ılıılı cısco

**Deployment Guide** 

# Cisco Next Generation Enterprise WAN

# Regional WAN Remote Access VPN Deployment Guide

September, 2011



# Contents

Cisco NGEW Architecture Overview	5
Internet Edge Topology	6
Internet Edge Deployment	6

**NOTICE:** ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

Copyright © 2011 Cisco Systems, Inc. All rights reserved.

# **Document Conventions**

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[]	Elements in square brackets are optional.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

# Screen examples use these conventions:

screen font	Terminal sessions and information in the displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Nonprinting characters, such as passwords, are in angle brackets.
<>	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

# **Cisco NGEW Architecture Overview**





Enterprise networks must adapt to meet new and evolving business requirements. The introduction of cloud services (private, public, or hybrid) poses new challenges to current enterprise network designs. A more distributed workforce, the proliferation of bandwidth-intensive video-enabled endpoints, and the consolidation of servers into a few centralized locations require networks to carry more traffic, with increased efficiencies, while demanding the same or a high level of performance and availability.

The Cisco<sup>®</sup> Next Generation Enterprise WAN (NGEW) is an end-to-end architecture that provides foundation building blocks for next-generation enterprise networks. The hierarchical design provides the scalability required by large enterprises, which can be extended and replicated throughout multiple regions and theaters. This consistency leads to ease of deployment, maintenance, and troubleshooting.

# Internet Edge Topology



Figure 2. Internet Edge (Detailed Topology)

The enterprise edge is the interface between the controlled enterprise network and users or resources that are outside of the enterprise's control or visibility. Users can be employees, partners, or customers. Resources can be Internet access, business-to-business connectivity and collaboration, hosted services, or hosted applications. The enterprise resource edge is also a place where services such as security, collaboration acceleration, etc. can reside.

The enterprise edge presents a diverse set of requirements because of the variety of user types accessing a variety of resources. This situation is compounded further because either may be located inside or outside of the enterprise network, meaning the enterprise edge can exist in many locations, but every location may not have the same set of requirements. In this phase of NGEW, we focus only on the Internet edge, also known as the web edge.

In the enterprise edge module a pair of Cisco ASR 1000 Aggregation Services Routers act as the edge routers facing the Internet. Cicso Adaptive Security Appliance (ASA) firewalls sit behind the Internet edge routers to provide firewall and Network Address Translation (NAT) functions. The Dynamic Multipoint VPN (DMVPN) and Easy VPN servers are behind firewalls. Two Cisco ASR 1000 Routers are used as DMVPN hubs and two as Easy VPN servers for redundancy with scaling. The DMVPN details are covered in the regional WAN (RWAN) deployment guide.

# Internet Edge Deployment

#### Overview

The Internet edge is the part of the network where the enterprise connects to the Internet service provider. It is also sometimes called the web edge. The web edge provides the company a web presence, provides access to the Internet for the company's users (employees and guests), and terminates some of the VPNs. In this architecture the Internet edge terminates Easy VPN Remote and Cisco AnyConnect<sup>™</sup> clients connecting from the Internet. The Internet edge is also the gateway for enterprise users to access the Internet securely. It also enables the enterprise IPv6 users to access the IPv4 Internet. Following are the details for implementing the Internet edge.

The devices used in this design are listed in Table 1.

#### Table 1. Design Devices

Component	Туре	Redundancy	Performance
Chassis model	Cisco ASR 1002	No	Based on RP and ESP
Cisco ASR 1000 Series Embedded Services Processor (ESP)	ESP10	No	Up to 4-Gbps cryptography
Cisco ASR 1000 Series Route Processor (RP)	RP1	No	Sub-second convergence/100 terabytes per second (TBps)

#### Easy VPN

The Cisco Easy VPN with Dynamic Virtual Tunnel Interface (DVTI) configuration provides a routable interface to selectively send traffic to different destinations, such as an Easy VPN concentrator, a different site-to-site peer, or the Internet. IP Security (IPsec) DVTI configuration does not require a static mapping of IPsec sessions to a physical interface, allowing for the flexibility of sending and receiving encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted when it is forwarded from or to the tunnel interface.

The traffic is forwarded to or from the tunnel interface by virtue of the IP routing table. Routes are dynamically learned during Internet Key Exchange (IKE) mode configuration and inserted into the routing table pointing to the DVTI. Dynamic IP routing can be used to propagate routes across the VPN. Using IP routing to forward the traffic to encryption simplifies the IPsec VPN configuration when compared with using access control lists (ACLs) with the cryptography map in native IPsec configuration.

In this design Easy VPN is deployed with two Cisco ASR 1000 Routers acting as Easy VPN servers. The Easy VPN remote clients are Cisco Integrated Services Routers (ISRs). All clients are configured with the two server addresses for redundancy. The Easy VPN servers are placed behind the firewall in this design. The Easy VPN clients are remote workers or home-office users who do not require much configuration on the client side.

The easiest way to define the users is the local user configuration. The more scalable way, however, is to define users on a RADIUS server. Both configurations follow:

```
no aaa new-model
!
username abc123 password 0 abc123
username ca-user2 password 0 ca-user2
```

If the users are defined on a RADIUS server, the following is the configuration:

#### Define the Phase 1 IKE Policy

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
crypto isakmp xauth timeout 5
```

#### **Define Client Configuration Group**

```
crypto isakmp client configuration group CA_GROUP2001
key cisco
pool CA_POOL2001
save-password
crypto isakmp profile ISAKMP_CA2001
match identity group CA_GROUP2001
client authentication list default
isakmp authorization list default
client configuration address respond
virtual-template 2001
!
```

#### **Define IPsec Policy**

!

