IP EIGRP Route Authentication

The IP Enhanced IGRP Route Authentication feature provides MD5 authentication of routing updates from the EIGRP routing protocol. The MD5 keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

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 IP EIGRP Route Authentication

EIGRP Route Authentication

EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol. The MD5 keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

Each key has its own key identifier (specified with the **key** *number* key chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and the MD5 authentication key in use.

You can configure multiple keys with specific lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in the order from lowest to highest, and

uses the first valid key that it encounters. Note that the device needs to know the time to configure keys with lifetimes.

How to Configure IP EIGRP Route Authentication

Defining an Autonomous System for EIGRP Route Authentication

Before you begin

Before you configure EIGRP route authentication, you must enable EIGRP. In this task, EIGRP is defined with an autonomous system number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no switchport**
5. **ip authentication mode eigrp** *autonomous-system* **md5**
6. **ip authentication key-chain eigrp** *autonomous-system key-chain*
7. **exit**
8. **key chain** *name-of-chain*
9. **key** *key-id*
10. **key-string** *text*
11. **accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
12. **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
13. **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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 1/0/9`	Configures an interface type and enters interface configuration mode.
Step 4	**no switchport** **Example:** `Device(config-if)# no switchport`	Puts an interface into Layer 3 mode
Step 5	**ip authentication mode eigrp** *autonomous-system* **md5** **Example:** `Device(config-if)# ip authentication mode eigrp 1 md5`	Enables MD5 authentication in EIGRP packets.
Step 6	**ip authentication key-chain eigrp** *autonomous-system key-chain* **Example:** `Device(config-if)# ip authentication key-chain eigrp 1 keychain1`	Enables authentication of EIGRP packets.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits to global configuration mode.
Step 8	**key chain** *name-of-chain* **Example:** `Device(config)# key chain keychain1`	Identifies a key chain and enters key chain configuration mode.
Step 9	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Identifies the key number and enters key chain key configuration mode.
Step 10	**key-string** *text* **Example:** `Device(config-keychain-key)# key-string 0987654321`	Identifies the key string.
Step 11	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **Example:** `Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite`	(Optional) Specifies the time period during which the key can be received.

	Command or Action	Purpose
Step 12	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **Example:** `Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite`	(Optional) Specifies the time period during which the key can be sent.
Step 13	**end** **Example:** `Device(config-keychain-key)# end`	Exits key chain key configuration mode and returns to privileged EXEC mode.

Defining a Named Configuration for EIGRP Route Authentication

Before you begin

Before you configure EIGRP route authentication, you must enable EIGRP. In this task, EIGRP is defined with a virtual instance name.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-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 key-chain** *name-of-chain*
8. **authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**}
9. **exit-af-interface**
10. **exit-address-family**
11. **exit**
12. **key chain** *name-of-chain*
13. **key** *key-id*
14. **key-string** *text*
15. **accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
16. **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
17. **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-instance-name* **Example:** `Device(config)# router eigrp virtual-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 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router-af)# network 172.16.0.0`	Associates networks with an EIGRP routing process.
Step 6	**af-interface** {**default** | *interface-type interface-number*} **Example:**	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
Step 7	**authentication key-chain** *name-of-chain* **Example:** `Device(config-router-af-interface)# authentication key-chain SITE1`	Specifies an authentication key chain for EIGRP.

	Command or Action	Purpose
Step 8	**authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**} **Example:** `Device(config-router-af-interface)# authentication mode md5`	Specifies the type of authentication used in an EIGRP address family for the EIGRP instance.
Step 9	**exit-af-interface** **Example:** `Device(config-router-af-interface)# exit-af-interface`	Exits address family interface configuration mode.
Step 10	**exit-address-family** **Example:** `Device(config-router-af)# exit-address-family`	Exits address family configuration mode.
Step 11	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.
Step 12	**key chain** *name-of-chain* **Example:** `Device(config)# key chain keychain1`	Identifies a key chain and enters key chain configuration mode.
Step 13	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Identifies the key number and enters key chain key configuration mode.
Step 14	**key-string** *text* **Example:** `Device(config-keychain-key)# key-string 0987654321`	Identifies the key string.
Step 15	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **Example:** `Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite`	(Optional) Specifies the time period during which the key can be received.
Step 16	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **Example:**	(Optional) Specifies the time period during which the key can be sent.

