White Paper

Cisco Mobile VPN—Enabling Cisco End-Device Based IP Mobility

Last Updated: February 2006

Cisco Mobile VPN is a new addition to the Cisco IOS IP Mobility solution that enables seamless and secure mobility for an end-device, such as a laptop or tablet PC. The solution allows a user to leverage various wireless and wired connections (WiFi, cellular data wireless, Ethernet, etc.) to remote access an organizational intranet anywhere, anytime in a secure and seamless manner. The solution offers its secure and seamless mobility by combining both the Cisco VPN technology and the Cisco IOS IP Mobility technology.

The Cisco IOS IP Mobility technology in the solution consists of the Cisco IOS Home Agent and the Windows-based Cisco Mobile Client. Together, they provide an uninterrupted application and service experience to end users while they are on the road, switch between access technologies, or across different IP networks-either private or public networks. The Cisco Mobile Client also offers an intelligent connection management function for end users. The function automatically selects the best interface based on either the administrative configured policy or the interface bandwidth. Additionally, it can perform the selection based on the WLAN signal strength. All of these actions are transparent from the users to offer a “seamless user experience”.

The Cisco VPN technology in the solution consists of the industry leading Cisco VPN client and Cisco IOS VPN gateway or Cisco VPN concentrators. Together with the Cisco IOS IP Mobility technology, the solution prevents a secure VPN connection from being disconnected when a user is on the move. As a result, the user does not need to restart and re-authenticate their VPN connection, as well as the intranet applications running on top of the VPN connection. This effectively improves the efficiency and productivity of a remote mobile worker while the security of corporate mobile traffic is protected.

CISCO IP MOBILITY TECHNOLOGY

The Cisco IOS IP Mobility technology in the solution consists of the Cisco IOS Home Agent and the Windows-based Cisco Mobile Client.

Cisco Mobile Client Overview

The Cisco Mobile client is complementary to other mobile solutions offered by Cisco as it extends mobility to end devices, such as laptops. This is particularly useful when the end devices roam outside of the area where mobility is currently served by a specific access router, for example by a Cisco Mobile Access Router.

The Cisco Mobile Client software is available for Windows 2000 (Service Pack 2) and for Windows XP.

The Cisco Mobile Client has the ability to manage network profiles, including the ability to interact with external network profile management tools, such as Cisco ACU or Windows XP wireless connection manager. This enables precise control of the settings to be used.

The default roaming interface selection is based on the link bandwidth among all available network interfaces in a system. The higher bandwidth is preferred. For example, a 802.11b 11Mbps interface will be preferred over a CDMA 2000 144k interface when both are available. This selection scheme is able to be prioritized within the configuration. For example, selection schemes could include location, cost, service providers, SSID, time of day, stability of links, path latency, etc. There is also the ability to preclude specific interfaces from being selected. This flexibility ensures that the specific requirements of an individual deployment can be easily met.

The Cisco Mobile Client is also proactive in providing seamless connectivity. For example, when WLAN signal strength decreases below a first threshold, a PPP connection is established in order to be available in case the WLAN signal continues to degrade. If the signal drops below the second threshold, then the connection can be moved over from the WLAN to the PPP connection. This “make before brake” ability can allow applications to continue working uninterrupted as the user moves from location to location.

The Cisco Mobile client also supports Network Access Identifier (NAI) RFC2794.

With the increase in WLANs, WLAN hotspots and second and third generation cellular networks enabling mobile workers more opportunity to connect to their home network, it is clear that the client software for a mobile device is one of the key components in a practical Mobile VPN solution.

Home Agent

A Cisco Home Agent is a IOS router on the home network serving as the anchor point for communication with the Cisco Mobile Client (a mobile device using this configuration is referred to as a mobile node). A Home Agent tunnels packets from a remote device, called a correspondent node, to the roaming mobile node (a Cisco Mobile Client). It does this by creating the tunnel between the Home Agent and a reachable point for the mobile node in the foreign network.

A Home Agent creates a mobility binding table that maps the home IP address of a mobile node to the current care-of address that the mobile node is using. To ensure that a failure of the Home Agent will not result in the mobile session being lost, Cisco IOS Software supports the Home Agent redundancy feature. This feature is configurable if required.

Cisco IOS Home Agents also support accounting, which can be used to track usage. This feature tracks when a mobile node starts a new Mobile IP session, when it changes its point of attachment and when the Mobile IP session has ended.

Cisco IOS Home Agents support policy routing. This feature supports route maps on Mobile IP tunnels created at the home agent and traffic can be directed based on the traffic sources NAI RFC 2794.

For a more in depth view of the Mobile IP solutions, including foreign agents authentication methods, please review the links in the reference section of this document.

VPN CHALLENGE FOR USERS ON THE MOVE

Background

Mobile VPNs are at the forefront of business efficiency allowing employees to be a fully functioning member of the company network wherever their physical location requires them to be.

Mobile networks can utilize multiple access networks which may or may not belong to the users home network. Due to this ability to use third party or public access networks, security is a high priority for the VPN user.

IPsec based VPNs are a common and trusted method of securing traffic that traverses across public or untrusted networks, including the Internet or Wireless LAN (WLAN), to private networks. IPsec provides data security through a flexible suite of encryption and tunneling mechanisms that protect packet payloads.

When a VPN user (ie: easy VPN user) wants to connect to an internal network, the user starts VPN client software and authenticates via a username and password. Once the user is authenticated, an IPsec tunnel is built between the node of the user and an IPsec VPN gateway on the remote end. Traffic from the node of the user can now traverse through this IPsec protected tunnel to the internal networks.

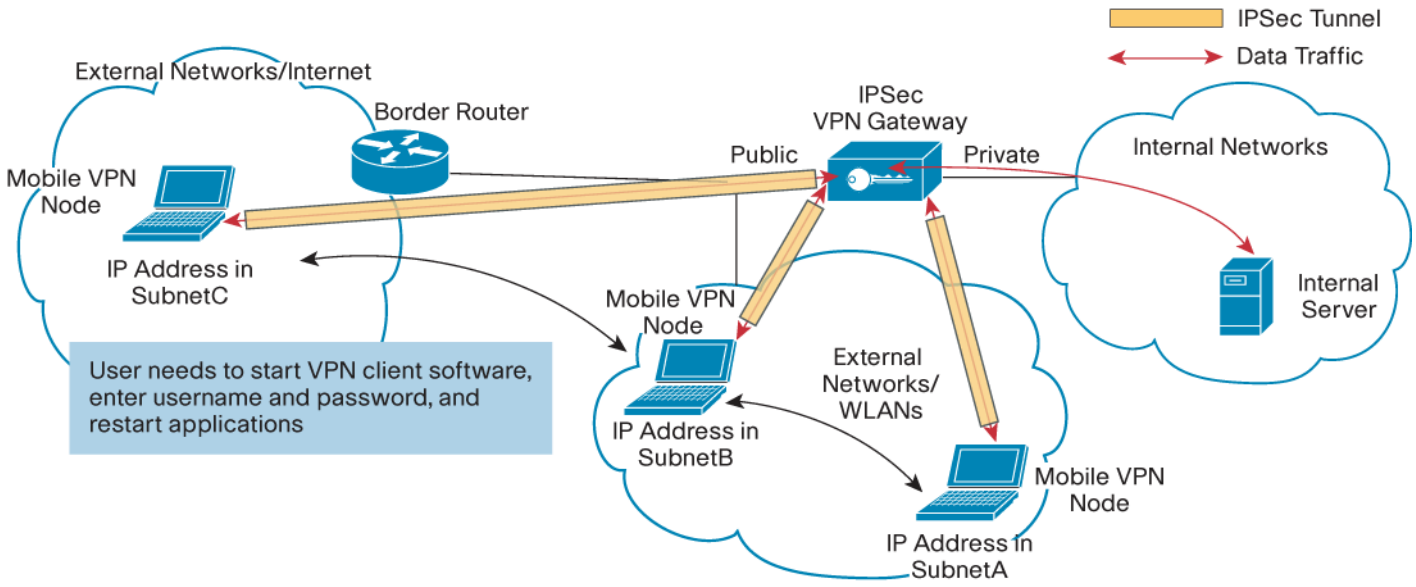
It is not uncommon for a VPN user to move from one place to the other. Law enforcement, military, corporate road warriors and transport employees are typical examples of mobile VPN users.

