

---

## Configure EIP-Based Microsegmentation for SD-LAN

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

Microsegmentation is a network security strategy that allows you to divide a network into smaller, isolated segments, called microsegments. You create each microsegment around a specific set of resources or services, and you define access controls and configure security policies that are specific for the resources and services in the microsegment. Traditional network security models primarily rely on securing the network perimeter, using methods such as firewalls to protect the entire network. With microsegmentation, you can apply security controls at a more granular level, providing an additional layer of security. You can create security zones in your network and apply security policies to each microsegment to provide enhanced security by restricting lateral movement within the network.

With Versa Operating System™ (VOS™) microsegmentation, you can place user client devices and clientless (headless) IoT devices into microsegments. For more information, see [Configure Microsegmentation](#).

If the security posture of a device does not meet the standards, the VOS software moves it from a microsegment that allows access to sensitive applications and data to a microsegment with more restrictive resource access policies.

Each VOS switch or access point in the LAN that combines Layer 2 or Layer 3 switching with an integrated next-generation firewall (NGFW) can handle the security requirements of the traffic that enters that device. This on-premise, ZTNA-distributed firewall-on-a-switch architecture scales well, and it reduces traffic latency by eliminating traffic hair-pinning to apply security services on a cloud security point of presence (PoP).

This article describes how to configure microsegmentation using endpoint information profiles (EIPs) for SD-LAN. You can configure EIP-based microsegmentation on Versa Cloud Services Gateway (CSG) and Versa Cloud Services Switch (CSX) platforms to connect a Versa SASE client in gateway-assisted trusted-network mode.

The configuration example for EIP-based microsegmentation in this article describes the following configuration flow:

- Configure a paired tunnel virtual interface (TVI), and add an interface to a virtual router (VR).
- Configure a virtual router to detect trusted networks, and configure the paired TVI to the virtual router.
- Add the TVI interface to the tenant organization.
- Add the paired TVI interface to the LAN network and LAN virtual router (LAN-VR).
- Add a static route on the tenant LAN-VR to the SASE gateway IP address through the paired TVI interface.
- Add client-facing interfaces and paired TVI interfaces to LAN zones.
- Configure zones and associate interfaces and LAN zones.
- Configure NGFW rules to allow traffic from the LAN zones.

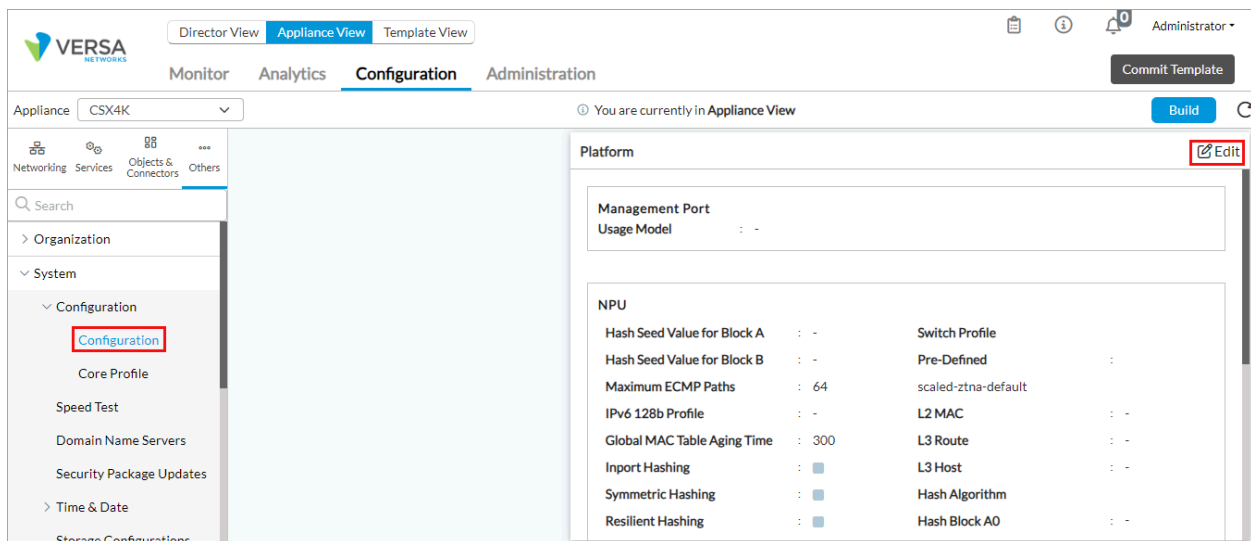
- Configure captive portal to associate the virtual router routing instance used for detecting trusted networks.
- Configure a DNS proxy with a redirection rule that responds to a domain name with a static IP address.
- Configure authentication profiles and users in the LDAP, local, or Security Assertion Markup Language (SAML) database.
- Configure EIP objects and associate them with custom EIP profiles, and configure microsegmentation policies to match the EIP profiles.
- Configure the SASE gateway for trusted-network mode.

## Before You Begin

For microsegmentation to work on CSG and CSX devices, you must select a scaled ZTNA profile as the NPU predefined switch profile.

To select a scaled ZTNA profile:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Configuration > Configuration in the left menu bar. The main pane displays panes related to system settings.



4. In the Platform pane, click  Edit. The Edit Platform popup window displays.

5. Select the NPU tab, and then select the Switch Profile tab.
6. Click the Predefined field, and then select a scaled ZTNA profile. The profile can be either scaled-ztna-default (as shown here) or scaled-ztna-routes.
7. Restart the device for the profile selection to take effect.
8. Click OK.


## Configure Paired Tunnel Interfaces

You configure two TVI interfaces for routing secure access traffic that reaches a captive portal through a client that is connected to trusted branch locations.

To configure the TVI interfaces:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Interfaces in the left menu bar.

The screenshot shows the Versa Networks configuration interface. At the top, there are tabs for Director View, Appliance View (selected), and Template View. Below these are Monitor, Analytics, Configuration (selected), and Administration. The Appliance dropdown is set to CSX4K. A horizontal menu bar contains various tabs: VNI, AE, ENet, IRB, T1/E1, Tunnel (highlighted with a red box), DSL, WWAN, Wi-Fi, uCPE, Loopback, Fabric, and Management. On the left, a vertical sidebar shows a tree view with categories like Networking, Services, Objects & Connectors, and Others. Under Networking, the 'Interfaces' tab is highlighted with a red box. The main area displays a table of interfaces. The table has columns: Name, Description, IP Address/Mask, MTU, Type, Pseudo Tunnel, and Pseudo Tunnel Remote Address. The table lists several interfaces, including ptvi1025, ptvi1044, ptvi513, ptvi532, tvi-0/10, tvi-0/100, and tvi-0/101. The 'tvi-0/100' and 'tvi-0/101' entries have descriptions starting with 'To take secure access cap...'. In the top right corner of the table, there is a '+ Add' button (highlighted with a red box), a 'Delete' button, and a table icon. At the bottom of the table, it says 'Rows per page 25 Showing 1 - 13 of 13'.

4. Select the Tunnel tab in the horizontal menu bar.
5. Click the  Add icon. In the Add Tunnel Interface popup window, select the Tunnel tab, and then enter information for the following fields.

Add Tunnel Interface

Tunnel
Pseudo Tunnel
PPPoE

Interface \*

tvi

0

/

101

☐ Disable
☐ Mirror Interface

Description

MTU

1400

Mode

IPsec

Tunnel Type

Paired

Paired Interface \*

tvi

0

/

100

☐ Next Routing Instance Nexthop

Multihoming
Active Mode

--Select--


ESI

Subinterfaces

+
trash
grid
<
1
>

	Unit	IP Address/Mask		DHCPv6	Interface Mode	VLAN ID	VLAN ID List
		IPv4	IPv6				
<input type="checkbox"/>	0			<input type="checkbox"/>			

OK
Cancel

6. In the Interface fields, enter the port and slot numbers for the TVI interface (here, 0 and 101).
7. In the Mode field, select IPsec.
8. In the Tunnel Type field, select Paired.
9. In the Paired Interface field, enter the port and slot number of the paired interface (here, 0 and 100).
10. In the Subinterfaces section, click the  Add icon. The Add Subinterface popup window displays.

**Add Subinterface**

General IPv4 IPv6 Bridge

Unit \*  
0

Description

VLAN ID  
0...4094 ☐ Disable

**Bandwidth**  
Uplink (Kbps) Downlink (Kbps)  
1...10000000 1...10000000

OK Cancel

11. Select the General tab, and then, in the Unit field, enter a unit number (here, 0).
12. Select the IPv4 tab, and then enter the IP address prefix and prefix length of the static IP addresses you want to use (here, 100.100.100.1/32 and 169.254.100.3/31).

**Add Subinterface**

General **IPv4** IPv6 Bridge

Static Address

<input type="checkbox"/>	IP Address/Mask	
<input type="checkbox"/>	100.100.100.1/32	
<input type="checkbox"/>	169.254.100.3/31	


OK Cancel

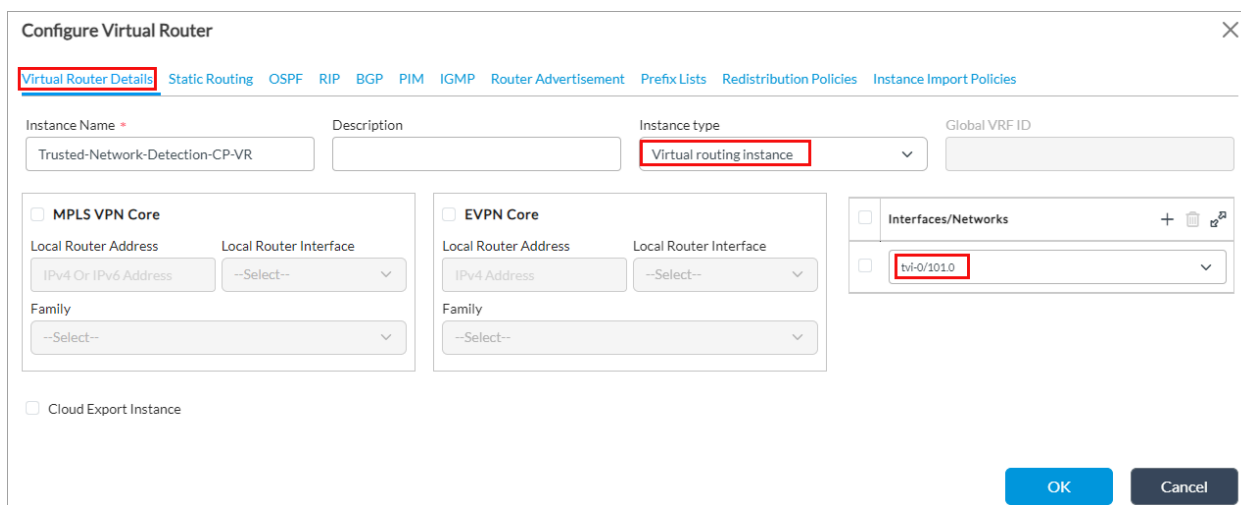
13. For the paired TVI interface (here, tvi-0/100), add the static IP address (here, 169.254.100.2/31).
14. For information about configuring other parameters, see Configure Tunnel Interfaces in [Configure Interfaces](#).

