

Practical Scenarios

Network Security All-in-one

ASA Firepower WSA Umbrella
VPN ISE Layer 2 Security

Redouane MEDDANE



Lulu Press, Inc

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

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

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
Cisco ASA FTD WSA Umbrella VPN ISE Layer 2 Security
All Right Reserved

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: Firewall 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

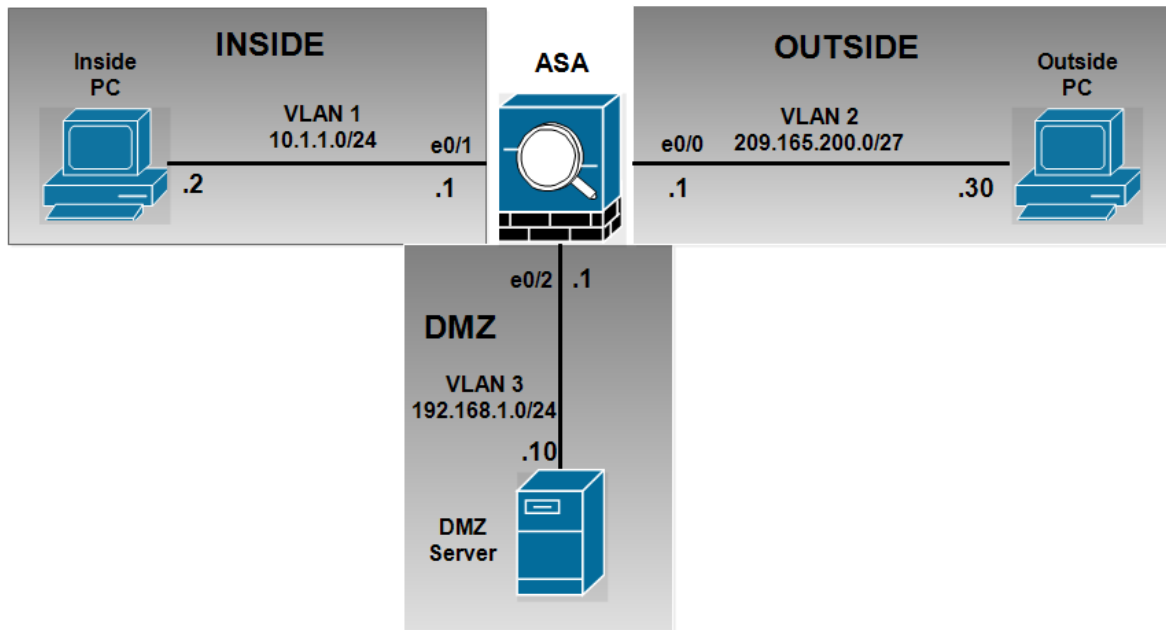
- Lab 1: DHCP Snooping IP source guard and ARP inspection

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
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
ciscoasa#
ciscoasa# show run interface vlan 2
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.1 255.255.255.224
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#
```

```
ciscoasa# show run interface vlan 1
```

```

!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
ciscoasa#
ciscoasa# show run interface vlan 2
!
interface Vlan2
nameif outside
security-level 0
ip address 209.165.200.1 255.255.255.224
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
```

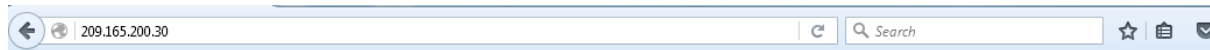
Verify the object network DMZ-SRV:

```
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#

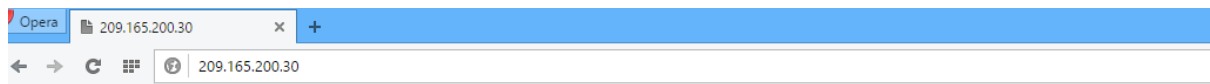
```

```

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-service-object)# service tcp destination eq 8080
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:

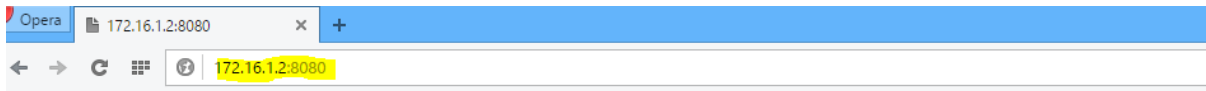
```
ciscoasa# show run object id DMZ_PAT
object network DMZ_PAT
  host 172.16.1.10
ciscoasa#
ciscoasa# show run object id HTTP_80
object service HTTP_80
  service tcp destination eq www
ciscoasa#
ciscoasa# show run object id HTTP_PROXY_PORT
object service HTTP_PROXY_PORT
  service tcp destination eq 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
<http://172.16.1.2:8080>:



DMZ web Server

WELCOME!

Verify 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#
```

```
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

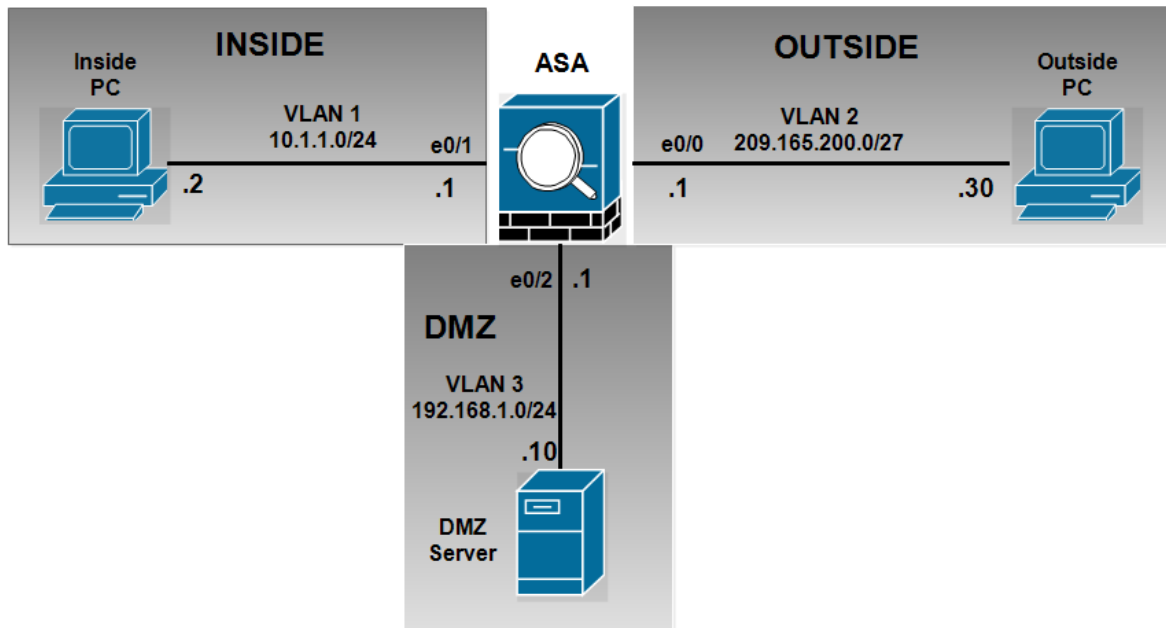
Auto NAT Policies (Section 2)
1 (DMZ) to (outside) source static DMZ-SRV 209.165.200.22
translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic INSIDE-NETWORK 209.165.200.20
translate_hits = 6, untranslate_hits = 0
ciscoasa#
```

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
  flags srIT 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#
```

```
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
ciscoasa(config)#
```

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 tpeq ftp
ciscoasa(config-service-object-group)# service-object tpeq 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-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-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)#  
ciscoasa(config-pmap-c)# policy-map global_policy  
ciscoasa(config-pmap)# 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 rnfrnrnto 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-map inspection_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 rnfrnrnto 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:

```

ciscoasa(config)# test regex redouane.exe "\.exe"
INFO: Regular expression match succeeded.
ciscoasa(config)#

```

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 rnfrnrnto put stou site dele mkdrmd
reset log
match filetype 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 appe cdup help rnfr rnto put stou site dele mkd rmd
        reset log, packet 0
      match filetype regex class DMZ-REGEX
        reset log, packet 0
ciscoasa#

```

```

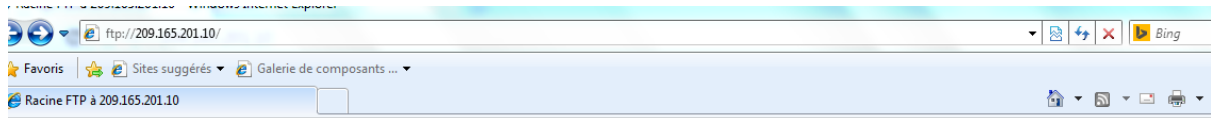
ciscoasa# show service-policy global inspect ftp

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 rnfrnrnto put stou site dele mkdrmd
  reset log, packet 0
  match filetype 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:

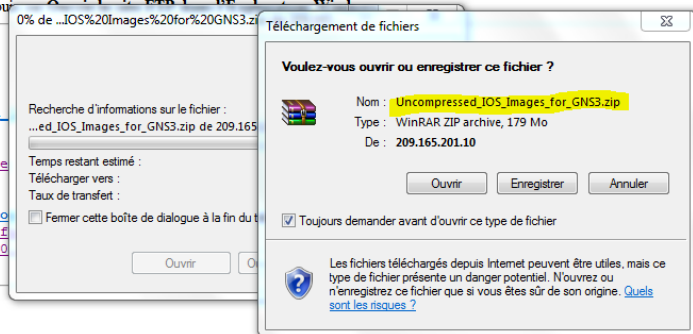


Racine FTP à 209.165.201.10

Pour afficher ce site FTP dans l'Explorateur Windows, cliquez sur Page, puis sur Ouvrir le site

```

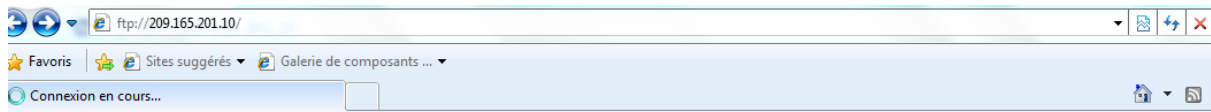
10/08/2015 12:00 Répertoire $RECYCLE.BIN
07/20/2015 12:00 6,565,736 ccsetup507.exe
07/25/2015 12:00 41,128,904 Firefox Setup 39.0.exe
07/20/2015 12:00 53,078,632 FoxitReader708.1216_prom
11/24/2015 03:36 3 ftp_ict.txt
11/24/2015 10:26 0 ftp.txt
07/20/2015 12:00 66,807,049 GNS3-1.3.7-all-in-one.exe
11/24/2015 03:40 Répertoire Logiciels
04/13/2011 12:00 454,656 Putty.exe
08/30/2015 12:00 Répertoire System Volume Information
07/20/2015 12:00 188,689,086 Uncompressed IOS Images for GNS3.zip
07/20/2015 12:00 4,021,144 USB Disk Security 6.5.0.0.exe
  
```



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

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
6	Dec 13 2015	06:26:30	303002	209.165.200.30	49802	192.168.1.10/21	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
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)
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
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:

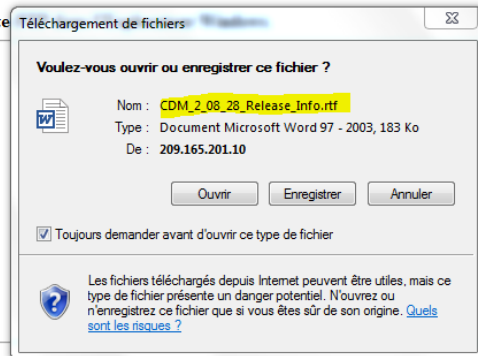


Racine FTP à 209.165.201.10

Pour afficher ce site FTP dans l'Explorateur Windows, cliquez sur Page, puis sur Ouvrir le site

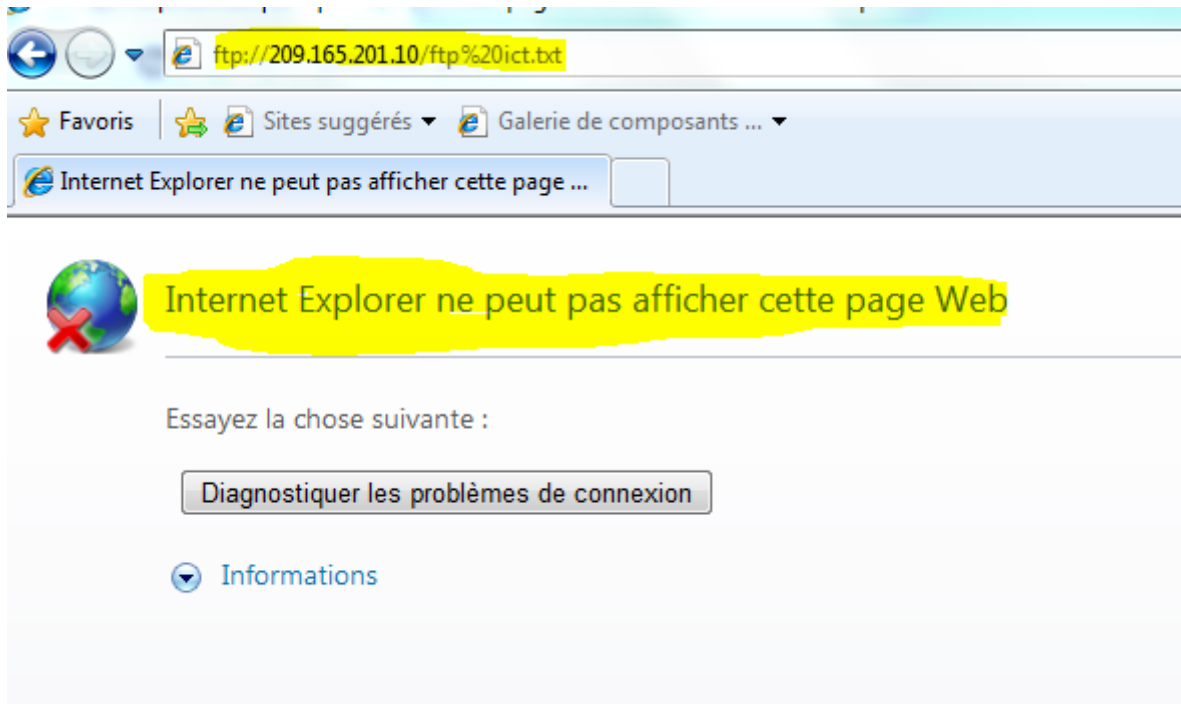
```

10/08/2015 12:00 Répertoire $RECYCLE.BIN
07/20/2015 12:00 6,565,736 ccsetup507.exe
02/13/2013 12:00 187,965 CDM 2 08 28 Release Info.rtf
07/25/2015 12:00 41,128,904 Firefox Setup 39.0.exe
07/20/2015 12:00 53,078,632 FoxitReader708.1216_prom L10N_Setup.exe
11/24/2015 03:36 3 ftp_ict.txt
11/24/2015 10:26 0 ftp.txt
07/20/2015 12:00 66,807,049 GNS3-1.3.7-all-in-one.exe
11/24/2015 03:40 Répertoire Logiciels
04/13/2011 12:00 454,656 Putty.exe
08/30/2015 12:00 Répertoire System Volume Information
07/20/2015 12:00 188,689,086 Uncompressed IOS Images for GNS3.zip
07/20/2015 12:00 4,021,144 USB Disk Security 6.5.0.0.exe
  
```



Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
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
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
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)
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:



The ASA displays a log message of the failure:

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
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)
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 DMZ:192.168.1.10/21 terminated by inspection engine, reason - inspector reset unconditionally.
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:192.168.1.10/21
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:

```
C:\Users\ [redacted] >
C:\Users\ [redacted] >ftp 209.165.201.10
Connecté à 209.165.201.10.
220-FileZilla Server 0.9.53 beta
220-written by Tim Kosse <tim.kosse@filezilla-project.org>
220 *****
Utilisateur (209.165.201.10:(none)) : [redacted]
331 Password required for [redacted]
Mot de passe :
230 Logged on
ftp> delete
Fichier distant Uncompressed IOS Images for GNS3.zip
Connexion fermée par l'hôte distant.
ftp>
ftp>
```

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

```
C:\Users\ [redacted] >ftp 209.165.201.10
Connecté à 209.165.201.10.
220-FileZilla Server 0.9.53 beta
220-written by Tim Kosse <tim.kosse@filezilla-project.org>
220 *****
Utilisateur (209.165.201.10:(none)) : [redacted]
331 Password required for [redacted]
Mot de passe :
230 Logged on
ftp> rename [redacted]
Nom d'origine Putty.exe
Nom de destination console.exe
Connexion fermée par l'hôte distant.
ftp>
```

Access ASA to see the log message displayed:

Latest ASDM Syslog Messages							
Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina Description
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
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.
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 rnrfr mto put stou site dele mkid rmd in policy-map FTP-POLICY, Reset connection from outside:209...
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:

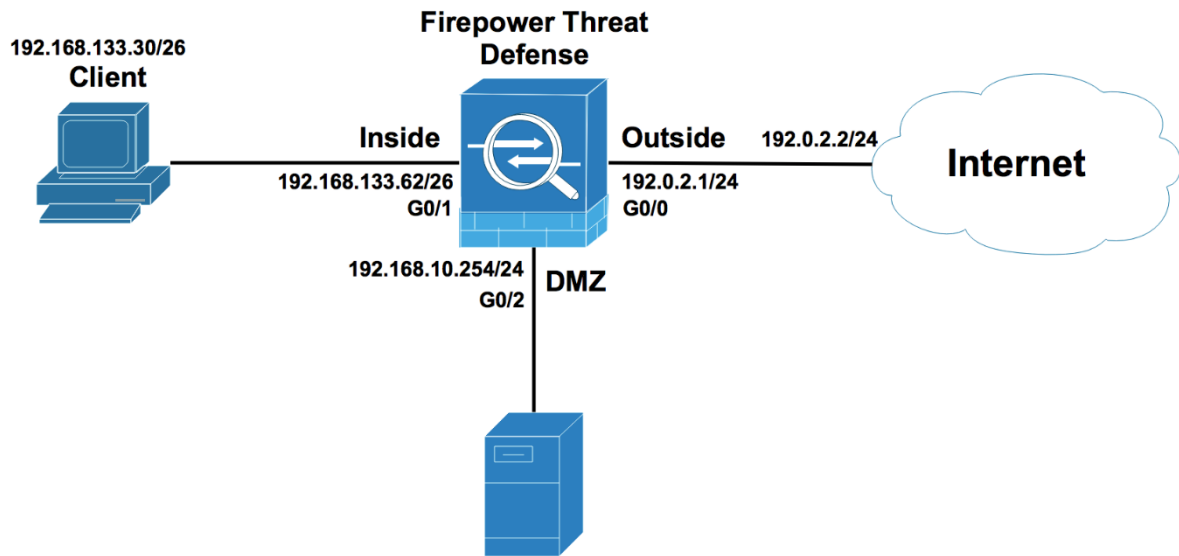
```
ciscoasa(config-pmap-c)# show service-policy

Global policy:
  Service-policy: 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: sqlnet, packet 0, drop 0, reset-drop 0
    Inspect: skinny , packet 0, drop 0, reset-drop 0
      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(config-pmap-c)#
```

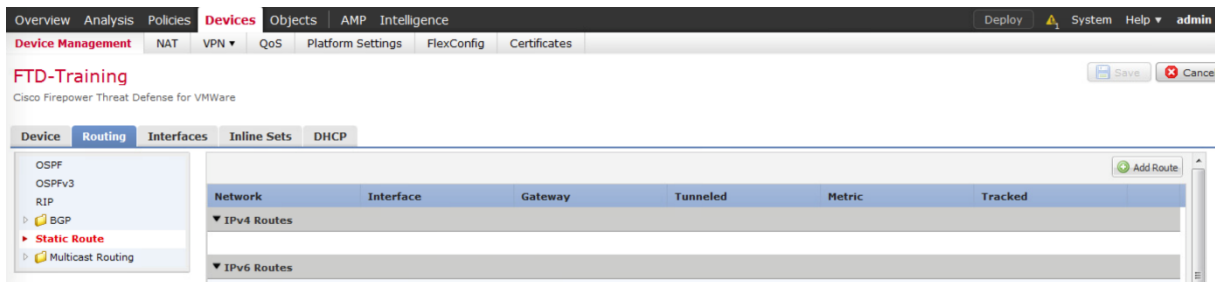
Network Security All-in-one WorkBook

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:



In the interface field, use the logical name outside as the outgoing interface and select any-ipv4, 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: IPv4 IPv6

Interface*:

Available Network

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-1
- IPv4-Private-192.168.0.0-
- IPv4-Private-All-RFC1918
- IPv6-to-IPv4-Relay-Anyca

Selected Network

- any-ipv4

Gateway*: (1 - 254)

Metric: (1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

OK Cancel

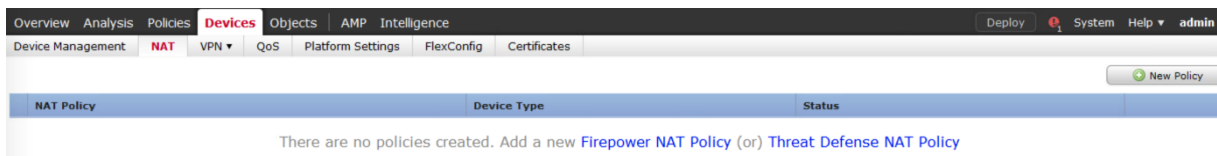
FTD-Training

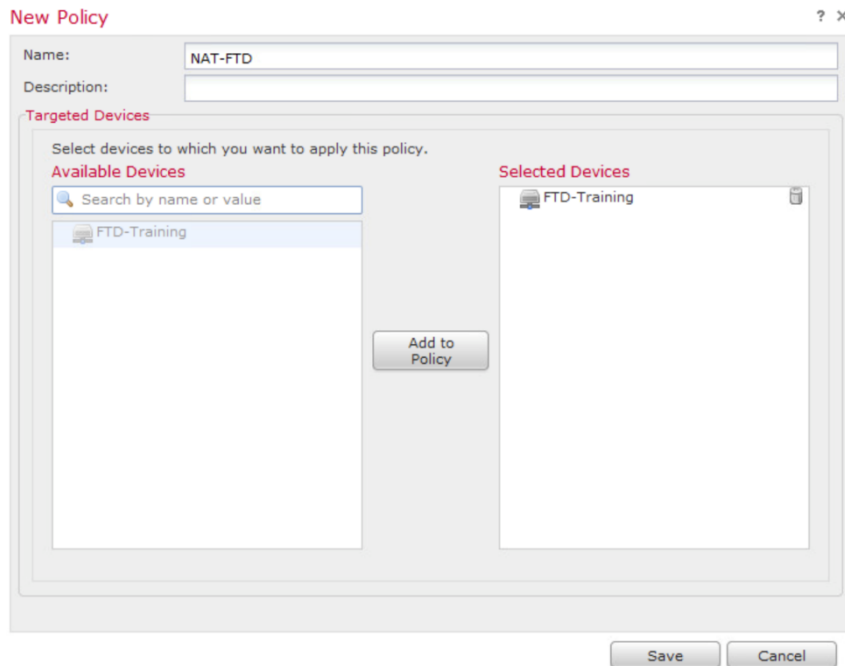
Cisco Firepower Threat Defense for VMWare

Device Routing Interfaces Inline Sets DHCP

Network	Interface	Gateway	Tunneled	Metric	Tracked
IPv4 Routes					
any-ipv4	outside	192.0.2.2	false	1	
IPv6 Routes					

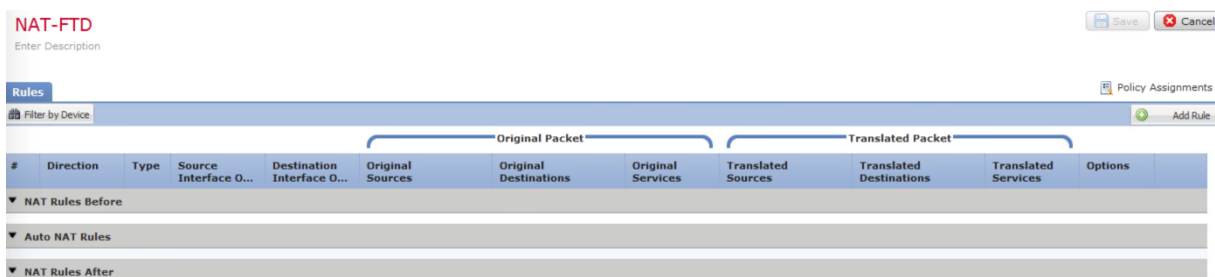
Under devices-NAT, create a new NAT policy named NAT-FTD, select the managed device you want to apply the NAT policy from the Available Devices to Selected Devices:



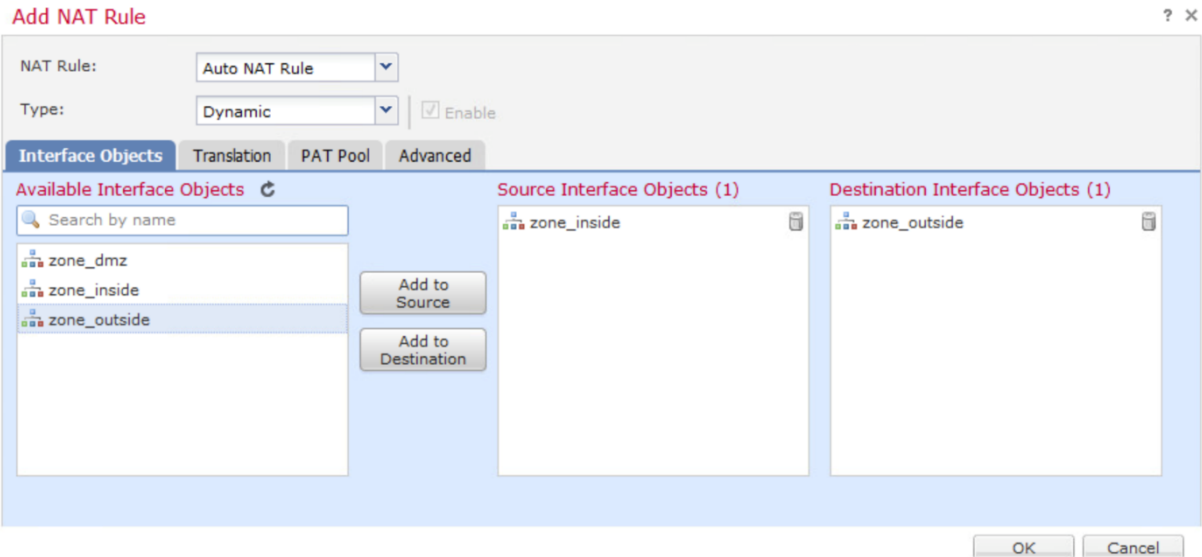


The NAT policy NAT-FTD is displayed, there are three sections, NAT Rules Before section 1, Auto NAT Rules section 2 and NAT Rules After section 3, FTD supports the same NAT configuration options as the Traditional Firewall ASA, so A NAT rule can be Auto-NAT or Manual NAT, Auto-NAT Rule also called object 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.

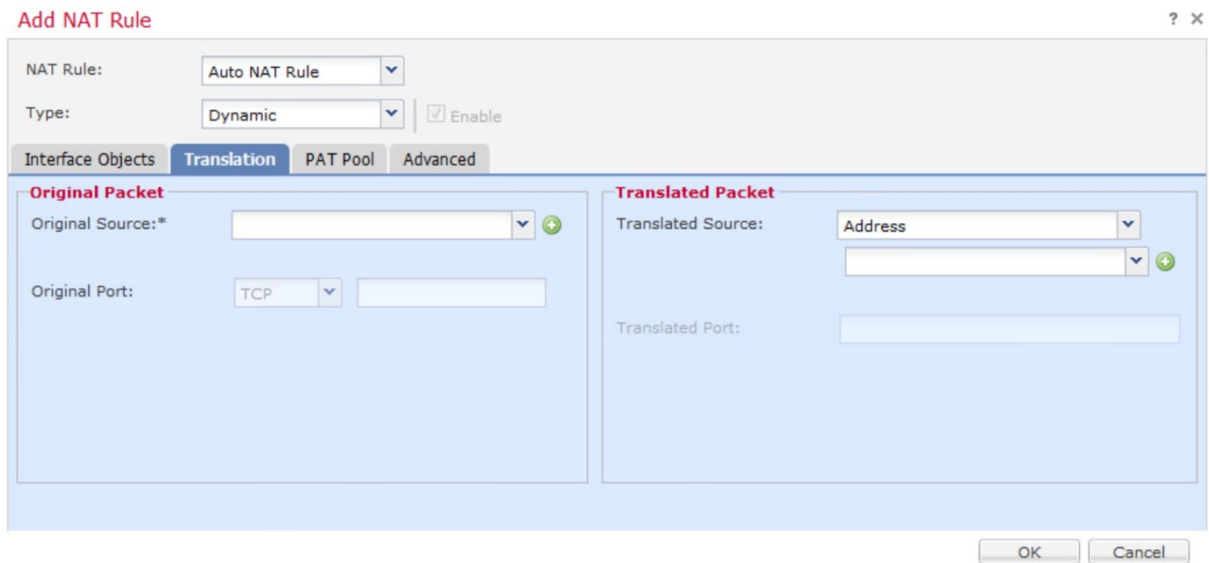
Click Add Rule, in the NAT Rule, select Auto NAT Rule and Type Dynamic to provide Port Address Translation, you have an option to select static if you want your server to be reachable from internet, if you select static you configure static NAT.



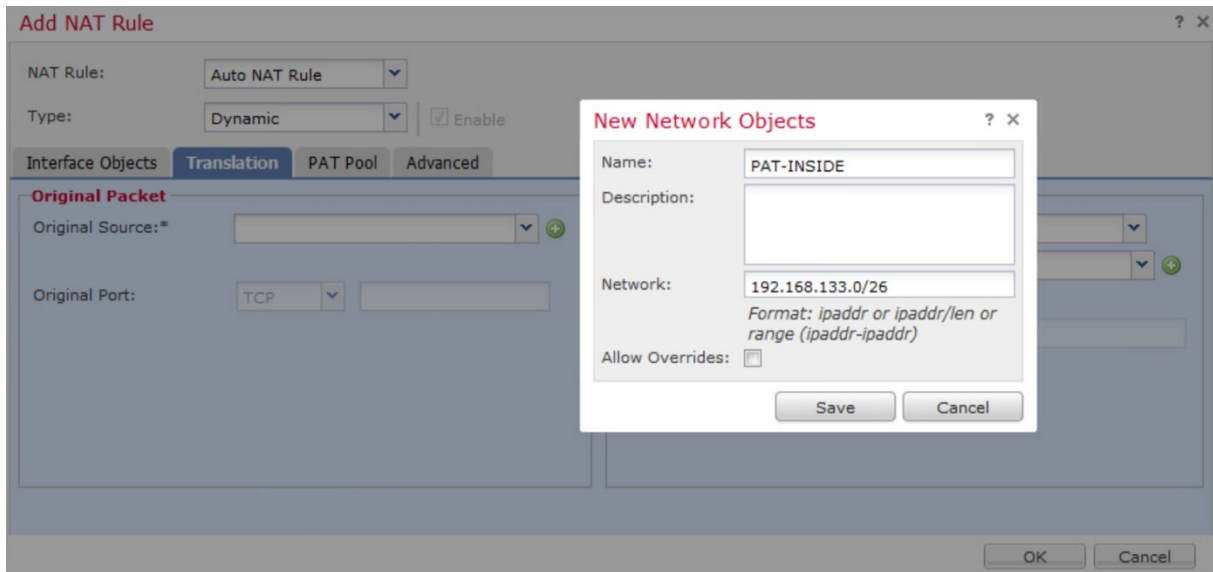
While on traditional ASA, you have to use nameif or the logical name in the NAT rules. On FTD, you need to use Security Zones. This is used for matching traffic.



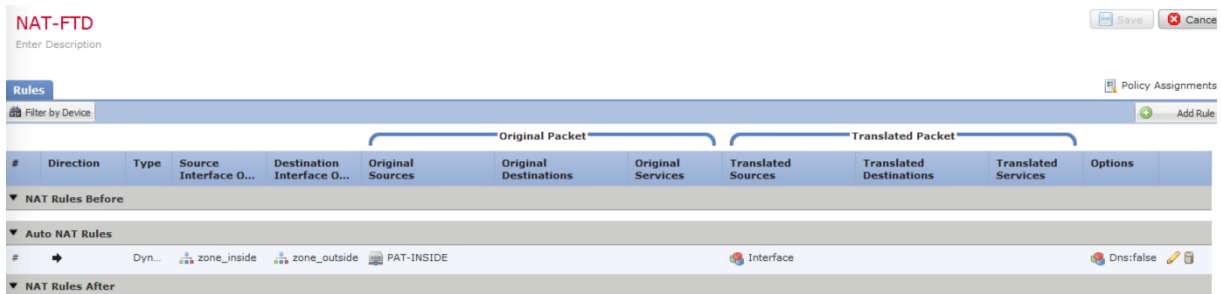
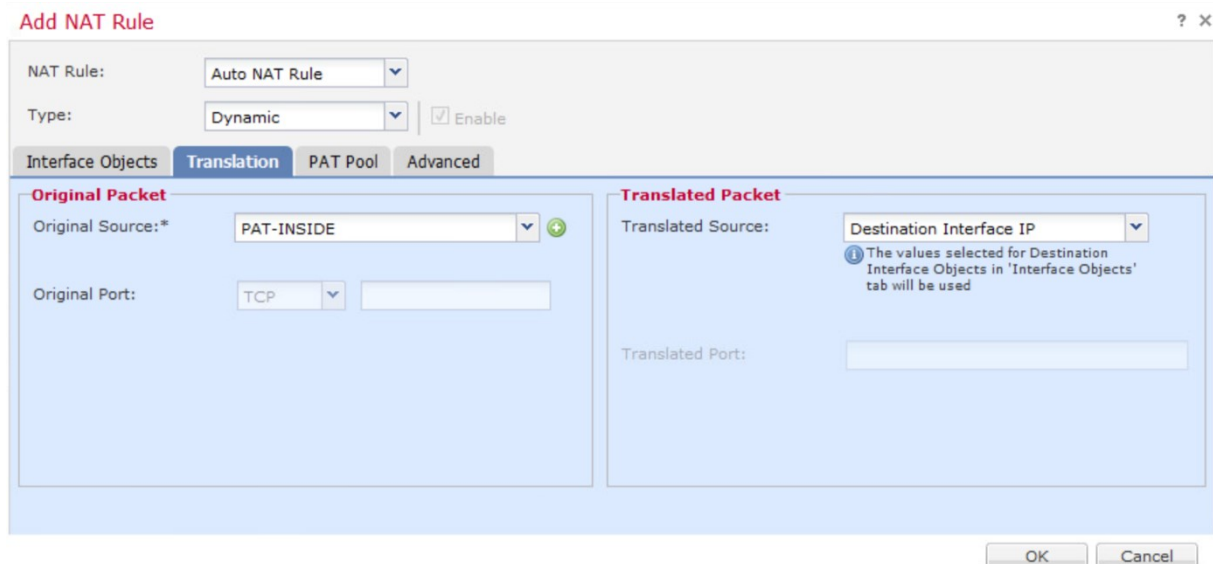
Translation has two sections. One is Original Packet, which is the conditions to match. The other is Translated Packet, here you see the Translated Source, this is how to translate the original source of the packet. The original packet is also called the Real Address. The Translated Source may be the 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.



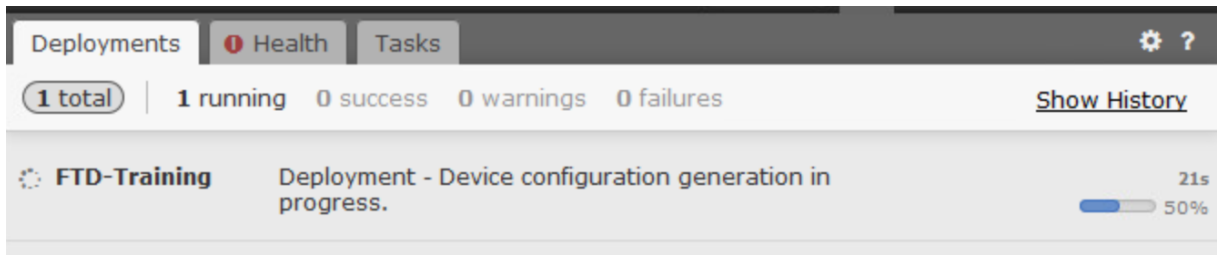
In the original Source create and add a Network Object for the inside network 192.168.133.0/26:



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



Deploy the NAT policy :

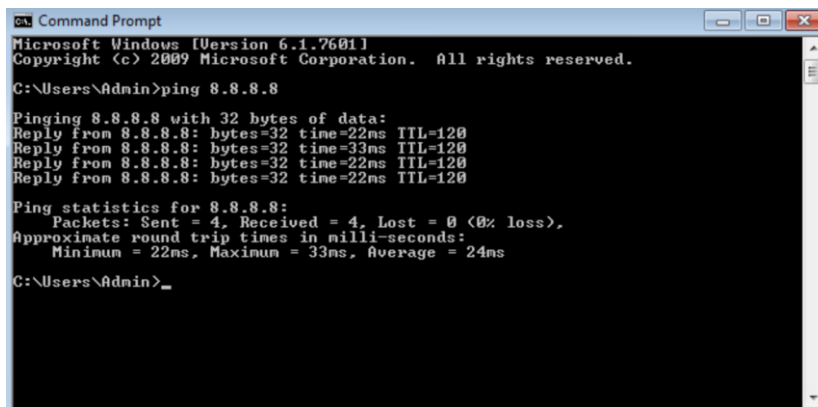


From CLI, verify the Auto-NAT configuration using the show run nat and the show run object commands:

```
> show running-config nat
!
object network PAT-INSIDE
 nat (inside,outside) dynamic interface
>
```

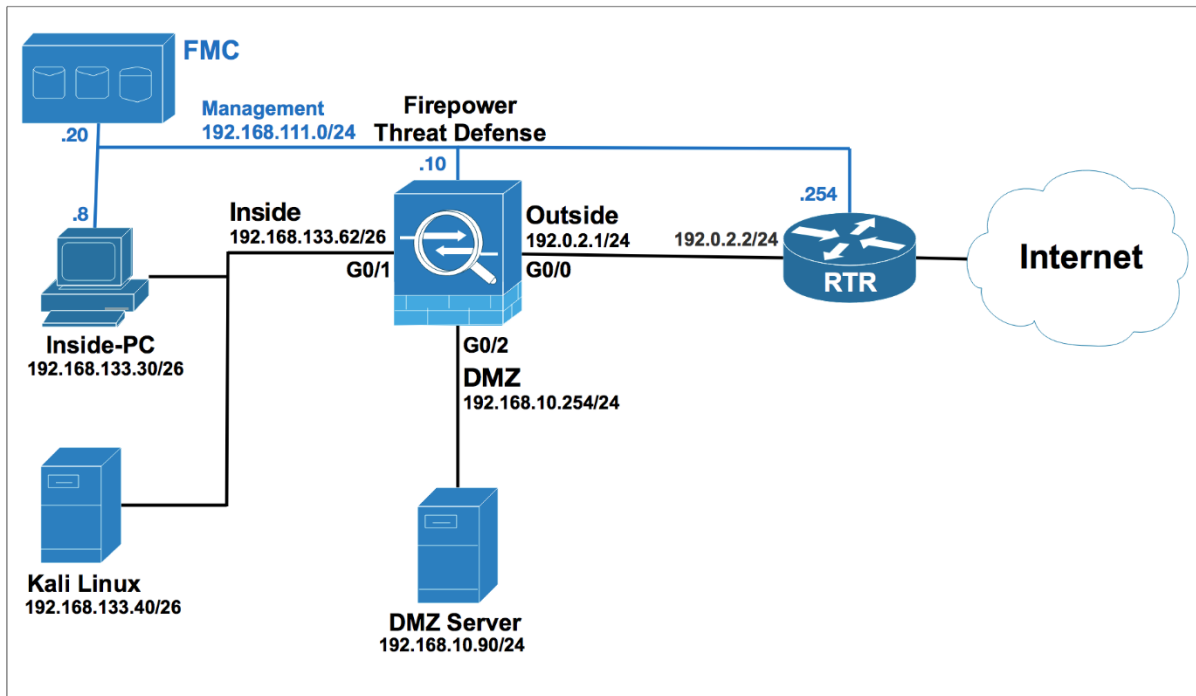
```
> show running-config object
object network PAT-INSIDE
 subnet 192.168.133.0 255.255.255.192
>
```

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

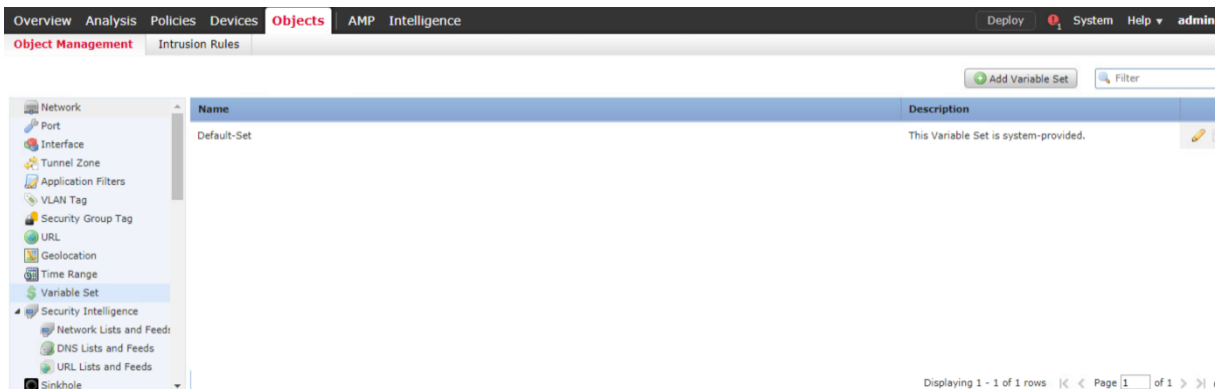


Verify that the ICMP packets are translated using the show nat command, and verify the translate_hits counter increased:

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.



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

? X

Name:

Description:

Variable Name	Type	Value	
Customized Variables			
<i>This category is empty</i>			
Default Variables			
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]	
DNS_SERVERS	Network	HOME_NET	
EXTERNAL_NET	Network	any	
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	
FTP_PORTS	Port	[21, 2100, 3535]	
GTP_PORTS	Port	[3386, 2123, 2152]	
HOME_NET	Network	any	

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

Edit Variable EXTERNAL_NET

? X

Name:

Type:

Available Networks

Search by name or value

- any
- IPv4-Private-All-RFC1918
- any-ipv4
- any-ipv6
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast
- PAT-INSIDE

Included Networks (0)

any

Excluded Networks (0)

none

Network Network

In the Name field enter **Inside-Network**, in the Network field enter **192.168.133.0/24**, your internal network.

New Network Objects ? x

Name:

Description:

Network:
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

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

Edit Variable EXTERNAL_NET ? x

Name:

Type:

Available Networks

Inside-Network

PAT-INSIDE

Included Networks (0)

Excluded Networks (1)

Inside-Network

Network

Network

Edit HOME_NET.

























Edit Variable Set Default-Set

? x

Name:

Description:

You have unsaved changes

Variable Name	Type	Value	
Customized Variables			
EXTERNAL_NET	Network	!Inside-Network	  
Default Variables			
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]	  
DNS_SERVERS	Network	HOME_NET	  
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	  
FTP_PORTS	Port	[21, 2100, 3535]	  
GTP_PORTS	Port	[3386, 2123, 2152]	  
HOME_NET	Network	any	  
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]	  

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

Edit Variable HOME_NET

Name: HOME_NET
Type: Network

Available Networks (3)

- EXTERNAL_NET
- TELNET_SERVERS
- Inside-Network

Included Networks (1)

- Inside-Network

Excluded Networks (0)

none

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 is system-provided.


You have unsaved changes Add

Variable Name	Type	Value	
Customized Variables			
EXTERNAL_NET	Network	!Inside-Network	
HOME_NET	Network	Inside-Network	
Default Variables			
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]	
DNS_SERVERS	Network	HOME_NET	
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	
FTP_PORTS	Port	[21, 2100, 3535]	
GTP_PORTS	Port	[3386, 2123, 2152]	
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]	

Save Cancel

Click **Yes** to confirm the changes.

Save

 This variable set is in use by an Access Control policy. Modifying it may affect detection, and you must reapply the policy before changes take effect.

Changes to the Default Set will also change the default values in all other sets. Do you wish to continue?

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**.



Create Intrusion Policy

Policy Information

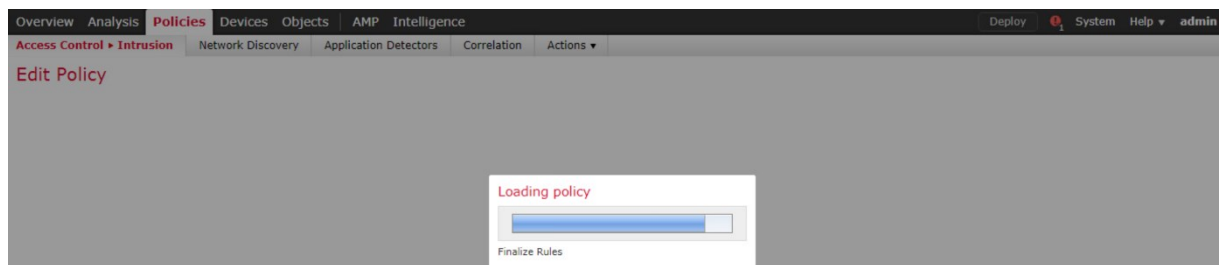
Name *

Description

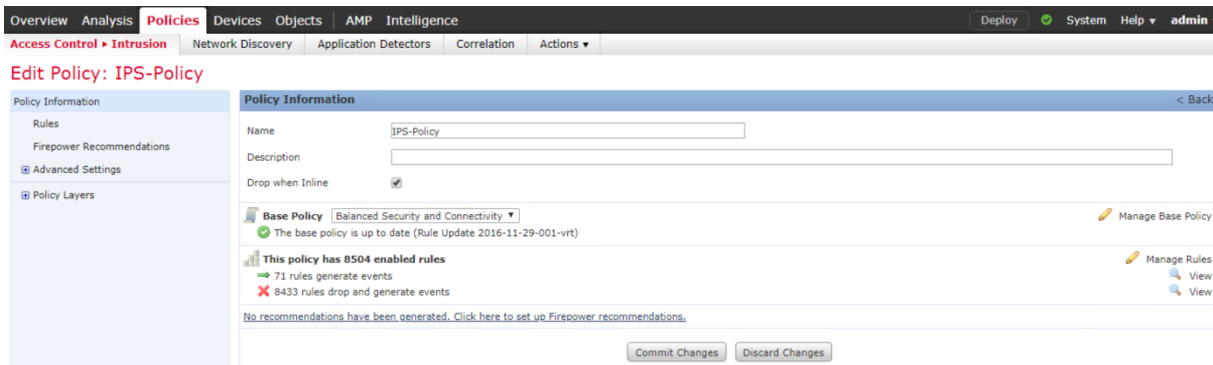
Drop when Inline

Base Policy

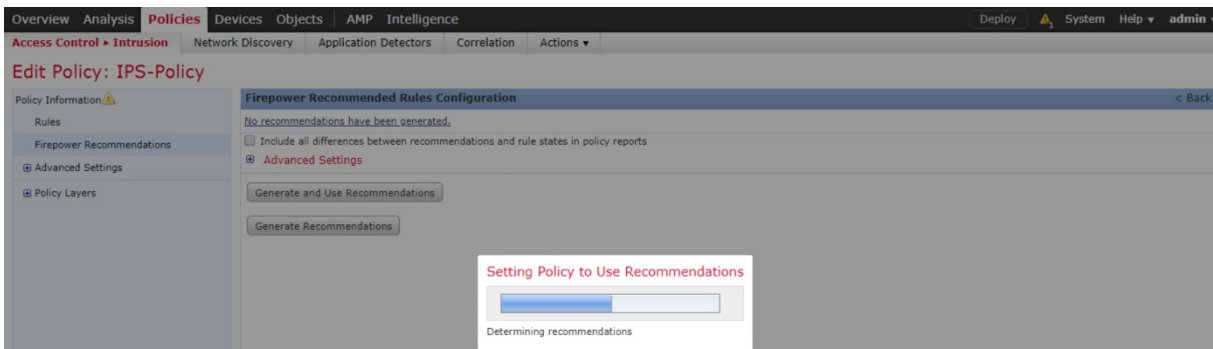
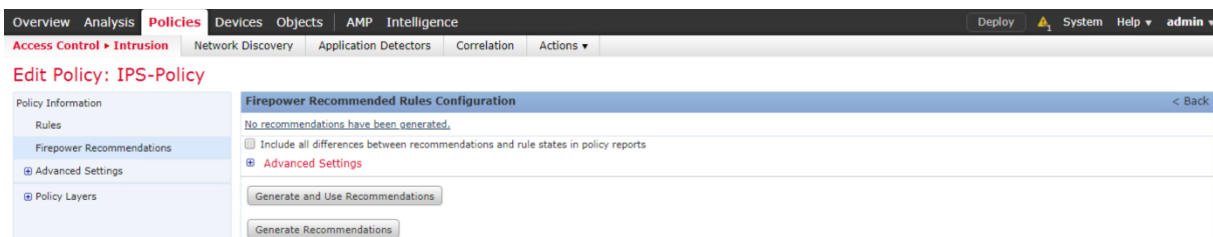
* Required



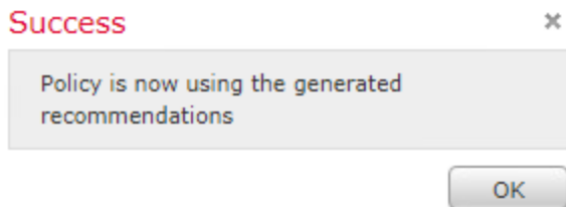
The IPS policy is edited.
Click the **Firepower Recommendations** option in the left panel of the window.

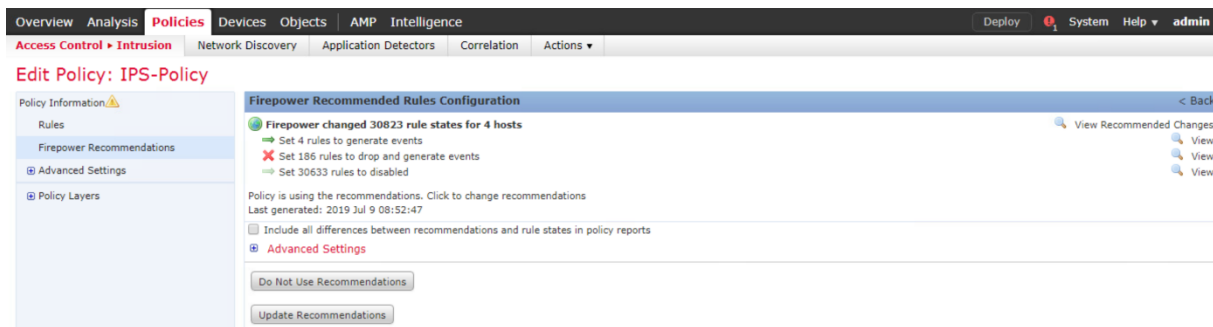


Click the **Generate and Use Recommendations** button.



The system informs you with message that the recommendation generation process is Successful. Click **OK**.





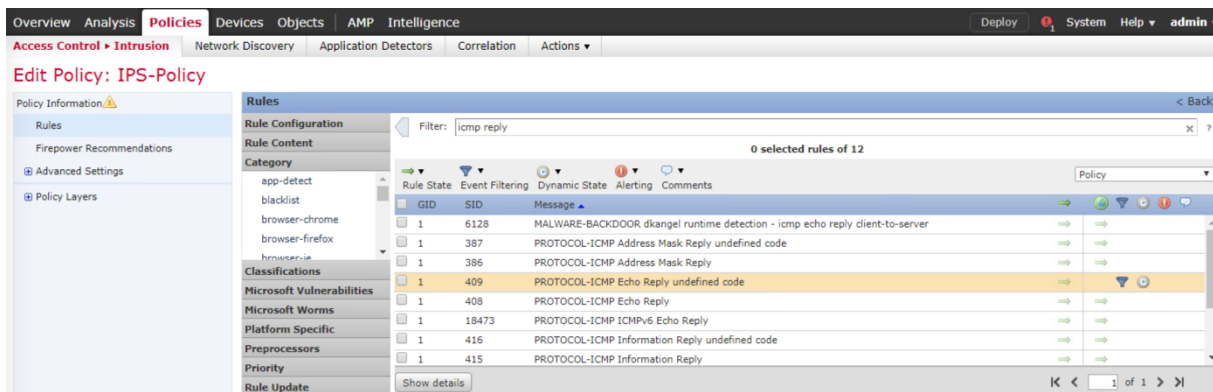
Click **Rule**, you will find a list of intrusion rules that are available on the system.

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**.

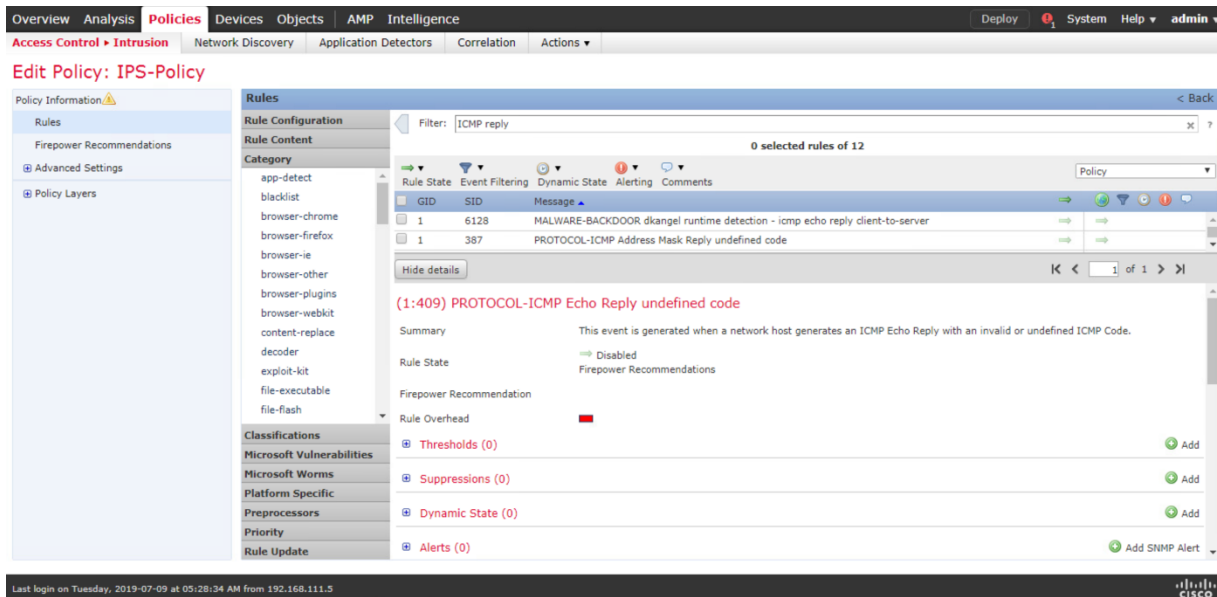


By default the state of the rule is **Disabled**.

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

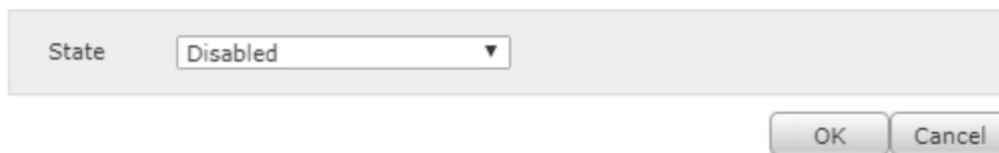
1. **Generate Events:** This option generates events when the rule matches the traffic.
2. **Drop and Generate Events:** This option generates events and drop traffic when the rule matches the traffic.
3. **Disable:** This option disables the rule.

Update that and change it to **Generate Events**.



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

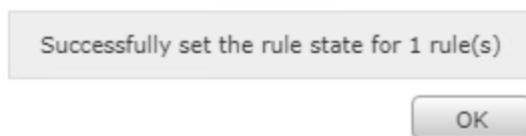
Set rule state for "PROTOCOL-ICMP Echo Reply undefined code" ? ✕



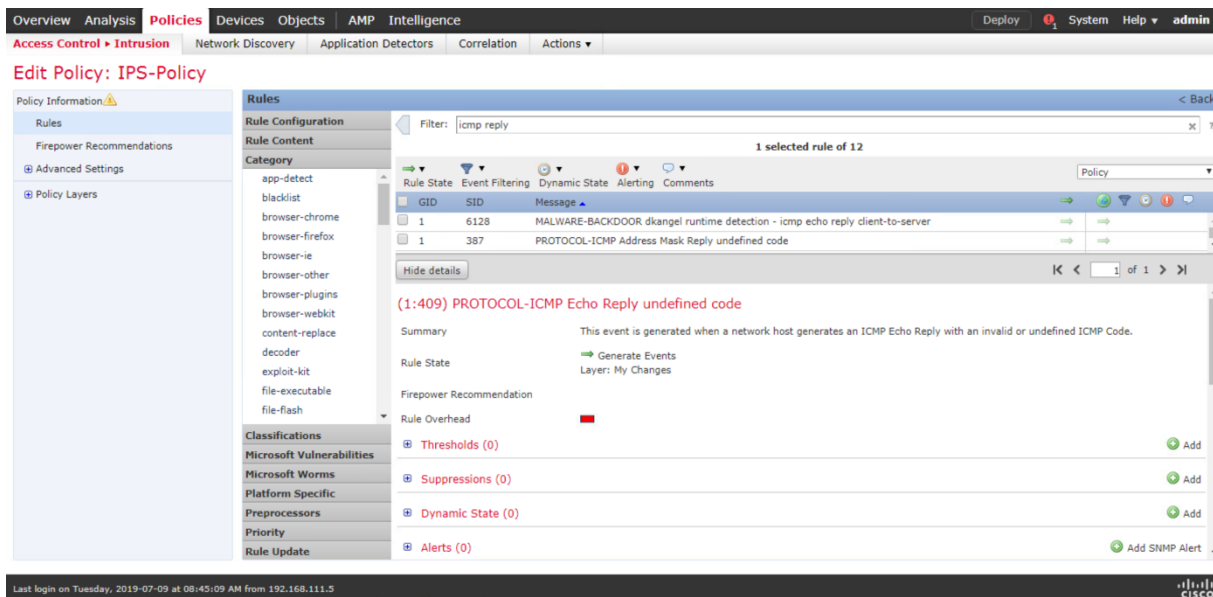
Set rule state for "PROTOCOL-ICMP Echo Reply undefined code" ? ✕



Success ✕



The state now is set to Generate Events.



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 may 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)	+ Add
⊞ Suppressions (0)	+ Add
⊞ Dynamic State (0)	+ 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" ? x

Type	Both ▼
Track By	Source ▼
Count	3
Seconds	10

Click **OK** to complete.

Success x

Successfully set the threshold for 1 rule(s)

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.

[-] **Thresholds (1)**

Type	Count	Seconds	Track By	
Both	3	10	Source	Delete

[+] **Suppressions (0)** + Add

[-] **Dynamic State (0)** + Add

There are no dynamic states for this rule

[+] **Alerts (0)** + Add SNMP Alert

[+] **Comments (0)** + Add

[+] **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" ? x

Track By	Destination ▼
Network	<input type="text"/>
Rate	<input type="text"/> Count / <input type="text"/> Seconds
New State	Drop and Generate Events ▼
Timeout	<input type="text"/>

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

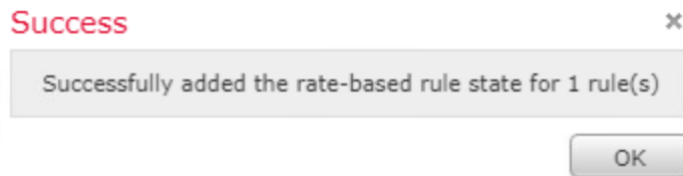
Track By:

Rate: Count / Seconds

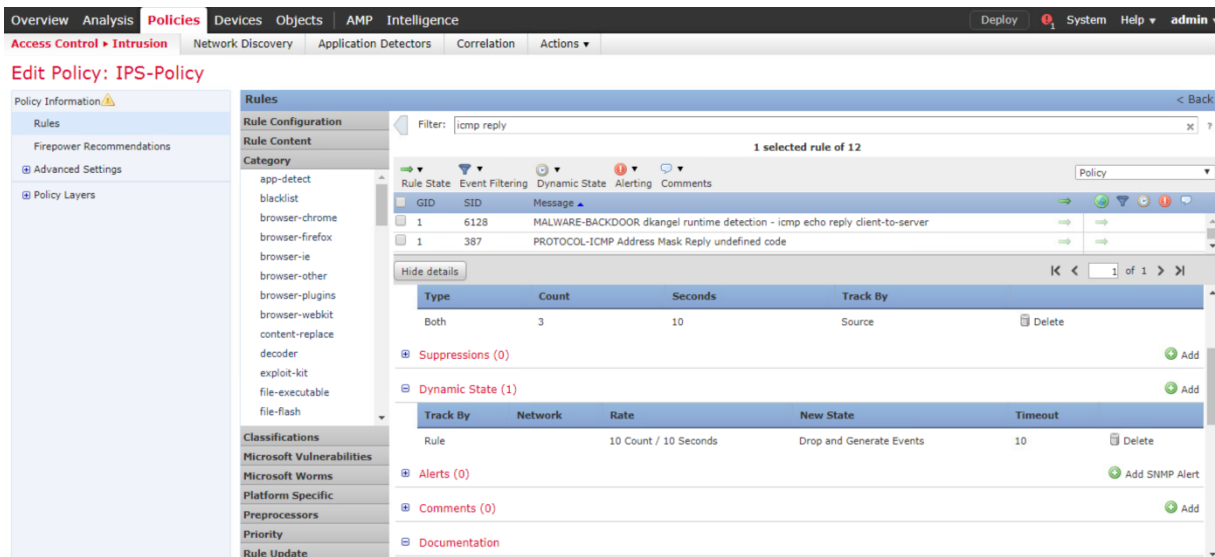
New State:

Timeout:

Click **OK** to complete.



You should have the following output.



Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Intrusion Network Discovery Application Detectors Correlation Actions

Edit Policy: IPS-Policy

Policy Information

Rules

Firepower Recommendations

Advanced Settings

Policy Layers

Rules

Rule Configuration

Rule Content

Category

- app-detect
- blacklist
- browser-chrome
- browser-firefox
- browser-ie
- browser-other
- browser-plugins
- browser-webkit
- content-replace
- decoder
- exploit-kit
- file-executable
- file-flash

Classifications

- Microsoft Vulnerabilities
- Microsoft Worms
- Platform Specific
- Preprocessors
- Priority
- Rule Update

Filter: icmp reply 1 selected rule of 12

Rule State	Event Filtering	Dynamic State	Alerting	Comments
1	6128	MALWARE-BACKDOOR dkangel runtime detection - icmp echo reply client-to-server		
1	387	PROTOCOL-ICMP Address Mask Reply undefined code		

Hide details

Type	Count	Seconds	Track By
Both	3	10	Source

Suppressions (0) Add

Dynamic State (1) Add

Track By	Network	Rate	New State	Timeout
Rule		10 Count / 10 Seconds	Drop and Generate Events	10

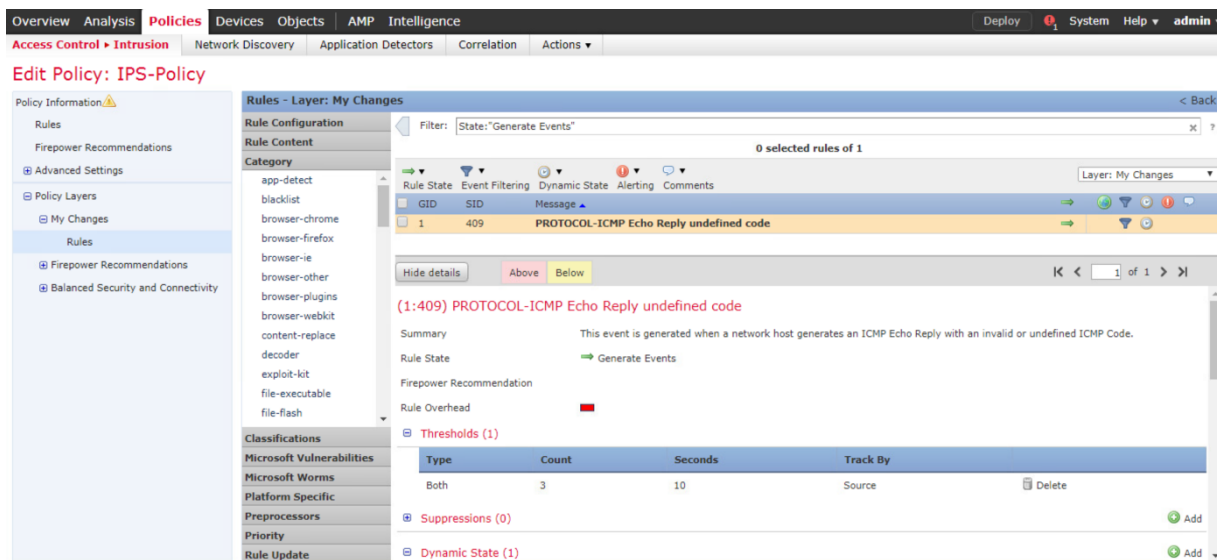
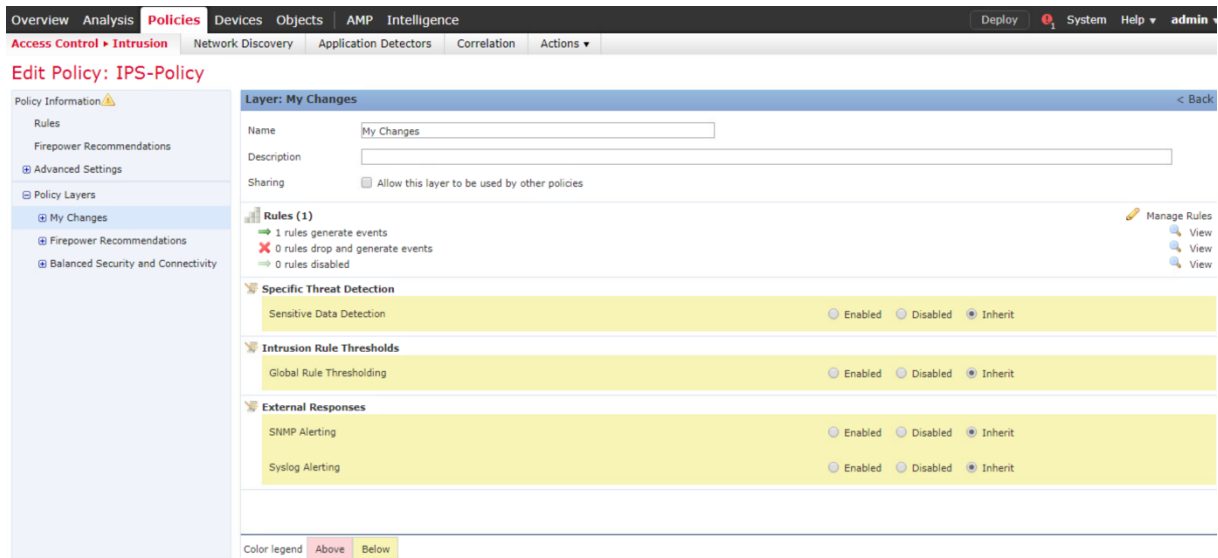
Alerts (0) Add SNMP Alert

Comments (0) Add

Documentation

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

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



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

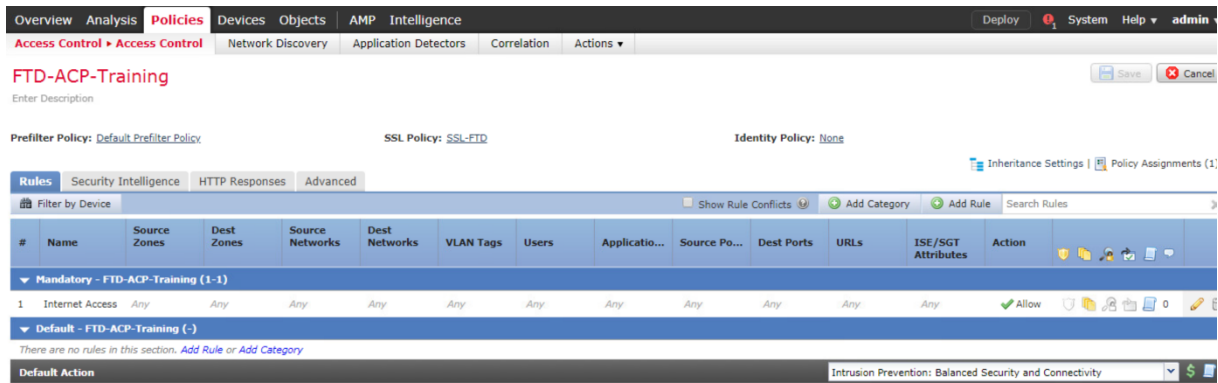
Click **OK** to complete.

Committing...

Gathering All Objects

Intrusion Policy	Drop when Inline	Status	Last Modified
IPS-Policy	Yes	No access control policies use this policy Policy not applied on any devices	2019-07-09 09:12:09 Modified by "admin"

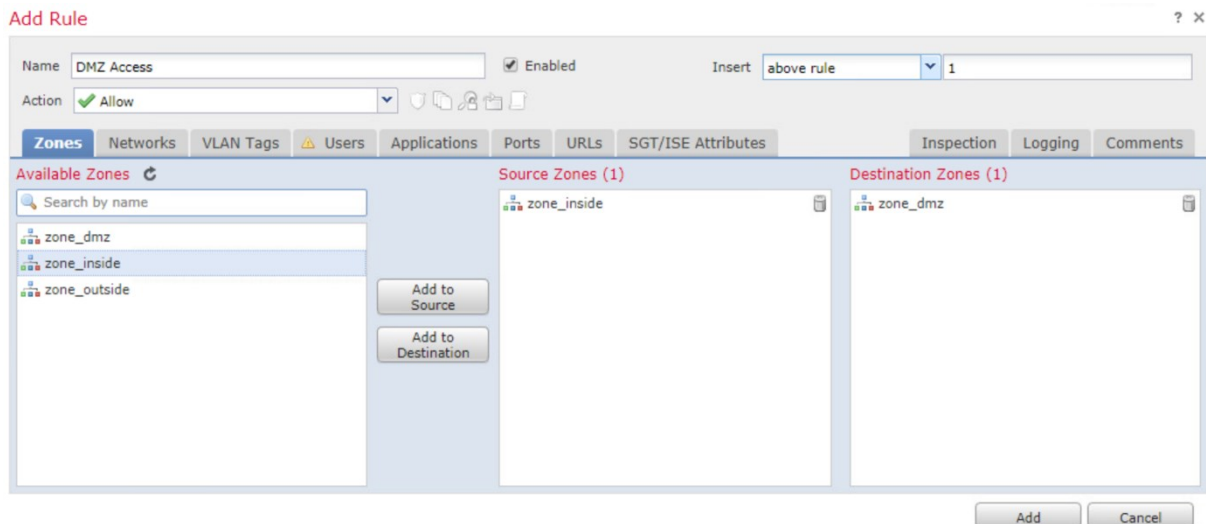
Navigate to the **Policies > Access Control > Intrusion**.
Edit the **FTD-ACP-Training** access control policy.



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**.



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

Add Rule ? x

Name: Enabled Insert:

Action:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes **Inspection** Logging Comments

Intrusion Policy: Variable Set:

File Policy:

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**.

Add Rule ? x

Name: Enabled Insert:

Action:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection **Logging** Comments

Log at Beginning of Connection
 Log at End of Connection

File Events:
 Log Files

Send Connection Events to:
 Event Viewer
 Syslog
 SNMP Trap

Click **Save**.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

FTD-ACP-Training You have unsaved changes Save Cancel

Enter Description

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None Inheritance Settings Policy Assignments (1)

Rules Security Intelligence HTTP Responses Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action
Mandatory - FTD-ACP-Training (1-2)													
1	DMZ Access	zone_inside	zone_dmz	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
2	Internet Access	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
Default - FTD-ACP-Training (-)													
There are no rules in this section. Add Rule or Add Category													

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

FTD-ACP-Training Save Cancel

Enter Description

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None Inheritance Settings Policy Assignments (1)

Rules Security Intelligence HTTP Responses Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source P...	Dest Ports	URLs	ISE/SGT Attributes	Action
Mandatory - FTD-ACP-Training (1-2)													
1	DMZ Access	zone_inside	zone_dmz	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
2	Internet Access	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
Default - FTD-ACP-Training (-)													
There are no rules in this section. Add Rule or Add Category													

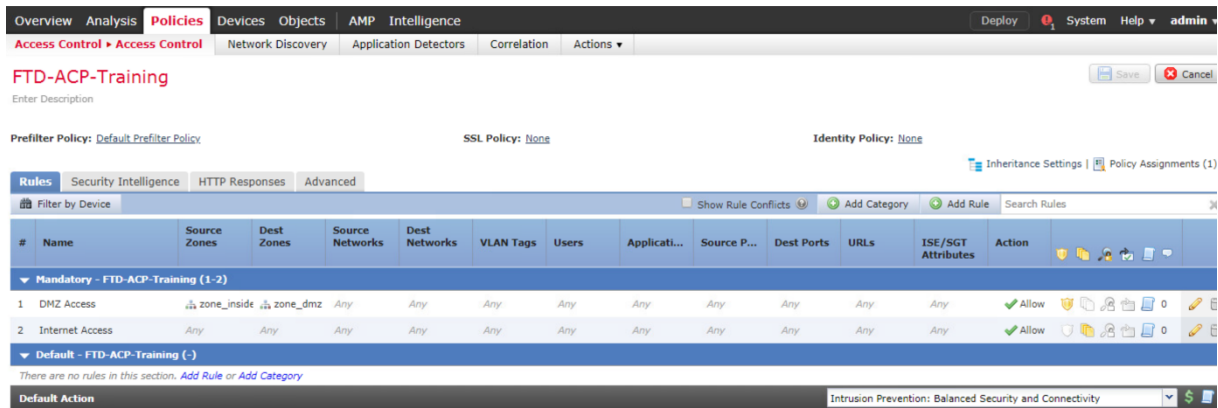
Deploy the Access Control Policy to the managed device.

Deploy Policies Version:2019-07-09 04:17 PM ? X

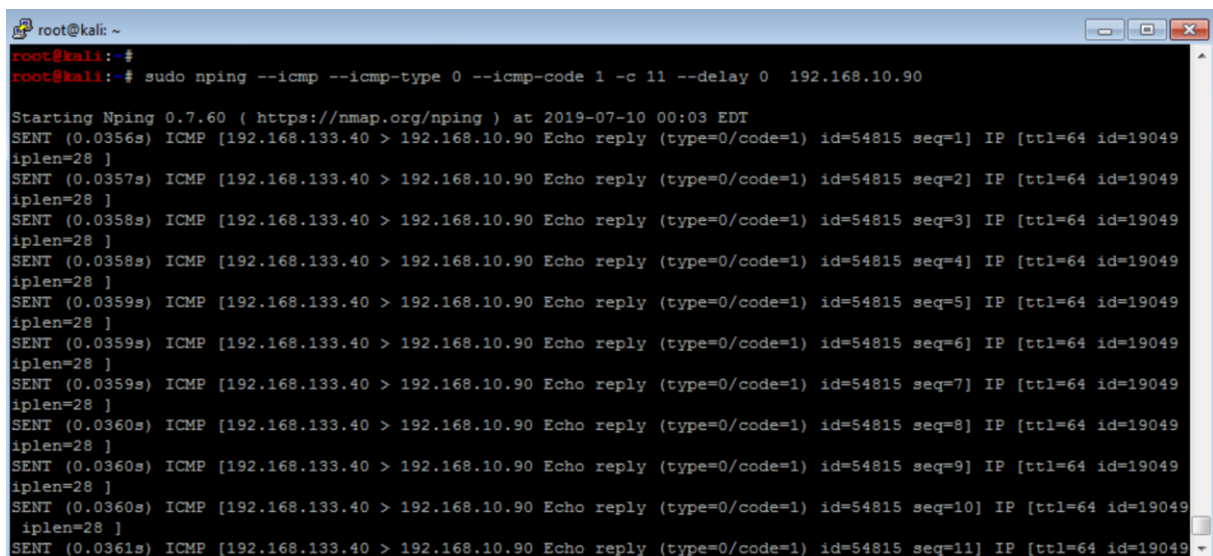
Device	Group	Current Version
<input checked="" type="checkbox"/> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Nat Policy: NAT-FTD <input checked="" type="checkbox"/> Access Control Policy: FTD-ACP-Training <input checked="" type="checkbox"/> DNS Policy: DNS-policy <input checked="" type="checkbox"/> Intrusion Policy: IPS-Policy <input checked="" type="checkbox"/> Intrusion Policy: Balanced Security and Connectivity <input checked="" type="checkbox"/> File Policy: File-policy <input checked="" type="checkbox"/> Prefilter Policy: Default Prefilter Policy <input checked="" type="checkbox"/> Network Discovery <input checked="" type="checkbox"/> Device Configuration (Details) 		2019-07-09 03:22 PM

Selected devices: 1

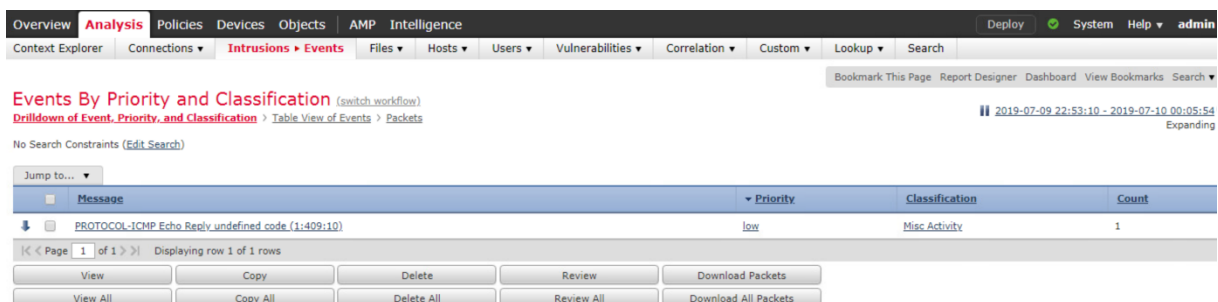
Deploy Cancel



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.



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



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.

Events By Priority and Classification (switch workflow)
 Drilldown of Event, Priority, and Classification > **Table View of Events** > Packets
 2019-07-09 22:53:10 - 2019-07-10 00:07:13
 Expanding
 Disabled Column

Search Constraints (Edit Search)

Jump to... ▾

Time	Priority	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID
2019-07-10 00:05:03	low	2	↓	192.168.133.40		192.168.10.90		0 (Echo Reply) / icmp	1 / icmp	Unknown (Unknown)	0

<< Page 1 of 1 >> | Displaying row 1 of 1 rows

View Copy Delete Review Download Packets
 View All Copy All Delete All Review All Download All Packets

IOC	Application Risk	Business Relevance	Ingress Security Zone	Egress Security Zone	Device	Ingress Interface	Egress Interface	Intrusion Policy	Access Control Policy	Access Control Rule	Network Analysis Policy
Medium	Medium	zone_inside	zone_dmz	FTD-Training	inside	dmz	IPS-Policy	FTD-ACP-Training	DMZ Access	Balanced Security and Connectivity	

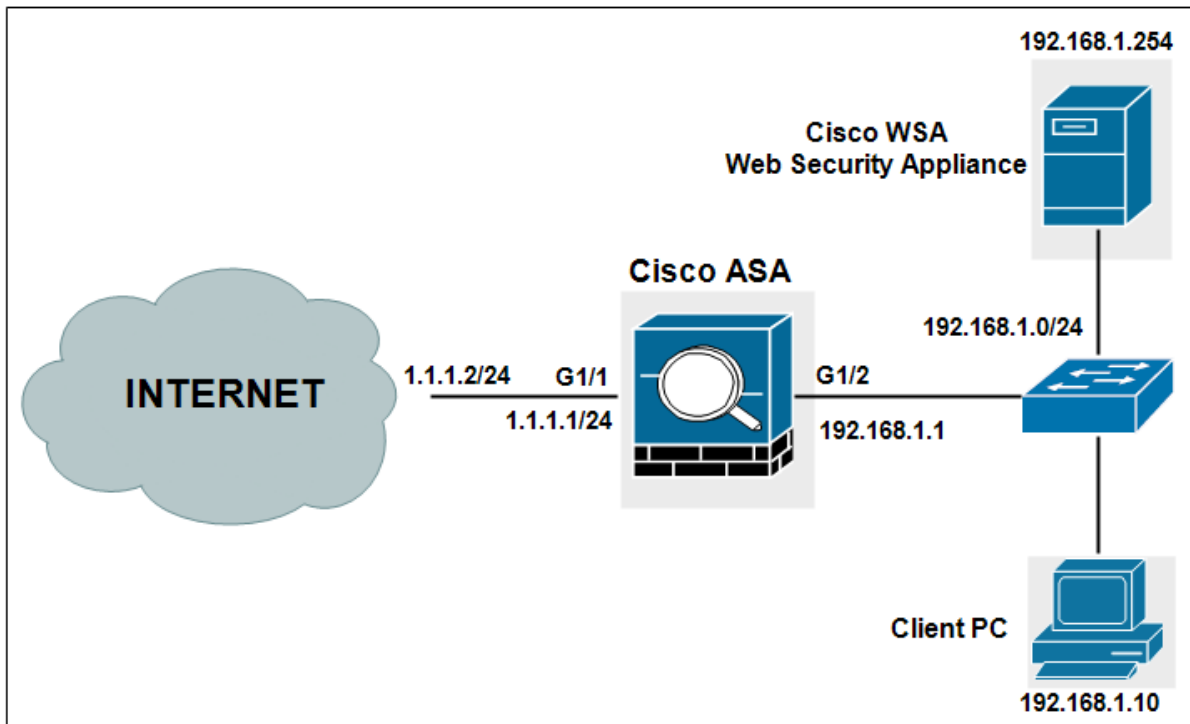
From the **Analysis > Intrusions > Events** page, click **Packets** to get detailed information about each event.

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



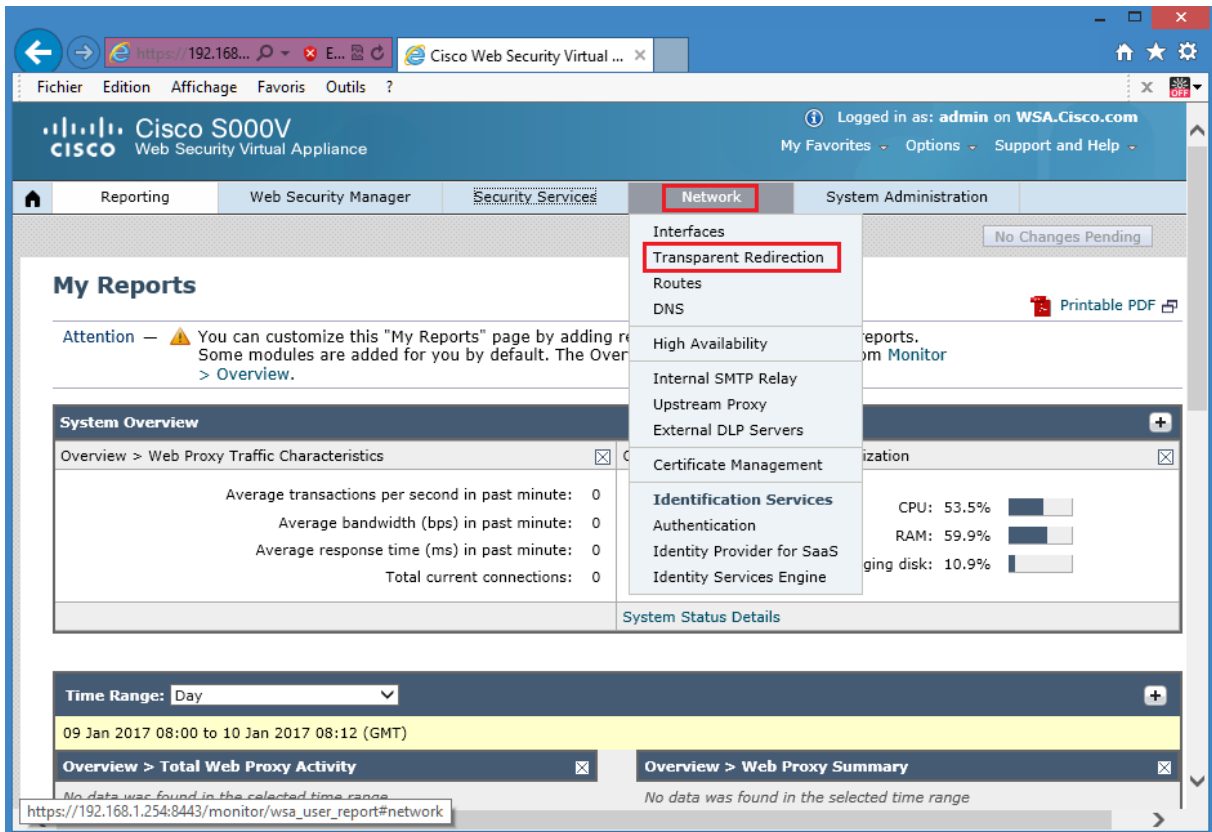
Common approaches include the following:

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.

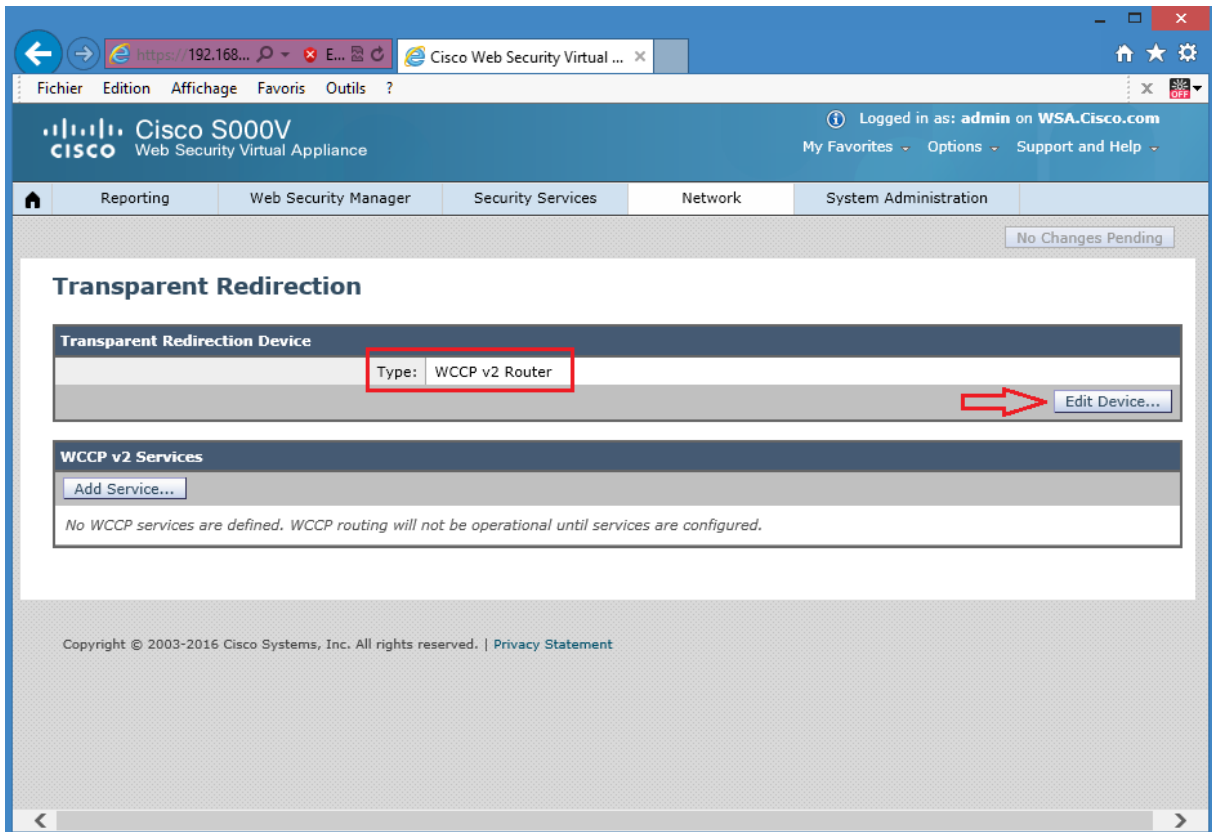
PBR: Routers can redirect HTTP and HTTPS traffic using PBR. However, PBR is implemented in software and therefore can be resource-sensitive.

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**.



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



Configuring WCCP Services

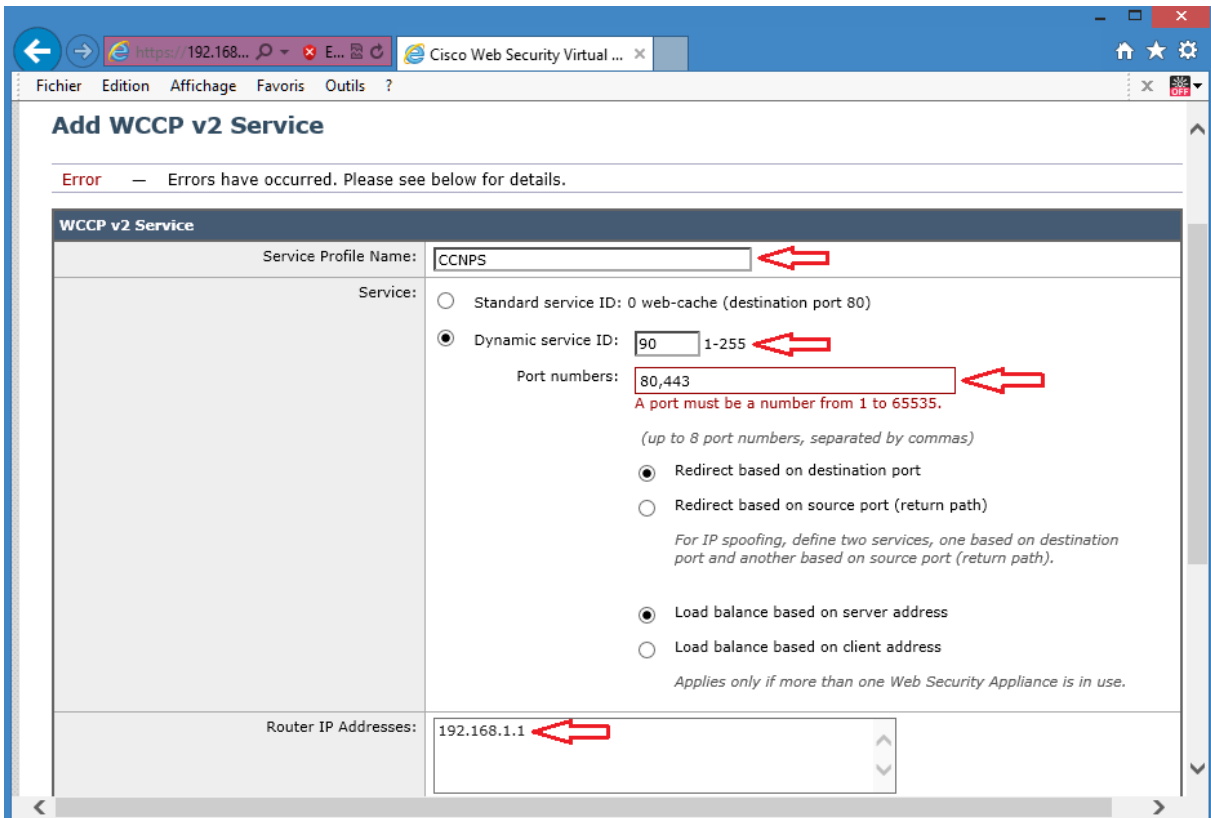
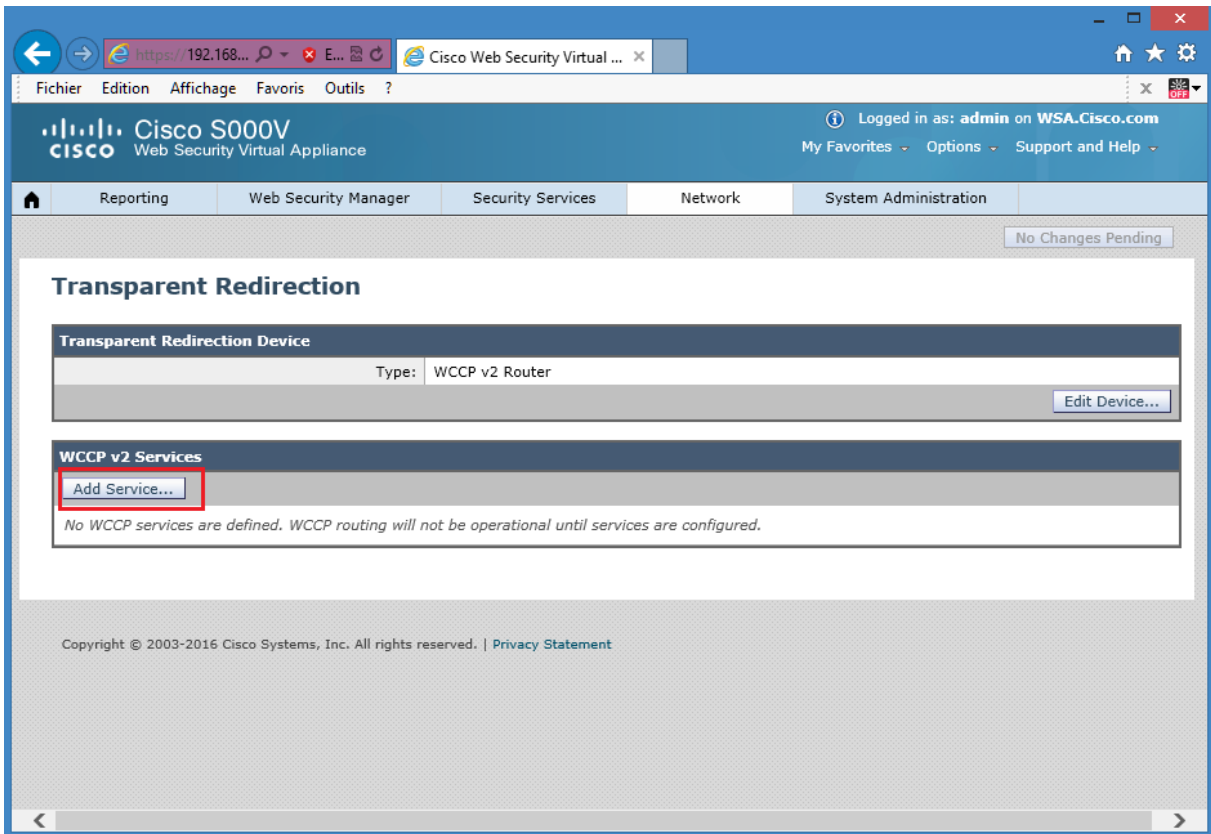
Under **WCCPv2** Services, click **Add Service** and add the following.

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)



Submit and commit your changes.

Router IP Addresses: 192.168.1.1

Router Security: Enable Security for Service

Passphrase:

Confirm Passphrase:

Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

Cancel Submit

Cisco S000V Web Security Virtual Appliance

Logged in as: admin on WSA.Cisco.com

Reporting Web Security Manager Security Services Network System Administration

Commit Changes >

Transparent Redirection

Transparent Redirection Device

Type: WCCP v2 Router

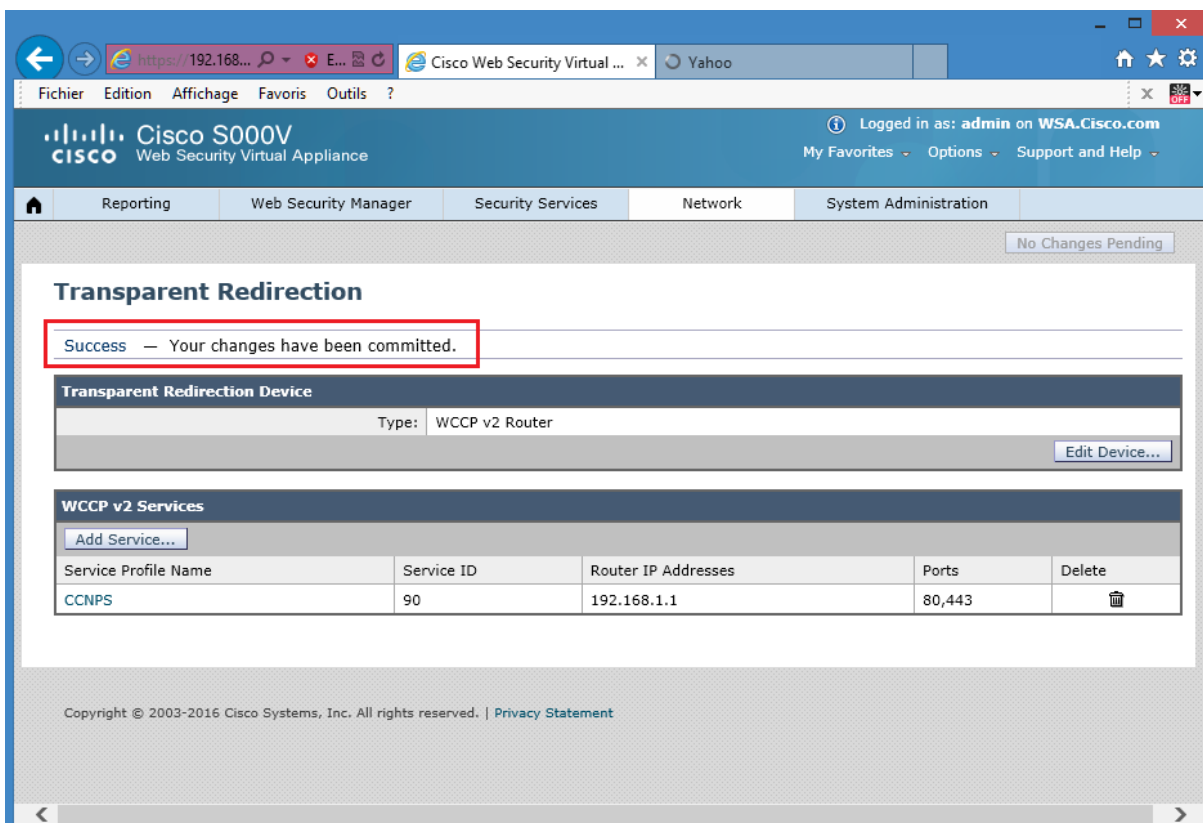
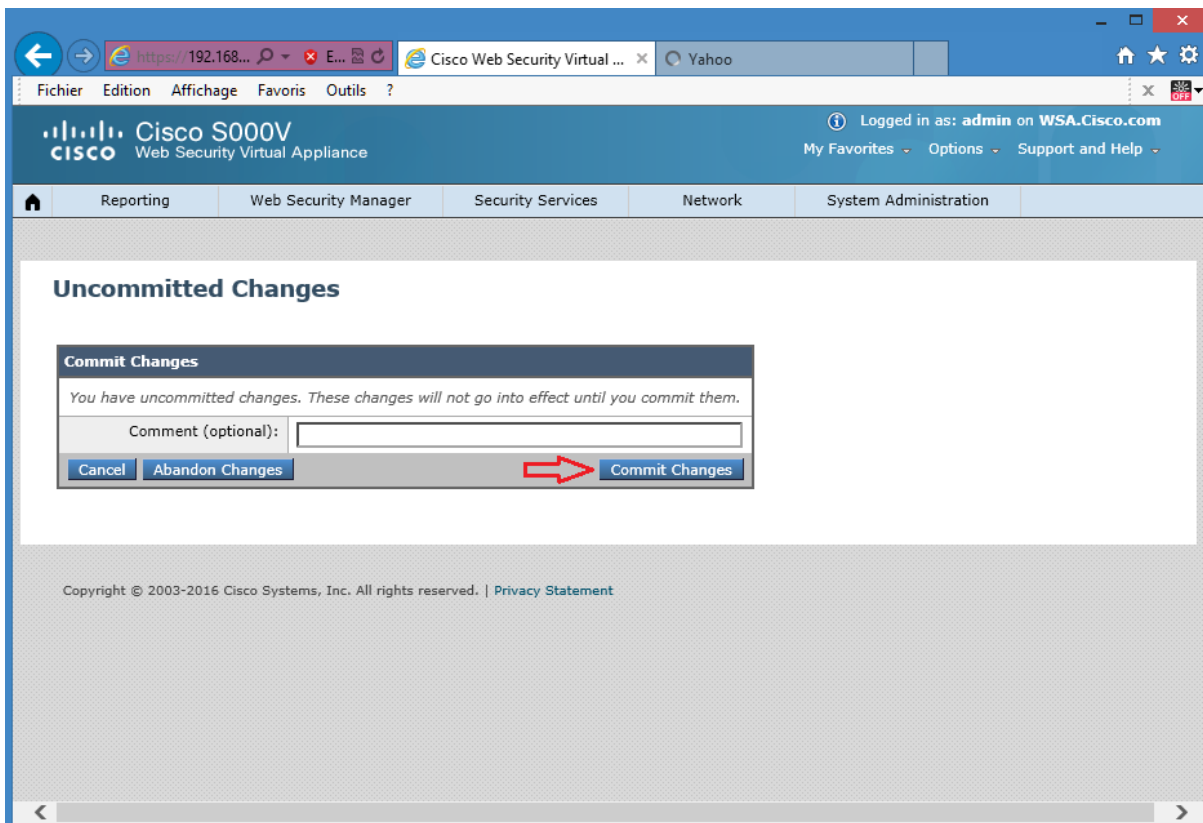
Edit Device...

WCCP v2 Services

Add Service...

Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
CCNPS	90	192.168.1.1	80,443	

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



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 successful:

