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/Aug13-290 For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd





BORDERLESS NETWORKS DEPLOYMENT GUIDE

11 11-1-

CISCO

SBA

Remote Mobile Access 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 10.5.204.5 255.255.2

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.

February 2013 Series

Table of Contents

What's In This SBA Guide	1
Cisco SBA Borderless Networks	1
Route to Success	1
About This Guide	1
Introduction	2
Business Overview	2
Technology Overview	3
Deployment Details	5
Configuring Access for Laptop Devices	5
Configuring Access for Mobile Devices: ActiveSync2	2
Configuring Access for Mobile Devices: AnyConnect Client2	8
Configure and connect mobile devices2	8

Appendix A: Product List	36
Appendix B: Configuration Example	38
Appendix C: Changes.	.51

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



Introduction

One of the most profound advances in modern networks is the degree of mobility those networks support. Users can move around wirelessly inside the campus and enjoy the same degree of connectivity as if they were plugged in using cables in their offices. Users can leave their primary networks completely and work from a home-office environment that offers the same connectivity and user experience as they would get in their offices. Users also have the option of being truly mobile and connecting from any place that offers Internet access. With smartphones and tablets, this mobility now commonly includes connecting while travelling down the highway or on a train. This guide describes business-use cases related to the truly mobile users who use a laptop, smartphone, or tablet device to connect through infrastructure that is not provided by their organizations. The guide does not cover use cases related to campus wireless access or home teleworker solutions.

Business Overview

As users move outside the boundaries of the traditional network, their requirements for access to job-related data, such as email, calendars, and more, don't change. To be productive, the network needs to allow users access wherever they are to whatever data they need to accomplish their tasks, from any device the organization allows. At the same time, the network must ensure that all access is secure and appropriate and that it follows organizational guidelines.

Mobile remote users connect using devices that can generally be broken down into two categories: laptop computers and the new group of mobile devices, such as smartphones and tablets. Networks have handled laptops for years. The newer mobile devices are being integrated currently. This integration continues to challenge network design and administration.

An organization's network must meet many requirements today that are sometimes contradictory. The network must be secure and prevent unauthorized access while being open enough to allow users to do their jobs regardless of where they are. As the mobility of users has increased, the requirements the network must meet have increased. In the past, a worker might have needed laptop connectivity while at the office or at home. Today, a worker needs access to the network from a smartphone while traveling, from a laptop while on site at a customer's or partner's office, or from both while sitting in the local coffee shop. And although providing this access is the primary requirement for the network, other requirements, such as ease of use and security, have not been relaxed.

Because these mobile users are outside the traditional perimeter (or physical border) of the network, their devices are exposed to potentially more malicious activity than a device that is located inside the protection of the network. So protection of the end device and the data being accessed and stored is critical. The mobile user's device needs to have protection from things such as malware and viruses. Ideally, this protection occurs even if the device is not connected to the headquarters network or if such a connection isn't possible. Because many mobile devices are smaller and are used much more often than a laptop, they are also more easily lost or stolen. In today's security environment where these devices potentially carry the same information that a laptop might, there is a need to protect the data on the devices and prevent unauthorized users from retrieving it.

As a standard part of their processes and guidelines, many organizations are required to control what sites users access on the Internet while they are using organizational resources. Providing this level of control for mobile users who do not reside within the boundaries of the network is challenging. To provide a complete solution, the network enforces standard access guidelines on the device, whether the device resides inside the headquarters or is connecting from a coffee shop. The end users should have similar experiences inside or outside the traditional network perimeter. They should also receive the same protection from malware whether they are inside the network or outside.

An often-overlooked component of access is ease of use. Having to check whether a secure connection is needed and enabled and having to constantly enter user credentials on a mobile device to enable a secure connection might make users look for ways to bypass the solution. Thus, a solution that is as integrated and seamless as possible doesn't impact users, hamper their day-to-day activities, or reduce their productivity as significantly. As part of ease of use, the solution should be automated as much as the platform allows, preventing users from either forgetting to follow the procedure or specifically trying to bypass procedures because they feel the procedures are restrictive. As more users move outside the boundaries of the network, a corresponding increase in network load occurs on the organization's Internet connection. This can raise costs. Intelligent routing of traffic is a priority to control which traffic from a user has to go through the Internet edge component of the organization's network and which traffic can be kept out on the Internet. Reducing security on this traffic is not an option that is readily available, Traffic destined for the Internet that has to be brought back to the Internet edge for security inspection increases bandwidth usage and load on the Internet edge design while increasing latency on user connections.

Technology Overview

The Cisco Smart Business Architecture (SBA) Internet edge design provides the basic framework for the enhancements and additions that will be discussed in this guide. A prerequisite for using this deployment guide is that you must have already followed the guidance in the *Remote Access VPN Deployment Guide*, which itself builds upon the *Firewall and IPS Deployment Guide*. The *Internet Edge Design Overview* describes the goals of the overall design and how the pieces interact together.

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.

The Internet edge design covers remote access (RA) VPN for laptops running the Cisco AnyConnect Secure Mobility Solution client (for SSL VPN or IP Security [IPsec] connections). A feature built into the Cisco AnyConnect 3.1 client is the ability to interface with the Cisco Cloud Web Security (CWS) service, formerly known as *Cisco ScanSafe Cloud Web Security*. This feature gives the Cisco AnyConnect client the ability to let Internet web traffic go out through a CWS proxy directly to the destination without forcing it through the organization's headend. Without Cisco CWS, the traffic must be routed down the VPN tunnel, inspected at the campus Internet edge, and then redirected to the original destination; this process consumes bandwidth and potentially increases user latency. With Cisco CWS, the connection can be proxied through the Cisco CWS cloud and never has to traverse the VPN tunnel.



Other capabilities for the Cisco AnyConnect 3.1 client include features that allow the client to reconnect if the tunnel goes down, to disable the tunnel if the client moves onto the trusted network, or to bring up the tunnel if the client moves from a trusted to an untrusted network. These features make using the client more seamless and friendly because users don't have to manually bring up the VPN tunnel. Users are prompted for credentials when the tunnel is needed, and the tunnel is brought down when it isn't needed.

Mobile devices typically use a different deployment model in which basic services, such as mail, calendar, and contacts, are provided over Microsoft ActiveSync, which gives quick access to these commonly used services. For access to other services, including voice, video, internally hosted web servers, file shares, or other network services, a VPN tunnel is required.

Mobile devices such as the iPhone and iPad and some Android devices have access to the Cisco AnyConnect 3.1 client, which allows Secure Sockets Layer (SSL) VPN connectivity (check the app store for the device in question for availability). Using Cisco AnyConnect to connect the device to the corporate network provides full access to the internal network. This document covers the additional configuration for remote access VPN for the Cisco AnyConnect 3.1 client that is required to activate Cisco CWS, Always On, and other features. It also covers interaction with the Cisco CWS management tool, ScanCenter. Last, the document covers configuration of Cisco Adaptive Security Appliance (ASA) to support mail and calendar services using Microsoft ActiveSync for mobile devices like smartphones and tablets and additionally, the configuration of the Cisco AnyConnect client for those mobile devices.

Notes

Deployment Details

The first part of the deployment details describes how to configure the components to enable Cisco CWS service for Cisco AnyConnect 3.1 users that connect with laptop devices. The second part of the deployment details describes how to configure access for mobile devices with ActiveSync. The third part describes how to configure access for mobile devices with the Cisco AnyConnect client.

Process

Configuring Access for Laptop Devices

- 1. Enable CWS security configuration
- 2. Configure ACL for trusted server
- 3. Configure ASA VPN policy for web security
- 4. Configure ASA AnyConnect group policies
- 5. Install certificate on the client
- 6. Test the AnyConnect configuration
- 7. Test Cloud Web Security
- 8. Configure Automatic VPN Policy
- 9. Test Trusted Network Detection
- 10. Enable Always On
- 11. Test the Always On setting
- 12. Synchronize the profiles to failover ASA

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.

If you want to apply specific policies based on user identity, you must have groups built in Active Directory (AD) in order to allow differentiation based on group membership.

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.

🖸 ScanCenter	logged into: Cisco_Smart Business Architecture Group	Logout Help Guides Contact Us 🏼 🏹 ScanSafe
	Home Dashboard Web Virus Spyware	Web Filtering Email Admin Reports
Your account Authentication Mar	nagement 🕢 Audit 🔹 HTTPS Inspectio	n 🕙 Downloads 💽
Manage Groups		
Search, add or dele	ete groups	
Search:	Search	Reload list 🚱
	Nothing found to display	
	Add Custom Group Add Directory Group	

Step 3: Click Add Custom Group.

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

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

Step 5: Navigate to 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.

		Home - Dashbo	ard - Web Virus - S	web Filtering	Email	Admin	Re
our account	Authentication Mar	nagement 💽 Audit	HTTPS I	nspection 🕢 Downloads			
Course Authorsh	Kanking Marra						
Group Authent	tication Keys						
	a Canada anticada and departicula						
	Create, activate and deactivate						
	Create, activate and deactivate						
					Reload list	3	
	To add or delete a group, go to the "	"Groups" link in the "Managemen		Action	<u>Reload list</u> 🕑 Sel.	}	
	To add or delete a group, go to the To Search: AnyConnect	'Groups" link in the "Managemen	t" menu or <u>dick here</u>	Action Create Key		•	
	To add or delete a group, go to the " Search: AnyConnect Group Name	'Groups" link in the "Management Search Key Ref	t" menu or <u>dick here</u> State		Sel.	•	

Step 7: Store a copy of this key by copying and pasting it into a secure file because it 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.



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.

