirection.

() () () () () () () () () () (.168 🔎 👻 😵 E 🗟 🖒 <i>i</i> 🥝 c	isco Web Security Virtual	×				ft 7	₹ ¤
Fie	chier Edition Affich	age Favoris Outils ?						x	辭
	cisco Web Secu	S000V rity Virtual Appliance			м	(i) Log ly Favorite	gged in as: admin or es – Options – Se	n WSA.Cisco.com upport and Help 👻	
٨	Reporting	Web Security Manager	Security Services		Network	Syst	em Administration		
	My Reports			Ľ	Interfaces Transparent Redire Routes DNS	ction	N	o Changes Pending	8
	Attention — 🔺 Yo So >	ou can customize this "My Re ome modules are added for y Overview.	ports" page by adding ou by default. The Ov	er	High Availability Internal SMTP Relay	ý	eports.)m Monitor		
	System Overview				Upstream Proxy External DLP Serve	rs		(Ð
	Overview > Web Pro:	xy Traffic Characteristics		C	Certificate Manager	nent	ization		\boxtimes
		Average transactions per seco Average bandwidth (by Average response time (n Total cu	nd in past minute: 0 os) in past minute: 0 os) in past minute: 0 rrrent connections: 0		Identification Ser Authentication Identity Provider fo Identity Services Er	r vices r SaaS ngine	CPU: 53.5% RAM: 59.9% ging disk: 10.9%		
				Syst	em Status Details				
	Time Range: Day							c	2
	09 Jan 2017 08:00 t	0 10 Jan 2017 08:12 (GMT)							
	Overview > Total V	Web Proxy Activity	×	0	verview > Web P	roxy Sur	mmary		⊻ ,
http	os://192.168.1.254:8443/i	monitor/wsa_user_report#network		N	o data was found ir	n the sele	cted time range		>

Click Edit Device.

Choose **WCCP v2 Router** from the drop-down that transparently redirects traffic to the appliance.

					- 🗆 🗙
(←) (→) (←) https://192	.168 🔎 👻 😵 E 🗟 🖒 <i>@</i> C	isco Web Security Virtual	×		<u> </u>
Fichier Edition Affich	age Favoris Outils ?				× ₩-
ululu Cisco	S000V			Cogged in as: admin	on WSA.Cisco.com
CISCO Web Secu	rity Virtual Appliance			My Favorites 👻 Options 👻	Support and Help 👻
▲ Reporting	Web Security Manager	Security Services	Network	System Administration	
					No Changes Pending
Transparent	Redirection				
Transparent Redire	ection Device				
	Type:	VCCP v2 Router			E la Decision
					Edit Device
WCCP v2 Services					
Add Service					
No WCCP services a	re defined. WCCP routing will no	t be operational until servic	es are configured.		
Copyright © 2003-201	6 Cisco Systems, Inc. All rights res	erved. Privacy Statement			
<					>

Configuring WCCP Services

Under WCCPv2 Services, click Add Service and add the following. Service Profile Name: CCNPS Dynamic Service ID: 90 (This is the number used to define this policy and is the ID used by Cisco ASA to request the policy) Port Numbers: 80,443 (In this policy, redirect ports are HTTP and HTTPS) Router IP Addresses: 192.168.1.1 (ASA inside IP address)

		_ _	×
(→) (→) https://192.168 , ○ - ♥ E	Cisco Web Security Virtual	× 💼	★ ¤
Fichier Edition Affichage Favoris Outils ?		2	< # ▼
CISCO Web Security Virtual Appliance		(i) Logged in as: admin on WSA.Cisco.com My Favorites - Options - Support and Help	m T
Reporting Web Security Manager	Security Services	Network System Administration	
		No Changes Pendi	ng
Transparent Redirection			
Teansavent Redirection Device			
Тапуратент кентесцой речсе	WCCP v2 Router		
		Edit Device.	
WCCP v2 Services			
Add Service			
No WCCP services are defined. WCCP routing will	not be operational until servi	ces are configured.	
Copyright © 2003-2016 Cisco Systems, Inc. All rights r	eserved. Privacy Statement		
×			>
		_ =	×
	Cisco Web Security Virtual		> × ★ ☆
← → ← https://192.168 ♀ ▼ ⊗ E ≧ ♥ € Fichier Edition Affichage Favoris Outils ?	Cisco Web Security Virtual		> ★ ¤ < 闘•
← → ← https://192.168 Ϙ • ♥ E № ♥ Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service	Cisco Web Security Virtual		> ★ ☆ < 闘 +
← ← ← https://192.168 ♀ - ♀ E № ♂ Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error – Errors have occurred. Please see	Cisco Web Security Virtual	 ★ ()	× * ¤ < •
← → ← https://192.168 ♀ マ E ڲ ♂ Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error – Errors have occurred. Please see WCCP v2 Service	Cisco Web Security Virtual	• • • • • • • • • • • • • • • • •	> * ¤ < •
← ← ← https://192.168 ♀ マ ♀ E ֎ ♂ Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error – Errors have occurred. Please see WCCP v2 Service Service Profile Name:	Cisco Web Security Virtual below for details.	× • • • • • • • • • • • • • • • • • • •	× ★ ☆ < III ~
C Dettps://192.168 D * Q E Q C Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error — Errors have occurred. Please see WCCP v2 Service Service Profile Name: Service:	Cisco Web Security Virtual e below for details.	×	× * ¤ * ® *
Image: Service	Cisco Web Security Virtual below for details. CCNPS Standard service ID: Dynamic service ID:	x n x 0 web-cache (destination port 80) 90 1-255	× ★ ☆ × •
Image: Constraint of the second state of the second sta	Cisco Web Security Virtual e below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	×	× ☆ × ↔
Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error Errors have occurred. Please see WCCP v2 Service Service Profile Name: Service:	Cisco Web Security Virtual below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	x n n y 0 web-cache (destination port 80) 90 1-255 80,443 A port must be a number from 1 to 65535.	× ★ ☆ ≪ 翻▼
Control Contro Control Control Control Control Control Control Control Control Co	Cisco Web Security Virtual E below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	x	× ☆ ★ × ₩ ▼
Image: Service Service WCCP v2 Service WCCP v2 Service Service Profile Name: Service	Cisco Web Security Virtual e below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	x 1-255 80,443 A port must be a number from 1 to 65535. (up to 8 port numbers, separated by commas) Redirect based on destination port Redirect based on source port (return path)	× ↔ ↔
Control Contro Control Control Control Control Control Control Control Control Co	Cisco Web Security Virtual below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	x n x n 0 web-cache (destination port 80) 90 1-255 80,443 A port must be a number from 1 to 65535. (up to 8 port numbers, separated by commas) • Redirect based on destination port • Redirect based on source port (return path) For IP spoofing, define two services, one based on destination	× * \$\$ * \$\$ * \$\$ *
Image: Service Service WCCP v2 Service WCCP v2 Service Service Profile Name: Service	Cisco Web Security Virtual e below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	 x n n	× ☆ ☆ · · · · · · · · · · · · · · · · ·
Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error – Errors have occurred. Please see WCCP v2 Service Service Profile Name: Service:	Cisco Web Security Virtual below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	 x n x x	× ☆ ☆ · · · · · · · · · · · · · · · · ·
Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error – Errors have occurred. Please see WCCP v2 Service Service Profile Name: Service:	Cisco Web Security Virtual E below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	 × n n	× ☆ ☆
Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error – Errors have occurred. Please see WCCP v2 Service Service Profile Name: Service:	Cisco Web Security Virtual e below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers:	X A A D Web-cache (destination port 80) O U U U U U U U U U U U U	× ↔ ↔
Fichier Edition Affichage Favoris Outils ? Add WCCP v2 Service Error – Errors have occurred. Please see WCCP v2 Service Service Profile Name: Service: Router IP Addresses:	Cisco Web Security Virtual below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers: 192.168.1.1	X A A C C C C C C C C C C C	
Image: Service Service WCCP v2 Service Error — Errors have occurred. Please see WCCP v2 Service Service Profile Name: Service	Cisco Web Security Virtual E below for details. CCNPS Standard service ID: Dynamic service ID: Port numbers: 192.168.1.1	X A A O web-cache (destination port 80) 90 1-255 80,443 A port must be a number from 1 to 65535. (up to 8 port numbers, separated by commas) Redirect based on destination port Redirect based on source port (return path) For IP spoofing, define two services, one based on destination port and another based on source port (return path). C Load balance based on server address Applies only if more than one Web Security Appliance is in use.	

Submit and commit your changes.

	X
(←) (→) ((←) (→) ((←) (→) ((→) (→) (→) (→) (→) (→) (→) (→) (→) (→)	🔮 Cisco Web Security Virtual × 🗎 🕆 🌣
Fichier Edition Affichage Favoris Outils ?	× 📷-
Router IP Addresses:	192.168.1.1
	Enter either IPv4 or IPv6 addresses; IP address families may not be combined within a single service profile. Separate multiple entries with line breaks or commas.
Router Security:	Enable Security for Service
	Passphrase: The passphrase must be between 1 and 7 characters long.
	Confirm Passphrase:
Advanced:	Optional settings for customizing the behavior of the WCCP v2 Router.
Cancel	Submit Y

10 Centtps://19	92.168 🔎 👻 😵 E 🗟 🖒 <i></i>	Cisco Web Security Virtua	al × 🖸 Yahoo		in ★
hier Edition Affic	hage Favoris Outils ?				×
uluulu. Cisco	S000V			 Logged in as: admin 	on WSA.Cisco.com
CISCO Web Sec	curity Virtual Appliance			My Favorites 👻 Options 🐱	Support and Help $ eq$
Reporting	Web Security Manager	Security Services	Network	System Administration	
					Commit Changes »
Transparent	t Redirection				
Transparent Redir	rection Device				
	Туре:	WCCP v2 Router			
					Edit Device
MCCD via Comisso					
WCCP v2 Services Add Service					
WCCP v2 Services Add Service Service Profile Name	e Ser	vice ID R	outer IP Addresses	Ports	Delete

						– 🗆 🗙
(-) -> 🥑 https://192	2.168 🔎 👻 😵 E 🗟 🖒 <i>[6</i>] C	isco Web Security Virtual	× 🔿 Yahoo		<u> </u>
Fi	ichier Edition Affich	hage Favoris Outils ?				× ₩ -
ŀ	cisco Web Secu	S000V urity Virtual Appliance			 Logged in as: admin My Favorites - Options - 	on WSA.Cisco.com Support and Help -
A	Reporting	Web Security Manager	Security Services	Network	System Administration	
	Uncommitte	d Changes	not go into effect until you	commit them.		
	Comment (optional):				
	Cancel Abando	n Changes		nmit Changes		
<	Copyright © 2003-201	16 Cisco Systems, Inc. All rights rest	erved. Privacy Statement			>
(→ <u></u> https://192	2.168 🔎 👻 😵 E 🗟 🖒 <i>ё</i> с	isco Web Security Virtual	× 🔾 Yahoo		- □ × ↑ ★ ‡

Reporting	Web Security Manager	Security Service	s Network	System Adminis	stration	
					N	o Changes Pendi
	Dedination					
ransparen						
Success — Your	changes have been comm	itted.				
in-l'-						
Fransparent Redir	ection Device					
	-	Ween nn i				
	Туре	WCCP v2 Router				
	Туре	WCCP v2 Router				Edit Device
WCCP v2 Services	Туре	: WCCP v2 Router				Edit Device
WCCP v2 Services	Туре	: WCCP v2 Router	_	_		Edit Device
WCCP v2 Services Add Service Service Profile Nam	Type	WCCP v2 Router	Router IP Addresses	Po	orts	Edit Device
WCCP v2 Services Add Service Service Profile Nam CCNPS	e S	WCCP v2 Router	Router IP Addresses 192.168.1.1	Po 80	orts 0,443	Edit Device
WCCP v2 Services Add Service Service Profile Nam CCNPS	e S 9	WCCP v2 Router	Router IP Addresses 192.168.1.1	Po 80	orts 0,443	Edit Device
WCCP v2 Services Add Service Service Profile Nam CCNPS	Type e S gr	WCCP v2 Router	Router IP Addresses 192.168.1.1	Po 80	orts 0,443	Edit Device
WCCP v2 Services Add Service Service Profile Nam CCNPS	Type e S 91	WCCP v2 Router	Router IP Addresses 192.168.1.1	Po 80	orts 0,443	Edit Dev

Configure the WCCP v2 device to work with the Cisco WSA

Create an access-list of the traffic that needs to be redirected to WCCP. In the example, HTTP and HTTPS traffic from the subnet 192.168.1.0/24 will be subjected of WCCP redirection.

ciscoasa(config)#access-list REDIRECT permit tcp 192.168.1.0 255.255.255.0 any eq
80
ciscoasa(config)#access-list REDIRECT permit tcp 192.168.1.0 255.255.255.0 any eq
443

Create an access-list containing WCCP servers. In the example, access list contains WSA host.

ciscoasa(config)#access-list WSA permit ip host 192.168.1.254 any

Enable a WCCP service group and identifies the service to be redirected. Also defines which cache engines participate in the service group, and what traffic should be redirected to the cache engine.

The standard service is web-cache, which intercepts TCP ports 80 and 443 traffic and redirects that traffic to the cache engines, but you can identify a service number between 0 and 254 (90 in this example).

ciscoasa(config)# wccp 90 group-list WSA redirect-list REDIRECT

Identifies an interface and enables WCCP redirection on the interface. In the example HTTP and HTTPS traffic that enters the inside interface to a service group 90 is redirected.

ciscoasa(config)# wccp interface inside 90 redirect in

The final configuration of the Cisco ASA:

```
ciscoasa(config)#access-list REDIRECT permit tcp 192.168.1.0 255.255.255.0 any eq
80
ciscoasa(config)#access-list REDIRECT permit tcp 192.168.1.0 255.255.255.0 any eq
443
ciscoasa(config)#access-list WSA permit ip host 192.168.1.254 any
ciscoasa(config)# wccp 90 group-list WSA redirect-list REDIRECT
ciscoasa(config)# wccp interface inside 90 redirect in
```

To verify WCCP operation in the Cisco ASA Adaptive Security Appliance, use the **show** wccp command and observe the number for **Total Packets Redirected** counter.

```
ciscoasa# sh wccp
Global WCCP information:
Router information:
Router Identifier: 192.168.1.1
Protocol Version: 2.0
```

Service Identifier: 90	
Number of Cache Engines:	1
Number of routers:	1
Total Packets Redirected: 0	
Redirect access-list:	REDIRECT
Total Connections Denied Redirect:	0
Total Packets Unassigned:	1
Group access-list:	WSA
Total Messages Denied to Group:	0
Total Authentication failures:	0
Total Bypassed Packets Received:	0
ciscoasa#	

Initiate HTTP traffic from Client PC and observe the counter again, which should be increasing.

ciscoasa# sh wccp	
Global WCCP information:	
Router information:	
Router Identifier:	192.168.1.1
Protocol Version:	2.0
Service Identifier: 90	
Number of Cache Engines:	1
Number of routers:	1
Total Packets Redirected: 7080	
Redirect access-list:	REDIRECT
Total Connections Denied Redirect:	0
Total Packets Unassigned:	27
Group access-list:	WSA
Total Messages Denied to Group:	0
Total Authentication failures:	0
Total Bypassed Packets Received:	0
ciscoasa#	

The **sh wccp 90 view** command displays also if the redirection between the Cisco WSA and the Cisco ASA is successfull:

```
ciscoasa# sh wccp 90 view
    WCCP Routers Informed of:
192.168.1.1
    WCCP Cache Engines Visible:
192.168.1.254
    WCCP Cache Engines NOT Visible:
        -none-
    ciscoasa#
```

Configure an Identity named **Internal Network**, which will be required to use Basic authentication. The Identity named will be identified based on the IP subnet and by the HTTP or HTTPS protocol.

Choose Web Security Manager > Identification Profiles. Click Add Identification Profile link.



						-	×	
$(\leftarrow) $	← → @ https://192.168 ♀ ▼ ♀ E ≧ ♥ @ Cisco Web Security Virtual ×							
Fichier	Fichier Edition Affichage Favoris Outils ? 🛛 🗙 🎆							
ahal	Upgrade Available 🗧 Logged in as: admin on WSA.Cisco.com							
cisco	 Web Secu 	rity Virtual Appliance			My Favorites 👻 Op	tions 👻 Support and I	Help 🚽	
▲	Reporting	Web Security Manager	Security Services	Network	System Administ	ration		
						No Changes F	Pending	
Talas		- Duefilee						
Ider	itificatio	n Profiles						
Client	t / User Identi	ification Profiles						
Add	Identification I	Profile						
						End-Liser		
Order	Transaction (Criteria	Authentication / Identi	fication Decision		Acknowledgement	Delete	
	Global Iden	tification Profile	Exempt from Authentic	ation / User Identificati	on	Not Available		
Edit	Order							
					•			
				User Identification Meth	nod: 📥 Authentication	n 🛛 🔁 Transparent Ider	ntification	
Copyri	ght © 2003-201	6 Cisco Systems, Inc. All rights re	served. Privacy Statement					
							· ·	

The Enable Identification Profile box should be checked by default.

Enter the **Internal Network** as the name.

Under the **Membership Definition > Define Members by Subnet**: Enter **192.168.1.0/24** as the subnet.

Under **Membership Definition > Define Members by Protocol**: Leave the **HTTP/HTTPS** box checked.

		×
← → ② https://192.168 ♀ ▼ S E S C	Cisco Web Security Virtual ×	₹ 🌣
Fichier Edition Affichage Favoris Outils ?	x	# ▼
Client / User Identification Profile Settings		^
✓ Enable Identification Profile		
Name: ?	Internal Network (e.g. my IT Profile)	
Description:	$\widehat{}$	
Insert Above:	1 (Global Profile) V	
User Identification Method		
Identification and Authentication: ?	For additional options, define an authentication realm (see Network > Authentication) or enable ISE (see Network > Identity Services Engine).	
Membership Definition		
Membership is defined by any combination of the f	ollowing options. All criteria must be met for the policy to take effect.	
Define Members by Subnet:	(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)	
Define Members by Protocol:	HTTP/HTTPS HTTP/HTTPS Native FTP	
h Advanced	Define additional group membership griteria	
P Advanced	Denne additional group membersnip criteria.	
Cancel	Subm	it Č

Click **Submit** then **Commit** the changes. Choose **Web Security Manager > Identification Profiles** to verify the newly created identity.

Image: Security Virtual × Image: Security Virtual × Image: Security Virtual Appliance Image: Security Services Network Success - Settings have been saved. Image: Security Services Network Image: Security Service Authentication / Identification Decision End-User Image: Add Identification Profile Exempt from Authentication / User Identification Image: Global Identification Profile Image: Security Services Image: Security Securit		×								
Fichier Edition Affichage Favoris Outils ? X Image: Security Virtual Appliance Image: Imag	← → A ttps://192.168 P ▼ S E S C @ Cisco Web Security Virtual ×									
Image: Security Virtual Appliance Image: Security Services Network Support and Help - Image: Security Manager Security Services Network System Administration Image: Security Manager Authentication / Identification Decision End-User Acknowledgement Delete Image: Manager Image: Mathematication / Identification / User Identification Image: Mathematication / Identification /	Fichier E	Fichier Edition Affichage Favoris Outils ?								
CISCO Web Security Virtual Appliance My Favorites - Options - Support and Help - Reporting Web Security Manager Security Services Network System Administration Identification Profiles Commit Changes > Commit Changes > Success – Settings have been saved. End-User Add Identification Profile End-User Authentication / Identification Decision End-User Order Transaction Criteria Authentication / Identification Decision End-User Delete 1 Internal Network Exempt from Authentication / User Identification (global profile) Image: Content	ahal	(1) Upgrade Available ≽ Logged in as: admin on WSA.Cisco.com								
Reporting Web Security Manager Security Services Network System Administration Commit Changes > Identification Profiles Success — Settings have been saved. Client / User Identification Profiles Add Identification Profiles Add Identification Profile Fnd-User Order Transaction Criteria Authentication / Identification Decision End-User 1 Internal Network Exempt from Authentication / User Identification (global profile) Image: Client / User Identification Profile 6 Global Identification Profile Exempt from Authentication / User Identification Not Available Image: Client / User Identification	CISCO Web Security Virtual Appliance My Favorites - Options - Support and Help -									
Commit Changes > Identification Profiles Success – Settings have been saved. Client / User Identification Profiles Add Identification Profile End-User Order Transaction Criteria Authentication / Identification Decision End-User 1 Internal Network Exempt from Authentication / User Identification Iglobal profile) Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Colspan="2">Colspan="2">Colspan="2">Image: Colspan="2">Image: Colspan="2">Authentication / Identification Decision Image: Colspan="2">Image: Colspan="2" 1 Internal Network Exempt from Authentication / User Identification Not Available Image: Colspan="2" <t< td=""><th>A R</th><td>Reporting</td><td>Web Security Manager</td><td>Security Services</td><td>Network</td><td>System Administration</td><td>n</td><td></td></t<>	A R	Reporting	Web Security Manager	Security Services	Network	System Administration	n			
Identification Profiles Success – Settings have been saved. Client / User Identification Profiles Add Identification Profile Order Transaction Criteria Authentication / Identification Decision End-User Acknowledgement Delete 1 Internal Network Subnets: 192.168.1.0/24 Protocols: HTTP/HTTPS Exempt from Authentication / User Identification (global profile) Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Authentication / User Identification 1 Internal Network Subnets: 192.168.1.0/24 Protocols: HTTP/HTTPS Exempt from Authentication / User Identification (global profile) Image: Colspan="2">Image: Colspan="2" Image: Colspan="2" Imag							Commit Char	nges »		
Client / User Identification Profiles Add Identification Profile Order Transaction Criteria Authentication / Identification Decision End-User Acknowledgement Delete 1 Internal Network Subnets: 192.168.1.0/24 Protocols: HTTP/HTTPS Exempt from Authentication / User Identification (global profile) Image: Coloradia Col	Iden Succe	Identification Profiles Success – Settings have been saved.								
Order Transaction Criteria Authentication / Identification Decision End-User Acknowledgement Delete 1 Internal Network Subnets: 192.168.1.0/24 Protocols: HTTP/HTTPS Exempt from Authentication / User Identification (global profile) im Global Identification Profile Exempt from Authentication / User Identification Not Available Image: Content of the content	Client Add	/ User Identi Identification P	fication Profiles							
1 Internal Network Subnets: 192.168.1.0/24 Protocols: HTTP/HTTPS Exempt from Authentication / User Identification (global profile) Image: Comparison of the	Order	Transaction C	Criteria	Authentication / Identif	ication Decision	End Ack	l-User nowledgement	Delete		
Global Identification Profile Exempt from Authentication / User Identification Not Available	1	Internal Net Subnets: 19 Protocols: H	twork 92.168.1.0/24 TTP/HTTPS	Exempt from Authentic	ation / User Identificatio	on (glo	bal profile)	ŵ		
Edit Order		Global Ident	tification Profile	Exempt from Authentic	ation / User Identificatio	on Not	Available			
Laconderm	Edit	Edit Order								
User Identification Method: 🐣 Authentication 눧 Transparent Identification										
Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. Privacy Statement	Copyrig									

chier E	dition Affichae	ge Favoris Outils ?	() ()	Ipgrade Available	Logged in as: admin	n on WSA.Cisco.co	x m
R	Leporting	Web Security Manager	Security Services	Network	System Administration		
						No Changes Pendi	ing
Iden	tification	Profiles					
Succe	ss — Your ch	anges have been committe	ed.				
Client	/ User Identifi	ication Profiles					
Add	Identification Pr	ofile					
Order	Transaction Cr	iteria	Authentication / Identific	cation Decision	End-Us Acknow	ser wledgement De	elete
1	Internal Netv Subnets: 19 Protocols: HT	Internal Network Subnets: 192.168.1.0/24 Protocols: HTTP/HTTPS					
	Global Identi	fication Profile	Exempt from Authentica	tion / User Identificatior	Not Av	ailable	
Edit (Order						
			U	Iser Identification Metho	d: 🖁 Authentication 🏻 🔓 T	ransparent Identifica	atio
	aht © 2003-2016	Cisco Systems, Inc. All rights res	served. Privacy Statement				
Copyrig	· ·						

Cisco WSA access Policies determine how to treat HTTP requests. There are five sets of access policy control settings:

Protocol and User Agents: This setting is for the port and protocol of the HTTP request (for example: block FTP over HTTP).

URL Filtering: For each custom and predefined URL category, a specific action can be specified.

Applications: You can block particular applications such as Yyahoo IM or WebEx, or classes of applications such as peer-to-peer. Also, you can impose bandwidth limits on certain type of media.

Web Reputation and Anti-Malware Filtering: Leverages Cisco expertise and database of web reputation and malware information.

From the Cisco WSA GUI, navigate to **Web Security Manager > Access Policies**.

						-	×
←)→	<mark>ể</mark> https:// 192.16	8 🔎 👻 😵 E 🗟 🖒 🏉 Cisco W	eb Security Virtual	×		1	ñ★ ☆
Fichier E	dition Affichage	e Favoris Outils ?					× 👬
راریالی cisco	• Cisco So Web Security	000V v Virtual Appliance	() U	pgrade Available	Logged in as: a My Favorites - Optio	admin on WSA.Cisco ons - Support and H	o.com Ielp 🚽
n R	eporting	Web Security Manager	ecurity Services	Network	System Administrat	tion	
Iden	tificatior	Authentication Identification Profiles SaaS Policies				No Changes P	ending
Succes Client	ss — Your c / User Identif	Web Policies Decryption Policies Routing Policies Access Policies Overall Bandwidth Limits		_	_	_	
Order	Transaction C	Data Transfer Policies Cisco Data Security	entication / Identific	ation Decision	E	nd-User cknowledgement	Delete
1	Internal Net Subnets: 19 Protocols: H1	Outbound Malware Scanning External Data Loss Prevention	pt from Authenticat	tion / User Identification) (c	global profile)	ŵ
	Global Ident	SOCKS Policies Custom Policy Elements	ipt from Authenticat	tion / User Identification	n N	lot Available	
Edit	Order	Custom URL Categories Define Time Ranges and Quotas				_	
		Bypass Settings L4 Traffic Monitor	U	ser Identification Method	d: Å Authentication	le Transparent Iden	tification
Copyrig	ht © 2003-2016 C	isco Systems, Inc. All rights reserved. o_security_manager/authentication/id	Privacy Statement				>

Click **Add Policy** and use these parameters: Use the **Policy Name** of **MY POLICY** Access Policy.

Under Policy Member Definition > Identifications Profiles and Users, choose Select One or More Identification Profiles from the drop down box.

Under **Identification Profile**, choose **Internal Network** from the drop down box. Recall the **Internal Network** identity was created previously.

R	reporting web Sec	curity Manager	Security Service	ces N	etwork Sy	No Char	nges Pendin
Acce	ess Policies						
Policie	25						
Add	Policy						
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delet
	Global Policy Identification Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enable	ed
Edit	Policy Order						
Copyrig	ght © 2003-2016 Cisco System	ns, Inc. All rights reserv	ed. Privacy State	ement			

			- • ×
< 🔿 🔁 https://192.168 🔎 👻 🗉 🖾 🖉 🥖	Cisco Web Security Virtual 🗙		<u>↑</u> ★ ☆
Fichier Edition Affichage Favoris Outils ?			× ₩ -
			No Changes Pending
Access Policy: Add Group			
Policy Settings			
✓ Enable Policy			
Policy Name: 🕐	MY POLICY (e.g. my IT policy)	Ç	
Description:		\sim	
Insert Above Policy:	1 (Global Policy) 🗸		
Delicy Mombas Definition			
Membership is defined by the combination of the f	ollowing options. All criteria must be m	et for the policy to take effect.	
Identification Profiles and Users:	Select One or More Identification Prof	iles 🗸 🧲	
	Identification Profile	Authorized Users and Groups	Add Identification Profile
	Internal Network	No authentication required	Ŵ
Advanced	Define additional group membership c	riteria.	
Cancel			Submit
<			>

Click **Submit** then **Commit** the changes.

							- 🗆	×
(←)→	葠 https://192.168 🔎 👻 💈 E 🖥	🗟 🖒 <i> is</i> co Web Secur	rity Virtual 🛛 🛛				ft 7	★ \$
Fichier E	Edition Affichage Favoris Outil	ls ?					x	*
ahal	L Cisco S000V		 Upgr 	adeAvailable 👒	Logged	in as: admin	on WSA.Cisco.com	n
cisco	Web Security Virtual Applianc	e			My Favorites 👻	Options 👻	Support and Help	
▲ R	Reporting Web Security M	1anager Security S	Services	Network	System Adm	inistration		
	· · · · · · · · · · · · · · · · · · ·					[□]	Commit Changes	»
Acce	ess Policies ass — The policy group "MY PC	DLICY" was added.						
Policie	25							
Add	Policy							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware	e and Reputation	Dele
1	MY POLICY Identification Profile: Internal Net All identified users	twork (global policy)	(global policy)	(global policy)	(global policy)	(global polic	y)	Ŵ
	Global Policy Identification Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputat Anti-Malware	tion: Enabled e Scanning: Enable	d
Edit	Policy Order							
Copyrig	ght © 2003-2016 Cisco Systems, Inc. /	All rights reserved. Privacy	Statement					

The Cisco WSA acceptable use controls include a range of filtering capabilities for downloaded web content. The two main areas of web usage controls are:

- Cisco Application Visibility.
- URL filters.

In the Cisco WSA GUI, choose **Web Security Manager > Web Policies > Access Policies**. Click the **(global)** link under **URL Filtering** for the **MY POLICY** access policy.

		_		_			×	
())	https://192.168 🔎 🔻 😵 E 🗟 🖒	<i>e</i> Cisco Web Secu	rity Virtual ×			fi 7	्र स्ट	
Fichier	Edition Affichage Favoris Outils ?					X	OFF T	
	() Upgrade Available S Logged in as: admin on WSA.Cisco.com							
cisc	• web Security virtual Appliance				Fly Fuvorices o			
^	Reporting Web Security Manage	er Security S	Services	Network	System Adm	inistration		
						No Changes Pending	5	
	D-lisis-							
ACC	ess Policies							
Succ	ess — Your changes have been com	mitted.						
Polici	les							
Ado	d Policy							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Dele	
1	MY POLICY Identification Profile: Internal Network All identified users	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	Ŵ	
	Global Policy Identification Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled		
Edit	Policy Order							
~ ~ ~			Chatamana					
Соруг	ight © 2003-2016 Cisco Systems, Inc. All righ	is reserved. Privacy	Statement					
<							>	

Block four predefined categories: Professional Networking, Social Networking, Streaming Audio and Streaming Video. Screen shot blocking **Professional NetworkingURL category** is shown below.
					-	□ ×
🗲 🕣 🧟 https://192.168 🔎 🔻 🙁 E 🗟 🖒 🎑 Cisco Web Security Virtual 🗴						⋔ ★ ¤
Fichier Edition Affichage Favoris Outils ?						× ₩-
Custom URL Category Filtering						~
No custom URL categories are defined. Add categories in the Web Security Manag	ger > Custom l	URL Catego	ries page.			
Predefined URL Category Filtering						- 10 C
These URL Categories are defined as group membership criteria. All other catego	ries are not ap	plicable for	this policy.			
	Use Override Global Settings					
	Global Settings	Block 3	Monitor ()	Warn ?	Quota-Based	Time-Ba:
Category	Select all	Select all	Select all	Select all	(Unavailable)	(Unavaila
					_	
	×				_	
Photo Search and Images	×					
	×					
Politics	×				-	
e Pornography	V				_	
V Professional Networking		\checkmark			-	
eal Estate	\checkmark				-	-
⊖ Reference	\checkmark				-	-
😝 Religion	\checkmark				-	-
😝 SaaS and B2B	\checkmark				-	-
😣 Safe for Kids	1				-	-
Canaal						~
						>

Screen shot blocking **Social Networking**, **Streaming Audio** and **Streaming Video**.**URL category** is shown below.

Fichier Edition Affichage Favoris Outils ? Ficeranica One Category Ficerany These URL Categories are defined as group membership criteria. All other categories a S	re not app Use Global	olicable for	this policy. Ov			× 👬
These URL Categories are defined as group membership criteria. All other categories a	Use Global	olicable for	this policy. Ov			
s	Use Global		Ov	i-l		
s	Global			erride Glob	al Settings	
	settings	Block	Monitor ()	Warn ?	Quota-Based	Time-Ba:
Category S	elect all	Select all	Select all	Select all	(Unavailable)	(Unavaila
↔ Search Engines and Portals	\checkmark				-	-
😝 Sex Education	<				-	-
😣 Shopping	1				-	-
Social Networking		\checkmark			-	-
● Social Science	1				-	_
😔 Society and Culture	1				_	_
⊖ Software Updates	1				-	_
⊖ Sports and Recreation	1				_	_
Streaming Audio		\checkmark			-	_
Streaming Video		\checkmark			-	_
😔 Tobacco	1				-	-
	i					

Click **Submit** then **Commit** the changes.

