Configure IP-Based and URL-Based Access Control Policies

IP-based access control policies

An IP-based access control policy controls the traffic going into and coming out of a Cisco device in the same way that an Access Control List (ACL) does. As with an ACL, an IP-based access control policy contains lists of permit and deny conditions that are applied to traffic flows based on various criteria, including the protocol type, source IP address, destination IP address, or destination port number.

IP-based access control policies can be used to filter traffic for various purposes, including security, monitoring, route selection, and network address translation.

An IP-based access control policy has two main components:

- **IP Network Groups**: IP network groups comprise IP subnets that share the same access control requirements. These groups can be defined only in Catalyst Center. An IP network group may have as few as one IP subnet in it.
- **Access Contract**: An access contract is a common building block that is used in both IP-based and group-based access control policies. It defines the rules that make up the access control policies. These rules specify the actions (permit or deny) done when traffic matches a specific port or protocol and the implicit actions (permit or deny) done when no other rules match.

Workflow to configure an IP-based access control policy

Before you begin

- Cisco ISE is not mandatory if you are adding groups within the **Policy** > **IP & URL Based Access Control** > **IP Network Groups** window while creating a new IP-based access control policy.
- If your browser or network has proxy settings configured, include the proxy subnets in the IP access control policy.
- Make sure that you have defined these global network settings and provision the device:
  - Network servers, such as AAA, DHCP, and DNS servers. For more information, see Configure global network servers.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Configure global device credentials.
  - IP address pools. For more information, see Configure IP address pools.
  - Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see Configure global wireless settings.

Procedure

Step 1 Create IP network groups.

For more information, see Create an IP Network Group, on page 3.

Step 2 Create an IP-based access control contract.

An IP-based access control contract defines a set of rules between the source and destination. These rules dictate the action (allow or deny) that network devices perform based on the traffic that matches the specified protocols or ports. For more information, see Create an IP-based access control contract, on page 4.

Step 3 Create an IP-based access control policy. The access control policy defines the access control contract that governs traffic between the source and destination IP network groups.

For more information, see Create an IP-based and URL-based access control policy, on page 5.

Configure global network servers

You can define the global network servers that become the default for your entire network.

Note You can override the global network settings on a site by defining site-specific settings.

Procedure

Step 1 From the main menu, choose **Design** > **Network Settings**.

Step 2 Click the **Servers** tab.

Step 3 Expand the **DHCP** area. Specify one or more dedicated Dynamic Host Configuration Protocol (DHCP) servers for managing the client device networking configuration.

Step 4 Check the **Add DHCP servers** check box to view the fields.

Step 5 In the **IP Address** field, enter the IP address of a DHCP server. Click the icon to add an IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

You must define at least one DHCP server in order to create IP address pools.

Step 6 Expand the **DNS** area to configure your network domain name, and specify Domain Name System (DNS) servers for hostname resolution.

Step 7 Check the **Set a domain name** check box to enter the domain name of a DNS server.

Step 8 Check the **Add DNS servers** check box to enter the IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

You must define at least one DNS server in order to create IP address pools.

Step 9 Expand the **NTP** area to specify one or more Network Time Protocol (NTP) servers to facilitate system clock synchronization for your network.

Step 10 Check the **Add NTP servers** check box to view the fields.

Step 11 In the **IP Address** field, enter the IP address of an NTP server. Click the icon to add an IP address.

Note

You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

Step 12 Click **Save**.

Create an IP Network Group

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP Network Groups**.

Step 2 Click **Add Groups**.

Step 3 In the **Name** field, enter a name for the IP network group.

Step 4 In the **Description** field, enter a word or phrase that describes the IP network group.

Step 5 In the **IP Address or IP/CIDR** field, enter the IP addresses that make up the IP network group.

Step 6 Click **Save**.

Edit or delete an IP Network Group

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP Network Groups**.

Step 2 In the **IP Network Groups** table, check the check box next to the group that you want to edit or delete.

Step 3 Do one of these tasks:

- To edit the group, click **Edit**. For more information about field definitions, see Create an IP Network Group, on page 3. Make your changes, and click **Save**.
- To delete the group, click **Delete** and then click **Yes** to confirm.

Create an IP-based access control contract

Use this procedure to create an IP-based access contract:

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **Access Contract**.

Step 2 Click **Add Contract**.

Step 3 In the **Name** field of the **Add Contract** slide-in pane, enter a name for the access contract.

Step 4 (Optional) In the **Description** field, enter a description for the access contract.

