Deployment Guide

Cisco Next Generation Enterprise WAN

Regional WAN Remote Access VPN Deployment Guide

September, 2011

Contents

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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.

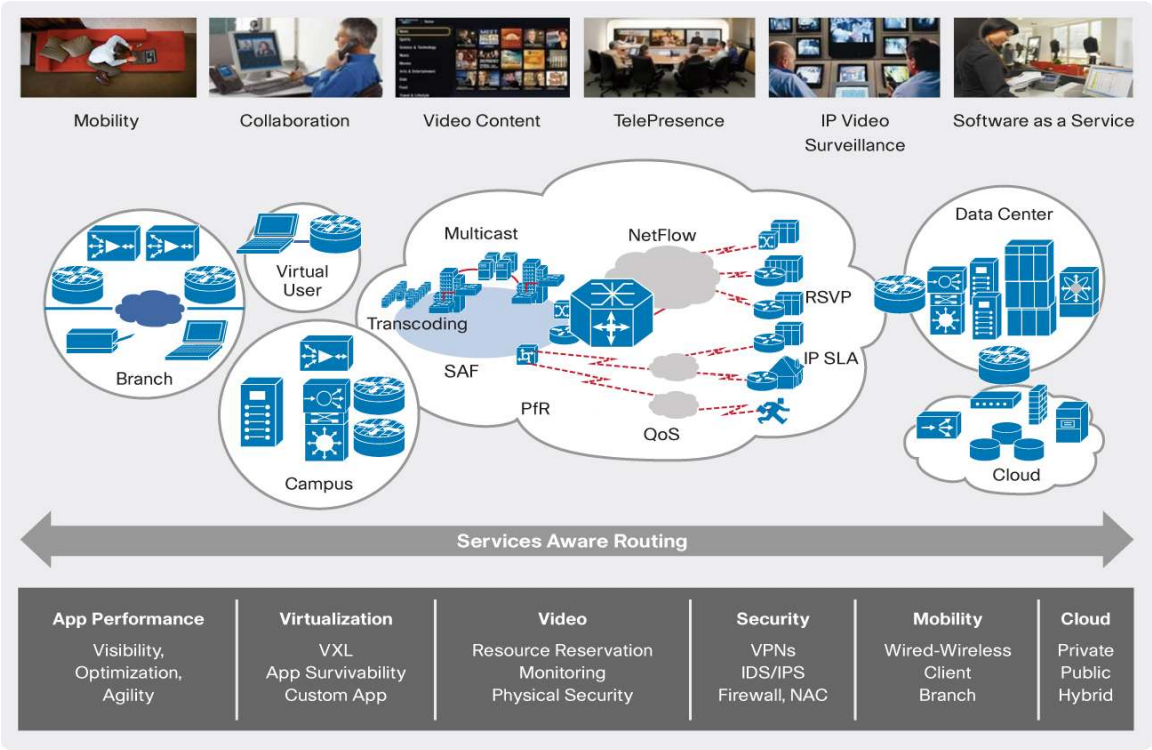
Screen examples use these conventions:

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.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco NGEW Architecture Overview

