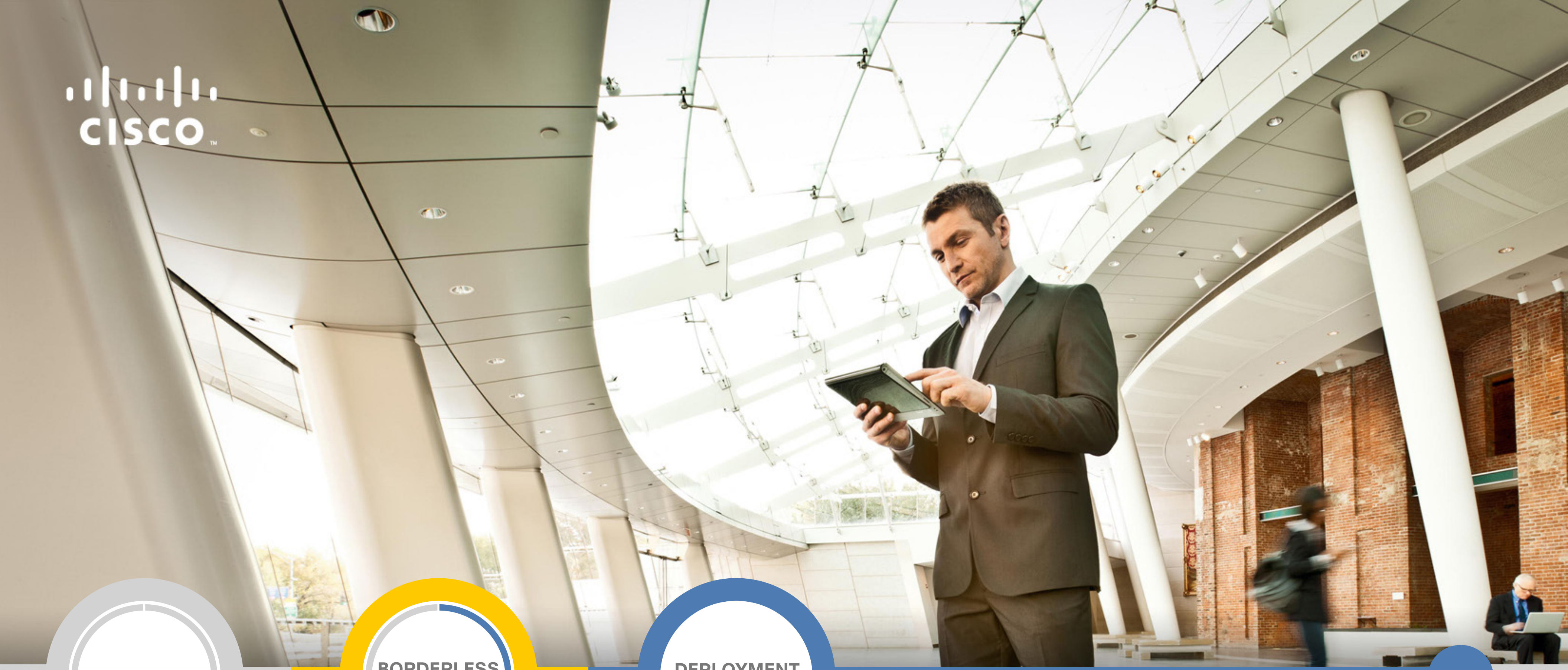
Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program.

For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-147

For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd

SBA



SBA

BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Cloud Web Security Using Cisco ASA Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100 
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

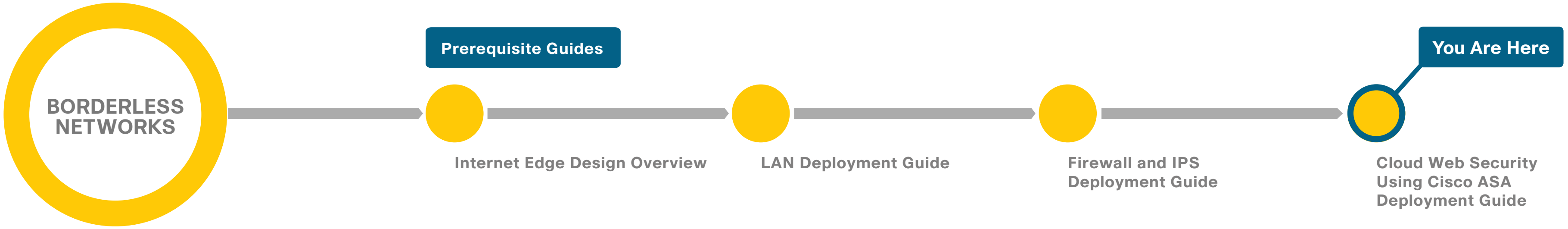
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- Deployment Details—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

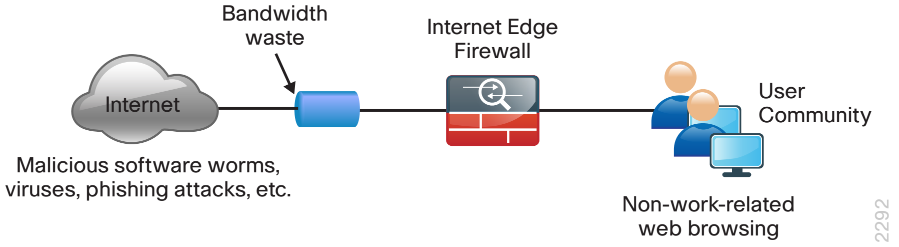

BORDERLESS NETWORKS
Prerequisite Guides
You Are Here
Internet Edge Design Overview
LAN Deployment Guide
Firewall and IPS Deployment Guide
Cloud Web Security Using Cisco ASA Deployment Guide

Introduction

Web access is a requirement for the day-to-day functions of most organizations, but a challenge exists to maintain appropriate web access for everyone in the organization, while minimizing unacceptable or risky use. A solution is needed to control policy-based web access in order to ensure employees work effectively and ensure that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk.

Another risk associated with Internet access for the organization is the pervasive threat that exists from accessing sites and content. As the monetary gain for malicious activities on the Internet has grown and developed, the methods used to affect these malicious and or illegal activities has grown and become more sophisticated. *Botnets*, one of the greatest threats that exists in the Internet today, is that of malicious Internet servers (mostly web) being used to host content that then attacks innocent user's browsers as they view the content. These types of attacks have been used very successfully by *bot herders* (originators of the attack) to gather in millions of infected members that are subject to the whims of the people who now control their machines. Other threats include the still popular and very broad threats of viruses and trojans, in which a user receives a file in some manner and is tricked into running it, and the file then executes malicious code. The third variant uses directed attacks over the network. Examples of these attacks are the Internet worms that gathered so much attention in the early to mid-2000s. These types of risks are depicted in the figure below.

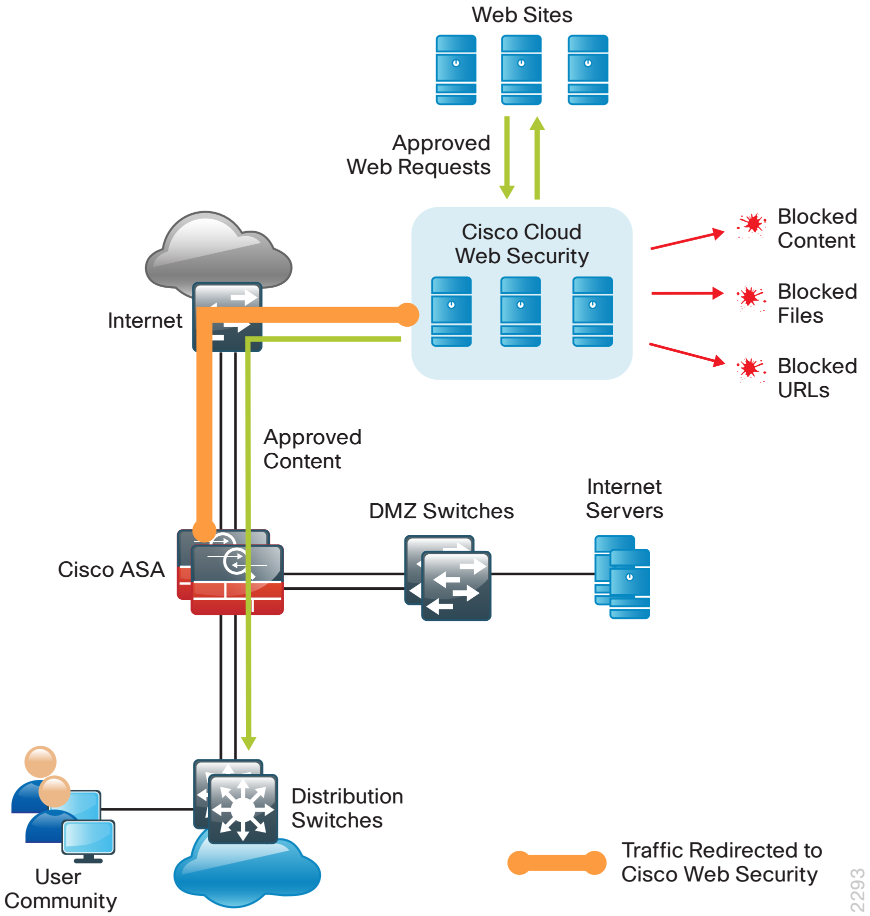
Figure 1 - Business reasons for deploying Cisco Cloud Web Security


Bandwidth waste
Internet Edge Firewall
Internet
User Community
Malicious software worms, viruses, phishing attacks, etc.
Non-work-related web browsing
2292

Business Overview

Cisco Cloud Web Security (CWS) addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection.

Figure 2 - Cloud Web Security deployment



Browsing websites can be risky, and many websites inadvertently end up distributing compromised or malicious content as a result of inattention to update requirements or lax security configurations. The websites that serve the compromised and malicious content are constantly changing as human-operated and worm-infested computers scan the Internet in search of additional web servers that they can infect in order to continue propagating. This dynamic environment introduces significant challenges to maintain up-to-date Internet threat profiles.

Technology Overview

The Cisco Smart Business Architecture (SBA) Internet edge design provides the basic framework for the enhancements and additions that are discussed in this guide. A prerequisite for using this deployment guide is that you must have already followed the guidance in the *Firewall and IPS Deployment Guide*.

Through the use of multiple techniques, Cisco CWS provides granular control over all web content that is accessed. These techniques include real-time dynamic web content classification, a URL-filtering database, and file-type and content filters. The policies enforced by Cisco CWS provide strong web security and control for an organization. Cisco CWS policies apply to all users regardless of their location and device type.

Internal users at both the primary site and at remote sites access the Internet by using the primary site's Internet-edge Cisco Adaptive Security Appliance (ASA), which provides stateful firewall and intrusion prevention capabilities. It is simple and straightforward to add Cisco CWS to a Cisco ASA appliance that is already configured and operational. This integration uses the Cloud Web Security Connector for Cisco ASA and requires no additional hardware.

Mobile remote users connect to their organization's network by using devices that generally fall into two categories: laptops and mobile devices such as smartphones and tablets. Because the devices operate and are used differently, the capabilities currently available for each group differ. Laptops and other devices that support the Cisco AnyConnect Secure Mobility Client with Cisco CWS are not required to send web traffic to the primary site. This solution is covered in detail in the *Remote Mobile Access Deployment Guide*. If you have an existing CWS deployment for remote-access users, the procedures are similar.

Cisco CWS using Cisco ASA also protects mobile users who are using a non-CWS enabled AnyConnect Secure Mobility Client that connects through remote access VPN as detailed in both the *Remote Access VPN Deployment Guide* and *Remote Mobile Access Deployment Guide*.

Cisco CWS is a cloud-based method of implementing web security that is similar in function to the Cisco Web Security Appliance (WSA), which uses an on-premise appliance for web security. This guide is focused on the deployment of Cisco CWS on Cisco ASA. For more information about using Cisco WSA in Cisco SBA, see the *Web Security Using Cisco WSA Deployment Guide*.

Some key differences between Cisco CWS and Cisco WSA include the items listed in the following table.

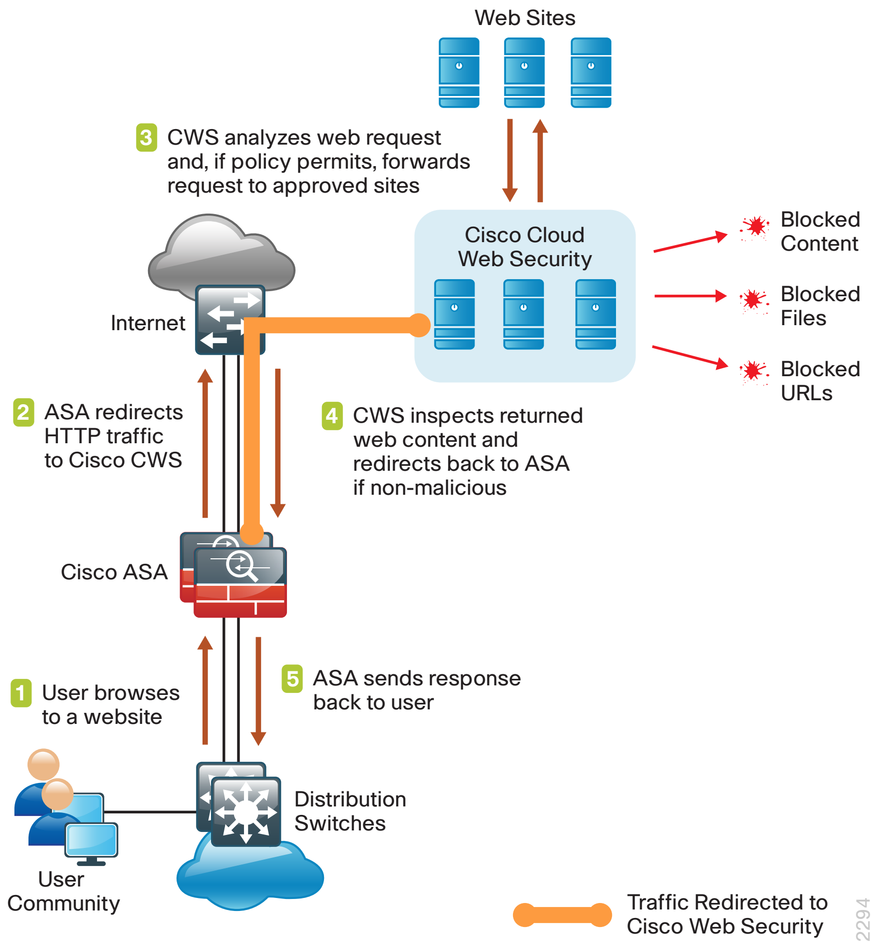
Table 1 - Cisco Web Security solution comparison

	Cisco CWS	**Cisco WSA**
Web/URL filtering	Yes	Yes
Supported protocols	HTTP/HTTPS	HTTP/HTTPS, FTP
Outbreak Intelligence (Zero-Day Malware)	Yes (Multiple scanners for malware)	Yes (URL/IP reputation filtering, Multiple scanners for malware)
Remote user security	Direct to cloud using Cisco AnyConnect	VPN backhaul
Remote user security (mobile devices)	VPN backhaul	VPN backhaul
Deployment	Redirect to cloud service	On Premise Redirect
Policy and reporting	Web portal (cloud)	On Premise

Many organizations provide guest access by using Wireless LAN and enforce an acceptable use policy and provide additional security for guest users by using Cisco CWS. This guide includes a section on how to deploy CWS for wireless guest users without requiring any configuration changes to Cisco ASA.

