
Configure Stateful Firewall

 For supported software information, click [here](#).

Stateful firewall provides a mechanism to enable full visibility of the traffic that traverses through the firewall and also enforces very fine grain access control on the traffic.

To classify the traffic, stateful firewall verifies its destination port and then tracks the state of the traffic and monitors every interaction of each connection until it is closed.

Stateful firewall grants or rejects access based not only on port and protocol but also on the packet history in the state table. When stateful firewall receives a packet, it checks the state table for an established connection or for a request for the incoming packet from an internal host. If nothing is found, the packet's access is subject to the access policy rule.

For stateful firewall, you configure a security access policy to classify traffic using a security access policy. A security access policy includes the stateful firewall rule that collates the defined objects and assigns an action to take based on the match conditions.

Note: You can configure a stateful firewall only for Layer 2, Layer 3, and Layer 4 protocols. If your license subscription includes next-generation firewall (NGFW), the stateful firewall options are not visible in the Director GUI.

Stateful firewall focuses on examining the information in Layer 2 (link layer), Layer 3 (network), and Layer 4 (transport) packets. For these packets, their Layer 3 and 4 information (IP address and TCP/UDP port number) is verified against the information stored in the state table to confirm that they are part of the current exchange. This method increases overall firewall performance because only the initiating packets must be unencapsulated for these layers and all layers up to the application layer (Layer 7).

For more advanced inspection capabilities, stateful targets vital packets for Layer 7 (application) examination, such as the packet that initializes a connection. If the inspected packet matches an existing firewall rule that permits it, the packet is passed and an entry is added to the state table. From this point forward, because the packets in that communication session match an existing state table entry, they are allowed access without a call for further application layer inspection. For more information about Layer 7 NGFW, see [Configure NGFW](#).

Each security access policy consists of one or more rules. Each rule consists of match criteria and enforcement actions. You can use one or more of these traffic attributes to specify the match criteria:

- IP headers
- Domain names

- Services, based on port and protocol
- Source and destination geographic location
- Source and destination IP addresses
- Source and destination zones
- Time-of-day scheduling

A rule matches when all match criteria defined in the rule matches. All rules in the security access policy are evaluated starting with the first rule in the policy. The first rule that matches is selected and the corresponding security actions are enforced. No other rules are evaluated.

It is recommended that in a security policy, you configure more specific rules first and then configure generic rules.

For a stateful firewall policy, you can configure the following enforcement actions:

- Logging
 - Start
 - End
 - Both
 - Never
- Action
 - Allow—Allow sessions that match the configured rule to pass.
 - Deny—Drop sessions that match the rule.
 - Reject—Drop sessions that match the rule and send a TCP reset (RST) packet for TCP sessions or an ICMP port unreachable message for UDP sessions.

Versa Operating System™ (VOS™) devices support Application Layer Gateway (ALG), which is a communication protocol to connect a VOS device with various services. For example, to send files through FTP and to establish calls with Versa devices using SIP, you configure ALG for a branch or a Controller of a tenant or organization. You can use ALG with CGNAT and without CGNAT (stateful firewall only). By default, ALG is enabled when a firewall or CGNAT service is active. For more information, see [Configure CGNAT](#).

Note that the VOS software does not support decryption of the QUIC protocol. For the VOS security software modules to work, you must block QUIC traffic.

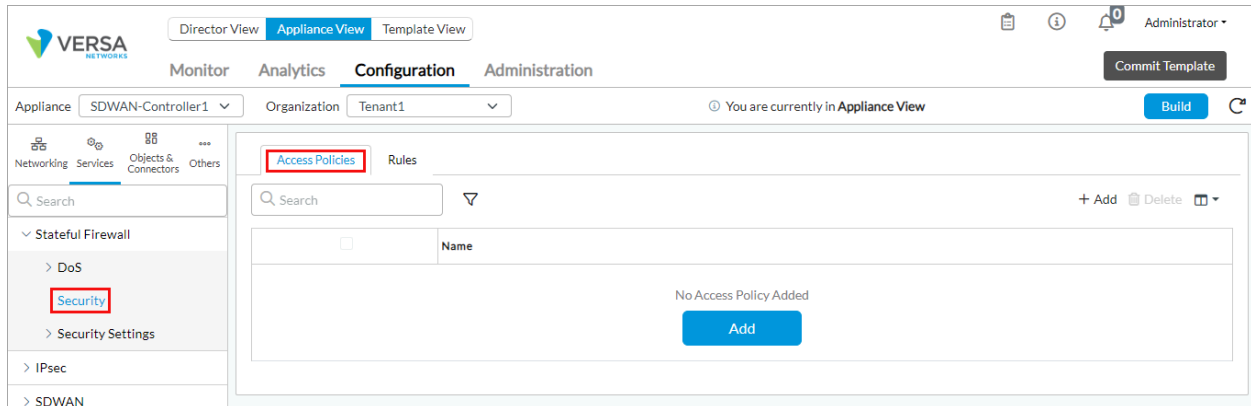
Configure Security Access Policy

To configure security access policy, you enable stateful firewall and create an access policy. You can define multiple security policies and isolate them on a per-tenant basis. For a tenant, each security policy must have a unique name.