Figure 1. Enterprise Network Architecture



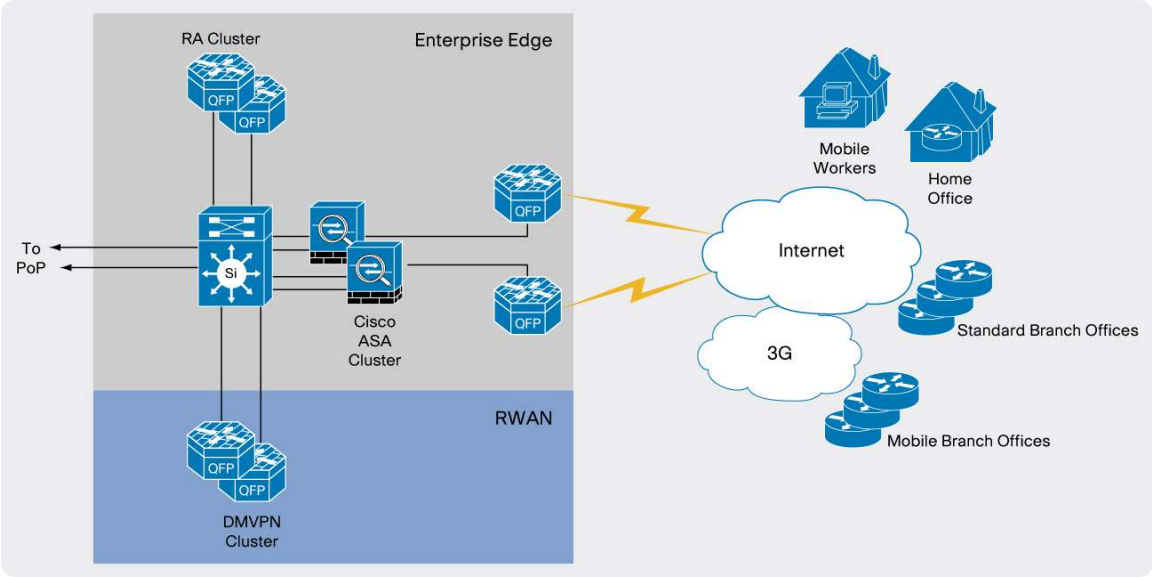
Enterprise networks must adapt to meet new and evolving business requirements. The introduction of cloud services (private, public, or hybrid) poses new challenges to current enterprise network designs. A more distributed workforce, the proliferation of bandwidth-intensive video-enabled endpoints, and 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® 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.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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) firewallls sit behind the Internet edge routers to provide firewall and Network Address Translation (NAT) funtions. 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.

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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™ 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	Type	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
```

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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
!
```

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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
!
ip local pool CA_POOL2001 9.1.0.1 9.1.0.254 group CA_GROUP2001
ip forward-protocol nd
!
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
!
```

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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

```
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

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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.

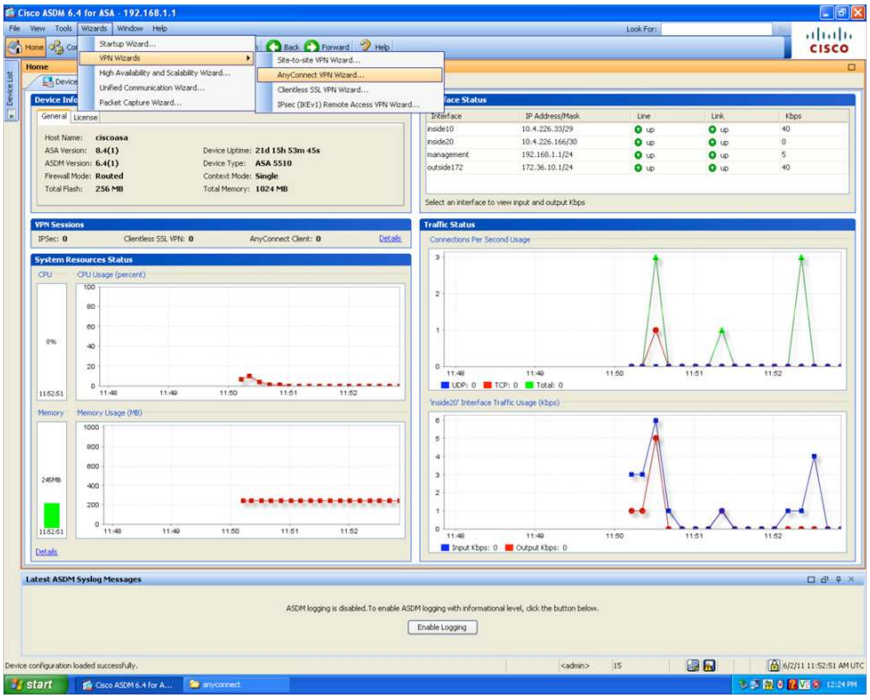
Cisco AnyConnect Security

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).

