Access Control

This chapter describes enhancements to IPSec Access Control.

The following topics are discussed:

Access Control via Blacklist or Whitelist

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

Overview

A blacklist or block list is a basic access control mechanism that allows everyone access, except for the members of the black list. The opposite is a whitelist, which denies access to everybody except for members of the white list.

A blacklist is a list or register of entities that, for one reason or another, are being denied a particular privilege, service, mobility, access or recognition.

A whitelist is a list or register of entities that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition.

With blacklisting, any peer is allowed to connect as long as it does not appear in the list. With whitelisting, no peer is allowed to connect unless it appears in the list. An operator may choose to implement one or the other. You can implement either a blacklist or whitelist; both listing techniques cannot be implemented simultaneously on a security gateway.

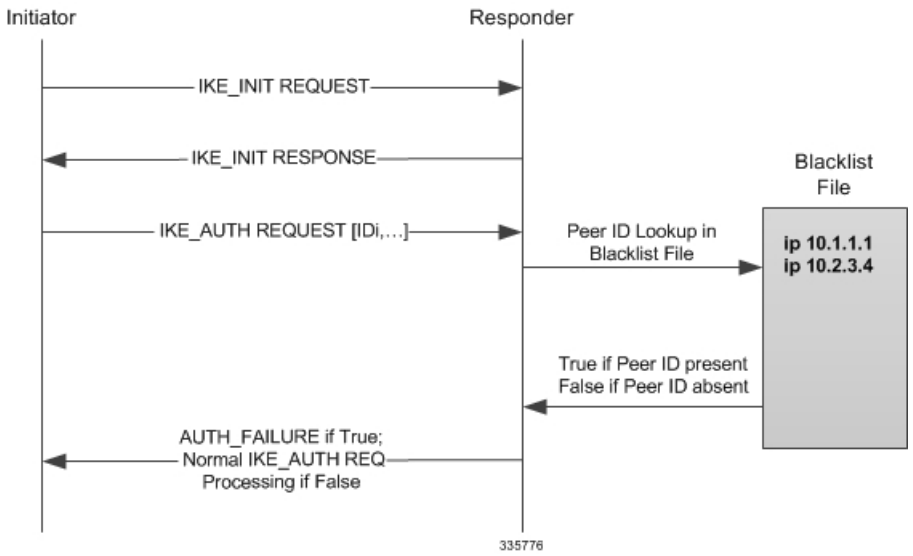
Blacklisting

The sequence of events when implementing blacklisting is briefly described below:

- The initiator sends IKE_INIT_REQUEST to the responder.
- The responder replies with IKE_INIT_RESPONSE.

- Once the IKE_INIT_RESPONSE is done, the Initiator sends IKE_AUTH_REQUEST to the responder along with its ID.
- Upon receipt of the IKE_AUTH_REQUEST, the responder checks for the presence of a matching peer ID in the blacklist.
- If the peer ID is present in the blacklist, the responder sends an IKE_AUTH_FAILURE to the initiator. Otherwise, the processing of IKE_AUTH_REQUEST follows the normal procedure for tunnel setup.

Figure 1: Blacklisting Implementation

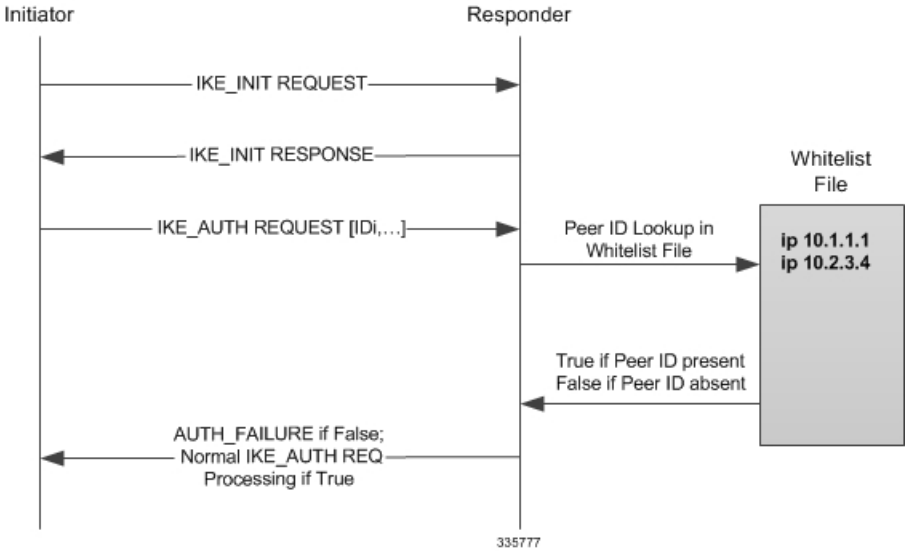


Whitelisting

The sequence of events when implementing whitelisting is briefly described below:

- The initiator sends IKE_INIT_REQUEST to the responder.
- The responder replies with IKE_INIT_RESPONSE.
- Once the IKE_INIT_RESPONSE is done, the Initiator sends IKE_AUTH_REQUEST to the responder along with its ID.
- Upon receipt of the IKE_AUTH_REQUEST, the responder checks for the presence of a matching peer ID in the whitelist.
- If the peer ID is present in the whitelist, the IKE_AUTH_REQUEST is processed normally. Otherwise, the gateway sends an IKE_AUTH_FAILURE to the initiator.

Figure 2: Whitelist Implementation



Blacklist and Whitelist File Format

File Format and Content

The blacklist/whitelist file can be in DOS or Unix format. DOS files will be internally converted to Unix format before being read.

