Duplicate Session Detection

This chapter describes how to configure IPSec to maintain only one IKE-SA per remote ID (peer IKE_ID). This feature is only support for the Wireless Security Gateway (WSG) service.

The following topics are discussed:

Process Overview

RFC 5996 does not restrict the creation of multiple IKE SAs having the same remote IKE_ID (not necessarily from the same peer). The remote IKE_ID specifies the remote peer ID: IDi when the gateway is the responder, and IDr when the gateway is the initiator. In such implementations, a new IKE_SA is created for every IKE_SA_INIT/IKE_AUTH exchanges, unless INITIAL_CONTACT is indicated. If an IKE_AUTH is received with INITIAL_CONTACT, the node is expected to delete all IKE_SAs having the same authenticated identity.

Important The StarOS IPSec stack does not currently support INITIAL_CONTACT.

When enabled via the StarOS **duplicate-session-detection** command in a WSG service, only one IKE_SA is allowed per remote IKE_ID. This feature is supported for WSG service, both RAS (Remote Access Service) and S2S (Site-to-Site) tunnel types.

The following sequence of figures indicates how StarOS IPSec managers handle duplicate IKE_SA scenarios when this feature is enabled.

Figure 1: No Duplicate Session Found

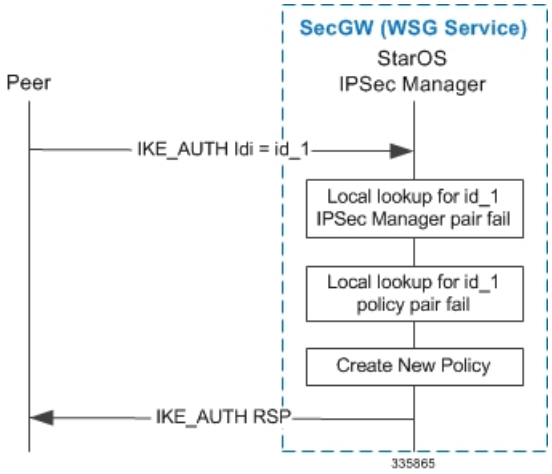


Figure 2: Duplicate Session Found in Same StarOS IPSec Manager

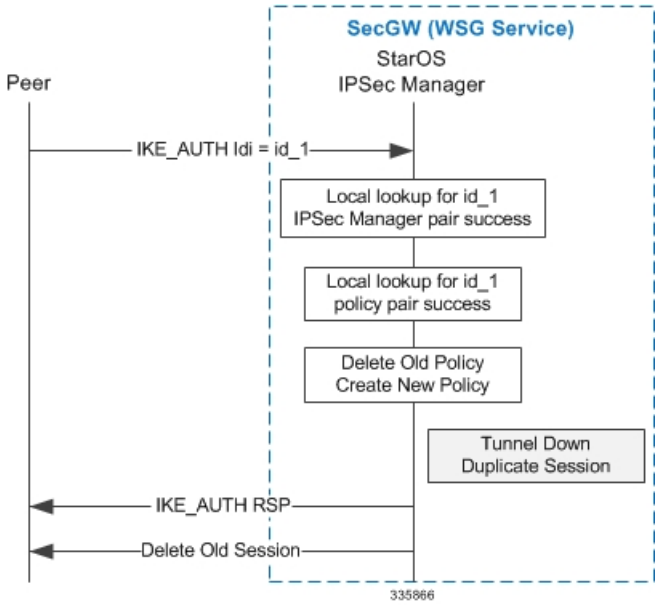