Navigate to **Web Security Manager > Access Policies** to verify changed settings for **URL filtering** of **MY POLICY** access policy.

							_ □	×
)))	실 https:// 192.1 0	58 🔎 🔻 😵 E 🗟 🖒	🥖 Cisco Web Secu	rity Virtual 🤉	<		†	* ¤
chier E	Edition Affichag	je Favoris Outils ?			anda Availabla	×	dia any adapta ao WCA Ciana ao	< 🎆
() CISCO	Cisco S Web Securit	000V vy Virtual Appliance			Jgrade Available	My Favorites	 Options - Support and Help 	÷
F	Reporting	Web Security Manage	er Security S	Services	Network	System Ac	Iministration	
							Commit Change	<mark>s »</mark>
Acce	ess Policie	25						
		<u> </u>						
Succe	ss — Setting	s have been saved.						
Policie	es							
Add	Policy							
Order	Group		Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delet
1	MY POLICY Identification P All identified us	Profile: Internal Network sers	(global policy)	Block: 4 Monitor: 75	(global policy)	(global policy)	(global policy)	Ŵ
	Global Policy	Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	
Edit	Policy Order						,	
								>
	6							×
	C https://192.1	p8) → 😵 E 🖾 C	😂 Cisco Web Secu	rity Virtual ⊃	K		n	X ¥ 7 [88]
				(i) U	ograde Available		ed in as: admin on WSA.Cisco.co	~ OFF
cisco	Web Securit	ty Virtual Appliance				My Favorites	 Options - Support and Help 	
F	Reporting	Web Security Manage	er Security f	Services	Network	System Ad	dministration	
				I			No Changes Pend	
A	oc Delicio	~						ng
ACCE	SS POlicie							ng
Succe								ng
Polici	ess — Your ch	anges have been com	mitted.					ng
Add	ess — Your ch	anges have been com	mitted.					ng
	ess — Your ch es Policy	anges have been com	mitted.		-	-	_	ng
Order	es – Your ch Policy Group	hanges have been com	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	ng]
Order 1	es — Your ch es Policy Group Identification F All identified u	ianges have been comi irofile: Internal Network sers	Protocols and User Agents (global policy)	URL Filtering Block: 4 Monitor: 75	Applications (global policy)	Objects (global policy)	Anti-Malware and Reputation (global policy)	ng) Delet

Network Security All-in-one Cisco ASA FTD WSA Umbrella VPN ISE Layer 2 Security All Right Reserved >

Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | Privacy Statement

<

The system Administration-Policy Trace tool allows you to test the the configured policy.

In the Cisco WSA GUI, choose **System Administration > Policy Trace**. Use these parameters:

URL: www.facebook.com Client IP Address: 192.168.1.10 Click the Find Policy Match link

					X
← → @ https://192	.168.1.254:8443/ 🔎 👻 😵 Erreur 🗟 🕻	🖉 🧉 Cisco Web Se	ecurity Virtual ×		↑ ★ 幕
Fichier Edition Affich	age Favoris Outils ?				× 🚟
Cisco Web Secu	S000V rity Virtual Appliance	① L	Jpgrade Available	Logged in as: admin on WS y Favorites - Options - Suppo	A.Cisco.com rt and Help 🚽
Reporting	Web Security Manager	Security Services	Network	System Administration	
My Reports	ou can customize this "My Reports ome modules are added for you b	" page by adding y default. The Ove	report modules from d erview page can be acc	Policy Trace Alerts Log Subscriptions Return Addresses SSL Configuration	nges Pending Printable PDF 곱
> System Overview	Overview.			Users Network Access	•
Overview > Web Prox	ty Traffic Characteristics Average transactions per second in p	ast minute: 0	Overview > System Res	System Time Time Zone Time Settings	
	Average bandwidth (bps) in p Average response time (ms) in p Total current c	ast minute: 0 ast minute: 0 connections: 17	Repoi	Configuration Configuration Summary Configuration File	
			System Status Details	Feature Key Settings Feature Keys	
Time Range: Day	✓ ● 11 Jan 2017 09:44 (GMT)			Upgrade and Updates Upgrade and Update Settings System Upgrade	•
Overview > Total V	Veb Proxy Activity		🛛 Overvie	System Setup	X Transactions
https://192.168.1.254:8443/i	monitor/wsa_user_report#system_admi	nistration			>

(→)	168.1.254:8443/ 🔎 👻 Erreu	r 🗟 🖒 🔏 Cisco Web Security Virtu:	al ×]		× ★ ☆
Fichier Edition Afficha	ge Favoris Outils ?					× <mark>‱</mark> ▼
vilivilio Cisco S cisco Web Securi	5000V ity Virtual Appliance	Upgrade Ava Upgrade Ava	ilable ⊗	Logged in as: admin o My Favorites - Options - S	on WSA.Cisco.com Support and Help —	^
Reporting	Web Security Manager	Security Services Ne	twork	System Administration		
					No Changes Pending	
Policy Trace						
Destination						
	URL:	www.facebook.com				
Transaction						٩.
	Client or User:	To represent a client by IP address, o address below.	:hoose "No a	uthentication or Identification"	' and enter the IP	
		Authentication / Identification:	No authen	tication or identification \checkmark		
		Client IP Address:	192.168.1	.10		
		User Name:				
▷ Advanced						
					Find Policy Mate	sh
Results						
<						>

You should see that test transaction to **www.facebook.com** is matched against **Internal Network** identity and **MY POLICY** access policy. Request is blocked based on **URL category**, because **MY POLICY** access policy blocks **Social Networking** URL category.



In the Cisco WSA GUI, choose **System Administration > Policy Trace**. Use these parameters:

URL: www.youtube.com Client IP Address: 192.168.1.10 Click the Find Policy Match link

	.168.1.254:8443/ 🔎 👻 Erreu	r 🗟 🖒 <i>ể</i> Cisco Web Security	Virtual ×]	 ^	× ★ ☆
Fichier Edition Affich	age Favoris Outils ?					× ‱▼
vilivili Cisco cisco Web Secu	S000V rrity Virtual Appliance	① Upgrad	e Available	Logged in as: admin o My Favorites - Options - S	on WSA.Cisco.com Support and Help 👻	^
A Reporting	Web Security Manager	Security Services	Network	System Administration		
					No Changes Pending	
Policy Trace						
Destination						
	URL:	www.youtube.com				
Transaction						
Tansaction	Client or User:	To represent a client by IP addr address below.	ess, choose "No	authentication or Identification"	and enter the IP	
		Authentication / Identificat	ion: No authe	ntication or identification \checkmark		
		Client IP Addr	ess: 192.168.1	1.10		
		User Na	me:			
▷ Advanced						
					Find Policy Mate	ch
Results						- 1
https://192.168.1.254:8443/	default					>

You should see that test transaction to **www.youtube.com** is matched against **Internal Network** identity and **MY POLICY** access policy. Request is blocked based on **URL category**, because **MY POLICY** access policy blocks **Streaming Video** URL category.



Test the URL filtering on the predefined URL categories:

From the Host PC, open a browser and connect via HTTP to **www.facebook.com**. The access should be blocked because the **Social Networking category** is blocked.

	- 🗆 🗙
(←)	↑ ★ ₽
Fichier Edition Affichage Favoris Outils ?	× ₩ -
This Page Cannot Be Displayed	
Based on your organization's access policies, access to this web site (http://www.facebook.com/) has been blocked because the web category "Social Networking" is not allowed.	
If you have questions, please contact your organization's network administrator and provide the codes shown below.	
Date: Tue, 10 Jan 2017 10:57:28 GMT Username: Source IP: 192.168.1.10 URL: GET http://www.facebook.com/ Category: Social Networking Reason: BLOCK-WEBCAT Notification: WEBCAT	

From the Host PC, open a browser and connect via HTTP to **www.myspace.com**. The access should be blocked because the **Social Networking category** is blocked.

	- 🗆 🗙
(←) ② http://www.myspace.com/ P ▼ ≥ C ② Notification: Policy: URL Fil ×	↑ ★ ☆
Fichier Edition Affichage Favoris Outils ?	x 🎇 -
This Page Cannot Be Displayed	
This Page Califiot Be Displayed	
Based on your organization's access policies, access to this web site (http://www.myspace.com/) has been blocked because the web category "Social Networking" is	
not allowed.	
If you have questions, please contact your organization's network administrator and provide the	
codes shown below.	
Date: Tue, 10 Jan 2017 10:53:35 GMT Username:	
Source IP: 192.168.1.10	
Category: Social Networking	

From the Host PC, open a browser and connect via HTTP to **www.twitter.com**. The access should be blocked because the **Social Networking category** is blocked.



From the Host PC, open a browser and connect via HTTP to **www.youtube.com**. The access should be blocked because the **Streaming Video category** is blocked.

	- 🗆 🗙
(←)	<u>↑</u> ★ ‡
Fichier Edition Affichage Favoris Outils ?	× ‱-
This Page Cannot Be Displayed	
Based on your organization's access policies, access to this web site (http://www.youtube.com/) has been blocked because the web category "Streaming Video" is not allowed.	
If you have questions, please contact your organization's network administrator and provide the codes shown below.	
Date: Tue, 10 Jan 2017 10:51:53 GMT Username: Source IP: 192.168.1.10 URL: GET http://www.youtube.com/ Category: Streaming Video Reason: BLOCK-WEBCAT Notification: WEBCAT	

From the Host PC, open a browser and connect via HTTP to **www.dailymotion.com**. The access should be blocked because the **Streaming Video category** is blocked.

	- 🗆 🗙
(() ② http://www.dailymotion.com/	↑ ★ ☆
Fichier Edition Affichage Favoris Outils ?	x 🎇 -
This Page Cannot Be Displayed	
Based on your organization's access policies, access to this web site	
(http://www.dailymotion.com/) has been blocked because the web category "Streaming Video"	
is not allowed.	
If you have questions, please contact your organization's network administrator and provide the codes shown below	
Date: Tue 40 Jap 2017 10:50:54 CMT	
Username:	
Source IP: 192.168.1.10	
Category: Streaming Video	
Noulication. WEDGAT	

From the Host PC, open a browser and connect via HTTP to **www.linkedin.com**. The access should be blocked because the **Professional Networking category** is blocked.

	- 🗆 🗙
(←) → Ø http://www.linkedin.com/ P - ≥ C Ø Notification: Policy: URL Fil ×	↑ ★ ₽
Fichier Edition Affichage Favoris Outils ?	× 🎇 -
This Page Cannot Be Displayed	
Based on your organization's access policies, access to this web site (http://www.linkedin.com/) has been blocked because the web category "Professional Networking" is not allowed.	
If you have questions, please contact your organization's network administrator and provide the codes shown below.	
Date: Tue, 10 Jan 2017 10:53:00 GMT	
Source IP: 192.168.1.10	
URL: GET http://www.linkedin.com/	
Reason: BLOCK-WEBCAT	
Notification. WEBGAT	

Verify blocked transactions in reports and web tracking messages: There are two reports of interest related to URL categories:

- **URL categories report:** This report gives composite information about which URL categories are being used and which URL categories are being blocked.
- **Users report:** This report gives detailed information about which URL categories have been visited or blocked for a particular user.

The URL category report is an example of many report types available for the web usage control functionality. These reports are printable in PDF format and can be exported in .csv format.

From the Cisco WSA GUI, choose **Reporting> Web Sites**. In the **Top Domains**: **Transactions Blocked chart**, you should see the blocked transaction different categories being blocked.

						- 🗆 🗙
(←) → (←) + <	😵 E 🗟 🖒 <i>[6]</i> Cisc	o Web Security Virtual	×			↑ ★ ¤
Fichier Edition Affichage Favoris	Outils ?					× 🚟 -
ululu Cisco S000V		 U 	Ipgrade Availabl	<mark>le ≈</mark> Logge	d in as: admin on WSA.	Cisco.com
CISCO Web Security Virtual A	ppliance			My Favorites	→ Options → Support a	and Help 🚽
Reporting Web Se	curity Manager	Security Services	Netwo	ork System	Administration	
> My Peports					No Chang	jes Pending
Overview						
Users					5- 5-	Printable PDF 🗗
Web Sites	nize this "My Repo	rts" page by adding	report modul	es from different rep	oorts.	
Application Visibility	are added for you	by default. The OV	erview page c	an be accessed from	Monitor	
Security						
Anti-Malware	actoristics		Quantian > E	ustom Resource Utiliza	tion	
Advanced Malware Protection	acteristics		Overview > 3	ystern Resource offizz	luon	
File Analysis	ctions per second in	past minute: 0			CPU: 75.6%	
Client Malware Risk	pandwidth (bps) in	past minute: 0			RAM: 73.7%	
Web Reputation Filters	Total current	connections: 7		Reporting / loggir	ng disk: 14.4%	_
L4 Traffic Monitor			System Status	s Details		
SOCKS Proxy			System Status	S Detdils		
Reports by User Location						
Reporting Services	~					•
Web Tracking	10:41 (GMT)					
System Capacity	:tivity			Overview > Web	Proxy Summary	×
Y	1#				%	Transactions
nttps://192.108.1.254:8443/monitor/wsa_	user_report#monitor					>

	50.1.254.04/3/ O - @ E	Rd Car we		1	– □ <mark>×</mark>
	56.1.204:8443/1 >> V	r 🖀 🖸 🖉 Cisco Web S	Security Virtual ×		ш X Ж
Fichier Edition Affichag	je Favoris Outils ?	0		-	X 🔐 🕇
ululu Cisco S	000V	(1)	Upgrade Available 👳	Logged in as: admin	n on WSA.Cisco.com
CISCO Web Securit	y Virtual Appliance			My Favorites - Options -	Support and Help -
Reporting	Web Security Manager	Security Services	Network	System Administration	
					No Changes Pending
Wab Sitas					
web Sites					😰 Printable PDF 🗗
Time Range: Day	~				
09 Jap 2017 11:00 to 1	10 Jap 2017 11:28 (CMT)				
09 Jan 2017 11:00 to 1	10 Jan 2017 11:38 (GMT)				
Top Domains: Total 1	Transactions	÷	Top Domains: Tran	sactions Blocked	•
104.192.108.	.134 146		twim	g.com 20	
360safe.	com 126		linkedi	n.com	
akamaized	.net 122		myspac	e.com	
cisco.	com 111		tacebo	bk.net 5	
adnxs.	com 56		twitte	sr.com	
Ding.	com 47		dailymotio	n.com	
taboola.	com 36		youtub	e.com 4	
msn.	com 35		209.170.9	7.237	
yahoo.	com 34		faceboo	K.com	
Ipi	31			t.co	
	0 100 2	00 300		0 10 20	30 40
	Transaction	ns		Transactio	ins

From the Cisco WSA GUI, choose **Reporting > URL Categories**. In the **Top URL Categories: Blocked and Warned Transactions chart**, you should see the blocked transaction different categories being blocked.

			- 🗆 🗙
(←) (→) (←) https://192.168 , (→) →	😵 E 🗟 🖒 🥖 Cisco Web Securit	y Virtual ×	↑★☆
Fichier Edition Affichage Favoris	s Outils ?		X X
CISCO Web Security Virtual A	ppliance		My Favorites - Options - Support and Help -
Reporting Web Se	ecurity Manager Security Se	ervices Network	System Administration
 My Reports Overview Users Web Sites URL Categories Application Visibility 	nize this "My Reports" page by are added for you by default.	vadding report modules i The Overview page can	No Changes Pending Printable PDF 🗗
Security			•
Anti-Malware Advanced Malware Protection	acteristics	🖂 Overview > Syste	m Resource Utilization
File Analysis AMP Verdict Updates Client Malware Risk Web Reputation Filters	ctions per second in past minute: bandwidth (bps) in past minute: sponse time (ms) in past minute: Total current connections:	0 0 310 7	CPU: 75.6%
L4 Traffic Monitor		System Status De	tails
Reports by User Location			
Reporting Services Web Tracking System Capacity Cuttor Catting https://192.168.1.254:8443/monitor/wsa	V 10:41 (GMT) tivity user_report#monitor	c	Iverview > Web Proxy Summary X % Transactions
			×
← → @ https://192.168.1.254:844	3/ 🎗 👻 😵 Erreur 🗟 🖒 <i>浸</i> Cisc	co Web Security Virtual 🗙	- □ × ↑ ★ ¤
Fichier Edition Affichage Favoris	3/ ⊅ → ♀ Erreur ≧ ⊄ 🧔 Cisc ; Outils ? () ()	co Web Security Virtual ×	- □ × ↑ ★ ☆ × - Logged in as: admin on WSA.Cisco.com My Favorites - Options - Support and Help -
Fichier Edition Affichage Favoris Cisco S000V Cisco Web Security Virtual Applia Reporting Web Securit	3/ D - O Erreur D C Cisc : Outils ? ince y Manager Security Service:	co Web Security Virtual ×) Upgrade Available s Network	
A market fichier Edition Affichage Favoris Fichier Edition Affichage Favoris Cisco S000V Cisco Web Security Virtual Applia Reporting Web Securit	3/ D - O Erreur D C Cisc Outils ? Ince y Manager Security Services	s Network	- □ × A
A market fichier Edition Affichage Favoris Fichier Edition Affichage Favoris Ilili. Cisco S000V Cisco Web Security Virtual Applia Reporting Web Securit URL Categories Time Papers Day	3/ D - O Erreur D C Cisc : Outils ? ince y Manager Security Services	s Network	
A fichier Edition Affichage Favoris Fichier Edition Affichage Favoris Cisco S000V Cisco Web Security Virtual Applia Reporting Web Securit URL Categories Time Range: Day 9 Jan 2017 11:00 to 10 Jan 2017 11:	3/ D - O Erreur D C Cisc 5 Outils ? ince y Manager Security Service: 01 (GMT)	co Web Security Virtual ×) Upgrade Available 😸 s Network	
A market fichier Edition Affichage Favoris Fichier Edition Affichage Favoris Ilili. Cisco S000V Cisco Web Security Virtual Applia Reporting Web Securit URL Categories Time Range: Day 09 Jan 2017 11:00 to 10 Jan 2017 11: Top URL Categories: Total Transact	3/ D - O Erreur D C Cisc : Outils ? mnce y Manager Security Services :01 (GMT) tions	co Web Security Virtual × Upgrade Available s Network	
Image: Day Og Jan 2017 11:00 to 10 Jan 2017 11: Top URL Categories: Total Transact Uncategorie Computers and Search Engines and Search Engines and Social Net Peer File	3/ D Cisc Outils ? Outils ? Manager Security Services Security Security Services Security Services Security Security Services Security Security Services Security Sec	s Network	
Image: Computers Image: Computer Advertia Image: Image: Computers Image: Computers Image: Computer Advertia Image: Image: Computer Advertia Image: Image: Image: Computer Advertia Image: Image: Image: Image: Computer Advertia Image: Image: Image: Image: Image: Image: Computer Advertia Image: Im	3/ D Cisc Cisc Cisc Cisc Cisc Cisc Cisc Cisc	co Web Security Virtual × Upgrade Available 😒 s Network Top U ransi	Logged in as: admin on WSA.Cisco.com My Favorites → Options → Support and Help → System Administration No Changes Pending RL Categories: Blocked and Warned Actions Social Networking 0 20 40 Transation

Block two additonals categories: Games, Sport and Recreation.

From the Host PC, open a browser and connect via HTTP to **www.skysports.com**. The access should be successful.



From the Host PC, open a browser and connect via HTTP to **www.aol.com**. Click in the Games link then in the Play Now link. The access should be successful.

<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	-	□ ×
Games on AOL.com: Free × +		
(i) Ž ≤ www.aol.com/games/?gm=1 C Q Search ★ i i	+	⋒ ≡
≡ games √		
	SE/	ARCH
Af0b		
Game of the Day		
Vegas World		
Play Now People are watching		
Trending in tech: Stay up to date with the latest on AOL video		
Watch Now		
EDITORS PICKS		
10x10!		
Word Champs		
GamePoint Bingo		×

In the Cisco WSA GUI, choose **Web Security Manager > Web Policies > Access Policies**. Click the **(global)** link under URL Filtering for the **MY POLICY** access policy. Partial screen shot blocking **Games category**.URL category is shown below.

<	curity Virtual	×				↑ ★	₽
Fichier Edition Affichage Favoris Outils ?						х	₩ ▼
Predefined URL Category Filtering							^
These URL Categories are defined as group membership criteria. All other categorie	es are not ap	plicable for	this policy.				
	Use		0	verride Glob	al Settings		
	Settings	Block 3	Monitor ()	Warn ?	Quota-Based	Time-Based	
Category	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)	
\varTheta Fashion	\checkmark				-	-	~
😝 File Transfer Services	\checkmark				-	-	
😝 Filter Avoidance	1				-	_	
\varTheta Finance	1				-	_	
😝 Freeware and Shareware	1				-	-	
😝 Gambling	1				-	_	
😢 Games		\checkmark			-	-	
😝 Government and Law	\checkmark				-	-	
😝 Hacking	\checkmark				-	_	
😝 Hate Speech	\checkmark				-	_	
😝 Health and Nutrition	\checkmark				-	-	
😝 Humor	1				-	_	_
Cancel					I	Subn	nit
Overall Web Activities Quota							
No time and volume quota has been defined. Define time and volume quota in Web	Security Ma	nager > De	fine Time R	anges and (Quotas.	>	

Partial screen shot blocking **Sport and Recreation category**.URL category is shown below.

< 🔿 🧭 https://192.168.1.254:8443/ 🔎 👻 🛿 Erreur 🗟 🖒 <i>@</i> Cisco Web Se	curity Virtual	×				† ★	₽
Fichier Edition Affichage Favoris Outils ?						x	₩ -
Predefined URL Category Filtering							
These URL Categories are defined as group membership criteria. All other categorie	s are not ap	plicable for	this policy.				
	Use		0\	verride Glob	al Settings		
	Settings	Block 3	Monitor ()	Warn ?	Quota-Based	Time-Based	
Category	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)	
⊖ Shopping	1				-	-	^
3 Social Networking		\checkmark			-	-	
\varTheta Social Science	\checkmark				-	-	
😝 Society and Culture	1				-	-	
\varTheta Software Updates	1				_	_	
Sports and Recreation		\checkmark			-	_	
🕴 Streaming Audio		1			-	_	
🕴 Streaming Video		1			-	_	
⊖ Tobacco	1				-	-	
\varTheta Transportation	1				-	-	
😝 Travel	1				-	_	~
Cancel Overall Web Activities Quota		1				Subn	nit
No time and volume quota has been defined. Define time and volume quota in Web	Security Ma	nager > De	efine Time R	anges and	Quotas.		~
<	, / //	y		3		>	

Click Submit then Commit the changes.

Navigate to **Web Security Manager > Access Policies** to verify changed settings for **URL filtering** of **MYPOLICY** access policy.

								×
(←)	🧉 https:// 192.168.1.254 :8443/ 🔎 👻 Er	reur 🗟 🖒 <i>i</i> Ci	isco Web Secu	rity Virtual 🗙			ĥ	* \$
Fichier E	dition Affichage Favoris Outils ?							× ‱▼
սիսի	▪ Cisco S000V		 U 	pgrade Available	≽ Logg	ed in as: admin	on WSA.Cisco.co	om
cisco	Web Security Virtual Appliance				My Favorites	→ Options →	Support and Help	
R R	eporting Web Security Manage	r Security S	Services	Network	System Ad	Iministration		
							No Changes Pend	ling
-								
Acce	ess Policies							
Succe	ss — Your changes have been com	mitted.						
Policie	25							
Add	Policy							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware ar	nd Reputation	Delete
1	MY POLICY Identification Profile: Internal Network All identified users	(global policy)	Block: 7 Monitor: 73	(global policy)	(global policy)	(global policy)		Ŵ
	Global Policy Identification Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputation Anti-Malware So	1: Enabled canning: Enabled	
Edit I	Policy Order							
<u> </u>								
Copyrig	gnt © 2003-2016 Cisco Systems, Inc. All right	ts reserved. Privacy	Statement					
1								,

From the Host PC, open a browser and connect via HTTP to **www.skysports.com**. The access should be blocked because the **Sport and Recreation category** is blocked.

	×
S Notification: Policy: URL F X +	
 () www.skysports.com () Q Search () () () () () () () () () ()	≡
	^
This Page Cannot Be Displayed	
Based on your organization's access policies, access to this web site (http://www.skysports.com/) has been blocked because the web category "Sports and Recreation" is not allowed.	
If you have questions, please contact your organization's network administrator and provide the codes shown below.	
	1
Date: Wed, 11 Jan 2017 10:59:11 GMT Username:	
Source IP2.168.1.10	
Category: Sports and Recreation	- 1
Reason: BLOCK-WEBCAT	
	~

From the Host PC, open a browser and connect via HTTP to **www.aol.com**. Try to access the games section. The access should be blocked because the **Games category** is blocked.

<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp 🗆	×
🖗 Notification: Gateway Tim 🗙 🕂	
 () www.aol.com/games/play/flowplay/vegas-wc () Q Search () () () () () () () () () ()	≡
	^
	1
This Page Cannot Be Displayed	
The system cannot communicate with the external server (www.aol.com). The Internet server may be busy, may be permanently down, or may be unreachable because of network problems.	
Please check the spelling of the Internet address entered. If it is correct, try this request later.	
If you have questions, please contact your organization's network administrator and provide the codes shown below.	
Date: Wed, 11 Jan 2017 10:24:32 GMT Username: Source IP: 192.168.1.10 URL: GET http://www.aol.com/games/play/flowplay/vegas-world/ Category: Search Engines and Portals Reason: UNKNOWN Notification: GATEWAY, TIMEOUT	
	~



Lab 6: Identification Profile and Access Policies

Create a new identification profile based on the AD Realm

Navigate to **Web Security Manager > Identification Profiles**. Select **Add Identification Profile**.

(ି ୯ ଜି	🔨 🔒 ht	tps:// 10.1.1.13 :8443/web_s	ecurity_manager/aut	hentication/identi	ties			⊠ ☆	2	Ł III\ Œ) ® ≡
)ı cı:	Cisco Web Sec	S000V urity Virtual Appliance						(i) Upgrade Ava	lable ⊗ l My Favorite	.ogged in as: adr s - Options -	nin on wsa. Support an	lab.local d Help 🔹
^	Reporting	Web Security Manager	Security Services	Network	System Adminis	stration						
											No Change	s Pending
Id	entificati	on Profiles										
Cl	ent / User Ide	ntification Profiles										
	Add Identification	Profile										
Or	der Transaction	Criteria	Authentication / Identific	ation Decision		End-User Acknowledgement	Delete					
	Global Ide	entification Profile	Exempt from Authentica	tion / User Identificatio	on	Not Available						
8												
			U	ser Identification Metho	od: Å Authenticatio	on 🍃 Transparent Ide	ntification					
Co	pyright © 2003-2	018 Cisco Systems, Inc. All rights	reserved. Privacy Statemer	ıt								

Use the following informations:

Name: Lab Profile

Under the User Identification Method section, in the Identification and Authentication field, select Authenticate Users option.

In the Authentication Realm field, select the AD1 Realm created previously, for the Select Scheme option, select Use Basic setting.

In the **Membership Definition** section, in the **Define Members by Subnet** section enter the inside **Network 10.1.1.0/24** as a criteria to apply the Identification Profile.

Click **Submit** and commit the configuration.

- C W	https://10.1.1.13:8443/web_security_manager/authentication/identities	··· 🖂 🕁	⊻ III\ 🗉 @
Cisco S000V Cisco Web Security Virtual Appliance		() Upgrade Available ≥ My Favo	Logged in as: admin on wsa.lab.local rites + Options + Support and Help +
Reporting Web Security Ma	nager Security Services Network System Administration		
			No Changes Pendin
Identification Profiles: A	dd Profile		
Client / User Identification Profile Set	nas		
Enable Identification Profile			
Na	ne: (?) Lab Profile		
Desc	(e.g. my IT Profile)	-	
Insert	Above: 1 (Global Profile) V		
User Identification Method			
Identification and Authenticat	on: () Authenticate Users		
Authentication	Api Api Select a Realm or Sequence: ① Lise Basic Select a Scheme If a user fails authentication: Support Guest privileges ⑦ Scheme setting applies to HTTP/HTTP's or	dy.	
	Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).		
Authentication Surroga	es: () 1P Address Persistent Cookie Session Cookie ® No Surrogate		
	If no surrogate is selected, re-authentication will not be available for Kerberos.		
) → C û	If no surrogate is selected, re-authentication will not be available for Kerberos.	© Å	
) → C ŵ 0 Insert	If no surrogate is selected, re-authentication will not be available for Kerberos.	ច ជ	÷ nv ⊡
)	If no surrogate is selected, re-authentication will not be available for Kerberos.	ច ជ	± ⊪/ ₪
	If no surrogate is selected, re-authentication will not be available for Kerberos. https://10.1.1.13:8443/web_security_manager/authentication/identities	© 1	± ₪\ ₪
C Insert User Identification Method Identification and Authentication Authentication	If no surrogate is selected, re-authentication will not be available for Kerberos. Image: https://10.1.1.13.8443/web_security_manager/authentication/identities Image: https://10.1.113.8443/web_security_manager/authentication/identities Image: https://10.1.113.8443/web_security_manager/authentimager/authenticatinget/authentication/identitinget/authentication	🖸 🏠	± ⊪. ⊡
	If no surrogate is selected, re-authentication will not be available for Kerberos. https://10.1.1.13/8443/web_security_manager/authentication/identities https://10.1.1.13/8443/web_security_manager/authentication/identities https://10.1.1.13/8443/web_security_manager/authentication/identities https://10.1.1.13/8443/web_security_manager/authentication/identities https://10.1.1.13/8443/web_security_manager/authentication/identities https://10.1.1.13/8443/web_security_manager/authentication/identities https://10.1.1.13/8443/web_security_manager/authentication https://10.1.11/8443/web_security_manager/authentication https://10.11/8443/web_security_manager/authentication https://10.11/8443/web_security_manager/authentication https:	ංං ල රූ 	. T IV []
C Insert Insert User Identification Method Identification and Authentication Authentication Authentication	If no surrogate is selected, re-authentication will not be available for Kerberos. Image: the selected is th	T	2 ± 11\ 10 (
C C Insert User Identification Method Identification and Authentication Authentication Authentication Surroga Membership Definition	If no surrogate is selected, re-authentication will not be available for Kerberos. Image: the selected of th	@ \$	2 ± lin. CD 4
	If no surrogate is selected, re-authentication will not be available for Kerberos. Image: https://10.11.13.8443/web_security_manager/authentication/identities Image: https://10.11.13.8443/web_security_manager/authentication Image: https://10.11.13.8443	@ \$	2 ± II\ CO
C O Insert User Identification Method Identification and Authentication Authentication Authentication Authentication Surroga Membership is defined by any combination Define Members by 5	If no surrogate is selected, re-authentication will not be available for Kerberos. Image: https://10.11.13.8443/web_security_manager/authentication/identities Image: https://10.11.13.8443/web_security_manager/authentication Image: https://10.11.13.8443/web_security_manager/authentication Image: https://10.11.13.8443/web_security_manager/authentication Image: https://10.11.13.8443/web_security_manager/authentication Image: https://10.11.0/24 Image: https://10.11.0/24	🖸 🏠	2 ± IA CO
C O Insert User Identification Method Identification and Authentication Authentication Authentication Authentication Surroga Membership Definition Membership Is defined by any combination Define Members by 5	If no surrogate is selected, re-authentication will not be available for Kerberos. Image: https://10.1.1.13/8443/web_security_manager/authentication/identities Image: https://10.1.1.13/8443/web_security_manager/authentication Image: https://10.1.1.1/10/14/10/11/10/14/10/14/10/11/10/14/10/14/10/11/10/14/10/11/10/14/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/14/10/11/10/11/10/14/10/11/10/11/10/14/10/11/10/1	🖂 🎝	2 ± 11\ 10 4
	If no surrogate is selected, re-authentication will not be available for Kerberos. Image: https://10.1.1.13.8443/web_security_manager/authentication/identities Image: https://10.1.1.13.8443/web_security_manager/authentication/identities Image: https://10.1.1.13.8443/web_security_manager/authentication/identities Image: https://10.1.1.13.8443/web_security_manager/authentication/identities Image: https://10.1.1.13.8443/web_security_manager/authentication/identities Image: https://10.1.1.13.8443/web_security_manager/authentication Image: https://10.1.1.13.8443/web_security_manager/authentication Image: https://10.1.1.1.8443/web_security_manager/authentication Image: https://10.1.1.1.8443/web_security_manager/authentication Image: https://10.1.1.1.8443/web_security_manager/authentication Select a Realm or Sequence: Image:	() A	2 <u>*</u> IA ()