When you configure multiple security policies, all rules of all the security access policies are evaluated in the order in which the security policies are configured.

To configure a security access policy:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Stateful Firewall > Security in the left menu bar, and select the Access Policies tab.



4. Click the + Add icon. In the Add Access Policy popup window, enter information for the following fields.

The 'Add Access Policy' popup window has a title bar with a close button (X). It contains the following fields:

- Name ***: A required text input field.
- Description**: A text input field.
- Tags**: A text input field.

At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (dark grey).

Field	Description
Name	Enter a name for the access policy name.
Description	Enter a text description for the access policy.
Tags	Enter a text string or phrase to associate with the policy. Tags allow you to locate a policy when you perform a filtered search of all policies. <i>Value:</i> Text string from 1 through 255 characters <i>Default:</i> None

- Click OK.

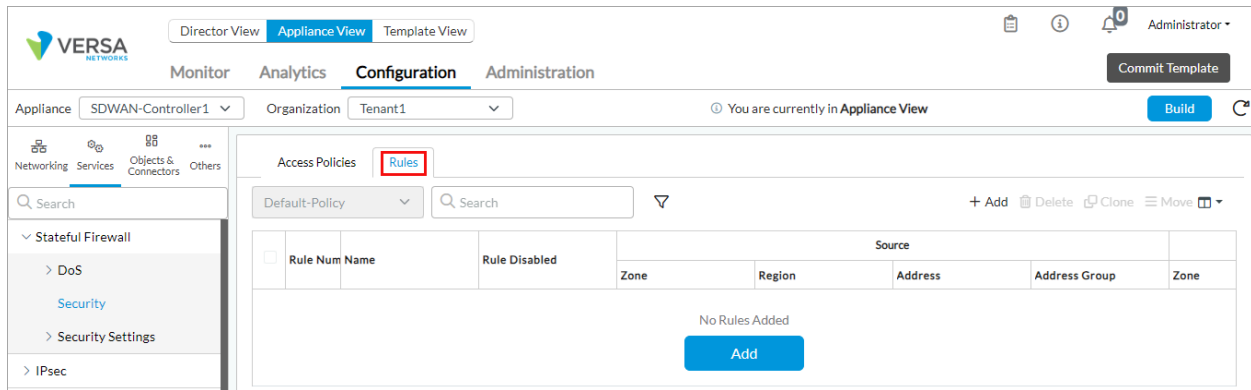
Configure Security Access Policy Rules

A security access policy consists of an ordered set of one or more policy rules. Each policy rule consists a set of match criteria and the enforcement actions. The security access policy rules within the stateful firewall policy are matched based on Layer 3 and Layer 4 information and time of day.

Note that you can apply firewall rules only for through traffic or for external traffic destined to the VOS device. You cannot use firewall rules to control traffic generated by the VOS device itself.

To configure a security access policy rule:

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Services > Stateful Firewall > Security in the left menu bar, and select the Rules tab.



4. Click the + Add icon to add a rule for the new security access policy. The Add Rule popup window displays.
5. Select the General tab and enter information for the following fields.

Add Rule

General

Source

Destination

Headers/Schedule

Enforce

Name *

Description

Tags

☐ Disable Rule

OK

Cancel

Field	Description
Name	Enter a name for the access policy rule.
Description	Enter a text description for the access policy rule.
Tags	Enter a keyword or phrase that allows you to filter the rule name. This is useful when you have many rules and want to view those that are tagged with a particular keyword.
Disable Rule	Click to disable the rule. You can disable a rule to skip it from evaluating traffic and to use other rules in the policy in the configuration order.

6. Select the Source tab to define the source zone and the source address of the incoming traffic to which the DoS protection policy rule applies. Enter information for the following fields.

