

Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new 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.



Teleworking—Cisco ASA 5505 Deployment Guide

-

TELEWORKING

SOLUTIONS

1111111

CISCO

SBA

SMART BUSINESS ARCHITECTURE

August 2012 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 August 2012 are the "August 2012 Series".

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

configure terminal

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

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

class-map [highest class name]

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

Router# enable

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

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

100 100 100

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

interface Vlan64

ip address 10.5.204.5 255.255.255.0

Comments and Questions

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

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

August 2012 Series

Table of Contents

What's In This SBA Guide1
Cisco SBA Solutions 1
Route to Success 1
About This Guide 1
Introduction
Business Overview2
Technology Overview2
Deployment Details
Configuring Internet Edge ASA for Teleworker VPN
Configuring Teleworker Cisco ASA 5505 Endpoints

Appendix A: Product List	15
Appendix B: Configuration Files.	16
VPN-ASA5525	16
ASA-5505	22
Appendix C: Changes	25

What's In This SBA Guide

Cisco SBA Solutions

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 Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

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

Business Overview

Many organizations face increasing need to offer a telecommuter solution to their employees. Employees perceive that commuting and water-cooler chatter are time they spend at work, and renting or buying office space and fixtures, and even deploying network infrastructure to host the work force, adds up to a substantial sum of capital and operating expense.

Providing an office-like work environment at the teleworker's home requires:

- A phone that is accessible as an extension on the organization's phone system.
- An unobtrusive, quiet, low-power solution to provide multiple Ethernet connections for one or more IP-phones or other desktop collaboration resources.
- One or more Ethernet connections for computers that access the organization's network, as well as Ethernet connectivity for other network-connected devices, such as printers and IP video surveillance equipment.

Employees don't need wireless connectivity at the telework site because all of the telework resources connect with wired Ethernet.

Technology Overview

Cisco ASA 5505 offers a low-cost option to provide teleworker connectivity to the organization. Cisco ASA 5505 provides secure connectivity for data and collaboration endpoints in a compact, fanless form factor, minimizing noise and space requirements.

The Cisco ASA 5505 teleworker solution integrates with the Internet Edge portion of the Cisco SBA design. The teleworker's connection terminates at resilient Cisco ASA firewalls at the organization's Internet edge. This solution is configured on the same ASA firewalls as the remote-access virtual private network (RAVPN) solution. This configuration applies to dedicated and shared-mode RAVPN deployments. Some of the configuration re-uses portions of the RAVPN configuration, although it may be configured to be completely independent of the RAVPN resources. The addition of the

head-end's support for Cisco ASA 5505 teleworker termination does not affect RAVPN connectivity, and the configuration can be applied without the imposition of a service outage.

The Cisco ASA 5505 teleworker solution provides access for endpoint devices, such as laptop and desktop computers, IP phones, printers, and other devices that connect to the network via wired Ethernet connections. Two of the Cisco ASA 5505's ports provide Power over Ethernet (PoE) to support IP phones, IP video surveillance, and other endpoints without cluttering the teleworker's office with additional cables and wall-wart power supplies.

The Cisco ASA 5505 teleworker solution offers:

- Low cost—With this solution, you get a Cisco ASA 5505, a Cisco IP phone, and the necessary license on the organization's Internet edge Cisco ASAs.
- Flexible connectivity—The Cisco ASA 5505's integrated Ethernet switch can accommodate multiple endpoint devices, including two interfaces that can provide PoE.
- **Simple deployment**—The Cisco ASA 5505 can be configured quickly with a brief text-file configuration.
- Security—Deactivation of the teleworker site's credentials on the Internet-edge appliance can terminate the teleworker's connectivity.

Ideally, the Cisco ASA 5505 teleworker device is preconfigured and sent home with the teleworker user. A newly-provisioned or existing desktop IP-phone can be taken home, as well, and registers to the Cisco Call Manager server over the VPN.

Deployment Details

Configuration of remote-access connectivity consists of two phases. In the first phase, you configure your resilient Internet-edge appliance pair to receive VPN connections from teleworkers' Cisco ASA 5505 appliances. In the second phase, you deploy configuration on the teleworkers' Cisco ASA 5505 hardware clients.

Process

Configuring Internet Edge ASA for Teleworker VPN

- 1. Configure IPsec(IKEv1) connection profile
- 2. Configure NAT exemption
- 3. Configure route advertisement

As a rule, the Internet-edge Cisco ASA configuration for Cisco ASA 5505 teleworker VPN is self-contained. A few aspects rely on configuration from the Internet-edge foundation, so you need to have followed the configuration steps for Cisco ASA-based Remote Access VPN in the Cisco SBA —Borderless Networks Remote Access VPN Deployment Guide.

Procedure 1

Configure IPsec(IKEv1) connection profile

The IPsec connection profile carries the bulk of the configuration that sets the behavior for VPN client connections, so you must apply a number of steps in this procedure to complete the central configuration.

Step 1: Navigate to the Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1)Connection Profiles tab,

Step 2: In the right pane under Connection Profiles, click the Add button.

