
VOS Edge Device Direct Internet Access

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

In a typical legacy enterprise VPN topology, internet traffic from the branch is directed to a hub site over a private MPLS link, and from the hub, it is sent to, or breaks out to, the internet. The internet-bound traffic typically passes through a web proxy that is placed in the hub, where it may be inspected by a firewall. With the advent of high-speed and more reliable internet circuits, it is more economical for enterprises to break traffic out to the internet directly at the branch office. Also, as enterprises move some of their enterprise workloads to the public cloud or use SaaS-based services such as Office 365, a better user experience is important. The breaking out of traffic to the internet at the branch is called direct internet access, or DIA.

The following are the primary advantages of DIA:

- Reduces the bandwidth requirements at headquarters
- Fewer network hops
- Reduces the latency and offers better optimization for internet applications because of direct routing

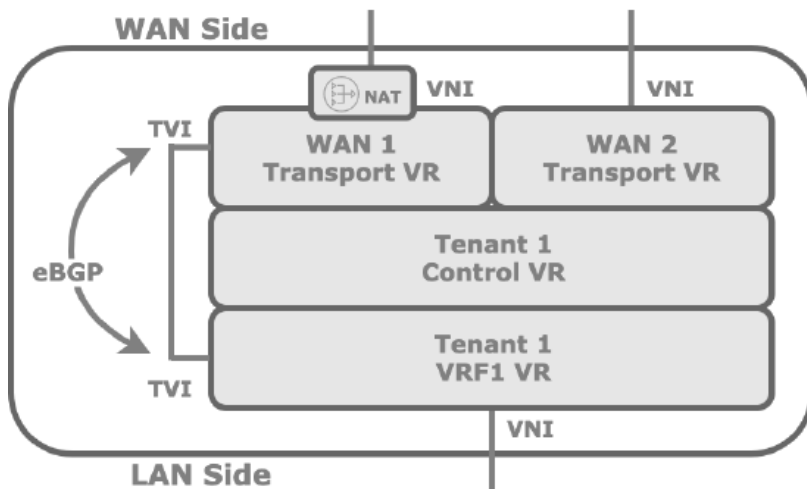
The increased reliability of the internet for WAN transport makes DIA desirable in branch deployments. However, sending traffic directly from the branch to the internet creates additional security challenges and the branch requires extra protection.

The DIA architecture discussed here is based on standard routing principles. Internally, a logical connection is created between a tenant VRF and the WAN transport VR. The tenant VRF uses EBGP to advertise the default route, and it uses the logical tunnel to resolve the next hop. A NAPT rule translates all LAN traffic into one public IP address space.

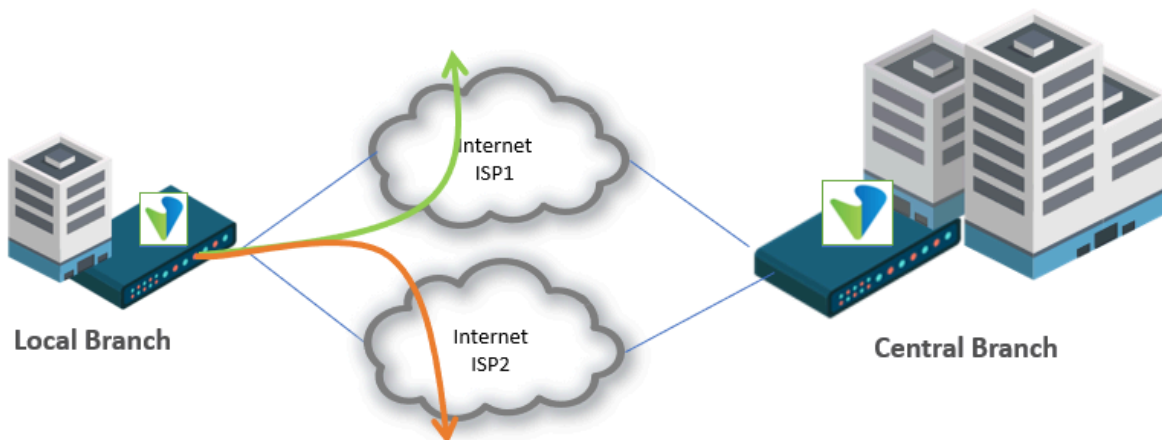
VOS Edge Device DIA Architecture

When you configure internet breakout on a branch, the configuration of the VOS edge device has the following main components, which are illustrated in the following figure:

- Internal connection between the VRF and the transport WAN VR, which is supported by an EBGP connection, to control route distribution
- CGNAT function, to translate the IP addresses of all internet-bound traffic to the public IP address that is typically attached to the transport WAN VR interface



When multiple WANs are available, you can achieve DIA redundancy and DIA load balancing, as shown in the following figure. To do this, you set the BGP local preference in the Director Workflow to select the preferred WAN interfaces. If you select the load-balancing option is selected, the same local preference value is used for both that default routes that are advertised over EBGP towards the VRF.



You configure DIA using Director Workflows, when you configure tunnels. For more information, see [Configure Direct Breakout to the Internet](#).

Central or Regional Internet Breakout

In a typical deployment, it is common to provide redundancy for the default route. For the two default routes, one points to a local DIA and the backup default route, with a less preferred metric, points to the central DIA. If the local branch internet circuit malfunctions, the locally sourced default route is withdrawn and the centrally sourced default route is activated.

You use the Director Workflow to create a local internet breakout and establish the central, regional, or remote backup in

the Create/Edit Template window > Tunnels tab, as shown in the following screenshot.

To configure this use case, ensure that you do not click the Gateway field for the local breakout edge device if you click the Gateway field for the central internet breakout edge device. When you click the Gateway field, the edge device announces the default route to the rest of the SD-WAN. If you do not click the Gateway field, the default route sourced by the local DIA infrastructure is visible only on the local edge device and is not visible anywhere else in the SD-WAN VPN. For more information, see [Configure Device Templates](#) and [Configure Site-to-Site Tunnels](#).

To view the route table on the local device, issue the **show route routing-instance** CLI command. For example:

```
admin@Site3-cli> show route routing-instance
Prot  Type  Dest Address/Mask  Next-hop  Age  Interface name
----  -
BGP   N/A   0.0.0.0/0         10.2.64.101  00:31:23 Indirect
BGP   N/A   +0.0.0.0/0        169.254.0.2  00:00:18 tvi-0/603.0
conn  N/A   +169.254.0.2/31   0.0.0.0     00:00:20 tvi-0/603.0
local N/A   +169.254.0.3/32   0.0.0.0     00:00:20 directly connected
BGP   N/A   172.1.118.0/24    10.2.64.101  00:31:23 Indirect
BGP   N/A   +172.1.118.0/24   10.2.64.102  00:31:23 Indirect
```

In the route table output above, the preferred route is the local breakout route, the route whose next hop is 169.254.0.2. You can check the BGP route table to verify that this route has a better (lower) distance, favoring EBGP over IBGP. For example:

```
admin@Site3-cli> show route routing-instance Enterprise1-LAN-VR 0.0.0.0/0

Routes for Routing instance : Enterprise1-LAN-VR AFI: ipv4 SAFI: unicast
[+] - Active Route

Routing entry for 0.0.0.0 (mask 0.0.0.0)
Known via 'BGP', distance 200,
  Redistributing via BGP
  Last update from 10.2.64.101 00:34:20 ago
Routing Descriptor Blocks:
* 10.2.64.101 , via Indirect 00:34:20 ago

Routing entry for 0.0.0.0 (mask 0.0.0.0) [+]
Known via 'BGP', distance 20,
  Redistributing via BGP
  Last update from 169.254.0.2 00:03:15 ago
Routing Descriptor Blocks:
* 169.254.0.2 , via Indirect 00:03:15 ago
```

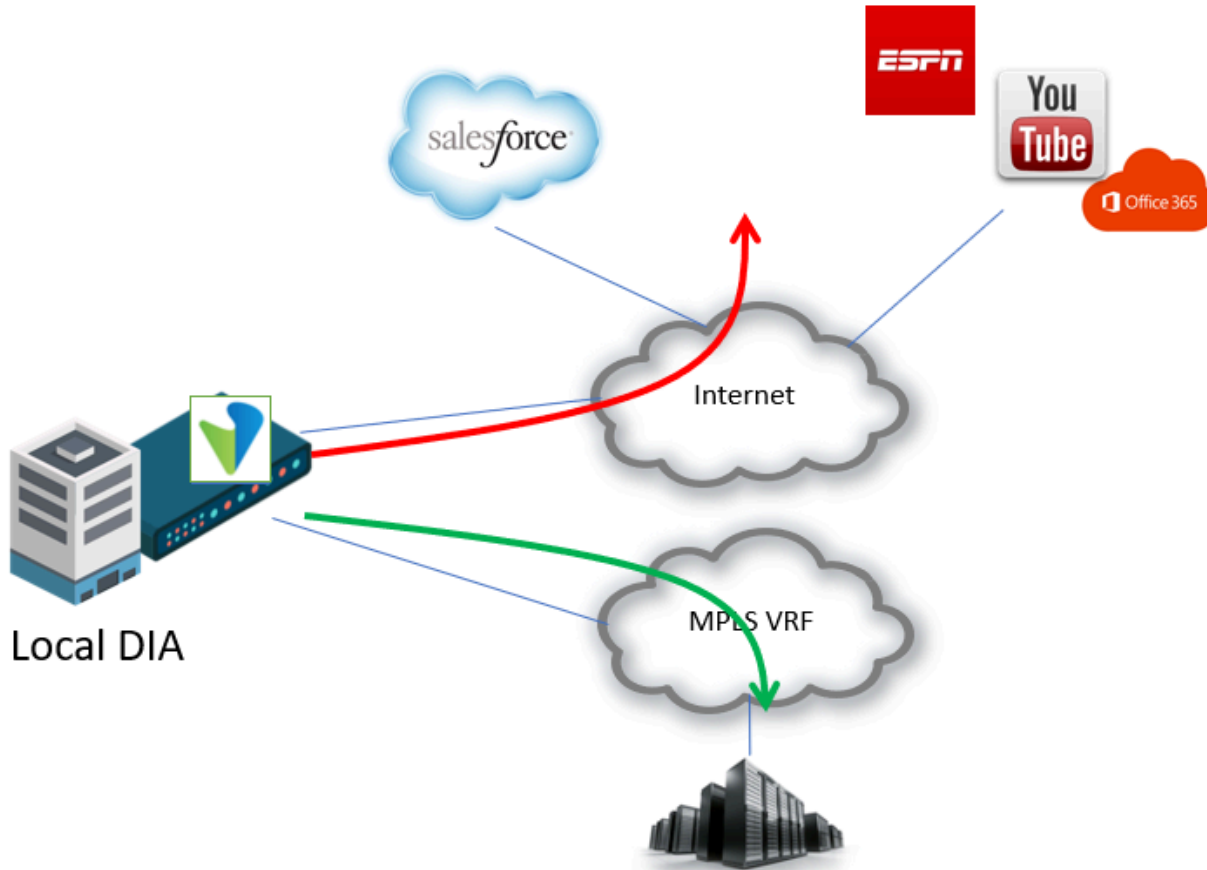
You can alter this behavior by manipulating the BGP preference in the configuration.

With this infrastructure, you can create advanced configurations by using route coloring with communities, where different regions prefer different regional default routes.

Breakout to an MPLS Underlay for Common Services

Another use case for DIA is a breakout service to the MPLS underlay. You can use this type of breakout to reach services offered by an MPLS provider from the underlay, such as VoIP services. You can also use this solution to provide gateway services during migration from a legacy MPLS network to an SD-WAN network.

You achieve the breakout to MPLS the same way as a local internet breakout service. In the Director Workflow, you create a split tunnel to the MPLS underlay, as illustrated below.



One important difference from an Internet breakout split tunnel is that you must not click the DIA field on the Tunnels tab in the Create or Edit Template window. Clicking this field creates a NAT instance, which is not required in a private MPLS underlay. If you prefer to advertise the routes imported from MPLS to the rest of the SD-WAN VPN, click the Gateway field on the Tunnels tab, as shown here:

VRF Names	WAN Interfaces	DIA	Gateway
--Select--	--Select--	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise1-LAN-VR	Internet-ISP1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The infrastructure shown in the screenshot above also creates an internal connection between the LAN-VR and the MPLS-VR, and it runs EBGp over the connection. In this way, the routes in the MPLS-VR are propagated to the LAN-VR.

