IKE: Initiate Aggressive Mode

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the IKE: Initiate Aggressive Mode feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

Feature Overview

The IKE: Initiate Aggressive Mode feature allows you to configure Internet Key Exchange (IKE) preshared keys as RADIUS tunnel attributes for IP Security (IPSec) peers. Thus, you can scale your IKE preshared keys in a hub-and-spoke topology.

Although IKE preshared keys are simple to understand and easy to deploy, they do not scale well with an increasing number of users and are therefore prone to security threats. Instead of keeping your preshared keys on the hub router, this feature allows you to scale your preshared keys by storing and retrieving them from an authentication, authorization, and accounting (AAA) server. The preshared keys are stored in the AAA server as Internet Engineering Task Force (IETF) RADIUS tunnel attributes and are retrieved when a user tries to “speak” to the hub router. The hub router retrieves the preshared key from the AAA server and the spokes (the users) initiate aggressive mode to the hub by using the preshared key that is specified in the Internet Security Association Key Management Policy (ISAKMP) peer policy as a RADIUS tunnel attribute.

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

RADIUS Tunnel Attributes

To initiate an IKE aggressive mode negotiation, the Tunnel-Client-Endpoint (66) and Tunnel-Password (69) attributes must be configured in the ISAKMP peer policy. The Tunnel-Client-Endpoint attribute will be communicated to the server by encoding it in the appropriate IKE identity payload; the Tunnel-Password attribute will be used as the IKE preshared key for the aggressive mode negotiation.

Benefits

The IKE: Initiate Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes. This feature is best implemented in a crypto hub-and-spoke scenario, by which the spokes initiate IKE aggressive mode negotiation with the hub by using the preshared keys that are specified as tunnel attributes and stored on the AAA server. This scenario is scalable because the preshared keys are kept at a central repository (the AAA server) and more than one hub router and one application can use the information.

Restrictions

TED Restriction

This feature is not intended to be used with a dynamic crypto map that uses Tunnel Endpoint Discovery (TED) to initiate tunnel setup. TED is useful in configuring a full mesh setup, which requires an AAA server at each site to store the preshared keys for the peers; this configuration is not practical for use with this feature.

Tunnel-Client-Endpoint ID Types

Only the following ID types can be used in this feature:

- ID_IPV4 (IPV4 address)
- ID_FQDN (fully qualified domain name, for example “foo.cisco.com”)
- ID_USER_FQDN (e-mail address)

Related Documents

- *Cisco IOS Security Command Reference*

Supported Platforms

This feature runs on all platforms that support IPSec and public key infrastructure (PKI).

- Cisco 800 series
- Cisco 805
- Cisco 806
- Cisco 828
- Cisco 1400 series
- Cisco 1600 series

- Cisco 1600-R series
- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 1751
- Cisco 2400 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco 7700 series
- Cisco MC3810
- Route Processor Module (RPM)
- Universal Route Module (URM)

Determining Platform Support Through Cisco 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 Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco 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. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco 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.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

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

- RFC 2409, *The Internet Key Exchange*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Prerequisites

Before configuring the Initiate Aggressive Mode IKE feature, you must perform the following tasks:

- Configure AAA
- Configure an IPSec Transform
- Configure a Static Crypto Map
- Configure an ISAKMP Policy
- Configure a Dynamic Crypto Map

For information on completing these tasks, refer to the chapters "Configuring Authentication" and "Configuring Internet Key Exchange for IPsec VPN,"

Configuration Tasks

See the following sections for configuration tasks for the IKE: Initiate Aggressive Mode feature. Each task in the list is identified as either required or optional.

- Configuring RADIUS Tunnel Attributes (required)
- Verifying RADIUS Tunnel Attribute Configurations (optional)

Configuring RADIUS Tunnel Attributes

To configure the Tunnel-Client-Endpoint and Tunnel-Password attributes within the ISAKMP peer configuration, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto map map-name isakmp authorization list list-name`	Enables IKE querying of AAA for tunnel attributes in aggressive mode.
Step 2	`Router(config)# crypto isakmp peer {ip-address ip-address | fqdn fqdn}`	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode and enters ISAKMP policy configuration mode.
Step 3	`Router(config-isakmp)# set aggressive-mode client-endpoint client-endpoint`	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
Step 4	`Router(config-isakmp)# set aggressive-mode password password`	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

Verifying RADIUS Tunnel Attribute Configurations

To verify that the Tunnel-Client-Endpoint and Tunnel-Password attributes have been configured within the ISAKMP peer policy, use the **show running-config** global configuration command.

Troubleshooting Tips

To troubleshoot the IKE: Initiate Aggressive Mode feature, use the following debug commands in EXEC mode:

Command	Purpose
`Router# debug aaa authorization`	Displays information on AAA authorization.
`Router# debug crypto isakmp`	Displays messages about IKE events.
`Router# debug radius`	Displays information associated with the RADIUS.

Configuration Examples

This section provides the following configuration examples:

- Hub Configuration Example
- Spoke Configuration Example
- RADIUS User Profile Example

Hub Configuration Example

The following example shows how to configure a hub for a hub-and-spoke topology that supports aggressive mode using RADIUS tunnel attributes:

```
!The AAA configurations are as follows:
aaa new-model
aaa authorization network ike group radius
aaa authentication login default group radius
```

```
!
! The Radius configurations are as follows:
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key rad123
!
! The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPSec configurations are as follows:
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
!
crypto dynamic-map Dmap 10
 set transform-set trans1
!
crypto map Testtag isakmp authorization list ike
crypto map Testtag 10 ipsec-isakmp dynamic Dmap
!
interface Ethernet0
 ip address 4.4.4.1 255.255.255.0
 crypto map Testtag
!
interface Ethernet1
 ip address 2.2.2.1 255.255.255.0
```

Spoke Configuration Example

The following example shows how to configure a spoke for a hub-and-spoke topology that supports aggressive mode using RADIUS tunnel attributes:

```
!The IKE configurations are as follows:
crypto isakmp policy 1
 authentication pre-share
!
! The IPSec configurations are as follows:
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
 access-list 101 permit ip 3.3.3.0 0.0.0.255 2.2.2.0 0.0.0.255
!
! Initiate aggressive mode using Radius tunnel attributes
crypto isakmp peer address 4.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
!
crypto map Testtag 10 ipsec-isakmp
 set peer 4.4.4.1
 set transform-set trans1
 match address 101
!
interface Ethernet0
 ip address 5.5.5.1 255.255.255.0
 crypto map Testtag
!
interface Ethernet1
 ip address 3.3.3.1 255.255.255.0
```

RADIUS User Profile Example

The following is an example of a user profile on a RADIUS server that supports the Tunnel-Client-Endpoint and Tunnel-Password attributes:

```
user@cisco.com  Password = "cisco", Service-Type = Outbound
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Type = :1:ESP,
    Cisco:Avpair = "ipsec:tunnel-password=cisco123",
    Cisco:Avpair = "ipsec:key-exchange=ike"
```