Cisco Support Community Expert Series Webcast

Integrating Cisco Cloud Web Security with ASA

Maite Cadenas
Service Deployment Manager

June 24, 2014

Polling Question 1

Do you have CWS (Cloud Web Security) deployed in your environment?

a. I have CWS and am using ASA Connector to redirect the web traffic

b. I have CWS but not using ASA Connector to redirect the web traffic

c. I have CWS and am planning to use ASA Connector to redirect the web traffic

d. I have CWS and using ASA Connector and other Connector types (WSA Connector/ISR Connector/standalone Connector/AnyConnect Web Security/others)

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Cisco Support Community Expert Series Webcast

Integrating Cisco Cloud Web Security with ASA

Maite Cadenas

Service Deployment Manager

June 24, 2014

Agenda

- Introduction to Cloud Web Security (CWS)
- Preparation for CWS ASA deployment
- Deploying CWS on ASA
- Verifications commands
- Best Practices
- Demo

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Introduction to Cloud Web Security (CWS)

- What is CWS
- Value of CWS
- Cloud connection methods

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Introduction

Disruptions comes in many forms…

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

CWS (Cloud Web Security)

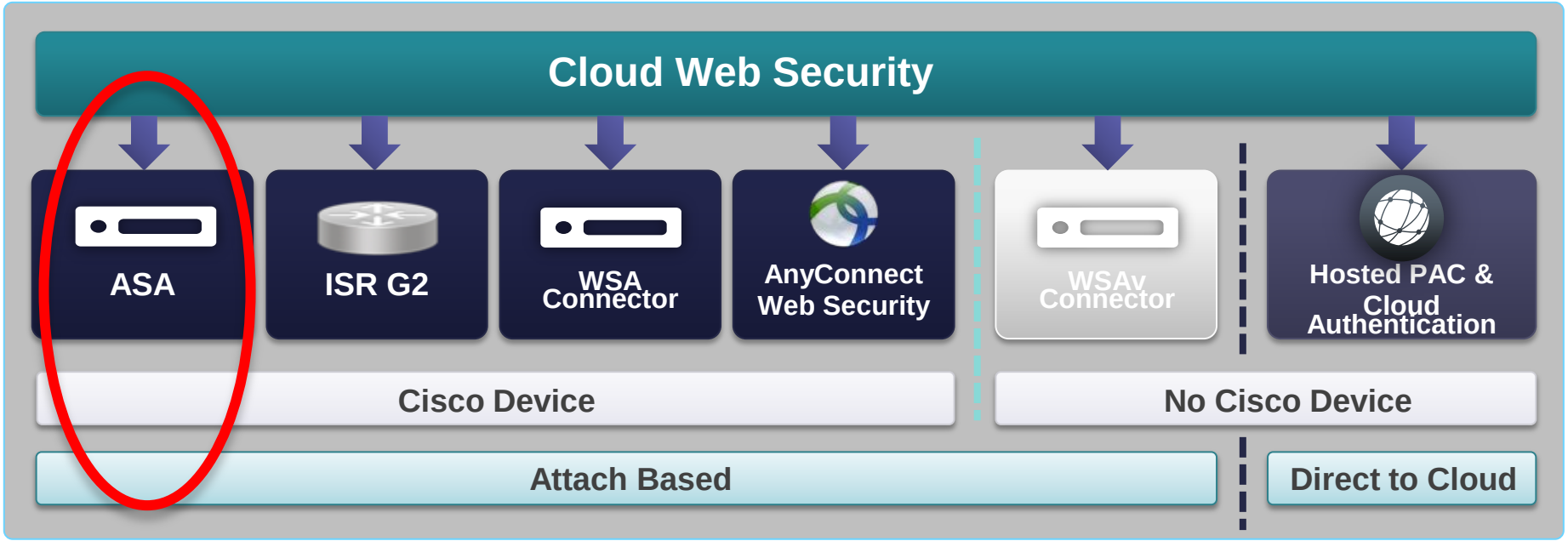
- What is it: A Cloud Based Premium Service
  - Real Time Scanning of HTTP/S web content
  - Robust, fast, scalable and reliable global data centre infrastructure
  - Flexible deployment options via Cisco attach model and direct to cloud
  - Support for roaming users
  - Centrally managed granular web filtering policies, with web 2.0 visibility and control
  - Close to real-time reporting with cloud retention, as part of the standard offering

- Value:
  - Strong protection
  - Complete control
  - Investment value

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Cloud Connection Methods

Use your existing Cisco asset to leverage CWS



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Preparation for CWS ASA deployment

