Creating and Managing IP Access Control Lists for Cisco WAAS Devices

This chapter describes how to use the Cisco Wide Area Application Services (Cisco WAAS) Central Manager GUI to centrally create and manage IP access control lists (ACLs) for your Cisco WAAS devices.

This chapter contains the following sections:

Note You must log in to the WAAS Central Manager GUI using an account with admin privileges to view, edit, or create IP ACL configurations.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the WAAS Central Managers and Cisco Wide Area Application Engines (Cisco WAEs) in your network. The term WAE refers to WAE appliances, WAE Network Modules (the Cisco NME-WAE family of devices).

Overview of IP ACLs for WAAS Devices

In a centrally managed WAAS network environment, administrators should be able to prevent unauthorized access to various devices and services. IP ACLs can filter packets by allowing you to permit or deny IP packets destined for a WAAS device.

The WAAS software supports standard and extended ACLs that allow you to restrict access to a WAAS device. The WAAS software can use the following types of ACLs:

- Interface ACL—Applied on the built-in, port channel, standby, and inline group interfaces. This type of ACL is intended to control management traffic (Telnet, SSH, and Central Manager GUI). The ACL rules apply only to traffic that is destined for the WAE or originates from the WAE, not Web Cache Communication Protocol (WCCP) transit traffic. Use the **ip access-group** interface configuration command to apply an interface ACL.

- Interception ACL—Applied globally to a WAAS device. This type of ACL defines what traffic is to be intercepted. Traffic that is permitted by the ACL is intercepted and traffic that is denied by the ACL is passed through the WAE. Use the **interception access-list** global configuration command to apply an interception ACL. For more information on using interception ACLs, see Configuring Interception Access Control Lists in Chapter 5, "Configuring Traffic Interception."
- WCCP ACL—Applied on inbound WCCP-redirected traffic to control access between an external server and external clients. The WAE acts like a firewall. Use the **wccp access-list** global configuration command to apply a WCCP ACL.
- SNMP ACL—Applied on an SNMP agent to control access to the SNMP agent by an external SNMP server that is polling for SNMP MIBs or SNMP statistics. Use the **snmp-server access-list** global configuration command to apply an SNMP ACL.
- Transaction-logs-flow ACL—Applied on the transaction logging facility to restrict the transactions to be logged. Use the **transaction-logs flow access-list** global configuration command to apply a transaction log ACL.

The following examples illustrate how interface ACLs can be used in environments that have WAAS devices:

- A WAAS device resides on the customer premises and is managed by a service provider, and the service provider wants to secure the device for its management only.
- A WAAS device is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit access to Telnet, SSH, and the WAAS Central Manager GUI to the IT source subnets.

To use ACLs, you must first configure ACLs and then apply them to specific services or interfaces on the WAAS device. The following are some examples of how interface ACLs can be used in various enterprise deployments:

- An application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access, primarily for security reasons. Because the interface is outside, many types of attacks are possible.) The WAAS device's outside address is globally accessible from the Internet, while its inside address is private. The inside interface has an ACL to limit Telnet, SSH, and GUI access.
- A WAE that is using WCCP is positioned on a subnet off the Internet router. Both the WAE and the router must have IP ACLs. IP access lists on routers have the highest priority, followed by IP ACLs that are defined on the WAEs.

Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to centrally configure and apply ACLs to your WAAS devices. For more information, see the Creating and Managing IP ACLs for WAAS Devices.

Creating and Managing IP ACLs for WAAS Devices

This section provides guidelines and an example of how to use the WAAS Central Manager GUI to create and manage IP ACLs for your WAAS devices.

When you create an IP ACL, you should note the following important points:

- IP ACL names must be unique within the device.
- IP ACL names must be limited to 30 characters and contain no white space or special characters.

- Each WAAS Central Manager device can manage up to 50 IP ACLs and a total of 500 conditions per device.
- When the IP ACL name is numeric, numbers 1 through 99 denote standard IP ACLs and numbers 100 through 199 denote extended IP ACLs. IP ACL names that begin with a number cannot contain nonnumeric characters.
- The WAAS Central Manager GUI allows the association of standard IP ACLs with SNMP and WCCP. Any device that attempts to access one of these applications associated with an ACL must be on the list of trusted devices to be allowed access.
- You can associate any previously configured standard IP ACL with SNMP and WCCP. However, you can associate an extended IP ACL only with the WCCP application.
- You can delete an IP ACL, including all conditions and associations with network interfaces and applications, or you can delete only the IP ACL conditions. Deleting all conditions allows you to change the IP ACL type if you choose to do so. The IP ACL entry continues to appear in the IP ACL listing. However, it is, in effect, nonexistent.
- If you specify an empty ACL for any of the ACL types used by WAAS, it permits all traffic.

To use the WAAS Central Manager GUI to create and modify an IP ACL for a single WAE, associate an IP ACL with an application, and then apply it to an interface on the WAE, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Configure** > **Network** > **TCP/IP Settings** > **IP ACL**.

The IP ACL window appears. By default, there are no IP ACLs defined for a WAE. The IP ACL window indicates if there are currently no IP ACLs configured for the WAE.

Step 3 Click **Add IP ACL** on the table heading row.

The **IP ACL** window appears. Fill in the fields as follows:

- In the Name field, enter a name, for example, test1. IP ACL names must be unique within the device, must be limited to 30 characters, and cannot contain any white spaces or special characters.

  By default, this new IP ACL is created as a standard ACL.
- To change this default setting and create this new ACL as an extended ACL, choose **Extended** from the ACL Type drop-down list.

Step 4 Click **OK** to save the IP ACL named test1. IP ACLs without any conditions defined do not appear on the individual devices.

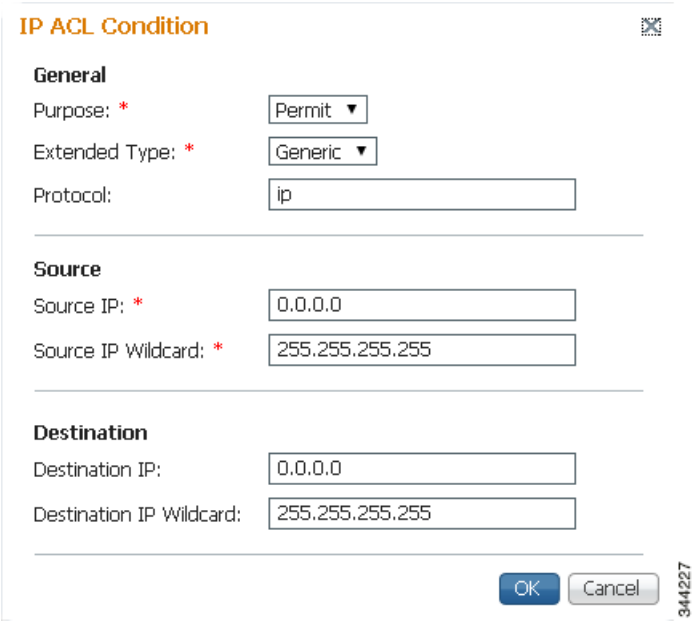
Step 5 Add conditions to the standard IP ACL named test1 that you just created:

a. Click the **Add IP ACL Condition**.

The IP ACL Condition window appears (Figure 9-1).

Note The number of available fields for creating IP ACL conditions depends on the type of IP ACL that you have created, either standard or extended.

Figure 9-1 Creating a New Condition for an Extended IP ACL Window



b. Enter values for the properties that are enabled for the type of IP ACL that you are creating, as follows:
   - To set up conditions for a standard IP ACL, go to Step 6.
   - To set up conditions for an extended IP ACL, go to Step 7.

Step 6 Set up conditions for a standard IP ACL:

a. From the Purpose drop-down list, choose a purpose (**Permit** or **Deny**).

b. In the Source IP field, enter the source IP address.

c. In the Source IP Wildcard field, enter a source IP wildcard address.

d. Click **OK** to save the condition.

   IP ACL conditions for the newly created IP ACL and its configured parameters are displayed in Table 9-1.

e. To add another condition to the IP ACL, select it and click **Add IP ACL Condition**.

f. Enter the details of the condition and click **OK** to save the additional condition.

g. For a newly created IP ACL condition to appear in a particular position, select the position and click **Insert**. The IP ACL condition is placed in the selected position.

h. To rearrange your list of conditions, select the condition (or multiple consecutive conditions) and use the Up or Down arrows, and click **Save Moved Rows** to commit the changes.
   Alternatively, you can select one or multiple consecutive conditions and click **Move to**, to specify the row number in which the IP ACL condition should be positioned. This is especially helpful when there are numerous conditions listed in the table. After you are satisfied with all your entries and the order in which the conditions are listed, click **Save Moved Rows** to commit the changes.

Note The order of the conditions listed in the WAAS Central Manager GUI becomes the order in which IP ACLs are applied to the device.

Note Click a column heading to sort by a configured parameter.

Table 9-1 describes the fields in a standard IP ACL.

Table 9-1 Standard IP ACL Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Source IP	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.

Step 7 Set up conditions for an extended IP ACL:

a. From the Purpose drop-down list, choose a purpose (**Permit** or **Deny**).

b. From the Extended Type drop-down list, choose a value (**Generic**, **TCP**, **UDP**, or **ICMP**). (See Table 9-2.)