These types of network users constantly move between locations, and may gain network access from different network media, such as 802.11 WLAN, CDMA2000 1xRTT, and GPRS wireless data connections. This constant movement presents a challenge to the VPN users—how can they maintain uninterrupted VPN connectivity?

When VPN users change their geographic locations, their mobile VPN nodes are likely to cross a subnet boundary, this means their device needs to learn a new IP address (ie: via some dynamic IP addressing allocation mechanism, such as Dynamic Host Control Protocol (DHCP) or point-to-point protocol's IP control protocol).

This changing or relearning of an IP address can effect applications and data transfer. The change of IP address forces any existing secure IPsec tunnel to be terminated as the tunnel termination point—the old IP address—is no longer valid. To regain the IPsec connection, the users need to restart the VPN clients and re-authenticate with their usernames and passwords. If there are some applications that were running during the VPN tunnel reestablishing process, they can time-out and would need to be restarted. If the applications are actively transmitting or receiving traffic during this process, the traffic is dropped. These reestablishing tasks are tedious for the mobile VPN users, and unacceptable for the operation of a mission critical application.

Figure 1. VPN Tunnel Reestablishment after Movement



In Figure 1, the networks are divided into two sides, internal and external networks. The external network includes WLANs and the Internet. The mobile user creates an IPsec tunnel between its mobile VPN node (shown as a laptop) and the IPsec VPN gateway while it is in the external network. When the mobile VPN node moves between WLANs and the Internet, its IP address changes from the subnet A to B to C. As a result, the IPsec tunnel endpoint changes after each subnet crossing. To regain the IPsec session, the mobile VPN user restarts the VPN client and enters their username and password after each movement.

ADDRESSING THE CHALLENGE USING CISCO MOBILE VPN

Mobile IP can provide seamless IP connectivity for an IP node, while enabling mobility in the node. Mobility refers to the ability to move across IP subnets and change to different access media, such as the 802.11, CDMA2000 1xRTT, or GPRS wireless Internet connection.

Mobile IP achieves seamless IP connectivity by providing a **fixed IP address** to a mobile node, ensuring its routing reach-ability while the node is moving across different IP networks. This characteristic provides a solution to mobilize VPN that uses IPsec as it **eliminates the need to change the IPsec tunnel endpoint**, which is the IP address of the mobile node. The IPsec VPN tunnel can be maintained and the upper-layer application services are uninterrupted.

The following highlights the benefits of the Mobile VPN solution:

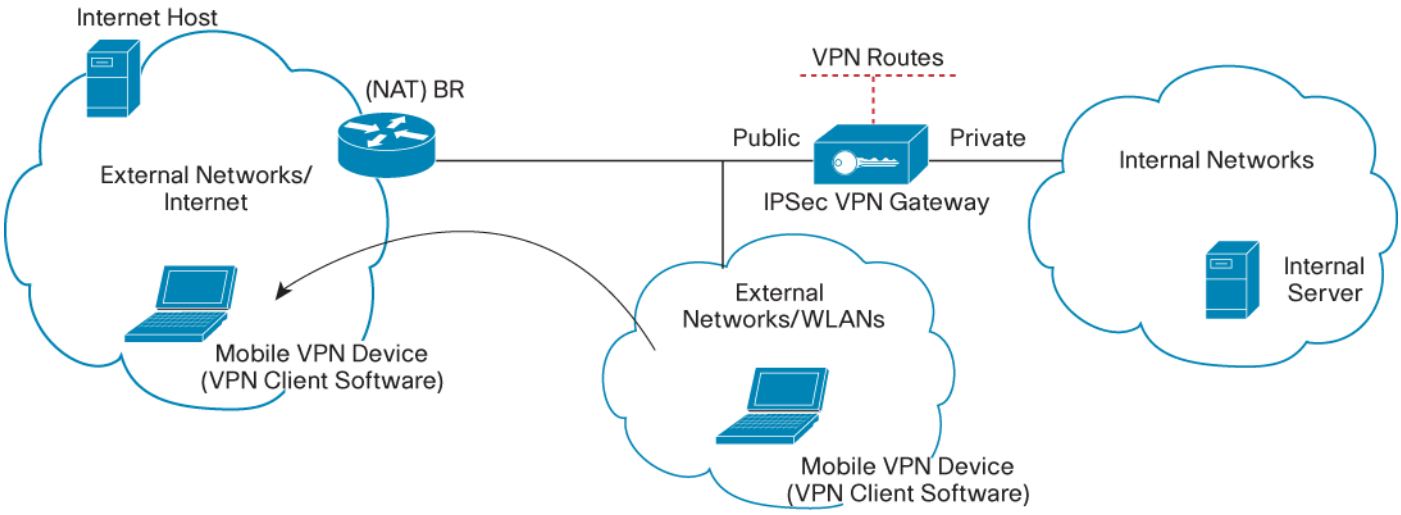
- Allow VPN users to enjoy mobility and maintain seamless IPsec VPN connections
- Simplify network administrative operations for VPN users
- Maintain mission critical application connectivity and services
- Extend IPsec security services to Mobile IP traffic

MOBILE VPN SOLUTION DETAILS

This section will detail the Mobile VPN solution by examining how Mobile IP and IPsec work together to provide mobility and security services. It will identify the components that are necessary to enable the solution. The solution is presumably built on existing VPN networks (Figure 2).

VPN Architecture Overview

Figure 2. VPN Architecture



In Figure 2, the Internet and WLANs are considered the external networks, to which a mobile VPN device can roam. When the mobile VPN node is in external networks, it needs to access internal networks using IPsec VPN. The IPsec VPN gateway is used as the IPsec VPN termination point for the mobile VPN node, and it is provisioned with the easy VPN service.