The file contents should follow the standard format described below. Each entry in the blacklist/whitelist file should contain the ID type so that the validation is performed for that ID type. The ID type and ID value in each entry should be separated by a **space**.

Important No other file types or formats are supported.

The sample file content is shown below.

```
# IP address IDS
ipv4 "33.33.33.1"
ipv4 "66.66.66.1"
ipv6 "11::1"
# FQDN IDs
fqdn "LS1-0.cisco.com"

# Email ID
email "user@sample.com"

# Distinguished Name ID
dn "C=US,ST=CA,L=SanJose,O=Cisco,OU=SMBU,CN=ixia.organization.bu.org"
```

Supported IKE ID Types

The following IKE ID types are supported in a blacklist or whitelist:

- 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

Blacklisting

Blacklisting can be used when requests from a particular identity must be blocked for a short period of time, such as if the subscriber has not paid his/her bill.

Whitelisting

Whitelisting can be used when requests from particular identities must be allowed to set up tunnels for a short period of time, such as when certain services are allowed only for subscribers who have subscribed for the service.

External Interfaces

The blacklist/whitelist file will be read from locations accessible by StarOS. Locations and protocols include:

- [file:]{/flash | /pcmcia1 | /hd-raid}[/directory]/filename
- [file:]{/flash | /usb1 | /hd-raid}[/directory]/filename
- tftp://host[:port][/directory]/filename
- ftp://[username[:password]@]host[:port][/directory]/filename
- sftp://[username[:password]@]host[:port][/directory]/filename

Important A black list or whitelist must be available to StarOS or blacklisting/whitelisting will not be performed even if enabled.

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 blacklist file

Configures a blacklist (access denied) file to be used by a security gateway (SeGW).

crypto blacklist file *pathname*

pathname specifies the location and protocol from which StarOS will retrieve the blacklist file.

Refer to the *Command Line Interface Reference* for a complete description of this command and its keywords.

crypto whitelist file

Configures a whitelist (access permitted) file to be used by a security gateway (SeGW).

crypto whitelist file *pathname*

pathname specifies the location and protocol from which StarOS will retrieve the whitelist file.

Refer to the *Command Line Interface Reference* for a complete description of this command and its keywords.

Context Configuration Mode

Enable blacklist

The blacklist 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 }
      blacklist
```

For a crypto template the configuration sequence is:

```
configure
  context ctxt_name
    crypto template template_name ikev2-dynamic
      blacklist
```

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

Enable whitelist

A whitelist 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 }
      whitelist
```

For a crypto template the configuration sequence is:

```
configure
  context ctxt_name
```

```
crypto template template_name ikev2-dynamic
  whitelist
```

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

Exec Mode

crypto blacklist file update

Updates the blacklist (access denied) file using the path specified when the blacklist was enabled.

```
crypto blacklist file update
```

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords. For additional information on blacklisting, refer to the *System Administration Guide*

crypto whitelist file update

Updates the whitelist (access granted) file using the path specified when the whitelist was enabled.

```
crypto whitelist file update
```

Refer to the *Command Line Interface Reference* for a complete description of these commands and their keywords. For additional information on blacklisting, refer to the *System Administration Guide*

show Commands

show crypto blacklist file

Displays the contents of the blacklist (access denied) file.

```
show crypto blacklist file
```

Refer to the *Statistics and Counters Reference* for a description of the information output by this command.

show crypto whitelist file

Displays the contents of the whitelist (access granted) file.

```
show crypto blacklist file
```

Refer to the *Statistics and Counters Reference* for a description of the information output by this command.

show crypto statistics ikev2

The output of this command displays statistics for blacklist or whitelist activities, including Child SA exchanges and SA rekeys.

show crypto template

The output of this command indicates whether blacklisting or whitelisting has been enabled.

IKE Call Admission Control

Call Admission Control (CAC) rate limits new IKE calls whenever a security gateway (SeGW) is experiencing an overload. If the SeGW receives more IKE_SA_INIT requests than it can handle, already established tunnels

could be affected as system resources, such as CPU, Message Queue etc., would be utilized to handle the new calls. The SeGW may be unable to process the Dead Peer Detections (DPDs) of existing tunnels on time, leading to their tear-off. Rate limiting preserves enough system resources to maintain existing calls.

In StarOS, this functionality is achieved through **congestion-control threshold** Global Configuration mode CLI commands. These commands monitor a variety of parameters that indicate whether the system has gone into overload. Parameters that can be monitored for congestion include (but are not limited to):

- **congestion-control threshold license-utilization** percent – percentage of maximum number of licensed sessions
- **congestion-control threshold max-sessions-per-service-utilization** percent – percentage of maximum subscriber sessions (**congestion-control threshold per-service-**service percent command)
- **congestion-control threshold message-queue-utilization** percent – percentage of message queue utilization (**congestion-control threshold message-queue-utilization** percent command)
- **congestion-control threshold message-queue-wait-time** time – wait time in seconds
- **congestion-control threshold port-rx-utilization** percent – average percentage of receive port utilization
- **congestion-control threshold port-specific {** slot/port **| all }** – percentage of utilization for a specific port
- **congestion-control threshold port-specific-rx-utilization** percent – percentage of receive utilization for a specific port
- **congestion-control threshold port-specific-tx-utilization** percent – transmit utilization for a specific port
- **congestion-control threshold port-tx-utilization** percent – average percentage of port transmit utilization
- **congestion-control threshold service-control-cpu-utilization** percent – average percentage of CPU utilization for service control
- **congestion-control threshold system-cpu-utilization** percent – average percentage of system CPU utilization
- **congestion-control threshold system-memory-utilization** percent – average percentage of CPU memory utilization

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