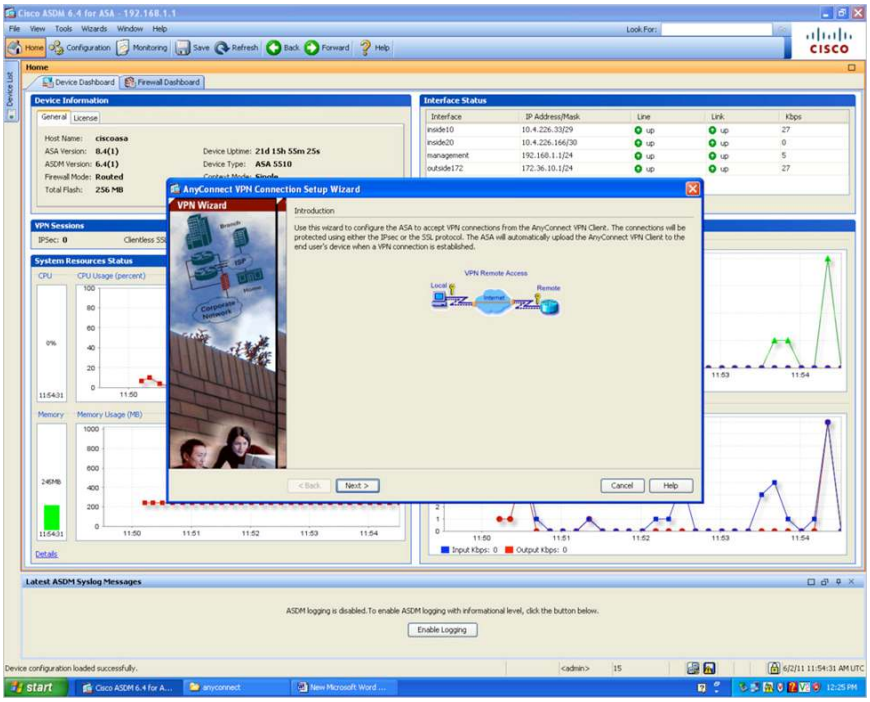
Figure 3. VPN Wizards



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

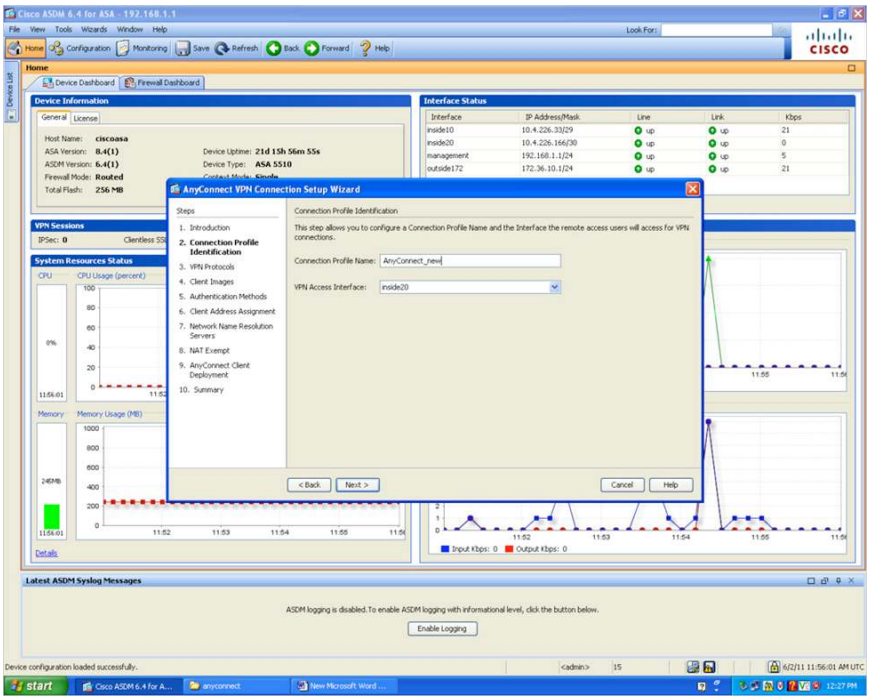
2. Click Next on the first screen (Figure 4).