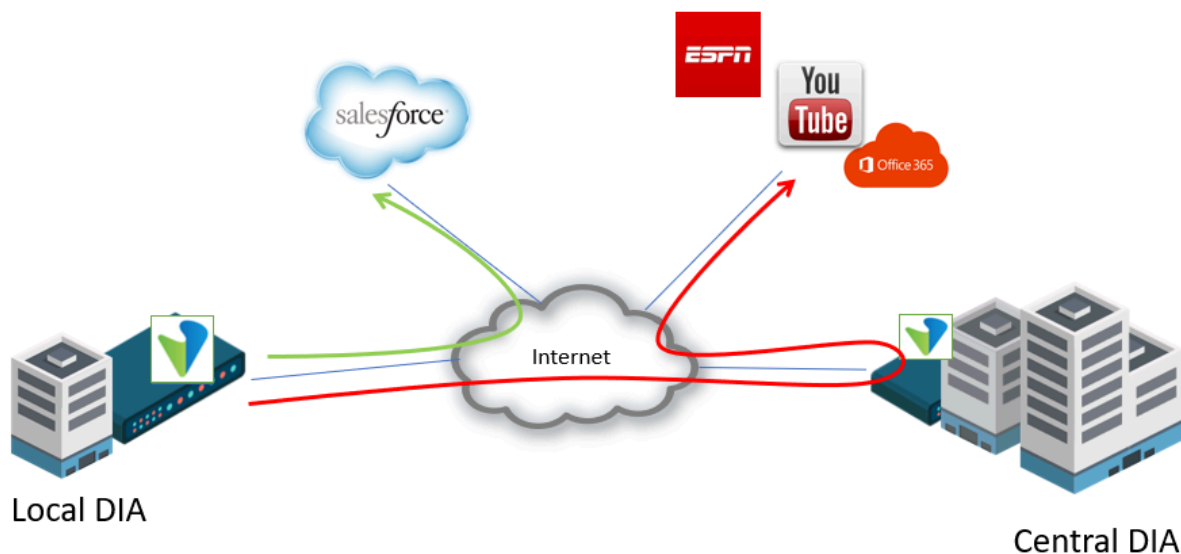
Next, you must import the MPLS VRF routes into the SD-WAN edge device. To do this requires a dynamic routing connection between the SD-WAN edge device and the MPLS provider infrastructure, which is typically the PE router. The easiest way is to configure the BGP connection on the Routing tab of the Create/Edit template:

Network	IBGP	Local AS	Neighbor IP	Peer AS	BFD
--Select--	<input checked="" type="checkbox"/>	1111	192.1.2.3	2222	<input checked="" type="checkbox"/>
MPLS-ISP1	false	1111	192.1.2.3	2222	false

Note that the remote PE router, which is operated by the managed service provider (MSP), must also be configured with similar dynamic routing.



Application-Based Breakout

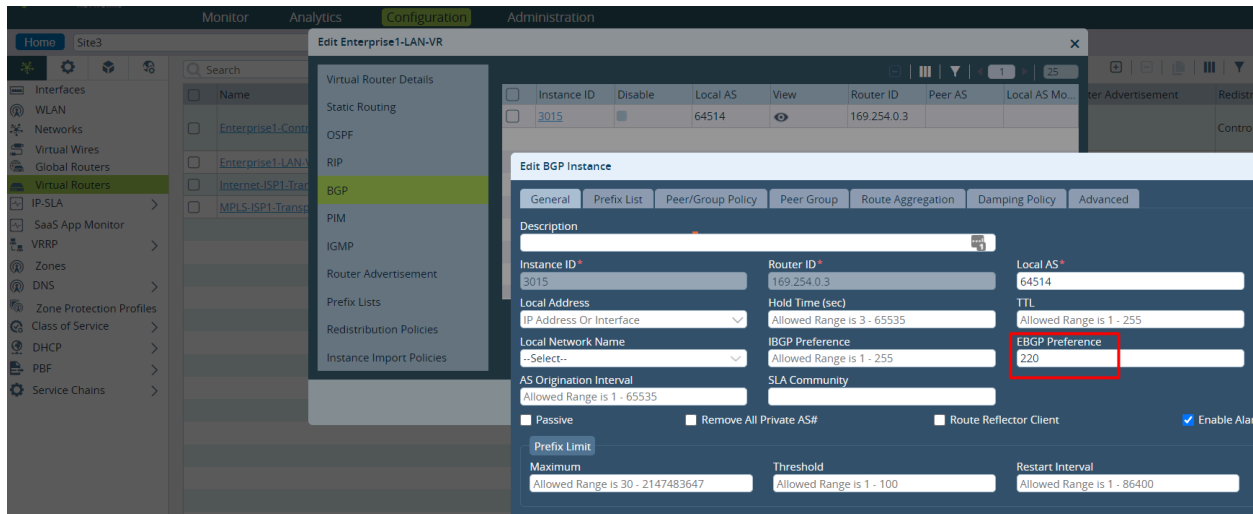
A common DIA use case is to provide a local breakout service for specific applications, in which the default route points a regional or central breakout point. This configuration is a little more involved and relies on the infrastructure shown in [Option 1: BGP to Exchange Routes with MPLS Provider on MPLS WAN Interface](#) and [Option 2: BGP with MPLS Provider on LAN Interface](#). For these usage case, the SD-WAN edge device has a local breakout infrastructure and also has an option to break out centrally. The following figure illustrates this use cae.



As described in [Breakout to MPLS Underlay for Common Services](#) above, this design prefers a local breakout over a central breakout. For the default internet-bound traffic to break out centrally, you must alter the preference to one that is higher than 200, because, by default, the EBGp route administrative distance (20) is better than that for the IBGP (200).

To set the EBGp preference to 220 for the LAN-VR, to make the router to central default router be the preferred route:

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 BGP tab in the left menu bar. The main pane displays a list of the BGP instances that are already configured.
6. Click the  Add icon. The Add BGP Instance popup window displays.
7. Select the General tab.
8. In the EBGp Preference field, enter 220.



9. For information about configuring the other fields, see [Configure BGP](#).
10. Click OK.

Now, all internet traffic breaks out at the central breakout point.

To verify that the central default route is preferred:

```
admin@Site3-cli> show route routing-instance Enterprise1-LAN-VR 0.0.0.0/0
```

```
Routes for Routing instance : Enterprise1-LAN-VR AFI: ipv4 SAFI: unicast
[+] - Active Route
```

```
Routing entry for 0.0.0.0 (mask 0.0.0.0) [+]
Known via 'BGP', distance 200,
  Redistributing via BGP
  Last update from 10.2.64.101 01:16:57 ago
Routing Descriptor Blocks:
* 10.2.64.101 , via Indirect 01:16:57 ago
```

```
Routing entry for 0.0.0.0 (mask 0.0.0.0)
Known via 'BGP', distance 220,
  Redistributing via BGP
  Last update from 169.254.0.2 00:00:06 ago
Routing Descriptor Blocks:
* 169.254.0.2 , via Indirect 00:00:06 ago
```

Now, all internet traffic breaks out at the central breakout point.

You can also verify that the central default route is preferred by checking whether some internet sessions on the local branch are SD-WAN sessions:

1. In the Appliance view, select the Monitor tab in the top menu bar.
2. Select a provider organization.

3. Select the Services tab.
4. Select Sessions. Check whether the SD-WAN column displays Yes or No.

The screenshot shows the Versa Networks SD-WAN configuration interface. The 'Monitor' tab is selected, and the 'Services' sub-tab is active. The 'Sessions' icon is highlighted. Below the navigation pane, a table displays traffic statistics for various applications.

Application	Source IP	Destination IP	Protocol	Source Port	Destination Port	SD-WAN	Natted
-	10.2.64.107	10.1.64.1	TCP	1154	43000	No	No
cnn	172.1.123.10	23.64.128.102	TCP	51858	443	Yes	No
mozilla	172.1.123.10	34.218.33.223	TCP	43612	443	Yes	No
mozilla	172.1.123.10	54.240.168.88	TCP	50668	443	Yes	No
google_gen	172.1.123.10	216.58.211.106	TCP	38546	443	Yes	No
ocsp	172.1.123.10	172.217.20.67	TCP	46062	80	Yes	No

For this use case, you must also modify the CGNAT rule. The change is simple, but important, you must modify the match condition of the rule to match the source zone, not the destination zone. To do this, you remove the destination zone and add a source zone in the Edit CGNAT Rule popup window. In the example here, you select the zone *W-ST-tenant-name-LAN-VR-internet-WAN-VR*. For more information, see [Configure CGNAT Rules](#).

The screenshot shows the Versa Networks SD-WAN configuration interface. The 'Configuration' tab is selected, and the 'CGNAT' rule is being edited. The 'Edit CGNAT Rule - DIA-Rule-Enterprise1-LAN-VR-Internet-ISP1' popup window is open, showing the 'Match' tab. The 'Source Zones' field is highlighted, and the zone 'W-ST-Enterprise1-LAN-VR-Internet-ISP1' is selected. The 'Destination Zones' field is empty.

To force a specific application to break out locally and to have the remaining internet-bound traffic break out centrally, you create an SD-WAN policy. This example locally breaks out the traffic to Salesforce.com:

1. Create a forwarding profile, here called SaaS_DIA. On the Next Hop tab, select the local DIA as the next hop. For more information, see [Configure SD-WAN Traffic-Steering](#).

Edit Forwarding Profile - SaaS_DIA

General | Circuit Priorities | Avoid Connections | FEC | Advanced Settings | Next Hop

Next Hop Selection Method: Load Balance
Next Hop Failure Action: Wait Recover

Next Hop Priorities List

<input type="checkbox"/>	Name	Priority	Nexthop IP address	Routing Instance	Site Name	Monitor	WAN Network
<input type="checkbox"/>	Local_WAN	1					Internet-ISP1

2. Create a forwarding profile rule to associate with the forwarding profile. For more information, see [Configure SD-WAN Traffic Steering Policy](#).

- a. Select the Source/Destination tab, and select the source zone.

Edit Rules - Salesforce_DIA

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

Source Address

☐ Source Zone
☐ Intf-LAN-Zone

- b. Select the Applications tab, and in the SaaS Application Groups table, select Salesforce-Apps.

Edit Rules - Salesforce_DIA

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

Applications

☐ Application List

SaaS Application Groups

☐ SaaS Application Group List
☐ Salesforce-Apps

- c. Select the Enforce tab, and in the Forwarding Profile field, select the forwarding profile you created in Step 1.

Edit Rules - Salesforce_DIA

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

Forwarding

Action: Allow Flow
Forwarding Profile: SaaS_DIA
View Forwarding Profile
Routing Instance: --Select--
☒ Enable Symmetric Forwarding of Return Traffic
☐ Enable Symmetric L2 Forwarding of Return Traffic

Logging

LEF Profile: Default-Logging-Profile
Event: Never
Rate Limit: 10

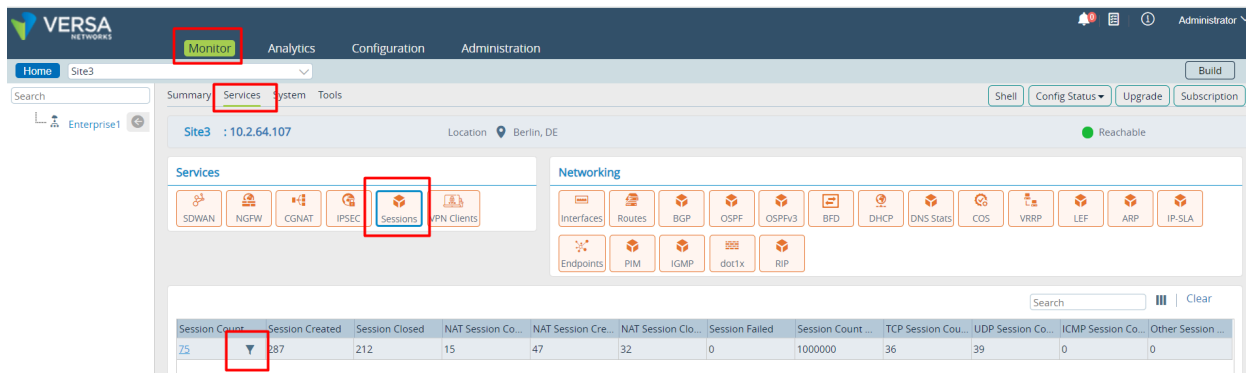
- d. Click OK.


To verify the configuration, open a browser and navigate to the website or application, Salesforce in this example.

