Ability to Disable Extended Authentication for Static IPsec Peers

Last Updated: October 20, 2011

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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.

Feature Overview

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 for IPsec VPNs" chapter in the *Cisco IOS Security Configuration Guide: Secure Connectivity*
- "Configuring Security for VPNs with IPsec" chapter in the *Cisco IOS Security Configuration Guide: Secure Connectivity*
- *Cisco IOS Security Command Reference*

Supported Standards MIBs and RFCs

Standards

None

MIBs

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

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:

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

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

- Configure an IPsec transform.
- Configure a static crypto map.
- Configure ISAKMP policy.

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, page 3
- Disabling Xauth for Static IPsec Peers, page 3

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 keystring address peer-address [mask] [no-xauth]`	Configures a preshared authentication key. 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. You must configure the local and remote peer for preshared keys. **Note** According to the design of preshared key authentication in IKE main mode, preshared keys must 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.

Configuration Examples

- Disabling Xauth for Static IPsec Peers Configuration, page 4

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
```

Feature Information for Ability to Disable Xauth for Static IPsec Peers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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.

Table 1 Feature Information for Ability to Disable Xauth for Static IPsec Peers

Feature Name	Releases	Feature Information
Ability to Disable Extended Authentication for Static IPsec Peers	12.2(4)T	This feature allows users to disable Xauth, preventing the routers from being prompted for Xauth information. The following command was modified: **crypto isakmp key**.