Image web inside in the index of the index	Interface		Allow Acces	S			
marzies outside - 16 outside - 16 v ✓ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. nection Profiles Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to comprofile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to configure the mapping from certificate to configure the mapping from certificate to configu							
Inside	dmz-web						
Judside-17 Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. Intection Profiles Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connorolie bare. Add G Edit Delete Name IPsec Enabled LZTP/IPsec Enabled Authentication Server Group Group Policy DefaultKAGroup Ø Ø LOCAL DftGrpPolicy DefaultWEBVPN Ø LOCAL DftGrpPolicy	nside				=		
Website*17 Image: Comparison of the session of the traffic of tr	outside-16				-		
Name IPsec Enabled L2TP/IPsec Enabled Authentication Server Group Group Policy DefaultRAGroup I I LOCAL DftGrpPolicy DefaultWEBVPN	Connection profile	(tunnel group) spe	ecifies how use	er is authenticated and o	ther par	ameters. You can configure the map	ping from certificate to conne
DefaultRAGroup V V LOCAL DfttGrpPolicy DefaultWEBVPN V V LOCAL DfttGrpPolicy	orofile <u>here</u> .	Delete					
DefaultWEBVPN 🗹 🗹 LOCAL DftGrpPolicy	Add C Edit	Delete IPsec Enabled	1	.2TP/IPsec Enabled		Authentication Server Group	Group Policy
	Add Add	Delete IPsec Enabled	1	.2TP/IPsec Enabled		Authentication Server Group	Group Policy DfltGrpPolicy
	Add C Edit Name DefaultRAGroup	Delete		.2TP/IPsec Enabled		Authentication Server Group LOCAL LOCAL	Group Policy DftGrpPolicy DftGrpPolicy

Step 3: On the **Add IPsec Remote Access Connection Profile** dialog box, enter the following details. This configuration affects the behavior of the Cisco ASA 5505 teleworker device, as described.

· Name—Teleworker5505

This entry is the name of the VPN group that is reflected in the Cisco ASA 5505 Easy VPN Client configuration.

IKE Peer Authentication Pre-Shared Key—cisco123

This entry is the group key that must be duplicated in the Cisco ASA 5505 Easy VPN Client configuration.

• Server Group—Select AAA-RADIUS or AD, depending on whether you are using ACS or Microsoft Active Directory for user authentication.

This entry selects the server that authenticates user names and passwords that are presented to open the Easy VPN Client tunnel.

ø	Edit IPsec Remote Access	Connection Profile: Tele	eworker5505
	<mark>Basic</mark> JAdvanced	Name:	Teleworker5505
		IKE Peer Authentication	
		Pre-shared Key:	•••••
		Identity Certificate:	None
		User Authentication —	
		Server Group:	AAA-RADIUS

Step 4: On the right side of the Group Policy list, click Manage.



Step 5: On the Configure Group Policies dialog box, click Add.



Step 6: On the Add Internal Group Policy dialog box, select General, and then in the Name box, enter 5505Group.

🚰 Add Internal Group Policy							
General	Name:	5505Group					
Servers							
	Banner:	🔽 Inherit					

Step 7: Expand the options panel by clicking More Options.

More Options 😵	S

Step 8: Next to Tunneling Protocols, clear Inherit, and then select IPsec IKEv1.

More Options				
Tunneling Protocols:	Inherit	Clientless SSL VPN	SSL VPN Client	V IPsec IKEv 1
IPv4 Filter:	🗸 Inherit			

Step 9: Navigate to **Advanced > Split Tunneling**, and in the right panel, next to **Policy**, clear **Inherit**.

Step 10: Next to Policy, in the drop-down list, ensure that Tunnel All Networks is selected.



Step 11: Navigate to Advanced > IPsec Client.

Step 12: Next to Store Password on Client System, clear Inherit and ensure that Disable is selected.

5	Add Internal Group Policy				
	General	Re-authentication on IKE Re-key:	🔽 Inherit	🔘 Enable	Allow entry
	AdvancedSolit Tuppeling			O Disable	
	Browser Proxy ⊕-AnyConnect Client	IP Compression:	📝 Inherit	🔘 Enable	Disable
	⊡ <mark>IPsec Client</mark> Client Access Rules	Perfect Forward Secrecy:	🔽 Inherit	🔘 Enable	O Disable
	Client Firewall Hardware Client	Store Password on Client System:	Inherit	Enable	Oisable

Step 13: Navigate to Advanced > IPsec Client> Hardware Client, and do the following:

- Next to **Require Interactive Client Authentication**, clear **Inherit** and ensure that **Enable** is selected.
- Next to Allow Network Extension Mode, clear Inherit and ensure that Enable is selected.
- · Click OK.

Add Internal Group Policy					
General	Require Interactive Client Authentication:	🔲 Inherit	Enable	O Disable	
■ Advanced	Require Individual User Authentication:	🔽 Inherit	🔘 Enable	🔘 Disable	
Split Tunneling Browser Proxy	User Authentication Idle Timeout:	🔽 Inherit	Unlimited		minutes
⊕ AnyConnect Client ⊡ IPsec Client	LEAP Bypass:	🗸 Inherit	🔘 Enable	🔘 Disable	
Client Access Rules	Cisco IP Phone Bypass:	🗸 Inherit	🔘 Enable	🔘 Disable	
Hardware Client	Allow Network Extension Mode:	🔲 Inherit	Enable	🔘 Disable	

Step 14: On the Configure Group Policies dialog box, click OK.

Step 15: On the Add IPsec Remote Access Connection Profile dialog box, clear Enable L2TP over IPsec protocol, and then click OK.

🔁 Ado	d IPsec Remote Access (Connection Profile	×
	asic dvanced	Name:	Teleworker 5505
		IKE Peer Authentication	
		Pre-shared Key:	•••••
_			✓ Manage
		Default Group Policy — Group Policy:	5505Group Manage (Following fields are attributes of the group policy selected above.) Image: Comparison of the group policy selected above.) Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selected above. Image: Comparison of the group policy selecte

Step 16: Navigate to Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles.

