## 

# **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.





## Remote Access VPN Deployment Guide

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 10.5.204.5 255.255.25.0

### **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 Guide	1
Cisco SBA Borderless Networks	1
Route to Success	1
About This Guide	1
Introduction	2
Related Reading	2
Design Goals	2
Remote Access VPN	5
Business Overview	5
Technology Overview	5
Deployment Details	6
Configuring Cisco Secure ACS	6
Configuring the Standalone RA VPN Firewall	12
Configuring the Remote-Access VPN	20

Summary	33
Appendix A: Product List	34
Appendix B: Configuration Example	36
Appendix C: Changes	40

## 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

Cisco SBA Borderless Networks is a solid network foundation designed to provide networks with up to 10,000 connected users the flexibility to support new users and network services without re-engineering the network. We created a prescriptive, out-of-the-box deployment guide that is based on best-practice design principles and that delivers flexibility and scalability.

The Cisco SBA—Borderless Networks Remote Access VPN Deployment Guide supports the remote user with secure remote access (RA). This guide covers the deployment of RA VPN services to either the primary Internet edge firewall or to a standalone RA VPN-specific device.

## **Related Reading**

The Cisco SBA—Borderless Networks Internet Edge Design Overview orients you to the overall Cisco SBA design and explains the requirements that were considered when selecting specific products.

The Cisco SBA—Borderless Networks Firewall and IPS Deployment Guide focuses on the Internet edge firewall and intrusion prevention system (IPS) security services that protect your organization's gateway to the Internet.

The Cisco SBA—Borderless Networks Remote Mobile Access Deployment Guide extends the remote access solution for mobile devices, such as phones and tablets, and for traditional devices, it offers expanded connection options, such as Cisco ScanSafe Cloud Web Security, Always-on VPN, and other features.

## **Design Goals**

This architecture is based on requirements gathered from customers, partners, and Cisco field personnel for organizations with up to 10,000 connected users. When designing the architecture, we considered the gathered requirements and the following design goals.

#### Notes



2189

#### Ease of Deployment, Flexibility, and Scalability

Organizations with up to 10,000 users are often spread out among different geographical locations, making flexibility and scalability a critical requirement of the network. This design uses several methods to create and maintain a scalable network:

- By keeping a small number of standard designs for common portions of the network, support staff is able to design services for, implement, and support the network more effectively.
- Our modular design approach enhances scalability. Beginning with a set of standard, global building blocks, we can assemble a scalable network to meet requirements.
- Many of the plug-in modules look identical for several service areas; this common look provides consistency and scalability in that the same support methods can be used to maintain multiple areas of the network. These modules follow standard core-distribution-access network design models and use layer separation to ensure that interfaces between the plug-ins are well defined.

#### **Resiliency and Security**

One of the keys to maintaining a highly available network is building appropriate redundancy in order to guard against failure in the network. The redundancy in our architecture is carefully balanced with the complexity inherent in redundant systems.

With the addition of a significant amount of delay-sensitive and dropsensitive traffic such as voice and video conferencing, we also place a strong emphasis on recovery times. Choosing designs that reduce the time between failure detection and recovery is important for ensuring that the network stays available even in the face of a minor component failure.

Network security is also a strong component of the architecture. In a large network, there are many entry points, and we ensure that they are as secure as possible without making the network too difficult to use. Securing the network not only helps keep the network safe from attacks but is also a key component to network-wide resiliency.

#### **Ease of Management**

While this guide focuses on the deployment of the network foundation, the design takes next-phase management and operation into consideration. The configurations in the deployment guides are designed to allow the devices to be managed via normal device-management connections, such as Secure Shell (SSH) Protocol and HTTPS, as well as via Network Management System (NMS). The configuration of the NMS is not covered in this guide.

#### **Advanced Technology-Ready**

Flexibility, scalability, resiliency, and security all are characteristics of an advanced technology-ready network. The modular design of the architecture means that technologies can be added when the organization is ready to deploy them. However, the deployment of advanced technologies, such as collaboration, is eased because the architecture includes products and configurations that are ready to support collaboration from day one. For example:

- Access switches provide Power over Ethernet (PoE) for phone deployments without the need for a local power outlet
- The entire network is preconfigured with quality of service (QoS) to support high-quality voice.
- Multicast is configured in the network to support efficient voice and broadcast-video delivery.
- The wireless network is preconfigured for devices that send voice over the wireless LAN, providing IP telephony over 802.11 Wi-Fi (referred to as mobility) at all locations.

The Internet edge is ready to provide soft phones via VPN, as well as traditional hard or desk phones.

## **Remote Access VPN**

### **Business Overview**

Many organizations need to offer network connectivity to their data resources for users, regardless of the user's location. Employees, contractors, and partners may need to access the network when traveling or working from home or from other off-site locations. The remote-access connectivity should support:

- A wide variety of endpoint devices.
- · Seamless access to networked data resources.
- Authentication and policy control that integrates with the authentication resources in use by the organization.
- Cryptographic security to prevent the exposure of sensitive data to
   unauthorized parties who accidentally or intentionally intercept the data.

## **Technology Overview**

The Cisco ASA family supports IP Security (IPsec), web portal, full-tunnel Secure Sockets Layer (SSL) VPNs for client-based remote access, and IPsec for site-to-site VPN. This section describes the basic configuration of SSL VPNs for remote access.

The Cisco AnyConnect Secure Mobility Client is recommended for remote users who require full network connectivity. The Cisco AnyConnect client uses SSL and is designed for automated download and installation. SSL access can be more flexible and is likely to be accessible from more locations than IPsec, as few companies block HTTPS access out of their networks. Cisco SBA Borderless Networks offer two different remote-access VPN designs:

- Remote-access (RA) VPN integrated with Cisco ASA Series firewall, in the integrated design module—This offers lower capital investment and reduces the number of devices the network engineering staff must manage.
- Remote-access VPN deployed on a pair of standalone Cisco ASAs, in the standalone design module—This design offers greater operational flexibility and scalability while providing a simple migration path from an existing RA VPN installation.

This document describes the configuration for remote-access VPN via Cisco AnyConnect for SSL connections. The configuration is broken into sections for each of the various access methods, and it begins with a configuration that is common to all of the access methods. Configurations for both the integrated and standalone design modules offer identical functionality and capability so that regardless of the design chosen, the user experience is unchanged from one design to the other. Unless specifically noted, the configuration described in this document is common to both the integrated and standalone designs.

Hardware applied in this design is selected based on the following performance values.

Table 1 - Hardware performance

Cisco ASA family product	Maximum SSL VPN sessions
Cisco ASA 5512-X	250
Cisco ASA 5515-X	250
Cisco ASA 5525-X	750
Cisco ASA 5545-X	2500

A different VPN group is required for each remote-access policy. This design includes three VPN groups:

- Administrative users—These users are authenticated by Cisco Secure Access Control System (ACS) using the RADIUS protocol and also have a local username and password fallback option. This ensures that VPN access is available when the Cisco Secure ACS or Microsoft Active Directory server is unavailable. Administrative users have full access to the entire network.
- **Employees**—These users are authenticated by Cisco Secure ACS and have open access to the entire network
- **Partners**—These users are authenticated by Cisco Secure ACS and, although they use a tunnel-all VPN policy, there is an access-list applied to the tunnels in order to restrict access to specific hosts.

## **Deployment Details**

#### **Reader Tip**

For more information about the baseline configuration of the appliance (including availability, routing, Internet and inside connectivity, and management or administration access), see the *Cisco SBA—Borderless Networks Firewall and IPS Deployment Guide*.

Cisco ASA's remote-access VPN termination capabilities can be configured from the command line or from the graphical user interface Cisco Adaptive Security Device Manager (ASDM). Cisco ASDM provides a guided step-bystep approach to the configuration of RA VPN and reduces the likelihood of configuration errors.

### **Process (Optional)**



Configuring Cisco Secure ACS

- 1. Define external groups
- 2. Create the device-type group
- 3. Create the network device
- 4. Create authorization profiles
- 5. Configure the access service
- 6. Create authorization rules

Authentication is the portion of the configuration that verifies that users' credentials (username and password) match those stored within the organization's database of users that are allowed to access electronic resources. Cisco Smart Business Architecture designs use either Cisco Secure ACS or Microsoft Active Directory for authentication of remote access VPN users. Cisco Secure ACS gives an organization enhanced ability to control the access that VPN users receive. For those organizations not interested in using Cisco Secure ACS, Microsoft Active Directory by itself will be used, and this process can be skipped.

When the Cisco ASA firewall queries the Cisco Secure ACS server (which then proxies the request to the Active Directory database) to determine whether a user's name and password is valid, Cisco Secure ACS also retrieves other Active Directory attributes, such as group membership, that Cisco Secure ACS may use when making an authorization decision. Based on the group membership, Cisco Secure ACS sends back a group policy name to the appliance, along with the success or failure of the login. Cisco ASA uses the group policy name in order to assign the user to the appropriate VPN group policy.

In this process, Active Directory is the primary directory container for user credentials and group membership. Before you begin this process, your Active Directory must have three groups defined: **vpn-administrator**, **vpn-employee**, and **vpn-partner**. These groups map users to the respective VPN access policies.

#### Procedure 1

**Step 1:** Navigate to the Cisco Secure ACS Administration Page. (Example: https://acs.cisco.local)

Step 2: In Users and Identity Stores > External Identity Stores > Active Directory, click the Directory Groups tab.

