Manage Predefined Inbound Routes

The table lists the feature history for managing predefined inbound routes.

Table 1: Feature History

Feature Name	Release Information	Description
Predefined Inbound Rules	March 2023 Release	With this feature you can specify trusted IP addresses. These IP addresses are applied to any new overlay that you create under the Smart Account for which you configure this feature. These IP addresses can also be applied to existing overlays under the Smart Account for which you configure this feature.

Information about predefined inbound rules

Predefined inbound rules allow you to manage control component access by automatically applying trusted IP addresses and prefixes to all existing and new overlays within a Smart Account. This feature eliminates the need for manual configuration per overlay and includes support for audit log entries for all allowed IP addresses.

An inbound rule includes the rule name, protocol and port range to which the rule applies, and source IP address or prefix information. You can create up to 200 inbound rules per fabric and up to 5 allowed list entries.

Note If you have dynamic IP requirements for an existing multitenant Cloud-Pro fabric hosted on AWS, you can request activation of Application Load Balancing (ALB) and Web Application Firewall (WAF) for the fabric. This option replaces the static IP allow list with WAF-based access control, removing the 200-rule limit and enabling scalable, flexible, and secure ingress management.

To enable ALB and WAF, you must file a CSOne ticket and include a mandatory justification.

Normal inbound rule management will not be available when ALB/WAF has been enabled on a fabric. This feature is irreversible once enabled.

Configure predefined inbound rules

Before you begin

1. Create a Smart Account.

   For more information on creating a Smart Account, see Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers.

2. Create a fabric.

   For more information on creating a Cisco SD-WAN Cloud-Pro fabric, see Create a Cisco SD-WAN Cloud-Pro Overlay Network.

Manage predefined inbound rules

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Admin Settings**.
2. Under **Actions**, click **. . .** adjacent to the appropriate Smart Account and choose **Manage Predefined Inbound Rules** from the drop-down list.
3. Click **Add Predefined Inbound Rules** to add a predefined inbound rule.
4. Configure the following fields:

Field	Description
Name	Enter a name for the predefined inbound rule.
Rule Type	Select the protocol to which the rule applies from the drop-down list. • **All** (rule applies to all protocols) • **SSH** • **HTTPS** • **Custom TCP rule** • **Custom UDP rule**

Field	Description
Protocol	**Protocol** is automatically populated depending on which **Rule Type** you choose.
Port Range	If you chose **Custom TCP rule** or **Custom UDP rule** for **Rule Type**, enter the port range to which the rule applies.
Source	Enter an IP address or an IP address prefix.
Description	Enter a description for the predefined inbound rule.
Automatically add this rule to ALL fabrics	Select this option to apply the predefined rules to all the existing fabrics associated with your Smart Account, as well as any new fabrics. If you do not select this option, the rule is not added to your existing fabrics.

5. Click **Add**.