💿 ScanCenter	logged into: Cisco	Smart Business Architecture Gr	oup	Logout Hel	p <u>Guides</u> <u>C</u> e	ontact Us 🛛 🖉 So	canSafe
	Home - I	Dashboard - Web Virus	Spyware	Web Filtering	Email	Admin	Reports
Management Notifications							
Web Filtering > Management > Filters > Manage filters							
	III Manage filter	s 📴 Edit a filter 📑 Crea	te a filter				
List of Filters							
Filter	lame	Created	on	Edit	Delete		
Filter Blocked Sites		27 Sep 12 16:01 UTC		E/	畲		
Filter Warned Sites		10 Oct 12 14:49 UTC		E/	۵.		
default		15 Feb 11 10:18 UTC		E/			

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), select **Active**.

Step 17: From the rule action list, choose Block.

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

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

1 Groups of 4	Search AnyConnect	Go	×
# A B C D E F G	H I J K L M N	OPQRSTUW	X Y Z
CWS AnyConnect			Select

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.

ScanCenter	logged into:	Cisco_Smart Bus	iness Architecture	Group	Logout	Help Guides	Contact	Us 💋	Scar	ıSa
	Home	Dashboar	d Web Viru	s Spyware	Web Filterin	g Emai		Admin		Repo
agement Notifications										
Itering > Management > Policy > Create a rule										
	III Manag	e policy	dit a rule 🛛 🐺 Q	eate a rule						
Name Block Blocked Sites Rule Action 🗢 Block 💌							Active			
Define Group ("WHO") Search for a group by clicking on "Ad NOT). If no group is selected, this rule will a for the rule to take effect. If a user	apply to anyone.	Adding multiple g	roups has the act	ion of "OR", so us	ers will need to be	in any of the				
Group		for a regular grou	p and an encept	ingroup one rore		n exception	Delete			
CWS AnyConnect							畲			
Add group 🕀							â			
Define Filters ("WHAT") Choose a Filter from the list and click Add Filter [Filter Blocked Sites Filter	"Add". To set a F		ition to the rule, s	elect the correspo	-	eption" box (a	tion of NO			
Filter Blocked Sites							窗			
Define Schedule ("WHEN") Choose a Schedule from the list and of NOT). Adding multiple schedule is not recon Add Schedule (Choose a schedule	nmended unless o	one is going to be			NOT")	t as exception	box (actio			
Define Schedule ("WHEN") Choose a Schedule from the list and of NOT). Adding multiple schedule is not recon	nmended unless o	one is going to be			NOT")		box (actio			

Next, create a new rule.

Step 23: Click Create a rule.

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

Step 25: From the Rule Action list, choose Warn.

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

Step 27: In 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 to all groups)

	5C	anCenter	logged into: Cisco	o_Smart Business Architecture (Group Lo	iqout <u>Help</u> <u>Guid</u>	les Contact U	s 📶 🤅	ScanSa
			Home	Dashboard - Web Virus	Spyware Web F	iltering En	nail	Admin	Reports
Mar	nagem	nent 🔹 Notifications	•						
ieb Fi	iltering	Management > Policy > Management	e policy						
			Manage pol	licy 🗮 Edit a rule 🛛 🐺 Cre	ate a rule				
Rules	higher	r in the list will take priority over the	e lower ones. Use the arrows to ch	nange the priority of each rule b	y moving them up or down	in the list.			
leas	e note	that anonymization rules are treate	ed separately from the main policy				in the same wa	y as the re	st of the rule
leas	e note		ed separately from the main policy				in the same wa	y as the re	st of the rule:
Pleas and a	e note inonym	that anonymization rules are treate	ed separately from the main policy e.				in the same wa	y as the re	st of the rule:
Pleas and a Ther	e note inonym	that anonymization rules are treate nization will always take precedence maximum of 100 enabled rule	ed separately from the main policy e.				in the same wa	y as the re	st of the rule:
Pleas and a Ther	e note inonym re is a	that anonymization rules are treate nization will always take precedence maximum of 100 enabled rule policy	ed separately from the main policy e.				in the same wa	y as the re Edit	st of the rule Delete
Pleas and a Ther Corr	e note nonym re is a npany p	that anonymization rules are treate nization will always take precedence maximum of 100 enabled rule policy	ed separately from the main policy 2. 2 s allowed for the policy.	r. Hence these appear in a separation of the	rate part of the table. The	e can be ordered			
Pleas and a Ther Com #	e note nonym re is a npany p	that anonymization rules are treate nization wil always take precedence maximum of 100 enabled rule policy ve Rules	ed separately from the main policy es allowed for the policy. Groups/Users/IPs	r. Hence these appear in a sepa Filter	© Schedule	e can be ordered	Active	Edit	Delete

Procedure 2

Configure ACL for trusted server

The Trusted Network Detection (TND) feature of Cisco CWS determines whether a host is connected directly to a *trusted network*, in this guide referring to a LAN or WLAN at an organization's primary or remote sites. Conversely, if a host connects to an organization through a remote access VPN, then the host is considered to be on an *untrusted network*.

The TND configuration requires a trusted server that is reachable for all hosts on the internal network but is unreachable for remote-access VPN users. The trusted server is required to support HTTPS connections.

Step 1: If a trusted server does not exist, deploy a server with an HTTP server and enable HTTPS. Ports other than TCP 443 may be used if necessary. (Example: 10.4.48.10:443)



Tech Tip

Access to the trusted server is blocked for remote access VPN users. Choose a trusted server that does not support applications required for these users.

Step 2: From a client on the internal network, navigate to the RA VPN firewall's inside IP address, and then launch the Cisco ASA Security Device Manager. (Example: https://10.4.24.24)

Step 3: In Configuration > Remote Access VPN > Network (Client) Access > Group Policies, select GroupPolicy_Employee, and then click Edit.

Step 4: On the Edit Internal Group Policy dialog box, click the two down arrows. The More options pane expands.

Step 5: For Filter, clear Inherit, and then click Manage.

Step 6: On the ACL Manager dialog box, click the Extended ACL tab, then click Add > Add ACL.

Step 7: On the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example Block_Trusted_Host)

Add ACL	23
ACL Name: Block_Trusted_Host	
OK Cancel Help	

Step 8: Click Add > Add ACE.

Step 9: On the Add ACE dialog box, configure the following values, and then click **OK**.

- · Action—Deny
- · Source-any4
- · Destination-10.4.48.10
- · Service—tcp/https
- Description—Trusted host is 10.4.48.10:443

💁 Add ACE	8
Action: 🔘 Pern	nit 💿 Deny
Source Criteria	
Source:	any4
User:	
Security Group:	
Destination Crite	ria
Destination:	10.4.48.10
Security Group:	
Service:	tcp/https
Description:	Trusted host is 10.4.48.10:443
🔽 Enable Loggi	ing .
Logging Leve	sl: Default 🔹
More Options	s 🛞
	OK Cancel Help

Step 10: Click Add > Insert After.

Step 11: On the Add ACE dialog box, configure the following values, and then click **OK**.

- Action—Permit
- Source—any4
- Destination—any4
- Service-ip
- Description—Permit all other traffic

Step 12: On the ACL Manager dialog box, click OK.

Block											
1	🗹 🧠 any	Sec. 10.4.48.10	🚥 https 🛛 😵 Deny								
2	🗹 🧠 any	🦚 any	💴 ip 🖌 🖌 Permit								

Step 13: On the Add Internal Group Policy dialog box, click OK.

Edit Internal Group Policy:	GroupPolicy_Employee							×
General	Name:	GroupPolicy_	Employee					
Servers ⊛Advanced	Banner:	📄 Inherit	Group "vpn-emplo	oup "vpn-employee" allows for unrestricted access with a tunnel all policy.				
	SCEP forwarding URL:	🔽 Inherit						
	Address Pools:	🔽 Inherit						Select
	IPv6 Address Pools:	📝 Inherit						Select
	More Options							۲
	Tunneling Protocols:		📝 Inherit	Clientless SSL VPN	SSL VPN Client	IPsec IKEv1	IPsec IKEv2	L2TP/IPsec
	Filter:		📄 Inherit	Block_Trusted_Host			•	Manage

Step 14: In the Group Policies pane, click Apply.



Configure ASA VPN policy for web security

Step 1: In Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile, select Add.

Step 2: On the Add AnyConnect Client Profile dialog box, in the Profile Name box, enter RA-WebSecurityProfile.

Step 3: In the Profile Usage list, choose Web Security Service Profile, click OK, and then click Apply.

🔂 Add AnyConn	ect Client Profile	—
Profile Name	RA-WebSecurityProfile	
Profile Usage	Web Security Service Profile 👻	
	le path for an xml file, ie. disk0:/ac_profile. The file will be eated if it does not exist.	
Profile Location	disk0:/ra-websecurityprofile.wsp	Browse Flash
		Upload
Group Policy	<unassigned></unassigned>	
	Enable 'Always On VPN' for selected group	
	OK Cancel Help	

Step 4: Select the newly created RA-WebSecurityProfile profile, and then click **Edit**.

Step 5: In Web Security > Scanning Proxy, if the status is "Scanning Proxy list is currently up-to-date.", then skip to Step 6. If the status is "Updates to the Scanning Proxy list are now available.", then click Update Proxies to update the list.

Step 6: In the drop-down list, choose a default proxy location that best matches your location.

Step 7: In **Web Security > Authentication**, in the Proxy Authentication License Key box, enter the group key created in Step 6 of Procedure 1, "Enable CWS security configuration."