Step 17: Under Access Interfaces, next to the appliance's primary outside interface, select Allow Access.

andela interference for 1	Dees seese						
Interface	Allow	Access					
nside							
utside-16							
utside-17							
Enable inbound VF inection Profiles	N sessions to bypass int	erface access lists. Group policy and	per-user authorization access lists still apply	to the traffic.			
Enable inbound VF Inection Profiles Connection profile (tu- tere, Add 2 Edit	N sessions to bypass int nnel group) specifies ho l Delete IPsec Enabled	erface access lists. Group policy and w user is authenticated and other pa LZTP/IPsec Enabled	per-user authorization access lists still apply arameters. You can configure the mapping fro Authentication Server Group	to the traffic. m certificate to connection prof Group Policy			
Enable inbound VF enection Profiles Connection profile (tu- nere, Add 2 Edit	N sessions to bypass int nnel group) specifies ho Delete IPsec Enabled	erface access lists. Group policy and w user is authenticated and other pu LZTP/IPsec Enabled	arameters. You can configure the mapping fro	to the traffic. m certificate to connection prof Group Policy DftGrpPolicy			
Enable inbound VF Inection Profiles Onnection profile (ture) Add C Edit Name DefaultRAGroup DefaultWEBVPNGr	N sessions to bypass int nnel group) specifies hor Delete IPsec Enabled	erface access lists. Group policy and w user is authenticated and other particular L2TP/IPsec Enabled	arameters. You can configure the mapping fro Authentication Server Group LOCAL	to the traffic. m certificate to connection prof Group Policy DfltGrpPolicy DfltGrpPolicy			
Enable inbound VF Inection Profiles Connection profile (tu. Inerc. Add 2 Edit Name DefaultRAGroup DefaultWEBVPNGr AnyConnect	N sessions to bypass int nnel group) specifies hor Delete IPsec Enabled	erface access lists. Group policy and w user is authenticated and other particular L2TP/IPsec Enabled	Authentication Access lists still apply arameters. You can configure the mapping fro Authentication Server Group LOCAL LOCAL AAA-RADIUS	to the traffic. m certificate to connection prof Group Policy DfltGrpPolicy DfltGrpPolicy GroupPolicy_AnyConne			

Step 18: Under Connection Profiles, verify that the new Teleworker 5505 profile appears, and then click Apply. The steps above apply the following configuration: group-policy **5505Group** internal group-policy 5505Group attributes password-storage disable vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall secure-unit-authentication enable nem enable exit. tunnel-group Teleworker5505 type remote-access tunnel-group Teleworker5505 general-attributes default-group-policy 5505Group authentication-server-group AAA-RADIUS tunnel-group Teleworker5505 ipsec-attributes ikev1 pre-shared-key cisco123 crypto ikev1 policy 70 encryption aes authentication crack crypto ikev1 policy 80 encryption aes authentication rsa-sig crypto ikev1 policy 90 encryption aes crypto ikev1 policy 40 encryption aes-192 authentication crack crypto ikev1 policy 50 encryption aes-192 authentication rsa-sig crypto ikev1 policy 60 encryption aes-192 crypto ikev1 policy 10 encryption aes-256 authentication crack crypto ikev1 policy 20 encryption aes-256 authentication rsa-sig crypto ikev1 policy 30 encryption aes-256

crypto ikev1 policy 100 authentication crack crypto ikev1 policy 110 authentication rsa-sig crypto ikev1 policy 120 crypto ikev1 policy 130 encryption des authentication crack crypto ikev1 policy 140 encryption des authentication rsa-sig crypto ikev1 policy 150 encryption des crypto ikev1 enable outside-16 crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-shahmac crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des espsha-hmac crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5hmac crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des espmd5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes espsha-hmac crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes espmd5-hmac 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 map outside-16 map 65535 ipsec-isakmp dynamic SYSTEM DEFAULT CRYPTO MAP crypto map outside-16 map interface outside-16

Procedure 2

Configure NAT exemption

The Internet-edge appliances must not apply network address translation (NAT) on traffic between the organization's private network and the IP-subnet that encompasses teleworkers' remote addresses. You must configure a policy that prevents the Internet-edge appliance from applying NAT.

Configure a network object for the summary address of the internal network. The network object will be used during the security policy configuration.

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

Step 2: Click Add > Network Object.

Step 3: In the Add Network Object dialog box, in the **Name box**, enter a description for the network summary. (Example: internal-network)

Step 4: In the Type list, select Network.

Step 5: In the **IP Address** box, enter the address that summarizes all internal networks. (Example: 10.4.0.0)

Step 6: In the **Netmask** box, enter the internal network summary netmask, and then click **OK**. (Example: 255.254.0.0)

뒄 Add Netwo	vrk Object	×
Name:	internal-network	
Type:	Network	•
IP Address:	10.4.0.0	
Netmask:	255.254.0.0	-
Description:	Internal Network	
NAT		*
	OK Cancel Help	

Step 7: Navigate to Configuration > Firewall > NAT Rules, and then click Add.

Step 8: On the Add NAT Rule dialog box, under Match Criteria: Original Packet, in the Source Address box, click the ellipsis (...).

🔂 Add NAT Rule			_	×
Match Criteria: Orig	ginal Packet			
Source Interface:	Any 🔹	Destination Interface:	Any	•
Source Address:	any	Destination Address:	any .)
		Service:	any .)

Step 9: On the Browse Original Source Address dialog box, expand the IPv4 Network Objects list, double-click internal-network, and then click OK.