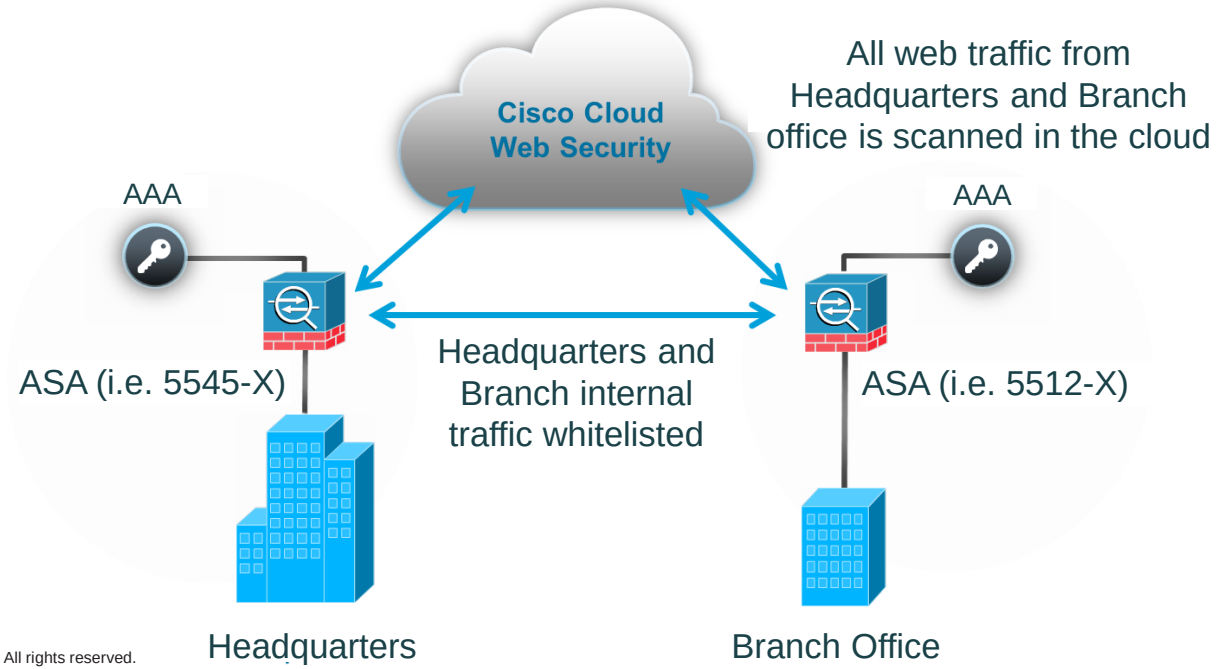
- Understanding CWS with ASA Connector
- Characteristics and limitations
- What you need before starting the deployment
- User granularity methods on ASA

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Understanding CWS with ASA Connector

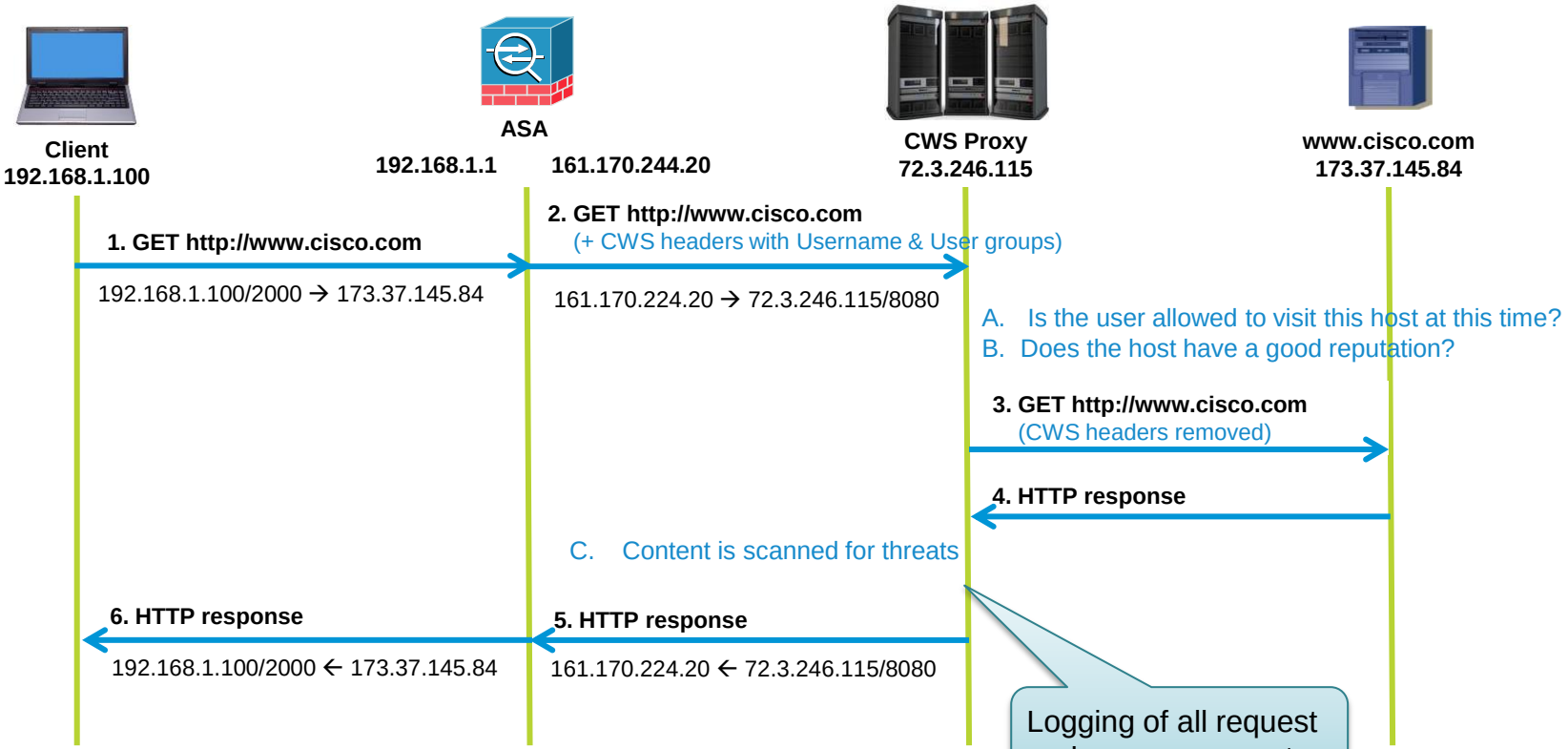
Transparent redirection to the cloud with Identity

Breaking out locally. No need to backhaul traffic to HQ



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Understanding CWS with ASA Connector – Packet Flow



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Characteristics of ASA Deployment

- The ASA Connector feature is available from v9.0, and runs on all ASA models
- Can be used for transparent deployment in HQ and branch offices
- Single and Multiple Context Modes are supported for HTTP and HTTPS traffic
- User granularity provided from AD via IDFW
- Automated fail-over to secondary data centre
- Zero touch on end point devices: No requirement to install software, or make any browser changes on end users' machines
- Feature called: Scansafe on ASA
- Licensing:
  - No need for special license on ASA (K8 → K9 free upgrade)
  - CWS licensing on a per-user or per bandwidth basis, so not tied to number of devices