Table 9-2 Extended IP ACL Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed or dropped. Choices are Permit or Deny.
Extended Type	Generic	Specifies the Internet protocol to be applied to the condition. When selected, the GUI window refreshes with applicable field options enabled. The options are generic, TCP, UDP, or ICMP.

After you choose a type of extended IP ACL, various options become available in the GUI, depending on what type you choose.

c. In the fields that are enabled for the chosen type, enter the data. (For more information, see Table 9-4 through Table 9-7.)

d. Click **OK** to save the condition.

IP ACL conditions for the newly created IP ACL and its configured parameters are displayed in Table 9-1.

e. To add another condition to the IP ACL, select it and click **Add IP ACL Condition**.

f. Enter the details of the condition in the window and click **OK** to save the additional condition.

g. For a newly created IP ACL condition to appear in a particular position, select the position and click **Insert**. The IP ACL condition is placed in the selected position.

h. To rearrange your list of conditions, select the condition (or multiple consecutive conditions) and use the Up or Down arrows. Click **Save Moved Rows** to commit the changes.
Alternatively, you can select one or multiple consecutive conditions and click **Move to**, to specify

the row number in which the IP ACL condition should be positioned. This is especially helpful when there are numerous conditions listed in the table. After you are satisfied with all your entries and the order in which the conditions are listed, click **Save Moved Rows** to commit the changes.

Note The order of the conditions listed in the WAAS Central Manager GUI becomes the order in which IP ACLs are applied to the device.

Note Click a column heading to sort by any configured parameter.

Step 8 Modify or delete an individual condition from an IP ACL:

a. Select the name of the IP ACL whose condition you want to modify.

b. A list of all the conditions that are currently applied to the IP ACL appears in the IP ACL Conditions, Table 9-1. Select the condition and click **Edit**.

c. To modify the condition, change any corresponding field as necessary in the IP ACL Condition window and click **OK** to save the modifications.

d. To delete the condition, select it and click **Delete** on the table header.

e. To rearrange your list of conditions, use the Up or Down arrows or the **Move to** column outlined in Step 6f and 7f.

Step 9 Associate a standard IP ACL with SNMP or WCCP:

a. Click the **Edit** icon next to the name of the device for which you want to associate a standard IP ACL with SNMP or WCCP.

b. Choose **Configure** > **Network** > **TCP/IP Settings** > **IP ACL Feature Usage**.

The IP ACL Feature Settings window appears.

c. From the SNMP or WCCP drop-down lists, choose the name of an IP ACL for SNMP or WCCP. (For more details, see Table 9-3.) If you do not want to associate an IP ACL with one of the applications, choose **Do Not Set**.

Table 9-3 IP ACL Feature Settings

Cisco WAAS Central Manager GUI Parameter	Function
SNMP	Associates a standard IP ACL with SNMP. This option is supported for all WAAS devices.
WCCP	Associates any of the IP ACLs with WCCP Version 2. This option is supported only for WAAS devices that are operating in WCCP interception mode and not for WAAS Central Manager devices.

d. Click **Submit** to save the settings.

Step 10 Apply an IP ACL to an interface:

a. Click the **Edit** icon next to the name of the device for which you want to apply an IP ACL to an interface on the WAE.

b. Choose **Configure** > **Network** > **Network Interfaces**.

The Network Interfaces window for the device appears. This window displays all the interfaces available on that device.

c. Click the **Edit** icon next to the name of the interface to which you want to apply an IP ACL.

The Network Interface settings window appears.

d. From the Inbound ACL drop-down list at the bottom of the window, choose the name of an IP ACL.

e. From the Outbound ACL drop-down list, choose the name of an ACL.

The only network interface properties that can be altered from the WAAS Central Manager GUI are the inbound and outbound IP ACLs. All other property values are populated from the device database and are read-only in the WAAS Central Manager GUI.

Step 11 Click **Submit** to save the settings.

Step 12 To use an IP ACL to define the traffic that should be intercepted, see the Configuring Interception Access Control Lists in Chapter 5, "Configuring Traffic Interception."

Step 13 (Optional) Delete an IP ACL:

a. Click the **Edit** icon next to the name of the device that has the IP ACL that you want to delete.

b. Choose **Configure > Network > TCP/IP Settings > IP ACL**.

If you created conditions for the IP ACL, you have two options for deletion:

- **Delete ACL**—Removes the IP ACL, including all the conditions and associations with network interfaces and applications.
- **Delete All Conditions**—Removes all the conditions, while preserving the IP ACL name.

c. To delete the entire IP ACL and its conditions, select the corresponding IP ACL and click **Delete**. You are prompted to confirm your action. Click **OK**. The record is deleted.

d. To delete only the conditions, select the condition or multiple conditions (consecutive or nonconsecutive conditions) and click **Delete**. When you are prompted to confirm your action, click **OK**. The conditions are deleted.