The Cisco ASA firewall family sits between the organization's internal network and the Internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security. The design uses Cisco ASA to implement a service policy that matches specified traffic and redirects the traffic to the Cisco CWS cloud for inspection. This method is considered a transparent proxy, and no configuration changes are required to web browsers on user devices.

Figure 3 - Cloud Web Security detailed traffic flow


Web Sites
3 CWS analyzes web request and, if policy permits, forwards request to approved sites
Cisco Cloud Web Security
Blocked Content
Blocked Files
Blocked URLs
Internet
2 ASA redirects HTTP traffic to Cisco CWS
4 CWS inspects returned web content and redirects back to ASA if non-malicious
Cisco ASA
1 User browses to a website
5 ASA sends response back to user
User Community
Distribution Switches
Traffic Redirected to Cisco Web Security
2294

The easiest way to apply the service policy is to modify the existing global service policy to add Cisco CWS inspection. The global policy applies to traffic received on any interface, so the same service policy applies to the following:

- Internal users at the primary site or at remote sites
- Wireless guest users connected to a demilitarized zone (DMZ) network
- Remote-access VPN users using a non-CWS enabled AnyConnect client connecting with either the integrated firewall and VPN model or standalone VPN model

The various traffic flows for each of these use cases are shown in the following figures.

Figure 4 - Cloud Web Security with internal and guest users

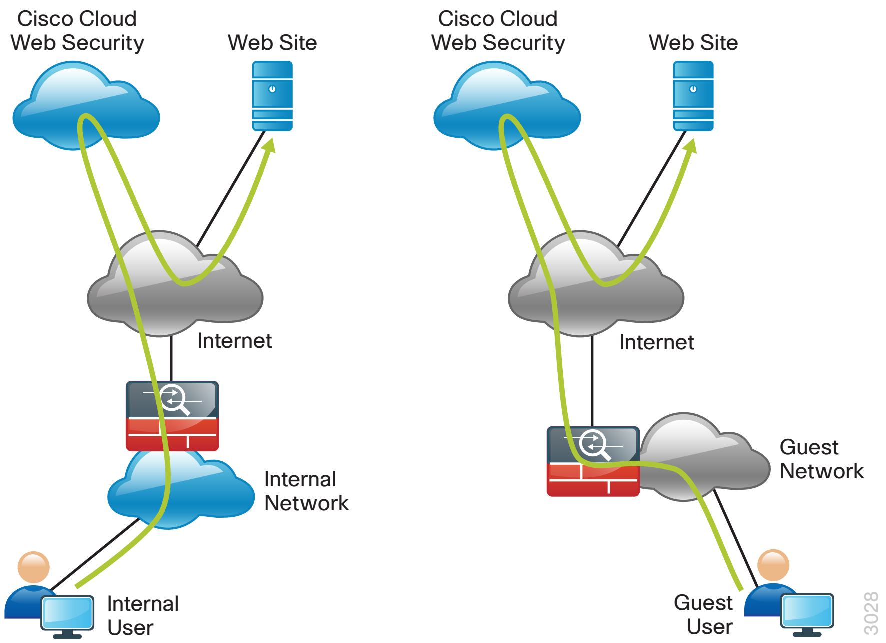
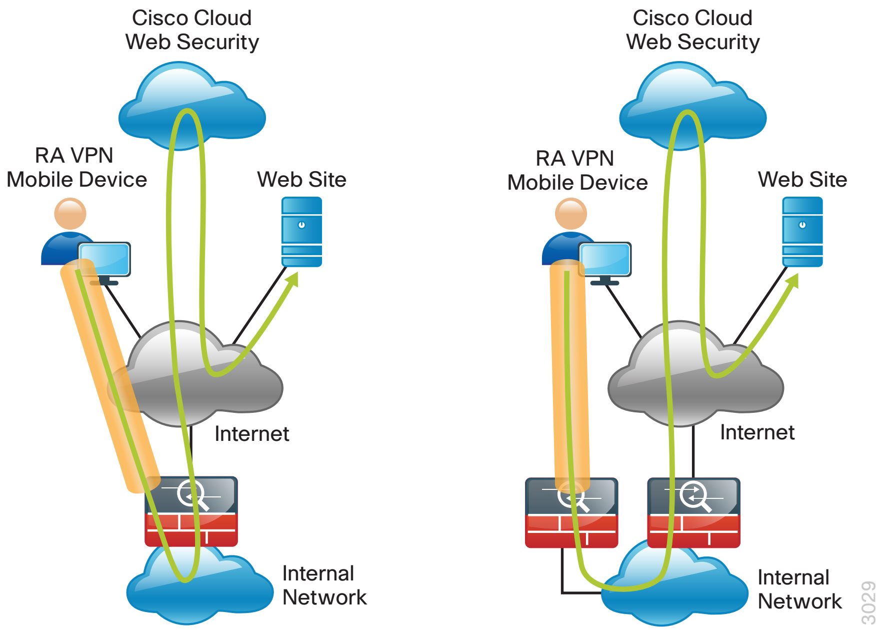


Figure 5 - Cloud Web Security for mobile devices using remote-access VPN



Certain source and destination pairs should be exempted from the service policy, such as remote-access VPN users accessing internal networks or internal users accessing DMZ networks. The creation of these exemptions is shown in the Deployment Details section of this guide.

The Cisco CWS cloud is accessed through a network of proxy servers, which have a broad geographic distribution in order to support a globally diverse set of customers. Cisco ASA is configured with a primary and secondary proxy server in order to provide high availability. Specific details for which proxy servers to use is provided by Cisco and based on the location and size of the deployment.

Cisco CWS is administered by using the CWS ScanCenter web portal. This includes creating filters and rules for policies, creating groups, activating keys, and viewing reports. All required CWS administration tasks are covered in this guide.

Notes

Deployment Details

The first part of this section describes how to configure the components in order to enable Cisco CWS service for internal users that access the Internet through the Internet-edge Cisco ASA, including users at the primary site and remote sites. Additionally, if internal users are using remote-access VPN from mobile devices, they are also protected with Cisco CWS. The second part of this section describes how to configure CWS for guest users, who may require a different policy than internal users.

Process

Configuring CWS Policies for Internal Users

1. Enable CWS security configuration

Procedure 1 Enable CWS security configuration

This guide assumes you have purchased a Cisco CWS license and created an administrative CWS account that allows a user to log in and manage the account.

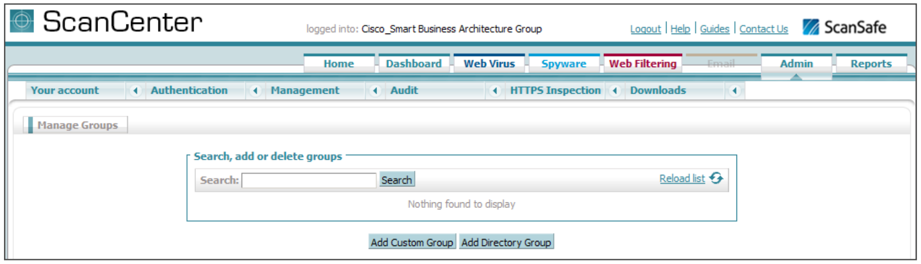
Step 1: Access the Cisco CWS ScanCenter Portal at the following location, and then log in with administrator rights:

https://scancenter.scansafe.com

Step 2: Navigate to **Admin** > **Management** > **Groups**.

Tech Tip

Policy can differ based on group assignment. The simplest method for assigning group membership is to generate a unique key for a group and use that key during deployment to group members. If more granular policies are required, other methods for group assignment include IP address range or mapping to an Active Directory group.



Nothing found to display

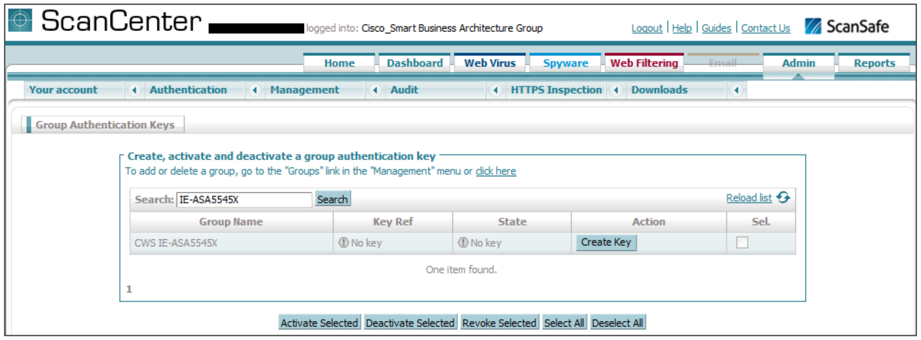
Step 3: Click **Add Custom Group**.

Step 4: In the Add New Custom Group pane, enter the group name (Example: CWS IE-ASA5545X), and then click **Save**.

A group-specific authentication license key is generated for use in the Cisco ASA VPN configuration.

Step 5: Navigate to **Admin** > **Authentication** > **Group Keys**.

Step 6: For the group created in Step 4, click **Create Key**. ScanCenter generates a key that it sends to an email address of your choosing.



[redacted] logged into: Cisco_Smart Business Architecture Group

Create, activate and deactivate a group authentication key

To add or delete a group, go to the "Groups" link in the "Management" menu or click here

Search: IE-ASA5545X Search Reload list

Group Name	Key Ref	State	Action	Sel.
CWS IE-ASA5545X	No key	No key	Create Key	□

One item found.

1

Step 7: Store a copy of this key by copying and pasting it into a secure file because the key cannot be rebuilt and can only be replaced with a new key. After it is displayed the first time (on generation) and sent in email, you can no longer view it in ScanCenter. After this key is generated, the page options change to Deactivate or Revoke.

Step 8: Navigate to **Web Filtering > Management > Filters**.

Tech Tip

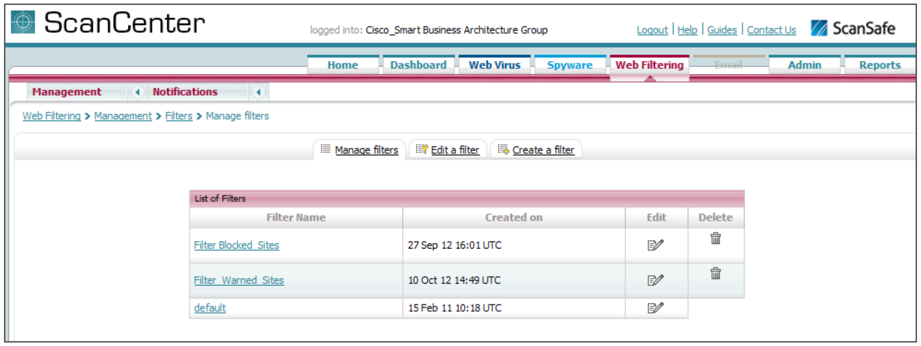
The filtering policy in this guide is an example only. The actual policy implemented should align with the organization's security policy and business requirements.

Step 9: Click **Create a filter**.

Step 10: Assign a name to the filter (Example: Filter Blocked Sites), select the categories blocked by your organization's policy (Examples: Pornography and Hate Speech), and then click **Save**. Access to these categories is completely restricted.

Step 11: Click **Create a filter**.

Step 12: Assign a name to the filter (Example: Filter Warned Sites), select the categories that are considered inappropriate by your organization's policy (Example: Gambling), and then click **Save**. Access to these categories is permitted, but only after accepting a warning message.



logged into: Cisco_Smart Business Architecture Group

Web Filtering > Management > Filters > Manage filters

List of Filters

Filter Name	Created on	Edit	Delete
Filter Blocked Sites	27 Sep 12 16:01 UTC	✎	🗑
Filter Warned Sites	10 Oct 12 14:49 UTC	✎	🗑
default	15 Feb 11 10:18 UTC	✎	

Step 13: Navigate to **Web Filtering > Management > Policy**.

Step 14: Select the Rule name **Default**, change the rule action to **Allow**, and then click **Save.**

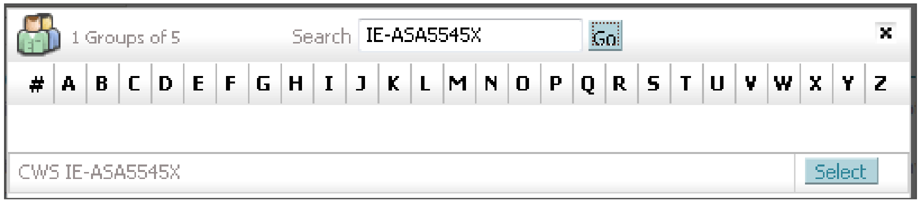
Step 15: Click **Create a rule**.

Step 16: Assign a name to the rule (Example: Block_Blocked_Sites), and then select **Active**.

Step 17: In the **Rule Action** list, choose **Block**.

Step 18: In the Define Group pane, click **Add group**.

Step 19: On the dialog box, in the **Search** box, enter the name of the group created in Step 4, and then click **Go**.



1 Groups of 5

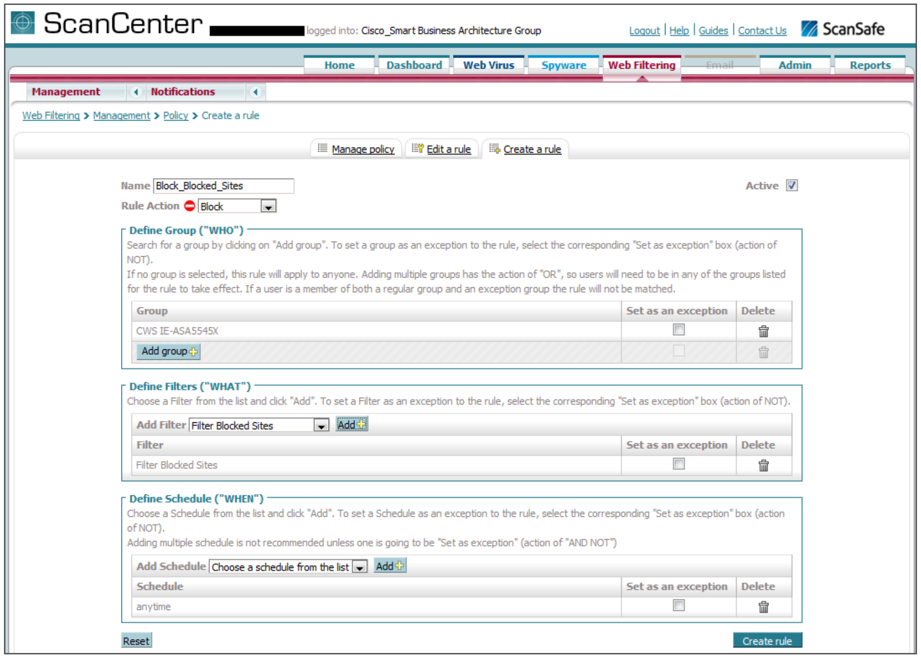
Search IE-ASA5545X

CWS IE-ASA5545X

Step 20: Click **Select**, and then click **Confirm Selection**.

