
Configure Direct Breakout to the Internet



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

Direct internet access (DIA) enables local breakout of internet-bound traffic or public cloud traffic directly from a branch to the internet. The following are the primary advantages of DIA:

- Prioritization of traffic flows.
- Reduced latency and cost savings as a result of direct routing and traffic flow optimization.
- Reduced bandwidth consumption—You can forward non-business traffic, such as the traffic from gaming, Facebook, and other applications, directly to the internet directly rather than having it go through an SD-WAN hub. Doing so decreases SD-WAN hub bandwidth, preventing it from getting overloaded.

This article describes the steps to configure direct breakout to the internet:

- Configure CGNAT to translate the private network addresses of Internet-bound traffic to public addresses.
- Configure a split tunnel to use for DIA traffic.
- Configure a policy that breaks out traffic to the Internet. This article shows examples of three different policies.

Configure CGNAT

To configure CGNAT, you do the following:

- Associate a CGNAT subscription plan with an organization.
- Configure Ethernet Interfaces
- Configure a customer virtual router and a transport virtual router—Traffic from the customer LAN is sent to the WAN through virtual routers. The customer virtual router connects to a transport virtual router, which directs traffic to the internet.
- Configure a transport virtual router.
- Configure CGNAT address and port pools and CGNAT rules.

Associate a CGNAT Subscription Plan with an Organization

When you create a device configuration template, you place a device in an organization and you associate a Versa Networks software subscription with the organization. The subscription defines an solution tier, and the solution tier must be one that supports CGNAT.



To associate a CGNAT subscription plan with an organization:

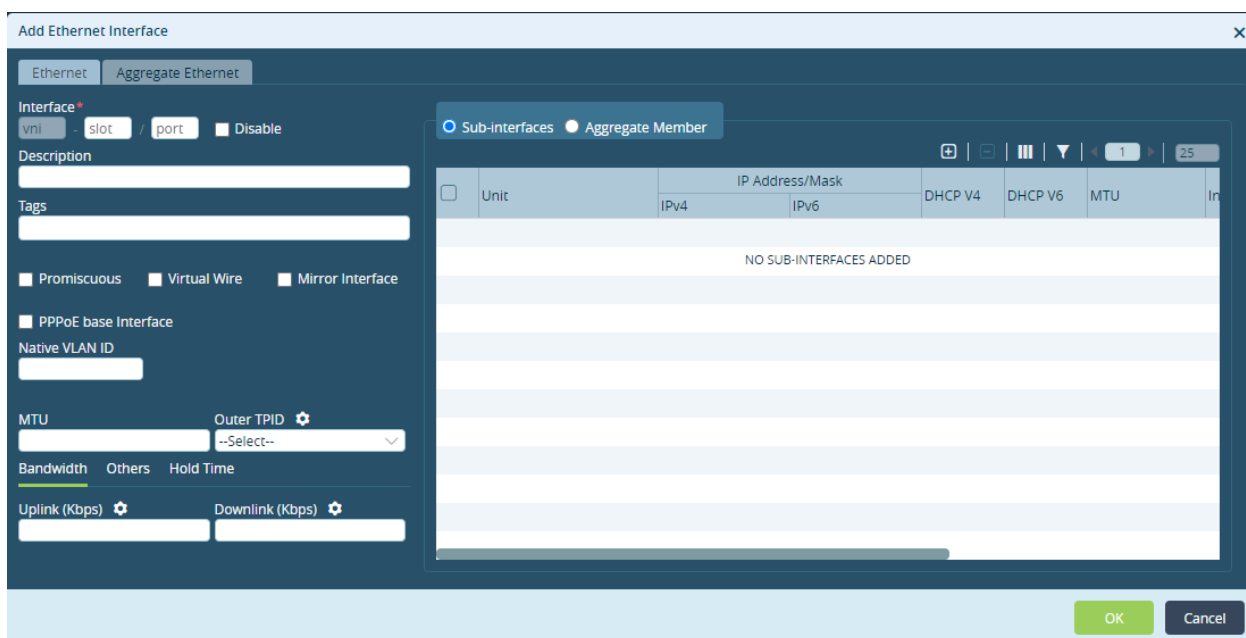
1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the left menu bar.
3. Select a template in the main pane.
4. In the Appliance view, select the organization's name.
5. In the Basic tab, in the Subscription group of fields, associate the organization with a subscription plan that supports CGNAT. For more information, see [Configure Basic Features](#).


Configure Ethernet Interfaces

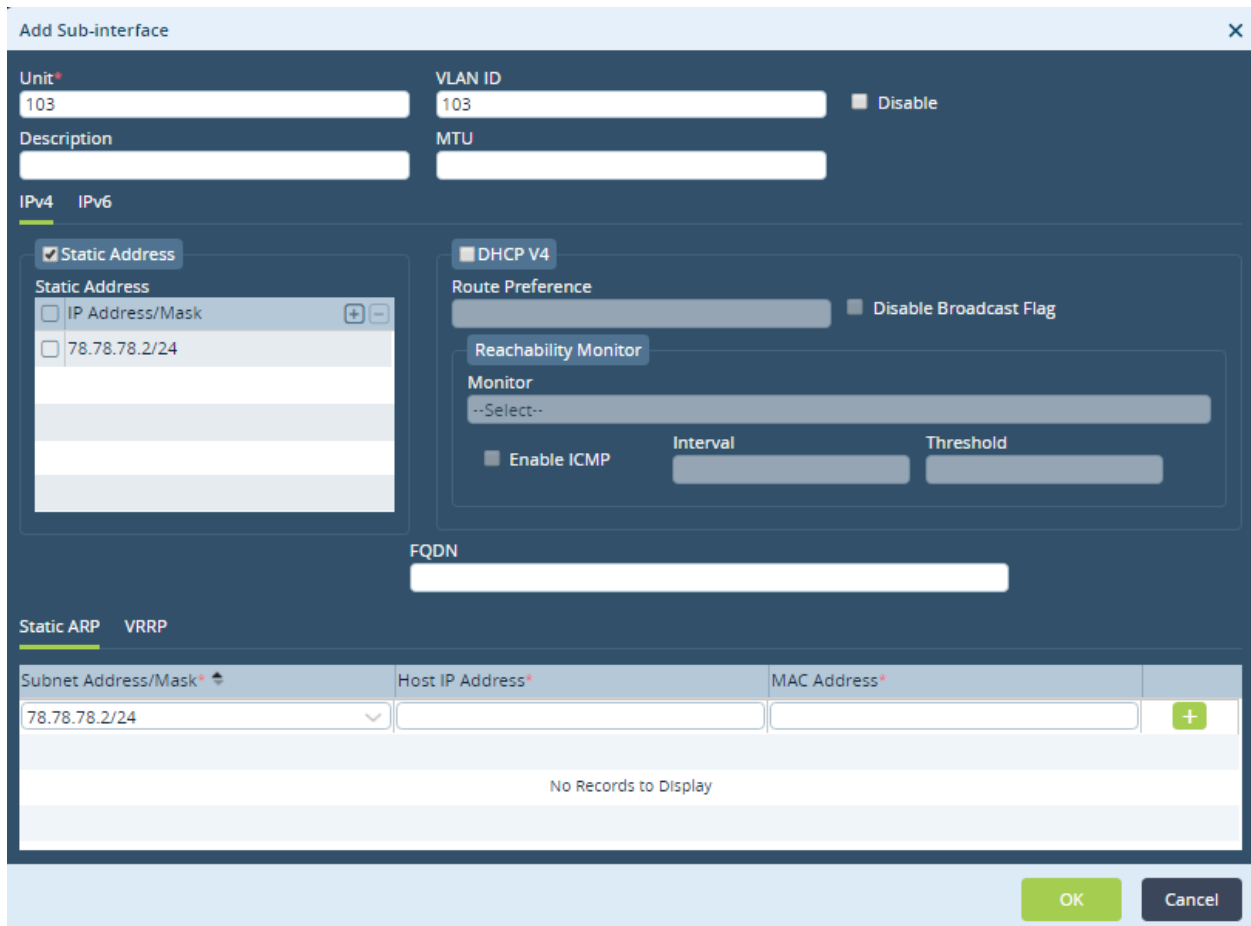
For CGNAT, you configure one or more Ethernet interfaces to route traffic from the customer LAN to the WAN.

To configure an Ethernet interface to route traffic from the customer LAN to the WAN:

1. In the Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the left menu bar.
 - c. Select an organization in the left navigation panel.
 - d. Select a template from 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.
4. Click the  Add icon to configure an interface. For information about configuring the fields, see [Configure Interfaces](#).



- Click Subinterfaces, and then click the  Add icon to add a subinterface.





- Configure a subinterface unit number and a static address. For information about configuring the other fields, see [Configure Interfaces](#).
- Click OK.
- Repeat Steps 1 through 7 to configure another WAN interface, if required.

