



Ability to Disable Extended Authentication for Static IPSec Peers

Feature History

Release	Modification
12.2(4)T	This feature was introduced.

This feature module describes the Ability to Disable Extended Authentication for Static IPSec Peers feature in Cisco IOS Release 12.2(4)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 5](#)

Feature Overview

The Ability to Disable Extended Authentication for Static IPSec Peers feature allows users to disable extended authentication (Xauth), preventing the routers from being prompted for Xauth information—username and password.

Without the ability to disable Xauth, a user cannot select which peer on the same crypto map should use Xauth. That is, if a user has router-to-router IP security (IPSec) on the same crypto map as a virtual private network (VPN)-client-to-Cisco-IOS IPSec, both peers are prompted for a username and password. In addition, a remote static peer (a Cisco IOS router) cannot establish an Internet Key Exchange (IKE) security association (SA) with the local Cisco IOS router. (Xauth is not an optional exchange, so if a peer does not respond to an Xauth request, the IKE SA is deleted.) Thus, the same interface cannot be used to terminate IPSec to VPN clients (that need Xauth) as well as other Cisco IOS routers (that cannot respond to Xauth) unless this feature is implemented.

Benefits

If VPN-client-to-Cisco-IOS IPSec and router-to-router IPSec exist on a single interface, the Ability to Disable Extended Authentication for Static IPSec Peers feature allows a user to disable Xauth while configuring the preshared key for router-to-router IPSec. Thus, the router will not prompt the peer for a username and password, which are transmitted when Xauth occurs for VPN-client-to-Cisco-IOS IPSec.

Restrictions

Xauth can be disabled only if preshared keys are used as the authentication mechanism for the given crypto map.

Related Documents

- “Configuring Internet Key Exchange Security Protocol” chapter in the *Cisco IOS Security Configuration Guide*, Release 12.2.
- “Internet Key Exchange Security Protocol Commands” chapter in the *Cisco IOS Security Command Reference*, Release 12.2.

Supported Platforms

- Cisco 800 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 series
- Cisco 7200 series
- Cisco uBR905 Cable Access Router
- Cisco uBR925 Cable Access Router

Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, 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 at <http://www.cisco.com/register>.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

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>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Before you can disable Xauth for static IPSec peers, you must complete the following tasks:

- Configure authentication, authorization, and accounting (AAA).

For information on completing this task, refer to the AAA chapters of the *Cisco IOS Security Configuration Guide*, Release 12.2.



Note Configuring AAA is required only if the VPN-client-to-Cisco-IOS is using AAA authentication.

- Configure an IPSec transform.

For information on completing this task, refer to the section “Defining Transform Sets” in the chapter “Configuring IPSec Network Security” of the *Cisco IOS Security Configuration Guide*, Release 12.2.

- Configure a static crypto map.

For information on completing this task, refer to the section “Creating Crypto Map Entries” in the chapter “Configuring IPSec Network Security” of the *Cisco IOS Security Configuration Guide*, Release 12.2.

- Configure ISAKMP policy.

For information on completing this task, refer to the section “Creating Policies” in the chapter “Configuring Internet Key Exchange Security Protocol” of the *Cisco IOS Security Configuration Guide*, Release 12.2.

Configuration Tasks

See the following sections for configuration tasks for the Ability to Disable Extended Authentication for Static IPSec Peers feature. Each task in the list is identified as either required or optional.

- [Disabling Xauth for Static IPSec Peers](#) (required)
- [Verifying Disabled Xauth for Static IPSec Peers](#) (optional)

Disabling Xauth for Static IPSec Peers

To disable Xauth for router-to-router IPSec, use the following command in global configuration mode:

Command	Purpose
Router(config)# crypto isakmp key <i>keystring</i> address <i>peer-address</i> [<i>mask</i>] [no-xauth]	<p>Configures a preshared authentication key.</p> <p>Use the no-xauth keyword if router-to-router IPSec is on the same crypto map as VPN-client-to-Cisco IOS IPSec. This keyword prevents the router from prompting the peer for Xauth information.</p> <p>You must configure the local and remote peer for preshared keys.</p> <p>Note According to the design of preshared key authentication in IKE main mode, preshared keys <i>must</i> be based on the IP address of the peers. Although you can send hostname as the identity of preshared key authentication, the key is searched on the IP address of the peer; if the key is not found (based on the IP address) the negotiation will fail.</p>

Verifying Disabled Xauth for Static IPSec Peers

To verify your configuration, use the **show running-config** command in EXEC mode.