```
crypto ipsec transform-set TS esp-3des esp-sha-hmac mode transport
```

### **Define Cryptography Profile for Easy VPN**

```
crypto ipsec profile IPSEC_CA2001
set transform-set TS
set reverse-route distance 5
set reverse-route tag 5
set isakmp-profile ISAKMP_CA2001
!
```

#### **Define Virtual Template**

```
interface Virtual-Template2001 type tunnel
no ip address
tunnel mode ipsec ipv4
tunnel vrf fus1010
tunnel protection ipsec profile IPSEC_CA2001
!
```

#### Routing on Easy VPN Server

```
router eigrp 300
network 10.4.11.231 0.0.0.0
network 10.4.226.16 0.0.0.3
network 10.4.226.24 0.0.0.3
network 10.4.226.32 0.0.0.7
redistribute static
 passive-interface default
no passive-interface GigabitEthernet0/0/0
 eigrp router-id 10.4.11.231
passive-interface default
no passive-interface GigabitEthernet0/0/0
eigrp router-id 10.4.11.231
1
ip local pool CA_POOL2001 9.1.0.1 9.1.0.254 group CA_GROUP2001
ip forward-protocol nd
1
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.4.226.33
ip route 67.0.0.0 255.0.0.0 10.4.226.33
ip route 223.255.254.253 255.255.255.255 15.1.0.1
ip route 223.255.254.254 255.255.255.255 15.1.0.1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 15.1.0.1
ip route vrf Mgmt-intf 223.255.0.0 255.255.0.0 1.2.0.1
ip route vrf fus1010 66.66.66.10 255.255.255.255 10.4.226.33
ip route vrf fus1010 172.36.10.0 255.255.255.0 10.4.226.33
1
```

# **Easy VPN Remote Configuration**

# **Define Cryptography Policy**

```
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
crypto isakmp xauth timeout 5
!
```

#### **Define IPsec Policy**

1

```
crypto ipsec transform-set TS esp-3des esp-sha-hmac mode transport
```

#### **Define Easy VPN Remote and Its Attributes**

```
crypto ipsec client ezvpn ca-user2
connect auto
group CA_GROUP2001 key cisco
mode network-extension
peer 172.36.10.3
peer 172.36.10.8
username ca-user2 password ca-user2
xauth userid mode local
!
```

#### Apply Easy VPN on the Outgoing Interface

```
interface GigabitEthernet1/1/0
ip address 66.66.66.10 255.255.255.0
negotiation auto
crypto ipsec client ezvpn ca-user2
!
```

# Define the Inside Interface