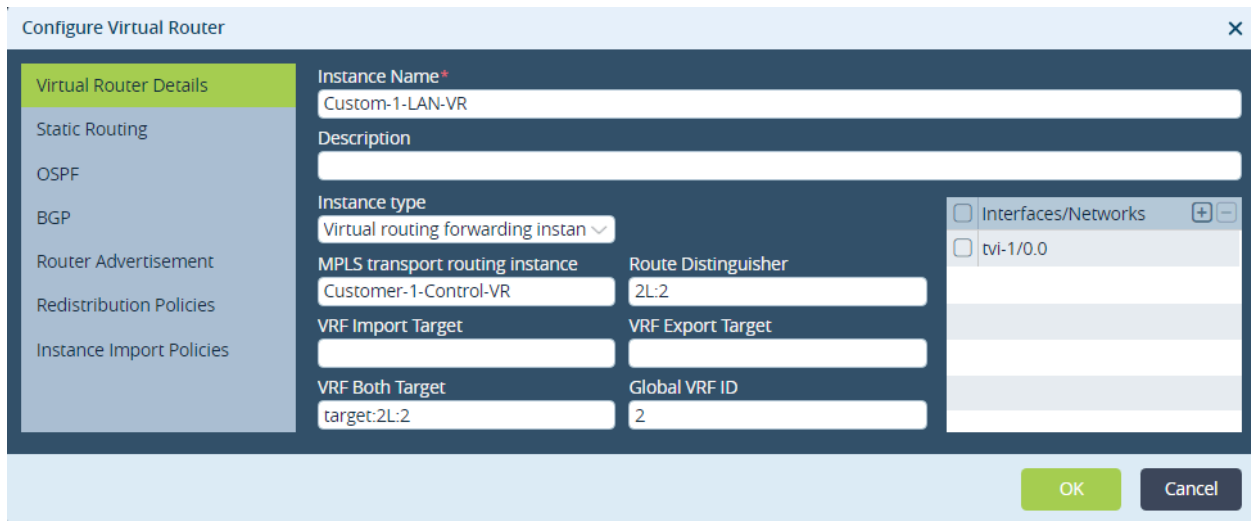
Configure a Customer Virtual Router


A customer virtual router connects to a transport virtual router, which directs traffic to the internet. For more information about configuring virtual routers, see [Configure Virtual Routers](#).

To configure a customer virtual router:

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Templates > Device Templates in the horizontal menu bar.

- c. Select an organization in the left menu bar.
- d. Select a post-staging template 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 Virtual Router Details tab, and enter information for the following fields.



Field	Description
Instance Name	Enter a name for the virtual router.
Instance Type	Select Virtual Routing Forwarding Instance.
MPLS transport routing instance	For MPLS, select the control virtual router to use as the MPLS routing instance.
Route Distinguisher	For MPLS, enter the route distinguisher for this instance.
VRF Both Target	Enter the target community to use when exporting Layer 3 VPN routes and when filtering these when importing them.
Global VRF ID	Enter an ID for the global VRF.
Interfaces/Networks	Select one or more interfaces to assign to the routing instance. Click the  Add icon to add an interface.

6. Select the BGP tab in the left menu bar, and then click the  Add icon. The Add BGP Instance popup window

displays.

Add BGP Instance

General | Advanced | Prefix List | Peer/Group Policy | Peer Group | Policy Options

Description

Instance ID* 1 Router ID* 20.20.22.2 Local AS* 1000 Peer AS

Local Address IP Address Or Interface Hold Time (sec) 90 TTL Password

Local Network Name --Select-- IBGP Preference 200 EBGP Preference 20

☐ Passive ☐ Remove All Private AS# ☐ Route Reflector Client ☐ Enable Alarms

Family

Family*	Loop	Prefix Limit
--Select--		
NO FAMILY ADDED		

OK Cancel

7. In the General tab, enter the required information.
8. Select the Peer Group tab. Click the Add icon and configure two peer groups:
 - One peer group is for traffic coming from the customer virtual router.
 - The second peer is for traffic going towards the transport virtual router.
9. In the Add Peer Group popup window, enter information for the following fields.

Add BGP Instance > Add Peer Group
✕

Name*

Description

Type

IBGP
▼

Peer AS

64512

Local Address

10.1.64.1

Hold Time (sec)

TTL

Password

Local Network Name

--Select--
▼

Local AS

General
Neighbors
Allow
Advanced


1

Family*	Loop	Prefix Limit	
--Select-- ▼	<input type="text"/>	<input type="text"/>	
IPv4 Versa Private			
IPv4 Layer 3 VPN Unicast			

OK

Cancel

Field	Description
Name	Enter a name for the peer group.
Type	Select EBGp.
Peer AS	Enter the peer's AS number.
Local Address	Enter the IP address of the local end of the BGP session.
Hold Time	Enter the hold time to use when negotiating with the peer.
TTL	Enter the time-to-live value, which is the number of hops a packet can travel in a network before the packet expires. <i>Range:</i> 1 through 255 <i>Default:</i> 64 (for EBGp)
Password	Enter the MD5 password used by this peer group.
Local Network Name	Select the network to which the peer group belongs.
General (Tab)	
Family	Select IPv4 Unicast.

10. Select the Neighbors tab, and click the  Add icon. In the Add Neighbor popup window, enter information in the Neighbor IP, Peer AS, and Local Address field. For the local address, enter the address of the paired TVI interface that is used to send traffic directly to the internet.

Add BGP Instance > Add Peer Group

Name*

from_grt_vrf

Description

Type

EBGP

Peer AS

Local Address

IPv4 Address

Hold Time (sec)

TTL

Password

Local Network Name

--Select--

General

Neighbors

Allow

Advanced

+

−

≡

▼

1

<input type="checkbox"/>	Neighbor IP	Peer AS	Local Address	Import	Export
<input type="checkbox"/>	1.1.1.1	12000	1.1.1.2		

OK

Cancel



11. Click OK.

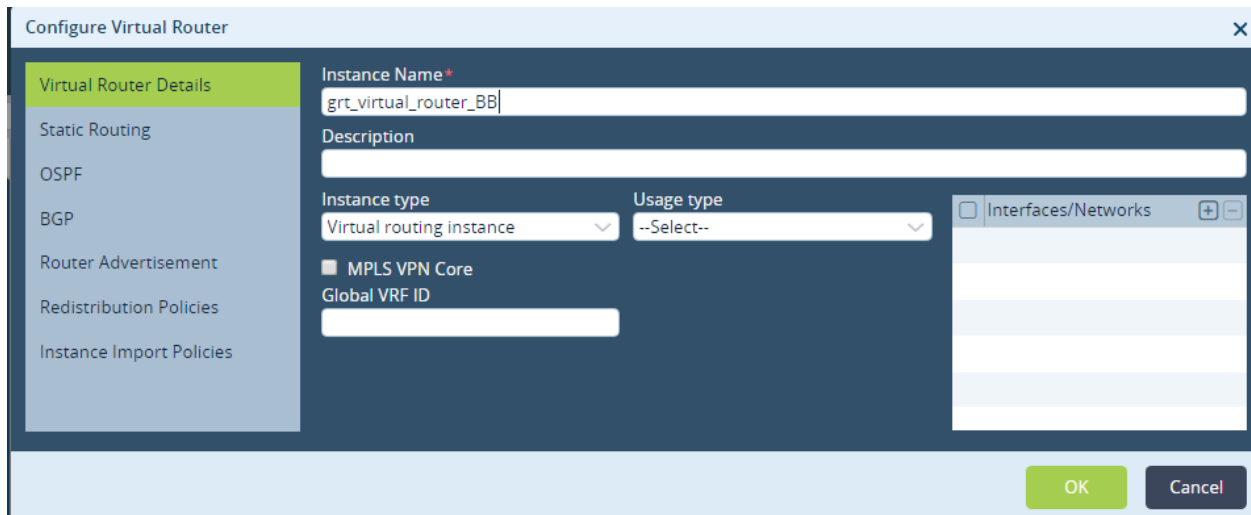
Configure a Transport Virtual Router


A transport virtual router directs traffic that it receives from a customer virtual router to the internet. For more information about configuring virtual routers, see [Configure Virtual Routers](#).


To configure a transport virtual router:

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 post-staging template 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 Virtual Router Details tab, and enter information for the following fields.



Field	Description
Instance Name	Enter a name for the virtual router.
Instance Type	Select Virtual Routing Instance.
Usage Type	Select the virtual router usage type.
MPLS VPN Core	For MPLS, click to configure the virtual router as the core router.
Global VRF ID	Enter an ID for the global VRF.
Interfaces/Networks	Select one or more interfaces to assign to the routing instance. Click the  Add icon to add an interface.

6. Select the BGP tab in the left menu bar, and then click the  Add icon. The Add BGP Instance popup window displays.

Add BGP Instance

General
Advanced
Prefix List
Peer/Group Policy
Peer Group
Policy Options

Description

Instance ID *
Router ID *
Local AS *
Peer AS

1
20.20.22.2
1000

Local Address
Hold Time (sec)
TTL
Password

IPv4 Address
90

Local Network Name
IBGP Preference
EBGP Preference

--Select--
200
20

Passive
Remove All Private AS#
Route Reflector Client


Family
1

Family *
Loop
Prefix Limit




--Select--

NO FAMILY ADDED

OK
Cancel

7. In the General tab, enter the required information.
8. Select the Peer Group tab, and click the  Add icon. In the Add Peer Group popup window, enter information for the following fields.

Field	Description
Name	Enter a name for the peer group.
Type	Select EBGp.
Peer AS	Enter the peer's AS number.
Local Address	Enter the IP address of the local end of the BGP session.
Hold Time	Enter the hold time to use when negotiating with the peer.
TTL	Enter the time-to-live value, which is the number of hops a packet can travel in a network before the packet expires. <i>Range:</i> 1 through 255 <i>Default:</i> 64 (for EBGp)
Password	Enter the MD5 password used by this peer group.
Local Network Name	Name of the local network to which the BGP instance belongs. This field lists the names of user-defined networks.
Local AS	Select the network to which the peer group belongs.