→ C' û	🛡 🛍 ht	ttps://10.1.1.13:8443/web_security_manager/authentication	Videntities			🛛 🕁	-		
IIIIII Cisco S000\ ISCO Web Security Virtua	/ I Appliance				(i) Upgrade A	vailable ≽ l My Favorite	ogged in as: adm s • Options •	in on ws a Support a	i .lab.l nd He
Reporting Web	Security Manager	Security Services Network System	Administration						
								Commit	Chan
dentification Prof	files								
Narning — The policy grou	up "Lab Profile" wa	as added.							
Groups that do groups in the p authenticate, r	o not require autho policy table for effe regardless of policy	entication should typically be ordered above authentication ective evaluation. Changing this order may require users to y group settings.	i-based o						
lient / User Identification	Profiles								
Add Identification Profile									
rder Transaction Criteria		Authentication / Identification Decision	End-User Acknowledgement	Delete					
Lab Profile	4	Authenticate:	(alabal profile)						
Protocols: HTTP/HTTP	rs S	Realm: AD1 (Scheme: Basic)	(giobal profile)						
Global Identification	Profile	Exempt from Authentication / User Identification	Not Available						
Edit Order									
pyright © 2003-2018 Cisco S	ystems, Inc. All right	User Identification Method: 📥 Auth s reserved. Privacy Statement	entication b Transparent Id	entification					
ργright © 2003-2018 Cisco S → C ⁴ Ω	ystems, Inc. All right	User Identification Method: A Auth	entication 🏷 Transparent Id //dentities	entification		I \$\frac{1}{2}	Ŧ	III\ C	G
pyrright © 2003-2018 Cisco S → C ⁴ û 1.11.1. Cisco S000 SCO Web Security Virtua	ystems, Inc. All right	User Identification Method: A Auth	entication 🏷 Transparent 1d //dentilies	entification	() Upgrade Ava	・・・・・マー☆ alable さ Lo My Favorites	¥ gged in as: admin - Options - St	lill (II)	(ab.l I He
equive bedowning pyrright © 2003-2018 Case 5 → C ² ŵ +1[+. Cisco S000\ SCO Web Security Virtual Reporting Web	ystems, Inc. All right	User Identification Method: a reserved. Privacy Statement ttps://10.1.1.3.8443/web_security_manager/authentication Security Services Network System	entication Transparent 1d	entification	 Upgrade Ave 	···· 당 습 siable 등 Lo My Favorites	¥ gged in as: admin - Options - Si	III\	(ab.l I He
Autocolomia apyright © 2003-2018 Cases 5 C C Web Security Virtual Reporting Web	ystems, Inc. All right	User Identification Method: a reserved. Privacy Statement tps://10.1.1.13/8443/web_security_manager/authentication Security Services Network System	Administration	entification	① Upgrade Avi	···· ♡☆ My favorites	ygged in as: admin Options - St	III\ III I on wsa.l upport an o Changes	ab.li 1 Hel
Pyrright © 2003-2018 Cases 5 > C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C' C'	vstems, Inc. All right	User Identification Method: s reserved. Privacy Statement ttps://10.1.1.13:8443/web_security_manager/authentication Security Services Network System	Administration	entification	① Upgrade Avi	···· ♡ ☆ alable ːː Lo Hy Favorites	र्ष gged in as: admin - Options - St	III Con Wsa. upport and o Changes	ab.I I He
Pyright © 2003-2018 Caco S C C C C C C C C C C C C C C C C C C	vstems, Inc. All right	User Identification Method: s reserved. Privacy Statement ttps://10.1.1.3:8443/web_security_manager/authentication Security Services Network System ted.	entication Transparent Id	entification	() Upgrade Av	*** 단 ☆ My Favorites	yged in as: admin - Options - Se №	III\ C I on wsa.l upport and o Changes	ab.I 1 He
Appropriate © 2003-2018 Cases 5 C C C C C C C C C C C C C	ystems, Inc. All right	User Identification Method: s reserved. Privacy Statement ttps://10.1.1.3:8443/web_security_manager/authentication Security Services Network System ted.	entication Transparent Id	entification	() Upgrade Av	••• 단 ☆ alable = Lo Hy Favorites	पूर ggod in ass admin , Options - Si ार	III III I on Wsa. Upport and o Changes	ab.l I He
Appropriate © 2003-2018 Cases 5 C C C C C C C C C C C C C	ystems, Inc. All right	User Identification Method: s reserved. Privacy Statement ttps://10.1.1.3.8443/web_security_manager/authentication Security Services Network System ted.	entication Transparent 1d	entification	() Upgrade Av	*** 영 ☆ alable ː Lo Hy Favorites	لي good in as: admin • Options • Si ۲۵	III\ (on wsa. upport an o Changes	ab.I i He
Appright © 2003-2018 Cace 5 C C C C C C C C C C C C C C C C C C	vstems, Inc. All right vstems, Inc. All right Appliance Security Manager Files have been committ Profiles	User Identification Method: a reserved. Privacy Statement ttps://10.1.1.13.8443/web_security_manager/authentication ttps://10.1.1.13.8443/web_security_manager/authentication ted. ted. Authentication / Identification Decision	entication Transparent Id /identities Administration	Delete	() Upgrade Av	••• 영 ☆ alable ː Lo Hy Favorites	ygod in as: admin - Options - Si .7tr	III C	ab.l d He
	Appliance Security Manager Files Profiles	User Identification Method: a reserved. Privacy Statement tps://10.1.113.8443/web_security_manager/authentication tps://10.1.113.8443/web_security_manager/authentication security Services Network System ted. Authentication / Identification Decision Authenticate: Resim: AD1 (Scheme: Basic)	Administration	Delete	() Upgrade Av	••• ♥ ✿ Mable ≤ Lo My favorites	⊻ god in ss: admin - Options - Ss Tr	II CI WSA.	ab.k j He
avered added and a second added adde	vstems, Inc. All right vstems, Inc. All right Appliance Security Manager Files have been committl profiles 4 S Profile	User Identification Method: a reserved. Privacy Statement tps://10.1.113.8443/web_security_manager/authentication security Services Network Security Services Network System ted. ted. ted. ted. ted. ted. ted. ted.	Administration	Delete	() Upgrade Ave	••• ♥ ✿ slable = Lo My Favorites	للے ged in as: admin Options - Sta Ta	In an usal	ab.k
epyright © 2003-2018 Cases 5	ystems, Inc. All right Image: manual state Image: manual state Appliance Security Manager Files Herein state have been committee Security Manager Profiles Herein state Mark Security Manager	User Identification Method: a reserved. Privacy Statement tps://10.1.113.8443/web_security_manager/authentication security Services Network System ted. ted. ted. Authentication / Identification Decision Authentication Easier: Resim: ADI (Scheme: Basic) Exempt from Authentication / User Identification	Administration	Delete	() Upgrade Ava	••• ♥ ✿ alable ⊌ Lo My Favorites	للل ged in as: admin Optons - Si ه	III C	ab.lk tHel

Configure two access policies for two AD groups.

Navigate to **Web Security Manager > Access Policies**. Click **Add Policy**.

	Cisco S000V Web Security Virtual A	ppliance						() Upgrade Available S Logged in as: admin on wsa.lab. My Favorites • Options • Support and Hi
R	eporting Web Se	curity Manager	Security Servi	es N	etwork Sy	stem Administration		
								No Changes Pe
Acce	ss Policies							
Policie	5							
Add	Policy							
		Protocols and				Anti Maluma and Dan Antina		
Order	Group	User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete	
Order	Group Global Policy Identification Profile: All	User Agents No blocked items	URL Filtering Monitor: 87	Applications Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	Delete	

In the **Policy Name**, enter the name **Sales Policy**.

Under the Identification Profiles and Users, select the Identification Profile Lab Profile created previously. Choose Selected Groups and Users.

Click No groups entered.

Under the **Directory search completed**, select **LAB/Sales** group in the **AD1** Realm, select the **Add** button and click **Done**.

← → ♂ û	🛡 🔒 ht	tps:// 10.1.1.13 :8443/web_secu	urity_manager/pro	xy_security/policy_g	roups		F V t	y ⊤ II/ E ®,
CISCO Web Securit	000V ty Virtual Appliance						() Upgrade Available ≥ My Fa	Logged in as: admin on wsa.lab.local vorites • Options • Support and Help •
Reporting	Web Security Manager	Security Services	Network	System Administr	ation			
								No Changes Pending
Access Policy	: Add Group							
,						_		
Policy Settings						_		
Enable Policy	Policy Name:	Calue Balley						
	Toncy Hume.	(e.g. my IT policy)						
	Description:							
				.1				
	Insert Above Policy:	1 (Global Policy) >						
Policy Member Defini	ition							
Membership is define	ed by the combination of the	e following options. All criteria r	must be met for th	e policy to take effect				
	for the first of the second states of the second st							
Identi	incation profiles and Users:	Select One or More Identificati	on Profiles V			-		
		Identification Profile	Authorized Us	ers and Groups	Add Identification Profile			
		Lab Profile		icated Users				
			Groups: No	o groups entered	由			
			Users: No	users entered				
	Advanced	Define additional group memb	ership criteria.					
Cancel					Submit	it		
		Hne://101113:8443/web.com	urity manager/pr	www.security/policy.c	TOUDE			<u>ት</u> ዜነ መ ወ ¹
		aps// 10111113/0445/1105_300	unty_munuger/pre	sy_security/poincy_g	noups			
								No Changes Pending
Access Policie	es: Policy "Sales	Policy": Edit Grou	ips					
						_		
Authorized Groups								
Start typing a grou domain name (for i	p name into the Directory S instance, type "group" to fir	Search field to see matching ent nd "DOMAIN\Group1"). The sear	tries from the direc rch is case-insensiti	tory. For Active Direc ve. The wildcard char	tory groups, omit the acter "*" may be used.			
However, it cannot	be used as the last charact	er.	Authorized Crosse	liet Alkomakiyati	u ann huna tha antica			
name (for instance,	, to add a group that belong exist in the Authorized Grou	i press Add to add them to the gs to a trusted domain or a gro up list, the duplicates will be av	up that is not yet a	vailable in the directo	ory). If group(s) are			
	Case in the Authorized Gro	ap not, the ouphtates will be du	construiny onlitte	ar 1				
Realm: AD1								
Directory Search: (?))	Add >	elected Groups					
		nuu »	LAB\Sales		^			
Directory search com	npieted (48 matches).							
LAB\Performance	e Log Users e Monitor Users	^						
LAB\Pre-Window LAB\Print Operat	ors 2000 Compatible Access							
LAB\Protected Us LAB\RAS and IAS	sers S Servers							
LAB\RDS Endpoi LAB\RDS Manage	ement Servers							
LAB\RDS Remote LAB\Read-only D	e Access Servers Domain Controllers							
LAB\Remote Des LAB\Remote Man	agement Users				×			
LAB\Replicator	wied				Remove	J		
LAB\Screma Adri LAB\Server Oper	ators							
LAB\Terminal Ser	iver License Servers							
LAB\Windows Au LAB\WinRMRemo	utnorization Access Group oteWMIUsers	~						
Consul								
Cancel					Don	ne		

→ C w	🔍 🛍 https://10).1.1.13 :8443/we	eb_security_m	anager/proxy_secu	urity/policy_groups				P	© ଘ	⊻ ⊪\ ⊔
IIIIII Cisco S000V ISCO Web Security Virtual App	liance							6	Upgrade Available	 Logge My Favorites • 	d in as: admin on wsa.lat Options - Support and i
Reporting Web Secu	rity Manager S	ecurity Services	Netv	work Sys	stem Administration						
											No Changes P
Access Policy: Add Gi	roup						_				
Policy Settings											
Pol	licy Name: ⑦ Sales F	Policy		_			-				
	(e.g. m	ny IT policy)					-				
Insert	Above Policy: 1 (Glo	bal Policy) \vee			.11		-				
Policy Member Definition											
Membership is defined by the com	nbination of the followi	ing options. All c	riteria must be	e met for the policy	r to take effect.						
Identification Profile	es and Lisers' Coloct	One or More Ide	ntification Brof	loc vi			_				
	Identif	ication Profile	A	uthorized Users and	d Groups Add Iden	fication Profile					
	Lab Pr	ofile	~ 0	All Authenticated U	Users		-				
			۲	Selected Groups a	ind Users 🕐						
				Groups: Realm: AD1 LAB\Sales Users: No users er	ntered	숩					
				Groups: Realm: AD1 LAB\Sales Users: No users er	ntered	留					
	▶ Advanced Define	additional group	membership o	Groups: Realm: AD1 LAB\Sales Users: No users er	ntered	\$					
Cuncel → C ² D	Advanced Define	additional group 1.1.13:8443/web	<i>membership</i> o	Groups: Realm: AD1 LAB\Sales Users: No users er criteria.	ity/policy_groups	Submi			6	7 습	∓ nv ⊡ (
Gincel → C ⁴ @ Itulu: Cisco S000V	Advanced Define	additional group 1.1.13:8443/web	membership o o_security_mar	Groups: Realm: AD1 LAB/Sales Users: No users er criteria.	ity/policy_groups	Submit	ut	Ĵ	···· 연 Upgrade Available	기 슈 로 Logged	الله عنه admin on wealabJ
Cancel → C ⁴ @ IIIIIII Cisco S000V ISCO Web Security Virtual Appl	 Advanced Define Define https://10. 	additional group 1.1.13:8443/web	membership o p_security_mar	Groups: Realm: AD1 LAB/Sales Users: No users er rriteria.	ity/policy_groups	Submi		Ð	••• 😌	D ☆ ≥ Logged My Pavorites - 0	له الله الله الله الله الله الله الله ا
Cancel → C ⁴ @ IIIII Cisco S000V ISCO Web Security Vintual Appl Reporting Web Security	 Advanced Define : Advanced bitps://10. Nance Set Set Set Set Set Set Set Set Set Set	additional group 1.1.13:8443/web	membership o o_security_man Netwo	Groups: Realm: ADs LAB/Sales Users: No users en criteria.	ntered ity/policy_groups	Submi		0	••• 단 Upgrade Available	기 ☆ E Logged My Pavorites - O	ل اللہ اللہ اللہ اللہ اللہ اللہ اللہ ال
Cancel → C ² ⓓ IIIII Cisco S000V ISCO Web Security Vintual Appl Reporting Web Securi	Advanced Define : Advanced Define : ty Manager Se	additional group 1.1.13:8443/web cunty Services	membership o p_security_man Netwo	Groups: Caroline Control Contr	ntered ity/policy_groups em Administration	Subm		٥	••• ල Upgrade Available	2 슈 또 Logged My Favorites - O	ل الله الله الله الله الله الله الله ال
Cancel → C ² ② IIIII Cisco SO00V ISCO Web Security Vinual Appl Reporting Web Secur Access Policies	Advanced Define Advanced Define ty Manager Se	additional group 1.1.13:8443/web cunty Services	membership o security_man Netwo	rrk Syste	ntered ity/policy_groups am Administration	Subm		0	••• ල	2 ✿ Eogged My Favorites - O	له الله الله الله الله الله الله الله ا
Cancel → C ² Cisco S000V Isco Veb Security Vintual Appl Reporting Web Secur Access Policies Success – The policy group "Sci	Advanced Define : Advanced Define : Advanced Define : Advance Advance Se ales Policy" was addee	additional group 1.1,13:8443/web cunity Services 4.	membership o security_man Netwo	Groups: Criteria. Realms: Adds LAb/Sales criteria. Adds nager/proxy_securi ork Syste	ntered ity/policy_groups em Administration	Submi		0	••• ල	D ☆ Logged Hy Favorites - C	ل الله الله الله الله الله الله الله ال
Cancel → C*	Advanced Define	additional group 1.1.13:8443/web curity Services 4.	membership o o_security_man Netwo	Groups: Realms ADS LAQSAes criteria. nager/proxy_securi	ntered ity/policy_groups rm Administration	Subm		0	*** ල	D ☆ S Logged My Favorites - C	± In\ ⊡ 0 in as: admin on wsalabJ iptions - Support and He Commit Chang
Cancel → C ² Cisco S000V Isco Veb Security Virtual Appl Reporting Web Secur Access Policies Success – The policy group "Sc Policies Add Policy	Advanced Define Define Advanced Define The second secon	additional group 1.1.13:8443/web curity Services 4.	membership o p_security_man	Groups: Realms ADs LANSAes Users: No users er nager/proxy_securi nager/proxy_securi	ntered ity/policy_groups m Administration	Subm		0	*** ල	D ☆ S Logged My Favorites - C	⊥ In\ □ 0 In as: admin on wealabJ ptions - Support and He Commit Charg
Cancel Cancel	Advanced Define Advanced Define Advanced Define time time time	additional group 1.1.13:8443/web curity Services 4. URL Filtering celebal codes)	membership o o_security_man Netwo Applications	Croups:	ntered ity/policy_groups am Administration Anti-Malware and Reputat celebal celeva	Submi		0	••• 🖯	2 ☆ Eogged My Pavorites - O	y lin 0 In as: admin on wsalab liptions - Support and He Commit Chang
Cancel Ca	Advanced Define Advanced Define tance try Manager Se try Wanager Se try Goldan policy try (global policy)	additional group 1.1.13:8443/web cunity Services 4. URL Filtering (global policy)	membership o p_security_man Netwo Applications (global policy)	objects (global policy)	ntered	Submit		٥	+++ C	2 ☆ Logged My Pavorites - O	± IIN □ 0 In as: admin on weatabl liptions - Support and He Commit Chang
Cancel Ca	Advanced Define Advanced Define Advanced Define	additional group 1.1.13:8443/web curity Services 4. URL Filtering (global policy) Montor: 872	membership o p_security_man Netwo Applications (global policy) Montor; 356	Croups:)1 Reduting all of the second	Ity/policy_groups	Submit		0	+++ C	2 ☆ Logged My Pavorites - O	± IIN □ 0 In as: admin on weatabl ptions - Support and He Commit Chang

Click Add Policy.

In the Policy Name, enter the name Contractors Policy.

Under the **Identification Profiles and Users**, select the Identification Profile **Lab Profile** created previously. Choose **Selected Groups and Users**.

Click No groups entered.

Under the **Directory search completed**, select **LAB/Contractors** group in the **AD1** Realm, select the **Add** button and click **Done**.

← → ♂ ☆	🖲 🗞 http	ps:// 10.1.1.13 :8443/web_securi	ty_manager/proxy_security/policy_g	roups			¥ ⊪\ © ®
CISCO Web Security Virt	0V tual Appliance				0	Upgrade Available 😸 Logged I My Favorites - Op	n as: admin on wsa.lab.local tions - Support and Help -
Reporting W	Veb Security Manager	Security Services	Network System Administr	ation			
							No Changes Pending
Access Policy: Co	ontactors						
Policy Settings							
Enable Policy							
	Policy Name: ?	Contactors Policy					
	Description:	(e.g. my IT policy)			-		
	Incert Above Policy:	1 (Color Doline)	.:		-		
	Insert Above Policy.	1 (Sales Policy)					
Policy Member Definition							
Membership is defined by	the combination of the	following options. All criteria mu	ust be met for the policy to take effect	h.			
Identificati	on Profiles and Users:	Select One or More Identification	n Profiles 🗸				
		Identification Profile	Authorized Users and Groups	Add Identification Profile			
		Lab Profile v	O All Authenticated Users				
			Selected Groups and Users ? Groups: No groups entered	a			
			Users: No users entered				
	Advanced (Define additional group member	ship criteria.				
← → ♂ û	🖲 🛃 htt	ps:// 10.1.1.13 :8443/web_securi	ity_manager/proxy_security/policy_s	groups		▣ ⊍ ☆	¥ II\ ⊡ ®°
← → C [*] ŵ	🛛 🔒 htt	ps://10.1.1.13:8443/web_secur	ity_manager/proxy_security/policy_s Network System Administ	groups		2 🛛 🌣	No Changes Pending
← → C' ŵ A Reporting W Access Policies:	Keb Security Manager	ps://10.1.1.13.8443/web_secur Security Services	Ity_manager/proxy_security/policy_g Network System Administ	ration		D © \$	11 II C C
 ← → C[*] ŵ Reporting W Access Policies: Authorized Groups 	C A htt	ps://10.1.1.13.8443/web_secur Security Services ctors Policy": Edit (Ity_manager/proxy_security/policy_g Network System Administ Groups	roups		0 0 \$	⊻ II\ D @
 ← → C' ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar 	C A htt Web Security Manager Policy "Contain me into the Directory Se	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (Ity_manager/proxy_security/policy_g Network System Administ Groups es from the directory. For Active Direc	troups			⊻ II\ D @
 ← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar However, it cannot be w 	Let the security Manager Policy "Contact me into the Directory Se cos, type "group" to fing sed as the last character	security Services Security Services ctors Policy": Edit (arch field to see matching entrin "DOMAINGroup1"). The search	Ity_manager/proxy_security/policy_g Network System Administ Groups es from the directory. For Active Direc is case-insensitive. The wildcard char	tory groups, omit the acter "*" may be used.			보 IIN II @
← → C' ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar domain name (for instance be us New York and the start of th	known and a second black and and a second black and	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entri "DOMAINGroup 1"). The search is to a trusted domain or a group list, the duplicates will be also	Ity_manager/proxy_security/policy_c_ Network System Administ Groups es from the directory, For Active Direct is case-intensitive. The wildcard char uthorized Groups list. Alternatively, yo that is not yet available in the director matically omitted.	ration tory groups, omit the acter ** may be used. u can type the entire ny). If group(s) are		□ ··· ♥ ☆	L III C C
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar domain name (for instan however, it cannot be us Select items from the D Select items from the D Select items from the D Select items from the D	Manager Web Security Manager Policy "Contact me into the Directory Se one, type "group" to find group to fund de a group that belongs in the Authorized Group	ps://10.1.1.13:8443/web_securi Security Services ctors Policy": Edit (arch field to see matching entri "POMAIN(Group 1"). The search to a trusted domain or a group list, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory, For Active Direct is case-insensitive. The wildcard char uthorized Groups list. Alternatively, yo that is not yet available in the director matically omitted.	ration tary groups, onit the acter ** may be used. w can type the entire ny). If group(s) are		0 ··· © \$	⊻ In
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar domain name (for instance, to a added threes from the D Select items from the D Select items from the D Select items from the D	Antropy of the second sec	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entri t 'DOMALINGroup 1'). The search t, to a trusted domain or a group list, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory. For Active Direct is case-insensitive. The wildoard char uthorized Groups list. Alternatively. yo that is not yet available in the director matically omitted.	ration tary groups, onit the acter ** may be used. su can type the entire ny). If group(s) are		0 ··· © \$	⊻ In
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar domain name (for instance, to a added threas from the D) Select iters from the D) Select iters from the D) Select iters from the D) Directory Search: ⑦	Antropy of the second sec	ps://10.1.1.13:8443/web_secur Security Services Ctors Policy": Edit (arch field to see matching entri " "DOMALINGROUP 1"). The search to a trusted domain or a group list, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory. For Active Direct is case-insensitive. The wildcard char uthorized Groups list. Alternatively. yo that is not yet available in the director matically omitted.	ration tary groups, onit the actory groups, onit the actor ** may be used. su can type the entire ny). If group(s) are			1 IN C Changes Pending
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar domain name (for instance, to a name (for instance, to a naded theres from the D) Select iters from the D Select iters from the D Directory Search: ⑦ Directory search complete	Antropy of the second sec	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entri " "DOMAIN(Group 1"). The search to a trusted domain or a group list, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory, For Active Direct is case-insensitive. The wildoard char uthorized Groups list. Alternatively, yo that is not yet available in the director matically omitted. without Groups mr ADI LAb/Contractors	ration tary groups, onit the acter ** may be used. su can type the entire ny). If group(s) are			⊻ In
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar dromain narre (for infar howers, cannot be narre (for infarare, to a added that already east Realm: ADI Directory Search: ⑦ Directory search complete LABVAlministrators LABVAlministrators	Antropy of the second sec	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entri t "DOMALINGROUP!"). The server t, to a trusted domain or a group list, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory. For Active Direct is case-insensitive. The wildcard char uthorized Groups list. Alternatively. yo that is not yet available in the director matically omitted. Exceed Groups mr ADI LAB/Contractors	ration tary groups, onit the actory groups, onit the actor ** may be used. su can type the entire ny). If group(s) are			🛨 In 🖸 📽
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar domain name (for instart, top a group nar domain name), (for instart, top a deled that already cost for instart, to a deled that already cost added that already cost Realm: ADI Directory Search: ⑦ Directory search complete LAB\Administrators	A the security Manager Policy "Contact me into the Directory Se sech list and a group that belongs in the Authorized Group id (48 matches). sesword Replication Grou s	ps://10.1.1.13:8443/web_securi Security Services ctors Policy": Edit (arch field to see matching entri t "DOMAINGroup 1"). The search t, to a trusted domain or a group o list, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory, For Active Direct is case-insensitive. The wildcard char uthorized Groups list. Alternatively, yo that is not yet available in the director matically omitted. Exceed Groups in: ADI LAB/Contractors	ration tary groups, onit the acter ** may be used. u can type the entire ny). If group(s) are			1 IN C Changes Pending
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group nar domain name (for instart, for a domain name), for instart, for a domain name (for instart, for a domain name). Start typing a group nar domain name (for instart, for a domain name). Extension of the domain name (for instart, for a domain name). Directory Search: ⑦ Directory Search: ⑦ Directory search complete LAB/Administrators LAB/Admininteredomaint Administrators LAB/Administrators <td>A state of the second sec</td> <td>ps://10.1.1.13.8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entrin "POMAIM/Group 1"). The search press Add to add the matching or group list, the duplicates will be auto</td> <td>Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory, For Active Direct is case-insensitive. The wildoard char uthorized Groups list. Alternatively, yo that is not yet available in the director matically omitted. with the directory that is not yet available in the director matically contractors</td> <td>ration tary groups, onit the acter ** may be used. u can type the entire ny). If group(s) are</td> <td></td> <td></td> <td>🛨 M 🗈 📽</td>	A state of the second sec	ps://10.1.1.13.8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entrin "POMAIM/Group 1"). The search press Add to add the matching or group list, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory, For Active Direct is case-insensitive. The wildoard char uthorized Groups list. Alternatively, yo that is not yet available in the director matically omitted. with the directory that is not yet available in the director matically contractors	ration tary groups, onit the acter ** may be used. u can type the entire ny). If group(s) are			🛨 M 🗈 📽
← → C ŵ Reporting W Access Policies: Authorized Groups Start typing a group hard formating a group hard formating to a group hard formating. To a group hard formating, to a group hard formating hard for the group hard formating hard formating hard formating hard for the group hard for the group hard formating hard for the group hard for	A second se	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entrin " DOMAIN(Group 1"). The search " TOMAIN(Group 1"). The search " Tomain or g argue hist, the duplicates will be auto	Ity_manager/proxy_security/policy_c Network System Administ Groups es from the directory, For Active Direct is case-insensitive. The wildcard char uthorized Groups list. Alternatively, yo that is not yet available in the director matically omitted. Extend Groups in: ADI LAB/Contractors	ration tary groups, onit the acter ** may be used. u can type the entire ny). If group(s) are			🛨 In 🖸 📽
← → C ŵ Reporting W Access Policies: Acteass Policies: Start typing a group nar domain name (for instart, top a group nar domain name (for instart, top); a group nar domain name (for instart, top); a group nar down of the literary form the D name (for instart, top); a group nar down of the literary of	A second se	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (arch field to see matching entrin "DOMAIN(Group1"). The search press Add to add them to the At to a trusted domain or a group list, the duplicates will be auto	ity_manager/proxy_security/policy_g Network System Administ Groups es from the directory. For Active Direct is case-insensitive. The wildcard char authoraced Groups list. Alternatively, yo that is not yet available in the director matically omitted. eted Groups bm AD1 LAB/Contractors	ration tary groups, onit the acter ** may be used. u can type the entire ry). If group(s) are			⊥ IN I I I
← → C ŵ Reporting W Access Policies: Actess Policies: Start typing a group hard format name (for instart, top a group hard format name (for instart, top); a group hard forward, cannot be used to the already east disease to the start of the start	A second se	ps://10.1.1.13:8443/web_secur Security Services ctors Policy": Edit (march field to see matching entrin " DOMAIN(Group 1"). The search of the security of the search press Add to add them to the A press Add to add them to the A to a trusted domain or a group list, the duplicates will be auto	Ity_manager/proxy_security/policy_c	ration tary groups, onit the acter ** may be used. u can type the entire my). If group(s) are Remove			IN □ ■
← → C ŵ Reporting W Access Policies: Access Policies: Atthorized Groups Start typing a group nar domain name (for instar However, Ic cannot be added that already east Realm: ADI Directory Search: ? Directory Search: PLAB\Society Domain LAB\Society Polyton LAB\Society Polyton <td>Key Security Manager Policy "Contar re into the Directory Se contary Security Manager Policy "Contar re into the Directory Security re into the Directory Security reserve Security Security reserve Security controlers security reserve Security r</td> <td>security Services Security Services ctors Policy": Edit (arch field to see matching entrin "DOMAIN(Group!"). The search " press Add to add them to the A to a trusted domain or a group list, the duplicates will be auto Add a Sele</td> <td>ity_manager/proxy_security/policy_g Network System Administ Groups es from the directory. For Active Direc is case-insensitive. The wildcard char uthoraed Groups list. Afternatively, yo that is not yet available in the director matically omitted. exted Groups bix/DI LAB/Contractors</td> <td>ration tay groups, omit the acter ** may be used. u can type the entire my). If group(s) are</td> <td></td> <td></td> <td>业 IN □ ●</td>	Key Security Manager Policy "Contar re into the Directory Se contary Security Manager Policy "Contar re into the Directory Security re into the Directory Security reserve Security Security reserve Security controlers security reserve Security r	security Services Security Services ctors Policy": Edit (arch field to see matching entrin "DOMAIN(Group!"). The search " press Add to add them to the A to a trusted domain or a group list, the duplicates will be auto Add a Sele	ity_manager/proxy_security/policy_g Network System Administ Groups es from the directory. For Active Direc is case-insensitive. The wildcard char uthoraed Groups list. Afternatively, yo that is not yet available in the director matically omitted. exted Groups bix/DI LAB/Contractors	ration tay groups, omit the acter ** may be used. u can type the entire my). If group(s) are			业 IN □ ●
	A second se	security Services Security Services ctors Policy": Edit (arch field to see matching entrin "DOMAIN(Group1"). The search " press Add to add them to the At to a trusted domain or a group list, the duplicates will be auto ddd a Sele	ity_manager/proxy_security/policy_g Network System Administ Groups es from the directory. For Active Direct is case-insensitive. The wildcard char utbrored Groups list. Afternatively, yo that is not yet available in the director matically omitted. exted Groups im AD1 LAB\Contractors	ration tay groups, omit the acter *** may be used. u can type the entire my). If group(s) are			业 IN □ ●
	A second se	security Services Security Services ctors Policy": Edit of arch field to see matching entrin "DOMAIN/Group1"). The search r, press Add to add them to the At is a trusted domain or a group list, the duplicates will be auto ddd = Sele Add = Sele Add = Ad	ity_manager/proxy_security/policy_g Network System Administ Groups es from the directory. For Active Direct is case-insensitive. The wildcard char utbroited Groups list. Afternatively, yo that is not ye available in the director matically omitted. kAB\Contractors	ration tory groups, omit the acter ** may be used. u can type the entire wy). It group(s) are			业 IN € ●

Click **Submit** and commit the configuration.