Add Rule

General

Source



Destination

Headers/Schedule

Enforce

☐



Source Zone

+ New Zone +  

Source Zone Not Configured

☐



Source Address

+ New Address + New Address Group +  

Source Address Not Configured

☐



Custom Geo Circle

+  

Custom Geo Circle Not Configured

☐



Region

+  

Region Not Configured

☐



State

+  

State Not Configured

☐

City

+  


City Not Configured

☐ Source Address Negate

☐ Source Location Negate

OK

Cancel

Field	Description
Source Zone	For zones that you have configured for interfaces and networks, select the source zone to apply the rule to traffic coming from any interfaces or networks in the zone. Click the  Add icon to add more source zones. Note that you cannot configure source zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see Configure Zones and Zone Protection Profiles .
Source Address	Select and specify one or more source address to which the DoS Protection policy rule applies. Click the  Add icon to add more source addresses.
Custom Geo Circle	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a custom geographic circle. A geographic circle consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. To configure a custom geographic circle, see Configure Custom Geographic Circles .
Region	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a region. To create a region, see Create a Region .
State	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a state.
City	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a city.
Source Address Negate	Enable this to select any address except the configured addresses.
Source Location Negate	Click to select any source locations except the configured source locations.

7. Select the Destination tab to define the destination zone and the destination address of the outgoing traffic to

which the DoS protection policy rule applies. Enter information for the following fields.

Add Rule

General

Source



Destination

Headers/Schedule

Enforce

☐



Destination Zone

+ New Zone +  

Destination Zone Not Configured

☐



Custom Geo Circle

+  

Custom Geo Circle Not Configured

☐



State

+  

State Not Configured

☐



Destination Address

+ New Address + New Address Group +  

Destination Address Not Configured

☐



Region

+  

Region Not Configured

☐

City

+  






City Not Configured

☐ Destination Address Negate

☐ Destination Location Negate

OK

Cancel

Field	Description
Destination Zone	For zones that you have configured for interfaces and networks, select the destination zone to apply the rule to traffic going to any interfaces or networks in the zone. Click the  Add icon to add more destination zones. Note that you cannot configure destination zones for zones that you have configured for routing instances or for organizations. For information about configuring zones, see Configure Zones and Zone Protection Profiles .
Destination Address	Select and specify one or more destination address to apply the DoS Protection policy rule to the traffic marked to specific destination.
Custom Geo Circle	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a custom geographic circle. A geographic circle consists of a point and the area enclosed by a circle drawn around that point. You specify the point by its latitude and longitude coordinates, and you specify the size of the circle by a distance. To configure a custom geographic circle, see Configure Custom Geographic Circles .
Region	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a region. To create a region, see Create a Region .
State	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a state.
City	(For Releases 22.1.2 and later.) Click the  Add icon, and then select a city.
Destination Address Negate	Enable this to specify any address except the configured addresses.
Destination Location Negate	Click to select any destination locations except the configured destination locations.

8. Select the Header/Schedule tab to define the IP header, services and schedule to which the security access rule applies. Enter information for the following fields.

Add Rule

General

Source

Destination

Headers/Schedule

Enforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

+

TTL

Condition

Greater than or equal to

Value (Max 255)

