

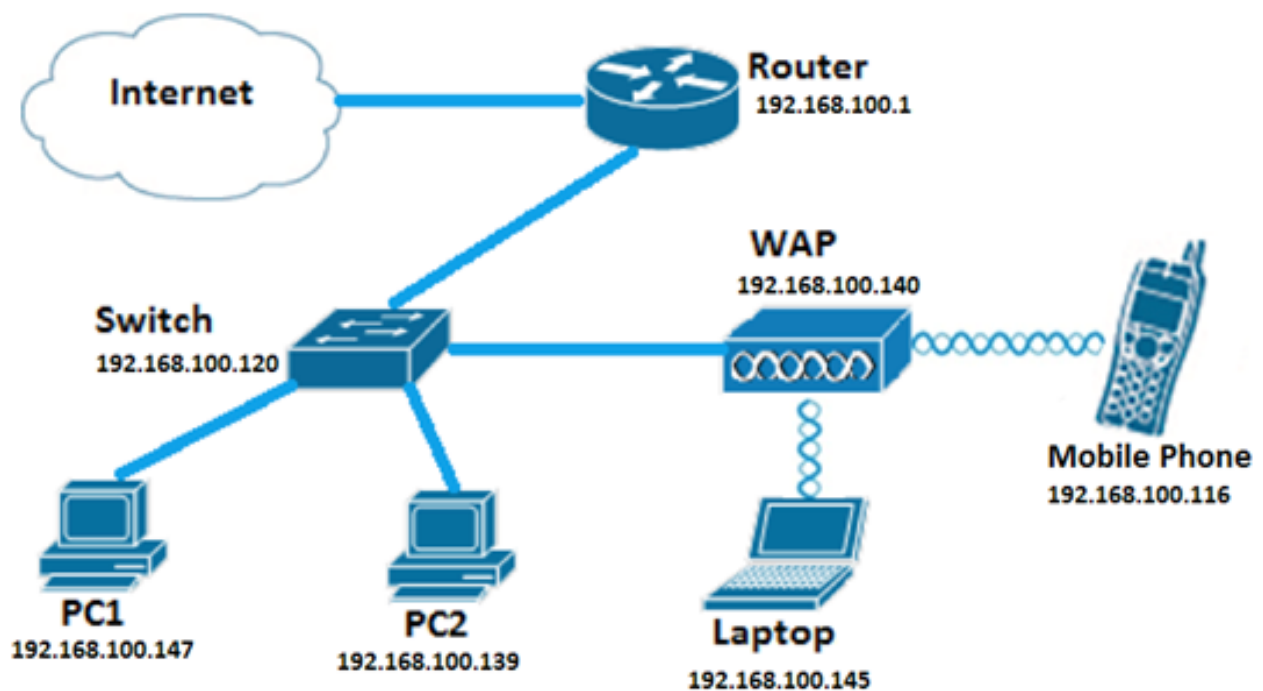
Configure IPv4 ACL on the WAP125 and WAP581

Introduction

Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) Access Control Lists (ACLs) are a set of rules applied to packets received by the Wireless Access Point (WAP). Each rule is used to determine whether access to the network should be permitted or denied. The ACLs can be configured to inspect fields of a frame like the source or destination IP address, the Virtual Local Area Network (VLAN) Identifier (ID), or the Class of Service (CoS). When a frame enters the WAP device port, it inspects the frame and checks the ACL rules against the content of the frame. If any of the rules match the content, a permit or deny action is taken on the frame.

Configuring IPv4 ACLs is typically used to authorize access to network resources to select devices in the network.

Note: There is an implicit deny at the end of every rule created.



Note: In this scenario, all traffic from PC2 will be allowed to access the network. All other traffic from other hosts will be denied.

Objective

This article aims to show you how to configure an IPv4 ACL on a WAP125 and WAP581 Access Point.

