



Real-Time Resolution for IPSec Tunnel Peer

After a user specifies a host name (instead of an IP address) for remote IP Security (IPSec) peer, the Real-Time Resolution for IPSec Tunnel Peer feature allows the host name to be domain name server (DNS) resolved before the router establishes the IPSec tunnel. Thus, the router can immediately discover whether the IP address of the peer has changed.

Feature History for Real-Time Resolution for IPSec Tunnel Peer

Release	Modification
12.3(4)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Real-Time Resolution for IPSec Tunnel Peer, page 2](#)
- [Information About Real-Time Resolution for IPSec Tunnel Peer, page 2](#)
- [How to Configure Real-Time Resolution, page 2](#)
- [Configuration Examples for Real-Time Resolution, page 4](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Restrictions for Real-Time Resolution for IPsec Tunnel Peer

Secure DNS Requirement

It is recommended that you use this feature only with secure DNS and when the DNS responses can be authenticated. Otherwise, an attacker can spoof or forge DNS responses and have access to Internet Key Exchange (IKE) authentication data, such as a certificate. If an attacker has a certificate that is trusted by the initiating host, the attacker can successfully establish Phase 1 IKE security association (SA), or the attacker can try to guess the preshared key that is shared between the initiator and the actual responder.

DNS Initiator

DNS names resolution for remote IPsec peers will work only if they are used as an initiator. The first packet that is to be encrypted will trigger a DNS lookup; after the DNS lookup is complete, subsequent packets will trigger IKE.

Information About Real-Time Resolution for IPsec Tunnel Peer

To configure real-time resolution for your IPsec peer, you should understand the following concept:

- [Benefits of Real-Time Resolution Via Secure DNS, page 2](#)

Benefits of Real-Time Resolution Via Secure DNS

When specifying the host name of a remote IPsec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the host name until right before the IPsec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the host name is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

DNS resolution assures users that their established IPsec tunnel is secure and authenticated.

How to Configure Real-Time Resolution

This section contains the following procedure:

- [Configuring Real-Time Resolution for IPsec Peers, page 2](#)

Configuring Real-Time Resolution for IPsec Peers

Use this task to configure a router to perform real-time DNS resolution with a remote IPsec peer; that is, the host name of peer is resolved via a DNS lookup right before the router establishes a connection (an IPsec tunnel) with the peer.

Prerequisites

Before creating a crypto map, you should perform the following tasks:

- Define Internet Security Association Key Management Protocol (ISAKMP) policies.
- Define IPSec transform sets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num ipsec-isakmp*
4. **match address** *access-list-id*
5. **set peer** {*host-name [dynamic] | ip-address*}
6. **set transform-set** *transform-set-name1 [transform-set-name2...transform-set-name6]*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num ipsec-isakmp</i> Example: Router(config)# crypto map secure_b 10 ipsec-isakmp	Specifies the crypto map entry to create (or modify) and enters crypto map configuration mode.
Step 4	match address <i>access-list-id</i> Example: Router(config-crypto-m)# match address 140	Names an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec in the context of this crypto map entry.

	Command or Action	Purpose
Step 5	<pre>set peer {host-name [dynamic] ip-address}</pre> <p>Example: Router(config-crypto-m)# set peer b.cisco.com dynamic</p>	<p>Specifies a remote IPsec peer.</p> <p>This is the peer to which IPsec-protected traffic can be forwarded.</p> <ul style="list-style-type: none"> dynamic—Allows the host name to be resolved via a DNS lookup just before the router establishes the IPsec tunnel with the remote peer. If this keyword is not specified, the host name will be resolved immediately after the host name is specified. <p>Repeat for multiple remote peers.</p>
Step 6	<pre>set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]</pre> <p>Example: Router(config-crypto-m)# set transform-set myset</p>	<p>Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).</p>

Troubleshooting Tips

To display crypto map configuration information, use the **show crypto map** command.

What to Do Next

You need to apply a crypto map set to each interface through which IPsec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association (SA) negotiation on behalf of traffic to be protected by crypto.