```
interface GigabitEthernet1/1/1
ip address 11.1.1.2 255.255.255.0
negotiation auto
crypto ipsec client ezvpn ca-user2 inside
!
```

#### **Routing on the Easy VPN Remote**

The client needs connectivity to the Easy VPN server. In most deployments just a default route to the Internet gateway is needed on the remote device.

#### Cisco AnyConnect Security

Cisco AnyConnect security is part of the edge design. Cisco AnyConnect security is implemented on the Cisco ASA Router firewall to allow remote users to connect to the corporate network. The Cisco ASA 5510 is used in this setup. Cisco Adaptive Security Device manager (ASDM) version 6.4 is used to deploy and manage the Cisco AnyConnect clients.

To configure Cisco AnyConnect security on the Cisco ASA Router, use the Cisco AnyConnect VPN wizard. The following screen shots are steps to follow on the wizard.

1. Select the Cisco AnyConnect wizard from the VPN Wizards menu (Figure 3).



#### Figure 3. VPN Wizards

2. Click Next on the first screen (Figure 4).

Figure	4.	Introduction	Screen
iguic	<b></b>	muouuouon	0010011

ISCO ASDM (	6.4 for ASA 192.168.1 Is Wizards Window Help	4				Look For:		المالي 👘
Home 2	Configuration 👩 Monitoring	Save 🚱 Refresh 🕻	Back 🜍 Forward 🦓 Help					CISC
Home								
- El Devi	ce Dasrboard	Jashboard						
Device In	(Information			Interface status	10 Address Mark	100		thes
General	License			incide10	10.4.226.22720	0.00	O un	27
Host Na	ame: ciscoasa			incide20	10.4.226.35/29	O up	Qup	0
ASA Ver	rsion: 8.4(1)	Device Uptime: 21d	15h 55m 25s	management	192.168.1.1724	0.00	0.0	5
ASDM W	Version: 6.4(1)	Device Type: ASA	5510	outside172	172.36.10.1/24	0.00	0.0	27
Frewal	Mode: Routed	Contact Moder Sind						271.
Total Fla	lash: 256 MB	AnyConnect VPN Con	nection Setup Wizard					
		VPN Wizard	Introduction				1	
CPU 0% 115431 Memory	CPU Usage (percent) CPU Usage (percent) 0 0 11:50 Memory Usage (MB) 1000 000 000 000 000 000 000 0				Rende Ziene		1163	1154
246748	400		< Back Next >		(	Cancel Hel		$\wedge   $
115401	0 11:50	11.51 11.52	11:53 11:54		·		1	
Details.				Input Kbps:	0 Output Kbps: 0	11.52	1153	11.54
Latest ASD	M Syslog Messages							0.00
			ASDM logging is disabled. To enable	e ASDM logging with informatic Enable Logging	anal level, click the button below.			
e configuration	n loaded successfully.				<admin></admin>	15		6/2/11 11:54:31

3. Give a profile name and select the inside interface (Figure 5).

Figure 5. Profile Name and Inside Interface

	Compation	ashboard		Interface Status				
General Host Na ASA Ver ASDM Vi Firewal	License me: ciscoasa sion: 8.4(1) ersion: 6.4(1) Mode: Routed	Device Uptime: 21d 15h Device Type: ASA 551 Crotact Modal Single	: 56m 55s 10	Interface inside10 inside20 management outside172	3P Address/Mask 10.4.226.33/29 10.4.226.166/30 192.160.1.1/24 172.36.10.1/24	Line Oup Oup Oup Oup	Unk O up O up O up	Kbps 21 0 5 21
VPN Sessi	ons Classifiers 55	Steps 1. Introduction	Connection Profile Identifica This step allows you to confi connections.	tion gure a Connection Profile Name ar	id the Interface the remote acces	is users will access for VPI		
9% 1156-01	esources Status CPU Usage (percent) 100 80 80 80 80 80 80 80 80 80 80 80 80 8	Identification 3. VFII Protocols 4. Clark Janges 5. Authentication Methods 6. Clark Address Assignment 7. Network Name Resolution Servins 8. Nat Exempt 9. AnyConnect Clark Deployment 10. Summary	Connection Profile Name: a	KryConnet_new  ksde20	×		<u> </u>	155 11
Memory	900						11	
245MB		1153 115	<back next=""></back>	1150		Cancel Help		<b>.</b>
245MB		1153 115	<back next=""></back>	1120 Deput Rbps: (	11.62 11.62 Cutput Rtips: 0	Cancel Help		100 11

4. Cisco AnyConnect security can use Secure Sockets Layer (SSL) or IPsec for security. Select SSL (Figure 6).

Dev	ice Dashboard 🔀 Firewall (	Dashboard						
Device In	formation			Interface Status		114420		
Host No ASA Ve ASDM V	License me: ciscoasa rsion: 8.4(1) /ersion: 6.4(1)	Device Uptime: 21d 15k Device Type: ASA 55	s 57m 25s 10	Interface inside10 inside20 management outside172	19-Address/Mask 10.4.226.33/29 10.4.225.166/30 192.160.1.1/24 172.36.10.1/24	0 up 0 up 0 up 0 up	0 up 0 up 0 up 0 up	21 0 7 21
Total Fi	IMode: Routed lash: 256 MB	AnyConnect VPN Connect	tion Setup Wizard				X	
		Steps	VPN Protocols					
PSec: 0 System F CPU 0% 1156-01 Memory	Cercles 59 Celocities 59 Celocities 59 Celocities 59 Celocities 59 Celocities 59 Celocities 69 Celoc	Connection Profile Identification     Why Protocols     Gene Tanges     Guert Profile     Guert Profile     Guert Anges     Guert     Gue	you would be the connection po State Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particle Particl	die to Apport. SSA to the remote access clean 2(2) requere that valid device or	As Cettan AnyConnect enticate be available on W Manage		11.65	1150
246748	400		< Back Next >		(	Cancel Help		
1156-01	0	1153 1154	11.55 11.56	11.52	11.50	1154	11.55	11.58
Detais.				Input Kbps: 0	0 Output Kbps: 0			
atest ASD	M Syslog Messages							084
			ASDM logging is disabled. To enable	ASDM logging with informatio	nal level, click the button below.			

Figure 6. SSL Security

5. The Cisco ASA Router can directly upload the selected image to the client (Figure 7).

Figure 7. Uploading Image

Device In	formation			Interface Status				
General	License			Interface	IP Address/Mask	Line	Link	Kbps
				inside10	10.4.226.33/29	0.0	Q up	5
Host Na	me: ciscoasa			inside20	10.4.226.166/30	Q up	Qup	0
ASA Ver	rsion: 8.4(1)	Device Uptime: 21d 15h	58m 5s	management	192.168.1.1/24	Q up	Q up	5
ASDM W	lersion: 6.4(1)	Device Type: ASA SS	0	outside172	172.36.10.1/24	O up	O up	5
Firewall Total Flu	Mode: Routed ash: 255 MB	E AnyConnect VPN Connec	tion Setup Wizard	11.12				
							-	
		sceps	Cienc Images					_
Inform O	Charles CO.	1. Introduction	ASA can automatically upload th	e latest AnyConnect package	to the client device when it access	ies the enterprise network		
an section	Cienciess 55	<ol> <li>Connection Profile</li> <li>Identification</li> </ol>	A regular expression can be use	d to match the user-agent of a	a browser to an image.			
System R	tesources Status	3 VDN Protocole	You can also minimize connection system to the top of the list.	n setup time by moving the ima	age used by the most commonly er	countered operation		
CPU	CPU Usage (percent)	4. Client Imager	a second and here and					