9. Select the Neighbors tab, and click the  Add icon. In the Add Neighbor popup window, enter information in the Neighbor IP, Peer AS, and Local Address field.
10. Select the Redistribution Policies tab in the left menu bar. Click the  Add icon, and in the Add Redistribution Policy popup window, enter a new for the redistribution policy.
11. Click the  Add icon to configure a term in the policy. In the Add Term popup window, enter information for the following fields.

Add Redistribution Policy > Add Term
✕

Term Name*
☐ Disable

Match

Action

Protocol

BGP

Address

IPv4 Or IPv6 Address/Prefix

Next Hop

IPv4 Or IPv6 Address/Prefix

Area

OSPF Tag

Static Tag

Community

Extended Community

IP-SLA Monitors

--Select--

OK

Cancel

Field	Description
Term Name	Enter a name for the term in the redistribution policy. The first instance created is evaluated first by the policy rule, and the remaining terms are evaluated in the order they are listed in the term name table.

12. Select the Match tab to define redistribution policy match conditions. Enter information for the following fields.

Field	Description
Protocol	Select the protocol to match for redistribution: <ul style="list-style-type: none"> ◦ BGP ◦ DHCP ◦ Direct ◦ OSPF ◦ SD-WAN ◦ Static
Address	Enter the IPv4 or IPv6 address of the route to match.
Next Hop	Enter the next-hop address for the route.
Community	For BGP, enter the community identifier.
Extended Community	For BGP, enter the extended community identifier.

13. Select the Action tab to define redistribution policy action conditions. Enter information for the following fields.

Field	Description
Accept/Reject	Select the action to take for the route: Accept—Accept all the traffic for the route. Reject—Rejects all the traffic for the route.
Origin	For BGP, select the source of the BGP route: <ul style="list-style-type: none"> Local EGP Remote IGP Unknown heritage
Next Hop	Enter the IP address of the next hop.
Community	For BGP, enter the community identifier to add to the route.
Extended Community	For BGP, enter the extended community identifier to add to the route.
Metric	Enter a metric value to add to the route.
Metric Conversion	Select the action on the metric value: <ul style="list-style-type: none"> Add IGP Set value Subtract

14. Click OK.
15. Repeat the Steps 11 through 14 to configure redistribution policy terms for the static and DHCP protocols.

Add Redistribution Policy

Name*

p1

Terms

+
-
|||
▼
1


<input type="checkbox"/>	Term Name	Match			
		Protocol	Address	Area	Community
<input type="checkbox"/>	t1	static			
<input type="checkbox"/>	t2	direct			
<input type="checkbox"/>	t3	dhcp			

OK
Cancel

Configure CGNAT Address Pool and Rules

You configure a CGNAT address pool and you define rules to translate the network addresses of the direct to Internet traffic. For more information about configuring CGNAT, see [Configure CGNAT](#).

To configure CGNAT address pools and rules:

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Templates > Device Templates in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a template in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Services  > CGNAT in the left menu bar. The main pane displays the CGNAT pools that are already configured.
- Click the Add icon to add a pool. The Add CGNAT Pool popup window displays.
- Select the General tab, and enter information for the following fields.

Add CGNAT Pool

General
IP Address
Port

Name*
Cust1_NAPT_Pool

Description

Tags

Timeout

ICMP (sec)
60
TCP (sec)
7440
UDP (sec)
300

OK
Cancel

Field	Description
Name	Enter a name for the pool. In this example, the pool name is Cust1_NAPT_Pool.
Timeout (Group of Fields)	
<ul style="list-style-type: none"> ICMP 	Enter the ICMP mapping timeout, in seconds. <i>Range:</i> 30 through 3600 seconds
<ul style="list-style-type: none"> TCP 	Enter the TCP mapping timeout, in seconds. <i>Range:</i> 240 through 10800 seconds
<ul style="list-style-type: none"> UDP 	Enter the UDP mapping timeout, in seconds. <i>Range:</i> 1 through 3600 seconds

6. Select the IP Address tab, and enter information for the following fields.

Field	Description
IP Address/Range	Click to use IP addresses, and enter IP addresses in the IP Address/Mask table.
Egress Network	Click to use egress networks, and enter egress networks in the Egress Network table.
Egress Interface	Click to use egress interfaces, and enter egress interfaces in the Egress Interface table.
Address Allocation Scheme	Select the scheme to use to allocate one port from each address in a range.
Routing Instance	Select the routing instance to use. After traffic is NATed, it is directed to this routing instance.
Provider Organization	Select the provider organization to which the CGNAT pool belongs. After traffic is NATed, it is directed to this provider organization.

7. Select the Port tab to configure NAPT, and enter information for the following fields.

Add CGNAT Pool

General

IP Address

Port

☐ Destination port

Low Port

High Port

☒ Source Port

Allocation Scheme

Automatic ports assignment

Low Port

High Port

☐ Allocate IP/port randomly

☐ Preserve source port range

☐ Preserve source port parity

☐ Port block allocation

Block Timeout

Block Size

Max Block per user

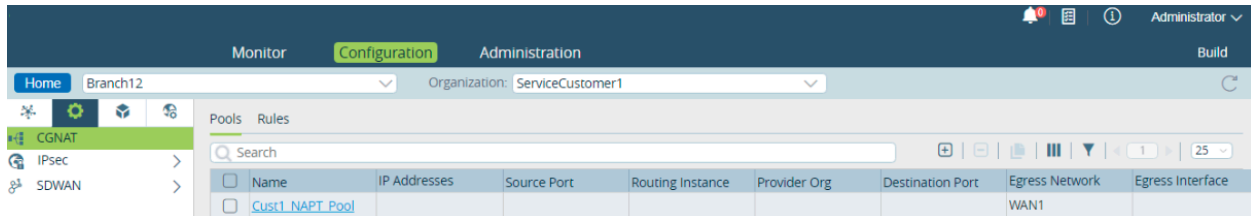
OK


Cancel

Field	Description
Destination Port (Group of Fields)	Click to configure the NAT destination port.
◦ Low Port	Enter the lowest port number in the range.
◦ High Port	Enter the highest port number in the range.
Source Port	Select to configure the NAT source port.
Allocation Scheme (Group of Fields)	Scheme to be used for source port allocation: <ul style="list-style-type: none"> ◦ Allocate Ports from Range ◦ Automatic Port Assignment
◦ Low Port	When the allocation scheme is to allocate ports from a range, enter the lowest port number of the range.
◦ High Port	When the allocation scheme is to allocate ports from a range, enter the highest port number of the range.
Allocate IP/Port Randomly	Select to allocate the IP addresses or port numbers randomly.
Port Block Allocation	Select to allocate the port numbers in blocks.
Block Timeout	When you select Port Block Allocation, enter how long to wait to receive a port number before breaking the connection. <i>Range:</i> 120 through 3600 seconds
Block Size	When you select Port Block Allocation, enter the size of the port block. The size must be divisible by 2. <i>Range:</i> 8 through 512 <i>Default:</i> 128
Maximum Block per User	When you select Port Block Allocation, enter the maximum block size to allocate per user. <i>Range:</i> 1 through 16

	<i>Default: 4</i>
--	-------------------

8. Click OK. The main pane displays the NAT pool that you just configured.



9. To define the rules to use for address translation, select the Rules tab in the horizontal menu bar.
10. Click the  Add icon. In the Add CGNAT Rule popup window, select the General tab and enter information for the following fields.

Field	Description
Name	Enter a name for the CGNAT rule.
Precedence	<p>Enter a value for the priority of the rule. You can configure multiple rules and assign each a priority. A rule or rules with a higher priority value take precedence over rules with a lower priority value.</p> <p><i>Range: 0 through 255</i> <i>Default: 1</i></p>

11. Select the Match tab to configure the criteria to select traffic for translation. For information about the fields, see [Configure CGNAT Rules](#).

Add CGNAT Rule

General Match Action

Source

Source Zones IP Address/Mask

Destination

Destination Zones IP Address/Mask

Routing Instance

Low Port High Port

IP Address Range

Range Name Low* High*

NO ADDRESS RANGE CONFIGURED

Protocol

OK Cancel

- Select the Action tab to define the action to take on the traffic that meets the matching criteria. Enter information for the following fields.