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

What you need before starting the deployment

- Access to ScanCenter portal for managing CWS service
- CWS proxies (Towers) details
- Be able to authenticate your traffic with CWS service
- Choose which traffic to send to CWS service
- Decide if you want to use user granularity

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Getting Proxies and Access to the ScanCenter Portal

- When an account is provisioned, email will be sent with:
  - Primary proxy
  - Backup Proxy
  - URL to access the Scan Center portal: https://scancenter.scansafe.com/portal/admin/login.jsp
  - Username/password
- To get an account provisioned:
  - Place an order
  - Request an evaluation

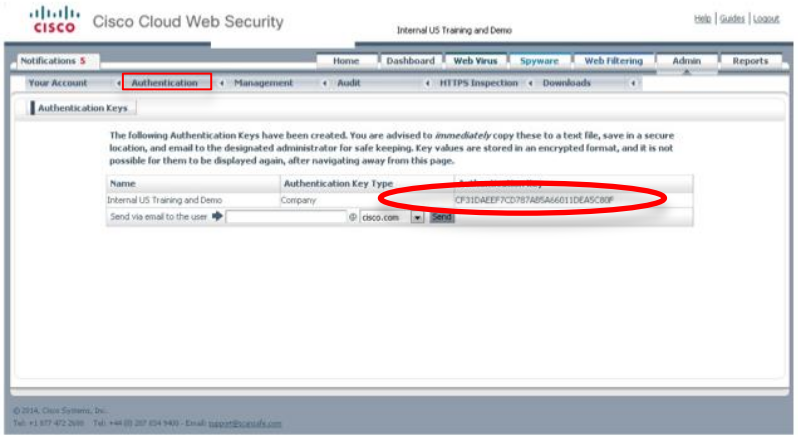
© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Authenticating Traffic (Authentication Keys)

Each ASA must use an Authentication Key → Generated in the ScanCenter portal

2 types:

Company Key	Group Key
1 key per portal	1 key per group 1 portal can have multiple groups
Authenticates traffic for multiple ASAs	Authenticates traffic for 1 ASA Possibility of creating 1 policy per ASA

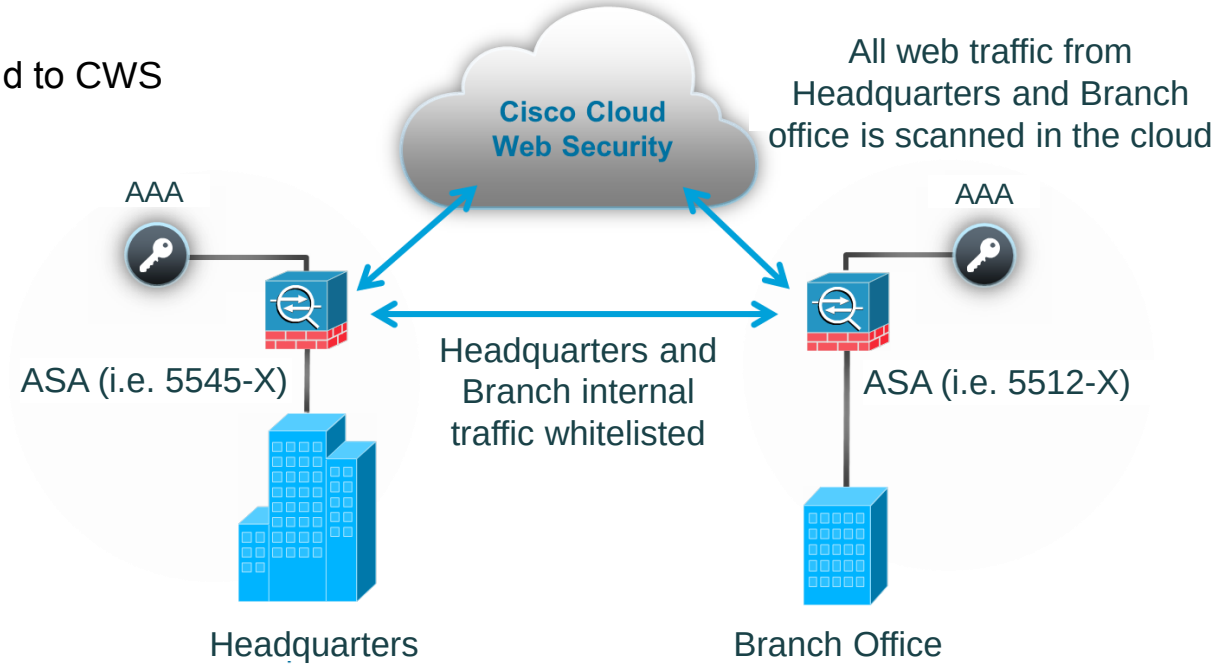


TIP: You can send the authentication key by email. Once it is generated, only the last 4 characters will be visible

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Choosing Which Traffic to Send to CWS

- HTTP and HTTPS traffic
- Whitelist:
  - Any traffic you don't want to send to CWS
  - Any internal traffic
  - VPN traffic



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

User Granularity (User Authentication Methods)

User Authentication methods on ASA

	AAA rules	IDFW (Identity Firewall)	Default username and group
User experience	Pop-up	Transparent	Transparent
Information provided	Username only. If configured, uses the default group	Username and group	Default username and group for all users
Characteristics	AAA server or local database	Integration with AD	Manually configured on the ASA

Alternative: SAML or EasyID (Cookie based)

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

ASA Sizing with CWS

Small Office and Branch Office				
ASA Platform	**5505**	**5510**	**5512-X**	**5515-X**
Maximum CWS Users	25	75	2,000	3,000