15. Click OK.


---

## Configure a Virtual Router To Detect Trusted Networks

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Click the  Add icon. The Configure Virtual Router popup window displays.



The screenshot shows the 'Configure Virtual Router' dialog box. The 'Virtual Router Details' tab is active. The 'Instance Name' field is 'Trusted-Network-Detection-CP-VR'. The 'Instance type' dropdown is set to 'Virtual routing instance'. The 'Interfaces/Networks' list contains one entry: 'tvi-0/101.0'. The 'OK' button is highlighted.

5. Select the Virtual Router Details tab.
6. In the Instance Name field, enter a name for the virtual router (here, Trusted-Network-Detection-CP-VR).
7. In the Instance Type field, select Virtual Routing Instance.
8. In the Interfaces/Networks field, click the  Add icon and then select the first paired interface (here, tvi-0/101.0) that you added in [Configure Paired Tunnel Interfaces](#), above.
9. For information about configuring other parameters, see [Set Up a Virtual Router](#).
10. Select the Static Routing tab, and then select the IPv4/v6 Unicast tab.

Configure Virtual Router

Virtual Router Details **Static Routing** OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

**IPv4/v6 Unicast** IPv4 Multicast IPv6 Multicast

+ - Copy Paste Filter 1 25

	Destination	View	Actions				Next Routing Instance	Metric	Preference	No Install	Min
			Interface	Nexthop IP Address	Monitor	Discard Reject					
No IPv4/v6 Unicast Static Routes Added											

OK Cancel

11. Click the **+** Add icon. The Add IPv4/v6 Unicast popup window displays.

Add IPv4/v6 Unicast

Destination \* **0.0.0.0/0** Monitor --Select-- Monitor Group --Select--

Metric Allowed Range is 1 - 4294967295 Preference **1** Tag

**Action**

Interface **tvi-0/101.0** ☒ Nexthop IP Address **169.254.100.2** ☐ Next Routing Instance --Select-- ☐ Discard ☐ Reject ☐ No Install

☐ **Enable ICMP**

Interval Allowed Range is 1 - 60 Threshold Allowed Range is 1 - 60

☐ **Enable BFD (Bidirectional Forwarding Detection)**

Minimum Receive Interval (msec) Allowed Range is 1 - 255000

Minimum Transmit Interval (msec)

OK Cancel

12. In the Destination field, enter the destination IP address or network (here, 0.0.0.0/0).
13. In the Preference field, enter 1 as the administrative distance (AD), or route preference, value of the static route.
14. In the Interface field in the Action section, select the first TVI interface (here, tvi-0/101.0) that you added in [Configure Paired Tunnel Interfaces](#), above.
15. In the Next-Hop IP Address field, enter the static IP address that you added for the paired TVI interface (here, 169.254.100.2) in [Configure Paired Tunnel Interfaces](#), above.
16. For information about configuring other parameters, see [Configure Static Routes](#).
17. Click OK.




## Add a TVI Interface and Routing Instance to the Tenant Organization

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.
  - d. Select an organization.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Limits in the left menu bar. The main pane displays the organizations associated with the device.
4. Click an organization name in the main pane (here, Tenant1). The Edit Organization Limit popup window displays.

The screenshot shows the 'Edit Organization Limit - Tenant1' window with the 'Traffic Identification' tab selected. The 'Interfaces' list on the left contains: pti1025, pti513, tvi-0/101.0 (highlighted with a red box), tvi-0/2.0, tvi-0/3.0, and tvi-0/603.0. The 'Networks' list on the right contains: LAN10 and fingerbank. At the bottom right are 'OK' and 'Cancel' buttons.

5. Select the Traffic Identification tab.
6. In the Interfaces field, click the Add icon, and then select the first interface (here, tvi-0/101.0) that you added in [Configure Paired Tunnel Interfaces](#), above.
7. Select the Resources tab.

The screenshot shows the 'Edit Organization Limit - Tenant1' window with the 'Resources' tab selected. It features four lists: 'Available Routing Instances' (containing Tenant1-Control-VR, Tenant1-LAN-VR, Tenant1-default-switch, Trusted-Network-Detection-CP-VR (highlighted), WAN1-Transport-VR, and provider-org-Control-VR), 'Owned Routing Instances' (containing Tenant1-Control-VR, Tenant1-LAN-VR, Tenant1-default-switch, and Trusted-Network-Detection-CP-VR (highlighted)), 'Available Provider Organizations' (containing provider-org), and 'Available Networks' (containing LAN10, WAN1, WAN2, WAN3, and fingerbank). A red message icon and text at the bottom left state: 'Please select newly added Routing Instance from Available Routing Instance before selecting in Owned Routing Instance'. 'OK' and 'Cancel' buttons are at the bottom right.

8. In the Available Routing Instances and Owned Routing Instances fields, click the  Add icon, and then select the virtual routing instance (here, Trusted-Network-Detection-CP-VR) that you added in [Configure a Virtual Router To Detect Trusted Networks](#), above.
9. For information about configuring other parameters, see [Configure Organization Limits](#).
10. Click OK.

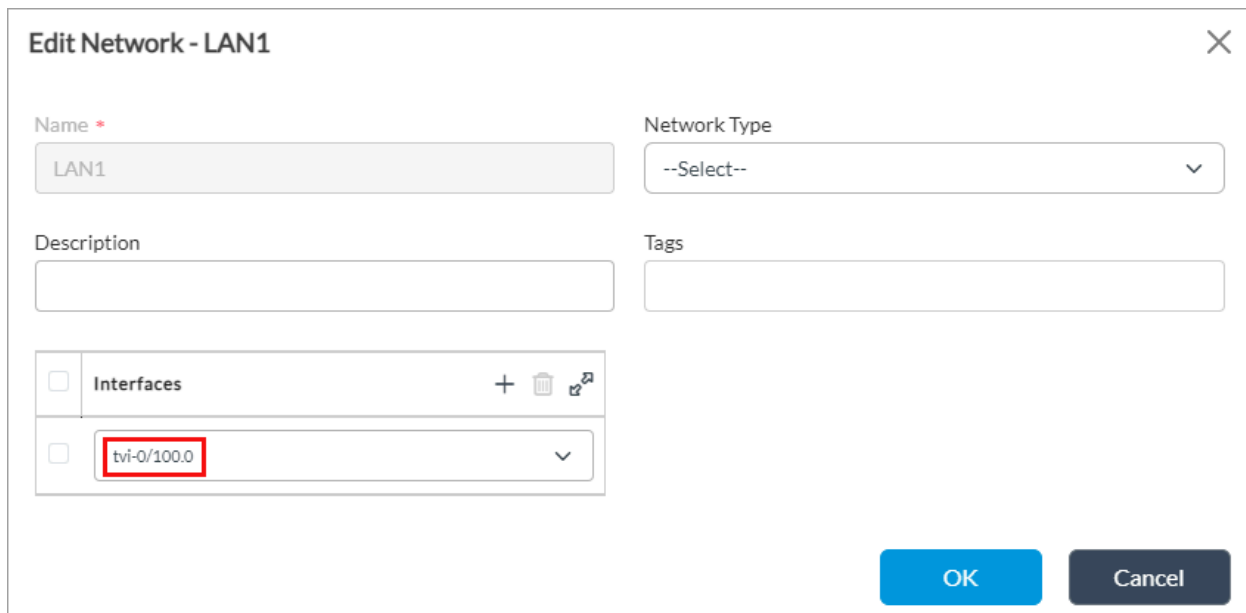
---

## Add Paired TVI Interfaces to the LAN Network and LAN Virtual Router

The paired TVI interfaces are used to connect to virtual routers. You add one TVI interface to connect to the LAN-VR network and a second TVI interface to connect to the virtual router that is used to detect trusted networks.

To add the paired TVI interface (here, tvi-0/100) to the LAN-VR network:

1. In the 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 Networking > Networks in the left menu bar.
4. Select the LAN network (here, LAN-1) for which you want to add the TVI interface. The Edit Network window displays.



**Edit Network - LAN1**

Name \* LAN1

Network Type --Select--


Description

Tags

☐ Interfaces

☐ tvi-0/100.0


OK Cancel

5. In the Interfaces field, click the  Add icon, and then select the first TVI interface (here, tvi-0/100.0) that you configured in [Configure Paired Tunnel Interfaces](#), above.

To add the TVI interface (here, tvi-0/101) to the tenant LAN-VR that is used to detect trusted networks:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Select the virtual router (here, Tenant-1-LAN-VR) for which you want to associate the TVI interface. The Edit VR window displays.

The screenshot shows the 'Edit Tenant1-LAN-VR' window. It has several tabs: 'Virtual Router Details', 'Static Routing', 'OSPF', 'RIP', 'BGP', 'PIM', 'IGMP', 'Router Advertisement', 'Prefix Lists', 'Redistribution Policies', and 'Instance Import Policies'. The 'Virtual Router Details' tab is active. Fields include: Instance Name (Tenant1-LAN-VR), Description (Tenant1 Lan VRF), Instance type (Virtual routing forwarding instance), Global VRF ID (21), Route Distinguisher (21L:106), VRF Import Target, VRF Export Target, and VRF Both Target (target:21L:21). There are also dropdowns for VRF Core Instance Type (MPLS VPN) and MPLS transport routing instance (Tenant1-Control-VR). A list of interfaces is shown, with 'tvi-0/100.0' highlighted by a red box. The list includes 'Interfaces/Networks', 'tvi-0/605.0', 'LAN10', 'LAN15', and 'tvi-0/100.0'. At the bottom right are 'OK' and 'Cancel' buttons.

5. In the Interfaces/Networks field, click the  Add icon, and then select the first TVI interface (here, tvi-0/100.0) that you configured in [Configure Paired Tunnel Interfaces](#), above.
6. Click OK.

## Add a Static Route to the SASE Gateway in the LAN VR

You add a static route to the SASE gateway in the LAN virtual router (here, Tenant1-LAN-VR) through the paired TVI interface.

To add a static route:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.

3. Select Networking > Virtual Routers in the left menu bar
4. Click the **+** Add icon. The Configure Virtual Router popup window displays.
5. Select the Static Routing tab, and then select the IPv4/v6 Unicast tab.
6. Click the **+** Add icon. The Add IPv4/v6 Unicast popup window displays.

7. In the Destination field, enter the SASE gateway destination IP address (here, 110.110.110.1/32).
8. In the Interface field in the Action section, select the paired TVI interface (here, tvi-0/100.0) that you added in [Configure Paired Tunnel Interfaces](#), above.
9. Click OK.

## Add Enterprise Names, a Gateway FQDN, and Services to the Tenant Organization

You add an enterprise name; a gateway FQDN; and CGNAT, NGFW, SD-WAN, and secure access services to the tenant organization.