Step 8: In the Service Password box, enter a new password that will be associated with the Web Security service when the service is running on the end host. (Example: c1sco123)

: RA-WebSecuri	litor - RA-WebSecurityProfile tyProfile	
Web Security Scanning Proxy	Authentication	
Advanced	Proxy Authentication License Key Service Password	"Use CWS-AmyConnect Group Authentication Key"
	Enable Enterprise Domains All Domains	Use Group Include List 🗸
	All Domains	Add Delete
		Delete
	Custom matching and reporting for ma	chines not joined to domains
	Custom Groups (optional)	Add
		Delete
		** change requires WebSecurity service restart

Step 9: In Web Security > Preferences, do the following:

- 1. Select Automatic Scanning Proxy Selection.
- 2. If your organization allows users to control use of web security functions, select **User Controllable**.
- 3. In the Trusted Network Detection section, select **Enable Trusted Network Detection**.
- 4. For New Trusted Server, enter the server IP address (Example: 10.4.48.10) configured in Procedure 2, "Configure ACL for trusted server," and then click **Add**.

: RA-WebSecurityPr Web Security Scanning Proxy	Preferences		
ie biceptoris Sgr Pererences Sgr Authentication ⊸ Advanced	Enable Cloud-Hosted Configuration Automatic Scanning Proxy Selection Order Scanning Proxies by Response Time Advanced Response Time Settings Enable Test Interval: Test Inactivity Timout (min.) Trusted Network Detection New Trusted Network Detection New Trusted Server at https://server>[:cp https://10.4.48.10:443	** ✓ User Controllable 1 ☆ hour(s) 0 ☆ minute(s) s ☆ ort>] Add Delete	
	Certificate hash:	Set	

Step 10: On the Add AnyConnect Client Profile Editor dialog box, click OK.

Step 11: On the AnyConnect Client Profile screen, click Apply.



Modifications to the AnyConnect Web Security Service Profile do not take effect on a client machine until after the next RA VPN connection, followed by a restart of the AnyConnect Web Security Agent service. A workstation reboot is the easiest way to restart this service.

Procedure 4

Step 1: In Cisco Adaptive Security Device Manager (ASDM), navigate to Configuration > Remote Access VPN > Network Client Access > Group Policies, select the GroupPolicy_Employee policy, and then click Edit.

Step 2: Under Advanced, select Split Tunneling.

Step 3: Next to Policy, clear the Inherit check box, and then choose Exclude Network List Below.

Step 4: Click Set up split exclusion for Web Security.

Step 5: On the Web Security Proxies Exclusion dialog box, in the Access list name box, enter CWS_Tower_Exclude, and then click Create Access List.

😼 Web Security Proxies Exclusion	8
Enter a new or select an existing access list used for Web Security split exclusion. ASDM will set up the access list for use in the network list.	
Access list name: CWS_Tower_Exclude Select.	
Create Access List Update Access List Cancel	

Step 6: In the Access List Result dialog box, review the list of proxies added to the access list, and then click **Close**.

Step 7: Next to Network List, clear the Inherit check box, and then choose CWS_Tower_Exclude.

Edit Internal Group Policy: GroupPolicy_Employee					
General The VPN client makes split tunneling decisions on the basis of a network list that can be specified below b Servers Network List fields.				basis of a network list that can be specified below by providing the proper parameter	s to 'Policy' and
Advanced Bokins Browser BArovser BAryCon B-Browser B-AryCon B-Browser B-AryCon	Proxy ect Client	DNS Names: Send All DNS Lookups Through Tunnel: Policy: IPv6 Policy: Network List: Pressing this button to set up split extu Set up split exclusion for Web Se Intercept DHCP Configuration M	Inherit Inherit Inherit Inherit sion for Web curity		Manage
Find:		Next Pr	evious		
	OK Cancel Help				

Step 8: Navigate to Advanced > AnyConnect Client. Under Optional Client Modules to Download, clear the Inherit check box, choose AnyConnect Web Security from the list, and then click OK.

Step 9: In the Always-On VPN section, clear the **Inherit** check box, and then select **Use AnyConnect Profile setting**.

Step 10: In the Client Profiles to Download section, click Add, under Profile Name, choose **RA-WebSecurityProfile**, and then click **OK**.

٦	Edit Internal Group Policy: GroupPolicy_Employee							
	General	Keep Installer on Client System:	📝 Inherit	O Yes	🔿 No			
	- Advanced	Datagram Transport Layer Security (DTLS):	💟 Inherit	🕐 Enable	🔿 Disable			
	Split Tunneling Browser Proxy	DTLS Compression:	📝 Inherit	💿 Enable	🔘 Disable			
	AnyConnect Client AnyConnect Client	SSL Compression:	📝 Inherit	🕐 Deflate	🔿 LZS	🕐 Disable		
		Ignore Don't Fragment(DF) Bit:	📝 Inherit	💿 Enable	🔘 Disable			
		Client Bypass Protocol:	📝 Inherit	🕐 Enable	🔘 Disable			
		FQDN of This Device:	V FQDN					
		MTU:	🔽 Inherit					
		Keepalive Messages:	📝 Inherit	Disable	Interval:	second	ls	
		Optional Client Modules to Download:	📄 Inherit	websecurity			-	0
		Always-On VPN:	📄 Inherit	💿 Disable	O Use Any	Connect Profile s	setting 🕤	
		Client Profiles to Download:	📄 Inherit					
			🕈 Add 🥤	Delete				
			Profile Nam	ie			Profile Usage/Type	
			RA-Profile RA-WebSec	urityProfile			AnyConnect VPN Profile Web Security Service Profile	
l	Find:	🔘 Next 🔘 Previou	s					
	OK Cancel Help							

Step 11: Click OK, and then click Apply.

Step 12: In Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile, select the AnyConnect VPN Profile (Example: RA-Profile), and then click Edit. Step 13: In VPN > Preferences (Part 1), select Local LAN Access, which is required for a split tunnel exclude policy. Clear User Controllable for Local LAN Access.

Profile: RA-Profile				
VPN WPreferences (Part 1) Preferences (Part 2)				
····· 🙀 Backup Servers ····· 🙀 Certificate Matching ····· 🚑 Certificate Enrollment	Use Start Before Logon	💟 User Controllable		
Mobile Policy	Show Pre-Connect Message			
Server List	Certificate Store			
	All			
	Certificate Store Override			
	🔄 Auto Connect On Start	🔽 User Controllable		
	📝 Minimize On Connect	📝 User Controllable		
	🔽 Local Lan Access	🔲 User Controllable		

Step 14: Click OK, and then click Apply.

Procedure 5

Install certificate on the client

As described in the *Remote Access VPN Deployment Guide*, a self-signed certificate is generated and applied to Cisco ASA's outside interfaces. Because the certificate used in the lab is self-signed, all clients generate an error until the certificate is manually added to the trusted certificates. Certificates signed by a public certificate authority (CA) don't need to be manually added.

Because some of the features configured later in this guide involve automatic certificate checking, it isn't acceptable to have the errors show up when self-signed certificates are used. This procedure solves the error problems.

Publicly signed certificates do not have these issues and are easier to use in practice.

Tech Tip

It is essential that the DNS Fully Qualified Domain Name (FQDN) for the Cisco ASA can be resolved and that the interface certificates on the RA VPN Cisco ASA match properly.

Step 1: On a client located outside the network, open a web browser (this procedure details the process for Internet Explorer), and go to the Cisco ASA address:

https://vpn-asa5525x.cisco.local

The first page reports a problem with the certificate.



Step 2: Click Continue to this website.

Step 3: On the next page, in the URL bar, click Certificate Error.

() 🙆 https://vpn-asa5525%. cisco 🔎 - 😵 C	er 監 Č X 🥔 SSL VPN Service 🗙 🏠 ☆ 怨
	With the security certificate presented by this website was not issued by a trusted certificate authority. This problem might indicate an attempt to fool you or intercept any data you send to the server. We recommend that you close this webpage. About certificate errors	× ice
	View certificates	
	GRC	enter your username and password.

Step 4: Select View Certificate.

Step 5: At the bottom of the Certificate page, select **Install Certificate**. When the Certificate Import Wizard opens, click **Next**.



Step 6: Select Place all Certificates in the following store, and then click Browse.

Step 7: Select Trusted Root Certification Authorities, and then click OK.

Select Certificate Store
Select the certificate store you want to use.
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Intrusted Certificates Intrusted Certificates Intermediate Certificates Inter
Show physical stores
OK Cancel

Step 8: Click Next, and then click Finish.

Step 9: Accept the security warning and install the certificate.



Tech Tip

When outside a lab environment, be very careful when installing certificates; after they are installed, they are implicitly trusted by the client. Publicly signed certificates do not have to be manually trusted.

Step 10: On the Certificate Import Wizard dialog box, click OK.

Step 11: In the Certificate window, click OK.

Step 12: Close and relaunch the browser, and then navigate to the following location:

https://vpn-asa5525x.cisco.local

The SSL VPN Service page loads without any certificate warnings or errors.

Step 13: If you are using a resilient Internet connection, the RA VPN firewall has two outside interfaces, each with a different IP address and DNS name. Repeat Step 1 through Step 11 for the secondary outside interface using the Cisco ASA address: https://vpn-asa5525x-fo.cisco.local.

Procedure 6

Test the AnyConnect configuration

Step 1: Log in using a known username and password that is part of the vpn-employee group in Windows AD. If Cisco AnyConnect 3.1 is not installed, the client software is downloaded and installed. If necessary, accept installation warnings.

Login
Please enter your username and password.
GROUP: AnyConnect -
USERNAME: user1
PASSWORD: •••••

Step 2: When connected, click the Cisco AnyConnect taskbar icon. This displays the client information panel.



Step 3: Verify there is a green check for both VPN and Web Security.

Step 4: Click **Disconnect**, and then verify that Web Security remains enabled.



Procedure 7

Test Cloud Web Security

Step 1: Open a web browser to http://whoami.scansafe.net. This browser returns diagnostic information from the Cisco CWS service.

← ← Mttp://whoami.scansafe.net/	8 日 日 8 ☆ 6 1
<pre>countryCode: US externalIp: groupNames: - CWS AnyConnect - "WinNT://Cisco-PC\\None" internalIp: 10.4.28.1 logicalTowerNumber: 1764 staticGroupNames: - CWS AnyConnect userName: "WinNT://Cisco-PC\\user1"</pre>	E

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



Step 2: Verify Cisco CWS Trusted Network Detection by selecting a client that is connected outside the network and has the Web Security module enabled, and then move that client inside the network.

When the client is inside, it should be able to reach the trusted server configured in Procedure 3, "Configure ASA VPN policy for web security," Step 9. (Example: 10.4.48.10:443)

The ability to connect to the trusted server successfully tells the Cisco AnyConnect client that it is directly connected to the internal network and that the Web Security module should not be run because the client is on a trusted network. The host's web connections to external websites are now secured by the organization's Internet edge devices and policy. This is verified on the Anyconnect client status pane.



Procedure 8

Configure Automatic VPN Policy

Trusted network detection for Cisco CWS has already been discussed. The Cisco AnyConnect client also has separate and distinct trusted network capabilities designed for use with Automatic VPN Policy.

The Always On setting for Cisco AnyConnect allows an administrator to enforce a situation in which, if a laptop is outside the network and has connectivity, a VPN connection to the headend occurs and all connections go through the main site, where security policy can be applied. If the device cannot connect to the VPN, then no connections would be allowed.

If policy enforcement is not the end-use case, but instead ease of use is the end goal, then enabling the Auto Connect on Start, Auto Reconnect, and Automatic VPN Policy features that define a trusted network satisfy many requirements without applying strict enforcement that the VPN tunnel be up at all times if network access to Cisco ASA is available. Enabling these features makes access to the internal network more seamless to the end user and presents less opportunity for end users to forget to bring up their VPN tunnel while working remotely or to attempt to bring up the VPN tunnel while on the internal network.

In order to identify whether a device is on the trusted network, before a VPN tunnel is enabled, the client checks either for a trusted DNS domain or DNS server (choose only one). If a trusted DNS domain or DNS server can be reached, then the client is on the trusted domain, and no VPN tunnel is needed. If not, then the VPN tunnel is needed to access internal resources.

Step 1: Navigate to ASDM > Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile, select RA-Profile, and then click Edit.

Step 2: In Preferences (Part 1), select Auto Connect On Start and Auto Reconnect, and, if policy permits, select User Controllable. In the Auto Reconnect Behavior list, ensure ReconnectAfterResume is chosen.

🕼 AnyConnect Client Profile Editor - RA-Profile 🧮 📧			
Profile: RA-Profile			
VPN 	Preferences (Part 1)		
	Use Start Before Logon Show Pre-Connect Message Certificate Store Certificate Store Override Auto Connect On Start Minimize On Connect Local Lan Access Auto Reconnect Behavior Auto Reconnect Behavior Reconnect AlterResume Auto Update RSA Secure ID Integration Autorubdate RSA Secure ID Integration Autorubdate RSA Secure ID Integration Autorubdate Windows Logon Enforcement SingleLocalLogon	User Controllable	
	LocalUsersOnly Clear SmartCard PIN IP Protocol Supported IPv4,IPv6	User Controllable	
	ОК	Cancel Help	

Step 3: In Preferences (Part 2), select Automatic VPN Policy.

Step 4: In the Trusted Network Policy list, choose **Disconnect**, and then, in the Untrusted Network Policy list, choose **Connect**.

Step 5: In the Trusted DNS Servers box, enter the IP address of the internal DNS server that should be accessible from anywhere in the internal network: **10.4.48.10**.

🖾 AnyConnect Client Profile Edit	or - RA-Profile		×
Profile: RA-Profile			About
VPN 	Preferences (Part 2)		
Backup Servers	Disable Automatic Certificate Selection	User Controllable	<u>^</u>
- 🛃 Certificate Enrollment	Proxy Settings	Native	
Mobile Policy	Allow Local Proxy Connections		
	Enable Optimal Gateway Selection	User Controllable	
	Suspension Time Threshold (hours)	4	
	Performance Improvement Threshold (%)	20	
	V Automatic VPN Policy		
	Trusted Network Policy	Disconnect	
	Untrusted Network Policy	Connect	
	Trusted DNS Domains		
	Trusted DNS Servers	10.4.48.10	
	Note: adding all DNS servers in use is recommen	nded with Trusted Network Detection	
	🔄 Always On	(More Information)	
	Allow VPN Disconnect		
	Connect Failure Policy	Closed	
	Allow Captive Portal Remediation		
	Remediation Timeout (min.)	5	
	Apply Last VPN Local Resource Rules		
	PPP Exclusion Disable	User Controllable	
	PPP Exclusion Server IP	User Controllable	
	Enable Scripting	User Controllable	-
	·		
	OK	Help	

Step 6: Click OK, and then click Apply.

Procedure 9

Test Trusted Network Detection

Test the configuration in order to ensure that Trusted Network Detection is functional and that the VPN client attempts to start at startup if needed or when the client moves outside the network.

Step 1: On a laptop outside the network, connect the VPN to Cisco ASA.

Step 2: Move the client into the internal network, and establish a network connection again. The client should identify that it is on a trusted network and that the VPN is not required (the Web Security check box should also be disabled because the client is on the trusted network).

Tech Tip

Cisco CWS Trusted Network Detection uses a trusted server for which it has a block filter that is configured on the RA VPN Cisco ASA.

Cisco AnyConnect client Trusted Network Detection uses a DNS server that is not reachable when the VPN is disconnected.



Step 3: Move the client back outside the network.

Step 4: At the VPN connect prompt, enter the credentials, and then verify that VPN and Web Security are enabled and the check boxes are green.

🕤 Cisco AnyCo	onnect Secure Mobility Client	
00:00:58	VPN: Connected to VPN-ASA5525X.cisco.loca	al. Disconnect
S	Web Security: Enabled (US West Coast)	
\$ ()		oltaba cisco
Procedure 10	Enable Always On	



Tech Tip

If an incorrect Always On configuration is pushed to the client, it is likely that the Cisco AnyConnect software will need to be uninstalled from the client and then reinstalled after the configuration is fixed.

Step 1: In Cisco ASDM, navigate to Configuration > Remote Access VPN > Network Client Access > AnyConnect Client Profile, select RA-Profile, and then click **Fdit**.

Step 2: In Preferences (Part 2), select Always On and Allow VPN Disconnect.



Step 4: Click OK, and then click Apply.

Procedure 11

Test the Always On setting

Tech Tip

This guide requires the use of the Cisco AnyConnect Secure Mobility Client build 3.1.00495. Newer builds of the client implement a stricter check on the certificate presented by the RA VPN Cisco ASA. If you are using self-signed certificates the Always On connection will fail.

Step 1: Connect a client, click the AnyConnect icon in the Windows Taskbar, and then click **Advanced**.

Step 2: On the VPN > Statistics tab, ensure Always On: has a value of Enabled.

Sisco AnyConnect Secure Mobility Client 11 11 11 AnyConnect Secure Mobility Client CISCO Virtual Private Network (VPN) Status Overview Preferences Statistics Route Details Firewall Message History VPN > Web Security Transport Information DTLS Protocol: Cipher: RSA_AES_256_SHA1 LZS Compression: Proxy Address: No Proxy Feature Configuration FIPS Mode: Disabled Enabled Trusted Network Detection: Always On: Enabled

Step 3: With the client disconnected, check that VPN Connection Required appears on the Cisco AnyConnect screen.



Step 4: Browse to a known good website. It should fail because no access is allowed without the VPN tunnel being enabled.



Step 5: Verify from a host on a trusted network that VPN is not required. With the client disconnected, check that Network Access: Available appears on the Cisco AnyConnect screen.

🕥 Cisco AnyCo	onnect Secure Mobility Client	
	VPN: On a trusted network. VPN-ASA5525X.cisco.local ▼	Connect
Network Acc	ess: Available	
Ś	Web Security: On a trusted network.	
\$ ()		altalia cisco

Procedure 12

Synchronize the profiles to failover ASA

When running an RA VPN Cisco ASA firewall pair, the Cisco AnyConnect VPN Profile file and the Web Security Service Profile files must be manually replicated to the secondary ASA firewall. All of the files listed in Table 1 must be replicated.



This procedure is required after any modification to either the Cisco AnyConnect VPN Profile or the Web Security Service Profile.

Table 1 - Cisco AnyConnect Client Profile files

Profile type	Profile name	Filename
AnyConnect VPN Profile	RA-Profile	ra-profile.xml
Web Security Service Profile	RA-WebSecurityProfile	ra-websecurityprofile.wsp
Web Security Service Profile	RA-WebSecurityProfile	ra-websecurityprofile.wso

Step 1: Navigate to Tools > File Management.

Step 2: Click File Transfer, and then select Between Local PC and Flash.

Browse to a destination on your local file system and copy the AnyConnect client profile file from the Cisco ASA disk (Example: ra-profile.xml) by selecting the profile and then clicking the left arrow.



Step 3: Repeat Step 2 for the remaining files in Table 1.

Step 4: After completing all of the file transfers, click Close.

Step 5: Navigate to the secondary RA VPN Cisco ASA's inside IP address, and then launch Cisco ASDM. (Example: https://10.4.24.23)



Step 6: Navigate to Tools > File Management.

Step 7: Click File Transfer, and then select Between Local PC and Flash.

