IKE Initiate Aggressive Mode

The IKE: Initiate Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IP security (IPsec) peer and to initiate an Internet Key Exchange (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.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Prerequisites for IKE Initiate Aggressive Mode

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 Internet Security Association and Key Management Protocol (ISAKMP) policy
- Configure a dynamic crypto map

Restrictions for IKE Initiate Aggressive Mode

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)

Information About IKE Initiate Aggressive Mode

Overview

The IKE: Initiate Aggressive Mode feature allows you to configure IKE preshared keys as RADIUS tunnel attributes for 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.

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

How to Configure IKE Initiate Aggressive Mode

Configuring RADIUS Tunnel Attributes

To configure the Tunnel-Client-Endpoint and Tunnel-Password attributes within the ISAKMP peer configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **isakmp authorization list** *list-name*
4. **crypto isakmp peer** {**ip-address** *ip-address* | **fqdn** *fqdn*}
5. **set aggressive-mode client-endpoint** *client-endpoint*
6. **set aggressive-mode password** *password*

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 map** *map-name* **isakmp authorization list** *list-name* **Example:** `Router (config)# crypto map testmap10 isakmp authorization list list ike`	Enables IKE querying of AAA for tunnel attributes in aggressive mode.
Step 4	**crypto isakmp peer** {**ip-address** *ip-address* | **fqdn** *fqdn*} **Example:** `Router (config)# crypto isakmp peer ip address 10.10.10.1`	Enables an IPsec peer for IKE querying of AAA for tunnel attributes in aggressive mode and enters ISAKMP policy configuration mode.
Step 5	**set aggressive-mode client-endpoint** *client-endpoint* **Example:** `Router (config-isakmp)# set aggressive-mode client-endpoint user-fqdn user@cisco.com`	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.

	Command or Action	Purpose
Step 6	**set aggressive-mode password** *password* **Example:** `Router (config-isakmp)#set aggressive-mode password cisco123`	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, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **debug aaa authorization**
3. **debug crypto isakmp**
4. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays information about AAA authorization.
Step 3	**debug crypto isakmp** **Example:** `Router# debug crypto isakmp`	Displays messages about IKE events.
Step 4	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS.

Configuration Examples for IKE Initiate Aggressive Mode

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 10.1.1.1 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-aes 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 FastEthernet0
 ip address 10.4.4.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.2.2.1 255.255.255.0
```

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-aes esp-sha-hmac
 access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
!
! Initiate aggressive mode using Radius tunnel attributes
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
!
crypto map Testtag 10 ipsec-isakmp
 set peer 10.4.4.1
```

```
 set transform-set trans1
 match address 101
!
interface FastEthernet0
 ip address 10.5.5.1 255.255.255.0
 crypto map Testtag
!
interface FastEthernet1
 ip address 10.3.3.1 255.255.255.0
```

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"
```

Additional References

The following sections provide references related to the IKE: Initiate Aggressive Mode feature.

Related Documents

Related Topic	Document Title
Security commands	*Cisco IOS Security Command Reference*
Configuring authentication	Configuring Authentication
Configuring IKE	Configuring Internet Key Exchange for IPsec VPNs
Recommended cryptographic algorithms	Next Generation Encryption

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 XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

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/techsupport

Feature Information for IKE Initiate Aggressive 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: Initiate Aggressive Mode

Feature Name	Releases	Feature Information
IKE: Initiate Aggressive Mode	Cisco IOS XE Release 2.1	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. The following commands were introduced or modified: **crypto isakmp peer**, **set aggressive-mode client-endpoint**, **set aggressive-mode password**.