Applicable Devices

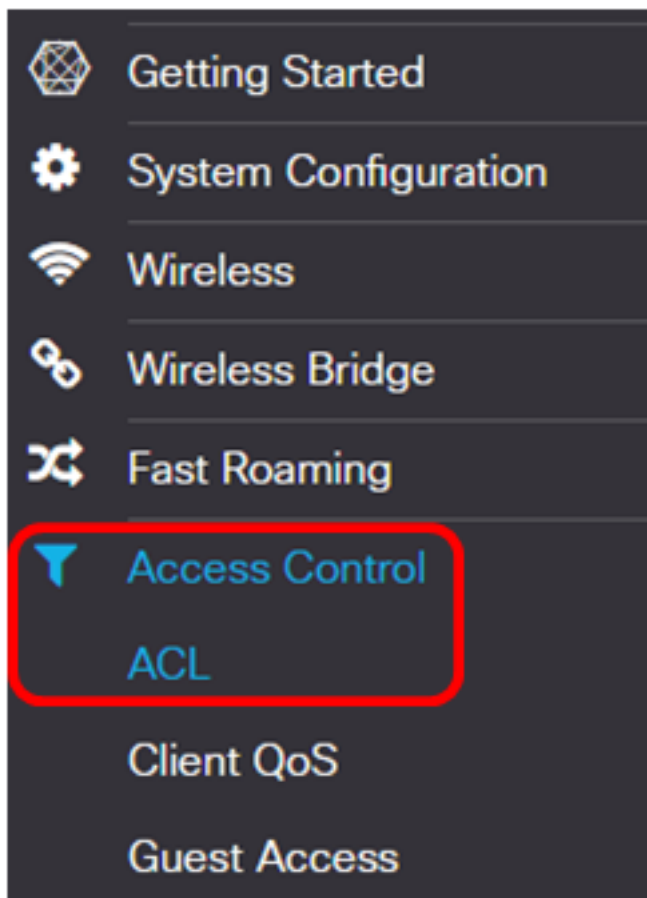
- WAP125
- WAP581

Software Version

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Configure an IPv4 ACL

Step 1. Log in to the web-based utility of the WAP and choose **Access Control > ACL**.



Step 2. Click the **+** button to create a new ACL.

ACL Table



Step 3. Enter a name for the ACL in the *ACL Name* field.

ACL Table

+ ✎ 🗑

| <input type="checkbox"/> | Enable | ACL Name | ACL Type |
|-------------------------------------|-------------------------------------|-------------|----------|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | IPv4TestACL | IPv4 |

Note: In this example, IPv4TestACL is entered.

Step 4. Choose IPv4 from the ACL Type drop-down list.

ACL Table

+ ✎ 🗑

| <input type="checkbox"/> | Enable | ACL Name | ACL Type |
|-------------------------------------|-------------------------------------|-------------|----------|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | IPv4TestACL | IPv4 |

IPv4
IPv6
MAC

Step 5. Click the + button and choose an interface from the Associated Interface drop-down list. The options are:

- 2.4G VAP 0 (SSID Name) — This option will apply the MAC ACL to the 2.4 GHz Virtual Access Point (VAP). The SSID Name section may change depending on the SSID name configured on the WAP.
- 5G VAP0 (SSID Name) — This option will apply the MAC ACL to the 5 GHz VAP.
- Ethernet Port — This option will apply the MAC ACL to the Ethernet interface of the WAP.

Associated Interface

☒ 2.4G VAP 0 (CiscoSB)

☒ 2.4G VAP 1 (CiscoTest)

☒ 5G VAP 0 (MyNetwork)

☒ Ethernet Port

OK Cancel

Note: Multiple interfaces can be associated to an ACL. However, it cannot be associated to an ACL when it has already been associated to another ACL. In this example, all interfaces are being associated to IPv4TestACL. Uncheck the box to disassociate the interface from the ACL.

Step 6. Click **OK**.

Associated Interface

☒ 2.4G VAP 0 (CiscoSB)

☒ 2.4G VAP 1 (CiscoTest)

☒ 5G VAP 0 (MyNetwork)

☒ Ethernet Port

OK Cancel

Step 7. Click the **More...** button to configure the parameters of the ACL.

Details Of Rule(s)

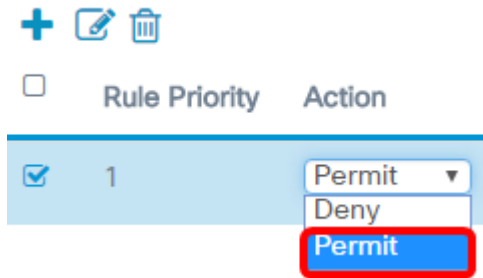
More...

Step 8. Click the **+** button to add a new rule.

☒ Rule Priority

Step 9. Choose an action from the Action drop-down list. The options are:

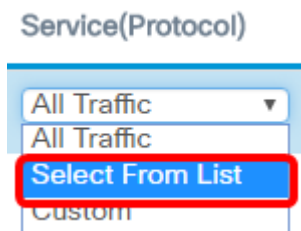
- Permit — This option will allow packets that match the ACL criteria to connect to the network..
- Deny — This option will prevent packets that match the ACL criteria from connecting to the network.



Note: In this example, Permit is chosen.

Step 10. Choose a service or protocol to be filtered from the Service (Protocol) drop-down list. The options are:

- All Traffic — This option will treat all packets as a match to the ACL filter.
- Select From List — This option will allow you to choose IP, ICMP, IGMP, TCP, or UDP as filters for the ACL. If this option is chosen, proceed to Step 11.
- Custom — This option will allow you to enter a custom protocol identifier as a filter for the packets. The value is a four-digit hexadecimal number. The range is 0 to 255.



Note: In this example, Select from List is chosen.

Step 11. Define the Protocol that needs to be allowed to connect to the network. The options are:

- ip — This option will let the access point filter the hosts accessing the network using their IP address as the filter.
- icmp — This option will let the access point filter Internet Control Message Protocol (ICMP) packets entering the network through the access point.
- igmp — This option will let the access point filter Internet Group Management Protocol (IGMP) packets entering the network through the access point.
- tcp — This option will let the access point filter Transmission Control Protocol (TCP) packets entering the network through the access point.
- udp — This option will let the access point filter User Datagram Protocol (UDP) packets entering the network through the access point.

Service(Protocol) Source IPv4 Address

Select From List Any

ip
icmp
igmp
tcp
udp

Note: In this example, ip is chosen.

Step 12. Define the Source IPv4 Address from the Source IPv4 Address drop-down list. The options are:

- Any — This option will let the WAP apply the filter to packets from any IP address.
- Single Address — This option will let the WAP apply the filter to packets from a specified IP address.
- Address/Mask — This option will let the WAP apply the filter to packets to an IP address and the mask of the IP.

Source IPv4 Address Source Port

Any All Traffic

Any

Single Address

Address/Mask

Note: In this example, Single Address is chosen.

Step 13. Enter the IP Address of the host that needs to be permitted when accessing the network.

Source IPv4 Address

Single Address

192.168.100.139

Note: In this example, 192.168.100.139 is entered. This is the IP address of PC2.

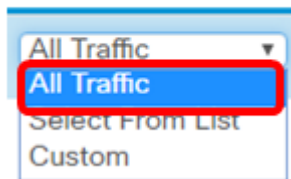
Step 14. Choose a source port for the condition. The options are:

- All Traffic — This option will allow all packets from the source port that meets the criteria.
- Select From List — This option allows you to choose ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www.
- Custom — This option will allow you to enter an IANA port number to match the source port identified in the datagram header. The port range is from 0 to 65535 and includes the following:

- 0 to 1023 — Well known ports
- 1024 — 49151 — Registered ports

- 49152 — 65535 — Dynamic and/or private ports

Source Port



A screenshot of a web interface showing a dropdown menu for 'Source Port'. The menu is open, displaying three options: 'All Traffic' (highlighted with a red rectangle), 'Select From List', and 'Custom'. The 'All Traffic' option is currently selected.