To update the tenant organization:

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.
  - d. Select an organization.
2. Select the Configuration tab in the top menu bar.
  3. Select Others > Organization > Limits in the left menu bar. The main pane displays the organizations associated with the device.
  4. Click an organization name in the main pane (here, Tenant1). The Edit Organization Limit popup window displays.

5. Select the General tab.
6. In the Enterprise Names field, click the Add icon, and then enter the name of an enterprise that is in the organization (here, sandbox).
7. In the Gateway FQDN field, click the Add icon, and then enter the fully qualified domain name (FQDN) of the organization's gateway (here, blr-sandbox.versa.com).
8. To add services to the organization, select the Services tab. Note that before you can add a service, you must enable that service on the VOS device. For example, to add NGFW, see Enable NGFW in [Configure NGFW](#).

9. In the Services field, click the Add icon, and then select cgnat, nextgen-firewall, sdwan, and secure-access.


10. For information about configuring other parameters, see [Configure Organization Limits](#).
11. Click OK.

---

## Configure Zones To Add Client-Facing Interfaces and Pair Tunnel Interfaces

You configure zones and associate them with interfaces and LAN networks. You can then configure NGFW rules that allow traffic from these zones.

To configure a zone and add paired TVI interfaces to them:

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 in the left menu bar. The table in the main pane displays the configured zones.
4. Click the  Add icon. The Add Zone popup window displays.

Add Zone

Name \*

T1-REMOTE-CPVR-VR

Description

Tags

Zone Protection Profile

--Select--

+ Create Zone Protection Profile

Log Profile

--Select--

+ Create Log Profile

Organization

--Select--

Routing Instance

--Select--

Interface and Networks

Networks

+

Networks Not Configured


Interfaces

+

tvi-0/101.0

OK

Cancel

- Add a name for the zone (here, T1-REMOTE-CPVR-VR).
- Select Interface and Networks.
- In the Interfaces field, click the  Add icon, and then select the paired TVI interface (here, tvi-0/101.0) that you added in [Configure Paired Tunnel Interfaces](#), above.
- For information about configuring other parameters, see [Configure Zones](#).
- Click OK.

To configure a client-facing zone and add LAN Ethernet interfaces to the zone:

1. In the Add Zone popup window, enter information for the following fields.

**Add Zone** [X]

Name \*  
L2-intf-zone

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** + [trash] [refresh]  
Networks Not Configured

**Interfaces** + [trash] [refresh]  
enet-0/24.1  
enet-0/18.1 [dropdown arrow]

OK Cancel

2. Enter a name for the zone (here, L2-intf-zone).
3. Select Interface and Networks.
4. In the Interfaces field, click the  Add icon, and then select the LAN Ethernet interfaces (here, enet-0/18.1 and enet-0/24.1) you want to associate with the zone. For more information, see [Configure LAN Ethernet Interfaces](#).



5. Click OK.

To configure a zone associated with your LAN network:

1. In the Add Zone popup window, enter information for the following fields.

**Add Zone**

Name \*  
Intf-LAN-Zone

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	Interfaces
<input type="checkbox"/> LAN1	<input type="checkbox"/> Interfaces Interfaces Not Configured

OK Cancel

2. Enter a name for the zone (here, Intf-LAN-Zone).
3. Select Interface and Networks.
4. In the Networks field, click the **+** Add icon, and then select the LAN (here, LAN1) you want to associate with the

zone.

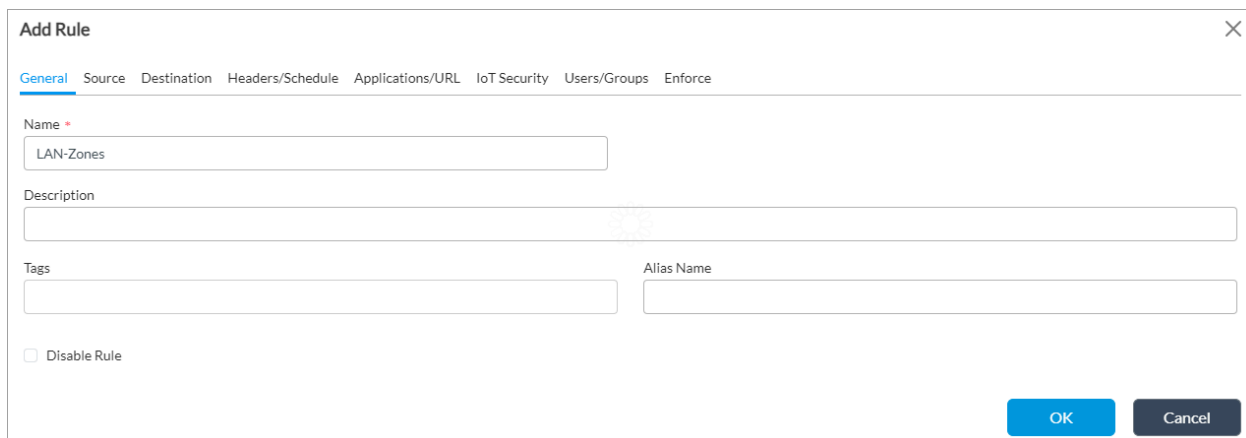
5. Click OK.

---

## Configure NGFW Rules To Allow Traffic from LAN Zones

To configure NGFW rules:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and then select the Rules tab.
4. Click the Add icon to define rules for the policy. The Add Rule popup window displays.



**Add Rule**

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce

Name \*  
LAN-Zones

Description

Tags

Alias Name

☐ Disable Rule

OK Cancel

5. Select the General tab, and then enter a name (here, LAN-Zones) for the rule in the Name field.
6. Select the Source tab.

**Add Rule**

General **Source** Destination Headers/Schedule Applications/URL IoT Security Users/Groups Enforce

☐ Source Zone + New Zone +

☐ Intf-LAN-Zone

☐ L2-intf-zone

☐ T1-REMOTE-CPVR-VR

☐ Source Address + New Address + New Address Group +

Source Address Not Configured

☐ Source Site Name +

Source Site Name Not Configured

☐ Source Address Negate

☐ Region +

Region Not Configured

☐ City +

City Not Configured

☐ State +

State Not Configured

☐ Source Location Negate

☐ Custom Geo Circle +

☐ Scalable Group Tag +

☐ EIP Profiles + Add EIP Profile +

OK Cancel

7. In the Source Zone field, click the Add icon, and then select the zones Intf-LAN-Zone, L2-intf-zone, and T1-REMOTE-CPVR-VR that you configured in [Configure Zones To Add Client-Facing Interfaces and Pair Tunnel Interfaces](#), above.
8. For information about configuring other parameters, see [Configure NGFW](#).
9. Click OK.

## Configure Captive Portal To Associate a Routing Instance

To modify the captive portal settings to add the routing instance that you configured for detecting trusted networks:

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 > Captive Portal in the left menu bar. The dashboard displays the Captive Portal Settings pane.
4. Click the Edit icon. The Edit Captive Portal Settings popup window displays.
5. Select the General tab.

Edit Captive Portal Settings

×

General

Custom Redirect Parameters

Anchoring

---Please Select---

▼

Global Expiration Time(min)

30

Provider Organization

---Please Select---

▼

SSL CA Certificate

---Please Select---

▼

Service Endpoints


▼

+ Add

	Routing Instance	Actions
<input type="checkbox"/>	Trusted-Network-Detection-CP-VR	

OK

Cancel

- In the Global Expiration Time field, enter how often users are redirected to the captive portal, in minutes. The first time a user enters a URL and is redirected to a captive portal page, the VOS device creates a cache entry. This cache entry expires after the global expiration time. Between the first time the user is redirected to the captive portal page and the expiration time, the captive portal action is not enforced and the user can go to the URL directly, without first seeing the captive portal page. The range is 1 through 65535 minutes, and the default is 30 minutes.
- In the Service Endpoints section, click the  Add icon to add a service endpoint. The Service Endpoint popup window displays.

**Service Endpoint**

Routing Instance \* HTTP Port HTTPS Port

Trusted-Network-Dete 80 443

IP Address 110.110.110.1 +

No Records to Display

Server URL \*.versa.com

Certificate ---Please Select---

Authentication Profile ---Please Select---

OK Cancel

8. In the Routing Instance field, select the routing instance (here, Trusted-Network-Detection-CP-VR) that you configured in [Configure a Virtual Router To Detect Trusted Networks](#), above.
9. In the HTTP Port field, enter the number (here, 80) of the HTTP port to use to redirect captive portal pages over HTTP.
10. In the HTTPS Port field, enter the number (here, 443) of the HTTPS port to use to redirect captive portal pages over HTTPS.
11. In the IP Address field, click the Add icon to add a service endpoint IP address (here, 110.110.110.1). Any traffic destined to this IP address is serviced by the captive portal.
12. In the Server group of fields, for URL, enter the captive portal server URL that is used to redirect traffic when any captive portal action is applied (here, \*.versa.com). This URL resolves to one of the IP address in the IP address list.
13. In the Certificate field, select the certificate to use for captive portal over SSL (here, RAS-Cert.crt).
14. For information about configuring other parameters, see Modify Captive Portal Settings in [Configure URL Filtering](#).
15. Click OK.

---

## Configure DNS Proxy

You configure DNS proxy with a redirection rule to respond to a domain name with a static IP address.

To configure a DNS proxy rule:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar
  - b. Select Devices > Devices in the horizontal bar.
  - c. Select an organization in the left menu bar.
  - d. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > DNS > Policies in the left menu bar.
4. Select the Rules tab in the horizontal menu.
5. Click Add or select an existing rule. The Add/Edit Redirection Rules popup window displays.
6. Select the General tab, and then enter a name for the rule (here, DNS-resolv-GW).

The screenshot shows the 'Edit Redirection Rules - DNS-resolv-GW' dialog box with the 'General' tab selected. The 'Name' field contains 'DNS-resolv-GW' and the 'Description' field is empty. The 'OK' and 'Cancel' buttons are at the bottom right.

7. Select the DNS Headers Match tab.

The screenshot shows the 'Edit Redirection Rules - DNS-resolv-GW' dialog box with the 'DNS Headers Match' tab selected. The 'Opcode' dropdown is set to 'Query'. The 'Query' section contains a table with the following data:

Type	Domain Name	Negate
--Select--		<input type="checkbox"/>
DNAME	Blr-sandbox.versa.com	<input checked="" type="checkbox"/>

The 'Advance Settings' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

8. In the Opcode field, select Query as the DNS header operation code.
9. In the Query section, select DNAME in the Type field.


10. In the Domain Name field, enter a domain name (here, Blr-sandbox.versa.com).
11. Select the Users/Groups tab, and then in the Match Users field, select Any.

