

---

## Configure Zones and Zone Protection Profiles

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

For network interfaces that have identical security requirements, you group them into a single entity called a security zone, or simply, a zone. You can then associate a security policy to the zone to apply the same protections to all interfaces in the zone. For example, you might want to create zones to group interfaces that connect to WiFi hotspots or interfaces that connect to a logical group of network access points for end users that are all on the same floor in a building.

You can configure up to 1024 zones per tenant.

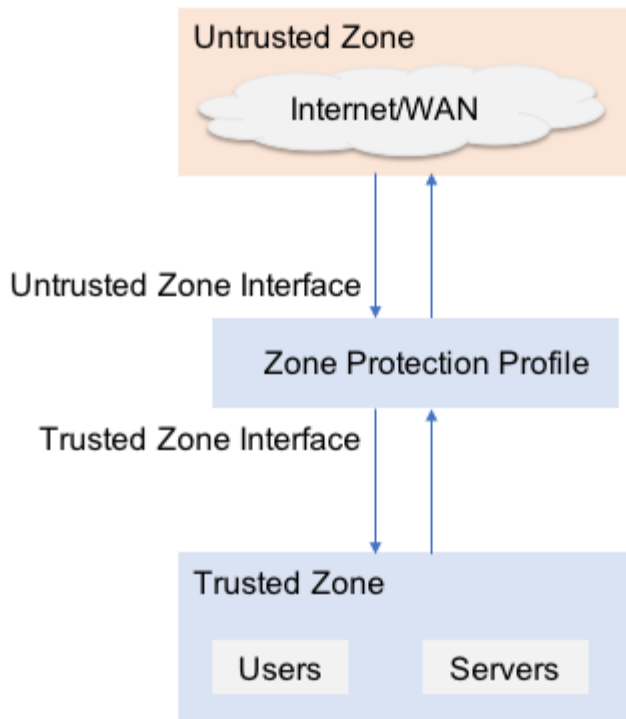
Associating policies with zones reduces the number of policies that you need to configure and maintain, and the policies can remain unchanged when the interfaces in a zone change.

To apply a basic level of security to network traffic as it enters a zone, you can define a zone protection profile. In this profile you define criteria to match malicious or unintended traffic, to prevent that traffic from entering the network, as illustrated in the figure below. The zone protection profile can detect and prevent the following types of traffic from entering the networks in the zone:

- Traffic floods of various protocols, such as TCP, UDP, and ICMP
- Port scans, host sweeps, and other types of reconnaissance traffic
- Malicious or spoofed packets

You can associate one zone protection profile with a zone.

You can use zone protection profiles to create trusted and untrusted zones, as illustrated in the following figure. Here, you place a zone protection profile between the untrusted zone and the trusted zone to prevent undesired types of traffic from entering the trusted zone. To filter traffic entering the trusted zone, you can also apply a firewall filter in which the source zone is the untrusted zone and the destination zone is the trusted zone.



Next-generation firewall (NGFW) rules determine inter-zone and intra-zone traffic:

- Inter-zone traffic—When you enable NGFW and do not configure NGFW rules, by default, inter-zone traffic is blocked. The implicit deny rule automatically blocks traffic.
- Intra-zone traffic (traffic to and from the same zone)—When you enable NGFW and do not configure NGFW rules, by default, intra-zone traffic is allowed. The implicit deny rule does not block this traffic. To block intra-zone traffic, configure a rule that matches the target zone for both source and destination zones, and then set the rule action as Deny. For more information, see [Configure NGFW](#).

---

## Configure Zones

To group together multiple interfaces that share the same security requirements, you configure a zone that contains all the interfaces. You can configure a zone on a per-tenant basis. For a given tenant, each zone must have a unique name. However, when a VOS device hosts different tenants, the tenants are isolated from each other, so the zones for two different tenants can have the same name.

To configure a zone:

1. In Director view:
  1. Select the Configuration tab in the top menu bar.
  2. Select Devices > Devices in the horizontal menu bar.
  3. Select an organization in the left menu bar.

4. Select a Controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Zones in the left menu bar. The table in the main pane displays the configured zones.

The screenshot shows the Versa Networks Appliance View Configuration page. The top navigation bar includes 'Director View', 'Appliance View' (selected), and 'Template View'. The main menu bar has 'Monitor', 'Analytics', 'Configuration' (selected), and 'Administration'. The left sidebar shows 'Networking' > 'Zones' selected. The main pane displays a table of configured zones.