A Cisco VPN3000 series concentrator or a Cisco IOS Software based VPN router can exemplify a VPN gateway. VPN client software, such as Cisco VPN Client Software, is used by the mobile VPN node to initiate the IPsec VPN connection to the VPN gateway. Additionally, a Border Router (BR) is used to inter-face the Internet. The BR also provides the Network Address Translation (NAT) function for the traffic using a private IP address to access the Internet. For example, when the VPN route is in the range of a private IP address, traffic from a VPN user to the Internet would be NAT-ed by the BR.

Adding Mobility—Components and their Roles

Only two components are required enable a VPN architecture to support Mobile users:

- Home Agent (HA) router
- Mobile IP client software on mobile VPN nodes

Optionally, a Foreign Agent (FA) can be deployed for enhanced scalability and performance; however, this document assumes that FA is not deployed.

Any Cisco routers, from Cisco 1700 Series Routers to Cisco 7200 Series Routers, can be an HA router. For the Mobile IP Client Software, the example uses the Cisco Mobile Client software.

The main role of the HA component is to provide an anchor point for a mobile VPN node. Regardless of the location of the mobile VPN node, the rest of the networks would consider the node's location at a network* on the HA. This implies traffic destined to the node will be routed to the HA. Another responsibility of the HA is to forward the traffic to the current location of the node. HA accomplishes this by forwarding the traffic to a Mobile IP tunnel built between the node and itself.

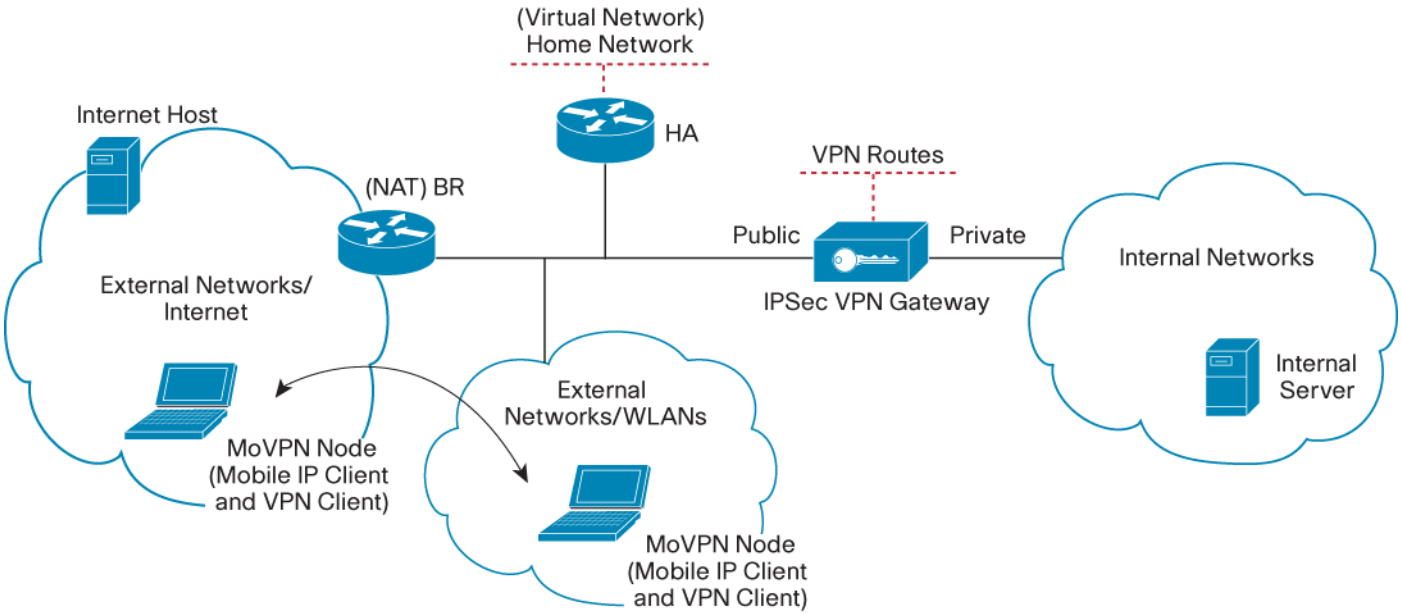
The main role of the Mobile IP client software component is to establish the Mobile IP tunnel used by the HA to forward the traffic to the node. When a Mobile IP client starts, it communicates with a HA to report/register its current physical location. This registration process creates a Mobile IP tunnel between the HA and the mobile VPN node. The end points of this tunnel are the HA address and the IP address that the node has acquired at its current subnet (Collocated Care-of-Address (CCoA). When the HA receives traffic destined to the mobile VPN node, it encapsulates the tunnel header and forwards the traffic to the remote end of the Mobile IP tunnel. Because the destination IP address of the tunnel header is the acquired IP address of the mobile node on its current subnet, the traffic is lead to the mobile VPN node.

This document will refer to a Mobile VPN node as a mobile VPN node with Mobile IP client software installed.

* The network on the HA is known as the home network of a mobile node. The home network is often referred to as the "virtual network" when the network is a logical interface on a HA

Figure 3 below shows the new network topology with Mobile IP components added to enable mobility.

