



# Configuring Access Lists and Filtering GSS Traffic

---

You can filter incoming traffic received by the GSS by using access lists. You create access lists at the CLI of each GSS device. This chapter describes how to create access lists and access groups to filter GSS traffic.

It contains the following major sections:

- [Filtering GSS Traffic Using Access Lists](#)
- [Deploying GSS Devices Behind Firewalls](#)

## Filtering GSS Traffic Using Access Lists

This section contains the following topics:

- [Access List Overview](#)
- [Creating an Access List](#)
- [Associating an Access List with a GSS Interface](#)
- [Disassociating an Access List from a GSS Interface](#)
- [Adding Rules to an Access List](#)
- [Removing Rules from an Access List](#)
- [Segmenting GSS Traffic by Ethernet Interface](#)
- [Displaying Access Lists](#)

## Access List Overview

The packet filtering tools on the GSS instruct each device to permit or refuse specific packets based on a combination of criteria that includes the following:

- Destination port of the packets
- Requesting host
- Protocol used (TCP, UDP, or ICMP)

You create packet-filtering tools, called access lists, from the GSS CLI. Access lists are collections of filtering rules that you create using the **access-list** CLI command. Each access list is a sequential collection of permit and deny conditions that apply to a source network IP address to control whether the GSS forwards or blocks routed packets. The GSS examines each packet to determine whether to forward or drop the packet based on the criteria specified within the access lists.

You can create any number of access lists on each GSS device. After creating an access list, you can append or remove rules from the list at any time. Apply access lists to one or both of the GSS Ethernet interfaces using the **access-group** command.

The GSS appends each additional criteria statement to the *end* of the access list statements. Be aware that you cannot delete individual statements after creating them. You can only delete an entire access list.

The order of access list statements is very important. When the GSS decides whether to forward or block a packet, it tests the packet against each criteria statement in the order that the statements were created. After a match is found, the GSS does not check any additional criteria statements.

If you create a criteria statement that explicitly permits all traffic, the GSS does not check any additional statements added after the explicit permit statement and permits all traffic. If you need additional statements, delete the access list and retype it with the new entries.

To ensure your GSS functions properly with access lists, identify the ports and protocols normally used by each GSS device. [Table 5-1](#) lists the types of expected inbound traffic received by the GSS.

**Note**

The GSS applies configured access lists to outgoing keepalives and filters them accordingly except for TCP and HTTP-head keepalives, which the GSS never blocks.

**Table 5-1 GSS-Related Ports and Protocols for Inbound Traffic**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
*	20–23	TCP	FTP, SSH, and Telnet server services on the GSS
20–23	*	TCP	Return traffic of FTP, Secure Copy (SCP), and Telnet GSS CLI commands
49 or user configured	*	TCP	Return traffic for TACACS+
*	53	UDP, TCP	GSS DNS server traffic
53	*	UDP	Return traffic of GSS software reverse lookup, “dnslookup” queries, and name server forwarding
123	123	UDP	Network Time Protocol (NTP) updates
*	161	UDP	Simple Network Management Protocol (SNMP) traffic
*	443	TCP	Primary GSSM GUI
1304	1304	UDP	CRA keepalives
1974	1974	UDP	Director Response Protocol (DRP) protocol traffic
*	2000	UDP	Inter-GSS periodic status reporting
*	2001–2005	TCP	Inter-GSS communication
2001–2005	*	TCP	Return traffic of inter-GSS communication

**Table 5-1 GSS-Related Ports and Protocols for Inbound Traffic (continued)**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
*	3002–3008	TCP	Inter-GSS communication
3002–3008	*	TCP	Return traffic of inter-GSS communication
*	3009	TCP	Received traffic of Cisco Application Networking Manager (ANM) communication
3340	*	TCP	Sticky and Config Agent communication
3341	*	TCP	Sticky communication source
3342	*	TCP	Sticky and DNS processes communication
*	5001	TCP	Global sticky mesh protocol traffic
5001	*	TCP	Return traffic of global sticky mesh protocol traffic
5002	*	UDP	Return traffic of KAL-AP keepalives

\*Any legal port number

## Creating an Access List

You can create an access list by using the **access-list** command in global configuration mode. You must have access to the CLI of each GSS device to create access lists for that device.

The syntax of this command is as follows:

```
access-list name { permit | deny } protocol [source-address source-netmask |
host source-address | any] operator port [port] [destination-port
operator port [port]]
```

The keywords and arguments are as follows:

- *name*—Alphanumeric name used to identify the access list you are creating.
- **permit**—Allows a connection when a packet matches the condition. All provisions of the condition must be met to make a match.
- **deny**—Prevents a connection when a packet matches the condition. All provisions of the condition must be met to make a match.
- *protocol*—Protocol for the traffic type. Recognized IP protocols include: **tcp** (Transmission Control Protocol), **udp** (User Datagram Protocol), and **icmp** (Internet Control Message Protocol).
- *source-address*—Network IP address from which the packet originated. The GSS software uses the *source-address* and *source-netmask* arguments to match the incoming packet to a source network.
- *source-netmask*—Subnet mask for the network from which the packet originated. The software uses the *source-address* and *source-netmask* arguments to match the incoming packet to a source network.
- **host**—Identifies the host machine that is the source of the packet.
- *source-address*—IP address of the device that is the source of the packet.
- **any**—Identifies the wildcard value for the packet source. With **any** used in place of the *source-address*, *source-netmask*, or **host** *source-address* values, the GSS matches packets from all incoming sources.
- *operator*—Arbitrary bytes within the packet. The *operator* can be one of the following values: **eq** (equal), **neq** (not equal), **range** (range).
- *port*—Source or destination port of the packet.
- **destination-port**—Compares the destination port of the packet with the access condition.

To configure an access list named *alist1* containing a rule that allows any traffic using the TCP protocol on port 443 on the GSS device, enter the following:

```
gss1.example.com# config  
gss1.example.com(config)# access-list alist1 permit tcp any  
destination-port eq 443
```

Use the **access-list** command for each access list that you intend to add to this GSS device. See the [“Adding Rules to an Access List”](#) section for instructions about adding more rules to an access list that already exists.

The following example shows a completed access list (alist1):

```
gss1.example.com(config)# show access-list
```

```
access-list: alist1
  access-list alist1 permit tcp any destination-port range 20 23
  access-list alist1 permit tcp any eq 20
  access-list alist1 permit tcp any eq 21
  access-list alist1 permit tcp any eq 23
  access-list alist1 permit tcp any eq 49
  access-list alist1 permit tcp any destination-port eq 53
  access-list alist1 permit udp any destination-port eq 53
  access-list alist1 permit udp any eq 53
  access-list alist1 permit udp any eq 123 destination-port eq 123
  access-list alist1 permit udp any destination-port eq 161
  access-list alist1 permit tcp any destination-port eq 443
  access-list alist1 permit udp any eq 1304 destination-port eq 1304
  access-list alist1 permit udp any destination-port eq 2000
  access-list alist1 permit tcp any destination-port range 2001 2005
  access-list alist1 permit tcp any range 2001 2005
  access-list alist1 permit tcp any destination-port range 3002 3008
  access-list alist1 permit tcp any range 3002 3008
  access-list alist1 permit udp any destination-port eq 5002
  access-list alist1 permit udp any eq 1974 destination-port eq 1974
  access-list alist1 permit tcp any destination-port eq 5001
  access-list alist1 permit tcp any eq 5001
  access-list alist1 permit icmp any
```

Kernel output

```
access-list alist1 on interface eth0 (1 references)
target      prot opt source          destination
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp dpts:20:23
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp spt:20
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp spt:21
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp spt:23
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp spt:49
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0        0.0.0.0/0        udp dpt:53
ACCEPT     udp  --  0.0.0.0/0        0.0.0.0/0        udp spt:53
ACCEPT     udp  --  0.0.0.0/0        0.0.0.0/0        udp spt:123 dpt:123
ACCEPT     udp  --  0.0.0.0/0        0.0.0.0/0        udp dpt:161
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp dpt:443
ACCEPT     udp  --  0.0.0.0/0        0.0.0.0/0        udp spt:1304 dpt:1304
ACCEPT     udp  --  0.0.0.0/0        0.0.0.0/0        udp dpt:2000
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp dpts:2001:2005
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp spts:2001:2005
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp dpts:3002:3008
ACCEPT     tcp  --  0.0.0.0/0        0.0.0.0/0        tcp spts:3002:3008
```

```

ACCEPT      udp  --  0.0.0.0/0      0.0.0.0/0      udp dpt:5002
ACCEPT      udp  --  0.0.0.0/0      0.0.0.0/0      udp spt:1974 dpt:1974
ACCEPT      tcp  --  0.0.0.0/0      0.0.0.0/0      tcp dpt:5001
ACCEPT      tcp  --  0.0.0.0/0      0.0.0.0/0      tcp spt:5001
ACCEPT      icmp --  0.0.0.0/0      0.0.0.0/0
DROP        all  --  0.0.0.0/0      0.0.0.0/0

```

## Associating an Access List with a GSS Interface

After you create an access list, associate it with one or both of the GSS Ethernet interfaces before you use the access list to filter incoming traffic received by the interface. If no access lists are associated with an interface, the GSS allows all incoming traffic received on that interface. After you apply an access list, the GSS allows only the type of traffic explicitly permitted by the access list. The GSS disallows all other traffic.

You can associate an access list with a GSS interface by using the **access-group** command in global configuration mode. You must have access to the CLI of each GSS device to associate access lists with a GSS interface.

The syntax of this command is as follows:

```
access-group name interface {eth0 | eth1}
```

The keywords and arguments are as follows:

- **name**—Name of a pre-existing access list.
- **interface**—Specifies an interface on the GSS to which the access list will be assigned.
- **eth0**—Identifies the first Ethernet interface on the GSS device.
- **eth1**—Identifies the second Ethernet interface on the GSS device.

The GSS does not allow you to assign the same preexisting access list to both Ethernet interfaces on the GSS device. If you attempt to use the **access-group** CLI command to assign the same access list to Ethernet 0 and Ethernet 1, the following error message appears:

```
%access-list list1 is already assigned to interface eth1.
```

If this error message appears, generate an identical access list for the second Ethernet interface on the GSS device.

For example, to associate the access list named *alist1* with the first interface on your GSS device, enter the following:

```
gss1.example.com# config  
gss1.example.com(config)# access-group alist1 interface eth0
```

Use the **access-group** command for each access list that you want to associate with the interface.

## Disassociating an Access List from a GSS Interface

You can dissociate an access list from the associated GSS interface by using the **no** form of the **access-group** command. Disassociating an access list from an interface removes all constraints applied to the Ethernet interface. You must have access to the CLI of each GSS device to disassociate access lists from a GSS interface.

For example, to disassociate the access list named *alist1* from the first interface on your GSS device, you enter:

```
gss1.example.com# config  
gss1.example.com(config)# no access-group alist1 interface eth0
```

See the “[Associating an Access List with a GSS Interface](#)” section for an explanation of **access-group** command syntax.

## Adding Rules to an Access List

After you create one or more access lists, you can append rules to them at any time by using the **access-list** command.

For example, to add a new rule to the access list named *alist1* to block all traffic from host 192.168.1.101, enter:

```
gss1.example.com# config  
gss1.example.com(config)# access-list alist1 deny tcp host  
192.168.1.101
```

See the “[Creating an Access List](#)” section for an explanation of **access-list** command syntax.

Use the **show access-list** command to verify that the rule is added to your access list.

```
gss1.example.com(config)# show access-list
access-list:alist1
access-list alist1 permit tcp any destination-port eq 443
access-list alist1 deny tcp host 192.168.1.101
```

## Removing Rules from an Access List

Access lists must contain at least one rule. Removing the only rule from an access list removes the list itself from the GSS. You can remove a rule from an existing access list by using the **no** form of the **access-list** command in global configuration mode.

For example, to remove the rule from the access list named *alist1* that blocks all traffic from host 192.168.1.101, enter:

```
gss1.example.com# config
gss1.example.com(config)# no access-list alist1 deny tcp host
192.168.1.101
```

See the “[Creating an Access List](#)” section for an explanation of **access-list** command syntax.

Use the **show access-list** command to verify that the rule has been removed from your access list.

```
gss1.example.com(config)# show access-list
access-list:alist1
access-list alist1 permit tcp any destination-port eq 443
```

## Segmenting GSS Traffic by Ethernet Interface

By default, the GSS devices listen for DNS traffic on both GSS Ethernet interfaces, 0 and 1.

In the case of inter-GSS communications, GSS devices listen for configuration and status updates on one interface only. If you use the Cisco Application Networking Manager (ANM) to manage the GSS devices, the devices use this same interface for communication with the ANM. Ethernet interface 0 is the default.

You can reconfigure which interface is used for both inter-GSS and ANM communications by using the **gss-communications** command. See the *Cisco Global Site Selector Getting Started Guide* for details.

For security reasons you can limit GSS traffic to one Ethernet interface, or segment traffic by constraining a certain type of traffic on a designated interface. By using the **access-list** and **access-group** commands discussed previously, you can define access lists that limit traffic on either of the two GSS Ethernet interfaces.

For example, remote management services such as Telnet, SSH, and FTP listen on all active interfaces. To force these remote management services to listen on only the second GSS Ethernet interface, enter:

```
gss1.example.com# config
gss1.example.com(config)#
gss1.example.com(config)# access-list alist1 permit tcp any
destination-port ftp
gss1.example.com(config)# access-list alist1 permit tcp any
destination-port ssh
gss1.example.com(config)# access-list alist1 permit tcp any
destination-port telnet
gss1.example.com(config)# access-group alist1 interface eth1
```

The commands listed above limit the second Ethernet interface (eth1) to the specified traffic. All other traffic is refused to that interface.

To deny the same traffic on the first Ethernet interface (eth0), enter:

```
gss1.example.com(config)#
gss1.example.com(config)# access-list alist1 deny tcp any
destination-port ftp
gss1.example.com(config)# access-list alist1 deny tcp any
destination-port ssh
gss1.example.com(config)# access-list alist1 deny tcp any
destination-port telnet
gss1.example.com(config)# access-group alist1 eth0
```

## Displaying Access Lists

You can display all configured access lists by using the **show access-list** command.

```
gss1.example.com(config)# show access-list

access-list: alist1
  access-list alist1 permit tcp any destination-port range 20 23
  access-list alist1 permit tcp any eq 20
  access-list alist1 permit tcp any eq 21
```

```

access-list alist1 permit tcp any eq 23
access-list alist1 permit tcp any eq 49
access-list alist1 permit tcp any destination-port eq 53
access-list alist1 permit udp any destination-port eq 53
access-list alist1 permit udp any eq 53
access-list alist1 permit udp any eq 123 destination-port eq 123
access-list alist1 permit udp any destination-port eq 161
access-list alist1 permit tcp any destination-port eq 443
access-list alist1 permit udp any eq 1304 destination-port eq 1304
access-list alist1 permit udp any destination-port eq 2000
access-list alist1 permit tcp any destination-port range 2001 2005
access-list alist1 permit tcp any range 2001 2005
access-list alist1 permit tcp any destination-port range 3002 3008
access-list alist1 permit tcp any range 3002 3008
access-list alist1 permit udp any destination-port eq 5002
access-list alist1 permit udp any eq 1974 destination-port eq 1974
access-list alist1 permit tcp any destination-port eq 5001
access-list alist1 permit tcp any eq 5001
access-list alist1 permit icmp any

```

## Kernel output

```

access-list alist1 on interface eth0 (1 references)
target      prot opt source          destination
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp dpts:20:23
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp spt:20
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp spt:21
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp spt:23
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp spt:49
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp dpt:53
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp spt:53
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp spt:123 dpt:123
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp dpt:161
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp dpt:443
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp spt:1304 dpt:1304
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp dpt:2000
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp dpts:2001:2005
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp spts:2001:2005
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp dpts:3002:3008
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp spts:3002:3008
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp dpt:5002
ACCEPT     udp  --  0.0.0.0/0       0.0.0.0/0       udp spt:1974 dpt:1974
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp dpt:5001
ACCEPT     tcp  --  0.0.0.0/0       0.0.0.0/0       tcp spt:5001
ACCEPT     icmp --  0.0.0.0/0       0.0.0.0/0
DROP       all  --  0.0.0.0/0       0.0.0.0/0

```

Use the **show access-group** command to display a list of the access lists associated with GSS interfaces Ethernet 0 and Ethernet 1.

```
gss1.example.com(config)# show access-group
access group alist1 interface eth0
```

## Deploying GSS Devices Behind Firewalls

This section describes how to configure your GSS for deployment behind a firewall. It contains the following topics:

- [GSS Firewall Deployment Overview](#)
- [Configuring GSS Devices Behind a Firewall](#)

### GSS Firewall Deployment Overview

In addition to the packet-filtering features of the **access-list** and **access-group** commands (see the “[Filtering GSS Traffic Using Access Lists](#)” section), you can also deploy your GSS devices behind an existing firewall on your enterprise network.

When you configure your GSS for deployment behind a firewall, you must allow DNS traffic into the device. If you have multiple GSS devices deployed so that traffic between the devices must pass through a firewall, configure the firewall to allow inter-GSS communications and inter-GSS status reporting. Depending on your GSS configuration, you can also allow other traffic to pass through the firewall. This requirement depends on your GSS configuration (for example, if you are using TCP-based or KAL-AP keepalives) and the ability to access certain GSS services through the firewall (for example, SNMP).

The GSS does not support deployment of devices behind a NAT for inter-GSS communication. The communication between the GSS devices cannot include an intermediate device behind a NAT because the actual IP address of the devices is embedded in the payload of the packets.

To configure your firewall to function with a GSS device, follow the guidelines outlined in [Table 5-2](#) and [Table 5-3](#) to permit inbound and outbound traffic transmitted to and received from the specified GSS ports. If you are using stateful firewalls, the rules for return traffic outlined in [Table 5-2](#) and [Table 5-3](#) may not be required.

In addition, use the **access-list** and **access-group** commands to enable authorized GSS traffic to the specified ports. By default, the GSS interface blocks all ports not explicitly permitted in your access list once you associate the access list with an Ethernet interface.

**Table 5-2 Inbound Traffic Going Through a Firewall to the GSS**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
*	20–23	TCP	FTP, SSH, and Telnet services
49 or user configured	*	TCP	Return traffic for TACACS+
*	53	UDP, TCP	GSS DNS server traffic
53	*	UDP	Return traffic of GSS software reverse lookup, “dnslookup” queries, and name server forwarding
80 or user-configured	*	TCP	Return traffic of TCP and HTTP keepalives
123	123	UDP	Return traffic of NTP updates
*	161	UDP	SNMP traffic
*	443	TCP	Primary GSSM GUI
1304	1304	UDP	Return traffic of CRA keepalives
1974	1974	UDP	Return traffic of DRP protocol traffic
*	2000	UDP	Inter-GSS periodic status reporting
*	2001–2005	TCP	Inter-GSS communication
2001-2005	*	TCP	Return traffic of inter-GSS communication
*	3002–3008	TCP	Inter-GSS communication
3002-3008	*	TCP	Return traffic of inter-GSS communication

**Table 5-2 Inbound Traffic Going Through a Firewall to the GSS (continued)**

Source Port (Remote Device)	Destination Port (GSS)	Protocol	Details
*	3009	TCP	Received traffic of Cisco ANM communication
*	5001	TCP	Global sticky mesh protocol traffic
3340	*	TCP	Sticky and Config Agent communication
3341	*	TCP	Sticky communication source
3342	*	TCP	Sticky and DNS processes communication
5001	*	TCP	Return traffic of global sticky mesh protocol traffic
5002	*	UDP	Return traffic of KAL-AP keepalives

\*Any legal port number

**Table 5-3 Outbound Traffic Originating from the GSS**

Source Port (GSS)	Destination Port (Remote Device)	Protocol	Details
20–23	*	TCP	Return traffic of FTP, SSH, and Telnet server services on the GSS
*	49 or user configured	TCP	TACACS+
*	20–23	TCP	Traffic of FTP, SCP, and Telnet GSS CLI commands
53	*	UDP, TCP	Return traffic of GSS DNS server traffic

**Table 5-3** *Outbound Traffic Originating from the GSS (continued)*

<b>Source Port (GSS)</b>	<b>Destination Port (Remote Device)</b>	<b>Protocol</b>	<b>Details</b>
*	53	UDP	GSS software reverse lookup, “dnslookup” queries, and name server forwarding
*	80 or user-configured	TCP	TCP and HTTP keepalives
123	123	UDP	NTP updates
161	*	UDP	Return traffic of SNMP traffic
443	*	TCP	Return traffic of Primary GSSM GUI
1304	1304	UDP	CRA keepalives
1974	1974	UDP	DRP protocol traffic
*	2000	UDP	Inter-GSS periodic status reporting
*	2001–2005	TCP	Inter-GSS communication
2001-2005	*	TCP	Return traffic of inter-GSS communication
*	3002–3008	TCP	Inter-GSS communication
3002-3008	*	TCP	Return traffic of inter-GSS communication
3009	*	TCP	Return traffic of Cisco ANM communication
3340	*	TCP	Sticky and Config Agent communication
3341	*	TCP	Sticky communication source
3342	*	TCP	Sticky and DNS processes communication
*	5001	TCP	Global sticky mesh protocol traffic

**Table 5-3** *Outbound Traffic Originating from the GSS (continued)*

Source Port (GSS)	Destination Port (Remote Device)	Protocol	Details
5001	*	TCP	Return traffic of global sticky mesh protocol traffic
*	5002	UDP	KAL-AP keepalives

\*Any legal port number

## Configuring GSS Devices Behind a Firewall

To configure GSS devices to operate behind a firewall, perform the following steps:

1. Determine the level of access and the services that you want enabled on your GSS and GSSM devices. Decide if you want to:
  - Allow FTP, SSH, and Telnet access to the GSS device
  - Permit GUI access to the primary GSSM

[Table 5-2](#) and [Table 5-3](#) list the GSS-related ports and protocols to enable for the GSS device to function properly.
2. Construct your access lists to filter traffic incoming and outgoing from your GSS device. See the “[Creating an Access List](#)” section for details.