```

ciscoasa# sh wccp 90 view

  WCCP Routers Informed of:
  192.168.1.1

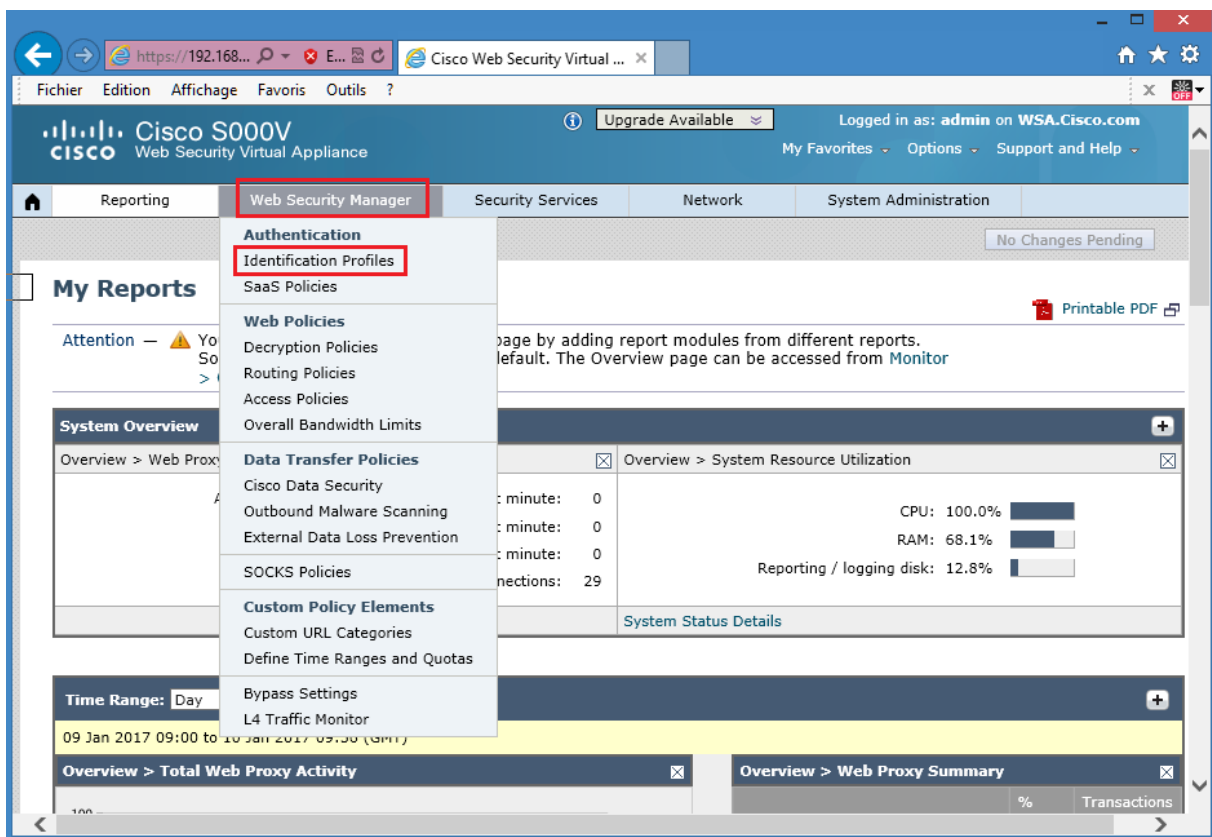
  WCCP Cache Engines Visible:
  192.168.1.254