Step 8: Browse to a destination on your local file system and copy the AnyConnect client profile file to the secondary Cisco ASA disk (Example: ra-profile.xml) by selecting the profile and then clicking the right arrow.

Step 9: Repeat Step 8 for the remaining files in Table 1.

Step 10: After completing all of the file transfers, click Close.

Step 11: Close Cisco ASDM on the secondary RA VPN Cisco ASA.

Process

Configuring Access for Mobile Devices: ActiveSync

- 1. Configure DNS entry
- 2. Configure the DMZ firewall
- 3. Configure ActiveSync access on Cisco ASA
- 4. Configure additional security

The first step in providing access for mobile devices like smartphones and tablets is providing email, calendar, and contacts availability. This is a basic requirement and for some users might be enough access. For those users that need or want full tunnel access or for those users connecting on more powerful devices such as tablets, full access can be achieved by using SSL VPN in some cases or through the built-in IPsec client. Full access is needed for things such as internal file shares, internal web servers for employee directories, any other internally hosted web applications, or other services such as voice or video.

To this end, most administrators deploy Microsoft ActiveSync on a Microsoft Forefront Threat Management Gateway (TMG) server in their demilitarized zones (DMZs). ActiveSync connects to the Microsoft Exchange system internally. This setup can provide access to email, calendars, and contacts from a wide variety of mobile devices, including devices that run the Android, iOS, and Windows Mobile operating systems.

The steps in this guide assume that the setup and configuration of TMG, Exchange, and ActiveSync is complete and functional. This process discusses the configuration of Cisco ASA to support such a deployment as well as additional security steps to help improve the overall security of such a deployment. **Reader Tip**

The following reference for Configuring ActiveSync publishing was used as a guideline for lab testing: http://technet.microsoft.com/en-us/library/cc995186.aspx

Procedure 1

Configure DNS entry

Prepare for the following configuration procedures by creating a DNS name that is referenced by the mobile email clients.

Table 2 - DNS names for TMG server (public DNS)

ISP	FQDN	Outside IP address
Primary	mobilemail.cisco.local	172.16.130.55
Secondary	mobilemail-fo.cisco.local	172.17.130.55

The same DNS name also needs to be configured on the internal DNS server. This is required if the mobile device is connected to the internal network.

Table 3 - DNS name for TMG server (internal DNS)

FQDN	DMZ IP address		
mobilemail.cisco.local	192.168.22.25		

Procedure 2 Configure the DMZ firewall

A new DMZ will host the TMG server and allow incoming connections from the outside to the TMG server. It will also allow the TMG server to connect to inside resources as required. Configuration of Cisco ASA firewall and the DMZ switch must be updated.

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

Step 2: Navigate to Configuration > Device Setup > Interfaces.

Step 3: Click Add, and then enter the required data. A new DMZ interface is created.

Add Interface
General Advanced IPv6
Hardware Port: GigabitEthernet0/1 • VLAN ID: 1122 Subinterface ID: 1122 Interface Name: dmz-tmg Security Level: 50 Dedicate this interface to management only Channel Group:
Enable Interface
IP Address O Use Static IP O Obtain Address via DHCP Use PPPoE
IP Address: 192.168.22.1 Subnet Mask: 255.255.255.0 •
Description: Interface to the TMG DMZ
OK Cancel Help

Step 4: Click OK, and then click Apply.

Step 5: Navigate to Configuration > Device Management > High Availability > Failover.

Step 6: Edit the dmz-tmg line to include the standby IP address for the interface: **192.168.22.2**.

Step 7: On the DMZ switch, add the appropriate VLAN to the trunk ports that connect to the appliances.

Primary appliance

interface GigabitEthernet**1/0/24**

switchport trunk allowed vlan add $\boldsymbol{1122}$

Secondary appliance

interface GigabitEthernet2/0/24

switchport trunk allowed vlan add $\boldsymbol{1122}$

Procedure 3

Configure ActiveSync access on Cisco ASA

To allow ActiveSync to work through an external firewall, two things must be done. The first is building a Network Address Translation (NAT) translation for the TMG server to the outside network. The second is allowing the needed connections to traverse the firewall. Allowing the connections to traverse the firewall includes outside hosts making connections to the TMG server, and also the TMG server making connections to the Exchange server.

Tech Tip

This process assumes that a resilient Internet connection is used. ActiveSync is available on either ISP using different IP addresses. This solution does not support the use of a single DNS name for resiliency. If there is a failure of the primary ISP (ISP-A), you must manually update the DNS name to refer to the secondary ISP address. This configuration is performed on the Cisco ASA firewall that controls access to the network and contains the DMZ where the TMG server resides. In this procedure, use the IP address and object name information provided in Table 4.

Table 4 - Addressing and naming for TMG server

ISP	Interface name	Outside IP address	Outside firewall object	DMZ IP address	DMZ firewall object
Primary	outside-16	172.16.130.55	outside-tmg-ISPa	192.168.22.25	dmz-tmg-ISPa
Secondary	outside-17	172.17.130.55	outside-tmg-ISPb	192.168.22.25	dmz-tmg-ISPb

Step 1: Open Cisco ASDM, and then navigate to Configuration > Firewall > Objects > Network Objects/Groups.

Step 2: Click Add > Network Object.

Step 3: On the **Add Network Object** dialog box, enter a name for this object for the TMG server, enter the IP address of the TMG server on the outside for the primary ISP, and then click **OK**.

🔂 Add Networl	k Object
Name:	outside-tmg-ISPa
Туре:	Host 👻
IP Version:	IPv4 O IPv6
IP Address:	172.16.130.55
Description:	TMG server on ISP-A
NAT	*
	OK Cancel Help

Step 4: Click Add > Network Object. This step creates the NAT object that ties the external address to the actual address of the TMG server in the DMZ.

Step 5: Enter the object name to be used to reference the TMG server in the Cisco ASA configuration, and then enter its actual address on the tmg-dmz (Example: outside-tmg-ISPa).

Step 6: Expand the NAT section.

Step 7: Select **Add Automatic Address Translation Rules**, in the **Type** list, choose **Static**, in the **Translated Addr** list, choose the TMG server network object that references the outside address of the TMG server created in Step 3, and then click **Advanced**.

Step 8: On the Advanced NAT Settings dialog box, change the **Source Interface** to **dmz-tmg** and the **Destination Interface** to the outside interface to that of the primary ISP, and then click **OK**.

🔂 Advanced NAT Settir	ngs 🛛 🔀
📄 Translate DNS repli	es for rule
🔲 Disable Proxy ARP	on egress interface
Lookup route table	to locate egress interface
Interface	
Source Interface:	dmz-tmg 👻
Destination Interface:	outside-16 👻
Service	
Protocol:	TEP tcp 👻
Real Port:	
Mapped Port:	
OK	Cancel Help

Step 9: On the Add Network Object dialog box, click OK.

🚰 Add Network	Object 💌
Name:	dmz-tmg-ISPa
Туре:	Host
IP Version:	
IP Address:	192.168.22.25
Description:	TMG on dmz-tmg
NAT	۲
🔽 Add Autom	atic Address Translation Rules
Туре:	Static 👻
Translated A	ddr: outside-tmg-ISPa
📃 Use one-	to-one address translation
PAT Pool	Translated Address:
🗌 Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
🔄 Transla	ate TCP and UDP ports into flat range 1024-65535 🗌 Include range 1-1023
🔄 Fall throu	ugh to interface PAT(dest intf): IPS-mgmt 🚽
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

Step 10: Repeat Step 2 through Step 9 for the secondary ISP as listed in Table 4.

Configuration > Firewall > Objects > Network	Objects/Groups			
💠 Add 👻 🎬 Edit 🏢 Delete 🛛 🔍 Where Used				
Filter:				
Name ^ 1	IP Address	Netmask	Description	Object NAT Address
Network Objects				
🖳 dmz-tmg-ISPa	192.168.22.25		TMG on dmz-tmg	172.16.130.55
🖳 dmz-tmg-ISPb	192.168.22.25		TMG on dmz-tmg	172.17.130.55
- 🖳 outside-tmg-ISPa	172.16.130.55		TMG server on ISP-A	
outside-tmg-ISPb	172.17.130.55		TMG server on ISP-B	

Step 11: Navigate to Configuration > Firewall > Access Rules, and then click Add > Add Access Rule.

Step 12: In the Edit Access Rule window, enter the following information:

- Interface—Any
- Action—Permit
- Source—any4
- Destination—dmz-tmg-network/24
- Service—tcp/http and tcp/https

This adds a new access control entry (ACE) rule to the global list of access rules. The rule allows outside hosts to make HTTP and HTTPS connections to hosts on the dmz-tmg network, which includes the TMG server.

💁 Add Access	Rule
Interface:	Any 👻
Action: 🧿 Perr	nit 💿 Deny
Source Criteria	
Source:	any4
User:	
Security Group:	
Destination Crite	eria
Destination:	192.168.22.0/24
Security Group:	
Service:	tcp/http, tcp/https
Description:	Permit HTTP/HTTPS traffic into the TMG DMZ
📝 Enable Logg	ing
Logging Levi	el: Default 👻
More Option	s 📎
	OK Cancel Help

Next, Create another Cisco ACE. This allows the TMG server access to the internal Exchange server,

Step 13: In the Edit Access Rule window, enter the following information:

- Interface—Any
- Action—Permit
- Source—dmz-tmg-network/24
- Destination—internal-exchange
- Service—tcp/http and tcp/https

💁 Add Access I	Rule	x
Interface:	Any 🔹	
Action: 💿 Perr	mit 💿 Deny	
Source Criteria		_
Source:	dmz-tmg-network/24	
User:		
Security Group:		
Destination Crite		_
Destination:	internal-exchange	
Security Group:		
Service:	http, https	
Description:	Permit HTTP/HTTPS from TMG DMZ to the internal Exchange server	
📃 Enable Logg	ing	
Logging Leve	el: Default 👻	
More Option	s	
	OK Cancel Help	

Step 14: Permit access, using the examples above, from the **dmz-tmg-network/24** to the internal Active Directory server and the internal DNS server in the data center. The AD server requires ports on TCP 88, 135, 389, and 445, and UDP 123 and 389. The DNS server requires UDP 53.