·) → C' û	0 🔒 https://10	.1.1.13:8443/web_se	ecurity_manager/proxy_secur	ity/policy_groups		▣ … ♡☆	⊻ III/ III ©°
Cisco S000 Cisco Web Security Virte	0V tual Appliance					① Upgrade Available	Logged in as: admin on wsa.lab.local s + Options + Support and Help +
Reporting We	eb Security Manager S	ecurity Services	Network Syste	em Administration			
							No Changes Pending
Access Policy: Co	ontactors				_		
Policy Settings							
	Policy Name: Contac (e.g. m	tors Policy y IT policy)					
	Description:						
	Insert Above Policy: 1 (Sale	es Policy) 🗸					
Policy Member Definition	the combination of the followi	na ontions. All criteri	a must be met for the policy t	o take effect			
Identificatio	on Profiles and Lisers:	One on Many Identifier	a must be met for the policy t	o take enect.			
	Identii	ication Profile	Authorized Users and (Groups Add Identification I	Profile		
	Lab Pr	ofile	→ ○All Authenticated Us	ers			
			Selected Groups and Groups:	d Users 🕐			
			Realm: AD1 LAB\Contractors	a			
			Users: No users ent	ered			
	Advanced Define	additional group men	nbership criteria.				
Cancel				1	Submit		
-)→ C' û	0 🖗 https://10	.1.1.13:8443/web_se	curity_manager/proxy_securi	ty/policy_groups		··· 🖂 🕁	⊻ ⊪\ ⊡ ©* ≣
ululu Cisco S00	0)/						the second tensor and when the second s
CIECO Mah Security Mat						(i) Upgrade Available My Favoritie	Logged in as: admin on wsa.lab.local
CISCO Web Security Virt	UV tual Appliance	curity Services	Network System	m Administration		(f) Upgrade Available 😸 My Pavorit	Logged in as: admin on wsa.tab.tocal es - Options - Support and Help -
CISCO Web Security Virt	UV tual Appliance /eb Security Manager Security Manager Security	ecurity Services	Network System	m Administration		(f) Upgrade Available ⊗ My Favorit	Cogged in as: admin on wsatabaca s • Options • Support and Help • Commit Changes >
CISCO Web Security Virt Reporting W Access Policies	UV Lual Appliance Yeb Security Manager Si	ecurity Services	Network System	m Administration		Upgrade Available Wy Favorit	Logged in as, admin on Wsalabaocal es - Options - Support and Help - Commit Changes *
CISCO Web Security Virt Reporting W Access Policies Success – Settings hav	UV Jual Appliance Veb Security Manager Si ve been saved.	ecurity Services	Network Syste	m Administration		() Upgrade Available S My Favorit	Cognet in as: down on vosadouoca s - Optons - Support and Help - Commt Changes >
cisco Web Security Virt Reporting W Access Policies Success — Settings hav Policies	VV Auf Appliance //eb Security Manager Si ve been saved.	curity Services	Network Syste	m Administration		() Upgrade Available 😒 My Revort	Cognet in as: dumin on vosa adaptocal s - Options - Support and Help -
CISCO Web Security Wirt Reporting W Access Policies Success – Settings hav Policies Add Policy	VV Applance Keb Security Manager S ve been saved. Protocols and	scurity Services	Network Syste	m Administration	-	(i) Upprade Available S My Favorit	Cognet in as: dumin on vosa ada.occar s - Options - Support and Help - Commit Changes >
Cisco Web Security Virt Reporting W Access Policies Success – Settings hav Policies Order Group Contactors Policy	Ve Applance Neb Security Manager S ve been saved. Protocols and User Agents	urity Services	Network System oppications Objects	m Administration	Delete	(i) Upprade Available S My favorit	Cognet in as: dumin on weakabuocat s - Options - Support and Help - Commit Changes -
CISCO Web Security Virt Reporting W Access Policies Success – Settings hav Policies Add Poly Order Group Contactors Poly. I Identicator Poly Subsection Poly Sector Poly	Ve been saved. Protocols and Ve brothel (global policy) Vcontractors)	URL Filtering A (global policy) (g	Network Syste	Administration	Delete	() Upgrade Available 🥃 My Favorit	Cognet In as: utumn on workautuuccar s - Options - Support and Help - Commit Changes >
CISCO Web Security Writ Reporting W Access Policies Success – Settings hav Policies Add Policy Order Group Contactors Policy I Gentification Profile 1 groups (AD1UAB Sales Policy 2 Identification Policy 2 Identification Policy 2 Identification Policy 3 Sales Policy 2 Identification Policy 3 Sales P	Ve been saved. Protocols and User Agents Lab Profile (global policy) Lab Profile (global policy)	URL Fitering A (global policy) (g	Network System Applications Objects global policy) (global policy)	Anti-Malware and Reputation (global policy) (global policy)	Delete	() Upgrade Available 🥃 My Favorit	Cognet in as: down on weakablocat s - Options - Support and Help - Commit Changes =
CISCO Web Security Write Reporting W Access Policies Success – Settings hav Policies Add Policy Order Group Contactors Policy Identification Profile 1 groups (AD1LAB Sales Policy Identification Profile 1 groups (AD1LAB Contactors Policy Identification Profile	Ve been saved. Ve been saved. Lab Proficeols and Viser Agents Lab Profit (global policy) Lab States; All No blocked iter	URL Fitering A (global policy) (g (global policy) (g (global policy) (g (global policy) (g	Network System Applications Objects global_collecy (global_policy) global_policy) (global_policy) tonitor: 356 No blocked item	Administration Anti-Malware and Reputation (global poley) (global poley) Web Reputation: Enabled Anti-Malware Scannag: Enabled	Delete	() Upgrade Available 🥃 My Favorit	Cognet in as: domin on vosa acusoca s - Options - Support and Help - Commit Changes >
Contactors Policies Add Policy Contactors Conta	W Appliance Web Security Manager S we been saved.	URL Fitering A (global policy) (g (global policy) (g (abal policy) (g (bal policy) (g) (bal policy) (g) (bal policy) (g) (bal policy) (Network System Applications Objects global policy) (global policy) global policy) (global policy) tonitor: 356 No blocked item	Administration Administration Anti-Halware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Halware Scanning: Enabled	Delete 2	() Upprade Available 🥃 My Favorit	Cognet in as: domin on wasaataboota s - Options - Support and Help - Commit Changes -
Crock Steamy Write Reporting Write Reporting Write Success Policies Success — Settings hav Policies Add Policy Order Group Contractors Policy Contractors Policy Contractors Policy Contractors Policy Sulars Policy Sulars Policy (AD)LAB Sulars Policy Identification Profile Igroups (AD)LAB Contractors Policy Identification Profile Identification Profile Identification Profile Edit Policy Order	Ve been saved. Protocols and User Agents Lab Profile (global policy) Lab Profile (global policy) Lab Profile (global policy) Lab Profile (global delive)	URL Fitering A (global poley) (g (global poley) (g (s Montor: 87 M	Network System upplications Objects global policy) (global policy) global policy) (global policy) stonitor: 356 No blocked items	Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Malware Scanning: Enabled	Delete 2 2	() Upprade Available 🥃 My favorit	Cognet in as: domin on wasaatabade s - Options - Support and Help -
Contactors Policies Contactors Policies Contactors Policy Contactors Po	ve been saved. Protocols and User Agents Lab Profile (global policy) Sales) (global policy) (sales) (global policy) (sales) (sale profile (global policy) (sales) (sale profile (s	uRL Fitering A (global poley) (g (global poley) (g (global poley) (g (global poley) (g .) Privacy Statement	Network System Applications Objects global policy) global policy) (global policy) global policy) (global policy)	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Malware Scanning: Enabled	Delete 2 3 3 4 4 4 4 4 4 4 4 4 4 4 4 4	() Upprade Available 🥃 My favorit	Cognet in as: domin on wasaatabade s - Options - Support and Help -
CISCO Web Security Writ Reporting W Access Policies Success – Settings hav Policies Add Polcy Order Group Contactors Policy I fidentification Profile I groups (AD1LAB Sales Policy Contactors Policy I fidentification Profile I groups (AD1LAB Color Policy Contactors Policy Contact	Ve been saved. (global policy) (Contractors) (global policy) (Sales) Savet been saved. (global policy) (Sales) Savet been saved. Savet been	Currty Services URL Filtering A (global policy) (global policy) (global policy) (global policy) (statement	Network System upplications Objects global policy) global policy) global policy) (global policy) tonitor: 356 No blocked item	m Administration Anti-Malware and Reputation (global policy) (global policy) Veb Reputation: Enabled Anti-Malware Scanning: Enabled	Delete	() Upgrade Available 🥃 My favorit	Cognet in as: unimit on wava.aux.uocat s Options - Support and Help - Commit Changes *
CISCO Web Security Write Reporting W Access Policies Success – Settings hav Policies Add Policy Order Group Contactors Policy 1 Identification Profile 1 groups (AD1LAB 1 groups (AD1LAB Copyright © 2003-2018 Cacce → C* ♠	W Appliance Web Security Manager Veb Security Manager Secu	LI.113:8443/committees	Network System Applications Objects global_policy) global_policy) global_policy) global_policy) tonitor: 356 No blocked item t?referrer=https://10.1.1.1388	Administration Anti-Malware and Reputation (global policy) (global policy) (global policy) Web Reputation: Enabled At3/web_security_manager/prov	Delete	 () Upgrade Available · · · · · · · · · · · · · · · · · · ·	Explore in as: unimit on wasaatabada s Options - Support and Help - Commit Changes ≥ ★ Wi\ □ @
CISCO Web Security Writ Reporting W Access Policies Success – Settings hav Policies Add Policy Order Group Contactors Policy Contactors Policy Contactors Policy Contactors Policy Lidentification Policie 1 groups (AD1LAB Global Policy Comparison Policy Comparis	W Appliance Web Security Manager Ve been saved.	Lunty Services	Network System Applications Objects global collecy (global policy) global policy) (global policy) global policy) tonitor: 356 No blocked item tereferrer=https://10.1.1.138	m Administration Anti-Malware and Reputation (global poley) (global poley) Veb Reputation: Enabled Anti-Malware Scanning: Enabled 443/web_security_manager/prov	Delete 0 1 y_security/policy.groups	() Upgrade Availabé ≤ Wy favorit	Logged in as: domin or was.lab.local
CISCO Web Security Writ Reporting W Access Policies Success – Settings hav Policies Add Poley Order Group Contactors Policy I demitication Policie 1 groups (AD1LAB Contention Policie 1 groups (AD1LAB Contactions Policy Contactions Policy Contaction	W Appliance Reb Security Manager S Ve been saved. Protocols and User Agents Lab Profit (global policy) Lab Profit (global policy) All No blocked iter States States States No blocked iter S All No blocked iter S S S S S S S S S S S S S	LURL Fitering A (global policy) (g (global policy) (global policy) (g (global policy) (global policy	Network System upplications Objects global policy) (global policy) global policy) (global policy) tontor: 356 No blocked item treferrer=https://10.1.1.13:8	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Malware Scanning: Enabled 443/web_security_manager/prov	Delete 2 2 y_security/policy_groups	 () Upgrade Available · · · · · · · · · · · · · · · · · · ·	Logged In as: admin on was.aa.aa.aa. Commit Changes • Commit Changes • Logged In as: admin on was.lab.local tes • Options • Support and Hep •
CISCO Web Security Virit Reporting W Access Policies Success - Settings hav Policies Add Policy Order Group Contactors Policy I deministration Profile 1 groups (ADIXAB Contactors Policy I deministration Profile Contactors Policy Contactors Policy I deministration Profile Edit Policy Order Copyright © 2003-2018 Classe - → C @ @ 	W Appliance We becunty Manager S Ve been saved. User Agents Lab Profile (global policy) Lab Sales) Sales) Sales) No blocked iter Sales) Sales) No blocked iter No blocked iter Sales)	LURL Fitering A URL Fitering A (global poley) (g (global poley) (global poley) (g	Network System upplications Objects global_colicy) (global policy) global_colicy) (global pol	m Administration Anti-Halware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Halware Scanning: Enabled 443/web_security_manager/prov	Delete	() Upgrade Available S Wy Favoritie	Cognet in as: admin on wasaatabada © Options - Support and Help - Commit Changes × Commit Changes × ↓ II\ □ ↓ Logged in as: admin on wasabbJocal tes - Options - Support and Help -
CISCO Web Security Write Reporting Write Access Policies Success – Settings hav Policies Add Policy Order Group Contactors Policy Cont	Ve been saved. Protocols and User Agents r tab Profile (global policy) (global policy) (sales) o Systems, Inc. All rights reserve o Systems, Inc. All rights reserve Aud Appliance r tab Appliance r tab Security Manager S	Curity Services URL Fitering A (global poley) (g (global poley) (g (global poley) (g (global poley) (g , global poley) (g , glo	Network System upplications Objects global policy) (global policy) global policy) (global policy) global policy) (global policy) it?referrer=https://10.1.1.13.8 Network System	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Malware Scanning: Enabled 443/web_security_manager/prox	Delete	() Upgrade Available s Wy favorit ♡ ☆ ① Upgrade Available s My Favorit	Logged in as: admin on was about the comment of the
ClisCo Web Security Write Reporting Write Access Policies Success – Settings hav Policies Add Policy Order Group Contractors Policy Contractors	W Appliance Web Security Manager Yeb Security Manager Yeb Security Manager Yeb Security Manager	curity Services 4	Network System upplications Objects global policy) (global policy) global policy) (global policy) global policy) (global policy) ionitor: 356 No blocked item i:	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Malware Scanning: Enabled 443/web_security_manager/prov m Administration	Delete	 () Upgrade Available · · · · · · · · · · · · · · · · · · ·	Cognet in as: domin on was.abs.bocat Commt Changes • Commt Changes • Commt Changes • Logged in as: admin on was.lab.locat tes • Options • Support and Help •
CISCO Web Security Write Reporting Write Success Policies Success – Settings have Policies Add Policy Order Group Constantions Policy Constantions Policy Constantions Policy Constantions Policy Constantions Policy Constantions Policy Sales Policy Order Copyright © 2003-2018 Cacce Copyright © 2003-2018 Cacce Cacce Cacce Cacce Copyright © 2003-2018 Cacce Cacce Cacce Cacce Copyright © 2003-2018 Cacce Cacce Cacce Cacce Cacce Cacce Cacce Cacce Cacce Cacce Cacc	W Appliance Web Security Manager Yeb Security Manager Yeb Deen saved. Protococks and Protococks and Protococks and Protococks and Protococks and (global policy) (gl	Curity Services URL Filtering A (global policy) (global policy	Network System opplications Objects alobal.colicy) (global policy) global policy) (global policy) tonitor: 356 No blocked item i: i: Network System Network System	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled At3/web_security_manager/prov m Administration	Delete	Image: Second State Sta	Logged In as: admin on was.lab.local Logged In as: admin on was.lab.local tes - Options - Support and Help -
ClsCO Web Security Write Reporting Write Access Policies Success – Settings have Policies Add Policy Order Group Contractors Policy Generatication Profile Generations Profile Generations Profile Generations Profile Generations Profile Generations Profile Comment Changes You have uncommitted Ch Comment Changes	W Appliance Web Security Manager S S Security Manager S S S S S S S S S S S S S S S S S S	curity Services URL Filtering A URL Filtering A (global policy) (g (global policy) (g (global policy) (g 1 Privacy Statement 1.1.13:8443/commit curity Services	Network System upplications Objects alabal colicy) (global policy) global policy) (global policy) threferrer=https://10.11.1138 Network System	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled 443/web_security_manager/pros am Administration	Delete	() Upgrade Available S Wy favoriti Wy favoriti	Logged In as: domin on wsa,tab.boca Commt Changes * Commt Changes * Logged In as: admin on wsa,tab.boca tes • Optons • Support and Help •
CISCO Web Security Write Reporting Write Success Policies Success – Settings have Policies Add Policy Order Group Contactors Policy Contactors Policy Co	W Appliance Web Security Manager S S Security Manager Protocols and Protocol	curity Services URL Fitering (global policy) (Network System upplications Objects alobal colicy) (global policy) global policy) (global policy) global policy) (global policy) threferrer=https://10.11.13:8 Network System our commit them	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled 443/web_security_manager/pros m Administration	Delete 2 2 3 4 4 4 4 4 4 4 4 4 4 4 4 4	() Upgrade Available *** Wy favorit *** Signal *** Signal *** () Upgrade Available ** Wy Favorit *** Wy Favorit	Commit on was.abunced Commit Changes * Commit Changes *
ClsCO Web Security Writ Reporting W Access Policies Success Success – Settings have Order Group Contactors Delicy Identification Folice Order Group Contactors Delicy Identification Folice I Geoda Folicy I Identification Folice I Geoda Folicy Copyright © 2003-2018 Cacce O Comment Changes You have uncommitted ch You have uncommitted ch Comment Changes You have uncommitted ch Comment Changes	W Appliance We been saved. Protocols and Proto	curity Services URL Filtering (global policy) (global	Network System upplications Objects ajobal colicy) (global policy) global policy) (global policy) global policy) (global policy) threferrer=https://10.11.1.13:80 Network System ou commit them. commit Changes	m Administration Anti-Malware and Reputation (global policy) (global policy) (global policy) Web Reputation: Enabled At3/web_security_manager/prov m Administration	Delete 2 2 2 3 3 4 4 4 4 4 4 4 4 4 4 4 4 4	 () Upgrade Available · · · · · · · · · · · · · · · · · · ·	Commit Changes . Commit Changes . Commit Changes . Commit Changes . Logged In as: admin on wsa,Jab,Jocal tes - Options - Support and Help -
CISCO Web Security Write Reporting Write Success Policies Success – Settings have Policies Add Policy Order Group Contactors Policy 1 Identification Policy 1 Identification Policy 1 Identification Policy 2 Subject (Palluka Global Policy Commit (Palluka Copyright © 2003-2018 Classe Copyright © 2003-2018 Classe Copyr	W Appliance We been saved. Protocols and User Agents Li Lab Profile (global policy)	curity Services URL Filtering	Network System applications Objects alobal policy) (global policy) global policy) (global policy) global policy) (global policy) threferrer=https://10.11.11388 Network System ou commit them. commit Changes	m Administration Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled Web_Reputation: Enabled 443/web_security_manager/prov m Administration	Delete P P P P P P P P P P P P P	Imported Available Imported Available Wy favorith Imported Available	Cognet in as: admin on wasaan.oca Commt Changes = Commt Changes = Commt Changes = Logged in as: admin on waslab.local es = Optons = Support and Help =

€ →	C' û 0	https://10.1.	1.13:8443/web_	security_mana	ger/proxy_security	//policy_groups			☑ ☆	⊻ ш/		₿ Ξ
ului cisco	Cisco S000V Web Security Virtual Appliance							Upgrade Avail	able ≥ Logged in as: My Favorites → Options	admin on w	sa.lab.lo t and Helj	pcal Ip -
A ₽	web Security Ma	inager Secu	rity Services	Network	System	Administration						
										No Char		ding
Acce	ss Policies											
Succe	ss - Your changes have been	committed										
Dellala		committed.										
Add	Policy											
Order	Group	Protocols and	URI Eltering	Applications	Objects	Anti-Malware and Reputation	Delete					
1	Contactors Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Contractors)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	â					
2	Sales Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Sales)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	ŵ					
	Global Policy Identification Profile: All	No blocked items	Monitor: 87	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled						
Edit	Policy Order											
Соругі	ght © 2003-2018 Cisco Systems, Inc.	All rights reserved.	Privacy Stateme	int								

Navigate to **Web Security Manager > Access Policies**.

In the **Contractors Policy** group, under the **URL Filtering** column, select the **(global policy)**.

For the **Social Networking** category, select the **Block** action. Click **Submit**.

$) \rightarrow$	C' û	Ū	https://10.1.	1.13:8443/web	_security_mana	ger/proxy_security	//policy_groups	
(111 CISCO	• Cisco S00 Web Security Virt	0V tual Appliance						
R	eporting W	/eb Security Ma	nager Secu	rity Services	Network	s System	Administration	
ce	ss Policies							
ucce	ss – Your change	es have been o	committed.					
olicie	5							
Add	Policy							
Order	Group		Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Contactors Policy Identification Profile 1 groups (AD1\LAB	: Lab Profile \Contractors)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	ŵ
2	Sales Policy Identification Profile 1 groups (AD1\LAB	:: Lab Profile S\Sales)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	畲
	Global Policy Identification Profile	: All	No blocked items	Monitor: 87	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	
								-

← → ♂ ✿	🛡 🔒 h	attps:// 10.1.1.13 :8443/web_se	curity_manager/pi	oxy_security/url_categories_http?i	action=FormEdit&policy_g	roup_type=http	&CSRFKey=037	… ⊠ ☆		⊻ ॥/ ₪	۲
cisco Web	CO SOOOV Security Virtual Appliance					Œ	Upgrade Availa	ble ⊗ My Favorite	Logged in as: adm es - Options -	i n on wsa.lab.lo Support and Hel	pcal p =
A Reporting	Web Security Manager	Security Services	Network	System Administration							
										No Changes Pen	ding
Access Po	licies: URL Filtering	: Contactors Polic	v								
			,								
Custom and Ex	ternal URL Category Filtering										
No custom and	d external URL categories are defi	ined. Add categories in the Wel	Security Manager	> Custom and External URL Catego	ries page.						
Predefined UR	L Category Filtering										
					Use Global Settings		O	verride Global Set	tings		
					Detenigo.	Block	Monitor	Warn 🕐	Quota-Based	Time-Based	
Category					Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)	
Science and	Technology				v				-	-	^
😔 Search Eng	ines and Portals				✓				-	-	
😔 Sex Educat	on				1				-	-	
😔 Shopping					1				-	-	
😌 Social Netw	orking					✓			-	-	
😔 Social Scien	ce				1				-	-	
😣 Society and	Culture								-	-	
😔 Software U	odates				✓				-	-	
😝 Sports and	Recreation				1				-	-	
😝 Streaming /	Audio				✓				-	-	
😝 Streaming V	/ideo				1				-	-	
😝 Tobacco					1				-	-	
😝 Transportat	ion				v				-	-	
😝 Travel					1				-	-	

In the **Sales Policy** group, under the **URL Filtering** column, select the (global policy). For the **Streaming Video** category, select the **Block** action.

ICK	k Submit and	d comn	nit the	e confi	iguratio	n.	
\rightarrow	C 🕜 🛈	https://10.1.	1.13:8443/web	_security_mana	ger/proxy_security	//policy_groups	
111 1 15CO	Cisco S000V Web Security Virtual Appliance						
Re	eporting Web Security Ma	anager Secu	rity Services	Network	c System	Administration	
Acce	ss Policies						
-							
Succes	ss — Settings have been saved	ł.					
Succes Policies	ss — Settings have been saved	ł.					
Succes Policies Add I	ss — Settings have been saved s Policy	1.			_	_	
Succes Policies Add I	ss — Settings have been saved s Policy Group	f. Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
Succes Policies Add I Order	ss — Settings have been saved policy Group Contactors Policy Identification Profile: Lab Profile 1 groups (ADULAB/Contractors)	Protocols and User Agents (global policy)	URL Filtering Block: 1 Monitor: 85	Applications (global policy)	Objects (global policy)	Anti-Malware and Reputation (global policy)	Delete
Success Policies Add I Order 1 2	ss — Settings have been saved Policy Group Contactors Policy Identification Profile: Lab Profile 1 groups (AD1/LAB/Contractors) Sales Policy Identification Profile: Lab Profile 1 groups (AD1/LAB/Sales)	Protocols and User Agents (global policy) (global policy)	URL Filtering Block: 1 Monitor: 85 (global policy)	Applications (global policy) (global policy)	Objects (global policy) (global policy)	Anti-Malware and Reputation (global policy) (global policy)	Delete
Success Policies Add I Order 1 2	ss — Settings have been saved Policy Group Contactors Policy Identification Profile: Lab Profile 1 groups (AD1/LAB/Contractors) Sales Policy Identification Profile: Lab Profile 1 groups (AD1/LAB/Sales) Global Policy Identification Profile: All	f. Protocols and User Agents (global policy) (global policy) No blocked items	URL Filtering Block: 1 Monitor: 85 (global policy) Monitor: 87	Applications (global policy) (global policy) Monitor: 356	Objects (global policy) (global policy) No blocked items	Anti-Malware and Reputation (global policy) (global policy) Web Reputation: Enabled Anti-Malware Scannig: Enabled	Delete

Contract Contract 1101 Ontone on Fi		T oney									
o custom and external URL categories	iltering s are defined. Add cat	tegories in the Web	Security Manager > C	ustom and External	URL Categories p	age.					
edefined URL Category Filtering											
						Use Global Settings	Block	Monitor	werride Global Set	tings Quota <u>-</u> Based	Time-Bas
tenory						Select all	Select all	Select all	Select all	(Unavailable)	(Unavailat
SaaS and B2B						Selecc all	Select di	Select di	Select di	(onavailable)	(Unavailat
Safe for Kids										-	_
Science and Technology						✓ ✓				-	-
Search Engines and Portals						1				-	-
Sex Education						 Image: A second s				-	-
Shopping						~				-	-
Social Networking						~				-	-
Social Science						~				-	-
Society and Culture										-	-
Software Updates										-	-
Streaming Audio						V					_
Streaming Video						4					_
Tobacco						J	v			_	_
Transportation										_	-
Travel										-	_
Weapons						v V				-	-
Web Hosting										_	_
C A 0	https://10.1.1	13:8443/web secu	ity manager/provy s	security/policy gray	IDS				$\sim \sim \sim$	Ļ	/ III\ (TT)
C W	Ma nttps://10.1.1.	.13:8443/web_secu	ity_manager/proxy_s	security/policy_grou	lbs				- U W	¥	
ulu, Cisco S000V							C	Upgrade Availa	ible 🗧	Logged in as: adm	in on wsa.la
ccess - Settings have been save	d.										
ccess — Settings have been save	d.	_	_	_							
cccess — Settings have been save licies Add Policy	d. Protocols and		-		_	-					
ccess — Settings have been save licles add Policy der Group Contractors Bolicy	d. Protocols and User Agents	URL Filtering Apple	ations Objects	Anti-Malware	and Reputation	Delete					
ccess – Settings have been save lices kdd Policy der Group Contactors Policy I Identification Profile Lab Profile 1 groups (ADJ VLAB/Contractors)	d. Protocols and User Agents (global policy)	URL Filtering Applie Block: 1 Monitor: 85 (globa	ations Objects	Anti-Malware	and Reputation	Delete					
ercess – Settings have been save icides der Group Contactors Policy Identification Profile: Lab Profile 1 groups (AD1UAB/Solfs) Sales Policy Identification Profile: Lab Profile 1 groups (AD1UAB/Solfs)	d. Protocols and User Agents (global policy) (global policy)	URL Filtering Applic Block: 1 Monitor: 85 (global Block: 1 Monitor: 85 (global	ations Objects I policy) (global polic I policy) (global polic	Anti-Malware (global policy ry) (global policy	and Reputation)	Delete					
Settings have been save definition de	d. Postocols and User Agents (global policy) (global policy) No blocked items	URL Fittering Apple Block: 1 Monitor: 85 (glob: Block: 1 Monitor: 87 (Monit	ations Objects i policy) (global polic i policy) (global polic global polic) xr: 356 No blocked	Anti-Malware yy) (global policy yy) (global policy titems Web Reputat	and Reputation)) don: Enabled Scanning: Enable	Delete 2 3 d					
Settings have been save Settings have been save Kide Kide Group Contactors Policy Identification Profile: Lab Profile I groups (ADI\LAB\Scales) Sates Policy Identification Profile: Lab Profile I groups (ADI\LAB\Scales) Global Policy Identification Profile: Lab Cobal Policy Identification Folicy Cobal Policy Identification Folicy Identification Identifi	d. Protocols and User Agents (global policy) (global policy) No blocked items	URL Filtering Apple Block: 1 Monitor: 85 (glob: Monitor: 87 (dobi Monitor: 87 Monit	ations Objects i policy) (global polic i policy) (global polic global polic yr: 356 No blocked	Anti-Malware y) (global policy y) (global policy ttems Web Reputat Anti-Malware	and Reputation)) ion: Enabled Scanning: Enable	Delete					
Settings have been save Settings have Settings have been save Settings have been sa	d. Protocols and User Agents (global policy) (global policy) (global policy) No blocked items All rights reserved. 1	URL Filtering Apple Block: 1 Block: 1 Block: 1 Monitor: 85 (glob) Monitor: 87 Monit Privacy Statement	ations Objects I policy (global polic global policy (global polic yr; 356 No blocked	Anti-Malware y) (global policy y) (global policy (tems Web Reputat Anti-Malware	and Reputation)) ion: Enabled Scannay: Enable	Delete					
cccss – Settings have been save id/de id/de id/de Group Contactors Policy Definition id/de/de/de/de/de/de/de/de/de/de/de/de/de	d. Protocols and User Agents (global policy) (global policy) No blocked items All rights reserved. All rights reserved.	URL Fitering Apple Biock: 1 Glob. Biock: 1 Glob. Biock: 1 Glob. Montor: 87 Glob. Privacy Statement	ations Objects I policy) (global polic I policy) (global polic I policy) (global polic yr: 356 No blocked ty_manager/proxy_s	Anti-Malware (global policy) (global policy) (and Reputation)) ion: Enabled Scanning: Enable	Delete			S 2	Ŧ	м со
cccss – Settings have been saved iccs iccs icc Group iccntactors Policy iccs iccs Policy iccs Icentification Profile: Lab Profile i groups (ADI UAB ISCB) Icentification Profile: Lab Profile i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI UAB ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI ISCB) i groups (ADI UAB ISCB) Icentification Profile: ADI ISCB) </td <td>d. Protocols and User Agents (global policy) (global policy) No blocked items All rights reserved. 1 All rights reserved. 1</td> <td>URL Filtering Apple Biock: 1 (glob) Monitor: 85 (glob) Monitor: 87 (glob) Monitor: 87 Monit</td> <td>ations Objects I policy) (global polic I policy) (global polic or: 356 No blocked</td> <td>Anti-Malware y) (global policy y) (global policy (global policy trems Web Reputation Anti-Malware ecurity/policy_grou</td> <td>and Reputation))) j) j) j) j) j) j) j) j) j) j) j)</td> <td>Delete 2 3 4</td> <td>٩</td> <td></td> <td> ♥ ☆ * × </td> <td>보 ogged in as: admin</td> <td>lii\ []</td>	d. Protocols and User Agents (global policy) (global policy) No blocked items All rights reserved. 1 All rights reserved. 1	URL Filtering Apple Biock: 1 (glob) Monitor: 85 (glob) Monitor: 87 (glob) Monitor: 87 Monit	ations Objects I policy) (global polic I policy) (global polic or: 356 No blocked	Anti-Malware y) (global policy y) (global policy (global policy trems Web Reputation Anti-Malware ecurity/policy_grou	and Reputation))) j) j) j) j) j) j) j) j) j) j) j)	Delete 2 3 4	٩		 ♥ ☆ * × 	보 ogged in as: admin	lii\ []
cccss – Settings have been saved icides icide for the saved	d. Protocols and User Agents (global policy) (global policy) (global policy) No blocked items All rights reserved. 1 All rights reserved. 1 anager Securit	URL Fitering Apple Biod: 1 B (glob) Monitor: 85 (glob) Monitor: 87 (Glob) Monitor: 87 (Monit Privacy Statement .13:8443/web_secur	ations Objects i policy) (global polic i policy) (global polic r: 356 No blocked ty_manager/provy_s Network	Anti-Malware y) (global policy y) (global policy teems Web Reputat Anti-Malware security/policy_grou	and Reputation)) por: Enabled Scannag: Enable n	Delete	0		 ♥ ☆ * < 1 	ogged in as: admit	III\ () non wsa.lab By ra Soopert and
cccss – Settings have been save iccs iccs iccd iccs iccs iccs iccs iccs iccs iccs iccs policy iccs iccs iccs policy icity policy <	d. Protocols and User Agents (global policy) (global policy) (global policy) No blocked items All rights reserved. 1 All rights reserved. 1 anager Securi	URL Fitering Apple Block: 1 Montor: 85 (glob) Block: 1 Montor: 87 (glob) Montor: 87 Mont Plivacy Statement 13:8443/web_secur	ations Objects I policy) (global polic I policy) (global polic	Anti-Malware (global policy (global policy) (global policy) (global policy) (global policy) (tems Web Reputat Anti-Malware) (tems) System Administration	and Reputation)) ion: Enabled Scanning: Enable	Delete 20 3	•		 ♥ ☆ * = ↓ 	오gged in as: admin	In on wealable Report and to Changes Pr
cccss – Settings have been save icides icides icide for a constructor policy icide icide constructors icide icide constructors icide icide constructors	d. Protocols and User Agents (global policy) (global policy) (global policy) All rights reserved. 1 All rights reserved. 1 anager Securit	URL Filtering Applic Block: 1 Monitor: 85 (glob) Monitor: 87 (glob) Monitor: 87 Monito Privacy Statement 13.8443/web_secur	ations Objects i policy) (global polic i policy) (global polic r: 356 No blocked ty_manager/prosy_s Network s	Anti-Malware y) (global policy y) (global policy terms Web Reputat Anti-Malware security/policy_grou	and Reputation))) aon: Enabled Scannang: Enable	Delete 2 3 4	•		 ♥ ☆ * × 	⊻ ogged in as: admit	III C n on wsa.lab io Changes Pe
cccss – Settings have been save iddes iddes idd Policy iddes idd Policy Order iddes idd Policy iddes idd Policy iddes idd Policy iddes idd Policy iddes	d. Protocols and User Agents (global policy) (global policy) (global policy) All rights reserved. 1 All rights reserved. 1 anager Securi Protocols and	URL Fitering Apple Block: 1 Montor: 85 (glob) Block: 1 Montor: 87 Mont Privacy Statement .13:8443/web_secur	ations Objects I policy) (global polic I policy) (global policy) (glob	Anti-Malware (global policy (global policy (global policy (global policy (terms) Web Reputat executivy/policy_grou System Administration	and Reputation)) ion: Enabled Scanning: Enable in	Delete 2 3 4 4 4 4 4 4 4 4 4 4 4 4 4	•	•••	 ○☆ ★ = ↓↓ 	보 ogged in as: admin	In on wealab Report and to Changes Pr
cccss – Settings have been save istes isted Policy ter Group istes Policy identification Profile: Lab Profile 1 groups (AD1LAB Koster) identification Profile: All distribution Profile: All cicbal Policy identification Profile: All cicbal Policy	d. Protocols and User Agents (global policy) (global policy) (global policy) All rights reserved. 1 All rights reserved. 1 anager Securi Protocols and (global policy) (global policy)	URL Filtering Apple Block: 1 (glob) Monitor: 85 (glob) Monitor: 87 (glob) Monitor: 87 Monit Privacy Stats II3.8443/web_secur	ations Objects 1 policy) (global polic	y) (global policy y) (global policy y) (global policy teems Web Reputat Anti-Malware System Administration	and Reputation))) por: Enabled Scannag: Enabled in and Reputation)	Delete Delete	0		 ♥ ☆ * * 	t ogged in as: admit	hin Compared and Arrival
cccss – Settings have been save idde iddex iddex iddex	d. Protocols and User Agents (global policy) (global policy) (global policy) All rights reserved. 1 All rights reserved. 1 All rights reserved. 1 Protocols and User Agents (global policy) (globa	URL Fitering Apple Block: 1 Montor: 85 (glob) Montor: 87 (glob) Montor: 87 Mont Pilvacy Statswet 13:8443/web_secur Ity Services URL Fitering Apple Block: 1 Montor: 85 (glob)	ations Objects I policy) (global polic I policy) (global polic) I policy) I policy) I policy I policy) (global polic) I policy) I policy I policy I policy) I policy I pol	Anti-Malware ry) (global policy ry) (global policy ry) (global policy recurity/policy_grou recurity/policy_grou	and Reputation))) ion: Enabled Scanning: Enable p5 and Reputation)))	Delete 2 2 2 2 2 2 2 2 2 2 2 2 2	٩	•••	* • L	노 ogged in as: admin	In on wsa.fab a on wsa.fab so changes Pe

From **jdoe-pc**, open a browser, the user is prompted to enter a username and password, the Identification Profile Lab Profile is configured previously to authenticate user via the AD1 Realm for the subnet 10.1.1.0/24. Use jdoe as a username and Cisco123 as a password and try to access youtube using the url https://www.youtube.com, the site should be blocked by the WSA since the Streaming Video URL category is blocked in the access policy named Sales Policy and jdoe user belongs to the LAB\ Sales group. The web page fails to load but there is no notification for jdoe user.

