Oracle® SD-WAN Aware

Features Guide

Release 4.3

Jan 2020

Oracle SD-WAN Aware Features Guide, Release 4.3

Contents

About This Guide

The purpose of this document is to describe features for all incremental releases of Oracle SD-WAN Edge.

Documentation Set

This table lists related documentation.

Document Name	Document Description
Oracle SD-WAN Aware Installation and Upgrade Guide	Contains information about installing and configuring Oracle SD-WAN Aware.
Oracle SD-WAN Aware Release Notes	Contains information about added features, resolved issues, requirements for use, and known issues in the latest Oracle SD-WAN Aware release.
Oracle SD-WAN Security Guide	Contains information about security methods within the Oracle SD-WAN solution.
Oracle SD-WAN Aware Features Guide	Collects feature descriptions and procedures for all incremental releases of this product. This guide is organized by release version.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.
   - For non-technical issues such as registration or assistance with My Oracle Support, select `2`.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Click the **Oracle Communications** link.
   Under the **SD-WAN** header, select a product.
4. Select the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Revision History

This section provides a revision history for this document

Date	Description
January 2020	• Initial release

1

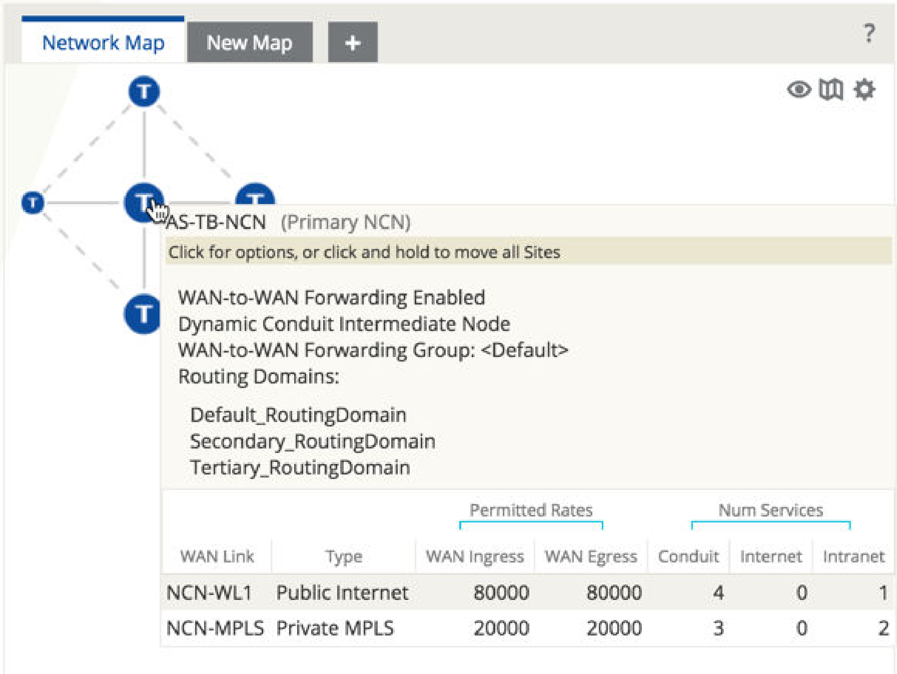
Release 2.0 Features

This chapter includes features and enhancements released in 2.0.

Virtual Routing and Forwarding (VRF)

Oracle SD-WAN Edge 5.0 introduces Virtual Routing and Forwarding (VRF) which gives network administrators tools to segment their networks to separate different types of network traffic, create and manage distinct routing domains, support and manage multiple tenants at Client Sites, and segment network traffic to support multiple networks. In Oracle SD-WAN Aware 2.0 Network Maps you can hover over a Site to view site elements including the Routing Domain.

> **Note:**
>
> Only the first eight Routing Domains will be displayed for a site. If more than eight Routing Domains are configured at a site, to see the full list click **More**.



AS-TB-NCN (Primary NCN)

Click for options, or click and hold to move all Sites

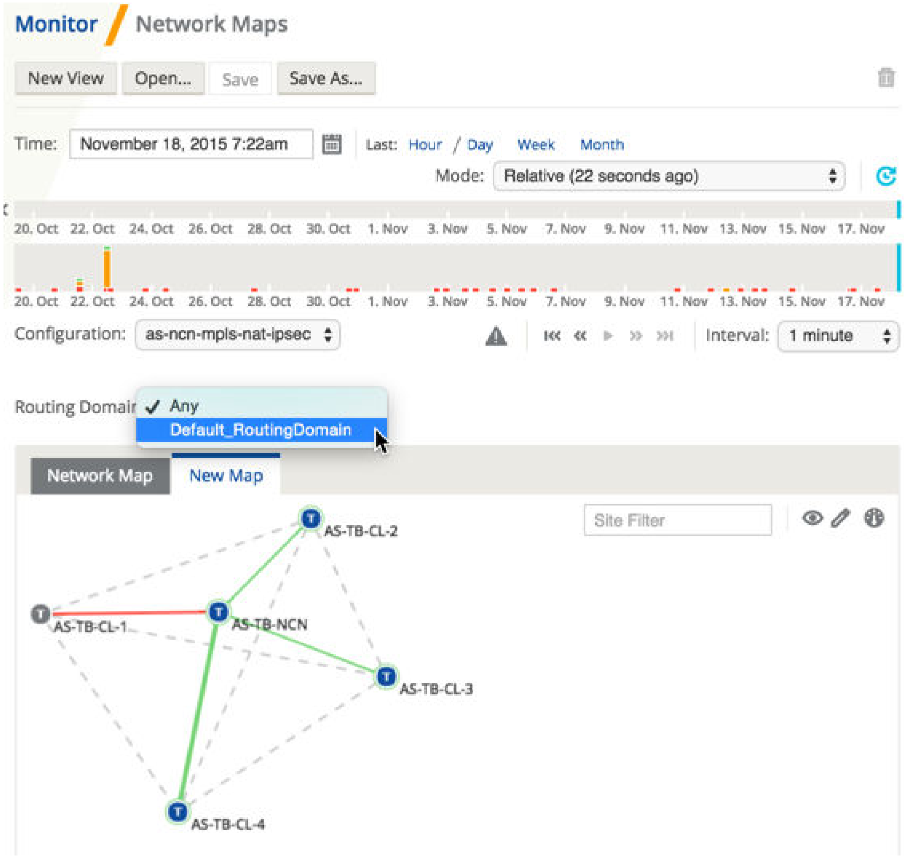
WAN-to-WAN Forwarding Enabled
Dynamic Conduit Intermediate Node
WAN-to-WAN Forwarding Group: <Default>
Routing Domains:

Default_RoutingDomain
Secondary_RoutingDomain
Tertiary_RoutingDomain

		Permitted Rates		Num Services		
WAN Link	Type	WAN Ingress	WAN Egress	Conduit	Internet	Intranet
NCN-WL1	Public Internet	80000	80000	4	0	1
NCN-MPLS	Private MPLS	20000	20000	3	0	2

Figure 1: Network Map Elements Including Routing Domains

From the **Monitor**, and then **Network Maps** screen you can click on the **Routing Domain** drop-down menu to filter the Sites displayed by Routing Domain.



Time: November 18, 2015 7:22am

Mode: Relative (22 seconds ago)

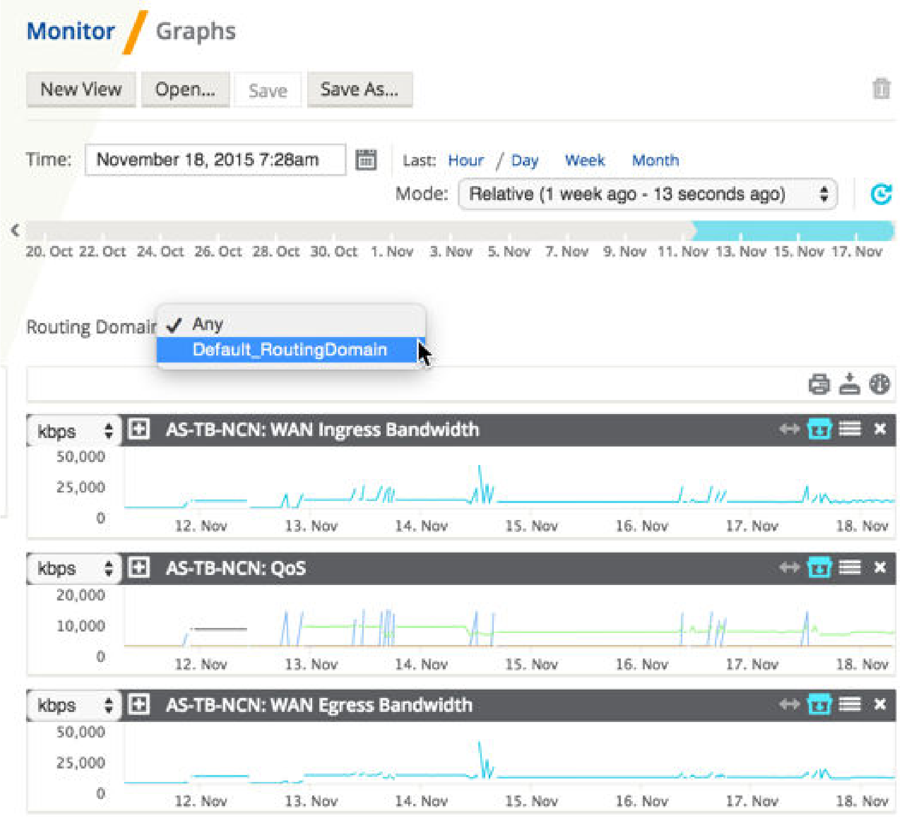
Configuration: as-ncn-mpls-nat-ipsec

Interval: 1 minute

Routing Domain: ✓ Any
Default_RoutingDomain

Figure 2: Network App Elements Filtered by Routing Domain

From the **Monitor**, and then **Graphs** screen you can click on the **Routing Domain** drop-down menu to filter the objects and properties displayed by Routing Domain. Sites not in the selected Routing Domain will be hidden in the tree.



Monitor / Graphs

Time: November 18, 2015 7:28am

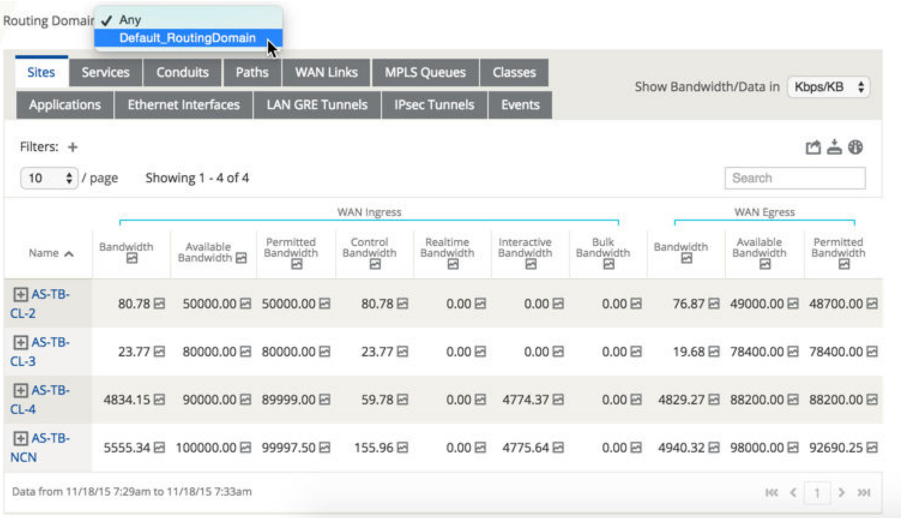
Mode: Relative (1 week ago - 13 seconds ago)

Routing Domain: ✓ Any / Default_RoutingDomain

New View
Open...
Save
Save As...
Last: Hour / Day Week Month
20. Oct 22. Oct 24. Oct 26. Oct 28. Oct 30. Oct 1. Nov 3. Nov 5. Nov 7. Nov 9. Nov 11. Nov 13. Nov 15. Nov 17. Nov
kbps
AS-TB-NCN: WAN Ingress Bandwidth
50,000
25,000
0
12. Nov 13. Nov 14. Nov 15. Nov 16. Nov 17. Nov 18. Nov
kbps
AS-TB-NCN: QoS
20,000
10,000
0
12. Nov 13. Nov 14. Nov 15. Nov 16. Nov 17. Nov 18. Nov
kbps
AS-TB-NCN: WAN Egress Bandwidth
50,000
25,000
0
12. Nov 13. Nov 14. Nov 15. Nov 16. Nov 17. Nov 18. Nov

Figure 3: Graph Objects Filtered by Routing Domain

From the **Monitor**, and then **Reports** screen you can click on the **Routing Domain** drop-down menu to filter Reports displayed by Routing Domain.



Routing Domain: ✓ Any / Default_RoutingDomain

Show Bandwidth/Data in: Kbps/KB

10 / page Showing 1 - 4 of 4

	WAN Ingress							WAN Egress		
Name	Bandwidth	Available Bandwidth	Permitted Bandwidth	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Bulk Bandwidth	Bandwidth	Available Bandwidth	Permitted Bandwidth
AS-TB-CL-2	80.78	50000.00	50000.00	80.78	0.00	0.00	0.00	76.87	49000.00	48700.00
AS-TB-CL-3	23.77	80000.00	80000.00	23.77	0.00	0.00	0.00	19.68	78400.00	78400.00
AS-TB-CL-4	4834.15	90000.00	89999.00	59.78	0.00	4774.37	0.00	4829.27	88200.00	88200.00
AS-TB-NCN	5555.34	100000.00	99997.50	155.96	0.00	4775.64	0.00	4940.32	98000.00	92690.25

Data from 11/18/15 7:29am to 11/18/15 7:33am

Figure 4: Reports Filtered by Routing Domain

Cloud for Amazon Web Services

Oracle SD-WAN Aware 2.0 introduces Cloud Aware for Amazon Web Services (AWS). Cloud Aware allows network administrators to leverage the power and functionality of Aware in an

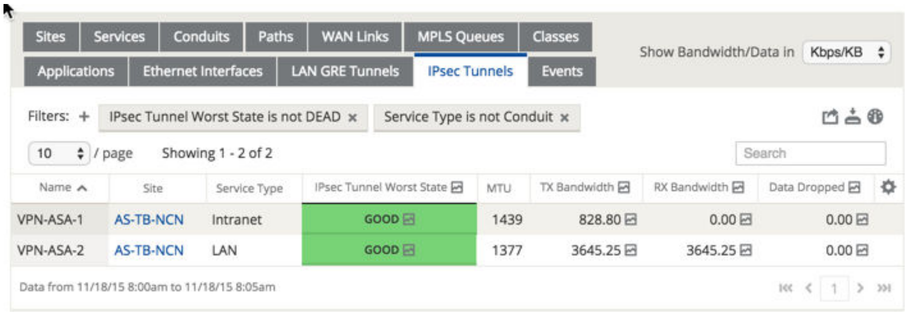
AWS cloud environment for business development. When you subscribe via an AWS subscription, a Cloud Aware instance runs on top of an existing AWS EC2 instance, and provides network administrators the ability to monitor and configure their Oracle WAN managed by that EC2 Instance.

IPSec Tunnel Monitoring

Oracle SD-WAN Edge 5.0 expanded on the IPsec Tunnel functionality introduced in Edge 4.4 by allowing third-party devices to terminate IPsec VPN Tunnels on the LAN or WAN side of Appliances. You can monitor those IPsec Tunnels using Aware 2.0 from the **IPsec Tunnels** tab of the **Monitor**, and then **Reports** screen. To refine the displayed report results, click on the Show/Hide Columns icon (⚙) and click the checkbox next to the attributes you prefer to display in the report.

The following data is displayed for each LAN GRE Tunnel:

- Name
- Site
- Service Type (e.g., Intranet, LAN, or Conduit)
- IPsec Tunnel Worst State
- MTU
- TX Bandwidth (i.e., Bandwidth Transmitted)
- TX Packets (i.e., Packets Transmitted)
- RX Bandwidth (i.e., Bandwidth Received)
- RX Packets (i.e., Packets Received)
- Data Dropped
- Packets Dropped



Show Bandwidth/Data in Kbps/KB

Filters: + IPsec Tunnel Worst State is not DEAD × Service Type is not Conduit ×

10 / page Showing 1 - 2 of 2 Search

Name	Site	Service Type	IPsec Tunnel Worst State	MTU	TX Bandwidth	RX Bandwidth	Data Dropped	⚙
VPN-ASA-1	AS-TB-NCN	Intranet	GOOD	1439	828.80	0.00	0.00	
VPN-ASA-2	AS-TB-NCN	LAN	GOOD	1377	3645.25	3645.25	0.00	

Data from 11/18/15 8:00am to 11/18/15 8:05am

Figure 5: IPsec Tunnel Report

To generate IPsec Tunnel graphs, go to **Monitor**, and then **Graphs** and under **[Site Name]**, and then **IPsec Tunnels**, and then **[IPsec Tunnel Name]** you can select from the following attributes:

- IPsec Tunnel Availability
- TX Bandwidth (i.e., Bandwidth Transmitted)
- RX Bandwidth (i.e., Bandwidth Received)
- Data Dropped
- Packets Dropped

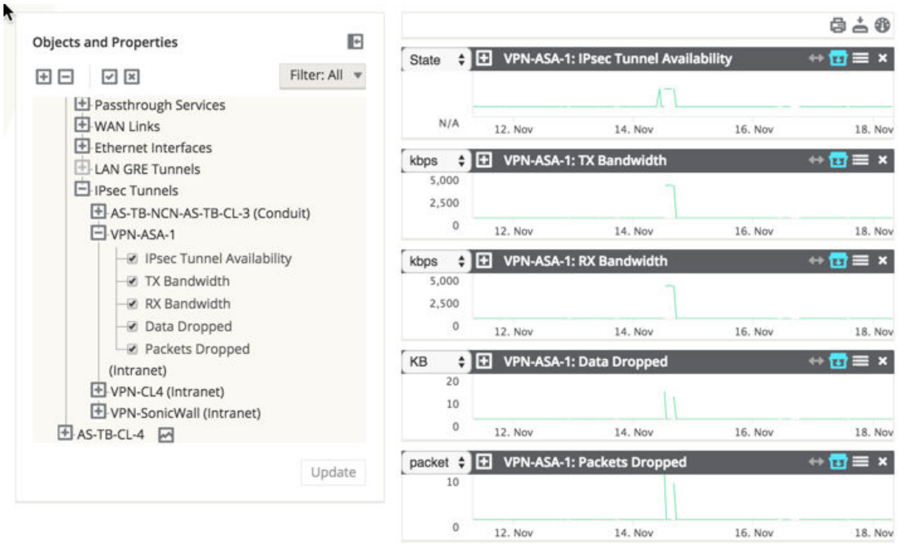


Figure 6: IPsec Tunnel Graphs

2

Release 2.1 Features

This chapter includes features and enhancements released in 2.0.

About This Product

Oracle APN

Some of the functionality described in this document is only supported for networks where *APN 5.1 GA* (or later) has been deployed. See *Oracle APN 5.1 GA Release Notes* and *Oracle Aware 2.1 GA Release Notes* for more details.

New Features in Oracle Aware 2.1

The following sections describe new features and enhancements delivered in Oracle Aware 2.1.

Oracle Virtual Appliance VT800 Support

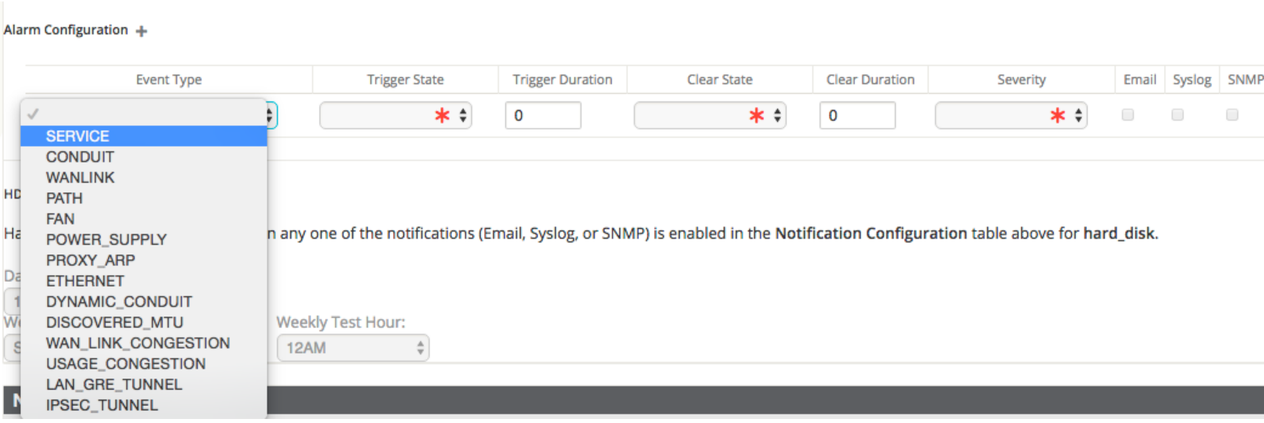
Aware 2.1 introduces support for the new Oracle Virtual Appliance VT800. This new virtual appliance supports different performance levels depending on how it is licensed. The VT800 supports up to 200 Mbps of full-duplex performance, 8 Public WAN Links, 32 Private WAN Links, and scales higher than the VT500 to support more Conduits, Paths, and tunnels. Aware 2.1 provides the same configuration, monitoring, reporting, security and diagnostic capabilities for the VT800 that it provides for the VT500.

Alarm System

APN 5.1 introduces a new Alarm System that streamlines the configuration and number of severity-based alerts for network administrators. Aware 2.1 allows you to configure and push Alarm configurations to Appliances.

To configure an Alarm:

1. Under **Manage**, and then **APN Appliance Settings**, click the **Include in File** checkbox in the **Notification Settings** area of the page.
2. Scroll down to the **Alarm Configuration** area and click the + to add a new alarm.
3. Choose an **Event Type** from the drop-down menu.

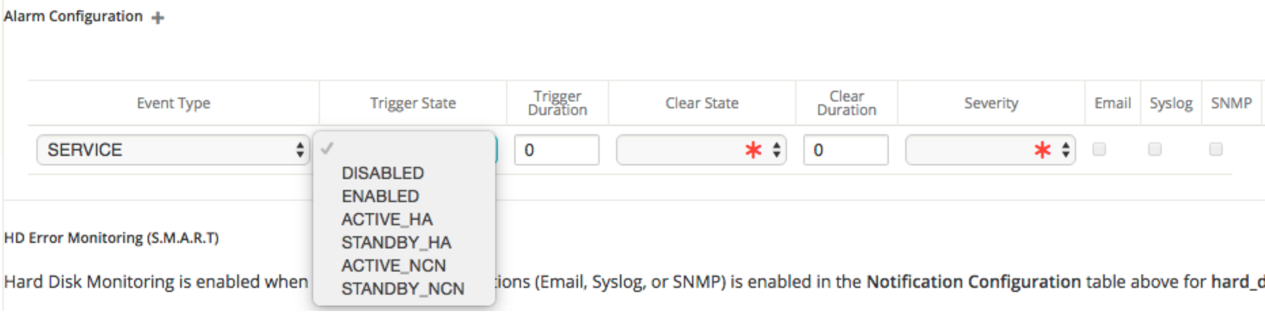


Trigger Duration	Clear Duration
0	0

Ha n any one of the notifications (Email, Syslog, or SNMP) is enabled in the **Notification Configuration** table above for **hard_disk**.