The TMG server also requires HTTP/HTTPS in order to access the Internet to perform occasional required updates.

Step 15: Permit HTTP/HTTPS from the dmz-tmg-network/24 to the destination any4.

lter: S	iource or De	Telete 🕇 🗲 🖌 🦄 🖿	dmz-tmg-netw		xport • 07 clear hits a	SHOW LOG I	racket frace	
	e	Source Criteria:			Destination Criteria:			
#	t Enabled	Source	User	Security Group	Destination	Security G	Service	Action
- 5	Global (44 ru	les, 5 filtered rules)						
4	V	晶晶 dmz-tmg-network/24			এ internal-ad		135 100 445 100 88 100 Idap 100 389 100 ntp	🖌 Perr
5	V	🖷 dmz-tmg-network/24			🖳 internal-dns		💴 domain	🖌 Perr
6	V	📲 dmz-tmg-network/24			🖳 internal-exchange		œ http ∞ https	🖌 Perr
7	V	📲 dmz-tmg-network/24			🏈 any4		œ http ∞ https	🖌 Pern
8	V	🧼 any4			📲 dmz-tmg-network/24		œ http ∞ https	🖌 Perm

Step 16: Move these access rules above any rule already configured that denies DMZ networks access to other networks, and then click **Apply**.

Procedure 4

Configure additional security

To increase the security of the deployment, ActiveSync includes some security options that administrators may deploy. These options include password requirements, inactivity timeout, device encryption, and a maximum number of failed password attempts before the data on the device is deleted. Security options vary by device. The organizational security policy should be used as a guide on how to approach the use of smartphones in the network.

Step 1: In the Exchange Management Console, navigate to Organization Configuration > Client Access.

Step 2: Click the Exchange ActiveSync Mailbox Policies tab, select the policy you want to view in the action pane, and then right-click Properties.

Step 3: On the **Password** tab, set the password requirements for Exchange ActiveSync clients as follows, and then click **OK**:

- 1. Select Require password.
- 2. Select **Allow simple password.** This check box allows pin-numberstyle simple passwords (a minimum level of security but easy to type and remember).
- 3. Select Require encryption on device.
- 4. Enter a number for **Number of failed attempts allowed.** This setting limits the number of failed password attempts before all information on the device is deleted.
- 5. Enter a time in minutes for **Time without user input before password must be re-entered**.

😵 Exchange Management Console	
File Action View Help	
🗢 🔿 🖄 📧 🔽 🗊	
 Microsoft Exchange On-Premises (e Organization Configuration Mailbox Client Access Hub Transport Mailbox Server Configuration Mailbox Client Access Hub Transport Mailbox Client Access Hub Transport Mailbox Client Access Mailbox Recipient Configuration Move Request Toolbox 	Client Access 1 object cook Web App Mailbox Policies Exchange ActiveSync Mailbox Policies create Filter Image: Client Access erties Image: Client Access assword Sync Settings Device perice alphanumeric password Image: Client Access Image: Client Access able password recovery Image: Client Access Image: Client Access applie active field attempts allowed: 10 Image: Client Access nimum password length: Image: Client Access Image: Client Access issword expiration (days): Image: Client Access Image: Client Access e password history: Image: Client Access Image: Client Access
•	
	OK Cancel Apply Help

Process

Configuring Access for Mobile Devices: AnyConnect Client

1. Configure full access using SSL VPN

Procedure 1

Configure full access using SSL VPN

The Cisco AnyConnect client is available for some versions of smartphones or tablets (check the app store for your phone for availability). If available, your device can be configured to connect to Cisco ASA by using SSL VPN to provide full access to the internal network and its resources.

Change the Cisco AnyConnect client profile that is used in order to better support the mobility of smartphones and tablets.

Step 1: In Cisco ASDM, navigate to Configuration > Remote Access VPN > Network Client Access > AnyConnect Client Profile.

Step 2: Select the profile with profile usage set to VPN that is assigned to the group policy that mobile phone users will be using (in this case, RA-Profile associated with GroupPolicy_Employee, GroupPolicy_Administrator, and GroupPolicy_Partner), and then click Edit.

Step 3: In the tree, select Server List, highlight the server host name (VPN-ASA5525X.cisco.local), and then click Edit.

Step 4: On the Server List Entry page, select Additional mobile-only settings, and then click Edit.

Step 5: Select Reconnect when roaming between 3G / Wi-Fi networks, and then click OK.

lost Display Name (required) QDN or IP Address	VPN-ASA5525X.cisco	User Group	Additional mobile-only settings
iroup URL			Mobile Settings Σ
ackup Server List			Apple IOS / Android Settings Certificate Authentication: Automatic •
Host Address		Add	Automatically choose client certificate to use.
	VPN-ASA5525X-FO.cisco.loca	Move Up Move Dow Delete	Apple IOS Only Settings Reconnect when roaming between 3G / Wifi networks Connect on Demand (requires certificate authentication)
rimary Protocol	<	SSL	Match Domain or Host On Demand Action Never Connect
Standard Authenticatic Auth Method During IKE Identity		IKE-RSA	Match Domain or Host On Demand Action

Process Configure and connect mobile devices

- 1. Configure and connect an iOS device
- 2. Configure and connect an Android device

Procedure 1

Configure and connect an iOS device

Step 1: On the iOS device, download the AnyConnect client from the app store.

Step 2: Launch the AnyConnect application.

Step 3: Click Add VPN Connection, enter vpn-asa5525x in the Description field, enter vpn-asa5525x.cisco.local in the Server Address field, and then click Save.



Next, test the connection.

Step 4: Select the connection created in Step 3. Enable the connection by moving the AnyConnect VPN slider from the **Off** to the **On** position. The group is AnyConnect. If you are using a self-signed certificate on your RAVPN ASA firewall, then you will receive an Untrusted VPN Server warning message. Click **Change Settings**.

Pad 🗢 🔆		3:35 PM	98% 🕮
cisco AnyConnec	ct Secure M	obility Client	
AnyConnect VPN		Graphs	Diagnostics Settings
Status C	Connecting		Bytes Received
Choose a connection			
✔ vpn-asa5525x	\bigcirc	760 Bytes	
Add VPN Connectio	AnyConnect ca the VPN serve		O DATA
	a severe secur Security Risks	this server could res rity compromise! <u>Explained</u>	ult in
	untrusted VPN users choose t If this setting is will no longer a	configured to block servers by default. I to keep this setting. s changed, AnyConn automatically block	ect rtes Sent
Status Overview	Keep Me Sat		
Server N	lot Available	570 Bytes	
Time Connected	00:00:00	475 Bytes 380 Bytes	NO DATA
Client Address	lot Available	285 Bytes	
Bytes Sent	0	190 Bytes	
Bytes Received	0	95 Bytes	
Details	>		

Step 5: Disable the Block Untrusted VPN setting by moving the slider to Off.



Step 6: Re-enable the connection by moving the AnyConnect VPN slider from the **Off** to the **On** position. The group is AnyConnect. If you are using a self-signed certificate on your RAVPN ASA firewall, then you will receive a warning message. Click **Continue**.

Pad 🗇 🔆		6:27 PM	82%	
cisco AnyConnect	Secure	Mobility Client		
AnyConnect VPN		Gra	phs Diagnostics	
Status Con	necting		Bytes Received	
Choose a connection				
✓ vpn-asa5525x	٥	760 Bytes		
Add VPN Connection	>	665 Bytes		
		570 Bytes		
		475 Bytes	NO DATA	
	AnyConn of VPN	Verify Server Ident ect can't verify the iden -ASA5525X.cisco.local J like to continue anywa Cancel	tity	
		Details	Bytes Sent	
		Continue		
		760 Bytes		
Status Overview		665 Bytes		
Server Not .	Available	570 Bytes		
Time Connected	00:00:00	475 Bytes	NO DATA	
Client Address Not	Available	380 Bytes		
	0	285 Bytes		
Bytes Sent		190 Bytes 95 Bytes		
Bytes Received	0	55 59103		
Details	>			

Step 7: Enter a valid username and password for authentication, and then click **Connect**.



Step 8: Once you are successfully connected, you can monitor the connection status and view performance graphs.



Procedure 2

Configure and connect an Android device

Step 1: On the Android device, download the AnyConnect client from the app store.

Step 2: Launch the AnyConnect application.

Step 3: Click Add VPN Connection, enter vpn-asa5525x in the Description field, enter vpn-asa5525x.cisco.local in the Server Address field, and then click Done.

Connection Editor					
Description vpn-asa5525x					\odot
Server Addr vpn-asa5525x.cise					0
	Preferences certificate and protocol s	ettings			
	1-1-1-1				
14					
	Cancel			one	
らら			<u>an</u> 49	*AD 6	:23 рм 💈

Next, test the connection.

Step 4: Select the connection. This moves the AnyConnect VPN slider from the **Off** to the **On** position. The group is AnyConnect. If you are using a self-signed certificate on your RAVPN ASA firewall, then you will receive an Untrusted VPN Server warning message. Click **Change Settings**.