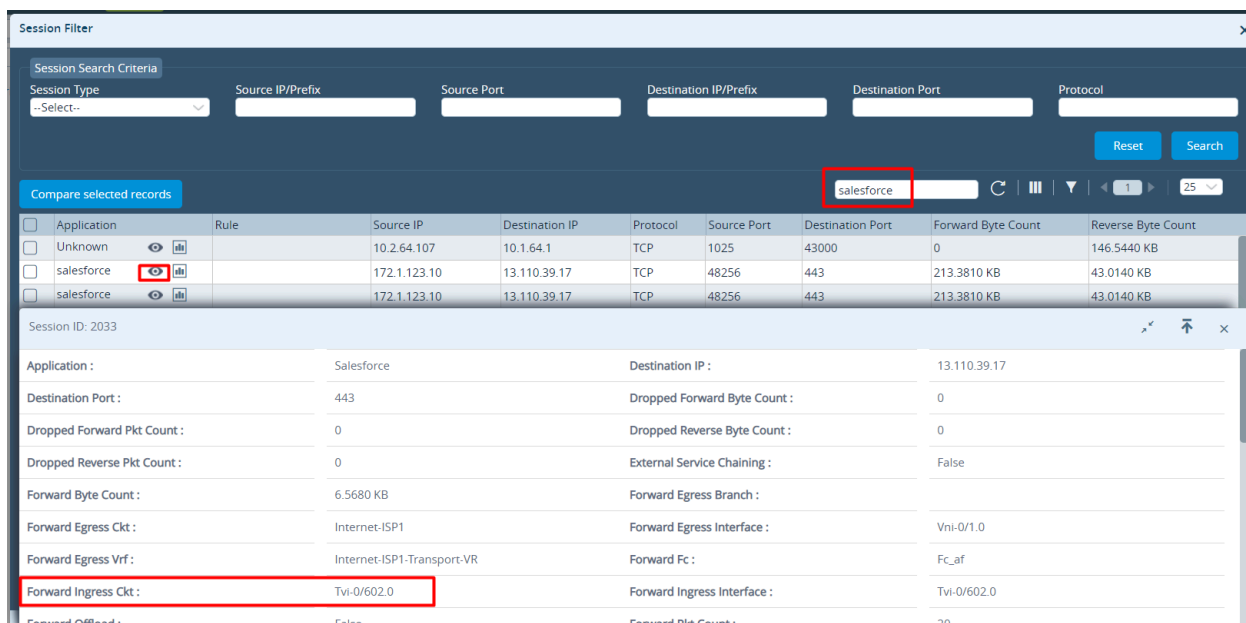
You can verify the operation in a number of ways.


To verify the session details and the egress:

1. In the Appliance view, select the Monitor tab in the top menu bar.
2. Select a provider organization.
3. Select the Services tab.
4. Select the Sessions tab, and search for salesforce.



5. Click the  Eye icon to view details. If the breakout to the local DIA is functioning correctly, the Ingress and Egress Circuit fields show the interface TVI-0/602, which is the interface that has the IP address that you set as the next hop.



6. To verify that sessions for other (non-Salesforce) traffic are not pointing to this TVI, select that application and click the ;  Eye icon to view details. Typically, you see that the Tx Branch is your central DIA edge device.

Best Practices

The following are best practices for using DIA:

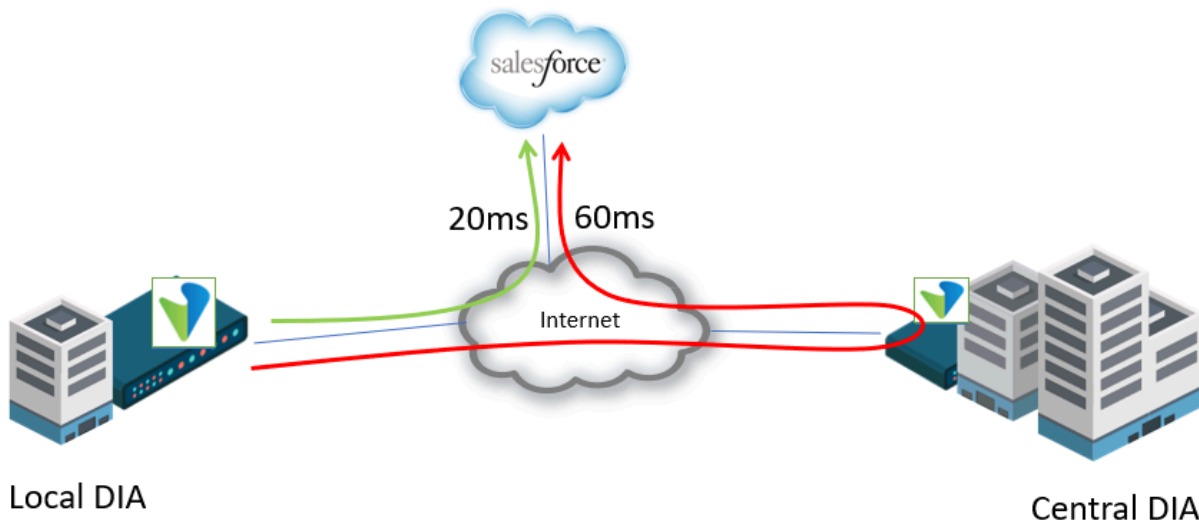
- Use the DIA gateway feature to enable central breakout to internet to ensure backup for local breakout.
- Use application-based local breakout to improve performance for one application or a group of applications.
- For application-based traffic steering, remove the default route populated by the workflow template to the central location, except for one or a group of applications.
- To test and verify application-based traffic steering, generate multiple traffic flows.
- Remove the local breakout default route—You can suppress the default route sourced by the local breakout DIA configuration, because it is not required for the configuration. If you retain it, the default route acts as a backup breakout point for the local site if the central breakout fails. If you steer traffic based on the application use case, the locally sourced default route is not required. If you do not need a local breakout except for specific applications, you must remove this default route. You can do this by filtering the default route with a prefix list or by removing the redistribution of static routes under redistribution policies.
- Deep packet inspection (DPI) application recognition—When you test the implementation, the traffic may not locally break out as expected. A common reason is that the DPI does not detect the application ID when the session is created. This is more common in lab setups than in production deployments, because production deployments have more application cache for the same application traffic. For example, the system is aware of the traffic that goes to a specific destination IP address, such as salesforce.com. To build up the application cache, create additional sessions, for example, by refreshing the browser.

Performance-Based SaaS Optimization for DIA

The Versa Networks SD-WAN solution selects the best internet breakout to reach SaaS applications by performing monitoring to measure application network performance. The following types of monitoring are available:

- Passive (inline monitoring)—VOS edge devices collect metrics for active TCP-based SaaS application sessions transiting the edge device. These metrics include the network and server response times and packet loss estimates in each direction. These metrics are used to assess application quality on a particular path and then to select the best path for the application.
- Active monitoring—Active monitoring proactively monitors SaaS locations using HTTP, ICMP, and TCP probes, exports the collected metrics to remote sites, and incorporates actively learned metrics in path selection. The metrics collected through active monitoring are latency (RTT) and packet loss.

The data collected by these measurement techniques are automatically combined with the existing SLA measurement over the overlay to select the best path, and the SD-WAN policy steers the traffic accordingly. The following figure illustrates how this works. Here, the local DIA branch measures a latency of 20 milliseconds to Salesforce.com, while from the same branch, it takes 60 milliseconds to reach Salesforce.com through the central DIA. Therefore, the logic in the local DIA branch steers the traffic to internet using the local DIA.



Basic Performance-Based Breakout Configuration

This section describes how to configure performance-based application breakout that is based on active monitoring of an SaaS application, and it build on the application-based breakout scenario. Performance-based breakout leverages the infrastructure of having local and remote DIA, and it requires that you modify the NAT rule. However, for performance-based breakout, you configure the SD-WAN policy differently.

For performance-based breakout, you create the following additional building blocks:

- SaaS application monitor on both the local and remote breakout edge devices
- SD-WAN SLA profile for the local edge device
- SD-WAN forwarding profile for the local edge device
- SD-WAN policy for the local edge device


In the design configuration example here, the Salesforce application breaks out using the breakout point that provides the lowest latency to this SaaS. The latency is measured from the point of view of the local edge device. This configuration example has two breakout options:

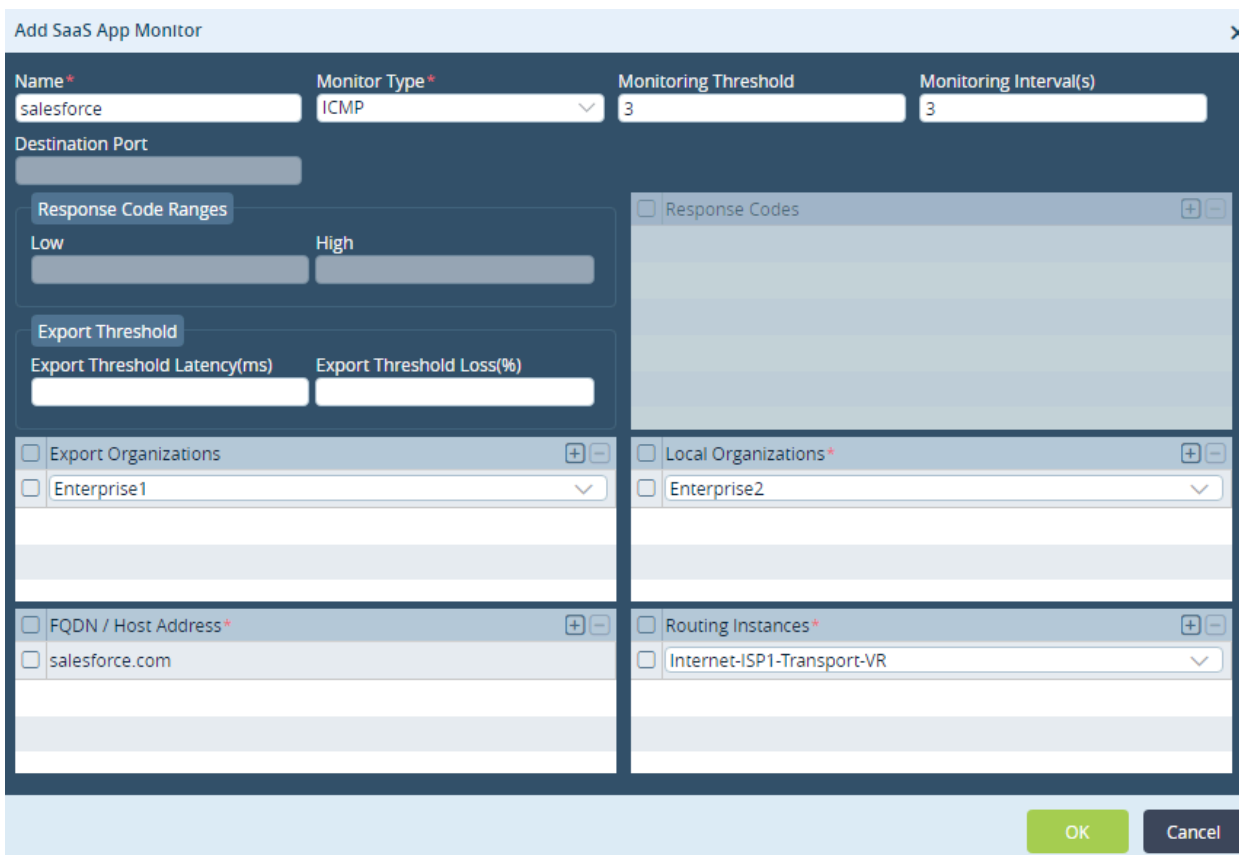
- Break out Salesforce traffic locally—The latency measurement is from the local edge device to Salesforce only, over the internet.
- Break out Salesforce traffic remotely—The latency measurement is from the local edge device to the remote edge device over the SD-WAN overlay, and then to Salesforce over the internet connection to the remote edge device. This configuration adds together the internet latency and overlay latency.




For both the local and remote edge devices, you configure a SaaS application monitor that checks the performance to a specific SaaS application FQDN. Note that the example here shows only the minimum required configuration for the SaaS application monitor, and it shows the configuration of the local edge device only. You might have different requirements or more complicated use cases. Many configuration options are available, and many alternative scenarios are possible, such as more local internet breakouts, more remote internet breakout places, and different SLA criteria.

For more information, see [Configure SaaS Application Monitoring](#), [Configure SLA Profiles for SD-WAN Traffic Steering](#), and [Configure SD-WAN Traffic Steering](#).

To configure performance-based monitoring for the Salesforce SaaS application:

1. Add a SaaS application monitor named salesforce:
 - a. In Appliance view, select the Configuration tab in the top menu bar.
 - b. Select Networking > SaaS App Monitor in the left menu bar.
 - c. Click the  Add icon to add a SaaS application monitor.



