
Configure 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 file, and performs other operations.
- Data session—Uploads or downloads actual files.

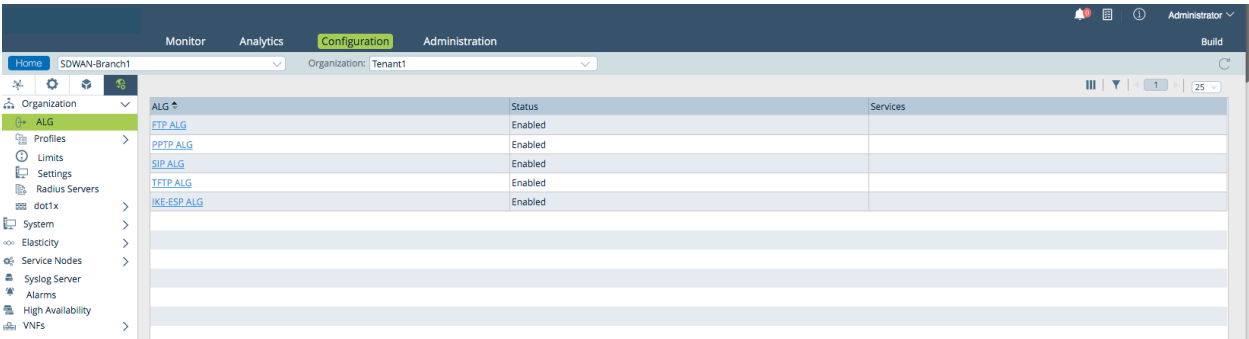
When the client initiates a session with the FTP server, it uses destination port 21. The client identifies the folder with the required content and then initiates the file download. Because the server must open a connection to the client for FTP to work, the client uses port 21 as the destination port 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 incoming connection from the server.

ALG supports operations for FTP, IKE ESP, PPTP, SIP, and TFTP. These operations are enabled by default.

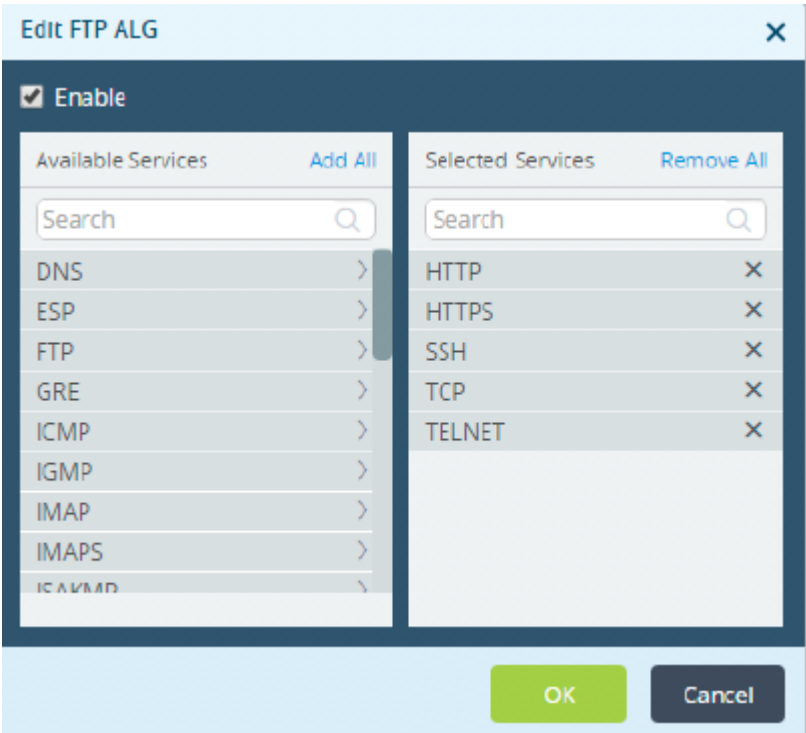
To configure ALG:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the left menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a device in the dashboard. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Others  > Organization > ALG in the left menu bar. The main pane displays the system-defined ALGs for different service protocols. By default, all ALGs are enabled. For each ALG, you can activate specific services.



4. Select an ALG instance. In the Edit ALG popup window, enter information for the following fields.



Field	Description
Enable	Click to activate or deactivate ALGs. Because all ALGs are enabled by default, this field is selected when the Edit ALG popup window displays.
Available Services	Click the desired service. The service moves to the

Field	Description
	Selected Services box.
Selected Services	Displays the list of selected services to activate on the ALG. Click the X to delete a service from the ALG.

5. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure CGNAT](#)

[Configure Stateful Firewall](#)