	100	4. Cient Images	Add 🛃 Replace 🁔 Dele	te 🕆 🗲				*
		S. Authentication Methods						A
		<ol><li>Client Address Assignment</li></ol>	Add Incompact Incom2.4.10	1230 dia	Regular expression to man	ton user-agent		
	60	<ol> <li>Network Name Resolution Servers</li> </ol>	disk0:/anvconnect-win-2.4.101	2-19.pkg				
0%	40	B. NAT Exercit disk0: Janyconnect-macosx-086-2.4.1012-49.pkg						
		o. Hor exempt						
	20	Deployment					11:5	11
	0	10. Summary					1000	
1157.11	11:53							
Memory	Memory Usage (MB)							
	1000 (							
	900							
			You can download Any-Connect	Client packages from Cisco by	searching 'AnyConnect VPN Client	t' or <u>click here</u> ,		
	600						_	
246MB	400		< Back Next >		(	Cancel Help		1
	200			2 /			_	/\
	0			1 + 4				× / \
1157:11	11.53	11.64 11.65	11.56 11.57	0	1153 1154	11.55	11.5	8 11
Datale				Input Kbps: 0	0 E Output Kbps: 0			
100.002								
atest Asna	M Syslan Messages							
ADD.	a strand - servages							0.0

Users can be specified locally or on the RADIUS or TACACS server. Select LOCAL and add a user (Figure 8).

Figure 8.	Adding Users
-----------	--------------

	ice Dashboard	lashboard						
Device In	formation			Interface Status				
General	License			Interface	IP Address/Mask	Line	Link	Kbps
Host Na	me: ciscoasa			inside10	10.4.226.33/29	O up	Qup	7
ASA Ver	rsion: 8.4(1)	Device Uptime: 21d 15h	59m 5s	management	192.168.1.1/24	Qup	0 00	5
ASDM V	Version: 6.4(1)	Device Type: ASA 551	0	outside172	172.36.10.1/24	O up	Q up	9
Firewall Total Fl	Mode: Routed	AnyConnect VPN Connec	tion Setup Wizard					
		Secs	Authentication Methods					
VPN Sessi	ions	1. Introduction	This step lets you specify the locati	on of the authentication serv	er.			
IPSec: 0	Clientless SS	2. Connection Profile	You can click on the "New" button	n to create a new server gro	up.			
System R	Resources Status	Identification	AAA Server Group: LOCAL	New				
CPU	CPU Usage (percent)	3. VPN Protocols	Constant Constant C					
	100	4. Client Images	Local Lines Database Details					
	80	5. Authentication Methods	Local User Dakabase Decass	Diere	62.			
	~	6. Clerit Address Assignment						
	60	7. Network Name Resolution	User to be Added					
0%	40	Servers Username: cisco Add >>					$\wedge$ /	
		8. NAT Exempt	Password: •••••					
	20	9. AnyConnect Client	Confirm Password:				11:57	11:
1159-11	1154	Deployment						
		10. Summary						
Memory	Memory Usage (MB)							
	1000							
	800							
	600							
245148			<back next=""></back>		ſ	Cancel Help		,
								F
	200	CONTRACTOR OF TAXABLE PARTY.	CALIFORNIA CONTRACTOR OF THE OWNER OF				/\	- /
11.62.11	0 1154	11.55 11.50	11.67 11.68		VI VIII		A.L.	A. 1
1100111				Terrathers 2	11.54 11.55	11:56	11.57	11:
Detais				Provi Kops: 3	Corpor keps: 1			
	M Suslan Messages							08
atest ASD	a stand a second des							
atest ASD	(1) story ( less only ( )							

7. Create a pool of addresses to be used by clients (Figure 9).

Figure 9. Creating Pool of Addresses

Device In	formation			Interface Status				
General Host Na ASA Ver ASDM W	License me: ciscoasa rsion: 8.4(1) ersion: 6.4(1)	Device Liptime: 21d 15k Device Type: ASA 55	59m 45s 0	Interface inside10 inside20 management outside172	IP Address/Mask 10.4.226.33/29 10.4.226.166/30 192.160.1.1/24 172.36.10.1/24	Une Oup Oup Oup	Link Oup Oup Oup	Kbps 10 0 5 10
Firewall Total Fis	Mode: Routed sh: 256 MB	AnyConnect VPN Connect	tion Setup Wizard	dela la				
		Steps	Client Address Assignment					
0% 115851 Memory	CPU Usage (percent) 100 80 60 40 20 0 11.54 11 Memory Usage (MB) 1000	a. vrsi Protocols     Authentication Methods     Authentication Methods     Authentication Methods     Authentication Methods     Authentication Methods     Angewing     Angewing     Angewing     Angewing     Angewing     Sammary	P v4 Address Flool P v4 Address Flool pen_users Details of the selected addre Starting IP Address: 2001.6 Subnet Missl: 255.25	5 Address Pool W New spool 5.200.254 5.255.0	-		Δ.	, 1150
246448	400 200 0 1154	105 1108 1	<back next=""></back>		(	Cancel Help		A.
Details				11.54	0 Output Kbps: 0	11.56	11.57	11.58
test ASDA	M Syslog Messages							0.4
		1	ASDM logging is disabled. To enable	ASDM logging with informatio	nal level, click the button below.			

8. Specify server names and domains (Figure 10).

Figure 10. Specifying Server Names and Domains

TASUM 6											- 6
ew Tools	s Wizerds Window Help	<b>D</b> . <b>A A</b>		1 <b>2</b> 45			Lo	sk.For:		100	ahal
6030	computation [3] Monitoring	Save Co Kerresh	Back Oronwar	a 🦿 Help							cisco
me Devi	ra Dashboard   😰 Freud D	hwatta									
Device In	formation				Interface Status						
General	License			-	Interface	IP Address/P	lask.	Line	Link	Kbps	
					inside10	10.4.226.33/3	19	D up	Q up	11	
Host Nar	me: ciscoasa				inside20	10.4.226.166	130	Q up	Q up	0	
ASA Ver	rsion: 8.4(1)	Device Uptime: 21d 16	2m 15s		management	192.168.1.1/2	м и	Q up	Qup	5	
ASDM Ve	lersion: 6.4(1)	Device Type: ASA 55	10		outside172	172.36.10.1/2	9	🗘 up	O up	12	
Firewall Total Fig	Mode: Routed ash: 256 MB	AnyConnect VPN Connect	tion Setup Wiz	ard				R	1		
		Secs	Network Name I	tesolution Servers							
VPN Sessi	ions	1. Introduction	This step lets yo	u specify how don	ain names are resolved for	he remote user when	accessing the intern	i network.			
IPSec: 0	Clientless 55	2. Connection Profile	DAS Secure	10.4.200.25							
System R	tesources Status	3. VPN Protocols	WINS Servers:	10.4.200.25						ħ	
CPU	CPU Usage (percent)	4. Clent Images	Domain Name:	cisco corel			-			Δ	
	100	5. Authentication Methods		torrect.						1	
	80	6. Client Address Assignment								1	
		7. Network Name									
		Resolution Servers									
	40	B. NAT Exempt									
	20	9. AnyConnect Client									
		Deployment							12.00		12:01
12:01:21	0 11:57	10. Summary							-		
Memory	Memory Usage (M8)										
	1000										
	800										
1.000	600										-
comp	400		< Back	Next >			Cancel	Help			Ā
_	200				21 / \		11				
					1. / \	. /		~			1
	0 11:57	11:58 11:59	12:00	12:01	0						
12:01:21					Treat Phone of	Cutout they - 0	11.90	11.00	12.00		12.01
12:01:21					a participation of						
120121 Details											
120121 Details					1.1						
120121 Detais	M Syslog Messages										08
test ASD*	M Syslog Messages										08
test ASD*	M Syslog Messages		ASDM logging is di	sabled. To enable A	SDM logging with informatio	val level, click the butt	on below.				08