<input type="checkbox"/>	Name	Log Profile	Zone Protection Profile	Interface List	Routing Instance	Networks	Org
<input type="checkbox"/>	Intf-LAN-Network-T1...					LAN-Network-T1	
<input type="checkbox"/>	Intf-WAN1-Zone					WAN1	
<input type="checkbox"/>	Intf-WAN2-Zone					WAN2	
<input type="checkbox"/>	Intf-WAN3-Zone					WAN3	
<input type="checkbox"/>	L-ST-Tenant1-LAN-VR...			twi-0/603.0			
<input type="checkbox"/>	L-ST-Tenant1-LAN-VR...						
<input type="checkbox"/>	L-ST-Tenant1-LAN-VR...						

Rows per page: 25 Showing 1 - 17 of 17

4. Click the Add icon. In the Add Zone popup window, enter information for the following fields.

Add Zone

Name \*

Description

Tags

Zone Protection Profile

--Select--

+ Create Zone Protection Profile

Log Profile

--Select--

+ Create Log Profile

☒ Organization

☐ Routing Instance

☐ Interface and Networks



Organization \*

--Select--

Routing Instance



--Select--

☐ Networks

+  

Networks Not Configured





☐ Interfaces

+  

Interfaces Not Configured

OK

Cancel

Field	Description
Name (Required)	Enter a name for the zone.
Description	Enter a text description for the zone.
Tags	Enter a keyword or phrase that allows you to filter the zone name.
Zone Protection Profile	Select a zone protection profile. This profile defines flood protection, scan protection, and traffic anomaly protection information, and it is applied to all traffic flows that enter the zone through the interfaces associated with the zone. For more information, see the <a href="#">Configure a Zone Protection Profile</a> section, below.
+ Create Zone Protection Profile	Click to create a zone protection profile. For more information, see the <a href="#">Configure a Zone Protection Profile</a> section, below.
Log Profile	Select a log profile to use to log alarms to an external device. By default, alarms are logged in syslog. Users see all alarms on their devices.
+ Create Logging Profile	Click to create a log profile. For more information, see <a href="#">Configure Log Export Functionality</a> .
Interface and Networks	Click to add an interface or a network to the security zone. <ul style="list-style-type: none"> <li>◦ In the Interface pane, click the  Add icon and select an interface from the list.</li> <li>◦ In the Networks pane, click the  Add icon and select a network from the list.</li> </ul>
Routing Instance	Click to add a routing instance to the security zone. <ul style="list-style-type: none"> <li>◦ In the Routing Instances pane, click the  Add icon and select a routing interface from the list.</li> </ul>
Organization	Click to add an organization to the zone. <ul style="list-style-type: none"> <li>◦ In the Organizations pane, click the  Add icon and select an organization from the list.</li> </ul>

5. Click OK.
6. If you have previously associated interfaces with network objects, such as Layer 7 objects, add the network objects to the zone. When you do this, all the interfaces that belong to the network object are added to the zone.

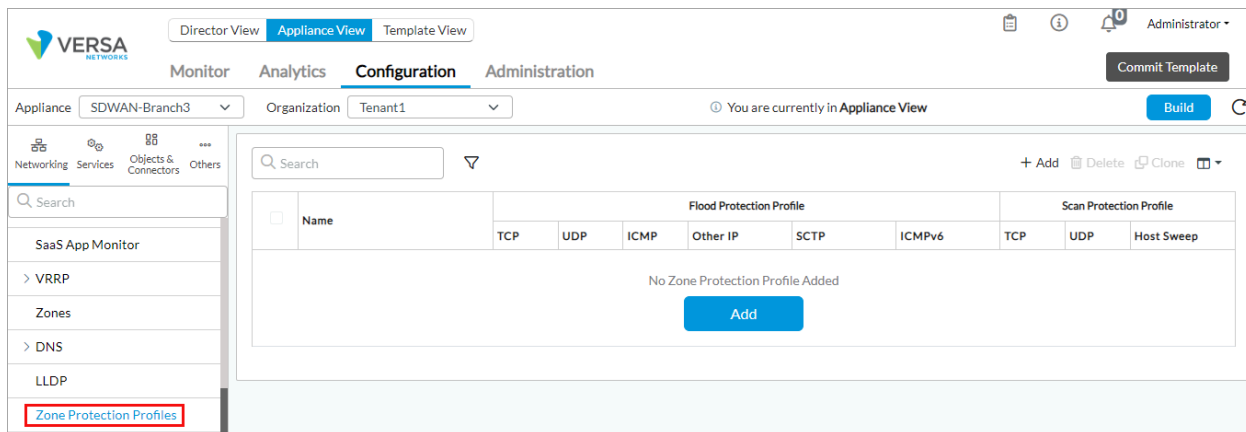
## Configure Zone Protection Profiles

You can create a zone protection profile to configure basic traffic profiling and reconnaissance detection. In the profile, you define flood protection, scan protection, and traffic anomaly protection information. A zone protection profile is applied only to the first packet of a new flow entering a zone. If a flow is idle for a while and then new packets in the flow enter the zone, the zone protection profile is not applied to the new packets because they are part of an existing flow.

