Crypto Maps

This chapter describes the various types of IPsec crypto maps supported under StarOS.

A crypto map is a software configuration entity that performs two primary functions:

- Selects data flows that need security processing.
- Defines the policy for these flows and the crypto peer to which that traffic needs to go.

A crypto map is applied to an interface. The concept of a crypto map was introduced in classic crypto but was expanded for IPSec.

Important A **match ip pool** command in a crypto group is not supported within crypto maps on the ASR 5500.

Guidelines are provided for configuring the following types of crypto maps:

ISAKMP Crypto Map Configuration

This section provides instructions for configuring ISAKMP crypto maps.

Important This section provides the minimum instruction set for configuring ISAKMP crypto maps on the system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *Crypto Map ISAKMP Configuration Mode* chapters in the *Command Line Interface Reference*.

To configure the ISAKMP crypto maps for IPSec:

Step 1 Configure ISAKMP crypto map by applying the example configuration in Configuring ISAKMP Crypto Maps, on page 2.

Step 2 Verify your ISAKMP crypto map configuration by following the steps in Verifying the ISAKMP Crypto Map Configuration, on page 2.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring ISAKMP Crypto Maps

Use the following example to create the ISAKMP crypto map:

```
configure
  context ctxt_name
    crypto map map_name ipsec-isakmp
      set peer agw_address
      set isakmp preshared-key isakmp_key
      set mode { aggressive | main }
      set pfs { group1 | group2 | group5 }
      set transform-set transform_name
      match address acl_name [ preference ]
      match crypto-group group_name { primary | secondary }
      end
```

Notes:

- *ctxt_name* is the system context in which you wish to create and configure the ISAKMP crypto maps.
- *map_name* is name by which the ISAKMP crypto map will be recognized by the system.
- *acl_name* is name of the pre-configured Access Control List (ACL). It is used for configurations not implementing the IPSec Tunnel Failover feature and match the crypto map to a previously defined crypto ACL. This is an optional parameter.
- *group_name* is name of the Crypto group configured in the same context. It is used for configurations employing the IPSec Tunnel Failover feature. This is an optional parameter. For more information, refer to the *Redundant IPSec Tunnel Fail-Over* chapter of this guide.
- For more information on parameters, refer to the *Crypto Map ISAKMP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Verifying the ISAKMP Crypto Map Configuration

Enter the following Exec mode command for the appropriate context to display and verify your ISAKMP crypto map:

```
show crypto map [ tag map_name | type ipsec-isakmp ]
```

This command produces an output similar to that displayed below that displays the configuration of a crypto map named test_map2.

```
Map Name : test_map2
=======================================
  Payload :
      crypto_acl2: permit tcp host 10.10.2.12 neq 35 any
```

```
Crypto map Type : ISAKMP
IKE Mode : MAIN
IKE pre-shared key : 3fd32rf09svc
Perfect Forward Secrecy : Group2
Hard Lifetime :
      28800 seconds
      4608000 kilobytes
Number of Transforms: 1
Transform : test1
      AH : none
      ESP: md5 3des-cbc
      Encaps mode: TUNNEL
Local Gateway: Not Set
Remote Gateway: 192.168.1.1
```

Caution Modification(s) to an existing ISAKMP crypto map configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.

Dynamic Crypto Map Configuration

This section provides instructions for configuring dynamic crypto maps. Dynamic crypto maps should only be configured in support of L2TP or Mobile IP applications.

Important This section provides the minimum instruction set for configuring dynamic crypto maps on the system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *Crypto Map Dynamic Configuration Mode Commands* chapters in the *Command Line Interface Reference*.

To configure the dynamic crypto maps for IPSec:

Step 1 Configure dynamic crypto maps by applying the example configuration in Configuring Dynamic Crypto Maps, on page 3.

Step 2 Verify your dynamic crypto map configuration by following the steps in Verifying the Dynamic Crypto Map Configuration, on page 4.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Dynamic Crypto Maps

Use the following example to create the dynamic crypto map on your system:

```
configure
  context ctxt_name
    crypto map map_name ipsec-dynamic
```

```
set pfs { group1 | group2 | group5 }
set transform-set transform_name
end
```

Notes:

- *ctxt_name* is the system context in which you wish to create and configure the dynamic crypto maps.
- *map_name* is name by which the dynamic crypto map will be recognized by the system.
- For more information on parameters, refer to the *Crypto Map Dynamic Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Verifying the Dynamic Crypto Map Configuration

Enter the following Exec mode command for the appropriate context to display and verify your dynamic crypto map configuration:

show crypto map [tag *map_name* **| map-type ipsec-dynamic]**

This command produces an output similar to that displayed below using the configuration of a dynamic crypto map named test_map3.

```
Map Name : test_map3
=======================================
  Crypto map Type : ISAKMP (Dynamic)
  IKE Mode : MAIN
  IKE pre-shared key :
  Perfect Forward Secrecy : Group2
  Hard Lifetime :
        28800 seconds
        4608000 kilobytes
  Transform : test1
        AH : none
        ESP: md5 3des-cbc
        Encaps mode: TUNNEL
  Local Gateway: Not Set
  Remote Gateway: Not Set
```

Caution Modification(s) to an existing dynamic crypto map configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.