Figure 4. Introduction Screen



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

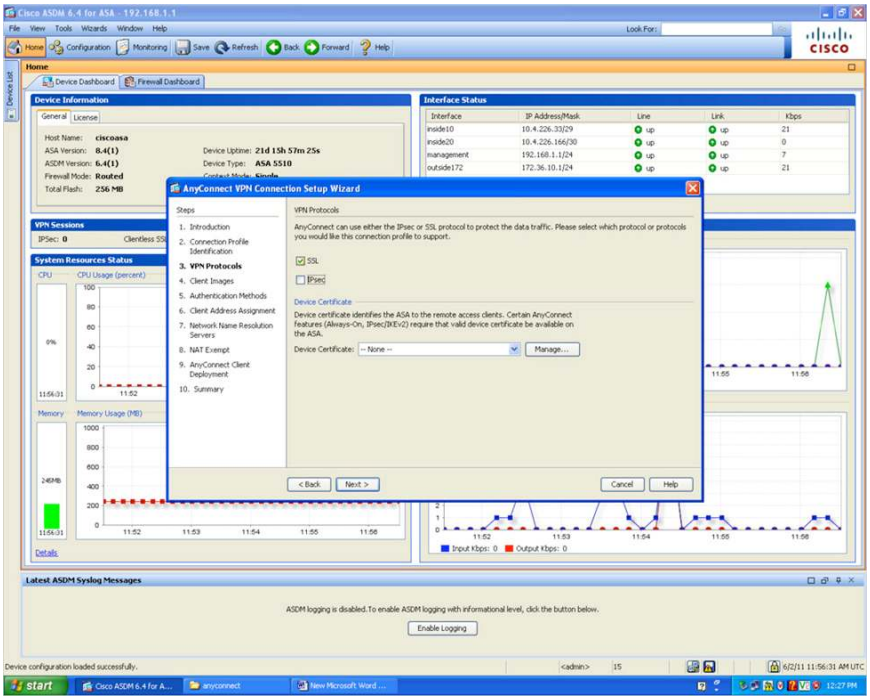
Figure 5. Profile Name and Inside Interface



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

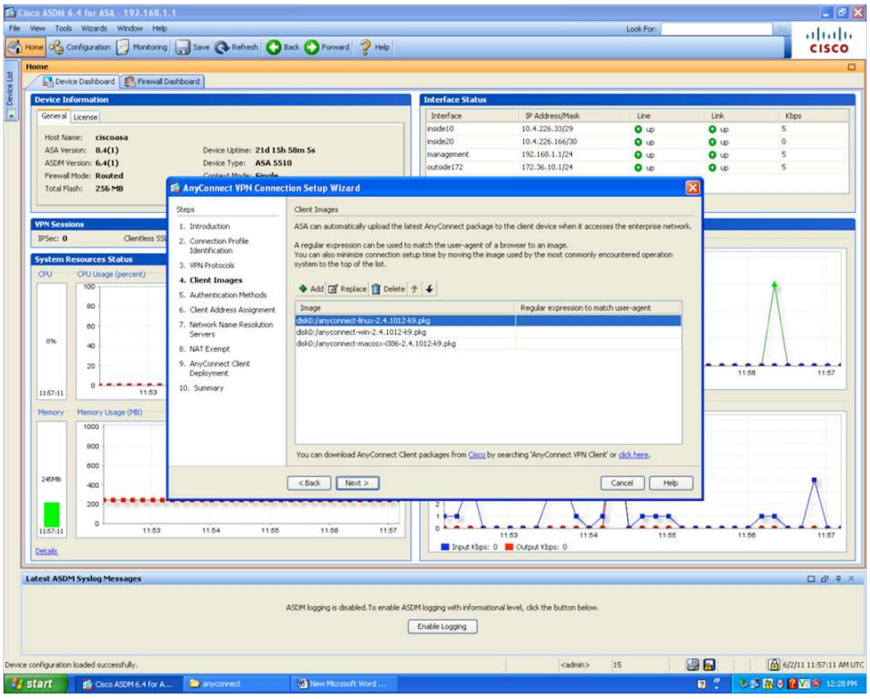
4. Cisco AnyConnect security can use Secure Sockets Layer (SSL) or IPsec for security. Select SSL (Figure 6).