Configuration Examples

This section provides the following configuration example:

- [Disabling Xauth for Static IPSec Peers Configuration](#)

Disabling Xauth for Static IPSec Peers Configuration

The following example shows how the local peer specifies the preshared key, designates the remote peer by its IP address, and disables Xauth:

```
crypto isakmp key sharedkeystring address 172.21.230.33 no-xauth
```

Command Reference

This section documents the modified command. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

crypto isakmp key

To configure a preshared authentication key, use the **crypto isakmp key** command in global configuration mode. You must configure this key whenever you specify preshared keys in an Internet Key Exchange (IKE) policy. To delete a preshared authentication key, use the **no** form of this command.

crypto isakmp key *keystring* **address** *peer-address* [*mask*] [**no-xauth**]

no crypto isakmp key *keystring* **address** *peer-address*

Syntax Description

<i>keystring</i>	Specify the preshared key. Use any combination of alphanumeric characters up to 128 bytes. This preshared key must be identical at both peers.
address	Use this keyword if the remote peer Internet Security Association Key Management Protocol identity was set with its IP address.
<i>peer-address</i>	Specify the IP address of the remote peer.
<i>mask</i>	(Optional) Specify the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)
no-xauth	(Optional) Use this keyword if router-to-router IPSec is on the same crypto map as a Virtual Private Network (VPN)-client-to-Cisco-IOS IPSec. This keyword prevents the router from prompting the peer for extended authentication (Xauth) information (username and password).

Defaults

There is no default preshared authentication key.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1)T	The <i>mask</i> argument was added.
12.2(4)T	The no-xauth keyword was added.

Usage Guidelines

Use this command to configure preshared authentication keys. You must perform this command at both peers.

If an IKE policy includes preshared keys as the authentication method, these preshared keys must be configured at both peers—otherwise the policy cannot be used (the policy will not be submitted for matching by the IKE process). The **crypto isakmp key** command is the second task required to configure the preshared keys at the peers. (The first task is accomplished with the **crypto isakmp identity** command.)

Use the **address** keyword if the remote peer ISAKMP identity was set with its IP address.

With the **address** keyword, you can also use the *mask* argument to indicate the remote peer ISAKMP identity will be established using the preshared key only. If the *mask* argument is used, preshared keys are no longer restricted between two users.

**Note**

If you specify *mask*, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

Preshared keys no longer work when **hostname** is sent as the identity; thus, **hostname** as the identity in preshared key authentication is no longer supported. According to the way preshared key authentication is designed in IKE main mode, the preshared keys *must* be based on the IP address of the peers. Although a user can still send the hostname as identity in preshared key authentication, the key is searched on the IP address of the peer; if the key is not found (based on the IP address), the negotiation will fail.

If **crypto isakmp identity hostname** is configured as identity, the preshared key *must* be configured with the peer's IP address for the process to work.

Use the **no-xauth** keyword to prevent the router from prompting the peer for Xauth information (username and password). This keyword disables Xauth for static IPSec peers. **no-xauth** should be enabled when configuring the preshared key for router-to-router IPSec—not VPN-client-to-Cisco-IOS IPSec.

Examples

In the following example, the remote peer “RemoteRouter” specifies an ISAKMP identity by address:

```
crypto isakmp identity address
```

Now, the preshared key must be specified at each peer.

In the following example, the local peer specifies the preshared key and designates the remote peer by its IP address and a mask:

```
crypto isakmp key sharedkeystring address 172.21.230.33 255.255.255.255
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp identity	Defines the identity the router uses when participating in the IKE protocol.
ip host	Defines a static host name-to-address mapping in the host cache.

■ crypto isakmp key