- d. In the Name field, enter "salesforce".
- e. In the FQDN/Host Address table, click the  Add icon to select the FQDN salesforce.com.
- f. Click OK.
2. Configure an SLA profile that references the SaaS application monitor you configured in Step 1:
 - a. In Appliance view, select the Configuration tab in the top menu bar.
 - b. Select Services  > SD-WAN > SLA Profiles in the left menu bar.
 - c. Click the  Add icon to add an SLA profile, or select an existing SLA profile, as shown here. The Create


SLA Profile or Edit SLA Profile popup window displays. (Note that the screenshot shows the incorrect SLA profile name. It should be "perf_DIA".)

- d. Select the SaaS App Monitor tab, and in the Monitor Name field, select salesforce. This example uses Low Latency, to have the network to choose the lowest latency or loss. Alternatively, you can set values for the maximum latency or maximum loss, to have all paths be considered as long as the maximum value is not reached.

The screenshot shows a window titled "Edit SLA Profile - perf_DIA". It has two tabs: "General" and "SaaS App Monitor". The "SaaS App Monitor" tab is active. Inside this tab, there is a "Monitor Name" dropdown menu with "salesforce" selected. Below it, there are two checkboxes: "Low Latency" (checked) and "Low Packet Loss" (unchecked). To the right of these checkboxes are two empty input fields labeled "Maximum Latency (ms)" and "Maximum Loss (%)". At the bottom right of the window are "OK" and "Cancel" buttons.

- e. Click OK.

3. Configure a forwarding profile that references the SLA profile you configured in Step 2:

- a. In Appliance view, select the Configuration tab in the top menu bar.
- b. Select Services  > SD-WAN > Forwarding Profiles in the left menu bar. The Add Forwarding Profile or Edit Forwarding Profile popup window displays.
- c. Click the Add icon to add a forwarding profile, or select an existing forwarding profile, as shown here.
- d. Select the General tab, and in the SLA Profile field, select the SLA profile.

Edit Forwarding Profile - perf_DIA

General Circuit Priorities Avoid Connections FEC Advanced Settings Next Hop

Name*
perf_DIA

Description

Tags

SLA profile
perf_DIA

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

☐ Stop When

Replication factor

Start When
Always

Circuit Utilization

☒ Evaluate Continuously

☐ Reorder

☒ Enable Symmetric Forwarding

OK Cancel

- e. Select the Next Hop tab and specify the breakout options for the traffic used by this forwarding profile. In this example, there is a local breakout and a remote breakout to the internet:
 - i. For the local internet breakout, select the local WAN interface, and for the remote internet breakout, select the remote site where the remote breakout is available.

Edit Forwarding Profile - perf_DIA

General Circuit Priorities Avoid Connections FEC Advanced Settings Next Hop

Nexthop Selection Method
Automatic

Nexthop Failure Action
Wait Recover

Next Hop Priorities List

	Name	Priority	Nexthop IP address	Routing Instance	Site Name	Monitor	WAN Network
<input checked="" type="checkbox"/>	Local WAN	1					Internet-ISP1
<input type="checkbox"/>	remote WAN	1			GW1		

- ii. Select the conditions for the breakout to use. In this example, because we have chosen to have the network automatically chooses the breakout that has the lowest latency, we select Automatic in the Next-Hop Selection Method field.
- iii. Set the same priority value (here, 1) for both breakouts.

Edit Forwarding Profile - perf_DIA

General Circuit Priorities Avoid Connections FEC Advanced Settings Next Hop


Nexthop Selection Method: Automatic Nexthop Failure Action: Wait Recover

Next Hop Priorities List

<input type="checkbox"/>	Name	Priority	Nexthop IP address	Routing Instance	Site Name	Monitor	WAN Network
<input checked="" type="checkbox"/>	Local WAN	1					Internet-ISP1
<input type="checkbox"/>	remote WAN	1			GW1		

f. Click OK.

4. Configure an SD-WAN policy that defines the traffic classification criteria for this configuration example.

- In Appliance view, select a post-staging template.
- Select the Configuration tab in the top menu bar.
- Select Configuration > Services  > SD-WAN > Policies > Rules in the left menu bar
- Click the Add icon to add a rule, or select an existing SD-WAN policy rule, as shown here.
- Select the Source/Destination tab, and in the Source Zone table, select the source zone. In this example, the source for the Salesforce traffic is a LAN zone.

Edit Rules - Salesforce_best_DIA

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

Source Address

Source Zone

Intf-LAN-Zone

Source Address Negate

Destination Address

Source Site

Source Site Name

Destination Site

Destination Site Name

Destination Address Negate

OK Cancel

f. Select the Applications tab, and in the SaaS Application Groups table, select Salesforce-Apps. Note that this

example works only with the SaaS Application Group classification.

The screenshot shows the 'Edit Rules - Salesforce_best_DIA' window with the 'Applications' tab selected. On the right side, under 'Saas Application Groups', there is a list with two items: 'Saas Application Group List' and 'Salesforce-Apps'. Both items have a checkbox to their left. A red rectangular box highlights this entire section. At the bottom right of the window are 'OK' and 'Cancel' buttons.

- g. Select the Enforce tab, and in the Forwarding Profile, select the forwarding profile you configured in Step 3.

The screenshot shows the 'Edit Rules - Salesforce_best_DIA' window with the 'Enforce' tab selected. The 'Forwarding' section on the left has a 'Forwarding Profile' dropdown menu highlighted with a red box; it currently shows 'perf_DIA'. Other options in this section include 'Action' (set to 'Allow Flow'), 'Nexthop IP address', and checkboxes for 'Enable Symmetric Forwarding of Return Traffic' and 'Enable Symmetric L2 Forwarding of Return Traffic'. The 'Logging' section on the right includes 'LEF Profile' (set to 'Default-Logging-Profile'), 'Event' (set to 'Never'), and 'Rate Limit' (set to '10'). At the bottom right are 'OK' and 'Cancel' buttons.

- h. Click OK.

To verify the performance-based breakout configuration:

1. Verify the operation of the SaaS application monitor at the local and remote breakout points by issuing the **show application-monitor local detail** CLI command.

The following output shows that the local breakout point measures the latency to Salesforce as 225 ms:

```
admin@Site3-cli> show application-monitor local detail
```

https://docs.versa-networks.com/Solutions/SD-WAN_Design/07_VOS_Edge_Device_Direct_Internet_Access

Updated: Thu, 24 Oct 2024 10:49:47 GMT

Copyright © 2024, Versa Networks, Inc.

```

APPLICATION
MONITOR                               LOSS   LATENCY LOCAL   EXPORT
NAME   ROUTING INSTANCE              TYPE PERCENTAGE MILLISEC ORGANIZATION
ORGANIZATION
-----
salesforce Internet-ISP1-Transport-VR icmp 0.0      225.53 Enterprise1 Enterprise1

```

The output at the remote breakout point measures the latency to Salesforce as 215 ms:

```

admin@GW1-cli> show application-monitor local detail
APPLICATION
MONITOR                               LOSS   LATENCY LOCAL   EXPORT
NAME   ROUTING INSTANCE              TYPE PERCENTAGE MILLISEC ORGANIZATION
ORGANIZATION
-----
salesforce Internet-ISP1-Transport-VR icmp 0.0      215.75 Enterprise1 Enterprise1

```

- For the Salesforce traffic to reach the remote breakout point, you must add latency of the overlay. To verify this latency, issue the following CLI command:

```

admin@Site3-cli> show orgs org Enterprise1 sd-wan sla-monitor metrics last-1m GW1
LOCAL REMOTE
WAN WAN TWO FWD REV PDU FWD
REV
SITE PATH FWD LOCAL WAN REMOTE WAN LINK LINK WAY DELAY DELAY LOSS
LOSS LOSS
NAME HANDLE CLASS LINK LINK ID ID DELAY VAR VAR RATIO RATIO
RATIO
-----
GW1 6627844 fc_ef Internet-ISP1 Internet-ISP1 2 2 171 0 1 0.0 0.0 0.0

```

- The command output in Steps 1 and 2 shows that the SD-WAN logic is computing the best path (in this example, based on latency) and will select the local breakout point because it is better. To verify this:

```

admin@Site3-cli> show orgs org-services Enterprise1 sd-wan policies Default-Policy rules nexthop
application-monitor detail
APPLICATION APPLICATION APPLICATION
MONITOR NEXTHOP NEXTHOP NEXTHOP NEXTHOP HIT MONITOR MONITOR
NAME PRIORITY NAME STATUS ACTIVE COUNT NAME TYPE
LATENCY LOSS
-----
Salesforce_best_DIA 1 Local_WAN up yes 127 salesforce icmp 226.87 0.
0
1 remote_WAN up - 88 salesforce icmp 389.7 0.0

```

- Verify whether Salesforce sessions are actually going to the local breakout:

```

admin@Site3-cli> show orgs org Enterprise1 sessions brief | select application salesforce
VSN VSN SESS DESTINATION SOURCE DESTINATION
ID VID ID SOURCE IP IP PORT PORT PROTOCOL NATTED SD-WAN
APPLICATION
-----



```

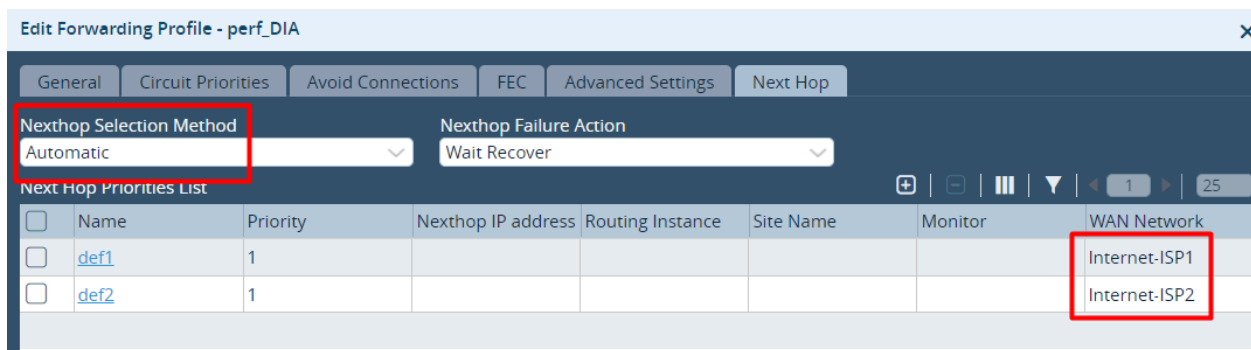
0	2	955	172.1.123.10	13.110.37.145	40880	443	6	No	No	salesforce
0	2	956	172.1.123.10	13.110.37.145	40880	443	6	Yes	No	salesforce
0	2	965	172.1.123.10	13.110.37.145	40886	443	6	No	No	salesforce
0	2	966	172.1.123.10	13.110.37.145	40886	443	6	Yes	No	salesforce
0	2	969	172.1.123.10	13.110.37.145	40890	443	6	No	No	salesforce
0	2	970	172.1.123.10	13.110.37.145	40890	443	6	Yes	No	salesforce

Variants of the Basic Performance-Based Breakout Configuration

The configuration example above is based on a performance-based breakout that has a local breakout option and a remote breakout option. You can use the same approach when there are multiple local breakout possibilities, for example, two WAN transports. If these local WANs are provided by different ISPs, each may have different performance characteristics. For example, the WAN transport provided by ISP1 might be closer to the SaaS application server than ISP2. Another common use case is when a cloud security provider provides the breakout. In this case, an IPsec or GRE tunnel directs the traffic to the cloud security provider and you can apply the same logic for all such use cases.

For these scenarios, you configure the next-hop selection method to Automatic in the forwarding profile, as follows:

1. Configure a forwarding profile with two ISPs as next-hop options. For more information, see [Configure SD-WAN Traffic-Steering](#).
2. In Appliance view, select the Configuration tab in the top menu bar.
3. Select Services  > SD-WAN > Forwarding Profiles in the left menu bar.
4. Click the  Add icon, or select an existing forwarding profile, as shown here.
5. Select the Next Hop tab.
6. In the Next-Hop Selection Method, select Automatic.
7. In the Next-Hop Failure Action field, select Wait Recover.



Edit Forwarding Profile - perf_DIA											
General		Circuit Priorities		Avoid Connections		FEC		Advanced Settings		Next Hop	
Next Hop Selection Method				Next Hop Failure Action							
Automatic				Wait Recover							
Next Hop Priorities List											
	Name	Priority	Next hop IP address	Routing Instance	Site Name	Monitor	WAN Network				
<input type="checkbox"/>	def1	1					Internet-ISP1				
<input type="checkbox"/>	def2	1					Internet-ISP2				

8. Click OK.

To verify which local breakout is the best performing one, issue the following CLI command:

```
admin@Site2-cli> show orgs org-services Enterprise1 sd-wan application-metrics brief
METRIC REMOTE REMOTE HIT
APPLICATION TYPE DESTINATION IP LOCAL CIRCUIT CIRCUIT SITE METRIC TTL COUNT
```

https://docs.versa-networks.com/Solutions/SD-WAN_Design/07_VOS_Edge_Device_Direct_Internet_Access

Updated: Thu, 24 Oct 2024 10:49:47 GMT

Copyright © 2024, Versa Networks, Inc.

```




-----
Concur-Apps VLR 0.0.0.0/0 Internet-ISP1 - - 11 2996 2
                  Internet-ISP2 - - 59 2997 1
23.38.19.188/32 Internet-ISP1 - - 7 2822 0
                  Internet-ISP2 - - 4 2996 1
92.123.164.163/32 Internet-ISP1 - - 11 2996 1
                  Internet-ISP2 - - 61 2997 5

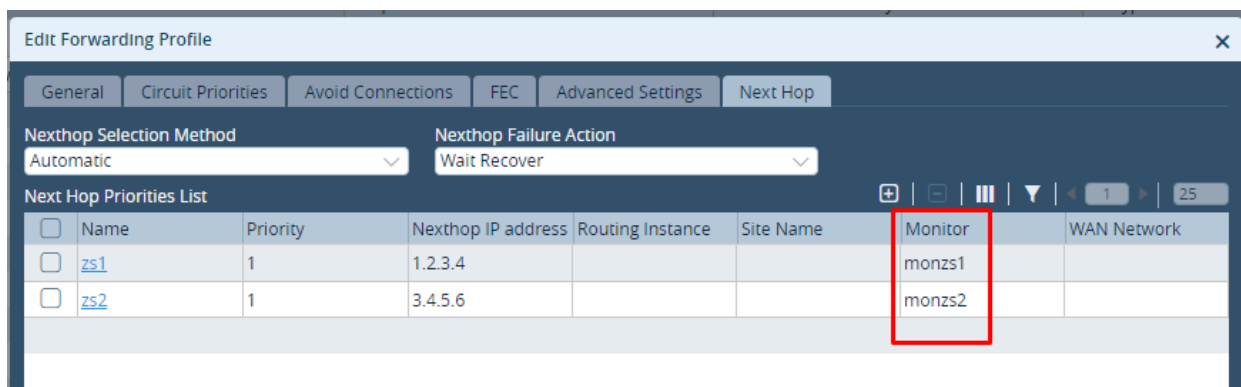
```

The CLI output above shows the different metrics for the local circuits toward ISP1 and ISP2. For this test, the internet circuit to ISP1 is impaired by high loss and high latency, resulting in a bad link score. Therefore, for the last entry in the output, the metric for ISP1 remains low, while the metric for ISP2 increases. The result is that ISP2 gets more sessions (a hit count of 5 compared to a hit count of 1 for ISP1).

Another example is a performance-based breakout to the best performing external cloud security provider. In this use case, you set the forwarding profile next hop to the IP address of the remote tunnel IP endpoint. For all scenarios, it is recommended that you add a monitor to the next hop. In this case, the monitor is verifying the IP endpoint of the tunnel. If the IP endpoint is not reachable, this next hop is not considered.



To configure the forwarding profile next hop to the IP address of the remote tunnel IP endpoint:

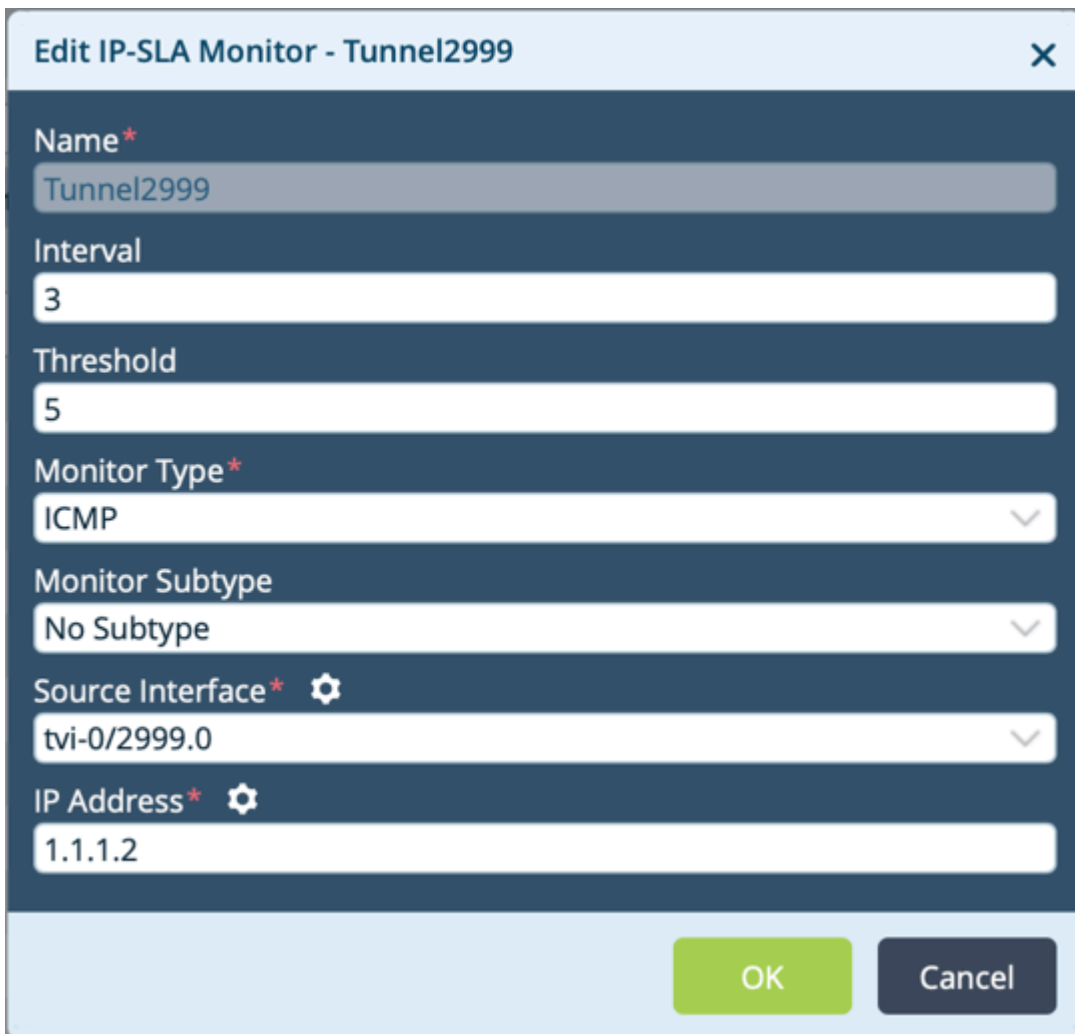
1. Configure a forwarding profile with two ISPs as next hop options. For more information, see [Configure SD-WAN Traffic-Steering](#).
2. In Appliance view, select the Configuration tab in the top menu bar.
3. Select Services  > SD-WAN > Forwarding Profiles in the left menu bar.
4. Click the  Add icon, or select an existing forwarding profile, as shown here. The Add Forwarding Profile or Edit Forwarding Profile popup window displays.
5. Select the Next Hop tab.
6. In the Next-Hop Select Method field, select Automatic.
7. In the Next-Hop Failure Action field, select Wait Recover.
8. Click the  Add icon, and in the Add Next-Hop Priorities popup window, specify the IP address for next hop to the remote tunnel IP end point. GRE and IPsec are the most common tunnel options. For more information, see [Configure Site-to-Site Tunnels](#) and [Configure Interfaces](#).



9. In the Monitor Field, select a monitor to use for the tunnel.
10. Click OK twice.

After you configure the tunnels, add a static route to route traffic to them. It is recommended that you monitor the tunnel endpoint is monitored so that if the tunnel fails, the static route is withdrawn. You do this by configuring an IP SLA monitor, as follows:

1. In Appliance view, select the Configuration tab in the top menu bar.
2. Select Networking  > IP SLA > Monitor in the left menu bar. The main pane displays the IP SLA monitor objects that are already configured. For more information, see [Configure IP SLA Monitor Objects](#).
3. Click the  Add icon, or select an existing IP SLA monitor, as shown below. The Add IP SLA Monitor or Edit IP SLA Monitor popup window displays.



Edit IP-SLA Monitor - Tunnel2999


Name*
Tunnel2999


Interval
3

Threshold
5

Monitor Type*
ICMP



Monitor Subtype
No Subtype

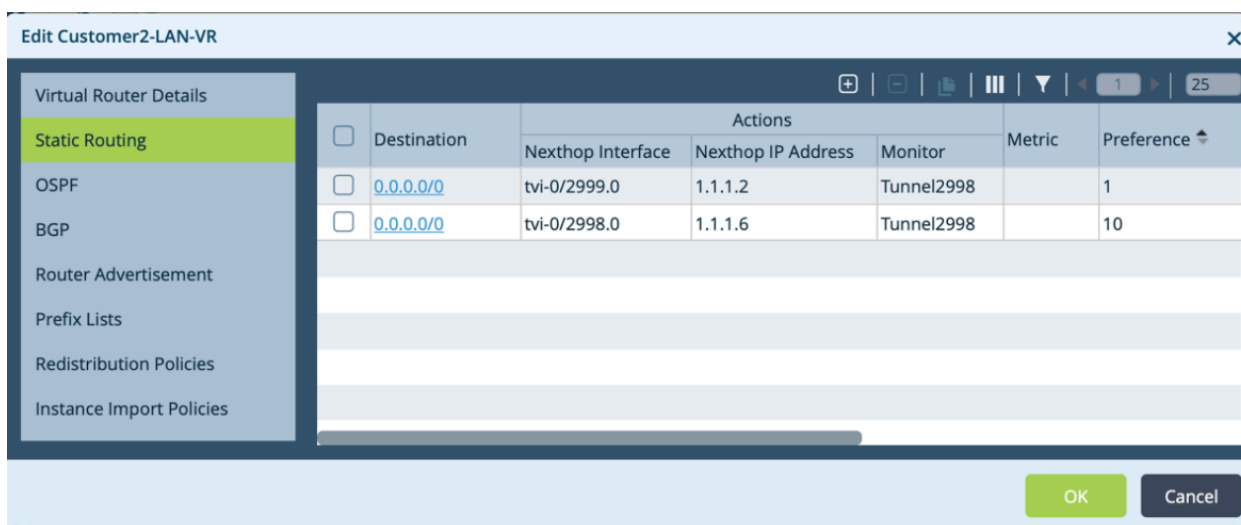
Source Interface* 
tvi-0/2999.0

IP Address* 
1.1.1.2

OK Cancel

4. Associate this IP SLA monitor with the static route. If you want an active/standby connection to the cloud security proxy, the preference or metric can influence which route to which tunnel is active. For more information, see [Associate an IP SLA Monitor Object with a Static Route](#).

- a. In Appliance view, select the Configuration tab in the top menu bar.
- b. Select Networking  > Virtual Routers in the left menu bar
- c. Select a virtual router instance.
- d. In the Edit VR popup window, select the Static Routing tab.
- e. Select the IPv4/IPv6 Unicast tab in the horizontal menu bar.
- f. Click the  Add icon to add a static route to associate with the monitor object. If you are adding an IP SLA monitor to an existing static route, click the address of the static route in the Destination column.



Best Practices for Performance-Based Breakout

SaaS application monitoring has many configuration options. Your SaaS application may not work for the basic measurement based on ICMP, as shown in this example, and for best results you may to ture the SaaS application monitor.

DNS proxy and web proxy may interfere with the functioning of the SaaS application, so check the following sections to understand the roles of these two types of proxies. If the functioning is affected, enhance the configuration with DNS proxy (always recommended) and web proxy chaining (required when you use a centralized web proxy).