Figure 6. SSL Security



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

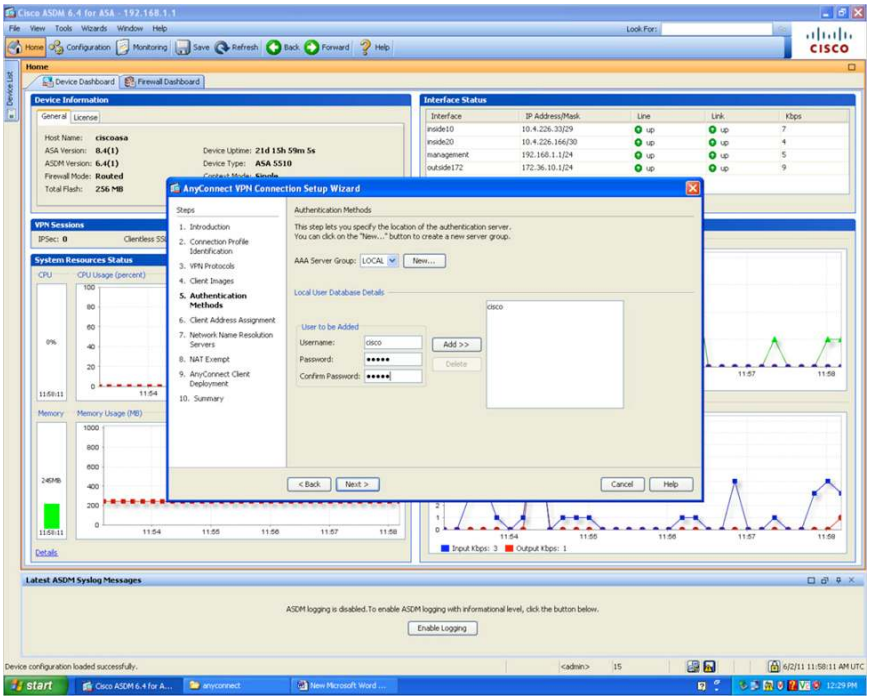
Figure 7. Uploading Image



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

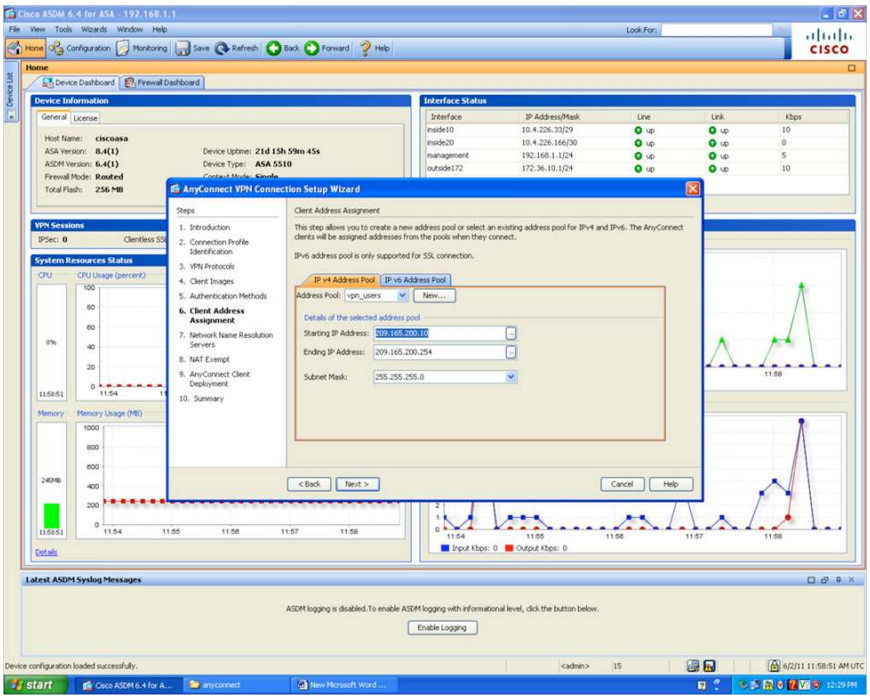
6. Users can be specified locally or on the RADIUS or TACACS server. Select LOCAL and add a user (Figure 8).

