MSDP MD5 Password Authentication

The MSDP MD5 password authentication feature is an enhancement to support Message Digest 5 (MD5) signature protection on a TCP connection between two Multicast Source Discovery Protocol (MSDP) peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.

History for the MSDP MD5 Password Authentication Feature

Release	Modification
12.4(2)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Prerequisites for MSDP MD5 Password Authentication

Before configuring MSDP MD5 password authentication, you should be familiar with MSDP concepts and configuration tasks. For more information, refer to the "Related Documents" section.

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

Information About MSDP MD5 Password Authentication

To configure MSDP MD5 password authentication, you must be familiar with the following concepts:

How MSDP MD5 Password Authentication Works

Developed in accordance with RFC 2385, the MSDP MD5 password authentication feature is used to verify each segment sent on the TCP connection between MSDP peers. The **ip msdp password peer** command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and verify the MD5 digest of every segment sent on the TCP connection.

Benefits of MSDP MD5 Password Authentication

- Protects MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.
- Uses the industry-standard MD5 algorithm for improved reliability and security.

How to Configure MSDP MD5 Password Authentication

This section contains the following required configuration task:

Configuring MSDP MD5 Password Authentication

This task explains how to configure MSDP MD5 password authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*]
4. **ip msdp** [**vrf** *name*] **password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*
5. **end**
6. **show ip msdp peer**

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	**ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*] **Example:** `Router(config)# ip msdp peer 10.32.43.144`	Enables MSDP and configures an MSDP peer as specified by the DNS name or IP address.
Step 4	**ip msdp** [**vrf** *name*] **password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string* **Example:** `Router(config)# ip msdp password peer 10.32.43.144 0 test`	Enables MD5 password encryption for a TCP connection between two MSDP peers. • MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. • If you configure or change the password or key used for MD5 authentication between two MSDP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the keepalive period expires. If the password is not entered or changed on the remote router before the keepalive period expires, the session will time out and the MSDP session will reset.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.
Step 6	**show ip msdp peer** **Example:** `Router# show ip msdp peer`	(Optional) Displays detailed information about MSDP peers. • Use this command to verify whether MD5 password authentication is enabled on an MSDP peer.

Troubleshooting Tips

If a router has a password configured for an MSDP peer, but the MSDP peer does not, a message such as the following will appear on the console while the routers attempt to establish a MSDP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the screen:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

The **debug ip tcp transactions** command is used to display information on significant TCP transactions such as state changes, retransmissions, and duplicate packets. In the context of monitoring or troubleshooting MSDP MD5 password authentication, use the **debug ip tcp transactions** command to verify that the MD5 password is enabled and that the keepalive message is received by the MSDP peer.

Configuration Examples for MSDP Password Authentication

This section contains the following configuration example:

- Configuring MSDP MD5 Password Authentication: Example, page 4

Configuring MSDP MD5 Password Authentication: Example

The following example shows how to enable MD5 password authentication for a TCP connection between two MSDP peers:

Router A

```
!
ip msdp peer 10.3.32.154
ip msdp password peer 10.3.32.154 0 test
!
```

Router B

```
!
ip msdp peer 10.3.32.153
ip msdp password peer 10.3.32.153 0 test
!
```

Additional References

The following sections provide references related to MSDP MD5 password authentication.

Related Documents

Related Topic	Document Title
MSDP concepts and configuration tasks	*Cisco IOS IP Multicast Configuration Guide*, Release 12.4
Multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*, Release 12.4

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

RFCs

RFC	Title
RFC 2385	*TCP MD5 Signature Option*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **ip msdp password peer**
- **show ip msdp peer**

ip msdp password peer

To enable Message Digest 5 (MD5) password authentication for TCP connections between two Multicast Source Discovery Protocol (MSDP) peers, use the **ip msdp password peer** command in global configuration mode. To disable this function, use the **no** form of this command.

ip msdp [**vrf** *name*] **password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*

no ip msdp [**vrf** *name*] **password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*

Syntax Description

vrf *name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
{*peer-name* | *peer-address*}	The Domain Name System (DNS) name or IP address of the MSDP peer.
encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Possible values are as follows: • **0**—Specifies that the text immediately following is not encrypted. • **7**—Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
string	Case-sensitive or encrypted password.

Command Default

MD5 password authentication for TCP connections between MSDP peers is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

The **ip msdp password peer** command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and verify the MD5 digest of every segment sent on the TCP connection.

If a router has a password configured for an MSDP peer, but the MSDP peer does not, a message such as the following will appear on the console while the routers attempt to establish a MSDP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the screen:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

Configuring an MD5 Password in an Established MSDP Session

If you configure or change the password or key used for MD5 authentication between two MSDP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the keepalive period expires. If the password is not entered or changed on the remote router before the keepalive period expires, the session will time out and the MSDP session will reset.

Examples

The following example shows how to configure an MD5 password for TCP connections to the MSDP peer at 10.3.32.152:

```
ip msdp password peer 10.3.32.152 0 test
```

Related Commands

Command	Description
show ip msdp peer	Displays detailed information about MSDP peers.

show ip msdp peer

To display detailed information about Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp peer** command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **peer** [*peer-address* | *peer-name*] [**accepted-sas** | **advertised-sas**]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	(Optional) Domain Name System (DNS) name or IP address of the MSDP peer for which information is displayed.
accepted-sas	(Optional) SAs accepted from this peer.
advertised-sas	(Optional) SAs advertised to this peer.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the Source Active (SA) message limit configured using the **ip msdp sa-limit** command.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.4(2)T	This command was modified to display whether an MSDP peer has Message Digest 5 (MD5) password authentication enabled.

Examples

The following is sample output from the **show ip msdp peer** command:

```
Router# show ip msdp peer 224.135.250.116

MSDP Peer 224.135.250.116 (rtp5-rp1.cisco.com), AS 109 (configured AS)
Description:
 Connection status:
   State: Up, Resets: 9, Connection source: Loopback2 (228.69.199.17)
   Uptime(Downtime): 1d10h, Messages sent/received: 436765/429062
   Output messages discarded: 0
   Connection and counters cleared 1w2d     ago
 SA Filtering:
   Input (S,G) filter: none, route-map: none
   Input RP filter: none, route-map: none
   Output (S,G) filter: none, route-map: none
   Output RP filter: none, route-map: none
 SA-Requests:
   Input filter: none
   Sending SA-Requests to peer: disabled
 Peer ttl threshold: 0
```

```
SAs learned from this peer: 32, SAs limit: 500
Input queue size: 0, Output queue size: 0
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip msdp peer Field Descriptions

Field	Description
MSDP Peer	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the IP address for the TCP local connection address.
Uptime (Downtime):	Days and hours the MSDP peer is up or down. If the time is less than 24 hours, it is shown in terms of hours:minutes:seconds.
Messages sent/received:	Number of SA messages sent to the MSDP peer/number of SA messages received from the MSDP peer.
SA Filtering:	Information regarding access list filtering of SA input and output, if any.
SA-Requests:	Information regarding access list filtering of SA requests, if any.
SAs learned from this peer:	Number of SA messages from the MSDP peer in the SA cache.
SAs limit:	SA message limit for this MSDP peer.

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

Glossary

encryption—Encryption is the translation of data into a secret code. Encryption is a way to achieve data security. Encryption prevents the password or key from being easily readable in the configuration file.

MD5—Message Digest 5. An algorithm that is used to create digital signatures. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest. When a one-way hash function is used, a calculated message digest is compared against the received message digest to verify that the message has not been tampered with. This comparison is called a *hashcheck*.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.