Step 3: Click Select.

Step 4: On the External User Groups pane, select the three vpn groups, and then click OK.

R	<b>V</b>	cisco.local/Users/vpn-administrator	GLOBAL
R	<b>v</b>	cisco.local/Users/vpn-employee	GLOBAL
R	<b>V</b>	cisco.local/Users/vpn-partner	GLOBAL

Step 5: On the Active Directory pane, click Save Changes.



Create the device-type group

**Step 1:** In Network Resources > Network Device Groups > Device Type, click **Create**.

Step 2: In the Name box, enter a name for the group. (Example: ASA)

Step 3: In the Parent box, select All Device Types, and then click Submit.

Network Resources >	Network Device Groups > Dev	ice Type > Create		
Device Group -	General			
🖕 Name:	ASA			
Description:				
👷 Parent:	All Device Types		Select	
Required field	lds			

#### **Procedure 3**

Create the network device

For the Cisco ASA firewall, create a network device entry in Cisco Secure ACS.

**Step 1:** In Network Resources > Network Devices and AAA Clients, click **Create**.

**Step 2:** In the Name box, enter the device hostname. (Example: IE-ASA5545)

Step 3: In the Device Type box, select All Device Types:ASA.

**Step 4:** In the IP box, enter the inside interface IP address of the Cisco ASA appliance. (Example: 10.4.24.30)

Step 5: Select TACACS+.

**Step 6:** Enter the TACACS+ shared secret key. (Example: SecretKey)

Step 7: Select RADIUS.

**Step 8:** Enter the RADIUS shared secret key, and then click **Submit**. (Example SecretKey)

Name:	IE-ASA5545	
Description	:	
etwork Devic	ce Groups	
ocation	All Locations	Select
Device Type	All Device Types:ASA	Select
P Address	Au	uthentication Options
<ul> <li>Single Addres</li> <li>IP: 10.4.2</li> </ul>	4.30	TACACS+ V Shared Secret: SecretKey Hide Single Connect Device Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support RADIUS V Shared Secret: SecretKey Hide
		CoA port: 1700  Enable KeyWrap  Key Encryption Key:  Message Authenticator Code Key:  Key Input Format ASCII HEXADECIMAL

#### Procedure 4

#### **Create authorization profiles**

Create two different authorization profiles to identify users that belong to either the vpn-administrator or vpn-partner groups in Active Directory.

**Step 1:** In Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles, click **Create.** 

**Step 2:** In the Name box, enter a name for the authorization profile. (Example: RA-Administrator)

**Step 3:** Click the **RADIUS Attributes** tab, and then in the Manually Entered pane, in the Attribute box, select **Class**.

Next, you must configure the attribute value to match the group policy that you will configure on the Cisco ASA appliance.

**Step 4:** In the Value box, enter the group policy name, and then click **Add**. (Example: GroupPolicy\_Administrators)

General Common Ta	sks RADIUS Attrib	utes		
Common Tasks Attribute	s			
Attribute		Туре	Value	
Manually Entered				
Attribute		Туре	Value	
Class		String	GroupPolicy_Administrators	
Add A Edit V	Replace /	elete		
Dictionary Type:	RADIUS-IETF		<b>•</b>	
RADIUS Attribute:			Select	
Attribute Type:				
Attribute Value:	Static		•	

**Step 5:** Repeat this procedure to build an authorization profile for partners, using the group policy **GroupPolicy\_Partner** value.

#### Procedure 5

Configure the access service

Create a policy to inspect for group membership in the return traffic from the Active Directory server.

Step 1: In Access Policies > Access Services, click Create.

Step 2: On the General tab, enter the name Remote Access.

#### Step 3: Select User Selected Service Type, and then click Next.

	click Finish.
Access Policies > Access Services > Create	
General Allowed Protocols	Access Policies > Access Services > Create
Step 1 - General         General         Name:       Remote Access         Description:         Access Service Policy Structure         Based on service template         Based on existing service         Based on existing service         User Selected Service Type         Network Access	<ul> <li>✓ General Allowed Protocols</li> <li>Step 2 - Allowed Protocols</li> <li>✓ Process Host Lookup</li> <li>Authentication Protocols</li> <li>✓ Allow PAP/ASCII</li> <li>← Allow CHAP</li> <li>↓ ○ Allow MS-CHAPy1</li> </ul>
User Selected Service Type Policy Structure V Identity Group Mapping V Authorization Back Next Finish Cancel	<ul> <li>Allow MS-CHAPv2</li> <li>Allow EAP-MD5</li> <li>Allow EAP-TLS</li> <li>Allow LEAP</li> <li>Allow PEAP</li> <li>Allow EAP-FAST</li> </ul>
	Preferred EAP protocol LEAP
	Back Next Finish Cancel

**Step 5:** In Access Policies > Access Services > Service Selection Rules, click **Customize**.

Step 4: On the Allowed Protocols tab, select Allow PAP/ASCII, and then

**Step 6:** On the Customize Conditions pane, move **Compound Condition** from **Available** to **Selected**, and then click **OK**.

vailable:		Selected:		
ACS Host Name		Protocol	~	
Device Filter		Compound Condition		$\overline{}$
Device IP Address				_
Device Port Filter	<			~
End Station Filter				
NDG:Device Type				
NDG:Location	>>>			$\sim$
Time And Date				
JseCase	11			$\mathbf{\Sigma}$

Step 7: On the Service Selection Rules pane, click Create.

Step 8: In the dialog box, name the rule Remote Access.

Step 9: Select Protocol.

Step 10: In the list at right, select match, and then in the box, enter Radius.

**Step 11:** Select **Compound Condition**, and then in the Dictionary list, choose **NDG**.

Step 12: For Attribute, select Device Type.

Step 13: For Value, select All Device Types: ASA.

**Step 14:** Under Current Condition Set, click **Add V**. The information is added to the Current Condition Set.

Step 15: In the Results Service list, choose Remote Access, and then click OK.

eneral ame: Remote Acc	ess Status:	Enabled 👻	0		
	stomize button in the ns and results are a				vhich policy
onditions Protocol:	match	- Rad	ius	Select	ו
Compound Con	dition:				J
Condition: Dictionary:		Attribute:			
NDG		<ul> <li>Device Type</li> </ul>		Select	
Operator:		Value:			
in 👻				Select	
Current Condition	Set:				
ſ	Add V Edit A	Replace V			
	NDG:Device Type in Al	Device Types:AS	A	*	
And > • Or > •					
				-	
L			Delete	eview	
esults					
ervice: Remote A	cess 🗸				

**Step 16:** Navigate to Access Policies > Access Services > Remote Access > Identity.

Step 17: In the Identity Source box, select AD1, and then click Save Changes.

**Step 18:** In Access Policies > Access Services > Remote Access > Authoriz ation, click **Customize**.

**Step 19:** On the Customize Conditions pane, move **AD1:ExternalGroups** from **Available** to **Selected**, and then click **OK**.

Available:	Selected:	
ACS Host Name Authentication Method Authentication Status Device Filter Device IP Address Device Port Filter Eap Authentication Method Eap Tunnel Building Method End Station Filter Identity Group	AD1:ExternalGroups	* K <

**Procedure 6** 

Create authorization rules

**Step 1:** In Access Policies > Access Services > Remote Access > Authoriza tion, click **Create**.

Step 2: Enter a rule Name.(Example: RA-Administrator)

Step 3: Under Conditions, select AD1:ExternalGroups.

**Step 4:** In the condition definition box, select the Active Directory group. (Example: cisco.local/Users/vpn-administrator).

**Step 5:** Under Results, select the authorization profile, and then click **Select**. (Example: RA-Administrator)

General		
Name: RA-Administrator	Status: Enabled	<b>▼</b>
		t area of the policy rules screen controls which ble here for use in policy rules.
Conditions		
Compound Condition:		-ANY-
AD1:ExternalGroups:		
contains any		
Select Deselect (	Clear	٣
Authorization Profiles:		
RA-Administrator		You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.
Select Deselect		

Step 6: Repeat Step 1 through Step 5 for the partner rule.

**Step 7:** Repeat Step 1 through Step 5 for the employee rule, using **Permit Access** as the authorization profile.

Step 8: On the Authorization pane, click the Default rule.

#### Step 9: Select DenyAccess as the authorization profile, and then click OK.

Filter:	Status   Match if:			Equals 👻	Equals 👻 Enabled 👻 Clear Filter Go 🗢				
		Status	Name	Compound Co	ndition		onditions rnalGroups		Results Authorization Profil
1		0	RA-Administrator	-ANY-		contains	any (cisco.local/Us	ers/vpn-administrator)	RA-Administrator
2		0	RA-Partner	-ANY-		contains	any (cisco.local/Us	ers/vpn-partner)	RA-Partner
3		0	RA-Employee	-ANY-		contains	any (cisco.local/Us	ers/vpn-employee)	Permit Access

Once the remote-access services have been created, you can change the order.

**Step 10:** In Access Policies > Access Services > Service Selection Rules, select the **Remote Access** policy, and then use the up arrow button to move it to the first position.