Internet Edge						
ASA Platform	**5520**	**5525-X**	**5540**	**5545-X**	**5550**	**5555-X**
Maximum CWS Users	300	4,000	1,000	5,000	2,000	6,000

Enterprise Data Centre				
ASA Platform	**5585-X SSP10**	**5585-X SSP20**	**5585-X SSP30**	**5585-X SSP40**
Maximum CWS Users	7,500	7,500	7,500	7,500

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Limitations

- With other features:
  - Supported in routed mode only
  - Does not support IPv6
  - CWS is not supported with extended PAT
  - CWS is not supported with ASA clustering
  - CWS not supported on ASA-SM
- Whitelisting on ASA
  - Supported by IP, FQDN and user
  - CSCue62571 ASA/ScanSafe: ENH: Need support to whitelist based on regex (Enhancement request)
- User granularity (CDA Limitations)
  - 1 user can be mapped to a maximum of 8 different IPs
  - 1 IP cannot be mapped to more than 1 user (1 IP – 1 user mapping)
- Other:
  - Terminal access (RDP, VNC): recommend using explicit proxy instead of transparent proxy
  - Citrix: Need to enable True IP for each user (Citrix feature)

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Deploying CWS on ASA

Configuration without user granularity

Whitelisting traffic

Adding User Granularity (IDFW (CDA))

Considerations in Multiple Context deployment

Configuring policies in the ScanCenter Portal

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Polling Question 2

Do you find configuring ASA Connector and CDA integration to be a complicated task?

a. Yes, I do, both ASA Connector and CDA integration

b. No, I do not, both are straight forward configuration

c. ASA Connector is simple, however CDA integration is complicated

d. ASA Connector is complicated, however CDA integration is simple

e. I am yet to find out

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Configure CWS on ASA without user granularity

Make sure you run version 9.x or above and K9 license applied

1. Configure CWS settings:

```
scansafe general-options
server primary fqdn proxyXX.scansafe.net port 8080
server backup fqdn proxyYY.scansafe.net port 8080
retry-count 5
license <Authentication key>
```

TIP: Domain Name Service (DNS) is required to resolve the Fully Qualified Domain Name (FQDN) of a Cisco CWS web services proxy server

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Configure CWS on ASA without user granularity

2. Configure CWS policy and apply it

```
access-list webcwsacl extended permit tcp any any eq www
access-list httpscwsacl extended permit tcp any any eq https
```

htt p / https

```
class-map cmap-http
match access-list webcwsacl
```

htt p

```
class-map cmap-https
match access-list httpscwsacl
```

https

```
policy-map type inspect scansafe http-pmap
parameters
default group asahttptraffic #optional
http
```

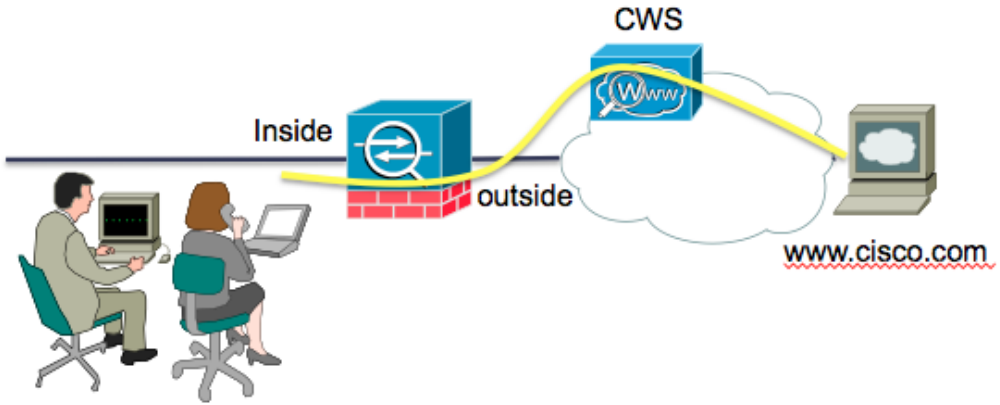
htt p

```
policy-map type inspect scansafe https-pmap
parameters
default group asahttpstraffic #optional
https
```

https

```
policy-map pmap-webtraffic
class cmap-http
inspect scansafe http-pmap fail-open
class cmap-https
inspect scansafe https-pmap fail-open
```

```
service-policy pmap-webtraffic interface inside
```



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

HTTPS Inspection on ScanCenter Portal

HTTPS traffic requires https inspection enabled in the portal to be able to scan it. Steps:

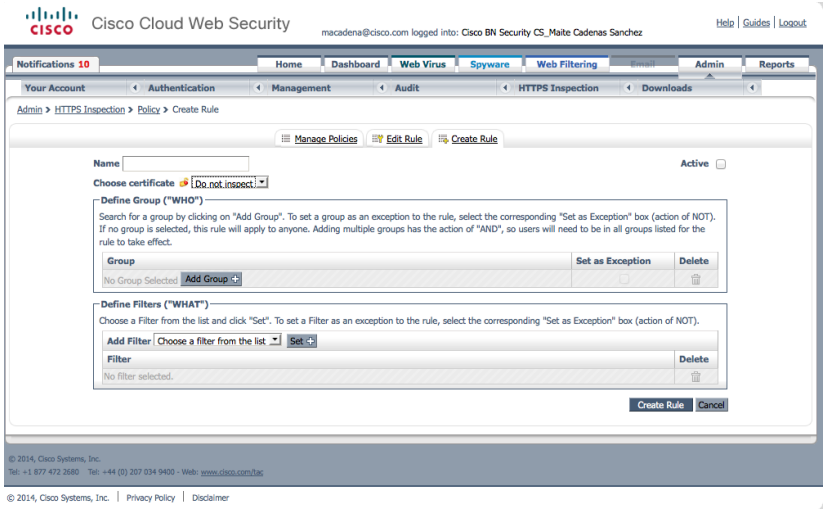
Create a certificate in the portal

Import certificate in the trusted root certificates store of the users

Configure filter and policy for https inspection in the portal

TIP: Exclude from HTTPS inspection sensitive categories:

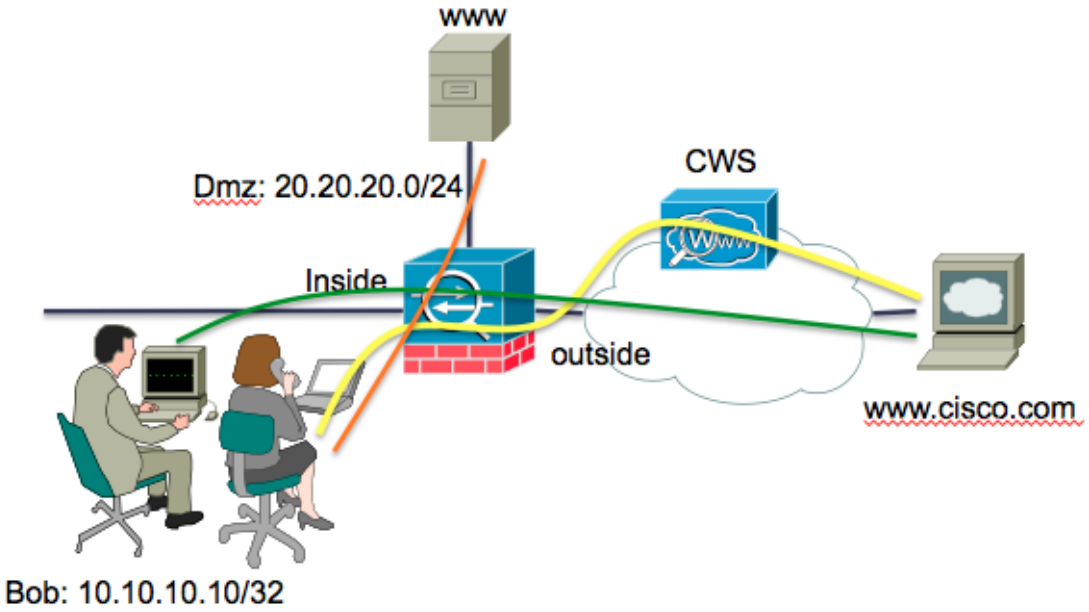
- Business and Industry
- Finance
- Government and Law
- Health and Nutrition
- SaaS and B2Bt



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Whitelist Traffic

By IP or fqdn using access-list:




```
object network DMZNetwork
 subnet 20.20.20.0 255.255.255.0
object network www.fifa.com
 fqdn www.fifa.com

object-group network WhitelistCWS
 network-object object DMZNetwork
 network-object object www.fifa.com

access-list webcwsacl extended deny tcp any object-group WhitelistCWS eq www
access-list webcwsacl extended deny tcp host 10.10.10.10 any eq www
access-list webcwsacl extended permit tcp any any eq www

access-list httpscwsacl extended deny tcp any object-group WhitelistCWS eq https
access-list httpscwsacl extended deny tcp host 10.10.10.10 any eq https
access-list httpscwsacl extended permit tcp any any eq https
```

http

https

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Adding user granularity (IDFW)

- Understanding IDFW
- Steps to configure IDFW
- Additional options

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

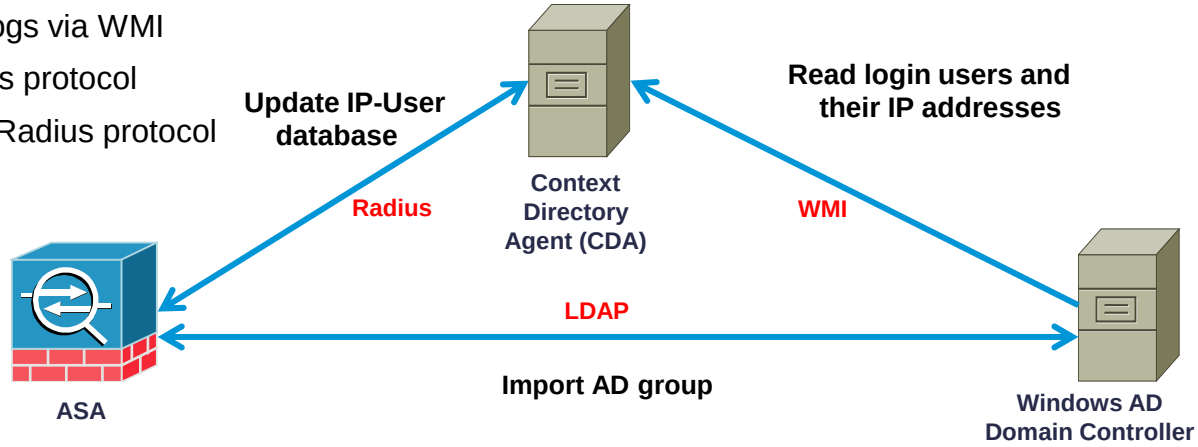
IDFW User Authentication with ASA Connector

Off-box process via Context Directory Agent (CDA)

- ASA Firewall:
  - Download AD group from AD domain controller via LDAP protocol
  - Receive IP-user mappings from CDA via Radius protocol
  - Report IP-user mappings from VPN/Cut-through-proxy to CDA.
  - Apply policies (ACL, MPF) based on user identity.