I20121	M Syslog Messages		ASDM logging is di	sabled. To enable A	SDM logging with informatio	nal level, click the but	on below.				0 8
120121 Detais	M Syslog Messages	\$	ASDM logging is de	sabled. To enable A	SDM logging with informatio	nal level, click the but	on below.				0 8
120121 Details test ASD*	M Syslog Messages	\$	ASCM logging is di	abled. To enable #	SDM logging with informatio Enable Logging	nal level, click the but	on below. admin> 15	6	8 60	6/2/1	1 12:01:21

9. VPN traffic should be exempt from translations (Figure 11).

Figure 11. Exempting VPN Traffic from Translations

serve morm	ation			Interface Statu				
General Licer Host Name:	ciscoasa	Too too too too too	2011	Interface Inside10 Inside20	JP Address/Mask 10.4.226.33/29 10.4.226.166/30	Une O up O up	Link Oup Oup	Kbps 10 0
ASA version: ASDM Version Firewall Mode	8.4(1) = 6.4(1) = Routed	Device Uptime: 210 160 Device Type: ASA 551 Contact Mode: Single	2m 55s 10	management outside172	192.168.1.1/24 172.36.10.1/24	O up O up	ф ф Ф Ф	5 10
Total Flash:	256 MB	AnyConnect VPN Connec	tion Setup Wizard					
		Steps	NAT Exempt					
VPN Sessions	6	1. Introduction	If network address tran	slation is enabled on the ASA, the	VPN traffic must be exempt from the	s translation.		
arsiec: 0	Clientless SSI	<ol> <li>Connection Profile Identification</li> </ol>	Exempt VPN traffic f	rom network address translation			-	
System Resou	rces Status	3. VPN Protocols	Inside Interface is th	he interface directly connected to	/our internal		t.	
CHU CPL	1 Usage (percent) 30 ;	4. Clent Images	network.		100			
		5. Authentication Methods	inside interface: o	UK5108172	× 1			
		Clerit Address Assignment     Local Network is the network a     clerit can access		network address(es) of the intern	(dress(es) of the internal network that			
	10	Servers	Local Network:	nv.	CI.			
1.1	40	B. NAT Exempt			0			
	20	<ol> <li>AnyConnect Client Deployment</li> </ol>	The traffic between	AnyConnect client and internal ne	work will be			12.01
12:02:01	1150	10. Summary	exempt from networ	k address translation.				
Memory Mer	norv ( Isone (MB)							
10	200 1							
	100							
24546			C Back Next 2			Cancel Help		
								$\wedge$
	200	CALIFORNIA DE LA CALIFICAL DE LA CALIFORNIA DE LA CALIFORNICA DE LA CALIFORNIA DE LA CALIFORNIA DE LA CALIFICAL	1. 10. 10. 10. 10. 10. 10. 10. 10. 10. 1	1		~	**	
12:02:01	0 11.50	11.59 12.0	0 12:01	12.01 0	11.58 11	159 12	00	12:01
Details				Input Kbp	s: 0 📕 Output Kbps: 0			
	days Marrisona							00
itest ASDM Sys	nogriessages							

Device Info General Li Host Name ASA Versio ASDM Vers Firewall Mo Total Flash	rmation cense t: ciscoasa an: 8.4(1) aion: 6.4(1) ode: Routed t: 256 MB	Device Liptme: 21d 16 Device Type: ASA 53 Credital Model: Studie States States	h 3m 15s 510 ction Setup Wizard	Interface Status Interface inside10 inside20 management	IP Address/Mask 10.4.226.33/29 10.4.226.166/30	Line O up	Link	Kbps
General Lin Host Name ASA Versio ASDM Vers Firewal Mo Total Flash	rrinadon rcense r: ciscoasa rr: 8.4(1) sion: 6.4(1) ode: Routed r: 256 MB	Device Uptime: 21d 16 Device Type: ASA 53 Contact Model: Studie Mary Connect VPN Connec Stars	h 3m 15s 510 ction Setup Wizard	Interface Inside10 Inside20 management	IP Address/Mask 10.4.226.33/29 10.4.226.166/30	Line O up	Link O uro	Kbps
Host Name ASA Versio ASDM Vers Firewal Mo Total Flash	cense :: ciscoasa ::: 8.4(1) son: 6.4(1) ode: Routed :: 256 MB	Device Uptime: 21d 16 Device Type: ASA 53 Costex Mode: Stanle MaryConnect VPN Conne Stans	h 3m 15s 510 ction Setup Wizard	inside10 inside20 management	IP Address/Mask. 10.4.226.33/29 10.4.226.166/30	O up	Link	KDps
Host Name ASA Versio ASDM Vers Firewall Mo Total Flash	:: ciscoasa m: 8.4(1) son: 6.4(1) ode: Routed h: 256 MB	Device Uptime: 21d 16 Device Type: ASA 53 Contract Model: Strong AnyConnect VPN Connect Steps	h 3m 15s 510 ction Setup Wizard	inside20 management	10.4.226.166/30	Up up		
ASA Versio ASDM Vers Firewall Mo Total Flash	m: 8.4(1) son: 6.4(1) ode: Routed h: 256 MB	Device Uptime: 21d 16 Device Type: ASA 55 Costart Mode: Stender	h 3m 15s 510 ction Setup Wizard	management		O un	0 10	21
ASDM Vers Firewall Mo Total Flash	son: 6.4(1) sde: Routed n: 256 MB	Device Type: ASA 55 Context Model: Encode Series	510 ction Setup Wizard	1 A 1 A 1 A 1 A 1	192.168.1.1/24	O up	Q up	5
Firewal Mo Total Flash	:de: Routed 1: 256 M8	AnyConnect VPN Conne	ction Setup Wizard	0UCSID01/2	172.36.10.1/24	O up	O up	75
Total Hash	1: 236 MB	Sans	ction Setup wizard					
	15	9 ans	and the second se					
1.0	15		AnyConnect Client Deployment					
VPN Session		1. Introduction	AnyConnect client program can b	e installed to a client device t	by one of the following two methos	55:		
IPSec: 0	Clientless S	2. Connection Profile	1) Web launch - On accession the	ASA uring a Web Browner 1	the AnuConnect clarit nackane will	he schonatically install		
Evetern Par	courses Status	Identification	<ol> <li>Pre-deployment - Manually ins</li> </ol>	tall the AnyConnect client pa	ckage.	be automatically inical	eu,	
STRUCTURES	Talling (and a	<ol> <li>VPN Protocols</li> </ol>						
00 0	100 -	4. Clent Images						
		5. Authentication Methods						
	80	6. Client Address Assignment						
	60	7. Network Name Resolution						
0%	2	Servers						
	40	8. NAT Exempt						
	20	9. AnyConnect Client						
		Deployment					12.01	12/02
12:02:21	11:50	10. Summary						
Memory 8	Memory Likage (MB)							
	1000 (							
	10000							
	800							
	600							
24546			< Back Next >		1	Cancel Help		
								1
	200			2	1		/	1
	0	1140 1200	12.01 12.02		A	1	· · · · · ·	1
120221	11.50	11.00 12.00	12.02	,	1.58 11.59	12.00	12:01	12:02
Details				Input Kbps:	12 Output Kbps: 9			
-				- Contraction				
Latest ASDM 5	Syslog Messages							0 8
			ASDM logging is disabled. To enable	ASDM logging with informatic Enable Logging	nal level, click the button below.			
configuration lo	aded successfully.				<admin></admin>	15		6/2/11 12:02:21

10. Verify the configured parameters and finish (Figure 12).

New Tools Wizards	Window Help					Look For:		ahal
one 🖧 Configuration	Monitoring 🕞 Sav	e 🕞 Refresh 🔇	Back 🕐 Forward 🦓 Help					CISCO
ome								
Device Dashboard	d 🚱 Firewall Dashboard							
Device Information	-			Interface Status				
General License				Interface	IP Address/Mask	Line	Link	Kbps
			1	inside10	10.4.226.33/29	O up	Qu Q	24
Most Name: CISCO	oasa	Denice Linkimet 21d 16h	200.25¢	inside20	10.4.226.166/30	O up	O up	2