Others

Schedules



--Select--

+ Schedule

Services

☐


Service List


+ New Service +  

Service List Not Configured

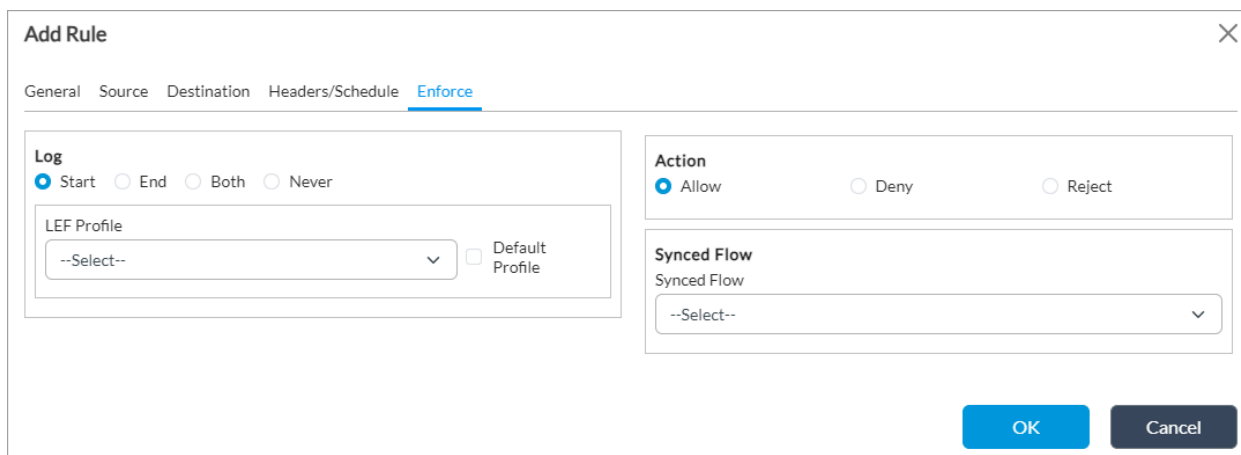
OK

Cancel

Field	Description
IP (Group of Fields)	
<ul style="list-style-type: none"> IP Version 	<p>Select the IP version:</p> <ul style="list-style-type: none"> IPv4 IPv6
<ul style="list-style-type: none"> IP Flags 	<p>For IPv4, select whether data packets can be fragmented:</p> <ul style="list-style-type: none"> Don't Fragment More Fragment
<ul style="list-style-type: none"> DSCP 	<p>Click the  Add icon to add a differentiated services code point (DSCP) value.</p>
TTL (Group of Fields)	
Condition	<p>Select the TTL condition to use for the match. The TTL is the number of hops that a packet can travel before it is discarded and indicates the lifespan of a packet. The condition can be one of the following boolean values:</p> <ul style="list-style-type: none"> Equal to—TTL value must be equal to the specified value to trigger the security access rule Greater than or equal to—TTL value must be greater than or equal to the specified value to trigger the security access rule Less than or equal to—TTL value must be less than or equal to the specified value to trigger the security access rule
Value	Enter the value for the TTL.
Others (Group of Fields)	
<ul style="list-style-type: none"> Schedules 	<p>Select a schedule to set the time and frequency at which the rule is in effect.</p>
Services (Group of Fields)	

<ul style="list-style-type: none"> ◦ Service List 	Click the  Add icon to select one or more services to apply the security access rule to the configured services.
--	---

9. Select the Enforce tab to select the applications and URIs to which the security access rule applies. Enter information for the following fields.



Field	Description
Log	<p>Select how to log the policy actions:</p> <ul style="list-style-type: none"> ◦ Start—Send a log at the start of the session. ◦ End— Send a log at the end of a session. ◦ Both— Send a log at the start and end of the session. ◦ Never—Do not set logs.
LEF Profile	Select the LEF profile to use. A LEF profile specifies where to log information.
Action	<p>Specify the action to take on matching traffic:</p> <ul style="list-style-type: none"> ◦ Allow—Allow sessions that match the rule to pass. ◦ Deny—Drop sessions that match the rule. ◦ Reject—Drop sessions that match the rule and send a TCP reset (RST) packet for TCP sessions or an ICMP port unreachable message for UDP sessions.

10. Click OK.

Monitor Stateful Firewall Security Access Policies

You monitor policies stateful firewall security access policies to view the traffic flow details when a policy is used. For more information, see [Monitor Device Services](#).

To monitor stateful firewall security access policies:

1. Select the Administration tab in the top menu bar.
 - a. Select Appliances in the left menu bar.
 - b. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the Provider Organization > Services tab.
4. Select SFW > Policies. The stateful firewall policy statistics display, and in the Rule Name column you can view statistics about the access policy rule that you create.

The screenshot displays the Versa Networks Appliance View interface. At the top, there are tabs for Director View, Appliance View (selected), and Template View. Below this is a navigation bar with Monitor, Analytics, Configuration, and Administration. The main content area shows the configuration for 'SDWAN-Controller1'. Under the 'Services' tab, the 'Policies' sub-tab is selected. A table displays the stateful firewall policy statistics for the 'Default-Policy'.

Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Inactive Session Count	First Hit Time	Last Hit Time
Stateful-firewall-Rul...	0	0	0	0	0	0	-	-

Click a rule name to view its configuration.

Configuration : Stateful-firewall-Rule-1



```
{
-  access-policy: {
    name: "Stateful-firewall-Rule-1",
    rule-disable: false,
-  match: {
    -  source: {
      -  zone: {
        -  zone-list: [
          "host"
        ]
      },
    -  address: {
      -  address-list: [
        "VIP_Analytics"
      ]
    }
  },
-  set: {
    action: "allow",
    -  log: {
      profile: "Default-Logging-Profile",
      event: "start"
    }
  }
}
```

Supported Software Information

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

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_Statefu...

Updated: Wed, 23 Oct 2024 08:19:16 GMT

Copyright © 2024, Versa Networks, Inc.

Additional Information

[Configure CGNAT](#)

[Configure DoS Protection](#)

[Configure Layer 7 Objects](#)

[Configure NGFW](#)

[Monitor Device Services](#)

[Versa Analytics Scaling Recommendations](#)