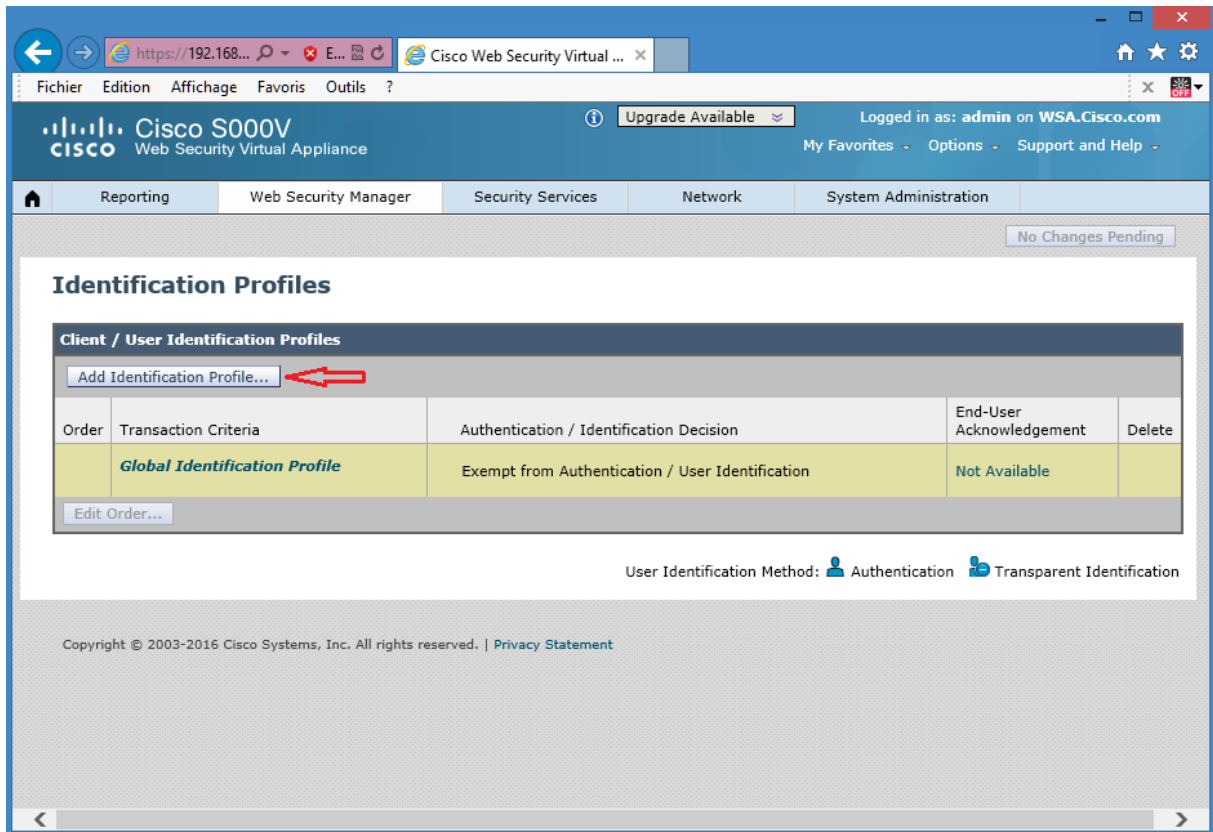
  WCCP Cache Engines NOT Visible:
  -none-
ciscoasa#

```

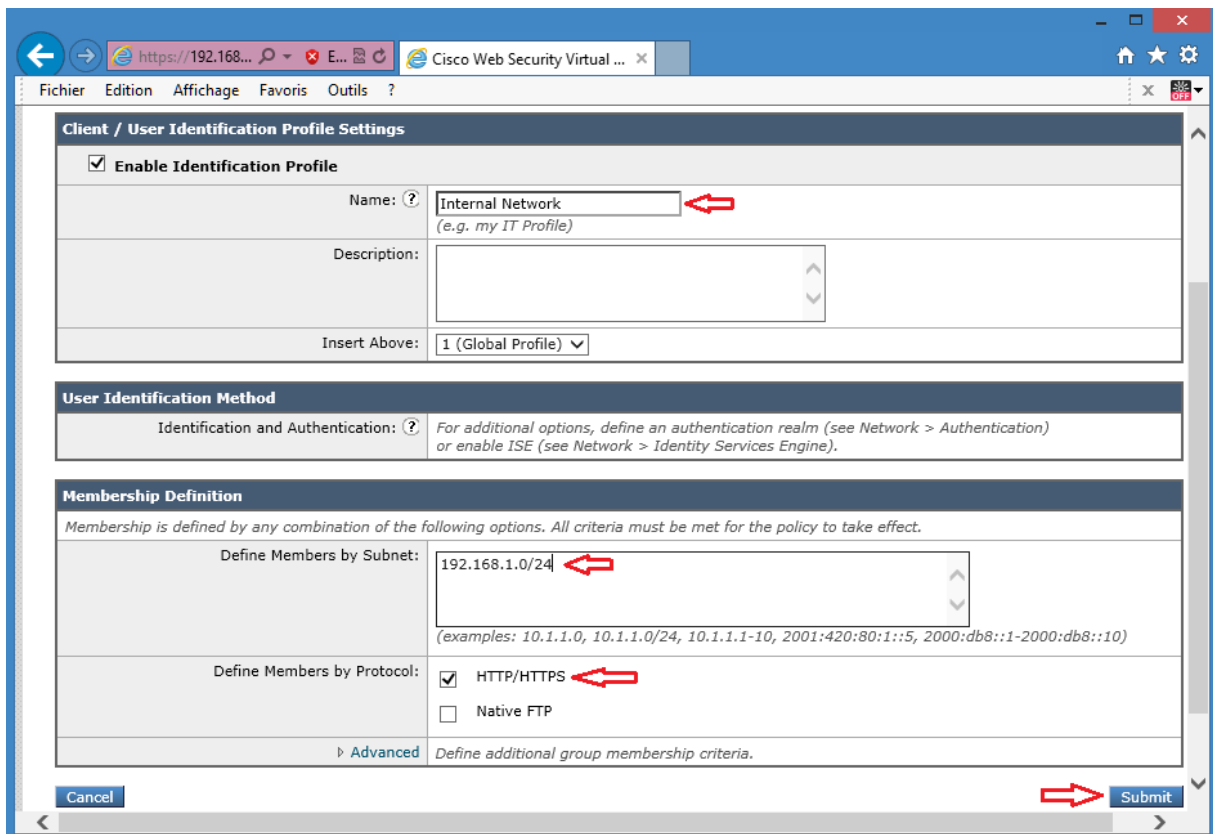
Configure an Identity named **Internal Network**, which will be required to use Basic authentication. The Identity named will be identified based on the IP subnet and by the HTTP or HTTPS protocol.

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





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.



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

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)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

[Edit Order...](#)

User Identification Method: Authentication Transparent Identification

Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

Success — Your changes have been committed.

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)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

[Edit Order...](#)

User Identification Method: Authentication Transparent Identification

Copyright © 2003-2016 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

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

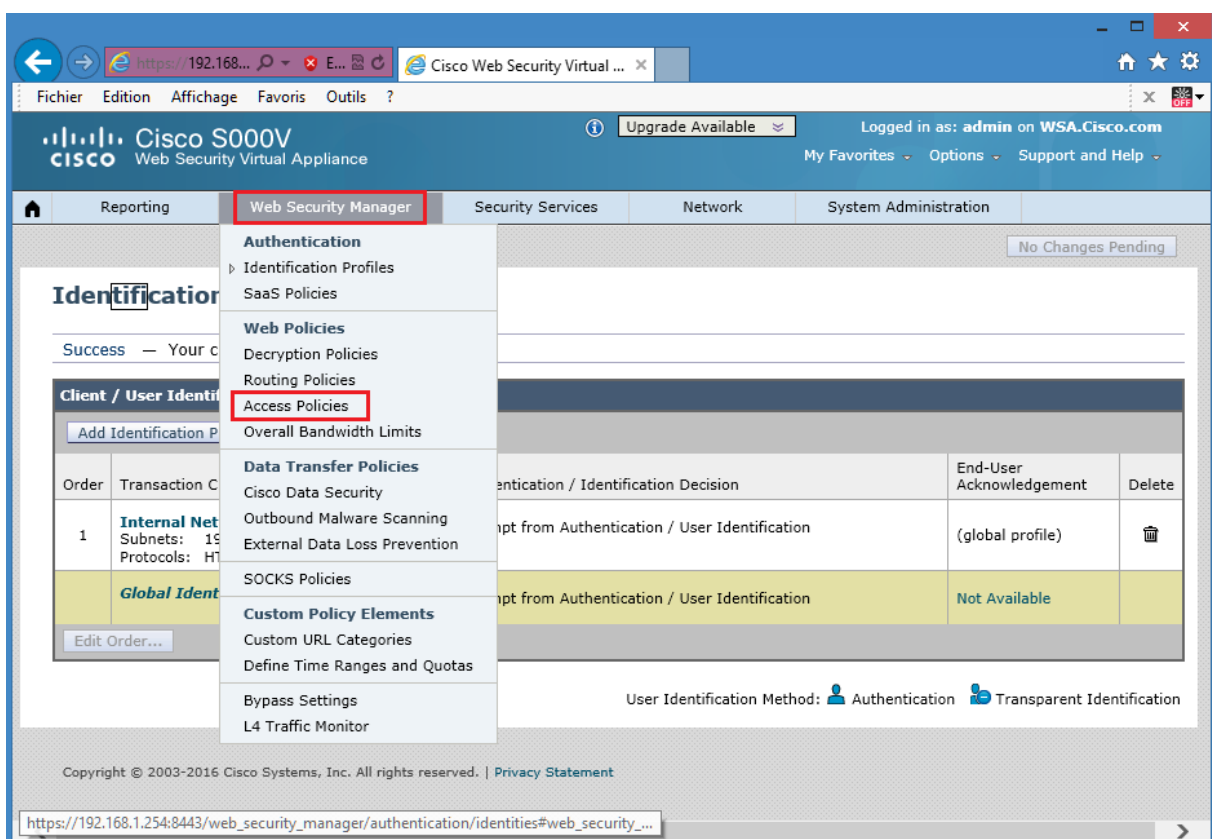
Protocol and User Agents: This setting is for the port and protocol of the HTTP request (for example: block FTP over HTTP).

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

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

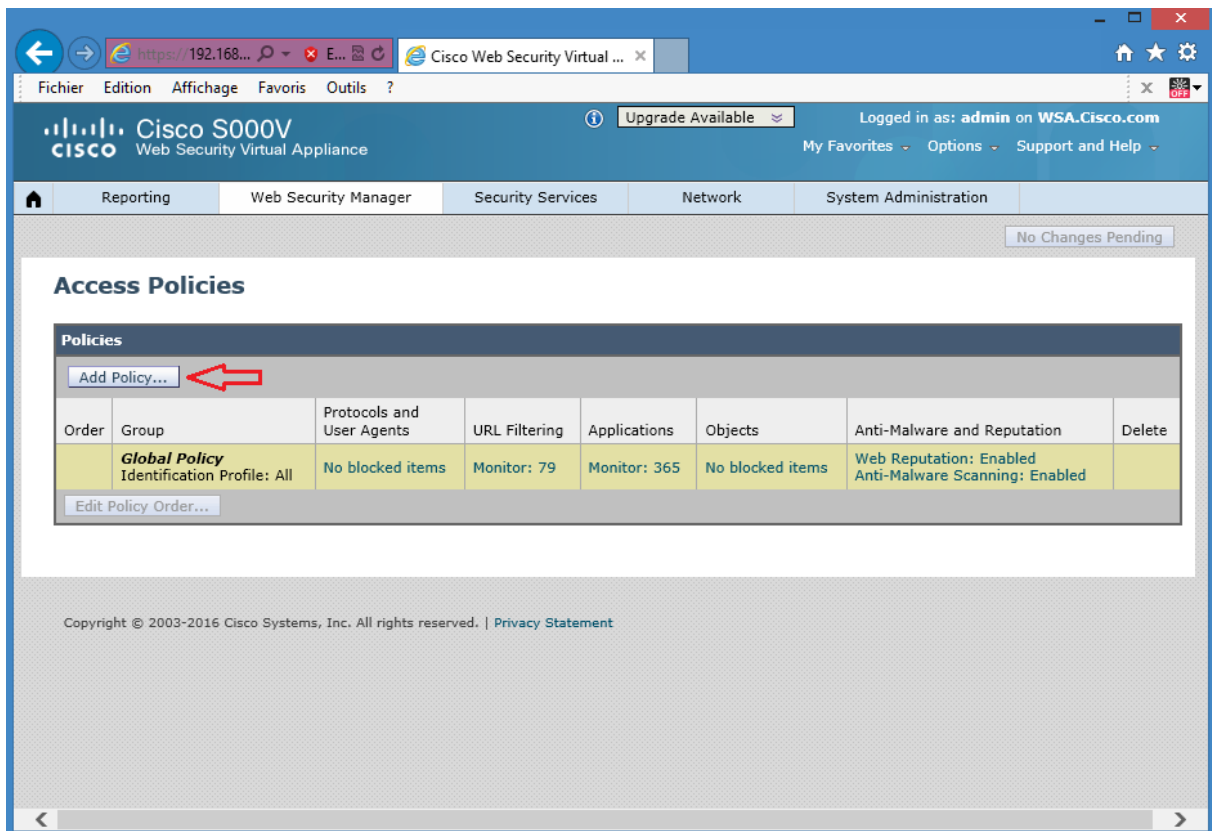
Web Reputation and Anti-Malware Filtering: Leverages Cisco expertise and database of web reputation and malware information.

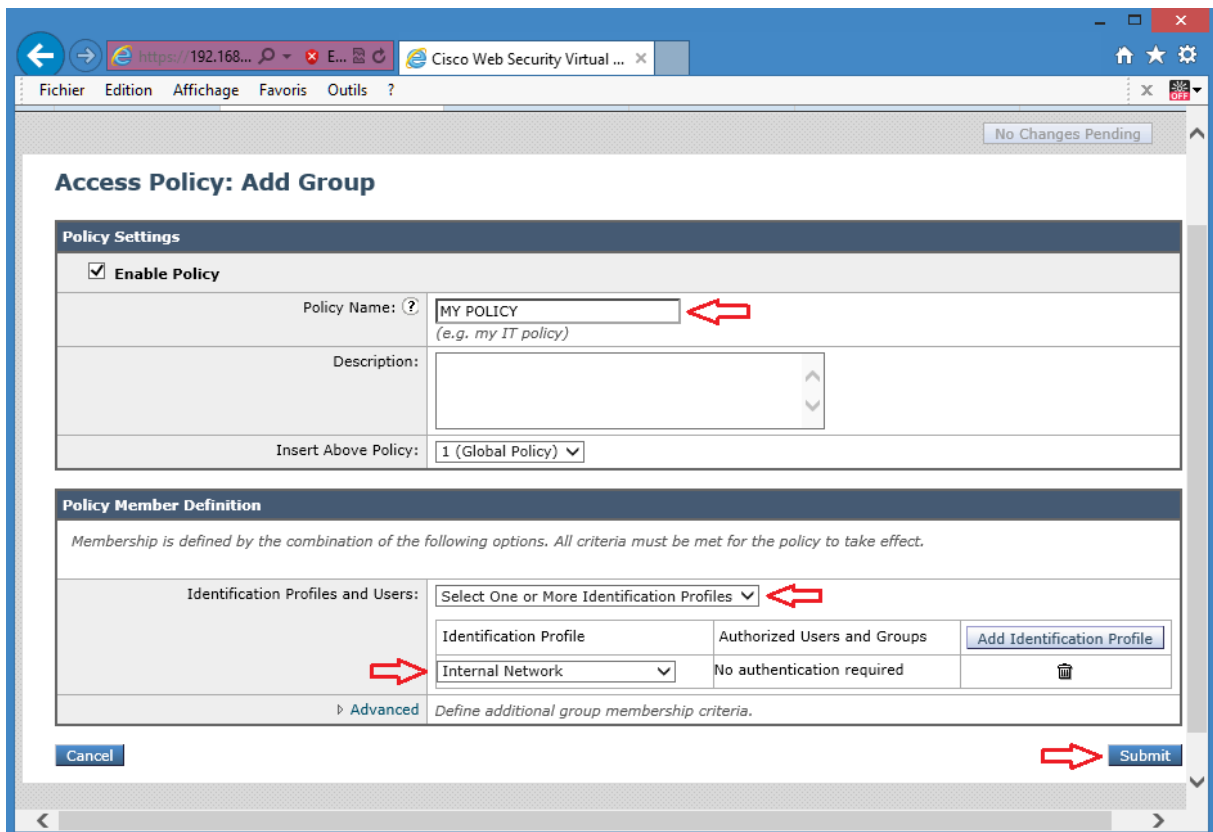
From the Cisco WSA GUI, navigate to **Web Security Manager > Access Policies**.



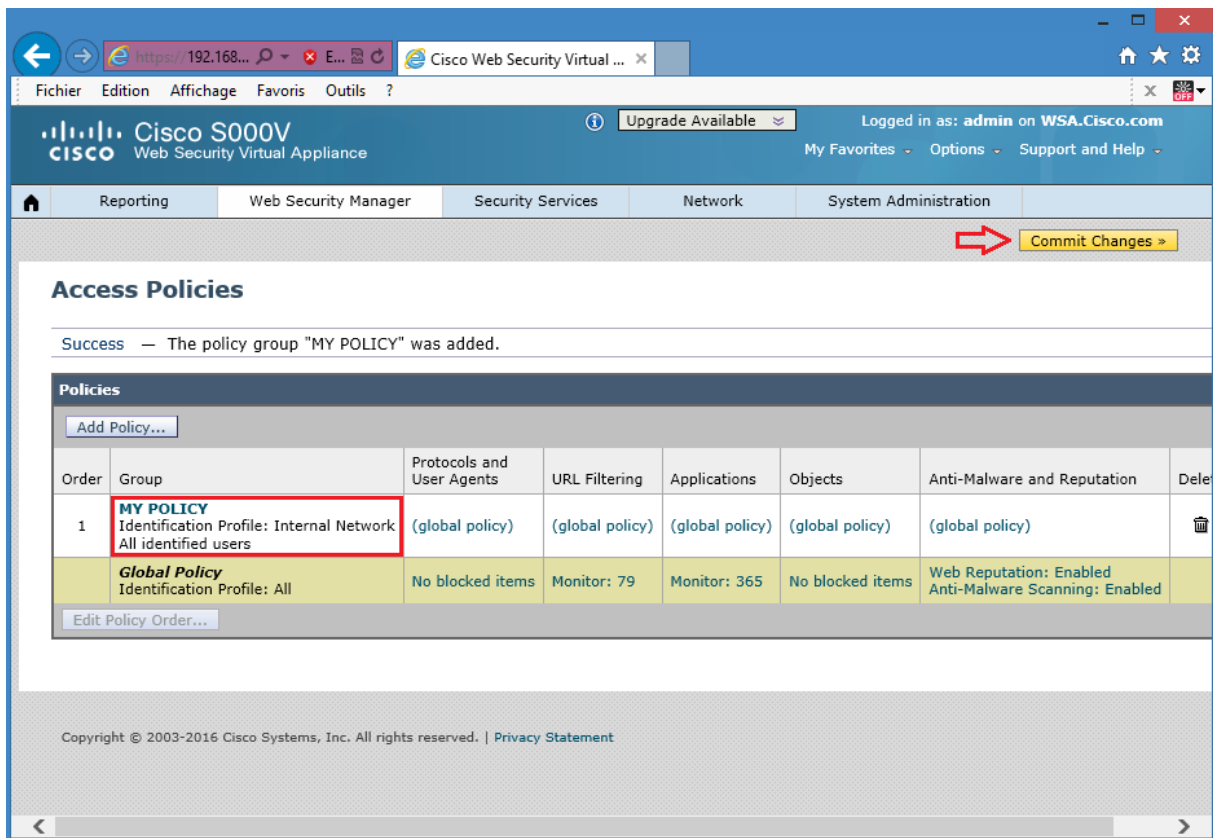
Click **Add Policy** and use these parameters:
Use the **Policy Name** of **MY POLICY** Access Policy.

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.





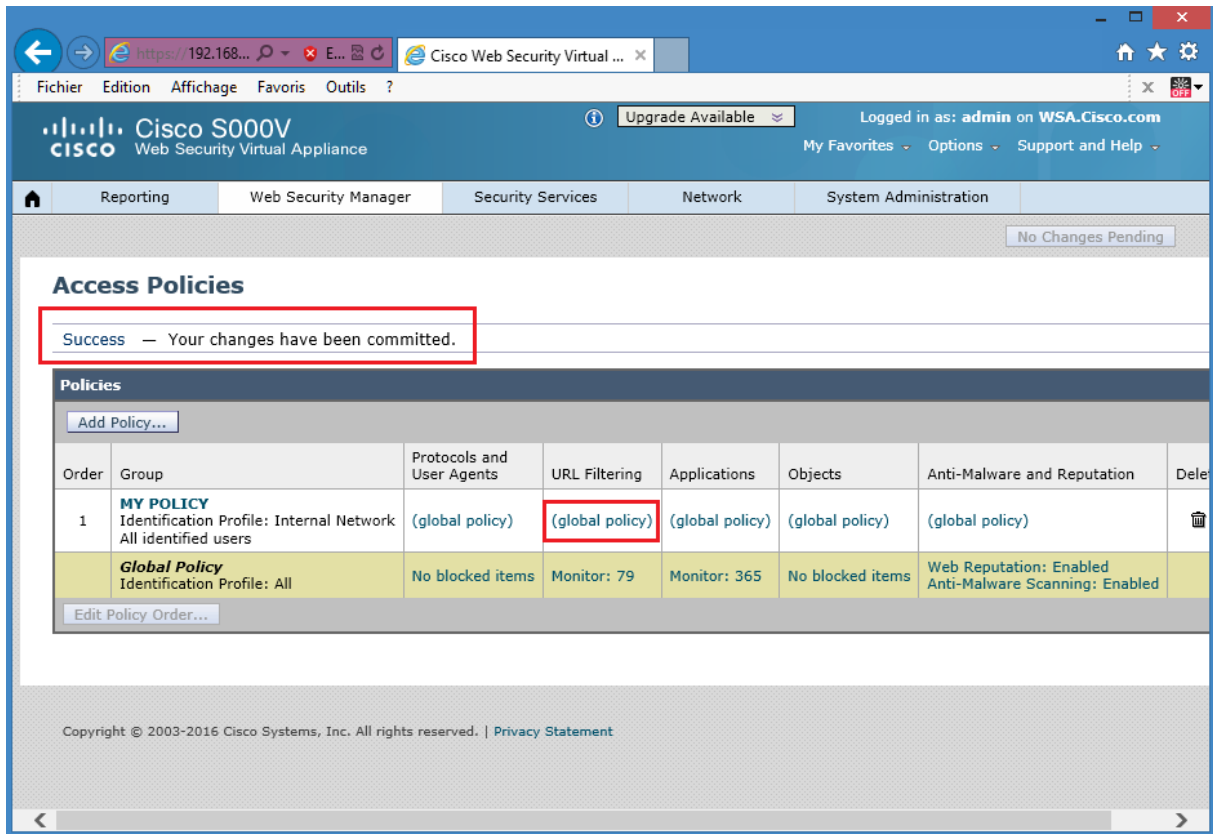
Click **Submit** then **Commit** the changes.



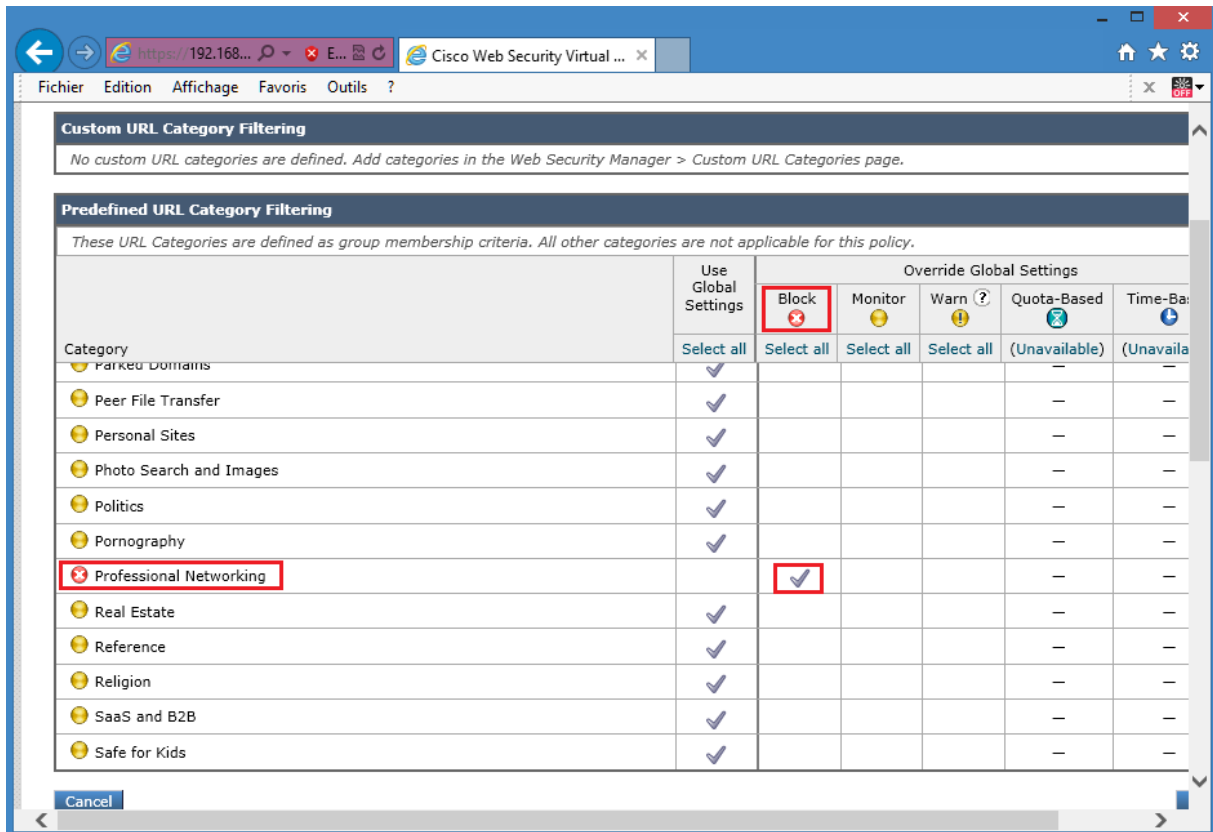
The Cisco WSA acceptable use controls include a range of filtering capabilities for downloaded web content. The two main areas of web usage controls are:

- Cisco Application Visibility.
- URL filters.

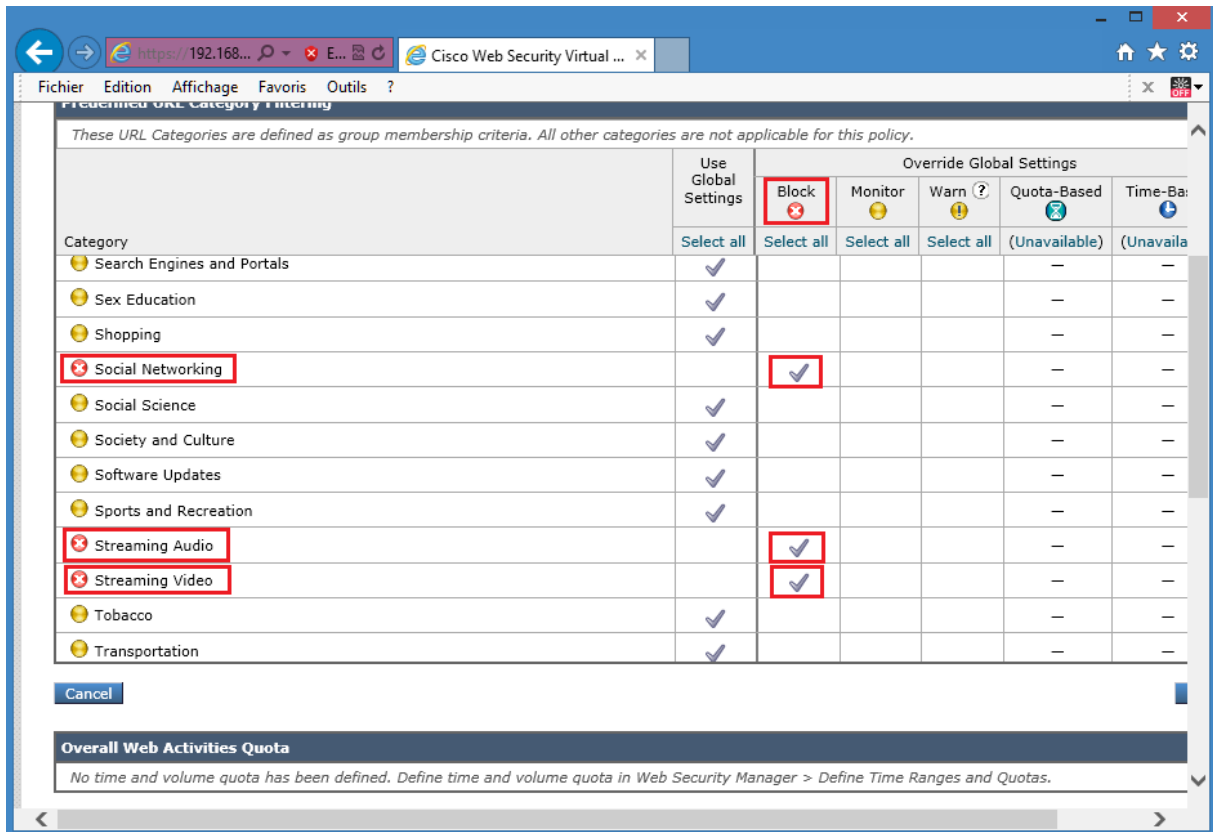
In the Cisco WSA GUI, choose **Web Security Manager > Web Policies > Access Policies**. Click the **(global)** link under **URL Filtering** for the **MY POLICY** access policy.



Block four predefined categories: Professional Networking, Social Networking, Streaming Audio and Streaming Video.
 Screen shot blocking **Professional Networking** URL category is shown below.



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



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.

Success — Settings have been saved.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	MY POLICY Identification Profile: Internal Network All identified users	(global policy)	Block: 4 Monitor: 75	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

Success — Your changes have been committed.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	MY POLICY Identification Profile: Internal Network All identified users	(global policy)	Block: 4 Monitor: 75	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 79	Monitor: 365	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

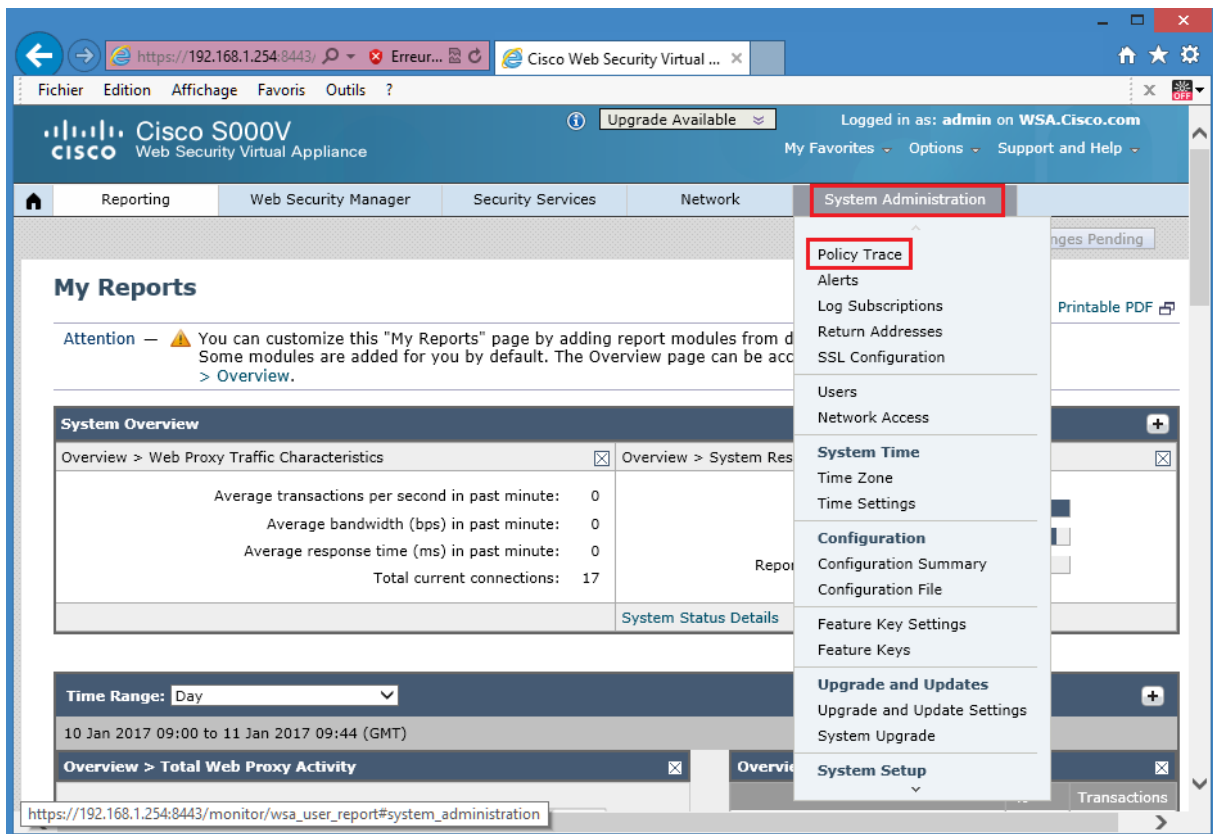
The **system Administration-Policy Trace** tool allows you to test the the configured policy.

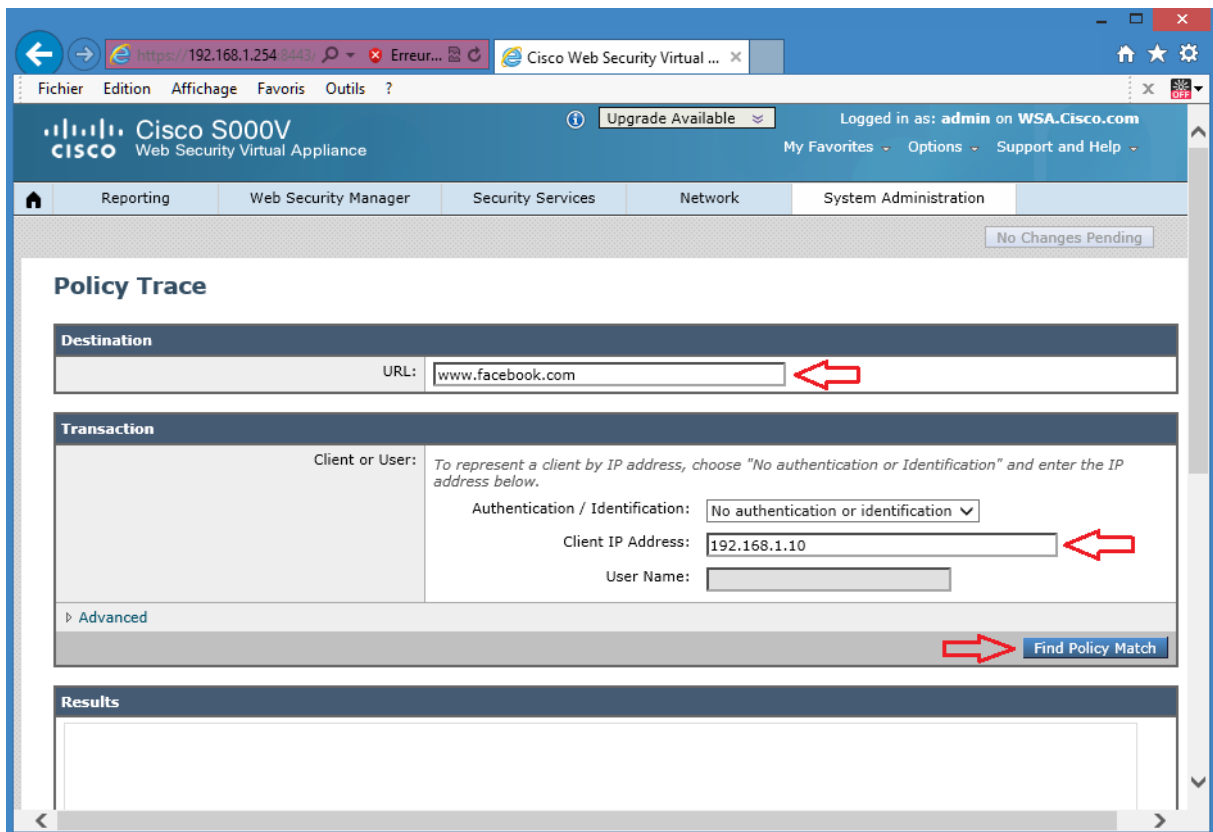
In the Cisco WSA GUI, choose **System Administration > Policy Trace**. Use these parameters:

URL: www.facebook.com

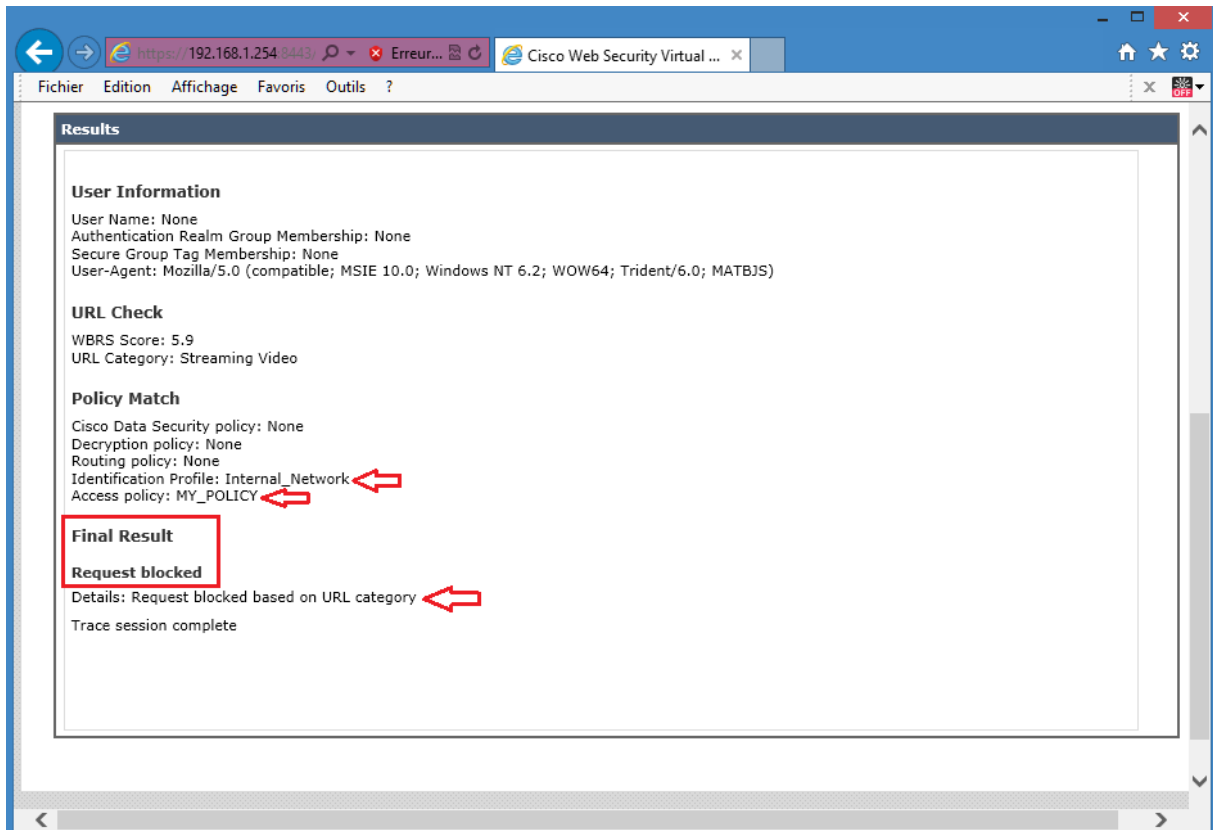
Client IP Address: 192.168.1.10

Click the **Find Policy Match** link





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.

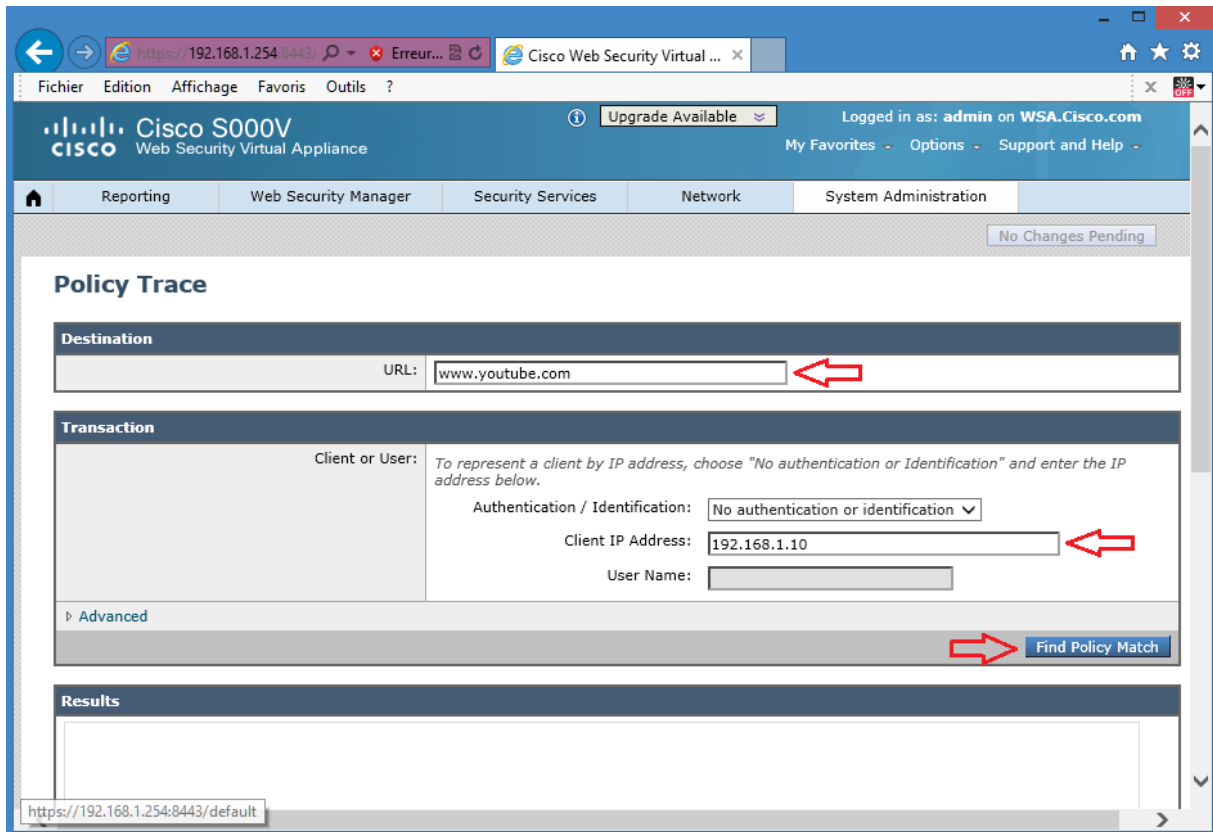


In the Cisco WSA GUI, choose **System Administration > Policy Trace**. Use these parameters:

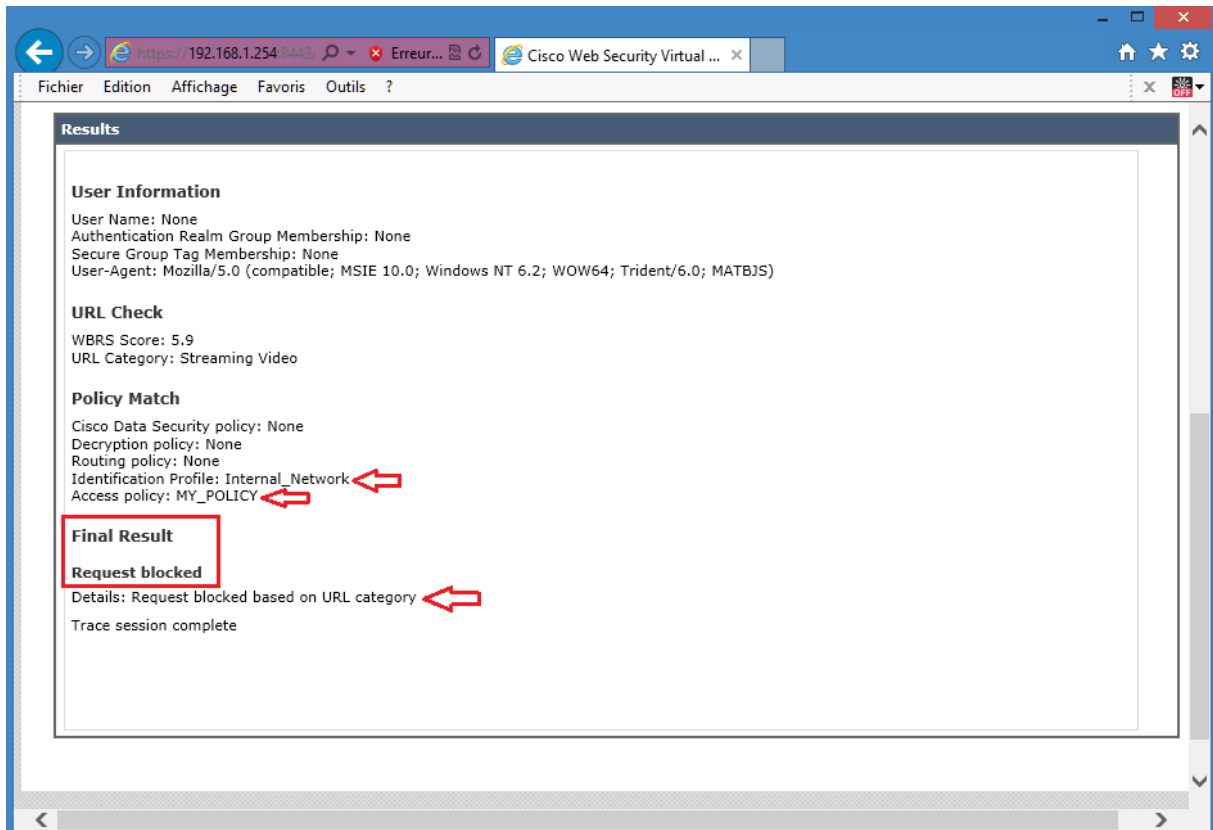
URL: www.youtube.com

Client IP Address: 192.168.1.10

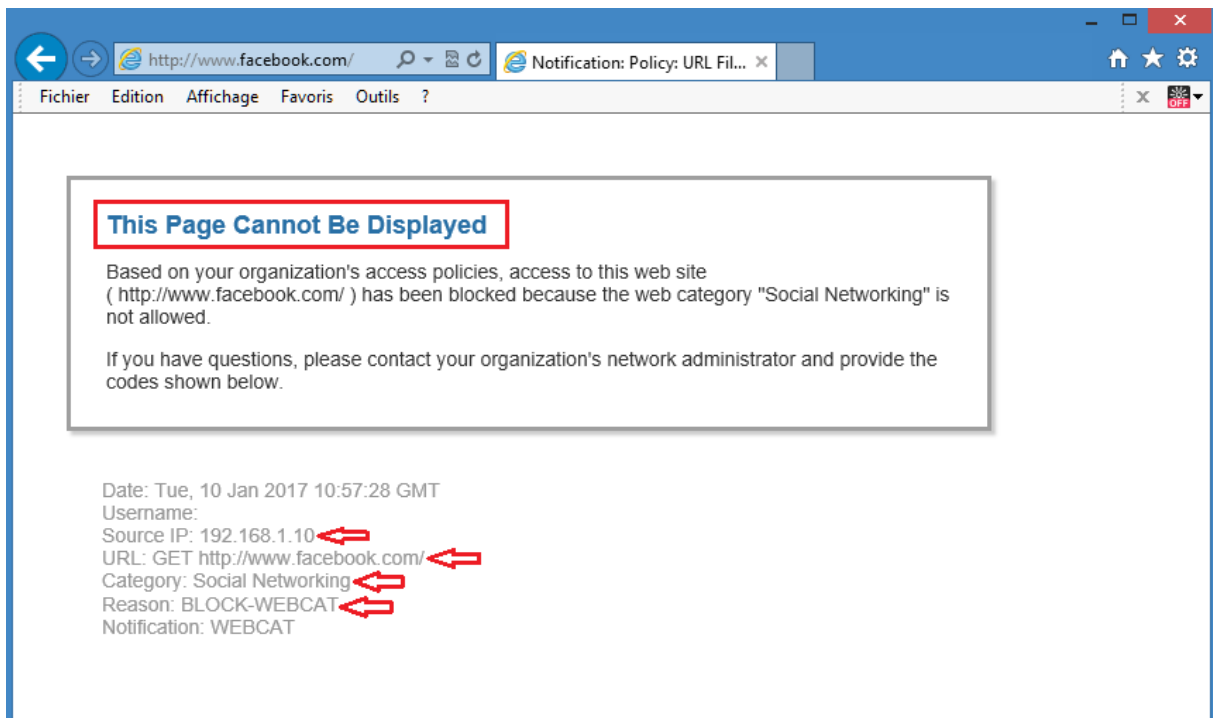
Click the **Find Policy Match** link



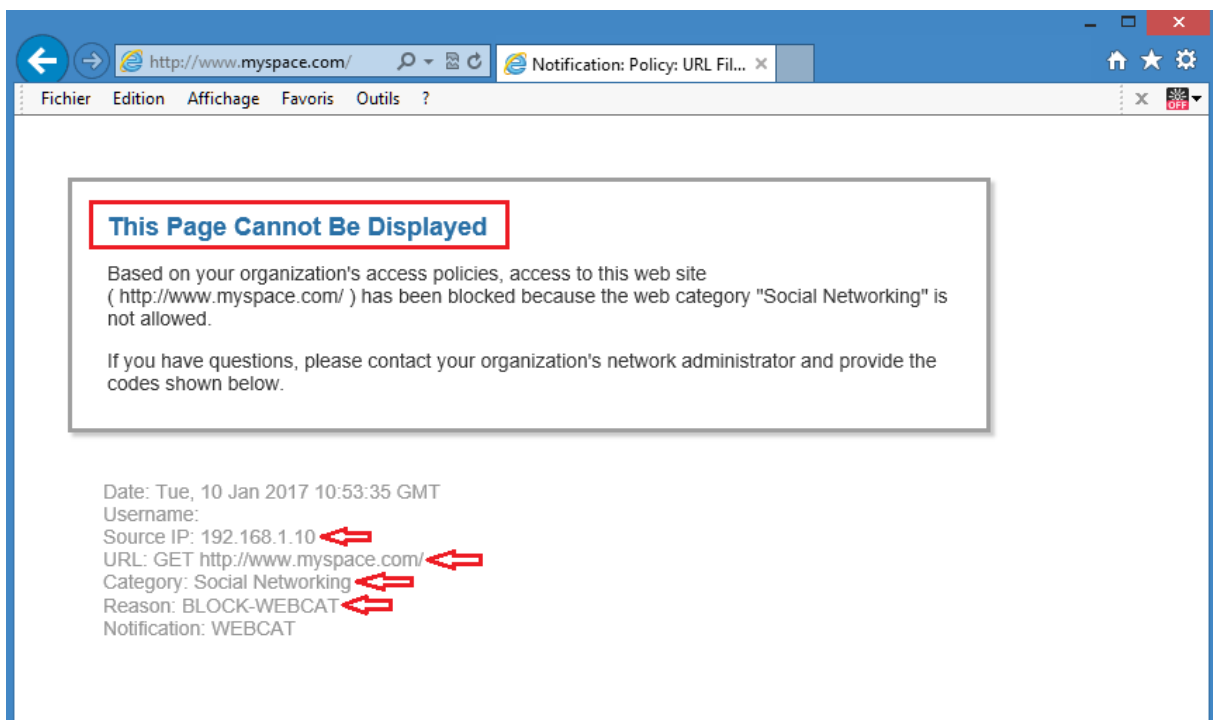
You should see that test transaction to **www.youtube.com** is matched against **Internal Network** identity and **MY POLICY** access policy. Request is blocked based on **URL category**, because **MY POLICY** access policy blocks **Streaming Video** URL category.



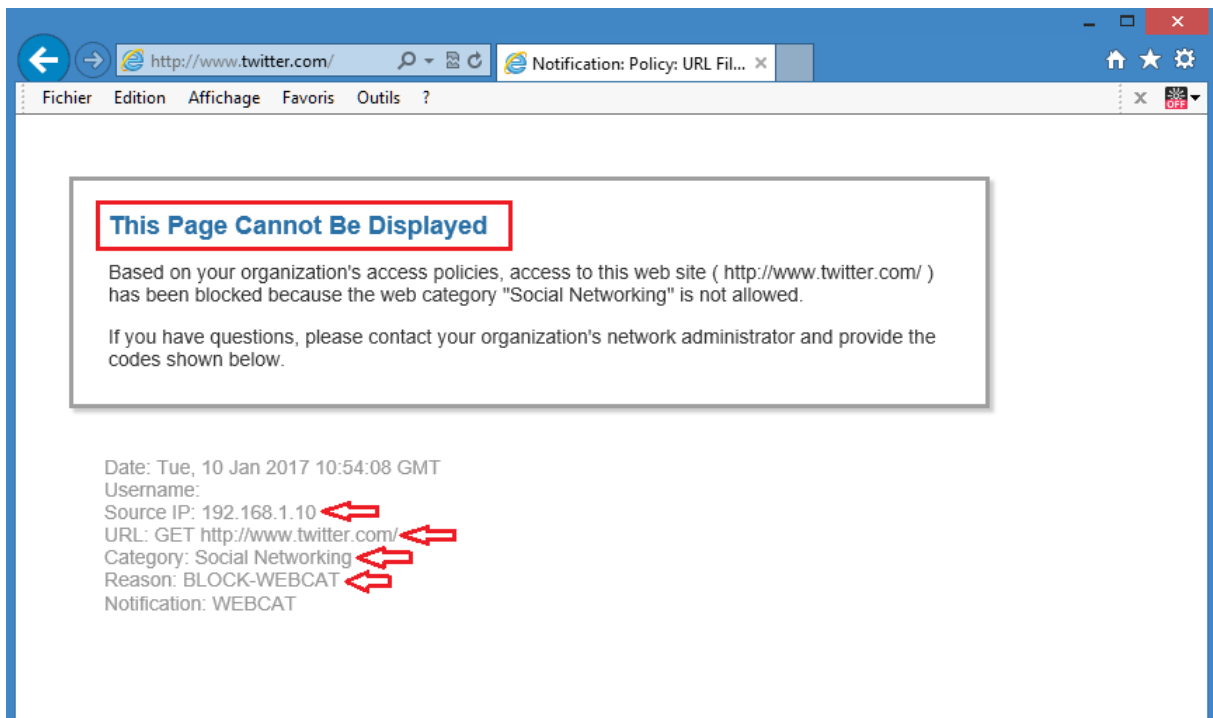
Test the URL filtering on the predefined URL categories:
From the Host PC, open a browser and connect via HTTP to **www.facebook.com**. The access should be blocked because the **Social Networking category** is blocked.



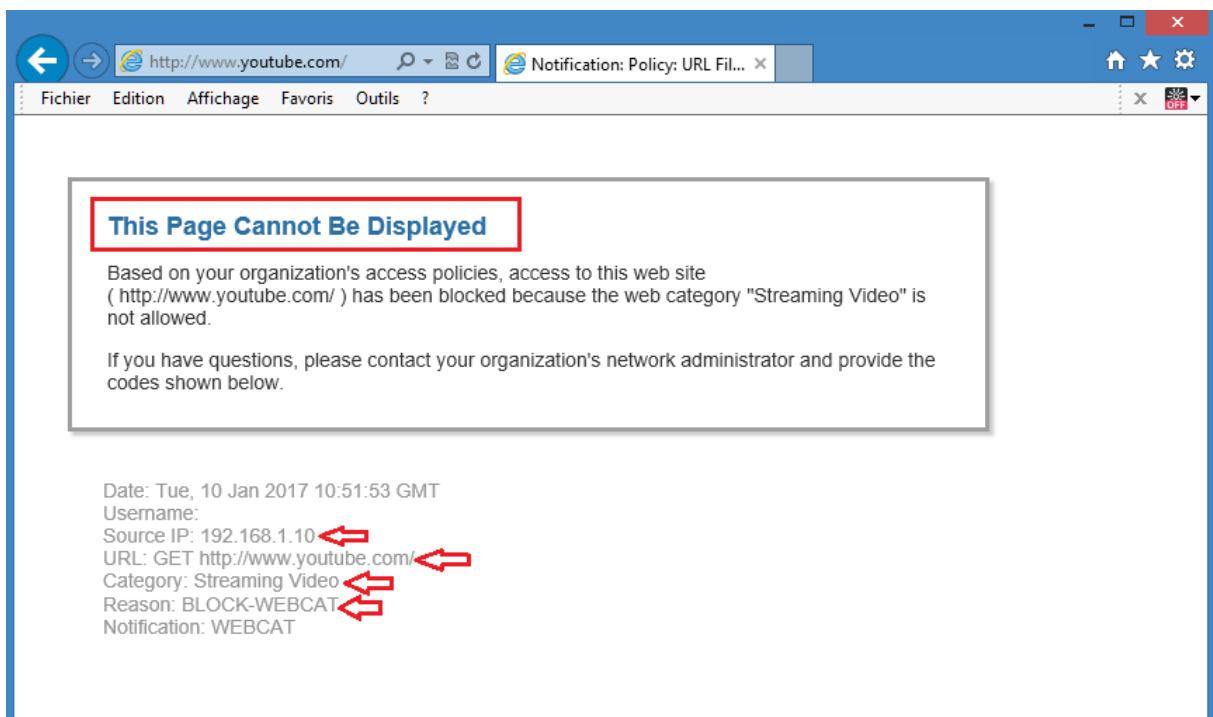
From the Host PC, open a browser and connect via HTTP to **www.myspace.com**. The access should be blocked because the **Social Networking** category is blocked.



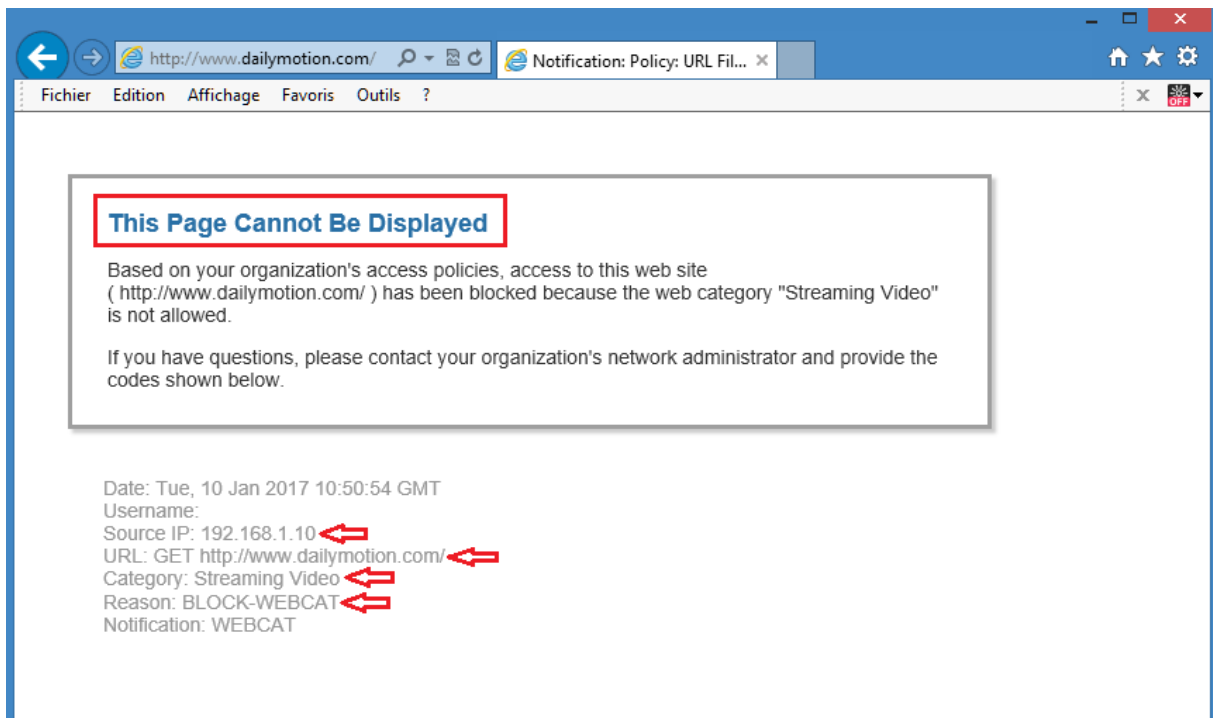
From the Host PC, open a browser and connect via HTTP to **www.twitter.com**. The access should be blocked because the **Social Networking** category is blocked.



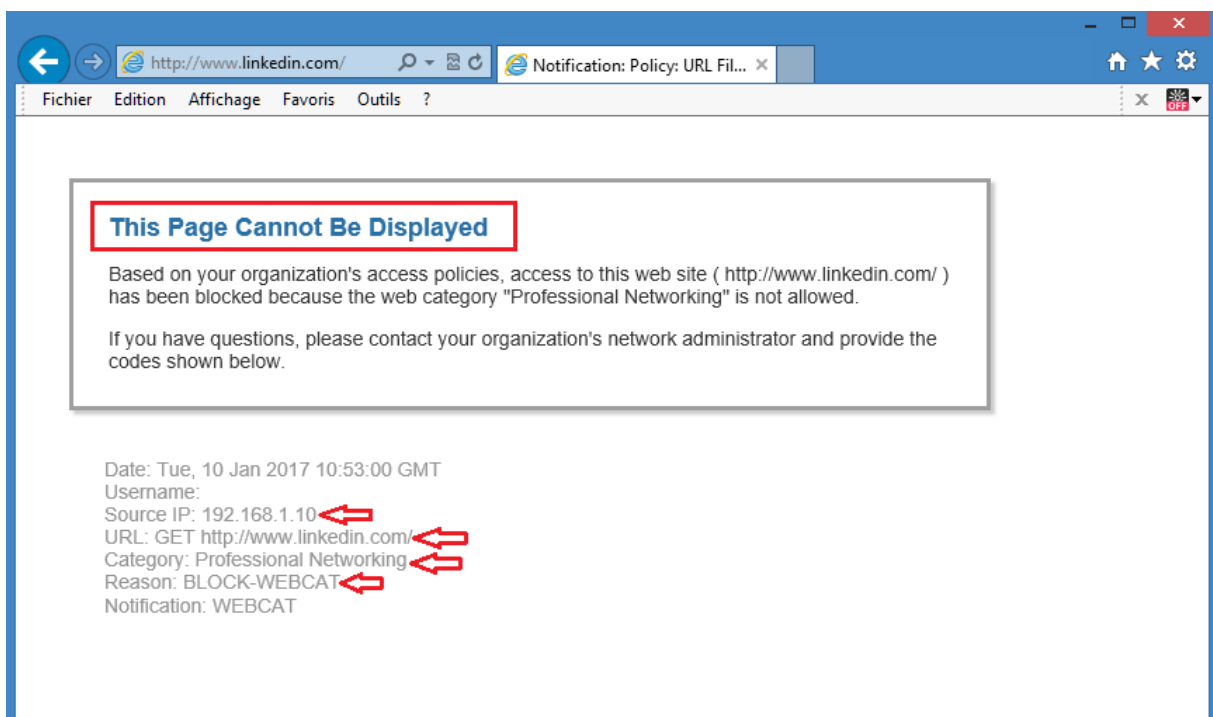
From the Host PC, open a browser and connect via HTTP to **www.youtube.com**. The access should be blocked because the **Streaming Video category** is blocked.



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.



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.

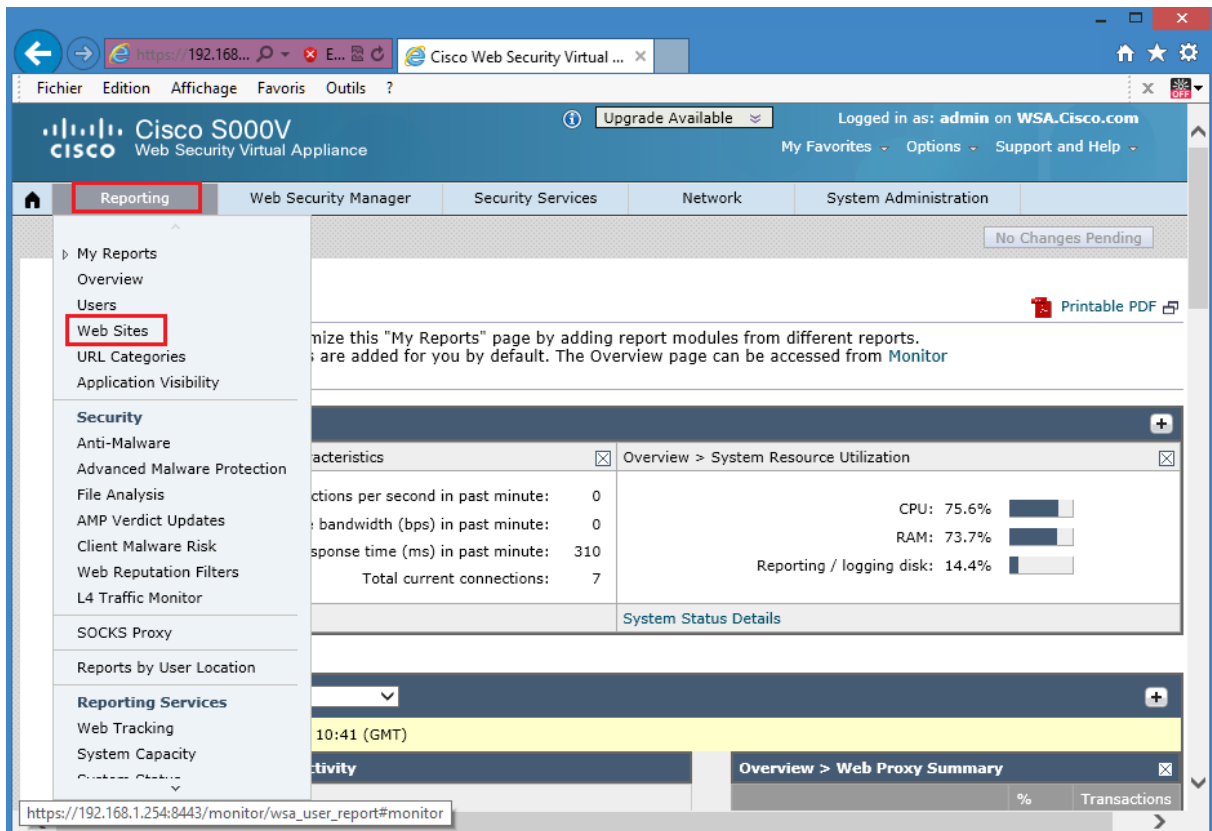


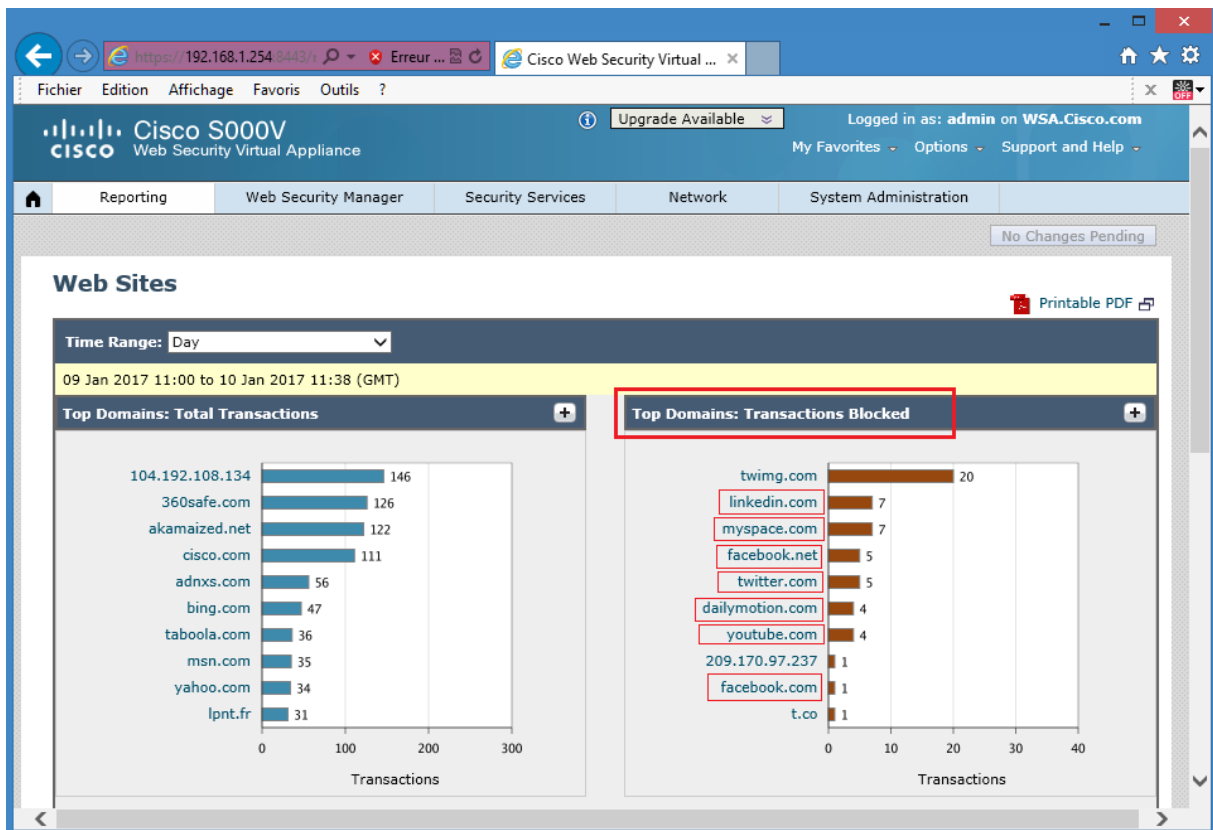
Verify blocked transactions in reports and web tracking messages:
There are two reports of interest related to URL categories:

- **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.

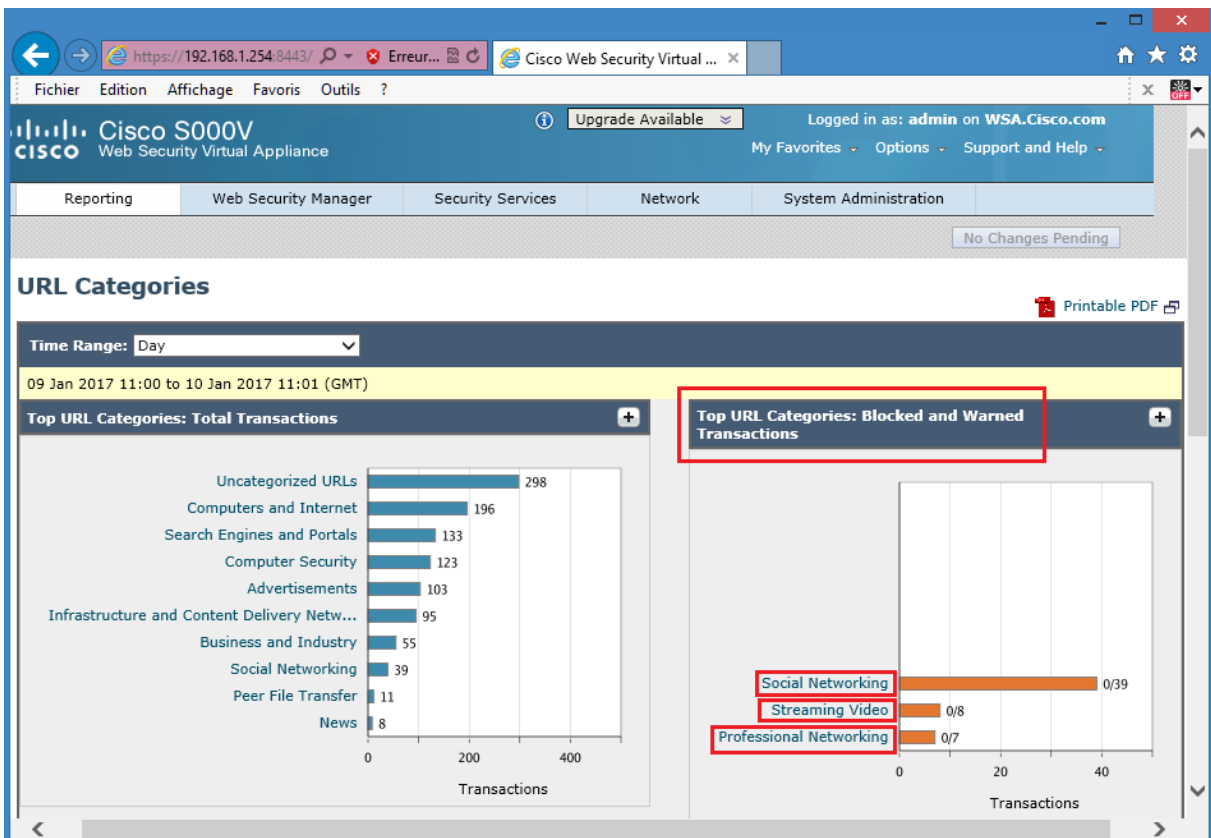
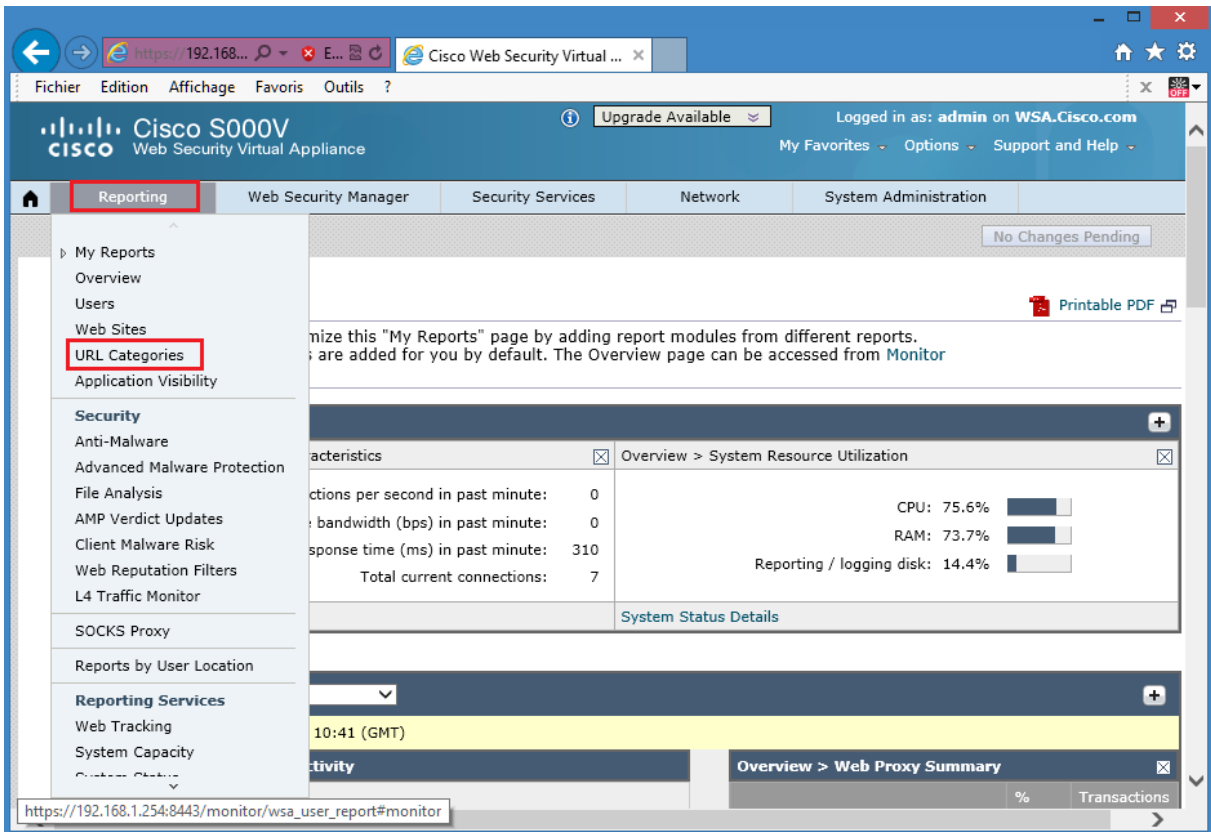
The URL category report is an example of many report types available for the web usage control functionality. These reports are printable in PDF format and can be exported in .csv format.

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.



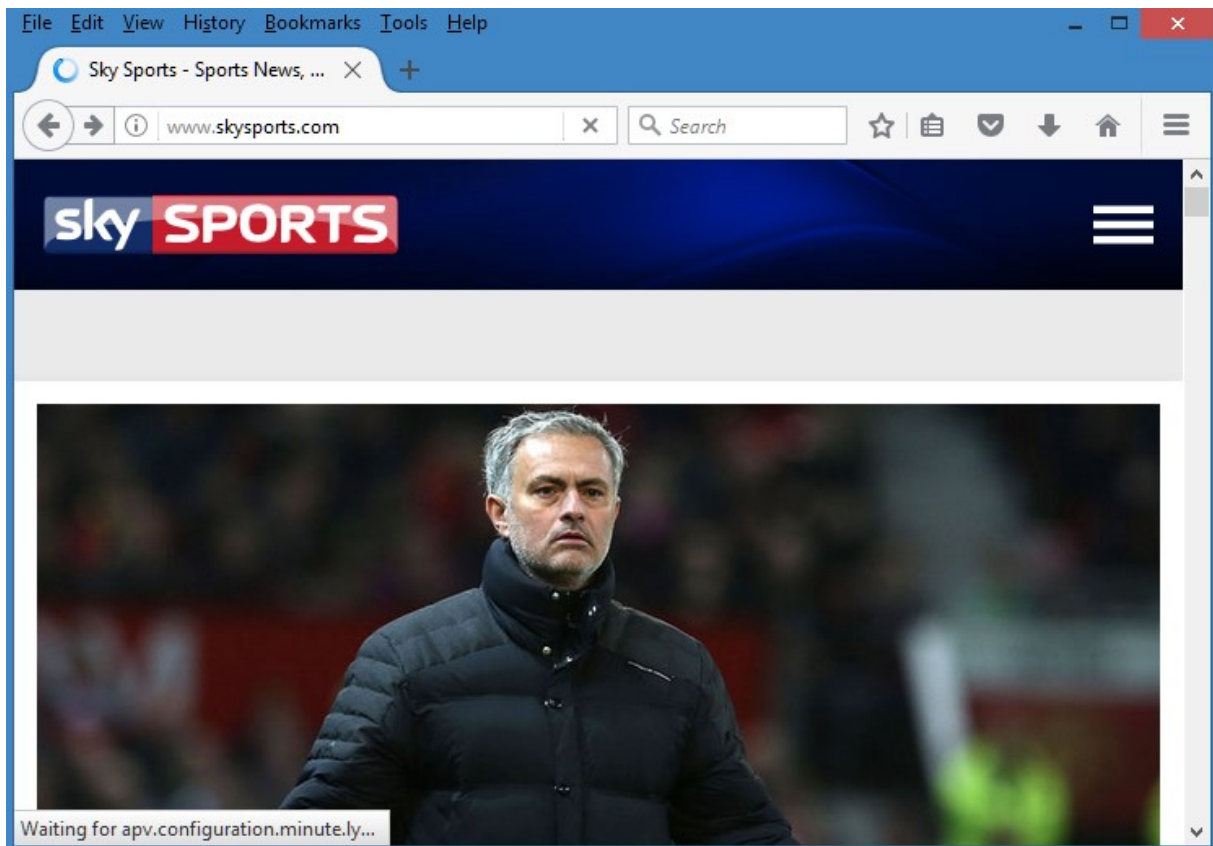


From the Cisco WSA GUI, choose **Reporting > URL Categories**. In the **Top URL Categories: Blocked and Warned Transactions** chart, you should see the blocked transaction different categories being blocked.

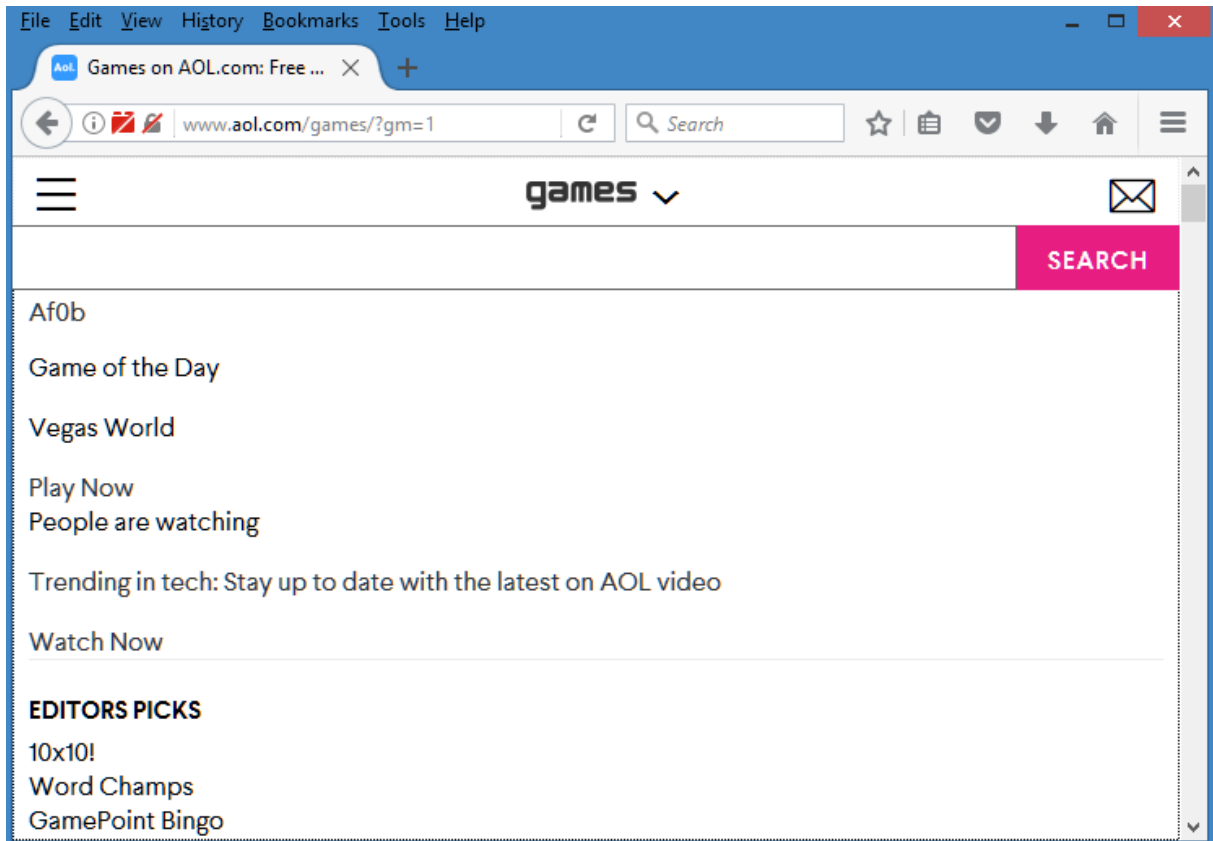


Block two additional categories: **Games, Sport and Recreation**.

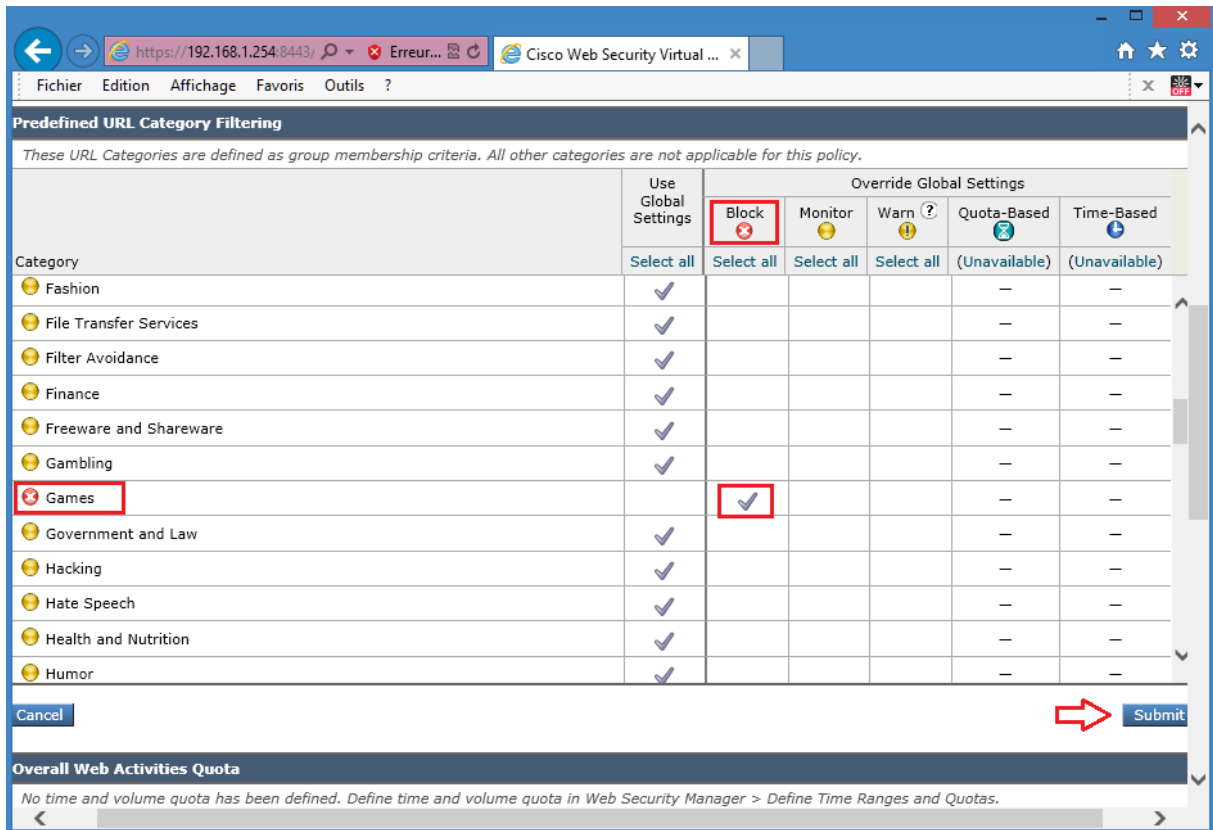
From the Host PC, open a browser and connect via HTTP to **www.skysports.com**. The access should be successful.



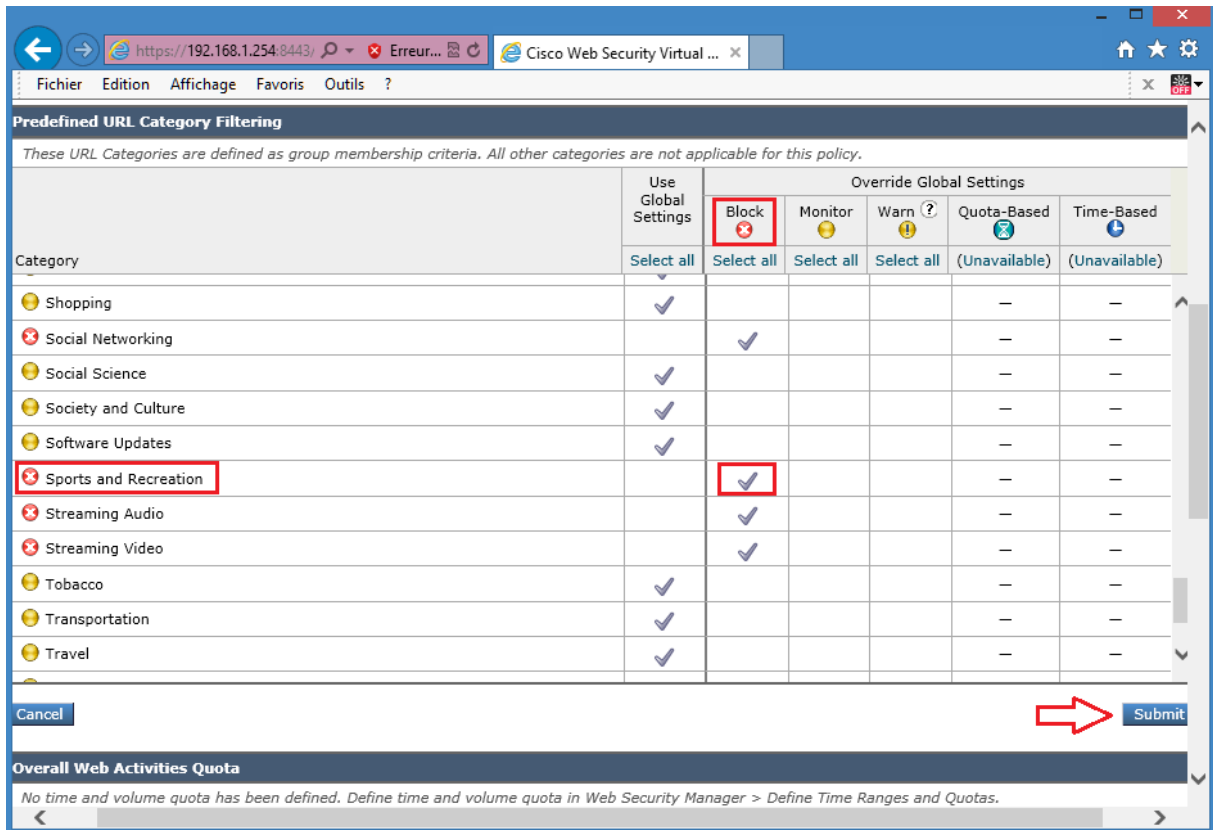
From the Host PC, open a browser and connect via HTTP to **www.aol.com**. Click in the Games link then in the Play Now link. The access should be successful.



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.

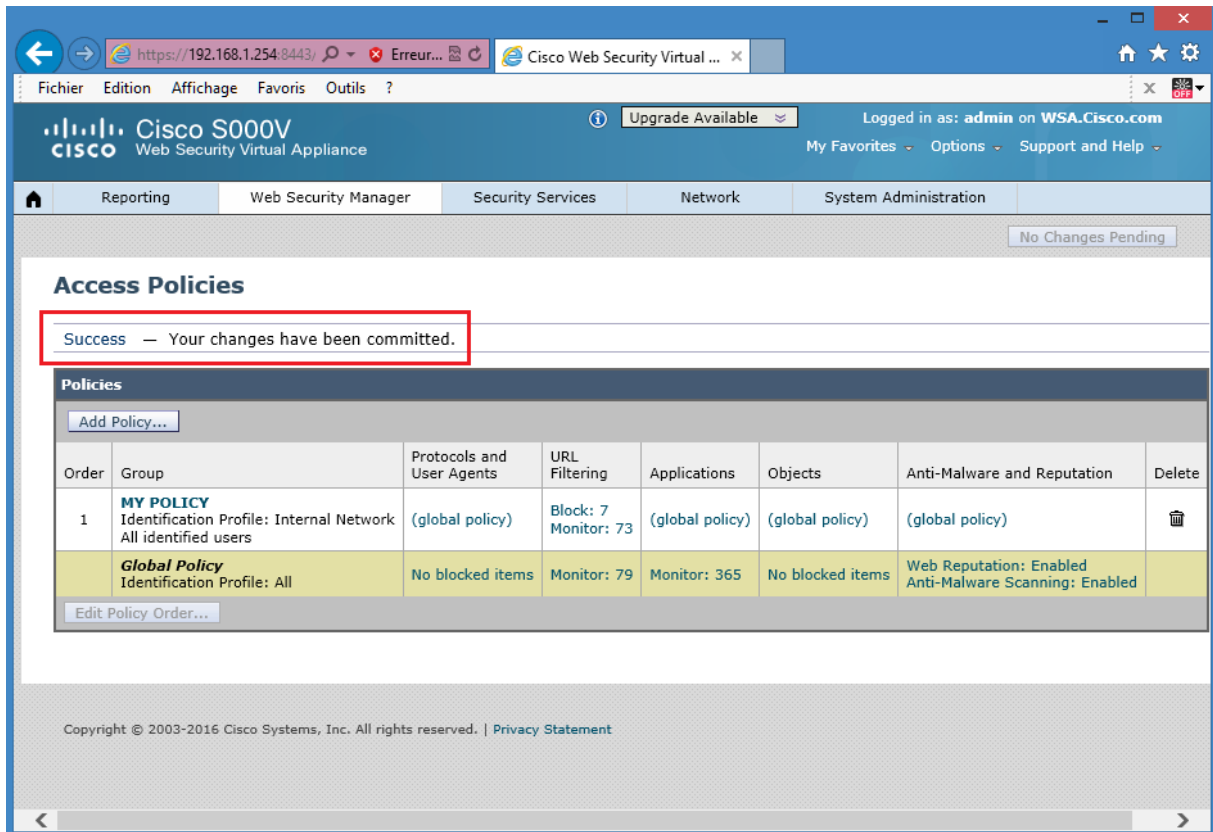


Partial screen shot blocking **Sport and Recreation** category. URL category is shown below.

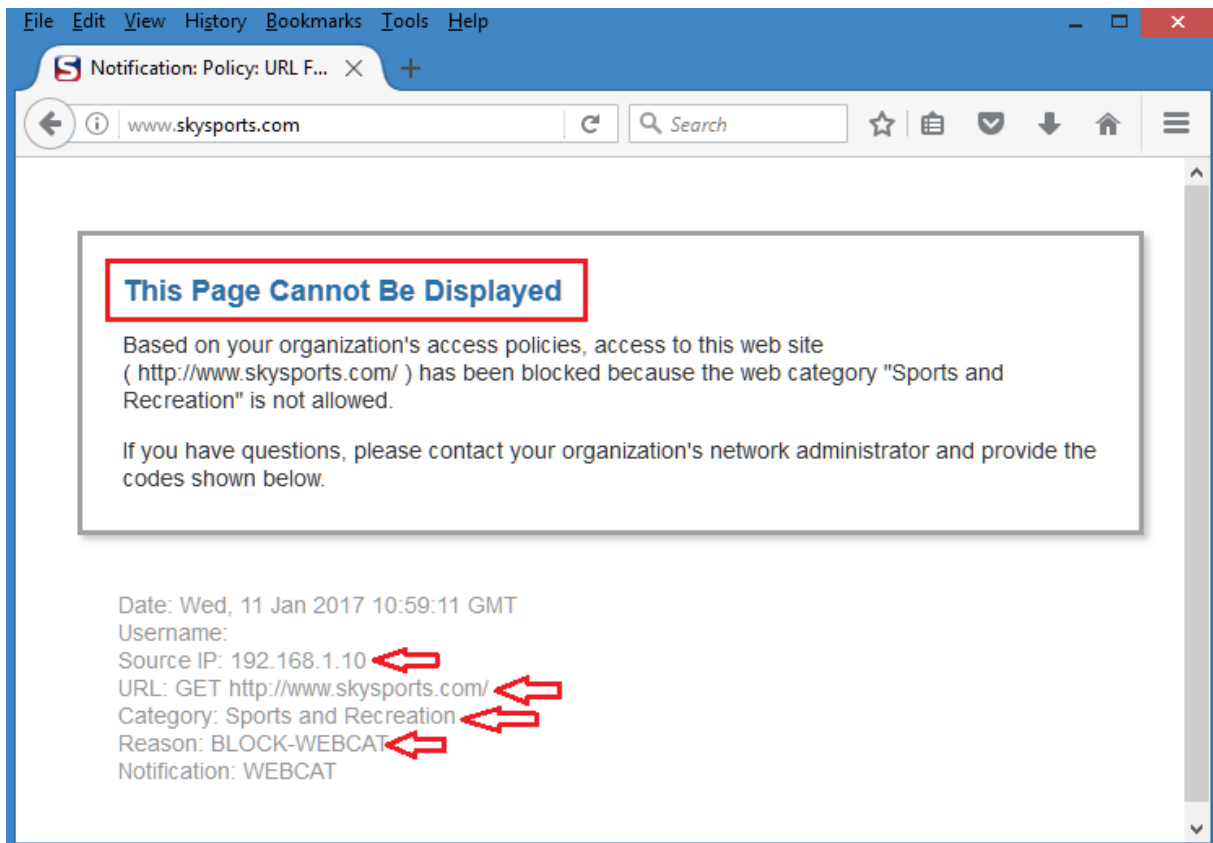


Click Submit then **Commit** the changes.

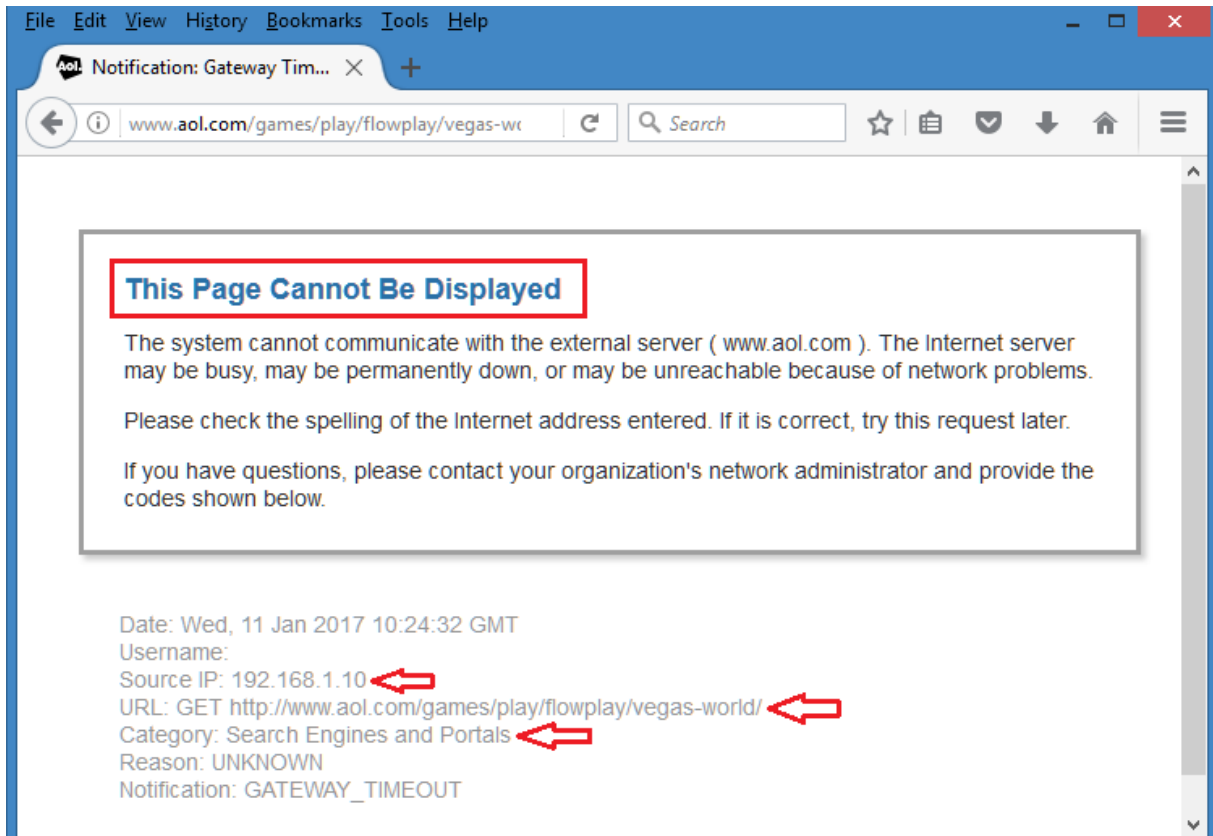
Navigate to **Web Security Manager > Access Policies** to verify changed settings for **URL filtering** of **MYPOLICY** access policy.



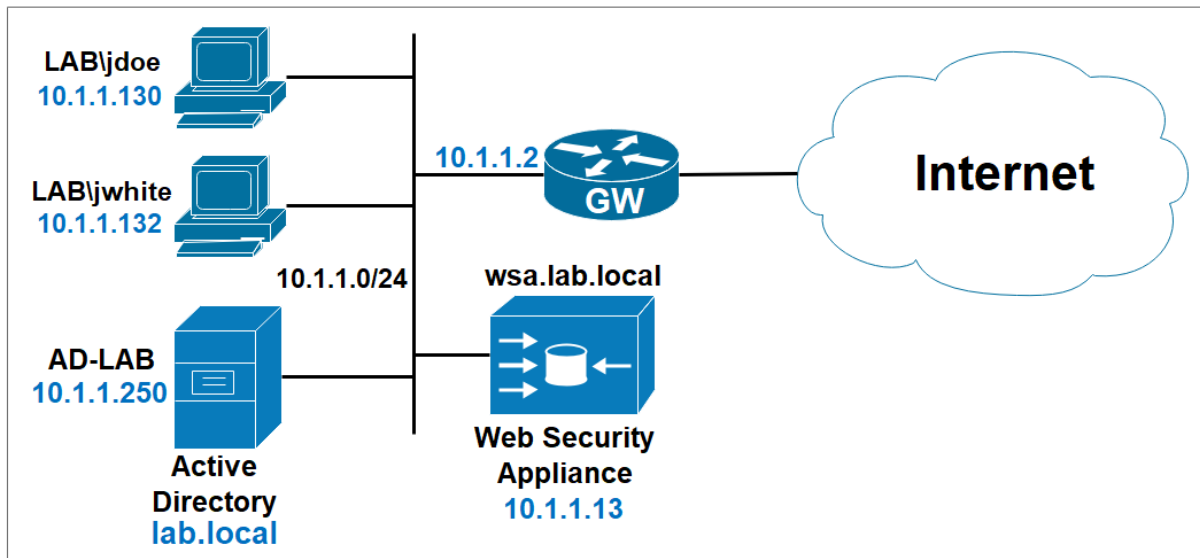
From the Host PC, open a browser and connect via HTTP to **www.skysports.com**. The access should be blocked because the **Sport and Recreation** category is blocked.



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.

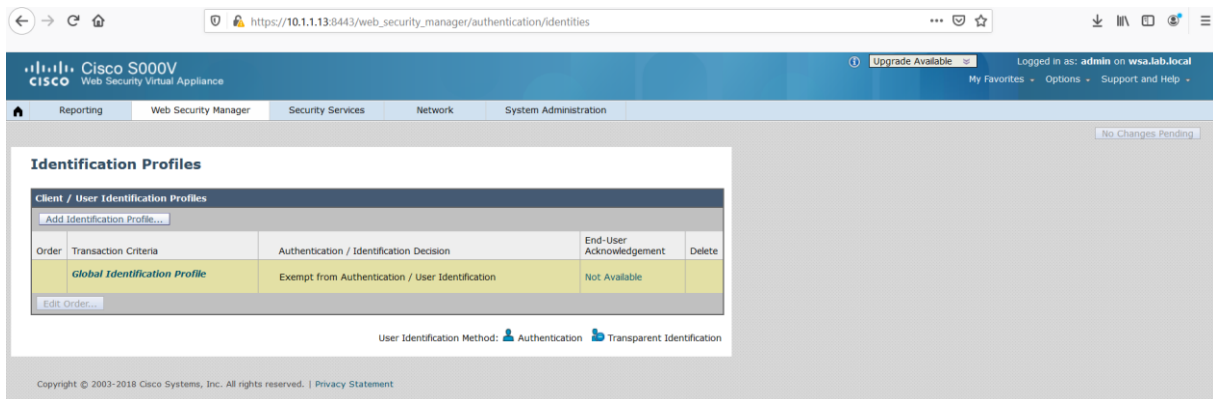


Lab 6: Identification Profile and Access Policies



Create a new identification profile based on the AD Realm

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



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.

The screenshot shows the 'Identification Profiles: Add Profile' configuration page. The 'Client / User Identification Profile Settings' section has the 'Enable Identification Profile' checkbox checked. The 'Name' field contains 'Lab Profile' and the 'Description' field is empty. The 'Insert Above' dropdown is set to '1 (Global Profile)'. The 'User Identification Method' section has 'Authenticate Users' selected for 'Identification and Authentication'. Under 'Authentication Realm', 'Select a Realm or Sequence' is 'AD1' and 'Select a Scheme' is 'Use Basic'. The 'If a user fails authentication' checkbox 'Support Guest privileges' is unchecked. Under 'Authentication Surrogates', 'No Surrogate' is selected. A 'Submit' button is visible at the bottom right.

This screenshot shows the 'Membership Definition' section of the configuration page. The 'Define Members by Subnet' field contains '10.1.1.0/24'. Below it, examples of subnets are listed: '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'. Under 'Define Members by Protocol', the 'HTTP/HTTPS' checkbox is checked, and the 'Native FTP' checkbox is unchecked. A 'Submit' button is located at the bottom right.

Identification Profiles

Warning — The policy group "Lab Profile" was added.
Groups that do not require authentication should typically be ordered above authentication-based groups in the policy table for effective evaluation. Changing this order may require users to authenticate, regardless of policy group settings.

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	Lab Profile Subnets: 10.1.1.0/24 Protocols: HTTP/HTTPS	Authenticate: Realm: AD1 (Scheme: Basic)	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

User Identification Method: Authentication Transparent Identification

Identification Profiles

Success — Your changes have been committed.

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	Lab Profile Subnets: 10.1.1.0/24 Protocols: HTTP/HTTPS	Authenticate: Realm: AD1 (Scheme: Basic)	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

User Identification Method: Authentication Transparent Identification

Configure two access policies for two AD groups.

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

Access Policies

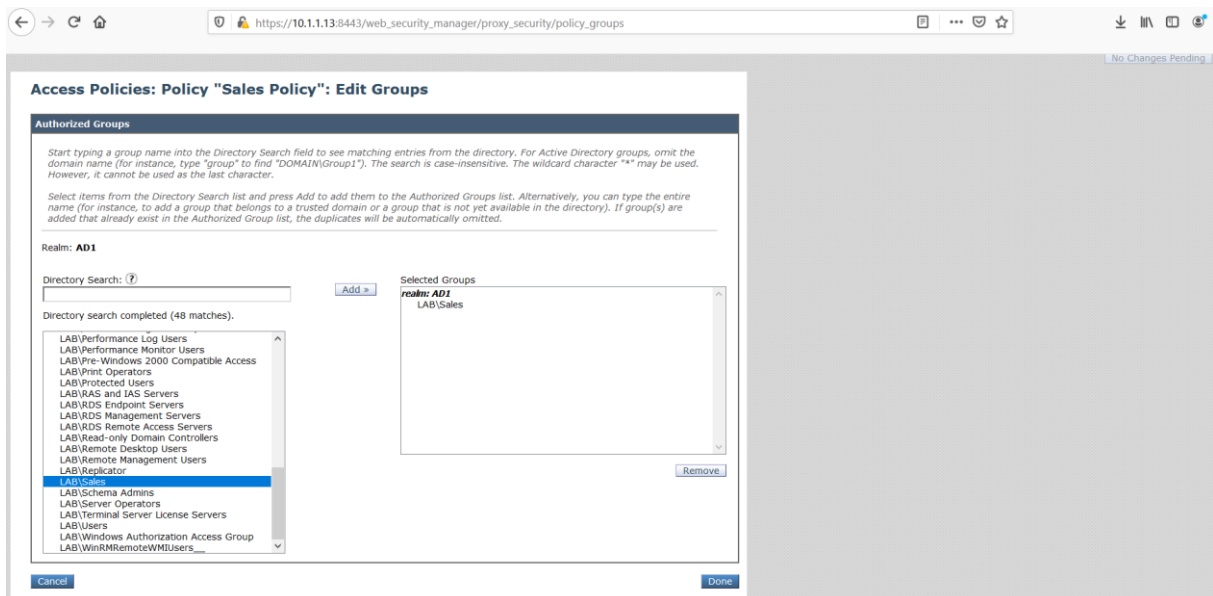
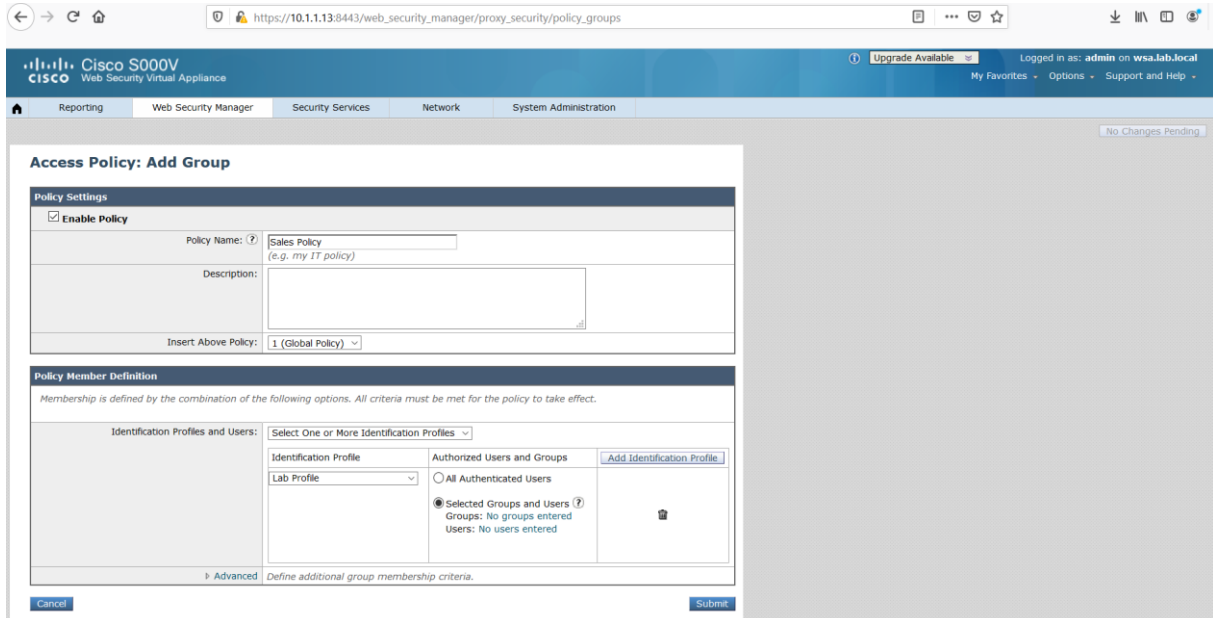
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
	Global Policy	No blocked items	Monitor: 87	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

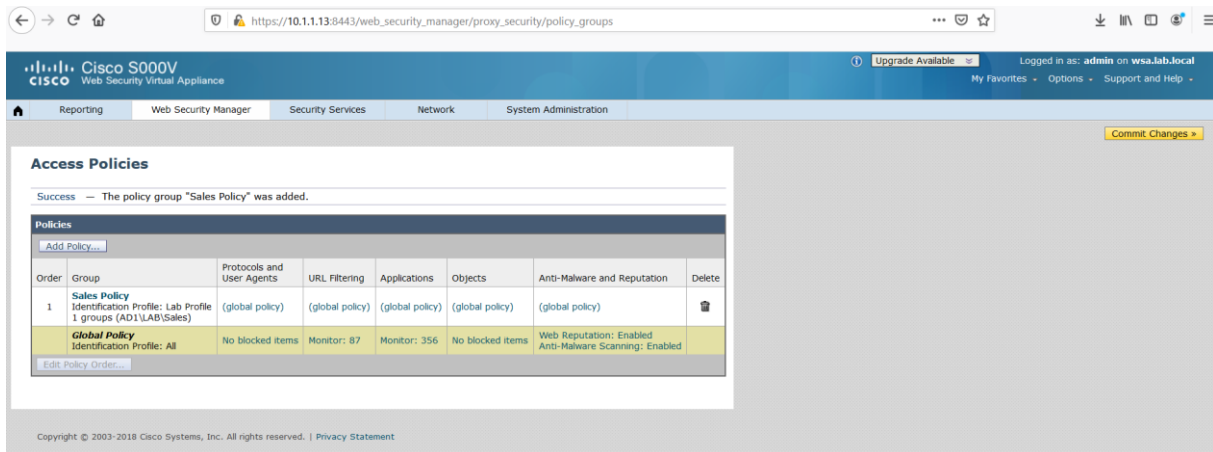
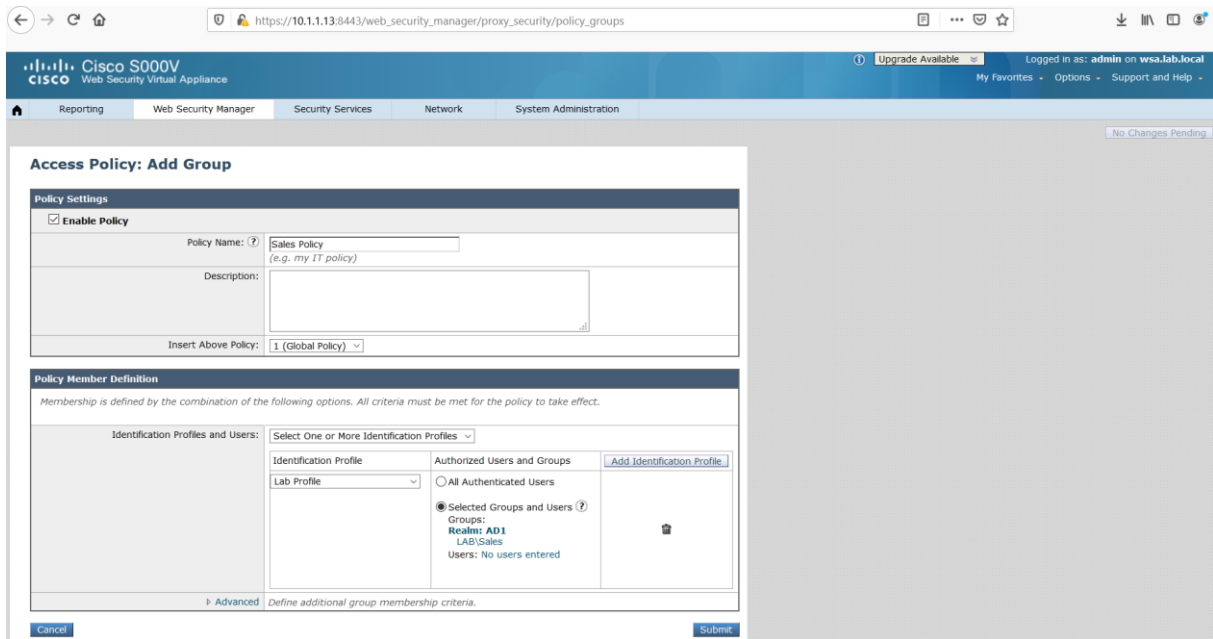
In the **Policy Name**, enter the name **Sales Policy**.

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**.





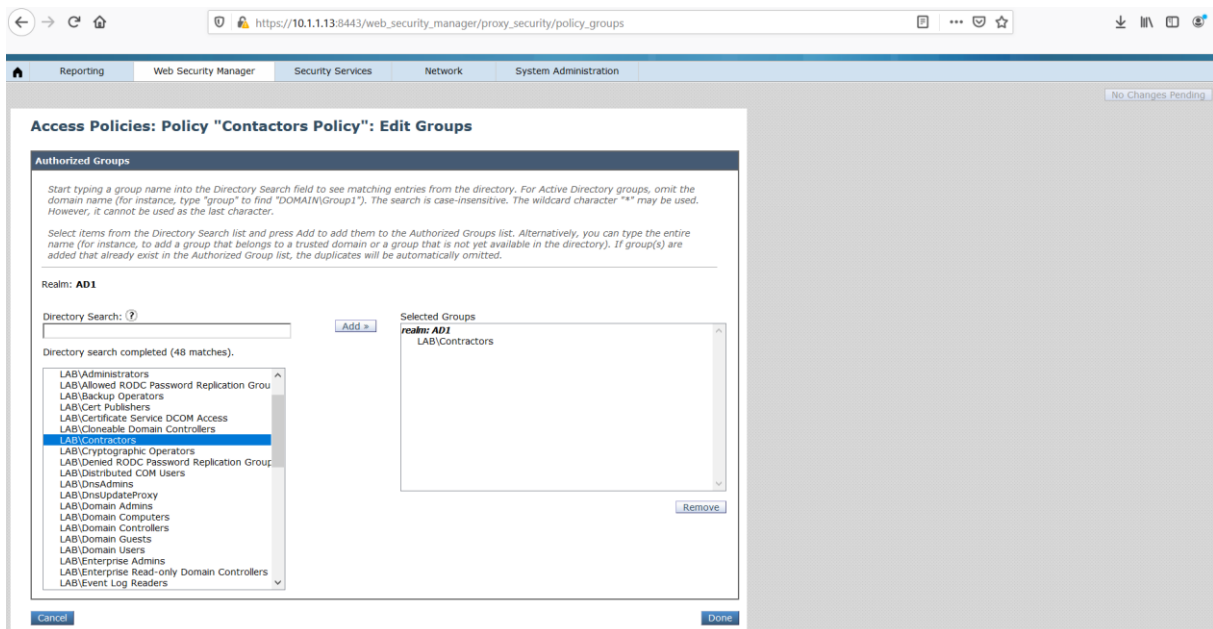
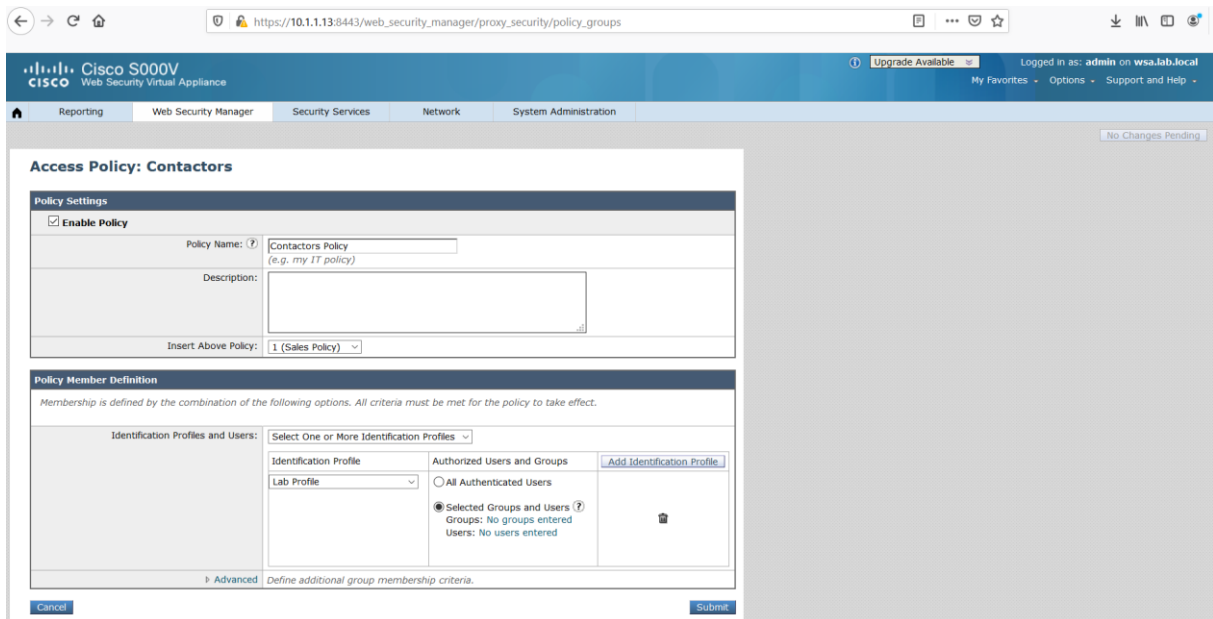
Click **Add Policy**.

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**.



Click **Submit** and commit the configuration.

← → ↻ 🏠 https://10.1.1.13:8443/web_security_manager/proxy_security/policy_groups Upgrade Available Logged in as: admin on wsa.lab.local

Reporting Web Security Manager Security Services Network System Administration

Access Policy: Contactors

Policy Settings

Enable Policy

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile:

Authorized Users and Groups: All Authenticated Users Selected Groups and Users

Groups: **Realm: AD1**
LAB/Contractors
Users: No users entered

← → ↻ 🏠 https://10.1.1.13:8443/web_security_manager/proxy_security/policy_groups Upgrade Available Logged in as: admin on wsa.lab.local

Reporting Web Security Manager Security Services Network System Administration

Access Policies

Success — Settings have been saved.

Policies

Order	Group	Protocols and User Agents	URL Filtering	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)	<input type="button" value="Delete"/>
2	Sales Policy Identification Profile: Lab Profile 1 groups (AD1\LAB/Sales)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	<input type="button" value="Delete"/>
	Global Policy Identification Profile: All	No blocked items	Monitor: 87	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | Privacy Statement

← → ↻ 🏠 https://10.1.1.13:8443/commit?referrer=https://10.1.1.13:8443/web_security_manager/proxy_security/policy_groups Upgrade Available Logged in as: admin on wsa.lab.local

Reporting Web Security Manager Security Services Network System Administration

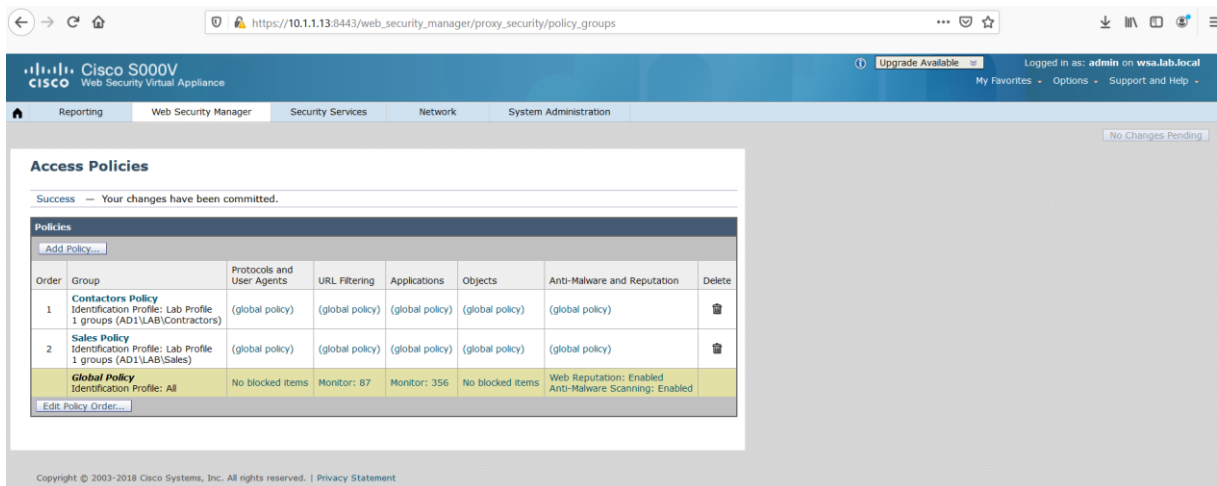
Uncommitted Changes

Commit Changes

You have uncommitted changes. These changes will not go into effect until you commit them.

Comment (optional):

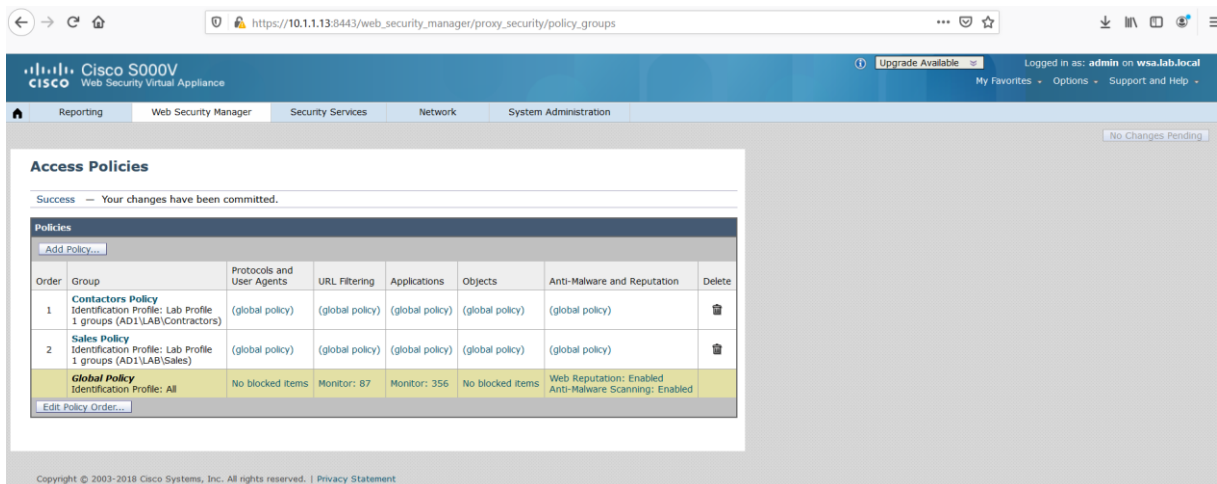
Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | Privacy Statement



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**.



Access Policies: URL Filtering: Contactors Policy

Custom and External URL Category Filtering

No custom and external URL categories are defined. Add categories in the Web Security Manager > Custom and External URL Categories page.

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Science and Technology	<input checked="" type="checkbox"/>					
Search Engines and Portals	<input checked="" type="checkbox"/>					
Sex Education	<input checked="" type="checkbox"/>					
Shopping	<input checked="" type="checkbox"/>					
Social Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Social Science	<input checked="" type="checkbox"/>					
Society and Culture	<input checked="" type="checkbox"/>					
Software Updates	<input checked="" type="checkbox"/>					
Sports and Recreation	<input checked="" type="checkbox"/>					
Streaming Audio	<input checked="" type="checkbox"/>					
Streaming Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Tobacco	<input checked="" type="checkbox"/>					
Transportation	<input checked="" type="checkbox"/>					
Travel	<input checked="" type="checkbox"/>					

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

Click **Submit** and commit the configuration.

Access Policies

Success — Settings have been saved.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Contactors Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Contractors)	(global policy)	Block: 1 Monitor: 85	(global policy)	(global policy)	(global policy)	
2	Sales Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Sales)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 87	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Access Policies: URL Filtering: Sales Policy

Custom and External URL Category Filtering

No custom and external URL categories are defined. Add categories in the Web Security Manager > Custom and External URL Categories page.

Predefined URL Category Filtering

Category	Use Global Settings	Override Global Settings				
		Block	Monitor	Warn (?)	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
SaaS and B2B	<input checked="" type="checkbox"/>					
Safe for Kids	<input checked="" type="checkbox"/>					
Science and Technology	<input checked="" type="checkbox"/>					
Search Engines and Portals	<input checked="" type="checkbox"/>					
Sex Education	<input checked="" type="checkbox"/>					
Shopping	<input checked="" type="checkbox"/>					
Social Networking	<input checked="" type="checkbox"/>					
Social Science	<input checked="" type="checkbox"/>					
Society and Culture	<input checked="" type="checkbox"/>					
Software Updates	<input checked="" type="checkbox"/>					
Sports and Recreation	<input checked="" type="checkbox"/>					
Streaming Audio	<input checked="" type="checkbox"/>					
Streaming Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Tobacco	<input checked="" type="checkbox"/>					
Transportation	<input checked="" type="checkbox"/>					
Travel	<input checked="" type="checkbox"/>					
Weapons	<input checked="" type="checkbox"/>					
Web Hosting	<input checked="" type="checkbox"/>					

Success — Settings have been saved.

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Contactors Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Contractors)	(global policy)	Block: 1 Monitor: 85	(global policy)	(global policy)	(global policy)	