ASDM Version: 6.4(	1) 1)	Device Type: ASA 551	0	management	192.168.1.1/24	O up	O up	5
Firewal Mode: Rout	ted	Contact Moder Single		outside172	172.36.10.1/24	O up	O up	27
Total Flash: 256	MB 🔂 AnyC	onnect VPN Connec	tion Setup Wizard					
	VPN W	/izard	European .					
VDN Conscions		1	Juneiary				-	
IDSact 0	Clentines SS		Here is the summary of the configura	tion.				
		a I	Name	Value				
System Resources S	Ratus	and man	B Summary					1
CPU CPU Usage	e (percent)		Name/Alias of the Connection Pro	fie AnyCor	nect_new			
100	L	1	VPN Access Interface	inside20				
80	50	corporate }	VPN Protocols Enabled	SSL only				
		Netwo	AnyConnect Client Images	3 packa	pes			1
	The state	1	Authentication Server Group	LOCAL				
40		and the second	Address Pool for the Client	209.16	.200.10 - 209.165.200.254			
20		A DESCRIPTION	DNS	Domain	Name: null			
			Network Address Translation	The pro	ected traffic is subjected to net	work address translation	12.01	12:02
							and the second second	
12:02:01	11.58	Tahill						
12:02:01 0	11.58	T						
12:02:01 0	11.58 sage (MB)	THE						
12:42:31 0	11.58 sage (P8)	6						Å
12:42:31 0 Memory Us 1000 - 800 -	11.58 soge (110)	6-						Å
12-02-03  Memory Memory Us  1000  0  0  0  0  0  0  0  0  0  0  0	11.58 sege (M8)	2-						Å
Nemory         Memory Us           12:02:31         0           10:00         -           900         -           246M6         400	11.56 ssge (HB)	<b>R</b> -	< Back Printh			Cancel Help		Å
12/82/01 0	11.58 sage (PB)	<u>}-</u>	< Back Prish			Cancel Help		Å
24646 400 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 -	1158 Soge (10)	2-	<back prish<="" td=""><td>2</td><td></td><td>Cancel Help</td><td></td><td>Å</td></back>	2		Cancel Help		Å
24646 200 400 100 100 100 100 100 100 100 100 1	11.54 coge (162)	1200	<back presh<="" td=""><td>2</td><td></td><td>Cancel Help</td><td></td><td></td></back>	2		Cancel Help		
12:02:01 Memory Memory Us 2:00 12:02:01 0 0 0 0 0 0 0 0 0 0 0 0 0	11.68 (ME) 11.68 11.59	12:00	< 8ad. Finish	2	1150	Cancel Help	1201	12.02
12-02-31 Memory Memory Us 2-6546 2-6546 12-02-31 12-02-31 12-02-31 0 	1158 soge (HB) 1158 1159	12:00	< 8ad. Prish	2 0 1150 Input Kbps: 2	1150 Cuput Hops: 0	Cancel Help	12.01	12.02
12:02:31 Memory Memory U 2:69% 2:69% 12:02:31 Cotats	1158 ssge (HB) 1158 1159	1200	CBack. Fresh 12:01 17:02	2 0 1150 2 Input Kbps: 2	1150 • Cusput Rips: 0	Cancel Help	12.01	12.02
12-02-31 Memory Memory Us 2-07-6 2-07-6 12-02-31 Memory City 0 0 0 0 0 0 0 0 0 0 0 0 0	1158 coge (10) 1158 1159 exercise	12:00	< 0x3 Fred. 12:01 12:02	2 0 1150 0 1150 0 1004 thos: 2	1150 Output fibes: 0	Cancel 1460	1201	1262
12-02-33 Memory Memory Us 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-66% 2-	11.50 (sopt (18)) 11.50 11.50 (cstoges	1200	< 6ack Freeh	2 0 1150 10 Januar Hoori 2	1150 Output Pibes: 0	Cancel Help	1201	1200
12:82:33 Memory Memory Us 2:87% 12:82:53 12:82:53 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:54 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 12:82:82 1	11.50 soge (10) 11.50 11.50 11.50	1200	C Bush Presh     12 01 12 02	2 0 11:60 2 Input Kbor: 2	1150 1150 © Output Higher &	Cancel Help	1201	12.02
12-02-33 Memory Memory Un 2-069-6 12-02-34 12-02-34 2-00 -00 -00 -00 -00 -00 -00 -0	11.50 exep(100) 11.50 11.59 execution	12.00	< Beck. Final. 12.01 12.02 ACM logging is disabled. To make ACM	2 1156 Provi k tops: 2 M logging with information Enable Logging	1159 Cutput figer 0	Cancel 1460	1201	1202 1202
12-02-34 Nemory U 2-0576 12-02-34 12-02-34 12-02-34 0 0 0 0 0 0 0 0 0 0 0 0 0	11.54 soge (10) 11.50 11.50 11.50 11.50	1200	201 1202	2 0 11 500	119 0 dugut itige: 0	Cancel Help	1201	1262
12-02-33 Memory Memory U 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-05/96 2-0	11.50 Incore (100) 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 11.50 1.	1200	< Beck Presh	Provi ktore: 2 Mogging with information Enable Logging	11.50 • Cutput Highs: 0 • Sutput Highs: 0 • Sutp	Cancel 1486		12 G2
12-02-34 Person V 2-02-54 12-02-54 12-02-54 12-02-54 0 0 0 0 0 0 0 0 0 0 0 0 0	11.50 1000 (90) 11.00 11.00 11.00 esseques esseques	12.00	C Clask Freeh	2 June 1156 Brown Khori 2 Mogang with information Enable Logging	110 0 Jupit ther: 0	Cancel Help		12 CC 1 1 1 2 CC 2 1 1 1 2 CC 2 1 1 1 1

Figure 12. Verification and Finishing

and the could a subles of the book of			<u></u>	el		Look For:	- aha
mote Access VPN	Tooling ation > Re	mesh Create VDN	Natural (Church)	RP	Connection Profiler		CISC
Introduction Network (Clerit) Access To Any Connect Connection Profiles To Any Connect Customization (Local To Any Connect Clerit Profile To Any Connect Clerit Profile To Any Connect Clerit Settings	The security applia VPN Client support Access Interfaces	nce automatically dep i IPsec (IKEv2) tunne iyConnect VPN Client	loys the Cisco AnyCon I as well as SSL tunnel access on the interfac	nect VPN Client to remote with Datagram Transport es selected in the table b	e users upon connection. The initia Layer Security (DTLS) tunneling of elow	i client deployment requires end-user adm stions.	inistrative rights. The Cisco AnyConnect
Group Policies	SSL access must be	enabled if you allow	AnyConnect client to b	e launched from a brows	er (Web Launch) .		
IPsec(IKEv1) Connection Profiles	Interface	SSL Access		IPsec (IKEv2) Aco	855		
Secure Mobility Solution		Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certificate	
Address Assignment	inside10		9			Post Settings	
Classifiers SCI VDN Arcars	inside_20					[ Torcounder in ]	
Clericess SSC 1114 Access	outside172	2	2				
DNS Advanced	Connection Profiles Connection profile	(tunnel group) specifi	es how user is authent	cated and other paramet	ters.		
	Add 🛃 Edit	Delete					
	Name	SSL Enable	d	IPsec Enabled	Allases	Authentication Method	Group Policy
	DefaultRAGroup			(v)		AAA(LOCAL)	Decorpeolog
	Connect	, ap	123	E	Connect	AAA(LOCAL)	Grandalay Connect
	Connect1			H	ConnectI	AAA(I OCAL)	GroupPolicy_Connect
	An/Corpect new	-	2 2		AnyConnect new	AAA/LOGAL)	GroupPolicy AnyCoppert new
S Derice Soup Grewal							

# NAT44

In NAT44 the Cisco ASA Router is used as the NAT device for IPv4 traffic getting out to the Internet. Other than some of the static NAT that is needed for different servers, the rest of the internal network goes through the NAT process dynamically. Following is the configuration for NAT on the Cisco ASA:

```
object network obj-10.4.226.42
nat (inside10,outside172) static 172.36.10.4
object network obj-10.4.226.35
nat (inside10,outside172) static 172.36.10.3
object network obj-10.4.226.34
nat (inside10,outside172) static 172.36.10.10
object network obj-10.4.226.32
nat (inside10,outside172) static 172.36.10.5
object network obj-10.4.226.26
nat (inside10,outside172) static 172.36.10.8
object network obj-dynamic-10.4.0.0
nat (inside20,outside172) dynamic obj-dynamic-172.36.10.0
```

# NAT64

In this phase of NGEW, Stateless NAT64 provides address family translation services from IPv6 to IPv4. NAT64 is a mechanism that addresses scenarios where native IPv6 communication is not possible; for example, when a device on the network does not support dual stack. This technology is one of several IPv4-to-IPv6 migration and coexistence technologies available from Cisco. Stateless NAT64 is the mapping algorithm between IPv4 and IPv6 addresses. It is expected that service providers' IPv4 addresses will be mapped into IPv6 and used by physical IPv6 hosts. The original IPv4 forms of these blocks of service providers' IPv4 addresses are used to represent the

physical IPv6 hosts in IPv4. This type of algorithm supports both IPv6- and IPv4-initiated communications. Stateless NAT64 does not maintain the bindings or session state like NAT44.

Following is the NAT64 configuration:

1