Untrusted VPN Server!	
AnyConnect cannot verify the identity of the VPN servyn-asa5525x Connecting to this server could result in a severe sec	
Security Risks Explained	
AnyConnect is configured to block untrusted VPN see setting - connecting to untrusted server could result If this setting is changed, AnyConnect will no longer malicious network devices.	in a severe security compromise.
Keep Me Safe	Change Settings
⇒ 今 □ 第 /	^ @ ⋈⊑ ∻ ≜ 9:17 ам 穿
Step 5: Allow connections to untrusted servers by clearing Block Untrusted Servers.

Settings	E,
Application Style	\odot
Launch at Startup Start AnyConnect services at boot time	
Hide Icon Hide the AnyConnect icon in status bar when idle	
Advanced Settings	
External Control Disable (default) - Outside applications will not be able to control AnyConnect. Changing this setting reduces the overall security of AnyConnect.	0
Block Untrusted Servers Do not allow connections to VPN servers with untrusted certificates.	
FIPS Mode Enable Federal Information Processing Standard	
⊃ 쇼 급 ^ ⊑ॼ◈▲单 9:18.	

Step 6: Re-enable the connection by moving the AnyConnect VPN slider from the **Off** to the **On** position. The group is AnyConnect. If you are using a self-signed certificate on your RAVPN ASA firewall, then you will receive a warning message. Click **Continue**.

cisco s	AnyConnect Secure Mobility Client			Ę
AnyConne Connecting to	ect VPN o vpn-asa5525x			jon
Choose a con	nection			
vpn-asa55	25x			
Add New V	PN Connection			
	AnyConnect			
	AnyConnect cannot verify the anyway? Certificate is from an unit Certificate is not identifie			
	Cancel	Details	Continue	
1		^	@⊾⊠∻▲ 9:	19 ам 🗊 📋

Step 7: Enter a valid username and password for authentication, and then click **OK**.

cisco	AnyC	onnect Mobility C	lient		1 Barrow	Ę
AnyC	onnect V ting to vpn-a	'PN asa5525x				101
Choose a						
vpn-a:	sa5525x					
Add N	ew VPN Co	nnection				
	/ 🕳					_
	Ar	nyConne	ect			
	Plea					
		nyConne				4
		mame ser1				
		sword				
		•••••				
			Cancel		ок	
€	仑	Г	5:3		◈⊷⊻ጶ₳	9:20 ам 穿 🗎

Step 8: Once you are successfully connected, you can monitor the connection status and view performance statistics.

uluilu cisco	AnyConnect Secure Mobility Client		Ę
AnyCon Connected	nnect VPN to vpn-asa5525x	1	ON
Choose a co			
vpn-asa	5525x		
Add New	VPN Connection		
	AnyConnect		
	Status		
	Server Time Connected		
	Client Address		
	Bytes Sent		
	Bytes Received	240562 Disconnect	
	Galicei	Disconnect	
Ð	合司第	^ @ ■ ■ ☆ ▲ 9:	25 ам 穿 📫

Time Connected	00:04:56
Status	Connected
Tunneling Mode	All Traffic
ddress Information	
Client	10.4.28.1
Server	172.16.130.122
Client (IPV6)	FE80::68CE:71A1:94B3:7142
ytes	
Sent	22556
Received	240562
rames	
Sent	268
Received	214
ontrol Frames	
Sent	19
Received	17
ransport Information	
Protocol	
Cipher	RSA_AES_256_SHA1
Compression	LZS
eature Configuration	그는 한 이번 바람이 가 있다는 동법 관람
FIPS Mode	Disabled
ecured Routes	이는 그 것은 영상을 하는 것을 받았다.
	0.0.0.0 / 0.0.0.0

Notes			
	ļ		

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)
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	IPS 7.1(6)E4
	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)
RA VPN Firewall	Cisco ASA 5545-X Firewall Edition - security appliance	ASA5545-K9	ASA 9.0(1)
	Cisco ASA 5525-X Firewall Edition - security appliance	ASA5525-K9	
	Cisco ASA 5515-X Firewall Edition - security appliance	ASA5515-K9	
	Cisco ASA 5512-X Firewall Edition - security appliance	ASA5512-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)
AnyConnect License	AnyConnect Essentials VPN License - ASA 5545-X (2500 Users)	L-ASA-AC-E-5545	_
	AnyConnect Essentials VPN License - ASA 5525-X (750 Users)	L-ASA-AC-E-5525	
	AnyConnect Essentials VPN License - ASA 5515-X (250 Users)	L-ASA-AC-E-5515	
	AnyConnect Essentials VPN License - ASA 5512-X (250 Users)	L-ASA-AC-E-5512	
	AnyConnect Premium VPN License (2500 users)	L-ASA-SSL-2500	
	AnyConnect Premium VPN License (500 Users)	L-ASA-SSL-500	
	AnyConnect Premium VPN License (250 Users)	L-ASA-SSL-250	
AnyConnect Mobile License	Cisco AnyConnect Mobile License	L-ASA-AC-M-5545	—
	Cisco AnyConnect Mobile License	L-ASA-AC-M-5525	

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE IP Base license

VPN Client

Functional Area	Product Description	Part Numbers	Software
VPN Client	Cisco AnyConnect Secure Mobility Client (Windows)	Cisco AnyConnect Secure Mobility Client	3.1.00495
	Cisco AnyConnect Secure Mobility Client (Mac OS X)	Cisco AnyConnect Secure Mobility Client	
	Cisco AnyConnect Secure Mobility Client (Linux)	Cisco AnyConnect Secure Mobility Client	
Mobile Device VPN Client	Cisco AnyConnect Secure Mobility Client (Apple iOS)	Cisco AnyConnect Secure Mobility Client	3.0.09097
	Cisco AnyConnect Secure Mobility Client (Android)	Cisco AnyConnect Secure Mobility Client	3.0.09093

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	

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

Appendix B: Configuration Example

RAVPN ASA5525X

```
ASA Version 9.0(1)
1
hostname VPN-ASA5525X
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RA-pool 10.4.28.1-10.4.31.254 mask 255.255.252.0
L
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.4.24.24 255.255.255.224 standby 10.4.24.23
 summary-address eigrp 100 10.4.28.0 255.255.252.0 5
interface GigabitEthernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
L
interface GigabitEthernet0/3
 no nameif
 no security-level
 no ip address
interface GigabitEthernet0/3.16
```

vlan 16 nameif outside-16 security-level 0 ip address 172.16.130.122 255.255.255.0 1 interface GigabitEthernet0/3.17 vlan 17 nameif outside-17 security-level 0 ip address 172.17.130.122 255.255.255.0 1 interface GigabitEthernet0/4 shutdown no nameif no security-level no ip address 1 interface GigabitEthernet0/5 shutdown no nameif no security-level no ip address ! interface GigabitEthernet0/6 shutdown no nameif no security-level no ip address 1 interface GigabitEthernet0/7 shutdown

no nameif no security-level no ip address L interface Management0/0 management-only shutdown no nameif no security-level no ip address L boot system disk0:/asa901-smp-k8.bin ftp mode passive clock timezone PST -8 clock summer-time PDT recurring dns server-group DefaultDNS domain-name cisco.local same-security-traffic permit intra-interface object network NETWORK OBJ 10.4.28.0 22 subnet 10.4.28.0 255.255.252.0 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 5505-pool subnet 10.4.156.0 255.255.252.0 description 5505 Teleworker Subnet object network internal-network subnet 10.4.0.0 255.254.0.0 description Internal Network access-list ALL BUT DEFAULT standard deny host 0.0.0.0 access-list ALL BUT DEFAULT standard permit any4 access-list RA PartnerACL remark Partners can access this internal 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 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-
access-list CWS_Tower_Exclude extended permit ip object asdm- websecproxy-72-37-248-27 any

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
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
proxy ACE
proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm-
proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm- websecproxy-70-39-231-182 any
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-70-39-231-182 any access-list CWS Tower Exclude remark ASDM-generated Web Security proxy ACE
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-
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
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-70-39-231-182 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
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 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 remark ASDM-generated Web Security proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm- websecproxy-70-39-231-190 any
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-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
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 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 remark ASDM-generated Web Security proxy ACE access-list CWS_Tower_Exclude remark ASDM-generated Web Security

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 ONC mercer Evaluate remark ACDM represented Web Converter
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
proxy ACE
proxy ACE
proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm-
proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm- websecproxy-70-39-176-131 any
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-70-39-176-131 any access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
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-
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
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-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
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 remark ASDM-generated Web Security proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm-
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 remark ASDM-generated Web Security proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm- websecproxy-72-37-249-171 any
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 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-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
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 remark ASDM-generated Web Security proxy ACE access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE access-list CWS_Tower_Exclude remark ASDM-generated Web Security

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
webbeeproxy of the day
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
access-list CWS_Tower_Exclude remark ASDM-generated Web Security
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE
access-list CWS_Tower_Exclude remark ASDM-generated Web Security proxy ACE access-list CWS_Tower_Exclude extended permit ip object asdm-