Filter: Status Match if: Equals V Enabled V Clear Filter Go V						
		Status	Name	Protocol	Conditions Compound Condition	Results Service
1		•	Remote Access	match Radius	NDG:Device Type in All Device Types:ASA	Remote Access
2		0	Rule-1	match Radius	-ANY-	Default Network /
3		•	Rule-2	match Tacacs	-ANY-	Default Device A
**		Default		III If no rules defined or no	enabled rule matches.	DenyAccess

#### **Process**



Configuring the Standalone RA VPN Firewall

- 1. Configure the LAN distribution switch
- 2. Apply Cisco ASA initial configuration
- 3. Configure internal routing
- 4. Configure user authentication
- 5. Configure time synchronization and logging
- 6. Configure device-management protocols
- 7. Configure HA on the primary Cisco ASA
- 8. Configure HA on the resilient Cisco ASA
- 9. Configure the outside switch
- 10. Configure primary Internet routing
- 11. Configure resilient Internet routing

If you are using an integrated deployment model where RA VPN services reside on the primary set of Internet edge firewalls, this process is not needed, and you can skip to "Configuring the Remote Access VPN." If you are using standalone RA VPN devices, then continue with this process.

#### Procedure 1

**Configure the LAN distribution switch** 

The LAN distribution switch is the path to the organization's internal network. A unique VLAN supports the Internet edge devices, and the routing protocol peers with the appliances across this network.

#### **Reader Tip**

This procedure assumes that the distribution switch has already been configured following the guidance in the Cisco SBA-Borderless Networks LAN Deployment Guide. Only the procedures required to support the integration of the firewall into the deployment are included in this guide.

Step 1: Configure the interfaces that are connected to the RA VPN-specific firewalls.

```
interface GigabitEthernet1/0/23
description VPN-ASA5525a Gig0/0
interface GigabitEthernet2/0/23
description VPN-ASA5525b Gig0/0
interface range GigabitEthernet1/0/23, GigabitEthernet2/0/23
switchport access vlan 300
switchport host
macro apply EgressQoS
logging event link-status
no shutdown
```

#### Procedure 2

**Apply Cisco ASA initial configuration** 

This procedure configures connectivity to the appliance from the internal network in order to enable management access.

Step 1: Configure the appliance host name.

hostname VPN-ASA5525

Step 2: Configure the appliance interface that is connected to the internal LAN distribution switch as a subinterface on VLAN 300. The interface is configured as a VLAN trunk port to allow flexibility to add additional connectivity.

interface GigabitEthernet0/0 no shutdown 1 interface GigabitEthernet0/0 nameif inside ip address 10.4.24.24 255.255.255.224 standby 10.4.24.23

Step 3: Disable the dedicated management interface.

interface Management0/0 no ip address shutdown

Step 4: Configure an administrative username and password.

username **admin** password [password] privilege 15



**Tech Tip** 

All passwords in this document are examples and should not be used in production configurations. Follow your company's policy, or if no policy exists, create a password using a minimum of 8 characters with a combination of uppercase, lowercase, and numbers.

#### **Procedure 3**

**Configure internal routing** 

A dynamic routing protocol is used to easily configure reachability between networks connected to the appliance and those that are internal to the organization. Because the RA VPN ASA device is not the default route for the inside network to get to the Internet, a distribute list must be used to filter out the default route from EIGRP updates to other devices.

**Step 1:** Create an access list to block default routes in updates.

access-list ALL\_BUT\_DEFAULT standard deny host 0.0.0.0 access-list ALL\_BUT\_DEFAULT standard permit any

**Step 2:** Enable Enhanced Interior Gateway Routing Protocol (EIGRP) on the appliance.

router eigrp 100

**Step 3:** Configure the appliance to advertise its statically defined routes including RA VPN clients but not default routes and connected networks that are inside the Internet edge network range.

no auto-summary network **10.4.0.0 255.254.0.0** redistribute static distribute-list **ALL\_BUT\_DEFAULT** out

**Step 4:** Configure EIGRP to peer with neighbors across the inside interface only.

passive-interface default

no passive-interface inside

**Step 5:** Summarize the remote access host routes in order to keep routing tables small.

interface GigabitEthernet0/0

summary-address eigrp 100 10.4.28.0 255.255.252.0 5

**Procedure 4** 

**Configure user authentication** 

#### (Optional)

As networks scale in the number of devices to maintain, it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization, and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root cause analysis. When AAA is enabled for access control, all management access to the network infrastructure devices (SSH and HTTPS) is controlled by AAA.



#### **Reader Tip**

The AAA server used in this architecture is the Cisco Secure ACS. Configuration of Cisco Secure ACS is discussed in the *Cisco SBA—Borderless Networks Device Management Using ACS Deployment Guide.* 

TACACS+ is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database was defined already to provide a fallback authentication source in case the centralized TACACS+ server is unavailable.

Step 1: Configure the TACACS+ server.

```
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (inside) host 10.4.48.15 SecretKey
```

**Step 2:** Configure the appliance's management authentication to use the TACACS+ server first and then the local user database if the TACACS+ server is unavailable.

- 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

**Step 3:** Configure the appliance to use AAA to authorize management users.

aaa authorization exec authentication-server

### Tech Tip

User authorization on the Cisco ASA firewall does not automatically present the user with the enable prompt if they have a privilege level of 15, unlike Cisco IOS devices.

#### Procedure 5

**Configure time synchronization and logging** 

Logging and monitoring are critical aspects of network security devices in order to support troubleshooting and policy-compliance auditing.

The Network Time Protocol (NTP) is designed to synchronize time across a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network.

Network devices should be programmed to synchronize to a local NTP server in the network. The local NTP server typically references a more accurate clock feed from an outside source.

There is a range of detail that can be logged on the appliance. Informationallevel logging provides the ideal balance between detail and log-message volume. Lower log levels produce fewer messages, but they do not produce enough detail to effectively audit network activity. Higher log levels produce a larger volume of messages but do not add sufficient value to justify the number of messages logged.

Step 1: Configure the NTP server.

ntp server 10.4.48.17

Step 2: Configure the time zone.

clock timezone PST -8
clock summer-time PDT recurring

Step 3: Configure which logs to store on the appliance.

logging enable
logging buffered informational

#### Procedure 6

**Configure device-management protocols** 

Cisco ASDM requires that the appliance's HTTPS server be available. Be sure that the configuration includes networks where administrative staff has access to the device through Cisco ASDM; the appliance can offer controlled Cisco ASDM access for a single address or management subnet (in this case, 10.4.48.0/24). HTTPS and Secure Shell (SSH) Protocol are more secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

Use SSH and HTTPS protocols in order to more securely manage the device. Both protocols are encrypted for privacy, and the non-secure protocols, Telnet and HTTP, are turned off.

Simple Network Management Protocol (SNMP) is enabled to allow the network infrastructure devices to be managed by a Network Management System (NMS). SNMPv2c is configured for a read-only community string.

**Step 1:** Allow internal administrators to remotely manage the appliance over HTTPS and SSH.

domain-name cisco.local
http server enable
http 10.4.48.0 255.255.255.0 inside
ssh 10.4.48.0 255.255.255.0 inside
ssh version 2

Step 2: Configure the appliance to allow SNMP polling from the NMS.

snmp-server host inside 10.4.48.35 community cisco
snmp-server community cisco

Procedure 7

**Configure HA on the primary Cisco ASA** 

This procedure describes how to configure active/standby failover for the primary RA VPN Cisco ASA. The failover key value must match on both devices in an active/standby pair. This key is used for two purposes: to authenticate the two devices to each other, and to secure state synchronization messages between the devices, which enables the Cisco ASA pair to maintain service for existing connections in the event of a failover.

Step 1: On the primary appliance, enable failover.

failover

**Step 2:** Configure the appliance as the primary appliance of the high availability pair.

failover lan unit primary

Step 3: Configure the failover interface.

failover lan interface failover GigabitEthernet0/2
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2

**Step 4:** Tune the failover poll timers. This minimizes the downtime experienced during a failover.

failover polltime unit msec 200 holdtime msec 800 failover polltime interface msec 500 holdtime 5

Step 5: Configure the failover interface IP address.

failover interface ip failover 10.4.24.97 255.255.258.248 standby 10.4.24.98

Step 6: Enable the failover interface.

interface GigabitEthernet0/2
no shutdown

**Step 7:** Configure the standby IP address and monitoring of the inside interface.

interface GigabitEthernet0/0

ip address 10.4.24.24 255.255.255.224 standby 10.4.24.23
monitor-interface inside

Procedure 8

**Configure HA on the resilient Cisco ASA** 

Step 1: On the secondary Cisco ASA, enable failover.

failover

**Step 2:** Configure the appliance as the secondary appliance of the high availability pair.

failover lan unit secondary

Step 3: Configure the failover interface.

failover lan interface failover GigabitEthernet0/2
failover key FailoverKey
failover replication http
failover link failover GigabitEthernet0/2

**Step 4:** Tune the failover poll timers. This minimizes the downtime experienced during a failover.

failover polltime unit msec 200 holdtime msec 800 failover polltime interface msec 500 holdtime 5

Step 5: Configure the failover interface IP address.

failover interface ip failover 10.4.24.97 255.255.258.248 standby 10.4.24.98

Step 6: Enable the failover interface. interface GigabitEthernet0/2 no shutdown

**Step 7:** To verify standby synchronization between the Cisco ASA devices, on the command-line interface of the primary appliance, issue the **show failover state** command.