Figure 1: Select Event Type

1. Choose a **Trigger State** from the drop-down menu. When the Event Type enters this state an Alarm is triggered. The options available on the Trigger State drop-down menu are determined by the Event Type.



Event Type	Trigger Duration	Clear Duration
SERVICE	0	0

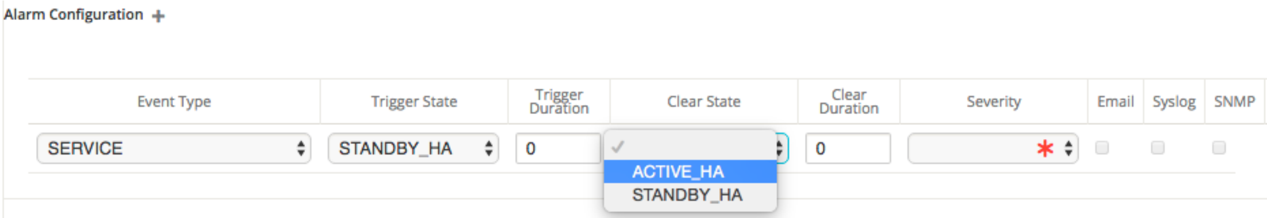
Hard Disk Monitoring is enabled when ions (Email, Syslog, or SNMP) is enabled in the **Notification Configuration** table above for **hard_d**

Figure 2: Select Trigger State

1. Enter the amount of time (in seconds) in the **Trigger Duration** field that the Event Type must remain in the Trigger State to trigger the Alarm. The default is 0 seconds, which would trigger the alarm immediately.

> **Note:**
>
> The Trigger Duration field is not available for some Event Types.

1. Choose a **Clear State** from the drop-down menu. When the Event Type enters this state the existing Alarm is cleared. The options available on the Clear State drop-down menu are determined by the Trigger State.



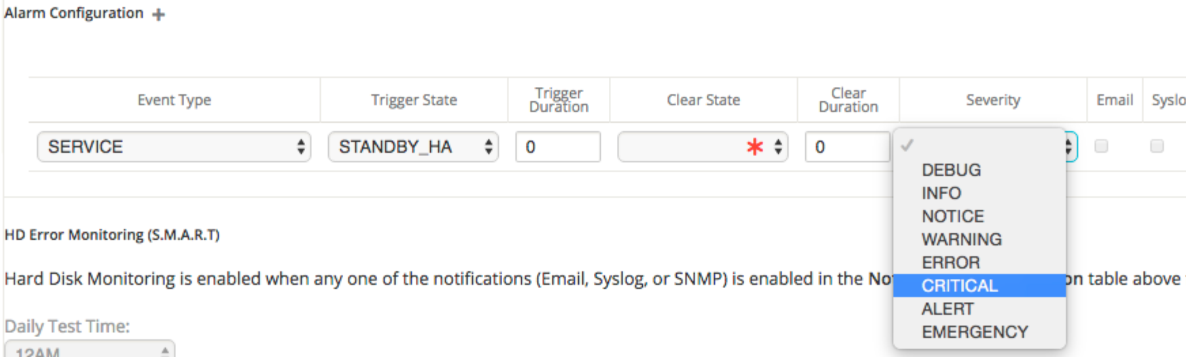
Event Type	Trigger State	Trigger Duration	Clear Duration
SERVICE	STANDBY_HA	0	0

Figure 3: Select a Clear State

1. Enter the amount of time (in seconds) in the **Clear Duration** field that the Event Type must remain in the Clear State to trigger the Alarm. The default is 0 seconds, which would clear the alarm immediately.

> **Note:**
>
> The Clear Duration field is not available for some Event Types.

1. Choose a **Severity** from the drop-down menu based on the urgency of the alarm. The Severity is displayed in the alert that is sent out when the Alarm is triggered and cleared.



Alarm Configuration +

Event Type	Trigger State	Trigger Duration	Clear State	Clear Duration	Severity	Email	Syslo
SERVICE	STANDBY_HA	0	*	0		□	□

HD Error Monitoring (S.M.A.R.T)

Hard Disk Monitoring is enabled when any one of the notifications (Email, Syslog, or SNMP) is enabled in the No on table above

Daily Test Time:

12AM

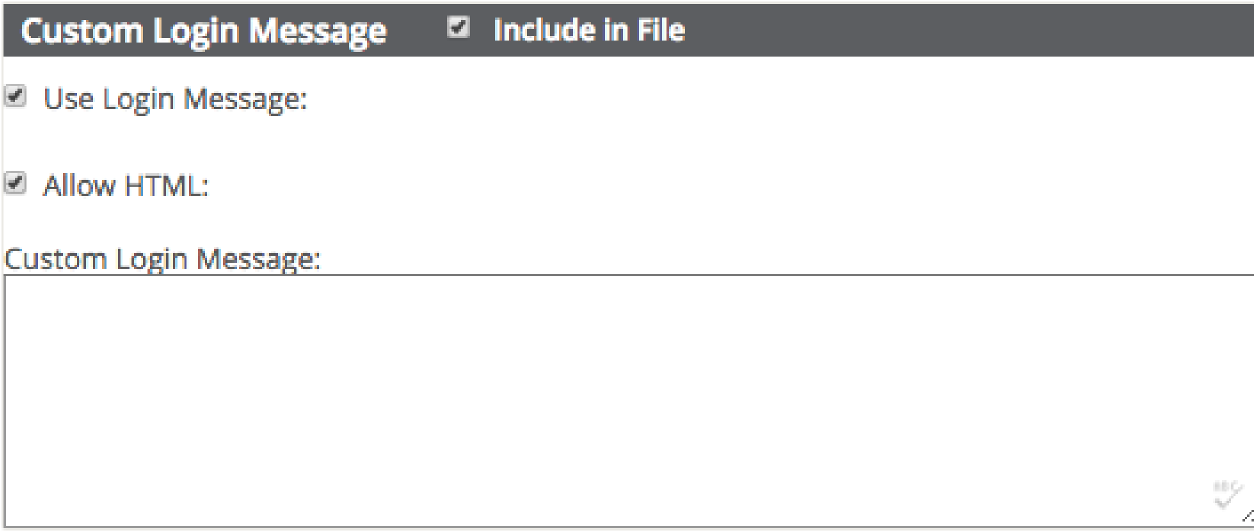
Figure 4: Choose a Severity

1. Select the alert delivery method by clicking the **Email**, **Syslog**, and **SNMP** checkboxes. You can select multiple delivery methods.
2. Repeat steps 1 through 1 to add additional Alarms.
3. Scroll to the top of the page and click **Save** to save the Alarm to the APN Appliance Settings file that is currently open, or click **Save As** to save it to a new Appliance Settings file.
4. Click the **Export…** button to export the Appliance Settings file with the alarm(s) you configured to appliances on your Oracle WAN or to download the file to your local machine.

Customizable Web Console

Aware 2.1 lets you customize the look and feel of your Appliance's Web Console. Network administrators can add a Custom Login Message, a Custom Support Link, and Upload a Custom Logo to brand their Appliances' web interfaces, and push these settings to the appliances directly from Aware.

From the **Manage**, and then **APN Appliance Settings** screen**,** click the **Include in File** checkbox in the **Custom Login Message** area. Click the **Use Login Message** checkbox and enter a message to appear on the login page for appliance users. Click the **Allow HTML** box to format and style your message with HTML.



Custom Login Message ☑ Include in File

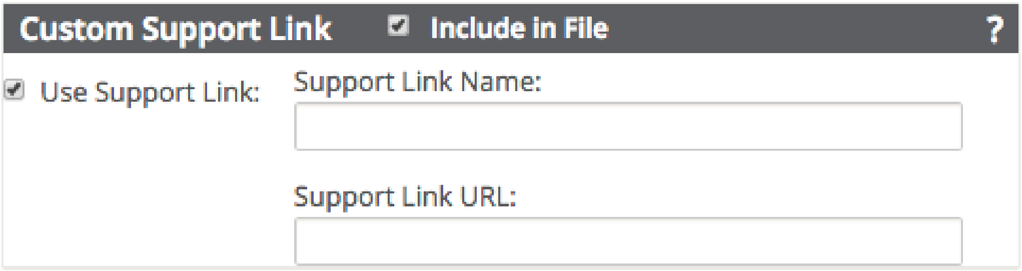
☑ Use Login Message:

☑ Allow HTML:

Custom Login Message:

Figure 5: Custom Login Message

In the **Custom Support Link** area of the **APN Appliance Settings** screen, click the **Include in File** checkbox. Enter a **Support Link Name** and your organization's **Support Link URL** to create a link on the appliance login page.



Custom Support Link ☑ Include in File ?

☑ Use Support Link:

Support Link Name:

Support Link URL:

Figure 6: Custom Support URL

From the **Upload Custom Logo** area of the **APN Appliance Settings** screen, you can upload a logo to replace the Oracle logo on your appliance. Click the **Include in File** checkbox, and then click the **Browse** button, choose the logo image you want to upload. Click **Upload** to save the image to Aware.

Note:

The Custom Logo must be an image file (.png, .jpg, or .gif) that is 167px wide and 72px high.

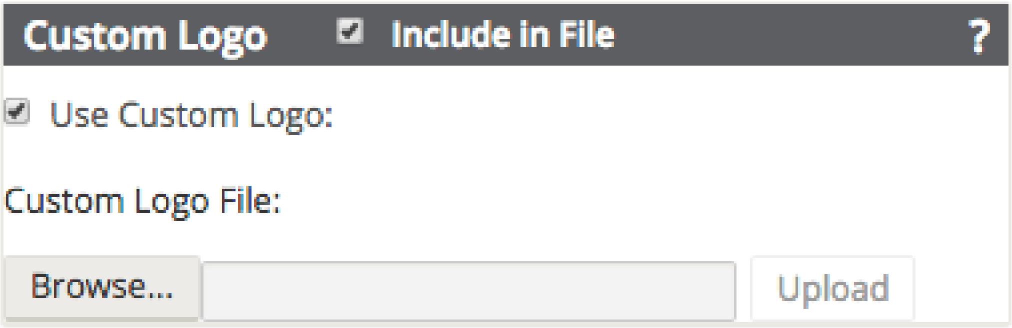
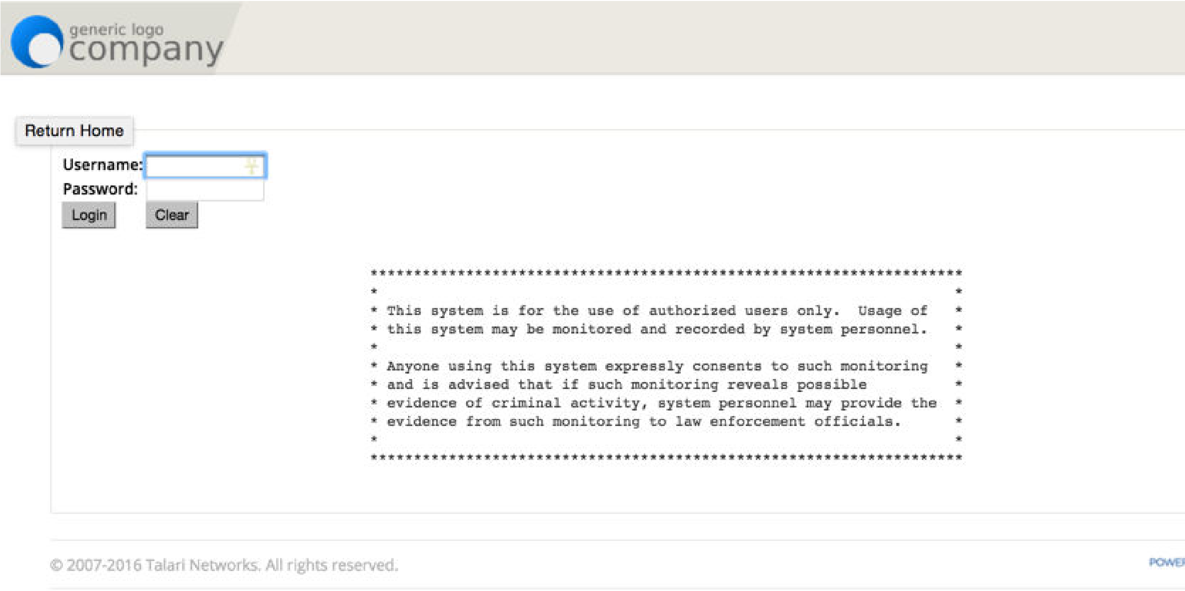


Figure 7: Custom Logo

When you are done, click **Save** to save the Alarm to the APN Appliance Settings file that is currently open, or click **Save As** to save it to a new Appliance Settings file. Click the **Export…** button to export the Appliance Settings file with the Custom Login Message, Custom Support Link, and Custom Logo you configured to appliances on your Oracle WAN or to download the file to your local machine.

Here is an example of the login screen of a Appliance with a Custom Logo and Custom Login Message.



```
**********************************************************************
*                                                                    *
* This system is for the use of authorized users only.  Usage of    *
* this system may be monitored and recorded by system personnel.    *
*                                                                    *
* Anyone using this system expressly consents to such monitoring    *
* and is advised that if such monitoring reveals possible           *
* evidence of criminal activity, system personnel may provide the   *
* evidence from such monitoring to law enforcement officials.       *
*                                                                    *
**********************************************************************
```

© 2007-2016 Talari Networks. All rights reserved.

Figure 8: Customized Web Console

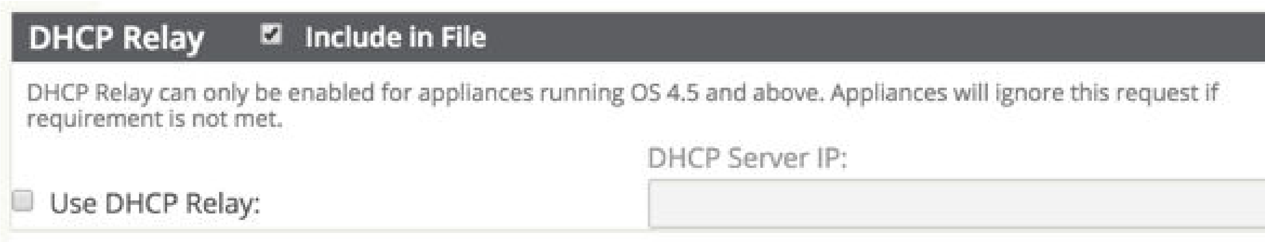
DHCP Relay

Network administrators can use the DHCP Relay service on the management port of Appliances to relay requests and replies between local DHCP Clients and a remote DHCP Server. This allows local hosts to acquire dynamic IP addresses from the remote DHCP Server. For a more in-depth explanation of DHCP Relay, please refer to *Using Appliances as DHCP Relay Agents*.

From the **Manage**, and then **APN Appliance Settings** screen you can configure **DHCP Relay** and push these settings directly to Appliances. Click the **Include in File** checkbox, and then click the **Use DHCP Relay** checkbox to enable the service. Enter the **DHCP Server IP**.

Note:

If you plan to use DHCP Relay on a Appliance configured for High Availability (HA), do not configure the service on both the Active and Standby appliance. Doing so will lead to duplicate IP addresses on the defined management network.



DHCP Relay ☑ Include in File

DHCP Relay can only be enabled for appliances running OS 4.5 and above. Appliances will ignore this request if requirement is not met.

☐ Use DHCP Relay:

DHCP Server IP:

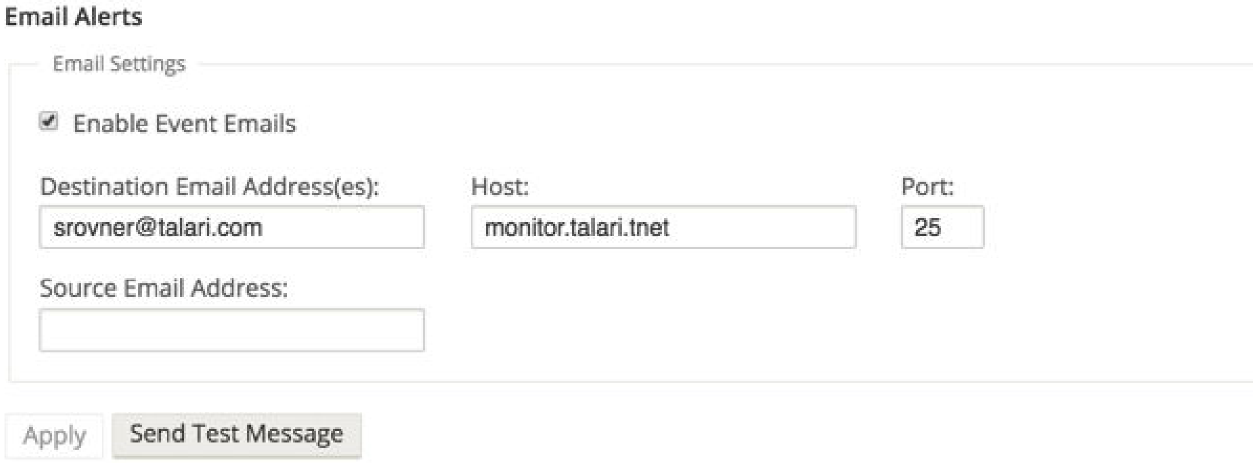
Figure 9: Enable DHCP Relay

When you are done, click **Save** to save the Alarm to the APN Appliance Settings file that is currently open, or click **Save As** to save it to a new Appliance Settings file. Click the **Export…** button to export the Appliance Settings file with the DHCP Relay you configured to appliances on your Oracle WAN or to download the file to your local machine.

Notification Enhancements

The following notification enhancements were introduced on the **Manage**, and then **Notifications** screen in Aware 2.1:

- Email alerts can be sent to multiple **Destination Email Address(es)**.
- The **Source Email Address** is now configurable.



Email Alerts

Email Settings

☑ Enable Event Emails

Destination Email Address(es): srovner@talari.com

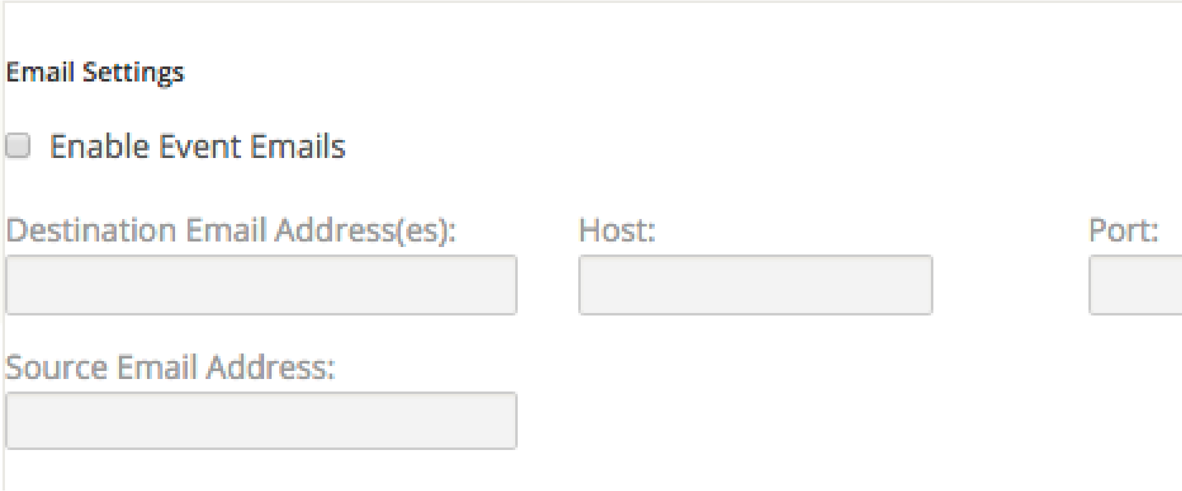
Host: monitor.talari.tnet

Port: 25

Source Email Address:

The following notification enhancements were introduced on the **Manage**, and then **APN Appliance Settings** screen in Aware 2.1:

- Email alerts can be sent to multiple **Destination Email Address(es)**.
- The **Source Email Address** is now configurable.
- Help Text for the **General Event Configuration** was added to clarify alert functionality.



Email Settings

☐ Enable Event Emails

Destination Email Address(es):

Host:

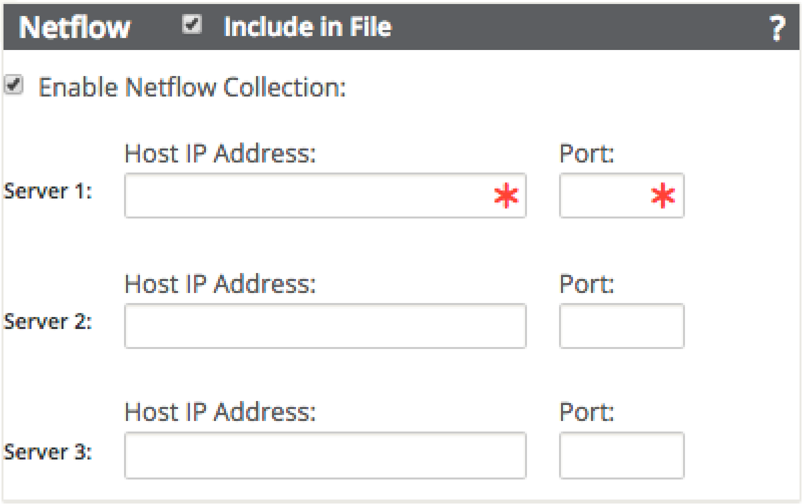
Port:

Source Email Address:

Figure 10: Configure Email Alerts

Multiple Netflow Collectors

Aware 2.1 allows you to configure multiple Netflow Hosts and push these settings directly to Appliances. From the **Manage**, and then **APN Appliance Settings** screen, click the **Include in File** checkbox. Click the **Enable Netflow Collection** checkbox, and enter the **IP Address** and **Port** numbers for up to three Netflow Hosts.



Netflow ☑ Include in File ?

☑ Enable Netflow Collection:

Server 1: Host IP Address: * Port: *

Server 2: Host IP Address: Port:

Server 3: Host IP Address: Port:

Figure 11: Multiple Netflow Hosts

When you are done, click **Save** to save the Alarm to the APN Appliance Settings file that is currently open, or click **Save As** to save it to a new Appliance Settings file. Click the **Export…** button to export the Appliance Settings file with the Netflow Host(s) you configured to appliances on your Oracle WAN or to download the file to your local machine.

Summary

Oracle's Aware 2.1 software introduces support for the new Oracle Virtual Appliance VT800, and the ability to configure and push Alarm configurations, DHCP Relay settings, Web Console Customizations, along with various other settings to Appliances throughout your network.

3

Oracle Aware 2.2 New Features Guide

About This Product

Oracle APN

Some of the functionality described in this document is only supported for networks where *APN 5.2 GA* (or later) has been deployed. See *Oracle APN 5.2 GA Release Notes* and *Oracle Aware 2.2 GA Release Notes* for more details.

New Features in Oracle Aware 2.2

The following sections describe new features and enhancements delivered in Oracle Aware 2.2.