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
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500
mtu outside-16 1500
mtu outside-17 1500
failover
failover lan unit secondary
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 10.4.24.97 255.255.258.248 standby 10.4.24.98 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 1 router eigrp 100 no auto-summary distribute-list ALL BUT DEFAULT out network 10.4.0.0 255.254.0.0 passive-interface default no passive-interface inside redistribute static 1 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 route inside 0.0.0.0 0.0.0.0 10.4.24.1 tunneled 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 sipdisconnect 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 timeout 5 key SecretKey user-identity default-domain LOCAL 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 espmd5-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-shahmac 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 espmd5-hmac crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5hmac crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 espsha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-shahmac crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 espsha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5hmac 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 reverseroute crypto map outside-16 map 65535 ipsec-isakmp dynamic SYSTEM DEFAULT CRYPTO MAP crypto map outside-16 map interface outside-16 crypto ca trustpoint VPN-ASA5525X-Trustpoint enrollment self subject-name CN=VPN-ASA5525X.cisco.local keypair VPN-ASA5525X-Keypair proxy-ldc-issuer crl configure crypto ca trustpoint VPN-ASA5525X-FO-Trustpoint enrollment self subject-name CN=VPN-ASA5525X-FO.cisco.local keypair VPN-ASA5525X-Keypair proxy-ldc-issuer crl configure crypto ca trustpoint ASDM TrustPoint0 enrollment self subject-name CN=VPN-ASA5525X

keypair foobar proxy-ldc-issuer crl configure crypto ca trustpool policy crypto ca certificate chain VPN-ASA5525X-Trustpoint certificate 196dbd50 30820379 30820261 a0030201 02020419 6dbd5030 0d06092a 864886f7 0d010105 0500304c 3121301f 06035504 03131856 504e2d41 53413535 3235582e 63697363 6f2e6c6f 63616c31 27302506 092a8648 86f70d01 09021618 56504e2d 41534135 35323558 2e636973 636f2e6c 6f63616c 301e170d 31323132 31373232 34353131 5a170d32 32313231 35323234 3531315a 304c3121 301f0603 55040313 1856504e 2d415341 35353235 582e6369 73636f2e 6c6f6361 6c312730 2506092a 864886f7 0d010902 16185650 4e2d4153 41353532 35582e63 6973636f 2e6c6f63 616c3082 0122300d 06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100be b40a3916 c07f0a5a ca49459f 1ff0fde1 18fdd1d3 1549f412 591ea3da d0fdc925 e590bd9f ddb0a47b 488cfbcc 0a8245de 2c1bba6c b63c12d4 9378e952 c3146de5 5cbaa719 c6cbc071 8ad5b3c1 fa3f9aaa f382b256 8518fa3b 0f4674d9 c973ec60 b78a92a9 ccaeca0a bf55510d 1dd0e6b9 19c8d200 ae13aa37 aed1dae8 f06cd971 9db5a13e ef9fab17 a66f1745 973ed31b 80cc10fc 27e7159b e2ada507 000d0161 56c3c3b5 dddb1010 2db93953 7bea683e 5d15e0e0 ec616cf1 d16bd4af e744c3ec ca686421 21ec21aa e05121c5 6dcc6c77 68638f87 2cee1f57 015fc2a4 bd5a4f36

ccfe7a2e 78c20b1b f0e5f5fa 01b82783 2fbf0748 1df74d18 113c52db 58a27b02 03010001 a3633061 300f0603 551d1301 01ff0405 30030101 ff300e06 03551d0f 0101ff04 04030201 86301f06 03551d23 04183016 80142836 731ddd16 be77e390 7c3543cb 6fcfbeba 47d7301d 0603551d 0e041604 14283673 1ddd16be 77e3907c 3543cb6f cfbeba47 d7300d06 092a8648 86f70d01 01050500 03820101 001f3f41 c292da00 7b7a5435 387b60fd 169ed55d 5a8634f9 1981a26b 950e84d2 fcc1608f 4c198baa 76c7e40a 36922ed3 ef561037 aled3dee 49c9e7b1 bf465d4a 31c45abc 42da8ed6 88721355 6e10c417 71a14481 6f379edf 7052500f fbdd0142 92ec9dc2 f82927e6 2cb3de0e 948f690b 9aa2d831 88c27c0c bbd11fa1 21a08fec 22da19d3 ded3c076 76540ade d9e996ab 7dc26518 ea1b999c fe8d54c9 a26d455f 678030ac 012ec360 fcab84d3 9271d88c e46e3def 45d6fa34 293d6bc6 89e014cc 740cc939 be773a31 640b7dec 8f5b32f2 db785864 b89a68ae bb5d8bc5 33cce6b9 b16a63ca 2d541dc2 79ed0483 3f9afc1c 3060aa60 0ecd97c5 6f1b0a1a 9af9e717 36 quit crypto ca certificate chain VPN-ASA5525X-FO-Trustpoint certificate 1a6dbd50 3082037f 30820267 a0030201 0202041a 6dbd5030 0d06092a 864886f7 0d010105 0500304f 31243022 06035504 03131b56 504e2d41 53413535 3235582d 464f2e63 6973636f 2e6c6f63 616c3127 30250609 2a864886 f70d0109 02161856 504e2d41 53413535 3235582e 63697363 6f2e6c6f 63616c30 1e170d31 32313231 37323234

3535355a 170d3232 31	323135	32323435	35355a30	4f312430
22060355 0403131b				
56504e2d 41534135 35	323558	2d464f2e	63697363	6f2e6c6f
63616c31 27302506				
092a8648 86f70d01 09	021618	56504e2d	41534135	35323558
2e636973 636f2e6c				
6f63616c 30820122 30	0d0609	2a864886	f70d0101	01050003
82010f00 3082010a				
02820101 00beb40a 39	16c07f	0a5aca49	459f1ff0	fde118fd
d1d31549 f412591e				
a3dad0fd c925e590 bd	9fddb0	a47b488c	fbcc0a82	45de2c1b
ba6cb63c 12d49378				
e952c314 6de55cba a7	19c6cb	c0718ad5	b3c1fa3f	9aaaf382
b2568518 fa3b0f46				
74d9c973 ec60b78a 92	a9ccae	ca0abf55	510d1dd0	e6b919c8
d200ae13 aa37aed1				
dae8f06c d9719db5 al.	3eef9f	ab17a66f	1745973e	d31b80cc
10fc27e7 159be2ad				
a507000d 016156c3 c3	b5dddb	10102db9	39537bea	683e5d15
e0e0ec61 6cf1d16b				
<u>d4afe744 c3ecca68 64</u>	2121ec	21aae051	21c56dcc	6c776863
8f872cee 1f57015f				
c2a4bd5a 4f36ccfe 7a	2e78c2	0b1bf0e5	f5fa01b8	27832fbf
07481df7 4d18113c				
52db58a2 7b020301 00	01a363	3061300f	0603551d	130101ff
04053003 0101ff30				
0e060355 1d0f0101 ff	040403	02018630	1f060355	1d230418
30168014 2836731d				
dd16be77 e3907c35 43	cb6fcf	beba47d7	301d0603	551d0e04
16041428 36731ddd				
16be77e3 907c3543 cb	6fcfbe	ba47d730	0d06092a	864886f7
0d010105 05000382				
0101001f 5a3e2fcc c3	84ca51	7519a55b	15d16c77	9a23ed00
72fba6fa ce0251dc				
274e59e8 664c0119 c4	2ae064	1956a610	a9f08787	3df62168

ebd48f27 clede1f6 63169317 bf070a22 f321d4b9 b6157593 59cb71cb bf8492fe ff8f8072 defb92eb 5d50b97c 24fd0c60 cd6ad778 afa18e73 b824b132 11970758 e0a8b8f9 75b0a458 90bdefdb 324a6eb0 547a703c 0eb1d205 26f894db 02632a6d 5b6c534b 77344868 10b4c4c3 811c073e e0193ddf bfcb3e0d 8eae3e4c 10d0a269 6f500e65 fbf99d3b 5f06061f 241a1679 4fb0cb00 f07a01da 930a4636 959afbfd 27e01065 d3730911 08eb3c6b c7494ff5 df273d77 adc52e75 79dd62a6 67d77785 e88d11 quit 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 threat-detection basic-threat threat-detection statistics access-list no threat-detection statistics tcp-intercept ntp server 10.4.48.17 ssl encryption aes256-shal aes128-shal 3des-shal ssl trust-point VPN-ASA5525X-FO-Trustpoint outside-17 ssl trust-point VPN-ASA5525X-Trustpoint outside-16 webvpn enable outside-16 enable outside-17 anyconnect-essentials anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1 anyconnect image disk0:/anyconnect-macosx-i386-3.1.00495-k9.pkg 2 anyconnect image disk0:/anyconnect-linux-3.1.00495-k9.pkg 3 anyconnect profiles RA-Profile disk0:/ra-profile.xml anyconnect profiles RA-WebSecurityProfile disk0:/rawebsecurityprofile.wsp anyconnect profiles RA-WebSecurityProfile.wso disk0:/rawebsecurityprofile.wso anyconnect enable tunnel-group-list enable group-policy 5505Group internal group-policy 5505Group attributes vpn-tunnel-protocol ikev1 password-storage disable split-tunnel-policy tunnelall 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 7KKG/zg/Wo8c.YfN 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://172.16.130.122/AnyConnect enable

```
group-url https://172.17.130.122/AnyConnect enable
I.
class-map inspection default
 match default-inspection-traffic
!
L
policy-map type inspect dns preset dns map
 parameters
  message-length maximum client auto
  message-length maximum 512
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
!
service-policy global policy global
prompt hostname context
: end
```



Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We updated the Cisco ASA firewall software to 9.0(1) with ASDM 7.0(2)
- We updated the AnyConnect Secure Mobility Client software for Windows, Mac OS X, and Linux to 3.1.00495
- We updated the AnyConnect Secure Mobility Client software for iOS to 3.0.09097
- We updated the AnyConnect Secure Mobility Client software for Android to 3.0.09093
- We updated various screenshots to reflect the new software versions.
- We made minor updates to improve the usability of the guide.
- We replaced the Microsoft ISA server with the Microsoft Forefront Threat Management Gateway.



Feedback

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



cisco.

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, WITH-OUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARSING 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 UT 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 ON OT 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.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

B-0000290-1 1/13