You can configure multiple profiles for a tenant.

To configure a zone protection profile:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a Controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Zones Protection Profiles from the left panel.



4. Click the  Add icon. The Add Zone Protection Profile popup window displays.

Add Zone Protection Profile

General
Flood
Scan
Packet Based Attack Protection

Name \*

Description

Tags

OK
Cancel

- Select the General tab and enter information for the following fields.

Field	Description
Name	Enter a name for the zone protection profile.
Description	Enter a text description for the zone protection profile.
Tag	Enter a keyword or phrase that allows you to filter the profile name.

- Select the Flood tab to configure protocol flood thresholds. Enter information for the following fields.

## Add Zone Protection Profile



General **Flood** Scan Packet Based Attack Protection

Protocol	Enable	Alarm Rate Packets (seconds)	Activate Rate Packets (seconds)	Maximum Rate Packets (seconds)	Drop Period (seconds)	Actions
TCP	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	Random ▾
UDP	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	
ICMP	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	
Other IP	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	
SCTP	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	
ICMPv6	<input type="checkbox"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="100000"/>	<input type="text" value="300"/>	

OK

Cancel



Field	Description
Protocol	<p>Displays the protocols for which you can configure flood thresholds:</p> <ul style="list-style-type: none"> <li>◦ ICMP</li> <li>◦ ICMPv6</li> <li>◦ Other IP</li> <li>◦ SCTP</li> <li>◦ TCP</li> <li>◦ UDP</li> </ul>
Enable	Click to select the protocol for which to enable flood protection.
Alarm Rate	<p>Enter the threshold value, in packets per second (pps), at which to generate an alarm. When the number of packets received matches or exceeds this value, an alarm is generated.</p> <p><i>Range:</i> 1 through 20000000 pps</p> <p><i>Default:</i> 100000 pps</p>
Active Rate	<p>Enter the threshold value, in pps, at which to activate the random early detection (RED) action. When the number of packets received matches or exceeds this value, packets are randomly dropped.</p> <p><i>Range:</i> 1 through 20000000 pps</p> <p><i>Default:</i> 100000 pps</p>
Maximum Rate	<p>Enter the threshold value, in pps, at which to drop all packets. When the number of packets received matches or exceeds this value, all packets are dropped.</p> <p><i>Range:</i> 1 through 20000000 pps</p> <p><i>Default:</i> 100000 pps</p>

Drop Period	<p>Enter a value for how long to drop packets.</p> <p><i>Range:</i> 1 through 18000 seconds</p> <p><i>Default:</i> 300 seconds</p>
Actions	<p>For TCP, select the action to take when the active rate threshold is exceeded:</p> <ul style="list-style-type: none"> <li>◦ Random Early Drops—Randomly drop packets.</li> <li>◦ SYN Cookies—Generate an acknowledgment, and ensure that the connection is not dropped during a SYN flood attack. This is the default.</li> </ul> <p><i>Default:</i> SYN Cookies</p>

7. Select the Scan tab to configure the scan intervals and thresholds. Enter information for the following fields.

Add Zone Protection Profile

General

Flood

Scan

Packet Based Attack Protection

Scan	Enable	Actions	Interval(seconds)	Threshold(Events)
TCP	<input type="checkbox"/>	Allow ▾	30	300
UDP	<input type="checkbox"/>	Allow ▾	30	300
HostSweep	<input type="checkbox"/>	Allow ▾	30	300

OK

Cancel

Field	Description
Scan	Displays the protocols and other objects for which you can configure scanning intervals and thresholds: <ul style="list-style-type: none"> <li>◦ Host sweep</li> <li>◦ TCP</li> <li>◦ UDP</li> </ul>
Enable	Click to select the protocol or object for which to enable scan protection.
Actions	Select the action to perform when an abnormal network scan is detected: <ul style="list-style-type: none"> <li>◦ Allow—Run the scan</li> <li>◦ Alert—Generate an alert</li> </ul>
Interval (Sec)	Enter a value for how often to scan traffic.  <i>Range:</i> 1 through 65535 seconds <i>Default:</i> 30 seconds <i>Recommended Value:</i> 30 seconds or less. Configuring a higher value can increase memory utilization on the VOS device.
Threshold (Events)	Enter a threshold value for events. When the number of events received matches or exceeds this value, an alarm is generated.  <i>Range:</i> 1 through 65535 <i>Default:</i> 300

8. Select the Packet-Based Attack Protection tab to protect the network from invalid data packets and other anomalous traffic.
9. Select the UDP/TCP/IP Discard tab and enter information for the following fields.