2	Sales Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Sales)	(global policy)	Block: 1 Monitor: 85	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 87	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

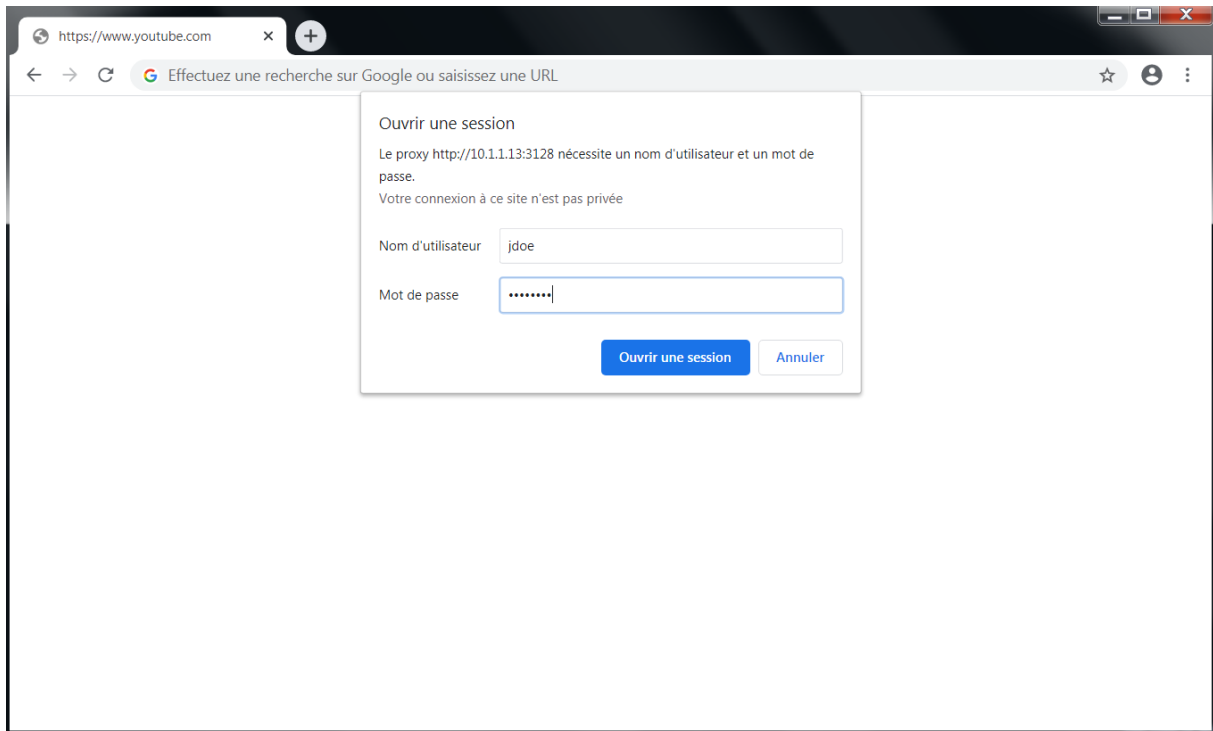
No Changes Pending

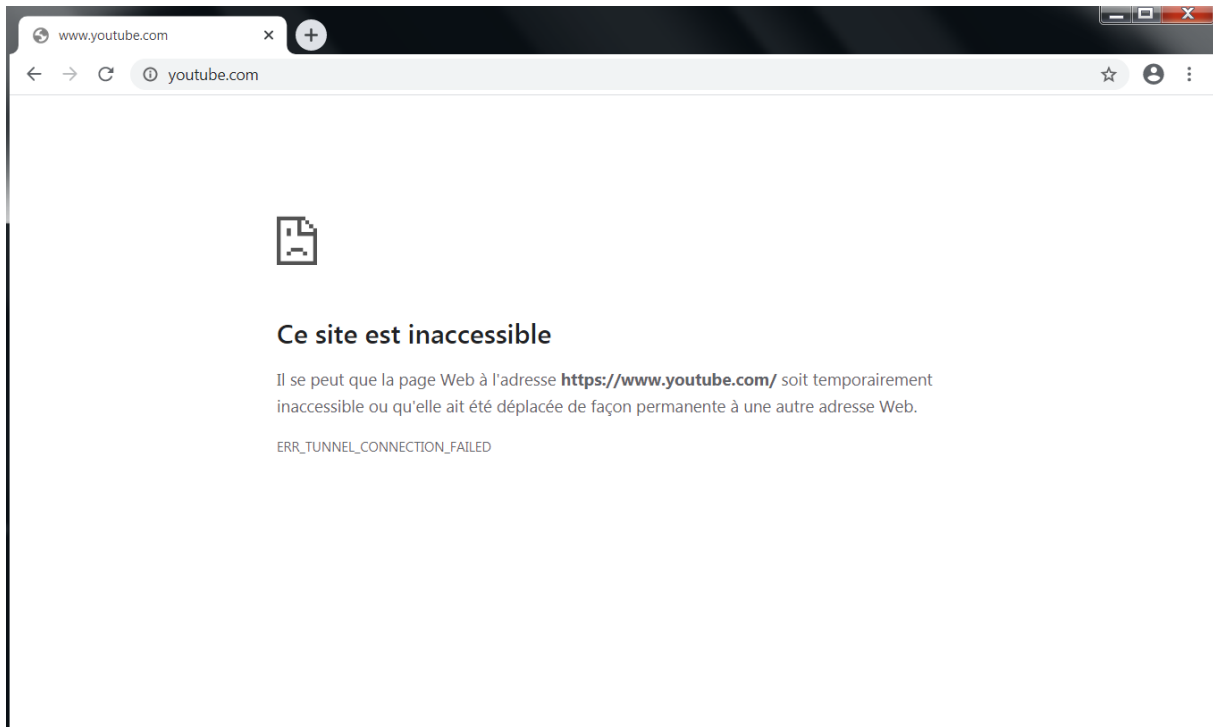
Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	Contactors Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Contractors)	(global policy)	Block: 1 Monitor: 85	(global policy)	(global policy)	(global policy)	
2	Sales Policy Identification Profile: Lab Profile 1 groups (AD1\LAB\Sales)	(global policy)	Block: 1 Monitor: 85	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Monitor: 87	Monitor: 356	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

From **jdoue-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 **jdoue** 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 **jdoue** user belongs to the **LAB\Sales** group. The web page fails to load but there is no notification for **jdoue** user.

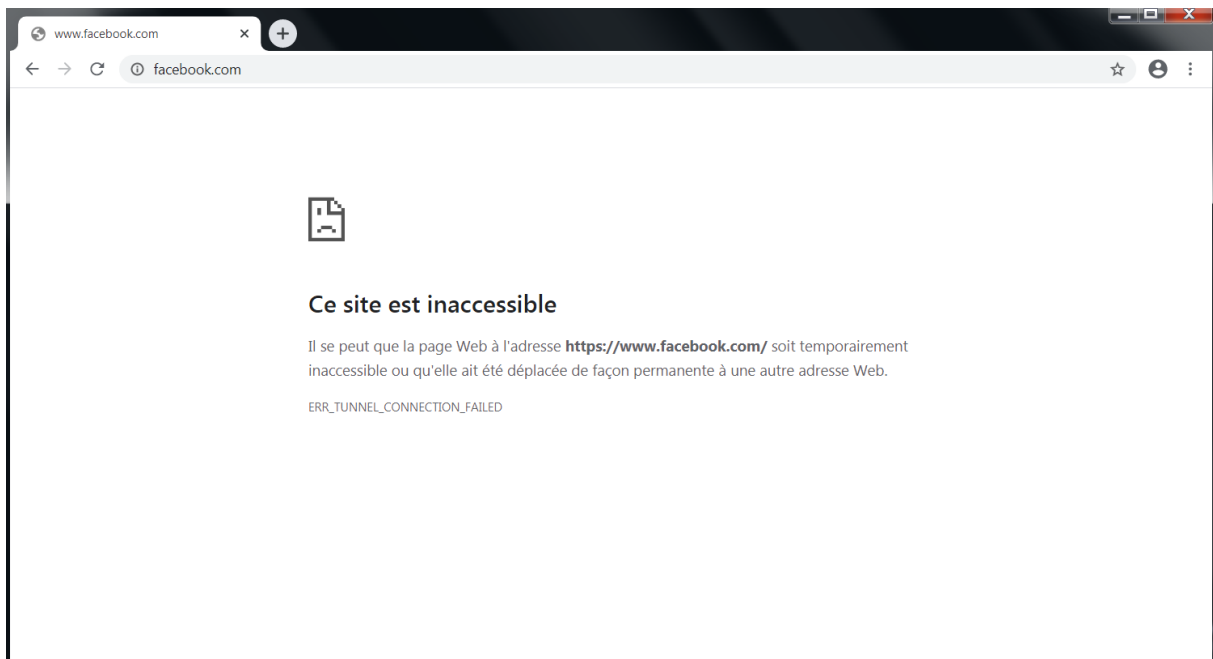
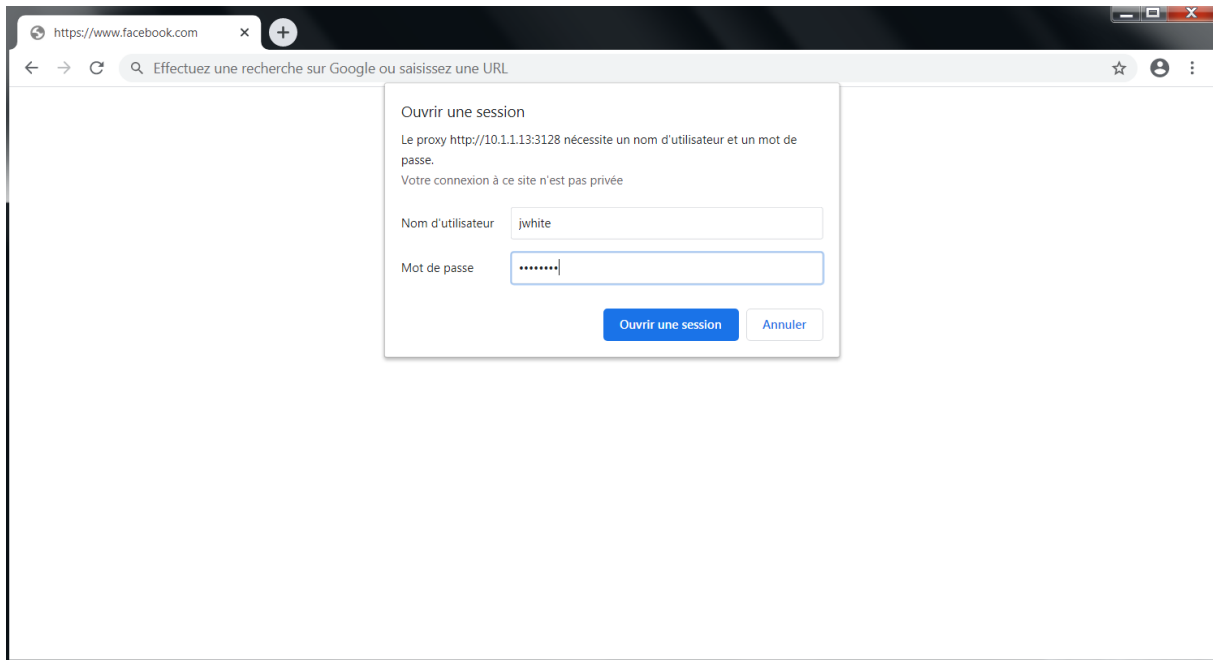
To display the default blocked page of WSA, we need https decryption.





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.

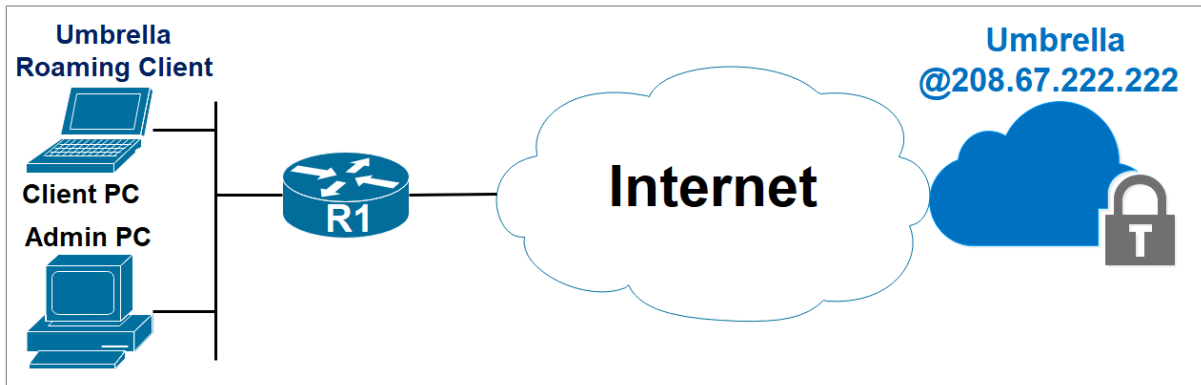
To display the default blocked page of WSA, we need https decryption.



Network Security All-in-one WorkBook

Cisco Umbrella

Lab 1: Cisco Umbrella Basic Configuration





Download the Umbrella Roaming Client.

Download Roaming Client

The roaming client protects laptops and desktops, on and off the network. Before installing the roaming client, read through the [documentation and prerequisites](#).


▲ For your [internal domains](#) to resolve, you must add them to the [internal domains list](#). It's important to add them before you deploy!

Cisco Umbrella Roaming Client

	Download Windows Client Supported Versions: Windows Vista, 7, 8, 10
	Download macOS Client Supported Versions: macOS 10.11+

AnyConnect Umbrella Roaming Security Module

Cisco AnyConnect can be configured to enable an Umbrella Roaming Security module which provides similar functionality to the roaming client. There are many deployment options, and each requires the customized profile downloaded below. [For full documentation, read here](#).

	Download Module Profile The Umbrella module requires AnyConnect for Windows or macOS, version 4.3 MR1 minimum. 4.3 MR4+ is recommended.
---	--

The AnyConnect 4.x client download can be found [here](#) (requires contract).

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

Verify Roaming Client Operation.

Umbrella Roaming Client (2.2.356.0)

IPv4 DNS status:

- Protected
- Encrypted
- User Identity:
- IPv4 Address: 10.254.253.120

IPv6 DNS status (BETA):

- Not Required
- Unencrypted
- User Identity:
- IPv6 Address:

IP Layer Enforcement status:

- Disabled

Details:

- Last Connected: 35 min ago
- Logging: Off
- Client Name: Redouane
- Organization Id: 3050180
- Device Id: 010174809F5C3355

[Run Diagnostic Tool](#)

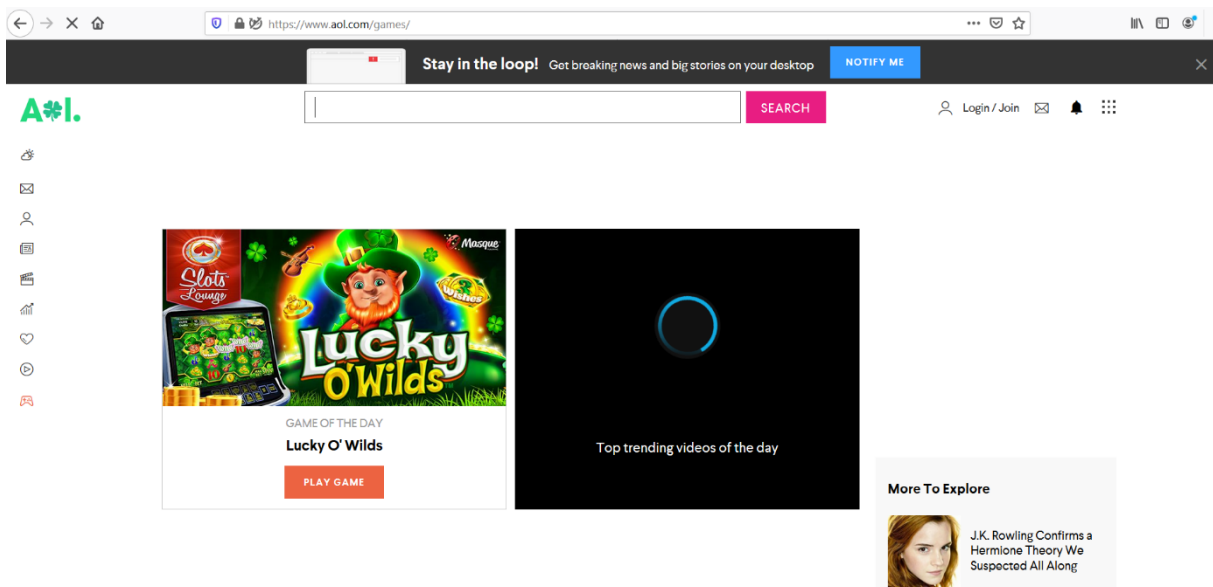
Navigate to **Deployments > Core Identities > Roaming Computers**. The hostname of the machine **Redouane** on which you installed the Umbrella roaming client, status and policy applied, is listed.

The screenshot shows the Cisco Umbrella dashboard for Roaming Computers. The left sidebar contains navigation options like Overview, Deployments, Core Identities, Networks, Network Devices, Roaming Computers, Mobile Devices, Chromebook Users, Configuration, Domain Management, Sites and Active Directory, Internal Networks, Root Certificate, Service Account Exceptions, Policies, Reporting, and Admin. The main content area shows a search bar and a table of Roaming Computers. The table has columns for Identity Name, Status, Tags, and Last Sync. Two entries are listed: 'F5-Server-1' (Offline, DNS Layer Encryption: disabled, Last Sync: 17 hours ago) and 'Redouane' (Protected & Encrypted at the DNS Layer, DNS Layer Encryption: enabled, Last Sync: 26 minutes ago).

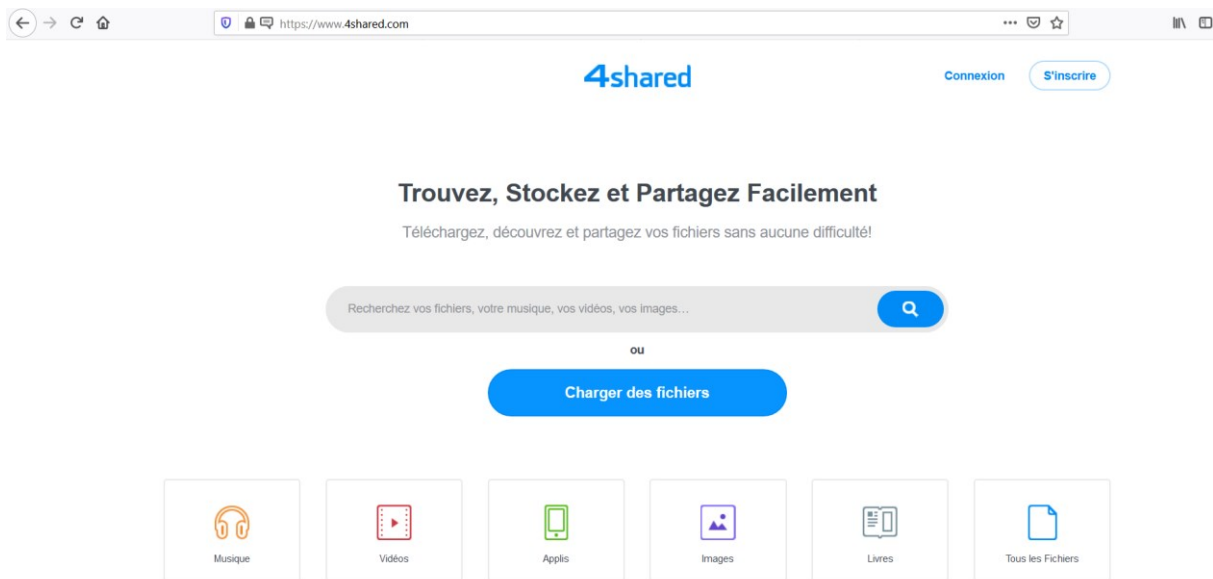
From the **Client PC**, access the URL **www.facebook.com**.



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

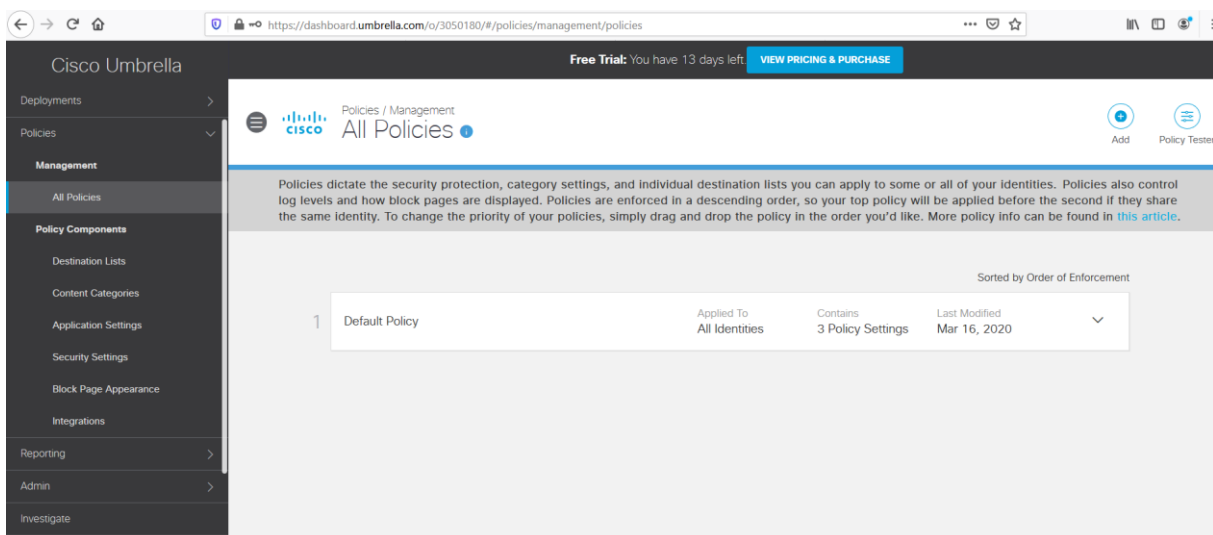


From the **Client PC**, access the URL **www.4shared.com**.

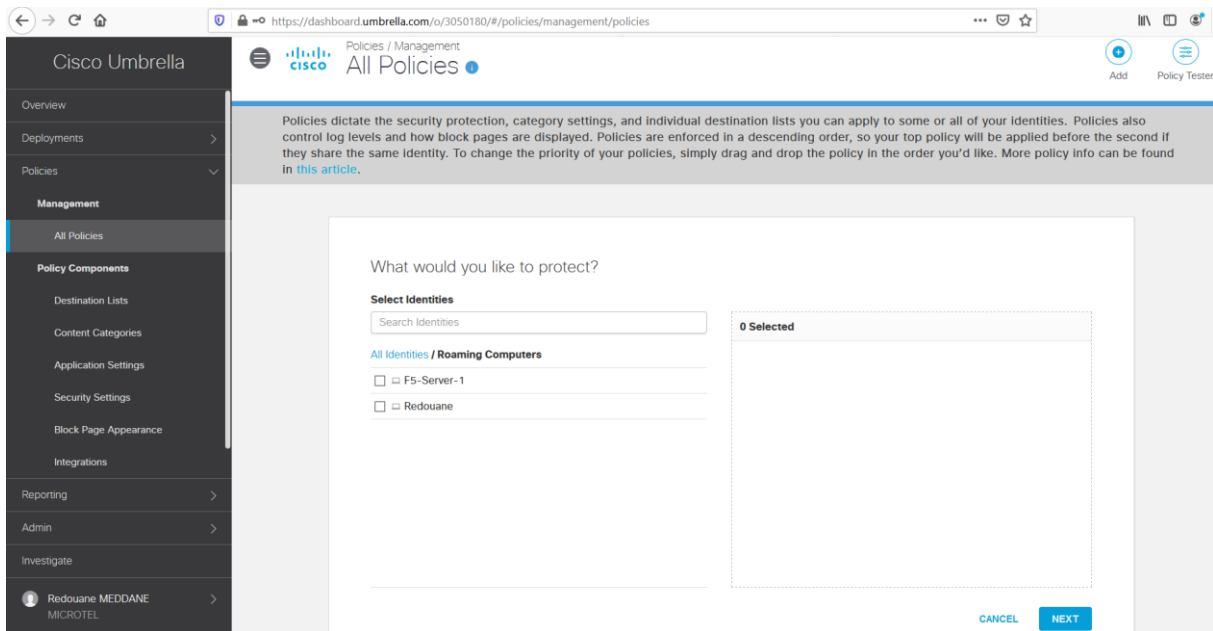
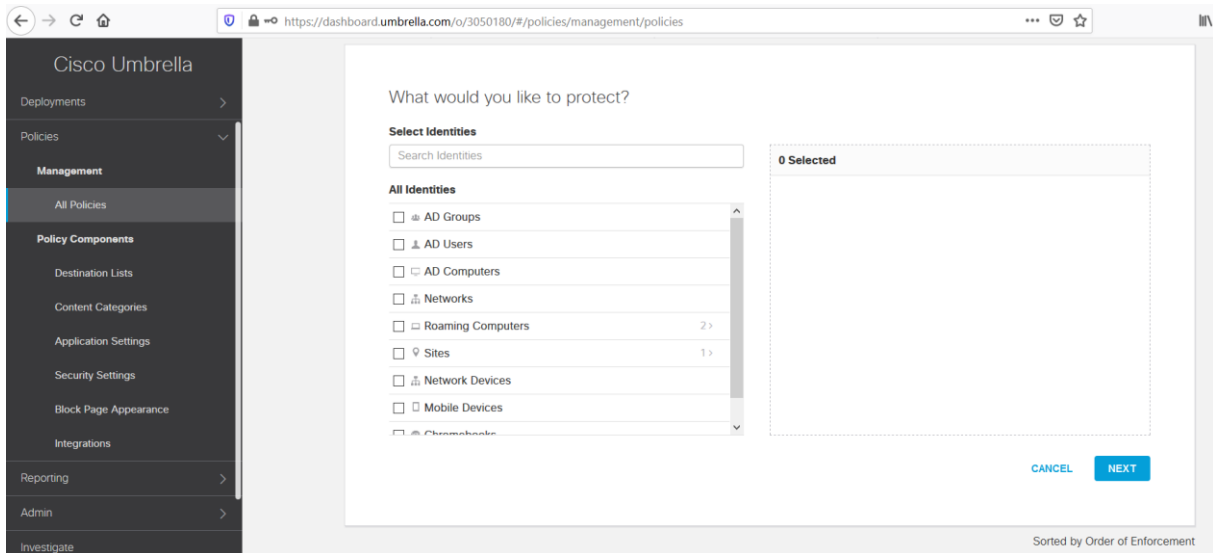


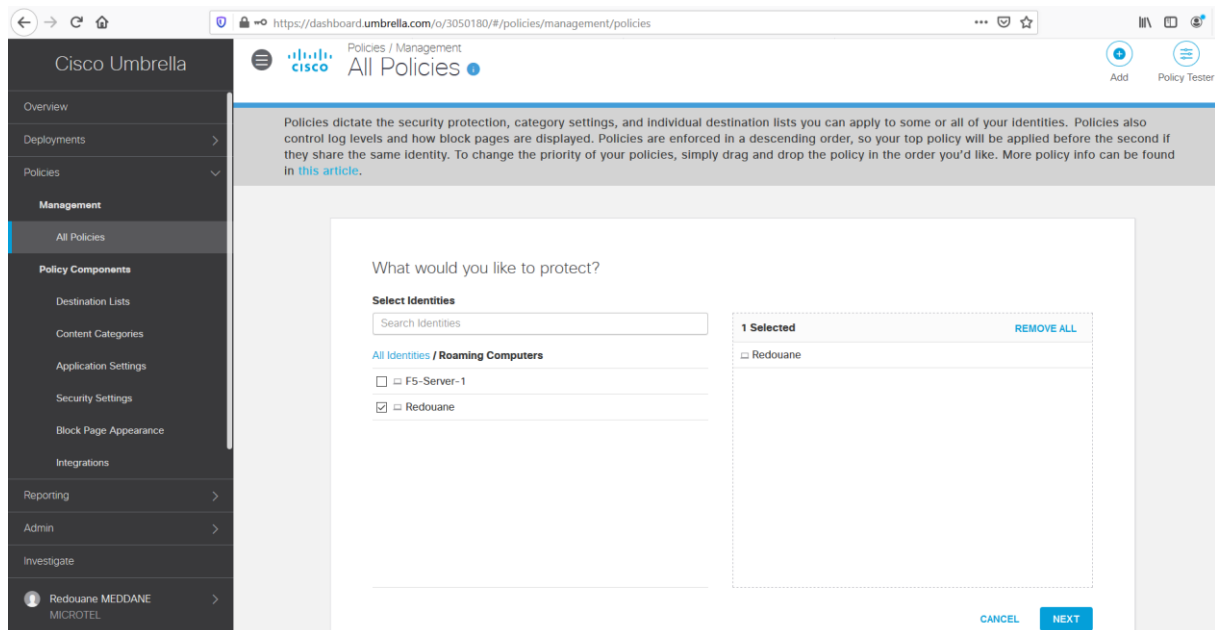
Create a policy based on the Machine s' Hostname **Redouane** as a condition.

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

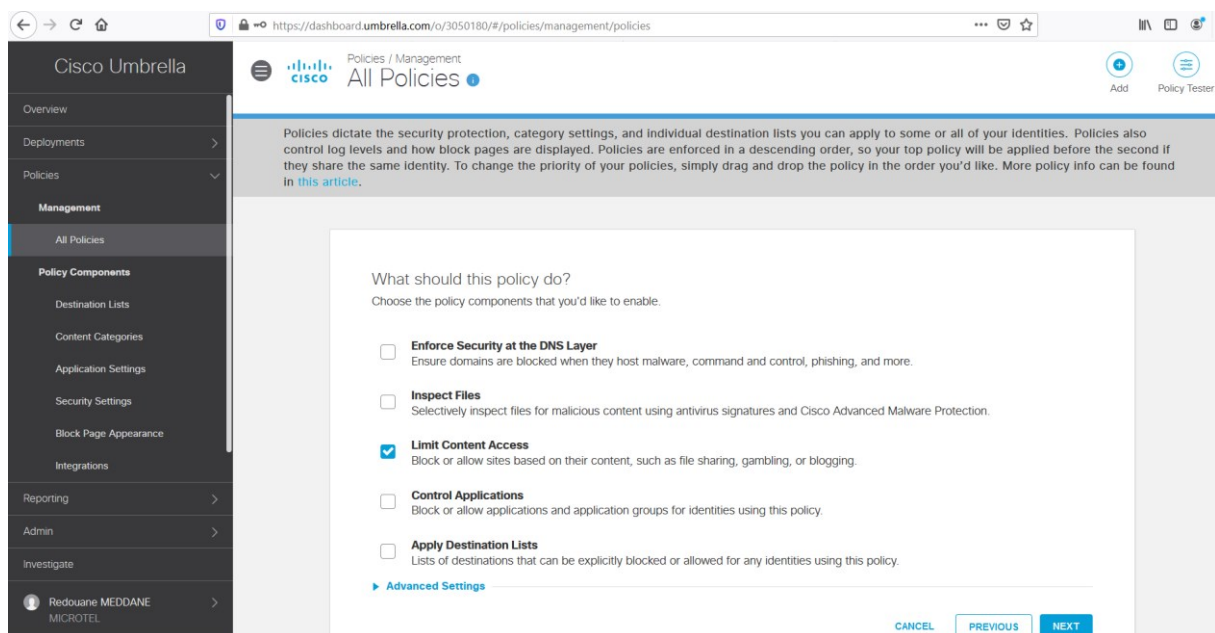


Select **Roaming Computers**, and the **Client PC** with the hostname **Redouane**. Select and then click **Next**.

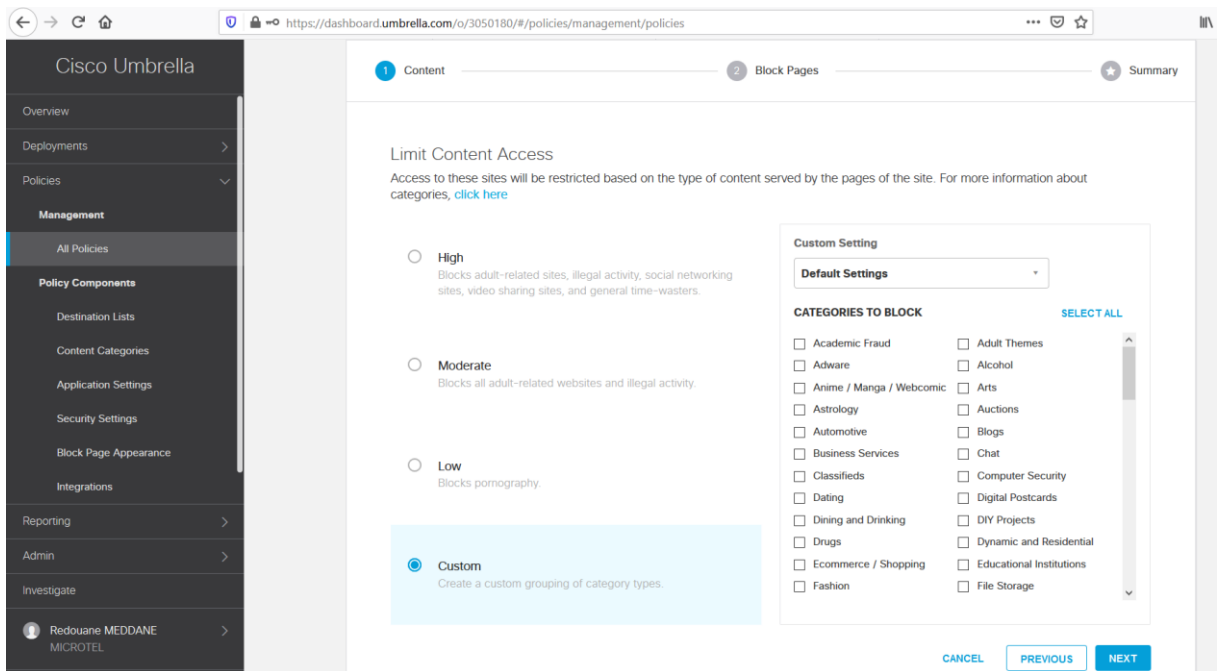
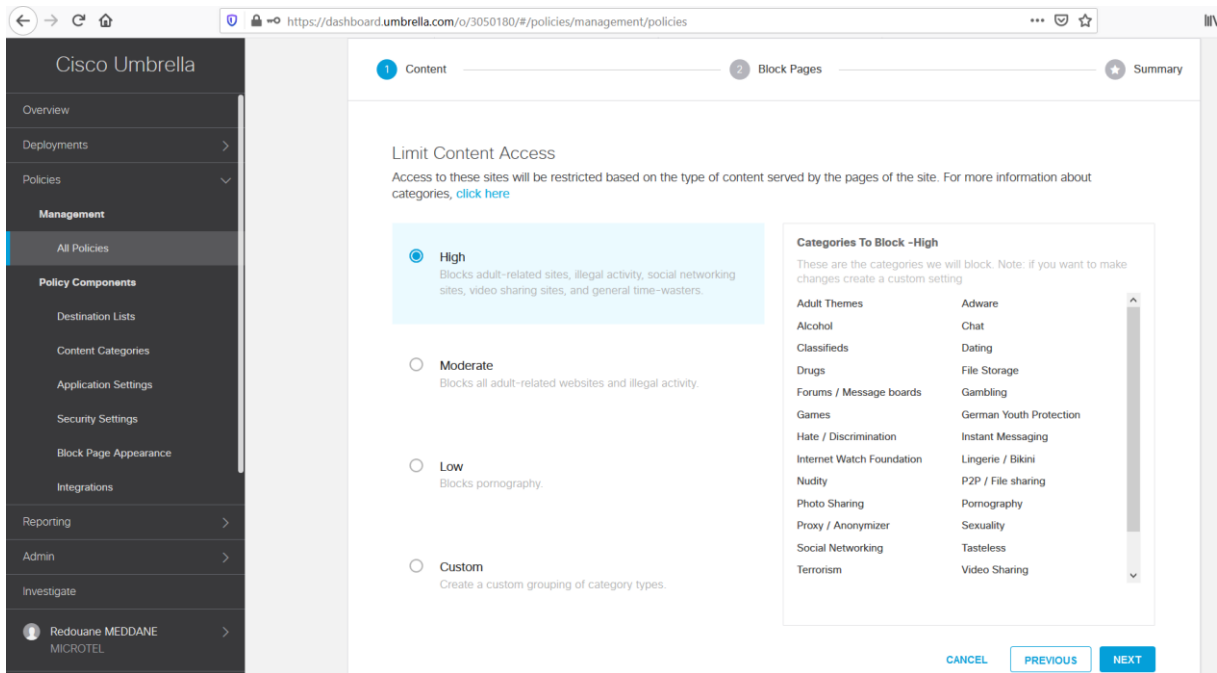




In the policy wizard, select the **Limit Content Access** component, this feature will be applied to the **Client PC**, then click **Next**.



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> ⋮ 🌟

Cisco Umbrella

- Overview
- Deployments >
- Policies >
 - Management
 - All Policies
 - Policy Components
 - Destination Lists
 - Content Categories
 - Application Settings
 - Security Settings
 - Block Page Appearance
 - Integrations
 - Reporting >
 - Admin >
 - Investigate
- Redouane MEDDANE >
 - MICROTEL

1 Content 2 Block Pages Summary

Limit Content Access

Access to these sites will be restricted based on the type of content served by the pages of the site. For more information about categories, [click here](#)

High
 Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

Moderate
 Blocks all adult-related websites and illegal activity.

Low
 Blocks pornography.

Custom
 Create a custom grouping of category types.

Custom Setting

Default Settings

CATEGORIES TO BLOCK SELECT ALL

<input type="checkbox"/> Fashion	<input type="checkbox"/> File Storage
<input checked="" type="checkbox"/> File Transfer Services	<input type="checkbox"/> Financial Institutions
<input type="checkbox"/> Forums / Message boards	<input type="checkbox"/> Freeware and Shareware
<input type="checkbox"/> Gambling	<input checked="" type="checkbox"/> Games
<input type="checkbox"/> German Youth Protection	<input type="checkbox"/> Government
<input type="checkbox"/> Hacking	<input type="checkbox"/> Hate / Discrimination
<input type="checkbox"/> Health and Fitness	<input type="checkbox"/> Humor
<input type="checkbox"/> Hunting	<input type="checkbox"/> Illegal Activities
<input checked="" type="checkbox"/> Illegal Downloads	<input type="checkbox"/> Infrastructure
<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Internet Telephony
<input type="checkbox"/> Internet Watch Foundation	<input type="checkbox"/> IT-ADM
<input type="checkbox"/> IT-AGCOM	<input type="checkbox"/> Jobs / Employment

CANCEL PREVIOUS NEXT

← → ↻ 🏠 <https://dashboard.umbrella.com/o/3050180/#/policies/management/policies> ⋮ 🌟

Cisco Umbrella

- Overview
- Deployments >
- Policies >
 - Management
 - All Policies
 - Policy Components
 - Destination Lists
 - Content Categories
 - Application Settings
 - Security Settings
 - Block Page Appearance
 - Integrations
 - Reporting >
 - Admin >
 - Investigate
- Redouane MEDDANE >
 - MICROTEL

1 Content 2 Block Pages Summary

Limit Content Access

Access to these sites will be restricted based on the type of content served by the pages of the site. For more information about categories, [click here](#)

High
 Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

Moderate
 Blocks all adult-related websites and illegal activity.

Low
 Blocks pornography.

Custom
 Create a custom grouping of category types.

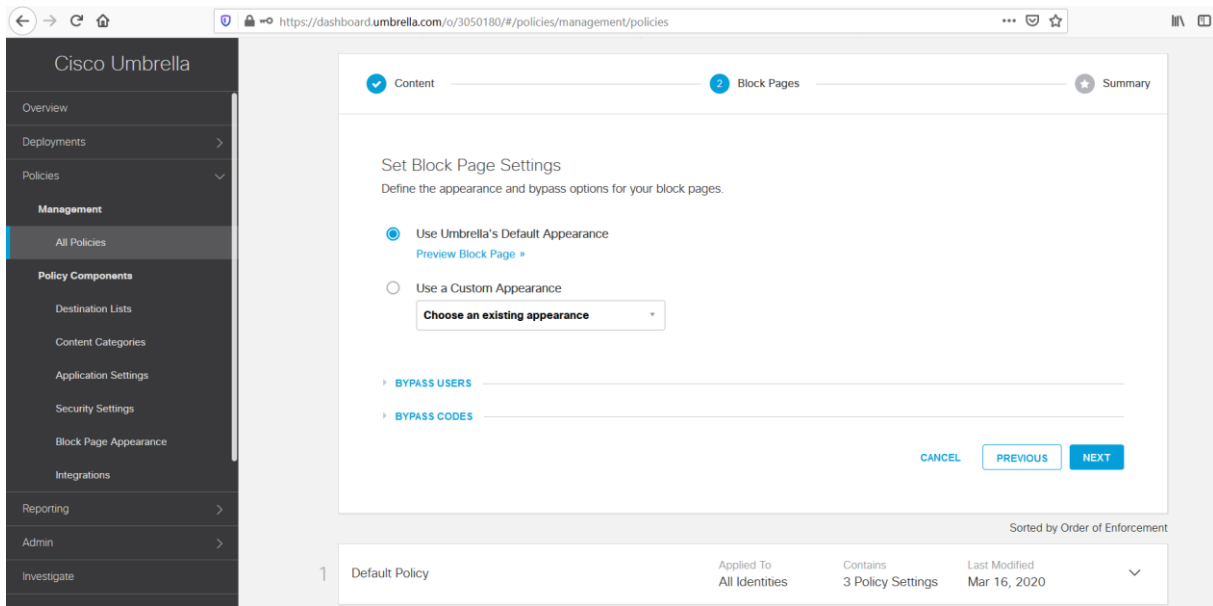
Custom Setting

Default Settings

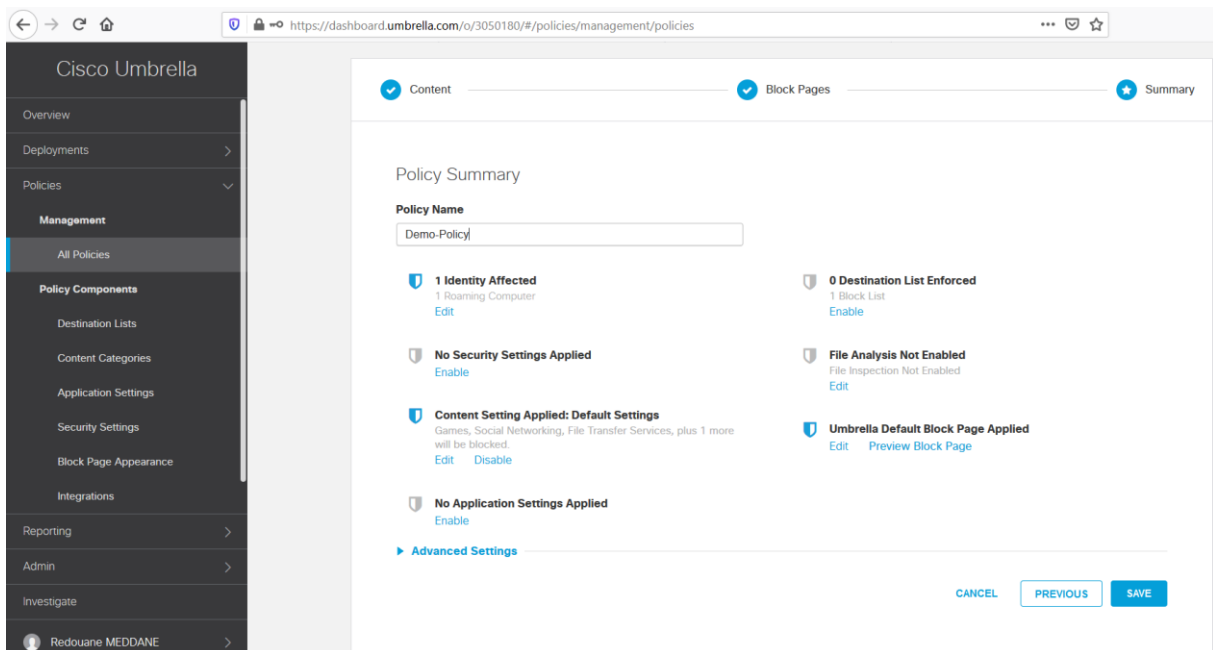
CATEGORIES TO BLOCK SELECT ALL

<input type="checkbox"/> Proxy / Anonymizer	<input type="checkbox"/> Radio
<input type="checkbox"/> Real Estate	<input type="checkbox"/> Religious
<input type="checkbox"/> Research / Reference	<input type="checkbox"/> SaaS and B2B
<input type="checkbox"/> Safe for Kids	<input type="checkbox"/> Science and Technology
<input type="checkbox"/> Search Engines	<input type="checkbox"/> Sex Education
<input type="checkbox"/> Sexuality	<input checked="" type="checkbox"/> Social Networking
<input type="checkbox"/> Social Science	<input type="checkbox"/> Society and Culture
<input type="checkbox"/> Software Updates	<input type="checkbox"/> Software / Technology
<input type="checkbox"/> Sports	<input type="checkbox"/> Tasteless
<input type="checkbox"/> Television	<input type="checkbox"/> Terrorism
<input type="checkbox"/> Tobacco	<input type="checkbox"/> Travel
<input type="checkbox"/> URL Shortener	<input type="checkbox"/> Video Sharing

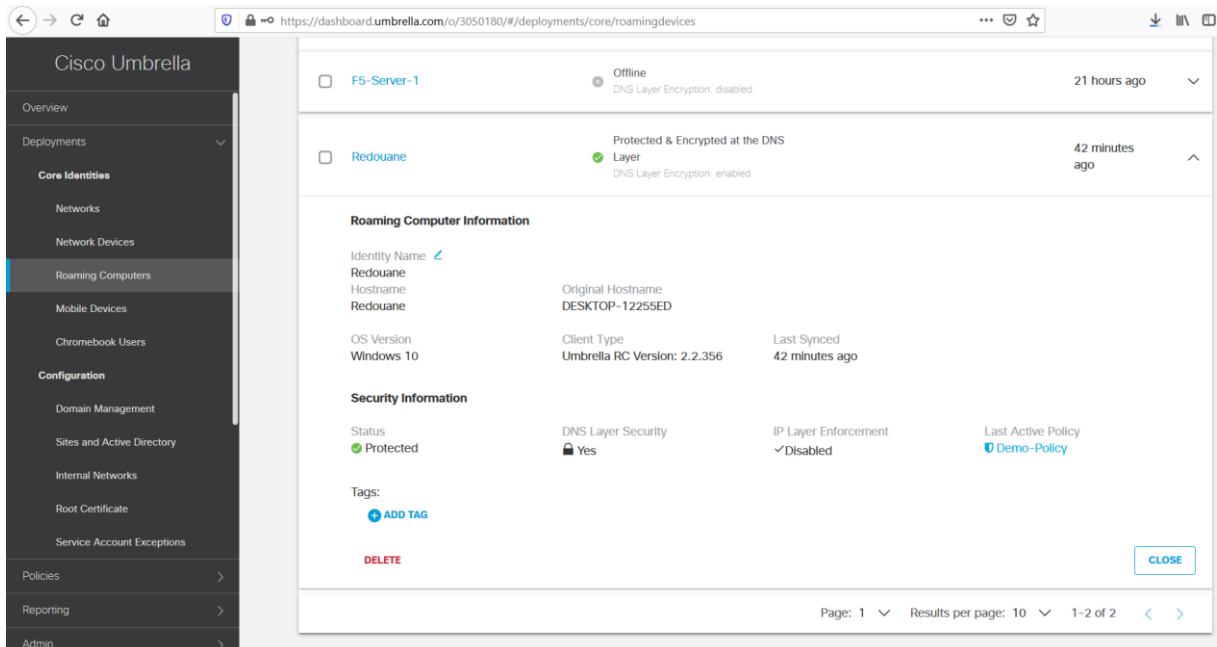
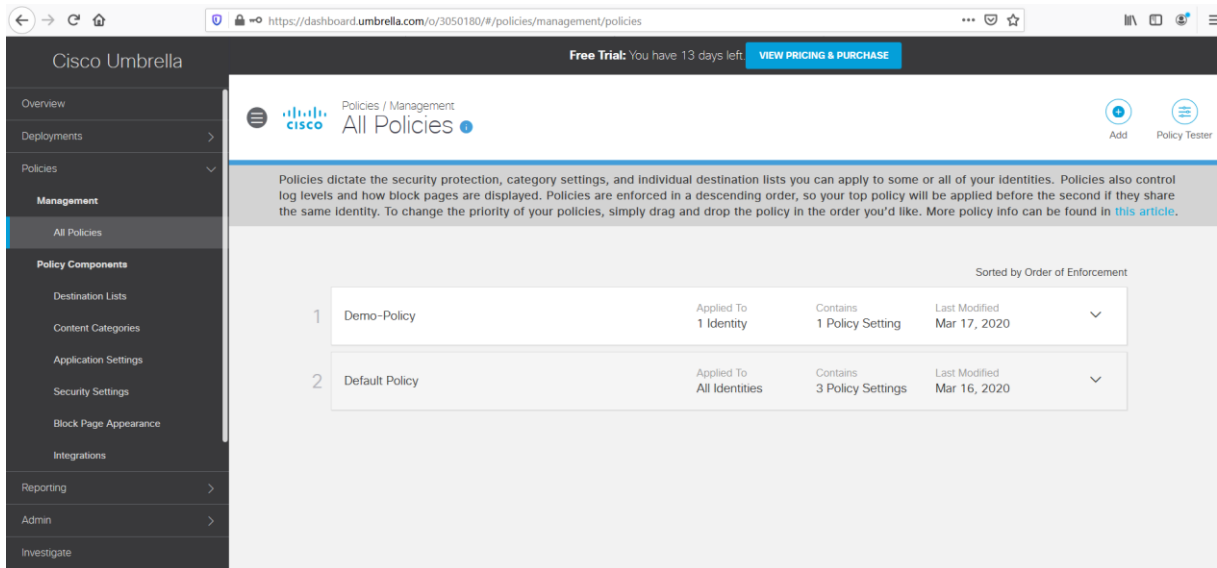
CANCEL PREVIOUS NEXT



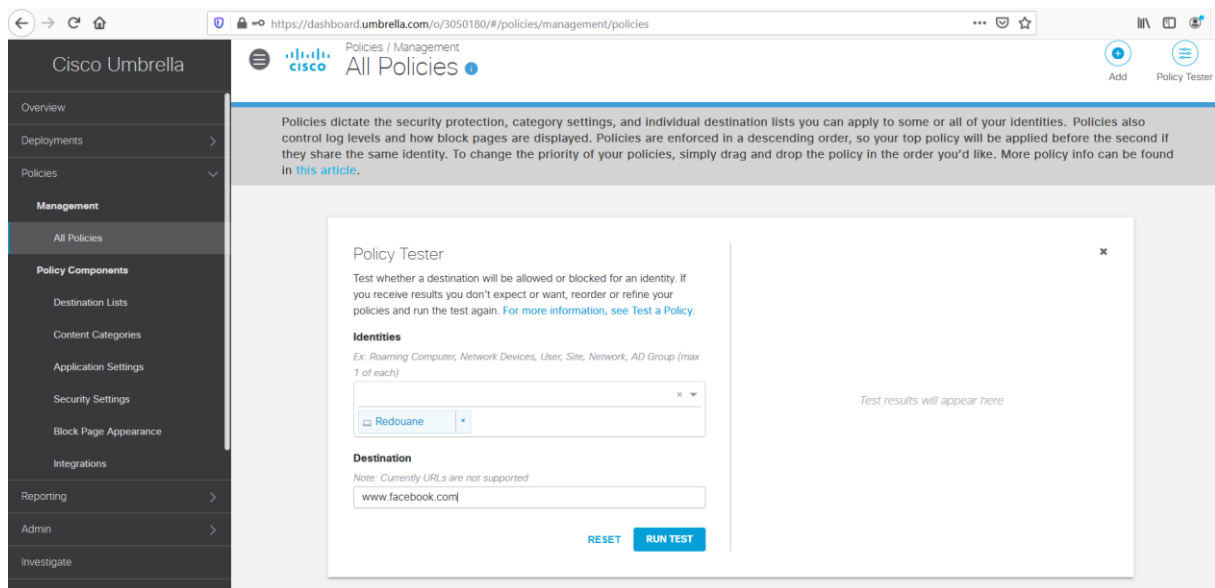
In the final step of the policy wizard, Enter the name **Demo-Policy** and click **Save**.



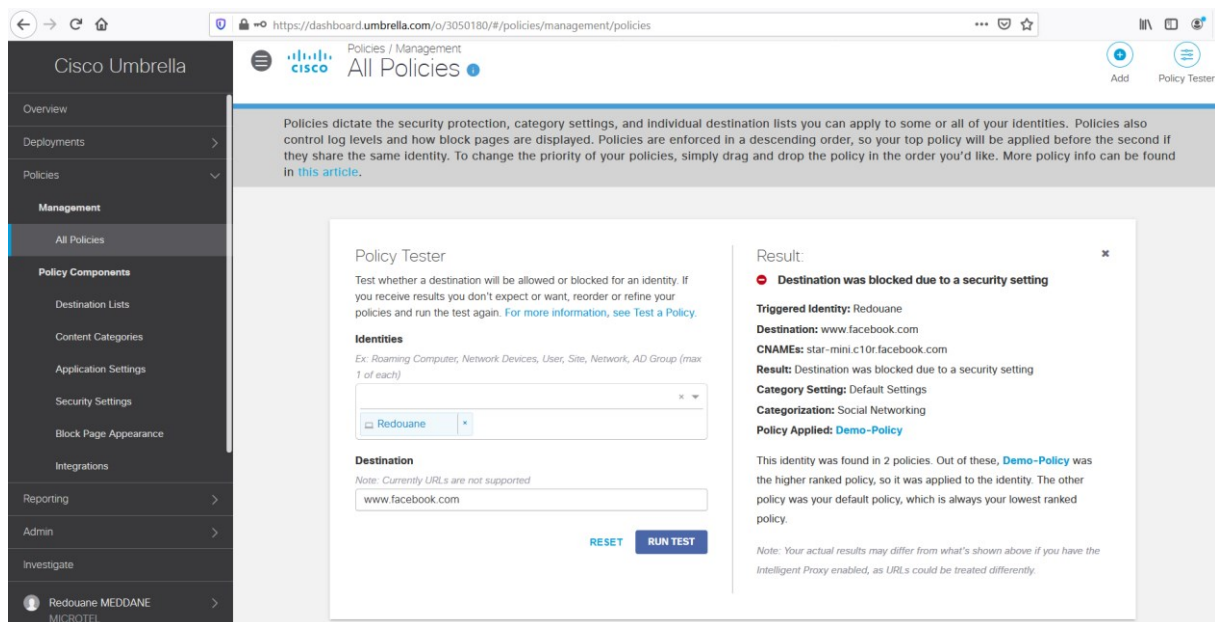
Navigate to **Deployments > Core Identities > Roaming Computers**.
Expand the Client PC **Redouane**, verify that the policy **Demo-Policy** is applied.



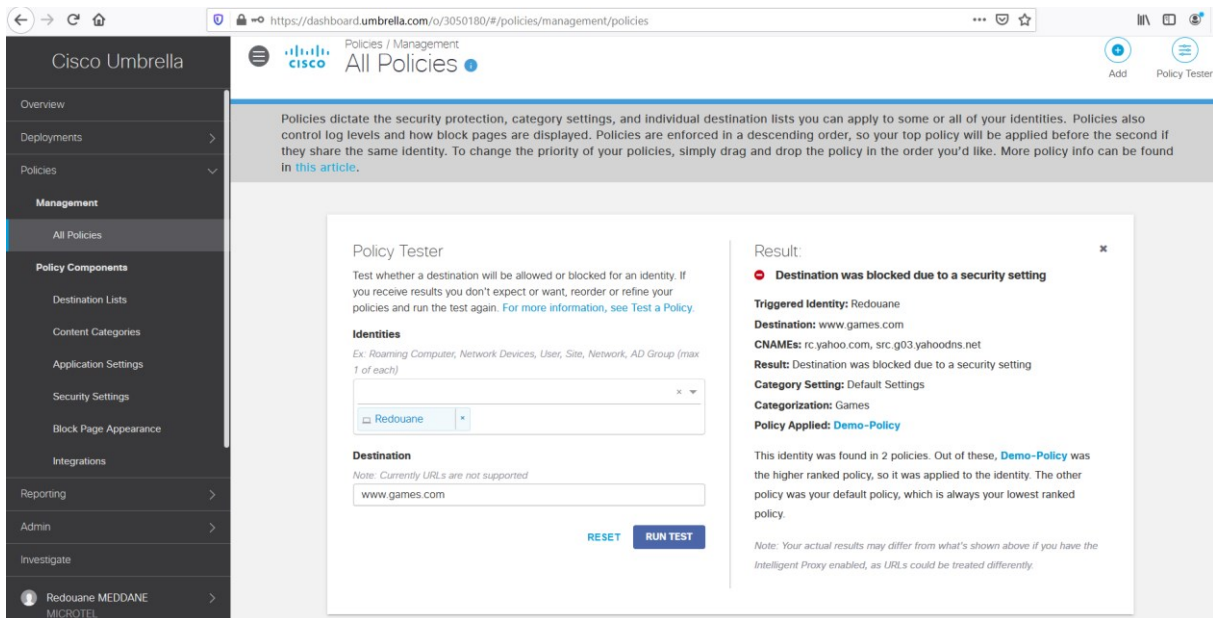
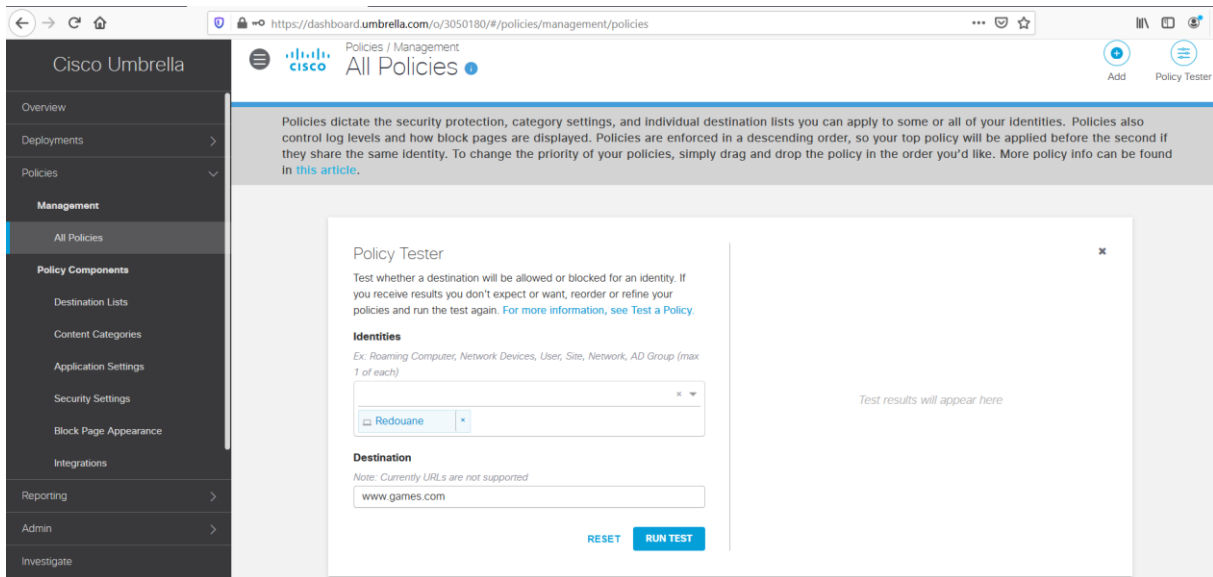
Navigate to **Policies > Management > All Policies**, Click the **Policy Tester** to test the policy **Demo-Policy**.



Under **Identities**, select the machine 's hostname **Redouane**, enter the URL www.facebook.com, 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.games.com, 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.

Cisco Umbrella Policies / Management All Policies

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if 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](#).

Policy Tester

Test whether a destination will be allowed or blocked for an identity. If 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](#).

Identities
Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)

Redouane

Destination
Note: Currently URLs are not supported

www.4shared.com

RESET RUN TEST

Test results will appear here

Sorted by Order of Enforcement

Cisco Umbrella Policies / Management All Policies

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if 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](#).

Policy Tester

Test whether a destination will be allowed or blocked for an identity. If 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](#).

Identities
Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)

Redouane

Destination
Note: Currently URLs are not supported

www.4shared.com

RESET RUN TEST

Result:

- Destination was blocked due to a security setting

Triggered Identity: Redouane
Destination: www.4shared.com
Result: Destination was blocked due to a security setting
Category Setting: Default Settings
Categorization: File Transfer Services
Policy Applied: Demo-Policy

This identity was found in 2 policies. Out of these, Demo-Policy was the higher ranked policy, so it was applied to the identity. The other policy was your default policy, which is always your lowest ranked policy.

Note: Your actual results may differ from what's shown above if you have the Intelligent Proxy enabled, as URLs could be treated differently.

Sorted by Order of Enforcement

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



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

Free Trial: You have 13 days left. [VIEW PRICING & PURCHASE](#)

Reporting / Core Reports
Activity Search

Schedule Download LAST 24 HOURS

Search request activity Advanced CLEAR Columns All Requests

CONTENT CATEGORIES Social Networking

VIEWING ACTIVITY FROM Mar 16, 2020 at 4:31 PM TO Mar 17, 2020 at 4:31 PM

Results per page: 50 1 - 50

Identity	Destination	Identity Used by Policy	Internal IP	External IP
Redouane	www.facebook.com	Redouane	10.254.253.120	105.96.14.98
Redouane	www.facebook.com	Redouane	10.254.253.120	105.96.14.98
Redouane	www.facebook.com	Redouane	10.254.253.120	105.96.14.98
Redouane	www.facebook.com	Redouane	10.254.253.120	105.96.14.98
Redouane	www.facebook.com	Redouane	10.254.253.120	105.96.14.98
Redouane	www.facebook.com	Redouane	10.254.253.120	105.96.14.98
Redouane	www.facebook.com	Redouane	10.254.253.120	105.96.14.98

FILTER BY:
Response: Allowed, Blocked, Proxied
Protocol: HTTP, HTTPS
Event Type: Antivirus, Application, Cisco AMP

Free Trial: You have 13 days left. [VIEW PRICING & PURCHASE](#)

Reporting / Core Reports
Activity Search

Schedule Download LAST 24 HOURS

Search request activity Advanced CLEAR Columns All Requests

CONTENT CATEGORIES Social Networking

VIEWING ACTIVITY FROM Mar 16, 2020 at 4:31 PM TO Mar 17, 2020 at 4:31 PM

Results per page: 50 1 - 50

Identity Used by Policy	Internal IP	External IP	Action	Categories
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking
Redouane	10.254.253.120	105.96.14.98	Blocked	Social Networking

FILTER BY:
Response: Allowed, Blocked, Proxied
Protocol: HTTP, HTTPS
Event Type: Antivirus, Application, Cisco AMP, Content Category

Reporting / Core Reports
Activity Search

Search request activity Advanced CLEAR Columns All Requests

CONTENT CATEGORIES Games

FILTER BY: Viewing activity from Mar 16, 2020 at 4:31 PM to Mar 17, 2020 at 4:31 PM Results per page: 50 1 - 4 of 4

Response Select All
 Allowed
 Blocked
 Proxied

Protocol Select All
 HTTP
 HTTPS

Event Type Select All
 Antivirus
 Application
 Cisco AMP
 Content Category
 Destination List
 Integration

Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action
Redouane	www.games.com	Redouane	10.254.253.120	105.96.14.98	Blocked
Redouane	www.games.com	Redouane	10.254.253.120	105.96.14.98	Blocked
Redouane	www.games.com	Redouane	10.254.253.120	105.96.14.98	Allowed
Redouane	www.games.com	Redouane	10.254.253.120	105.96.14.98	Allowed

Reporting / Core Reports
Activity Search

Search request activity Advanced CLEAR Columns All Requests

CONTENT CATEGORIES File Transfer Services

FILTER BY: Viewing activity from Mar 16, 2020 at 4:31 PM to Mar 17, 2020 at 4:31 PM Results per page: 50 1 - 50

Response Select All
 Allowed
 Blocked
 Proxied

Protocol Select All
 HTTP
 HTTPS

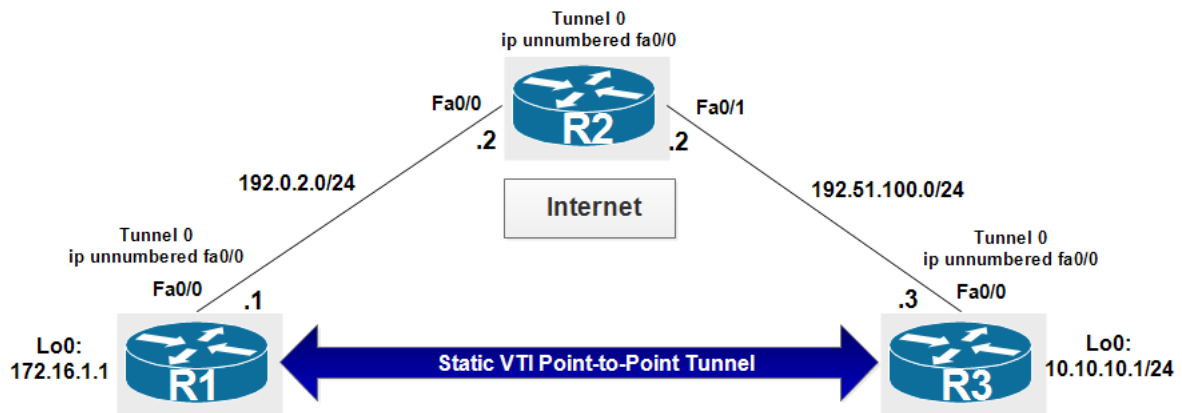
Event Type Select All
 Antivirus
 Application
 Cisco AMP
 Content Category

Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action
Redouane	www.4shared.com	Redouane	10.254.253.120	105.96.14.98	Blocked
Redouane	www.4shared.com	Redouane	10.254.253.120	105.96.14.98	Blocked
Redouane	www.4shared.com	Redouane	10.254.253.120	105.96.14.98	Blocked
Redouane	www.4shared.com	Redouane	10.254.253.120	105.96.14.98	Blocked
Redouane	dc393.4shared.com	Redouane	10.254.253.120	105.96.14.98	Allowed
Redouane	dc393.4shared.com	Redouane	10.254.253.120	105.96.14.98	Allowed
Redouane	dc400.4shared.com	Redouane	10.254.253.120	105.96.14.98	Allowed
Redouane	dc612.4shared.com	Redouane	10.254.253.120	105.96.14.98	Allowed

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
 !
interface FastEthernet0/0
 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 crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
192.0.2.1    192.51.100.1 QM_IDLE       1001 ACTIVE
IPv6 Crypto ISAKMP SA
R1#
```

```
R3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
192.0.2.1    192.51.100.1 QM_IDLE       1001 ACTIVE
IPv6 Crypto ISAKMP 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): (0.0.0.0/0.0.0.0/0/0)
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
!!!!
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): (0.0.0.0/0.0.0.0/0/0)
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)
```