```
interface GigabitEthernet0/0/0
description Towards Internet and IPv4 address
ip address 172.37.10.2 255.255.255.252
negotiation auto
nat64 enable
cdp enable
!
```

```
interface GigabitEthernet0/0/2
description Towards Internal network and IPv6 address
ip address 172.36.10.2 255.255.255.0
negotiation auto
ipv6 address 2001::1/128
ipv6 enable
nat64 enable
cdp enable
```

```
router bgp 65018
bgp log-neighbor-changes
network 172.36.10.0 mask 255.255.255.0
neighbor 66.66.66.10 remote-as 65025
neighbor 172.37.10.1 remote-as 65016
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/1
ip route 10.4.0.0 255.255.0.0 172.36.10.1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 15.1.0.1
!
ipv6 route 2001::1B01:10C/128 GigabitEthernet0/0/2
ipv6 route 2001::AC24:A64/128 GigabitEthernet0/0/2
ipv6 route 2001::AC24:A65/128 GigabitEthernet0/0/2
ipv6 route 2001::AC24:A65/128 GigabitEthernet0/0/2
ipv6 route 2001::AC24:A65/128 GigabitEthernet0/0/2
ipv6 route 2001::AC24:A66/128 2001::AC24:A65
```

nat64 prefix stateless 2001::/96
nat64 route 172.36.10.100/32 GigabitEthernet0/0/2



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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

Printed in USA