#### IE-ASA5540# show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Standby Ready	None	

====Configuration State=== Sync Done ====Communication State=== Mac set

#### Procedure 9

#### **Configure the outside switch**

In this procedure, we configure the outside switch connection of the RA VPN Cisco ASA firewall. For this deployment, we are assuming a Dual ISP design. We also assume the outside switch is already configured with a base install and that the only changes required are to allow the RA VPN devices to connect. If this is not the case, please follow the steps in the *Cisco SBA— Borderless Networks Firewall and IPS Configuration Files Guide*, starting at the "Configuring the Firewall Internet Edge" process.

Step 1: Configure the interfaces that connect to the appliances.

```
interface GigabitEthernet1/0/20
description VPN-ASA5525a Gig0/3
!
interface GigabitEthernet2/0/20
description VPN-ASA5525b Gig0/3
!
interface range GigabitEthernet1/0/20, GigabitEthernet2/0/20
switchport trunk allowed vlan 16,17
switchport mode trunk
spanning-tree portfast trunk
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

#### Procedure 10

**Configure primary Internet routing** 

In this procedure, we configure the outside interface of the RA VPN Cisco ASA firewall. For this deployment, we are assuming a Dual ISP design. If this is not the case, please follow the steps in the *Cisco SBA—Borderless Networks Firewall and IPS Configuration Files Guide*, starting at the "Configuring the Firewall Internet Edge" process.

**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://ie-asa5525.cisco.local/)

**Step 2:** In Configuration > Device Setup > Interfaces, click the interface that is connected to the outside switch. (Example: GigabitEthernet0/3)

Step 3: Click Edit.

**Step 4:** In the Edit Interface dialog box, select **Enable Interface**, and then click **OK**.

Step 5: On the Interface pane, click Add > Interface.

**Step 6:** In the Add Interface dialog box, in the Hardware Port list, select the interface enabled in Step 4. (Example: GigabitEthernet0/3)

**Step 7:** In the VLAN ID box, enter the VLAN number for the primary Internet VLAN. (Example: 16)

**Step 8:** In the Subinterface ID box, enter the VLAN number for the primary Internet VLAN. (Example: 16)

Step 9: Enter an Interface Name. (Example: outside-16)

Step 10: In the Security Level box, enter a value of 0.

Step 11: Enter the interface IP Address. (Example: 172.16.130.122)

**Step 12:** Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

🖬 Add Interface	×
General Advanced IPv6	
Hardware Port: GigabitEthernet0/0 v VLAN ID: 16	
Subinterface ID: 16	
Interface Name: outside-16	
Security Level: 0	
Dedicate this interface to management only	
Channel Group:	
✓ Enable Interface	
IP Address      Obtain Address via DHCP O Use PPPoE	
IP Address:     172. 16. 130. 122       Subnet Mask:     255. 255. 255. 0	
Description:	
OK Cancel Help	

Step 13: On the Interface pane, click Apply.

**Step 14:** Navigate to Configuration > Device Management > High Availability > Failover.

**Step 15:** On the Interfaces tab, in the Standby IP Address column, enter the IP address of the standby unit for the interface you just created. (Example: 172.16.130.121)

#### Step 16: Select Monitored, and then click Apply.

figuration > Device Mai	nagement > H	ligh Availability > Fai	<u>lover</u>			
tup Interfaces Criteria	MAC Addresses					
efine interface standby IP a . Press the Tab or Enter key			-click on a standby a	ddress or click on a mon	itoring checkbox t	o edit
	-					
Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored	
GigabitEthernet0/0	inside	🖳 10.4.24.24	255.255.255.224	🖳 10.4.24.23	<b>V</b>	
GigabitEthernet0/3.16	outside-16	🖳 172.16.130.122	255.255.255.0	🖳 172.16.130.121	<b>V</b>	
GigabitEthernet0/3.17	outside-17	🖳 172.17.130.122	255.255.255.0	🖳 172.17.130.121	<b>V</b>	
		Apply	Reset			
		Appry	Keset			

Next, you create the default route to the primary Internet CPE's address.

**Step 17:** In Configuration > Device Setup > Routing > Static Routes, click **Add**.

**Step 18:** In the Add Static Route dialog box, in the Interface list, chose the interface created in Step 9. (Example: outside-16)

Step 19: In the Network box, enter 0.0.0.0/0.0.0.0.

**Step 20:** In the Gateway IP box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)

🔄 Add Static Route	🖾 Add Static Route							
IP Address Type: () IPv4 () IPv6								
Interface:	Interface: outside-16 👻							
Network:	0.0.0.0/0.0.0.0							
Gateway IP:	172.16.130.126 Metric: 1							
Options								
None	None							
Tunneled (Def	<ul> <li>Tunneled (Default tunnel gateway for VPN traffic)</li> </ul>							
Tracked								
Track ID:	Track IP Address:							
SLA ID:	Target Interface: inside 🚽							
Monitoring C	Options							
	icked option starts a job for monitoring the ite, by pinging the track address provided.							
ОК	Cancel Help							

Step 21: On the Static Routes pane, click Apply.



Now you configure the resilient Internet connection.

Step 1: Navigate to Configuration > Device Setup > Interfaces.

Step 2: On the Interface pane, click Add > Interface.

**Step 3:** In the Add Interface dialog box, in the **Hardware Port** list, choose the interface enabled in Step 4 above. (Example: GigabitEthernet0/3)

**Step 4:** In the VLAN ID box, enter the VLAN number for the resilient Internet VLAN. (Example: 17)

**Step 5:** In the Subinterface ID box, enter the VLAN number for the resilient Internet VLAN. (Example: 17)

**Step 6:** Enter an **Interface Name**. (Example: outside-17)

Step 7: In the Security Level box, enter a value of 0.

Step 8: Enter the interface IP Address. (Example: 172.17.130.122)

**Step 9:** Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

Step 10: On the Interface pane, click Apply.

Add Interface	x
General Advanced IPv6	
Hardware Port: GgabitEthernet0/0  VLAN ID: 17 Subinterface ID: 17 Interface Name: outside-17 Security Level: 0 Dedicate this interface to management only Channel Group: P Address P Address	
Use Static IP     Obtain Address via DHCP     Use PPPoE	
IP Address: 172.17.130.122 Subnet Mask: 255.255.255.0 •	
OK Cancel Hep	

**Step 11:** Navigate to Configuration > Device Management > High Availability > Failover.

**Step 12:** On the Interfaces tab, in the Standby IP Address column, enter the IP address of the standby unit for the interface you just created. (Example: 172.17.130.121)

#### Step 13: Select Monitored, and then click Apply.

Interface         Criteria         MAC Addresses           Define Interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.           Interface Name         Name         Active IP Address         Subnet Mask/ Prefix Length         Standby IP Address         Monitored           - GoablitEthemeti0.0         Inside         # 10.4.24.24         25.52.55.25.25.25         # 10.4.24.23         (v)					• <u>Failover</u>	> High Availability >	nagement :	nfiguration > Device Ma
editing an address. Interface Name Name Active IP Address Subnet Mask/ Prefix Length Standby IP Address Monitored						ses	MAC Addres	tup Interfaces Criteria
Interface Name Name Active IP Address Prefix Length Standby IP Address Monitored		reckbox to edit it. Press the Tab or Enter key after	a monitoring ch	by address or click on a	uble-click on a stand	d monitoring status. Do	addresses an	
Interface Name Name Active IP Address Prefix Length Standby IP Address Monitored	_							
- GigabitEthernet0/0 inside 🚇 10.4.24.24 255.255.225 🚇 10.4.24.23			Monitored	Standby IP Address		Active IP Address	Name	Interface Name
			<b>V</b>	🖳 10.4.24.23	255.255.255.224	4, 10.4.24.24	inside	GigabitEthernet0/0
-GigabitEthernet0/3.16 outside-16 🚇 172.16.130.122 255.255.0 🚇 172.16.130.121			<b>V</b>	🖳 172.16.130.121	255.255.255.0	🖳 172.16.130.122	outside-16	GigabitEthernet0/3.16
GigabilEthernet0/3.17 outside-17 😫 172.17.130.122 255.255.0 😫 172.17.130.121 🔽				🖳 172.17.130.121	255.255.255.0	🖳 172.17.130.122	outside-17	GigabitEthernet0/3.17

Next, you edit the default route to the primary Internet CPE's address.

**Step 14:** Navigate to Configuration > Device Setup > Routing > Static Routes.

Step 15: Select the default route to the Internet, and click Edit.

**Step 16:** In the Edit Static Route dialog box, in the Options pane, select **Tracked**.

Step 17: In the Track ID box, enter 1.

**Step 18:** In the Track IP Address box, enter an IP address in the ISP's cloud. (Example: 172.18.1.1)

Step 19: In the SLA ID box, enter 16.

**Step 20:** In the Target Interface list, select the primary Internet connection interface, and then click **OK**. (Example: outside-16)

🔂 Edit Static Route	<b>•••</b>							
IP Address Type:  IPv4 IPv6								
Interface:	Interface: outside-16 🗸							
Network:	any							
Gateway IP:	172.16.130.126 Metric: 128							
Options								
None								
Tunneled (Det	— Tunneled (Default tunnel gateway for VPN traffic)							
Tracked								
Track ID: 1	Track IP Address: 172.18.1.1							
SLA ID: 16	Target Interface: outside-16 👻							
Monitoring C	Monitoring Options							
	cked option starts a job for monitoring the ite, by pinging the track address provided.							
OK	Cancel Help							

#### Process



Configuring the Remote-Access VPN

- 1. Configure remote access
- 2. Create the AAA server group
- 3. Define the VPN address pool
- 4. Configure remote access routing
- 5. Configure the group-URL
- 6. Configure resilient Internet connection
- 7. Configure the partner policy
- 8. Configure the admin policy
- 9. Configure Cisco AnyConnect Client Profile

The majority of the VPN configuration tasks are addressed in the Cisco AnyConnect VPN Connection Setup Wizard. Depending on requirements, additional work might need to be completed after the wizard.

#### Procedure 1

**Configure remote access** 

Step 1: Navigate to Wizards > VPN Wizards > AnyConnect VPN Wizard.

**Step 2:** In the AnyConnect VPN Connection Setup Wizard dialog box, click **Next**.

Step 3: Enter a Connection Profile Name. (Example: AnyConnect)

Step 4: In the VPN Access Interface list, select the primary Internet connection, and then click Next. (Example: outside-16)

Steps	Connection Profile Identifi	cation	
1. Introduction	This step allows you to co	nfigure a Connection Profile Name and the Interface the rer	note access users will access for VPM