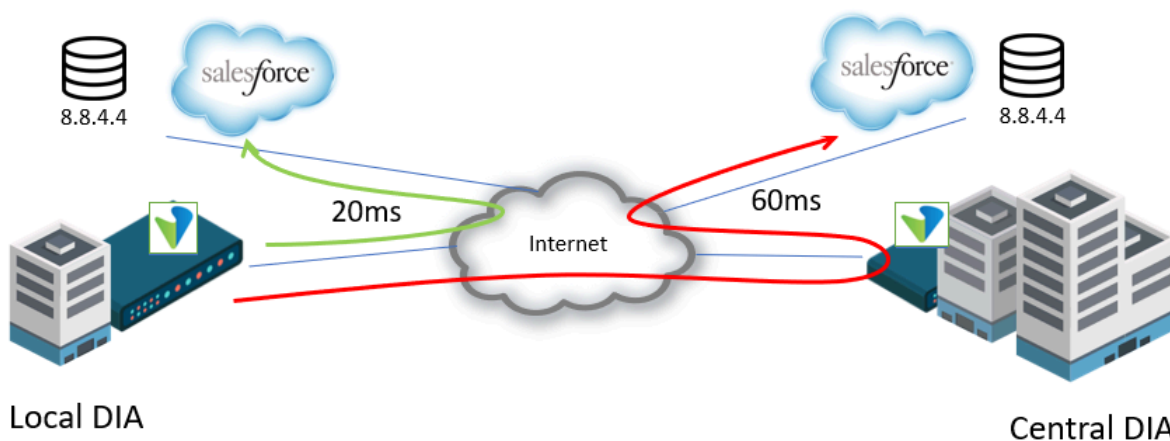
Note that the you can optimize the SaaS applications listed in the SaaS application group list. Applications that are not listed cannot leverage the performance-based breakout functionality.

DNS Proxy in Breakout Scenarios

The end-user application experience may depend on where the application breaks out from. For example, suppose a globally deployed enterprise SD-WAN VPN uses a local internet breakout in Hong Kong and a central breakout in London. The end users use an internal DNS server in London. If a user in Hong Kong does a DNS query for

Salesforce.com from the London DNS server, the query likely fetches the IP address of the London-based instance of Salesforce.com. However, in Hong Kong there is also an instance of the Salesforce.com SaaS. If the network decides to breakout in Hong Kong for Salesforce.com, it must query the Hong Kong DNS server to receive the IP address of the local instance. This scenario requires a DNS proxy. The configuration in this section shows that a local DNS proxy policy rule matches Salesforce.com, and based on where in the network the policy decides that the best breakout point is, that DNS server is used. The DNS server might be the Google DNS server in Hong Kong or the Google DNS server in London.

The following shows that internal metrics report a better performance, measured hereby latency, to the local SaaS. This local SaaS can be contacted only if the local instance of the global DNS service (here, the Google DNS server in Hong Kong) is used. If the remote global DNS is used, the pointer is to the remote SaaS. In that case, traffic still breaks out locally, but it follows the internet to get to the remote SaaS.




DNS Proxy Configuration


The DNS proxy configuration described here is an extension to the use case described in [Performance-Based SaaS Optimization](#).

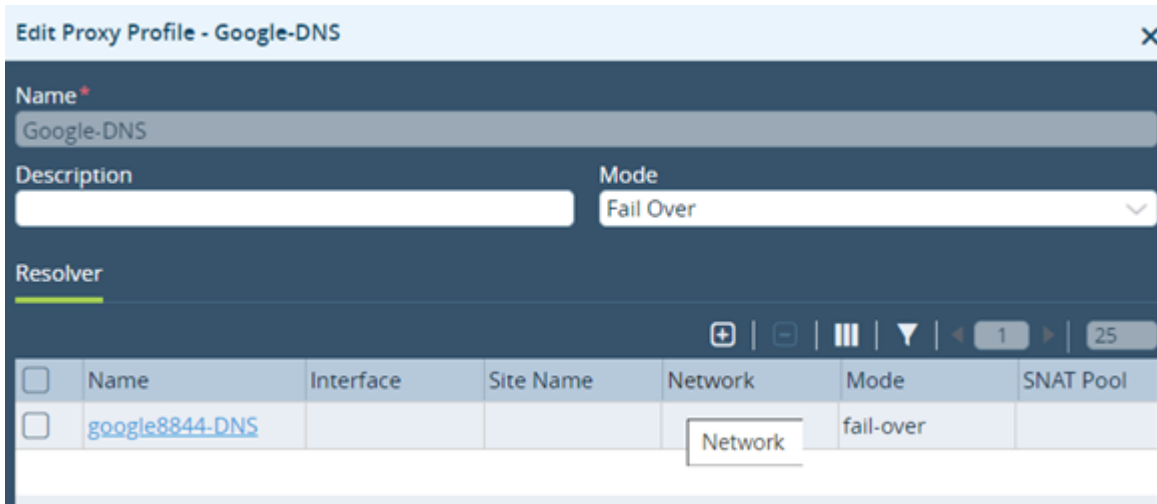
You configure the DNS proxy only on the local DIA edge device. No additional configuration is required on the central DIA edge device.

For performance-based SaaS optimization, you must use the DNS server of the local ISP or a global DNS provider, such as a Google DNS server. This configuration example uses the Google DNS server 8.8.4.4 for Salesforce.com.

To configure the DNS proxy:

1. Configure a DNS proxy profile. For more information, see [Configure DNS Proxy Profiles](#).
 - a. In Appliance view, select the Configuration tab in the top menu bar.
 - b. Select Networking  > DNS > Proxy Profiles in the left menu bar.

- c. Click the  Add icon, or select an existing proxy profile, as shown here. The Add Proxy Profile or Edit Proxy Profile popup window displays.
- d. In the Name field, enter a name for the DNS proxy profile. Here, the name is Google-DNS.




Edit Proxy Profile - Google-DNS

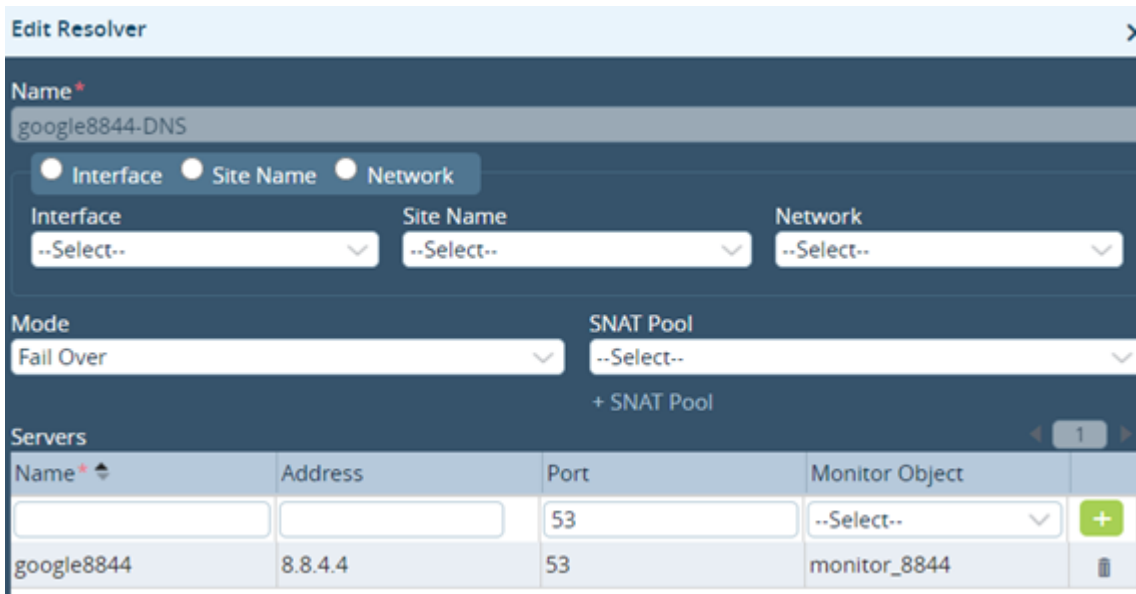
Name*
Google-DNS

Description Mode
Fail Over

Resolver

Name	Interface	Site Name	Network	Mode	SNAT Pool
<input type="checkbox"/> google8844-DNS			Network	fail-over	

- e. Select the Resolver tab to configure a DNS resolver.
- f. Click the  Add icon, or select an existing DNS resolver, as shown here. The Add Resolver or Edit Resolver popup window displays.



Edit Resolver

Name*
google8844-DNS

☒ Interface ☐ Site Name ☐ Network

Interface Site Name Network
--Select-- --Select-- --Select--

Mode SNAT Pool
Fail Over --Select--
+ SNAT Pool


Servers

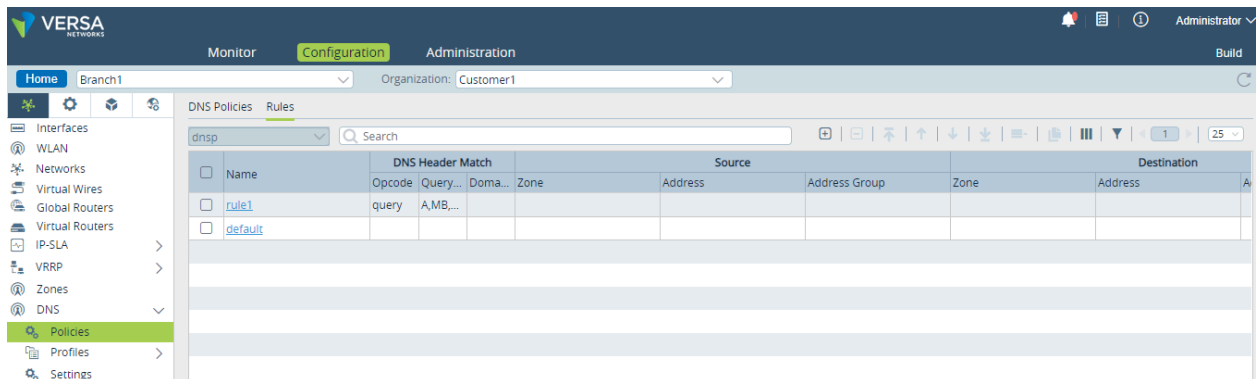
Name*	Address	Port	Monitor Object
<input type="text"/>	<input type="text"/>	53	--Select--
google8844	8.8.4.4	53	monitor_8844


It is recommended that you monitor the reachability of the configured DNS server. If the DNS server is not reachable, the monitor fails, the DNS proxy stops forwarding DNS queries to that DNS server, and instead, the DNS server configured on the client is used. Because the DNS server is dynamically assigned, for this example, only the specification of the DNS server is relevant. This example chooses to monitor the

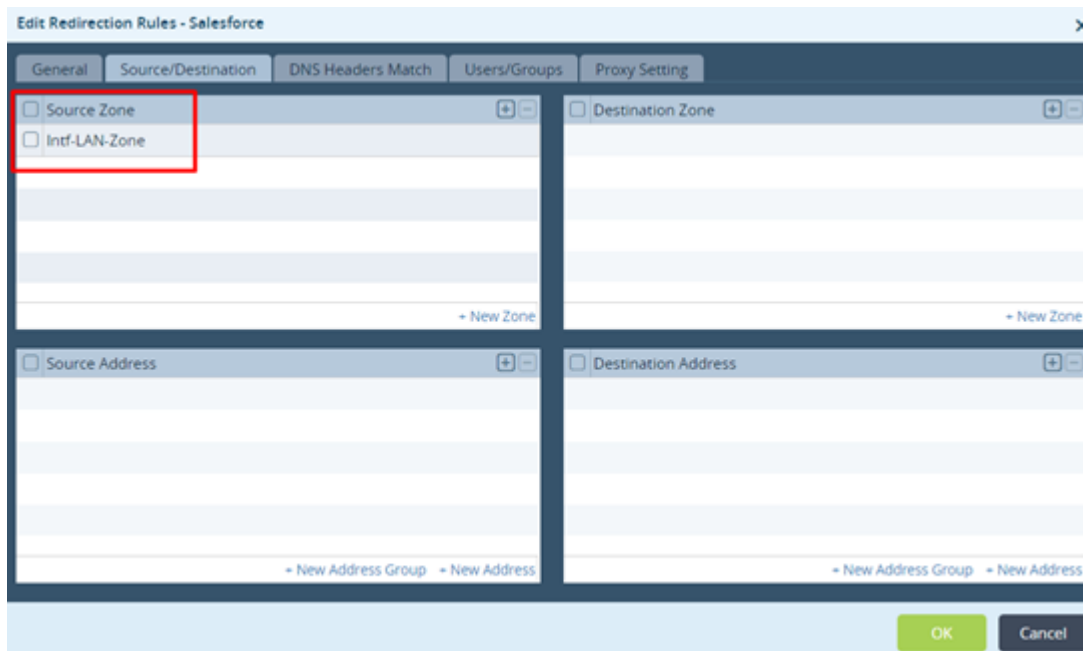
reachability of the DNS server by applying an IP SLA monitoring object. If the DNS server is not reachable, this DNS profile is not used, thus avoiding the potential blackholing of DNS queries.