Figure 3. A Mobile VPN Solution Topology Example

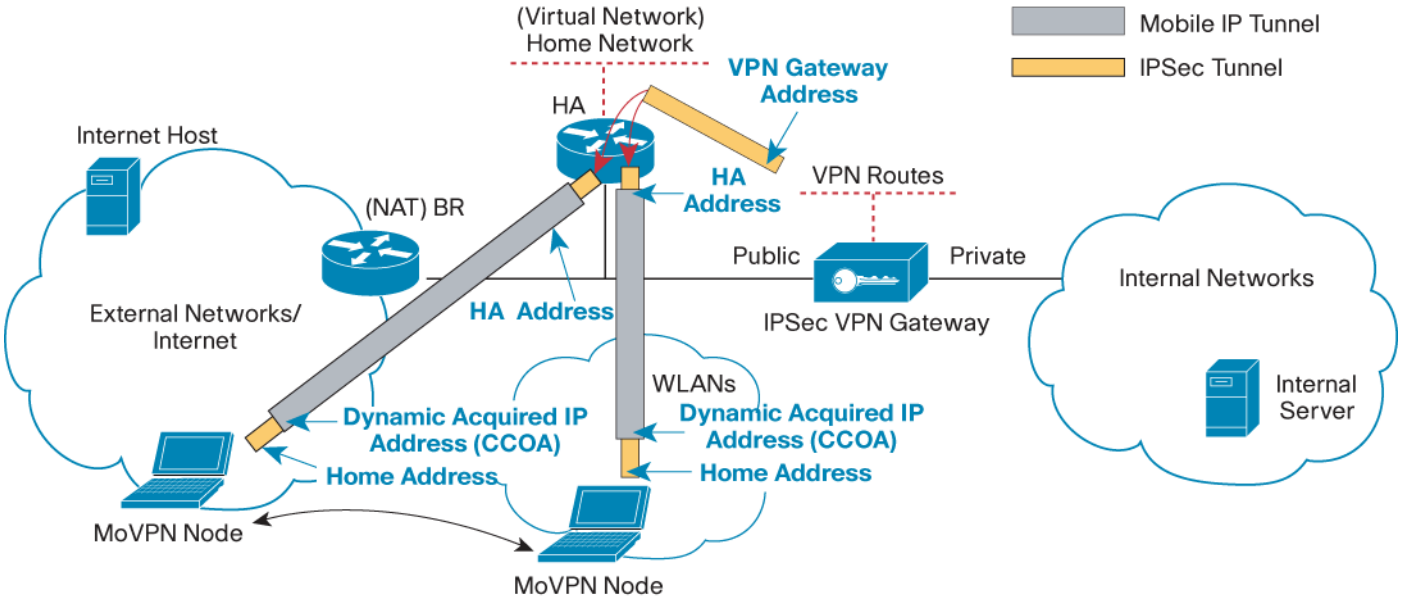


IPsec and Mobile IP Inter-Operation

As discussed in the previous section, the Mobile VPN node is considered logically located on the home network of the HA. When it initiates an IPsec tunnel, the tunnel is **logically** built between the node's home network and the node's IPsec VPN gateway. Because the HA knows the Mobile VPN node is **actually** located at the end of the Mobile IP tunnel, it extends the IPsec tunnel through the Mobile IP tunnel to the Mobile VPN node.

When the Mobile VPN node moves from one location to another (ie: from WLAN to Internet through CDMA2000 1xRTT), its Mobile IP client will register with the HA to report its new location. This triggers a new Mobile IP tunnel between the current location of the Mobile VPN node and the HA to be built, and the old Mobile IP tunnel to be tore down. Consequently, the HA extends the IPsec tunnel to the new Mobile IP tunnel that leads to the Mobile VPN node. The movement of the Mobile VPN node is transparent to the IPsec VPN gateway. From the VPN gateway perspective, the Mobile VPN node is always in its home network on HA. The IPsec tunnel endpoint never changes, and the tunnel is not disrupted. This effectively allows a Mobile VPN user to enjoy mobility while maintaining seamless secure VPN connectivity.

Figure 4. Mobile IP Tunnel and IPsec Tunnel Inter-Operation



In Figure 4, the thin orange tunnel represents an IPsec tunnel, and the wider gray tunnel represents a Mobile IP tunnel. The tunnel endpoints are labeled with their IP addresses.

Assume that the Mobile VPN node boots up in the WLANs area. The Mobile VPN node first acquires an IP address dynamically. The Mobile VPN node then enables the Mobile IP client software. This triggers a Mobile IP tunnel between the node in the WLAN and the HA to be built (shown as the grey tunnel). The tunnel endpoint IP addresses are the Mobile VPN node's dynamically acquired IP address and a pre-configured HA address.

The Mobile VPN node subsequently enables its VPN client. An IPsec tunnel is built between the Mobile VPN node and the IPsec VPN gateway. The endpoints for this IPsec tunnel are the home address of the Mobile VPN node and the IP address of the VPN gateway.

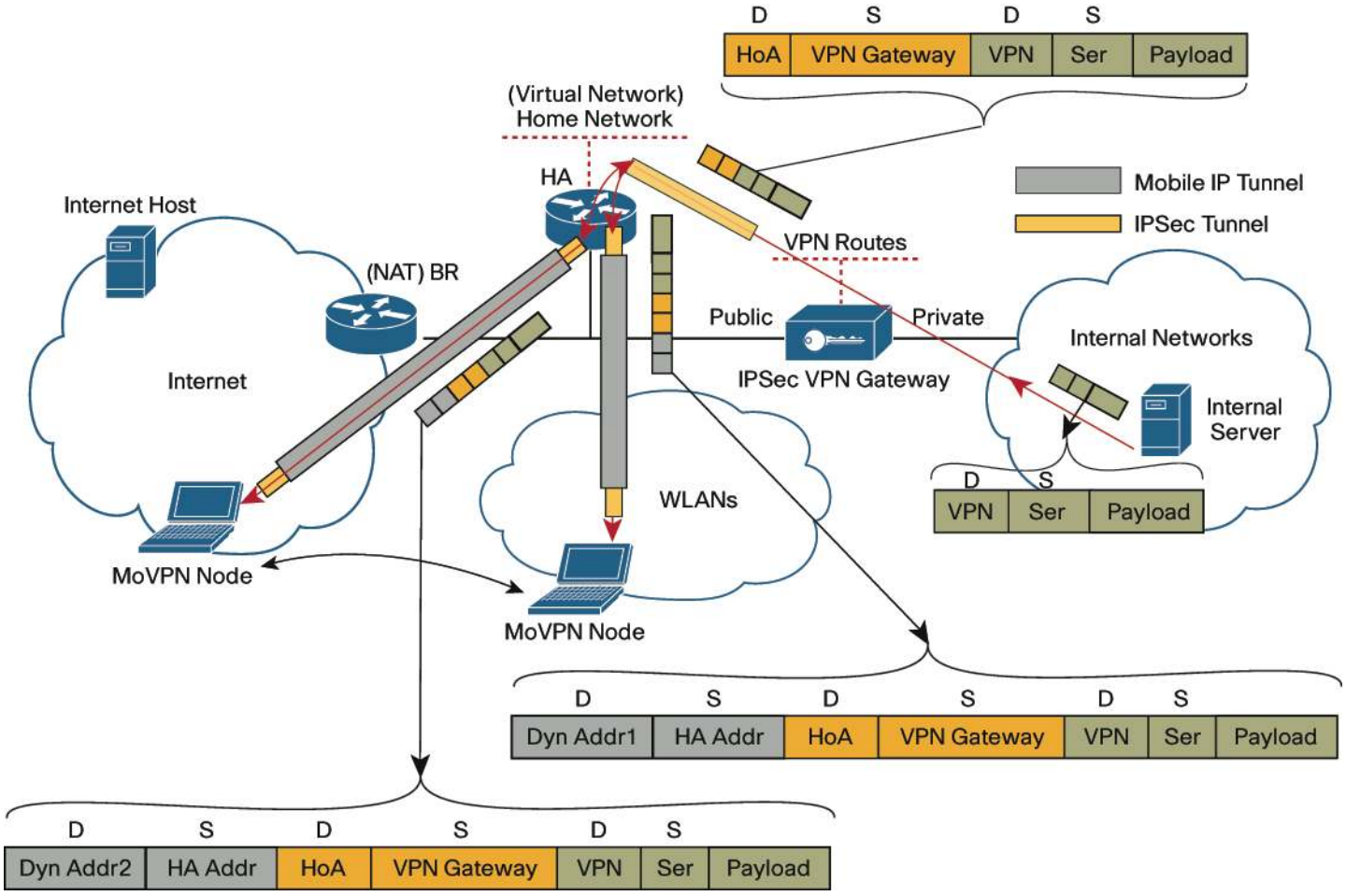
1. Top part between the VPN gateway and the HA: represents the IPsec tunnel from the VPN gateway perspective (as the VPN gateway assumes the Mobile VPN node is in the home network).
2. Lower part between the HA and the Mobile VPN node within a Mobile IP tunnel: represents the IPsec tunnel that is extended through the Mobile IP tunnel to reach the current location of the Mobile VPN node by the HA.