2. Connection Profile Identification	connections.		
3. VPN Protocols	Connection Profile Name:	AnyConnect	
4. Client Images	VPN Access Interface:	outside-16	
5. Authentication Methods	With Access interface.		
6. Client Address Assignment			
<ol> <li>Network Name Resolution Servers</li> </ol>			
8. NAT Exempt			
<ol> <li>AnyConnect Client Deployment</li> </ol>			
10. Summary			

Generate a self-signed identity certificate and install it on the appliance.



Step 5: In the Device Certificate pane, click Manage.

Step 6: In the Manage Identity Certificates dialog box, click Add.

Step 7: On the Add Identity Certificate dialog box, select Add a new identity certificate.



Step 8: For Key Pair, select New.

**Step 9:** In the Add Key Pair dialog box, select **Enter new key pair name**, and then in the box, enter a name. (Example: sslpair)

Step 10: Click Generate Now.

🔁 Add Ko	ey Pair
Name:	<ul> <li>Use default key pair name</li> </ul>
	Enter new key pair name: sslpair
Size:	1024 🔹
Usage:	General purpose     Special
6	ienerate Now Cancel Help

**Step 11:** In the Add Identity Certificate dialog box, in **Certificate Subject DN**, enter the fully qualified domain name used to access the appliance on the outside interface. (Example: CN=IE-ASA5545.cisco.local)

Step 12: Select Generate self-signed certificate and Act as Local certificate authority and issue dynamic certificates to TLS-Proxy, and then click Add Certificate.

🔁 Add Identity Certificate	×
Trustpoint Name:	ASDM_TrustPoint0
Import the identity certified	ficate from a file (PKCS12 format with Certificate(s)+Private Key):
Decryption Passphrase:	
File to Import From:	Browse
Add a new identity certified	ficate:
Key Pair:	sslpair    Show  New
Certificate Subject DN:	CN=IE-ASA5545.cisco.local Select
🔽 Generate self-signed	l certificate
🔽 Act as local certi	ficate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Certif	icate Cancel Help

**Step 13:** The Enrollment Status dialog box shows that the enrollment succeeded. Click **OK**.

Step 14: In the Manage Identity Certificates dialog box, click OK.

**Step 15:** On the VPN Protocols page, clear **IPsec**, verify that the certificate you created is reflected in the Device Certificate field, and then click **Next**.

Steps	VPN Protocols
Introduction     Introduction     Connection Profile     Identification     VPI Protocols     VPI Protocols     Clent timages     Authentication Methods     Clent Address Assignment     Network Name Resolution     Servers     NAT Exempt     AnyConnect Clent     Deployment     Summary	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protoc you would like this connection profile to support. SSL Device Certificate Device Certificate Device Certificate dentifies the ASA to the remote access dents. Certain AnyConnect features (Always-On, IPsec/IXEx2) require that valid device certificate be available on the ASA. Device Certificate: [ASDM_TrustPoint0:hostname=IE-ASA5540.disco.local,  Manage
	< Back Next > Cancel Help

Step 16: On the Client Images page, click Add.

Step 17: In the Add AnyConnect Client Image dialog box, click Browse Flash.

**Step 18:** In the Browse Flash dialog box, select the appropriate AnyConnect client image to support your user community, and then click **OK**.

😼 Browse Flash				×
Folders	Files			
⊟ <mark>⊘ disk0:</mark>	FileName	Size (bytes)	Date Modified	
	🗀 coredumpinfo		12/31/02 16:04:02	
	crypto_archive		12/31/02 16:04:00	
🕀 🛄 sdesktop	🗀 log		12/31/02 16:03:46	
🗄 ·· 🛄 tmp	🔁 sdesktop		11/20/10 19:42:04	
	🛄 tmp		08/11/11 13:31:26	
	anyconnect-linux-3.0.3	8,937,241	08/16/11 14:16:56	
	anyconnect-linux-64-3	6,893,306	08/16/11 14:16:40	
	anyconnect-macosx-i3	7,890,341	08/16/11 14:16:16	Ξ
	anyconnect-win-3.0.30	22,824,805	08/16/11 14:16:02	

#### **Tech Tip**

If your Cisco ASA does not already have AnyConnect Client images loaded in the flash disk, you can use the **Upload** button in the Add AnyConnect Client Image dialog box to install new or updated client images into the flash disk of the appliance.

Step 19: In the Add AnyConnect Client Image dialog box, click OK.

**Step 20:** Repeat Step 17 through Step 19 for all the required Cisco AnyConnect client images.

#### Step 21: On the Client Images page, click Next.

AnyConnect VPN Connection	n Setup Wizard	<b>X</b>
Steps	Client Images	
1. Introduction	ASA can automatically upload the latest AnyConnect package	ge to the client device when it accesses the enterprise network.
2. Connection Profile Identification	A regular expression can be used to match the user-agent of You can also minimize connection setup time by moving the i	
3. VPN Protocols	system to the top of the list.	
4. Client Images	💠 Add 📝 Replace 前 Delete 🕈 🗲	
5. Authentication Methods		
6. Client Address Assignment	Image	Regular expression to match user-agent
7. Network Name Resolution	disk0:/anyconnect-linux-3.0.07059-k9.pkg	
Servers	disk0:/anyconnect-macosx-i386-3.0.07059-k9.pkg	
8. NAT Exempt	disk0:/anyconnect-win-3.0.07059-k9.pkg	
<ol> <li>AnyConnect Client Deployment</li> </ol>		
10. Summary		
	You can download AnyConnect Client packages from Cisco	by searching 'AnyConnect VPN Client' or <u>dick here</u> .
	<back next=""></back>	Cancel Help

Remaining in the wizard, you now create a new AAA server group to authenticate remote-access users. To authenticated users, the server group uses either NTLM to the Active Directory server or RADIUS to the Cisco Secure ACS server.

#### **Procedure 2**

#### **Create the AAA server group**

For VPN user authentication, you point Cisco ASA to either the Cisco Secure ACS you configured earlier or to the organization's Active Directory server.

If the authentication process authenticates directly to Active Directory, complete Option 1 of this procedure. If the authentication process uses Cisco Secure ACS, complete Option 2 of this procedure.

#### **Option 1. Use Active Directory for AAA**

Step 1: On the Authentication Methods page, next to AAA Server Group, click New.

**Step 2:** In the New Authentication Server Group dialog box, enter the following values, and then click **OK**:

- Server Group Name: AD
- Authentication Protocol—NT
- · Server IP Address-10.4.48.10
- Interface-inside
- NT Domain Controller Name—AD-1

📴 New Authentication Server Group		×
To add more servers to the group o	r group containing one authentication server. or change other AAA server settings, go to nt > Users/AAA > AAA Server Groups.	
Server Group Name:	AD	
Authentication Protocol:	NT •	
Server IP Address:	10.4.48.10	
Interface:	[inside -	
NT Domain Controller Name:	AD-1	
OK	Cancel Help	

#### Step 3: On the Authentication Methods page, click Next.

Steps	Authentication Methods
Introduction     Connection Profile     Identification     VPN Protocols     VPN Protocols     Client Images     Authentication     Hethods     Client Address Assignment     Network Name Resolution     Servers     NAT Exempt     AnyConnect Client     Deployment     Summary	This step lets you specify the location of the authentication server. You can click on the "New" button to create a new server group. AAA Server Group: AD  New AAA Server Group Details AAA Server Group Details AAA Carrier Composition of the authentication server. Server Name or IP Address Interface Timeout 10.4.48,10 reside 5
	< Back Next > Cancel Help

#### Option 2. Use Cisco Secure ACS for AAA

Step 1: On the Authentication Methods page, next to AAA Server Group, click New.

**Step 2:** In the New Authentication Server Group dialog box, enter the following values, and then click **OK**:

- Server Group Name—AAA-RADIUS
- Authentication Protocol—RADIUS
- Server IP Address—10.4.48.15 (IP address of the Cisco Secure ACS server)
- Interface—inside
- Server Secret Key—SecretKey
- Confirm Server Secret Key—SecretKey

New Authentication Server Gro	up	
To add more servers to the gro	erver group containing one authentication server. up or change other AAA server settings, go to ement > Users/AAA > AAA Server Groups.	
Server Group Name:	AAA-RADIUS	
Authentication Protocol:	RADIUS	
Server IP Address:	10.4.48.15	
Interface:	inside 🔹	
Server Secret Key:	•••••	
Confirm Server Secret Key:	•••••	
ОК	Cancel Help	

Step 3: On the Authentication Methods page, click Next.



Next, you define the remote-access VPN address pool that will be assigned to users when they connect to the VPN service.



**Define the VPN address pool** 

You need to decide on an appropriate address space for your RA VPN address pool. In this example you use 4 class-C address ranges (~1000 addresses) as the pool.

**Step 1:** On the Client Address Assignment page, in the IPv4 Address Pool tab, click **New**.

**Step 2:** In the Add IP Pool dialog box, enter the following values, and then click **OK**:

- · Name-RA-pool
- Starting IP Address—10.4.28.1
- Ending IP Address—10.4.31.254
- · Subnet Mask-255.255.252.0

뒄 Add IP Pool	
Name:	RA-pool
Starting IP Address:	10.4.28.1
Ending IP Address:	10.4.31.254
Subnet Mask:	255.255.252.0
ОК	Cancel Help

**Step 3:** On the Client Address Assignment page, verify that the pool you just created is selected, and then click **Next**.

Steps       Client Address Assignment         1. Introduction       This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect client will be assigned addresses from the pools when they connect.         3. VPN Protocols       IPv6 address pool is only supported for SSL connection.         4. Client Images       IPv6 Address Pool         5. Authentication Methods       IPv6 Address Pool         6. Client Address       IPv6 Address pool         7. Network Name Resolution Servers       Starting IP Address: 10.4.31.255         8. NAT Exempt       Subnet Mask:         9. AnyConnect Client Deployment       Subnet Mask:         10. Summary       Subnet Mask:
2. Connection Profile Identification       clents will be assigned addresses from the pools when they connect.         1. VPN Protocols       IPv6 address pool is only supported for SSL connection.         3. VPN Protocols       IP v4 Address Pool         4. Clent Images       IP v4 Address Pool         5. Authentication Methods       Address Pool         6. Chent Address Assignment       Details of the selected address pool Servers         7. Network Name Resolution Servers       Ending IP Address:         9. AnyConnect Client Deployment       Subnet Mask:

**Step 4:** On the Network Name Resolution Servers page, enter the organization's **DNS Servers** (Example: 10.4.48.10) and the organization's **Domain Name** (Example: cisco.local), and then click **Next**.

AnyConnect VPN Connection	Setup Wizard 🗾	3
Steps	Network Name Resolution Servers	
1. Introduction	This step lets you specify how domain names are resolved for the remote user when accessing the internal network.	
2. Connection Profile Identification	DNS Servers: 10.4.48.10	
3. VPN Protocols	WINS Servers:	
4. Client Images	Domain Name: cisco.local	
5. Authentication Methods		
6. Client Address Assignment		
7. Network Name Resolution Servers		
8. NAT Exempt		
<ol> <li>AnyConnect Client Deployment</li> </ol>		
10. Summary		
		-
	< Back Next > Cancel Help	

If you are using RA VPN integrated with Cisco ASA Series firewalls, NAT exemption must be configured for traffic from the LAN that is going to the remote-access clients. If this were not configured, traffic to clients would be translated, changing the source address of the traffic and making it impossible for clients to receive traffic correctly from servers with which they communicate.

Step 5: If you are implementing a standalone VPN design, skip to Step 8.

If you are implementing an integrated VPN design, in the wizard, on the NAT Exempt page, select **Exempt VPN traffic from network address translation**.

Step 6: In the Inside Interface list, select inside.

Step 7: In the Local Network box, enter any, and then click Next.

AnyConnect VPN Connection	n Setup Wizard	×
Steps I. Introduction 2. Connecton Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignment 7. Network Name Resolution Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	NAT Exempt If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.          If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.         If deal Interface is the interface directly connected to your internal network.         Inde Interface:         Inde Interface:         Local Network is the network address(ee) of the internal network that dent can access.         Local Network:       mry         The traffic between AnyConnect dent and Internal network will be exempt from network address translation.	
	< Back Next > Cancel Hep	,

Step 8: On the AnyConnect Client Deployment page, click Next.

Step 9: On the Summary page, click Finish.

Finally, you must upload the Cisco AnyConnect client images to the secondary appliance.

**Step 10:** On the secondary appliance, copy the following Cisco AnyConnect client images to the local flash disk.

Etp://10.4.4	18.27/anyconnect-	win-3.0.	07059-k9.pkg	disk0:
--------------	-------------------	----------	--------------	--------

ftp://10.4.48.27/anyconnect-macosx-i386-3.0.07059-k9.pkg

disk0:

ftp://10.4.48.27/anyconnect-linux-3.0.07059-k9.pkg disk0:

#### Procedure 4

#### **Configure remote access routing**

Traffic from remote-access VPN clients to and from the Internet must be inspected by the organization's firewall, IPS, and policy controls such as Cisco IronPort Web Security Appliance. To accomplish this, all traffic to and from the VPN clients must be routed toward the LAN distribution switch, regardless of the traffic's destination, so that the Cisco ASA policy engine has the visibility to handle the traffic correctly.

Step 1: In Configuration > Device Setup > Routing > Static Routes, click Add.

**Step 2:** In the Add Static Route dialog box, configure the following values, and then click **OK**.

- · Interface-inside
- Network—any
- · Gateway IP-10.4.24.1
- Options—Tunneled (Default tunnel gateway for VPN traffic)

🔂 Add Static Route	: 🔓 🗾
IP Address Type:	IPv4
Interface:	inside 🔹
Network:	any
Gateway IP:	10.4.24.1 Metric: 255
Options	
None	
Tunneled (Details)	fault tunnel gateway for VPN traffic)
Tracked	
Track ID:	Track IP Address;
SLA ID:	Target Interface: inside 👻
Monitoring C	Options
	acked option starts a job for monitoring the ite, by pinging the track address provided.
ОК	Cancel Help

#### Step 3: Verify the configuration, and then click Apply.

Configuration	n > Device Se	tup > Routin <mark>q</mark> >	<u>Static Routes</u>			
Specify station		nly 🔘 IPv6 only				
Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options	Add
inside	0.0.0.0	0.0.0.0	10.4.24.1	255	Tunneled	Euit
outside-16	0.0.0.0	0.0.0.0	172.16.130.126	128	Tracked ID - 1 Address - 172.18.1.1 Interface - outside-16	Delete
			Apply	Reset		

Cisco ASA advertises the each connected user to the rest of the network as individual host routes. Summarizing the address-pool reduces the IP route table size for easier troubleshooting and faster recovery from failures.

**Step 4:** In Configuration > Device Setup > Routing > EIGRP > Summary Address, click **Add**.

**Step 5:** In the Add EIGRP Summary Address Entry dialog box, configure the following values, and then click **OK**.

- EIGRP AS—100
- Interface—GigabitEthernet0/0
- IP Address—10.4.28.0 (Enter the remote-access pool's summary network address.)
- Netmask—255.255.252.0
- Administrative Distance—5

付 Add EIGRP Summary	Address Entry		×
EIGRP AS:	100 👻	Interface: GigabitEth	ernet0/0 👻
IP Address:	10.4.28.0	Netmask: 255.255.2	252.0 🗸
Adminstrative Distance:	5	(default 5)	
	OK Cancel	Help	

#### Step 6: On the Summary Address pane, click Apply.

Next, you allow intra-interface traffic. This is critical in allowing VPN users (specifically remote workers with Cisco Unified Communications software clients) to communicate with each other.

Step 7: Navigate to Configuration > Device Setup > Interfaces.

Step 8: Select Enable traffic between two or more hosts connected to the same interface, and then click Apply.

nterface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Add 🔻
igabitEthernet0/0	inside	Enabled	100	10.4.24.24	255.255.255.224	native	Edit
igabitEthernet0/1		Disabled				native	Delata
igabitEthernet0/2		Enabled				native	Delete
igabitEthernet0/3		Enabled				native	
igabitEthernet0/3.16	outside-16	Enabled	0	172.16.130.122	255.255.255.0	vlan 16	
igabitEthernet0/3.17	outside-17	Enabled	0	172.17.130.122	255.255.255.0	vlan17	
igabitEthernet0/4		Disabled				native	
igabitEthernet0/5		Disabled				native	
igabitEthernet0/6		Disabled				native	
igabitEthernet0/7		Disabled				native	
anagement0/0		Disabled				native	
III						+	
] Enable traffic between tv			-		levels		
] Enable jumbo frame rese		connected	to the sumer				

#### Procedure 5

Configure the group-URL

The Cisco AnyConnect client's initial connection is typically launched with a web browser. After the client is installed on a user's computer, subsequent connections can be established through the web browser again or directly through the Cisco AnyConnect client, which is now installed on the user's computer. The user needs the IP address or DNS name of the appliance, a username and password, and the name of the VPN group to which they are assigned. Alternatively, the user can directly access the VPN group with the group-url, after which they need to provide their username and password.

If using the Dual ISP design, expect to offer VPN connectivity through both ISP connections, and be sure to provide group-urls for the IP address or host names for both ISPs.

**Step 1:** Navigate to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles.

**Step 2:** In the Connection Profiles pane, select the profile created in the previous procedure (Example: AnyConnect), and then click **Edit**.

**Step 3:** On the Edit AnyConnect Connect Profile dialog box, navigate to Advanced > Group Alias/Group URL.

Step 4: On the Group URLs pane, click Add.

**Step 5:** In the URL box, enter the URL containing the firewall's primary Internet connection IP address and a user group string, and then click **OK**. (Example: https://172.16.130.134/AnyConnect)

🔂 Add	Group URL	×
URL:	https://172.16.130.124/AnyConnect	
	V Enabled	
(	OK Cancel Help	

**Step 6:** If you are using the Dual ISP design, which has a resilient Internet connection, repeat Step 1- Step 5, using the firewall's resilient Internet connection IP address. (Example: https://172.17.130.124/AnyConnect)

If you are using the Single ISP design, advance to the next procedure.

#### Procedure 6

**Configure resilient Internet connection** 

#### (Optional)

**Step 1:** Navigate to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles.

**Step 2:** In the Configuration window, in the Access Interfaces pane, select the interface attached to the resilient Internet connection. (Example: outside-17)

Step 3: Under SSL Access, select Allow Access, and then click Apply.

	and the difference of the		rfaces selected in the tab to be launched from a br				
SL access must be	SSL Access	w AnyConnect client	IPsec (IKEv2) Ac				
interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services		Device Certificate	1
iside	(m)		(m)			Death Cathlana	7
utside-16	<b>V</b>	<b>V</b>			_	Port Settings	
utside-17					~		
→ In Page Setting → I Allow user to se Shutdown porta nection Profiles →	lect connection pro		alias, on the login page.	Otherwise, DefaultWebVPNGro	up will be the	connection profile.	
Allow user to se     Shutdown porta     Shutdown porta     connection profiles	lect connection pro	ofile, identified by its a	alias, on the login page.	Otherwise, DefaultWebVPNGro ameters. You can configure the	up will be the	connection profile.	n profile <u>here</u> ,
Allow user to se     Shutdown porta     Shutdown porta     connection profiles	lect connection pro il login page. (tunnel group) spe	ofile, identified by its a cifies how user is auth	alias, on the login page.	Otherwise, DefaultWebVPNGro ameters. You can configure the	up will be the	connection profile.	n profile <u>bars</u> , Group Policy
Page Setting  Page Setting  Page Setting  Page Setting  Shutdown portation profiles  onnection profile  Add  G Edit	lect connection pro il login page. (tunnel group) spe Tolete End	ofile, identified by its a cifies how user is auth	alias, on the login page. nenticated and other par	Otherwise, DefaultWebVPNGro ameters. You can configure the	up will be the	connection profile. m certificate to connectio ication Method	