Step 21: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 10 (Example: Filter Blocked Sites), and then click **Add**.

Step 22: Click **Create rule**. The policy rule has now been created.



[redacted] logged into: Cisco_Smart Business Architecture Group

Web Filtering > Management > Policy > Create a rule

Name: Block_Blocked_Sites

Active ☑

Rule Action: Block

Define Group ("WHO")

Search for a group by clicking on "Add group". To set a group as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect. If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as an exception	Delete
CWS IE-ASA5545X	☐	🗑
Add group		

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

Add Filter: Filter Blocked Sites

Filter	Set as an exception	Delete
Filter Blocked Sites	☐	🗑

Define Schedule ("WHEN")

Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

Adding multiple schedule is not recommended unless one is going to be "Set as exception" (action of "AND NOT")

Add Schedule: Choose a schedule from the list

Schedule	Set as an exception	Delete
anytime	☐	🗑

Next, create a new rule.

Step 23: Click **Create a rule**.

Step 24: Assign a name to the rule (Example: Warn_Warned_Sites), and then select **Active**.

Step 25: In the **Rule Action** list, choose **Warn**.

Step 26: In the Define Group pane, click **Add group**.

Step 27: On the dialog box, in the search box, enter the name of the group created in Step 4, and then click **Go**.

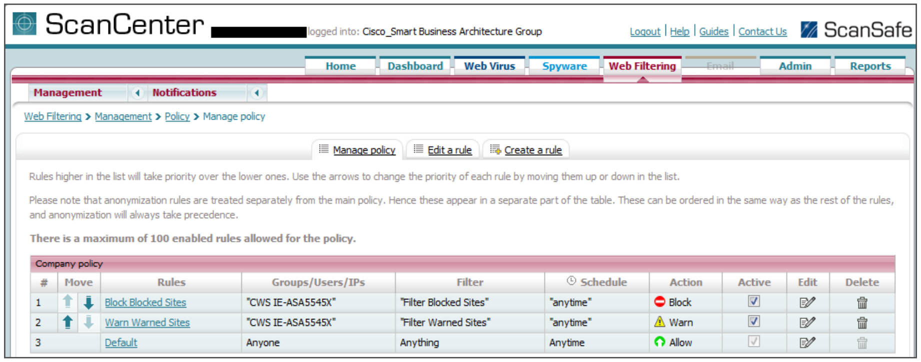
Step 28: Click **Select**, and then click **Confirm Selection**.

Step 29: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 12 (Example: Filter Warned Sites), and then click **Add**.

Step 30: Click **Create rule**. The policy rule has now been created.

Because all rules are evaluated on a first-hit rule, the following is the correct order for the rules in this example:

1. Block Blocked Sites (which blocks access to restricted categories)
2. Warn Warned Sites (which allows access to sites but with a warning)
3. Default (which permits all other sites)



[redacted] logged into: Cisco_Smart Business Architecture Group

Web Filtering > Management > Policy > Manage policy

Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.

There is a maximum of 100 enabled rules allowed for the policy.

Company policy

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	↑ ↓	Block Blocked Sites	"CWS IE-ASA5545X"	"Filter Blocked Sites"	"anytime"	Block	☑	✎	🗑
2	↑ ↓	Warn Warned Sites	"CWS IE-ASA5545X"	"Filter Warned Sites"	"anytime"	Warn	☑	✎	🗑
3		Default	Anyone	Anything	Anytime	Allow	☑	✎	🗑

Process

Configuring ASA for Cisco Cloud Web Security

1. Configure CWS servers
2. Configure ASA firewall objects
3. Configure ASA service policy
4. Test Cloud Web Security

Procedure 1 Configure CWS servers

Cisco ASA is configured with a primary and backup server. You will receive a provisioning email after purchasing your Cisco CWS license. This email includes the primary and backup server address that you use for configuring Cisco ASA. An example email is included in “Appendix C” in this guide.

Table 2 - Provisioning email explicit proxy setting example

Primary web services proxy address	proxyXXXX.scansafe.net
Web services proxy port	8080
Secondary web services proxy address	proxyXXXX.scansafe.net
Web services proxy port	8080

Tech Tip

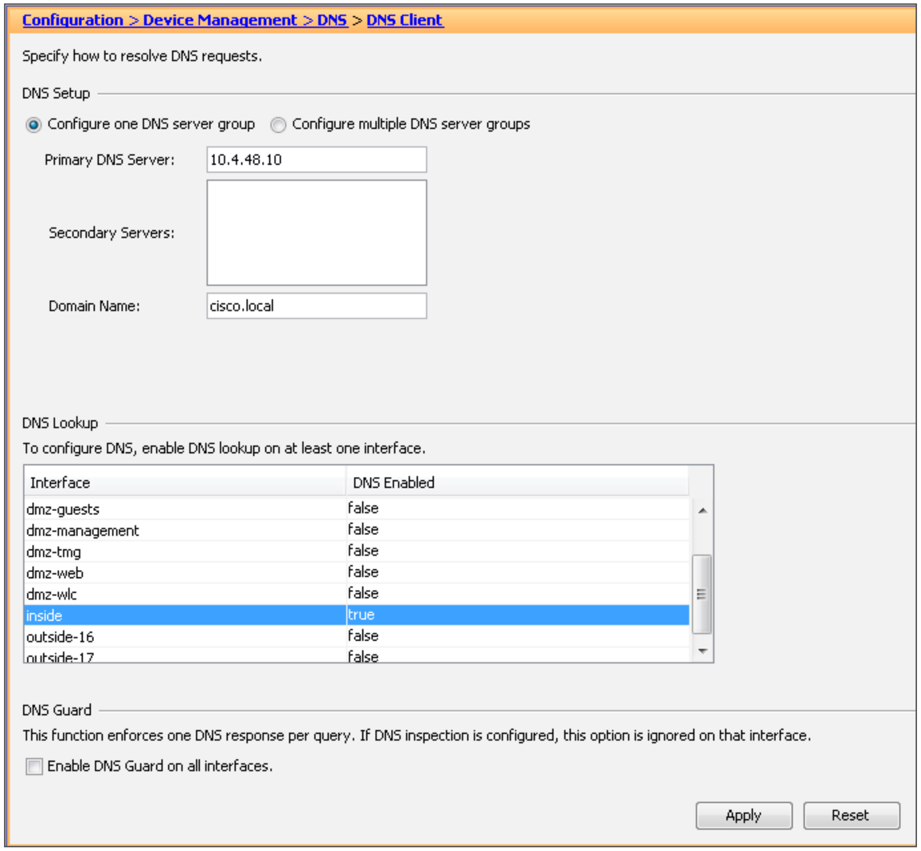
Domain Name Service (DNS) is required to resolve the Fully Qualified Domain Name (FQDN) of a Cisco CWS web services proxy server.

Step 1: From a client on the internal network, navigate to the Internet-edge firewall’s inside IP address, and then launch Cisco ASA Security Device Manager. (Example: https://10.4.24.30)

Step 2: If the firewall is not configured to use DNS resolution, configure it now in **Configuration > Device Management > DNS > DNS Client.**

- Primary DNS Server—**10.4.48.10**
- Domain Name—**cisco.local**

Step 3: In the DNS Lookup pane, scroll to view the **Interface** list, click in the **DNS Enabled** column for the interface that is used to reach the DNS server (Example: inside), choose **True**, and then click **Apply**.



Configuration > Device Management > DNS > DNS Client

Specify how to resolve DNS requests.

DNS Setup

● Configure one DNS server group ○ Configure multiple DNS server groups

Primary DNS Server: 10.4.48.10

Secondary Servers:

Domain Name: cisco.local

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
dmz-guests	false
dmz-management	false
dmz-tmg	false
dmz-web	false
dmz-wlc	false
inside	true
outside-16	false
outside-17	false

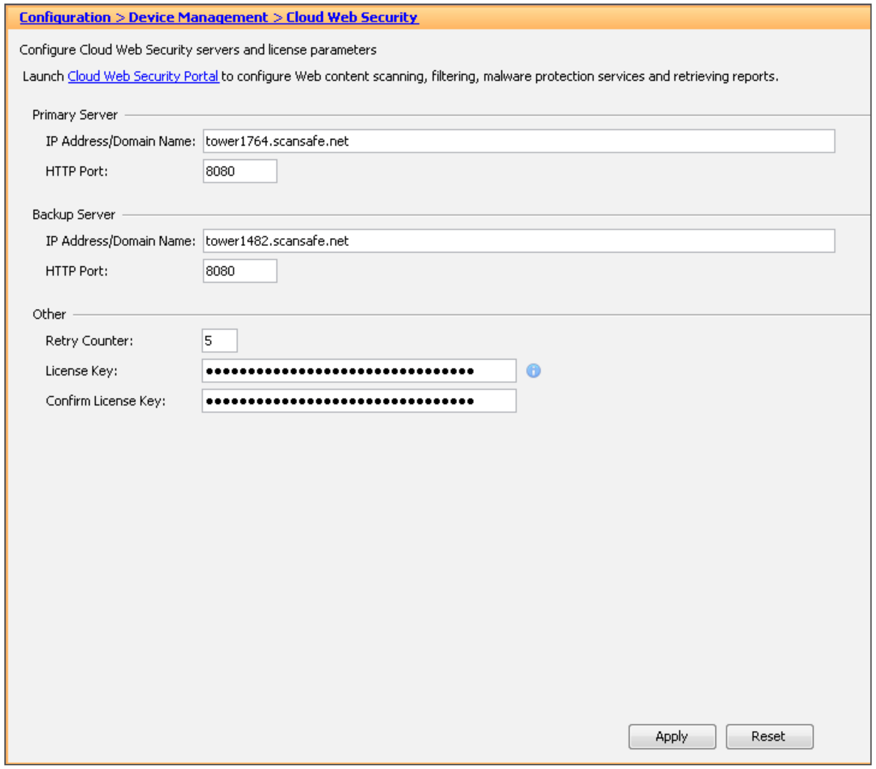
DNS Guard

This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

□ Enable DNS Guard on all interfaces.

Step 4: In Configuration > Device Management > Cloud Web Security, configure the following values from Table 2, and then click Apply.

- Primary Server IP Address/Domain Name—<FQDN from provisioning email>
- Secondary Server IP Address/Domain Name—<FQDN from provisioning email>
- License Key—<Group key from Step 6 of Procedure 1 in “Configuring CWS Policies for Internal Users” process >



Configuration > Device Management > Cloud Web Security

Configure Cloud Web Security servers and license parameters

Launch Cloud Web Security Portal to configure Web content scanning, filtering, malware protection services and retrieving reports.

Primary Server

IP Address/Domain Name:	tower1764.scansafe.net
HTTP Port:	8080

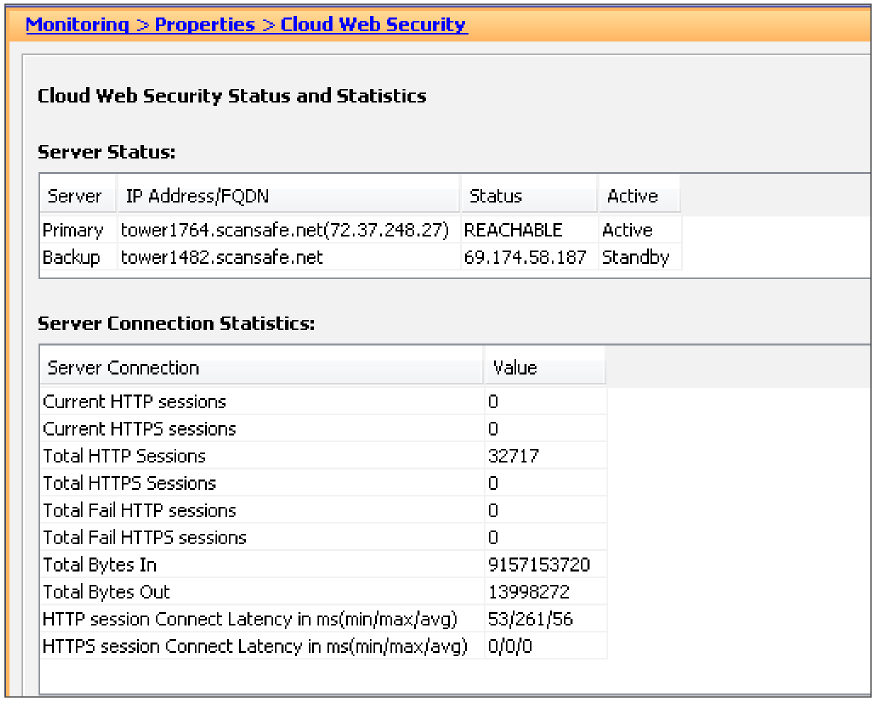
Backup Server

IP Address/Domain Name:	tower1482.scansafe.net
HTTP Port:	8080

Other

Retry Counter:	5
License Key:	••••••••••••••••••••••••••••••••
Confirm License Key:	••••••••••••••••••••••••••••••••

Step 5: In Monitoring > Properties > Cloud Web Security, verify the Cisco CWS server status. Your primary server should show a status of REACHABLE.



Monitoring > Properties > Cloud Web Security

Cloud Web Security Status and Statistics

Server Status:

Server	IP Address/FQDN	Status	Active
Primary	tower1764.scansafe.net(72.37.248.27)	REACHABLE	Active
Backup	tower1482.scansafe.net	69.174.58.187	Standby

Server Connection Statistics:

Server Connection	Value
Current HTTP sessions	0
Current HTTPS sessions	0
Total HTTP Sessions	32717
Total HTTPS Sessions	0
Total Fail HTTP sessions	0
Total Fail HTTPS sessions	0
Total Bytes In	9157153720
Total Bytes Out	13998272
HTTP session Connect Latency in ms(min/max/avg)	53/261/56
HTTPS session Connect Latency in ms(min/max/avg)	0/0/0

Procedure 2 Configure ASA firewall objects

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Table 3 - Firewall network objects

Network object name	IP address	Netmask
internal-network	10.4.0.0/15	255.254.0.0
dmz-networks	192.168.16.0/21	255.255.248.0

Step 2: Repeat Step 3 through Step 7 for all objects listed in Table 3. If the object already exists, then skip to the next object listed in the table.

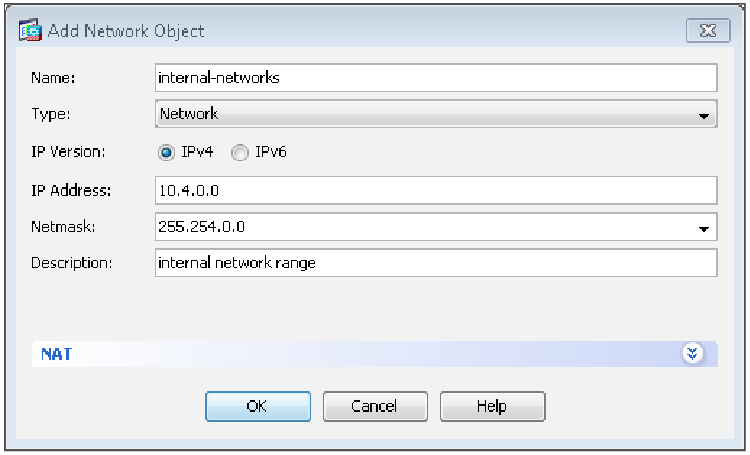
Step 3: Click **Add > Network Object**.

