Remote Secrets

This chapter describes how StarOS supports the use of remote secrets.

Important The commands described in this chapter appear in the CLI for this release. However, they have not been qualified for use with any current Cisco StarOS gateway products.

The following topics are discussed:

PSK Support for Remote Secrets

Overview

StarOS CLI commands support the creation of local and remote pre-shared keys (PSKs) associated with crypto maps and crypto templates. Refer to the descriptions of the **crypto map** and **crypto template** commands in the *Context Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

StarOS also allows the operator to configure a remote secret list that contains PSKs based on remote ID types. The remote secret list can contain up to 1000 entries; only one remote secret list is supported per system. The remote secret list bound to a crypto map and/or crypto template.

Each entry in the remote secret list consists of either an alphanumerical string of 1 through 255 characters, or a hexadecimal string of 16 to 444 bytes.

Implementation

The general sequence for implementing the use of a remote PSK is as follows:

- The initiator sends an IKE_INIT_REQUEST to the responder.
- The responder replies with an IKE_INIT_RESPONSE.
- When the IKE_INIT_RESPONSE is received, the Initiator sends an IKE_AUTH_REQUEST to the responder along with its peer ID.

- When the responder receives the IKE_AUTH_REQUEST, it derives the peer ID from the IKE_AUTH_REQUEST to search the remote secret list for the PSK. If the remote secret list is bound to the respective map/template, it takes the PSK from the list. Otherwise, it will take the remote PSK from the respective map or template.

Supported IKE ID Types

The following IKE ID types are support supported in a remote secret list entry:

- ID_IP_ADDR (supports IPv4 and IPv6 address notations)
- ID_IPV4_ADDR (IPv4 address in dotted-decimal notation)
- ID_FQDN (Fully Qualified Domain Name
- ID_RFC822_ADDR (Email address)
- ID_IPV6_ADDR (IPv6 address in colon-separated notation)
- ID_DER_ASN1_DN (Abstract Syntax Notation One – Distinguished Name)
- ID_DER_ASN1_GN (Abstract Syntax Notation One – General Name)
- ID_KEY_ID (Opaque byte stream)

Deployment Scenarios

A group of remote clients can be configured to use a separate pre-shared key, even if they are using the same crypto map or crypto template.

CLI Commands

Important The commands described below appear in the CLI for this release. However, they have not been qualified for use with any current Cisco StarOS gateway products.

Global Configuration Mode

crypto remote-secret-list

Specifies the name of the remote secret list for storing remote secrets based on the ID type. This command sends you to the Remote Secret List Configuration mode and the **remote-id-id-type** command. Only one active remote-secret-list is supported per system.

crypto remote-secret-list*listname*

Important You must unbind the remote-secret-list from any crypto maps or templates before it can be deleted.

For additional information, refer to the *Remote Secret List Configuration Commands* chapter of the *Command Line Interface Reference* and the *System Administration Guide*.

remote-id id-type

Configures the remote pre-shared key based on the ID type.

```
remote-id id-type { der-asn1-dn | fqdn | ip-addr | key-id | rfc822-addr
} id id_value secret [ encrypted ]  key key_value
```

Context Configuration Commands

Enable remote secret list

The remote secret list must be enabled in a crypto map or crypto template.

For a crypto map the configuration sequence is:

```
configure
  context ctxt_name
    crypto map template_name { ikev2-ipv4 | ikev2-ipv6 }
      remote-secret-list
```

For a crypto template the configuration sequence is:

```
configure
  context ctxt_name
    crypto template template_name ikev2-dynamic
      remote-secret-list
```

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords.

show Commands

show configuration

Configured remote secrets are displayed in the output of the **show configuration** command

show crypto map

Configured remote secrets are also displayed in the following **show crypto map** commands:

- **show crypto map**
- **show crypto map map-type ikev2-ipv4-cfg**
- **show crypto map map-type ikev2-ipv6-cfg**
- **show crypto map tag** *map-name*

show crypto template

Configured remote secrets are also displayed in the following **show crypto template** commands:

- **show crypto template**
- **show crypto template map-type ikev2-dynamic**
- **show crypto template tag** *map-name*

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords.