



# 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, on page 1](#)
- [Configuring Duplicate Session Detection, on page 4](#)
- [Verifying the Duplicate Session Detection Configuration, on page 5](#)

## 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

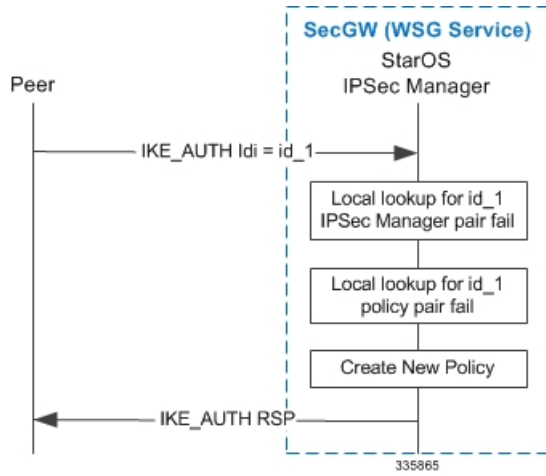


Figure 2: Duplicate Session Found in Same StarOS IPSec Manager

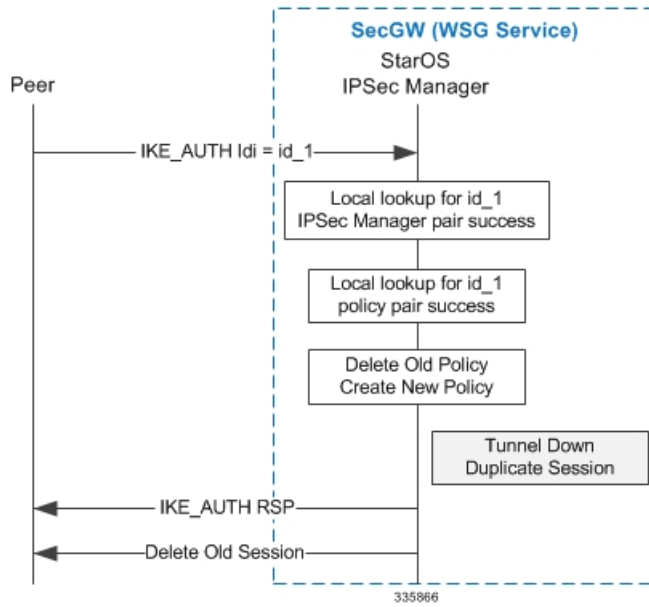