Page Setting — Alow user to se Shutdown porta Shutdown porta Shutdown porta Connection Profiles — Onnection profile Add C Edit Iame	lect connection pro- il login page. (turnel group) spe Delete End SSL Enable	ofile, identified by its a cifies how user is auth	alias, on the login page. nenticated and other par C C Match C	Otherwise, DefaultWebVPNGro ameters. You can configure the	up will be the mapping fro Authent	connection profile. m certificate to connectio ication Method :AL)	Group Policy



**Step 1:** In Configuration > Remote Access VPN > Network (Client) Access > Group Policies, click **Add**.

**Step 2:** On the Add Internal Group Policy dialog box, enter a **Name**. (Example: GroupPolicy\_Partner)

General	Name:	GroupPolicy_	Partner	
Servers Advanced	Banner:	📄 Inherit	Your access is restircted to the partner server	
	SCEP forwarding URL:	🔽 Inherit		
	Address Pools:	🔽 Inherit		Select.
	IPv6 Address Pools:	🔽 Inherit		Select.
	More Options			
	Prore Options			
	Piore options			
	Piore Options			
	Piore options			
	Prore options			

Step 3: Click the two down arrows. The More Options pane expands.

Step 4: For IPv4 Filter, clear Inherit, and then click Manage.

Step 5: On the ACL Manager dialog box, click Add > Add ACL.

**Step 6:** In the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example RA\_PartnerACL)

🔁 Add ACL
ACL Name: RA_PartnerACL
OK Cancel Help

Step 7: Click Add > Add ACE.

Step 8: In the Add ACE dialog box, for Action, select Permit.

**Step 9:** In the Address box, enter the IP address and netmask that the partner is allowed to access, and then click **OK**. (Example: 10.4.48.35/32)

CE	×
Permit O Deny	
10.4.48.35/32	
	Permit      Deny

Step 10: In the ACL Manager dialog box, click OK.

	ACL Extended ACL	🕺 🖻 🛍	*
No	Address	Action	Description
E RA_Pa	artnerACL		
1	10.4.48.35	🖌 Permit	Partners can access this internal host only

Step 11: In the Add Internal Group Policy dialog box, click OK.

ral	Name: GroupPolicy_P	Partner	
vers anced	Banner: Inherit	Your access is restircted to the partner server	7
	SCEP forwarding URL: 📝 Inherit		5
	Address Pools: 📝 Inherit		Select
	IPv6 Address Pools: 💟 Inherit		Select
	More Options		(
	Tunneling Protocols:	☑ Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2	L2TP/IPsec
	IPv4 Filter:	Inherit RA_PartnerACL	Manage
	IPv6 Filter:	V Inherit	Manage
	NAC Policy:	V Inherit	Manage
	Access Hours:	Inherit v	Manage
	Simultaneous Logins:	☑ Inherit	
	Restrict access to VLAN:	V Inherit	
	Connection Profile (Tunnel Group) Lo		
	Maximum Connect Time:	Inherit Unlimited minutes	
	Idle Timeout:	V Inherit Unlimited minutes	
	On smart card removal:	☑ Inherit	
:	Next P	Previous	

Step 12: On the Group Policies pane, click Apply.

**Procedure 8** 

**Configure the admin policy** 

**Step 1:** In Configuration > Remote Access VPN > Network (Client) Access > Group Policies, click **Add**.

**Step 2:** On the Add Internal Group Policy dialog box, enter a **Name**. (Example: GroupPolicy\_Administrators)

🔂 Add Internal Group Policy				×
General	Name:	GroupPolicy_	Administrators	
Servers Advanced	Banner:	🔲 Inherit	Your access is via an unrestricted split tunnel.	
	SCEP forwarding URL:	🗸 Inherit		
	Address Pools:	🔽 Inherit		Select
	IPv6 Address Pools:	🔽 Inherit		Select
	More Options			*
Find:		Next 🔘	Previous	
			OK Cancel Help	

Step 3: In the navigation tree, click Advanced > Split Tunneling.

Step 4: For Policy, clear Inherit, and then select Tunnel Network List Below.

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

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

**Step 7:** In the Add ACL dialog box, enter an **ACL Name**, and then click **OK**. (Example RA\_SplitTunnelACL)

🔂 Add ACL 📃	<
ACL Name: RA_SplitTunnelACL	
OK Cancel Help	

Step 8: Click Add > Add ACE.

**Step 10:** In the Address box, enter the internal summary IP address and netmask, and then click **OK**. (Example: 10.4.0.0/255.254.0.0)

🔁 Add A	CE 🔤
Action:	Permit      Deny
Address:	10.4.0.0/255.254.0.0
Descriptio	
Internal r	

Step 11: Click Add > Add ACE.

Step 12: In the Add ACE dialog box, for Action, select Permit.

**Step 13:** In the Address box, enter the DMZ summary IP address and netmask, and then click **OK**. (Example: 192.168.16.0/21)

🔯 Add A	CE	×
Action:	ermit O Deny	
Address:	192.168.16.0/21	
Descriptio	n:	
DMZ netv	vorks	
	OK Cancel Help	

Step 14: In the ACL Manager dialog box, click OK.

	ACL Extended ACL		
🗣 Add	🝷 📝 Edit 🎁 Delete   🕈 🦄	f 🛛 🕺 🖷 💼	h =
No	Address	Action	Description
🗏 RA_P	artnerACL		
1	8, 10.4.48.35	🖌 Permit	Partners can access this internal host only
🗄 RA_S	plitTunnelACL		
1	10.4.0.0/15	🖌 Permit	Internal networks
2	192.168.16.0/21	🖌 Permit	DMZ networks

Step 15: In the Add Internal Group Policy dialog box, click OK.

General Servers			require traffic to go through the tunnel and those that do not require tunneling. The security appliance ork list, which is an ACL that consists of list of addresses on the private network.
Spit Tunneling     Browser Proxy     ⊕-AnyConnect Client	DNS Names: Send All DNS Lookups Through Tunnel:	✓ Inherit	○ Yes ○ No
⊕-IPsec Client	Policy:	Inherit	Turnel Network List Below
	Network List:		RA_SplitTurnelACL Manage
	Intercept DHCP Configuration M	essage from	Hicrosoft Clients 🛞
Find:	Next O Pro	evious	

Step 16: On the Group Policies pane, click Apply.

Procedure 9

**Configure Cisco AnyConnect Client Profile** 

Cisco AnyConnect Client Profile is the location where some of the newer configuration of the Cisco AnyConnect client is defined. Cisco AnyConnect 2.5 and later use the configuration in this section, including many of the newest features added to the Cisco AnyConnect client.

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

**Step 2:** In the Add AnyConnect Client Profile dialog box, in the Profile Name box, enter **ra\_profile**, and then click **OK** and **Apply**.

Add AnyConn	ect Client Profile	×
Profile Name Profile Usage	ra_profile  VPN	
	le path for an xml file, ie. disk0:/ac_profile. The file wil be eated if it does not exist.	
Profile Location	disk0:/ra_profile.xml	Browse Flash
		Upload
Group Policy	<unassigned></unassigned>	
	OK Cancel Hep	

**Step 3:** On the AnyConnect Client Profile pane, select the ra\_profile you just built, and then click **Edit**.

The Server List Panel allows you to enter names and addresses for the appliances to which the Cisco AnyConnect Client is allowed to connect.

#### Step 4: Click Server List > Add.

**Step 5:** In the Server List Entry dialog box, in the Hostname box, enter the name of the remote-access firewall. (Example: IE-ASA5545)

**Step 6:** In the FQDN or IP Address box, enter the firewall's primary Internet connection IP address. (Example: 172.16.130.124)

**Step 7:** In the User Group box, enter the name defined in Step 3. (Example: AnyConnect)

**Step 8:** If you are using the standalone VPN design, in the Host Address box, enter the firewall's resilient Internet connection IP address, and then click **Add**. (Example: 172.17.130.124)

If you are using the integrated VPN design, proceed to the next step.

#### Step 9: Click OK.

Host Display Name (required) IE-ASA5545		Additional mobile-only settings	Edit
FQDN or IP Address	User Group		
172.16.130.124	/ AnyConnect		
Group URL			
172.16.130.124/AnyConnect		<i>v</i> 0	
Backup Server List		Load Balancing Server List	
		"Always On" is disabled. Load Balancing Fi	elds have been disabled.
Host Address	Add	Host Address	Add
172, 17, 130, 124	Move Up		Delete
	Move Down		
	Delete		
Primary Protocol	SSL 🗸	Automatic SCEP Host	
Standard Authentication Only (IOS gateways)		CA URL	
Auth Method During IKE Negotiation	IKE-RSA 👻	Prompt For Challenge Password	
IKE Identity		CA Thumbprint	

**Step 10:** On the AnyConnect Client Profile pane, click **Change Group Policy**.

**Step 11:** In the Change Group Policy for Profile dialog box, in the available group policies list, select the three group policies you just created, click the right arrow, and then click **OK**.

Change Group Policy for Profile ra_profile	e 💌
This panel is used to assign (or unassign) the se Profile Name: ra_profile	elected profile to one or more group policies.
Profile Usage: VPN	Enable 'Always On VPN' for selected group(s)
Available Group Policies DfitGrpPolicy	Selected Group Policies GroupPolicy_Administrators GroupPolicy_AnyConnect GroupPolicy_Partner
OK	Close

Step 12: On the AnyConnect Client Profile pane, click Apply.

## Summary

This deployment guide is a reference design for Cisco customers and partners. It covers the Internet edge component of Borderless Networks and is meant to be used in conjunction with the Cisco SBA—Borderless Networks LAN Deployment Guide in addition to the MPLS WAN Deployment Guide, Layer 2 WAN Deployment Guide, and VPN WAN Deployment Guide, which can be found at http://www.cisco.com/go/sba/

If your network is beyond the scale of this design, please refer to the Cisco Validated Designs (CVD) for larger deployment models. CVDs can be found on Cisco.com. The Cisco products used in this design were tested in a network lab at Cisco. The specific products are listed at the end of this document for your convenience.

### Notes

## Appendix A: Product List

## Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 8.6(1)1, IPS 7.1(4) E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	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
Mobile License	AnyConnect Essentials VPN License - ASA 5545-X (2500	ASA-AC-E-5545	—
	Users)		
	AnyConnect Essentials VPN License - ASA 5525-X (750	ASA-AC-E-5525	
	Users)		
	AnyConnect Essentials VPN License - ASA 5515-X (250	ASA-AC-E-5515	
	Users)		
	AnyConnect Essentials VPN License - ASA 5512-X (250	ASA-AC-E-5512	
	Users)		

## **VPN Client**

Functional Area	Product Description	Part Numbers	Software
VPN Client	Cisco AnyConnect Secure Mobility Client	Cisco AnyConnect Secure Mobility Client	3.0.07059

## **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

## **LAN Distribution Layer**

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1
Virtual Switch Pair	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	IP services
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
Modular Distribution Layer	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG)
Switch	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	Enterprise Services
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(1)SE2
Switch	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	IP Services
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

## Appendix B: Configuration Example

#### **RA VPN ASA-5525-X**