Add CGNAT Rule

General Match Action

☐ Disable Translation

NAT Mode*

Source Pool*

Destination Pool

LEF Profile

☐ Endpoint Independent Mapping

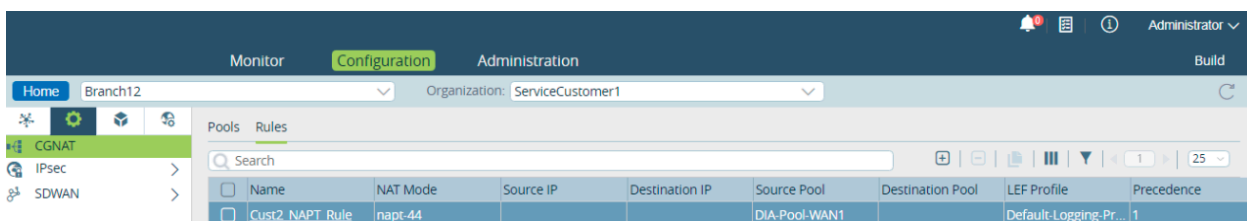
☐ Endpoint Independent Filter

☐ Address Pooling Paired

OK Cancel

Field	Description
Disable Translation	Click to disable address translation.
NAT Mode	Select napt-44 to translate the transport identifier of the IPv4 private network to a single IPv4 external address.
Source Pool	Source pool to associate with the translation mode. In this example, select Cust1_NAPT_POOL, which is the pool you created in Step 5.
Destination Pool	Select the destination pool to associate with the translation mode.
LEF Profile	Select the log export functionality profile to use for logging.
Endpoint-Independent Mapping	Click to enable endpoint-independent mapping, which NAT uses to perform translation for the duration of the session.
Endpoint-Independent Filter	Click to enable endpoint-independent filtering. Endpoint-independent filtering checks only the destination IP address and destination port of an inbound packet sent by an external endpoint when deciding whether to pass the packet.
Address Pooling Paired	Click to enable paired address pooling. Use this option for applications that require that all sessions associated with a single internal IP address to be mapped to the same external IP address for the duration of a session.

13. Click OK. The main pane displays the CGNAT rule that you just configured.



Configure a Tunnel for DIA

To enable DIA, the VOS software leverages the split tunnel mechanism, which allows a branch to use the same or multiple internet links for both internet and VPN traffic. Split tunnels allow a branch to simultaneously access dissimilar security domains such as a public network (for example, internet) and a local LAN or WAN, using the same or different


https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

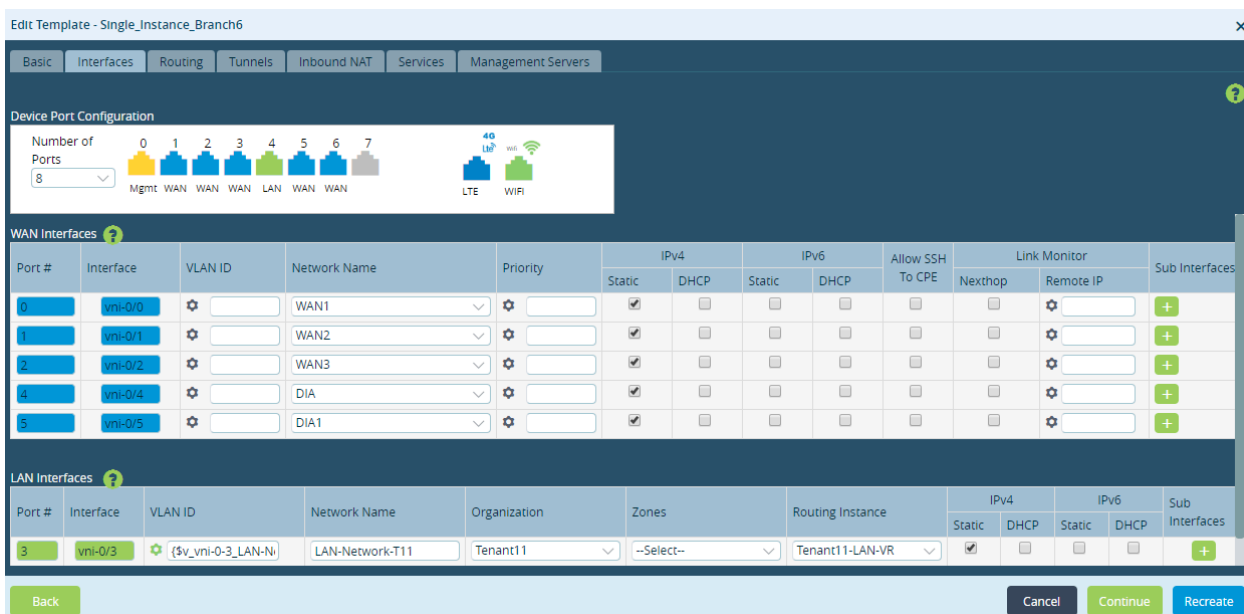
Updated: Wed, 23 Oct 2024 08:10:23 GMT

Copyright © 2024, Versa Networks, Inc.

network connections.

To configure a tunnel for DIA:

1. In Director view, select the Workflows tab in the top menu bar.
2. Select Template > Templates in the left menu bar.
3. Click the  Add icon to create a new template or click the name of an existing template to modify it. The Create Template or Edit Template popup window displays. For complete information about creating templates, see [Create and Manage Post-Staging Templates](#).
4. Select the Interfaces tab.
5. In the Device Port Configuration group of fields, click each port icon and select WAN as the type of interface. Then in the WAN Interfaces table, configure each WAN interface.



Device Port Configuration






Number of Ports: 8

0 1 2 3 4 5 6 7


Mgmt WAN WAN WAN LAN WAN WAN

4G LTE WiFi

WAN Interfaces

Port #	Interface	VLAN ID	Network Name	Priority	IPv4		IPv6		Allow SSH To CPE	Link Monitor		Sub Interfaces
					Static	DHCP	Static	DHCP		Nexthop	Remote IP	
0	vni-0/0		WAN1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
1	vni-0/1		WAN2		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2	vni-0/2		WAN3		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4	vni-0/4		DIA		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5	vni-0/5		DIA1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

LAN Interfaces

Port #	Interface	VLAN ID	Network Name	Organization	Zones	Routing Instance	IPv4		IPv6		Sub Interfaces
							Static	DHCP	Static	DHCP	
3	vni-0/3	{\$v_vni-0-3_LAN-N}	LAN-Network-T11	Tenant11	--Select--	Tenant11-LAN-VR	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Back Cancel Continue Recreate

6. Select the Tunnels tab to create a split tunnel. Select the name of the VRF and the WAN interface, and click DIA. as shown below. Then click Recreate.

Edit Template - Single_Instance_Branch6

Basic Interfaces Routing Tunnels Inbound NAT Services Management Servers

Split Tunnels ?

VRF Names	WAN Interfaces	DIA	Gateway	
Tenant11-LAN-VR	DIA	<input checked="" type="checkbox"/>		+
Tenant12-LAN-VR	DIA1	<input type="checkbox"/>		+

Load Balance

Site to Site Tunnels

Name	Peer Type	WAN/LAN Network	LAN VRF	Vpn Profile	BGP Enabled	
	--Select--	--Select--	--Select--	--Select--	<input type="checkbox"/>	+

No Records to Display

Back Cancel Continue Recreate

- Click Recreate.
- The Diff and Merge window displays. Click Deploy.

Diff and Merge

Active Template

Current (Read-Only)

```

49 {
50 }
51 vni "vni-0/0" {

```

Newly Generated (Editable)

```

49 {
50 }
51 tvi "tvi-0/602" {
52   description "WAN side Split Tunnel interface between DIA1 and Tenant12-LAN-VR";
53   enable "true";
54   paired-interface "tvi-0/603";
55   type "paired";
56   unit "0" {
57     enable "true";
58     family {
59       inet {
60         address "169.254.0.2/31" ;
61       }
62     }
63   }
64 }
65 tvi "tvi-0/603" {
66   description "LAN side Split Tunnel interface between DIA1 and Tenant12-LAN-VR";
67   enable "true";
68   paired-interface "tvi-0/602";
69   type "paired";
70   unit "0" {
71     enable "true";
72     family {
73       inet {
74         address "169.254.0.3/31" ;
75       }
76     }
77   }
78 }

```

Deploy Cancel

- In the main Templates window, select the template you deployed and click Commit Template.

Monitor Configuration Workflows Administration Analytics Commit Template

Organization: provider-org

Infrastructure >

Template >

Templates

Name	Status	Last Modified Time	Last Modified By
Branch-5-hub-template	Saved	Wed, May 13 2020, 11:49	Administrator
Multi_Tenant_PostStaging	Deployed	Tue, Jul 23 2019, 14:22	Administrator
Multi_Tenant_PostStaging_Branch5	Deployed	Tue, Jul 23 2019, 15:20	Administrator
Single_Instance_Branch6	Deployed	Wed, May 13 2020, 11:58	Administrator
Staging	Deployed	Tue, Jul 23 2019, 14:23	Administrator

- Click OK in the Commit popup window to commit the updated template.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:10:23 GMT

Copyright © 2024, Versa Networks, Inc.

Commit

Organization*
provider-org

Template Service Template

Select Template*
Single_Instance_Branch6

Reboot

Auto Merge
Overwrite

Device Groups

	Devices	Device Type	Template State	Appliance State	Device Modified	Differences	Association
Single_Instance	<input checked="" type="checkbox"/>						
	<input checked="" type="checkbox"/>	SDWAN-Branch6	Branch	OUT_OF_SYNC	IN_SYNC		

OK Cancel

To verify the DIA tunnel configuration:

- Issue the **show interface brief** CLI command to view details about the interfaces. The output shows that the split tunnel has been created.
- Issue the **show bgp neighbor** brief CLI command to check whether the BGP session has been established over the split tunnel to advertise the default route in the LAN routing instance. This route is used to forward the internet traffic directly, bypassing the hub device.
- Issue the **show routing-instance** *DIA-routing-instance-name* CLI command to verify that the static route has been created in the DIA routing instance and has been redistributed in BGP.
- Issue the **show routing-instance** *LAN-routing-instance-name* CLI command to verify that the default route received in the LAN routing instance has the next-hop TVI IP address on the DIA routing instance.