The screenshot shows the 'Edit Redirection Rules - DNS-resolv-GW' dialog box with the 'Users/Groups' tab selected. The 'Match Users' dropdown is set to 'Any'. The 'User Group Profile' dropdown is set to '--Select--'. There are checkboxes for 'Local Database' and 'External Database'. Below these are two sections: 'Users' and 'Groups', each with a '+ New Custom User' or '+ New Custom Group' button and a trash icon. The 'Users' section shows 'Users Not Configured' and the 'Groups' section shows 'Groups Not Configured'. At the bottom right are 'OK' and 'Cancel' buttons.

12. Select the Proxy Setting tab.

The screenshot shows the 'Edit Redirection Rules - DNS-resolv-GW' dialog box with the 'Proxy Setting' tab selected. The 'Actions' section has radio buttons for 'Proxy Setting', 'Server Setting' (which is selected and highlighted with a red box), and 'None'. The 'Proxy Setting' section includes a 'Proxy Profile' dropdown set to '--Select--', a 'Number of Domains to Cache' input field, and a 'DNS64 Prefix' input field. There is a '+ Proxy Profile' button and an 'Override Question' text area. Below these are checkboxes for 'Only IPv4 WAN Available', 'Network Obfuscation', 'Apply Policy Based Forwarding', and 'Unique IP Per Client'. The 'Dynamic Destination IP Pool' dropdown is set to '--Select--' and the 'Cache TTL Upper Limit (seconds)' input field is empty. The 'Server Setting' section has a table with columns 'Address', 'Monitor Object', and an action column. The 'Address' row shows '100.100.100.1' (highlighted with a red box) and the 'Monitor Object' row shows '--Select--'. There is a '+ Add' button and a trash icon. The 'Logging Setting' section has a 'LEF Profile' dropdown set to '--Select--' and a 'Default Profile' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

13. In the Actions section, click Server Setting.

14. In the Server Setting section, click the  Add icon, and then enter the IP address of the server (here, 100.100.100.1). This address maps the host that the SASE client uses to connect to the gateway to the gateway server.
15. For information about configuring other parameters, see [Configure DNS Redirection Rules](#).
16. Click OK.

---

## Configure Authentication Profiles and Users in a Database


You configure authentication profiles and use them to identify users that use Versa SASE client to connect to the SASE gateway. You configure these users or user groups using an external, an LDAP, a local, or a SAML database, or any other database.

The following example shows how to use a local database to authenticate users. For this, you do the following:

- Configure the local authentication method.
- Configure an authentication profile, and then associate it with the local authentication method.
- Add local database users.
- Add the authenticator profile for local database users.

---

## Configure an Authentication Method

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 Object and Connectors > Connectors > Users/Groups > Authentication Methods in the left menu bar.
4. Click the  Add icon. The Add Authentication Methods popup window displays.





5. In the Name field, enter a name for the authentication method (here, local-auth).
6. In the Authentication Method field, select Local Profile.
7. Click OK.

For more information, see [Configure an Authentication Method](#).

---

## Configure an Authentication Profile

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 Object and Connectors > Connectors > Users/Groups > Authentication Profiles in the left menu bar.
4. Click the  Add icon. The Add Authentication Profile popup window displays.

5. Select the General tab.
6. In the Name field, enter a name for the authentication profile (here, local-auth).
7. In the Default Authentication Method field, click the  Add icon, and then select the authentication method that you configured in [Configure an Authentication Method](#), above (here, local-auth).
8. For information about configuring other parameters, see [Configure an Authentication Profile](#).
9. Click OK.

## Configure Local Database Users


To configure local database users, see [Configure Local Database Users](#).

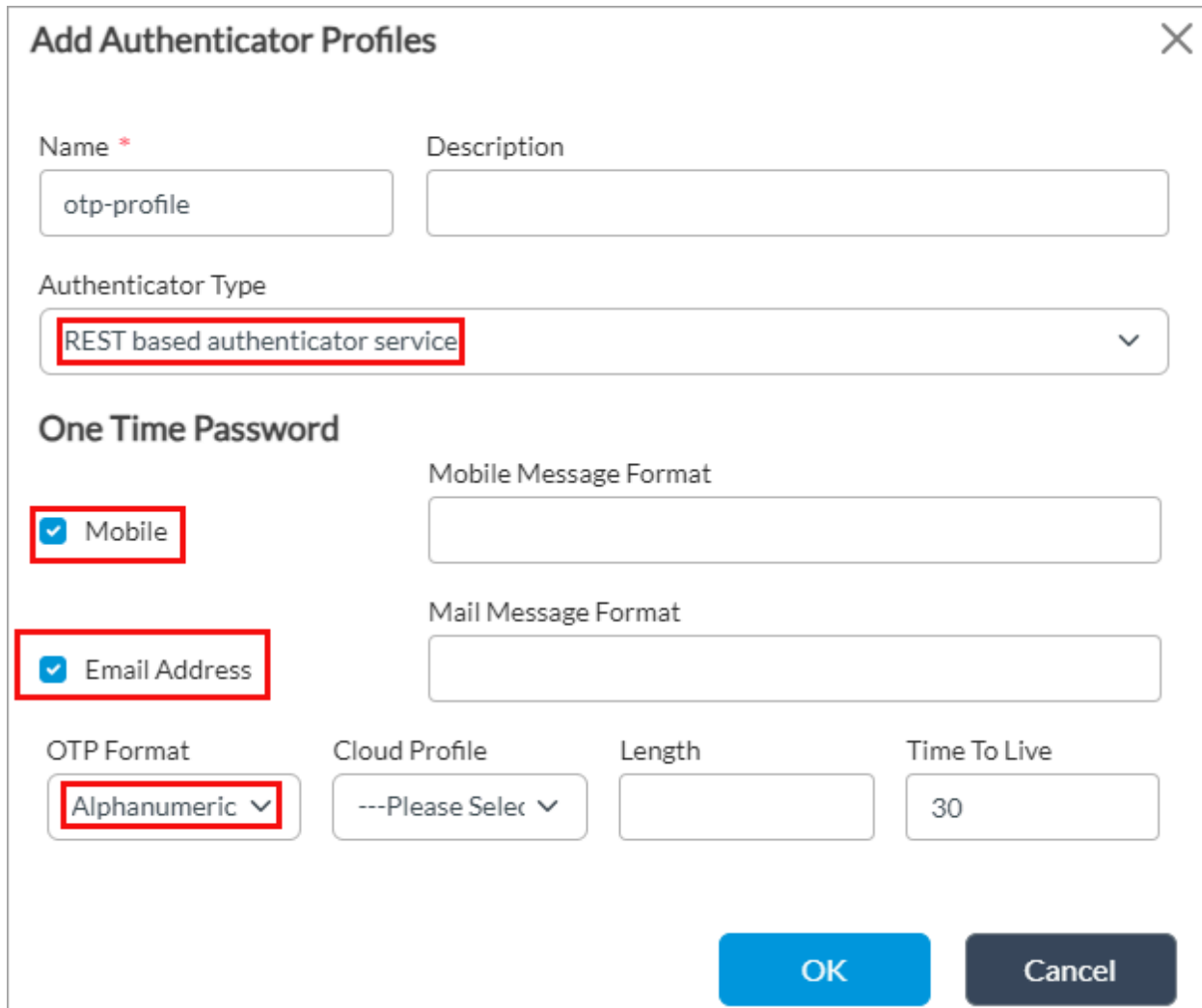
## Configure an Authenticator Profile

Before you configure an authenticator profile, ensure that SMTP server settings are enabled, to support two-factor authentication using a one-time password (OTP). For more information about receiving an OTP through email, see [Configure SMTP Server Settings](#).

To configure an authenticator profile:

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 Objects & Connectors > Connectors > Users/Groups > Authenticator Profiles in the left menu bar.
4. Click the  Add icon. The Add Authenticator Profiles popup window displays.



The image shows a 'Add Authenticator Profiles' popup window. It has a title bar with a close button (X). The form contains several fields and sections:

- Name \***: A text input field containing 'otp-profile'.
- Description**: An empty text input field.
- Authenticator Type**: A dropdown menu with 'REST based authenticator service' selected and highlighted by a red box.
- One Time Password**: A section header.
- Mobile**: A checkbox that is checked and highlighted by a red box.
- Mobile Message Format**: An empty text input field.
- Email Address**: A checkbox that is checked and highlighted by a red box.
- Mail Message Format**: An empty text input field.
- OTP Format**: A dropdown menu with 'Alphanumeric' selected and highlighted by a red box.
- Cloud Profile**: A dropdown menu with '---Please Select' selected.
- Length**: An empty text input field.
- Time To Live**: A text input field containing '30'.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

5. In the Name field, enter a name for the authenticator profile (here, otp-profile).
6. In the One-Time Password select, click Mobile and Email Address.
7. In the OTP Format field, select Alphanumeric.
8. For information about configuring other parameters, see [Configure an Authenticator Profile](#).
9. Click OK.

---

## Configure EIP Objects and Profiles


You configure EIP objects and EIP profiles, and then you associate them with a microsegmentation policy.

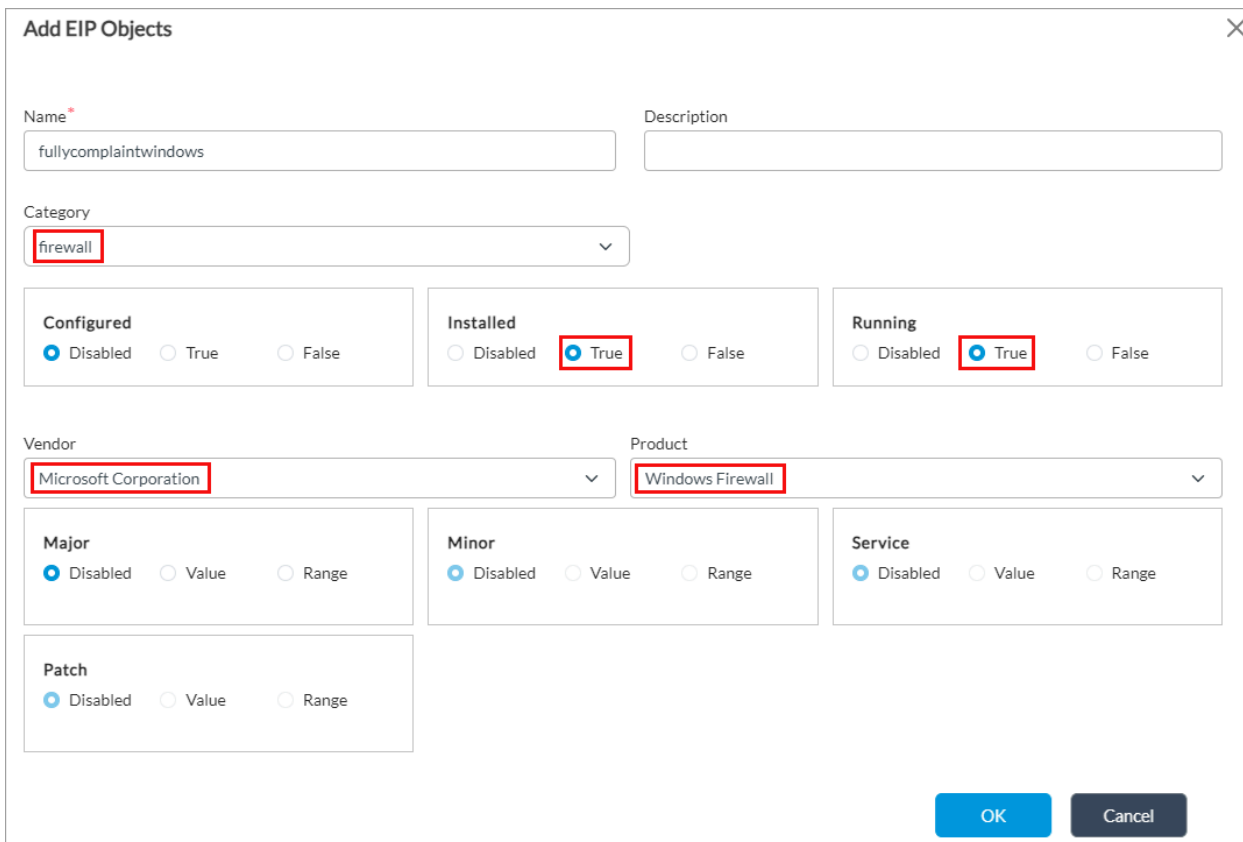
---

### Configure EIP Objects

In this example, we configure Windows firewall-based EIP objects.

