Mobile IP Support for Foreign Agent Reverse Tunneling

The Mobile IP--Support for Foreign Agent Reverse Tunneling feature prevents packets sent by a mobile node from being discarded by routers configured with ingress filtering by creating a reverse tunnel between the foreign agent and the home agent.

Feature Specifications for Mobile IP--Support for FA Reverse Tunneling

Feature History	
Release	Modification
12.2(13)T	This feature was introduced.
Supported Platforms	
For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.	

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Mobile IP Support for FA Reverse Tunneling

- Cisco Express Forwarding (CEF) switching is currently not supported on a foreign agent with reverse tunneling enabled. With CEF switching enabled, a foreign agent will not encapsulate the FA-HA tunnel header on traffic received from a mobile node or a mobile router. To disable CEF on the foreign agent, use the **no ip cef** global configuration command.

Foreign agent reverse tunneling may adversely impact process switching and fast switching performance when Mobile IP is enabled because:

- All packets arriving at the foreign agent from an interface that has reverse tunneling enabled need to be checked to determine if they need to be reverse tunneled.
- At the home agent only IP packets that contain a source address from an authenticated mobile user are decapsulated and allowed to enter a corporate network.

Before enabling foreign agent reverse tunneling, you should be aware of the following security considerations:

- It is possible for any mobile node to insert packets with the source address of a registered user. Enabling reverse tunneling on a foreign agent can increase this existing security consideration because reverse tunneling provides a one-way path into a private network. You can prevent this problem by enforcing link-layer authentication before permitting link-layer access.

See the part "Authentication, Authorization, and Accounting (AAA)" in the Cisco IOS Security Configuration Guide, Release 12.2 *for more information, including instructions for configuring authentication.*

- If foreign agent reverse tunneling creates a tunnel that transverses a firewall, any mobile node that knows the addresses of the tunnel endpoints can insert packets into the tunnel from anywhere in the network. It is recommended to configure Internet Key Exchange (IKE) or IP Security (IPSec) to prevent this.

See the part "IP Security and Encryption" in the Cisco IOS Security Configuration Guide, Release 12.2 for more information, including instructions for configuring IKE and IPSec.

How to Enable Reverse Tunneling on a Foreign Agent

Enabling Foreign Agent Reverse Tunneling

The Cisco IOS implementation of foreign agent reverse tunneling is in the direct delivery style. In direct delivery, if the mobile node (a device such as a personal digital assistant that can change its point of attachment from one network to another) is using a foreign agent care-of address, it sends nonencapsulated packets to the foreign agent. The foreign agent detects the packets sent by the mobile node and encapsulates them before forwarding them to the home agent. If the mobile node is using a collocated care-of address, the foreign agent tunnels the unencapsulated packets directly to the home agent.

Perform this task to configure a foreign agent to provide default services, including reverse tunneling.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **ip mobile foreign-agent care-of** *interface*
5. **ip mobile foreign-agent reverse-tunnel private-address**
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **ip irdp**
9. **ip irdp maxadvertinterval** *seconds*
10. **ip irdp minadvertinterval** *seconds*
11. **ip irdp holdtime** *seconds*
12. **ip mobile foreign-service reverse-tunnel** [**mandatory**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 4	**ip mobile foreign-agent care-of** *interface* **Example:** `Router(config)# ip mobile foreign-agent care-of serial0`	Enables foreign agent services when at least one care-of address is configured. • This is the foreign network termination point of the tunnel between the foreign agent and home agent. The care-of address is the IP address of the interface. The interface, whether physical or loopback, need not be the same as the visited interface.