Step 4: On the Add Network Object dialog box, in the **Name** box, enter the Network object name from Table 3. (Example: internal-network)

Step 5: In the **Type** list, choose **Network**.

Step 6: In the **IP Address** box, enter the IP address of the object from Table 3. (Example: 10.4.0.0)

Step 7: In the **Netmask** box, enter netmask of the object from Table 3, and then click **OK**. (Example: 255.254.0.0)



Add Network Object

Name: internal-networks

Type: Network

IP Version: ● IPv4 ○ IPv6

IP Address: 10.4.0.0

Netmask: 255.254.0.0

Description: internal network range

Step 8: After adding all of the objects listed in Table 3, in the Network Objects/Groups pane, click **Apply**.

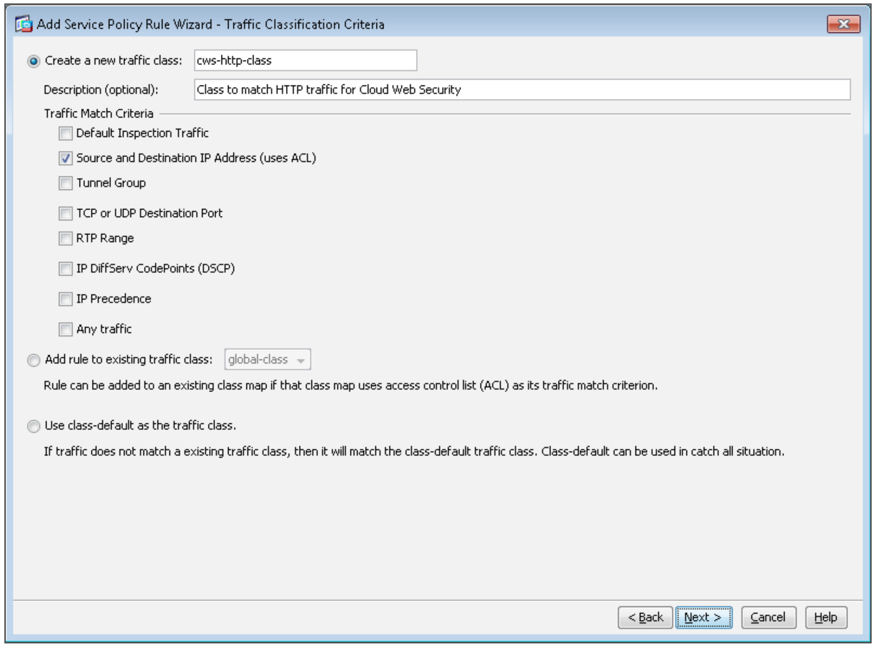
Procedure 3 Configure ASA service policy

The existing global service policy is modified to enable Cisco CWS.

Step 1: In **Configuration > Firewall > Service Policy Rules**, select **Add > Add Service Policy Rule**.

Step 2: Skip the Add Service Policy Rule Wizard – Service Policy dialog box by clicking **Next**.

Step 3: On the Add Service Policy Rule Wizard – Traffic Classification Criteria dialog box, in the **Create a new traffic class** box, enter **cws-http-class**, for Traffic Match Criteria, select **Source and Destination IP Address**, and then click **Next**.



Add Service Policy Rule Wizard - Traffic Classification Criteria

● Create a new traffic class: cws-http-class

Description (optional): Class to match HTTP traffic for Cloud Web Security

Traffic Match Criteria

- □ Default Inspection Traffic
- ☑ Source and Destination IP Address (uses ACL)
- □ Tunnel Group
- □ TCP or UDP Destination Port
- □ RTP Range
- □ IP DiffServ CodePoints (DSCP)
- □ IP Precedence
- □ Any traffic

○ Add rule to existing traffic class: global-class

Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match criterion.

○ Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

Next, create the single global policy for Cisco CWS in order to match traffic on all interfaces. Since this policy may be used by internal users and remote access VPN users, certain source and destination traffic pairs are exempted from the CWS policy by using **Do not match** as shown in the following table. The final policy rule matches all other source and destination pairs.

Table 4 - Example Policy for Cisco Cloud Web Security

Action	Source object	Destination object	Service	Description
Do not match	any4	internal-network	ip	Do not match any to internal networks
Do not match	any4	dmz-networks	ip	Do not match any to DMZ networks
Match	any4	any4	tcp/http	Match HTTP to any other networks

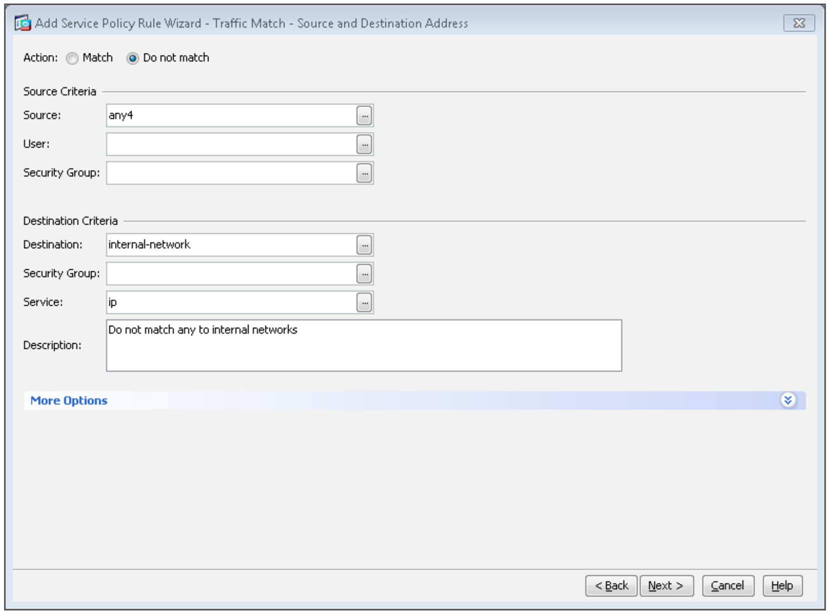
The Add Service Policy Rule Wizard allows only a simple policy containing a single match entry, so the following steps are used to configure only the first entry in Table 4. You configure the remaining entries in Table 4 after you complete the first pass of the wizard.

Step 4: On the Add Service Policy Rule Wizard – Traffic Match – Source and Destination Address dialog box, for **Action**, select the action listed in the first row of Table 4. (Example: Do not match)

Step 5: In the **Source** box, enter the source object listed in the first row of Table 4. (Example: any4)

Step 6: In the **Destination** box, enter the destination object listed in the first row of Table 4. (Example: internal-network)

Step 7: In the **Service** box, enter the service listed in the first row of Table 4. (Example: ip), and then click **Next**.



Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ○ Match ● Do not match

Source Criteria

Source: any4

User:

Security Group:

Destination Criteria

Destination: internal-network

Security Group:

Service: ip

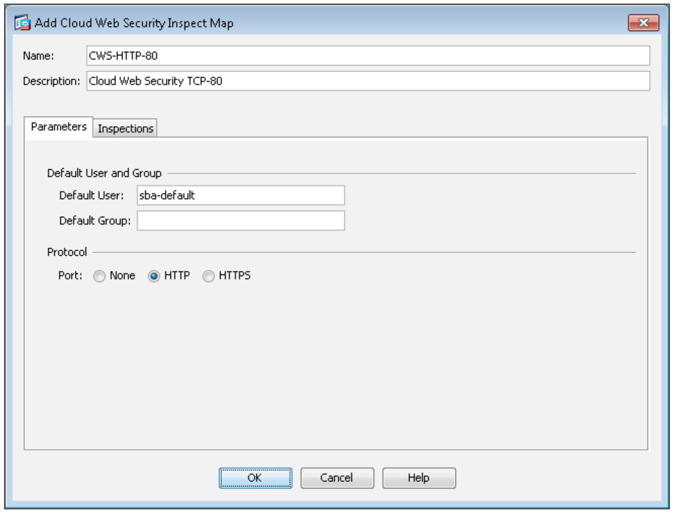
Description: Do not match any to internal networks

Step 8: On the Add Service Policy Rule Wizard – Rule Actions dialog box, click the **Protocol Inspection** tab, select **Cloud Web Security**, and then click **Configure**.

Step 9: On the Select Cloud Web Security Inspect Map dialog box, click **Add**.

Step 10: On the Add Cloud Web Security Inspect Map dialog box, enter a name (Example: CWS-HTTP-80). On the Parameters tab, in the **Default User** box, enter a username that will be used by default (Example: sba-default).

Step 11: Select **HTTP**, and then click **OK**.



Add Cloud Web Security Inspect Map

Name: CWS-HTTP-80

Description: Cloud Web Security TCP-80

Default User and Group

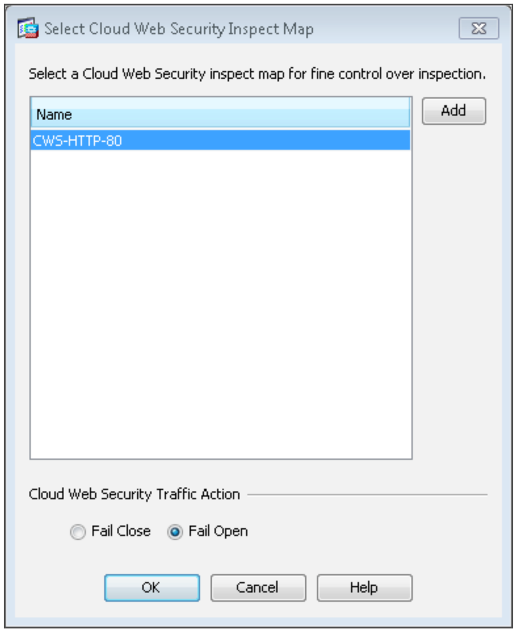
Default User: sba-default

Default Group:

Protocol

Port: ○ None ● HTTP ○ HTTPS

Step 12: On the Select Cloud Web Security Inspect Map dialog box, select the inspect map you created in Step 10, for Cloud Web Security Action, select **Fail Open**, and then click **OK**.



Select Cloud Web Security Inspect Map

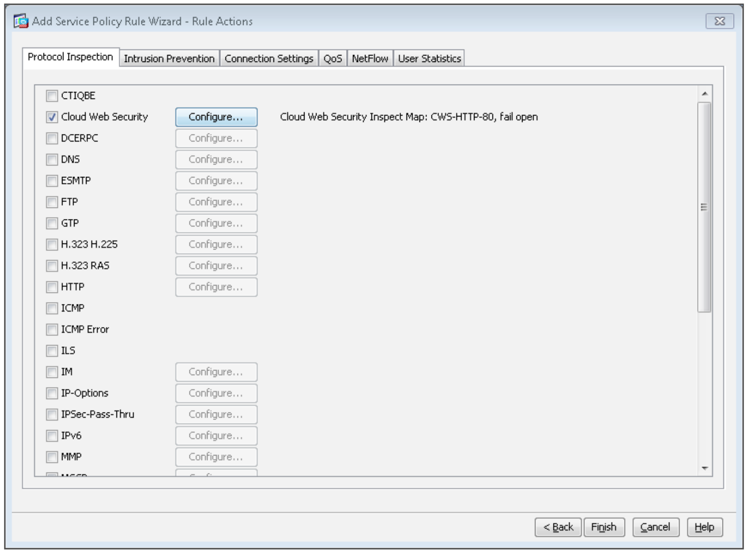
Select a Cloud Web Security inspect map for fine control over inspection.

Name
CWS-HTTP-80

Cloud Web Security Traffic Action

○ Fail Close ● Fail Open

Step 13: On the Add Service Policy Rule Wizard – Rule Actions dialog box, click **Finish**.



Add Service Policy Rule Wizard - Rule Actions

Protocol Inspection

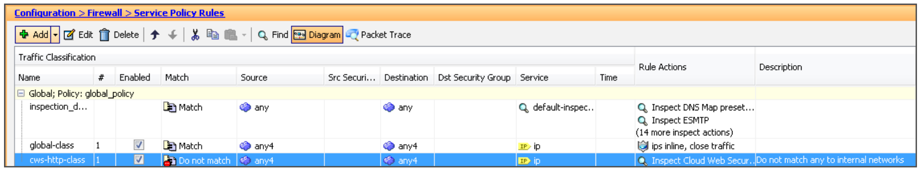
□ CTIQBE
☑ Cloud Web Security — Cloud Web Security Inspect Map: CWS-HTTP-80, fail open
□ DCERPC
□ DNS
□ ESMTP
□ FTP
□ GTP
□ H.323 H.225
□ H.323 RAS
□ HTTP
□ ICMP
□ ICMP Error
□ ILS
□ IM
□ IP-Options
□ IPSec-Pass-Thru
□ IPv6
□ MMP

Because the Add Service Policy Rule Wizard allowed only a simple policy containing a single match entry, use the following steps in order to configure the remaining entries from Table 4, which are replicated in Table 5.

Table 5 - Example Policy for Cloud Web Security (remaining entries from Table 4)

Action	Source object	Destination object	Service	Description
Do not match	any4	dmz-networks	ip	Do not match any to DMZ networks
Match	any4	any4	tcp/http	Match HTTP to any other networks

Step 14: In **Configuration > Firewall > Service Policy Rules**, select the highest numbered rule for the Cisco CWS policy (Example: cws-http-class). Right-click to Copy, and then right-click to Paste After.

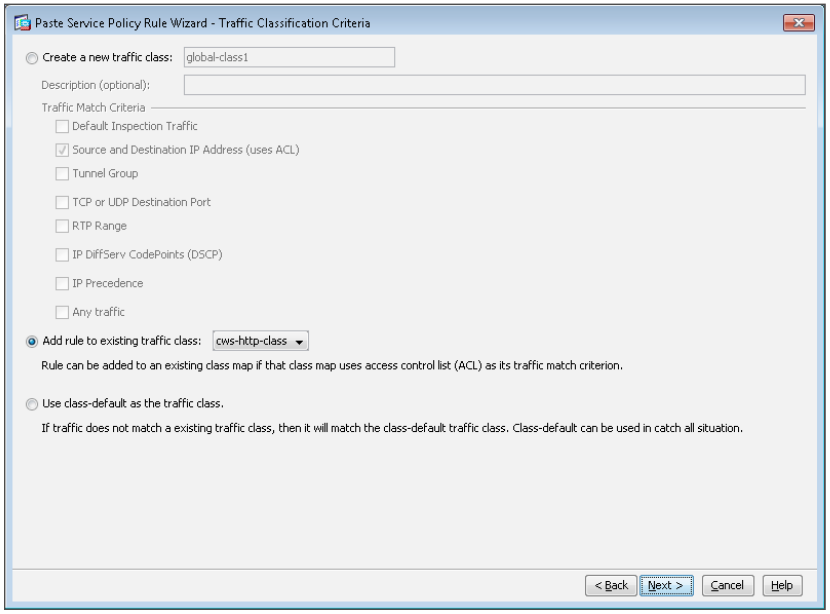


Configuration > Firewall > Service Policy Rules

Traffic Classification										Rule Actions	Description
Name	#	Enabled	Match	Source	Src Securi...	Destination	Dst Security Group	Service	Time		
⊟ Global; Policy: global_policy											
inspection_d...			Match	any		any		default-inspec...		Inspect DNS Map preset... Inspect ESMTP (14 more inspect actions)	
global-class	1	☑	Match	any4		any4		ip		ips inline, close traffic	
cws-http-class	1	☑	Do not match	any4		any4		ip		Inspect Cloud Web Secur...	Do not match any to internal networks

Step 15: Skip the Paste Service Policy Rule Wizard – Service Policy dialog box by clicking **Next**.