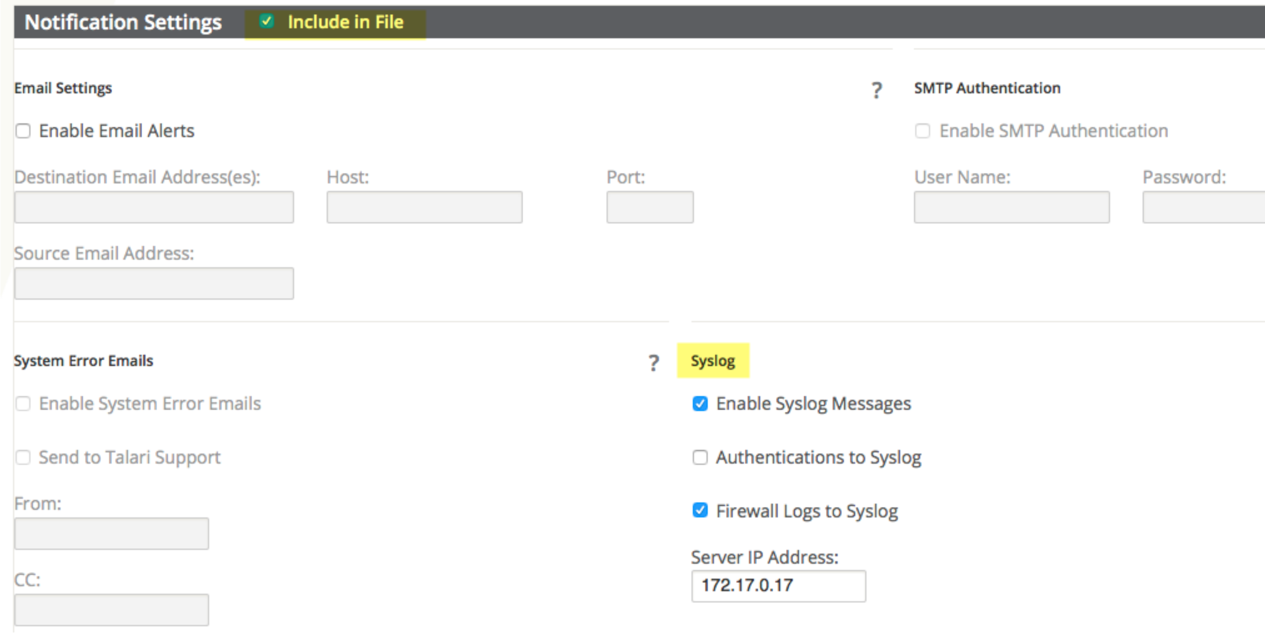
Support for 550 Sites

As APN 5.2 now supports the ability for a T5200, functioning as an NCN, to create up to 550 static Conduits. In turn, Aware 2.2 also has the capability to poll as many as 550 APN Appliances.

Firewall Logs to Syslog

APN 5.2 provides a firewall built into the Oracle Application. The firewall allows Policies between Services and Zones, and supports Static NAT, Dynamic NAT (PAT), and Dynamic NAT with Port Forwarding. Additionally, using Aware R2.2 provides the user with the ability to log firewall connections and flow logs to an external syslog server.

To enable the Firewall Logs to Syslog Feature, navigate to **Manage > APN Appliance Settings** and check the box that says **Include in File** in the **Notification Settings** section. Enable the feature and include the appropriate server IP address.



Notification Settings ☑ Include in File

Email Settings ?

□ Enable Email Alerts

Destination Email Address(es):

Host:

Port:

Source Email Address:

SMTP Authentication

□ Enable SMTP Authentication

User Name:

Password:

System Error Emails ?

□ Enable System Error Emails

□ Send to Talari Support

From:

CC:

Syslog

☑ Enable Syslog Messages

□ Authentications to Syslog

☑ Firewall Logs to Syslog

Server IP Address: 172.17.0.17

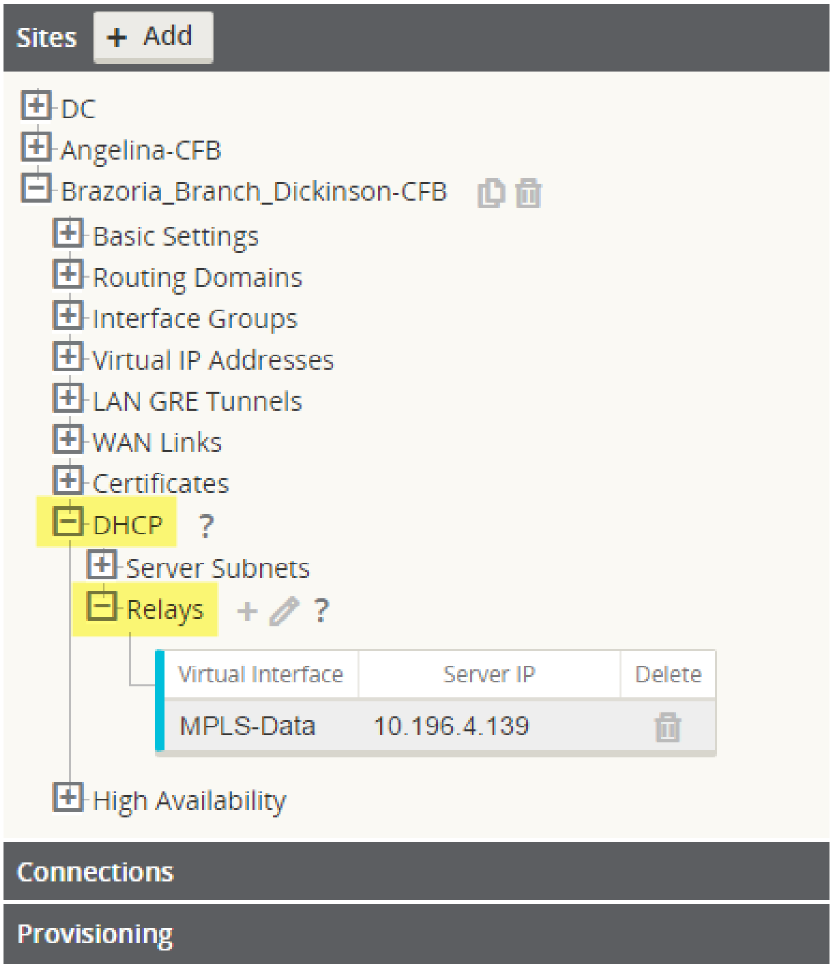
DHCP Relay & DHCP Server

As of APN 5.2, devices on the same network as the Appliance's LAN/VLAN interface may now use the Oracle DHCP Relay & DHCP Server features to provide those devices with their IP configuration. These features help to simplify the client site network by reducing the amount of equipment necessary. The configuration changes necessary to utilize this feature can be executed from the web UI of Aware 2.2 under **Manage > APN Configuration**.

DHCP Relay

Network administrators can now use the DHCP Relay service on data ports of Appliances to relay requests and replies between local DHCP Clients and a remote DHCP Server. This allows local hosts to acquire dynamic IP addresses from the remote DHCP Server.

To configure DHCP Relay, navigate to **Sites > [Site Name] > DHCP.** Expand **Relays** then specify the data ports to be used and the Server IP address.



Virtual Interface	Server IP	Delete
MPLS-Data	10.196.4.139	🗑

DHCP Server

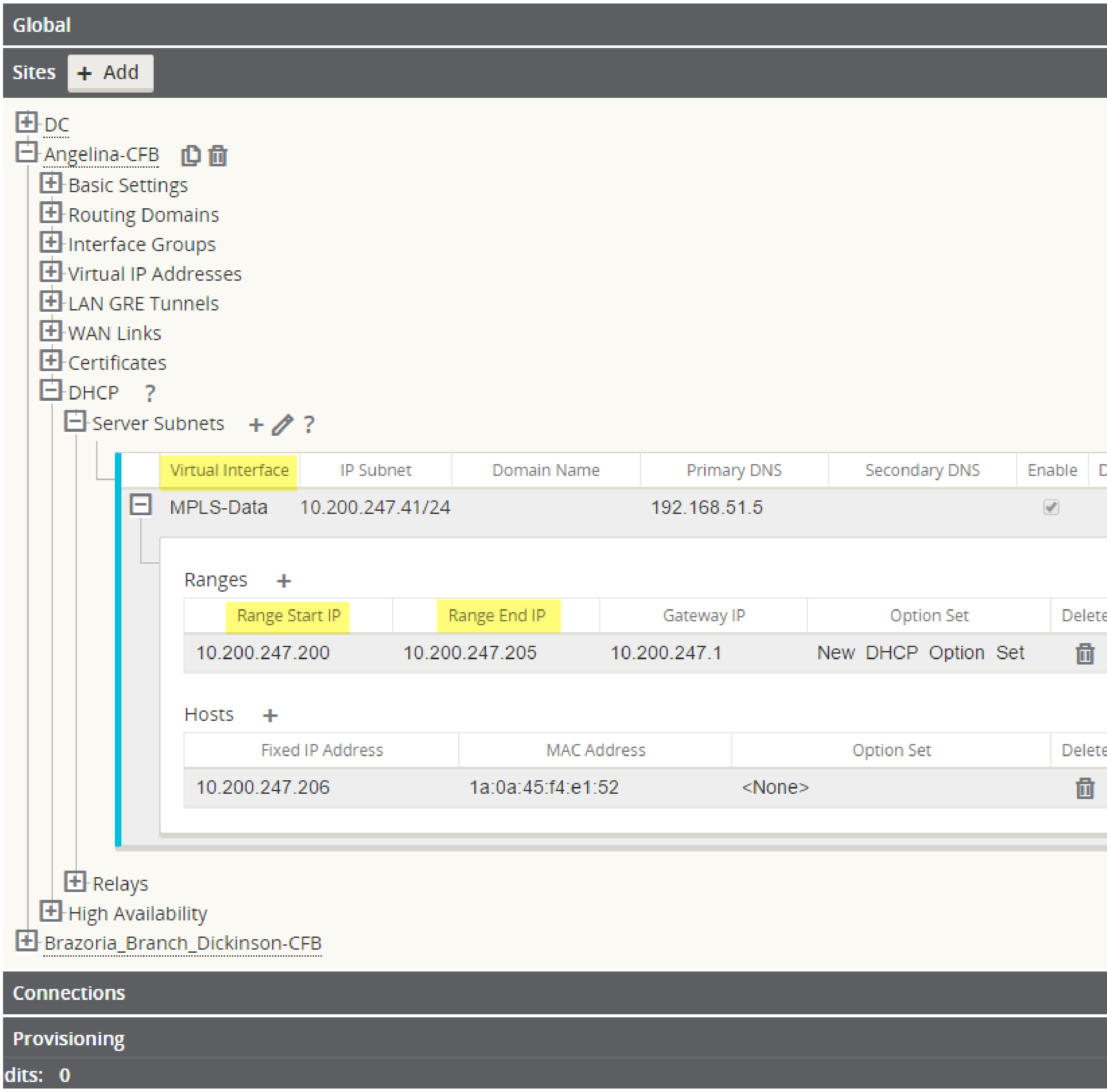
Network administrators can now also use the DHCP Server feature on data ports of Appliances to allow local hosts to acquire dynamic or static IP addressing directly from the Appliance.

To configure DHCP Server:

1. Navigate to **Sites** > **[Site Name]** > **DHCP** and expand **Server Subnets.**
2. Select the Virtual Interface to be used and specify the range of IP addresses allowed to be dynamically assigned to local hosts.

Users may also choose to enter additional information in this section that hosts will then be configured with as well, such as gateway IP, DNS, and an Option Set (described below).

The **Hosts** option of this drop down allows users to manually tie specific IP addresses to specific hosts via host MAC address if desired.



Virtual Interface	IP Subnet	Domain Name	Primary DNS	Secondary DNS	Enable	D
MPLS-Data	10.200.247.41/24		192.168.51.5		✓	

Ranges +

Range Start IP	Range End IP	Gateway IP	Option Set	Delete
10.200.247.200	10.200.247.205	10.200.247.1	New DHCP Option Set	🗑

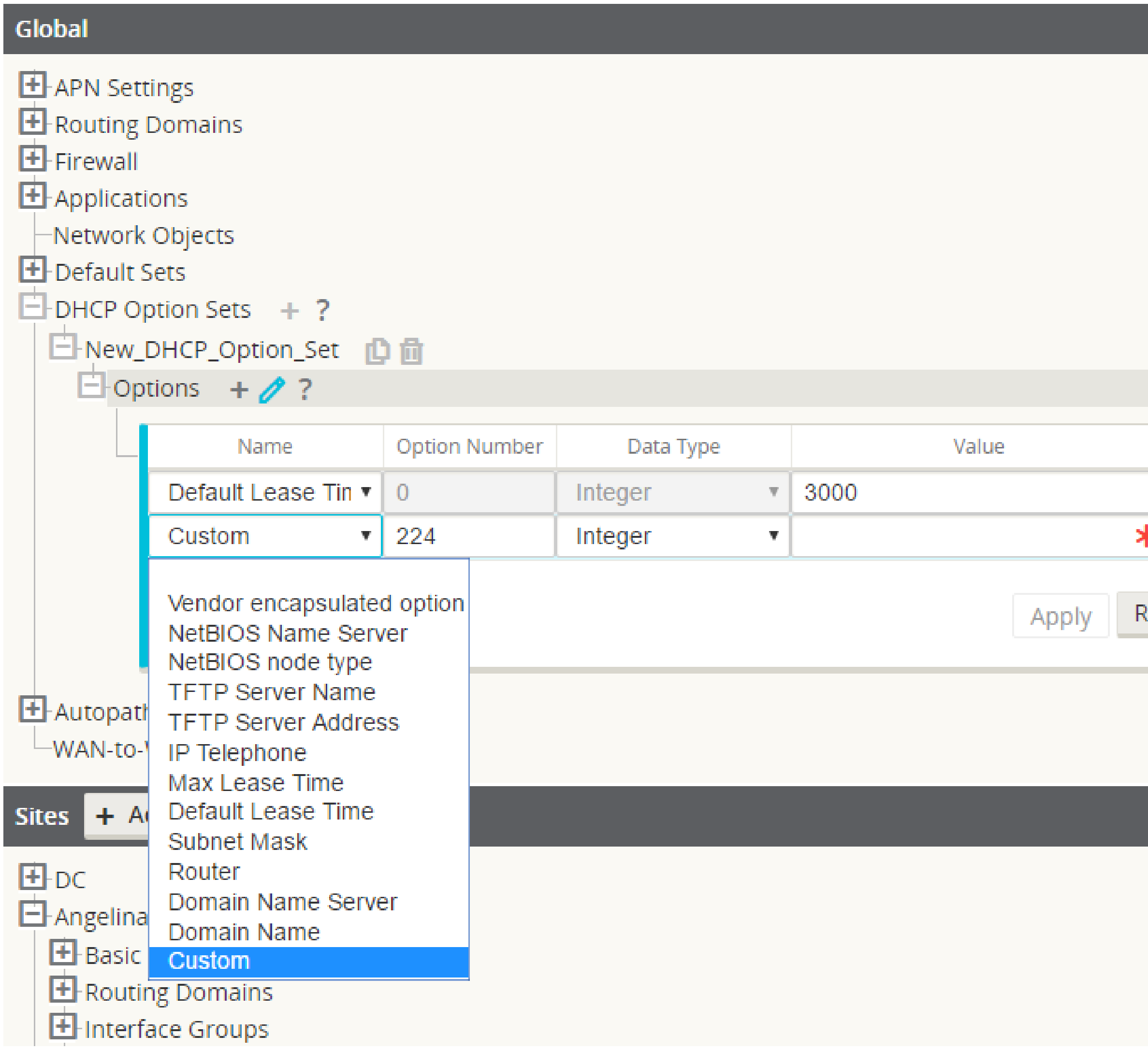
Hosts +

Fixed IP Address	MAC Address	Option Set	Delete
10.200.247.206	1a:0a:45:f4:e1:52	<None>	🗑

Note:

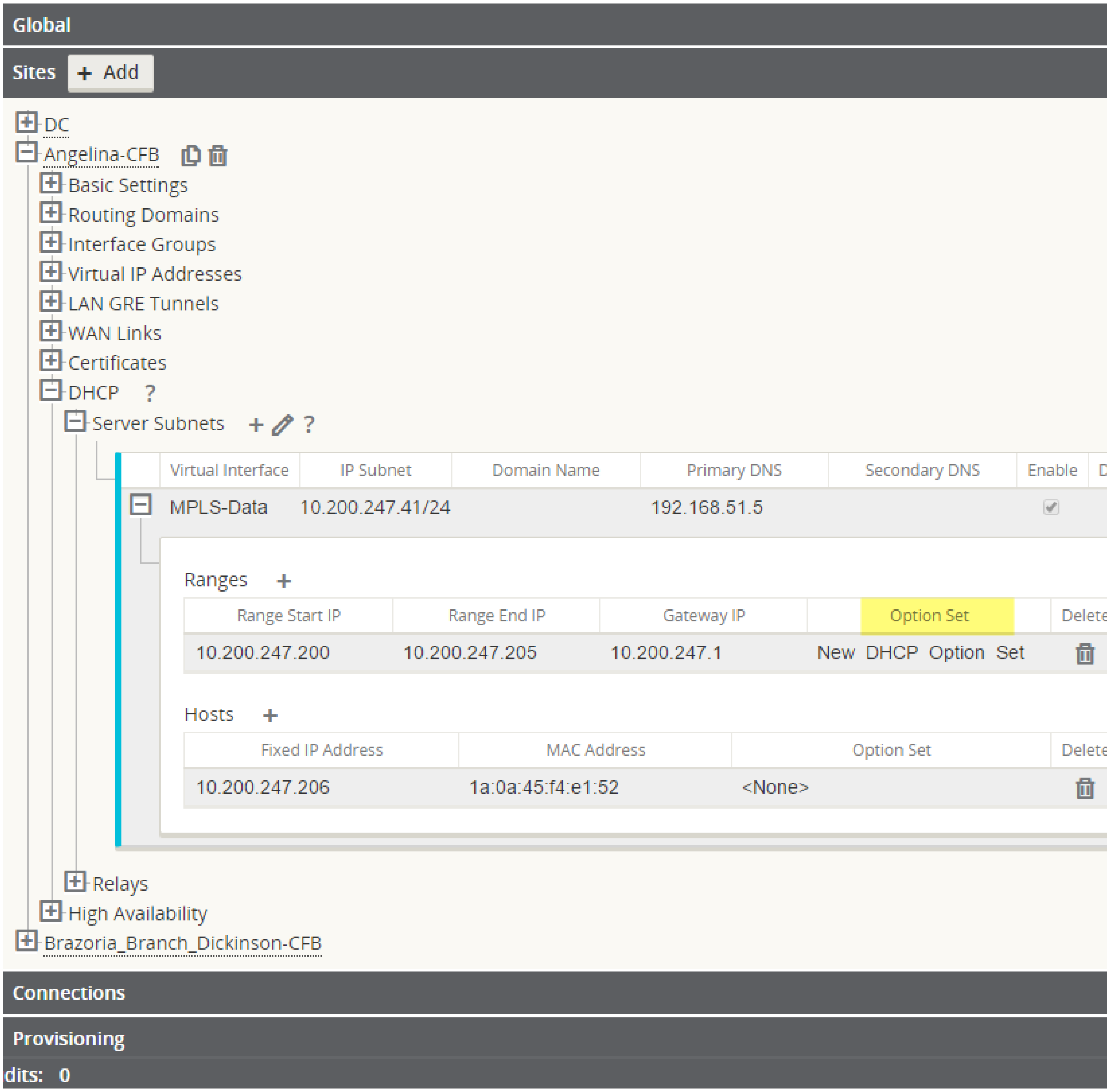
The following feature is optional, not required.

DHCP Option Sets are a group of DHCP settings or paramters that can be applied to inidividual IP address ranges. To create DHCP Option Sets, navigate to the **Global** section of the configuration and expand **Options**. Enter as many or as little settings are you would like to include in the set, then click **Apply**.



Name	Option Number	Data Type	Value
Default Lease Tin	0	Integer	3000
Custom	224	Integer	

Your DHCP Option Set must then be tied to a DHCP range and is done so in the **Sites** section where the IP address range was defined.



Global

Sites + Add

- DC
- Angelina-CFB
  - Basic Settings
  - Routing Domains
  - Interface Groups
  - Virtual IP Addresses
  - LAN GRE Tunnels
  - WAN Links
  - Certificates
  - DHCP ?
    - Server Subnets + ?

	Virtual Interface	IP Subnet	Domain Name	Primary DNS	Secondary DNS	Enable	D
⊟	MPLS-Data	10.200.247.41/24		192.168.51.5		✓	

Ranges +

Range Start IP	Range End IP	Gateway IP	Option Set	Delete
10.200.247.200	10.200.247.205	10.200.247.1	New DHCP Option Set	🗑

Hosts +

Fixed IP Address	MAC Address	Option Set	Delete
10.200.247.206	1a:0a:45:f4:e1:52	<None>	🗑

    - Relays
  - High Availability
- Brazoria_Branch_Dickinson-CFB

Connections

Provisioning

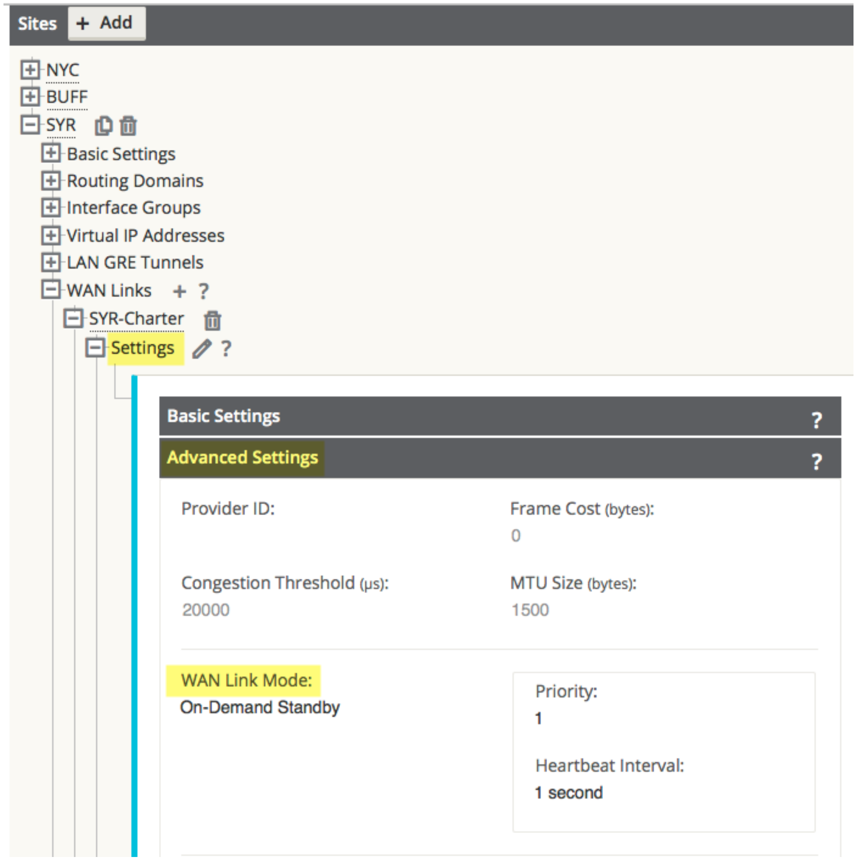
dits: 0

Standby WAN Link (VSAT)

Introduced in APN 5.2, this feature gives users the ability to have as many as three Standby WAN Links with customizable priorities per location, providing users the flexibility to use the more expensive links only when needed. The Standby WAN Links may be activated to supplement Conduit bandwidth when specified thresholds are met (On-Demand Standby) or when all primary WAN Links are DEAD or Disabled (Last-Resort Standby).