```
ASA Version 8.6(1)1
1
hostname VPN-ASA5525
domain-name cisco.local
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
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
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 Т 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 Т 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 1 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

interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
ftp mode passive
clock timezone PST -8
clock summer-time PDT recurring
dns domain-lookup inside
dns server-group DefaultDNS
name-server 10.4.48.10
domain-name cisco.local
same-security-traffic permit intra-interface
object network NETWORK_OBJ_10.4.28.0_22
subnet 10.4.28.0 255.255.252.0
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 ALL_BUT_DEFAULT standard deny host 0.0.0.0
access-list ALL_BUT_DEFAULT standard permit any
pager lines 24
logging enable
logging buffered informational
logging asdm informational
mtu inside 1500 mtu outside-16 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 10.4.24.97 255.255.255.248 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 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 0.0.0.0 172.16.130.126 128 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 key \*\*\*\*\* 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 \*\*\*\*\* 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 ca trustpoint ASDM TrustPoint0 enrollment self subject-name CN=VPN-ASA5525.cisco.local keypair sslpair proxy-ldc-issuer crl configure crypto ca certificate chain ASDM TrustPoint0 crypto ikev2 remote-access trustpoint ASDM TrustPoint0 1 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 trust-point ASDM TrustPoint0 outside-16 ssl trust-point ASDM TrustPoint0 outside-17 webvpn enable outside-16 enable outside-17 anyconnect-essentials anyconnect image disk0:/anyconnect-linux-3.0.07059-k9.pkg 1 anyconnect image disk0:/anyconnect-macosx-i386-3.0.07059-k9.pkg 2 anyconnect image disk0:/anyconnect-win-3.0.07059-k9.pkg 3 anyconnect profiles ra profile disk0:/ra profile.xml anyconnect profiles web security profile disk0:/web security profile.wsp anyconnect profiles web security profile.wso disk0:/web security profile.wso anyconnect enable tunnel-group-list 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 split-tunnel-policy excludespecified split-tunnel-network-list value Scansafe Tower Exclude default-domain value cisco.local webvpn anyconnect modules value dart, websecurity anyconnect profiles value ra profile type user

```
anyconnect profiles value web security profile.wso type
                                                                           inspect dns preset dns map
                                                                           inspect ftp
websecurity
  always-on-vpn disable
                                                                           inspect h323 h225
group-policy GroupPolicy Administrators internal
                                                                           inspect h323 ras
group-policy GroupPolicy Administrators attributes
                                                                           inspect ip-options
banner value Your acess is via unrestricted split tunnel.
                                                                           inspect netbios
 split-tunnel-policy tunnelall
                                                                           inspect rsh
 split-tunnel-network-list value RA SplitTunnelACL
                                                                           inspect rtsp
 webvpn
                                                                           inspect skinny
  anyconnect profiles value ra profile type user
                                                                           inspect esmtp
group-policy GroupPolicy Partner internal
                                                                           inspect sqlnet
group-policy GroupPolicy Partner attributes
                                                                           inspect sunrpc
banner value Your Access is restricted to the partner server
                                                                           inspect tftp
 vpn-filter value RA PartnerACL
                                                                           inspect sip
webvpn
                                                                           inspect xdmcp
  anyconnect profiles value ra profile type user
                                                                         1
username admin password w2Y.60p4j7clVDk2 encrypted privilege 15
                                                                         service-policy global policy global
tunnel-group AnyConnect type remote-access
                                                                         prompt hostname context
                                                                         no call-home reporting anonymous
tunnel-group AnyConnect general-attributes
 address-pool RA-pool
                                                                         call-home
 authentication-server-group AAA-RADIUS
                                                                          profile CiscoTAC-1
 default-group-policy GroupPolicy AnyConnect
                                                                           no active
tunnel-group AnyConnect webvpn-attributes
                                                                           destination address http https://tools.cisco.com/its/service/
 group-alias AnyConnect enable
                                                                         oddce/services/DDCEService
                                                                           destination address email callhome@cisco.com
 group-url https://172.16.130.122/AnyConnect enable
 group-url https://172.17.130.122/AnyConnect enable
                                                                           destination transport-method http
                                                                           subscribe-to-alert-group diagnostic
class-map inspection default
                                                                           subscribe-to-alert-group environment
match default-inspection-traffic
                                                                           subscribe-to-alert-group inventory periodic monthly 23
                                                                           subscribe-to-alert-group configuration periodic monthly 23
                                                                           subscribe-to-alert-group telemetry periodic daily
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
```

## Appendix C: Changes

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

- We updated Cisco ASA 5500 Adaptive Secure Appliances to model 5525-X or 5545-X.
- We updated the Cisco ASA Software from version 8.4.2 to version 8.6.1.1.
- We added ability to use either Active Directory or Cisco Secure ACS for user authentication.



### 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 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)