To define an IP ACL from the CLI, you can use the **ip access-list** global configuration command, and to apply the IP ACL to an interface on the WAAS device, you can use the **ip access-group** interface configuration command. To configure the use of an IP ACL for SNMP, you can use the **snmp-server access-list** global configuration command. To specify an IP ACL that the WAE applies to the inbound WCCP redirected traffic that it receives, you can use the **wccp access-list** global configuration command. To configure an interception ACL, you can use the **interception access-list** global configuration command.

List of Extended IP ACL Conditions

When you define a condition for an extended IP ACL, you can specify the Internet protocol to be applied to the condition (as described in Step 7 in the Creating and Managing IP ACLs for WAAS Devices).

The list of extended IP ACL conditions are as follows:

- Generic (Table 9-4)
- TCP (Table 9-5)
- UDP (Table 9-6)

- ICMP (Table 9-7)

Table 9-4 Extended IP ACL Generic Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	Generic	Matches any IP.
Protocol	ip	IP (**gre**, **icmp**, **ip**, **tcp**, or **udp)**. To match any IP, use the keyword **ip**.
Source IP[1]	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard[1]	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.

Table 9-5 Extended IP ACL TCP Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	TCP	Matches the TCP IP.
Established	Unchecked (false)	When checked, a match with the ACL condition occurs if the TCP datagram has the ACK or RST bits set, indicating an established connection. Initial TCP datagrams used to form a connection are not matched.
Source IP	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Source Port 1	0	Decimal number or name of a TCP port. Valid port numbers are 0 to 65535. Valid TCP port names are as follows: **ftp**, **ftp-data**, **https**, **mms**, **netbios-dgm**, **netbios-ns**, **netbios-ss**, **rtsp**, **ssh**, **telnet**, and **www**.

Table 9-5 Extended IP ACL TCP Conditions (continued)

Field	Default Value	Description
Source Operator	range	Specifies how to compare the source ports against incoming packets. Choices are <, >, ==, !=, or range.
Source Port 2	65535	Decimal number or name of a TCP port. See Source Port 1, in this table.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination Port 1	0	Decimal number or name of a TCP port. Valid port numbers are 0-65535. Valid TCP port names are as follows: **ftp**, **ftp-data**, **https**, **mms**, **netbios-dgm**, **netbios-ns**, **netbios-ss**, **rtsp**, **ssh**, **telnet**, and **www**.
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a TCP port. See Destination Port 1, in this table.

Table 9-6 Extended IP ACL UDP Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	UDP	Matches the UDP IP.
Established	—	Not available for UDP.
Source IP	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Source Port 1	0	Decimal number or name of a UDP port. Valid port numbers are 0-65535. Valid UDP port names are as follows: **bootpc**, **bootps**, **domain**, **mms**, **netbios-dgm**, **netbios-ns**, **netbios-ss**, **ntp**, **snmp**, **snmptrap**, **tacacs**, **tftp**, and **wccp**.
Source Operator	range	Specifies how to compare the source ports against incoming packets. Choices are <, >, ==, !=, or range.
Source Port 2	65535	Decimal number or name of a UDP port. See Source Port 1, in this table.

Table 9-6 Extended IP ACL UDP Conditions (continued)

Field	Default Value	Description
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination Port 1	0	Decimal number or name of a UDP port. Valid port numbers are 0-65535. Valid UDP port names are as follows: **bootpc**, **bootps**, **domain**, **mms**, **netbios-dgm**, **netbios-ns**, **netbios-ss**, **ntp**, **snmp**, **snmptrap**, **tacacs**, **tftp**, and **wccp**.
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a UDP port. See Destination Port 1, in this table.

Table 9-7 Extended IP ACL ICMP Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	ICMP	Matches the ICMP IP.
Source IP	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.

Table 9-7 Extended IP ACL ICMP Conditions (continued)

Field	Default Value	Description
ICMP Param Type	None	The ICMP parameter choices are **None**, **Type/Code**, or **Msg**. • **None**—Disables the ICMP Type, Code, and Message fields. • **Type/Code**—Allows ICMP messages to be filtered by ICMP message type and code. Also enables the ability to set an ICMP message code number. • **Msg**—Allows a combination of type and code to be specified using a keyword. Activates the ICMP message drop-down list. Disables the ICMP Type field.
ICMP Message	administratively-prohibited	Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list.
ICMP Type	0	Number from 0-255. This field is enabled when you choose **Type/Code**.
Use ICMP Code	Unchecked	When checked, enables the ICMP Code field.
ICMP Code	0	Number from 0-255. Message code option that allows ICMP messages of a particular type to be further filtered by an ICMP message code.