To enable this feature in Aware 2.2, navigate to **Manage > APN Configuration**. The example shown below is of the On-Demand Standby option:

1. Set the WAN Link mode under **Sites > [Site Name] > WAN Links > [WAN Link Name] > Settings > Advanced Settings > WAN Link Mode.**



Provider ID:

Frame Cost (bytes): 0

Congestion Threshold (μs): 20000

MTU Size (bytes): 1500

WAN Link Mode: On-Demand Standby

Priority: 1

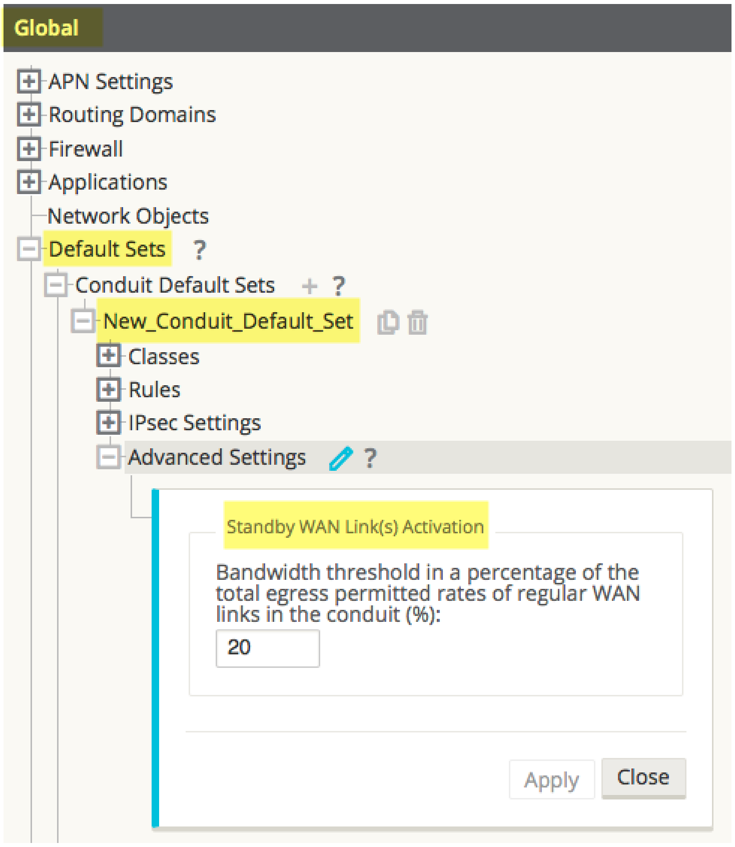
Heartbeat Interval: 1 second

The **Priority** option is a value to indicate which Standby WAN Link will be activated in which order and the **Heartbeat Interval** can either be set or disabled.

> **Note:**
>
> A more detailed definition of the three modes available can be found by clicking the **?** icon to display the help text.

> **Note:**
>
> A WAN Link configured in Standby mode can not have Internet or Intranet Services enabled on it, this will result in a Configuration Audit Error.

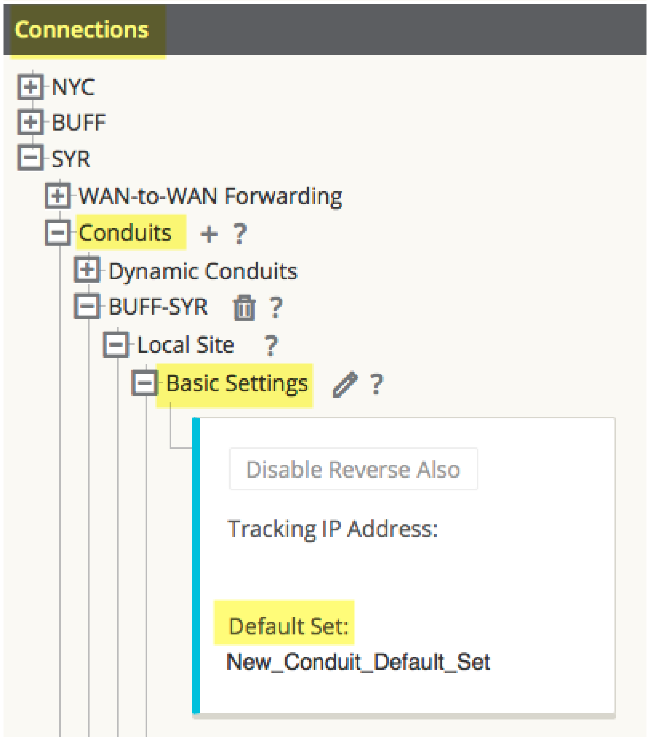
2. Create a Default Set in the **Global** section that will be used for Conduits using the On-Demand Standby WAN Link.



Bandwidth threshold in a percentage of the total egress permitted rates of regular WAN links in the conduit (%): 20

Under **Advanced Settings**, the user is able to specify a bandwidth threshold in terms of a percentage of the total WAN Egress Permitted Rates of regular WAN Links. If the available bandwidth provided by the regular WAN Links in the conduit falls below this bandwidth threshold, On-Demand Standby WAN Links in the Conduit will be activated to supplement bandwidth.

Apply the Default Set to specific Conduits under **Connections** > **[Site Name]** > **Conduits** > **[Conduit Name]** > **Local Site** > **Basic Settings** > **Default Set.**



Tracking IP Address:

Default Set:
New_Conduit_Default_Set

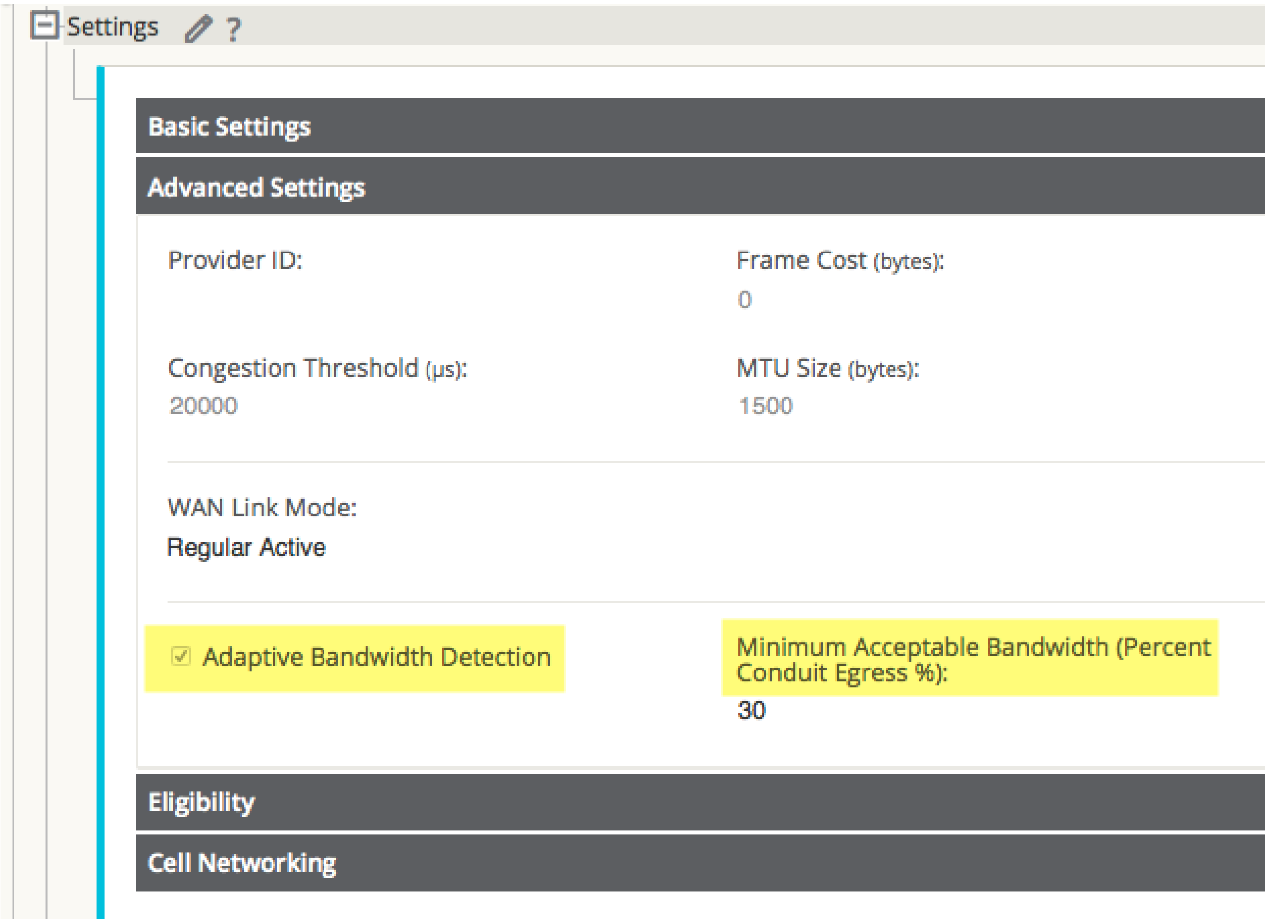
> **Note:**
>
> Step 2 is only required when choosing the On-Demand Standby option and is not applicable for Last-Resort Standby WAN Links.

Adaptive Bandwidth Detection

This feature is introduced in APN 5.2 for users with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, whose available bandwidth varies based upon weather and atmosphere conditions, location, line of site obstructions, etc. It allows the Appliance to adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range, to use the maximum amount available without marking the paths BAD.

To enable this feature using in the web UI of Aware 2.2, navigate to **Manage > APN Configuration**. Then:

1. Go to **Sites > [Site Name] > WAN Links > [WAN Link Name] > Settings > Advanced Settings.**
2. Check the **Adaptive Bandwidth Detection** box and enter in the **Minimum Acceptable Bandwidth.**



Provider ID:

Frame Cost (bytes): 0

Congestion Threshold (µs): 20000

MTU Size (bytes): 1500

WAN Link Mode: Regular Active

☑ Adaptive Bandwidth Detection

Minimum Acceptable Bandwidth (Percent Conduit Egress %): 30

Note:

There is no specific logging or event alerts for this feature, but users may refer to **Monitor** > **Reports** > **WAN Links** for a historical trend in bandwidth rates.

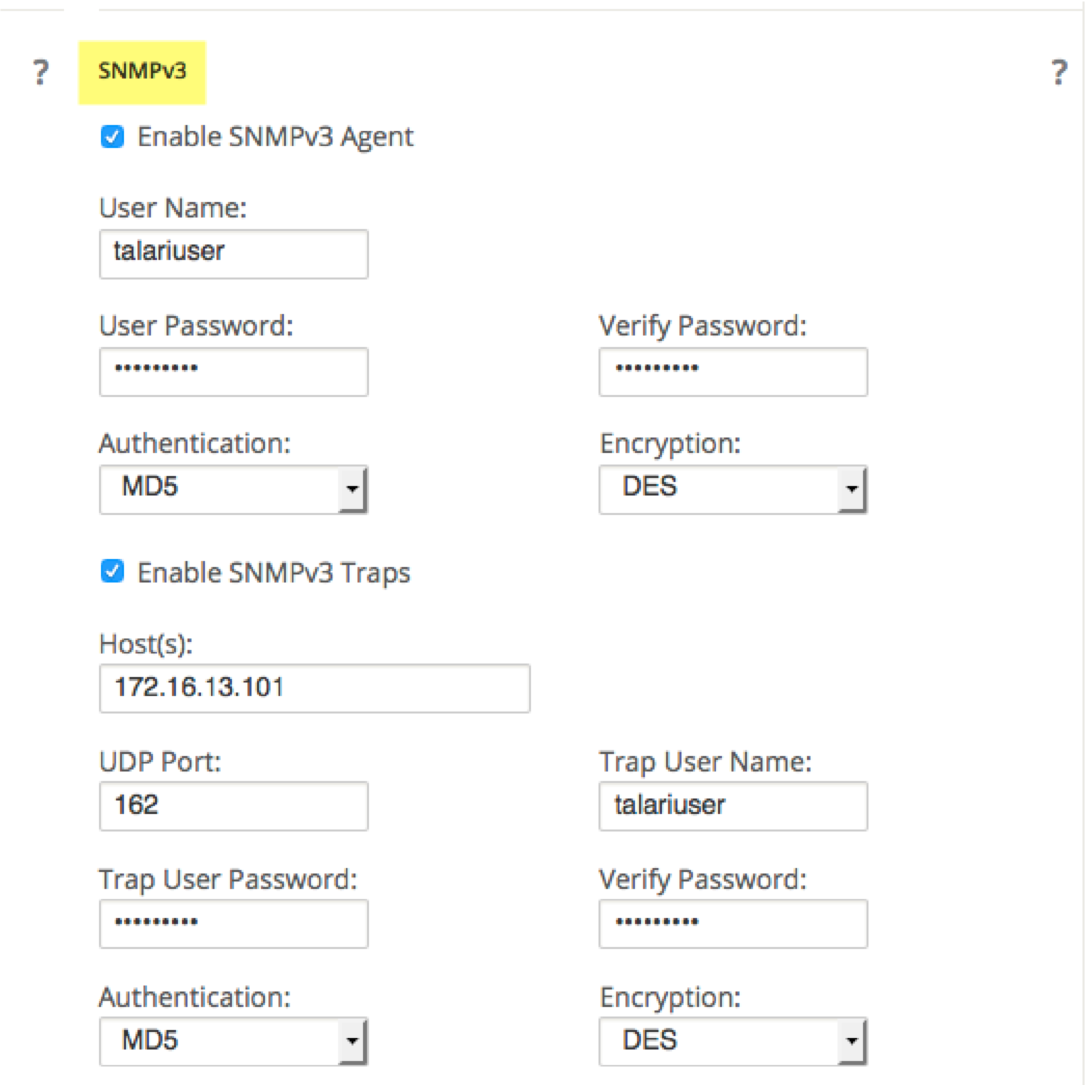
SNMPv3 Polling and Trap Capability

Note:

Oracle only supports a single user account for each SNMPv3 capability.

APN 5.2 GA introduces support for SNMPv3 polling and trap capability, and in turn, Aware R2.2 allows users to configure and push SNMPv3 settings to Appliances.

To configure SNMPv3 using Aware, navigate to **Manage** > **APN Appliance Settings** and check the box that says **Include in File** in the **Notification Settings** section. Then fill out the SNMPv3 settings as required.



SNMPv3

☑ Enable SNMPv3 Agent

User Name: talariuser

User Password: •••••••••

Verify Password: •••••••••

Authentication: MD5

Encryption: DES

☑ Enable SNMPv3 Traps

Host(s): 172.16.13.101

UDP Port: 162

Trap User Name: talariuser

Trap User Password: •••••••••

Verify Password: •••••••••

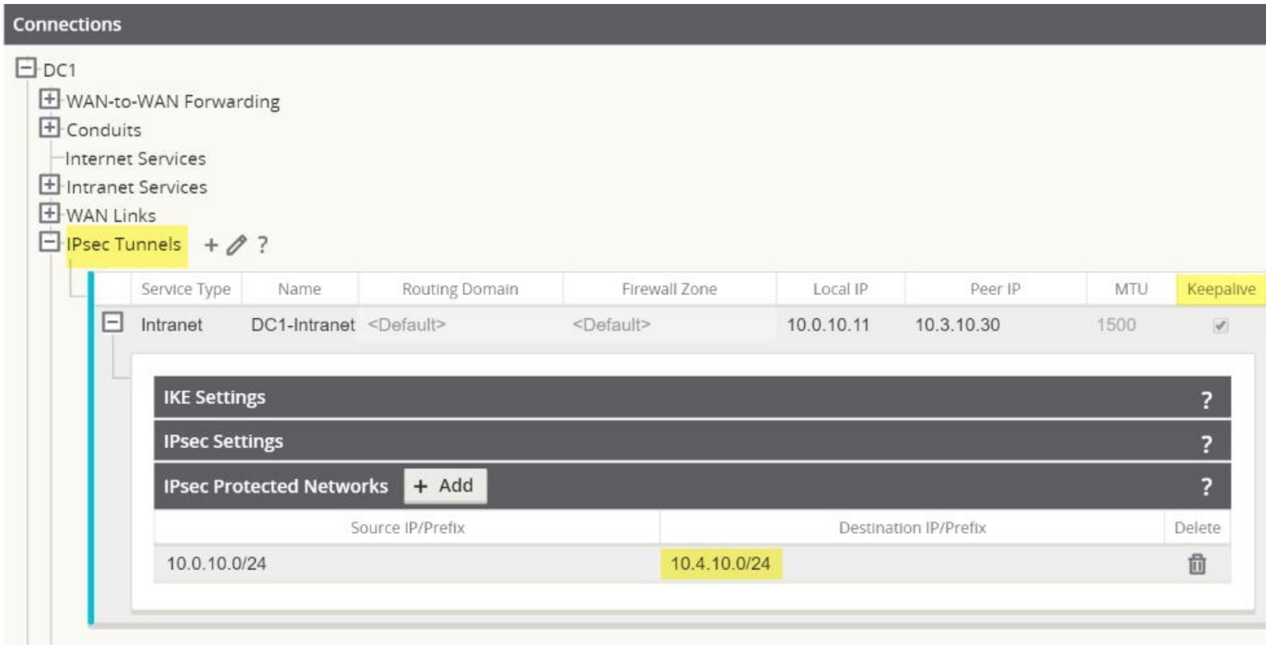
Authentication: MD5

Encryption: DES

Eligibility for IPsec Non-Conduit Routes

Prior to APN R5.2, IPsec tunnel routes would remain in the route table even if the tunnel became unavailable. This behavior can now be adjusted in the Configuration Editor when accessed from the web UI of Aware 2.2 under **Manage > APN Configuration**.

Using the **Keepalive** option under **Connections > [Site Name] > IPsec Tunnels** enhances such behavior so that the IPsec Non-Conduit Routes will now be considered ineligible when the IPsec tunnel is no longer available.



Service Type	Name	Routing Domain	Firewall Zone	Local IP	Peer IP	MTU	Keepalive
Intranet	DC1-Intranet	<Default>	<Default>	10.0.10.11	10.3.10.30	1500	☑

Source IP/Prefix	Destination IP/Prefix	Delete
10.0.10.0/24	10.4.10.0/24	🗑

Routing Enhancements

- OSPF Type 5 to Type 1

Users now have the ability to decide whether learned OSPF routes are exported as external Type 5 or intra-area Type 1. All Route Learning configuration changes may be done from the web UI of Aware 2.2 under **Manage > APN Configuration**.

- Hairpin from non-WAN-to-WAN Forwarding Site

Users may now configure a 0.0.0.0/0 route to hairpin Internet traffic between two locations without impacting any additional locations. If used for Intranet traffic, specific Intranet routes will be added to the Client site to forward Intranet traffic through the Conduit to the hairpin site. Configuration changes using Aware 2.2 are done from the web UI under **Manage > APN Configuration.**

Summary

Oracle's Aware 2.2 software introduces support for polling of up to 550 APN sites, the ability to log Firewall connections and flow logs to a syslog server, and push SNMPv3 settings out to Appliances. Additionally, new features such as, DHCP Relay & Server, Standby WAN Link, Adaptive Bandwidth Detection, and Eligibility for IPsec Non-Conduit Routes, that are enabled in the configuration file may all be done so by accessing the Configuration Editor from the Aware 2.2 web UI.

4

Release 3.0 Features

This chapter includes features and enhancements released in 3.0.

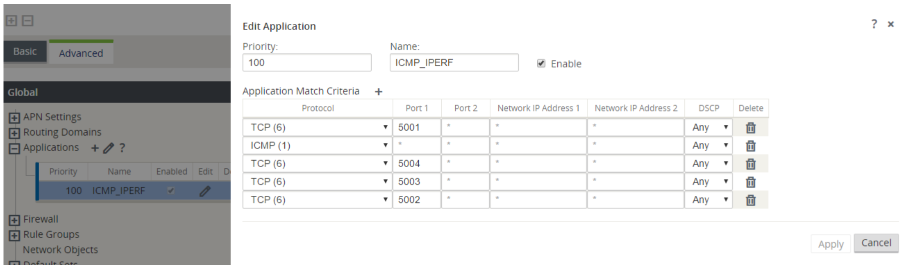
Application/Packet Filtering

> **Note:**
>
> Prior to 3.0, the objects that perform MOS scoring were originally called "Applications" but have been renamed "Rule Groups" in this, and future, releases.

Applications are a set of one or more rule match criteria, such as IP address, Protocol, DSCP, or Port Number. An Application is a way to put an identifier on a packet when it enters the system to track it. Once a flow has been matched to an Application type, the Application identifier can be used either on the rule or firewall filter as possible match criteria to handle this type of traffic as needed.

Applications

From **Manage > Configuration**, Import the current configuration from the NCN. Navigate to **Advanced > Global > Applications** click **Add (+)** to create a new Application that will allow for multiple different criteria.



Priority	Name	Enabled	Edit
100	ICMP_IPERF	✓	

Edit Application

Priority: 100

Name: ICMP_IPERF

☑ Enable

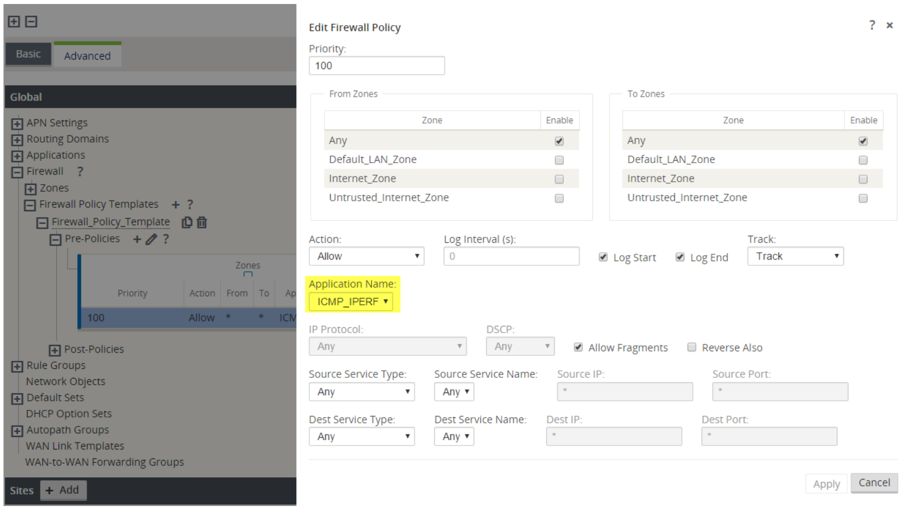
Application Match Criteria

Protocol	Port 1	Port 2	Network IP Address 1	Network IP Address 2	DSCP	Delete
TCP (6)	5001	*	*	*	Any	🗑
ICMP (1)	*	*	*	*	Any	🗑
TCP (6)	5004	*	*	*	Any	🗑
TCP (6)	5003	*	*	*	Any	🗑
TCP (6)	5002	*	*	*	Any	🗑

Figure 1: Add a new Application

Apply The Application to Firewall Policies

Once an Application is created you can then make a firewall policy that will treat all specified match criteria the same way. This can be done from a Global level via **Global > Firewall > Firewall Policy Templates.** This will apply to all firewalls within the network.