Step 16: On the Paste Service Policy Rule Wizard – Traffic Classification Criteria dialog box, select **Add rule to existing traffic class**, and then from list of classes, choose the class created in Step 3 (Example: cws-http-class). Click **Next**.



Paste Service Policy Rule Wizard - Traffic Classification Criteria

○ Create a new traffic class: global-class1

Description (optional):

Traffic Match Criteria

□ Default Inspection Traffic

☑ Source and Destination IP Address (uses ACL)

□ Tunnel Group

□ TCP or UDP Destination Port

□ RTP Range

□ IP DiffServ CodePoints (DSCP)

□ IP Precedence

□ Any traffic

● Add rule to existing traffic class: cws-http-class

Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match criterion.

○ Use class-default as the traffic class.

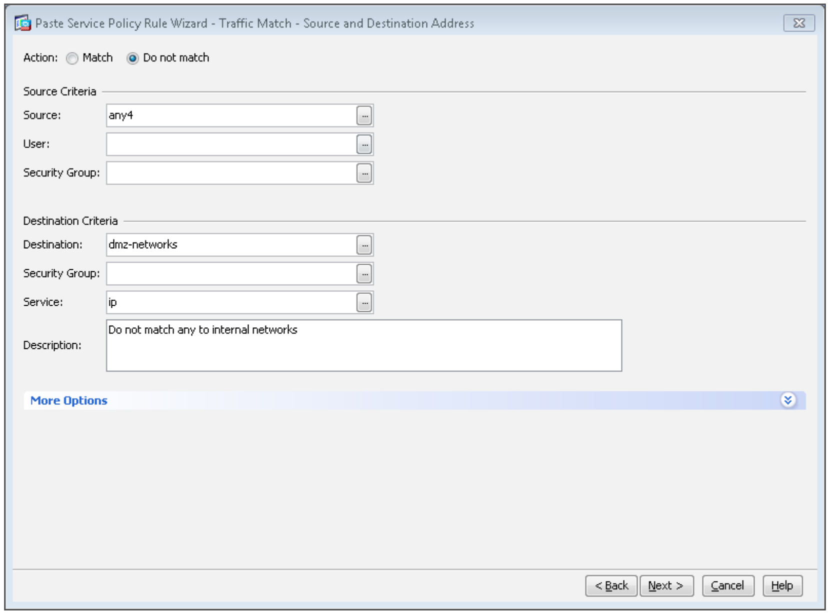
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

Step 17: On the Paste Service Policy Rule Wizard – Traffic Match – Source and Destination Address dialog box, for **Action**, select the action listed in Table 5. (Example: Do not match)

Step 18: In the **Source** box, enter the source object listed in Table 5. (Example: any4)

Step 19: In the **Destination** box, enter the destination object listed in Table 5. (Example: dmz-networks)

Step 20: In the **Service** box, enter the service listed in Table 5. (Example: ip), and then click **Next**.



Paste Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ○ Match ● Do not match

Source Criteria

Source: any4

User:

Security Group:

Destination Criteria

Destination: dmz-networks

Security Group:

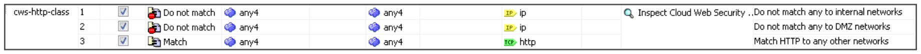
Service: ip

Description: Do not match any to internal networks

Step 21: On the Paste Service Policy Rule Wizard – Rule Actions dialog box, click **Finish**.

Step 22: Repeat Step 14 through Step 21 for all of the entries in Table 5.

Step 23: Verify that your service policy rules match the following figure, and then click **Apply**.



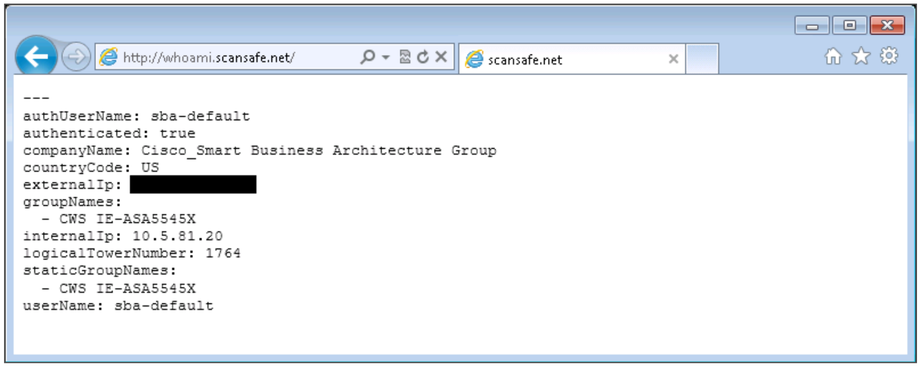
cws-http-class	1	☑	Do not match	any4		any4		ip		Inspect Cloud Web Security ..	Do not match any to internal networks
	2	☑	Do not match	any4		any4		ip			Do not match any to DMZ networks
	3	☑	Match	any4		any4		http			Match HTTP to any other networks

Procedure 4 Test Cloud Web Security

Step 1: From a client machine on the internal network, open a web browser to the following website:

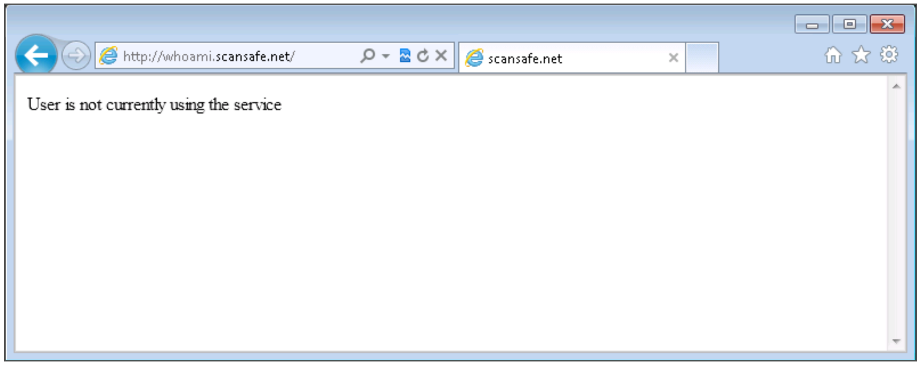
http://whoami.scansafe.net

This website returns diagnostic information from the Cisco CWS service.



```
---
authUserName: sba-default
authenticated: true
companyName: Cisco_Smart Business Architecture Group
countryCode: US
externalIp: [redacted]
groupNames:
  - CWS IE-ASA5545X
internalIp: 10.5.81.20
logicalTowerNumber: 1764
staticGroupNames:
  - CWS IE-ASA5545X
userName: sba-default
```

If the service is not active, the following information is returned.



User is not currently using the service

Notes

Process

Configuring CWS Policies for Guest Users

1. Enable CWS security configuration
2. Test Cloud Web Security

This is an optional process that is only required if you want to apply a different Cisco CWS policy for guest users. Otherwise, the same policy created for internal users is applied.

Reader Tip

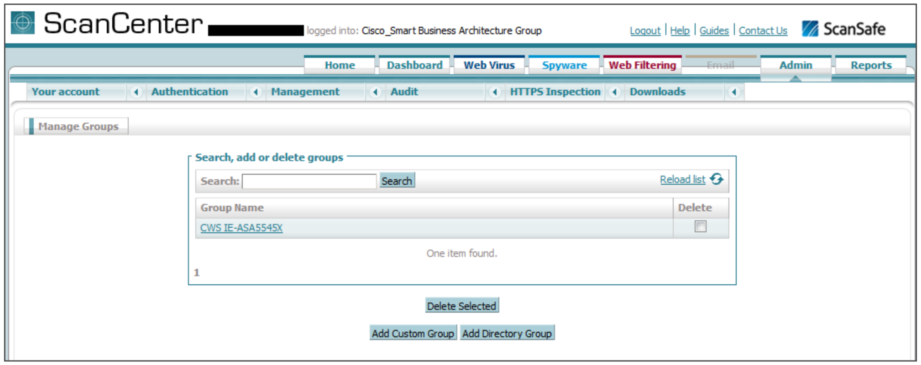
This process assumes that wireless LAN guest access has already been configured following the guidance in the *Wireless LAN Deployment Guide*. Only the procedures required to enable Cisco CWS for an existing guest user deployment are included.

Procedure 1 Enable CWS security configuration

Step 1: Access the Cisco CWS ScanCenter Portal at the following location, and then log in with administrator rights:

https://scancenter.scansafe.com

Step 2: Navigate to **Admin > Management > Groups**.


ScanCenter [redacted] logged into: Cisco_Smart Business Architecture Group

Search, add or delete groups

Search:

Group Name	Delete
CWS IE-ASA5545X	□

One item found.

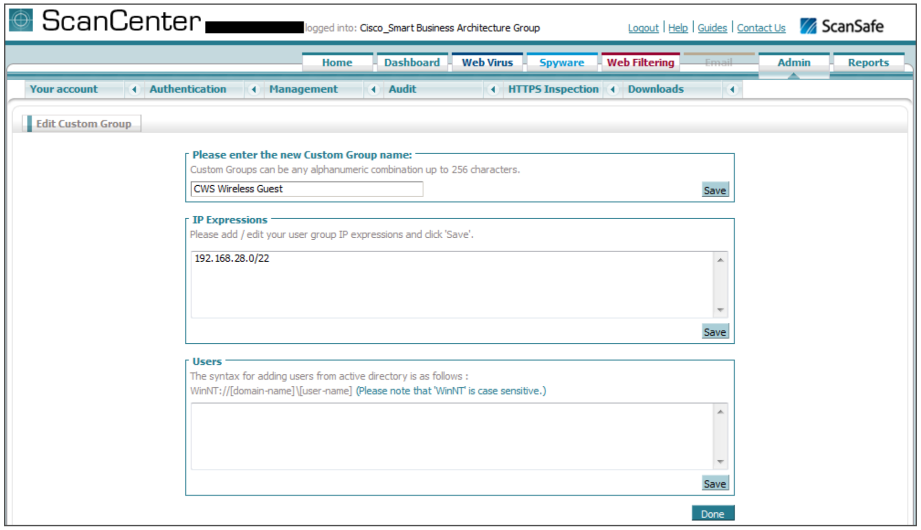
1

Step 3: Click **Add Custom Group**.

Step 4: On the Add New Custom Group pane, enter the group name (Example: CWS Wireless Guest), and then click **Save**.

Step 5: On the **Admin > Management > Groups** page, click the link for the group created in Step 4.

Step 6: In the IP Expressions pane, add the IP subnet range that corresponds to the wireless guest DMZ configuration in the *Wireless LAN Deployment Guide*, click **Save**, and then click **Done**.


ScanCenter [redacted] logged into: Cisco_Smart Business Architecture Group

Please enter the new Custom Group name:

Custom Groups can be any alphanumeric combination up to 256 characters.

CWS Wireless Guest

IP Expressions

Please add / edit your user group IP expressions and click 'Save'.

192.168.28.0/22

Users

The syntax for adding users from active directory is as follows :
WinNT://[domain-name]\[user-name] (Please note that 'WinNT' is case sensitive.)

Step 7: Navigate to **Web Filtering > Management > Filters**.

Tech Tip

The filtering policy in this guide is an example only. The actual policy implemented should align with the organization's security policy and business requirements. This example uses a whitelist policy and uses filters that initially select all categories for blocking or warning. Only specifically selected categories are exempt.

If you make the whitelist too limited, web browsing to many common websites may be restricted.

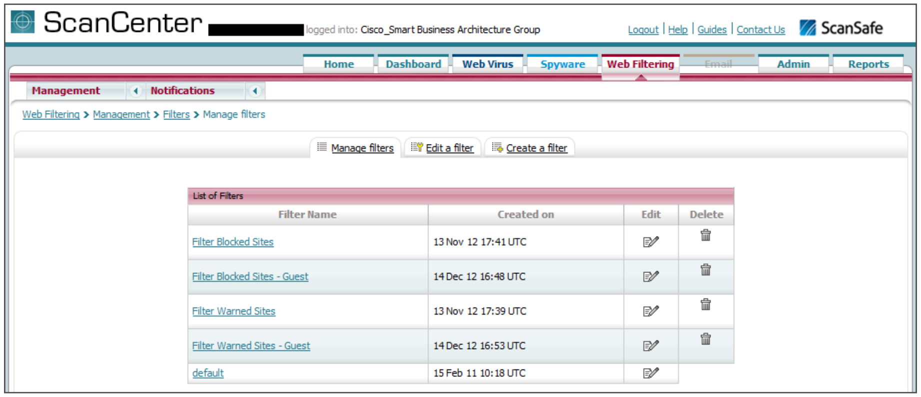
If your policy uses both a block list and a warn list as suggested in this example, all permitted categories must be contained in both lists.

Step 8: Click **Create a filter**.

Step 9: Assign a name to the filter (Example: Filter Blocked Sites - Guest), click **Select All**, clear the categories permitted by your organization's policy (Examples: Search Engines and Portals, News, Social Networking and Travel), and then click **Save**. Access to all other categories is completely restricted.

Step 10: Click **Create a filter**.

Step 11: Assign a name to the filter (Example: Filter Warned Sites - Guest), click **Select All**, clear the categories that are considered appropriate by your organization's policy that do not require a warning (Example: Gambling), and then click **Save**. Access to all other categories is permitted, but only after accepting a warning message.



ScanCenter [redacted] logged into: Cisco_Smart Business Architecture Group

Web Filtering > Management > Filters > Manage filters

List of Filters

Filter Name	Created on	Edit	Delete
Filter Blocked Sites	13 Nov 12 17:41 UTC	✎	🗑
Filter Blocked Sites - Guest	14 Dec 12 16:48 UTC	✎	🗑
Filter Warned Sites	13 Nov 12 17:39 UTC	✎	🗑
Filter Warned Sites - Guest	14 Dec 12 16:53 UTC	✎	🗑
default	15 Feb 11 10:18 UTC	✎	

Step 12: Navigate to **Web Filtering > Management > Policy**.

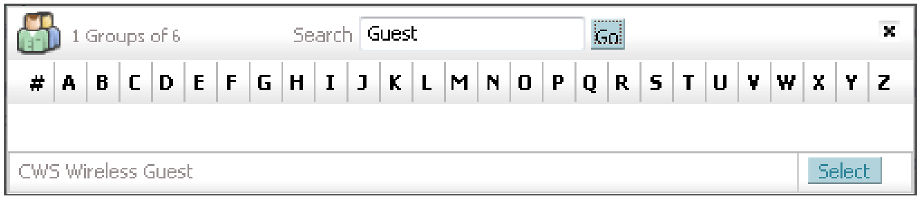
Step 13: Click **Create a rule**.