	Command or Action	Purpose
	`Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite`	
Step 17	**end** **Example:** `Device(config-keychain-key)# end`	Exits key chain key configuration mode and returns to privileged EXEC mode.

Configuration Examples for IP EIGRP Route Authentication

Example: EIGRP Route Authentication—Autonomous System Definition

The following example shows how to enable MD5 authentication on EIGRP packets in autonomous system 1.

Device A will accept and attempt to verify the MD5 digest of any EIGRP packet with a key equal to 1. It will also accept a packet with a key equal to 2. All other MD5 packets will be dropped. Device A will send all EIGRP packets with key 2.

Device B will accept key 1 or key 2 and will use key 1 to send MD5 authentication because key 1 is the first valid key of the key chain. Key 1 is not valid after December 4, 2006. After this date, key 2 is used to send MD5 authentication, and this key is valid until January 4, 2007.

The figure below shows the scenario.

Device A Configuration

```
Device> enable
Device(config)# configure terminal
Device(config)# router eigrp 1
Device(config-router)# exit
Device(config)# interface Gigabitethernet 1/0/9
Device(config-if)# no switchport
Device(config-if)# ip authentication mode eigrp 1 md5
Device(config-if)# ip authentication key-chain eigrp 1 key1
Device(config-if)# exit
Device(config)# key chain key1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 04:48:00 Dec 4 1996
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string 1234567890
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite
```

Device B Configuration

```
Device> enable
```

```
Device(config)# configure terminal
Device(config)# router eigrp 1
Device(config-router)# exit
Device(config)# interface Gigabitethernet 1/0/9
Device(config-if)# no switchport
Device(config-if)# ip authentication mode eigrp 1 md5
Device(config-if)# ip authentication key-chain eigrp 1 key2
Device(config-if)# exit
Device(config)# key chain key2
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string 1234567890
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite
```

Example: EIGRP Route Authentication—Named Configuration

The following example shows how to enable MD5 authentication on EIGRP packets in a named configuration.

Device A will accept and attempt to verify the MD5 digest of any EIGRP packet with a key equal to 1. It will also accept a packet with a key equal to 2. All other MD5 packets will be dropped. Device A will send all EIGRP packets with key 2.

Device B will accept key 1 or key 2 and will use key 1 to send MD5 authentication because key 1 is the first valid key of the key chain. Key 1 is not valid after December 4, 2006. After this date, key 2 will be used to send MD5 authentication because it is valid until January 4, 2007.

Device A Configuration

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# network 172.16.0.0
Device(config-router-af)# af-interface Gigabitethernet 1/0/1
Device(config-router-af-interface)# authentication key-chain SITE1
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit-af-interface
Device(config-router-af)# exit-address-family
Device(config-router)# exit
Device(config)# key chain SITE1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string 1234567890
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite
```

Device B Configuration

```
Device> enable
```

```
Device# configure terminal
Device(config)# router eigrp virtual-name2
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# network 172.16.0.0
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# authentication key-chain SITE2
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit-af-interface
Device(config-router-af)# exit-address-family
Device(config-router)# exit
Device(config)# key chain SITE2
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
```

The following example shows how to configure advanced SHA authentication with password password1 and several key strings that will be rotated as time passes:

```
!
key chain chain1
 key 1
  key-string securetraffic
  accept-lifetime 04:00:00 Dec 4 2006 infinite
  send-lifetime 04:00:00 Dec 4 2010 04:48:00 Dec 4 2008
 !
 key 2
  key-string newertraffic
  accept-lifetime 01:00:00 Dec 4 2010 infinite
  send-lifetime 03:00:00 Dec 4 2010 infinite
 exit
!
router eigrp virtual-name
  address-family ipv6 autonomous-system 4453
    af-interface ethernet 0
       authentication mode hmac-sha-256 0 password1
       authentication key-chain key1
  !
!
```

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

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.