Edit Firewall Policy

Priority: 100

From Zones

Zone	Enable
Any	☑
Default_LAN_Zone	☐
Internet_Zone	☐
Untrusted_Internet_Zone	☐

To Zones

Zone	Enable
Any	☑
Default_LAN_Zone	☐
Internet_Zone	☐
Untrusted_Internet_Zone	☐

Action: Allow

Log Interval (s): 0

☑ Log Start ☑ Log End

Track: Track

Application Name: ICMP_IPERF

IP Protocol: Any

DSCP: Any

☑ Allow Fragments ☐ Reverse Also

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: Any

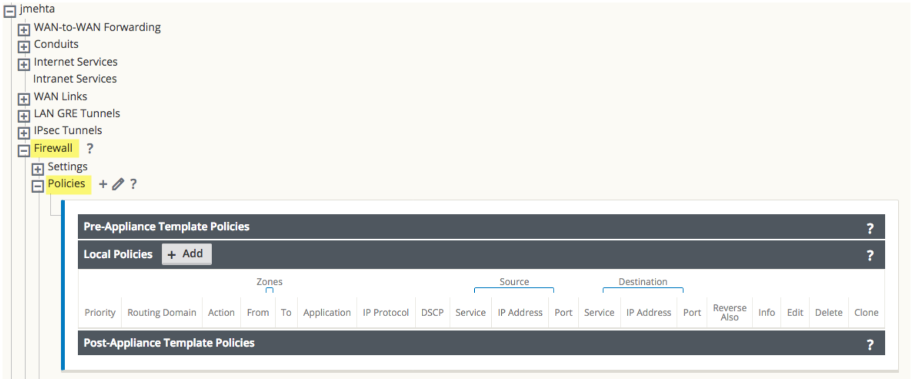
Dest IP: *

Dest Port: *

Apply Cancel

Figure 2: Associating a Firewall Policy with an Application

Firewall policies can also be configured from a Site level via **Connections > [Site Name] > Firewall > Policies**. These will only affect traffic at that site.

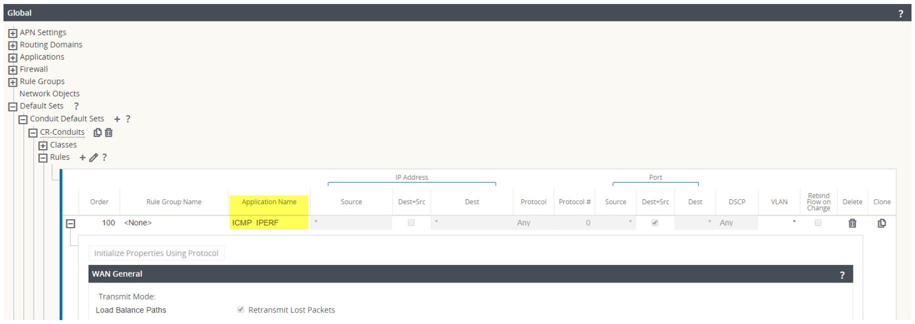


	Zones				Source			Destination						
Priority	Routing Domain	Action	From	To	Application	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone

Figure 3: Associating a Firewall Policy with an Application at the Site Level

Apply The Application to QoS Rules

Once an Application is created you can then make a single QoS rule that will treat all specified match criteria the same. This can be done from a Global level under **Global > Default Sets > Conduit Default Sets > Rules**.



			IP Address					Port							
Order	Rule Group Name	Application Name	Source	Dest=Src	Dest	Protocol	Protocol #	Source	Dest=Src	Dest	DSCP	VLAN	Rebind Flow on Change	Delete	Clone
100	<None>	ICMP IPERF	*	☐	*	Any	0	*	☑	*	Any	*	☐		

Initialize Properties Using Protocol

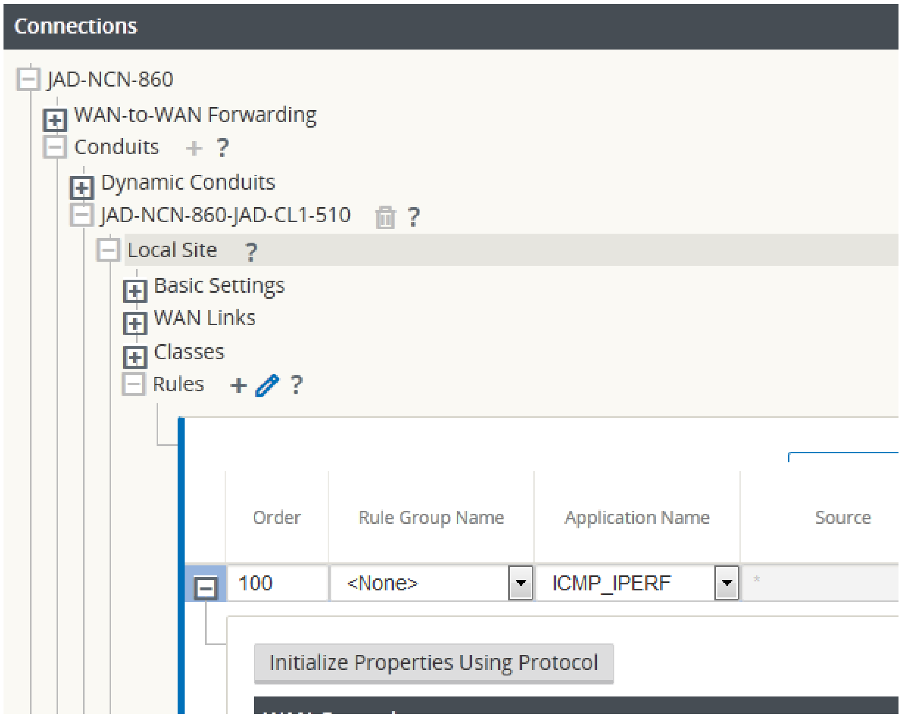
WAN General ?

Transmit Mode:

Load Balance Paths ☑ Retransmit Lost Packets

Figure 4: Adding Application to a global QoS Rule

QoS rules can also be configured, and Applications can be added to them, at a site level under **Connections > [Site Name] > Conduits > [Path Name] > Local Site > Rules**. These will only affect the traffic at that site.

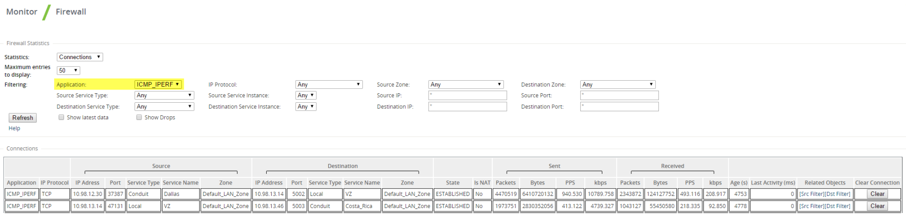


Order	Rule Group Name	Application Name	Source
100	<None>	ICMP_IPERF	*

Figure 5: Adding Application to a Local QoS Rule

Tracking Based on Firewall Policy

Users can check to see the statistics for Applications for the Firewall Policy under **Monitor > Firewall** in the web UI and select Applications from the dropdown. This allows users to easily see all connections that match to the selected Application, where they are coming from, where they are going to, and how much traffic they are generating. With this, the user can easily see how their Firewall policies are acting on the traffic for each Application.



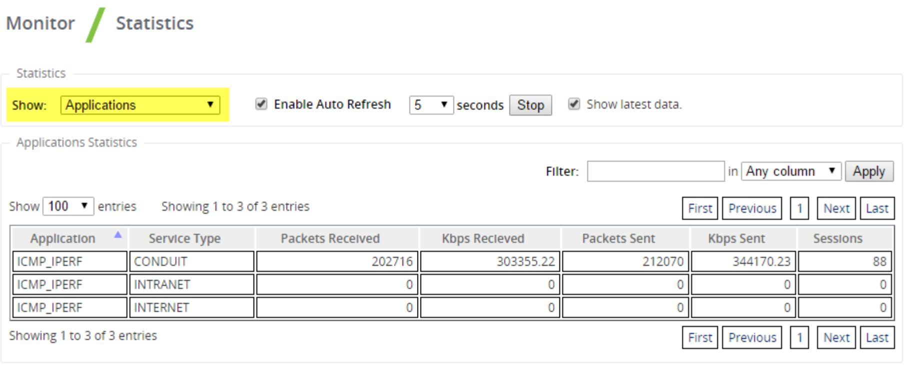
Statistics: Connections
Maximum entries to display: 50
Filtering: Application: ICMP_IPERF
IP Protocol: Any
Source Zone: Any
Destination Zone: Any
Source Service Type: Any
Source Service Instance: Any
Source IP: *
Source Port: *
Destination Service Type: Any
Destination Service Instance: Any
Destination IP: *
Destination Port: *
□ Show latest data
□ Show Drops

		Source					Destination							Sent				Received							
Application	IP Protocol	IP Adress	Port	Service Type	Service Name	Zone	IP Address	Port	Service Type	Service Name	Zone	State	Is NAT	Packets	Bytes	PPS	kbps	Packets	Bytes	PPS	kbps	Age (s)	Last Activity (ms)	Related Objects	Clear Connection
ICMP_IPERF	TCP	10.98.12.30	37387	Conduit	Dallas	Default_LAN_Zone	10.98.13.14	5002	Local	VZ	Default_LAN_Zone	ESTABLISHED	No	4470519	6410720132	940.530	10789.758	2343872	124127752	493.116	208.917	4753	0	[Src Filter][Dst Filter]	Clear
ICMP_IPERF	TCP	10.98.13.14	47131	Local	VZ	Default_LAN_Zone	10.98.13.46	5003	Conduit	Costa_Rica	Default_LAN_Zone	ESTABLISHED	No	1973751	2830352056	413.122	4739.327	1043127	55450580	218.335	92.850	4778	0	[Src Filter][Dst Filter]	Clear

Figure 6: Filtering Firewall statistics by Application

Tracking Based on QoS Rule

Users can check to see the status of the current Application for the Rule created under **Monitor > Statistics** in the web UI and select Applications from the dropdown. This allows the user to be able to see at a glance the amount of traffic being generated by a specific Application, and how many sessions are generating it. This can be useful to track bandwidth utilization for specific application types.



Monitor / Statistics

Statistics

Show: Applications ▾ ☑ Enable Auto Refresh 5 ▾ seconds Stop ☑ Show latest data.

Applications Statistics

Filter: in Any column ▾ Apply

Show 100 ▾ entries Showing 1 to 3 of 3 entries First Previous 1 Next Last

Application	Service Type	Packets Received	Kbps Recieved	Packets Sent	Kbps Sent	Sessions
ICMP_IPERF	CONDUIT	202716	303355.22	212070	344170.23	88
ICMP_IPERF	INTRANET	0	0	0	0	0
ICMP_IPERF	INTERNET	0	0	0	0	0

Showing 1 to 3 of 3 entries First Previous 1 Next Last

Figure 7: Tracking QoS by Application

VRF Firewall Enhancements

6.0 GA introduces VRF Firewall enhancements to allow for multiple VRFs, each having access to the Internet, and can be implemented via 3.0 GA. Each VRF is configured to be associated with a different user group, for example, employee or guests, while keeping the traffic from each isolated. This feature allows each Routing Domain (user group) access to the Internet through a common Access Interface. This provides the following capability:

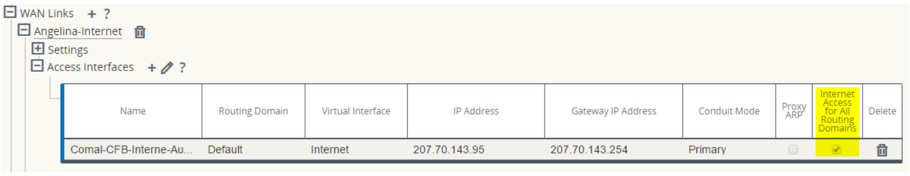
- Local guest-user Internet access
- Employee-user Internet access for defined applications
- Employee-users may continue hairpin all other traffic to the NCN
- Allow the user to add specific routes per Routing Domain, if required
- When enabled, this feature applies to all Routing Domains

Users may also create multiple access interfaces to accommodate separate public facing IP addresses. Either option provides the required security necessary per user group.

> **Note:**
>
> Detailed instructions for how to configure VRFs can be found in the 5.0 *New Features Guide.*

Below are the steps to configure this option. From Aware, navigate to **Manage > Configuration** and Import the current configuration.

1. Create Internet Service for a Site under **Connections > [Site Name] > Internet Services** and enable the **Use** checkbox under **WAN Links.**
2. Enable the checkbox labeled **Internet Access for All Routing Domains** under **Sites > [Site Name] > WAN Links > [WAN Link Name] > Access Interfaces.**



⊟ WAN Links + ?
⊟ Angelina-Internet
⊞ Settings
⊟ Access Interfaces + ?

Name	Routing Domain	Virtual Interface	IP Address	Gateway IP Address	Conduit Mode	Proxy ARP	Internet Access for All Routing Domains	Delete
Comal-CFB-Interne-Au...	Default	Internet	207.70.143.95	207.70.143.254	Primary	☐	☑	

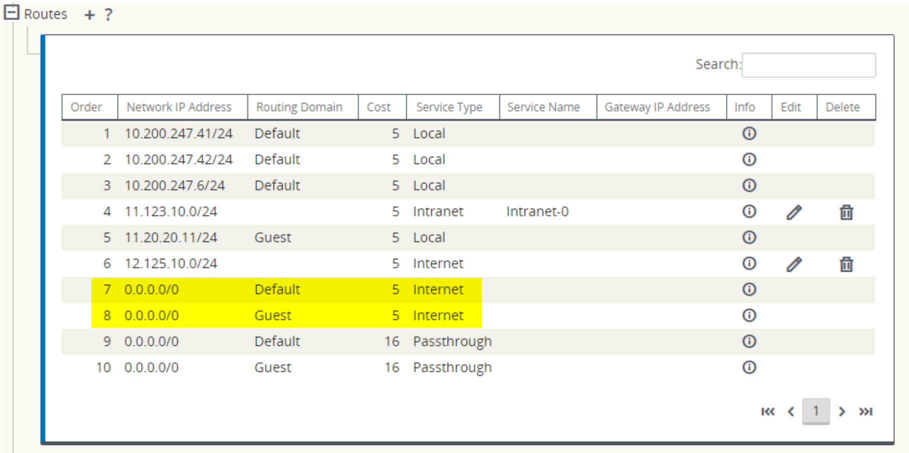
Figure 8: Enabling Internet access for All Routing Domains

Selecting this checkbox allows the platform to use this Access Interface for Internet Service on all configured Routing Domains.

Users may choose to configure either a shared Access Interface or one Access Interface for each group (separate public facing IP addresses).

Note:

After completing the following steps you should see 0.0.0.0/0 routes added, one per Routing Domain, under **Connections > [Site Name] > Routes**



Routes + ?

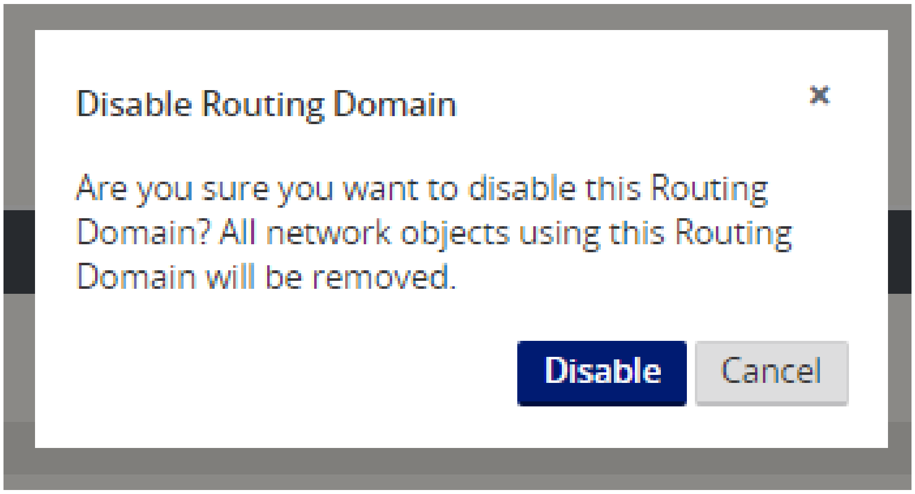
Search:

Order	Network IP Address	Routing Domain	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	10.200.247.41/24	Default	5	Local			ⓘ		
2	10.200.247.42/24	Default	5	Local			ⓘ		
3	10.200.247.6/24	Default	5	Local			ⓘ		
4	11.123.10.0/24		5	Intranet	Intranet-0		ⓘ	✎	🗑
5	11.20.20.11/24	Guest	5	Local			ⓘ		
6	12.125.10.0/24		5	Internet			ⓘ	✎	🗑
7	0.0.0.0/0	Default	5	Internet			ⓘ		
8	0.0.0.0/0	Guest	5	Internet			ⓘ		
9	0.0.0.0/0	Default	16	Passthrough			ⓘ		
10	0.0.0.0/0	Guest	16	Passthrough			ⓘ		

Figure 9: Verifying Routes Added for Each Routing Domain

Note:

It is no longer required to have all Routing Domains enabled at the NCN. Disabling RDs at the NCN that are in use at a Branch site will produce a popup message:



Disable Routing Domain

Are you sure you want to disable this Routing Domain? All network objects using this Routing Domain will be removed.

Figure 10: Removing a Routing Domain

Users may confirm that each Routing Domain is using the Internet Service by checking the Routing Domain column in the Flows table of the APNA web UI under **Monitor > Flows.**

Users may also check the routing table for each Routing Domain from the APNA web UI under **Monitor > Statistics > Routes.**

Configuration using Templates

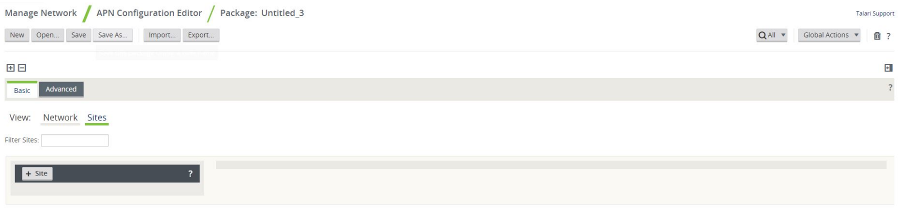
3.0 GA also supports the ability to configure the new Templates that are introduced In Oracle SD-WAN Edge 6.0 GA. New customers with five or more basic sites to setup for the first time will enjoy time savings while setting up new sites and WAN Links. With the use of templates, users may configure certain settings one-time and then duplicate the settings across more than one site as needed. This functionality is presented to the user in two key ways. First, the ability to create and administer WAN Link templates. Second a tab, which simplifies the setup of basic sites. Each of these is accessed via the Basic tab. Under the Basic tab, you have the Network option used for WAN Link templates and the Site option, which simplifies the configuration process for a site.

WAN Link Templates

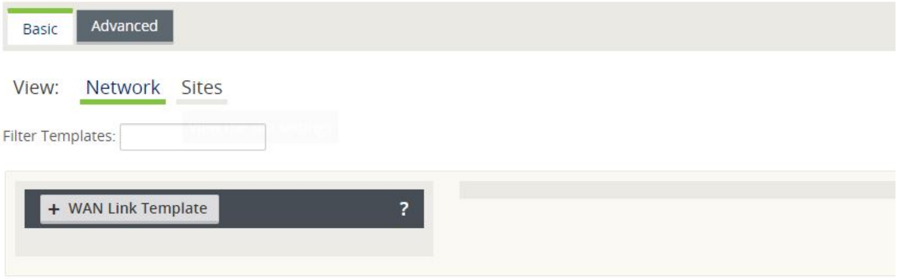
The WAN Link Templates functionality provides users with a way to setup basic configuration for WAN Links and reuse these across the network to save time. The WAN Link Templates feature exists within both the Basic configuration mode and the Advanced configuration mode, with minimal differences between the two modes in Oracle SD-WAN Edge 6.0 GA.

Below are the steps to use this feature through the Basic configuration mode:

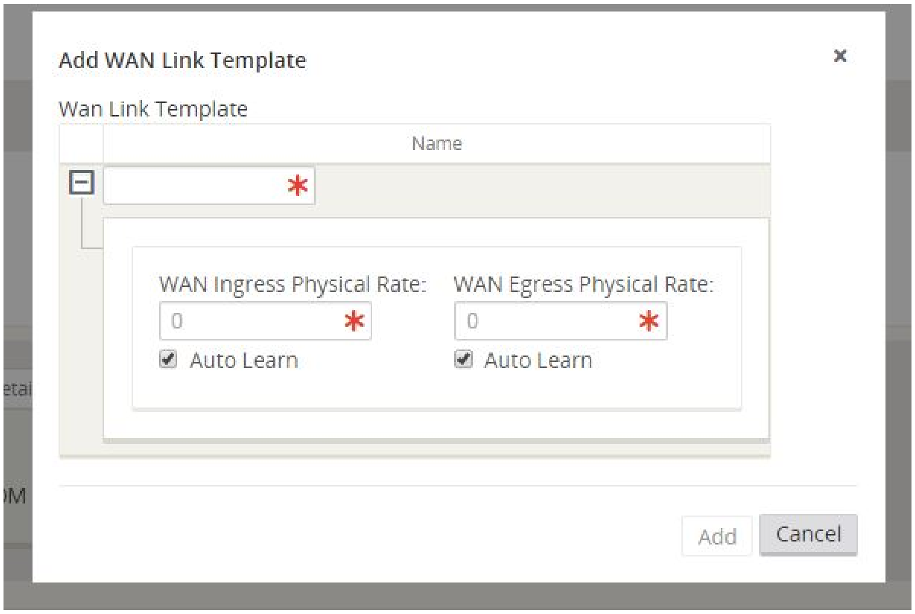
Manage Network > APN Configuration Editor > New > Basic.



Click Network to change from the (default) Sites view to Network view.



Click **+ WAN Link Template** to view the Add WAN Link Template screen shown below.



Add WAN Link Template

Wan Link Template

Name

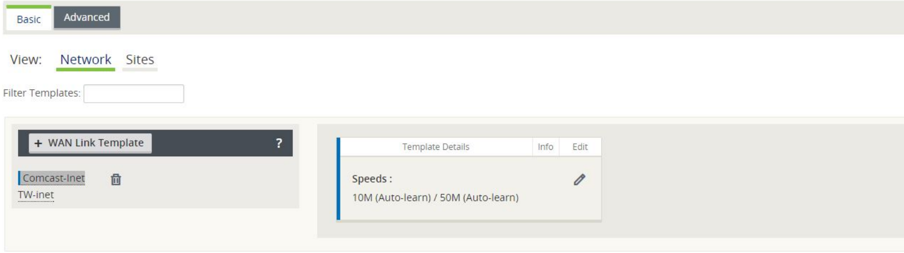
WAN Ingress Physical Rate: 0 *

☑ Auto Learn

WAN Egress Physical Rate: 0 *

☑ Auto Learn

Once a WAN Link Template is added, it will be displayed as one of the WAN Link Templates on the Network view within Basic mode.