Step 14: Assign a name to the rule (Example: Block_Blocked_Sites_Guest), and then select **Active**.

Step 15: In the **Rule Action** list, choose **Block**.

Step 16: In the Define Group pane, click **Add group**.

Step 17: On the dialog box, in the **Search** box, enter the name of the group created in Step 4, and then click **Go**.



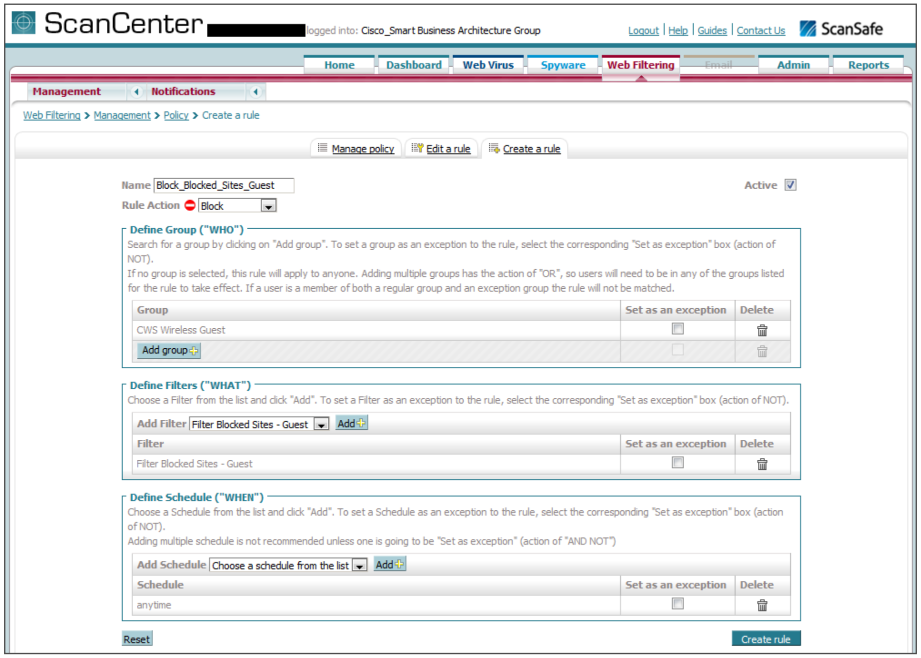
Search: Guest

CWS Wireless Guest

Step 18: Click **Select**, and then click **Confirm Selection**.

Step 19: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 8 (Example: Filter Blocked Sites - Guest), and then click **Add**.

Step 20: Click **Create rule**. The policy rule has now been created.



[redacted] logged into: Cisco_Smart Business Architecture Group

Web Filtering > Management > Policy > Create a rule

Name Block_Blocked_Sites_Guest

Active ☑

Rule Action Block

Define Group ("WHO")

Search for a group by clicking on "Add group". To set a group as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect. If a user is a member of both a regular group and an exception group the rule will not be matched.

Group	Set as an exception	Delete
CWS Wireless Guest	☐	🗑
Add group	☐	🗑

Define Filters ("WHAT")

Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

Add Filter Filter Blocked Sites - Guest

Filter	Set as an exception	Delete
Filter Blocked Sites - Guest	☐	🗑

Define Schedule ("WHEN")

Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).

Adding multiple schedule is not recommended unless one is going to be "Set as exception" (action of "AND NOT")

Add Schedule Choose a schedule from the list

Schedule	Set as an exception	Delete
anytime	☐	🗑

Next, create a new rule.

Step 21: Click **Create a rule**.

Step 22: Assign a name to the rule (Example: Warn_Warned_Sites_Guest), and then select **Active**.

Step 23: In the **Rule Action** list, choose **Warn**.

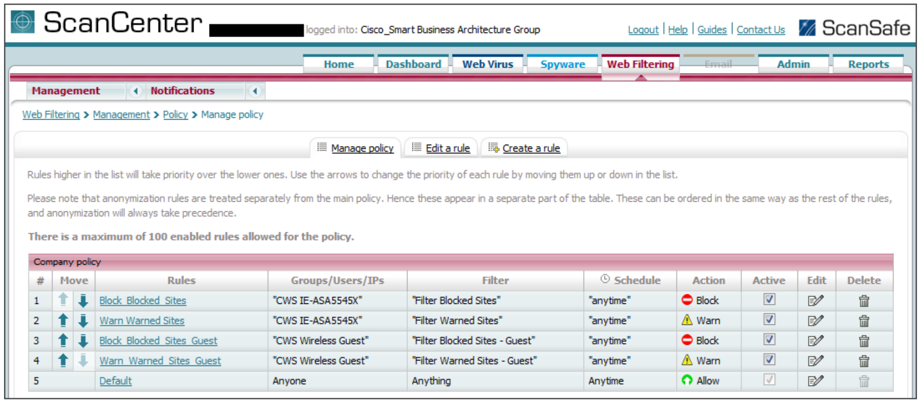
Step 24: In the Define Group pane, click **Add group**.

Step 25: On the dialog box, in the search box, enter the name of the group created in Step 4, and then click **Go**.

Step 26: Click **Select**, and then click **Confirm Selection**.

Step 27: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 10 (Example: Filter Warned Sites - Guest), and then click **Add**.

Step 28: Click **Create rule**. The policy rule has now been created.



[redacted] logged into: Cisco_Smart Business Architecture Group

Web Filtering > Management > Policy > Manage policy

Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.

There is a maximum of 100 enabled rules allowed for the policy.

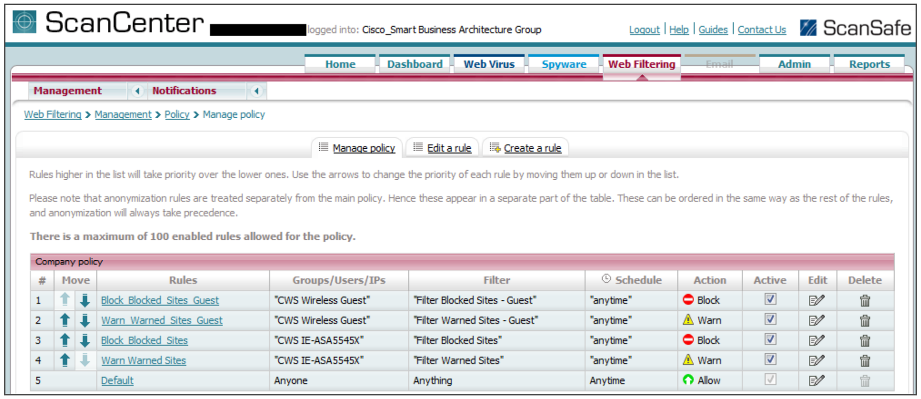
Company policy

#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	↑ ↓	Block_Blocked_Sites	"CWS IE-ASA5545X"	"Filter Blocked Sites"	"anytime"	Block	☑	✎	🗑
2	↑ ↓	Warn Warned Sites	"CWS IE-ASA5545X"	"Filter Warned Sites"	"anytime"	Warn	☑	✎	🗑
3	↑ ↓	Block_Blocked_Sites_Guest	"CWS Wireless Guest"	"Filter Blocked Sites - Guest"	"anytime"	Block	☑	✎	🗑
4	↑ ↓	Warn_Warned_Sites_Guest	"CWS Wireless Guest"	"Filter Warned Sites - Guest"	"anytime"	Warn	☑	✎	🗑
5		Default	Anyone	Anything	Anytime	Allow	☑	✎	🗑

Since the guest user traffic and internal user traffic is all redirected from the same Cisco ASA, the same group key is used. In order to properly match the guest traffic by the source IP address, the guest rules must be evaluated first.

Step 29: Click the Up arrow next to the Block_Blocked_Sites_Guest rule until it is listed first.

Step 30: Click the Up arrow next to the Warn_Warned_Sites_Guest rule until it is listed second, and then click **Apply Changes**.



[redacted] logged into: Cisco_Smart Business Architecture Group

Web Filtering > Management > Policy > Manage policy

Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.

There is a maximum of 100 enabled rules allowed for the policy.

Company policy

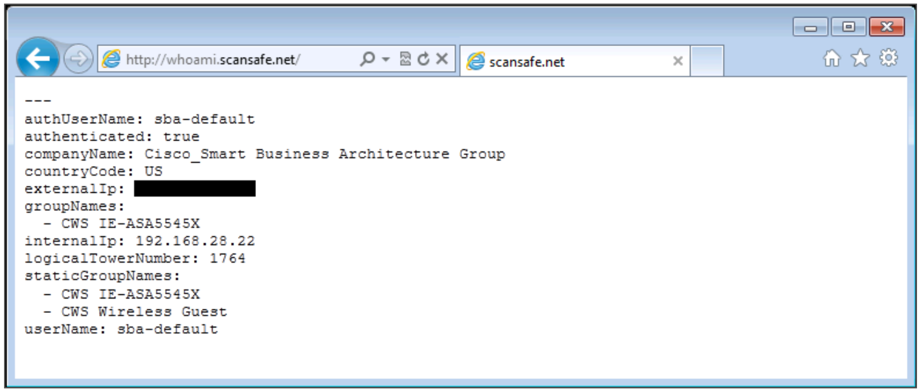
#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	↑ ↓	Block_Blocked_Sites_Guest	"CWS Wireless Guest"	"Filter Blocked Sites - Guest"	"anytime"	Block	☑	✎	🗑
2	↑ ↓	Warn_Warned_Sites_Guest	"CWS Wireless Guest"	"Filter Warned Sites - Guest"	"anytime"	Warn	☑	✎	🗑
3	↑ ↓	Block_Blocked_Sites	"CWS IE-ASA5545X"	"Filter Blocked Sites"	"anytime"	Block	☑	✎	🗑
4	↑ ↓	Warn Warned Sites	"CWS IE-ASA5545X"	"Filter Warned Sites"	"anytime"	Warn	☑	✎	🗑
5		Default	Anyone	Anything	Anytime	Allow	☑	✎	🗑

Procedure 2 Test Cloud Web Security

Step 1: From a client machine on the guest network, open a web browser to the following website:

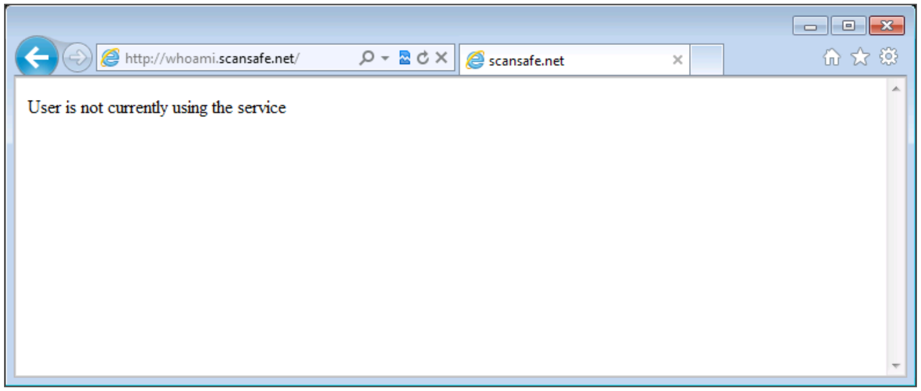
http://whoami.scansafe.net

This website returns diagnostic information from the Cisco CWS service.



```
---
authUserName: sba-default
authenticated: true
companyName: Cisco_Smart Business Architecture Group
countryCode: US
externalIp: [redacted]
groupNames:
  - CWS IE-ASA5545X
internalIp: 192.168.28.22
logicalTowerNumber: 1764
staticGroupNames:
  - CWS IE-ASA5545X
  - CWS Wireless Guest
userName: sba-default
```

If the service is not active, the following information is returned.



User is not currently using the service

Notes

Appendix A: Product List

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(6)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Web Security

Functional Area	Product Description	Part Numbers	Software
Cloud Web Security	Cisco Cloud Web Security (ScanSafe)	Cisco Cloud Web Security	—
	Cisco Cloud Web Security (ScanSafe)	Please Contact your Cisco Cloud Web Security Sales Representative for Part Numbers: scansafe-sales-questions@cisco.com	