2. Configure DNS proxy policy rule to specify matching conditions, that is, where the DNS query originates from and to which FQDN it applies). For more information, see [Configure DNS Redirection Rules](#).

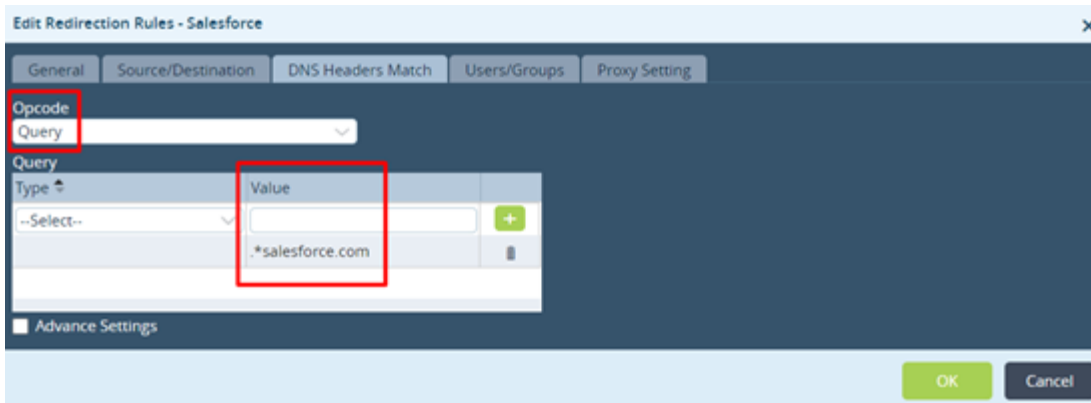
- a. In Appliance view, select the Configuration tab in the top menu bar.
- b. Select Networking  > DNS > Policies in the left menu bar.
- c. Select the Rules tab in the horizontal menu.



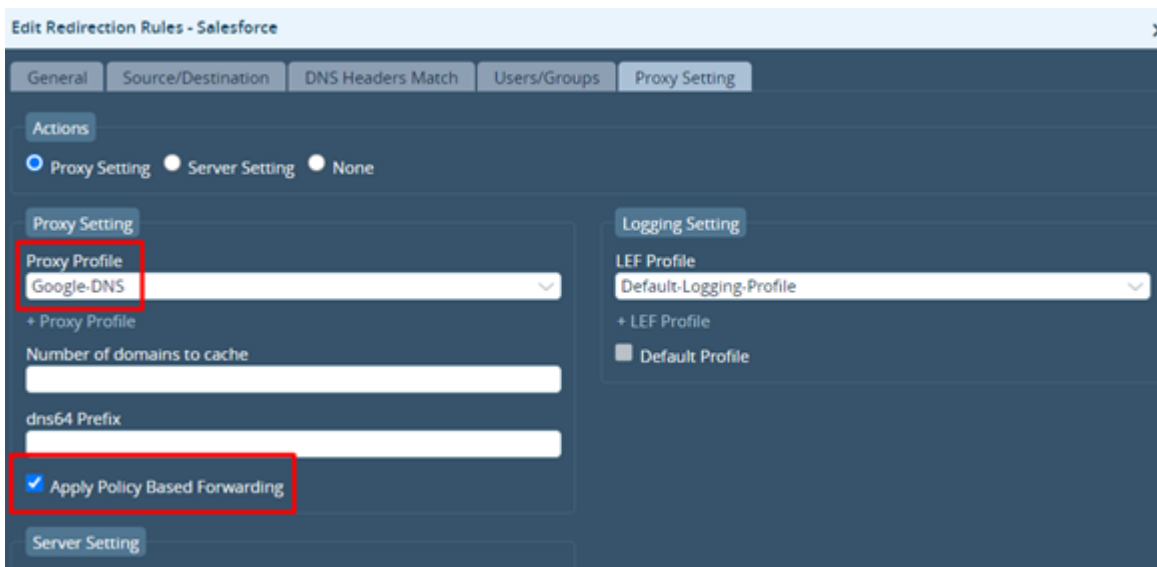
- d. Click the  Add icon. The Add Redirection Rules popup window displays.
- e. Select the Source/Destination tab, and in the Source Zone table, select the source zone.



- f. Select the DNS Headers Match tab and enter the following information:



- g. In the Opcode field, select the value Query.
- h. In the Query Value field, select the FQDN regex notation. The exact value of regex notation is important. Because we want the query for be for all traffic designated to the Salesforce.com domain, use the regex notation "*.salesforce.com".
- i. Select the Proxy setting tab.



- j. In the Actions field, click Proxy Setting.
- k. In the Proxy Profile field, select the proxy profile you created in Step 1, here, Google-DNS.
- l. Click Apply Policy-Based Forwarding. This setting enables the looking up of SD-WAN policies to ensure that the SaaS application breaks out to the best performing DIA. If you do not select this option, the DNS server 8.8.4.4 is used, but the egress interface is now DTVI-0/51, which is the overlay tunnel to the gateway. You can also verify whether the proxy, here, follows the routing table to get to the specified DNS server. Because the SD-WAN policy may dynamically decide whether the break out is local or central, the DNS proxy must follow that decision.
- m. In the LEF Profile field, select the log profile to use, which is useful when you want to verify DNS queries.

3. Click OK.

To verify the DNS proxy configuration:

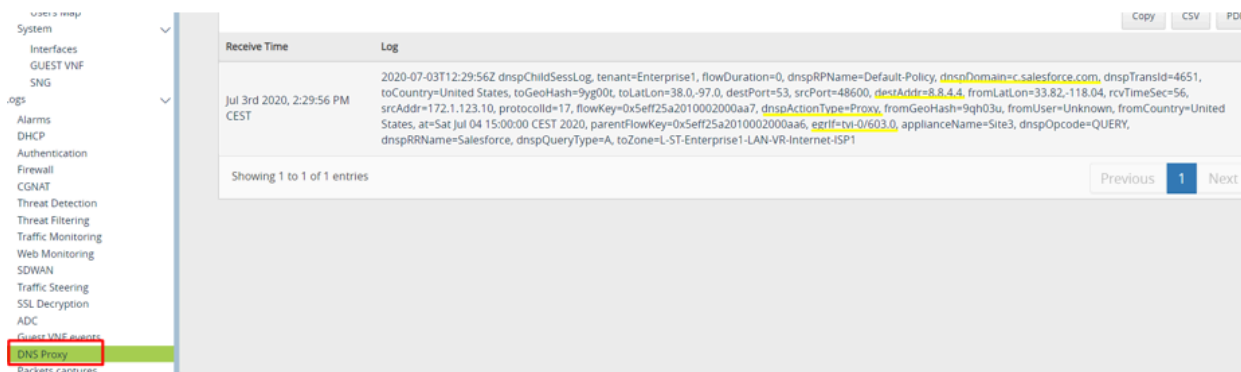
1. To verify that the current path to Salesforce.com is the best performing path, issue the following CLI command:

```
admin@Site3-cli> show orgs org-services Enterprise1 sd-wan policies Default-Policy rules nexthop
application-monitor detail
```

MONITOR	NEXTHOP	NEXTHOP	APPLICATION	APPLICATION	APPLICATION	APPL
NAME	PRIORITY	NAME	STATUS	ACTIVE	COUNT	NAME
LATENCY	LOSS					TYPE
Salesforce_best_DIA	1	Local_WAN	up	yes	79	salesforce icmp 326.42 0.0
	1	remote_WAN	up	-	108	salesforce icmp 398.2 0.0

The output shows that the path to Salesforce.com from the local breakout has the lowest latency (326 ms compared to 398 ms) and is the active path.

2. To verify that the configuration is functioning correctly and that the DNS query is sent to the Google DNS server from the local DIA:
 - a. Select Analytics > Home > Logs > DNS Proxy.



- b. Zoom in to view details:

The output above shows that for salesforce.com, the DNS server 8.8.4.4 is used (the default DNS for the client is an enterprise internal DNS) and that the egress interface is TVI-0/603, which is the internal interface for DIA. (Check the dnspDomain, destPort, destAddr, and egrIf fields in the output.) You can also verify the DIA interface by issuing the **show interface brief** CLI command.

3. To whether the local DIA might be impaired and so the central DIA is preferred, issue the following CLI command:

```
admin@Site3-cli> show orgs org-services Enterprise1 sd-wan policies Default-Policy rules nexthop
application-monitor detail
```

MONITOR	NEXTHOP	NEXTHOP	APPLICATION	APPLICATION	APPLICATION	APPL
NAME	PRIORITY	NAME	STATUS	ACTIVE	COUNT	NAME
LATENCY	LOSS					TYPE
Salesforce_best_DIA	1	Local_WAN	up	-	191	salesforce icmp 329.41 0.0

In Analytics, you can display the details:

This verification shows that the DNS server 8.8.4.4 is used, but the egress interface is now DTVI-0/51, which is the overlay tunnel to the gateway. You can also verify the DIA interface by issuing the **show interface dynamic tunnels** CLI command.

Best Practices for DNS Proxy

The configuration example here describes how the SD-WAN network can dynamically intercept the client DNS query and forwards the query to the DIA point that provides the best SaaS performance. The example shows the minimum configuration required for this use case to work.

One can image more advanced uses of DNS proxy. For example, enterprises often use their own internal DNS server. You might configure a global DNS external service, such as Google DNS, and an internal DNS for the IP endpoints, but you prefer local breakout to a global external DNS. For this type of scenarios, a DNS proxy provides a solution, intercepting DNS traffic for the internal domain (based on the internal FQDN) and having the rest of the traffic be served by the global external DNS.

Security Services for Internet Breakout

Traditionally, enterprises follow strict security policies to connect LANs to the internet. In legacy networks, in which internet access is typically provided from a centralized internet breakout, you can easily enforce security at one location. A centralized stack of firewall services, often acting as web proxy, inspect the traffic coming from or going to the internet against enterprise security policies. However, now, with the introduction of local internet breakout services, you must ensure that enterprise security policies do not change, because you still want to scrub internet-bound traffic.

The following list summarizes some of the security scenarios observed in the field:

- There is no additional security at local internet breakout. Rather, you rely on NAT to secure the enterprise LAN. This is an unsecured strategy, and there are no controls to monitor or mitigate compromised networks.
- Security policies are enforced through a nearby cloud security proxy of a third-party cloud security provider. This is a secure alternative, but costly cloud security proxy services may not always be provided locally, and this can result in less than optimal application experiences for end users.
- Security policies are enforced through a third-party firewall, and all internet-bound local breakout traffic is scrubbed by that firewall. In the case of the Versa Networks solution, this third-party firewall is typically virtualized as a guest VM on a Versa uCPE. This is a secure method, but it is complex to manage, and you have to manage the lifecycle of the security solution separately.
- Security policies are enforced using the Versa networks next-generation firewall (NGFW) with unified threat management (UTM) features.





Enterprise security administrators may also make risk assessments about which types of application to break out locally, without performing a full stack inspection. If you do local internet breakout for a particular application, for example, Office 365, and you break out all other internet traffic centrally, Microsoft claims that the Office 365 service is extremely secure.