To configure EIP objects:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > EIP Objects in the left menu bar.
4. Click the  Add icon. The Add EIP Objects popup window displays.



**Add EIP Objects**

Name <sup>\*</sup> fullycomplaintwindows Description

Category firewall

**Configured**  
☒ Disabled ☐ True ☐ False

**Installed**  
☐ Disabled ☒ True ☐ False

**Running**  
☐ Disabled ☒ True ☐ False

Vendor Microsoft Corporation Product Windows Firewall

**Major**  
☒ Disabled ☐ Value ☐ Range

**Minor**  
☒ Disabled ☐ Value ☐ Range

**Service**  
☒ Disabled ☐ Value ☐ Range

**Patch**  
☒ Disabled ☐ Value ☐ Range

OK Cancel

5. In the Name field, enter a name for the EIP object (here, fullycomplaintwindows).

6. In the Category field, select Firewall.
7. In the Installed and Running fields, click True.
8. In the Vendor field, select the vendor (here, Microsoft Corporation).
9. In the Product field, select a product from the vendor you select (here, Windows Firewall).
10. Click OK.
11. Add a second EIP object (here, Partialcompliantwindows) with the values displayed in the following screenshot.

**Edit EIP Objects - Partialcompliantwindows**

Name\*  Description

Category

**Configured** ☐ ☒ ☐

**Installed** ☐ ☒ ☐

**Running** ☐ ☐ ☒

Vendor  Product

**Major** ☒ ☐ ☐

**Minor** ☒ ☐ ☐

**Service** ☒ ☐ ☐

**Patch** ☒ ☐ ☐

**OK** **Cancel**

12. Click OK.

## Configure EIP Profiles

To configure an EIP agent profile:


1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Custom Objects > SASE Client > EIP Agent Profiles in the left menu

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_EIP-Based\\_Microsegmentation\\_for...](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_EIP-Based_Microsegmentation_for...)

Updated: Wed, 23 Oct 2024 08:45:51 GMT

Copyright © 2024, Versa Networks, Inc.

bar.

- Click the  Add icon. The Add EIP Profiles popup window displays.

Add EIP Profiles

Name\*

Partialcompliant


Description


LEF Profile


--Select--


+ Create Log Profile


☐ Default Profile






















1




25



<input type="checkbox"/>	Name	Description	Match Categories
No Rules Added			

OK

Cancel

- In the Name field, enter a name for the EIP profile (here, Partialcompliant).
- Click the  Add icon to add a rule for the profile. The Add Rules popup window displays.
- Select the General tab, and then enter a name for the rule.

Add Rules

General

Match

Name\*

rule1

Description

OK

Cancel

8. Select the Match tab.

Add Rules

General

Match

Match Categories

+

<

1


>

25

<input type="checkbox"/>	Category	User Defined EIP Objects	Predefined EIP Objects
No Rules Added			

OK

Cancel

9. In the Match Categories section, click the  Add icon. The Add Rules Add Match Category popup window displays.

**Add Rules Add Match Category**

Category  
 firewall

User Defined EIP Objects

<input type="checkbox"/>	User Defined EIP Objects	+ Add EIP Object + [trash] [refresh]
<input checked="" type="checkbox"/>	Partialcompliantwindows	

Predefined EIP Objects

<input type="checkbox"/>	Predefined EIP Objects	+ [trash] [refresh]
Predefined EIP Objects Not Configured		

OK Cancel

10. In the Category field, select Firewall.
11. In the User-Defined EIP Objects field, click the **+** Add icon, and then select the EIP object that you configured in [Configure EIP Objects](#), above.
12. Click OK.
13. Repeat Steps 4 through 13 to create another EIP profile (here, the name is VSA-client, and fullycomplaintwindows is the EIP object associated with the rule match category).


## Configure a SASE Gateway for Gateway–Trusted Network Mode

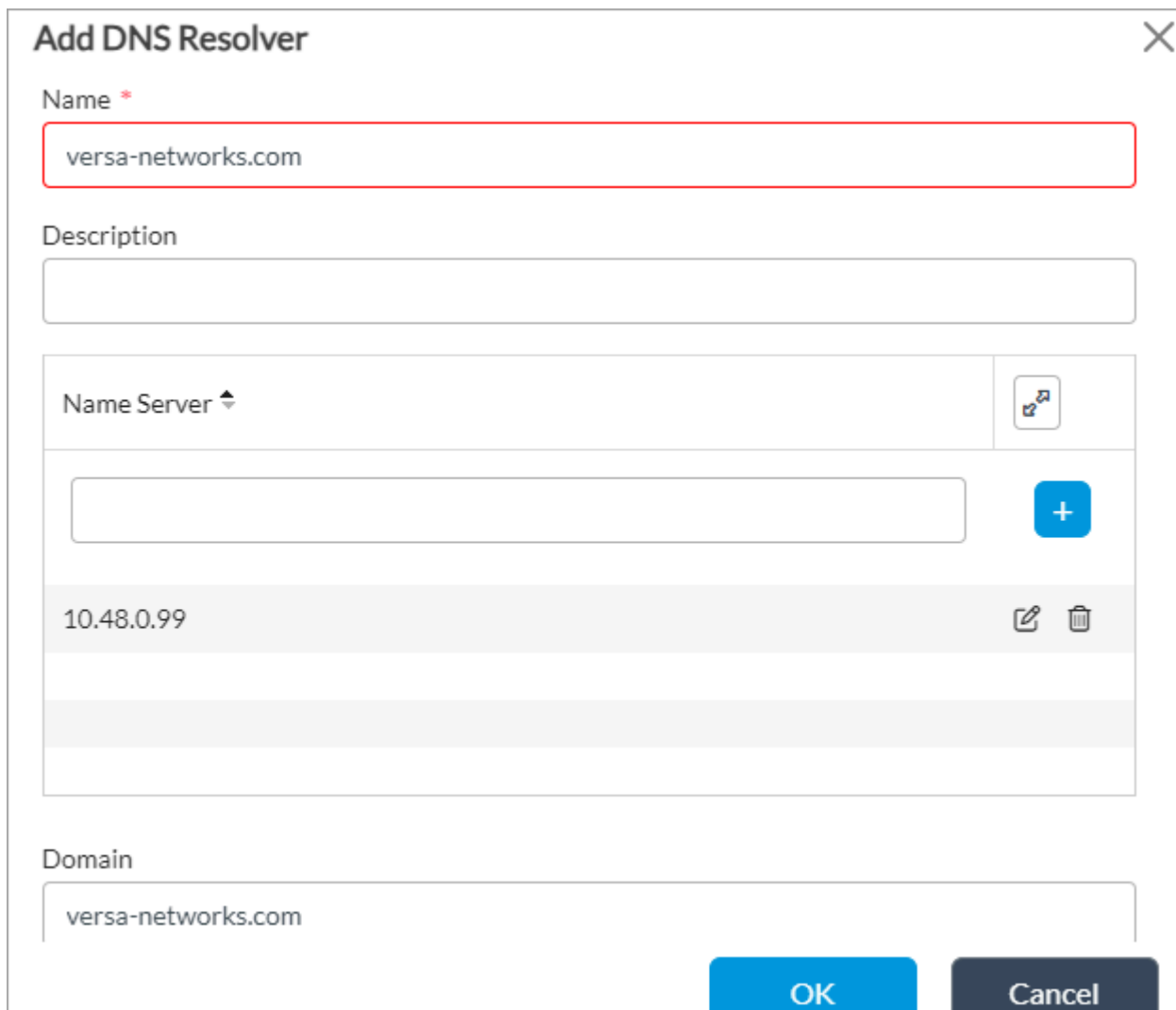
If you enable the detection of trusted networks for a SASE gateway, when the client attempts to connect to the gateway, you can configure the gateway so that informs the client that it is connected to a trusted network so that the client can then bypass the tunnel.

The following sections describe a configuration example to enable a SASE gateway for detecting trusted networks.




## Configure a DNS Resolver

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal> DNS Resolvers in the left menu bar.
4. Click the  Add icon. The Add DNS Resolver popup window displays.