Filter:				Filter C	ea
Name	IP Address	Netmask	Description	Object	
📇 amz-amvpn-1	192, 100, 10, 10		NAL URE	outside-d	
🖳 dmz-dmvpn-2	192.168.18.11		NAT the s	outside-d	
🖳 dmz-esa-ISPa	192.168.17.25		NAT the	outside-e	
📑 dmz-networks	192.168.16.0	255.255.248.0	The Orga		
	192.168.16.100		NAT the	outside	
	192.168.17.100		NAT the	outside	
🖳 internal-dns	10.4.48.10		DNS in th		
🖳 🖳 internal-exchange	10.4.48.25		Exchange		
🛃 internal-network	10.4.0.0	255.254.0.0	The orga		
🔤 internal-network-ISPa	10.4.0.0	255.254.0.0	All Intern	any (P),	
📲 Internal-network-ISPb	10.4.0.0	255.254.0.0	All Intern	any (P),	
🔤 🖳 internal-ntp	10.4.48.17		NTP serv		=
📲 internall-network-ISPb	10.4.0.0	255.254.0.0	All Intern		
🖳 outside-cvo-1	172.16.130.2				
🖳 outside-dmvpn-ISPa	172.16.130.1		DMVPN h		
\cdots 🖳 outside-dmvpn-ISPb	172.17.130.1		DMVPN h		
🖳 outside-esa-ISPa	172.16.130.25		ESA on IS		
📟 🖳 outside-webserver-ISPa	172.16.130.100		Webserv		
🖳 outside-webserver-ISPb	172.17.130.100		Webserv		
🧼 🏟 any					-
Selected Original Source Address					
					_

Step 10: On the Add NAT Rule dialog box, under Match Criteria: Original Packet, in the Destination Address box, click the ellipsis (...).

付 Add NAT Rule				x		
Match Criteria: Original Packet —						
Source Interface:	Any 👻	Destination Interface:	Any	•		
Source Address:	internal-network	Destination Address:	any			
		Service:	any			
Action: Translated Packet						
Source NAT Type:	Static 👻					
Source Address:	Original ···	Destination Address:	Original			
PAT Pool Translated Address:		Service:	Original			
Round Robin	Round Robin					
Fall through to interface PAT						
Options						
📝 Enable rule						
Translate DNS replies that mate	th this rule					
Disable Proxy ARP on egress in	terface					
Lookup route table to locate eg	ress interface					
Direction: Both 👻						
Description:						
	OK Cancel	Help				

Step 11: On the Browse Original Destination Address dialog box, click Add, and then click Network Object.

Browse Original Destination Address					
👍 Add 🗸 📝 Edit 📋 Delete 🔍 W	here Used				
Network Object					
Network Object Group IP Address Netmask					
⊡- IPv4 Network Objects	,				

Step 12: On the Add Network Object dialog box, enter the following values, and then click OK.

- · Name-5505-pool
- Type—Network
- IP Address—10.4.156.0
- · Netmask-255.255.252.0
- Description—5505 Teleworker Subnet

🔁 Add Netwo	ork Object			
Name:	5505-pool			
Type:	Network 👻			
IP Address:	10.4.156.0			
Netmask:	255.255.252.0 👻			
Description:	5505 teleworker subnet			
NAT	*			
	OK Cancel Help			

Step 13: On the Browse Original Destination Address dialog box, expand the IPv4 Network Objects list, double-click 5505-pool, and then click OK.

Filter:					Filter C	lea
Name	A 1	IP Address	Netmask	Description	Object	
⊡. IPv4 Ne	twork Objects					-
- 🚅	5505-pool	10.4.156.0	255.255.252.0	5505 Tele		Γ
··· 🖳	dmz-cvo-1	192.168.18.20			outside-c	
···· 🖳	dmz-dmvpn-1	192.168.18.10		NAT the	outside-d	
··· 🖳	dmz-dmvpn-2	192.168.18.11		NAT the s	outside-d	
···· 🖪	dmz-esa-ISPa	192.168.17.25		NAT the	outside-e	
🚅	dmz-networks	192.168.16.0	255.255.248.0	The Orga		Ξ
···· 🖳	dmz-webserver-ISPa	192.168.16.100		NAT the	outside	
···· 🖳	dmz-webserver-ISPb	192.168.17.100		NAT the	outside	
···· 🖳	internal-dns	10.4.48.10		DNS in th		
···· 🖪	internal-exchange	10.4.48.25		Exchange		
🚅	internal-network	10.4.0.0	255.254.0.0	The orga		
··· 🚅	internal-network-ISPa	10.4.0.0	255.254.0.0	All Intern	any (P),	
🚅	Internal-network-ISPb	10.4.0.0	255.254.0.0	All Intern	any (P),	
···· 🖳	internal-ntp	10.4.48.17		NTP serv		
🚅	internall-network-ISPb	10.4.0.0	255.254.0.0	All Intern		
···· 🖪	outside-cvo-1	172.16.130.2				
···· 🚨	outside-dmvpn-ISPa	172.16.130.1		DMVPN h		
···· 🚨	outside-dmvpn-ISPb	172.17.130.1		DMVPN h		
🖳	outside-esa-ISPa	172.16.130.25		ESA on IS		-

Step 14: Under Options, ensure that Enable Rule is selected and that the indicated direction is Both, and then click OK.

🚰 Add NAT Rule			×
Match Criteria: Original Packet —			
Source Interface:	Any 👻	Destination Interface:	Any 🔹
Source Address:	internal-network	Destination Address:	5505-pool
		Service:	any 💮
Action: Translated Packet			
Source NAT Type:	Static 👻		
Source Address:	Original	Destination Address:	Original
PAT Pool Translated Address:		Service:	Original
Round Robin			
Fall through to interface PAT			
Options			
📝 Enable rule			
Translate DNS replies that mate	h this rule		
Disable Proxy ARP on egress in	terface		
Lookup route table to locate eg	ress interface		
Direction: Both 🗸			
Description:			
	OK Cancel	Help	

Step 15: Review the configuration, and then click Apply.