	Command or Action	Purpose
Step 5	**ip mobile foreign-agent reverse-tunnel private-address** **Example:** `Router(config)# ip mobile foreign-agent reverse-tunnel private-address`	Forces a mobile node with a private home address to register with reverse tunneling.
Step 6	**interface** *type number* **Example:** `Router(config)# interface serial0`	Configures an interface and enters interface configuration mode.
Step 7	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.0.1 255.255.255.255`	Sets a primary IP address of the interface.
Step 8	**ip irdp** **Example:** `Router(config-if)# ip irdp`	Enables ICMP Router Discovery Protocol (IRDP) processing on an interface.
Step 9	**ip irdp maxadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp maxadvertinterval 10`	(Optional) Specifies the maximum interval in seconds between advertisements.
Step 10	**ip irdp minadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp minadvertinterval 7`	(Optional) Specifies the minimum interval in seconds between advertisements.
Step 11	**ip irdp holdtime** *seconds* **Example:** `Router(config-if)# ip irdp holdtime 30`	(Optional) Length of time in seconds that advertisements are held valid. • Default is three times the **maxadvertinterval**period.
Step 12	**ip mobile foreign-service reverse-tunnel** [**mandatory**]	Enables foreign agent service on an interface. • Enables foreign agent reverse tunneling on the interface. This command also appends Mobile IP information such

	Command or Action	Purpose
	Example: `Router(config-if)# ip mobile foreign-service reverse-tunnel mandatory`	as care-of address, lifetime, and service flags to the advertisement.

Enabling Foreign Agent Reverse Tunneling on the Mobile Router

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **ip mobile router**
5. **address** *address mask*
6. **home-agent** *ip-address*
7. **reverse-tunnel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.

	Command or Action	Purpose
Step 4	**ip mobile router** **Example:** `Router(config)# ip mobile router`	Enables the Mobile Router and enters mobile router configuration mode.
Step 5	**address** *address mask* **Example:** `Router(mobile-router)# address 10.1.0.1 255.255.255.255`	Sets the home IP address and network mask of the mobile router.
Step 6	**home-agent** *ip-address* **Example:** `Router(mobile-router)# home-agent 10.1.1.1`	Specifies the home agent that the mobile router uses during registration.
Step 7	**reverse-tunnel** **Example:** `Router(mobile-router)# reverse-tunnel`	Enables the reverse tunnel function.

Verifying Foreign Agent Service Configuration

Perform this task to optionally verify that the interface has been configured to provide foreign agent services, including foreign agent reverse tunneling.

SUMMARY STEPS

1. **enable**
2. **show ip mobile globals**
3. **show ip mobile interface**
4. **show ip mobile traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip mobile globals** **Example:** `Router# show ip mobile globals`	(Optional) Displays global information for mobile agents.
Step 3	**show ip mobile interface** **Example:** `Router# show ip mobile interface`	(Optional) Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
Step 4	**show ip mobile traffic** **Example:** `Router# show ip mobile traffic`	(Optional) Displays protocol counters.

Additional References

The following sections provide additional references related to the Mobile IP--Support for FA Reverse Tunneling feature:

Related Documents

Related Topic	Document Title
Authentication	The part " Authentication, Authorization, and Accounting (AAA)" in the Cisco IOS Security Configuration Guide, Release 12.2
IKE and IPSec security protocols	The part " IP ISecurity and Encryption" in the Cisco IOS Security Configuration Guide, Release 12.2
Mobile IP	Introduction to Mobile IP
Cisco mobile networks	Cisco Mobile Networks
Mobile wireless configuration	Cisco IOS Mobile Wireless Configuration Guide, Release 12.2
Mobile wireless commands	Cisco IOS Mobile Wireless Command Reference, Release 12.2

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs[1]	MIBs Link
• RFC2006-MIB • CISCO-MOBILE-IP-MIB	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1 Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs[2]	Title
RFC 2002	IP Mobility Support
RFC 2003	IP Encapsulation within IP
RFC 2005	Applicability Statement for IP Mobility Support
RFC 2006	The Definitions of Managed Objects for IP Mobility Support

RFCs[2]	Title
RFC 3024	*Reverse Tunneling for Mobile IP, revised*

2 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **debug ip mobile**
- **ip mobile foreign-agent**
- **ip mobile foreign-service**
- **show ip mobile traffic**