- Context Directory Agent (CDA):
  - Monitor AD domain controllers' security logs via WMI
  - Push IP-user mappings to ASA via Radius protocol
  - Receive IP-user mappings from ASA via Radius protocol

- AD Domain controller:
  - Authenticate users
  - Generate user logon security logs
  - Reply ASA's LDAP query for user/group information



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Adding user granularity (IDFW)

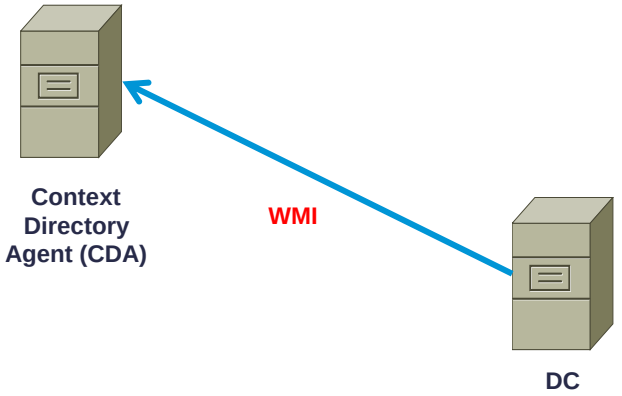
1) Install Context Directory Agent (CDA) latest version, currently 1.0 patch 2

Download available at www.cisco.com

2) Make sure the AD meets all the requirements for successful connection with CDA. (CDA install guide: http://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10/cda_install.html)

Goal: CDA needs to get the successful login information to get the user-to-IP mappings.

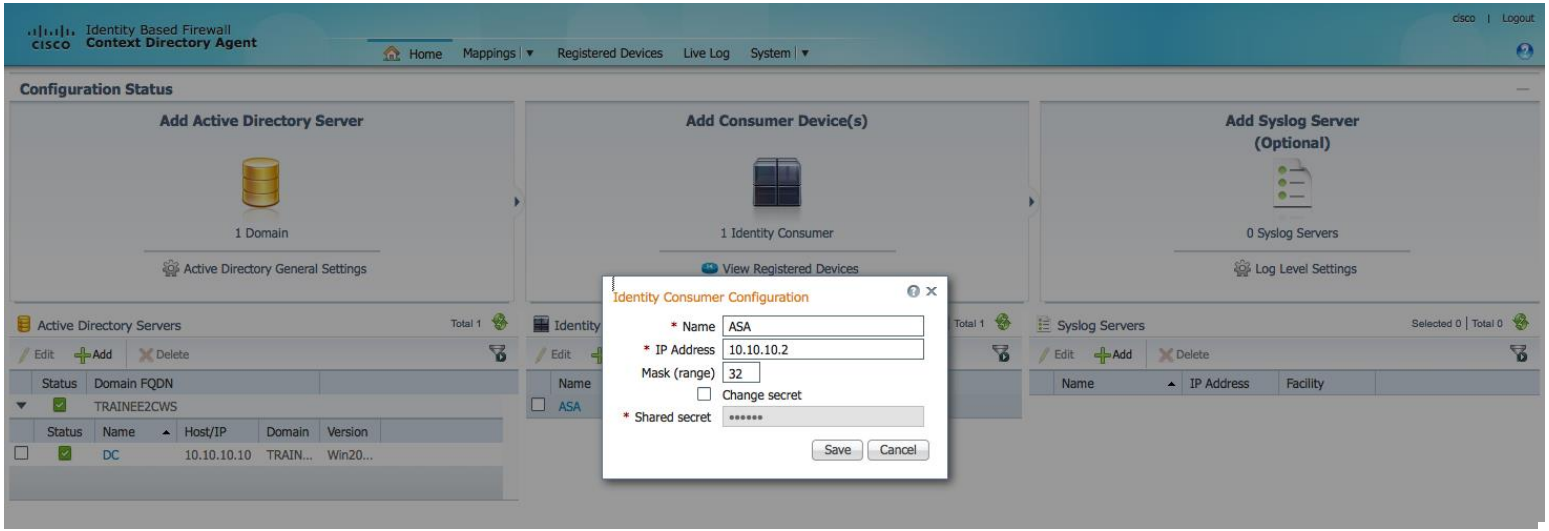
TIP: CDA is the replacement for Ad Agent which is End of Download since last 31st July 2013

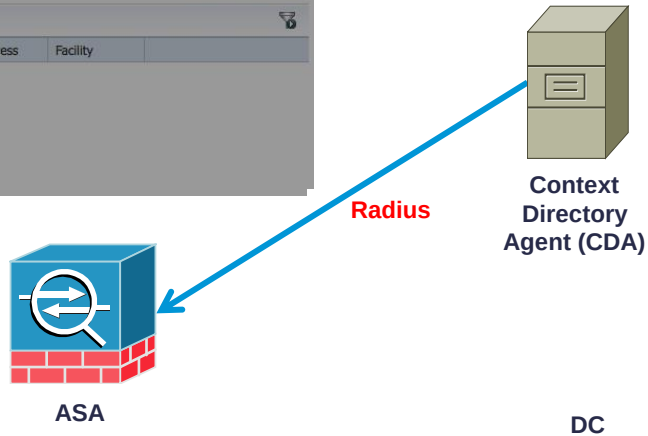


© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Adding user granularity (IDFW)

3) CDA: Configure Active Directory Senders and Identity Consumer (ASA)





© 2013-2014 Cisco and/or its affiliates. All rights reserved.

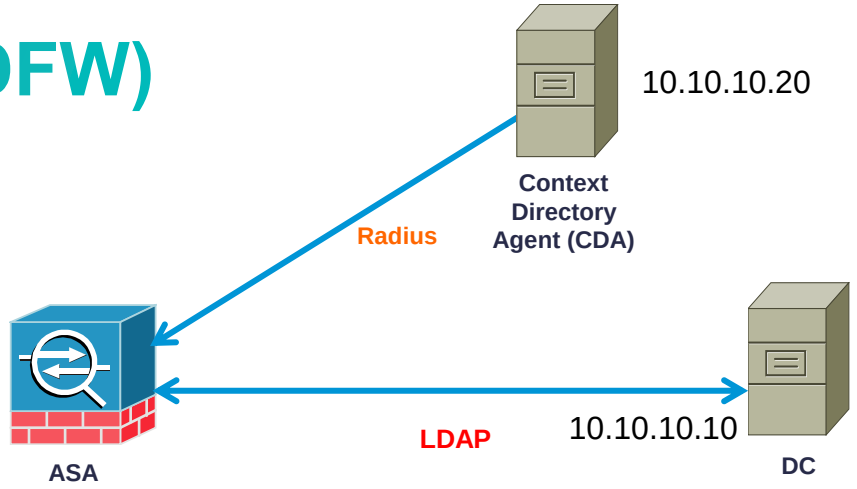
Adding user granularity (IDFW)