Configure Policy for DIA

The steps in the previous two sections, for configuring CGNAT and DIA tunnels, help achieve routing based DIA. That is, internet traffic follows the default route for local breakout. However, when a branch has more than one internet circuit, or if you want to perform selective local breakout (that is, to have only certain applications use DIA and have all others follow the default route to a central breakout location), you must configure policy-based internet access.

You can use the following types of policies when you configure DIA:

- Policy-based forwarding (PBF) policy—You use PBF policy to evaluate traffic that matches a non-SD-WAN in the routing instance. The routes can be static, connected, OSPF, EBGp, or RTI. You can use PBF with a next hop when you enable local DIA for the branch and the default route on the LAN virtual router (VR) points to the transport

VR.

- SD-WAN policy—You use SD-WAN policy to evaluate traffic that matches an SD-WAN (Layer 3 VPN) learned route. You can use SD-WAN policy with a next hop for remote DIA, where the default and preferred routes are learned from the SD-WAN.
- Application-based policy-based routing (PBR)—In application-based PBR, initial sessions choose the next hop based on the routing table, not based on the PBF or SD-WAN next hop. The session must succeed in order to build the application cache for the first time. It may take a few sessions to fully populate the application cache, because some applications can map to different IP addresses in a region. When a new session matches the application cache table, it is forwarded based on the next hop configured in the PBF or SD-WAN policy. This means that it is important that the initial session succeed based on default routing.

When you configure policy for DIA, note the following:

- For application-based DIA to function correctly, you must modify the CGNAT rule in the default CGNAT configuration so that it matches the source zone on the WAN side of the split tunnel instead of matching the destination zone on the LAN side. For Releases 21.1.1 and later, you can use the default CGNAT configuration to match traffic going towards the DIA split tunnels and then configure PBF or SD-WAN rules as appropriate.
- In SD-WAN-based or a PBF-based DIA, the IP address that you configure for the next hop in the rule must be the IP address on the WAN side of the split tunnel. Also, you must not specify the routing instance.
- For application-based DIA, you must always include a source zone-based match condition in the SD-WAN or PBF rule to match only the traffic that originates from the LAN zone. If you do not, the same PBF or SD-WAN rule matches the second session created in the transport VR. Typically, the match source zone should be an Intf-LAN zone.

The remainder of this section discusses three use cases that illustrate how to configure policy for DIA:

- Configure link preference for DIA using PBF policy.
- Route traffic via local DIA using SD-WAN policy.
- Route specific traffic via a hub and route rest of the traffic via local DIA.

Use Case: Link Preference for DIA using PBF

This use case shows how traffic can be forwarded over two different internet links based on application or URL. You could use this when you have two WAN links, one that is a high-bandwidth link and the second that is a low-bandwidth link and you want to send business traffic over the high-bandwidth link and non-business traffic over the low-bandwidth link. Because the default route is not SD-WAN-based, you can use PBF to split the traffic.

Before you can configure the PBF policy, you must do the following:

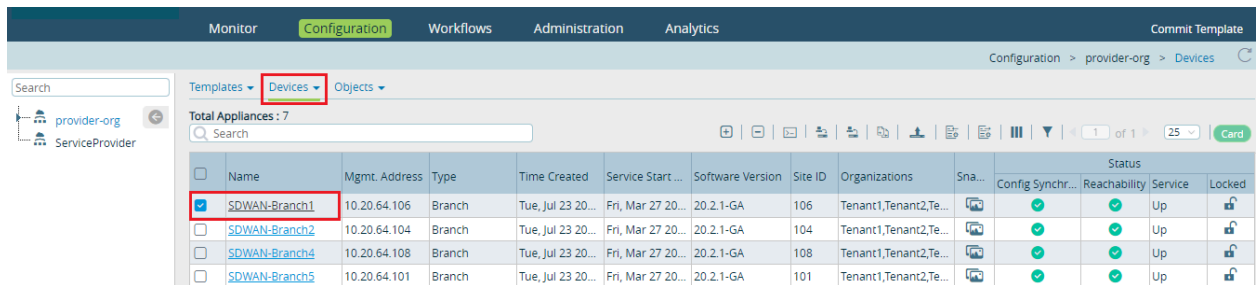
- Deploy all headend components.
- Configure all internet traffic to break out locally.
- Ensure that there are two interfaces with DIA; that is, internet must be accessible over both links.

In this example, the interfaces that are used for local internet breakout are named DIA and DIA-1, and traffic is split between the two interfaces. Traffic to Yahoo is forwarded over the DIA-1 internet link, and all other traffic is forwarded over the DIA internet link.


After you complete the configuration, two default routes are received from BGP in the LAN VR. Also, default route is active based on the local preference, and all the traffic is send over that internet breakout.

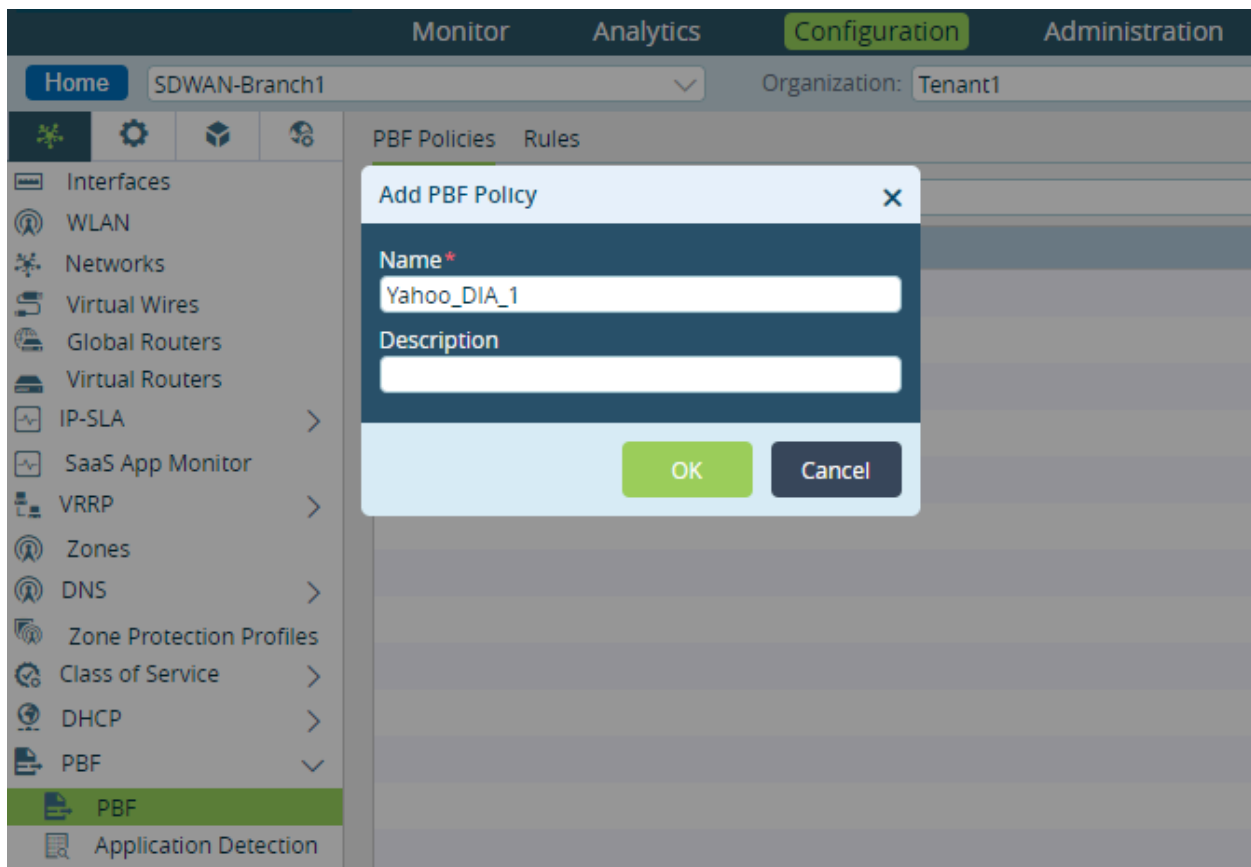
To configure PBF to split traffic:

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 the branch on which you want to configure DIA using PBF. The view changes to Appliance view.