Cisco ASDM applies the following configuration:

object network 5505-pool
subnet 10.4.156.0 255.255.252.0
description 5505 teleworker subnet
<pre>nat (any,any) source static internal-network internal-network</pre>
destination static 5505-pool 5505-pool

Procedure 3

Configure route advertisement

The Internet-edge appliances must advertise the teleworker sites' networks to the internal network. RAVPN address pools are advertised as host routes by reverse route injection (RRI) and summarized on the Internet-edge distribution switch. Teleworker subnets are advertised by RRI, as well, but without summarization; the teleworker subnets remain intact as eight-number (/29) subnets advertised to the rest of the network.

Step 1: Navigate to Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps.

Step 2: Select the crypto map listed under the primary outside interface, and then click **Edit**.

	Traf	fic Selection				Transform Set (IKEv1) IPser Proposal (II		
ype:Priority	#	Source	Destination	Service	Action	Transform Set (IKEV1)	IPsec Proposal (IKEV2)	
interface: outside-16								
dynamic: 65535.65535	1	🧐 any	🗇 any	₽ ip	✓ Protect	ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-128-MD5 ESP-AES-122-SHA ESP-AES-256-SHA ESP-AES-256-MD5 ESP-30ES-SHA ESP-30ES-SHA ESP-30ES-SHA ESP-DES-SHA ESP-DES-SHA		
	m	1						

Step 3: Click the Tunnel Policy (Crypto Map) - Advanced tab.

Step 4: Select Enable Reverse Route Injection, and then click OK.

🔂 Edit IPsec Rule	×
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
🐨 Enable NAT-T	
V Enable Reverse Route Inj	
Security Association Lifetime Settings	
Time: 8:0:0 hh:mm:ss	
Traffic Volume: 4608000 K Bytes	
OK Cancel Help	

Step 5: On the Crypto Maps pane, click Apply.

Step 6: Navigate to Configuration > Device Setup > Routing > EIGRP > Redistribution.

Step 7: On the Redistribution pane, locate the static routing redistribution configuration, and verify that a route-map is defined in the static route redistribution for Enhanced Interior Gateway Routing Protocol (EIGRP). You may need to scroll the window to the far right to view the Route Map column (in the figure below, the Route Map column was moved). If no route-map is configured, you should review and apply the RAVPN-pool advertisement steps in the SBA —Borderless Networks Remote Access VPN Deployment Guide.

🚰 Cisco ASDM 6.4 for ASA - 10.4.24.	24						
File View Tools Wizards Win	dow Help					Look For:	
Home 🖧 Configuration	Ionitoring	Save 💽 Refresh	🕒 Back 🜔	Forward	P Help		
Device List	0 9 ×	Configuration > D	evice Setup	> Routing >	EIGRP > Redis	tribution	
🕈 Add 📋 Delete 🚿 Connect		Define the condition	ns for redistri	buting routes fi	om one routing p	protocol to an	other.
Find: Go		EIGRP Process	Protocol	Route Map	Bandwidth	Delay	Reliability
10.4.24.24		100	Static	redistribute			
Device Setup							

Step 8: Navigate to Configuration > Firewall > Advanced > Standard ACL.

Step 9: Add the Cisco ASA 5505 teleworker's subnet to the route-map's access-list by selecting the **redistribute-list** entry in the ACL list, clicking **Add**, and then clicking **Add ACE**.

Home 🖧 Configuration 🔯 Monitoring	Save 🔇 Refresh 🔇 Back 🚫 Forward 🢡 Help
Device List 리 무 ×	Configuration > Firewall > Advanced > Standard ACL
🕈 Add 📋 Delete 🚿 Connect	💠 Add 🗸 🗹 Edit 📋 Delete 🛧 🗲 🐰 ங 💼 -
Find: Go	Add ACL Action Description
10.4.24.24	Add ACE
10.7.27.30	👷 Insert
Firewall 급 무	Insert After
Advanced	1 🏟 any 🖌 Permit
- Anti-Spoofing	RA_SplitTunnelACL
Encrypted Traffic Inspection	1 📑 10.4.0.0/15 🖌 Permit
Certificate Management	
Fragment	
TCP Ontions	
Virtual Access	
ACL Manager	
Standard ACL	
A	

Step 10: On the Add ACE dialog box, next to the **Address** box. click the ellipsis (...).

🔂 Add A	CE				
Action:	Permit	Deny			
Address:			(\subset	

Step 11: On the Browse Address dialog box, in the Address box, type 10.4.156.0/22, and then click OK.

Name	IP Address	Netmask	Descrip	Object	
⊡··IPv4 Network Objects					
🌍 any	0.0.0.0	0.0.00			
	10.4.24.0	255.255.255.224			
	172.16.130.0	255.255.255.0			
outside-17-network	172.17.130.0	255.255.255.0			
	10.4.0.0	255.254.0.0			
··· 🖳 10.4.28.0	10.4.28.0	255.255.252.0			
D 40 40 40	10 10 10 10	200 200 200 200			1

Step 12: Verify that Permit is selected and that 10.4.156.0/22 is the value for Address.

Step 13: On the Add ACE dialog box, in the Description box, enter 5505 teleworker subnet, and then click OK.

🔂 Add A	CE E	×
Action:	Permit O Deny	
Address:	10.4.156.0/22	
Descriptio	n:	
5505 tele	worker subnet	
	OK Cancel Help	

Step 14: In the Standard ACL pane, click Apply.