When the Mobile VPN node moves from the WLAN to the Internet, it acquires a new IP address on its new attached local subnet and builds a new Mobile IP tunnel. This new Mobile IP tunnel has a new endpoint on one side of the tunnel, which is a new dynamically acquired IP address used by the HA to identify the current location of the Mobile VPN node. The other side of the tunnel, the HA address, is unchanged. The HA now uses this new tunnel to direct the traffic destined for the home address of the Mobile VPN node. This effectively extends the original IPsec tunnel to the new location of the Mobile VPN node, as the IPsec tunnel endpoint is the home address of the Mobile VPN node. Thus, the IPsec tunnel is never torn down and the Mobile VPN service is uninterrupted.

Data Traffic Flow

This section will examine how the data traffic flows over the Mobile IP and IPsec tunnels.

Figure 5. Data Traffic Flow



When users send traffic from the internal server to the Mobile VPN node, the traffic has the server's IP address as the source IP address and the Mobile VPN node's VPN address as the destination IP address. From the perspective of the internal networks, the Mobile VPN node is located in the VPN gateway. This leads the traffic to the VPN gateway**. The VPN gateway then encrypts the traffic and adds the IPsec header. The IPsec header has the VPN gateway IP address as the source IP address, and the home address of the Mobile VPN node (HoA) as the destination IP address.

The VPN gateway looks up its routing table and forwards the traffic to the IPsec tunnel—the top part between the gateway and the HA specifically (from the VPN gateway perspective, the home address of the Mobile VPN node is located at the HA). The HA now has the traffic. Upon receiving the traffic, the HA looks up its routing table and finds that the Mobile VPN node is **actually** located on the end of a Mobile IP tunnel. The HA encapsulates the Mobile IP header with the HA address as the source IP address, and the dynamic IP address (acquired by the Mobile VPN node) as the destination IP address. It then forwards the traffic to the Mobile IP tunnel, leading the traffic to the Mobile VPN node. The Mobile VPN node decapsulates the Mobile IP header before it decrypts/decapsulates the IPsec packet. This process recovers the original IP packets from the internal server.

** The VPN gateway is advertised as the VPN route and uses the VPN route to assign an IP address to the Mobile VPN node.

When the Mobile VPN node moves to the Internet, the traffic flows in the previously mentioned manner. The difference is that the HA will encapsulate the traffic with the new Mobile IP tunnel header upon receiving the traffic from the VPN gateway. This new Mobile IP tunnel header has the new dynamically acquired IP address of the Mobile VPN node in the destination IP address; the traffic is sent to the new location of the Mobile VPN node. The node then performs the same decapsulation and decryption processes to recover the packets from the Internet server.

When the traffic flows from the Mobile VPN node to the internal network (if the Mobile IP Reverse Tunnel feature [RT] is enabled), it follows a similar process across the same path. The difference is that the sequence of encapsulation and encryption processes would be reversed.

Traffic flow between the Mobile VPN node and the Internet is also similar to the flow between the Mobile VPN node and the internal private networks. The main difference is that the VPN gateway will forward the traffic to the BR router, instead of forwarding the traffic to internal networks. The BR then performs NAT on the traffic if the VPN route is in the private IP address range.

Solution Summary

Today, many VPN users, including law enforcement, military, transport workers and corporate warriors, change their location constantly. This movement would present a challenge if their IPsec VPN connections are disrupted each time their movement crossed a subnet boundary.

To regain secure VPN connectivity, users would need to interrupt their work pattern to reestablish their secure connections after each change of subnet location. The reestablishment processes are tedious and ultimately disruptive for mobile workers and unacceptable for a mission critical application operation.

Cisco Mobile IP technology addresses this issue by providing a fixed IP address to the mobile VPN users as they move across the subnet boundary. Furthermore, it ensures the routing reachability of the fixed IP address to the VPN users. These two features allow the mobile VPN user to maintain a seamless secure VPN connection while they are in motion. As a result, this solution effectively eliminates the disruptive reestablishment processes and provides undisrupted application service for mission critical applications.

MOBILE VPN DEPLOYMENT AND CONFIGURATION EXAMPLE

Deployment and Configuration Example

Following are the highlights of the Mobile VPN solution deployment notes, based on the topology in this section:

- **HA addresses must be publicly accessible**

  This is required, so a Mobile VPN node can move to the public Internet while the HA is still reachable.

- **IPsec VPN gateway may need to permit UDP 1645 (for AAA authentication) for getting through its public interface (for both in and out directions)**

  This is an optional implementation, which would be necessary if HA retrieves the Mobile IP Security Associations (SA) of a Mobile VPN node from an AAA server. This is not required if the SA is configured on the HA or if the AAA server is located outside of the VPN gateway.

- **IPsec VPN gateway should inject VPN routes**

  This is to provide reachability of VPN routes. If the VPN gateway has already provided IPsec VPN service to Mobile VPN nodes, this is likely already enabled.

- **HA should redistribute Mobile VPN node's home networks into a routing protocol**

  Unless a static routing protocol is used, HA should advertise its home networks via a dynamic routing protocol. This ensures that the remainder of the networks can route the traffic to the home networks.

- **VPN routes can be in private address scope, given NAT is used**

  If the VPN gateway is using a private IP address pool to assign a Mobile VPN node an IP address and if the Mobile VPN node needs to reach the Internet, traffic from the Mobile VPN node would need to be NAT-ed to a public IP address.

- **Mobile IP Reverse tunnel feature needs to be enabled**

  This is necessary in order to bypass potential Reverse Path Forwarding (RPF) check, which is likely deployed on Internet Service Provider (ISP) networks.

- **Home networks may need to be NAT-ed when the home network is in the private IP address scope**

  If mobile users are allowed to enjoy mobility without enabling IPsec VPN while surfing the Internet, the home networks of the mobile users needs to be NAT-ed.

Operation Note:

- **Mobile VPN node needs to enable Mobile IP first and then IPsec**

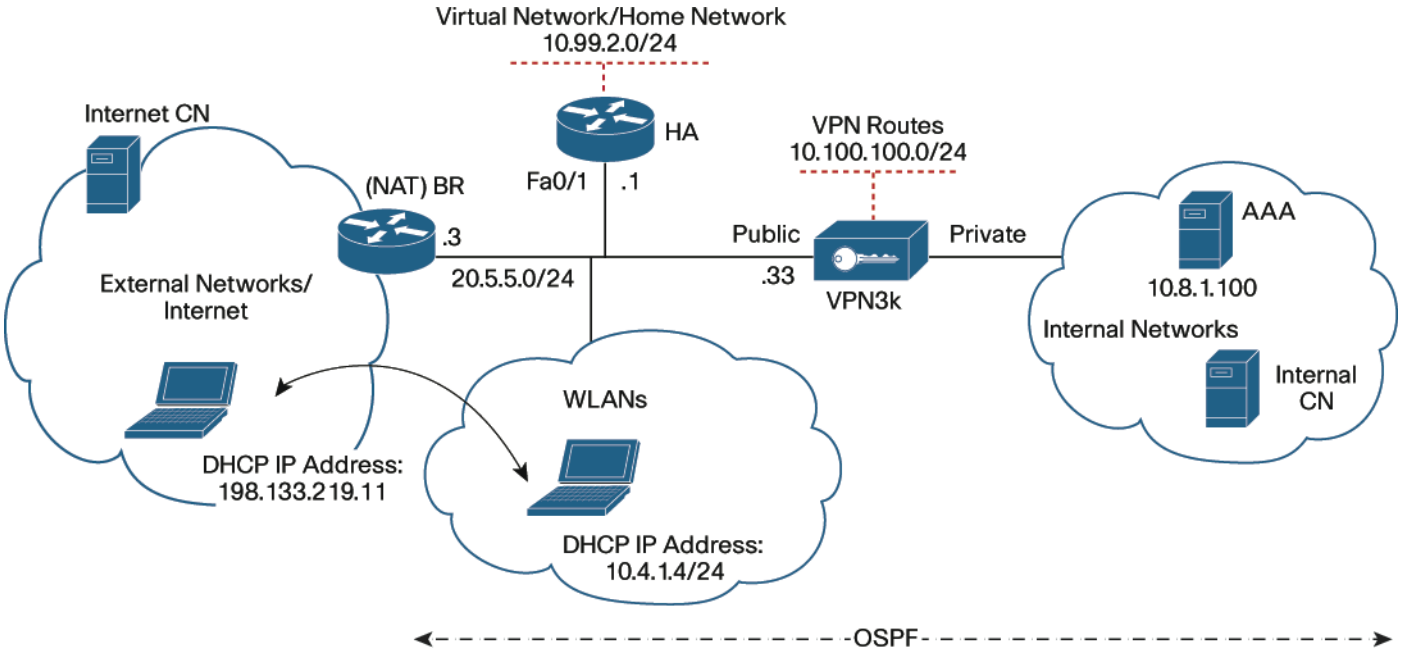
  This feature is needed because IPsec tunnels must run on top of Mobile IP tunnels in order to avoid changes in the IPsec tunnel endpoint.

Configuration Example

This section provides a configuration example for the Mobile IPsec VPN solution. The configuration example will be built based on the topology in the previous section. Assume that the IPsec VPN portion of the configurations has implemented already; therefore, this document will not show the IPsec VPN configurations.

Topology

Figure 6. The Mobile IP VPN Configuration Topology Example



Description

In the setup, the home network for Mobile VPN nodes is 10.99.2.0 with 24 bits for the subnet mask. The IP address—10.99.2.1—within the home network is the Mobile VPN node's home address. The home network will be redistributed into the OSPF routing protocol that is enabled on HA.

This document uses the IP address of the HA interface fa0/1 as the Mobile VPN node's HA address. This IP address is 20.5.5.1, which is publicly accessible. This ensures the reach-ability of the HA when our Mobile VPN node is roaming the Internet.

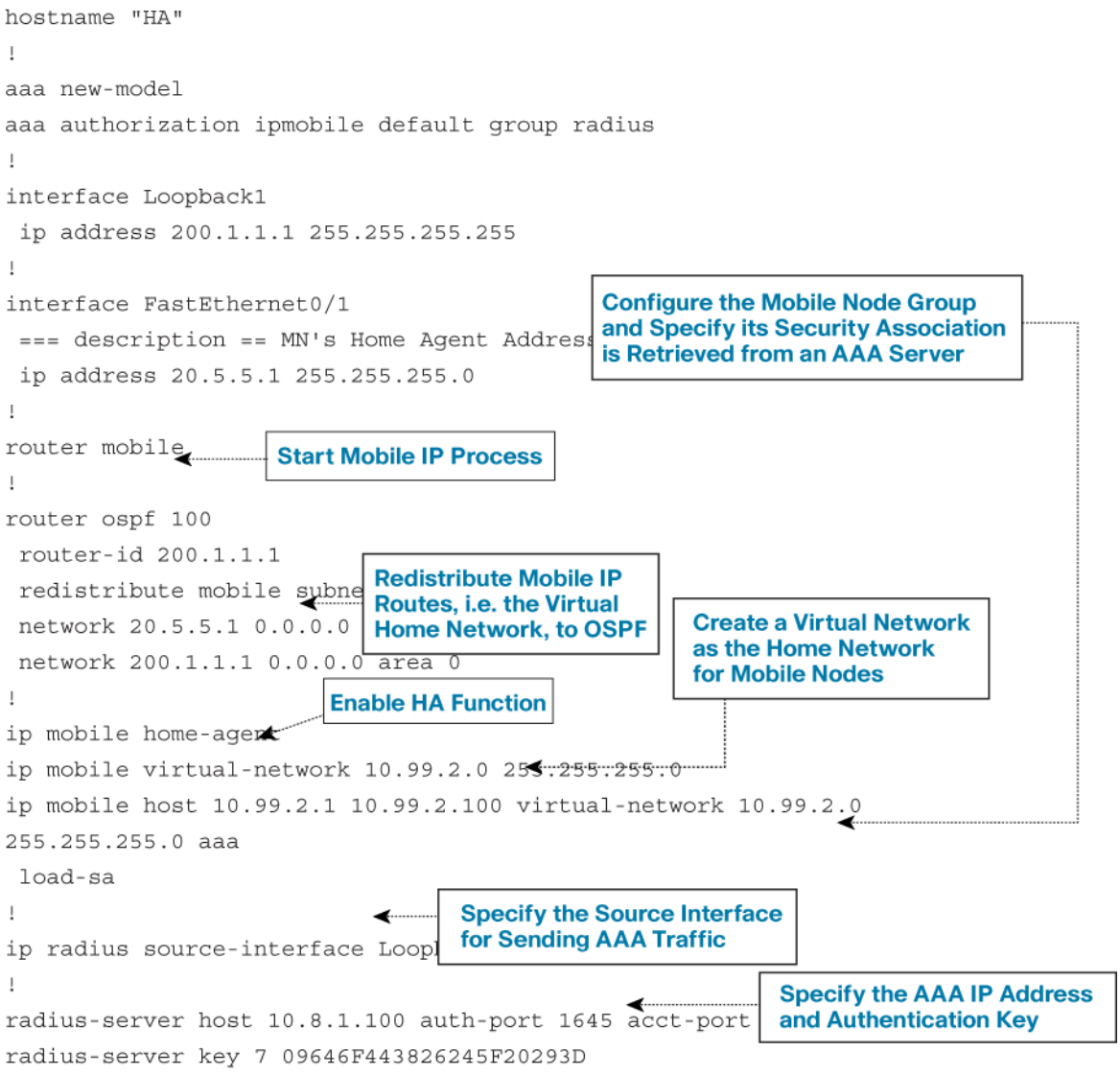
For authenticating Mobile IP Registration Requests (RRQ messages) from a Mobile VPN node, the HA is configured to query a AAA server to retrieve the Mobile VPN's Mobile IP SA. The AAA server is located inside the internal networks and has the IP address 10.8.1.100. As the AAA server is located in the internal networks, the authentication query messages and the reply messages (identified by UDP port 1645) must pass through the VPN3000 concentrator. The VPN3000 concentration must be configured to permit this.