The image shows a 'Add DNS Resolver' popup window. It has a title bar with a close button (X). The form contains the following fields and controls:


- Name \***: A text input field containing 'versa-networks.com', highlighted with a red border.
- Description**: An empty text input field.
- Name Server**: A section with a dropdown menu (currently showing 'Name Server'), a list of IP addresses, and a '+ Add' button.
  - The list contains one entry: '10.48.0.99'.
  - Each entry has edit and delete icons to its right.
- Domain**: A text input field containing 'versa-networks.com'.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

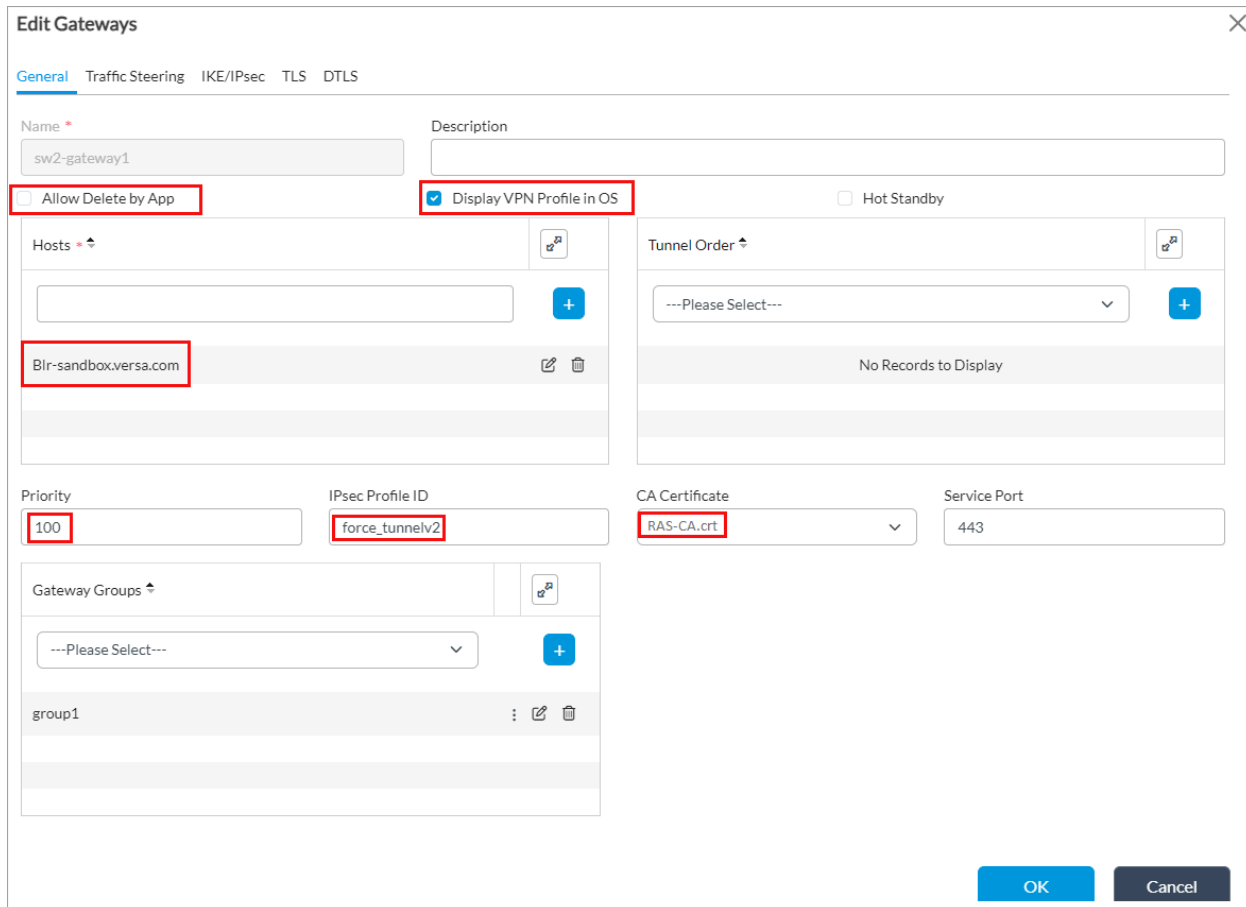
5. In the Name field, enter a name for the DNS resolver (here, versa-networks.com).
6. In the Name Server field, enter the DNS name IP address (here, 10.48.0.99) and click the  Add icon.

7. In the Domain field, enter the name of the domain in which the DNS resolver is located (here, versa-networks.com).
8. Click OK.

---

## Configure a Secure Access Gateway Server

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateways in the left menu bar.
4. Click the  Add icon. The Add Profiles popup window displays.



**Edit Gateways**

General Traffic Steering IKE/IPsec TLS DTLS

Name \* sw2-gateway1 Description

☒ Allow Delete by App ☒ Display VPN Profile in OS ☐ Hot Standby

Hosts \* Blr-sandbox.versa.com

Tunnel Order \* ---Please Select---


No Records to Display

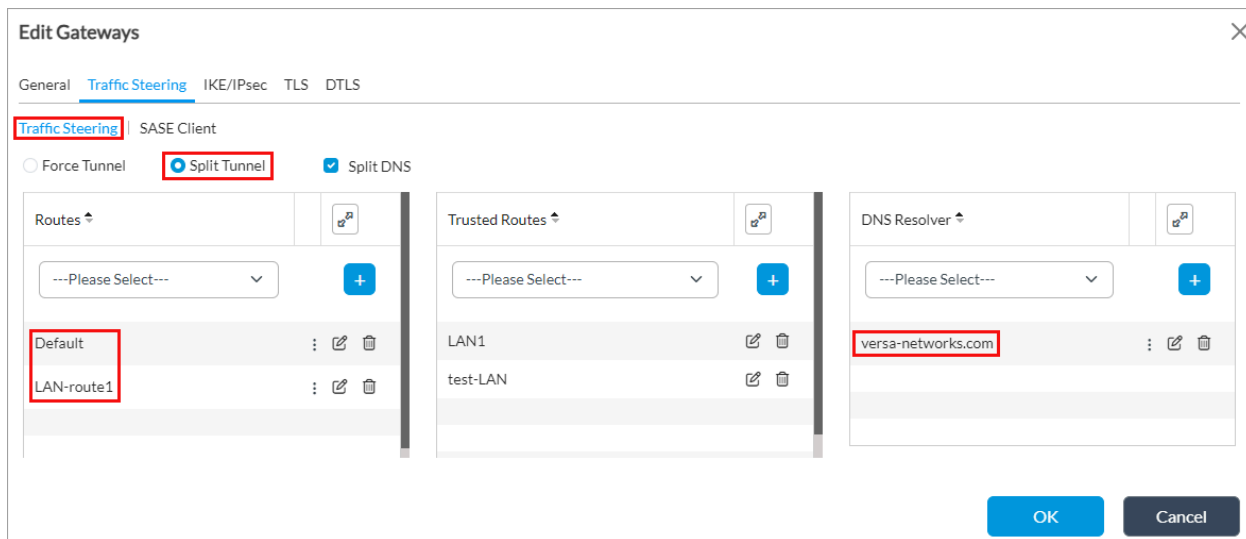
Priority 100 IPsec Profile ID force\_tunnelv2 CA Certificate RAS-CA.crt Service Port 443

Gateway Groups \* group1



OK Cancel

5. Select the General tab.
6. In the Name field, enter a for the gateway profile (here, sw2-gateway1).

7. Ensure that Allow Delete by App is not enabled. When it is enabled, gateways can be deleted on the secure access client.
8. Click Display VPN Profile in OS to display configured VPN profiles in the native user device's operating system.
9. In the Hosts field, enter the IP address or FQDN of the host that the SASE client uses to connect to the gateway and click the  Add icon to add (here, Blr-sandbox.versa.com).
10. In the Priority field, enter a value to set the order in which the server is listed on the SASE client (here, 100).
11. In the IPsec Profile ID field, enter the identifier of the IPsec profile of the secure access server profile (here, force\_tunnelv2).
12. In the CA Certificate field, select the CA certificate for the captive portal certificate (here, RAS-CA.crt).
13. Select the Traffic Steering tab.



The screenshot shows the 'Edit Gateways' dialog box with the 'Traffic Steering' tab selected. Under the 'SASE Client' section, the 'Split Tunnel' option is selected. The 'Routes' list contains 'Default' and 'LAN-route1'. The 'Trusted Routes' list contains 'LAN1' and 'test-LAN'. The 'DNS Resolver' list contains 'versa-networks.com'. The 'OK' and 'Cancel' buttons are at the bottom right.

14. Select the lower Traffic Steering tab.
15. Click Split Tunnel.
16. Optionally, in the Routes field, select the secure access routes, and then click the  Add icon. For more information, see [Configure Secure Access Routes](#).
17. In the DNS Resolver field, select the DNS resolver that you configured in [Configure a DNS Resolver](#), above, (here, versa-networks.com), and then click the  Add icon.
18. For information about configuring other parameters, see Configure Secure Access Servers in [Configure Versa Secure Access Service](#).
19. Click OK.

## Configure the Secure Access Gateway Service


To configure the secure access gateway service to detect trusted networks, and to configure other settings:

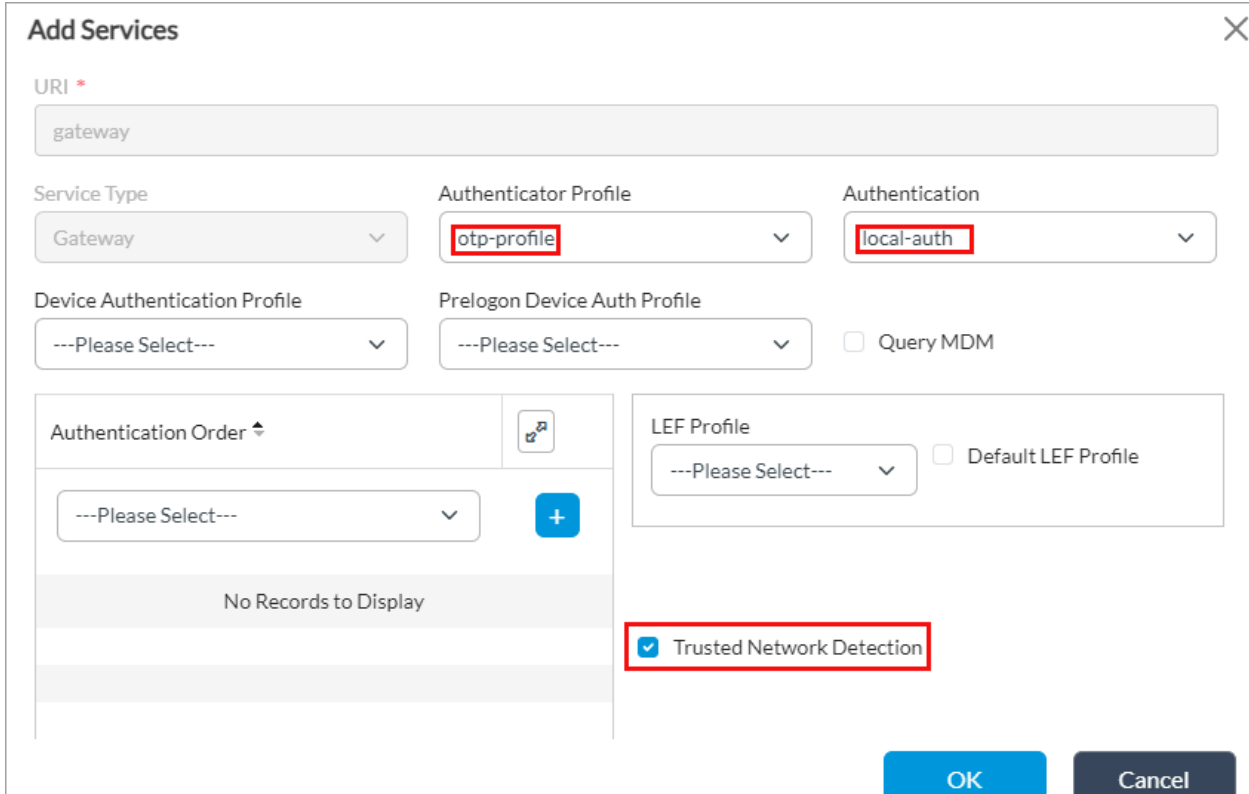
1. In Director view:

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_EIP-Based\\_Microsegmentation\\_for...](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_EIP-Based_Microsegmentation_for...)