The second secon			
\leftrightarrow \rightarrow \mathbf{C} G Effectuez une recherche sur	Google ou saisissez u	ne URL	☆ \varTheta :
	Ouvrir une session Le proxy http://10.1.1. passe. Votre connexion à ce s	n 13:3128 nécessite un nom d'utilisateur et un mot de site n'est pas privée	
	Nom d'utilisateur	jdoe	
	Mot de passe		
		Ouvrir une session Annuler	

To display the default blocked page of WSA, we need https decryption.



From **jwhite-pc**, open a browser, the user is prompted to enter a username and password, the Identification Profile Lab Profile is configured previously to authenticate user via the AD1 Realm for the subnet 10.1.1.0/24. Use **jwhite** as a username and Cisco123 as a password and try to access facebook using the url https://www.facebook.com, the site should be blocked by the WSA since the Social Networking URL category is blocked in the access policy named Contractors Policy and jwhite user belongs to the LAB\ contractors group. The web page fails to load but there is no notification for jwhite user.

To display the default blocked page of WSA, we need https decryption.

S https://www.facebook.com						
\leftarrow \rightarrow C Q Effectuez une recherche sur Google o	ou saisissez une URL				☆	e :
	Ouvrir une sessi Le proxy http://10.1 passe. Votre connexion à c	ON .1.13:3128 nécessite un nom d'utilisateur et un mot ce site n'est pas privée	t de			
	Nom d'utilisateur	jwhite				
	Mot de passe	••••••				
		Ouvrir une session Ani	nuler			
www.iacebook.com						0
← → C (0) facebook.com					Ŷ	9:0

S www.facebook.com	+		
\leftrightarrow \rightarrow C () facebook.com		\$ Θ	:
	лъ		
	Ce site est inaccessible		
	Il se peut que la page Web à l'adresse https://www.facebook.com/ soit temporairement inaccessible ou qu'elle ait été déplacée de façon permanente à une autre adresse Web.		
	ERR_TUNNEL_CONNECTION_FAILED		

Network Security All-in-one WorkBook Cisco Umbrella



Х

Lab 1: Cisco Umbrella Basic Configuration

Download the Umbrella Roaming Client.





Navigate to **Deployments > Core Identities > Roaming Computers** and click **Roaming Client**.

Verify Roaming Client Operation.


Navigate to **Deployments > Core Identities > Roaming Computers**.

he hostname of the machine **Redouane** on which you installed the Umbrella roaming client, status and policy applied, is listed.

← → ♂ ☆	0 🔒 🗝 b	https://dashboard. umbrella.com /o/3050	180/#/deployments/core/roamingdevices	🗵	☆ III\ ED S
Cisco Umbrella			Free Trial: You have 13 days left.	VIEW PRICING & PURCHASE	
Overview		Deployments / Core Iden			(±)
Deployments	~	Roanning Co	Shiputers o		Roaming Client Settings
Core Identities		Roaming Computers are those th	at are protected by either the Umbrella Roaming (Client, or the Umbrella Roaming Security mod	ule for AnyConnect. This
Networks		area of the Dashboard gives you the upper-right. Once installed	the ability to deploy and manage your Roaming C use the search to find computers and check the st	Computers. To deploy either agent type, click t	he "Download" button in can be expanded for more
Network Devices		detail about its state and tags ca	n be added to group computers together.		
Roaming Computers					
Mobile Devices		Q Search	Advanced 🗸		
Chromebook Users					
Configuration		2 Total			
Domain Management		🗌 Identity Name 🔺	Status	Tags	Last Sync 🔻
Sites and Active Directory				•	
Internal Networks		F5-Server-1	Offline DNS Layer Encryption: disabled		17 hours ago 🗸 🗸
Root Certificate					
Service Account Exceptions		Redouane	Protected & Encrypted at the DNS Cayer Layer		26 minutes ago
Policies	>		UNS Layer Encryption: enabled		
Reporting	>			Page: 1 ∨ Results per page: 10 ∨	1-2 of 2 < >
Admin	>				

From the Client PC, access the URL www.facebook.com.

← → ℃ ŵ	0 A https://www.facebook.com		🗵	☆ Ⅲ	\ 🗉 🔮
	facebook	Adresse e-mail ou mobile Mot de pa	usse Connexion ons de compte oubliées ?		
	Avec Facebook, partagez et restez en contact avec votre entourage.	Inscription C'est rapide et facile.			
		Prénom	Nom de famille		
		Nouveau mot de pass	3e		
		Date de naissance			
		Genre			
		○ Femme ○ Homm	e O Personnalisé 🛛		
		En appuyant sur inscription, vous ac générales, notre Politique d'utilisatio Politique d'utilisation des cookies. Vo notifications par texto de notre part et moment vous désabonner.	ceptez nos Conditions n des données et notre pus recevrez peut-être des et vous pouvez à fout		
		Inscription			

From the Client PC, access the URL www.games.com.



From the Client PC, access the URL www.4shared.com.

$\leftarrow \rightarrow$ C \triangle	🖸 🔒 📮 https://v	www.4shared.com				🗵	☆	III\ 🖸
			4 sł		Connexion	S'inscrire		
		Trouve Télécharge Recherchez vos fichiers,	z, Stockez et z, découvrez et partage votre musique, vos vidéos, vo	Partagez Facil z vos fichiers sans aucun s images	ement e difficulté!			
			Charger o	les fichiers				
	Musique	Vidéos	 Applis	Images	Livres	Tous les F	Fichiers	

Create a policy based on the Machine s' Hostname **Redouane** as a condition.

Navigate to **Policies > Management > All Policies** and click **Add**.

← → C' ŵ	0	≙ -•• ⊧	ttps://dashb	ooard.umbrella.com/o/3050180/#/p		ເ ☆	liil\	•		
Cisco Umbrella					Free Trial: You have 13	3 days left. VIEW P	RICING & PURCHASE			
Deployments			ababa	Policies / Management						
Policies	~	a	cisco	All Policies 🛛					Add	Policy Tester
Management										
All Policies			Policies of log levels	lictate the security protection and how block pages are dis	n, category settings, and individual splayed. Policies are enforced in a	destination lists y descending order	ou can apply to some , so your top policy w	or all of your identities.	Policies also c second if they	ontrol share
Policy Components			the same	identity. To change the priori	ity of your policies, simply drag an	a arop the policy	in the order you'd like	. More policy into can be	found in this a	article.
Destination Lists								Sorted by Order o	f Enforcement	
Content Categories										
Application Settings			1	Default Policy		Applied To All Identities	Contains 3 Policy Settings	Last Modified Mar 16, 2020	~	
Security Settings										
Block Page Appearance										
Integrations										
Reporting	>									
Admin	>									
Investigate										

Select **Roaming Computers**, and the **Client PC** with the hostname **Redouane**. Select and then click **Next**.

(←) → C' @	🕖 🔒 🗝 https://da	ashboard.umbrella.com/o/3050180/#/policies/manag	ement/policies		… ⊠ ☆	1111
Cisco Umbrella						
Deployments	>	What would you like to prote	ct?			
Policies	~ 1	Select Identities				
Management		Search Identities		0 Selected		
		All Identities				
All Policies		🗌 💩 AD Groups	^			
Policy Components		□ ± AD Users				
Destination Lists		□ □ AD Computers				
Content Categories		🗋 🚠 Networks				
Application Settings		Roaming Computers	2>			
		Sites	1>			
Security Settings		A Network Devices				
Block Page Appearance		Omega Mobile Devices				
Integrations		Chromobooks	Ŷ			
Reporting	>				CANCEL	
Admin	>					
Investigate					Sorted by Order of En	forcement
Cisco Umbrella Overview Deployments >	Policies of control lo	Policies / Management All Policies • dictate the security protection, category setting og levels and how block pages are displayed. Po	s, and individual destinatio	on lists you can apply to some or all of your Id lescending order, so your top policy will be app	Add	Policy Tester
Policies 🗸	they shar in this ar	re the same identity. To change the priority of ye ticle.	our policies, simply drag a	and drop the policy in the order you'd like. Mor	e policy info can be	found
Management						
All Delining						
All Policies						
Policy Components		What would you like to protect?				
Destination Lists		Select Identities				
Content Categories		Search identities	0 Se	elected		
Application Settings		All Identities / Roaming Computers				
Security Settings		D = P5-Server-1				
Block Page Appearance		Redouane				
Internetiona	•					
integrations						
Reporting >						
Admin >						
Investigate						
Redouane MEDDANE MICROTEL				CANCEL	NEXT	

← → ♂ ☆	U	🔒 🗝 ht	tps://dashb	oard. umbrella.com /o/305018	0/#/policies/managemen	t/policies		… 🖂 🏠	Ir	II\ 🗓 📽
Cisco Umbrella		⊜	cisco	Policies / Management					Add	Policy Tester
Overview										
Deployments	>		Policies d control log they share	ictate the security protec g levels and how block p e the same identity. To ch	ction, category setting ages are displayed. P nange the priority of y	is, and individual des olicies are enforced our policies, simply (tination lists you can app in a descending order, so drag and drop the policy	ily to some or all of your identities. Po your top policy will be applied befor in the order you'd like. More policy in	ilicies also e the seco fo can be	o ond if found
Policies	~	1	in this art	icle.				,,		
Management										
All Policies										
Policy Components				What would you	u like to protect?					
Destination Lists				Select Identities						
Content Categories				Search Identities			1 Selected	REMOVE ALL		
Application Settings				All Identities / Roaming	Computers		Redouane			
Security Settings				Bedouane						
Block Page Appearance										
Integrations										
Reporting										
Admin										
Investigate										
Redouane MEDDANE MICROTEL	>							CANCEL	J.	

In the policy wizard, select the **Limit Content Access** component, this feature will be applied to the **Client PC**, then click **Next**.

← → ♂ ☆	0 🔒 ==0	https://dasł	board.umbrella.com/o/3050180/#/policies/management/policies	⊠ ☆	lur	\ 🗉 🔹						
Cisco Umbrella	€	aliali cisco	Policies / Management All Policies •		Add	Policy Tester						
Overview												
Deployments	>	Policies	dictate the security protection, category settings, and individual destination lists you can apply to some or all og levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy	of your identities. P will be applied befo	olicies also re the secor	nd if						
Policies	~	they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in this article.										
Management												
All Policies												
Policy Components			What should this policy do?									
Destination Lists			Choose the policy components that you'd like to enable.									
Content Categories			Enforce Security at the DNS Laver									
Application Settings			Ensure domains are blocked when they host malware, command and control, phishing, and more.									
Security Settings			Inspect Files Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Prote	ction.								
Block Page Appearance			Limit Content Access									
Integrations			Block or allow sites based on their content, such as file sharing, gambling, or blogging.									
Reporting	>		Control Applications Block or allow applications and application groups for identities using this policy.									
Admin	>		Apply Destination Lists									
Investigate			Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.									
Redouane MEDDANE MICROTEL	>		Advanced Settings CANCEL	PREVIOUS								

In the Limit Content Access, select the Custom option.



Select the categories you want to block, Games, File Transfer Services, Illegal Downloads and Social Networking, then click Next.



← → ♂ ☆	💿 🔺 🗝 https://dashboard.umbrella.com/o/3050180/#/policies/management/policies	… ⊠ ☆	lii\
Cisco Umbrella	Content 2 Block Pages	Summar	y
Overview			
Deployments Policies Management All Policies	 Set Block Page Settings Define the appearance and bypass options for your block pages. Use Umbrella's Default Appearance Preview Block Page • 		
Policy Components Destination Lists Content Categories Application Settings Security Settings	Use a Custom Appearance Choose an existing appearance * BYPASS USERS		
Block Page Appearance Integrations	CANC	CEL PREVIOUS NEXT	
Reporting	<u>></u>	Sorted by Order of Enforcer	ment
		Softed by Order of Ellipicer	nont
Investigate	Default Policy Applied To Contains All Identities 3 Policy Settings	Last Modified V Mar 16, 2020	

In the final step of the policy wizard, Enter the name **Demo-Policy** and click **Save**.

(←) → 健 @	🕖 🔒 🗝 https://dashb	oard.umbrella.com/o/3050180/#/policies/management/policies	… ⊠ ☆
Cisco Umbrella		Content Slock Pages	🖌 Summary
Overview		•	
Deployments	>		
Policies	~	Policy Summary	
Management		Policy Name	
All Policies		Demo-roicy	
Policy Components		1 Identity Affected 1 Rearing Computer 1 Block List	
Destination Lists		Edit Enable	
Content Categories		No Security Settings Applied Image: Security Settings Applied File Analysis Not Enabled File Inspection Not Enabled	
Application Settings		Edit	
Security Settings		Content Setting Applied: Default Settings Games, Social Networking, File Transfer Services, plus 1 more Umbrella Default Block Page Appl	ied
Block Page Appearance		Kill De blocked. Edit Preview Block Page Edit Disable	
Integrations	·	No Application Settings Applied	
Reporting	>	Enable	
Admin	>	Advanced Settings	
Investigate		CANCEL	PREVIOUS
Redouane MEDDANE	>		

Navigate to **Deployments > Core Identities > Roaming Computers**. Expand the Client PC **Redouane**, verify that the policy **Demo-Policy** is applied.

← → ♂ ☆	0	nttps://	/dashbc	oard. umbrella.com /o/3050180/#/policies/ma	anagement/policies			⊠ ☆	hir		. Ξ
Cisco Umbrella					Free Trial: You have 13 da	ays left. VIEW PF	RICING & PURCHASE				
Overview				Policies / Management							
Deployments	>		co	All Policies					Add	Pol	icy Tester
Policies	~	Polic	ries di	ctate the security protection, categori	ny settings, and individual de	estination lists v	ou can apply to some	or all of your identities	Policies also	contro	AL.
Management		log l the s	levels same i	and how block pages are displayed. I identity. To change the priority of you	Policies are enforced in a de r policies, simply drag and o	escending order	, so your top policy v	vill be applied before the	second if the	y share	e 9.
All Policies					· · · · · · · · · · · · · · · · · · ·	,	,,	,			
Policy Components								Sorted by Order of	of Enforcement		
Destination Lists			1	Dama-Baliay	Ap	plied To	Contains	Last Modified	~		
Content Categories				Demo-Policy	1	Identity	1 Policy Setting	Mar 17, 2020			
Application Settings			2	Default Policy	Ap	plied To	Contains	Last Modified	~		
Security Settings			2	Denduit Folicy	AI	Ildentities	3 Policy Settings	Mar 16, 2020			
Block Page Appearance											
Integrations											
Reporting	>										
Admin	>										
Investigate											
(←) → ୯ ଜ	U	🔒 🗝 http:	s://dasl	hboard.umbrella.com/o/3050180/#/deplo	yments/core/roamingdevices			⊘ ☆		⊻	III\ 🖽
Cisco Umbrella				F5-Server-1	Offline DNS Layer Encryption	n: disabled			21 hours a	go	~
Cisco Umbrella				F5-Server-1	Offline DNS Layer Encryption	n: disabled			21 hours a	go	~
Cisco Umbrella ^{Overview} Deployments	~	-		F5-Server-1	Offline DNS Layer Encryption Protected & Encrypt Layer	n: disabled			21 hours ag	go	~
Cisco Umbrella Overview Deployments Core Identities	~	-	0	F5-Server-1 Redouane	Offline DNS Layer Encryption Protected & Encrypt Layer DNS Layer Encryption	n: disabled			21 hours ag 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Networks	~	-	0	F5-Server-1 Redouane	Offline DNS Layer Encryptor Protected & Encryptor Elayer DNS Layer Encryptor	1: disabled oted at the DNS 1: enabled			21 hours at 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Networks Network Devices	~	-	0	F5-Server-1 Redouane Roaming Computer Information Identity Name ∠	Offline DNS Layer Encryptor Protected & Encrypt Layer DNS Layer Encryptor	1: disabled			21 hours ag 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Network Network Devices Roaming Computers	~	-	0	F5-Server-1 Redouane Roaming Computer Information Identity Name Z Redouane Hostname	Offine DNS Layer Encryptor Protected & Encryptor Construction DNS Layer Encryptor DNS Layer Encryptor	t disabled			21 hours ag	go	~
Cisco Umbrella Overview Deployments Core Identities Networks Network Devices Roarning Computers Mobile Devices	~			F5-Server-1 Redouane Roaming Computer Information Identity Name Redouane Hostname Redouane	Offline DNS Layer Encryptor Protected & Encryptor Layer DNS Layer Encryptor DNS Layer Encryptor	t disabled			21 hours ag	go	~
Cisco Umbrella Overview Deployments Core Identities Networks Network Devices Rearning Computers Mobile Devices Chromebook Users	~			F5-Server-1 Redouane Roaming Computer Information Identity Name Hostname Redouane OS Version Windows 10	Offline DNS Layer Encryptor Protected & Encryptor Layer DNS Layer Encryptor UNS Layer Encryptor UNS Layer Encryptor UNS Layer Encryptor Layer DNS Layer Encryptor Layer DNS Layer Encryptor Layer DNS Layer Encryptor Layer DNS Layer Encryptor Layer Layer Layer DNS Layer Encryptor Layer Layer Layer DNS Layer Encryptor Layer Layer DNS Layer Encryptor Layer Layer	t disabled ted at the DNS t enabled Last 56 42 m	Synced		21 hours a 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Networks Network Roarning Computers Mobile Devices Chromebook Users Configuration	~		0	F5-Server-1 Redouane Roaming Computer Information Identity Name Redouane Hostname Redouane OS Version Windows 10	Offline DNS Layer Encryptor Protected & Encryptor Layer DNS Layer Encryptor DISTOP-12255ED Client Type Umbrelia RC Version: 2.2.3	to disabled toted at the DNS tote at t	Synced ninutes ago		21 hours ay 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Networks Network Devices Roaming Computers Mobile Devices Chromebook Users Configuration Domain Management	~			F5-Server-1 Redouane Roaming Computer Information Identity Name Redouane Hostname Redouane OS Version Windows 10 Security Information	Offline DNS Layer Encryptor Protected & Encryptor Layer DNS Layer Encryptor Light and the encryptor DNS Layer Encryptor Light and the encryptor United and the encryptor	tr disabled toted at the DNS tr enabled Last 156 42 m	Synced ninutes ago		21 hours a 42 minutes ago	÷	~
Cisco Umbrella Overview Deployments Core Identities Network Network Devices Roaming Computers Mobile Devices Chromebook Users Configuration Domain Management Sites and Active Directory	×			F5-Server-1 Redouane Roaming Computer Information Identity Name Redouane Hostname Redouane OS Version Windows 10 Security Information Status © Protected	Offline DNS Layer Encryptor Protected & Encryptor Layer DNS Layer Encryptor Original Hostname DESKTOP-12255ED Client Type Umbrella RC Version: 2.2.3 DNS Layer Security M Yes	t: disabled bited at the DNS t: enabled Last 56 42 m IP Li VD	: Synced ninutes ago ayer Enforcement sabled	Last Active Po © Demo-Polic	21 hours at 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Networks Network Devices Roaming Computers Chromebook Users Chromebook Users Configuration Domain Management Sites and Active Directory Internal Networks	~			F5-Server-1 Redouane Roaming Computer Information Identity Name Redouane OS Version Windows 10 Security Information Status Protected Tage:	Offine DNS Layer Encryptor Protected & Encryptor Layer DNS Layer Encryptor DNS Layer Security DNS Layer Security Yes	t disabled ted at the DNS t enabled Last 156 42 m IP Li VDI	Synced ninutes ago ayer Enforcement isabled	Last Active Po Demo-Polic	21 hours at 42 minutes ago	;	~
Cisco Umbrella Overview Deployments Core Identities Network Network Devices Roarning Computers Chromebook Users Chromebook Users Configuration Domain Management Sites and Active Directory Internal Networks Root Certificate	Ŷ			F5-Server-1 Redouane Roaming Computer Information Identify Name 2 Redouane Hostname Redouane OS Version Windows 10 Security Information Status Protected Tags: PADD TAG	Offine DNS Layer Encryptor Layer DNS Layer Encryptor DNS Layer Encryptor DNS Layer Encryptor DNS Layer Encryptor DNS Layer Encryptor DNS Layer Encryptor DNS Layer Security DNS Layer Security Yes	tr disabled toted at the DNS tr enabled Last 556 42 m IP Li VDi	Synced ninutes ago ayer Enforcement sabled	Last Active Po Demo-Polic	21 hours at 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Networks Network Devices Rearning Computers Chromebook Users Configuration Domain Management Sites and Active Directory Internal Networks Root Certificate Service Account Exceptions	×			F5-Server-1 Redouane Roaming Computer Information Identity Name Redouane Postname Redouane OS Version Windows 10 Security Information Status Protected Tags: ADD TAG	 Offline DNS Layer Encryptor Layer DNS Layer Encryptor Layer DNS Layer Encryptor Cliginal Hostname DESKTOP-12255ED Client Type Umbrelia RC Version: 2.2.3 DNS Layer Security M Yes 	tr disabled toted at the DNS tr enabled 56 42 m IP Li VDI	Synced ninutes ago ayer Enforcement sabled	Last Active P¢ ♥ Demo-Polic	21 hours ay 42 minutes ago	go	~
Cisco Umbrella Overview Deployments Core Identities Network Network Devices Roarning Computers Nobile Devices Chromebook Users Configuration Domain Management Sites and Active Directory Internal Networks Root Certificate Service Account Exceptions	~			F5-Server-1 Redouane Roaming Computer Information Medouane Hostname Redouane Nos Version Windows 10 Security Information Status e Protected Tags: • ADD TAG DELETE	 Offline DNS Layer Encryptor Layer DNS Layer Encryptor Layer DNS Layer Encryptor Original Hostname DESKTOP-12255ED Client Type Umbrella RC Version: 2.2.3 DNS Layer Security Ares 	tr disabled ted at the DNS tr enabled t56 Last ↓P Li ↓P Li ↓Di	: Synced ninutes ago ayer Enforcement sabled	Last Active Pc ♥ Demo-Polic	21 hours as 42 minutes ago	go	~ ~
Cisco Umbrella Overview Deployments Core Identities Networks Network Devices Roarning Computers Mobile Devices Chromebook Users Chromebook Users Chromebook Users Configuration Domain Management Sites and Active Directory Internal Networks Root Certificate Service Account Exceptions Pellicies	~ ~ ~			F5-Server-1 Redouane Roaming Computer Information Identity Name Redouane Hostname Redouane OS Version Windows 10 Security Information Status Protected Tags:	Offline DNS Layer Encryptor Layer DNS Layer Encryptor Criginal Hostname DESKTOP-12255ED Client Type Umbrella RC Version: 2.2.3 DNS Layer Security Yes	tr disabled bited at the DNS tr enabled 156 Last 107	Synced ninutes ago ayer Enforcement sabled	Last Active Pc ♥ Demo-Polic Results per page: 10 ∨	21 hours as 42 minutes ago	go c.o.	SE SE

Navigate to **Policies > Management > All Policies**, Click the **Policy Tester** to test the policy **Demo-Policy**.

← → ♂ ☆	0	🔒 == h	ittps://dashb	oard.umbrella.com/o/3050180/#/policies/management/policies	⊍ ☆	ſ	III\ 🗉 📽					
Cisco Umbrella		⊜	diada cisco	Policies / Management All Policies •		(B) Add	Policy Tester					
Overview			Dellaiss d	lateto the security protection, estensory settings, and individual dest	insting lists you can apply to some or all of your ideal	ities Delleies als						
Deployments	>		control lo	g levels and how block pages are displayed. Policies are enforced in a the same identity. To change the priority of your policies, simply d	n a descending order, so your top policy will be applie rag and drop the policy in the order you'd like. More r	d before the seco	ond if					
Policies	~	they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in this article.										
Management												
All Policies				Deliau Tenter								
Policy Components				POIICY TESLET Test whether a destination will be allowed or blocked for an identity. If		î						
Destination Lists				you receive results you don't expect or want, reorder or refine your policies and run the test again. For more information, see Test a Policy.								
Content Categories				Identities								
Application Settings				Ex: Roarning Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)								
Security Settings				× •	Test results will appear here							
Block Page Appearance				Redouane ×								
Integrations	•			Destination								
Reporting				Note: Currently URLs are not supported www.facebook.com								
Admin				RESET RUN TEST								
Investigate												
			-									

Under **Identities**, select the machine 's hostname **Redouane**, enter the URL <u>www.facebook.com</u>, click **Run TEST**, in the **Results** section, you should see that the Access is blocked by the policy **Demo-Policy** as expected.

(←) → C' @	0 🔒 🗝	https://dashk	ooard.umbrella.com/o/3050180/#/policies/management/policies	··· 🗵 🌣	lu'	\ 🗉 🔹
Cisco Umbrella	0	diada cisco	Policies / Management All Policies I		Add	Policy Tester
Overview		Dolloios	distate the security protection, extensory settings, and individual de-	stination lists you can apply to some or all of your identities. D		
Deployments	>	control lo	actate the security protection, category settings, and individual despine the security protection, category settings, and individual despine the setting of	in a descending order, so your top policy will be applied befor	e the secon	nd if
Policies	~	in this art	ticle.	arag and drop the policy in the order you'd like, more policy in	o can be n	buna
Management						
All Policies						
Policy Components			Policy Tester Test whether a destination will be allowed or blocked for an identity. If	Result: Destination was blocked due to a security setting	×	
Destination Lists			you receive results you don't expect or want, reorder or refine your policies and run the test argin. For more information, see Test a Policy	Triggered Identity: Redouane		
Content Categories			Identities	Destination: www.facebook.com		
Application Settings			Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)	CNAMEs: star-mini.c10r.facebook.com Result: Destination was blocked due to a security setting		
Security Settings			x •	Category Setting: Default Settings		
Block Page Appearance			Redouane ×	Policy Applied: Demo-Policy		
Integrations	•		Destination	This identity was found in 2 policies. Out of these, Demo-Policy was	s	
Reporting	>		Note: Currently URLs are not supported www.facebook.com	the higher ranked policy, so it was applied to the identity. The other policy was your default policy, which is always your lowest ranked		
Admin	<u> </u>			policy.		
Investigate			RESET RUN TEST	Note: Your actual results may differ from what's shown above if you have	the	
				Intelligent Proxy enabled, as URLs could be treated differently.		
Redouane MEDDANE MICROTEL	>					

Under **Identities**, select the machine 's hostname **Redouane**, enter the URL <u>www.games.com</u>, click **Run TEST**, in the **Results** section, you should see that the Access is blocked by the policy **Demo-Policy** as expected.



Under Identities, select the machine 's hostname Redouane, enter the URL www.4shared.com, click Run TEST, in the Results section, you should see that the Access is blocked by the policy **Demo-Policy** as expected.

(←) → C' ŵ	0 🔒 🗝	https://dashi	ooard.umbrella.com/o/3050180/#/policies/management/policies	··· 🖂 🕁	lil\	•
Cisco Umbrella	€	cisco	Policies / Management All Policies •		b	Policy Tester
Overview		Dellalas			-1	
Deployments	>	control lo they shar	Sictate the security protection, category settings, and individual des og levels and how block pages are displayed. Policies are enforced i e the same identity. To change the priority of your policies, simply of	thation lists you can apply to some or all of your identities. Policies in a descending order, so your top policy will be applied before the frag and drop the policy in the order you'd like. More policy info can	also secon be fo	d if und
Policies	~	in this ar	licle.			
Management						
All Policies			Policy Tester	×		
Policy Components			Test whether a destination will be allowed or blocked for an identity. If			
Destination Lists			you receive results you don't expect or want, reorder or refine your policies and run the test again. For more information, see Test a Policy.			
Content Categories			Identities			
Application Settings			Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)			
Security Settings			X ¥	Test results will appear here		
Block Page Appearance			Redouane *			
Integrations	ľ		Destination			
Reporting	>		Note: Currently URLs are not supported www.4shared.com			
Admin	>					
Investigate			RESET RUN TEST			
Redouane MEDDANE	>			Sorted by Order of Enforcem	ient	
MICROTEL						
	0 0-	https://dashk	nosed umbralla.com (o/2020.190/#/oolicios/management/oolicios	··· 🖸 🔶	hits.	E (1)
			Policies / Management	W		
Cisco Umbrella		cisco	All Policies •	A	dd	Policy Tester
Overview		Policies	lictate the security protection, category settings, and individual des	tination lists you can apply to some or all of your identities. Policies	also	
Deployments	>	control lo	ing levels and how block pages are displayed. Policies are enforced in the the same identity. To change the priority of your policies, simply of	in a descending order, so your top policy will be applied before the	secon	d if
Policies	~	in this art	licle.	and and a op the policy in the order you a like. More policy into car	i be io	unu
Management						
All Policies			Delieu Teatra	Devile		
Policy Components			POIICY LESTER	Result: * Destination was blocked due to a security setting		
Destination Lists			you receive results you don't expect or want, reorder or refine your policies and run the test again. For more information. see Test a Policy	Triggered Identity: Redouane		
Content Categories			Identities	Destination: www.4shared.com		
Application Settings			Ex: Roarning Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)	Result: Destination was blocked due to a security setting Category Setting: Default Settings		
Security Settings			x •	Categorization: File Transfer Services		
Block Page Appearance			Redouane ×	This identity was found in 2 policies. Out of these. Dome. Definitions		
Integrations			Destination	the higher ranked policy, so it was applied to the identity. The other		
Reporting	>		Note: Currently URLs are not supported www.4shared.com	policy was your default policy, which is always your lowest ranked policy.		
Δrdmin	~			Note: Your actual results may differ from what's shown above if you have the		
Investigate	-		RESET RUN TEST	Intelligent Proxy enabled, as URLs could be treated differently.		
investigate						
Redouane MEDDANE MICROTEL	>			Sorted by Order of Enforcem	ient	

From the Client PC, try to access the URLs <u>www.facebook.com</u>, <u>www.games.com</u> and <u>www.4shared.com</u>. You should see the default Block Page displayed from Umbrella.

← → ♂ û	🛛 📓 https://block.opendns.com/main?url=88888815716668706780807615688078&ablock&server=fra19&prefs=&tagging=&nre	f … 🛛 🌣	⊻ III\ 🗉 📽
	cisco: Cisco Umbrella		
	Ce site est bloqué à cause du filtrage du contenu.		
	www.facebook.com		
	Désolé, www.facebook.com a été bloqué par votre administrateur réseau.		
	Ce site a été bloqué en raison des catégories sumares: Social Networking		
	> Détails du diagnostic		
	Conditions Politique de confidentialité Contact		
← → ♂ ☆	🛿 🚔 https://block.opendns.com/main?url=888888152184736683706915688078&ablock&server=fra19&prefs=&tagging=&nref	⊌ ☆	⊻ III\ 🗉 📽
	<text><text><text><text><text><text><text></text></text></text></text></text></text></text>		
	A http://block.papadar.com/main2utl-8888881C736C78208415C880788ablock&scauer-fra108urafe-&stansion-&suraf	··· 🖂 💠	↓ ₩\ @ @
	Ce site est bloqué à cause du filtrage du contenu. Www.games.com Désolé, www.games.com a été bloqué par votre administrateur réseau. Ce site a été bloqué en raison des catégories subartes: Games > Détails du diagnostic	у н	
	Conditions Politique de confidentialité Contact		

Navigate to **Reporting > Core Reports >** Activity **Search**, you should see the log about the attempts blocked by Umbrella for the **Client PC**.