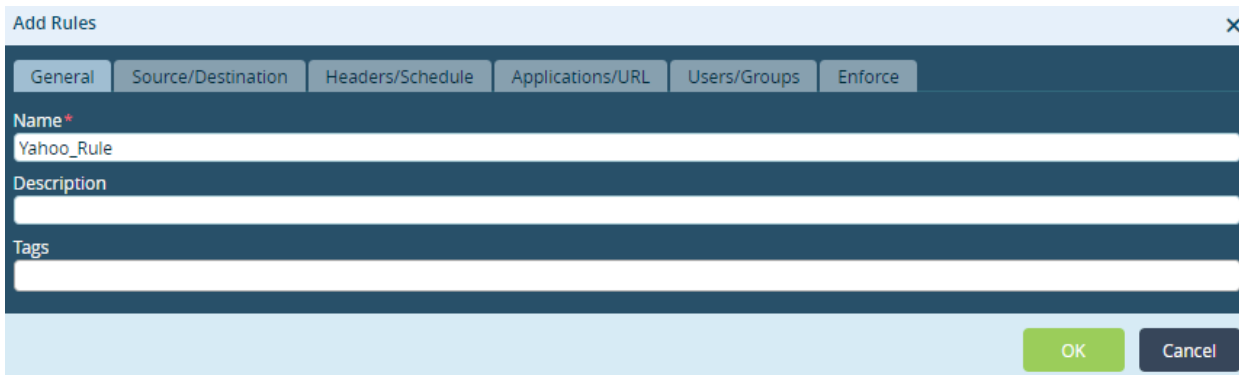
Name	Mgmt. Address	Type	Time Created	Service Start ...	Software Version	Site ID	Organizations	Sna...	Config Synchr...	Reachability	Service	Locked
<input checked="" type="checkbox"/> SDWAN-Branch1	10.20.64.106	Branch	Tue, Jul 23 20...	Fri, Mar 27 20...	20.2.1-GA	106	Tenant1,Tenant2,Te...				Up	
<input type="checkbox"/> SDWAN-Branch2	10.20.64.104	Branch	Tue, Jul 23 20...	Fri, Mar 27 20...	20.2.1-GA	104	Tenant1,Tenant2,Te...				Up	
<input type="checkbox"/> SDWAN-Branch4	10.20.64.108	Branch	Tue, Jul 23 20...	Fri, Mar 27 20...	20.2.1-GA	108	Tenant1,Tenant2,Te...				Up	
<input type="checkbox"/> SDWAN-Branch5	10.20.64.101	Branch	Tue, Jul 23 20...	Fri, Mar 27 20...	20.2.1-GA	101	Tenant1,Tenant2,Te...				Up	

2. Select Networking  > PBF > PBF in the left menu bar, and add a PBF policy. For more information, see [Configure Policy-Based Forwarding](#). In our example, the name of the policy is Yahoo_DIA_1.



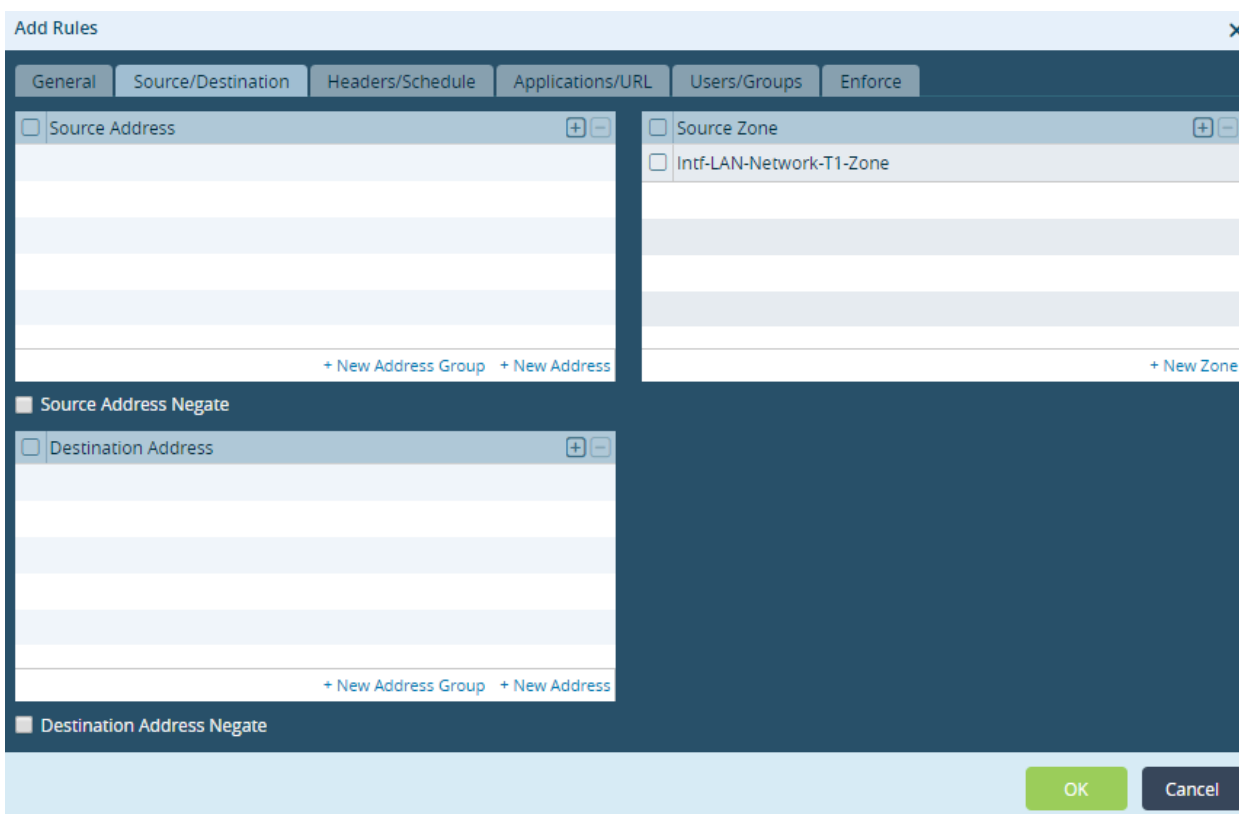
3. Select the Rules tab and create a rule for the traffic to Yahoo.

- a. Click the  Add icon. The Add Rules popup window displays.
- b. Select the General tab, and enter a name for the rule. In the example here, the name is Yahoo_Rule.



The screenshot shows the 'Add Rules' popup window with the 'General' tab selected. The 'Name' field contains 'Yahoo_Rule'. The 'Description' and 'Tags' fields are empty. The 'OK' and 'Cancel' buttons are at the bottom right.

- c. Select the Source/Destination tab, and then in the Source Address table, select the LAN VR that is the source of incoming traffic.



The screenshot shows the 'Add Rules' popup window with the 'Source/Destination' tab selected. The 'Source Address' table is empty. The 'Source Zone' table contains one entry: 'Intf-LAN-Network-T1-Zone'. The 'Destination Address' table is empty. The 'Destination Address Negate' section is collapsed. The 'OK' and 'Cancel' buttons are at the bottom right.


- d. Select the Applications/URL table, and then in the Application List table, select YAHOO.

The 'Add Rules' dialog box is shown with the 'Applications/URL' tab selected. It features two main sections: 'Applications' and 'URL Categories'. The 'Applications' section has a list with 'Application List' and 'YAHOO'. The 'URL Categories' section has a list with 'URL Category List'. Both sections have expand/collapse icons. At the bottom of each list are buttons for '+ New Group' and '+ New Application' (for Applications) or '+ New URL Category' (for URL Categories). The dialog has 'OK' and 'Cancel' buttons at the bottom right.

- e. Select the Enforce tab. In the Next-Hop IP Address field, enter the next hop IP address for the DIA_1 transport VR. For Releases 20.2 and later, you can specify multiple next hops in a single rule, and you can specify their priority order or that their priority be equal. So, instead of specifying the IP address of the paired TVI interface, you configure a next hop by specifying the interface type as WAN Networks. For more information, see [Configure SD-WAN Traffic-Steering Forwarding Profiles](#).

The 'Add Rules' dialog box is shown with the 'Enforce' tab selected. It has two main sections: 'Forwarding' and 'Monitor'. The 'Forwarding' section includes fields for 'Action' (set to 'Allow Flow'), 'Next Hop IP Address' (set to '169.254.0.4'), and 'Routing Instance' (set to '--Select--'). There are also checkboxes for 'Enable Symmetric Forwarding of Return Traffic' and 'Enable Symmetric L2 Forwarding of Return Traffic'. The 'Monitor' section includes fields for 'Address' (empty), 'Routing Instance' (set to '--Select--'), 'Action' (set to 'wait-recover'), 'Interval(sec)' (set to '3'), and 'Threshold(Events)' (set to '5'). The dialog has 'OK' and 'Cancel' buttons at the bottom right.

- e. Click OK.

4. Select Services  > CGNAT to configure CGNAT pools for the DIA and DIA1 transport VR. By default, the CGNAT rule is applied based on the LAN VRs and performs NAT on all internet-bound traffic with the DIA interface IP address as the egress. This traffic is forwarded based on the configured NAT rule and the egress or NAT interface. For more information, see [Configure CGNAT Rules](#).

Monitor

Analytics

Configuration

Administration

Home

SDWAN-Branch2

Organization: Tenant1

Build

CGNAT

Next Gen Firewall

IPsec

SDWAN

Web Proxy

Pools

Rules

Search

<input type="checkbox"/>	Name	IP Addresses	Source Port	Routing Instance	Provider Org	Destination Port	Egress Network	Egress Interface
<input type="checkbox"/>	DIA-Pool-DIA	10.10.10.10 - 10.10.10.10		DIA-Transport-VR			DIA	
<input type="checkbox"/>	DIA-Pool-DIA1	172.17.33.10 - 172.17.33.10		DIA1-Transport-VR			DIA-1	

- Select and Rules tab, and then in the Edit CGNAT Rule popup window, select the Match tab.
- Delete the zone selected in the Destination Zones table. Then, in the Source Zones table, add the WAN VR and select the appropriate routing instance. Note that the paired IP address is in the WAN of the split tunnel. It is important to modify the CGNAT rule, because if a packet is evaluated with the default configuration, the CGNAT rule is applied first and the PBF next hop does not take place. The CGNAT rule, as shown below, must match based on the source zone (here, W-ST-Tenant1-LAN-VR-WAN1) and not the destination zone. CGNAT and PBR do not function simultaneously in the same working session and must be split. Here, the CGNAT rule is modified so that it is applied to the DIA VR (WAN side), not on the LAN side. Doing this creates two sessions, one each in LAN-VR and DIA-VR. After these modifications to the CGNAT rule, the traffic is evaluated against the PBF in the LAN-VR and matching traffic is forwarded based on the action configured for the PBF rule.