IE-ASA5545X

```
ASA Version 9.0(1)
!
hostname IE-ASA5545X
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RA-pool 10.4.28.1-10.4.31.254 mask 255.255.252.0
!
interface GigabitEthernet0/0
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/0.300
 vlan 300
 nameif inside
 security-level 100
 ip address 10.4.24.30 255.255.255.224 standby 10.4.24.29
 summary-address eigrp 100 10.4.28.0 255.255.252.0 5
!
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.1116
 description Web Server connection on VLAN 116
 vlan 1116
 nameif dmz-web
 security-level 50
 ip address 192.168.16.1 255.255.255.0 standby 192.168.16.2
 ipv6 address 2001:db8:a:1::1/64 standby 2001:db8:a:1::2
 ipv6 enable
!
interface GigabitEthernet0/1.1117
 vlan 1117
 nameif dmz-email
 security-level 50
 ip address 192.168.17.1 255.255.255.0 standby 192.168.17.2
!
interface GigabitEthernet0/1.1118
 vlan 1118
 nameif dmz-dmvpn
 security-level 75
 ip address 192.168.18.1 255.255.255.0 standby 192.168.18.2
!
interface GigabitEthernet0/1.1119
 vlan 1119
 nameif dmz-wlc
 security-level 50
 ip address 192.168.19.1 255.255.255.0 standby 192.168.19.2
!
```

```
interface GigabitEthernet0/1.1122
 description Interface to the TMG DMZ
 vlan 1122
 nameif dmz-tmg
 security-level 50
 ip address 192.168.22.1 255.255.255.0 standby 192.168.22.2
!
interface GigabitEthernet0/1.1123
 vlan 1123
 nameif dmz-management
 security-level 50
 ip address 192.168.23.1 255.255.255.0 standby 192.168.23.2
!
interface GigabitEthernet0/1.1128
 vlan 1128
 nameif dmz-guests
 security-level 10
 ip address 192.168.28.1 255.255.252.0 standby 192.168.28.2
!
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
!
interface GigabitEthernet0/3
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3.16
 description Primary Internet connection on VLAN 16
 vlan 16
 nameif outside-16
 security-level 0
 ip address 172.16.130.124 255.255.255.0 standby 172.16.130.123
 ipv6 address 2001:db8:a::1/64 standby 2001:db8:a::2
 ipv6 enable
!
interface GigabitEthernet0/3.17
 description Resilient Internet connection on VLAN 17
 vlan 17
 nameif outside-17
 security-level 0
 ip address 172.17.130.124 255.255.255.0 standby 172.17.130.123
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif IPS-mgmt
 security-level 0
 no ip address
!
boot system disk0:/asa901-smp-k8.bin
```

```
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 10.4.48.10
 domain-name cisco.local
same-security-traffic permit intra-interface
object network internal-network
 subnet 10.4.0.0 255.254.0.0
 description The organization’s internal network range
object network dmz-networks
 subnet 192.168.16.0 255.255.248.0
 description The organization’s DMZ network range
object network internal-network-ISPa
 subnet 10.4.0.0 255.254.0.0
 description PAT traffic from inside out the primary Internet connection
object network internal-network-ISPb
 subnet 10.4.0.0 255.254.0.0
 description PAT traffic from inside out the secondary internet connection
object network outside-webserver-ISPa
 host 172.16.130.100
 description WebServer on ISP A
object network dmz-webserver-ISPa
 host 192.168.16.100
object network outside-webserver-ISPb
 host 172.17.130.100
 description WebServer on ISPb
object network dmz-webserver-ISPb
 host 192.168.16.100
 description NAT the webserver in the DMZ to outside address on ISP B
object network dmz-dmvpn-1
 host 192.168.18.10
 description NAT the primary DMVPN hub router in the DMZ to ISP A
object network dmz-dmvpn-2
 host 192.168.18.11
 description NAT the secondary DMVPN hub router in the DMZ to ISP B
object network outside-dmvpn-ISPa
 host 172.16.130.1
 description DMVPN hub router on ISP A
object network outside-dmvpn-ISPb
 host 172.17.130.1
 description DMVPN hub router on ISP B
object network dmz-web-net-v6
 subnet 2001:db8:a:1::/64
object network dmz-webserver-ispa-v6
 host 192.168.16.111
object network outside-webserver-ispa-v6
 host 2001:db8:a::111
object network dmz-ipv6-natpool
 range 192.168.16.32 192.168.16.63
object network outside-IPv6-all
 subnet ::/0
object network dmz-guest-network-ISPa
 subnet 192.168.28.0 255.255.252.0
 description DMZ outside PAT addresses for ISPa
object network internal-wlc-5508
 host 10.4.46.64
 description Internal 5508 WLC
object network internal-wlc-flex-7500
 host 10.4.46.68
 description Internal FlexConnect 7500 WLC
object network dmz-wlc-2504-1
 host 192.168.19.56
 description Primary 2504 Anchor Controller for Guest Wireless Access
object network dmz-wlc-5508
 host 192.168.19.54
 description 5508 Anchor Controller for Guest Wireless Access
object network dmz-wlc-2504-2
```

```
 host 192.168.19.57
 description Resilient 2504 Anchor Controller for Guest Wireless
object network internal-aaa
 host 10.4.48.15
 description Internal AAA Server
object network internal-ntp
 host 10.4.48.17
 description Internal NTP Server
object network internal-dhcp
 host 10.4.48.10
 description Internal DHCP Server
object network internal-dns
 host 10.4.48.10
 description Internal DNS Server
object network dmz-wlc-primary-5508-RP
 host 192.168.19.154
 description Primary WLC Redundancy Port
object network dmz-wlc-resilient-5508-RP
 host 192.168.19.155
 description Resilient WLC Redundancy Port
object network internal-exchange
 host 10.4.48.25
 description Internal Exchange server
object network NETWORK_OBJ_10.4.28.0_22
 subnet 10.4.28.0 255.255.252.0
object network internal_ISE-1
 host 10.4.48.46
 description Internal ISE-AdvGuest Server
object network outside-esa-ISPa
 host 172.16.130.25
object network dmz-esa370-ISPa
 host 192.168.17.25
 description ESAc370 on email DMZ
object network outside-esa-ISPb
 host 172.17.130.25
object network dmz-esa370-ISPb
 host 192.168.17.25
```

```
 description ESAc370 on email DMZ
object network 5505-pool
 subnet 10.4.156.0 255.255.252.0
 description 5505 Teleworker Subnet
object network asdm-websecproxy-115-111-223-66
 host 115.111.223.66
object network asdm-websecproxy-122-50-127-66
 host 122.50.127.66
object network asdm-websecproxy-184-150-236-66
 host 184.150.236.66
object network asdm-websecproxy-196-26-220-66
 host 196.26.220.66
object network asdm-websecproxy-201-94-155-66
 host 201.94.155.66
object network asdm-websecproxy-202-167-250-90
 host 202.167.250.90
object network asdm-websecproxy-202-167-250-98
 host 202.167.250.98
object network asdm-websecproxy-202-177-218-66
 host 202.177.218.66
object network asdm-websecproxy-202-79-203-98
 host 202.79.203.98
object network asdm-websecproxy-46-255-40-58
 host 46.255.40.58
object network asdm-websecproxy-46-255-40-90
 host 46.255.40.90
object network asdm-websecproxy-46-255-40-98
 host 46.255.40.98
object network asdm-websecproxy-69-10-152-66
 host 69.10.152.66
object network asdm-websecproxy-69-174-58-179
 host 69.174.58.179
object network asdm-websecproxy-69-174-58-187
 host 69.174.58.187
object network asdm-websecproxy-69-174-87-131
 host 69.174.87.131
object network asdm-websecproxy-69-174-87-163
```

```
 host 69.174.87.163
object network asdm-websecproxy-69-174-87-171
 host 69.174.87.171
object network asdm-websecproxy-69-174-87-75
 host 69.174.87.75
object network asdm-websecproxy-70-39-176-115
 host 70.39.176.115
object network asdm-websecproxy-70-39-176-123
 host 70.39.176.123
object network asdm-websecproxy-70-39-176-131
 host 70.39.176.131
object network asdm-websecproxy-70-39-176-139
 host 70.39.176.139
object network asdm-websecproxy-70-39-176-35
 host 70.39.176.35
object network asdm-websecproxy-70-39-176-59
 host 70.39.176.59
object network asdm-websecproxy-70-39-177-35
 host 70.39.177.35
object network asdm-websecproxy-70-39-177-43
 host 70.39.177.43
object network asdm-websecproxy-70-39-231-107
 host 70.39.231.107
object network asdm-websecproxy-70-39-231-163
 host 70.39.231.163
object network asdm-websecproxy-70-39-231-171
 host 70.39.231.171
object network asdm-websecproxy-70-39-231-180
 host 70.39.231.180
object network asdm-websecproxy-70-39-231-182
 host 70.39.231.182
object network asdm-websecproxy-70-39-231-188
 host 70.39.231.188
object network asdm-websecproxy-70-39-231-190
 host 70.39.231.190
object network asdm-websecproxy-70-39-231-91
 host 70.39.231.91
object network asdm-websecproxy-72-37-244-163
 host 72.37.244.163
object network asdm-websecproxy-72-37-244-171
 host 72.37.244.171
object network asdm-websecproxy-72-37-248-19
 host 72.37.248.19
object network asdm-websecproxy-72-37-248-27
 host 72.37.248.27
object network asdm-websecproxy-72-37-249-139
 host 72.37.249.139
object network asdm-websecproxy-72-37-249-147
 host 72.37.249.147
object network asdm-websecproxy-72-37-249-163
 host 72.37.249.163
object network asdm-websecproxy-72-37-249-171
 host 72.37.249.171
object network asdm-websecproxy-72-37-249-195
 host 72.37.249.195
object network asdm-websecproxy-72-37-249-203
 host 72.37.249.203
object network asdm-websecproxy-80-254-147-251
 host 80.254.147.251
object network asdm-websecproxy-80-254-148-194
 host 80.254.148.194
object network asdm-websecproxy-80-254-150-66
 host 80.254.150.66
object network asdm-websecproxy-80-254-154-66
 host 80.254.154.66
object network asdm-websecproxy-80-254-154-98
 host 80.254.154.98
object network asdm-websecproxy-80-254-155-66
 host 80.254.155.66
object network asdm-websecproxy-80-254-158-147
 host 80.254.158.147
object network asdm-websecproxy-80-254-158-155
 host 80.254.158.155
object network asdm-websecproxy-80-254-158-179
```

```
 host 80.254.158.179
object network asdm-websecproxy-80-254-158-187
 host 80.254.158.187
object network asdm-websecproxy-80-254-158-211
 host 80.254.158.211
object network asdm-websecproxy-80-254-158-219
 host 80.254.158.219
object network asdm-websecproxy-80-254-158-35
 host 80.254.158.35
object network dmz-tmg-ISPa
 host 192.168.22.25
 description TMG on dmz-tmg
object network dmz-tmg-ISPb
 host 192.168.22.25
 description TMG on dmz-tmg
object network outside-tmg-ISPa
 host 172.16.130.55
 description TMG server on ISP-A
object network outside-tmg-ISPb
 host 172.17.130.55
 description TMG server on ISP-B
object network internal-ad
 host 10.4.48.10
 description Internal Active Directory Server
object-group service DM_INLINE_SERVICE_1
 service-object tcp destination eq ftp
 service-object tcp destination eq ftp-data
 service-object tcp destination eq tacacs
 service-object udp destination eq ntp
 service-object udp destination eq syslog
object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_2 tcp
 port-object eq www
 port-object eq https
object-group icmp-type DM_INLINE_ICMP_1
 icmp-object echo
 icmp-object echo-reply
object-group service DM_INLINE_SERVICE_2
 service-object esp
 service-object udp destination eq 4500
 service-object udp destination eq isakmp
object-group service DM_INLINE_SERVICE_3
 service-object esp
 service-object udp destination eq 4500
 service-object udp destination eq isakmp
object-group service DM_INLINE_TCP_3 tcp
 port-object eq www
 port-object eq https
object-group network internal-wlc-group
 description Internal Wireless LAN Controllers
 network-object object internal-wlc-5508
 network-object object internal-wlc-flex-7500
object-group network dmz-wlc-group
 description Wireless LAN Controllers in the DMZ
 network-object object dmz-wlc-2504-1
 network-object object dmz-wlc-5508
 network-object object dmz-wlc-2504-2
object-group service DM_INLINE_SERVICE_4
 service-object tcp destination eq tacacs
 service-object udp destination eq 1812
 service-object udp destination eq 1813
object-group service DM_INLINE_TCP_4 tcp
 port-object eq ftp
 port-object eq ftp-data
object-group service DM_INLINE_SERVICE_5
 service-object 97
 service-object udp destination eq 16666
 service-object udp destination eq 5246
 service-object udp destination eq 5247
object-group service DM_INLINE_SERVICE_6
 service-object tcp destination eq domain
 service-object udp destination eq domain
```

```
object-group network DM_INLINE_NETWORK_1
 network-object object dmz-networks
 network-object object internal-network
object-group service DM_INLINE_TCP_5 tcp
 port-object eq www
 port-object eq https
object-group network dmz-wlc-RP-group
 description DMZ Wireless LAN Controllers Redundancy Port Group
 network-object object dmz-wlc-primary-5508-RP
 network-object object dmz-wlc-resilient-5508-RP
object-group service DM_INLINE_UDP_1 udp
 port-object eq 1812
 port-object eq 1813
object-group service DM_INLINE_TCP_6 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_TCP_7 tcp
 port-object eq www
 port-object eq https
object-group service DM_INLINE_SERVICE_7
 service-object tcp destination eq 135
 service-object tcp destination eq 445
 service-object tcp destination eq kerberos
 service-object tcp destination eq ldap
 service-object udp destination eq 389
 service-object udp destination eq ntp
object-group service DM_INLINE_TCP_8 tcp
 port-object eq www
 port-object eq https
access-list global_access remark Permit management protocols from the management DMZ to the internal network
access-list global_access extended permit object-group DM_INLINE_SERVICE_1 192.168.23.0 255.255.255.0 object internal-network
access-list global_access remark Allow anyone to access the webservers in the DMZ
access-list global_access extended permit tcp any 192.168.16.0 255.255.255.0 object-group DM_INLINE_TCP_1
access-list global_access extended permit icmp any 192.168.18.0 255.255.255.0 object-group DM_INLINE_ICMP_1
access-list global_access extended permit object-group DM_INLINE_SERVICE_3 any object dmz-dmvpn-2
access-list global_access remark Allow traffic to the DMVPN hub routers
access-list global_access extended permit object-group DM_INLINE_SERVICE_2 any object dmz-dmvpn-1
access-list global_access remark Allow WLC’s to communicate with the NTP server locate din the data center.
access-list global_access extended permit udp object-group dmz-wlc-group object internal-ntp eq ntp
access-list global_access remark Allow DMZ based WLC’s to communicate with the AAA/ACS Server on the internal network.
access-list global_access extended permit object-group DM_INLINE_SERVICE_4 object-group dmz-wlc-group object internal-aaa
access-list global_access extended permit tcp object-group dmz-wlc-group any object-group DM_INLINE_TCP_4
access-list global_access remark Allow DMZ based WLC’s to communicate with the internal WLC’s
access-list global_access extended permit object-group DM_INLINE_SERVICE_5 object-group dmz-wlc-group object-group internal-wlc-group
access-list global_access remark Allow DMZ WLC’s to obtain IP address via internal DHCP server
access-list global_access extended permit udp object-group dmz-wlc-group object internal-dhcp eq bootps
access-list global_access remark Allow wireless guest users to obtain an IP address from the internal DHCP server.
access-list global_access extended permit udp 192.168.28.0 255.255.252.0 object internal-dhcp eq bootps
access-list global_access remark Allow Guest Wireless Users to resolve DNS names.
access-list global_access extended permit object-group DM_INLINE_SERVICE_6 192.168.28.0 255.255.252.0 object internal-dns
access-list global_access remark Allow wireless guest users access to the DMZ based webservers, possibly for walled garden
```

```
access
access-list global_access extended permit tcp 192.168.28.0 
255.255.252.0 192.168.16.0 255.255.255.0 object-group DM_INLINE_
TCP_5
access-list global_access remark Allow Standby AP-SSO WLC’s to 
communicate to internal NTP server using RP Port
access-list global_access extended permit udp object-group dmz-
wlc-RP-group object internal-ntp eq ntp
access-list global_access remark Allow ELC to connect to ISE
access-list global_access extended permit udp 192.168.19.0 
255.255.255.0 object internal_ISE-1 object-group DM_INLINE_UDP_1
access-list global_access remark guest client web auth access to 
ISE
access-list global_access extended permit tcp 192.168.28.0 
255.255.252.0 object internal_ISE-1 eq 8443
access-list global_access remark Deny traffic from the wireless 
guest network to the internal and dmz resources
access-list global_access extended deny ip 192.168.28.0 
255.255.252.0 object-group DM_INLINE_NETWORK_1
access-list global_access remark Allow Wireless DMZ users access 
to the internet
access-list global_access extended permit ip 192.168.28.0 
255.255.252.0 any
access-list global_access remark Exchange to ESA outbound SMTP
access-list global_access extended permit tcp object internal-
exchange 192.168.17.0 255.255.255.0 eq smtp
access-list global_access remark Block other outbound SMTP
access-list global_access extended deny tcp object internal-
network any4 eq smtp
access-list global_access remark Internet to ESA inbound SMTP
access-list global_access extended permit tcp any4 192.168.17.0 
255.255.255.0 eq smtp
access-list global_access remark ESA to Exchange inbound SMTP
access-list global_access extended permit tcp 192.168.17.0 
255.255.255.0 object internal-exchange eq smtp
access-list global_access remark DNS
access-list global_access extended permit udp 192.168.17.0 
255.255.255.0 object internal-dns eq domain
access-list global_access remark NTP
access-list global_access extended permit udp 192.168.17.0 
255.255.255.0 object internal-ntp eq ntp
access-list global_access remark Block other to internal networks
access-list global_access extended deny ip 192.168.17.0 
255.255.255.0 object internal-network
access-list global_access remark ESA to internet outbound SMTP
access-list global_access extended permit tcp 192.168.17.0 
255.255.255.0 any4 eq smtp
access-list global_access remark HTTP to Internet
access-list global_access extended permit tcp 192.168.17.0 
255.255.255.0 any4 eq www
access-list global_access remark HTTPS to Internet
access-list global_access extended permit tcp 192.168.17.0 
255.255.255.0 any4 eq https
access-list global_access remark Deny IP traffic from the DMZ to 
any other network
access-list global_access extended deny ip object dmz-networks 
any4
access-list global_access extended deny tcp object internal-
network any4 eq telnet
access-list global_access extended permit ip object internal-
network any4 log disable
access-list global_access extended permit tcp any6 object dmz-
web-net-v6 object-group DM_INLINE_TCP_2
access-list global_access extended permit tcp any6 object dmz-
webserver-ispa-v6 object-group DM_INLINE_TCP_3
access-list global_access remark Permint HTTP/HTTPS traffic onto 
the TMG DMZ
access-list global_access extended permit tcp any4 192.168.22.0 
255.255.255.0 object-group DM_INLINE_TCP_6
access-list global_access remark Permit HTTP/HTTPS from TMG to 
the internal Exchange Server
access-list global_access extended permit tcp 192.168.22.0 
255.255.255.0 object internal-exchange object-group DM_INLINE_
TCP_7 log disable
```

```
access-list global_access remark Internal DNS
access-list global_access extended permit udp 192.168.22.0 255.255.255.0 object internal-dns eq domain
access-list global_access remark TMG Server requires HTTP/HTTPS to get to the internet for updates.
access-list global_access extended permit tcp 192.168.22.0 255.255.255.0 any4 object-group DM_INLINE_TCP_8
access-list global_access extended permit object-group DM_INLINE_SERVICE_7 192.168.22.0 255.255.255.0 object internal-ad
access-list global_mpc extended permit ip any4 any4
access-list RA_PartnerACL remark Partners can access this host only.
access-list RA_PartnerACL standard permit host 10.4.48.35
access-list RA_SplitTunnelACL remark Internal Networks
access-list RA_SplitTunnelACL standard permit 10.4.0.0 255.254.0.0
access-list RA_SplitTunnelACL remark DMZ networks
access-list RA_SplitTunnelACL standard permit 192.168.16.0 255.255.248.0
access-list WCCP_Redirect_List remark Block RFC-1918 10.0.0.0/8
access-list WCCP_Redirect_List extended deny ip any4 10.0.0.0 255.0.0.0
access-list WCCP_Redirect_List remark Block RFC-1918 172.16.0.0/12
access-list WCCP_Redirect_List extended deny ip any4 172.16.0.0 255.240.0.0
access-list WCCP_Redirect_List remark Block RFC-1918 192.168.0.0/16
access-list WCCP_Redirect_List extended deny ip any4 192.168.0.0 255.255.0.0
access-list WCCP_Redirect_List remark Permit all others
access-list WCCP_Redirect_List extended permit ip any4 any4
access-list global_mpc_1 remark Do not match any to internal networks
access-list global_mpc_1 extended deny ip any4 object internal-network
access-list global_mpc_1 remark Do not match any to DMZ networks
access-list global_mpc_1 extended deny ip any4 object dmz-networks
access-list global_mpc_1 remark Match HTTP to any other networks
access-list global_mpc_1 extended permit tcp any4 any4 eq www
access-list Block_Trusted_Host remark Trusted Host is 10.4.48.10:443
access-list Block_Trusted_Host extended deny tcp any4 host 10.4.48.10 eq https
access-list Block_Trusted_Host remark Permit all other traffic
access-list Block_Trusted_Host extended permit ip any4 any4
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-35 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-147-251 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-155 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-147 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-179 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-websecproxy-80-254-158-187 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
```

```
websecproxy-80-254-158-211 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-80-254-158-219 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-80-254-148-194 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-46-255-40-58 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-46-255-40-90 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-46-255-40-98 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-80-254-150-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-80-254-154-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-80-254-154-98 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-80-254-155-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-196-26-220-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-201-94-155-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-184-150-236-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-69-10-152-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-244-171 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-244-163 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-248-19 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-248-27 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-107 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
```

```
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-91 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-171 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-163 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-180 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-182 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-188 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-231-190 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-69-174-58-179 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-69-174-58-187 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-176-35 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-176-59 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-176-115 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-176-123 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-176-131 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-176-139 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-249-171 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-249-163 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-249-139 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
```

```
websecproxy-72-37-249-147 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-249-195 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-72-37-249-203 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-177-35 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-70-39-177-43 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-69-174-87-75 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-69-174-87-171 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-69-174-87-131 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-69-174-87-163 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-202-167-250-98 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-202-167-250-90 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-115-111-223-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-122-50-127-66 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-202-79-203-98 any
access-list CWS_Tower_Exclude remark ASDM-generated Web Security 
proxy ACE
access-list CWS_Tower_Exclude extended permit ip object asdm-
websecproxy-202-177-218-66 any
!
scansafe general-options
 server primary ip 72.37.248.27 port 8080
 server backup ip 69.174.58.187 port 8080
 retry-count 5
 license 6B2F23DCD7704A3947F02CBA6A17BCF2
!
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu dmz-web 1500
mtu dmz-email 1500
mtu dmz-dmvpn 1500
mtu dmz-wlc 1500
mtu dmz-tmg 1500
mtu dmz-management 1500
mtu dmz-guests 1500
mtu outside-16 1500
mtu outside-17 1500
mtu IPS-mgmt 1500
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/2
failover polltime unit msec 200 holdtime msec 800
failover polltime interface msec 500 holdtime 5
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2
failover interface ip failover 10.4.24.33 255.255.255.248 standby 
10.4.24.34
monitor-interface inside
monitor-interface dmz-web
monitor-interface dmz-email
monitor-interface dmz-dmvpn
monitor-interface dmz-wlc
monitor-interface dmz-tmg
monitor-interface dmz-management
monitor-interface dmz-guests
monitor-interface outside-16
monitor-interface outside-17
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-702.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (inside,outside-17) source static any any destination static 
NETWORK_OBJ_10.4.28.0_22 NETWORK_OBJ_10.4.28.0_22 no-proxy-arp 
route-lookup
nat (inside,outside-16) source static any any destination static 
NETWORK_OBJ_10.4.28.0_22 NETWORK_OBJ_10.4.28.0_22 no-proxy-arp 
route-lookup
nat (any,any) source static internal-network internal-network 
destination static 5505-pool 5505-pool
!
object network internal-network-ISPa
 nat (any,outside-16) dynamic interface
object network internal-network-ISPb
 nat (any,outside-17) dynamic interface
object network dmz-webserver-ISPa
 nat (any,outside-16) static outside-webserver-ISPa
object network dmz-webserver-ISPb
 nat (any,outside-17) static outside-webserver-ISPb
object network dmz-dmvpn-1
 nat (any,any) static outside-dmvpn-ISPa net-to-net
object network dmz-dmvpn-2
 nat (any,any) static outside-dmvpn-ISPb net-to-net
object network outside-IPv6-all
 nat (outside-16,dmz-web) dynamic pat-pool dmz-ipv6-natpool 
round-robin
object network dmz-guest-network-ISPa
 nat (any,outside-16) dynamic interface
object network dmz-esa370-ISPa
 nat (any,outside-16) static outside-esa-ISPa
object network dmz-esa370-ISPb
 nat (any,outside-17) static outside-esa-ISPb
object network dmz-tmg-ISPa
 nat (dmz-tmg,outside-16) static outside-tmg-ISPa
object network dmz-tmg-ISPb
 nat (dmz-tmg,outside-17) static outside-tmg-ISPb
access-group global_access global
ipv6 route outside-16 ::/0 2001:db8:a::7206
!
router eigrp 100
 no auto-summary
 network 10.4.24.0 255.255.252.0
 network 192.168.16.0 255.255.248.0
 passive-interface default
 no passive-interface inside
 redistribute static
```

```
!
route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 1 track 1
route outside-17 0.0.0.0 0.0.0.0 172.17.130.126 50
route outside-16 172.18.1.1 255.255.255.255 172.16.130.126 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15
 key SecretKey
aaa-server AAA-RADIUS protocol radius
aaa-server AAA-RADIUS (inside) host 10.4.48.15
 key SecretKey
 radius-common-pw SecretKey
aaa authentication enable console AAA-SERVER LOCAL
aaa authentication ssh console AAA-SERVER LOCAL
aaa authentication http console AAA-SERVER LOCAL
aaa authentication serial console AAA-SERVER LOCAL
aaa authorization exec authentication-server
http server enable
http 10.4.48.0 255.255.255.0 inside
snmp-server host inside 10.4.48.35 community cisco
no snmp-server location
no snmp-server contact
snmp-server community cisco
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
sla monitor 16
 type echo protocol ipIcmpEcho 172.18.1.1 interface outside-16
sla monitor schedule 16 life forever start-time now
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set reverse-route
crypto map outside-16_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside-16_map interface outside-16
crypto ca trustpoint _SmartCallHome_ServerCA
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=IE-ASA5545X
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint IE-ASA5545X-Trustpoint
```

```
 enrollment self
 subject-name CN=IE-ASA5545X.cisco.local
 keypair IE-ASA5545X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpoint IE-ASA5545X-FO-Trustpoint
 enrollment self
 subject-name CN=IE-ASA5545X-FO.cisco.local
 keypair IE-ASA5545X-Keypair
 proxy-ldc-issuer
 crl configure
crypto ca trustpool policy
crypto ikev1 enable outside-16
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
```

```
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 16 reachability
telnet timeout 5
ssh 10.4.48.0 255.255.255.0 inside
ssh timeout 5
ssh version 2
console timeout 0
!
```

```
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
wccp web-cache redirect-list WCCP_Redirect_List
wccp 90 redirect-list WCCP_Redirect_List
ntp server 10.4.48.17
ssl encryption aes256-sha1 aes128-sha1 3des-sha1
ssl trust-point IE-ASA5545X-Trustpoint outside-16
ssl trust-point IE-ASA5545X-FO-Trustpoint outside-17
webvpn
 enable outside-16
 enable outside-17
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
 anyconnect image disk0:/anyconnect-linux-3.1.00495-k9.pkg 2
 anyconnect image disk0:/anyconnect-macosx-i386-3.1.00495-k9.pkg 3
 anyconnect profiles RA-Profile disk0:/ra-profile.xml
 anyconnect profiles RA-WebSecurityProfile disk0:/ra-websecurityprofile.wsp
 anyconnect profiles RA-WebSecurityProfile.wso disk0:/ra-websecurityprofile.wso
 anyconnect enable
 tunnel-group-list enable
group-policy 5505Group internal
group-policy 5505Group attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev1
 password-storage disable
 split-tunnel-policy tunnelall
 default-domain value cisco.local
 secure-unit-authentication enable
 nem enable
group-policy GroupPolicy_Employee internal
```

```
group-policy GroupPolicy_Employee attributes
 banner value Group “vpn-employee” allows for unrestricted access with a tunnel all policy.
 vpn-filter value Block_Trusted_Host
 split-tunnel-policy excludespecified
 split-tunnel-network-list value CWS_Tower_Exclude
 webvpn
  anyconnect modules value websecurity
  anyconnect profiles value RA-Profile type user
  anyconnect profiles value RA-WebSecurityProfile.wso type websecurity
  always-on-vpn profile-setting
group-policy GroupPolicy_AnyConnect internal
group-policy GroupPolicy_AnyConnect attributes
 wins-server none
 dns-server value 10.4.48.10
 vpn-tunnel-protocol ssl-client
 default-domain value cisco.local
group-policy GroupPolicy_Partner internal
group-policy GroupPolicy_Partner attributes
 banner value Group “vpn-partner” allows for access control list (ACL) restricted access with a tunnel all policy.
 vpn-filter value RA_PartnerACL
 webvpn
  anyconnect profiles value RA-Profile type user
group-policy GroupPolicy_Administrator internal
group-policy GroupPolicy_Administrator attributes
 banner value Group “vpn-administrator” allows for unrestricted access with a split tunnel policy.
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value RA_SplitTunnelACL
 webvpn
  anyconnect profiles value RA-Profile type user
username admin password w2Y.6Op4j7clVDk2 encrypted privilege 15
tunnel-group AnyConnect type remote-access
tunnel-group AnyConnect general-attributes
 address-pool RA-pool
 authentication-server-group AAA-RADIUS
 default-group-policy GroupPolicy_AnyConnect
 password-management
tunnel-group AnyConnect webvpn-attributes
 group-alias AnyConnect enable
 group-url https://172.16.130.124/AnyConnect enable
 group-url https://172.17.130.124/AnyConnect enable
tunnel-group Teleworker5505 type remote-access
tunnel-group Teleworker5505 general-attributes
 authentication-server-group AAA-RADIUS
 default-group-policy 5505Group
tunnel-group Teleworker5505 ipsec-attributes
 ikev1 pre-shared-key cisco123
!
class-map global-class
 match access-list global_mpc
class-map cws-http-class
 description Class to match HTTP traffic for Cloud Web Security
 match access-list global_mpc_1
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map type inspect scansafe CWS-HTTP-80
 description Cloud Web Security TCP-80
 parameters
  default user sba-default
  http
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
 class global-class
  ips inline fail-close
 class cws-http-class
  inspect scansafe CWS-HTTP-80 fail-open
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/
oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 2
  subscribe-to-alert-group configuration periodic monthly 2
  subscribe-to-alert-group telemetry periodic daily
hpm topN enable
: end
```