← → C ^a	0- 🖨 🕖	https://dashb	oard.umbrella.co	m /o/3050180/#/	eports/activity	?encodedFilters=JTdCJTIyc2	2VsZWN0ZWREYXRIU	mFuZ2VJZHglMjIlN	40E •••	☑ ☆	<u>↓</u> III\	•
Cisco Umbrella					F	ree Trial: You have 13 d	ays left. VIEW PRIC	ING & PURCHASE				
Core Reports		ahaha	Reporting / Co	re Reports					6		🛱 LAST 2	4 HOURS -
Security Overview	9	cisco	Activity	Search					Sch	edule Download		TICORO
Security Activity												
Activity Search												
App Discovery		U	Q Search rec	quest activity		Advanc	ced • CLEAR			Columns	All Request	s 🔻
Additional Reports			CONTENT CATEG	GORIES Social Ne	working X							
Total Requests				0	O Viewin	g activity from Mar 16, 2020 a	t 4:31 PM to Mar 17, 2	020 at 4:31 PM				
Activity Volume		Personee		Salast All	0	,			Resu	lts per page: 50 🔻	1 - 50 <	>
Top Destinations			wed	Select All								
Top Categories			ked ied		Identity	Destination		Identity Used b	y Policy 🔞	Internal IP	External IP	>====
Top Identities					Redoua	ine www.facebook.co	m	Redouane		10.254.253.120	105.96.14.98	•
Management	'	Protocol		Select All	Redoua	ne www.facebook.co	m	Redouane		10.254.253.120	105.96.14.98	····
Exported Reports			TP TPS		Redoua	me www.tacebook.co	m	Redouane		10.254.253.120	105.96.14.98	
Scheduled Reports					Redoua	ne www.facebook.co	m	Redouane		10.254.253.120	105.96.14.98	
Admin Audit Log		Event Typ	e	Select All	Redoua	ne www.facebook.co	m	Redouane		10.254.253.120	105.96.14.98	
Admin	>		Dication		Redoua	ne www.facebook.co	m	Redouane		10.254.253.120	105.96.14.98	
			NAMD									
← → ♂ ☆		https://dashb	oard.umbrella.co	om/o/3050180/#/	reports/activity	/				☑ ☆	<u>↓</u> III\	
← → ♂ ŵ Cisco Umbrella	0 🔒 =0	https://dashb	oard.umbrella.co	om/o/3050180/#/	reports/activity	F ree Trial: You have 13 d.	ays left. VIEW PRIC	ING & PURCHASE			<u>↓</u> III\	. [] .
(← → ໕ ໖ Cisco Umbrella ^{Core Reports}	0	https://dashb	Reporting / Co	m/o/3050180/#/	reports/activity F	Free Trial: You have 13 d	ays left. VIEW PRIC	ING & PURCHASE		 □ ☆ □ ↓ 	⊻ III\ ≅ LAST 2	
← → C' ŵ Cisco Umbrella Core Reports Security Overview	0 4	https://dashb	Reporting / Co	mr/o/3050180/#/ are Reports / Search	reports/activity	Free Trial: You have 13 d	ays left. VIEW PRIC	ING & PURCHASE	••• (Sch	E Composed	⊻ III\ ∰ LAST 2	4 HOURS -
← → C ^a ŵ Cisco Umbrella Core Reports Security Overview Security Activity	0 🖬 ===	https://dashb بالبداله cisco	Reporting / Co Activity	m/o/3050180/#/ we Reports / Search	reports/activity	/ Free Trial: You have 13 d	ays left. VIEW PRIC	ING & PURCHASE	••• (Sch	E the Download	⊻ IIN	4 HOURS ~
← → C û û Cisco Umbrella Core Reports Security Overview Security Activity Activity Search		nltulu cisco	Reporting / Co Activity	mr/o/3050180/#/ rre Reports / Search	reports/activity	r ree Trial: You have 13 d	ays left VIEW PRIC	ING & PURCHASE	••• ((Sch		± 11\ ≝ LAST 2	4 HOURS -
← → C ☆ ☆ Cisco Umbrella Core Reports Security Overview Security Activity Activity Search App Discovery		athatha cisco	Reporting / Co Activity	m/o/3050180/#/ we Reports / Search quest activity	reports/activity	/ Free Trial: You have 13 d Advant	ays left VIEW PRIC	ING & PURCHASE	•••		⊥ IIN LAST 2	4 HOURS ~
← → C' ☆ Cisco Umbrella Core Reports Security Overview Security Activity Activity Search App Discovery Additional Reports		allulli cisco	Reporting / Co Activity	re Reports / Search quest activity	reports/activity F	/ iree Trial: You have 13 d Advand	ays left VIEW PRIC	ING & PURCHASE	•••	Columns	⊥ IIN LAST 2	4 HOURS T
C → C ☆ Cisco Umbrella Core Reports Security Overview Security Activity Activity Search App Discovery Additional Reports Total Requests		etter by	Reporting / Co Activity	m/o/3050180/#/ re Reports / Search quest activity sories Social Ne	tworking ×	/ Free Trial: You have 13 d Advance g activity from Mar 16, 2020 a	ays left VIEW PRIC	ING & PURCHASE	 Sch		보 III	4 HOURS ~
C → C ☆ Cisco Umbrella Core Reports Security Overview Security Activity Activity Search App Discovery Additional Reports Total Requests Activity Volume		FILTER BY: Response	Reporting / Co Activity Q. Search rec CONTENT CATEG	m/o/3050180/#/ vre Reports / Search quest activity social Ne Select All	working ×	r ree Trial: You have 13 d Advant g activity from Mar 16, 2020 a	ays left VIEW PRIC	ING & PURCHASE	 Sch		± III)	s v
← → C ^a ŵ Cisco Umbrella Core Reports Security Overview Security Activity Activity Search Additional Reports Total Requests Activity Volume Top Destinations		ritiniti cisco Filter By: Response	Reporting / Co Activity Q. Search rec CONTENT CATEGO	m/o/3050180/#/ ve Reports / Search quest activity social Ne Q Select All	working ×	ree Triat: You have 13 d Advanc g activity from Mar 16, 2020 a	ays left VIEW PRIC	ING & PURCHASE	C () Sch	Columns	± IIN ▲ LAST 2 All Request 1 - 50 <	4 HOURS -
C → C ☆ ŵ Cisco Umbrella Core Reports Security Overview Security Activity Activity Search App Discovery Additional Reports Total Requests Activity Volume Top Destinations Top Categories		FILTER BY: Response O Allon O Bloc	Reporting / Co ACTIVITY	m/o/3050180/#/ ve Reports v Search quest activity contes Social Ne Select All	teports/activity F tworking × Viewin K	ree Trial: You have 13 d ree Trial: You have 13 d Advan g activity from Mar 16, 2020 a Identity Used by Policy	ays left VIEW PRIC ced • CLEAR it 4:31 PM to Mar 17, 2 Internal IP	ING & PURCHASE	Sch Resu Action	Categories	± IIN	4 HOURS - 5 - >
Core Reports Core Reports Security Overview Security Activity Security Activity Activity Search App Discovery Additional Reports Total Requests Activity Volume Top Destinations Top Categories Top Identities		Image: state	Reporting / Co Activity Q. Search red CONTENT CATEG	m/o/3050180/#/ we Reports / Search quest activity Social Ne Select All	working × vworking ×	7 Free Trial: You have 13 d Free Trial: You have 13 d Advanc g activity from Mar 16, 2020 a Identity Used by Policy	ays left VIEW PRIC	ING & PURCHASE	Control Contro		± IIN ≧ LAST 2 All Request 1 - 50 <	4 HOURS ▼
C → C ☆ C ☆ C ☆ C is co Umbrella Core Reports Security Overview Security Overview Security Activity Activity Search Activity Search Additional Reports Total Requests Activity Volume Top Destinations Top Categories Top Identities Management		Attps://dashb Attps://dashb Pluter By: Response Allow Protocol Protocol	Reporting / Co Activity Q. Search rec contrast catego wed ked	m/o/3050180/#// re Reports / Search quest activity select All Select All	tworking ×	ree Trial: You have 13 d ree Trial: You have 13 d Advant g activity from Mar 16, 2020 a Mentity Used by Policy Redouane Redouane Redouane Redouane Redouane Redouane	ays left VIEW PRIC	ING & PURCHASE	Control Contro		± IIN ▲ LAST 2 All Request 1 - 50 <	4 HOURS ▼
C → C ☆ C ☆ Cisco Umbrella Core Reports Security Overview Security Overview Security Activity Activity Search Activity Search Additional Reports Total Requests Activity Volume Top Destinations Top Categories Top Identifies Management Exported Reports		FR.TER BY. Protocol Protocol Protocol Protocol Protocol Protocol Protocol	Reporting / Co Activity Q. Search red context CATEO wed ked lied	m/o/3050180/#/ ve Reports / Search quest activity quest activity Q Select All Select All	working ×	ree Trial: You have 13 d ree Trial: You have 13 d Advant g activity from Mar 16, 2020 a Identity Used by Policy Redouane Redouane Redouane Redouane Redouane Redouane Redouane	ays left VIEW PRIC	ING & PURCHASE	Set Set Resu Action • Blocked • Blocked • Blocked		± III\	4 HOURS - S - S - S - D - D - D - D - D - D - D - D
Core Reports Core Reports Core Reports Security Overview Security Overview Core Reports Security Activity Activity Search Activity Search Activity Search Cotal Reports Total Reports Total Requests Activity Volume Top Destinations Top Categories Top Identities Management Exported Reports Scheduled Reports		FLTER BY. Response O Alloo O Bloc O Protocol M HTT M HTT	Reporting / Co Activity Q Search rec CONTENT CALL wed ked died	m/o/3050180/#/ ve Reports / Search quest activity 20035 Social Ne Q Select All	working ×	ree Trial: You have 13 d ree Trial: You have 13 d Advant g activity from Mar 16, 2020 a Redouane	ays left VIEW PRIC ced CLEAR t 4-31 PM to Mar 17, 2 Internal IP 10.254 253.120 10.254 2554 2554 10.254 2554 2554 10.254 2554 1	ING & PURCHASE	Resu Action Blocked Blocked Blocked Cellone		± III\	4 HOURS - 3 - 3 - 3 - - - - - - - - - - - - - -
Core Reports Core Reports Security Overview Security Activity Security Activity Activity Search App Discovery Additional Reports Total Requests Activity Volume Total Requests Activity Volume Total Requests Activity Volume Top Destinations Top Categories Top Identities Management Exported Reports Scheduled Reports Admin Audit Log		PRITER BY Response ○ Allor ○ Protocol ○ # HTT ○ # HTT Event Typ ○ # Add	Reporting / Co ACTIVITY Q. Search red CONTENT CATEG Wed ked lied	m/o/3050180/#/ ve Reports / Search quest activity 20085 Social Ne Select All Select All Select All	working X Viewin	ree Trial: You have 13 d Tree Trial: You have 13 d Advanc Advanc advance advan	Ays left VIEW PRICE Cect CLEAR t.4.31 PM to Mar 17, 2 Internal IP 10.254.253.120 10.254.255.120 10.254.255.255 10.254.255.255 10.254.255.255 10.254.255 10.254.255.255 10.	ING & PURCHASE	Resu Action Blocked Blocked Blocked Blocked Blocked Blocked Cked		± IIN	4 HOURS - 4 HOURS - 5 - 3 - 6 - 10 -
Core Reports Core Reports Security Overview Security Overview Security Activity Security Activity Activity Search Activity Search Additional Reports Additional Reports Total Requests Activity Volume Top Destinations Top Destinations Top Destinations Top Destinations Top Identities Management Exported Reports Scheduled Reports Addmin Audit Log Addmin		Protocol ■ Protocol	Reporting / Co ACTIVITY Q. Search red content cated wed ked ied IP PS ie ivitus	m/o/3050180/#/ ve Reports v Search quest activity social Ne Select All Select All	teports/activity s tworking × Viewin	ree Trial: You have 13 d ree Trial: You have 1	ays left VIEW PRIC Ced ▼ CLEAR t 4.31 PM to Mar 17, 2 Internal IP 10.254.253.120 10.254.253.120 10.254.253.120 10.254.253.120 10.254.253.120 10.254.253.120 10.254.253.120 10.254.253.120	ING & PURCHASE	Resu Action Blocked Blocked Blocked Blocked Blocked Blocked Blocked Blocked Blocked Blocked Blocked		± IIN	x ■ (*) x + HOURS × x + HOUR

← → ♂ ☆	🖲 🖶 🗝 h	ttps://dashb	ooard.umbrella.com/	o/3050180/#/r	reports/activity?encod	dedFilters=JTdCJTlyc2VsZWN	NOZWREYXRIUmFuZ2VJZHgIMj	IIMOE 🚥 🖂	☆	<u>↓</u> III\ (D ©
Cisco Umbrella	⊜	uluilu cisco	Reporting / Core P Activity S	Reports Search				Schedule		🛗 LAST 24 H	IOURS -
Security Overview											
Security Activity		•		at a still de s				_			
Activity Search		U	C Search reque	St activity		Advanced +	CLEAR		Columns A	I Requests	
App Discovery			CONTENT CATEGORI	ES Games 🗙	t						
Additional Reports		FILTER BY		Q	Viewing activit	y from Mar 16, 2020 at 4:31 P	M to Mar 17, 2020 at 4:31 PM				
Total Requests		Response	9	Select All				Results per p	age: 50 👻 1 -	4 of 4 < >	
Activity Volume			wed		1. Annalas	Beerlander				-	
Top Destinations		Bloc	ked kied		Identity	Destination	Identity Used by Policy 🍯	Internal IP	External IP AC	ion ;	
Top Categories					Redouane	www.games.com	Redouane	10.254.253.120	105.96.14.98	Blocked	2
Top Identities		Protocol		Select All	Redouane	www.games.com	Redouane	10.254.253.120	105.96.14.98	Allowed	2
Management			TP TPS			www.games.com		10.254.253.120	105.96.14.98	Allowed (2
Exported Reports					< neurodane	www.guites.com		10.104.100.110	105.50.14.50		>
Scheduled Reports		Event Typ	0e	Select All							
Admin Audit Log			plication								
Admin	>	Cise	co AMP ntent Category								
Investigate		□ III Des	stination List								
← → C ☆ Cisco Umbrella Core Reports Security Overview	0 4>	https://dash	Reporting / Core Activity	Reports Search	1/reports/activity?enc	odedFilters=JTdCJTlyc2VsZl	WN0ZWREYXRIUmFuZ2V/ZHg	iMjilM0: ••• 🤅	Download	⊻ III' ∰ LAST :	\ 🗊 4
Security Activity											
Activity Search			Q Search requ	lest activity		Advanced •	CLEAR		E Columns	All Request	ts 🔻
App Discovery			CONTENT CATEGO	RIES File Tran	sfer Services X						
Additional Reports				0	Viewing acti	vity from Mar 16, 2020 at 4:3	1 PM to Mar 17, 2020 at 4:31 PM	A			
Total Requests		Respons		Select All				Results	s per page: 50 🔻	1 - 50 <	>
Activity Volume			owed	OCICCI Par							
Top Destinations			ocked		Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action	>
Top Categories					Redouane	www.4shared.com	Redouane	10.254.253.1	20 105.96.14.98	Blocked	.
Top Identities		Protocol		Select All	Redouane	www.4shared.com	Redouane	10.254.253.1	20 105.96.14.98	Blocked	•
Management		⊡ен	TTP TTPS		Redouane	www.4shared.com	Redouane	10.254.253.1	20 105.96.14.98	Blocked	•
Exported Reports					Redouane	www.4shared.com	Redouane	10.254.253.1	20 105.96.14.98	Blocked	•
Scheduled Reports		Event Ty	rpe	Select All	Redouane	dc393.4shared.com	Redouane	10.254.253.1	20 105.96.14.98	Allowed	•
Admin Audit Log		□ Â Ar	ntivirus oplication		Redouare	dc400 4shared com		10.254.253.1	20 105.96.14.98		
Admin	>		sco AMP		Redouane	dc612.4shared.com	Redouane	10.254.253.1	20 105.96.14.98	Allowed	<u> </u>

Network Security All-in-one WorkBook VPN Technologies

Lab 1: Static VTI Point-To-Point tunnel



R1:

interface Lo0
ip address 172.16.1.1 255.255.255.0
!
<pre>interface FastEthernet0/0</pre>
ip address 192.0.2.1 255.255.255.0
no shutd
!
ip route 0.0.0.0 0.0.0.0 192.0.2.2

R2:

interface FastEthernet0/0
ip address 192.0.2.2 255.255.255.0
no shutd
!
interface FastEthernet0/1
ip address 192.51.100.2 255.255.255.0
no shutd
!
ip route 10.10.10.0 255.255.255.0 192.51.100.1
ip route 172.16.1.0 255.255.255.0 192.0.2.1

R3:

interface Lo0
 ip address 10.10.10.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.51.100.1 255.255.255.0
 no shutd
!

ip route 0.0.0.0 0.0.0.0 192.51.100.2

Create an ISAKMP policy with the following parameters:

- 1. Authentication: **pre-shared**
- 2. Encryption algorithm: AES 128
- 3. Hash algorithm: SHA
- 4. Key exchange method: 14
- 5. Lifetime: 1 hour

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authe pre
R1(config-isakmp)#hash sha
R1(config-isakmp)#encr aes 128
R1(config-isakmp)#group 14
R1(config-isakmp)#lifetime 3600
```

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authe pre
R3(config-isakmp)#hash sha
R3(config-isakmp)#encr aes 128
R3(config-isakmp)#group 14
R3(config-isakmp)#lifetime 3600
```

On R1 create a PSK and bind it to the IP address of R3:

R1(config)#crypto isakmp key cisco address 192.51.100.1

On R3 create a PSK and bind it to the IP address of R1:

R3(config)#crypto isakmp key cisco address 192.0.2.1

On R1 and R3 create an IPsec transform set for user traffic protection. Use ESP with 128 bit AES as the encryption transform, and use ESP with SHA (HMAC variant) as the authentication transform:

R1(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac R3(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac

Create an IPsec profile and include transform set in the profile:

```
R1(config)#crypto ipsec profile MYPROFILE
R1(ipsec-profile)#set transform-set MYSET
```

R3(config)#crypto ipsec profile MYPROFILE R3(ipsec-profile)#set transform-set MYSET

On R1 create a new tunnel interface. Configure the interface to use the IP address of fa0/0. Specify a tunnel source fa0/0 and a tunnel destination 192.51.100.1:

R1(config)#int tunnel 0
R1(config-if)#ip unnumbered fa0/0
R1(config-if)#tunnel source fa0/0
R1(config-if)#tunnel destination 192.51.100.1

On R3 create a new tunnel interface. Configure the interface to use the IP address of fa0/0. Specify a tunnel source fa0/0 and a tunnel destination 192.0.2.1:

R3(config)#int tunnel 0 R3(config-if)#ip unnumbered fa0/0 R3(config-if)#tunnel source fa0/0 R3(config-if)#tunnel destination 192.0.2.1

Specify IPsec as the tunnel encapsulation. Specify the traffic protection policy by referencing the configured IPsec profile.

R1(config)#interface tunnel 0
R1(config-if)#tunnel mode ipsec ipv4
R1(config-if)#tunnel protection ipsec profile MYPROFILE

R3(config)#interface tunnel 0 R3(config-if)#tunnel mode ipsec ipv4 R3(config-if)#tunnel protection ipsec profile MYPROFILE

On R1 create a static route to 10.10.10.0/24:

R1(config)#ip route 10.10.10.0 255.255.255.0 tunnel 0

On R3 create a static route to 172.16.1.0/24:

R3(config)#ip route 172.16.1.0 255.255.255.0 tunnel 0

On R1 and R2. Verify the ISAKMP Security Association using the show crypto isakmp sa command, the status should be active:

R1#show crypt TPv4 Crypto T	o isakmp sa SΔKMP SΔ			
dst	src	state	conn-id status	
192.0.2.1	192.51.100.1	QM_IDLE	1001 ACTIVE	
IPv6 Crypto I	SAKMP SA			
R1#				
R3#show crypt IPv4 Crypto I	o isakmp sa SAKMP SA			
dst	src	state	conn-id status	
192.0.2.1	192.51.100.1	QM_IDLE	1001 ACTIVE	
IPv6 Crypto I	SAKMP SA			
R3#				

On R1 and R2. Verify the IPsec Security Association using the show crypto ipsec sa command. Notice there are no packets encapsulated or de-encapsulated (encrypted or decrypted):

R1#show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.0.2.1
   protected vrf: (none)
   local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
   current_peer 192.51.100.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.1, remote crypto endpt.: 192.51.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xB49AA172(3030032754)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xBD1DE05F(3172851807)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow id: 1, sibling flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4325414/3512)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0x53F6272C(1408640812)
        transform: esp-aes esp-sha-hmac,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: 3, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4187316/3513)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xA551FC8C(2773613708)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: 2, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4325414/3512)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0xB49AA172(3030032754)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
```

```
conn id: 4, flow_id: 4, sibling_flags 80000040, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4187316/3513)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
outbound ah sas:
outbound pcp sas:
R1#
```

From R1, ping 10.10.10.1 (R3 router internal IP. The ping should be successful:

R1#ping 10.10.10.1 source 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
IIIII
Success rate is 100 percent (5/5), round-trip min/avg/max = 464/490/528 ms
R1#

On R1 verify the status of the IPsec SA again. Observe the packet count for encrypted and decrypted increase by five packets. The static VTI point-to-point interface is operational:

```
R1#show crypto ipsec sa
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.0.2.1
   protected vrf: (none)
   local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
   current peer 192.51.100.1 port 500
     PERMIT, flags={origin is acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.0.2.1, remote crypto endpt.: 192.51.100.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xB49AA172(3030032754)
     PFS (Y/N): N, DH group: none
     inbound esp sas:
      spi: 0xBD1DE05F(3172851807)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: 1, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4325414/3444)
        IV size: 16 bytes
        replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)
      spi: 0x53F6272C(1408640812)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: 3, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4187315/3445)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xA551FC8C(2773613708)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: 2, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4325414/3444)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
      spi: 0xB49AA172(3030032754)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 4, flow_id: 4, sibling_flags 80000040, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4187315/3445)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
     outbound ah sas:
     outbound pcp sas:
R1#
```

Lab 3: VPN Site-to-Site with dynamic IP



Site to Site IPSec VPN with Dynamic IP Endpoint is typically used when we have a branch sites which obtains a dynamic public IP from the Internet ISP. For example an ADSL connection. One important note is that Site-to-Site VPN with Dynamic remote routers Public IP addresses can only be brought up by the remote site routers as only they are aware of the Hubs router Public IP address.

R1 the Hub has a static public IP address. R2 and R3 the spokes have a public dynamic IP addresses.

Configure the IP addressing as illustrated in the topology:

R1:

interface Loopback0
ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0
ip address 14.0.0.1 255.255.255.0
no shutdown
!
ip route 0.0.0.0 0.0.0.0 14.0.0.4

```
R2:
```

interface Loopback0
 ip address 10.2.2.2 255.255.255.0
!
interface FastEthernet0/0
 ip address 24.0.0.2 255.255.255.0
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 24.0.0.4

```
R3:
interface Loopback0
ip address 10.3.3.3 255.255.255.0
!
interface FastEthernet0/0
ip address 34.0.0.3 255.255.255.0
no shutdown
!
ip route 0.0.0.0 0.0.0 34.0.0.4
```

Configure NAT translation to translate the LAN networks connected to R1, R2 and R3. Exclude traffic between LAN networks from NAT operation. Note on R2 and R3, only the traffic coming from their LAN network to the R1's LAN network should be excluded.

```
R1(config)#ip access-list extended NAT-ACL
R1(config-ext-nacl)#deny ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
R1(config-ext-nacl)#deny ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255
R1(config-ext-nacl)#permit ip 10.1.1.0 0.0.0.255 any
R1(config)ip nat inside source list NAT-ACL interface FastEthernet0/0 overload
```

```
R2(config)#ip access-list extended NAT-ACL
R2(config-ext-nacl)#deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
R2(config-ext-nacl)#permit ip 10.2.2.0 0.0.0.255 any
R2(config)ip nat inside source list NAT-ACL interface FastEthernet0/0 overload
```

```
R3(config)#ip access-list extended NAT-ACL
R3(config-ext-nacl)#deny ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
R3(config-ext-nacl)#permit ip 10.3.3.0 0.0.0.255 any
R3(config)ip nat inside source list NAT-ACL interface FastEthernet0/0 overload
```

Enable the NAT on Lo0 (inside) and fa0/0 (outside) interfaces.

R1(config)interface Loopback0 R1(config-if)ip nat inside R1(config)interface fa0/0 R1(config-if)ip nat outside

R2(config)interface Loopback0 R2(config-if)ip nat inside R2(config)interface fa0/0 R2(config-if)ip nat outside

R1(config)interface Loopback0 R1(config-if)ip nat inside R1(config)interface fa0/0 R1(config-if)ip nat outside

Configure Interesting Traffic:

```
R1(config)#ip access-list extended VPN-TO-R2
R1(config-ext-nacl)#permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
```

```
R1(config)#ip access-list extended VPN-TO-R3
R1(config-ext-nacl)#permit ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255
```

R2(config)#ip access-list extended VPN-TO-R1 R2(config-ext-nacl)#permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255

R3(config)#ip access-list extended VPN-TO-R1 R3(config-ext-nacl)#permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255

Configure Phase 1 ISAKMP:

For ISAKMP policy use the following parameters:

1-Encryption: aes
 2-Hash: sha
 3-Authentication: pre-share
 4-Diffie-Helman: Group 1

On R1:

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 1
```

On R2:

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 1
```

On R3:

```
R3(config)#crypto isakmp policy 1
R3(config-isakmp)#encr aes
R3(config-isakmp)#hash sha
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 1
```

On R2 and R3, define the pre-shared key for authentication with the Hub R1 14.0.0.1:

R2(config)#crypto isakmp key cisco address 14.0.0.1

R3(config)#crypto isakmp key cisco address 14.0.0.1

Configure Phase 2 IPsec on Spokes R2 and R3:

On R2 and R3. Configure a transform set with AES encryption and SHA-HMAC for authentication.

R2(config)#crypto ipsec transform-set TEST esp-aes esp-sha-hmac

R3(config)#crypto ipsec transform-set TEST esp-aes esp-sha-hmac

On R2 and R3. Configure a crypto map and attach the transform-set, the peer address of R1 and the ACL that defines the interesting traffic:

R2(config)#crypto map VPNMAP 10 ipsec-isakmp % NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured. R2(config-crypto-map)# set peer 14.0.0.1 R2(config-crypto-map)# set transform-set TEST R2(config-crypto-map)# match address VPN-TO-R1

R3(config)#crypto map VPNMAP 10 ipsec-isakmp % NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured. R3(config-crypto-map)# set peer 14.0.0.1 R3(config-crypto-map)# set transform-set TEST R3(config-crypto-map)# match address VPN-TO-R1

Attach the crypto map above to the Fa0/0 interface:

R2(config)#interface FastEthernet0/0
R2(config-if)# crypto map VPNMAP

R3(config)#interface FastEthernet0/0 R3(config-if)# crypto map VPNMAP

On R1, define the pre-shared key for authentication with the Spokes R2 and R3. We configure a wildcard mask (0.0.0 0.0.0.0) for the pre-shared key because we don't know the public IP addresses of R2 and R3 since they a dynamic IP addresses. R1 will accept isakmp requests from any router which has the correct pre-shared key.

R1(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0

Remember, R2 and R3 are configured previously with a static crypto map which was referencing a peer IP address of R1 (14.0.0.1). Since the IP address of R2 and R3 are not known, we need to configure a "Dynamic Crypto Map" which will be used in the "Static Crypto Map".

First on R1 configure two transform set with AES encryption and SHA-HMAC for authentication. Note (we can use one transform set which will be used for encryption for both R2 and R3):

R1(config)#crypto ipsec transform-set TEST-TO-R2 esp-aes esp-sha-hmac R1(config)#crypto ipsec transform-set TEST-TO-R3 esp-aes esp-sha-hmac

Create a dynamic crypto map (DYNMAP-R2) and references the transform set "TEST-TO-R2" and the ACL "VPN-TO-R2":

R1(config)#crypto dynamic-map dynmap-R2 10 R1(config-crypto-map)# set transform-set TEST-TO-R2 R1(config-crypto-map)# match address VPN-TO-R2

Create a dynamic crypto map (DYNMAP-R3) and references the transform set "TEST-TO-R3" and the ACL "VPN-TO-R3":

R1(config)#crypto dynamic-map dynmap-R3 20 R1(config-crypto-map)# set transform-set TEST-TO-R3 R1(config-crypto-map)# match address VPN-TO-R3

Then create a static crypto map (VPNMAP) which uses the dynamic map configured previously:

R1(config)#crypto map VPNMAP 10 ipsec-isakmp dynamic dynmap-R2 R1(config)#crypto map VPNMAP 20 ipsec-isakmp dynamic dynmap-R3

Attach the static crypto map (VPNMAP) to the fa0/0 interface:

R1(config)#interface FastEthernet0/0 R1(config-if)#crypto map VPNMAP

To test, deny the translation of ICMP packets in the ACL "NAT-ACL"

R1(config-ext-nacl)#ip access-list extended NAT-ACL R1(config-ext-nacl)#21 deny icmp 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255 R1(config-ext-nacl)#22 deny icmp 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255

R2(config-if)#ip access-list ext NAT-ACL R2(config-ext-nacl)#15 deny icmp 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255

R3(config-if)#ip access-list ext NAT-ACL R3(config-ext-nacl)#15 deny icmp 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255

Let's try a ping from R3 to the LAN network of the HUB with a the lo0 interface as a source. Note Only the Spoke routers R2 and R3 are aware of R1 public IP address (14.0.0.1) because it is static, and therefore only the Spoke router can initiate the VPN tunnel.

R3#ping 10.1.1.1 sou lo0 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: Packet sent with a source address of 10.3.3.3 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 220/246/272 ms R3#

The ISAKMP has been established between R1 and R3:

```
R3#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
```

```
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA
C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime
Cap.
1002 34.0.0.3 14.0.0.1
Engine-id:Conn-id = SW:2
IPv6 Crypto ISAKMP SA
R3#
```

The IPsec SA is established between R1 and R3. Since one ICMP packet is lost, the number of the encrypted/decrypted packet is 4:

```
R3#show crypto ipsec sa | s local|remote|pkts
Crypto map tag: VPNMAP, local addr 34.0.0.3
local ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
local crypto endpt.: 34.0.0.3, remote crypto endpt.: 14.0.0.1
```

R3#

On R1, the Hub has only one ISAKMP sa with R3, the ISAKMP sa is not yet negociated with R2:

```
R1#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA
C-id Local
                     Remote
                                   I-VRF Status Encr Hash Auth DH Lifetime
Cap.
1003 14.0.0.1
                     34.0.0.3
                                            ACTIVE aes sha psk 1 23:54:06
      Engine-id:Conn-id = SW:3
IPv6 Crypto ISAKMP SA
R1#
```

The IPses SA on R1 shown the same number of encrypted/decrypted packets (4) :

R1#show crypto ipsec sa | s local|remote|pkts Crypto map tag: VPNMAP, local addr 14.0.0.1

<pre>local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)</pre>
<pre>remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)</pre>
<pre>#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4</pre>
<pre>#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4</pre>
<pre>#pkts compressed: 0, #pkts decompressed: 0</pre>
<pre>#pkts not compressed: 0, #pkts compr. failed: 0</pre>
<pre>#pkts not decompressed: 0, #pkts decompress failed: 0</pre>
local crypto endpt.: 14.0.0.1, remote crypto endpt.: 34.0.0.3

R1#

Let's try a ping from R2 with Lo0 as the source to the LAN network of R1:

R2#ping 10.1.1.1 sou lo0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 172/220/252 ms
R2#

The ISAKMP sa has been established between R1 and R2:

```
R2#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA
C-id Local
                     Remote
                                     I-VRF Status Encr Hash Auth DH Lifetime
Cap.
1002 24.0.0.2
                     14.0.0.1
                                            ACTIVE aes sha
                                                              psk 1 23:59:10
      Engine-id:Conn-id = SW:2
IPv6 Crypto ISAKMP SA
R2#
```

The IPsec SA on R2 shown 4 four encrypted/decrypted packets, because one ICMP echo is lost:

```
R2#show crypto ipsec sa | s local|remote|pkts
Crypto map tag: VPNMAP, local addr 24.0.0.2
local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
local crypto endpt.: 24.0.0.2, remote crypto endpt.: 14.0.0.1
```

R2#

R1 has now two ISAKMP sa with R2 and R3:

```
R1#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA
C-id Local
                                I-VRF Status Encr Hash Auth DH Lifetime
                     Remote
Cap.
1004 14.0.0.1
                     24.0.0.2
                                            ACTIVE aes sha
                                                              psk 1 23:57:24
      Engine-id:Conn-id = SW:4
1003 14.0.0.1
                     34.0.0.3
                                            ACTIVE aes sha
                                                              psk 1 23:48:25
      Engine-id:Conn-id = SW:3
IPv6 Crypto ISAKMP SA
R1#
```

Now R1 has built two IPsec sa with R2 and R3:

```
R1#show crypto ipsec sa | s local|remote|pkts
    Crypto map tag: VPNMAP, local addr 14.0.0.1
   local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
     local crypto endpt.: 14.0.0.1, remote crypto endpt.: 24.0.0.2
   local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
     local crypto endpt.: 14.0.0.1, remote crypto endpt.: 34.0.0.3
R1#
```

The show crypto session command at R1 router displays all remote Spoke routers public IP addresses:

R1#show crypto session Crypto session current status

```
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 24.0.0.2 port 500
IKEv1 SA: local 14.0.0.1/500 remote 24.0.0.2/500 Active
IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 10.2.2.0/255.255.255.0
Active SAs: 2, origin: dynamic crypto map
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 34.0.0.3 port 500
IKEv1 SA: local 14.0.0.1/500 remote 34.0.0.3/500 Active
IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 10.3.3.0/255.255.255.0
Active SAs: 2, origin: dynamic crypto map
```

Network Security All-in-one WorkBook Cisco Identity Service Engine

Lab 3: Advanced 802.1X Configuration



The challenge is: A user jdoe is allowed to access the network only through the physical port FastEthernet 0/1 of the switch and the user jwhite is allowed to access the network only through the physical port FastEthernet 0/2.

The compound conditions is as follow:

If the ISE sees in the Radius Access Request sent by the switch the Subject Radius User-Name Attribute = jdoe AND if ISE sees also the Port Radius NAS PORT Id Attribute = FastEthernet 0/1 then the ISE will apply an appropriate Authorization Profile. Otherwise ISE will deny the access, in other words if the user jdoe is connected to another physical port, the ISE server will block the network access.

If the ISE sees in the Radius Access Request sent by the switch the Subject Radius User-Name Attribute = jwhite AND if ISE sees also the Port Radius NAS PORT Id Attribute = FastEthernet 0/2 then the ISE will apply an appropriate Authorization Profile.

On Switch SW-1, configure radius service.

SW-1(config)#radius server ISE-RAD SW-1(config-radius-server)#address ipv4 192.168.1.254 SW-1(config-radius-server)#key cisco

Enable AAA and create an 802.1X authentication method list.

SW-1(config)#aaa new-model SW-1(config)#aaa authentication dot1x default group radius

Enable 802.1X authentication globally on your switch.

SW-1(config)#dot1x system-auth-control

Configure the switch for use RADIUS authorization.

SW-1(config)#aaa authorization network default group radius

Configure the switch for RADIUS accounting.

SW-1(config)#aaa accounting dot1x default start-stop group radius

Configure the port for access mode.

SW-1(config)#int fa1/0/48 SW-1(config-if)#switchport mode access

Enable 802.1X authentication on the ports Fa0/1 and Fa0/2.

SW1(config)#int fa0/1 SW1(config-if)#authentication port-control auto SW1(config-if)#dot1x pae authenticator

SW1(config)#int fa0/2 SW1(config-if)#authentication port-control auto SW1(config-if)#dot1x pae authenticator

Create Two users.

Navigate to Administration > Identity Management > Identities.

Create a user jdoe with password Cisco123.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	୍ ଡ	•	
► System	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC				
	y Sources Identity Source Sequences				
G	Naturek Annane Heare Liet 5 Naur Maturek Annane Hear				
Users	Vetwork Access User				
Latest Manual Network Scan Results	* Name jsoe				
	Password Type: Internal Users •				
	Password Re-Enter Password				
	*Login Password Generate Password				
	Enable Password ()				
	User Information				
	Account Options				
	Account Disable Policy				
	Vuser Groups				
	Select an item 📀 — 🕂				
	Submit Cancel				

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	۹,	0	• •
System	Network Resources				
✓Identities Groups External Identity	Sources Identity Source Sequences				
0	Mahunde Annana Hanza List s. Nam Mahunak Annana Hana				
Users	Network Access User Network Access User Network Access User				
Latest Manual Network Scan Results					
	* Name juhite				
	Status 🛃 Enabled 💌				
	Email				
	▼ Passwords				
	Password Type: Internal Users				
	Password Re-Enter Password				
	* Login Password Generate Password ()				
	Enable Password ()				
	User Information				
	Account Options				
	Account Disable Policy				
	Presoure Groune				
	* vaei olivupa				
	Select an item 💿 🗕 🚽				

Create a user jwhite with password Cisco1234.

-Index Identity Services Engine	Home Conte	xt Visibility	rations 🕨 I	Policy	- Administration	Work Cent	ers			License W	arning 🔺	Q	0	0	•
System Identity Management	Network Resources	Device Portal Mar	nagement p	xGrid Servic	es 🔹 🕨 Feed Se	rvice + Threat	Centric NAC								
✓ Identities Groups External Identity	Sources Identity S	Source Sequences	Settings												
0	Network Acco	es lleem													
Users	Network Acce	ss users													
Latest Manual Network Scan Results												Selecte	d 0 Total	3 🏀 i	∰ •
	/ Edit 🕂 Add	📴 Change Status 👻	Pimport	Export 👻	🗙 Delete 👻 🖳	Duplicate				Show	Al			*	8
	Status	Name		Description	1	First Name	Last Name	Email Address	User Identity Groups	Admin					
	🗌 🗹 Enabled	🡤 jdoe				John	Doe								
	🗌 🔽 Enabled	👤 jwhite													
	🗌 🗹 Enabled	👤 test													

Create Network Device Group

Navigate to Administration > Network Resources > Network Device Groups.

Click **Add** and Type **ALL Switches** as the Name. Select **All Device Types** in the **Parent Group** field. Click **Save**.

-itel: Identity Services Engine Home Context Visibility Operations	Policy Administration Work Centers	License Warning 🔺 🔍 🐵 🔿 🌣
System Identity Management Vetwork Resources Device Portal Management	pxGrid Service Feed Service Threat Centric NAC	
Network Devices Network Device Groups Network Device Profiles External RADIUS S	Servers RADIUS Server Sequences NAC Managers External MDM + Location Se	vices
Network Device Groups		
All Groups Choose group -		
C Refresh 🕈 Add Duplicate 🖸 Edit 🗎 Trash 👁 Show group members	s 😩 Import 🔮 Export 👻 🗮 Flat Table 🦨 Expand All 💉 Collapse All	0-
□ Name	Description	No. of Network Devices
All Device Types	All Device Types	-
All Locations	All Locations	**
Is IPSEC Device	Is this a RADIUS over IPSEC Device	**

Add Group				×	
Name *	ALL Switches				
Description					
Parent Group *	All Device Types			× •	
			Cancel	Save	
Home Home	Context Visibility Operations	Policy Administration Work Centers		License Warning 🔺 🤇	2.00¢
System Identity Management Network R Network Devices Network Device Groups Network	etwork Device Profiles External RADIUS Se	pxGrid Services + Feed Service + Threat Ce rvers RADIUS Server Sequences NAC Manaj	ntric NAC		
Network Device Groups					
All Groups Choose group -					
C Refresh + Add Duplicate C Edit	Trash T	🛎 Import 🛛 💆 Export 👻 🔳 Flat Table	Expand All Collapse All		0-
□ Name		Description	No. of Ne	twork Devices	
All Device Types		All Device Types	-		
ALL Switches			0		
All Locations		All Locations	-		
Is IPSEC Device		Is this a RADIUS over IPSEC Device	-		

Add the Switch as AAA Client in the Cisco ISE

Navigate to Administration > Network Resources > Network Devices. The Network Devices window will open.

In the right section window, click Add. The AAA Client window opens. In the Name field, type SW-1 as the name of your switch. In the IP Address field, enter 192.168.1.1/32. this the IP address of the switch interface that will forward RADIUS packets to Cisco ISE.

From the **Device Type** drop-down menu, select **All Switches**.

To activate Radius Authentication Settings, click the check box. In the Shared Secret field, enter a shared secret of cisco. Click the Submit button.
dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍	0 0 ¢
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC		
Network Devices Network Device Gr	Toups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services		
G	Network Devices List > SW-1		
Network Devices	Network Devices		
Default Device	* Name SW-1		
Device Security Settings	Description		
	IP Address * * IP: 192.168.1.1 / 32	<u>@</u> +	
	* Device Profile 📸 Cisco 💌 🕀		
	Model Name		
	Software Version		
	* Network Device Group		
	Location All Locations 📀 Set To Default		
	IPSEC No 📀 Set To Default		
	Device Type ALL Switches O		
	RADIUS Authentication Settings		
	RADIUS UDP Settings		
	Protocol RADIUS		
	* Shared Secret Show		

Navigate to **Policy > Policy Sets**.

Click the plus icon (+) to create a new Policy Set.

dent	ity Serv	ices Engine	Home	Context Visibility	 Operations 	▼ Policy	Administration	Work Centers	License War	ing 🔺	९ 😡	• •
Policy Sets	Profili	ng Posture	Client Provisioni	ng Policy Element	ents							
Policy Se	ts								ResetAll Hit	ounts	Reset	Save
+ st	atus F	Policy Set Nan	ne	Description		Condition	s		Allowed Protocols / Server Seque	nce Hi	ts Actions	s View
Coarch				2000.0								
Search								-				
								+				
	0	Default		Default policy se	t				Default Network Access × *	+ 1	4 🗘	>
										_		

Enter Wired as the policy set Name.

altalta cisco	Identity	Services Engine	Home	Context Visibility	 Operations 	▼Policy	Administration	 Work Centers 			License W	/arning 🔺	Q	0	o o
Policy	Sets	Profiling Posture	Client Provisio	oning Policy Eleme	ents										
Policy	/ Sets										ResetAll H	litcounts		Reset	Save
+	Statu	us Policy Set Nar	ne	Description		Condition	S			Allowed Protocols	/ Server Seq	uence	Hits	Actions	View
Searc	h														
1	Ø	Wired						+		Select from list		+		٥	>
	Ø	Default		Default policy se	t					Default Network Ac	cess ×	+	14	٥	>
														Reset	Save

Click in the **Conditions field** to create a new condition and treat the following condition:

Click the words **Click to add an attribute** to select an attribute for the new condition.

Click the Symbol **Network device** and select the following condition **DEVICE:Device Type EQUALS All Device Types#All Switches**.

Assign the Allowed Protocols/Server Sequence named Default Network Access.

Click Save.

dentity Se	rvices Engine Home	Context Visibility		License Warning 🔺	٩	0	0
Policy Sets Pro	filing Posture Client Provisioning	Policy Elements					
Policy Sets				ResetAll Hitcounts	Re	set	Save
+ Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search							
/ 0	Wired		DEVICE: Device Type EQUALS All Device Types#ALL Switches	Default Network Access × * +		٥	>
Ø	Default	Default policy set		Default Network Access x * +	14	¢	>
					Pa	toot	Savo
					Ne	set	Jave
dentity Se	rvices Engine Home	Context Visibility	Policy Administration Work Centers	License Warning 🔺	Q	0 C	•
Policy Sets Pro	filing Posture Client Provisioning	g Policy Elements					
Policy Sets				PerstAll Hitsourt	Da		Sauo
				Reserver Hitcourts	Re		
+ Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search							
0	Wired		DEVICE-Device Type EQUALS All Device Types#ALL Switches	Default Network Access × • +	0	٥	>
0	Default	Default policy set		Default Network Access × * +	14	٥	>
					R		



Lab 4: Guest Access With Self-Registered Portal

Configure Authentication, Authorization and Accounting for DOT1X.

```
SW-1(config)#aaa new-model
SW-1(config)#aaa authentication dot1x default group radius
SW-1(config)#aaa authorization network default group radius
SW-1(config)#aaa accounting dot1x default start-stop group radius
SW-1(config)#aaa accounting network default start-stop group radius
```

Enable DOT1X globally.

```
SW-1(config)#dot1x system-auth-control
```

Configure an ACL that will be used to classify the traffic that will be redirected to WebAuth. This ACL should permit all HTTP (TCP/80) and HTTPS traffic (TCP/443). All web traffic should be redirected to the Web Authentication portal. The ACL will be forwarded by an authorization profile configured later on the ISE.

```
SW-1(config)#ip access-list extended ACL-WEB-REDIRECT
SW-1(config-ext-nacl)# permit tcp any any eq www
SW-1(config-ext-nacl)# permit tcp any any eq 443
SW-1(config-ext-nacl)# deny ip any any
```

configure radius service.

SW-1(config)#radius server ISE-RAD
SW-1(config-radius-server)#address ipv4 192.168.1.254
SW-1(config-radius-server)#key cisco

Configure the Switch to accept the Downloadable ACL sent by ISE.

SW-1(config)#radius-server vsa send authentication

The Guest PC is connected to interface fa0/3 on SW-1. Configure the following commands on fa0/3 interface.

SW-1(config)#interface FastEthernet0/3
SW-1(config-if)# switchport mode access
SW-1(config-if)# authentication order mab dot1x
SW-1(config-if)# authentication port-control auto
SW-1(config-if)# mab
SW-1(config-if)# dot1x pae authenticator
SW-1(config-if)# dot1x timeout tx-period 10
SW-1(config-if)# spanning-tree portfast

Generate an RSA key pair with modulus 1024, and enable HTTP and HTTPS services. The RSA key pair is needed to support HTTPS connections. The switch must run the HTTP and HTTPS services to be able to redirect users to Central WebAuth running on the Cisco ISE.

SW-1(config)#crypto key generate rsa SW-1(config)#ip http server SW-1(config)#ip http secure-server

Access the ISE GUI using the url HTTPS://192.168.1.254 .

Create Network Device Group

Navigate to Administration > Network Resources > Network Device Groups.

Click Add and Type ALL Switches as the Name. Select All Device Types in the Parent Group field. Click Save.

esco Home Context Visibility Operations	Policy Administration Work Centers	License Warning 🔺 🔍 🎯 🔿 🌣
System Identity Management Vetwork Resources Device Portal Management	pxGrid Services	
Network Devices Network Device Groups Network Device Profiles External RADIUS S	Cervers RADIUS Server Sequences NAC Managers External MDM Location Se	vices
Network Device Groups		
All Groups Choose group -		
C Refresh	: 🔰 Import 🔮 Export 🕶 🚍 Flat Table 🖌 Expand All 🖌 Collapse All	0-
□ Name	Description	No. of Network Devices
All Device Types	All Device Types	-
All Locations	All Locations	-
□ → Is IPSEC Device	Is this a RADIUS over IPSEC Device	

Add Group				×
Name *	ALL Switches			
Description				
Parent Groun *			× •	
, aren oroup	Air Device Types		~ *	
		(Cancel Save	
dentity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers		License Warning 🔺 🔍 💿 🌣
System → Identity Management ▼Network R	Resources Device Portal Management	pxGrid Service + Feed Service + Threat Centric NAC		
Network Devices Network Device Groups N Network Device Groups	etwork Device Profiles External RADIUS Se	rvers RADIUS Server Sequences NAC Managers External MDI	 Location Services 	
All Groups Choose group -				
C Refresh + Add Duplicate C Edit	Trash Trash Show group members	🛎 Import 🔮 Export 👻 📑 Flat Table 🦨 Expand All	✓ Collapse All	0-
□ Name		Description	No. of Network Devices	
All Device Types		All Device Types	-	
ALL Switches			0	
All Locations		All Locations	-	
 Is IPSEC Device 		Is this a RADIUS over IPSEC Device		

Add the Switch as AAA Client in the Cisco ISE

••

Navigate to **Administration > Network Resources > Network Devices**. The **Network Devices** window will open.

In the right section window, click **Add**. The AAA Client window opens. In the **Name** field, type **SW-1** as the name of your switch. In the **IP Address field**, enter **192.168.1.1/32**. this the IP address of the switch interface that will forward RADIUS packets to Cisco ISE. From the **Device Type** drop-down menu, select **All Switches**.

To activate Radius Authentication Settings, click the check box. In the **Shared Secret** field, enter a shared secret of **cisco**. Click the **Submit** button.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍	0 0 ¢
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC		
Network Devices Network Device Gr	Toups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services		
G	Network Devices List > SW-1		
Network Devices	Network Devices		
Default Device	* Name SW-1		
Device Security Settings	Description		
	IP Address * * IP: 192.168.1.1 / 32	<u>@</u> +	
	* Device Profile 📸 Cisco 💌 🕀		
	Model Name		
	Software Version		
	* Network Device Group		
	Location All Locations 📀 Set To Default		
	IPSEC No 📀 Set To Default		
	Device Type ALL Switches O		
	RADIUS Authentication Settings		
	RADIUS UDP Settings		
	Protocol RADIUS		
	* Shared Secret Show		

Navigate to **Policy > Policy Sets**.

Click the plus icon (+) to create a new Policy Set.

dent	ity Serv	ices Engine	Home	Context Visibility	 Operations 	▼ Policy	Administration	Work Centers	License War	ing 🔺	९ 😡	• •
Policy Sets	Profili	ng Posture	Client Provisioni	ng Policy Element	ents							
Policy Se	ts								ResetAll Hit	ounts	Reset	Save
+ st	atus F	Policy Set Nan	ne	Description		Condition	s		Allowed Protocols / Server Seque	nce Hi	ts Actions	s View
Coarch				2000.0								
Search								-				
								+				
	0	Default		Default policy se	t				Default Network Access × *	+ 1	4 🗘	>
										_		

Enter Wired as the policy set Name.

altalta cisco	Identity	Services Engine	Home	Context Visibility	 Operations 	▼Policy	Administration	 Work Centers 			License W	/arning 🔺	Q	0	o o
Policy	Sets	Profiling Posture	Client Provisio	oning Policy Eleme	ents										
Policy	/ Sets										ResetAll H	litcounts		Reset	Save
+	Statu	us Policy Set Nar	ne	Description		Condition	S			Allowed Protocols	/ Server Seq	uence	Hits	Actions	View
Searc	h														
1	Ø	Wired						+		Select from list		+		٥	>
	Ø	Default		Default policy se	t					Default Network Ac	cess ×	+	14	٥	>
														Reset	Save

Click in the **Conditions field** to create a new condition and treat the following condition:

Click the words **Click to add an attribute** to select an attribute for the new condition.

Click the Symbol **Network device** and select the following condition **DEVICE:Device Type EQUALS All Device Types#All Switches**.

Assign the Allowed Protocols/Server Sequence named Default Network Access.

Clic	k Sa	ive.					
Policy	Sets Pro	rvices Engine Home	Context Visibility	Policy Administration Work Centers	License Warning 🔺	९ 🔮	0 ¢
Policy	Sets				ResetAll Hitcounts	Reset	Save
+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence H	its Actions	View
Search	h						
1	Ø	Wired		DEVICE: Device Type EQUALS All Device Types#ALL Switches	Default Network Access × * +	٥	>
	0	Default	Default policy set		Default Network Access × * +	14 Q	>
						Reset	Save
ahaha cisco	Identity Se	ervices Engine Home	Context Visibility		License Warning 🔺	୍ 👔	o o
Policy	Sets Pro	filing Posture Client Provisionin	g Policy Elements				
Policy	/ Sets				ResetAll Hitcounts	Reset	Save
+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence H	its Actions	View
Searc	h						
	Ø	Wired		DEVICE: Device Type EQUALS All Device Types#ALL Switches	Default Network Access × * +	0 ¢	>
	Ø	Default	Default policy set		Default Network Access × • +	14 🗘	>

Reset Save

Create Authentication Policy for the Wired connection.

Navigate to **Policy > Policy Set > Wired** Edit the **Policy Set**.

Click the (+) symbol to create a new authentication policy.

dentity Service	es Engine _{Home}	Context Visibility Operations	✓ Policy Administration	Work Centers	License Warning 🔺	् 🛞	• •
Policy Sets Profiling	Posture Client Provisioni	ing					
Policy Sets → Wi	ired				ResetAll Hitcounts	Reset	Save
Status Pol	licy Set Name	Description	Conditions		Allowed Protocols / Ser	ver Sequenc	e Hits
Search							
Ø Wi	ired		DEVICE Device Type E	QUALS All Device Types#ALL Switches	Default Network Access	× - 4	• •
★ Authentication Po	plicy (1)						
+ Status R	Rule Name	Conditions			Use	Hits	Actions
Search							
				+			
0					All_User_ID_Stores ×	*	~
O	Jefault				> Options	0	Ŷ
> Authorization Poli	icy - Local Exceptions						
> Authorization Poli	icy - Global Exceptions						
> Authorization Poli	icy (1)						

Enter the name Dot1X for Wired. Click the (+) symbol to assign a condition to the rule. Assign the condition Wired_802.1X. Use the Identity Source Internal Users.

Policy Se	entity Ser	vices Engine _{Home} ling Posture Client Provision	Context Visibility Operations	Policy Administration Work Centers	License Warning 🔺 🔍	0	• •
		14 <i>5</i> -1	· · · · · · · · · · · · · · · · · · ·				
Policy	Sets →	vvired			ResetAll Hitcounts	Reset	Save
	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server	Sequence	Hits
Search						_	
	Ø	Wired		DEVICE Device Type EQUALS All Device Types#ALL Switches	Default Network Access	× • +	0
❤ Auth	entication	n Policy (2)					
+	Status	Rule Name	Conditions		Use	Hits	Actions
Searc	h						
	0				Internal Users × v		*
	0	Dot1X for Wired		+	> Options		Ŷ
					All_User_ID_Stores * *		
	\odot	Default			> Options	0	¢
Policy Se	entity Oct ets Profil	ling Posture Client Provision	Context Visibility Operations	Yorky Fadministration F Work Centers			0 0
Folicy		Wild			ResetAll Hitcounts	Reset	Save
Quest	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server	Sequence	; Hits
Search	0	Wired		DEVICE Device Type EQUALS All Device Types#ALL Switches	Default Network Access	× - +	0
✓ Auth	entication	Policy (2)					
+	Status	Rule Name	Conditions		Use	Hits	Actions
Search	h						
	0	Desta V for 195 of			Internal Users × v		~
	0	Dot1X for Wired	Wired_802.1X		> Options		Ŷ
					DenyAccess × 🔻		
-	0	Default			> Options	0	¢
> Auth	orization F	Policy - Local Exceptions					
> Auth	orization F	Policy - Global Exceptions					
> Auth	orization F	Policy (1)					

Reset Save

Create a **DACL** which will control access prior to web authentication.

In ISE, navigate to **Policy >Policy Elements-Results, Authorization >Downloadable ACLs**. Click **Add**.

Enter Web-Auth-ACL in the Name field.

Define the ACL entries as follow, make sure the connectivity toward ISE **192.168.1.254** is allowed, also allow DHCP so that the PC can get an IP address. Optionally you can permit ICMP for troubleshooting purposes.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	୍ ଡ	•	ø
Policy Sets Profiling Posture Clie	ent Provisioning Policy Elements				
Dictionaries + Conditions - Results					
Authentication	Downloadable ACL List > New Downloadable ACL Downloadable ACL				
✓ Authorization	* Name Web-Auth-ACL				
Authorization Profiles	Description				
Downloadable ACLs					
▶ Profiling	IP version				
► Posture	* DACL Content 1234567 permit ip any bost 192 168 1 254 6910112 permit toda any any bost any can bootops 13341511 cermit uda any any bootops any any bost any				
Client Provisioning	6171818 permit (cmp any any 2022222 3242620				
	2/22230 0313233 3430363 73303440				
	Check DACL Syntax				
	Submit Cancel				

Create another **DACL** which will allow access to network after web authentication. Click Add.

Enter **Guest-ACL** in the **Name** field, allow all traffic.

dentity Services Engine	Home Context Visibility Operations	✓ Policy Administration	Work Centers		License Warning 🔺	୍ 🕜	•
Policy Sets Profiling Posture C	Client Provisioning Policy Elements						
Dictionaries Conditions Result	lts						
► Authentication	Downloadable ACL List > New Downloadable A	ACL					
	Downloadable ACL						
✓ Authorization	* Name Guest-ACL						
Authorization Profiles	Description						
Downloadable ACLs							
▶ Profiling	IP version IP v4 O IPv6 O Agnosti	c 🕡					
▶ Posture	* DACL Content 1234567 permit ip any any 89101112						
	1314151 6171819						
Client Provisioning	2021222						
	2728293						
	3435363						
	7383940						
	Check DACL Syntax			(i)			
	Submit Cancel						
dentity Services Engine	Home		Work Centers		License Warning 🔺	୍ 📀	0 0
Policy Sets Profiling Posture C	Client Provisioning Policy Elements						
Dictionaries Conditions Resul	ts						
. Automatication	Downloadable ACLs						
Authentication						Selected 0 Total	8 😵 🎡 🖕
▼ Authorization	/ Edit 🕂 Add 🖺 Duplicate 🗙 Delete				Show All		- 8
Authorization Profiles	Name	Description					
Autorization Frontes	ACL-Admin						
Downloadable ACLs	ACL-Employee	Dama al laud traffic					
▶ Profiling		Deny al ipv4 traffic					
1 Destaur	Guest-ACL	bony ar pro danc					
Postuře	PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic					
Client Provisioning	PERMIT_ALL_IPV6_TRAFFIC	Alow all ipv6 Traffic					
-	Web-Auth-ACL						

Create an authorization profile for web authentication. Navigate to Policy > Policy Elements > Results, Authorization > Authorization Profiles. Click Add.

Configure these attributes: Name: Web portal profile Access Type: ACCESS_ACCEPT DACL: Web-Auth-ACL

Note: This ACL controls traffic allowed prior to successful authentication of the user by Web Auth.

Web Redirection: Centralized Web Authentication, **ACL:** ACL-WEB-REDIRECT, **Value:** Self-Registered Guest Portal (Default)

Note: This ACL does not block traffic. It specifies which of the allowed traffic is redirected to the web authentication portal.

Identity Services Engine ns ▼Policy → Ad ng 🔺 Policy Sets Profiling Posture Client Provisioning

Policy Elements Conditions
 Results Dictionaries Authorization Profiles > New Authorization Profile Authentication Authentication
 Authorization Authorization Profile * Name web portal profile Description Authorization Profiles Downloadable ACLs * Access Type ACCESS_ACCEPT * Profiling Network Device Profile 🛛 🗰 Cisco 💌 🕀 ▶ Posture Service Template Client Provisioning Track Movement Passive Identity Tracking Common Tasks î Web-Auth-ACL 0 DACL Name IPv6 DACL Name cisco Context Visibility Operations
 Policy
 Administration Policy Sets Profiling Posture Client Provisioning ▼ Policy Element Dictionaries + Conditions - Results Authorization Profiles > New Authorization Profile Authentication Authorization Profile ✓ Authorization * Name web portal profile Description Authorization Profiles * Access Type ACCESS_ACCEPT Ŧ Downloadable ACLs ▶ Profiling Network Device Profile 🛛 🖶 Cisco 👻 🕀 Posture Service Template Track Movement Client Provisioning Passive Identity Tracking Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) (j) ACL ACL-WEB-REDIRECT Value gistered Guest Portal (default) + Centralized Web Auth Display Certificates Renewal Message

Make sure the redirect **ACL** name matches exactly the **ACL** configured on the switch. Click **Submit**.

Create an authorization profile for guest access after web authentication.

Navigate to **Policy > Policy Elements > Results, Authorization > Authorization Profiles**. Click **Add**.

Configure these attributes: Name: **Guest profile** Access Type: **ACCESS_ACCEPT** DACL: **Guest-ACL**. Click **Submit**.

dentity Services Engine	Home Context Visibility Operations		rs 🛛 License Warning 🔺 ৭ 🚳	
Policy Sets Profiling Posture Cl	ient Provisioning Policy Elements			
Dictionaries Conditions Result	5			
0				
Authentication	Authorization Profiles > New Authorization Pr	ofile		
	Authorization Profile			
- Authorization	* Name Guest Profile			
Authorization Profiles	Description		it.	
Downloadable ACLs	* Access Type ACCESS_ACCEPT	Ŧ		
▶ Profiling	Network Device Profile 🗰 Cisco 💌 🕀			
+ Posture	Service Template			
. Oliver Brendelseder	Track Movement			
Client Provisioning				
	Massive Identity Tracking			
	▼ Common Tasks			
				^
	E DACL Name	Guest-ACL		
	IPv6 DáCL Name			
Openation Identity Services Engine Policy Sets Profiling Posture C Dictionaries Conditions • Result	Home Context Visibility Operation Client Provisioning Policy Elements Its	s ▼Policy → Administration → Work Cen	License Warning 👗 🔍 🧃	000
Authentication	Standard Authorization Profiles			
- Authorization	For Policy Export go to Administration > Sy	stem > Backup & Restore > Policy Export Page	Selected 0 Total	12 🦓 🖄
Autorization	/ Edit 📥 Add 🕞 Duplicate 💥 Delet	e	Show A	- W W V
Authorization Profiles	Name	Profile	Description	
Downloadable ACLs	Admin-profile	🚓 Cisco 🕀		
▶ Profiling	Blackhole_Wireless_Access	🚓 Cisco 🕀	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE AC	CL on the Wirele
) Posture	Cisco_IP_Phones	👬 Cisco 🕀	Default profile used for Cisco Phones.	
	Cisco_Temporal_Onboard	🝰 Cisco 🕀	Onboard the device with Cisco temporal agent	
Client Provisioning	Cisco_WebAuth	🝰 Cisco 🕀	Default Profile used to redirect users to the CWA portal.	
	Employee-profile	🚓 Cisco 🕀		
	Guest Profile	🟥 Cisco 🕀		
	NSP_Onboard	🚢 Cisco 🕀	Onboard the device with Native Supplicant Provisioning	
	Non_Cisco_IP_Phones	🚓 Cisco 🕀	Default Profile used for Non Cisco Phones.	
	web portal profile	🚓 Cisco 🕀		
	DenyAccess		Default Profile with access type as Access-Reject	
	PermitAccess		Default Profile with access type as Access-Accept	

Navigate to Policy > Policy Sets. Edit the Policy Set named Wired.

dentity Se	ervices Engine Home	Context Visibility		License Warning 🔺	, Q	0	o o
Policy Sets Pro	ofiling Posture Client Provisioning	Policy Elements					
Policy Sets				ResetAll Hitcount	s R	leset	Save
+ Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search							
Ø	Wired		DEVICE-Device Type EQUALS All Device Types#ALL Switches	Default Network Access × * +	61	٥	>
Ø	Default	Default policy set		Default Network Access × • +	15	٥	>

Expand the **Authorization Policy**. Scroll down until you see the Default Authorization Policy. In the **Results (Profiles)**, select the Authorization Profile Web portal profile.

Sets Prof	ing rostore onerkirton.								
Ø	Wired			JALS All Device Types#ALL Switches		Default Ne	etwork Access	× • •	•
uthentication	n Policy (2)								
uthorization	Policy - Local Exceptions								
uthorization	Policy - Global Exceptions	S							
uthorization	Policy (5)								
				Results					
Status	Rule Name	Condi	tions	Profiles	ş	Security Groups		Hits	A
arch									
Ø	Employee AuthoZ	484	IdentityGroup-Name EQUALS User Identity Groups:Emp-Group	×Employee-profile	+	Select from list	- +	1	
ø	Admin AuthoZ	123.	IdentityGroup Name EQUALS User Identity Groups:Admin-Grou	up ×Admin-profile	+	Select from list	- +	11	
0			Radius-User-Name EQUALS jdoe			Output from East			
0	Jdoe AuthoZ	AND	Radius-NAS-Port-Id EQUALS FastEthernet0/1	× PermitAccess	+	Select from list	* +	1	
0			Radius-User-Name EQUALS jwhite						
0	Jwhite AuthoZ	AND		× PermitAccess	-	Select from list	· •	1	
			Radius-NAS-Port-Id EQUALS FastEthemetu/2						
Identity Se	Default rivices Engine Home filing Posture Client Provis	F Context Visioning F Polic	Kaalus HAS-Part-d EQUAL's FastEltremetu2	* DenyAccess	٠	Select from list	۲ 🕇	4	C
Identity Se Sets Prot	Default rvices Englne Home filing Posture Client Provi: Wired	Context Visioning Police		Work Centers	٠	Select from list	Warning 🔺 🔍	4 0 × • +	0
Identity Se Sets Prot	Default rvices Engine Home filing Posture Client Provis Wired	Context Vis isioning Polic		Work Centers ALS All Device Types#ALL Switches	*	Select from list License Default Ne	Warning 🛕 🔍	4 • * * +	G
Contraction of the second seco	Default rvices Engine Home filing Posture Client Provit Wired n Policy (2)	Context Visioning Police		Work Centers ALS All Device TypestALL Switches	*	Select from list License Default Ne	Warning A C	4 • * * +	0
Identity Sets Prof	Default Invices Engine Home filing Posture Client Provid Wred In Policy (2) Policy - Local Exceptions	Context Visioning Police	Administration Verrations Verrations Verrations Verrations Verration Device Device Type EQU	Work Centers ALS AI Device Types#ALL Switches	*	Select from list License Default Ne	Warning A Q	4 * * * +	
Identity Se Sets Prot Uthentication Uthorization	Default Invices Engine Home filing Posture Client Provi Wred In Policy (2) Policy - Local Exceptions Policy - Global Exceptions	Context Visioning Police	Kadaus HAS-Part-d EQUAL'S PastElementu2	Work Centers Mult All Device Types#ALL Switches	*	Select from list License Default Ne	Warning A Q	4 • * * *	
Cleantity Se Identity Se Y Sets Prof Cuthentication uthorization uthorization	Default INICES Engline Home filing Posture Client Provid Wired In Policy (2) Policy - Local Exceptions Policy - Global Exceptions Policy (5)	Context Visioning Potic S		Work Centers ALS All Device Types#ALL Switches	*	Select from list License Default Ne	Warning A. Q.	4 * * * +	
Cantily See Sets Prof withentication withorization withorization	Default INICES Engine Home tiling Posture Client Provid Wred Policy (2) Policy - Global Exceptions Policy (5)	Context Visioning Police			۲	Select from list License Default Ne	Warning A Q	4 × • +	
C Identify Se Sets Prot withentication uthorization uthorization uthorization status	Default INICES Engine INICES Engine Vered Inices Engine Vered Inices Engine Inices	Context Vie isioning Polic S Condition	tions		*	Select from list License Default Ne Security Groups	Warning A Q	4 * * • +	
Control Contro	Default INICES Engine Home Ring Posture Client Provie Wred In Policy (2) Policy - Local Exceptions Policy - Global Exceptions Policy (5) Rule Name	Context Vie isioning Polic S Condition	tions		*	Select from list License Default Ne Security Groups	Warning A Q	4 • • • • •	
Control Contro	Default Invices Engine term Invices Engine Clert Provi Wred In Policy (2) Policy - Local Exceptions Policy (5) Rule Name Employee Autho2	Context Visioning Polic S Condition			* \$	Select from list	Warning A C	4 • • • • •	
Identity Se Identity Se Sets Prof withentication withorization withorization withorization status arch	Default Intermediate Invices Engline Jeane Realing Posture Clent Provis Wred Clent Provis In Policy (2) Intermediate Policy - Local Exceptions Policy - Global Exceptions Policy (5) Intermediate Employee Authol Intermediate Admin Authol Intermediate	 Context Visioning Polic S S S S S 			* \$	Select from list License Default Ne Security Groups Select from list Select from list	Warrang A C	4 • • • • •	
Identity Se Sets Prof withentication withorization withorization withorization status arch Status	Default Invices Engine Home filing Posture Clent Provid Wred In Policy (2) Policy - Local Exceptions Policy (5) Policy (5) Engloyee Autho2 Admin Autho2 Policy Clent Provid Policy Autho2 Policy - Policy - Policy Policy Policy - Policy Policy Policy Policy Policy Policy Policy	Context Vice isioning Polic S S Gondi data data data	Image: Second		*	Select from list License Default Ne Select from list Select from list Select from list	Varang A C, Work Access	4 • • • • • • • • • • • • • • • • • • •	
Identity See sets Prof withentication uthorization uthorization withorization arch Status G G G G	Default Invices Engline Viced Clent Provid Wred Clent Provid In Policy (2) Intervention In Policy - Local Exceptions In Policy (5) Exceptions In Policy (5) Exceptions In Policy (6) Exceptions In Policy (7) Ex	Context Visioning Context Visioning Police s Condition s AND			* * * *	Select from list	Warning A C	4 • Hits 1 11	
Identity Se y Sets Prof withentication uthorization uthorization uthorization status arch © 0 0 0 0 0 0 0 0 0 0 0 0 0	Default Internet Internet Client Provid Wred Client Provid Wred Client Provid In Policy (2) Internet In Policy - Local Exceptions Internet In Policy - Global Exceptions Internet	Context Visioning Polic S Condition			* * * *	Select from list License Default Ne Security Groups Select from list Select from list Select from list	Warming A C	4 • • • • • • • • • • • • • • • • • • •	
Identity Se Sets Prof withentication uthorization uthorization arch Status arch	Default INJUGES Engline Reality Object In Policy (2) Policy - Local Exceptions Policy - Solobal Exceptions	Conduct Vice isioning Polic S Condi a			*	Select from list License License License License License License License License License License License License License License License License License License License License Li	Warrang A C	4 Hits 1 1 1 1 1	

Create an Authorization Policy for guest access. Enter the name Guest Access.

Click in the **Conditions field** to create a new condition.

cisco Ide	entity Serv	vices Engine Home	Context V	isibility	Operations	▼Policy	Administration	Work Centers			License W	arning 🔺	۹, (9 (o c
Policy Se	ets Profil	ing Posture Client Provisionin	g 🕨 Pol	icy Elements	s										
	0	Wired				₽ D	EVICE-Device Type E	EQUALS All Device Types#ALL St	witches		Default Netwo	ork Access	× *	+	61
> Auth	entication	Policy (2)													
> Auth	orization F	Policy - Local Exceptions													
> Auth	orization F	Policy - Global Exceptions													
✓ Auth	orization F	Policy (6)													
									Results						
•	Status	Rule Name	Cond	ditions					Profiles		Security Groups		н	its	Actions
Search	h														
1	0	Guest Access					+		Select from list	+	Select from list	× •	F		٥
	Ø	Employee AuthoZ	485	IdentityGr	roup-Name EQU	ALS User Id	lentity Groups:Emp-Gr	roup	× Employee-profile	+	Select from list		F.	1	٥
	Ø	Admin AuthoZ	48-	IdentityGr	roup Name EQU	ALS User Id	lentity Groups:Admin-G	Group	× Admin-profile	+	Select from list		F.	11	٥
	0	.ldoe AuthoZ		1	Radius User-Na	me EQUAL	\$ jdoe		×PermitAccess	+	Select from list		F	1	ø
		2002 00025	AND		Radius NAS-Por	t-ld EQUAL	\$ FastEthernet0/1								Ŧ
	Ø	.lwhite AuthoZ		2	Radius-User-Na	me EQUAL:	S jwhite		* PermitAccess	+	Select from list		F	1	ø
		STITUL FOR ME	AND		Radius NAS-Por	t-ld EQUAL	S FastEthernet0/2							·	-

From the Library Select the Guest_Flow condition and move it to the Editor.

Conditions Studio

Librar	y		Editor					
Sea	rch by Name			Click to add	d an attribute	6		× ^
Q		🔮 ి: 🧟	, ^t	Equals	~	Attribute value		
	BYOD_is_Registered	<i>()</i>						
	Catalyst_Switch_Local_Web_Authenticat ion	<i>i</i>)				+ New AND OR		
	Compliance_Unknown_Devices	()						
	Compliant_Devices	<i>(</i>)						
	EAP-MSCHAPv2							
	EAP-TLS							
	Guest_Flow	<i>(i)</i>						
	MAC_in_SAN							
	Network_Access_Authentication_Passed	<i>(i)</i>						
	Non_Cisco_Profiled_Phones	<i>()</i>						\rightarrow
							Close	Use

ØX

Conditions Studio

Library		Editor					
Search by Name			Guest_Flow				
	C t ?		Set to 'Is not'		()	Duplicate	E
BYOD_is_Registered	<i>(i)</i>						
Catalyst_Switch_Local_Web_Authenticat	t 🥡			+ New AND OR			
Compliance_Unknown_Devices	<i>(i</i>)						
Compliant_Devices	<i>(i)</i>						
EAP-MSCHAPv2	<i>i</i>						
EAP-TLS	<i>i</i>						
Guest_Flow	<i>()</i>						
MAC_in_SAN	<i>(i)</i>						
Network_Access_Authentication_Passed	(i) t						
Non_Cisco_Profiled_Phones	<i>(i)</i>						
						Close	

IF you edit the **Guest_Flow** condition you see the Attribute **Network Access: UseCase Equals Guest Flow**.

What does Guest Flow mean?

Guest-access authorization with ISE happens in two stages. The initial flow is a MAC authentication Bypass (MAB), where ISE authorizes the endpoint for URL redirect to itself. This results in the web traffic from the guest user's device to be redirected to the ISE Guest portal. Note that at this stage, the network device (switch or WLC) and ISE will track the endpoint's network connection with a common session ID. When a guest user logs in with

guest credentials, the guest user ID is merged with the existing MAB session. This part of the process is termed as Guest Flow, where an existing MAB session gets guest user context appended to it.



In the **Results (Profiles)**, select the Authorization Profile **Guest profile**. Click **Save**.

diale Ide	entity Ser	vices Engine Home	 Context V 	isibility • Operation	ns Velicy	y Administration	♦ Work Centers					License Warning 🔺	Q,	0	0	0
Policy Se	ets Profil	ling Posture Client Provisio	oning 🔹 🕨 Pol	licy Elements												
	0	Wired			₽	DEVICE Device Type	EQUALS All Device Type	s#ALL Swite	ches		D	efault Network Acces	5	x • 🕈		61
> Auth	entication	Policy (2)														
> Auth	orization F	Policy - Local Exceptions														
> Auth	orization f	Policy - Global Exceptions														
✓ Authority	orization I	Policy (6)														
								F	Results							
+	Status	Rule Name	Con	ditions				P	Profiles		Security Group	DS		Hits	Actio	ons
Search	h															
1	Ø	Guest Access		Guest_Flow					× Guest Profile	+	Select from list		+		¢	Ł
	Ø	Employee AuthoZ	485	IdentityGroup-Name	EQUALS User	r Identity Groups:Emp-G	iroup		× Employee-profile	+	Select from list	-	+	1	٥	Ł
	Ø	Admin AuthoZ	4 84	IdentityGroup-Name	EQUALS User	r Identity Groups:Admin-	Group		× Admin-profile	+	Select from list	-	+	11	¢	ł
	0	Idea Autho 7	AND	1 Radius-Us	er-Name EQUA	ALS jdoe			Permitessee		Salact from list					×
		Sance Humble	ANL	Radius NA	S-Port-Id EQUA	ALS FastEthernet0/1			- I CHINCALCOS					1	~	
	0	white Autho7		Radius-Us	er-Name EQUA	ALS jwhite			× Permit∆ccess	+	Select from list		+		ð	\$
		Same Counce	ANL	Radius NA	S-Port-Id EQU	ALS FastEthernet0/2									~	

There are two authorization rules for guest access; the **Default** rule redirects unknown endpoints to the Web portal profile for presenting to a Guest portal, and the **Guest Access** rule is used after users enter their credentials (**Guest Flow**). This grants them internet access (**Guest Profile**).

cisco lo	entity Serv	vices Engine Home	Context Vi	isibility	Operations	▼Policy	Administration	n 🔹 Work Cen	ters			Licens	e Warning 🔺 🛛 🔾	. 0	•
Policy S Auth	ets Profili norization F	ing Posture Client Provisioning Policy - Global Exceptions	Poli	icy Elemen	ts										
► Auth	norization F	Policy (6)													
										Results					
+	Status	Rule Name	Cond	litions						Profiles		Security Groups		Hits	Actions
Searc	h														
	0	Guest Access		Guest_F	low					Suest Profile	+	Select from list	- +	0	٥
	0	Employee AuthoZ	趣	Identity	iroup∙Name EQ I	UALS User Id	fentity Groups:Emp-	Group		× Employee-profile	+	Select from list	- +	1	۵
	0	Admin AuthoZ	48.	Identity	Froup Name EQ	UALS User k	lentity Groups:Admir	n-Group		× Admin-profile	+	Select from list	- +	11	٥
	Ø	Jdoe AuthoZ	AND	1	Radius-User-N	ame EQUAL	S jdoe			× PermitAccess	+	Select from list	- +	1	٥
					Radius-NAS-Po	ort-Id EQUAL	S FastEthernet0/1								
	Ø	.lwhite AuthoZ		1	Radius-User-N	ame EQUAL	S jwhite			* PermitAccess	+	Select from list	- +	1	ø
	Ŭ				Radius NAS-Po	ort-ld EQUAL	S FastEthernet0/2								Ť
	0	Default								×web portal profile	+	Select from list	- +	4	٥

Create a MAB Authentication Policy under the Policy Set Wired.

Edit Authentication Policy and create Rule for MAB method, use the predefined condition Wired_MAB, this condition is based on two other conditions, this is what we call Compound Condition, there are two attributes for MAB, the NAS Port Type Equal Ethernet attribute to identify the media used by the endpoint, and Service Type Equal Call Check attribute to identify the authentication method, Call Check means MAB method.

Note: for Dot1X, the Service Type is Framed.

Use the Identity Source Internal Endpoints.

cisco lo	lentity Se	rvices Engine Home	 Context Visibility 	 Operations 	▼ Policy	 Administration 	Work Centers		License Warning 🔺	९ \varTheta	• •
Policy S	ets Prof	filing Posture Client Provi	sioning	nents							
Policy	Sets →	Wired							ResetAll Hitcounts	Reset	Save
	Status	Policy Set Name	Description		Condition	าร			Allowed Protocols / Serve	er Sequenc	e Hits
Search											
	0	Wired			₽ D	EVICE-Device Type E	QUALS All Device Types#ALL Switches		Default Network Access	x = 4	61
♥ Aut	nenticatio	n Policy (3)									
+	Status	Rule Name	Conditions					Use		Hits	Actions
Searc	:h										
	~							Internal U	isers ×	•	~
	0	Dot1X for Wired	U Wire	d_802.1X				> Opti	ons	19	Ŷ
	0	NAD		J MAD				Internal E	indpoints ×	•	~
	U	READ		CO_NAD				> Option	ons		*
	0	Defect						DenyAcc	ess ×	•	~
	ø	Default						> Opti	ons	18	*

In the authentication policy, **MAB** for unknown internal endpoints, select **Continue**, which allows guest endpoints (which are unknown) to continue authentication and be authorized for redirection to the guest portal.

Člick Save.

diado Id	entity Ser	vices Engine Home	Context \	Visibility	▼ Policy	Administration	Þ	Work Centers		License Warning 🔺	Q	0	• •
Policy Se	ets Profil	ing Posture Client Provision	iing 🔹 🕨 Po	blicy Elements									
Policy	Sets 🔶	Wired								ResetAll Hitcounts	R	teset	Save
	Status	Policy Set Name	Descr	ription	Condition	าร				Allowed Protocols / Se	rver Se	equence	Hits
Search													
	0	Wired			₽ De	EVICE-Device Type E	EQUA	ALS All Device Types#ALL Switches		Default Network Access		× • +	61
✓ Auth	entication	Policy (3)											
+	Status	Rule Name	Con	ditions					Use			Hits	Actions
Search	h												
	0	B. 4976-197-1	9						Internal U	Isers	x •		~
	U	Dot1x for Wired		Wired_802.1X					> Optio	ons		19	¥
									Internal E	indpoints	× v		
									♥ Optio	ons			
									If Auth fa	a			
	Ø	MAB	P	Wired MAB					REJEC	× T	*		ø
	Ŭ	00000		Wild_linds					If User n	ot found			*
									CONTI	NUE ×	*		
									# Proces	is fail			
									DROP	×	¥		

diality lo	dentity Ser	vices Engine Home	Context Visibility	Policy Administration Work Centers	License Warning 🔺 🔍	0	• •
Policy S	iets Prof	iling Posture Client Provisioning	Policy Elements				
Policy	Sets +	Wired			ResetAll Hitcounts	Reset	Save
	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server S	Sequence	Hits
Search							
	0	Wired		DEVICE Device Type EQUALS All Device TypestIALL Switches	Default Network Access	x • 🕇	61
★ Aut	hentication	Policy (3)					
+	Status	Rule Name	Conditions		Use	Hits	Actions
Sear	:h						
	Ø	Dot1X for Wired	Wired_802.1X		Internal Users × •	19	٥
					Options		
	Ø	MAB	Wired MAB		Internal Endpoints × *	0	ø
					> Options		
	Ø	Default			DenyAccess × *	18	ø
	Ŭ				> Options		

On the **Guest PC**, disable the 802.1X supplicant, wait few seconds.

Navigate to **Operations > Radius > Live Logs**.

Notice the **Guest PC** with MAC **008c.fa29.b453** is authenticated with MAB and redirected to the web portal, the Authorization Profile **Web portal profile** is applied. Click **Authentication Detail Report**.

dialia Iden	ntity Services Engine	Home Context	t Visibility	▼ Operations	Policy Admini	stration				L	icense Warning 🔺	୍ ଡ	0	0
▼RADIUS	Threat-Centric NAC Live Lo	gs + TACACS +	Troublesho	ot + Adaptive N	letwork Control Reports	5								
Live Logs	Live Sessions													
	Misconfig	jured Supplicants 🛛		Misconfigured Ne	etwork Devices 🕔	RADIUS Drops	с	lient Stopped Res	ponding	Repea	t Counter 🔕			
		0		()	0		4			2			
								Refresh	ver	Show Latest 2	0 records 🗸 🤟 Within	Last 30 r	ninutes	~
C Refresh	Reset Repeat Counts	🚨 Export To 🔻										▼ Fi	lter 🔻	۰.
Time	e	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorizati	IP Address	Netwo	ork Devi	ice
×		~			Identity	Endpoint ID	Endpoint Profil	Authentication	Authorization F	Authorization F	IP Address	Netwo	ork Devic	e
Nov	12, 2019 11:37:12.323 PM	0	0	2	00:8C:FA:29:B4:53	00:8C:FA:29:B4:53	Unknown	Wired >> MAB	Wired >> De	web portal pr	192.168.1.2			
Nov	12, 2019 11:37:11.299 PM		0		#ACSACL#-IP-We							SW-1		
Nov	12, 2019 11:36:17.302 PM		O.		#ACSACL#-IP-We							SW-1		
Nov	12, 2019 11:36:17.279 PM		o		00:8C:FA:29:B4:53	00:8C:FA:29:B4:53	Unknown	Wired >> MAB	Wired >> De	web portal pr		SW-1		
Nov	12, 2019 11:33:41.339 PM	2	0		#ACSACL#-IP-We							SW-1		
Nov	12, 2019 11:33:41.309 PM	2	0		00:8C:FA:29:B4:53	00.8C:FA:29.B4:53	Unknown	Wired >> MAB	Wired >> De	web portal pr		SW-1		
Nov	12, 2019 11:32:10.108 PM	٥	0		INVALID	00:8C:FA:29:B4:53		Wired >> Do	Wired			SW-1		
Nov	12, 2019 11:26:49.310 PM	2	Q		#ACSACL#-IP-AC							SW-1		
Nov	12, 2019 11:26:49.279 PM	2	0		administrator	00:8C:FA:29:B4:53	Unknown	Wired >> Do	Wired >> Ad	Admin-profile		SW-1		

The Authentication Policy MAB and Authorization Profile **Web portal profile** are applied, in the **Results** section the ISE is sending two attributes, an URL Redirection that starts with <u>https://ISE.lab.local/..../cwa</u>, cwa means Centralized Web Authentication, the second attribute is a Dacl called Web-Auth-ACL.

Overview

F (
Event	5200 Authentication succeeded
Username	00:8C:FA:29:B4:53
Endpoint Id	00:8C:FA:29:B4:53 ⊕
Endpoint Profile	Unknown
Authentication Policy	Wired >> MAB
Authorization Policy	Wired >> Default
Authorization Result	web portal profile

Authentication Details

Source Timestamp	2019-11-12 23:36:17.279
Received Timestamp	2019-11-12 23:36:17.279
Policy Server	ISE
Event	5200 Authentication succeeded
Username	00:8C:FA:29:B4:53
User Type	Host
Endpoint Id	00:8C:FA:29:B4:53
Calling Station Id	00-8C-FA-29-B4-53

Result	
UserName	00:8C:FA:29:B4:53
User-Name	00-8C-FA-29-B4-53
Class	CACS:C0A80101000000190095AB64:ISE/362840588/102
cisco-av-pair	url-redirect-acl=ACL-WEB-REDIRECT
cisco-av-pair	url-redirect=https://ISE.lab.local:8443/portal /gateway?sessionId=C0A80101000000190095AB64& portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa& token=bb9b634884edbae6f59f8fd351ca40ed
cisco-av-pair	url-redirect=https://ISE.lab.local:8443/portal /gateway?sessionId=C0A80101000000190095AB64& portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa& token=47bec4a0b56e1f30249822ad82c130c7
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-Web-Auth-ACL-5dcb3583
cisco-av-pair	profile-name=Unknown
LicenseTypes	Base license consumed

On the switch verify that the Dacl Web-Auth-ACL is downloaded.



You can view the details of the authentication on the switch using the **sh authentication session int f0/3** command, notice the **URL Redirect** and the **Dacl Web-Auth-ACL**.



<u>F</u> ichier Editio <u>n</u> <u>A</u>	ffichage <u>H</u> istorique <u>M</u> arque-pages <u>O</u> utils <u>?</u>			-		×
ۏ Nouvel onglet	× +					
← → C ²	ⓐ Q 192.168.1.20 → Q Rechercher		lii\	•	٢	≡
🌣 Most Visited	🖨 Getting Started 🚟 Cisco.com Login Page					
					*	^
	G Rechercher sur le Web	\rightarrow			¥	
	Sites les plus visités 🗸					
	wikipedia reddit @amazon twitter					
	☆ Éléments-clés ∨					
	Commencez à naviguer puis nous afficherons des articles, des vidéos ou d'autres pages que vous avez récemment visités ou ajoutés aux marque-pages.					

From the Guest PC, try to access the web server at http://192.168.1.20.

The Guest PC is redirected to the URL Redirect https://ISE.lab.local/...../cwa, but the PC fails the **DNS** Resolution.



Since we don't have a DNS server to resolve the URL Redirect to the IP address 192.168.1.254 of ISE, we can override this by instructing the ISE to replace the hostname ISE.lab.local by its IP address in the Authorization Profile of Web Redirection, so edit the Authorization Profile Web portal profile.

Go to **Policy > Policy Elements > Results**, expand **Authorization** in the Left Menu. Expand **Authorization Profiles**. Click on the Authorization profile Web portal profile. Scroll to **Web Redirection (CWA, DRW, MDM, NSP, CPP)**.

-thefter Identity Services Engine Hon	ne Context Visibility Operations	licy Administration Work Centers	License Warning 🔺 🔍 🔘 💿	0
Policy Sets Profiling Posture Client P	rovisioning Policy Elements			
Dictionaries + Conditions - Results				
0				
Authentication	Standard Authorization Profiles	In a Destruct Delay Count Date		
- Authorization	For Poicy Export go to Administration > System > bac	kup & Restore > Policy Export Page	Selected 0 Total 12 😵 🐐	ŝ.
Authorization Profiles	/ Edit 🕂 Add 🖳 Dupicate 🗙 Delete		Show AI	8
Autorization Frones	Name	Profile	Description	
Downloadable ACLS	Admin-profile	👬 Cisco 🕀		
▶ Profiling	Blackhole_Wireless_Access	📸 Cisco 🕀	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the	Wirele
Posture	Cisco_IP_Phones	📸 Cisco 🕀	Default profile used for Cisco Phones.	
	Cisco_Temporal_Onboard	ata Cisco ⊕	Onboard the device with Cisco temporal agent	
Client Provisioning	Cisco_WebAuth	🏙 Cisco 🕀	Default Profile used to redirect users to the CWA portal.	
	Employee-profile	🚓 Cisco 🕀		
	Guest Profile	🟥 Cisco 🕀		
	NSP_Onboard	🟥 Cisco 🕀	Onboard the device with Native Supplicant Provisioning	
	Non_Cisco_IP_Phones	🏥 Cisco 🕀	Default Profie used for Non Cisco Phones.	
	web portal profile	🚓 Cisco 🕀		
	DenyAccess		Default Profile with access type as Access-Reject	
	PermitAccess		Default Profile with access type as Access-Accept	

Place a check mark in the **Static IP/Host name FQDN** box. Enter the IP address of the ISE **192.168.1.254**.

Click Save.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	0,	0	0	Ø,
Policy Sets Profiling Posture Cli	ient Provisioning Policy Elements					
Dictionaries + Conditions - Result	S					
0						
Authentication	Authorization Profiles > web portal profile Authorization Profile					
▼ Authorization	* Name web portal profile					
Authorization Profiles	Description					
Downloadable ACLs	* Access Type ACCESS_ACCEPT *					
▶ Profiling	Network Device Profile 🛛 🏦 Cisco 💌 🕀					
▶ Posture	Service Template					
Client Provisioning	Track Movement					
	Passive Identity Tracking					
	Common Tasks					
	Web Redirection (CWA, MDM, NSP, CPP) (j)					^
	Centralized Web Auth * ACL ACL-WEB-REDIRECT Value egistered Guest Portal (default) *					
						н.
	Display Certificates Renewal Message					
	Static IP/Host name/FQDN					
	Suppress Profiler CoA for endpoints in Logical Profile					

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺	Q,	0	•	ø
Policy Sets Profiling Posture Cl	ient Provisioning Policy Elements					
Dictionaries Conditions Result	S					
0	Autominise Durflers - such mental see Be					
Authentication	Authorization Profile					
- Authorization	*Name web portal profile					
Authorization Profiles	Description					
Downloadable ACLs	* Access Type ACCESS_ACCEPT *					
▶ Profiling	Network Device Profile dtt Cisco V					
Posture	Service Template					
Client Provisioning	Track Movement 🔲 👔					
	Passive Identity Tracking					
	▼ Common Tasks					
	Web Redirection (CWA, MDM, NSP, CPP)					^
	Centralized Web Auth + ACL ACL-WEB-REDIRECT Value egistered Guest Portal (default) +					
						1
	Display Certificates Renewal Message					
	Static IP/Host name/FQDN 192.168.1.254					
	Suppress Profiler CoA for endpoints in Logical Profile					
						~

In the **Attributes Details**, you can verify the **cisco-av-pair**, for URL Redirect, the hostname **ISE.lab.local** is replaced by the IP address **192.168.1.254**.

▼ Advanced Attributes Settin	ngs				
Select an item	O =	⊘ — ∔			
 Attributes Details 					
Access Type = ACCESS_ACCEPT DACL = Web-Auth-ACL cisco-av-pair = url-redirect-acl=ACL cisco-av-pair = url-redirect=https://	-WEB-REDIRECT /192.168.1.254:port/portal/	ateway?sessionId=SessionIdValue&por	tal=27041710-2e58-11e9-98ft	۰-0050568775a3&daysToExpiry=۱	value&action=cwa
Save					

From the **Guest PC**, disable and enable the Network Card. On the Switch a console message is displayed with a successful mab authentication and authorization.

SW-1#		
*Mar	1 02:55:34.791:	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
*Mar	1 02:55:35.797:	%LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
*Mar	1 02:55:38.079:	%AUTHMGR-5-START: Starting 'mab' for client (008c.fa29.b453) on Interface Fa0/3 AuditSessionID C0A801010000001B00A0CA70
*Mar	1 02:55:38.138:	%MAB-5-SUCCESS: Authentication successful for client (008c.fa29.b453) on Interface Fa0/3 AuditSessionID C0A801010000001B00A0CA70
*Mar	1 02:55:38.138:	%AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (008c.fa29.b453) on Interface Fa0/3 AuditSessionID COA801010
00000	1B00A0CA70	
*Mar	1 02:55:39.169:	%AUTHMGR-5-SUCCESS: Authorization succeeded for client (008c.fa29.b453) on Interface Fa0/3 AuditSessionID C0A801010000001B00A0CA70
*Mar	1 02:55:39.589:	%LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar	1 02:55:40.596:	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
SW-1#		

The **show authenti session int f0/3** command shown that the IP address **192.168.1.254** is sent by ISE instead of **ISE.Iab.Iocal**.

o authe sess i	nt f0/3
Interface	: FastEthernet0/3
MAC Address	: 008c.fa29.b453
IP Address	: 192.168.1.2
User-Name	: 00-8C-FA-29-B4-53
Status	: Authz Success
Domair	: DATA
Oper host mode	: single-host
er control dir	: both
Authorized By	: Authentication Server
Vlan Group	: N/A
ACS ACL	: xACSACLx-IP-Web-Auth-ACL-5dcb3583
L Redirect ACL	: ACL-WEB-REDIRECT
URL Redirect	: https://ISE.lab.local:8443/portal/gateway?sessionId=COA801010000001B00A0CA70&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa
a3481c730c6470	cbd00f1cfa4575c5a2
URL Redirect	: https://192.168.1.254:8443/portal/gateway?sessionId=C0A801010000001B00A0CA70&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa
d4511ff560e802	5668365afb2c6a5f01
ession timeout	: N/A
Idle timeout	: N/A
non Session II	: C0A80101000001B00A0CA70
cct Session II	: 0x0000020
Handle	: 0xEB00001C
e methods list	
Method State	
nab Autho	Success
dotly Not r	
doctx Noc I	
	D authe sess i Interface MaC Address IP Address User-Name Status Domain Frontstmade Authorized By Vian Group Vian Group ACS ACL URL Redirect ACL Redirect ACL Redirect ACL Redirect ACL Redirect ACS ACL URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Adslc730c6470 URL Redirect Status Adslc730c6470 URL Redirect Status S

Navigate to **Operations > Radius > Live Logs**. Notice the **Guest PC** with MAC **008c.fa29.b453** is authenticated with MAB and redirected to the web portal, the Authorization Profile **Web portal profile** is applied. Click Authentication Detail Report.

diality Ide	ntity Services Engine	Home Conte	ext Visibility	▼ Operations	Policy Adminis	tration				License W	arning 🔺 👘	R 😐	• •
▼ RADIUS	Threat-Centric NAC Live I	.ogs + TACACS	Troubleshoe	ot + Adaptive N	etwork Control Reports								
Live Logs	Live Sessions												
	Miscon	Misconfigured Supplicants			twork Devices 🛛	RADIUS Drops	Client Stopped Responding 🕕			Repeat Counter			
	0			0		0	4			3 📥			
								Refresh New	ver	Show Latest 20 records	~ Within	Last 30 m	iinutes ~
C Refres	sh 🛛 Reset Repeat Cour	its 🔮 Export To 🕶										y Filt	ier• 🔷•
Tin	ne	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P	Authenticat	Authorizati	Authorization Profiles	IP Address		Network De
×		×	1		Identity	Endpoint ID	Endpoint Profil	Authentication	Authorization F	Authorization Profiles	IP Address	~	Network Dev
Nov	v 12, 2019 11:48:27.349 PM	0	ò	3	00:8C:FA:29:B4:53	00:8C:FA:29:B4:53	Unknown	Wired >> MAB	Wired >> De	web portal profile	192.168.1.2		
Nov	v 12, 2019 11:48:26.333 PM	2	ò		#ACSACL#-IP-We								SW-1
Nov	v 12, 2019 11:37:11.299 PM	M	ò		#ACSACL#-IP-We								SW-1
Nov	v 12, 2019 11:36:17.302 PM	~	à		#ACSACL#-IP-We								SW-1
Nov	v 12, 2019 11:36:17.279 PM	~	ġ.		00:8C:FA:29:B4:53	00:8C:FA:29:B4:53	Unknown	Wired >> MAB	Wired >> De	web portal profile			SW-1
Nov	v 12, 2019 11:33:41.339 PM	~	à		#ACSACL#-IP-We								SW-1
Nov	v 12, 2019 11:33:41.309 PM	~	ò		00:8C:FA:29:B4:53	00:8C:FA:29:B4:53	Unknown	Wired >> MAB	Wired >> De	web portal profile			SW-1
Nov	v 12, 2019 11:32:10.108 PM	0	à		INVALID	00:8C:FA:29:B4:53		Wired >> Do	Wired				SW-1
Nov	v 12, 2019 11:26:49.310 PM	×	ò		#ACSACL#-IP-AC								SW-1
Nov	v 12, 2019 11:26:49.279 PM	_	0		administrator	00:8C:FA:29:B4:53	Unknown	Wired >> Do	Wired >> Ad	Admin-profile			SW-1

From the Guest PC, try to access the web server at http://192.168.1.20.

Network Security All-in-one ASA Firepower WSA VPN ISE Layer 2 Security

Redouane MEDDANE 3xCCNP Collaboration, Security and Enterprise

END

Lulu Press, Inc Morrisville, North Carolin