Easy VPN Remote RSA Signature Support

The Easy VPN Remote RSA Signature Support feature provides support for the Rivest, Shamir, and Adleman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote devices.

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.

Prerequisites for Easy VPN Remote RSA Signature Support

- You must have a Cisco Virtual Private Network (VPN) remote device and be familiar with configuring the device.
- You must have a certification authority (CA) available to your network before you configure this interoperability feature. The CA must support the public key infrastructure (PKI) protocol of Cisco Systems, which is the Simple Certificate Enrollment Protocol (SCEP) (formerly called certificate enrollment protocol [CEP]).

- You should be familiar with IP Security (IPsec) and PKI and with configuring RSA key pairs and CAs.

Restrictions for Easy VPN Remote RSA Signature Support

- This feature should be configured only when you configure both IPsec and Internet Key Exchange (IKE) on your network.
- Easy VPN does not support RSA signature and preshared key authentication at the same time. A router can have one or more RSA signature-authenticated Easy VPN tunnels or preshared key-authenticated Easy VPN tunnels. However, only tunnels with the same authentication method are up at any time.
- Cisco IOS software does not support CA server public keys that are greater than 2048 bits.

Information About Easy VPN Remote RSA Signature Support

Easy VPN Remote RSA Signature Support Overview

The Easy VPN Remote RSA Signature Support feature allows you to configure RSA signatures on your Easy VPN remote device. The signatures can be stored on or off your remote device.

How to Configure Easy VPN Remote RSA Signature Support

Configuring Easy VPN Remote RSA Signature Support

To enable the RSA signatures, when you are configuring the Easy VPN remote and assigning the configuration to the outgoing interface, you must omit the **group** command. The content of the first Organizational Unit (OU) field will be used as the group. For information about configuring Cisco Easy VPN remote devices, refer to the Cisco Easy VPN Remote module.

Troubleshooting Easy VPN RSA Signature Support

To troubleshoot your Easy VPN remote RSA signature configuration, you can use the following **debug** commands. The **debug** commands can be used in any order or individually.

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto ipsec client ezvpn** **Example:** `Router# debug crypto ipsec client ezvpn`	Displays information about the VPN tunnel as it relates to the Easy VPN remote configuration.
Step 3	**debug crypto isakmp** **Example:** `Router# debug crypto isakmp`	Displays messages about IKE events.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	Cisco IOS Security Command Reference
Configuring Internet Key Exchange for IPsec VPNs	Configuring Internet Key Exchange for IPsec VPNs
Deploying RSA keys	Deploying RSA Keys Within a PKI
Certificate Authorities	• Easy VPN Server • Cisco IOS PKI Overview: Understanding and Planning a PKI • Deploying RSA Keys Within a PKI • Configuring Certificate Enrollment for a PKI
Configuring a Cisco Easy VPN remote device	Cisco Easy VPN Remote

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Easy VPN Remote RSA Signature Support

Table 1: Feature Information for Easy VPN Remote RSA Signature Support

Feature Name	Releases	Feature Information
Easy VPN Remote RSA Signature Support	12.3(7)T1 12.2(33)SRA 12.2(33)SXH	The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adleman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device. The following sections provide information about this feature: The following commands were introduced or modified: **debug crypto ipsec client ezvpn**, **debug crypto isakmp**.