Updated: Wed, 23 Oct 2024 08:45:51 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
  3. Select Services > Secure Access > Gateway> General in the left menu bar.
  4. Click the  Edit icon. The Add Services popup window displays.



5. In the Authenticator Profile field, select the authenticator profile that you configured in [Configure an Authenticator Profile](#), above (here, otp-profile).
6. In the Authentication field, select local-auth.
7. Click Trusted Network Detection to enable the detection of trusted networks for the gateway. When you configure the detection of trusted networks on a VOS device, the SASE client attempts to reach the host by bypassing the tunnel. For more information, see [Use the Versa SASE Client Application](#).
8. For information about configuring other parameters, see Configure a Secure Access Gateway in [Configure the Secure Access Service Gateway](#).
9. Click OK.


## Configure Secure Access Portal

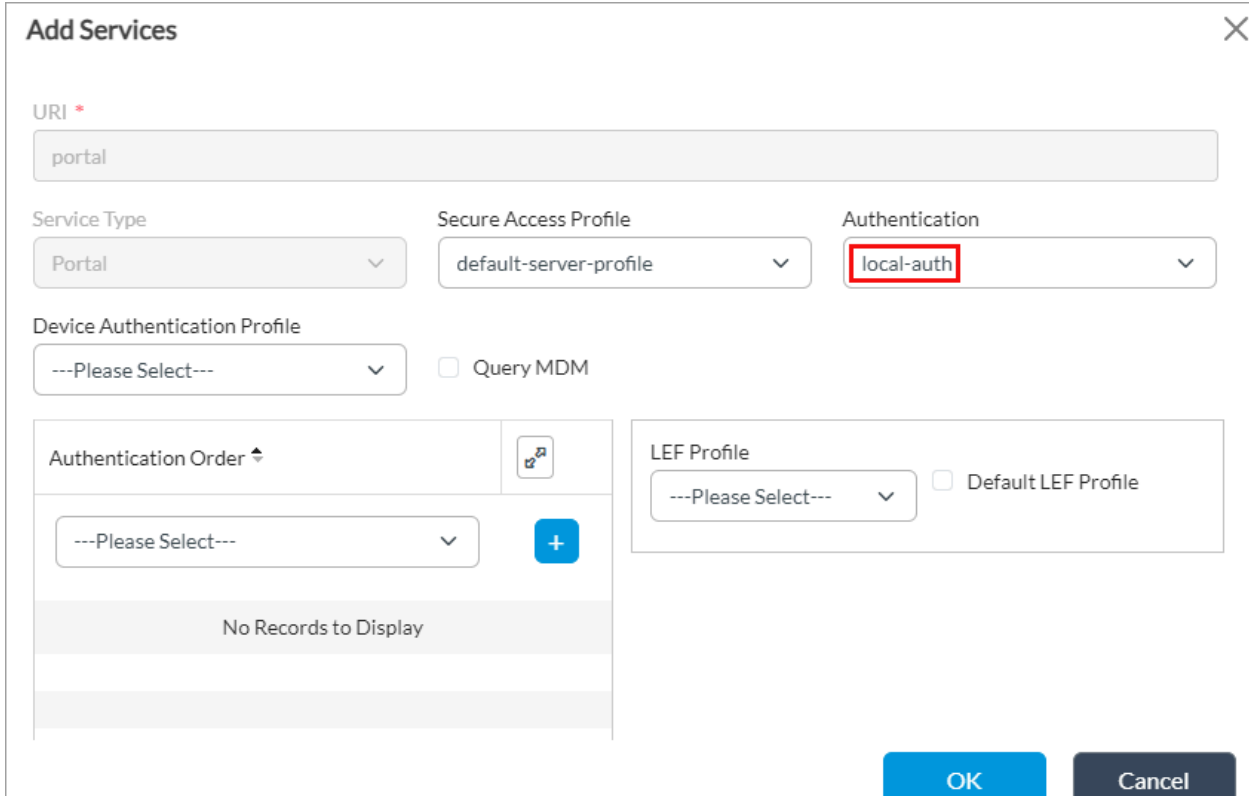
1. In Director view:

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_EIP-Based\\_Microsegmentation\\_for...](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_EIP-Based_Microsegmentation_for...)

Updated: Wed, 23 Oct 2024 08:45:51 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
  3. Select Services > Secure Access > Portal > General in the left menu bar.
  4. Click the  Edit icon. The Add Services popup window displays.




5. In the Authentication field, select local-auth.
6. For information about configuring other parameters, see Add a Secure Access Portal in [Configure Versa Secure Access Service](#).
7. Click OK.

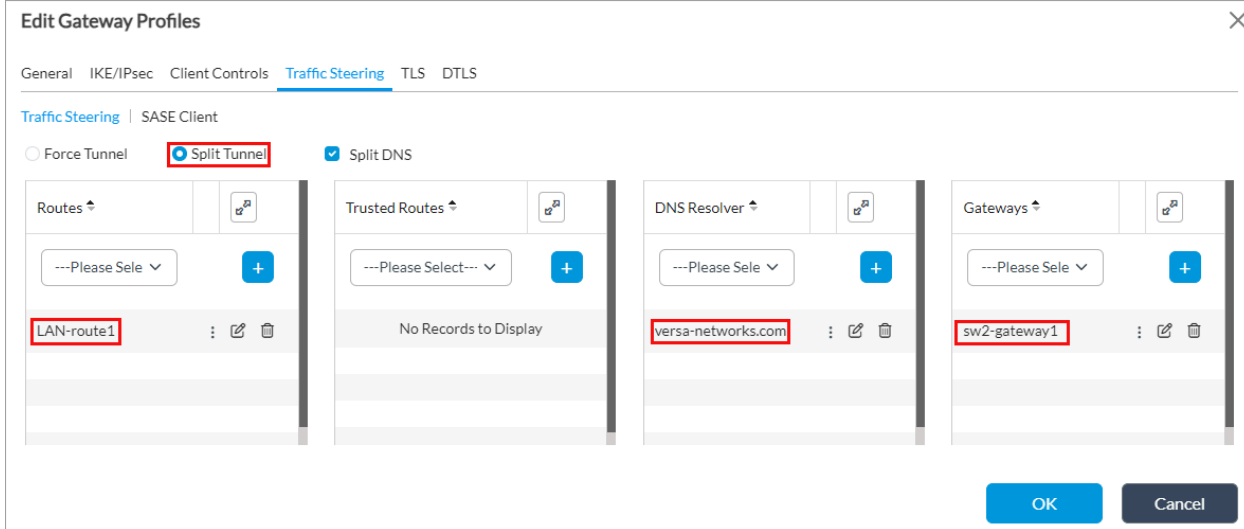
## Configure a Secure Access Gateway Profile




You configure a secure access gateway profile and associate with it the gateway that you configure.

To configure a secure access profile:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.

- b. Select Templates > Device Templates in the horizontal menu bar.
- c. Select an organization in the left menu bar.
- d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateway Profiles in the left menu bar.
4. Click the  Add icon. The Add Profiles popup window displays.
5. Select the Traffic Steering tab.



6. Click Split Tunnel.
7. Optionally, in the Routes field, select the secure access routes, and then click the  Add icon. For more information, see [Configure Secure Access Routes](#).
8. In the DNS Resolver field, select the DNS resolver that you configured in [Configure a DNS Resolver](#), above, (here, versa-networks.com), and then click the  Add icon.
9. In the Gateways field, select the gateway that you configured in [Configure a Secure Access Gateway Server](#), above, (here, sw2-gateway1), and then click the  Add icon.
10. For information about configuring other parameters, see Configure Secure Access Gateway Profiles in [Configure Versa Secure Access Service](#).
11. Click OK.

## Add a Secure Access Portal Policy Rule To Set the EIP Agent Profile

You configure a secure access portal policy rule to associate EIP profiles and other match criteria with a policy.


To configure a secure access portal policy rule:

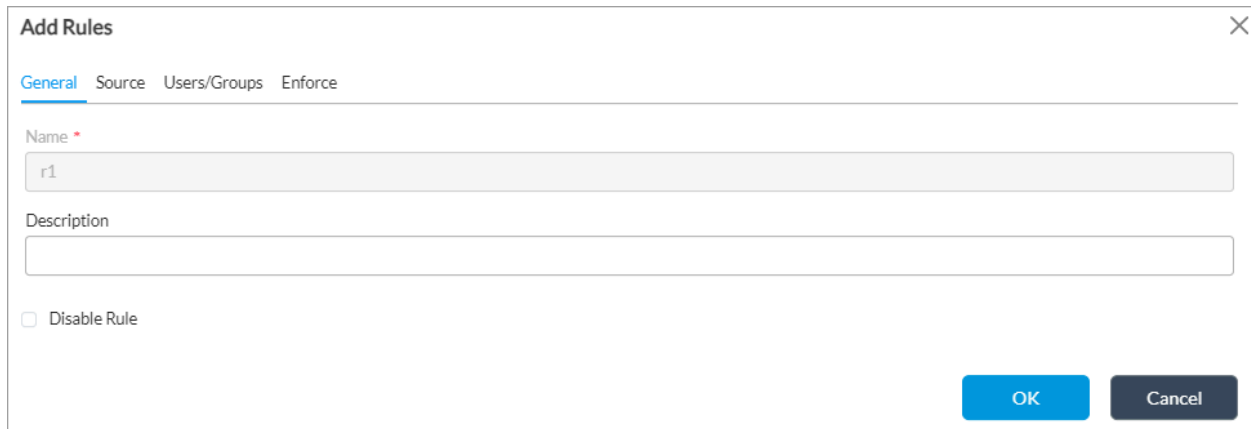
1. In Director view:

[https://docs.versa-networks.com/Secure\\_SD-LAN/Configuration\\_from\\_Director/Configure\\_EIP-Based\\_Microsegmentation\\_for...](https://docs.versa-networks.com/Secure_SD-LAN/Configuration_from_Director/Configure_EIP-Based_Microsegmentation_for...)

Updated: Wed, 23 Oct 2024 08:45:51 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
- b. Select Templates > Device Templates in the horizontal menu bar.
- c. Select an organization in the left menu bar.
- d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Policies in the left menu bar, and then select the Rules tab.
4. Click the  Add icon. The Add Rules popup window displays.
5. Select the General tab, and then enter a name (here, r1).