4) Configuration on ASA:

```
aaa-server AD protocol ldap
aaa-server AD (inside2) host 10.10.10.10
 server-port 389
 ldap-base-dn DC=trainee2cws,DC=local
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn
CN=Administrator,CN=Users,DC=trainee2cws,DC=local
 server-type microsoft

aaa-server CDA protocol radius
 ad-agent-mode
aaa-server CDA (inside2) host 10.10.10.20
 key ***** #key configured in CDA
```

TIP: Domain must match the NetBIOS name




```
user-identity domain TRAINEE2CWS aaa-server AD
user-identity default-domain TRAINEE2CWS
user-identity action netbios-response-fail remove-user-ip
user-identity ad-agent active-user-database full-download
user-identity ad-agent aaa-server CDA
user-identity user-not-found enable
user-identity monitor user-group TRAINEE2CWS\\Users
user-identity monitor user-group TRAINEE2CWS\\Group1
```

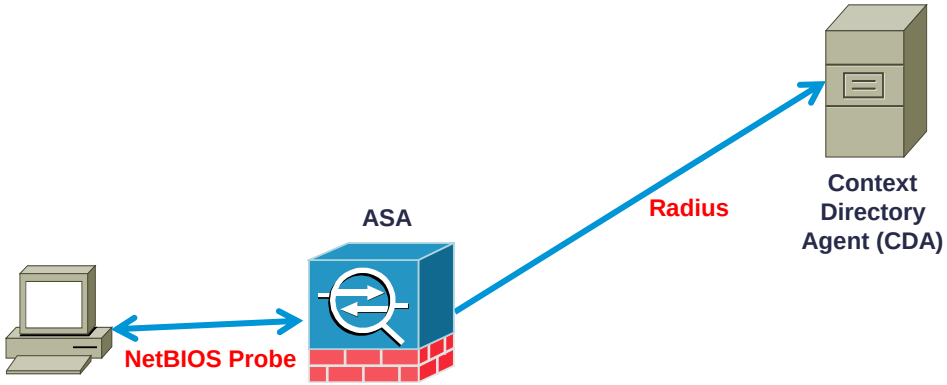
© 2013-2014 Cisco and/or its affiliates. All rights reserved.

User granularity (IDFW) additional options

Possibility to match traffic to be sent to CWS based on users or groups

Whitelisting per user available

TIP: If you lose user granularity after 5 minutes add the following commands on ASA:
---
no user-identity logout-probe netbios local-system probe-time minutes 15 retry-interval seconds 3 retry-count 3 match-any
  no user-identity action mac-address-mismatch remove-user-ip
  no user-identity action netbios-response-fail remove-user-ip
---



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Multiple Context Deployment (Considerations)

System context:

- Define CWS proxies
- Which context the CWS is enabled
- Add unique authentication key per context (optional)

Admin context:

Make sure there is route to reach CWS towers

Context running CWS

Define the policy map and whitelisting

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Configuring policies in the ScanCenter Portal