📴 Cisco ASDM 6.4 for ASA - 10.4.24.24						
File View Tools Wizards Window Help					Look For:	
Home 🖓 Configuration 🔯 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🢡 Help						
Device List 🗇 🕂 🗡	Co	nfiqura	tion > Firewall > Advanced	> <u>Standard AC</u>	<u>1</u>	
🕈 Add 📋 Delete 🚿 Connect	+	Add +	🗹 Edit 📋 Delete 🛧 🗲	🐰 🗈 💼 -	·	
Find: Go	No		Address	Action	Description	
10.4.24.24		🗇 redistribute-list				
		1	10.4.28.0/22	🖌 Permit		
		2	10.4.156.0/22	🖌 Permit	5505 teleworker subnet	
Firewall a p		Scansa	fe_Tower_Exclude			
Advanced		RA_Full	TunnelACL			
Anti-Spoofing		1	🏟 any	🎸 Permit		
⊕-Io Encrypted Traftc Inspection ⊕-Io Encrypted Traftc Inspection ⊕-Io Fragment ⊕-Io IP Audit		RA_Spli	tTunnelACL			
		1	10.4.0.0/15	🖌 Permit		

Cisco ASDM applies the following configuration:

crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set

reverse-route

access-list redistribute-list remark **5505 teleworker subnet** access-list redistribute-list standard permit **10.4.156.0**

255.255.252.0



Configuring Teleworker Cisco ASA 5505 Endpoints

- 1. Configure inside VLAN and switch ports
- 2. Define global device configuration
- 3. Configure outside VLAN and switch port
- 4. Configure Cisco ASA 5505 DHCP server
- 5. Configure Cisco ASA 5505 Easy VPN client

Each teleworker's Cisco ASA 5505 endpoint must be configured to connect to your resilient Internet-edge appliance. Because this configuration is likely to be deployed on multiple devices, the configuration is shown only in the command-line interface to streamline deployment. All Cisco ASA 5505 teleworker sites connect using Network Extension Mode, which allows teleworker-site endpoints to connect freely to the organization's LAN. Connecting in Network Extension Mode is particularly critical for endpoints, such as IP phones and video surveillance cameras, which might be susceptible to NAT's modification of data traffic.

Each site must use a unique inside-IP subnet. Otherwise, all configuration is identical between sites. To avoid conflicting address assignments, Cisco recommends that you maintain a spreadsheet of subnet assignments for the various users that will be issued Cisco ASA 5505 telecommuter equipment.

User name Subnet		ASA 5505 LAN address	Hostname	
Employee1	10.4.156.0/29	10.4.156.1	5505site1	

Procedure 1

Configure inside VLAN and switch ports

Each Cisco ASA 5505 teleworker site needs a unique inside subnet, which you should track in a spreadsheet, as recommended in the introduction of this section.

Step 1: Configure the VLAN 1 interface for the teleworker site's LAN.

interface Vlan1
no ip address
nameif inside
security-level 100
ip address 10.4.156.1 255.255.248

Step 2: Associate the Cisco ASA 5505's Ethernet 0/1 through Ethernet 0/7 interfaces with VLAN 1, and instruct the teleworker to connect PoE-enabled devices to the Ethernet 0/6 and 0/7 ports.

interface Ethernet0/1
switchport access vlan 1
no shutdown
...
interface Ethernet0/7
switchport access vlan 1
no shutdown

Procedure 2

Step 1: Configure the Cisco ASA 5055's hostname and domain name.

hostname 5505site1

domain-name cisco.local

- Step 2: Define a local administrative username. username admin password clscol23 privilege 15
- Step 3: Set the enable password.

enable password **clsco123**

Step 4: Define the management configuration.

http server enable http 10.0.0.0 255.0.0.0 inside ssh 10.0.0.0 255.0.0.0 inside management-access inside

Step 5: If you are using centralized AAA, define authentication servers for management access.

aaa-server AAA-SERVERS protocol tacacs+

aaa-server AAA-SERVERS (inside) host 10.4.48.15

key SecretKey

aaa authentication http console AAA-SERVERS LOCAL aaa authentication ssh console AAA-SERVERS LOCAL



Step 1: Configure a VLAN interface to receive an IP address via DHCP from the teleworker's Internet gateway device.

interface Vlan2 nameif outside

- security-level 0
- ip address dhcp setroute

Step 2: Associate the Cisco ASA 5505's Ethernet 0/0 interface with VLAN 2, and instruct the teleworker to connect Ethernet 0/0 to their Internet gateway device.

interface Ethernet0/0
switchport access vlan 2
no shutdown

Procedure 4

Configure Cisco ASA 5505 DHCP server

The Cisco ASA 5505 must be configured to provide IP-addresses for the teleworker endpoints, such as computers, phones, printers, and video surveillance devices. Each site must use a unique subnet, which should be tracked in a spreadsheet, as recommended in the introduction of this section.

Step 1: Define the DHCP scope address range. The DHCP scope must be in the same subnet as the inside (VLAN 1) interface.

```
dhcpd address 10.4.156.2-10.4.156.6 inside
```

Step 2: Configure the DNS and domain-name values that will be distributed to clients.

dhcpd dns **10.4.48.10** interface inside dhcpd domain **cisco.local** interface inside

Step 3: Define DHCP option 150 to provide the Cisco Unified Call Manager Server address for Cisco IP phones.

dhcpd option 150 ip **10.4.48.120**

Step 4: Enable the DHCP scope.

dhcpd enable inside

Procedure 5

Configure Cisco ASA 5505 Easy VPN client

Cisco ASA 5505 uses Easy VPN network-extension mode to negotiate the VPN connectivity to the Internet-edge Cisco ASA Remote Access server.