Basic | Advanced

View: Network Sites

Filter Templates:

+ WAN Link Template ?

Comcast-Inet

TW-inet

Template Details | Info | Edit

Speeds :
10M (Auto-learn) / 50M (Auto-learn)

Basic Configuration Mode

6.0 GA introduces the Basic configuration mode as our first step in a larger ease of use evolution. Network administrators with basic sites will be able to reduce repetitive tasks and configure new sites with minimal clicks. Combined with WAN Link Templates (see above) the Basic configuration is a very powerful tool to be up and running with minimal manual configuration.

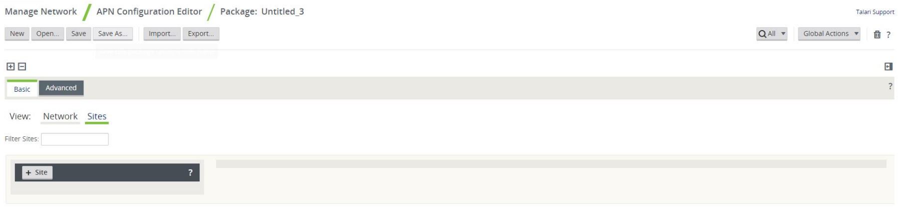
The concept of the **Basic > Sites** view is to simplify the configuration process to allow the user to create a configuration file, which will generate a Conduit between the defined sites. The required configuration properties for a Conduit between sites include:

- **Appliance**
- **Interface**
- **WAN Links**
- **Static Routes**

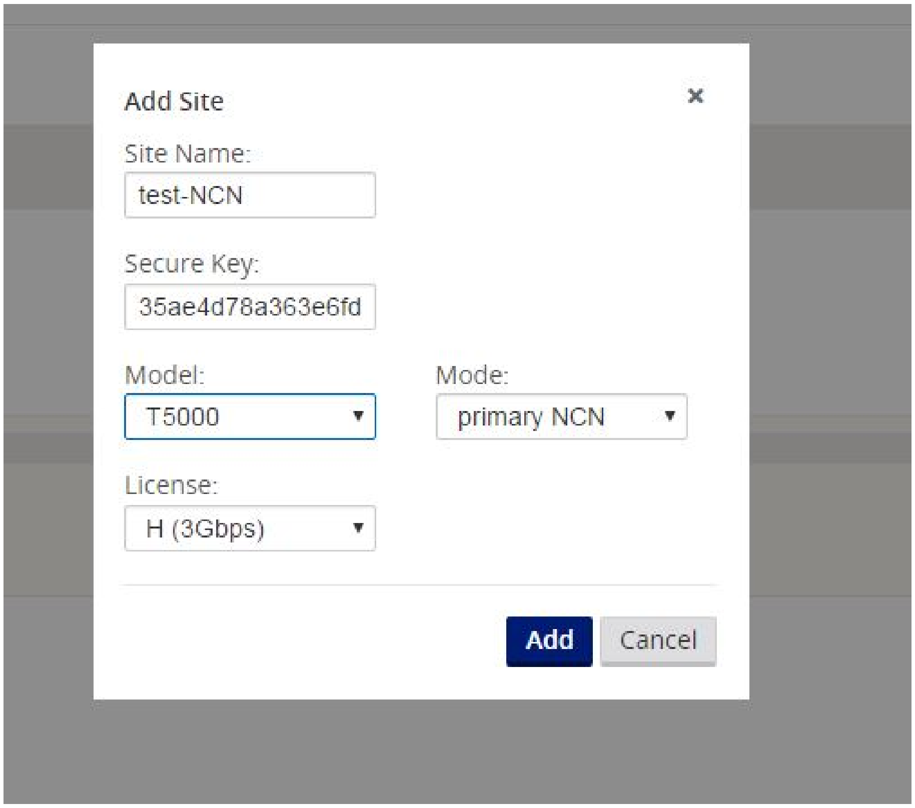
Existing users will observe that one configuration change on the Basic mode view may in fact modify or change more than one setting in Advance mode. Basic mode does allow the Import of existing configurations, and allows the user to move between Basic and Advanced modes.

Below are the steps to use the Basic configuration mode.

Manage Network > Configuration Editor > New > Basic.



Click + **Site** and enter basic site details.



Site Name: test-NCN

Secure Key: 35ae4d78a363e6fd

Model: T5000

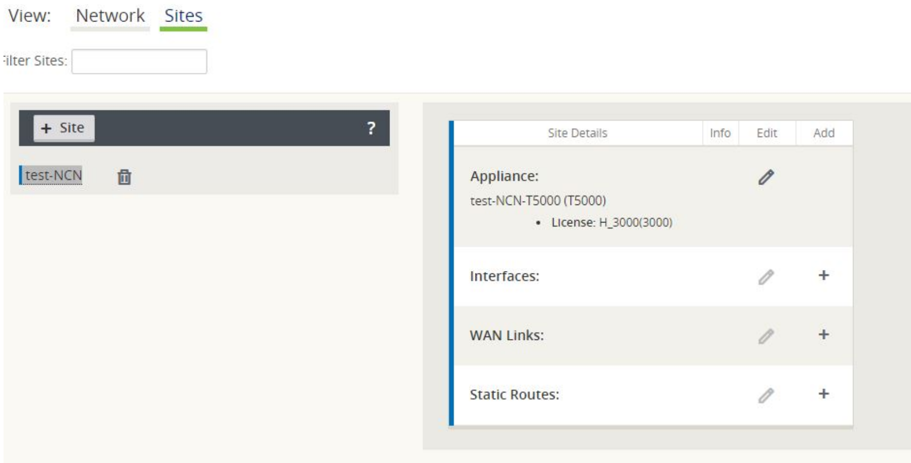
Mode: primary NCN

License: H (3Gbps)

Add from the Add Site Dialog will present the basic site details in the site list to the left and display a Site Summary to the right. The Site Summary provides the ability to add, view, and edit site details for interfaces, WAN Links, and Static Routes.

Appliance

From this point forward if the user desires to edit Appliance information just entered in the previous step, they can click the Edit icon to the right of the Appliance settings in the summary view.

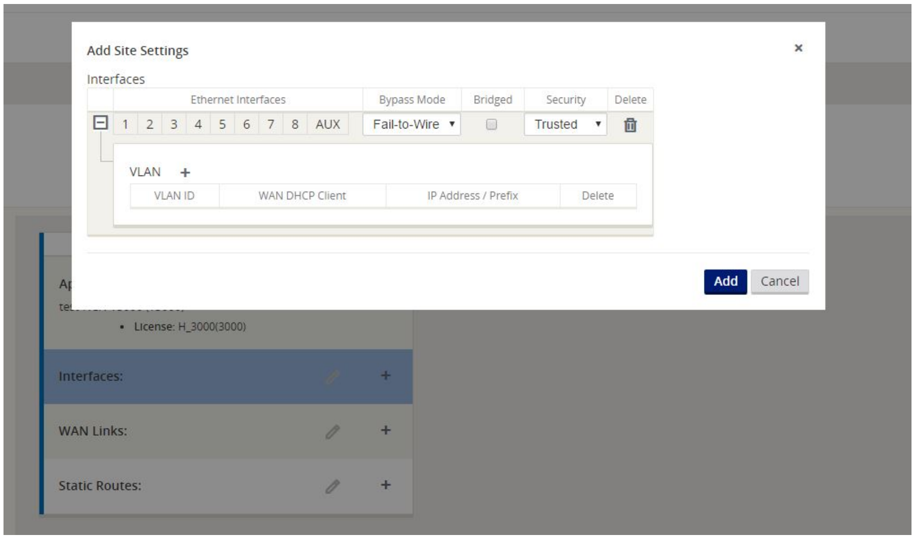


Appliance:
test-NCN-T5000 (T5000)

- License: H_3000(3000)

Interfaces

Clicking the Add / Edit Icon to the right of the Interfaces summary view shown for the site will provide the ability to add, edit, and delete Interfaces.



Ethernet Interfaces	Bypass Mode	Bridged	Security	Delete
1 2 3 4 5 6 7 8 AUX	Fail-to-Wire	☐	Trusted	🗑

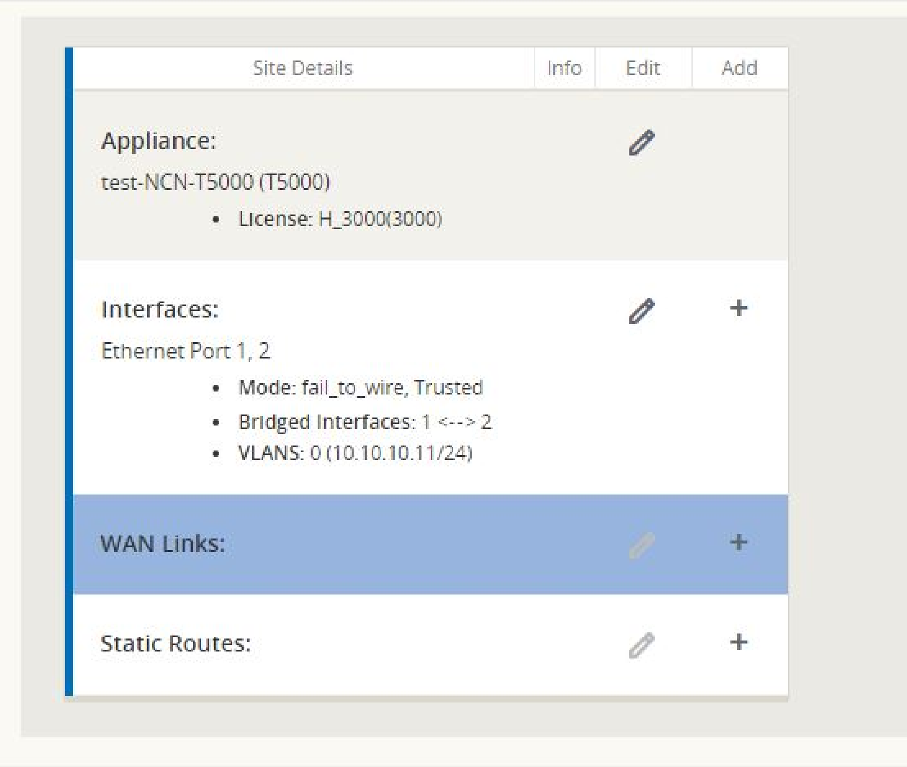
VLAN ID	WAN DHCP Client	IP Address / Prefix	Delete

- License: H_3000(3000)

The Interface option allows the user to define the physical topology of the site, such as the ports, logical VLANs and security level for the physical ports. At this level, the user can also define if the WAN interface will use DHCP for an IP address, or they may statically assign an IP address. This allows the user to configure multiple options under the same panel.

WAN Links

Clicking the Edit Icon to the right of the WAN Links summary view shown for the site will provide the ability to add, edit, and delete WAN Links.



Site Details	Info	Edit	Add

Appliance:

test-NCN-T5000 (T5000)

- License: H_3000(3000)

Interfaces:

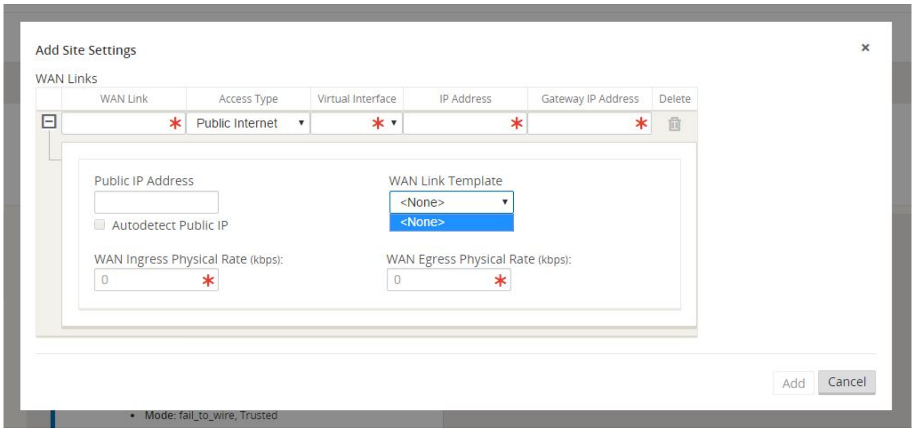
Ethernet Port 1, 2

- Mode: fail_to_wire, Trusted
- Bridged Interfaces: 1 <--> 2
- VLANS: 0 (10.10.10.11/24)

WAN Links:

Static Routes:

While Adding / Editing a WAN Link, the option to use a WAN Link Template is provided. After selecting a WAN Link Template, the WAN Link will be configured using the WAN Link Template values. The user has the option to overwrite the Template values if desired. Additionally once the Virtual Interface is selected, the IP address is automatically provided from the interface configuration.



Add Site Settings

WAN Links

WAN Link	Access Type	Virtual Interface	IP Address	Gateway IP Address	Delete
*	Public Internet	*	*	*	

Public IP Address

□ Autodetect Public IP

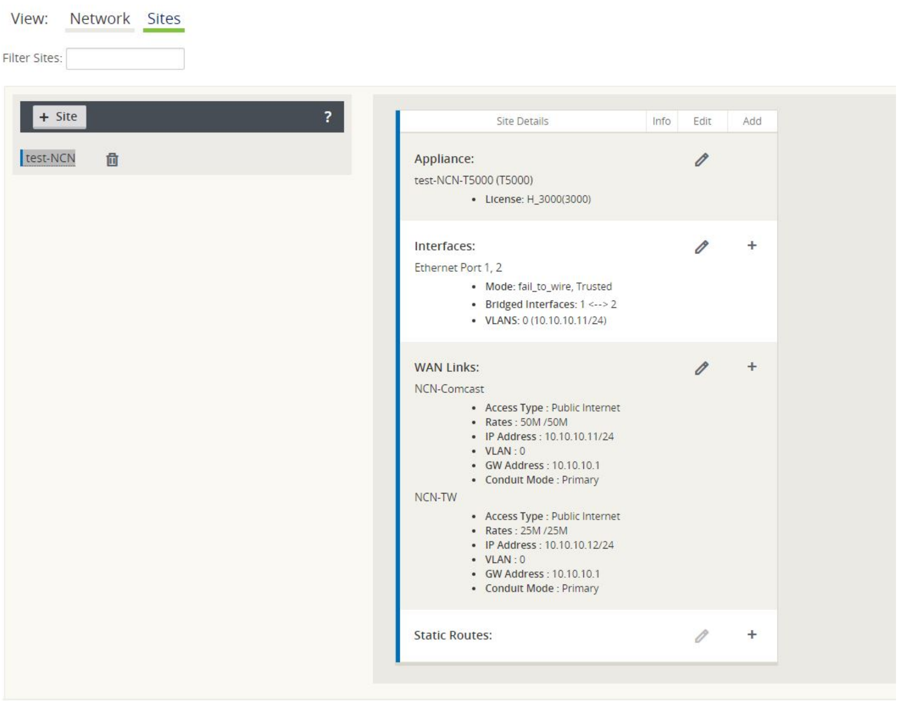
WAN Link Template

<None>

WAN Ingress Physical Rate (kbps): 0 *

WAN Egress Physical Rate (kbps): 0 *

A summary view of WAN Links is then displayed in Basic mode after the initial configuration is complete.



Appliance:
test-NCN-T5000 (T5000)
- License: H_3000(3000)

Interfaces:
Ethernet Port 1, 2
- Mode: fail_to_wire, Trusted
- Bridged Interfaces: 1 <--> 2
- VLANS: 0 (10.10.10.11/24)

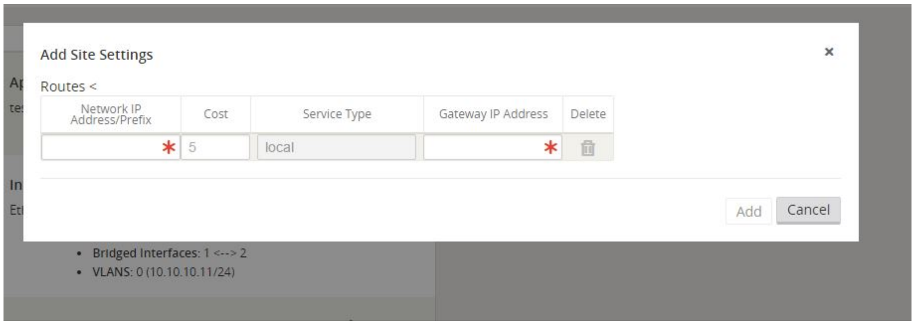
WAN Links:
NCN-Comcast
- Access Type : Public Internet
- Rates : 50M /50M
- IP Address : 10.10.10.11/24
- VLAN : 0
- GW Address : 10.10.10.1
- Conduit Mode : Primary

NCN-TW
- Access Type : Public Internet
- Rates : 25M /25M
- IP Address : 10.10.10.12/24
- VLAN : 0
- GW Address : 10.10.10.1
- Conduit Mode : Primary

Static Routes:

Static Routes

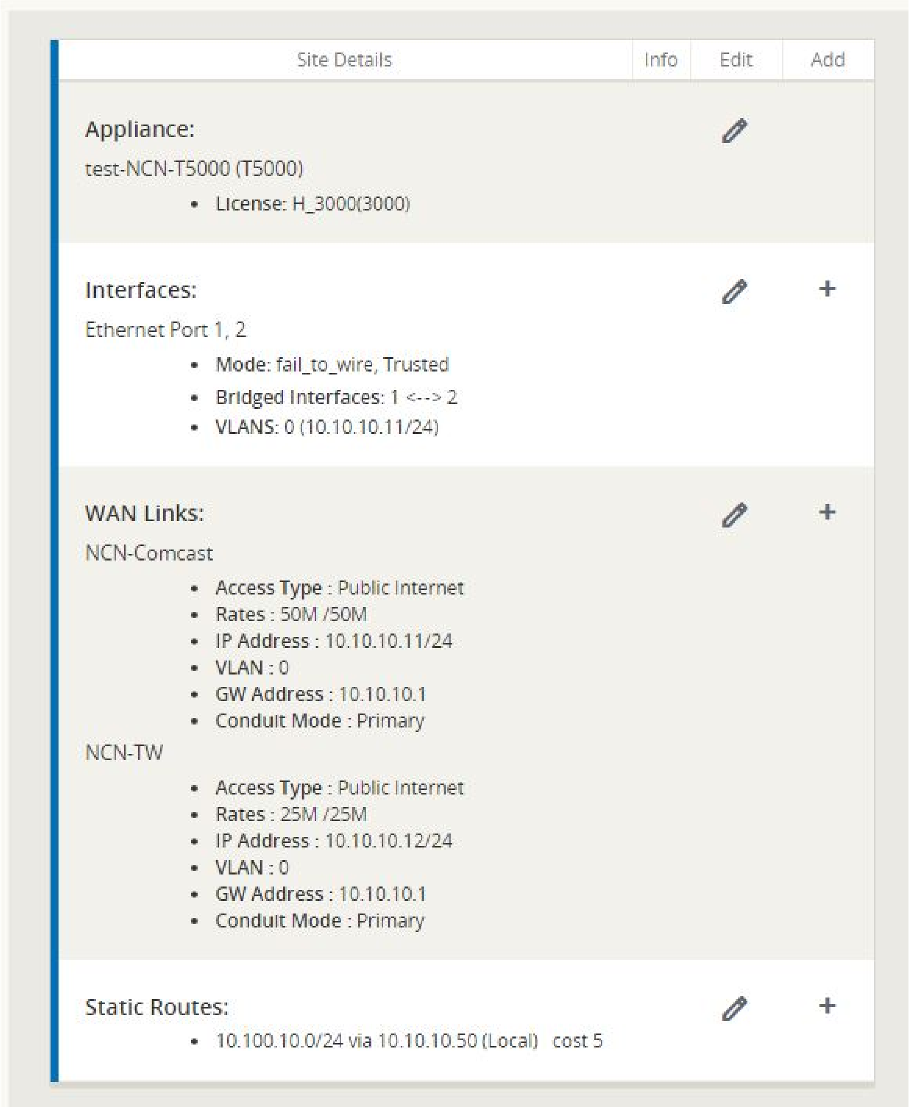
Clicking the Add / Edit icon to the right of the Static Routes area will take the user to the Add / Edit Static Routes dialog. Currently the user can only add local routes within the Basic configuration view.



Network IP Address/Prefix	Cost	Service Type	Gateway IP Address	Delete
*	5	local	*	

- Bridged Interfaces: 1 <--> 2
- VLANS: 0 (10.10.10.11/24)

After configuration, the summary view will display the site information configured and provide the ability to edit all items, as well as add more Interfaces, WAN Links, or Static Routes as needed.



Appliance:

test-NCN-T5000 (T5000)

- License: H_3000(3000)

Interfaces:

Ethernet Port 1, 2

- Mode: fail_to_wire, Trusted
- Bridged Interfaces: 1 <--> 2
- VLANS: 0 (10.10.10.11/24)

WAN Links:

NCN-Comcast

- Access Type : Public Internet
- Rates : 50M /50M
- IP Address : 10.10.10.11/24
- VLAN : 0
- GW Address : 10.10.10.1
- Conduit Mode : Primary

NCN-TW

- Access Type : Public Internet
- Rates : 25M /25M
- IP Address : 10.10.10.12/24
- VLAN : 0
- GW Address : 10.10.10.1
- Conduit Mode : Primary

Static Routes:

- 10.100.10.0/24 via 10.10.10.50 (Local) cost 5

The Basic view is intended to simplify the configuration process and provide the user the ability to create a configuration file quickly and easily. For more complicated configurations, the user may create a Basic configuration using this mode, then proceed to the Advanced mode to complete the configuration.

5

Release 3.1 Features

This chapter includes features and enhancements released in 3.1.

Oracle SD-WAN Edge as an Autonomous System (eBGP)

6.1 adds support for using Oracle SD-WAN Edge as an Autonomous System (AS), which behaves as a contiguous AS from a BGP perspective.

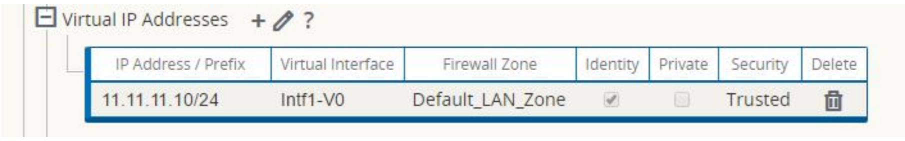
The primary use-case intended for Oracle SD-WAN Edge as an AS consists of the NCN and Geo-NCN configured as Route-Reflectors, and Clients using an iBGP peering session to the NCN and Geo-NCN for BGP reachability information.

To configure BGP using Oracle SD-WAN Aware, navigate to **Manage > Configuration** and **Import** the current configuration file from the Active NCN to get started.

Configure Trusted Virtual IP Address

You must select one trusted Virtual IP address (VIP) at each site to use for iBGP peerings across Oracle SD-WAN Edge.