Figure 3: Duplicate Session Found in Different StarOS IPSec Manager

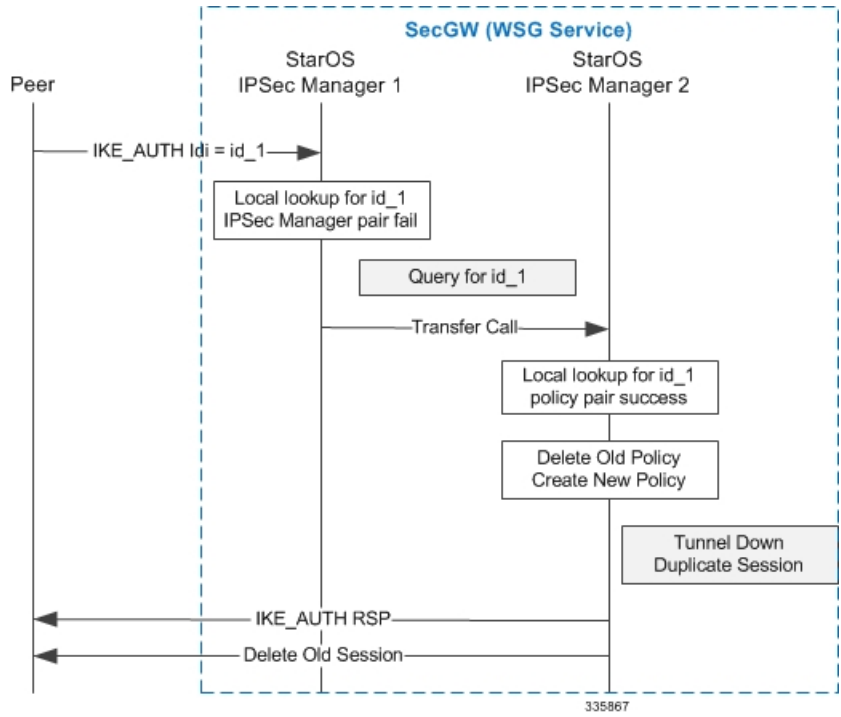


Figure 4: Duplicate Session Found When SecGW (WSG Service) is the Initiator

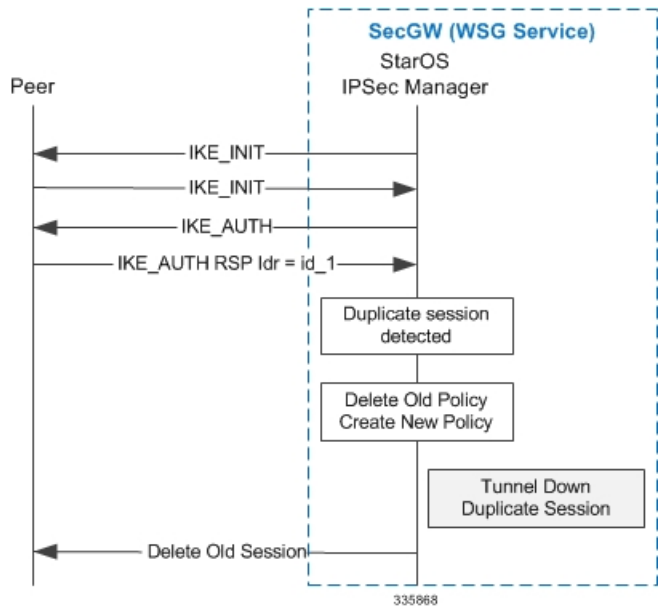
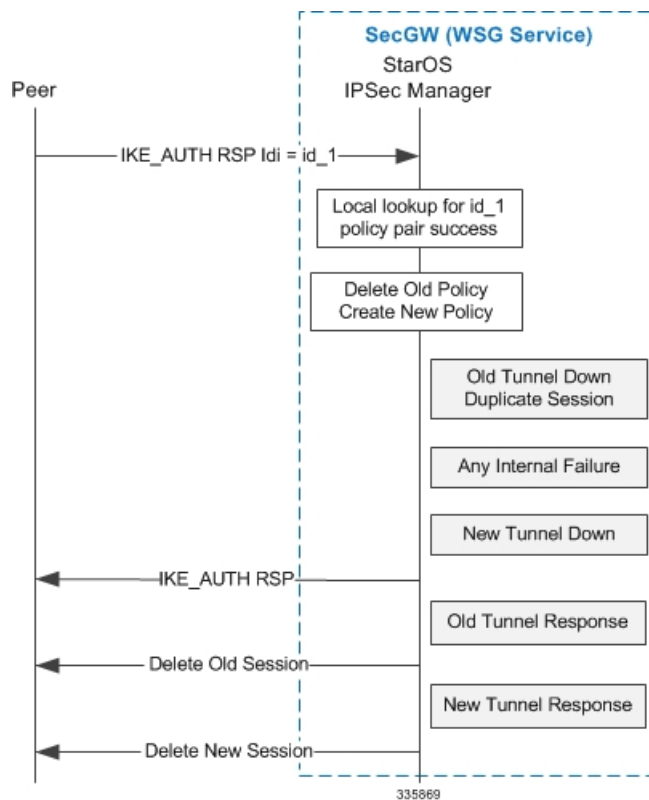


Figure 5: Internal Failures Encountered After Duplicate Session is Detected



## 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
```

