EIGRP/SAF HMAC-SHA-256 Authentication

The EIGRP/SAF HMAC-SHA-256 Authentication feature enables packets in an Enhanced Interior Gateway Routing Protocol (EIGRP) topology or a Service Advertisement Framework (SAF) domain to be authenticated using Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) message authentication codes. This module discusses this feature from an EIGRP perspective; it gives a brief overview of this feature and explains how to configure it.

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.

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.

Information About EIGRP/SAF HMAC-SHA-256 Authentication

EIGRP Neighbor Relationship Maintenance

Neighbor relationship maintenance is the process that devices use to dynamically learn of other devices on their directly attached networks. Devices must also discover when their neighbors become unreachable or inoperative. Neighbor relationship maintenance is achieved with low overhead by devices when they periodically send small hello packets to each other. As long as hello packets are received, the Cisco software can determine whether a neighbor is alive and functioning. After the status of the neighbor is determined, neighboring devices can exchange routing information.

The reliable transport protocol is responsible for the guaranteed, ordered delivery of Enhanced Interior Gateway Routing Protocol (EIGRP) packets to all neighbors. The reliable transport protocol supports intermixed transmission of multicast and unicast packets. Some EIGRP packets (such as updates) must be sent reliably; this means that the packets require acknowledgment from the destination. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities, hello packets need not be sent reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello packet with an indication in the packet informing receivers that the packet need not be acknowledged. The reliable transport protocol can send multicast packets quickly when unacknowledged packets are pending, thereby ensuring that the convergence time remains low in the presence of varying speed links.

Some EIGRP remote unicast-listen (any neighbor that uses unicast to communicate) and remote multicast-group neighbors may peer with any device that sends a valid hello packet, thus causing security concerns. By authenticating the packets that are exchanged between neighbors, you can ensure that a device accepts packets only from devices that know the preshared authentication key.

HMAC-SHA-256 Authentication

Packets exchanged between neighbors must be authenticated to ensure that a device accepts packets only from devices that have the same preshared authentication key. Enhanced Interior Gateway Routing Protocol (EIGRP) authentication is configurable on a per-interface basis; this means that packets exchanged between neighbors connected through an interface are authenticated. EIGRP supports message digest algorithm 5 (MD5) authentication to prevent the introduction of unauthorized information from unapproved sources. MD5 authentication is defined in RFC 1321. EIGRP also supports the Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication method. When you use the HMAC-SHA-256 authentication method, a shared secret key is configured on all devices attached to a common network. For each packet, the key is used to generate and verify a message digest that gets added to the packet. The message digest is a one-way function of the packet and the secret key. For more information on HMAC-SHA-256 authentication, see FIPS PUB 180-2, SECURE HASH STANDARD (SHS), for the SHA-256 algorithm and RFC 2104 for the HMAC algorithm.

If HMAC-SHA-256 authentication is configured in an EIGRP network, EIGRP packets will be authenticated using HMAC-SHA-256 message authentication codes. The HMAC algorithm takes as input the data to be authenticated (that is, the EIGRP packet) and a shared secret key that is known to both the sender and the receiver; the algorithm gives a 256-bit hash output that is used for authentication. If the hash value provided by the sender matches the hash value calculated by the receiver, the packet is accepted by the receiver; otherwise, the packet is discarded.

Typically, the shared secret key is configured to be identical between the sender and the receiver. To protect against packet replay attacks because of a spoofed source address, the shared secret key for a packet is defined as the concatenation of the user-configured shared secret (identical across all devices participating in the authenticated domain) with the IPv4 or IPv6 address (which is unique for each device) from which the packet is sent.

The device sending a packet calculates the hash to be sent based on the following:

- Key part 1—the configured shared secret.
- Key part 2—the local interface address from which the packet will be sent.
- Data—the EIGRP packet to be sent (prior to the addition of the IP header).

The device receiving the packet calculates the hash for verification based on the following:

- Key part 1—the configured shared secret.

- Key part 2—the IPv4 or IPv6 source address in the IPv4 or IPv6 packet header.
- Data—the EIGRP packet received (after removing the IP header).

For successful authentication, all of the following must be true:

- The sender and receiver must have the same shared secret.
- The source address chosen by the sender must match the source address in the IP header that the receiver receives.
- The EIGRP packet data that the sender transmits must match the EIGRP packet data that the receiver receives.

Authentication cannot succeed if any of the following is true:

- The sender does not know the shared secret expected by the receiver.
- The IP source address in the IP header is modified in transit.
- Any of the EIGRP packet data is modified in transit.

How to Configure EIGRP/SAF HMAC-SHA-256 Authentication

Configuring HMAC-SHA-256 Authentication

Before you begin

Perform this task to configure an interface to use basic Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication with an encrypted password—password1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **network** *ip-address* [*wildcard-mask*]
6. **af-interface** {**default** | *interface-type interface-number*}
7. **authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**}
8. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 46000`
		Enters IPv4 or IPv6 VRF address family configuration mode and configures an EIGRP routing instance.

Step 5	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router-af)# network 172.16.0.0`	Associates a network with an EIGRP routing process. **Note** This command is used only while configuring an IPv4 routing instance.
Step 6	**af-interface** {**default** | *interface-type interface-number*} **Example:** `Device(config-router-af)# af-interface ethernet 0/0`	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
Step 7	**authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**} **Example:**	Specifies the type of authentication to be used in an EIGRP address family for the EIGRP instance. In this case, the HMAC-SHA-256 authentication method is used.

	Command or Action	Purpose
	`Device(config-router-af-interface)# authentication mode hmac-sha-256 7 password1`	
Step 8	**end** **Example:** `Device(config-router-af-interface)# end`	Exits address family interface configuration mode and returns to global configuration mode.

Configuration Examples for EIGRP/SAF HMAC-SHA-256 Authentication

Example: Configuring HMAC-SHA-256 Authentication

The following example shows how to configure Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication with password password1.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name1
Device(config-router)# address-family ipv6 autonomous-system 45000
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# authentication mode hmac-sha-256 0 password1
Device(config-router-af-interface)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol

Standards and RFCs

Standard/RFC	Title
FIPS PUB 180-2	*SECURE HASH STANDARD (SHS)*
RFC 1321	*The MD5 Message-Digest Algorithm*
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*

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 Overview of Cisco TrustSec

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 Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
IPv6 enablement - Inline Tagging	Cisco IOS XE Fuji 16.8.1	The support for IPv6 is introduced.