Edit CGNAT Rule - DIA-Rule-Tenant1-LAN-VR-WAN1

General
Match
Action

Source

Source Zones

☐ Source Zones
☐ W-ST-Tenant1-LAN-VR-WAN1

IP Address/Mask

☐ IP Address/Mask

Routing Instance

DIA-1-Transport-VR

IP Address Range

Range Name
Low
High

NO ADDRESS RANGE CONFIGURED

Destination

Destination Zones

☒ L-ST-Tenant1-LAN-VR-WAN1

IP Address/Mask

☐ IP Address/Mask

Destination Interface
Destination Network

--Select--
--Select--

Low Port
High Port

IP Address Range

Range Name
Low
High

NO ADDRESS RANGE CONFIGURED

Protocol

OK
Cancel

- Click OK.

To verify the DIA configuration:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:10:23 GMT

Copyright © 2024, Versa Networks, Inc.

- Issue the **show configuration | display set | match pbf** CLI command to verify the PBF policy.
- Issue the **show orgs org-services organization-name pbf policy policy-name rules statistics** CLI command to verify that Yahoo traffic from the LAN side has started. You can also check the session details to verify whether the LAN-side traffic is being routed based on the PBF policy settings. The NAT rule is evaluated on WAN side.

Use Case: Route Application Traffic via Local Internet for Remote Breakout


This use case shows how, in LAN VR, the default route is learned over SD-WAN and is preferred over the local DIA default route. You could use this type of configuration to route some traffic using local DIA and to apply SD-WAN policy to steer the traffic to local DIA. In this example, SD-WAN policy is used to route SD-WAN traffic and PBF is used to route non-SD-WAN traffic.

Before you can configure the SD-WAN policy, you must do the following:

- Deploy all headend components.
- Enable internet traffic breakout on branch.
- Enable internet traffic breakout on the hub with a gateway enabled so that the default route can be sent to all other branches.
- Configure two default routes in the LAN VR, of which the default route from hub is preferred over local DIA so that all traffic to the hub goes over SD-WAN. To verify this configuration, issue the **show route routing-instance routing-instance name** CLI command.

The example here shows how to configure an SD-WAN policy to route traffic to Yahoo locally and to route other traffic to a hub over SD-WAN. You may have to modify the default CGNAT rule so that NAT is performed on the Transport VR and remote DIA is performed for the rest of the traffic. For more information, see Step 2 in the [Use Case: Route Application Traffic via Hub or Remote Branch for Local Breakout](#) section.

To add an SD-WAN rule to route traffic to Yahoo:

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  > SD-WAN > Policies in the left menu bar, and select the Rules tab.
4. In the General tab, enter a name for the rule. In the example here, the name is Yahoo_Local.

Add Rules [X]

General Source/Destination Headers/Schedule Applications URL Users/Groups Forwarding Class Enforce

Name*
Yahoo_Rule

Description

OK Cancel

5. Select the Source/Destination tab, and in the Source Zone table, add a LAN-VR for traffic from the LAN.

Add Rules [X]

General **Source/Destination** Headers/Schedule Applications URL Users/Groups Forwarding Class Enforce

☐ Source Address [+] [-]

☐ Source Zone [+] [-]
☐ Intf-LAN-Network-T1-Zone

+ New Address Group + New Address + New Zone

☒ Source Address Negate

☐ Destination Address [+] [-]

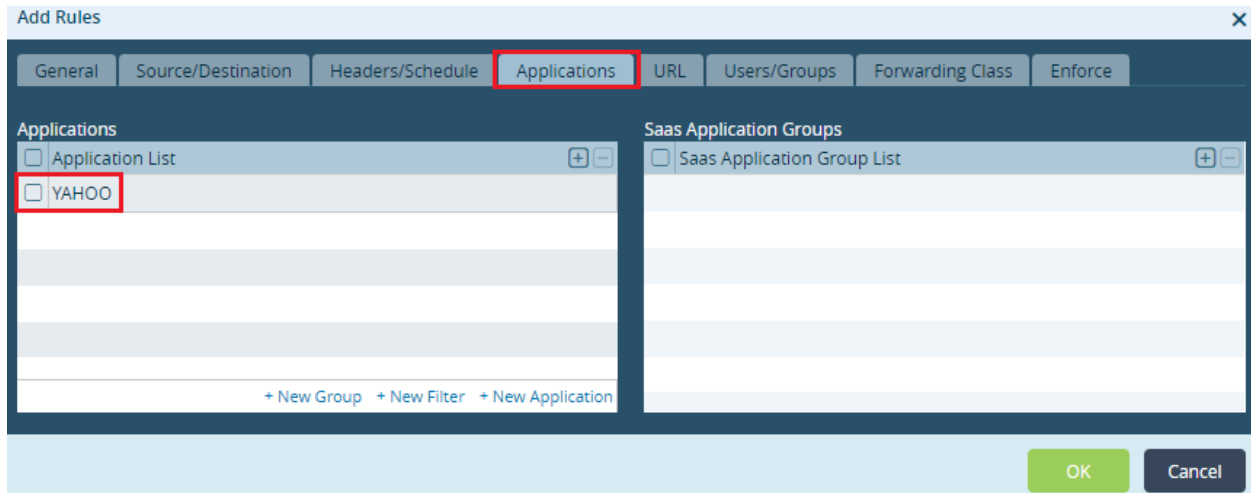
Source Site
☐ Source Site Name [+] [-]

Destination Site
☐ Destination Site Name [+] [-]

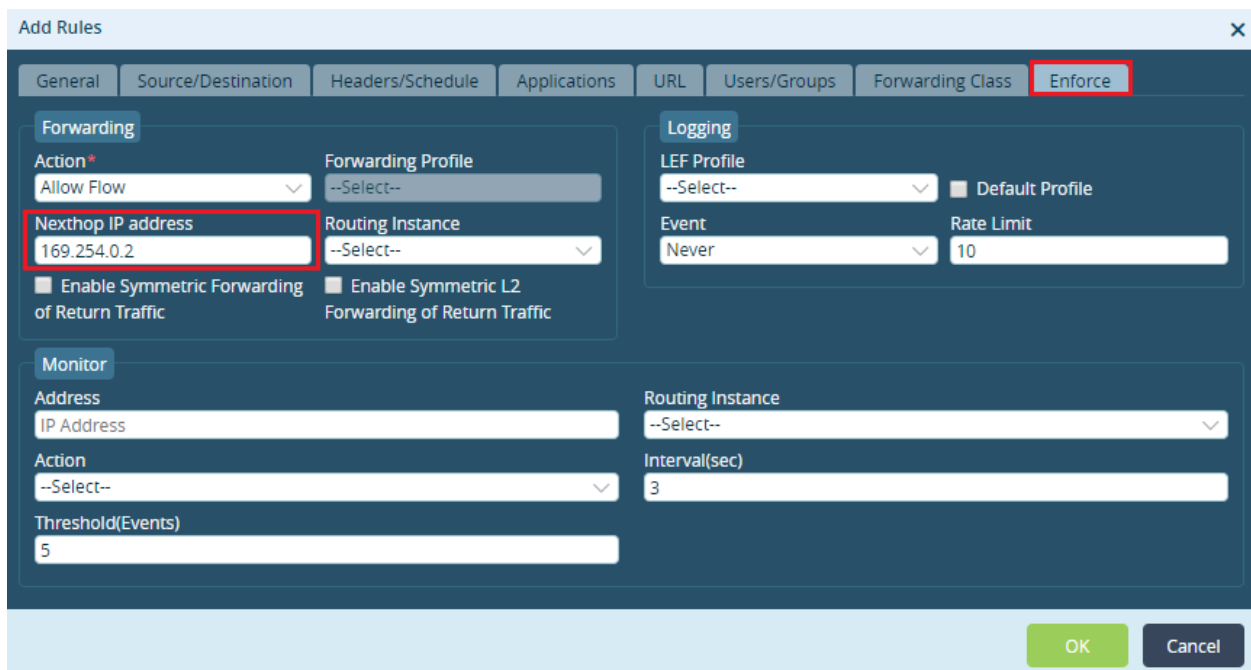
☒ Destination Address Negate

OK Cancel

6. Select the Applications/URL tab, and in the Applications table, select YAHOO from the Application List.



7. Select the Enforce tab, and in the Next-Hop IP Address field, enter the IP address of the next hop, to route traffic towards the TVI IP address of the DIA transport VR. Note that when you specify the next-hop IP address, do not also specify the routing instance. If you specify the routing instance, the route lookup for the next-hop IP address is performed in that routing instance.



8. Click OK.

For more information about SD-WAN policy and rules, see [Configure SD-WAN Policy](#).

To verify the DIA configuration:

- Issue the **show orgs org organization-name brief | select application application-name** CLI command to verify whether, in the first session, traffic to the application is routed over the-WAN to identify the application.

