IKE Responder-Only Mode

Last Updated: October 17, 2011

The IKE Responder-Only Mode feature provides support for controlling the initiation of Internet Key Exchange (IKE) negotiation and rekeying. When a device is configured as a responder-only device, it will not initiate IKE main, aggressive, or quick modes (for IKE and IP security [IPsec] security association [SA] establishment) nor will it rekey IKE and IPsec SAs. The device will respond to any negotiations initiated by its peers.

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.

Prerequisites for IKE Responder-Only Mode

- This feature is configurable only under an IPsec profile and is relevant only to a virtual interface scenario.

Restrictions for IKE Responder-Only Mode

- Neither static nor dynamic crypto maps are supported.

Information About IKE Responder-Only Mode

Benefits of the IKE Responder-Only Mode Feature

Since the advent of virtual private network (VPN) features that allow simultaneous bidirectional IKE negotiations (with or without interesting traffic), issues with the handling and recovery of data from duplicate IKE SAs have occurred. IKE as a protocol has no ability to compare IKE negotiations to determine whether there is already an existing or in-process negotiation between two peers taking place. These duplicate negotiations can be costly in terms of resources and confusing to router administrators. When a device is configured as a responder-only device, it will not initiate IKE main, aggressive, or quick modes (for IKE and IPsec SA establishment), nor will it rekey IKE and IPsec SAs, thus the likelihood of duplicate SAs is reduced.

The other benefit of this feature is to allow controlled support for negotiating connections in one direction only in a load-balancing scenario. It is not recommended that the servers or hubs initiate VPN connections toward the clients or spokes because these devices are all being accessed by a single-facing IP address as advertised via the load balancer. If the hubs were to initiate the connection, they would be doing so using an individual IP address, thus circumventing the benefits of the load balancer. The same is true of rekeying requests being sourced from the hubs or servers behind the load balancer.

This feature is particularly relevant in static virtual interfaces where events such as routing protocol convergence can generate simultaneous tunnel negotiations.

How to Configure IKE Responder-Only Mode

Configuring a Device As IKE Responder-Only

To configure your device as IKE responder-only, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **responder-only**

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 ipsec profile** *name* **Example:** `Router (config)# crypto ipsec profile vti`	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode.
Step 4	**responder-only** **Example:** `Router (ipsec-profile)# responder-only`	Configure a device as responder-only.

Configuration Examples for IKE Responder-Only Mode

The following example shows that a device has been configured as responder-only:

```
crypto ipsec profile vti
 set transform-set 3dessha
 set isakmp-profile clients
 responder-only
```

Additional References

The following sections provide references related to the IKE Responder-Only Mode feature.

Related Documents

Related Topic	Document Title
Security commands	*Cisco IOS Security Command Reference*

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IKE Responder-Only Mode

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 IKE Responder-Only Mode

Feature Name	Releases	Feature Information
IKE Responder-Only Mode	12.4(24)T	This feature provides support for controlling the initiation of IKE negotiation and rekeying. When a device is configured as a responder-only device, it will not initiate IKE main, aggressive, or quick modes (for IKE and IPsec SA establishment), nor will it rekey IKE and IPsec SAs. The device will respond to any negotiations initiated by its peers. The following command was introduced: **responder-only**.