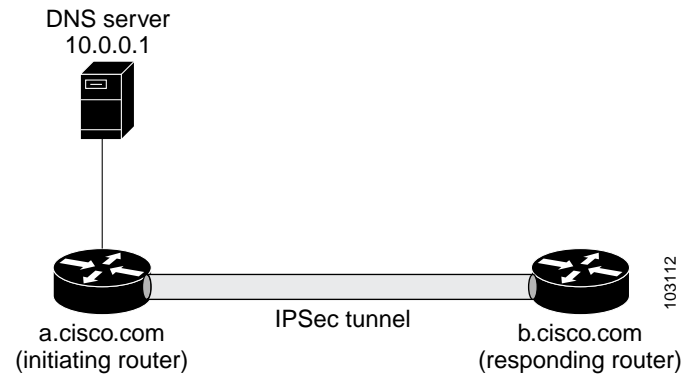
Configuration Examples for Real-Time Resolution

This section provides the following configuration example:

- [Configuring Real-Time Resolution for an IPsec Peer: Example, page 4](#)

Configuring Real-Time Resolution for an IPsec Peer: Example

[Figure 1](#) and the following example illustrate how to create a crypto map that configures the host name of a remote IPsec peer to DNS resolved via a DNS lookup right before the Cisco IOS software attempts to establish a connection with that peer.

Figure 1 Real-Time Resolution Sample Topology

```

! Configure the initiating router.
hostname a.cisco.com
ip domain name cisco.com
ip name server 10.0.0.1
!
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 30.0.0.1
  crypto map secure_b
access-list 140 permit ...
!
! Configure the responding router (the remote IPSec peer).
hostname b.cisco.com
!
crypto map secure_a 10 ipsec-isakmp
  match address 150
  set peer 30.0.0.1
  set transform-set
interface serial0/1
  ip address 40.0.0.1
  crypto map secure_a
access-list 150 ...

! DNS server configuration

b.cisco.com    40.0.0.1    # the address of serial0/1 of b.cisco.com

```

Additional References

The following sections provide references related to Real-Time Resolution for IPsec Tunnel Peer.

Related Documents

Related Topic	Document Title
Crypto maps	The chapter “Configuring IPsec Network Security” in the <i>Cisco IOS Security Configuration Guide</i>
ISAKMP policies	The chapter “Configuring Internet Key Exchange Security Protocol” in the <i>Cisco IOS Security Configuration Guide</i>
IPsec and IKE configuration commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

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, and tools. 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

This section documents the following modified command. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

- [set peer \(IPSec\)](#)

set peer (IPsec)

To specify an IP Security (IPsec) peer in a crypto map entry, use the **set peer** command in crypto map configuration mode. To remove an IPsec peer from a crypto map entry, use the **no** form of this command.

```
set peer {host-name [dynamic] | ip-address}
```

```
no set peer {host-name [dynamic] | ip-address}
```

Syntax Description

<i>host-name</i>	Specifies the IPsec peer by its host name. This is the peer's host name concatenated with its domain name (for example, myhost.example.com).
dynamic	(Optional) The host name of the IPsec peer will be resolved via a domain name server (DNS) lookup right before the router establishes the IPsec tunnel.
<i>ip-address</i>	Specifies the IPsec peer by its IP address.

Defaults

No peer is defined

Command Modes

Crypto map configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	The dynamic keyword was added.

Usage Guidelines

Use this command to specify an IPsec peer for a crypto map.

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used (because, in general, the peer is unknown).

For crypto map entries created with the **crypto map map-name seq-num ipsec-isakmp** command, you can specify multiple peers by repeating this command. The peer that packets are actually sent to is determined by the last peer that the router heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, Internet Key Exchange (IKE) tries the next peer on the crypto map list.

For crypto map entries created with the **crypto map map-name seq-num ipsec-manual** command, you can specify only one IPsec peer per crypto map. If you want to change the peer, you must first delete the old peer and then specify the new peer.

You can specify the remote IPsec peer by its host name only if the host name is mapped to the peer's IP address in a DNS or if you manually map the host name to the IP address with the **ip host** command.

The dynamic Keyword

When specifying the host name of a remote IPsec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the host name until right before the IPsec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the host name is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

Examples

The following example shows a crypto map configuration when IKE will be used to establish the security associations. In this example, a SA could be set up to either the IPsec peer at 10.0.0.1 or the peer at 10.0.0.2.

```
crypto map mymap 10 ipsec-isakmp
  match address 101
  set transform-set my_t_set1
  set peer 10.0.0.1
  set peer 10.0.0.2\
```

The following example shows how to configure a router to perform real-time DNS resolution with a remote IPsec peer; that is, the host name of peer is resolved via a DNS lookup right before the router establishes a connection (an IPsec tunnel) with the peer.

```
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 30.0.0.1
  crypto map secure_b
access-list 140 permit ...
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPsec SAs should be requested for each source/destination host pair.

Command	Description
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec SAs.
set session-key	Specifies the IPsec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.