OSPF routing protocol is presumably enabled in the internal networks. In addition, the VPN3000 concentrator and the BR router in the external networks also participate in the OSPF routing.

In this example, the VPN3000 concentrator has the easy VPN service configured for the Mobile VPN node. The VPN route assigning to the mobile VPN nodes is taken from the 10.100.100.0 subnet (with 24 bits for the subnet mask). The route is injected into the OSPF routing protocol in order to ensure the reach-ability of the VPN routes.

The VPN subnet is in the private IP address range, so NAT-ing (or PAT) is required for the Mobile VPN users to reach the Internet. The BR router provides this NAT-ing function. In addition, Mobile VPN users enjoy mobility while only accessing the Internet without using IPsec. Thus, it can be assumed that the BR router also provides the NAT-ing function for the Mobile VPN nodes' home networks.

Home Agent Configuration



Cisco Mobile Client Configuration

The Cisco Mobile Client can be configured either using a configuration file or via a GUI tool. In this example we will use the GUI tool.

A full description of all the configuration options is included in the Cisco Mobile Client user guide. Below are the steps to access the tool to begin configuration.

When CMC is used for the first time, you will be asked for a password. Please enter your choice of password. **NOTE:** This password will be required to activate any profile created.

Figure 7. Mobile Client

Right click the Cisco Mobile Client (CMC) icon in the taskbar on the monitor, and select **"Configure a Profile"**

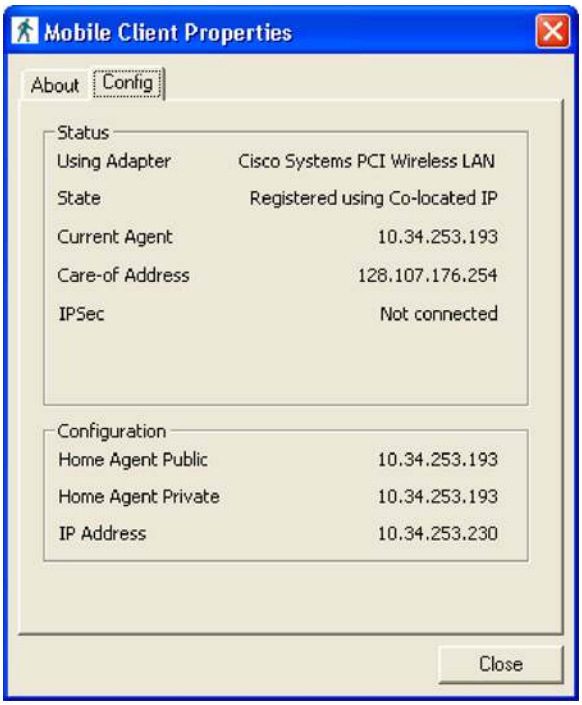
Figure 8. Cisco Mobile Client (CMC) Icon

Right click CMC and select **"Profiles…"**. Highlight the profile and hit **"Activate"**. You will be asked to enter the CMC password. The active profile shows in bold.

Figure 9. Mobile Client Profiles

To enable the CMC application, right click CMC and select **"Enable"**. The icon of CMC should show a change in state/color. Double click CMC and click on the **"Config"** tab and verify the status.

Figure 10. Mobile Client Properties



VPN3000 Configuration

Since the assumption is that the IPsec VPN service has already been deployed, the only additional necessary configuration is to permit the AAA authentication traffic to pass through the VPN3000 concentrator. To accomplish this, the VPN3000 configuration should be modified. In summary, the following two configuration tasks are needed:

- Adding rules to permit AAA authentication traffic (UDP port 1645)
- Assign rules to the public filter

Adding Rules to Permit AAA Authentication Traffic (UDP Port 1645)

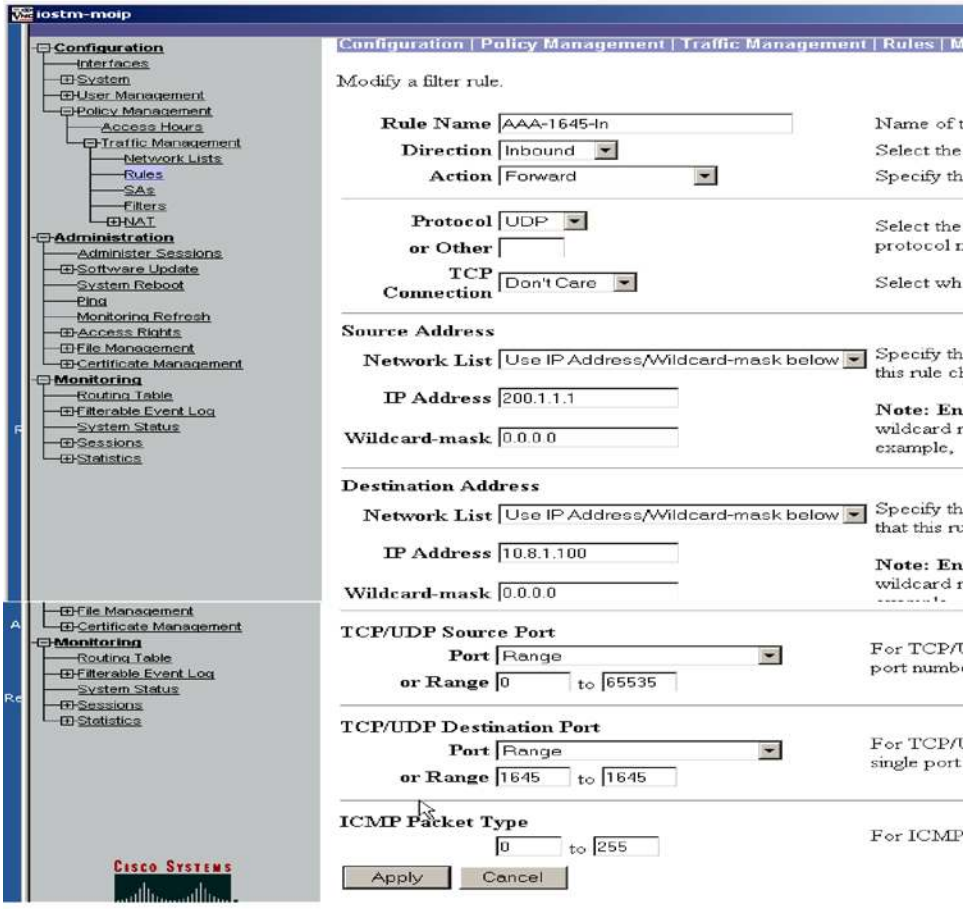
To configure the following rule:

Configuration>Policy Management>Traffic Management>Rules via the VPN Manager tool.

The rules, named “AAA-1645-In,” are defined in Figure 11. This permits AAA authentication traffic coming from the HA toward the AAA server to pass through the VPN3000 concentrator.