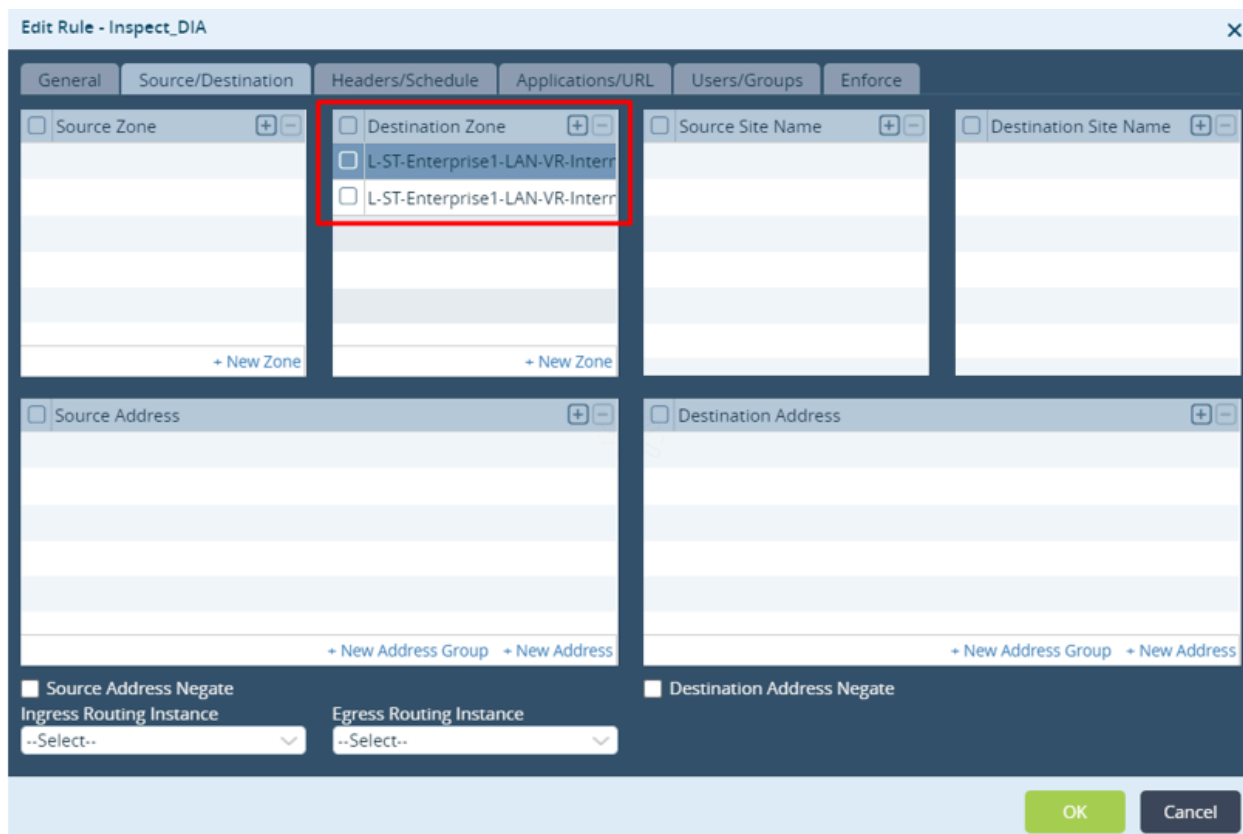
(Microsoft claims that full-stack security is performed on their applications.) For performance reasons they suggest that you not enforce additional security policies, and that if you adopt this suggestion, you do not need to implement additional security services.

For any breakout to the internet, Versa Networks recommends that you deploy, at a minimum, IDS/IPS with the Versa-recommended profile and antivirus. These two features ensures that all traffic from untrusted networks is inspected, regardless of whether the application provider claims to be secure. Note that you must also implement SSL decryption at the branch to effectively investigate the SSL stream.

The following example shows how to configure NGFW security for DIA traffic. In this scenario, for all firewall policy rules that have an allow rule and that apply to an internet-bound application, and therefore are logically are broken out to the internet, you must attach a UTM security profile to the firewall policy rule.

To configure NGFW security for DIA traffic, configure the NGFW access policy rule:

1. In Appliance view, select the Configuration tab in the top menu bar.
2. Select Services  > Next Gen Firewall  > Security > Policies  in the left menu bar, and select the Rules tab.
3. Click the  Add icon to define rules for the policy, or select an existing rule, as shown here.
4. Select the Source/Destination tab:



5. In the Destination Zone table, select *L-ST-organization-name-VR-WAN-name* as the destination zone. In this example, there are two local internet breakout points, so you must select the matching zone for both. You can leave all other matching criteria blank.
6. Select the Enforce tab:

The screenshot shows the 'Edit Rule - Inspect_DIA' window with the 'Enforce' tab active. The 'Actions' section has 'Apply Security Profile' selected. The 'Log' section has 'End' selected for events and 'Default Profile' selected for the profile. The 'Profiles' section has 'Anti-Virus' and 'Vulnerability' checked, with 'Scan Web and Email Traffic' and 'Versa Recommended Profile' selected respectively. The 'Packet Capture' section is also visible.

7. In the Actions field, click Apply Security Profile.
8. In the Log field, click Default Profile.
9. Click Antivirus and select an option. Here, the option selected is Scan Web and Email Traffic.
10. Click Vulnerability and select an option. Here, the option selected is Versa Recommended Profile, which performs malware inspection using the VOS antivirus module and IDS/IPS using the VOS vulnerability module.
11. Click OK.

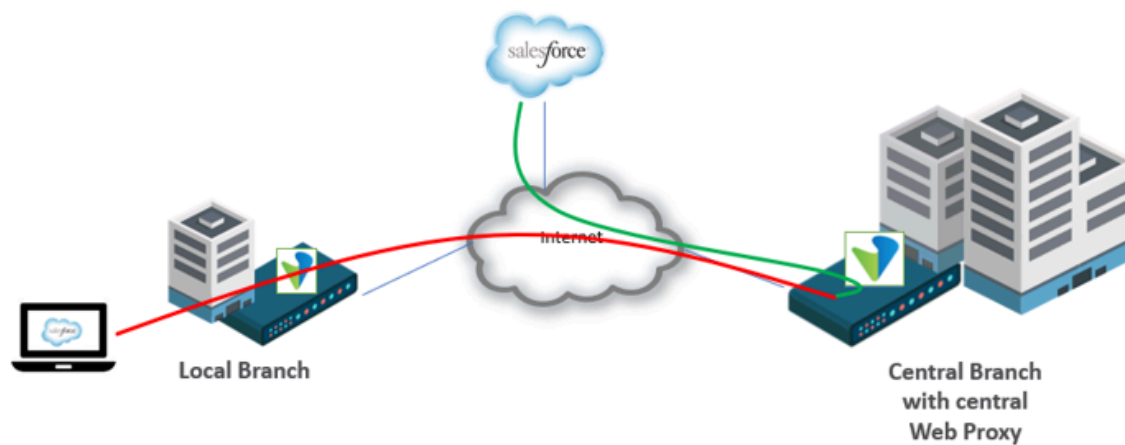
Web Proxies with Different Breakout Services

Using web proxies to provide enterprise security for internet access is a common use case and a best practice. Using web proxies provides you with more control over the traffic that goes to the internet, because the web proxy inspects all the internet-bound traffic. Another benefit is that with web proxies, you do not have to announce a default route in the

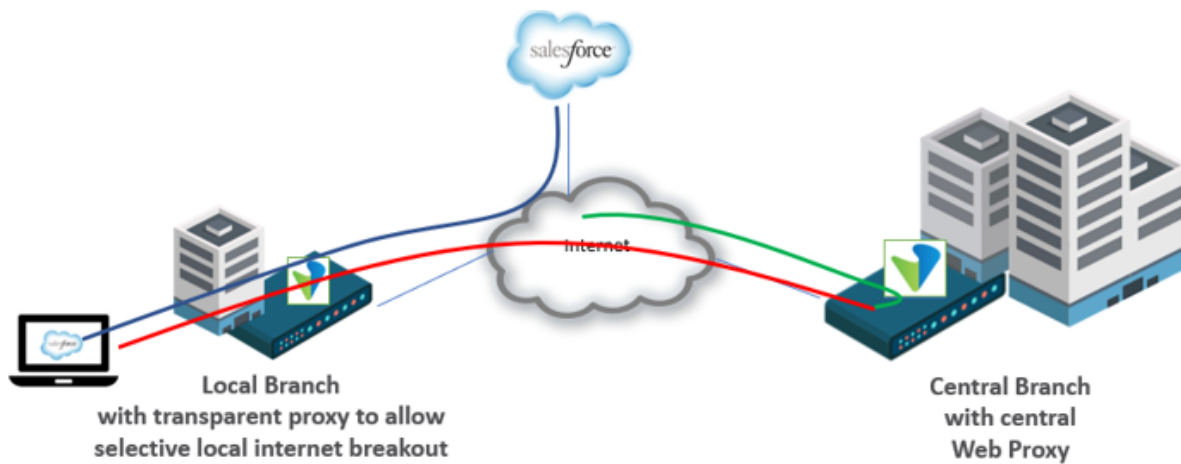
enterprise LAN. Instead, endpoints reach the internet by connecting to the proxy server, as specified in the endpoint configuration and a proxy autoconfiguration (PAC) file.

However, if you prefer to leverage quality-of-experience improvements for specific SaaS applications, as discussed in DNS proxy section, above, you must intercept the connection to the centralized proxy service to allow local internet breakout. The local DIA point must intercept the proxy session and act as an alternative web proxy dynamically, without modifying the endpoint proxy configuration.

The following figure shows how the Versa VOS edge device software can function as web proxy. Alternatively, you can use an existing third-party web proxy at the central location. However, it becomes difficult for the local branch to do a local internet breakout, because the client configuration includes an explicit central web proxy endpoint. The VOS web proxy software web proxy addresses this scenario.

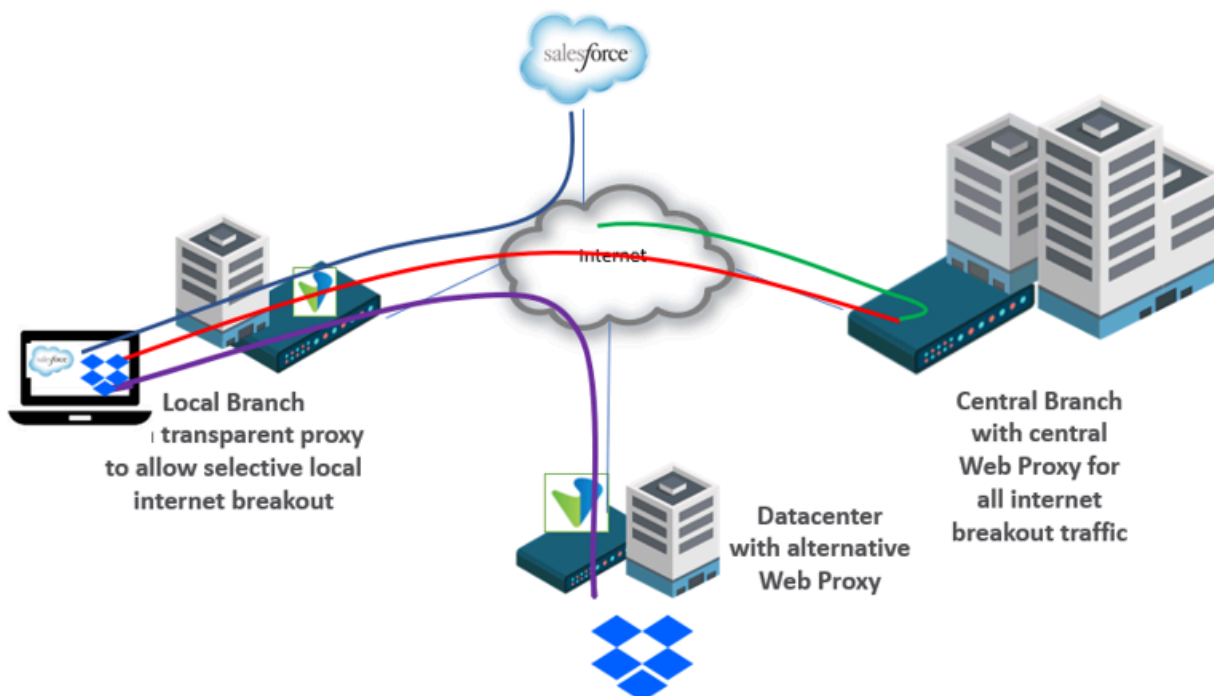


In the following figure, the local branch is configured to provide local DIA only for Salesforce.com. Because the client computer, by default, sends all HTTPS traffic to the central explicit web proxy, the local branch monitors the explicit proxy port number for queries to Salesforce.com. When it detects these queries, the local branch can use a transparent web proxy to break out to the internet and then forward the traffic to internet. You must also configure the DNS proxy feature so that DNS queries to Salesforce.com are intercepted.



A more advanced use case is to use multiple web proxies. In addition to redirecting local internet breakout for specific SaaS traffic, using multiple web proxies allows you to redirect specific traffic to an alternative proxy service, a process that is called proxy chaining.

The following figure shows that the VOS edge devices in the data center and in the central branch are both configured for explicit web proxy. The client in the local branch is configured with a proxy in the central branch. However, the local branch can break out Salesforce.com directly to the internet and can proxy-chain dropbox.com traffic to the data center branch. You use DNS proxy configurations to select the correct DNS server.



Supported Software Information

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

Additional Information

[Configure Basic Features](#)

[Configure Direct Breakout to the Internet](#)

[Configure DNS Proxy Profiles](#)

[Configure DNS Redirection Rules](#)

[Configure IP SLA Monitor Objects](#)

[Configure SaaS Application Monitoring](#)

[Configure SD-WAN Traffic Steering](#)

[Configure SLA Profiles for SD-WAN Traffic Steering](#)

[Configure Virtual Routers](#)

[Performance-Based SaaS Optimization](#)

[SD-WAN Gateway Use Cases](#)

[VOS Edge Device DIA Architecture and Best Practices](#)