Manual Crypto Map Configuration

This section provides the minimum instruction set for configuring manual crypto maps on the system. For more information on commands that configure additional parameters and options, refer to the *Context Configuration Mode Commands* and *Crypto Map Manual Configuration Mode Commands* chapters in the *Command Line Interface Reference*.

To configure the manual crypto maps for IPSec:

Step 1 Configure manual crypto map by applying the example configuration in Configuring Manual Crypto Maps, on page 5.

Step 2 Verify your manual crypto map configuration by following the steps in Verifying the Manual Crypto Map Configuration, on page 5.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Important Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

Configuring Manual Crypto Maps

Use the following example to create the manual crypto map on your system:

```
configure
   context ctxt_name
      crypto map map_name ipsec-manual
         set peer agw_address
         match address acl_name [ preference ]
         set transform-set transform_name
         set session-key { inbound | outbound } { ah ah_spi [ encrypted ]
key ah_key | esp esp_spi [ encrypted ] cipher encryption_key [ encrypted ]
authenticator auth_key }
         end
```

Notes:

- *ctxt_name* is the system context in which you wish to create and configure the manual crypto maps.
- *map_name* is name by which the manual crypto map will be recognized by the system.
- *acl_name* is name of the pre-configured ACL. It is used for configurations not implementing the IPSec Tunnel Failover feature and match the crypto map to a previously defined crypto ACL. This is an optional parameter.
- The length of the configured key must match the configured algorithm.
- *group_name* is name of the crypto group configured in the same context. It is used for configurations using the IPSec Tunnel Failover feature. This is an optional parameter.
- For more information on parameters, refer to the *Crypto Map Manual Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Verifying the Manual Crypto Map Configuration

Enter the following Exec mode command for the appropriate context to display and verify your manual crypto map configuration:

show crypto map [tag *map_name* **| map-type ipsec-manual]**

This command produces an output similar to that displayed below that displays the configuration of a crypto map named test_map.

```
Map Name : test_map
=====================================
  Payload :
        crypto_acl1: permit tcp host 1.2.3.4 gt 30 any
  Crypto map Type : manual(static)
  Transform : test1
        Encaps mode: TUNNEL
  Transmit Flow
        Protocol : ESP
        SPI : 0x102 (258)
        Hmac : md5, key: 23d32d23cs89
        Cipher : 3des-cbc, key: 1234asd3c3d
  Receive Flow
        Protocol : ESP
        SPI : 0x101 (257)          Hmac : md5, key: 008j90u3rjp
        Cipher : 3des-cbc, key: sdfsdfasdf342d32
  Local Gateway: Not Set
  Remote Gateway: 192.168.1.40
```

Caution Modification(s) to an existing manual crypto map configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.

Crypto Map and Interface Association

This section provides instructions for applying manual or ISAKMP crypto maps to interfaces configured under StarOS.

Important Dynamic crypto maps should not be applied to interfaces.

Important This section provides the minimum instruction set for applying manual or ISAKMP crypto maps to an interface on the system. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To apply the crypto maps to an interface:

Step 1 Configure a manual or ISAKMP crypto map.

Step 2 Apply the desired crypto map to a system interface by following the steps in Applying a Crypto Map to an Interface, on page 7.

Step 3 Verify your manual crypto map configuration by following the steps in Verifying the Interface Configuration with Crypto Map, on page 7.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Applying a Crypto Map to an Interface

Use the following example to apply an existing crypto map to an interface on your system:

```
configure
   context ctxt_name
      interface interface_name
      crypto-map map_name
      end
```

Notes:

- *ctxt_name* is the system context in which the interface is configured to apply crypto map.
- *interface_name* is the name of a specific interface configured in the context to which the crypto map will be applied.
- *map_name* is name of the preconfigured ISAKMP or a manual crypto map.

Verifying the Interface Configuration with Crypto Map

Enter the following Exec mode command for the appropriate context to display and verify that your interface is configured properly:

```
show configuration context ctxt_name | grep interface
```

The interface configuration aspect of the display should look similar to that shown below. In this example an interface named 20/6 was configured with a crypto map called isakmp_map1.

```
interface 20/6
ip address 192.168.4.10 255.255.255.0
      crypto-map isakmp_map1
```