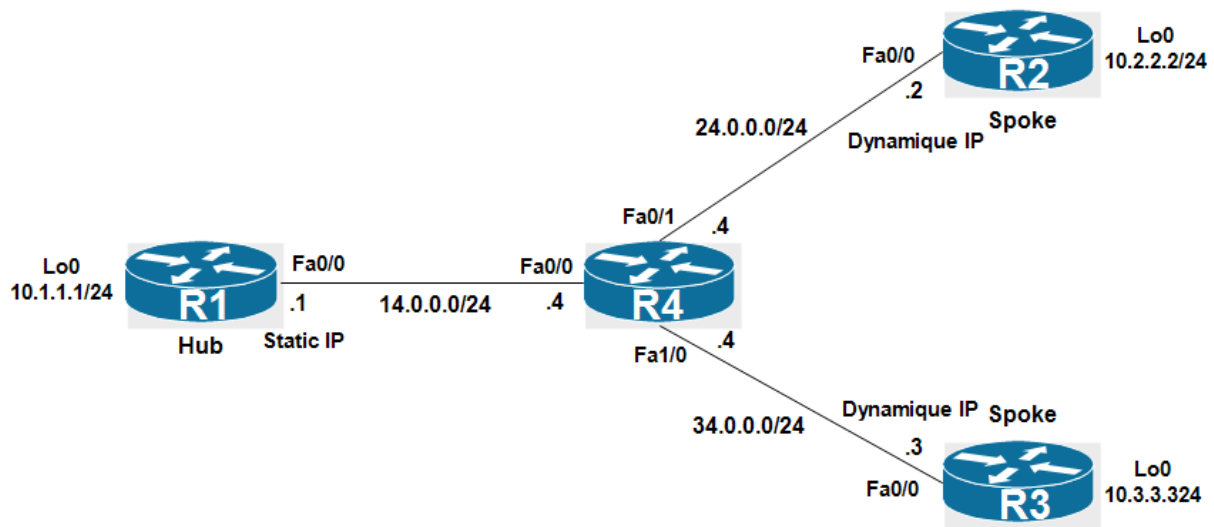
```
spi: 0xB49AA172(3030032754)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 4, flow_id: 4, sibling_flags 80000040, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4187315/3445)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

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 0.0.0.0 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-T0-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-T0-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-T0-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-T0-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-T0-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 0.0.0.0) 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-T0-R2 esp-aes esp-sha-hmac
R1(config)#crypto ipsec transform-set TEST-T0-R3 esp-aes esp-sha-hmac
```