Figure 8. Adding Users



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

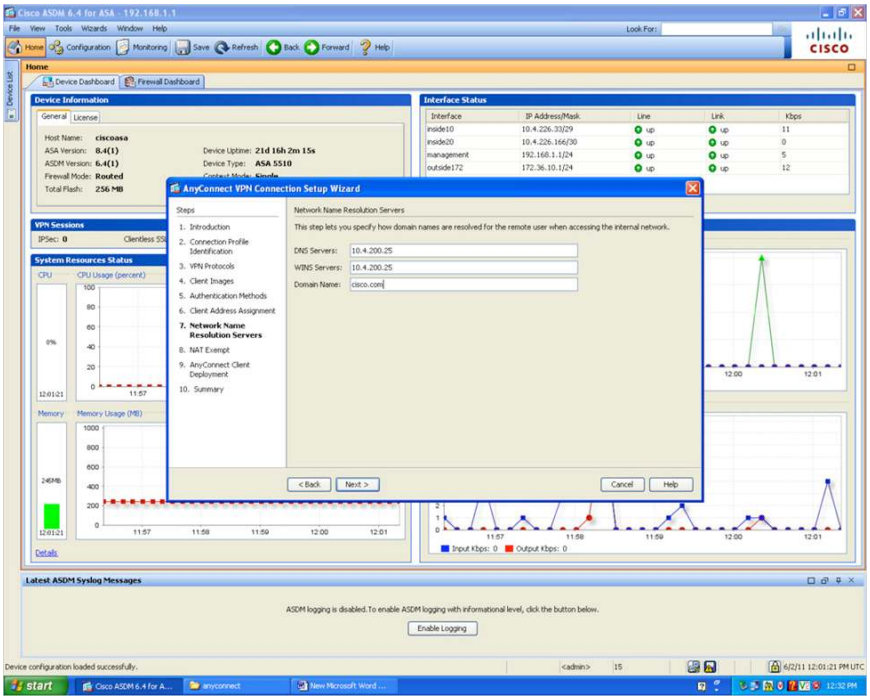
Figure 9. Creating Pool of Addresses



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

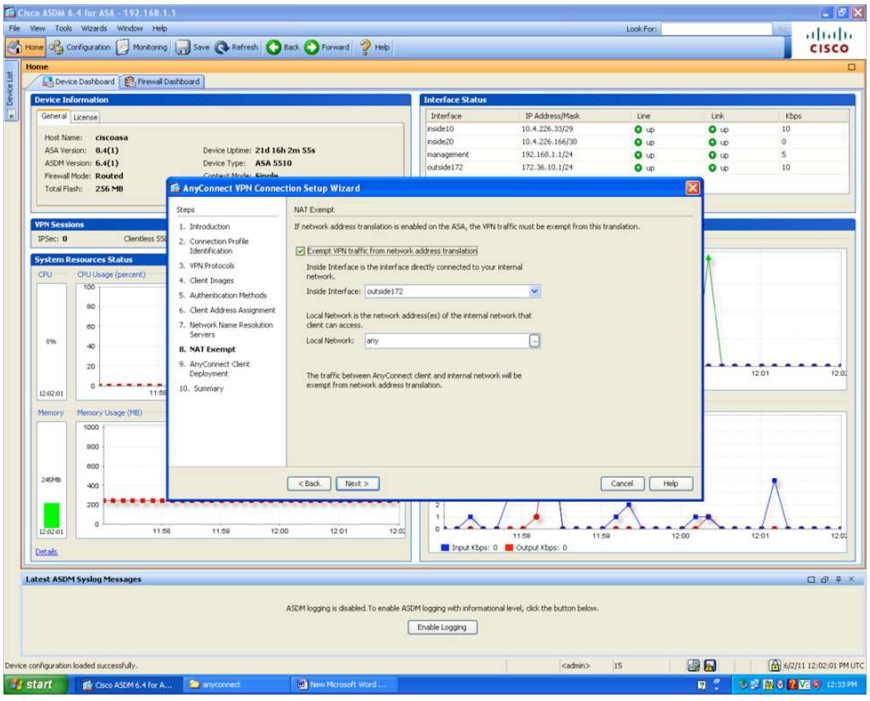
8. Specify server names and domains (Figure 10).