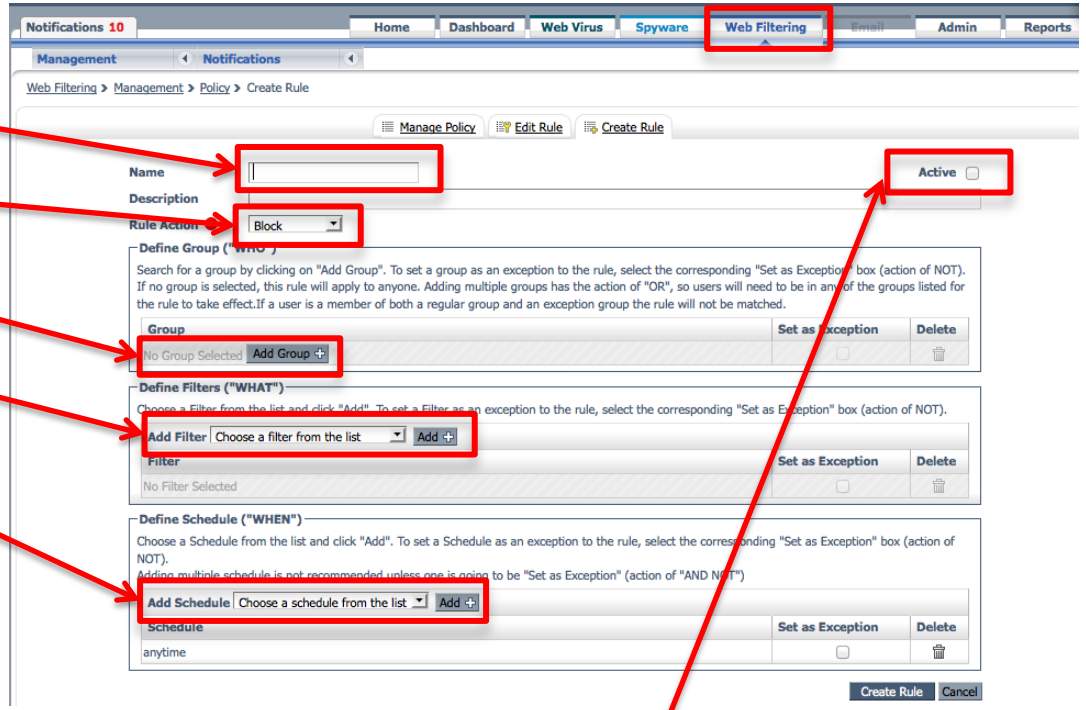
Policy Name

Action taken

Who: Group

What: Filter

When: Schedule

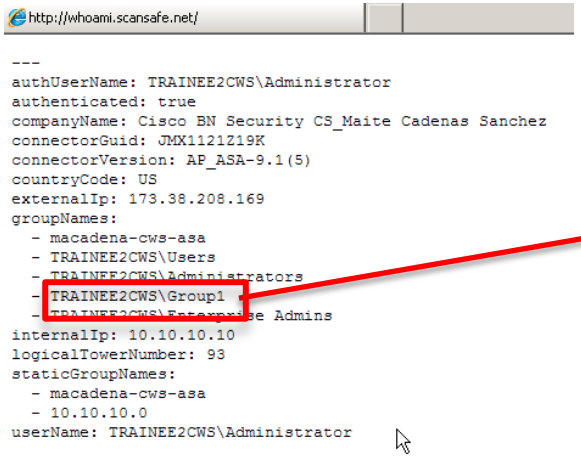


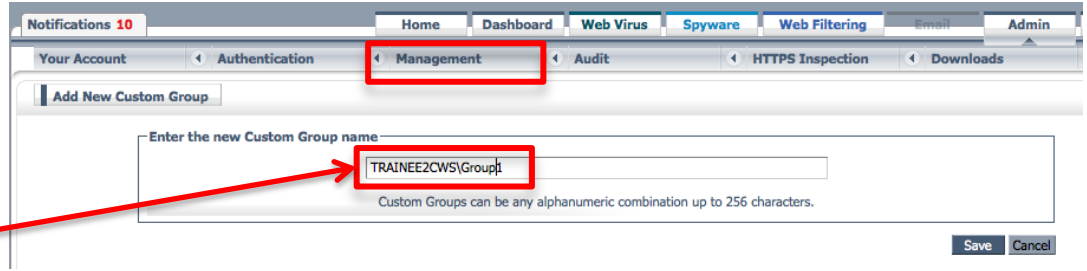
Activate the rule

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Configuring policies in the Scancenter Portal

Group: Needs to match with whoami.scansafe.net output





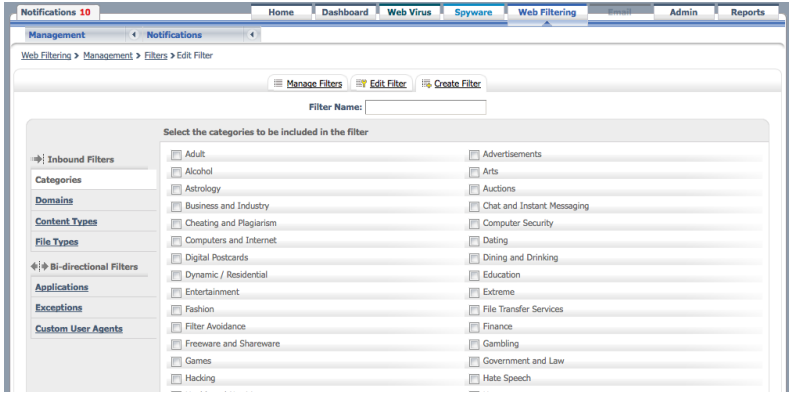
TIP: Besides it is an Active Directory group, you need to add it as a CUSTOM GROUP due to the syntax

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Configuring policies in the ScanCenter Portal

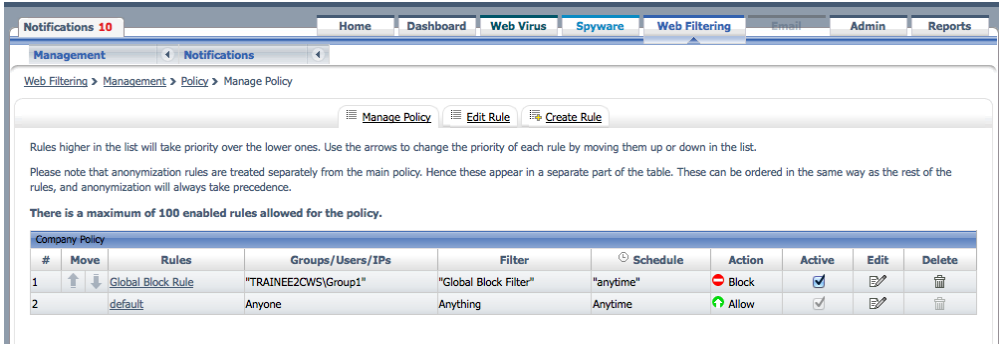
Filter:

Select the conditions to match for the action you want to apply in the policy



Policies:

Are applied from top to bottom



© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Polling Question 3

Do you use CLI or ASDM to configure ASA Connector?

a. CLI

b. ASDM

c. Both

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Verifications

- On User's Browser:
  - whoami.scansafe.net
  - policytrace.scancenter.net
- On ASA:
  - CWS service
    - Show scansafe server
    - Show scansafe statistics
  - IDFW service (user granularity)
    - Show user-identity ad-agent
    - Show user-identity user active list

TIP:
To test connectivity to the towers, telnet to towers on port 8080 or from ASA use TCP ping. ICMP protocol is blocked in the towers

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Best Practices

- While deploying: Whitelist everyone except the test machine. Once testing is completed successfully, rollout the rest.
- Recommendations: 9.1.5 or 9.2.1 to include fix for CSCul47395: ASA should allow out-of-order traffic through normalizer for ScanSafe (better performance).
- ASA-CX and CWS: Make sure that traffic to CWS is whitelisted from ASA-CX, otherwise ASA-CX has precedence.
- Exception “scansafe.com” from HTTPS inspection in the ScanCenter portal to avoid blocking yourself from accessing it.

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

DEMO

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Thank you for Your Time!

Please take a moment to complete the evaluation

Thank you.