Add Zone Protection Profile

General

Flood

Scan

Packet Based Attack Protection

UDP/TCP/IP Discard

ICMP

☐ IP Frag

☐ IP Spoof

☐ Reject Non-SYN TCP

☐ UDP Malformed

IP Options

☐ Security

☐ Stream

☐ Unknown

☐ Malformed

☐ Loose Source Routing

☐ Strict Source Routing

☐ Timestamp

☐ Record Route

OK

Cancel

Field	Description
IP Frag	Click to drop fragmented packets.
IP Spoof	Click to drop spoofed packets, which are packets that are received on one interface but that have a different outgoing interface.
Reject Non-SYN TCP	Click to drop packets in a session if the first packet has a non-SYN flag.
UDP Malformed	Click to drop packets in the case of a checksum error.
IP Options	<p>Select one or more IP options. The IP options are defined <a href="#">RFC 791</a> and <a href="#">RFC 1108</a>.</p> <ul style="list-style-type: none"> <li>◦ Security—Allows hosts to send security and other parameters (IP option 130; RFCs 791 and 1108)</li> <li>◦ Stream—Stream identifier (IP option 136; RFCs 791 and 1108)</li> <li>◦ Unknown—IP options field is unknown</li> <li>◦ Malformed—IP options field is formatted incorrectly</li> <li>◦ Loose-source routing—Routes IP packets based on information provided by the source (IP option 3; RFC 791)</li> <li>◦ Strict-source routing—Routes IP packets based on information provided by the source (IP option 137; RFC 791)</li> <li>◦ Timestamp—Timestamp information (IP option 4; RFC 791)</li> <li>◦ Record route—Routes IP packets based on information provided by the source (IP option 7; RFC 791)</li> </ul>

10. Select the ICMP tab and enter information for the following fields.

Add Zone Protection Profile
✕

General
Flood
Scan
Packet Based Attack Protection

UDP/TCP/IP Discard | ICMP

☐ Ping Zero ID
☐ Fragment
☐ Large Packet (Length > 1024 bytes)
☐ Error Message
☐ Malformed Packet

OK
Cancel

Field	Description
Ping Zero ID	Click to drop ICMP ping packets whose identifier value is 0.
Fragment	Click to drop packets that contain ICMP fragments.
Large Packet	Click to drop ICMP packets larger than 1024 bytes.
Error Message	Click to drop packets if the ping request generated error messages.
Malformed Packet	Click to drop malformed ICMP packets.

11. Click OK.

## View Zone Protection Logs

To view the zone protection logs on Versa Analytics:

1. In Director view, select the Analytics tab.
2. Select Logs > Threat Detection > DoS Threat Logs in the left menu bar. The zone protection logs display. For example:

Analytics-Cluster-A-Versa-Ana... Asia/Calcutta

**DOS Threat Log**

☐ Show Domain Names

Search:

Show 50 entries

Copy CSV PDF

Receive Time	Appliance	Threat Type	Attack Name	Attacker	Victim	Scan Ports Count	Action	From Zone	To Zone	Severity Level
Apr 14th 2022, 10:00:04 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:54:14 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:51:50 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:49:26 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:48:25 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:47:01 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:45:23 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:41:54 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:40:26 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:38:46 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 9:16:09 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 8:51:31 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 8:39:17 PM IST	Hub-01	Flood	UDP			0	Alarm	Intf-INET-Zone		1
Apr 14th 2022, 8:36:55 PM IST	Hub-01	Flood	TCP SYN			0	Alarm	Intf-INET-Zone		1

Showing 1 to 14 of 14 entries

Previous 1 Next

Note that for zone protection profiles, the Attacker and Victim columns are not populated, because the purpose of the profile is to limit the rate at which sessions are created. The Attacker and Victim columns are populated only when you configure a classified DoS profile in which you configure the Classification Key field to be either both Destination IP Only and Source IP Only, or Source and Destination IP. For more information, see [Configure DoS Protection](#).

## Supported Software Information

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

## Additional Information

[Configure Basic Features](#)

[Configure DoS Protection](#)

[Configure Layer 7 Objects](#)