Create a dynamic crypto map (DYNMAP-R2) and references the transform set "TEST-T0-R2" and the ACL "VPN-T0-R2":

```
R1(config)#crypto dynamic-map dynmap-R2 10
R1(config-crypto-map)# set transform-set TEST-T0-R2
R1(config-crypto-map)# match address VPN-T0-R2
```

Create a dynamic crypto map (DYNMAP-R3) and references the transform set "TEST-T0-R3" and the ACL "VPN-T0-R3":

```
R1(config)#crypto dynamic-map dynmap-R3 20
R1(config-crypto-map)# set transform-set TEST-T0-R3
R1(config-crypto-map)# match address VPN-T0-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        ACTIVE aes  sha    psk  1  23:58:55
      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 negotiated 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 IPsec 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

```



```

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#

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          Remote          I-VRF   Status  Encr Hash   Auth DH Lifetime
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
```

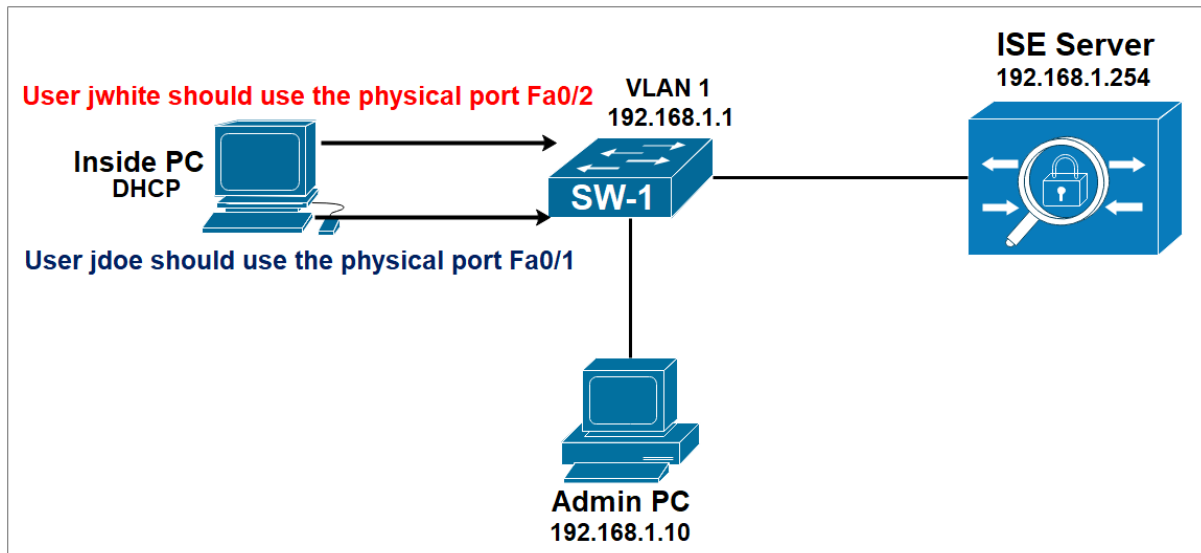
```
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 34.0.0.3 port 500
IKEv1 SA: local 14.0.0.1/500 remote 34.0.0.3/500 Active
IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 10.3.3.0/255.255.255.0
Active SAs: 2, origin: dynamic crypto map
```

```
R1#
```

**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 **jdoue** with password **Cisco123**.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The current page is titled "Network Access Users List > New Network Access User". The form fields are as follows:

- Name:** jdoue
- Status:** Enabled (checked)
- Email:** (empty)
- Passwords:**
 - Password Type:** Internal Users
 - * Login Password:** (masked with dots) and **Re-Enter Password:** (masked with dots). There are "Generate Password" buttons next to each.
 - Enable Password:** (empty) and **Re-Enter Password:** (empty). There are "Generate Password" buttons next to each.
- User Information:** (collapsed)
- Account Options:** (collapsed)
- Account Disable Policy:** (collapsed)
- User Groups:** (collapsed)

At the bottom of the form, there is a "Select an item" dropdown menu and "Submit" and "Cancel" buttons.

Create a user **jwhite** with password **Cisco1234**.

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/> Enabled	jdoe		John	Doe			
<input checked="" type="checkbox"/> Enabled	jwhite						
<input checked="" type="checkbox"/> 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**.

Name	Description	No. of Network Devices
<input checked="" type="checkbox"/> All Device Types	All Device Types	--
<input type="checkbox"/> All Locations	All Locations	--
<input type="checkbox"/> Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group



Name *

Description

Parent Group *

Cancel

Save

The screenshot shows the Cisco Identity Services Engine Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. The 'Network Device Groups' section is active, showing a table with columns: Name, Description, and No. of Network Devices. The table contains the following data:

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.

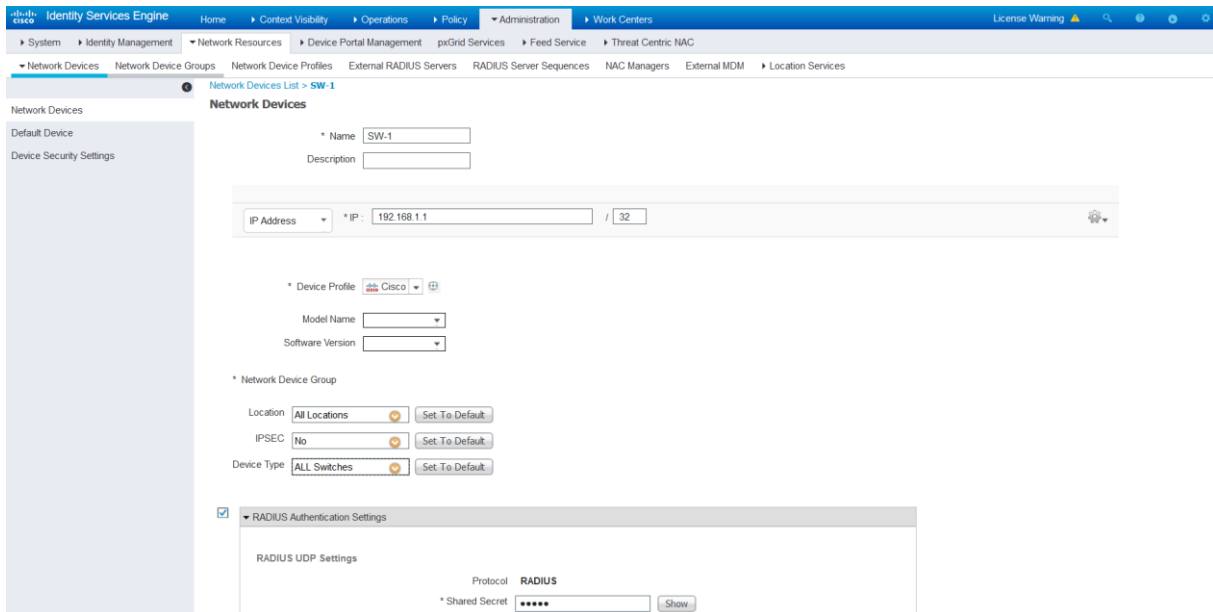
In the **IP Address** field, enter **192.168.1.1/32**. this the IP address of the switch interface that will forward RADIUS packets to Cisco ISE.

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

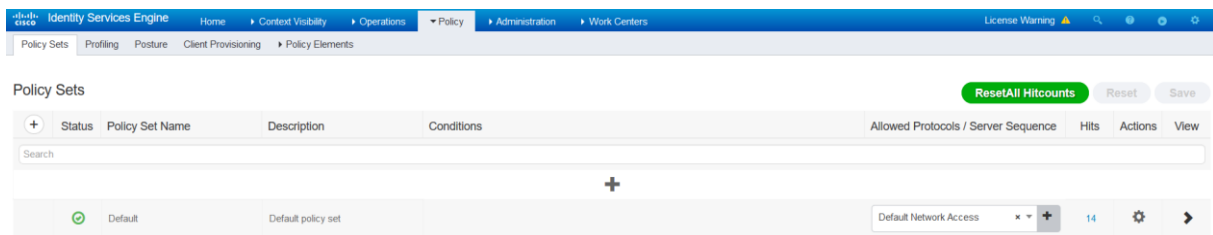
To activate Radius Authentication Settings, click the check box.

In the **Shared Secret** field, enter a shared secret of **cisco**.

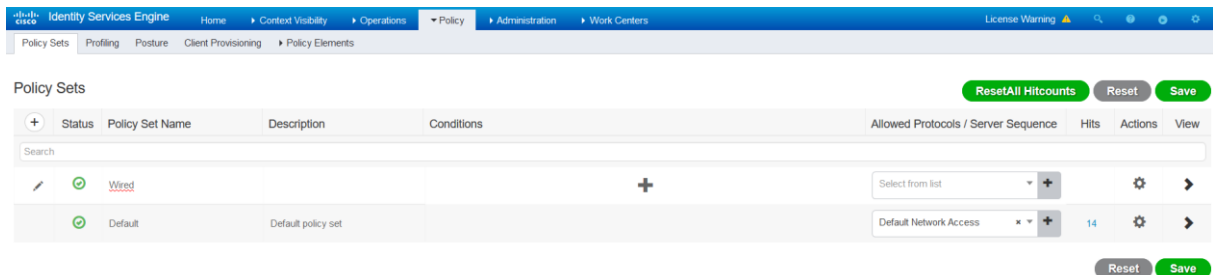
Click the **Submit** button.



Navigate to **Policy > Policy Sets**.
Click the plus icon (+) to create a new Policy Set.



Enter **Wired** as the policy set **Name**.



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**.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Policy Sets

ResetAll Hitcounts | Reset | Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Wired		DEVICE Device Type EQUALS All Device Types#ALL Switches	Default Network Access x +		⚙️ ▶️	
✓	Default	Default policy set		Default Network Access x +	14	⚙️ ▶️	

Reset | Save

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

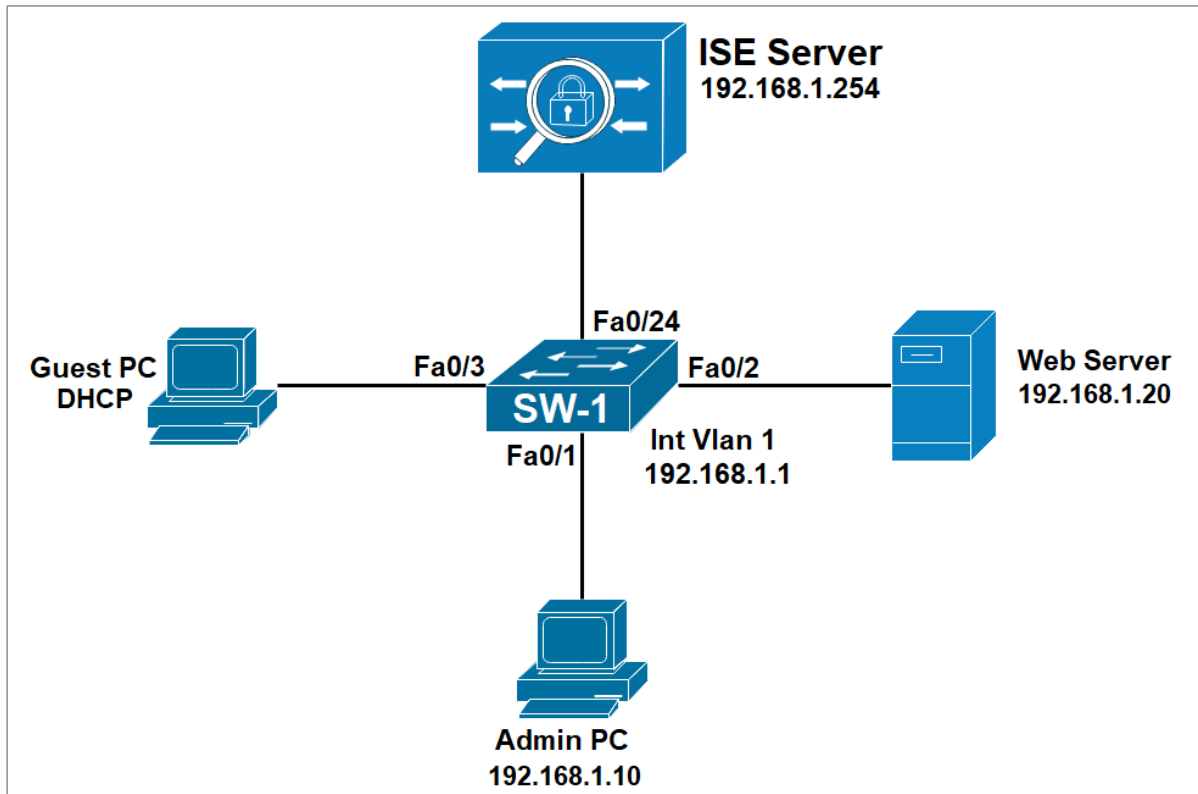
Policy Sets

ResetAll Hitcounts | Reset | Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Wired		DEVICE Device Type EQUALS All Device Types#ALL Switches	Default Network Access x +	0	⚙️ ▶️	
✓	Default	Default policy set		Default Network Access x +	14	⚙️ ▶️	

Reset | Save

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](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**.

