Configure Application Layer Gateway (ALG)

For supported software information, click here.

Application Layer Gateway (ALG) is a security component that enhances firewall and CGNAT operations. ALG allows you to use customized NAT traversal filters with Versa Operating System™ (VOS™) devices to support address and port translation for application layer control and data protocols such as FTP and SIP. For these protocols to work through CGNAT or a firewall, either the application has to identify an address–port number combination that allows incoming packets or NAT has to monitor control traffic and dynamically open up port mappings by creating firewall pinholes.

The following is an example of how a SIP ALG is used with FTP. In active mode, FTP uses two sessions:

- Control session—Lists folders and files, signals the creation of folders and files, deletes files, and performs other operations.
- Data session—Uploads or downloads actual files.

When the client initiates a session with the FTP server, it uses destination port 21. The client identifies the folder with the required content and then initiates the file download. Because the server must open a connection to the client for FTP to work, the client uses port 21 as the destination port to the server. This port listens to incoming connections from the server on the external IP address and a port of its choice. Then, the server starts a connection to the IP address and port that the client sent in its control message. However, if the client is behind a firewall, the firewall is unable to identify the port to open for the incoming connection. Also, if the client is behind a NAT, the client sends an internal IP address to the server, but the server cannot identify the destination IP address to use after the NAT translation. To resolve this issue, you use ALG. ALG listens for connections on port 21 and waits for the data connection to establish. When ALG detects a packet that initiates a file download, ALG modifies the packet to add an external NAT IP address and then creates a temporary firewall rule to allow the incoming connection from the server.
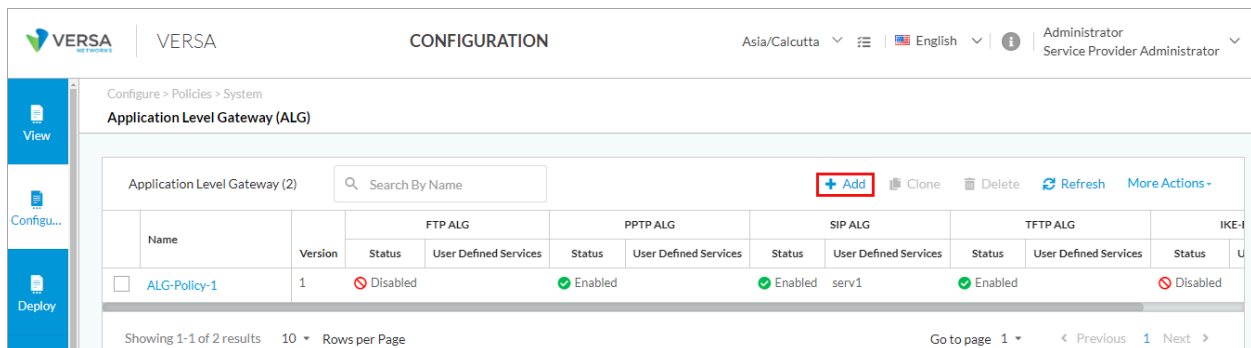
ALG supports operations for FTP, IKE ESP, PPTP, SIP, and TFTP. These operations are enabled by default.
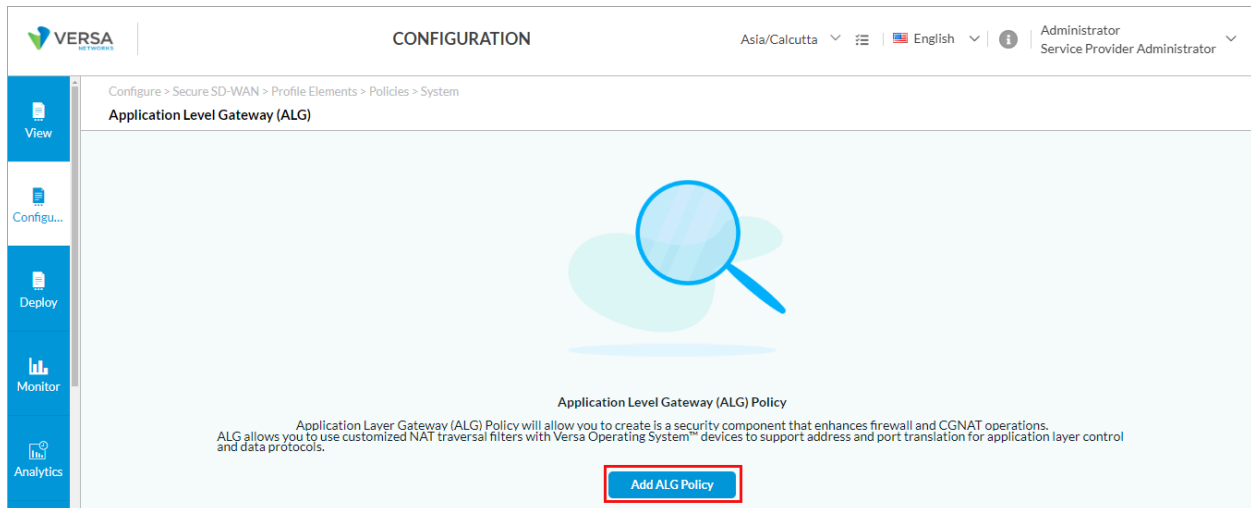
To configure ALG:

1. Go to Configure > Secure SD-WAN > Profile Elements > Policies > System > ALG Configurations.
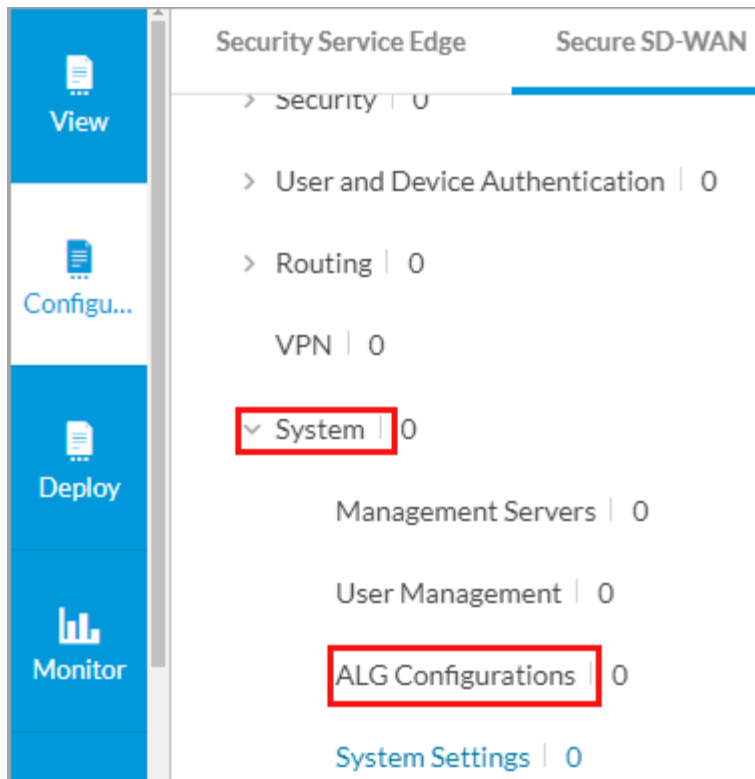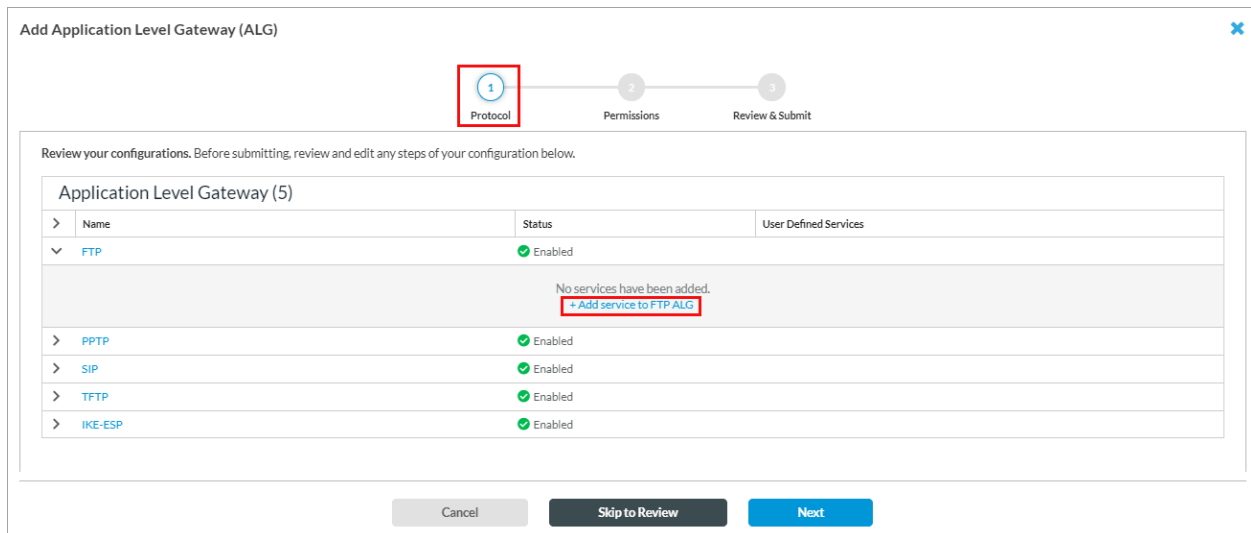
The Application Level Gateway (ALG) screen displays.

If there are no existing policies, the following screen displays.

2. Click Add ALG Policy or click + Add. The Add Application Level Gateway (ALG) screen displays the system-defined ALGs for various service protocols. By default, all ALGs are enabled. For each ALG, you can activate specific services.

3. In Step 1, Protocol, click an ALG instance to edit it, or click + Add Service to *Instance Name* ALG. The Edit Application Level Gateway screen displays. For example, if you click FTP or + Add Service to FTP ALG, the Edit FTP Application Level Gateway screen displays.

a. Click the ⬤ toggle button to disable the ALG.

b. To activate a service on the ALG, select the service name or search for a service in search box and select the service to add.

c. Click Save.

4. Click Next to go to Step 2, Permissions, to set or update permissions for each role. The default permission for each role is preselected, and you can update it. The roles are Enterprise Administrator, Enterprise Operator, Service Provider Administrator, and Service Provider Operator. The role permissions are Edit, Hide, and Read.

5. Click Next to go to Step 3, Review and Submit, to review the information.

6. In the General section, enter a name for the ALG policy and, optionally, a description.

7. For all other sections, review the information. To make changes, click the ✏️ Edit icon.

8. Click Save.

You can associate an ALG configuration with a basic master profile or a system sub profile. For more information, see Configure Profiles.

Supported Software Information

Releases 12.1.1 and later support all content described in this article.

Additional Information

Configure Profiles