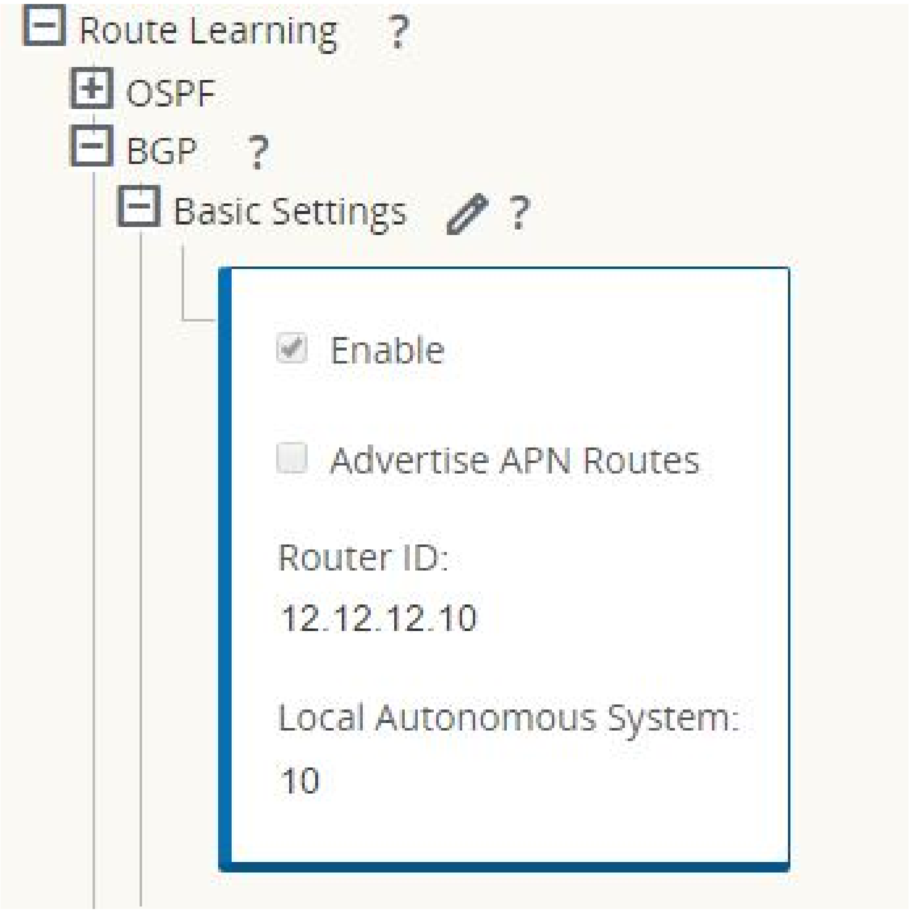
To use a Virtual IP Address for Dynamic Routing, go to **Sites**, and then **[Site Name]**, and then **Virtual IP Addresses**. Click the **Identity** checkbox for a Virtual IP Address to use it for IP services.



IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
11.11.11.10/24	Intf1-V0	Default_LAN_Zone	☑	☐	Trusted	🗑

To configure BGP (iBGP or eBGP) follow the steps below:

1. Under **Connections > [Site Name] > Route Learning > BGP > Basic Settings** click the **Edit (✎) icon.**
2. Click the **Enable** checkbox, click the **Advertise Routes** checkbox if you wish to advertise Oracle SD-WAN Edge. Routes to the router that Oracle is peering with, enter an optional **Router ID**, and enter the number of the Local Autonomous System. Click **Apply** to enable BGP.



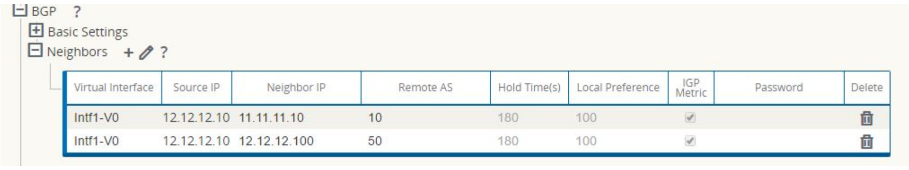
☑ Enable

□ Advertise APN Routes

Router ID:
12.12.12.10

Local Autonomous System:
10

1. Expand **BGP**, and then **Neighbors** and click the **Add (+)** icon**.**



Virtual Interface	Source IP	Neighbor IP	Remote AS	Hold Time(s)	Local Preference	IGP Metric	Password	Delete
Intf1-V0	12.12.12.10	11.11.11.10	10	180	100	☑		🗑
Intf1-V0	12.12.12.10	12.12.12.100	50	180	100	☑		🗑

Note:

If there is only one Routing Domain configured, the Routing Domain column will not appear. If **Identity** is not checked for a specific Virtual IP Address (see the Virtual IP Address Identity section for more details), the associated **Virtual Interface** will not be available for IP services.

Note:

If the Remote AS matches the Oracle Local Autonomous System, then this will be **iBGP** peering, otherwise, it will be **eBGP** peering.

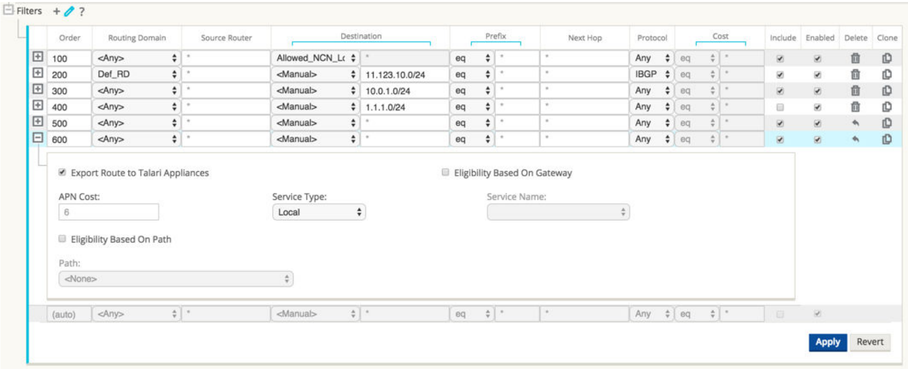
1. Choose a **Virtual Interface** from the drop-down menu. The Virtual Interface will determine the **Source IP Address**.

2. Enter the IP Address of the BGP Neighbor router in the **Neighbor IP** field.
3. In the **Hold Time (s)** field, enter the Hold Time, in seconds, to wait before declaring a neighbor down (the default is 180).
4. In the **Local Preference (s)** field, enter the Local Preference value, in seconds, which is used for selection from multiple BGP routes (the default is 100).
5. Click the **IGP Metric** checkbox to enable the comparison of internal distances to calculate the best route.
6. In the **Password** field, enter a password for MD5 authentication of BGP sessions (authentication is not required).

Import Filters

Filters are used to import or exclude routes learned dynamically based on specific match criteria.

1. Expand **Route Learning > Import Filters** and click the **Add (+)** icon**.**



Order	Routing Domain	Source Router	Destination		Prefix		Next Hop	Protocol	Cost		Include	Enabled	Delete	Clone
100	<Any>	*	Allowed_NCN_Lc	*	eq	*	*	Any	eq	*	☑	☑		
200	Def_RD	*	<Manual>	11.123.10.0/24	eq	*	*	IBGP	eq	*	☑	☑		
300	<Any>	*	<Manual>	10.0.1.0/24	eq	*	*	Any	eq	*	☑	☑		
400	<Any>	*	<Manual>	1.1.1.0/24	eq	*	*	Any	eq	*	☐	☑		
500	<Any>	*	<Manual>	*	eq	*	*	Any	eq	*	☑	☑		
600	<Any>	*	<Manual>	*	eq	*	*	Any	eq	*	☑	☑		
(auto)	<Any>	*	<Manual>	*	eq	*	*	Any	eq	*	☐	☑		

☑ Export Route to Talari Appliances

☐ Eligibility Based On Gateway

APN Cost: 6

Service Type: Local

Service Name:

☐ Eligibility Based On Path

Path: <None>

Note:

If there is only one Routing Domain configured, the Routing Domain column will not appear.

1. Click the **(+)** next to your new Filter to expand the settings.
2. Create an Import Filter entry that will match BGP-specific criteria, such as source router or next hop for example, and Import as a Conduit route steered to the appropriate Conduit. This is referred to as “south-bound” iBGP route learning.
3. You can use the criteria below to construct each Filter that you create.
4. Once you have configured your filter, click **Apply**.

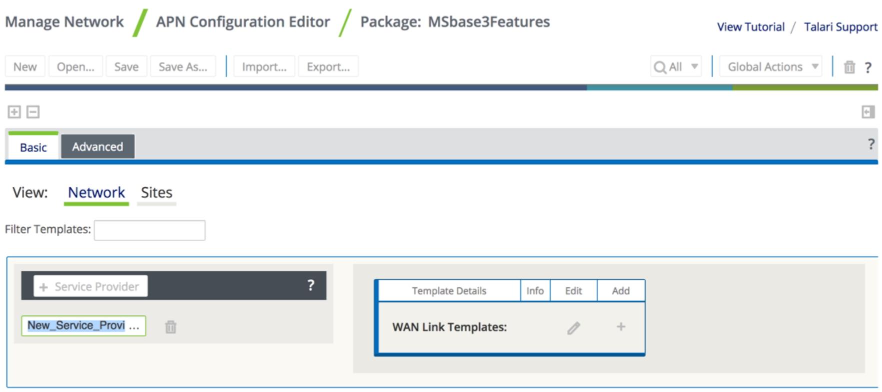
- **Order:** The Order in which filters are prioritized. The first filter that a route matches to will be applied to that route.
- **Routing Domain**: To match routes from a specific routing domain, choose one of the configured Routing Domains from the drop-down menu.
- **Source Router**: To match routes from a specific source router, enter the IP address of the Source Router.
- **Destination**: To match routes by destination, choose **Manual** from the drop-down menu and enter an IP Address and Netmask in the adjacent field or choose from the list of available **Network Objects**.
- **Prefix**: To match routes by prefix, choose a match predicate from the drop-down menu and enter a Route prefix in the adjacent field.
  - The predicates are:
    - eq: Equal to
    - lt: Less than
    - le: Less than or equal to
    - gt: Greater than
    - ge: Greater than or equal to
- **Next Hop:** To match routes by next hop, enter the IP address of the Next Hop.
- **Protocol:** To match routes by protocol, choose the protocol from the drop-down menu (**Any**, **OSPF**, or **BGP**) to learn routes from.
- **Cost:** If the protocol for your filter is OSPF, to match routes by cost, choose a match predicate from the drop-down menu and enter a route cost in the adjacent field.
  - The predicates are:
    - eq: Equal to
    - lt: Less than
    - le: Less than or equal to
    - gt: Greater than
    - ge: Greater than or equal to
- **Include**: Click the checkbox to **Include** routes that match this filter. Otherwise matching routes are ignored.
- **Enabled:** Click the checkbox to **Enable** this filter. Otherwise the filter is ignored.
- **Clone**: Click the **Clone** icon to make a copy of an existing Filter.
- **Export Route to Appliances**: Click the checkbox to export matching routes to Appliances at other Sites when **WAN-to-WAN Forwarding** is enabled. This functionality is enabled by default and only applies for the following Service Types: Local, LAN GRE Tunnel, and LAN IPsec Tunnel.
- **Eligibility Based On Gateway**: Click the checkbox to ensure that a matching route is not used if its Gateway is unreachable.
- **Oracle Cost:** Enter the cost that the Appliance applies to matching routes (the default is 6).
- **Service Type:** Select the Service Type (e.g., Local, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel, or Passthrough) that will be assigned to matching routes.
- **Service Name**: For Intranet, LAN GRE Tunnel, and LAN IPsec Tunnel, specify the name of the configured Service Type to use.
- **Eligibility Based on Path**: Click the checkbox to ensure that a matching route is not used if a chosen Path is dead. Choose a **Path** from the list of available Paths on the drop-down menu below.

Oracle SD-WAN Edge 6.1 now supports BGP attribute manipulation for ingress and egress per peer. Please contact your Oracle Representative for additional information on this topic.

WAN Link Template – Broadband, MPLS, and Private Intranet

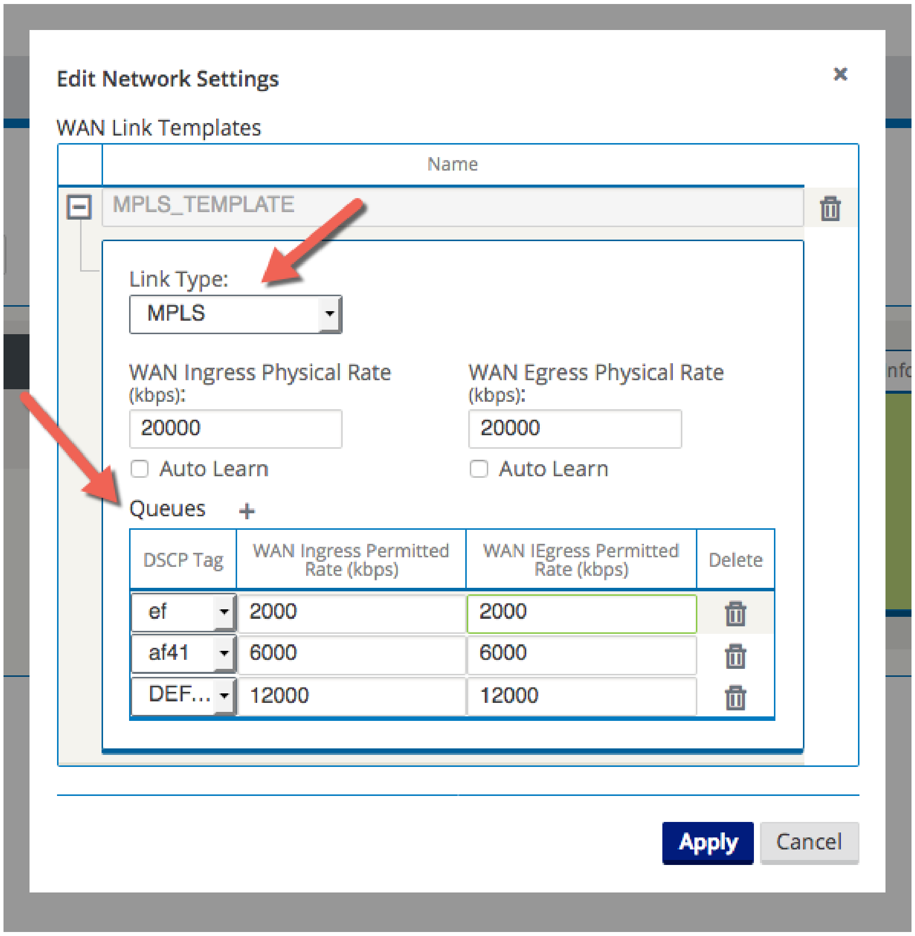
Edge software has introduced a WAN Link Template feature that includes the ability to configure Service Provider-specific WAN Link Templates for Broadband, MPLS, and Private Intranet connections. This allows for a quicker site configuration by applying a WAN Link Template for newly created sites, as well as an easier way to clone branch locations with similar Service Provider attributes.

To create a WAN Link Template based on Service Provider attributes using Aware, navigate to **Manage > Configuration** and **Import** the current configuration from the Active NCN to get started. Under the **Basic** tab, select the **Network** view and click + **Service Provider.**



A New_Service_Provider option will appear, click inside this box to change the name, then click the + icon to create a new WAN Link Template.

Select the Link Type from the drop down and enter the WAN Ingress and Egress bandwidth rates. If your WAN Link is an MPLS link, you will have the ability to enter up to 8 queues based on DSCP Tag.



MPLS_TEMPLATE

Link Type: MPLS

WAN Ingress Physical Rate (kbps): 20000

□ Auto Learn

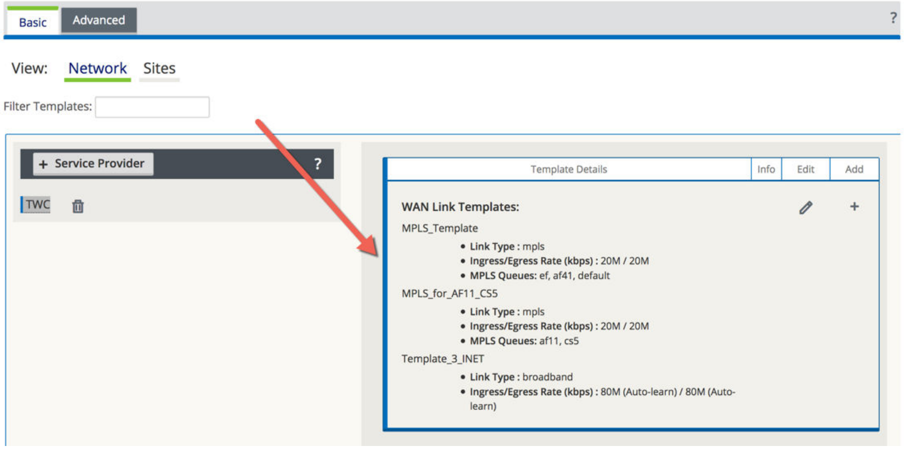
WAN Egress Physical Rate (kbps): 20000

□ Auto Learn

Queues +

DSCP Tag	WAN Ingress Permitted Rate (kbps)	WAN IEgress Permitted Rate (kbps)	Delete
ef	2000	2000	🗑
af41	6000	6000	🗑
DEF...	12000	12000	🗑

The user may define multiple WAN Link Templates per Provider. Three Templates are shown in the example below for Provider "TWC", but the user may configure as many as thirty-two.



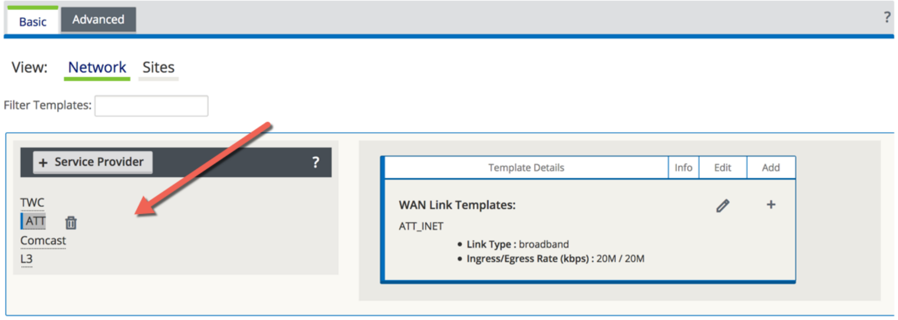
WAN Link Templates:

MPLS_Template
- **Link Type :** mpls
- **Ingress/Egress Rate (kbps) :** 20M / 20M
- **MPLS Queues:** ef, af41, default

MPLS_for_AF11_CS5
- **Link Type :** mpls
- **Ingress/Egress Rate (kbps) :** 20M / 20M
- **MPLS Queues:** af11, cs5

Template_3_INET
- **Link Type :** broadband
- **Ingress/Egress Rate (kbps) :** 80M (Auto-learn) / 80M (Auto-learn)

The user may also define up to twenty Service Providers, although only four are shown in this example.

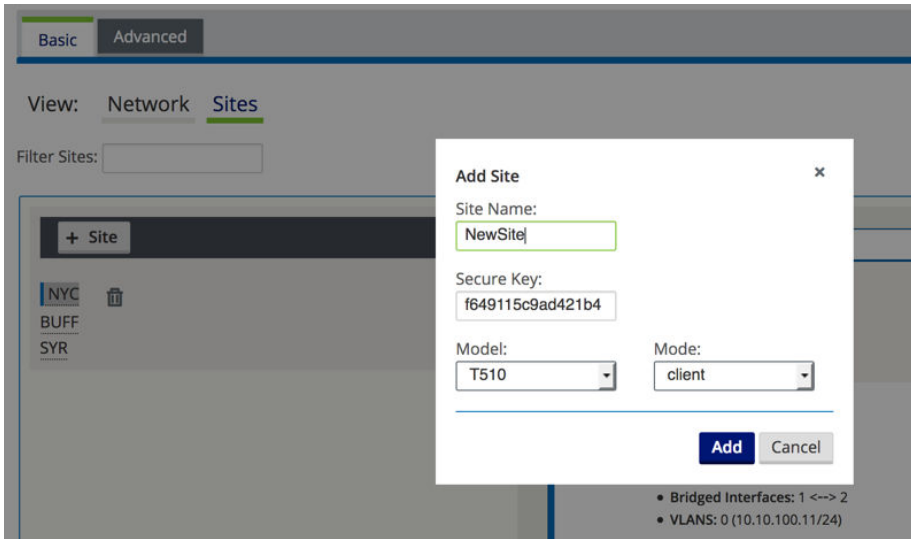


WAN Link Templates:

ATT_INET
- **Link Type :** broadband
- **Ingress/Egress Rate (kbps) :** 20M / 20M

Once the Service Providers have been defined and WAN Link Templates have been created for them, users will save time by assigning a WAN Link Template to the configuration when creating a new Client site.

To create a new Client site using your WAN Link Templates, select the **Sites** view then the + **Sites** button.



Add Site

Site Name: NewSite

Secure Key: f649115c9ad421b4

Model: T510

Mode: client

- **Bridged Interfaces:** 1 <--> 2
- **VLANS:** 0 (10.10.100.11/24)

Name your new Client site, select the Model and Mode, then click **Add.** A box will appear on the right-hand side of the screen allowing you to select some basic configuration options for your new Client. Click the + icon next to WAN Links then choose which WAN Link Template to use.

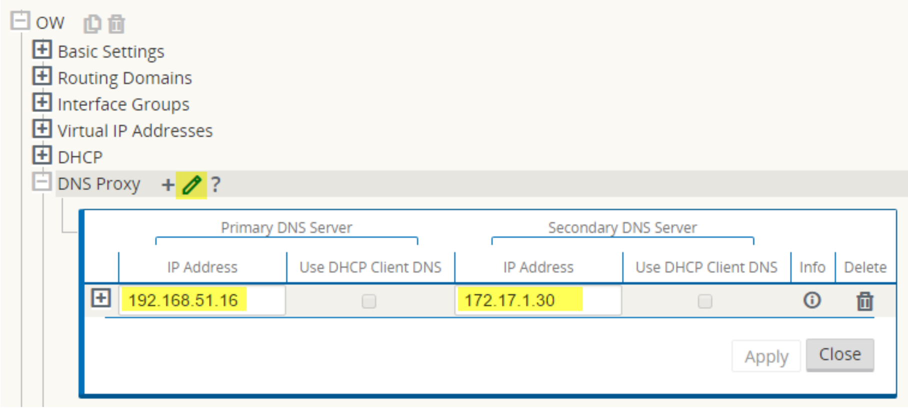
Once your new Client site is active within the Edge network, Aware may begin polling this site by selecting the **Poll** checkbox on the **Manage > Discovery** page.

Application Identification: DNS Proxy

To enhance our Application Identification capability, Oracle has added the DNS Proxy feature in Oracle SD-WAN Edge 6.1. Users now have the ability to use a Appliance as a DNS Proxy Server by directing DNS requests to one of the Oracle Virtual IP addresses. An advantage of DNS Proxy is that Oracle can use the DNS information obtained and apply it to a set of defined Application Match Criteria. This Application criteria can then be applied to a Rule or Firewall Policy. This allows the user to defined an Application in a Rule and Override to local Service, for example the Internet Service (if one is defined at the site). A sample reason for doing so is that the user may want certain web sites sent out the local Internet circuit verses backhauling these sites through the Conduit to the NCN site.