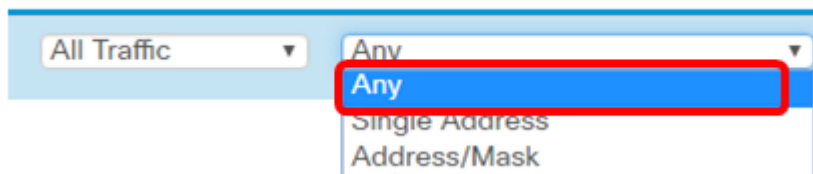
Note: In this example, All Traffic is chosen.

Step 15. Choose a destination address from the Destination IPv4 Address drop-down list. The options are:

- Any — This option treats any IP address as a match to the ACL statement.
- Single Address — This option lets you enter a specific IP address for the ACL condition.
- Address/Mask — This option lets you enter an IP address range or mask.

Source Port

Destination IPv4 Address



A screenshot of a web interface showing two dropdown menus. The 'Source Port' dropdown is set to 'All Traffic'. The 'Destination IPv4 Address' dropdown is open, showing three options: 'Any' (highlighted with a red rectangle), 'Single Address', and 'Address/Mask'. The 'Any' option is currently selected.

Note: In this example, Any is chosen.

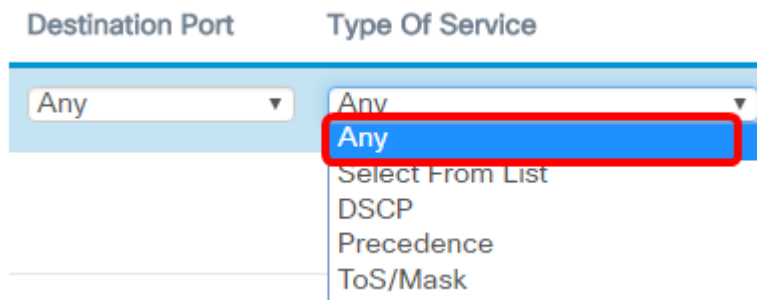
Step 16. Choose a destination port from the Destination Port drop-down list. The options are:

- Any — This option treats all of the destination ports of the packets as a match to the statement in the ACL.
- Select From List — This option lets you choose a keyword associated with the destination port to match. The options are: ftp, ftpdata, http, smtp, snmp, telnet, tftp, and www. These keywords translate to their corresponding port numbers.
- Custom — This option will allow you to enter an IANA port number to match the source port identified in the datagram header. The port range is from 0 to 65535 and includes the following:
 - 0 to 1023 — Well known ports
 - 1024 — 49151 — Registered ports
 - 49152 — 65535 — Dynamic and/or private ports

Step 17. Choose a type of service to match the packet type from the Type of Service drop-down list. The options are:

- Any — This option treats any service as a match for the packets.
- Select From List — This option matches the packets based on their Differentiated Services Code Point, (DSCP), Class of Service (CoS), or Expedited Forwarding (EF) values.
- DSCP — The option matches the packets based on their custom DSCP value. When choosing this option, enter a value from 0 to 63 in the DSCP Value field.
- Precedence — This option matches the packets based on their IP precedence value. When this option is chosen, enter an IP Precedence value from 0 to 7.

- ToS/Mask — This option lets you enter an IP ToS Mask to identify the bit positions in the IP Tos Bits value that are used for comparison against the IP ToS field in a packet.

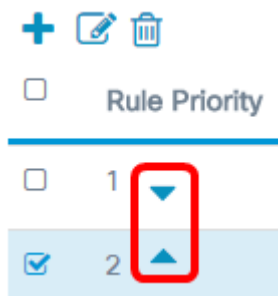


The screenshot shows a configuration interface with two dropdown menus. The first is labeled 'Destination Port' and has 'Any' selected. The second is labeled 'Type Of Service' and has a dropdown menu open. The menu options are 'Any', 'Select From List', 'DSCP', 'Precedence', and 'ToS/Mask'. The 'Any' option is highlighted with a red rectangle.