Step 5 From the **Implicit Action** drop-down list, choose either **Deny** or **Permit**.

Step 6 Click **Add** to add a port or protocol.

Step 7 In the **Add Port/Protocol** dialog box, do these steps:

a) From the **Action** drop-down list, choose either **Deny** or **Permit**.
b) From the **Port/Protocol** drop-down list, choose a port or protocol.
c) Click **Save**.

Step 8 If Catalyst Center doesn't have the port or protocol that you need, click **Create Port/Protocol** to create a port and protocol, and do these steps in the **Create Port/Protocol** dialog box:

a) In the **Name** field, enter a name for the port or protocol.
b) From the protocol drop-down list, choose a protocol.

c) In the **Port Range** field, enter the port range.
d) If you want Catalyst Center to configure the port or protocol as defined and not report any conflicts, check the **Ignore Conflict** check box.
e) Click **Save**.

Step 9 (Optional) To include more rules in the access contract, click **Add** and repeat Step 7, on page 4.

Step 10 Click **Save**.

Edit or delete an IP-based access control contract

If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that is deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **Access Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete, and do one of these tasks:

- To make changes to the contract, click **Edit**, make the changes, and click **Save**. For more information about field definitions, see Create an IP-based access control contract, on page 4.

  Note
  If you make changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.

- To delete the contract, click **Delete**.

Create an IP-based and URL-based access control policy

You can create a post authentication Access Control List (ACL) for your network. The list can be based on IPs, URLs, or both.

Before you begin

See Workflow to configure an IP-based access control policy, on page 2.

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**.

Step 2 Click **Add Policy**.

Alternatively, instead of the first two steps, you can click the menu icon and choose **Workflows** > **Create IP & URL-Based Access Control Policy**. If an **Overview** window opens, click **Let's Do it** to start the workflow.

Step 3 In the **Policy Name and Details** window:

a) Enter a name and description for the policy.

b) Under **Select ACL Type**, check the required check boxes:

- **IPv4 or IPv6**: Configure IP-based access control policy.
- **URL**: Configure URL-based access control policy.
- **IPv4** and **URL**: Configure both IPv4-based and URL-based access control policies.
- **IPv6** and **URL**: Configure both IPv6-based and URL-based access control policies.

Step 4 In the **Select Sites and SSID** window, choose the site where you want to apply the policy and select the SSIDs.

Ensure that the site is already provisioned with an SSID.

For Flex or fabric SSIDs, ensure that an AP is provisioned at the site.

If you choose URL ACL, you cannot select local SSIDs along with Flex or fabric SSIDs.

Step 5 If you chose IP ACL, configure custom rules for IP ACL in the **IP Access Control List** window:

If you want to...	Then...
Add a rule	**a.** Click **Add New Rule**. **b.** In the **Add New Rule** dialog box, choose a source, destination, contract, and direction from the corresponding drop-down lists. **Note** For bidirectional rules, ensure that the source and destination are different. Use only custom contracts when the source and destination are set to **Any**. **c.** Click **Add**.
Edit a rule	**a.** Click the pencil icon for the rule that you want to edit. **b.** Edit the required configuration. **c.** Click **Save**. **Note** You cannot edit the default rule.
Delete a rule	Click the delete icon for the rule that you want to delete. **Note** You cannot delete the default rule.

If you want to...	Then...
Update the sequence of a rule	Click the icon for the rule, and drag and drop the rule to the required position. **Note** You cannot update the sequence of the default rule.

Step 6 If you chose URL ACL, do these steps in the **URL Access Control List** window:

a. Enter the URL.

Note
You can include up to twenty URLs.

b. From the **Action** drop-down list, choose **Permit** or **Deny**.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 Schedule the task for deployment.

Depending on Visibility and Control of Configurations settings, you can either:

- Deploy the device configurations immediately or schedule the deployment for later. For details, see Deploy your device configurations now or later.
- Preview and deploy the device configurations. For details, see Preview and deploy your device configurations.

Step 9 On the **Tasks** window, monitor the task deployment.

Edit or delete an IP-based and URL-based access control policy

If you need to, you can change or delete an IP-based and URL-based access control policy.

Procedure

Step 1 From the main menu, choose **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**.

Step 2 To edit a policy, click the name of the policy that you want to edit, make the required changes, and click **Save & Schedule**. For more information, see Create an IP-based and URL-based access control policy, on page 5.

Step 3 To delete a policy, check the check box next to the policy that you want to delete and click **Delete**.