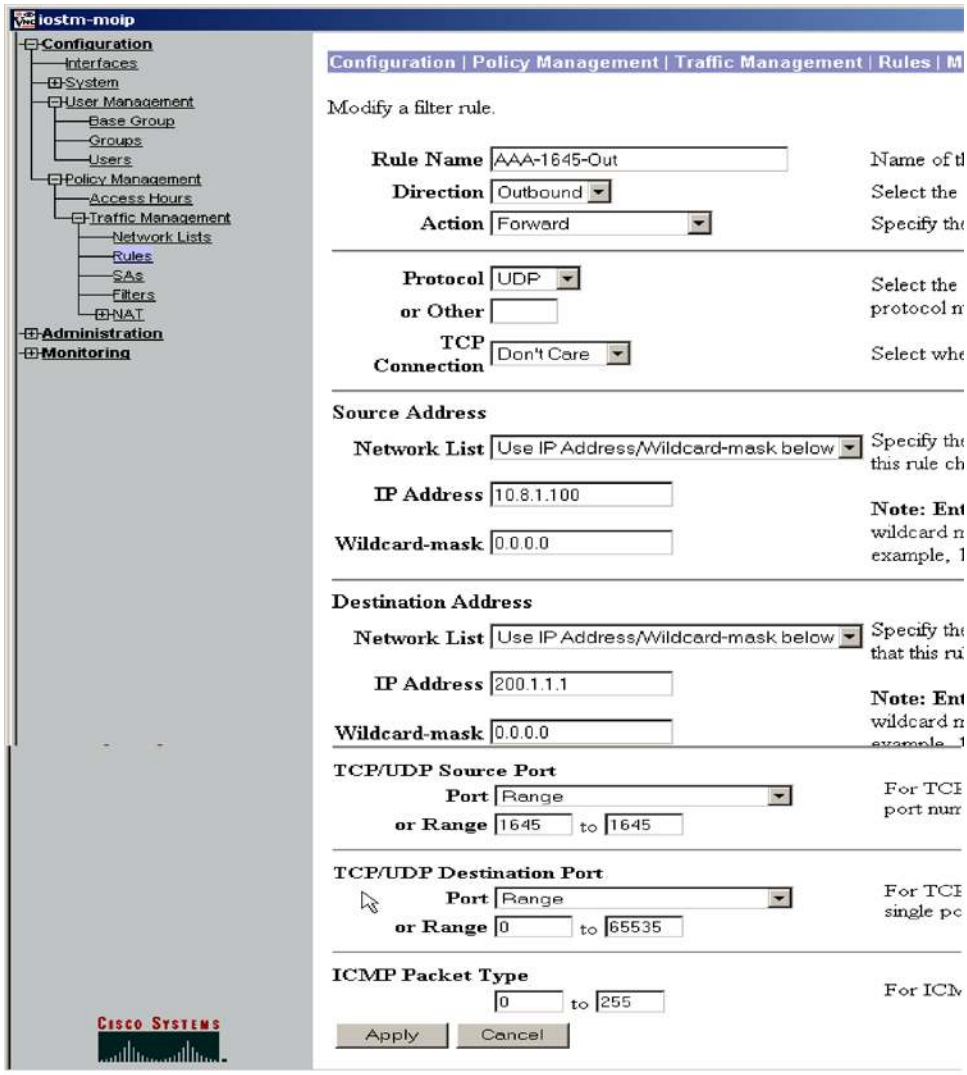
This is defined by specifying the source IP address and the source wildcard-mask with the 200.1.1.1 and 0.0.0.0 values respectively. It identifies the HA, and only the HA. To identify the AAA server, the destination IP address and the source wildcard-mask are configured with 10.8.1.100 and 0.0.0.0 respectively. Finally, to identify the AAA authentication traffic, the range of the destination port is configured with “1645 to 1645.”

Figure 11. Adding Rules to Permit AAA Authentication Traffic



The following rules, named “AAA-1645-Out,” permit the AAA authentication reply message in the other direction—from the AAA server to the HA. The source and destination IP addresses, masks, and UDP ports are the opposite of the previous direction.

Figure 12. AAA-1645-Out



Assign Rules to the Public Interface

To configure the following rule:

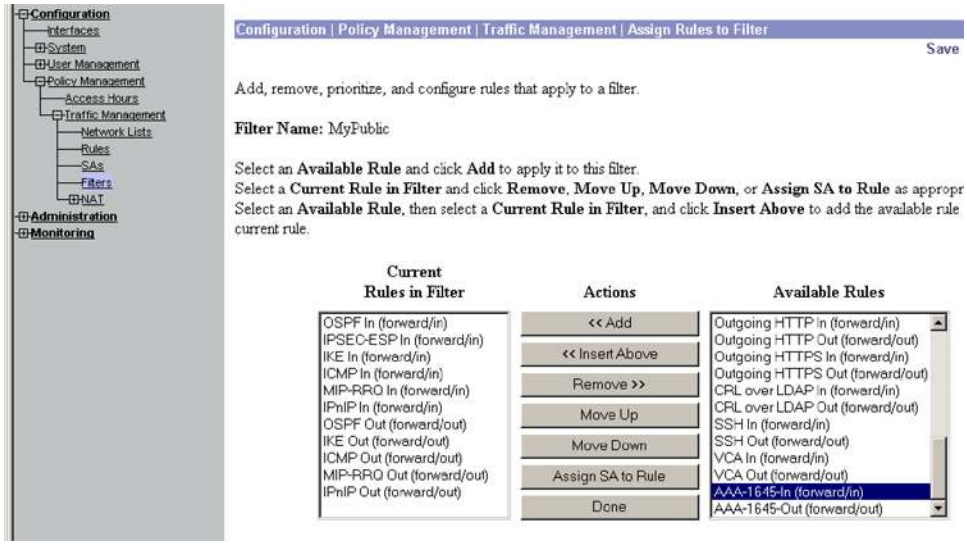
Configuration>Policy Management>Traffic Management>Filters via the VPN Manager tool

The following tasks assign the rules that were defined in the previous step to the filter that is applied to the public interface on the VPN3000 concentrator. The filter name in this example is “MyPublic.” To accomplish this, first select the proper filter—the “MyPublic” filter—and, then, click on the “Assign Rules to Filter” tab as shown below.

Figure 13. Assign Rules to the Public Interface

The next step is to add the two previous defined rules to the filter by selecting the “AAA-1645-In” rule and the “AAA-1645-Out” rule and clicking on the “<<Add” button.

Figure 14. Adding Rules to the Filter



The rules will be applied to the filter automatically after the above two steps.

Finally, the configuration may need to be saved, in order to keep the configuration after the VPN3000 is rebooted.

REFERENCE

Cisco Mobile IP White Paper [MIP]

http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800a4444.shtml

Introduction to Mobile IP

http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800c9906.shtml

Cisco IP Mobility Solution Quick Setup Guide for Registered CCO Users

http://www.cisco.com/cgi-bin/Software/Tablebuild/doftp.pl?ftpfile=cisco/wireless/mobile-client/1.0/CMC-Setup-Guide.doc&app=Tablebuild&status=showC2A

Mobile IP Command Reference 12.4T

http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a0080496feb.html

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA 205393.CB_ETMG_PI_2.06