- Issue the **show orgs org service *organization-name* sd-wan policies Default-Policy rules statistics brief** CLI command to view statistics for how much traffic matches the SD-WAN rule. Traffic is routed over the local DIA starting with the second session.



Use Case: Route Application Traffic via Hub or Remote Branch for Local Breakout

This use case describes how to route specific traffic via the hub and the rest of the traffic via the local DIA. This example shows how traffic to the Yahoo application goes to the hub first and is then forwarded to the internet, whereas all other traffic is routed locally.

Before you can configure this case, you must do the following:

- Deploy all headend components.
- Enable internet traffic breakout on the hub with a gateway enabled so that the default route can be sent to all other branches.

The example here shows how to split the traffic to Yahoo using the DIA-1 internet link and rest of the the traffic using the DIA internet link.

1. Configure an SD-WAN traffic-steering forwarding profile. For more information, see [Configure SD-WAN Traffic-Steering Forwarding Profiles](#).
 - a. In Director view, select the Configuration tab from 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 from the main pane. The view changes to Appliance view.
 - e. Select the Configuration tab.
 - f. Select Services  > SD-WAN > Forwarding Profiles in the left menu bar.
 - g. Click the  Add icon. The Add Forwarding Profile popup window displays.
 - h. In the General tab, enter a name for the SD-WAN forwarding profile. In the example here, the name of the forwarding profile is Yahoo_Forwarding_Profile.

Add Forwarding Profile ✕

General Circuit Priorities Avoid Connections FEC Advanced Settings Next Hop

Name *
Yahoo_Forwarding_Profile

Description

Tags

SLA profile --Select-- Encryption Optional Connection Selection Method Weighted Round Robin

+ SLA Profile

Recompute Timer (sec) 300 Path Reconsider Interval (sec) SLA Violation Action Forward Load Balancing Option --Select--

Replication

☐ Enable Replication factor Start When Always

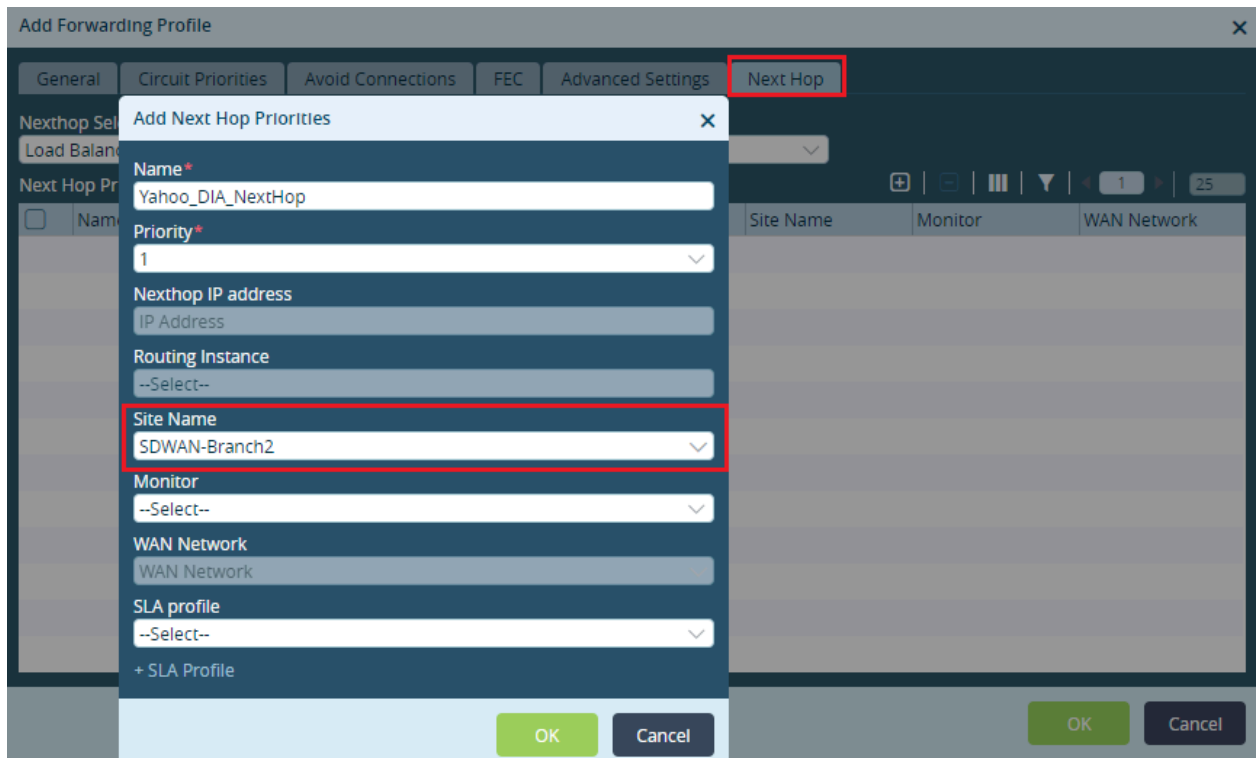
☐ Stop When Circuit Utilization


☒ Evaluate Continuously ☐ Reorder ☐ TURN Redirection ☒ Enable Symmetric Forwarding

OK Cancel

i. Select the Next Hop tab.

j. Click the  Add icon. The Add Next-Hop Priorities popup window displays.



- k. In the Name field, enter a name for the next-hop priority. Here, the name is Yahoo_DIA_NextHop.
 - l. In the Site Name field, select a site.
 - m. Click OK.
 - n. Click OK to add the SD-WAN forwarding profile.
2. Create an SD-WAN rule for traffic to Yahoo, and then associate the forwarding profile with the rule. Note that this configuration is applicable for Releases 20.2 and later. For Release 16.1R2, you can import the default route from the hub and then configure an SD-WAN rule to match the Yahoo traffic and send the action to Yahoo.
 - a. In Director view, 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 the Configuration tab in the top menu bar.
 - e. Select Services  > SD-WAN > Policies in the left menu bar, and select the Rules tab.
 - f. In the General tab, enter a name for the rule. In the example here, the name is Yahoo_Rule.

Add Rules [X]

General Source/Destination Headers/Schedule Applications URL Users/Groups Forwarding Class Enforce

Name *
Yahoo_Rule

Description

OK Cancel

- g. Select the Source/Destination tab, and select a LAN VR that is the source of incoming traffic.

Add Rules [X]

General Source/Destination Headers/Schedule Applications URL Users/Groups Forwarding Class Enforce

☐ Source Address [+] [-]

☐ Source Zone [+] [-]
☐ Intf-LAN-Network-T1-Zone

+ New Address Group + New Address

+ New Zone

☒ Source Address Negate

☐ Destination Address [+] [-]

+ New Address Group + New Address

☒ Destination Address Negate

Source Site

☐ Source Site Name [+] [-]

Destination Site

☐ Destination Site Name [+] [-]

OK Cancel

- h. Select the Applications/URL tab, and in the Applications table, select YAHOO from the Application List.

Add Rules

General | Source/Destination | Headers/Schedule | **Applications** | URL | Users/Groups | Forwarding Class | Enforce

Applications

☐ Application List

☐ YAHOO

+ New Group + New Filter + New Application

SaaS Application Groups

☐ SaaS Application Group List

OK Cancel

- i. Select the Enforce tab, and in the Forwarding Profile field, select the forwarding profile you created in Step 1. Note that you must not select a routing instance.

Add Rules

General | Source/Destination | Headers/Schedule | Applications | URL | Users/Groups | Forwarding Class | **Enforce**

Forwarding

Action *
Allow Flow

Forwarding Profile
Yahoo_Forwarding_Profile

View Forwarding Profile

Nexthop IP address
IP Address

Routing Instance
--Select--

☐ Enable Symmetric Forwarding of Return Traffic ☐ Enable Symmetric L2 Forwarding of Return Traffic

Logging

LEF Profile
--Select--

Event
Never

Rate Limit
10

☐ Default Profile

Monitor

Address
IP Address

Action
--Select--

Threshold(Events)
5

Routing Instance
--Select--

Interval(sec)
3

OK Cancel

- j. Click OK.

3. Modify the CGNAT rule:

- a. Select Services > CGNAT in the left menu bar.
- b. Select the CGNAT rule, and click the Edit icon.
- c. Select the Match tab, and modify source zone so the PBF policy evaluates traffic first and performs NAT on

the WAN side, as shown below.

d. Click OK.

To verify the the DIA configuration:

- Issue the **show orgs org organization-name brief | select application yahoo** CLI command to verify whether traffic to Yahoo is routed via the remote breakout. traffic from the LAN side has started.
- Issue the **show orgs org organization-name sessions extensive | select application yahoo** CLI command to check session details for the Yahoo application.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- For Releases 21.1.1 and later, you can use the default CGNAT configuration to match traffic going towards the DIA split tunnels and then configure PBF or SD-WAN rules as appropriate.

Additional Information

[Configure Basic Features](#)

[Configure CGNAT](#)

[Configure Interfaces](#)

[Configure Policy-Based Forwarding](#)

[Configure SaaS Application Monitoring](#)

[Configure SD-WAN Policy](#)

[Configure SD-WAN Traffic-Steering](#)

[Configure Virtual Routers](#)

[Create and Manage Post-Staging Templates](#)