**Add Rules** [X]

General | Source | Users/Groups | Enforce

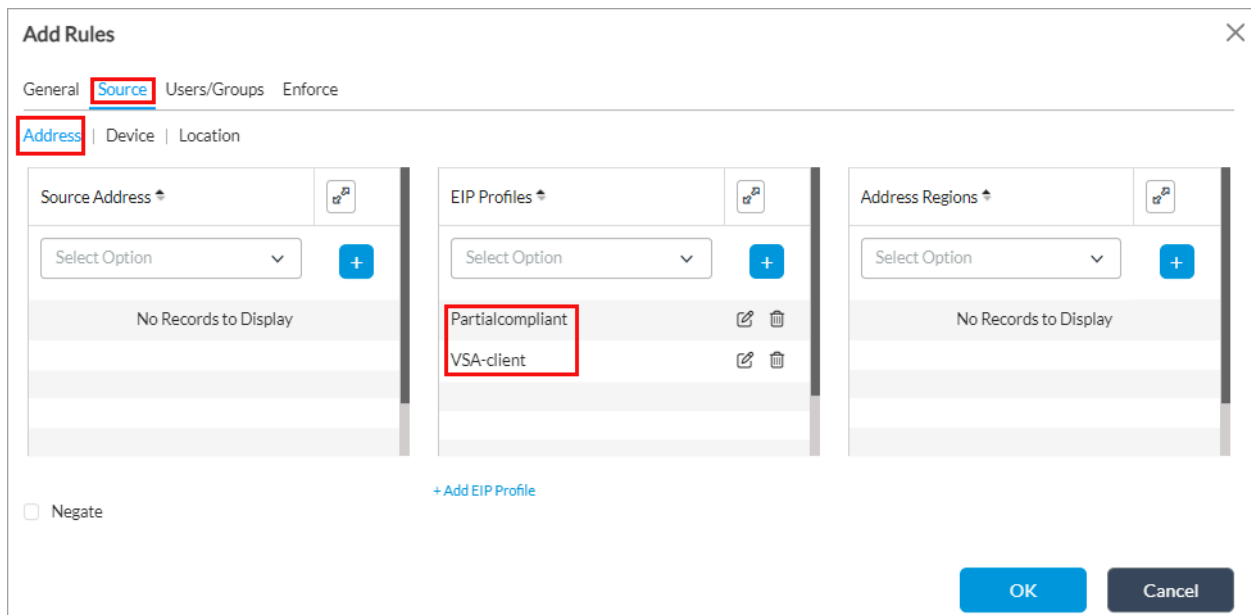
Name \*  
r1

Description  
[Empty text box]

☐ Disable Rule

OK Cancel

6. Select the Source tab, and then select the Address tab.



**Add Rules** [X]

General | **Source** | Users/Groups | Enforce

**Address** | Device | Location

Source Address

Select Option [v] [Add]

No Records to Display

EIP Profiles

Select Option [v] [Add]

Partialcompliant	[Edit]	[Delete]
VSA-client	[Edit]	[Delete]

+ Add EIP Profile


Address Regions

Select Option [v] [Add]

No Records to Display

☐ Negate

OK Cancel

7. In the EIP Profiles field, select the EIP profiles that you configured in [Configure EIP Profiles](#), above, (here, Partialcompliant and VSA-client), and then click the  Add icon .

8. Select the Users/Groups tab. In the Match Users field, select Known.

The screenshot shows the 'Add Rules' dialog box with the 'Users/Groups' tab selected. The 'Match Users' dropdown is set to 'Known'. The 'User Group Profile' dropdown is set to '---Please Select---'. There are checkboxes for 'Local Database' and 'External Database'. Below these are two sections: 'Users' and 'Groups', each with a 'Select Option' dropdown and a '+' button. Both sections show 'No Records to Display'. At the bottom right are 'OK' and 'Cancel' buttons.

9. Select the Enforce tab.

The screenshot shows the 'Add Rules' dialog box with the 'Enforce' tab selected. The 'Action' dropdown is set to 'Allow'. The 'Authenticator Profile' dropdown is set to '---Please Select---'. The 'Secure Access Profile' dropdown is set to 'default-server-profile'. The 'EIP Agent Profiles' dropdown is set to 'Versa\_Recommended'. The 'Message' field contains the text 'Microsegmentation profile configured'. At the bottom right are 'OK' and 'Cancel' buttons.

10. In the Action field, select an action (here, Allow).
11. In the Secure Access Profile, select a profile (here, default-server-profile).
12. In the EIP Agent Profiles field, select a predefined EIP profile (here, Versa\_Recommended).
13. For information about configuring other parameters, see Add a Secure Access Portal Policy Rule in [Configure Versa Secure Access Service](#).
14. Click OK.

You also add a secure access gateway policy rule with enforce action set to Allow. For more information, see Add a Secure Access Gateway Policy Rule in [Configure Versa Secure Access Service](#).

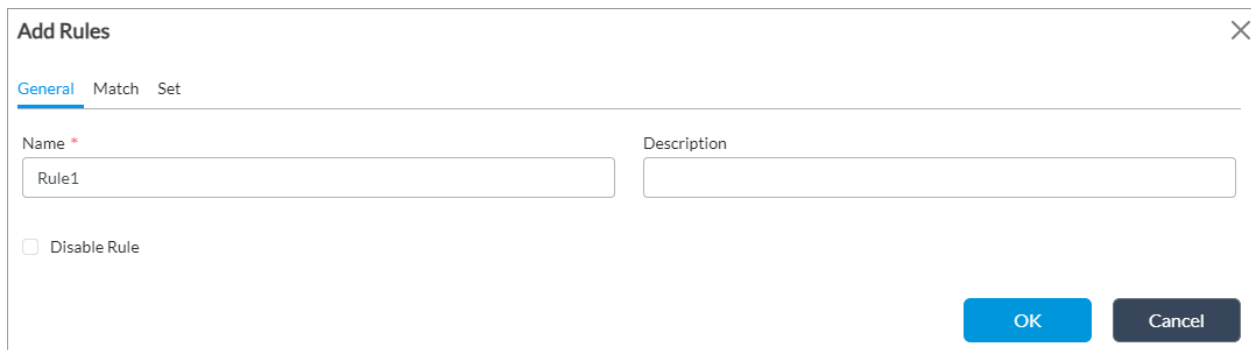
## Configure Microsegmentation Rules To Associate EIP Profiles

You configure microsegmentation policy rules to associate EIP profiles for EIP-based microsegmentation.



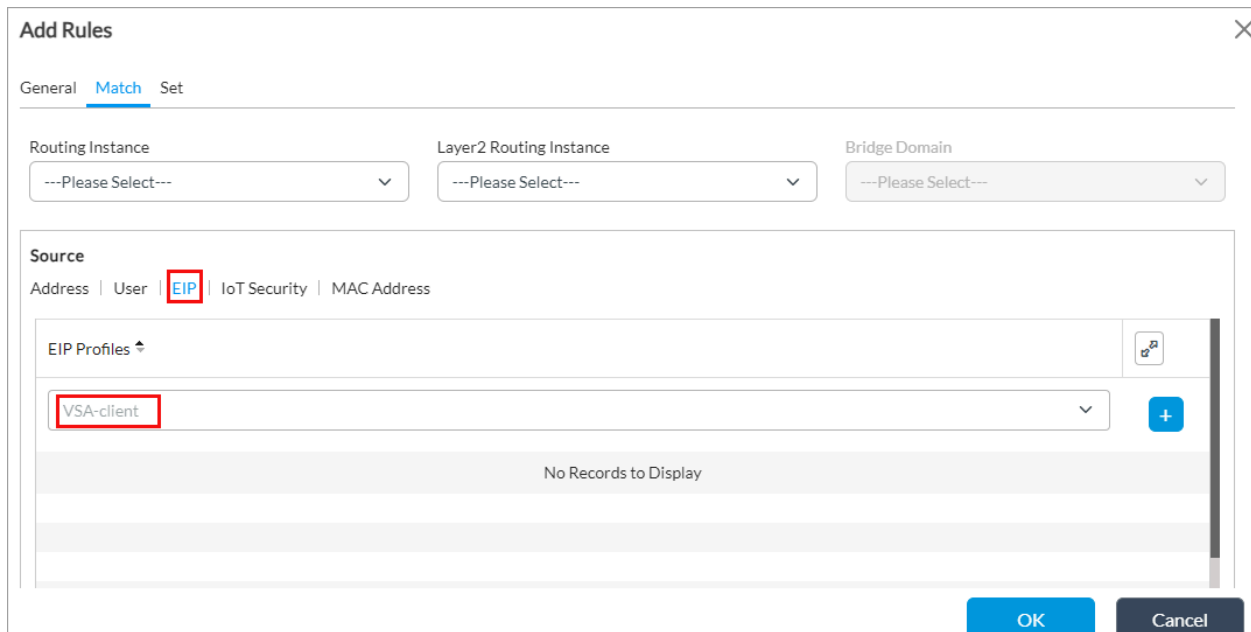
To configure a microsegmentation policy rule:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select the device from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Microsegmentation > Policies in the left menu bar.
4. Select the Rules tab, and then click + Add.
5. Select the General tab, and then enter a name.




The screenshot shows the 'Add Rules' dialog box with the 'General' tab selected. It has a title bar with a close button (X). Below the title bar are three tabs: 'General' (active), 'Match', and 'Set'. The 'General' tab contains a 'Name' field with the text 'Rule1' and a 'Description' field. Below these fields is a checkbox labeled 'Disable Rule'. At the bottom right are 'OK' and 'Cancel' buttons.

6. Select the Match tab. In the Source section, select the EIP tab.



The screenshot shows the 'Add Rules' dialog box with the 'Match' tab selected. It has a title bar with a close button (X). Below the title bar are three tabs: 'General', 'Match' (active), and 'Set'. The 'Match' tab contains three dropdown menus: 'Routing Instance', 'Layer2 Routing Instance', and 'Bridge Domain', all with the text '---Please Select---'. Below these is a 'Source' section with four tabs: 'Address', 'User', 'EIP' (active), and 'IoT Security | MAC Address'. The 'EIP' tab shows a list of 'EIP Profiles' with a dropdown menu containing 'VSA-client' and a blue '+' button. Below the list is a message 'No Records to Display'. At the bottom right are 'OK' and 'Cancel' buttons.

7. In the EIP Profiles field, select an EIP profile that you configured in [Configure EIP Profiles](#), above, (here, VSA-client), and then click the  Add icon.
8. Select the Set tab. In the Scalable Group Tag field, select or add a tag for the rule (here, VSA-200).

The screenshot shows a dialog box titled "Add Rules" with a close button (X) in the top right corner. It has three tabs: "General", "Match", and "Set", with "Set" being the active tab. Below the tabs, there is a label "Scalable Group Tag" followed by a dropdown menu. The dropdown menu is open, showing a list with "VSA-200" selected. At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (dark grey).

9. For more information about configuring other parameters, see [Configure Microsegmentation Rules](#).
10. Repeat Steps 1 through 8 to add a second microsegmentation rule and associate the other EIP profile (Partialcompliant) that you configured in [Configure EIP Profiles](#), above.

---

## Supported Software Information

Releases 22.1.3 and later support all content described in this article.

---

## Additional Information

[Configure DNS Proxy](#)

[Configure Interfaces](#)

[Configure Microsegmentation](#)

[Configure NGFW](#)

[Configure Organization Limits](#)

[Configure the Versa Secure Access Service](#)

[Configure URL Filtering](#)

[Configure User and Group Policy](#)

[Configure Virtual Routers](#)

[Configure Zones and Zone Protection Profiles](#)

[Use the Versa SASE Client Application](#)