Step 1: Apply the Easy VPN client configuration for the remote Cisco ASA 5505: The vpngroup and password values must match the IPsec Remote Access Connection Profile that you configured on the Internet-edge appliance.

vpnclient server 172.16.130.122

Step 2: Set network-extension mode:

vpnclient mode **network-extension-mode**

Step 3: Define the Easy VPN client connection attributes. The vpngroup and password values must match the IPsec Remote Access Connection Profile that you configured on the Internet-edge appliance.

vpnclient vpngroup **Teleworker5505** password **cisco123**

Step 4: Enable the Cisco ASA 5505's Easy VPN client:

vpnclient enable

The teleworker must manually initiate their VPN connection; when the user employs a web browser to access web content on your internal network, Cisco ASA 5505 intercepts the connection and provides an interactive login prompt. The user must provide login credentials, at which point the VPN connection is negotiated with the provided username and password.



The IP Phone connected to the Cisco ASA 5505 can't place or receive calls if the user's VPN connection is not active.

In the event that a teleworker's VPN access must be revoked, the authentication server should deny the teleworker's access.

Appendix A: Product List

Remote-Site

Functional Area	Product Description	Part Numbers	Software
Remote Site Appliance	Cisco ASA 5505 Firewall Edition Bundle security appliance	ASA5505-BUN-K9	8.4(4)1

Internet Edge

Functional Area	Product Description	Part Numbers	Software	
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 8.6(1)1, IPS 7.1(4)	
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	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	6.6.114	
RA VPN Firewall	Cisco ASA 5545-X Firewall Edition - security appliance	ASA5545-K9	8.6(1)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 ASA5512-X Security Plus license	ASA5512-SEC-PL		
	Firewall Management	ASDM	6.6.114	

Appendix B: Configuration Files

VPN-ASA5525

```
hostname VPN-ASA5525
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
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
L
interface GigabitEthernet0/2
 description LAN/STATE Failover Interface
interface GigabitEthernet0/3
 no nameif
 no security-level
no ip address
L
interface GigabitEthernet0/3.16
 description Prymary Internet connection VLAN 16
```

vlan 16 nameif outside-16 security-level 0 ip address 172.16.130.122 255.255.255.0 standby 172.16.130.121 T interface GigabitEthernet0/3.17 description Resilient Internet connection on VLAN 17 vlan 17 nameif outside-17 security-level 0 ip address 172.17.130.122 255.255.255.0 standby 172.17.130.121 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 T interface GigabitEthernet0/6 shutdown no nameif no security-level no ip address T interface GigabitEthernet0/7 shutdown no nameif no security-level no ip address T interface Management0/0

shutdown no nameif no security-level no ip address 1 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 RA-Pool subnet 10.4.28.0 255.255.252.0 description RA VPN client pool 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 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 inside access in extended permit ip any any access-list redistribute-list standard permit 10.4.28.0 255.255.252.0 access-list redistribute-list remark 5505 Teleworker subnet access-list redistribute-list standard permit 10.4.156.0 255.255.252.0

pager lines 24 logging enable logging buffered informational logging asdm informational mtu inside 1500 mtu outside-16 1500 mtu outside-17 1500 ip local pool RA-pool 10.4.28.1-10.4.31.255 mask 255.255.252.0 failover failover lan unit primary failover lan interface failover GigabitEthernet0/2 failover polltime unit msec 200 holdtime msec 800 failover polltime interface msec 500 holdtime 5 failover key ***** 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-66114.bin no asdm history enable arp timeout 14400 nat (inside,outside-16) source static any any destination static NETWORK OBJ 10.4.28.0 22 NETWORK OBJ 10.4.28.0 22 no-proxy-arp route-lookup nat (any, any) source static Internal Network Internal Network destination static 5505-Pool 5505-Pool access-group inside access in in interface inside 1 route-map redistribute-map permit 1 match ip address redistribute-list 1 router eigrp 100 no auto-summary

network 10.4.0.0 255.254.0.0 passive-interface default no passive-interface inside redistribute static route-map redistribute-map route outside-16 0.0.0.0 0.0.0.0 172.16.130.126 128 track 1 route inside 0.0.0.0 0.0.0.0 10.4.24.1 tunneled timeout xlate 3:00:00 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 kev ***** aaa-server AAA-RADIUS protocol radius aaa-server AAA-RADIUS (inside) host 10.4.48.15 timeout 5 kev ***** 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 10.4.0.0 255.254.0.0 inside no snmp-server location no snmp-server contact snmp-server community ***** 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 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 map outside-17 map 65535 ipsec-isakmp dynamic SYSTEM DEFAULT CRYPTO MAP crypto map outside-17 map interface outside-17 crypto map outside-16 map 65535 ipsec-isakmp dynamic SYSTEM DEFAULT CRYPTO MAP crypto map outside-16 map interface outside-16 crypto ca trustpoint ASDM TrustPoint1 enrollment self subject-name CN=VPN-ASA5525.cisco.local keypair sslpair proxy-ldc-issuer crl configure