Step 18. (Optional) Repeat Step 8 to Step 17 until the ACL is complete.

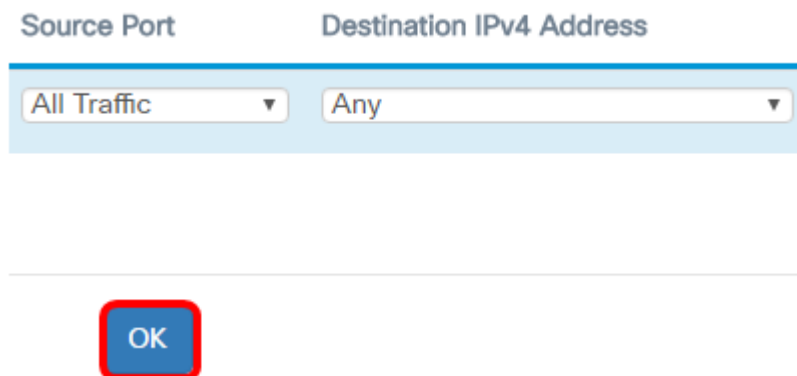
Note: Since there is an implicit deny at the end of every rule created, there is no need to add a deny rule to the ACL to prevent access from other devices in the network.

Step 19. (Optional) Change the order of the conditions on the ACL by clicking the up and down buttons until they are in the correct order.



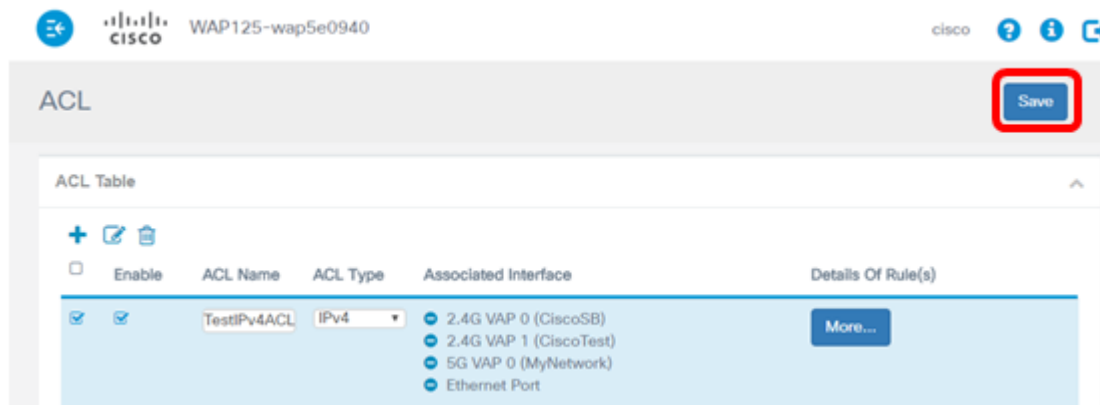
The screenshot shows a configuration interface with a 'Rule Priority' section. At the top, there are three icons: a plus sign, a pencil, and a trash can. Below them is a checkbox labeled 'Rule Priority'. Underneath, there is a table with two columns: a checkbox and a number. The first row has an unchecked checkbox and the number '1'. The second row has a checked checkbox and the number '2'. The 'Rule Priority' section is highlighted with a red rectangle.

Step 20. Click **OK**.



The screenshot shows a configuration interface with two dropdown menus. The first is labeled 'Source Port' and has 'All Traffic' selected. The second is labeled 'Destination IPv4 Address' and has 'Any' selected. Below these is a red button labeled 'OK'.

Step 21. Click **Save**.



You should now have completed setting up an IPv4 ACL that would allow only one host to access the network when connected to the WAP.