Notes

Appendix C: Provisioning Email Example

From: ScanSafe Provisioning [mailto:provisioning@scansafe.net]
Subject: Provisioning Notification: Customer X / PO Ref:XXXXXXXX

On Day-Month-Year we completed the provisioning of the ScanSafe Web Security services for Customer X in accordance with the order details below:

Services:	Subscription Seats and Services
Term:	Subscription Months
Registered IP Addresses:	-None configured yet-
Domains:	-None configured yet-

The service is now available and you should make the necessary configuration changes described below to use the service. Please configure your system so that external Web traffic is sent via ScanSafe, using the explicit proxy setting below:

Primary Web Services Proxy Address:	proxyXXXX.scansafe.net
Web Services Proxy port:	8080
Secondary Web Services Proxy Address:	proxyXXXX.scansafe.net
Web Services Proxy port:	8080

The exact configuration changes required will vary depending in your specific existing infrastructure.

To log in to the service configuration Web portal and administer the service, please visit https://scancenter.scansafe.com/portal/admin/login.jsp and enter your email and password details below:

Email:	contact@CustomerX.com
Password :	-Not Shown-
Company ID:	XXXXXXXXXX

As part of our ongoing commitment to quality and service, a member of the ScanSafe Customer Services team will be in touch with you to ensure that the service is functioning according to your expectations.

If you require any assistance or experience any problems with the service, please do not hesitate to contact our support team.

We appreciate your choosing ScanSafe to provide Web security and look forward to a successful working partnership with you.

Customer Services

EMEA +44 (0) 207 034 9400

US + (1) 877 472 2680

support@scansafe.com

This email and any attachments are strictly confidential and intended for the addressee(s) only. If this email has been sent to you in error, please let us know by forwarding it to us at support@scansafe.com.

Neither ScanSafe nor its directors, officers or employees accepts any liability for the accuracy or completeness of this email. Unless expressly stated to the contrary, no contracts may be concluded on behalf of ScanSafe by means of e-mail communication.

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLiERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.