crypto ca certificate chain ASDM_TrustPoint1
certificate 199fc84f
30820270 308201d9 a0030201 02020419 9fc84f30 0d06092a
864886f7 0d010105
0500304a 3120301e 06035504 03131756 504e2d41 53413535
32352e63 6973636f
2e6c6f63 616c3126 30240609 2a864886 f70d0109 02161756
504e2d41 53413535
32352e63 6973636f 2e6c6f63 616c301e 170d3132 30363034
31373532 35345a17
0d323230 36303231 37353235 345a304a 3120301e 06035504
03131756 504e2d41
53413535 32352e63 6973636f 2e6c6f63 616c3126 30240609
2a864886 f70d0109
02161756 504e2d41 53413535 32352e63 6973636f 2e6c6f63
616c3081 9f300d06
092a8648 86f70d01 01010500 03818d00 30818902 818100d6
2c54cc0b felcffa0
ba51f93a 7d0017b1 e17a7765 31a16ee9 f9153059 a81d6ee0
c7b98f84 09930b89
f88877d7 8b22c3eb
3828b31f b2440c42 2102cf43 1ae023db 962c5224 0a6225af
11a2dc48 02e1dc72
8be4a007 42739a90 7cb16882 9815cd9f 576aa4b7 7bb4cf02
03010001 a3633061
300f0603 551d1301 01ff0405 30030101 ff300e06 03551d0f
0101ff04 04030201
86301f06 03551d23 04183016 80148d1b 53b7eff9 ebf29730
4632e70c cd0922ea
3e75301d 0603551d 0e041604 148d1b53 b7eff9eb f2973046
32e70ccd 0922ea3e
75300d06 092a8648 86f70d01 01050500 03818100 c66af82c
d9402d37 9663a12d
13489b6f 8b3fdcb1
cb0a050d 8038afb3 daff4a30 2ed0d49a 9629d5ca c8d3c3f0

0e5b2df9 d57b02f1 e1618468 b80be22f 89942cb5 34e3d05b 63f4edb1 3835ddd0 0542e2b1 d76c112b c2d5ef2e e9858080 fd297929 131784cc e628b546 quit crypto ikev1 enable outside-16 crypto ikev1 enable outside-17 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 aroup 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 crypto ikev1 policy 65535 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 1 track 1 rtr 16 reachability telnet timeout 5 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 trust-point ASDM TrustPoint1 outside-17 ssl trust-point ASDM TrustPoint1 outside-16 webvpn enable outside-16 enable outside-17 anyconnect image disk0:/anyconnect-linux-2.5.2014-k9.pkg 1 anyconnect image disk0:/anyconnect-macosx-i386-2.5.2014-k9.pkg 2 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 3 anyconnect profiles ra profile disk0:/ra profile.xml anyconnect enable tunnel-group-list enable group-policy 5505Group internal group-policy 5505Group attributes vpn-tunnel-protocol ikev1 l2tp-ipsec password-storage disable split-tunnel-policy tunnelall secure-unit-authentication enable nem enable 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 webvpn anyconnect profiles value ra profile type user group-policy GroupPolicy Administrators internal group-policy GroupPolicy Administrators attributes banner value Your acess is via unrestricted split tunnel. split-tunnel-policy tunnelall split-tunnel-network-list value RA SplitTunnelACL webvpn anyconnect profiles value ra profile type user group-policy GroupPolicy Partner internal group-policy GroupPolicy Partner attributes

banner value Your Access is restricted to the partner server vpn-filter value RA PartnerACL webvpn anyconnect profiles value ra profile type user username admin password w2Y.60p4j7clVDk2 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 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 tunnel-group Teleworker5505 type remote-access tunnel-group Teleworker5505 general-attributes authentication-server-group AAA-RADIUS default-group-policy 5505Group tunnel-group Teleworker5505 ipsec-attributes ikev1 pre-shared-key ***** ! class-map inspection default match default-inspection-traffic 1 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 L service-policy global policy global prompt hostname context no call-home reporting anonymous call-home profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/ oddce/services/DDCEService destination address email callhome@cisco.com destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic monthly 23 subscribe-to-alert-group configuration periodic monthly 23 subscribe-to-alert-group telemetry periodic daily Cryptochecksum:daab272354b93c144a6e62651655b319 : end

ASA-5505

hostname 5505site1 domain-name cisco.local enable password 9jNfZuG3TC5tCVH0 encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0/0 switchport access vlan 2

1 interface Ethernet0/1 ! interface Ethernet0/2 1 interface Ethernet0/3 1 interface Ethernet0/4 1 interface Ethernet0/5 1 interface Ethernet0/6 1 interface Ethernet0/7 1 interface Vlan1 nameif inside security-level 100 ip address 10.4.156.1 255.255.258.248 1 interface Vlan2 nameif outside security-level 0 ip address dhcp setroute 1 ftp mode passive dns server-group DefaultDNS domain-name cisco.local pager lines 24 mtu outside 1500 mtu inside 1500 icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 timeout xlate 3:00:00 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-SERVERS protocol tacacs+ aaa-server AAA-SERVERS (inside) host 10.4.48.15 kev ***** user-identity default-domain LOCAL aaa authentication http console AAA-SERVERS LOCAL aaa authentication ssh console AAA-SERVERS LOCAL http server enable http 10.0.0.0 255.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ikev1 policy 65535 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 telnet timeout 5 ssh 10.0.0.0 255.0.0.0 inside ssh timeout 5 console timeout 0 management-access inside vpnclient server 172.16.130.122 vpnclient mode network-extension-mode vpnclient vpngroup Teleworker5505 password ***** vpnclient enable dhcpd option 150 ip 10.4.48.120 1 dhcpd address 10.4.156.2-10.4.156.6 inside

dhcpd dns 10.4.48.10 interface inside dhcpd domain cisco.local interface inside dhcpd enable inside 1 threat-detection basic-threat threat-detection statistics access-list no threat-detection statistics tcp-intercept webvpn username admin password e1z89R3cZe9Kt6Ib encrypted privilege 15 class-map inspection default match default-inspection-traffic 1 1 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 no call-home reporting anonymous call-home profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/ oddce/services/DDCEService destination address email callhome@cisco.com destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:3166aa566ffb90383d46ce8e325e2c1f

: end

Notes

Appendix C: Changes

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

- We upgraded the Cisco ASA software to 8.6(1).
- We made minor changes to improve the readability of this guide.



Feedback

Click here to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

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 ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF 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 ON ON 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.

© 2012 Cisco Systems, Inc. All rights reserved.



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.

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)