Figure 3: Duplicate Session Found in Different StarOS IPSec Manager

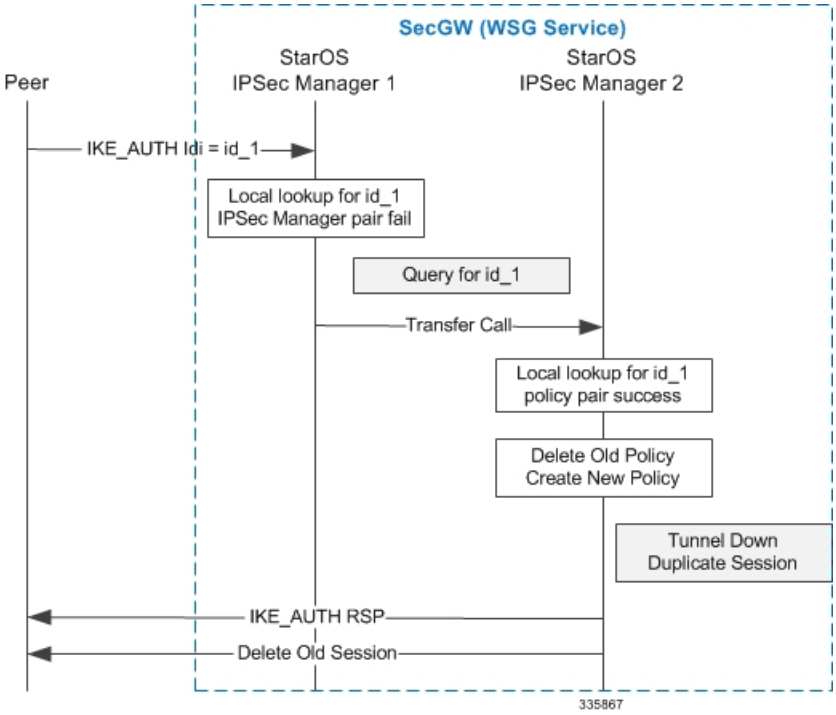


Figure 4: Duplicate Session Found When SecGW (WSG Service) is the Initiator

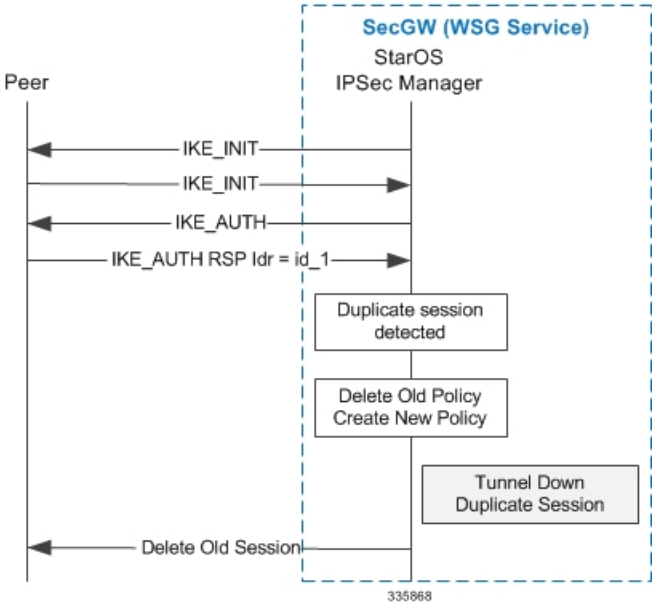
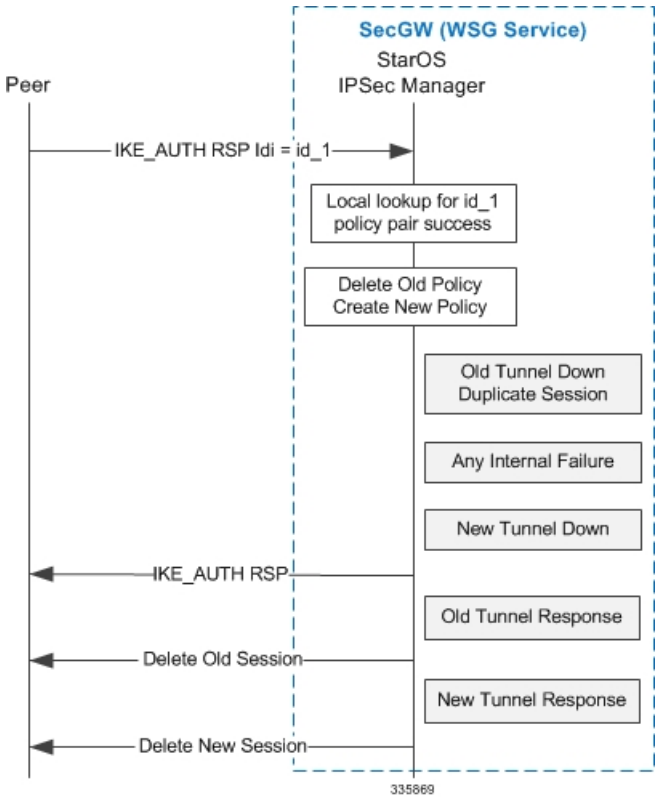


Figure 5: Internal Failures Encountered After Duplicate Session is Detected<



Configuring Duplicate Session Detection

Use the following example to enable duplicate session detection:

```
configure
   context wsg_ctx_name
      wsg-service wsg_srvc_name
         duplicate-session-detection
         end
```

Notes:

- *wsg_ctx_name* is the StarOS context associated with a WSG service.
- *wsg_srvc_name* is the name of the WSG service in the current context that you want to configure for duplicate session detection.
- Any changes made to a WSG service require that the service must be restarted to apply any changed parameters. You restart the service by unbinding and binding the IP address to the service context.
- For more information on parameters, see the *WSG Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- By default duplicate session detection is disabled.

Verifying the Duplicate Session Detection Configuration

Enter the following Exec mode command for the WSG context to display and verify your duplicate session detection configuration:

show wsg-service all *wsg_srvc_name*

The output of this command will include the following parameter:

```
Duplicate-session-detection : Enabled/Disabled
```