The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The breadcrumb navigation is Administration > Network Resources > Network Device Groups. The page title is Network Device Groups. There are buttons for Refresh, Add, Duplicate, Edit, and Trash. Below the buttons is a table with columns for Name, Description, and No. of Network Devices. The table contains three rows: All Device Types, All Locations, and Is IPSEC Device. The 'All Device Types' row is selected with a checkbox.

Name	Description	No. of Network Devices
<input checked="" type="checkbox"/> All Device Types	All Device Types	--
<input type="checkbox"/> All Locations	All Locations	--
<input type="checkbox"/> Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group



Name *

Description

Parent Group *

Cancel

Save

Identity Services Engine Administration Work Centers License Warning

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Device Groups

All Groups Choose group

Refresh Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

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.

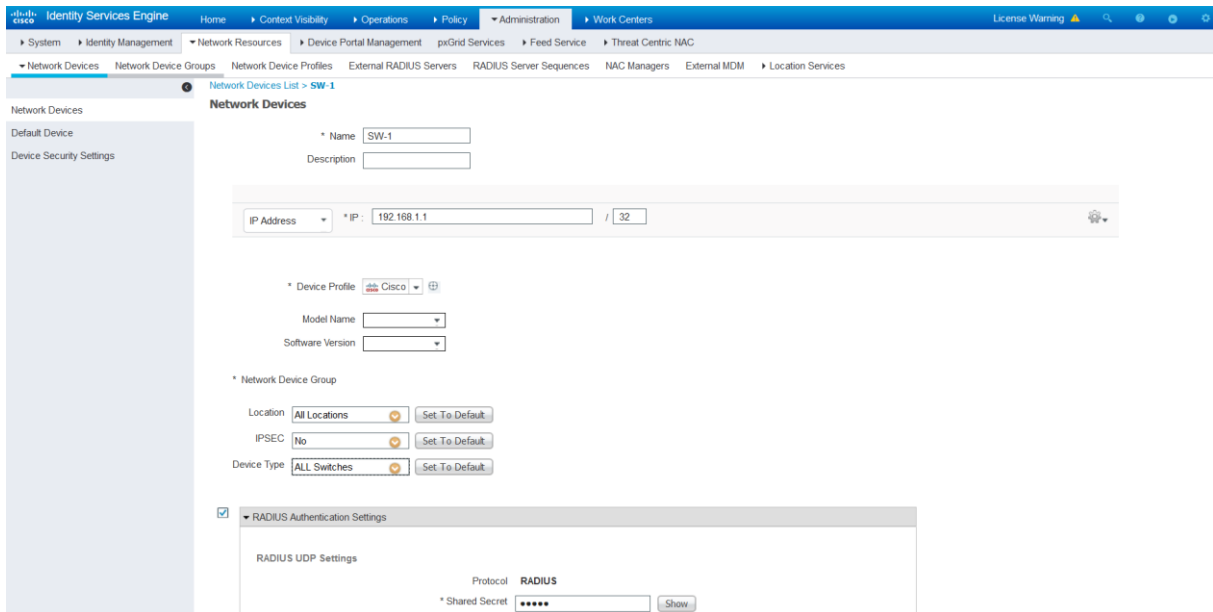
In the **IP Address** field, enter **192.168.1.1/32**. this the IP address of the switch interface that will forward RADIUS packets to Cisco ISE.

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

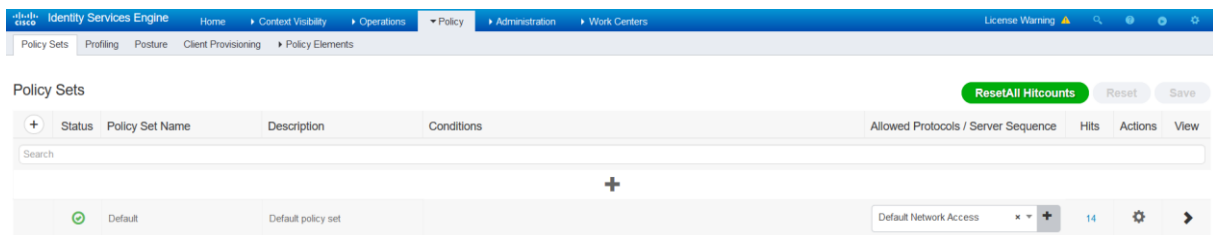
To activate Radius Authentication Settings, click the check box.

In the **Shared Secret** field, enter a shared secret of **cisco**.

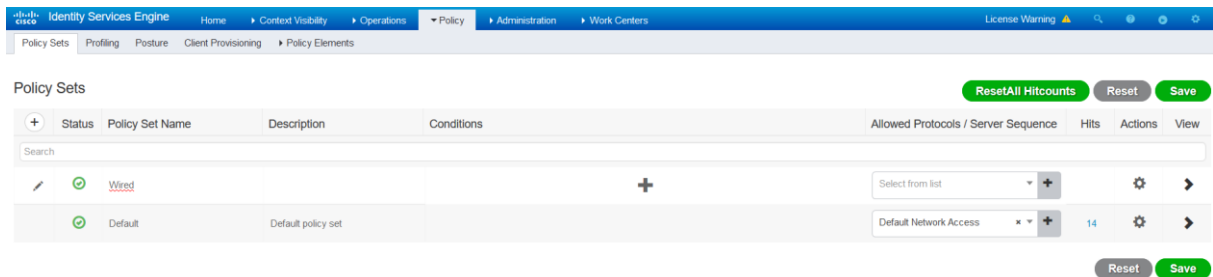
Click the **Submit** button.



Navigate to **Policy > Policy Sets**.
Click the plus icon (+) to create a new Policy Set.



Enter **Wired** as the policy set **Name**.



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**.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	Wired		DEVICE Device Type: EQUALS All Device Types#ALL Switches	Default Network Access		⚙️	➔
✔	Default	Default policy set		Default Network Access	14	⚙️	➔

Buttons: **ResetAll Hitcounts**, **Reset**, **Save**

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	Wired		DEVICE Device Type: EQUALS All Device Types#ALL Switches	Default Network Access	0	⚙️	➔
✔	Default	Default policy set		Default Network Access	14	⚙️	➔

Buttons: **ResetAll Hitcounts**, **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.

Policy Sets → Wired

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	Wired		DEVICE Device Type: EQUALS All Device Types#ALL Switches	Default Network Access	0	⚙️	➔

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		All_User_ID_Stores	0	⚙️

Buttons: **ResetAll Hitcounts**, **Reset**, **Save**

Enter the name Dot1X for Wired.

Click the **(+)** symbol to assign a condition to the rule.

Assign the condition **Wired_802.1X**.

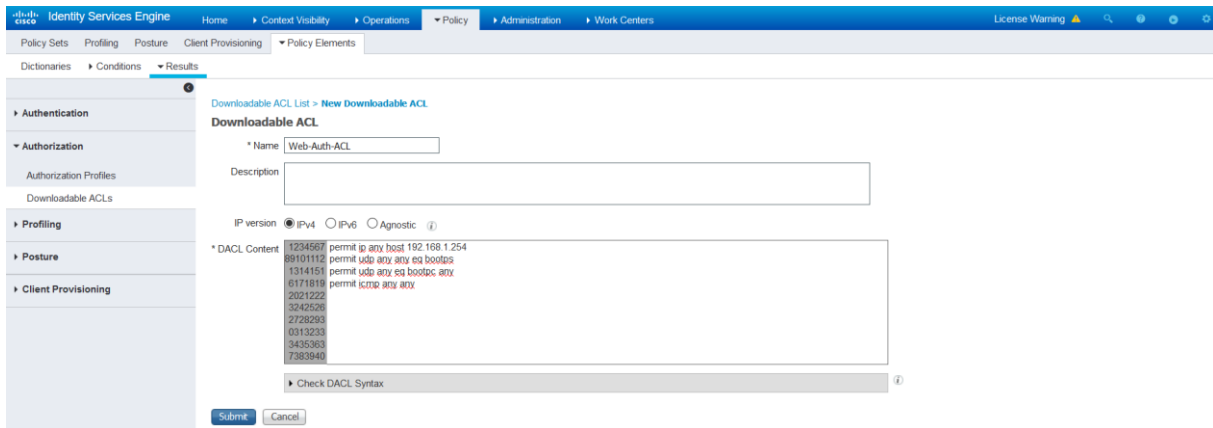
Use the Identity Source **Internal Users**.

The image displays two screenshots of the Cisco Identity Services Engine (ISE) interface, specifically the 'Policy Sets' configuration page for a 'Wired' policy set.

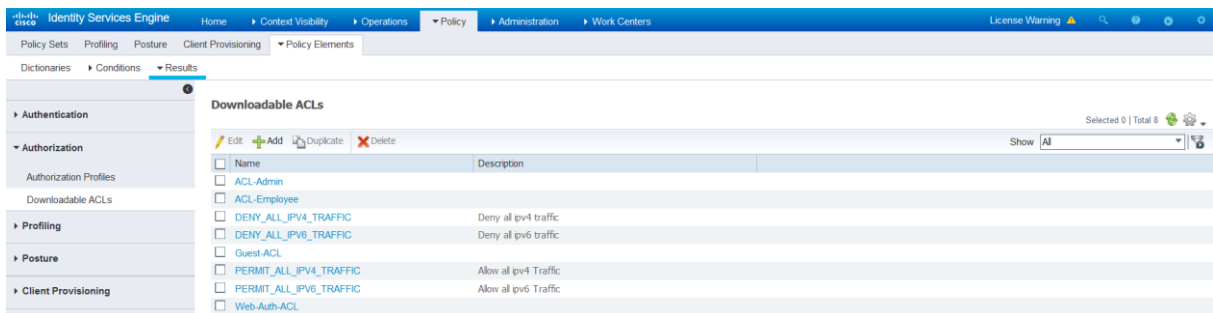
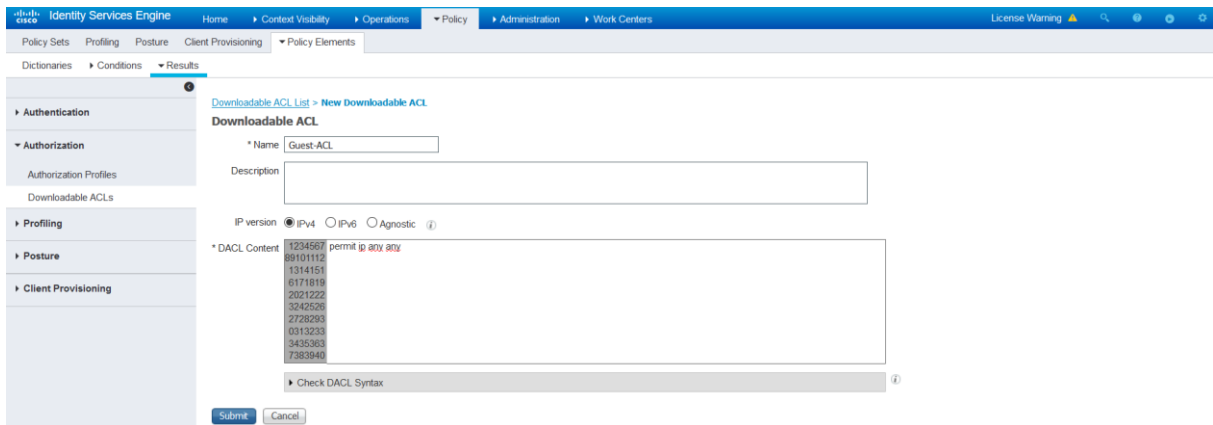
Top Screenshot: Shows the 'Authentication Policy' section. The 'Wired' policy set is active. Under 'Authentication Policy (2)', there are two rules: 'Dot1X for Wired' and 'Default'. The 'Dot1X for Wired' rule is selected, and its configuration is visible, showing 'Internal Users' as the user type and 'Options' as the action. The 'Default' rule is also visible, showing 'All_User_ID_Stores' as the user type and 'Options' as the action.

Bottom Screenshot: Shows the 'Authorization Policy' section. The 'Wired' policy set is active. Under 'Authorization Policy (2)', there are two rules: 'Wired_802.1X' and 'DenyAccess'. The 'Wired_802.1X' rule is selected, and its configuration is visible, showing 'Internal Users' as the user type and 'Options' as the action. The 'DenyAccess' rule is also visible, showing 'DenyAccess' as the user type and 'Options' as the action.

Create a **ACL** 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.



Create another **DACL** which will allow access to network after web authentication.
Click **Add**.
Enter **Guest-ACL** in the **Name** field, allow all traffic.



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.

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

Click **Submit**.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > New Authorization Profile'. The 'Authorization Profile' section has the following fields: Name (web portal profile), Description (empty), Access Type (ACCESS_ACCEPT), Network Device Profile (Cisco), Service Template (unchecked), Track Movement (unchecked), and Passive Identity Tracking (unchecked). The 'Common Tasks' section has 'DACL Name' checked and set to 'Web-Auth-ACL', and 'IPv6 DACL Name' unchecked.

This screenshot is similar to the previous one but shows the 'Web Redirection' settings. The 'Common Tasks' section now includes 'Voice Domain Permission' (unchecked), 'Web Redirection (CWA, MDM, NSP, CPP)' (checked), and 'Display Certificates Renewal Message' (checked). The 'Web Redirection' settings are: Centralized Web Auth (selected), ACL (ACL-WEB-REDIRECT), and Value (Registered Guest Portal (default)).

Create an authorization profile for guest access after web authentication.

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

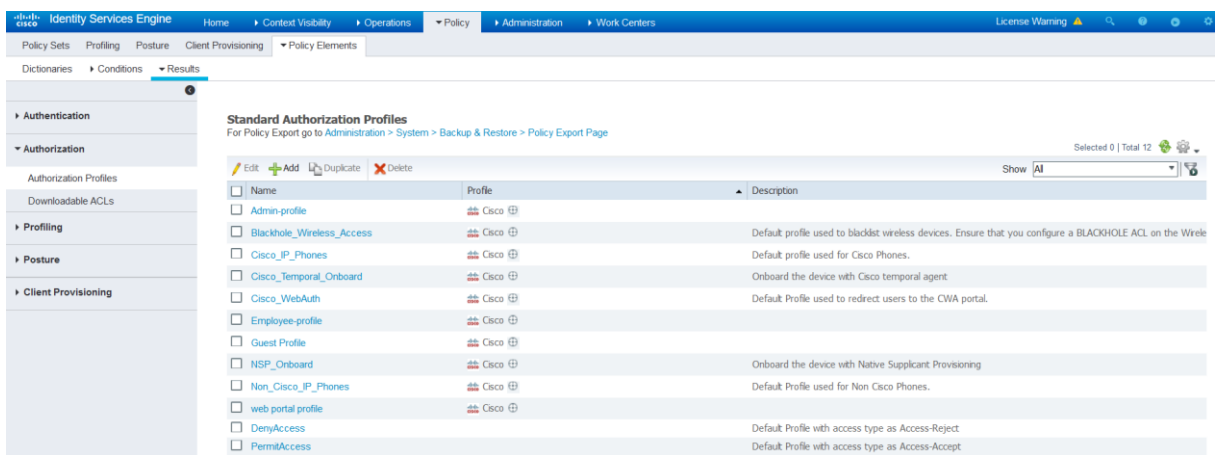
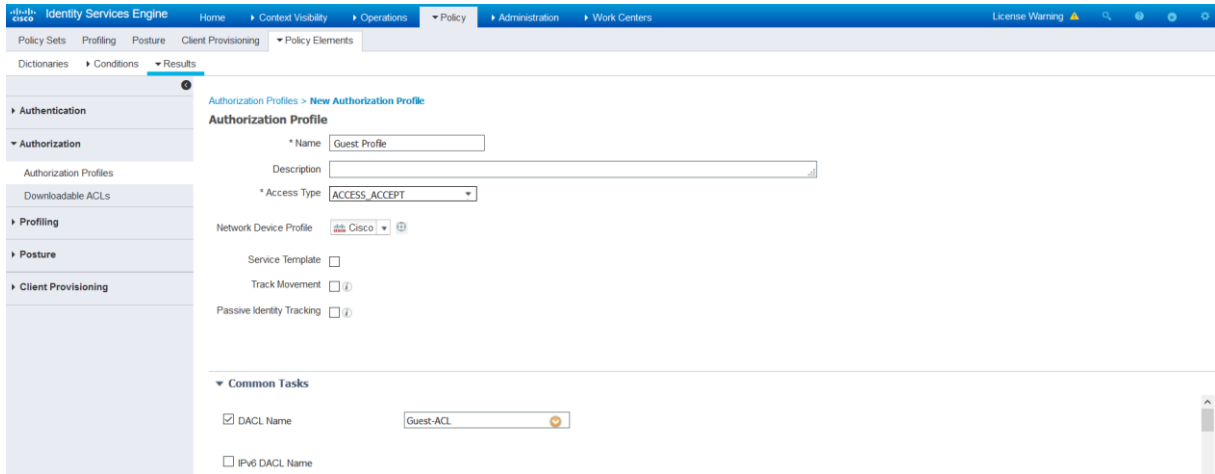
Configure these attributes:

Name: **Guest profile**

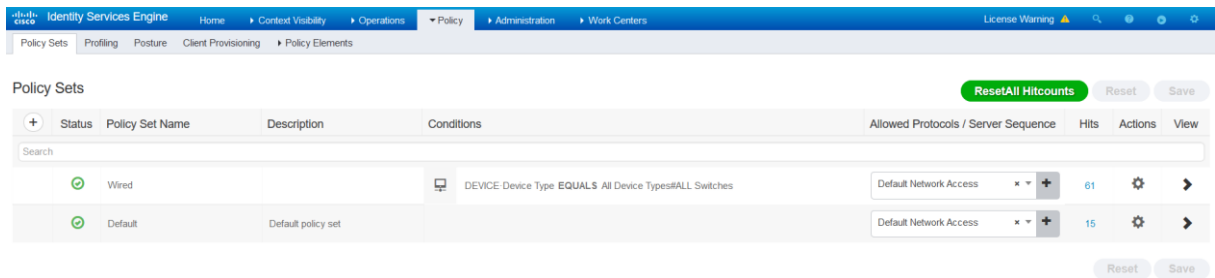
Access Type: **ACCESS_ACCEPT**

DACL: **Guest-ACL**.

Click **Submit**.



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



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

Cisco Identity Services Engine									
Policy Administration									
Wired									
DEVICE Device Type EQUALS All Device Types#ALL Switches									
Default Network Access									
61									
Authentication Policy (2)									
Authorization Policy - Local Exceptions									
Authorization Policy - Global Exceptions									
Authorization Policy (5)									
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions	
Search									
	✔	Employee AuthoZ	IdentityGroup Name EQUALS User Identity Groups Emp-Group		Employee-profile	Select from list	1		⚙️
	✔	Admin AuthoZ	IdentityGroup Name EQUALS User Identity Groups Admin-Group		Admin-profile	Select from list	11		⚙️
	✔	Jdoe AuthoZ	AND Radius User-Name EQUALS jdoe Radius NAS-Port-Id EQUALS FastEthernet0/1		PermitAccess	Select from list	1		⚙️
	✔	Jwhite AuthoZ	AND Radius User-Name EQUALS jwhite Radius NAS-Port-Id EQUALS FastEthernet0/2		PermitAccess	Select from list	1		⚙️
	✔	Default			DenyAccess	Select from list	4		⚙️

Cisco Identity Services Engine									
Policy Administration									
Wired									
DEVICE Device Type EQUALS All Device Types#ALL Switches									
Default Network Access									
61									
Authentication Policy (2)									
Authorization Policy - Local Exceptions									
Authorization Policy - Global Exceptions									
Authorization Policy (5)									
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions	
Search									
	✔	Employee AuthoZ	IdentityGroup Name EQUALS User Identity Groups Emp-Group		Employee-profile	Select from list	1		⚙️
	✔	Admin AuthoZ	IdentityGroup Name EQUALS User Identity Groups Admin-Group		Admin-profile	Select from list	11		⚙️
	✔	Jdoe AuthoZ	AND Radius User-Name EQUALS jdoe Radius NAS-Port-Id EQUALS FastEthernet0/1		PermitAccess	Select from list	1		⚙️
	✔	Jwhite AuthoZ	AND Radius User-Name EQUALS jwhite Radius NAS-Port-Id EQUALS FastEthernet0/2		PermitAccess	Select from list	1		⚙️
	✔	Default			web portal profile	Select from list	4		⚙️

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

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

Identity Services Engine									
Policy Elements									
Wired									
DEVICE Device Type EQUALS All Device Types ALL Switches									
Default Network Access									
61									
Authentication Policy (2)									
Authorization Policy - Local Exceptions									
Authorization Policy - Global Exceptions									
Authorization Policy (6)									
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions	
Search									
	+	Guest Access			Select from list	Select from list			
	+	Employee AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Emp-Group		Employee-profile	Select from list	1		
	+	Admin AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Admin-Group		Admin-profile	Select from list	11		
	+	Jdoe AuthoZ	AND Radius User-Name EQUALS jdoe Radius NAS-Port-Id EQUALS FastEthernet0/1		PermitAccess	Select from list	1		
	+	Jwhite AuthoZ	AND Radius User-Name EQUALS jwhite Radius NAS-Port-Id EQUALS FastEthernet0/2		PermitAccess	Select from list	1		

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

Conditions Studio

Library

Search by Name

BYOD_is_Registered	
Catalyst_Switch_Local_Web_Authenticat ion	
Compliance_Unknown_Devices	
Compliant_Devices	
EAP-MSCHAPv2	
EAP-TLS	
Guest_Flow	
MAC_in_SAN	
Network_Access_Authentication_Passed	
Non_Cisco_Profiled_Phones	

Editor

Click to add an attribute

Equals Attribute value

+ New AND OR

Close Use

Conditions Studio

Conditions Studio interface showing the Library and Editor panes. The Library pane lists various conditions, and the Editor pane shows the 'Guest_Flow' condition being edited, with options to Duplicate or Edit, and a '+ New AND OR' button.

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.

Screenshot of the Cisco Identity Services Engine (ISE) interface showing the Library and Editor panes. The Library pane lists various conditions, and the Editor pane shows the 'Network Access-UseCase' condition being edited, with options to Duplicate or Save, and a '+ New AND OR' button.

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

Status	Rule Name	Conditions	Results	Hits	Actions
On	Guest Access	Guest_Flow	Guest Profile		
On	Employee AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Emp-Group	Employee-profile	1	
On	Admin AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Admin-Group	Admin-profile	11	
On	Jdoe AuthoZ	AND Radius User-Name EQUALS jdoe Radius NAS-Port-Id EQUALS FastEthernet0/1	PermitAccess	1	
On	Jwhite AuthoZ	AND Radius User-Name EQUALS jwhite Radius NAS-Port-Id EQUALS FastEthernet0/2	PermitAccess	1	

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**).

Status	Rule Name	Conditions	Results	Hits	Actions
On	Guest Access	Guest_Flow	Guest Profile	0	
On	Employee AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Emp-Group	Employee-profile	1	
On	Admin AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Admin-Group	Admin-profile	11	
On	Jdoe AuthoZ	AND Radius User-Name EQUALS jdoe Radius NAS-Port-Id EQUALS FastEthernet0/1	PermitAccess	1	
On	Jwhite AuthoZ	AND Radius User-Name EQUALS jwhite Radius NAS-Port-Id EQUALS FastEthernet0/2	PermitAccess	1	
On	Default		web portal profile	4	

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**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Wired ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wired		DEVICE Device Type EQUALS All Device Types#ALL Switches	Default Network Access	61

▼ Authentication Policy (3)

+	Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1X for Wired		Wired_802.1X	Internal Users Options	19	⚙️
✎	MAB		Wired_MAB	Internal Endpoints Options		⚙️
✔	Default			DenyAccess Options	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.
Click **Save**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Wired ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wired		DEVICE Device Type EQUALS All Device Types#ALL Switches	Default Network Access	61

▼ Authentication Policy (3)

+	Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1X for Wired		Wired_802.1X	Internal Users Options	19	⚙️
✎	MAB		Wired_MAB	Internal Endpoints Options If Auth fail: REJECT If User not found: CONTINUE If Process fail: DROP		⚙️

The screenshot shows the Cisco ISE Policy Sets configuration for the 'Wired' policy set. The main table lists the policy set with a status of 'On' and 61 hits. Below it, the 'Authentication Policy (3)' section is expanded to show three rules:

Status	Rule Name	Conditions	Use	Hits	Actions
On	Dot1X for Wired	Wired_802.1X	Internal Users	19	Options
On	MAB	Wired_MAB	Internal Endpoints	0	Options
On	Default		DenyAccess	18	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.f29.b453** is authenticated with MAB and redirected to the web portal, the Authorization Profile **Web portal profile** is applied. Click **Authentication Detail Report**.

The screenshot shows the Cisco ISE Live Logs interface. At the top, there are summary statistics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (4), and Repeat Counter (2). Below this is a table of live log entries:

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
Nov 12, 2019 11:37:12.323 PM	On		2	008C FA 29 B4 53	008C FA 29 B4 53	Unknown	Wired >> MAB	Wired >> De...	web portal pr...	192.168.1.2	
Nov 12, 2019 11:37:11.299 PM	On			#ACSACL#IP-We...							SW-1
Nov 12, 2019 11:36:17.302 PM	On			#ACSACL#IP-We...							SW-1
Nov 12, 2019 11:36:17.279 PM	On			008C FA 29 B4 53	008C FA 29 B4 53	Unknown	Wired >> MAB	Wired >> De...	web portal pr...		SW-1
Nov 12, 2019 11:33:41.339 PM	On			#ACSACL#IP-We...							SW-1
Nov 12, 2019 11:33:41.309 PM	On			008C FA 29 B4 53	008C FA 29 B4 53	Unknown	Wired >> MAB	Wired >> De...	web portal pr...		SW-1
Nov 12, 2019 11:32:10.108 PM	Off			#INVALID	008C FA 29 B4 53		Wired >> Do...	Wired			SW-1
Nov 12, 2019 11:26:49.310 PM	On			#ACSACL#IP-AC...							SW-1
Nov 12, 2019 11:26:49.279 PM	On			administrator	008C 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 <https://ISE.lab.local/...../cwa>, cwa means **Centralized Web Authentication**, the second attribute is a Dacl called **Web-Auth-ACL**.

Overview

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
License Types	Base license consumed

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

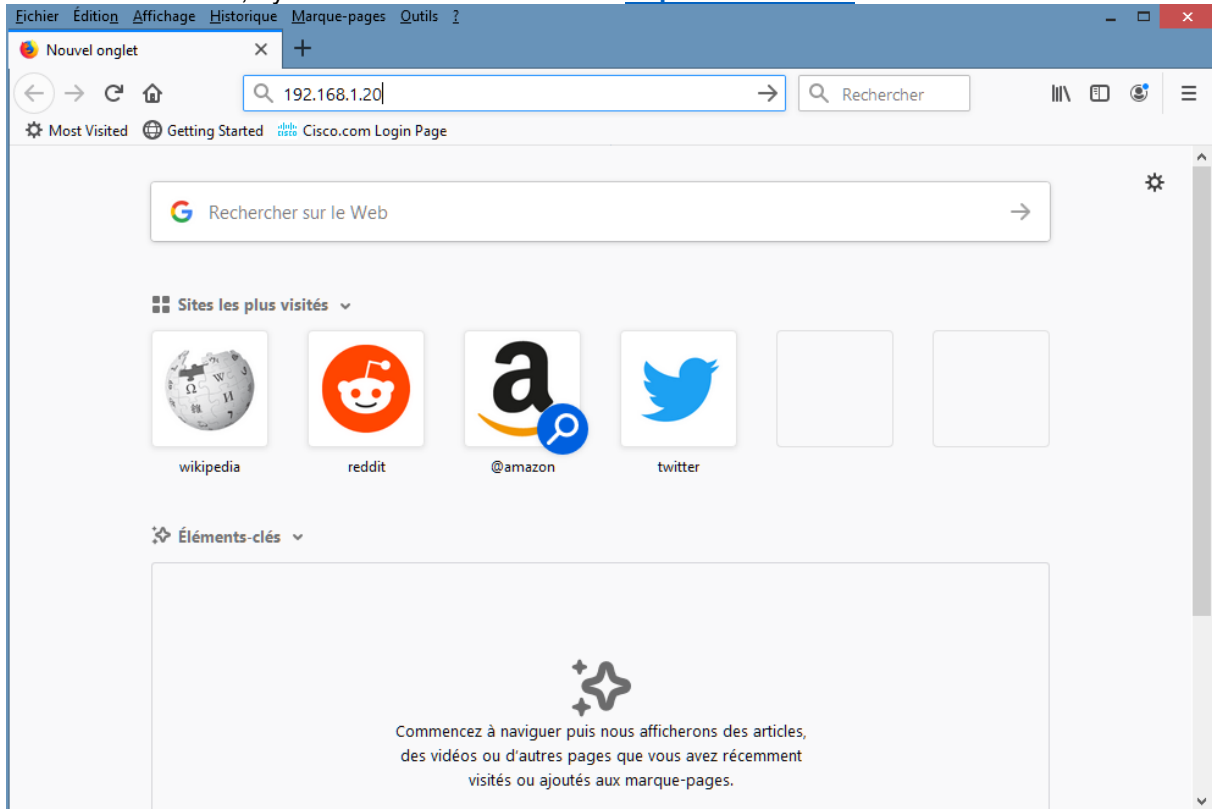
```
SW-1#sh ip access-lists | s Web-Auth-ACL
Extended IP access list xACSACLx-IP-web-Auth-ACL-5dcb3583 (per-user)
 10 permit ip any host 192.168.1.254
 20 permit udp any any eq bootps
 30 permit udp any eq bootpc any
 40 permit icmp any any
SW-1#
```

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**.

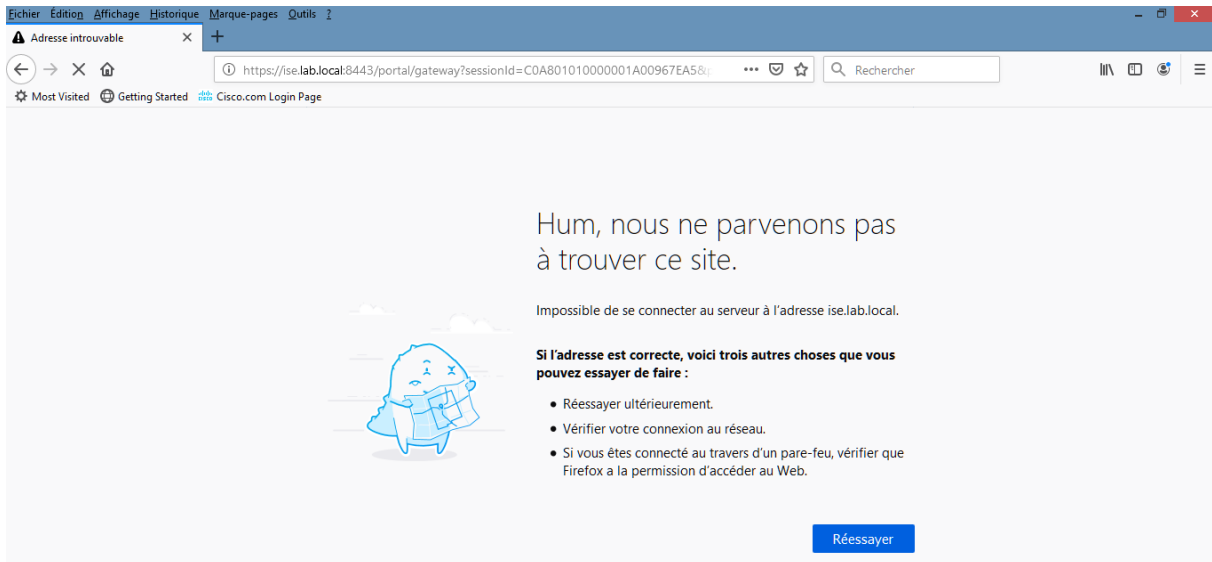
```
SW-1#sho auth sess int f0/3
  Interface: FastEthernet0/3
  MAC Address: 008c.f29.b453
  IP Address: 192.168.1.2
  User-Name: 00-8C-FA-29-B4-53
  Status: Authz Success
  Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  ACS ACL: XACSACLx-IP-Web-Auth-ACL-5dcb3583
  URL Redirect ACL: ACL-WEB-REDIRECT
  URL Redirect: https://ISE.lab.local:8443/portal/gateway?sessionId=C0A801010000001A00967EA5&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa&token=f31c2c18b71781918c113630742b85e
  URL Redirect: https://ISE.lab.local:8443/portal/gateway?sessionId=C0A801010000001A00967EA5&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa&token=7169f2d6bbd75688cf96309c7fe6cb3
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: C0A801010000001A00967EA5
  Acct Session ID: 0x0000001F
  Handle: 0x6F00001B

Runnable methods list:
  Method State
  mab Authz Success
  dot1x Not run
SW-1#
```

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

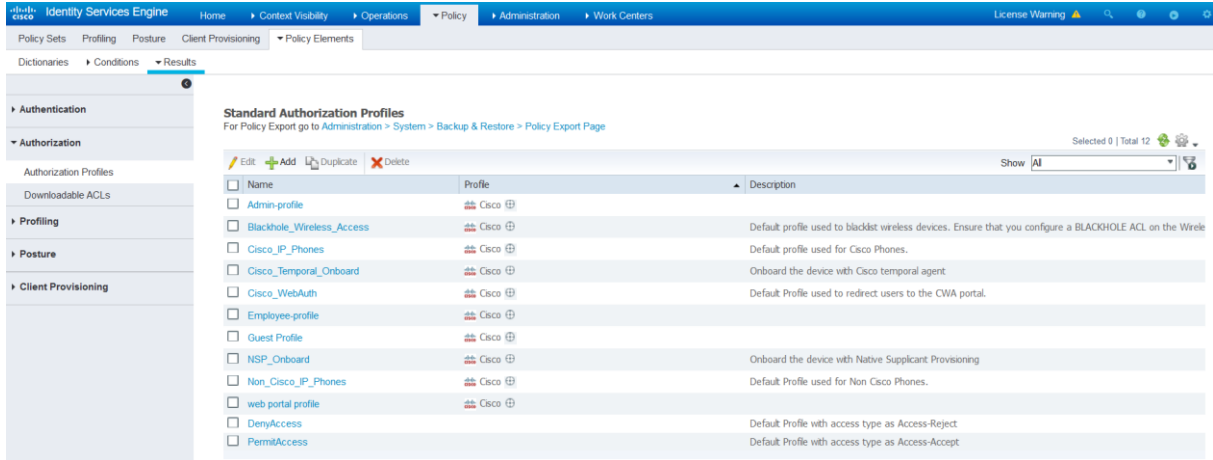


The **Guest PC** is redirected to the URL Redirect <https://ISE.lab.local/...../cwa>, but the PC fails the DNS Resolution.



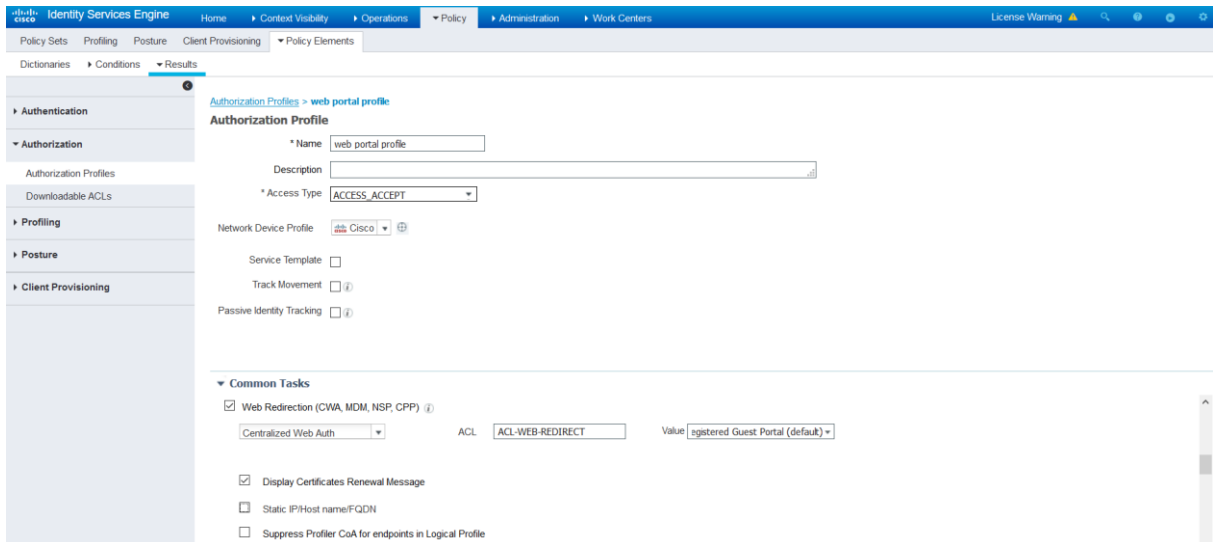
Since we don't have a DNS server to resolve the URL Redirect to the IP address **192.168.1.254** of ISE, we can override this by instructing the ISE to replace the hostname **ISE.lab.local** by its IP address in the Authorization Profile of Web Redirection, so edit the Authorization Profile Web portal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

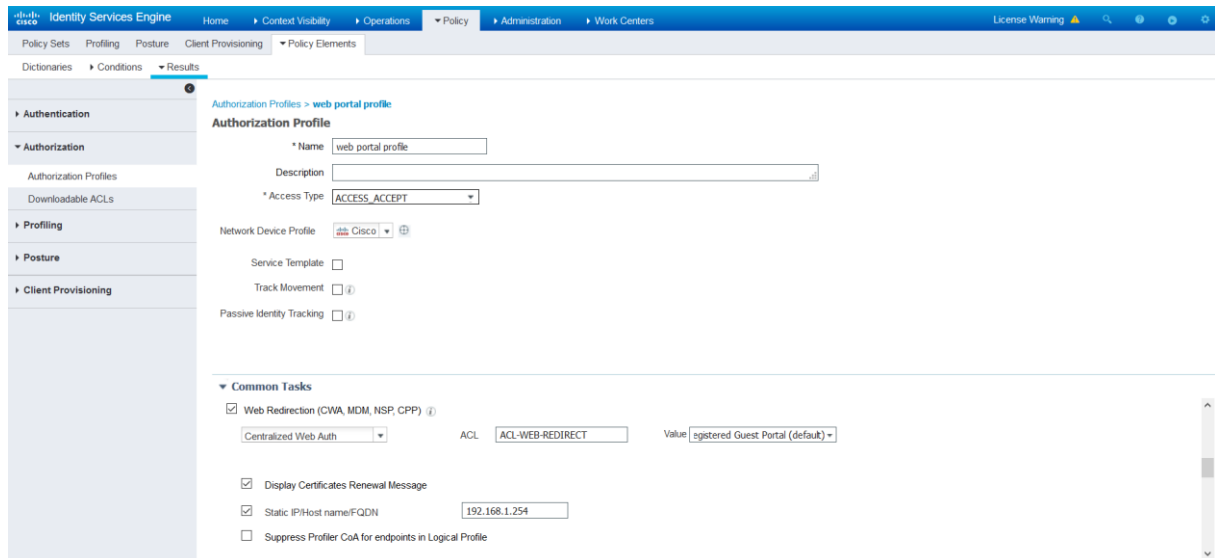
Go to **Policy > Policy Elements > Results**, expand **Authorization** in the Left Menu. Expand **Authorization Profiles**. Click on the Authorization profile **Web portal profile**. Scroll to **Web Redirection (CWA, DRW, MDM, NSP, CPP)**.



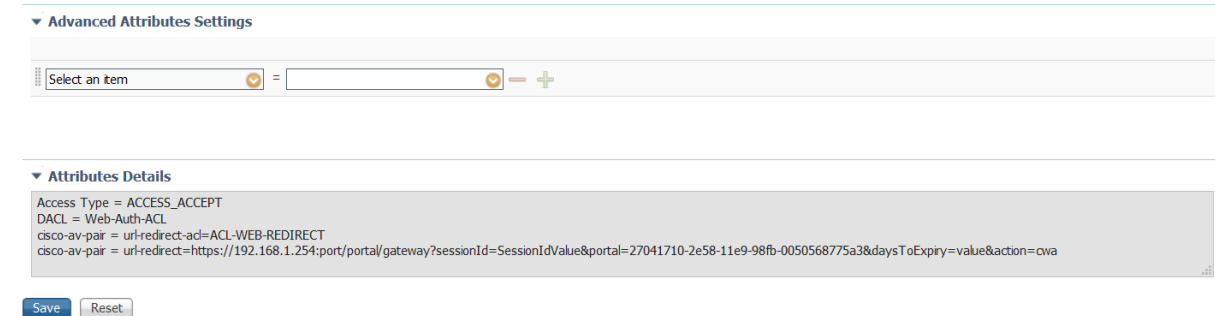
Place a check mark in the **Static IP/Host name FQDN** box. Enter the IP address of the ISE **192.168.1.254**.

Click **Save**.





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**.



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.f429.b453) on Interface Fa0/3 AuditSessionID COA801010000001B00A0CA70
*Mar 1 02:55:38.138: %MAB-5-SUCCESS: Authentication successful for client (008c.f429.b453) on Interface Fa0/3 AuditSessionID COA801010000001B00A0CA70
*Mar 1 02:55:38.138: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (008c.f429.b453) on Interface Fa0/3 AuditSessionID COA801010000001B00A0CA70
*Mar 1 02:55:39.169: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (008c.f429.b453) on Interface Fa0/3 AuditSessionID COA801010000001B00A0CA70
*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.lab.local**.

```

SW-1#sho auth sess int 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
  Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  ACS ACL: xACSACLX-IP-Web-Auth-ACL-5dcb3583
  URL Redirect ACL: ACL-WEB-REDIRECT
  URL Redirect: https://ISE.lab.local:8443/portal/gateway?sessionId=COA801010000001B00A0CA70&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa
&token=a3481c730c6470cb00f1cfa4575c5a2
  URL Redirect: https://192.168.1.254:8443/portal/gateway?sessionId=COA801010000001B00A0CA70&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa
&token=d4511ff560e8025668365afb2c6a5f01
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: COA801010000001B00A0CA70
  Acct Session ID: 0x00000020
  Handle: 0xEB00001C

Runnable methods list:
  Method      State
  mab         Authz Success
  dot1x       Not run

```

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**.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Profiles	IP Address	Network Dev
Nov 12, 2019 11:48:27.349 PM	●		3	008C-FA-29-B4-53	008C-FA-29-B4-53	Unknown	Wired >> MAB	Wired >> De...	web portal profile	192.168.1.2	SW-1
Nov 12, 2019 11:48:26.333 PM	✓			#ACSACL#-IP-We...							SW-1
Nov 12, 2019 11:37:11.299 PM	✓			#ACSACL#-IP-We...							SW-1
Nov 12, 2019 11:36:17.302 PM	✓			#ACSACL#-IP-We...							SW-1
Nov 12, 2019 11:36:17.279 PM	✓			008C-FA-29-B4-53	008C-FA-29-B4-53	Unknown	Wired >> MAB	Wired >> De...	web portal profile		SW-1
Nov 12, 2019 11:33:41.339 PM	✓			#ACSACL#-IP-We...							SW-1
Nov 12, 2019 11:33:41.309 PM	✓			008C-FA-29-B4-53	008C-FA-29-B4-53	Unknown	Wired >> MAB	Wired >> De...	web portal profile		SW-1
Nov 12, 2019 11:32:10.108 PM	✗			INVALID	008C-FA-29-B4-53		Wired >> Do...	Wired			SW-1
Nov 12, 2019 11:26:49.310 PM	✓			#ACSACL#-IP-AC...							SW-1
Nov 12, 2019 11:26:49.279 PM	✓			administrator	008C-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

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