Figure 10. Specifying Server Names and Domains

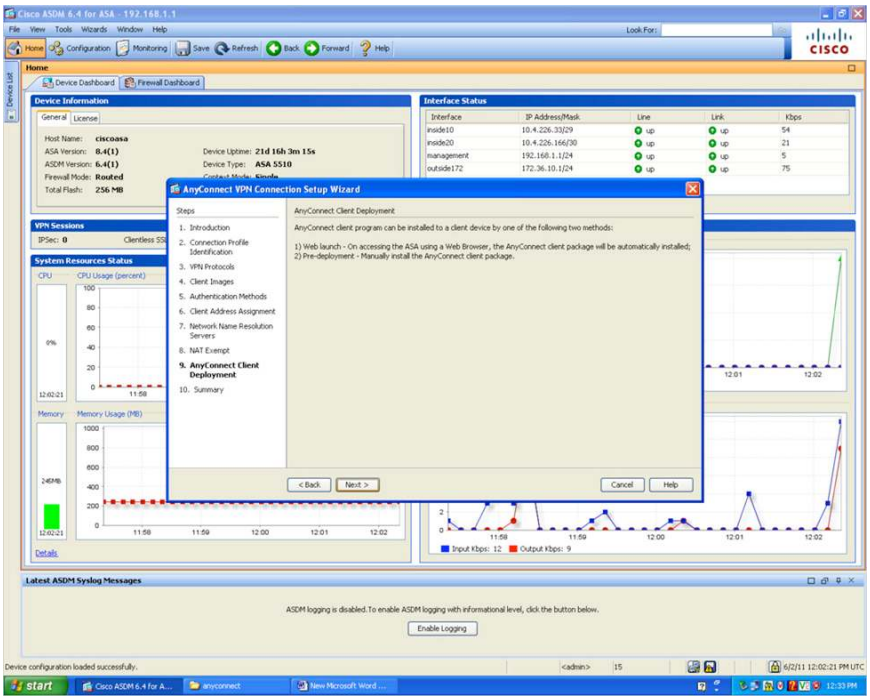


9. VPN traffic should be exempt from translations (Figure 11).

Figure 11. Exempting VPN Traffic from Translations

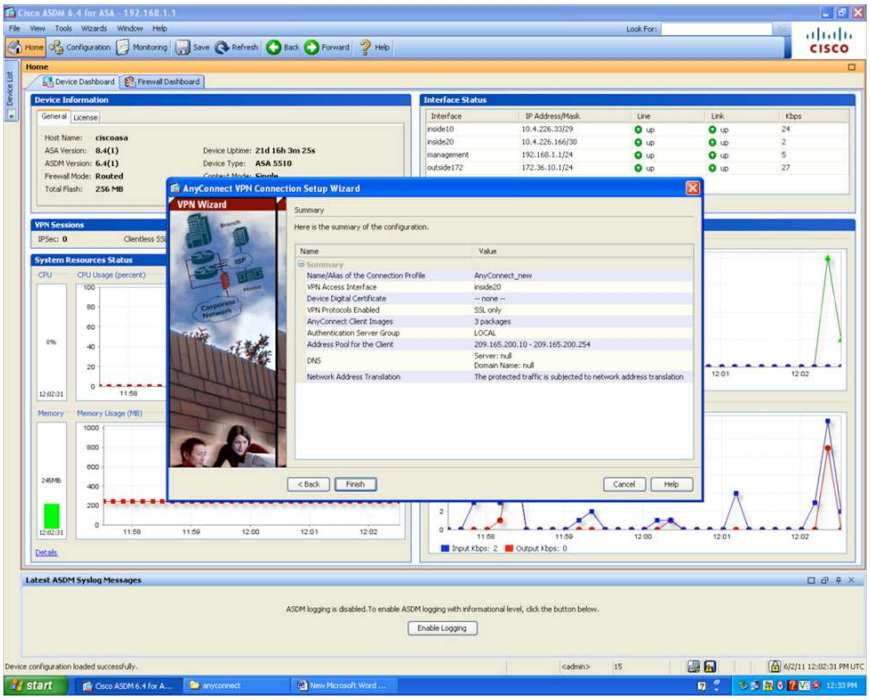


© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

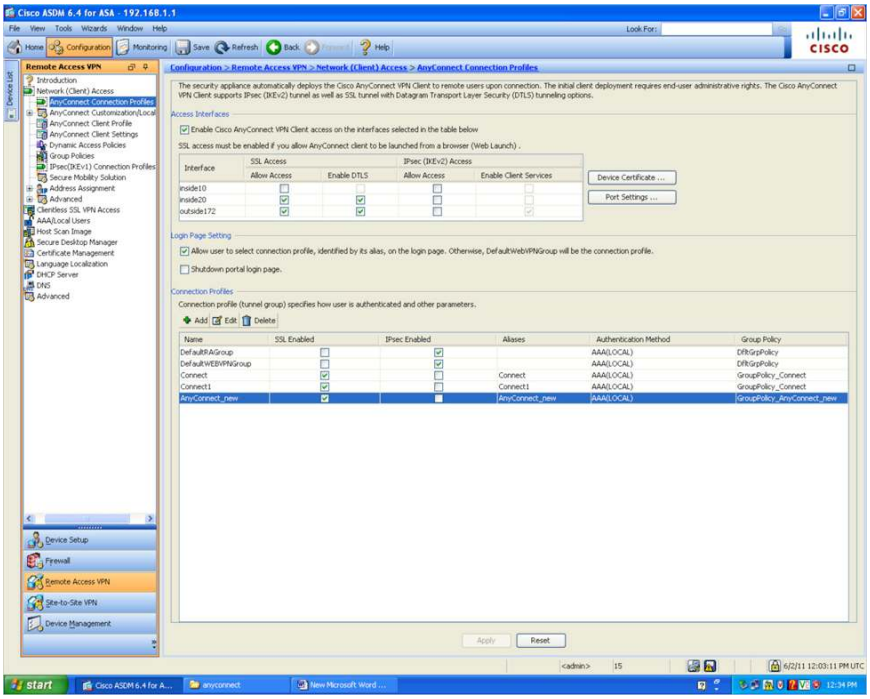


10. Verify the configured parameters and finish (Figure 12).

Figure 12. Verification and Finishing



© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.



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

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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:

```
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 2001::AC24:A65
ipv6 route 2001::AC24:A64/128 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
```

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 C07-683958-00 10/11

© 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.