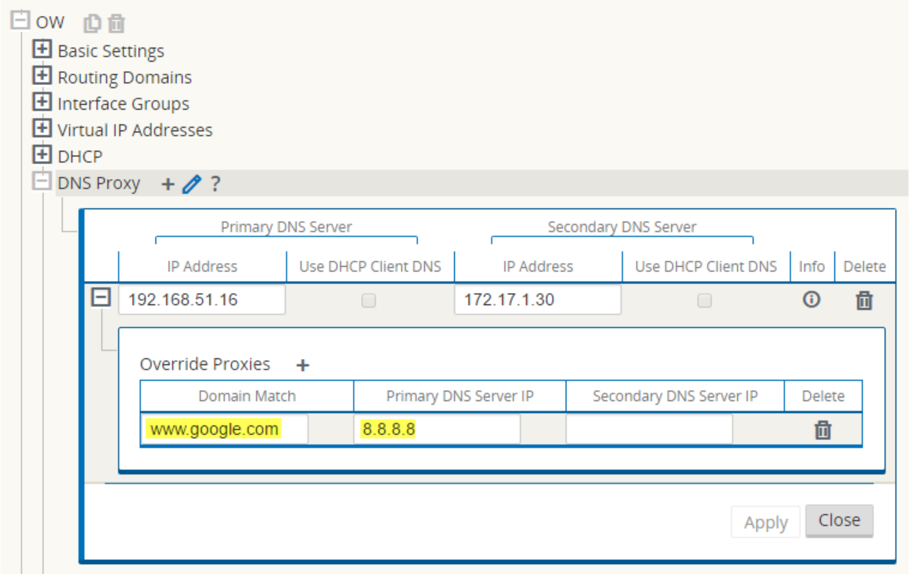
Enabling DNS Proxy

From Aware, navigate to **Manage > Configuration** and **Import** the current configuration file from the Active NCN. On the Advanced view tab, navigate to **Sites > [Site Name] > DNS Proxy**. Users can manually configure the Primary and Secondary DNS server IP addresses to be used, or select the **Use DHCP Client DNS** checkbox to dynamically learn the server IP addresses via the DHCP Client from an Interface Group.



	Primary DNS Server		Secondary DNS Server			
	IP Address	Use DHCP Client DNS	IP Address	Use DHCP Client DNS	Info	Delete
⊞	192.168.51.16	□	172.17.1.30	□	ⓘ	🗑

Click the **(+)** icon to expand and configure Override Proxies for DNS requests matching certain domain names.



⊟ OW

⊞ Basic Settings

⊞ Routing Domains

⊞ Interface Groups

⊞ Virtual IP Addresses

⊞ DHCP

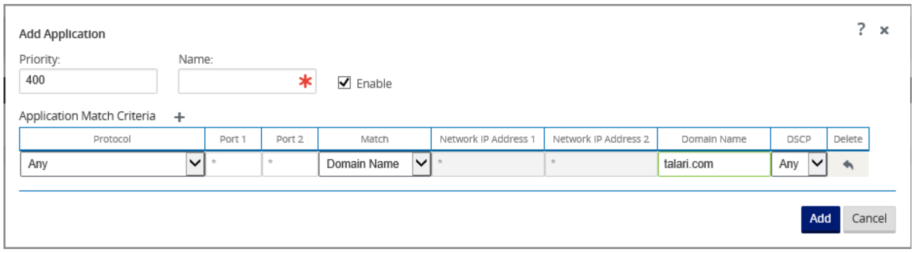
⊟ DNS Proxy + ?

	Primary DNS Server		Secondary DNS Server			
	IP Address	Use DHCP Client DNS	IP Address	Use DHCP Client DNS	Info	Delete
⊟	192.168.51.16	☐	172.17.1.30	☐	ⓘ	🗑

Override Proxies +

Domain Match	Primary DNS Server IP	Secondary DNS Server IP	Delete
www.google.com	8.8.8.8		🗑

The user may now define the Application Match Criteria, such as Oracle.com for example.



Add Application

Priority: 400

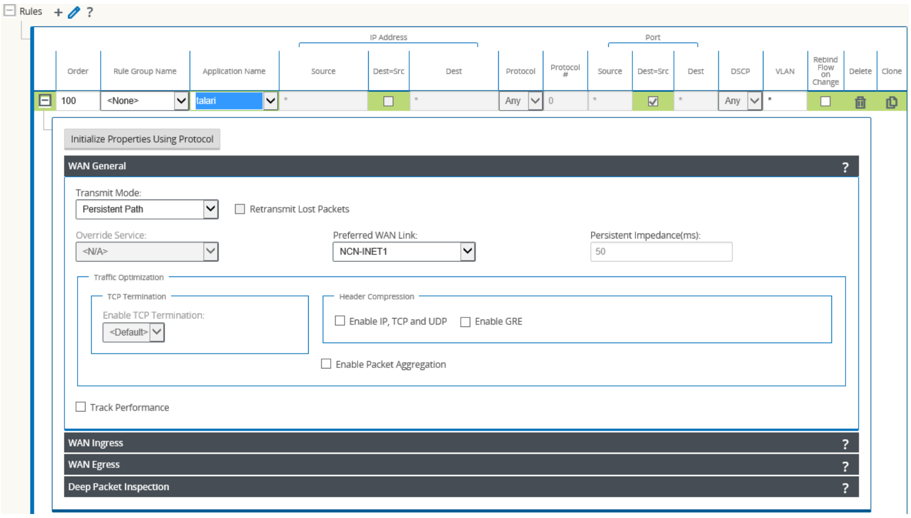
Name: *

☑ Enable

Application Match Criteria +

Protocol	Port 1	Port 2	Match	Network IP Address 1	Network IP Address 2	Domain Name	DSCP	Delete
Any	*	*	Domain Name	*	*	talari.com	Any	↶

Once defined, the user can apply this to a Rule (shown below) or Firewall Policy.



⊟ Rules + ?

				IP Address					Port							
	Order	Rule Group Name	Application Name	Source	Dest=Src	Dest	Protocol	Protocol #	Source	Dest=Src	Dest	DSCP	VLAN	Rebind Flow on Change	Delete	Clone
⊟	100	<None>	talari	*	☐	*	Any	0	*	☑	*	Any	*	☐	🗑	⧉

Initialize Properties Using Protocol

WAN General

Transmit Mode: Persistent Path

☐ Retransmit Lost Packets

Override Service: <N/A>

Preferred WAN Link: NCN-INET1

Persistent Impedance(ms): 50

Traffic Optimization

TCP Termination

Enable TCP Termination: <Default>

Header Compression

☐ Enable IP, TCP and UDP ☐ Enable GRE

☐ Enable Packet Aggregation

☐ Track Performance

When configuring such a rule, the user has additional options covered in the next section.

Persistent Path Traffic Steering

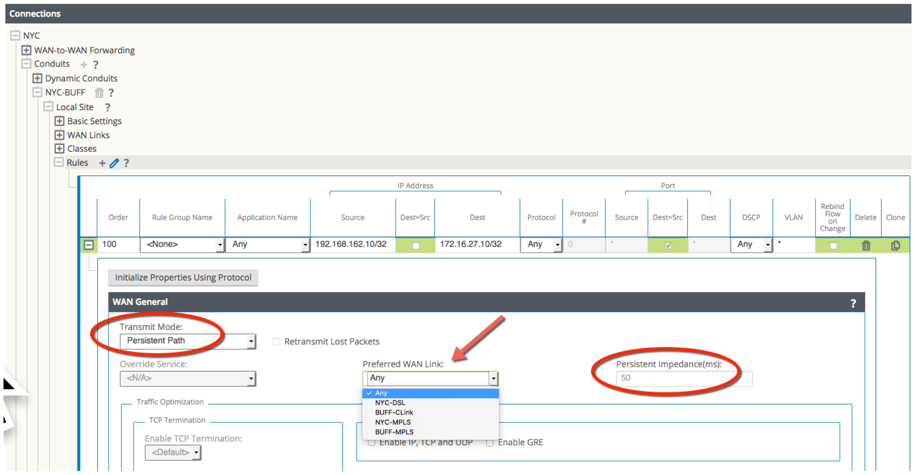
6.1 GA introduces Persistent and Conduit Path Steering providing users the option to select a favored WAN Link when creating a Conduit Rule using Persistent Path as the Transmit Mode.

As an example, a user may now use Path Steering to direct voice traffic down the MPLS WAN Link.

> **Note:**
>
> This option is only available for Conduit-specific Rules. It is not an available option for a Rule in Global Conduit Default Sets.

To create a Rule using this feature from Aware, navigate to **Manage > Configuration** and **Import** the current configuration file from the Active NCN. Then go to **Connections > [Site Name] > Conduits > [Conduit Name] > Local Site > Rules**. Enter the desired Rule criteria then click the **(+)** icon to expand the Rule. Select Persistent Path as the Transmit Mode, then choose a Preferred WAN Link for this Rule.

The chosen Path will be the one used for new flows matching this Rule as long as the queue depth is not above the user configurable Persistent Impedance value, which is 50ms by default. When traffic is being queued for more than that amount of time using Paths on the selected WAN Link, then all flows will be moved to other available Paths.



				IP Address					Port							
	Order	Rule Group Name	Application Name	Source	Dest=Src	Dest	Protocol	Protocol #	Source	Dest=Src	Dest	DSCP	VLAN	Rebind Flow on Change	Delete	Clone
⊟	100	<None>	Any	192.168.162.10/32	☐	172.16.27.10/32	Any	0	*	☑	*	Any	*	☐		

Transmit Mode: Persistent Path

☐ Retransmit Lost Packets

Override Service: <N/A>

Preferred WAN Link: Any

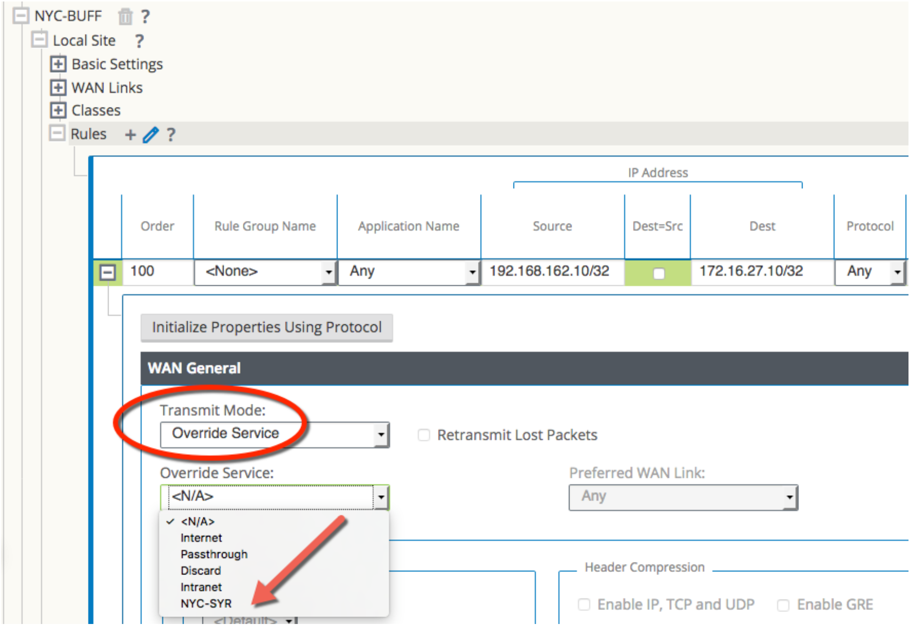
Persistent Impedance(ms): 50

Enable TCP Termination: <Default>

☐ Enable IP, TCP and UDP ☐ Enable GRE

Service Override Traffic Steering

When creating a Rule and using Override Service as the Transmit Mode, in addition to Internet, Passthrough, Discard, and Intranet options, users may now select an alternate Conduit Service. If the selected service is down, the flow will be mapped to its original service. This feature is particularly useful when using Application Match Criteria, as the user can now match on a Host Name and direct that traffic to the local Internet Service.



			IP Address			
Order	Rule Group Name	Application Name	Source	Dest=Src	Dest	Protocol
100	<None>	Any	192.168.162.10/32	□	172.16.27.10/32	Any

Transmit Mode: Override Service

□ Retransmit Lost Packets

Override Service: <N/A>

Preferred WAN Link: Any

Header Compression

□ Enable IP, TCP and UDP □ Enable GRE

Note:

This option is only available for Conduit-specific Rules. It is not an available option for a Rules in Global Conduit Default Sets.

6

Release 3.1 GA P2 Features

This chapter includes features and enhancements released in 3.1 GA P2.

New Features in 3.1 GA P2

The following sections describe new features and enhancements delivered in Oracle SD-WAN Aware 3.1GA P2.

- Site Templates

Users now have the ability to configure Bridge Pairs, VLANs, and Ethernet Interfaces using Site Templates from Aware. This reduces configuration complexity when adding branch locations with similar topologies and saves the user time.

To create a Site Template using Aware, begin on the Basic tab, select the Network view, and click the + **Site Template** button.

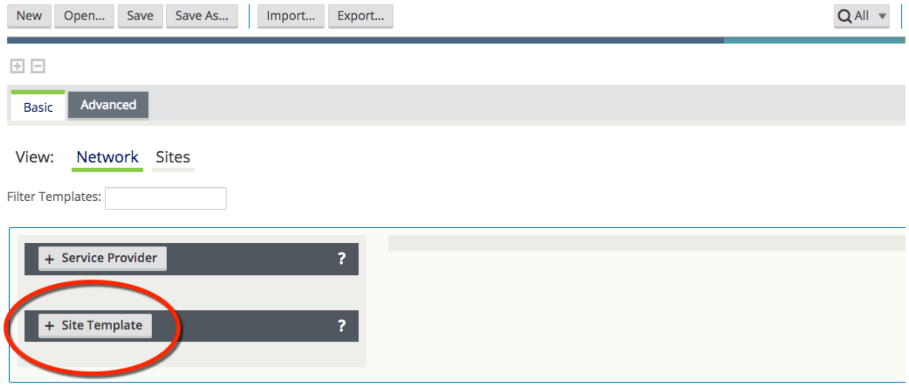


Figure 1

Here, you will select which Ethernet Interfaces should be used, set the Bypass Mode, choose whether to bridge the Interfaces, pick a Security setting, add any required VLANs, and set the WAN DHCP Client option. Click the **Add** button and observe the New_Site_Template now appears on the left-hand side of the page. To change the template name or edit any of its settings, simply click on it.

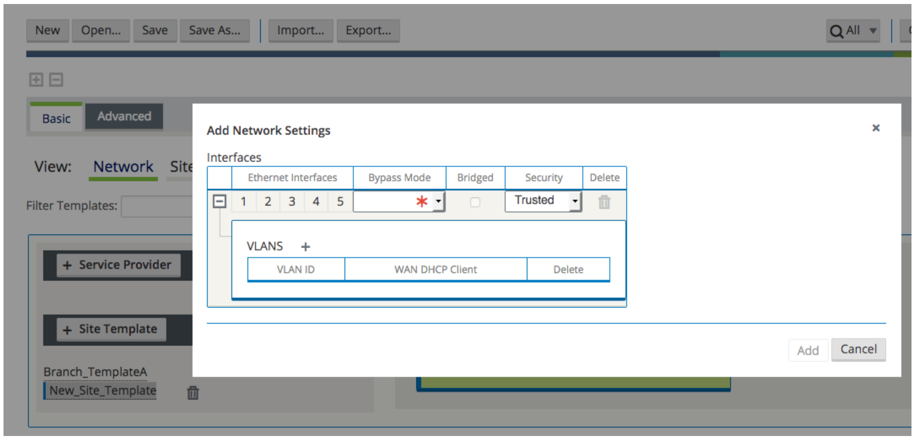
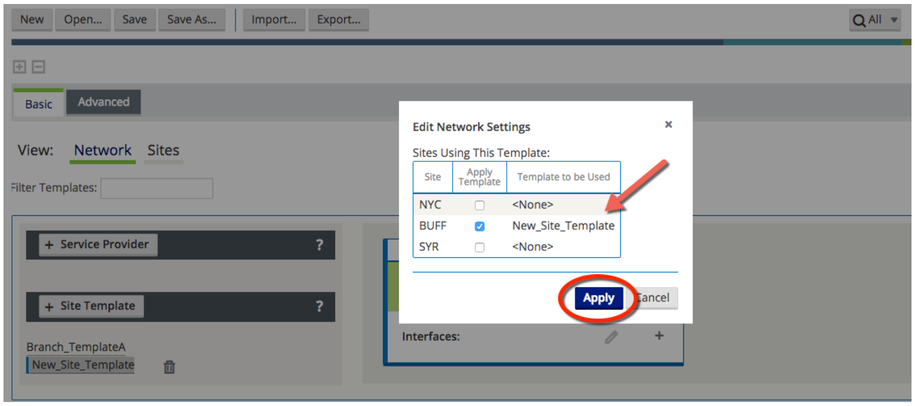


Figure 2

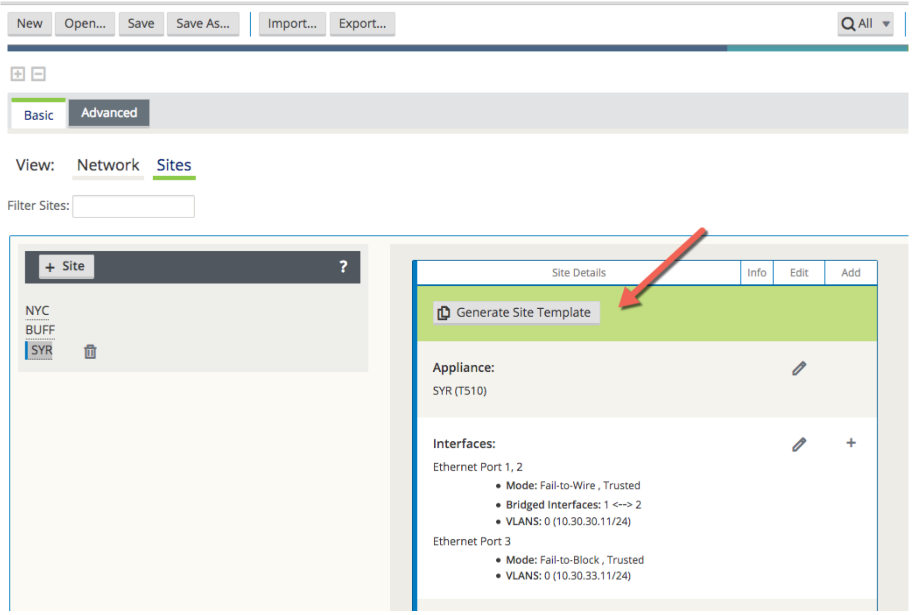
The user will then select which sites should begin using the template.



Site	Apply Template	Template to be Used
NYC	□	<None>
BUFF	☑	New_Site_Template
SYR	□	<None>

Figure 3

Additionally, users may create a Site Template based on an existing site within the configuration. To do so, change the view to Sites, select the branch site name, and click **Generate Site Template.**



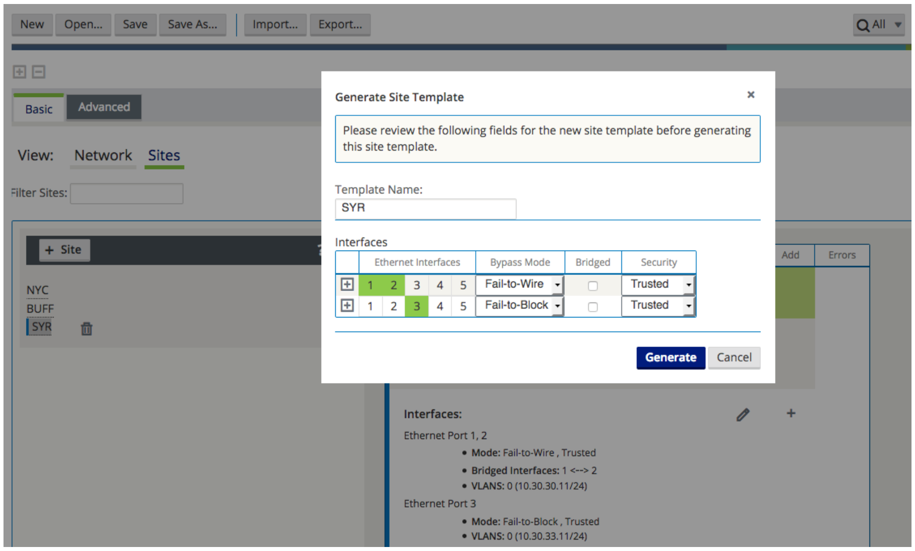
Appliance:
SYR (T510)

Interfaces:
Ethernet Port 1, 2
- **Mode:** Fail-to-Wire , Trusted
- **Bridged Interfaces:** 1 <--> 2
- **VLANS:** 0 (10.30.30.11/24)

Ethernet Port 3
- **Mode:** Fail-to-Block , Trusted
- **VLANS:** 0 (10.30.33.11/24)

Figure 4

In this example, a new Site Template from the existing site, “SYR”. You can confirm the settings in the pop up window and change the template name. The new template has been named Branch_TemplateA.



Generate Site Template

Please review the following fields for the new site template before generating this site template.

Template Name:
SYR

Interfaces

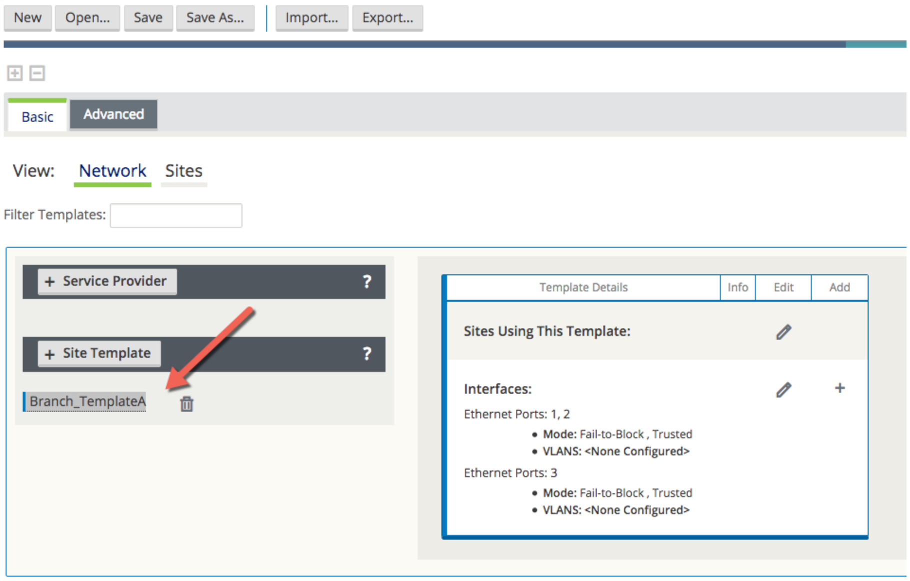
	Ethernet Interfaces					Bypass Mode	Bridged	Security
⊞	1	2	3	4	5	Fail-to-Wire	□	Trusted
⊞	1	2	3	4	5	Fail-to-Block	□	Trusted

Interfaces:
Ethernet Port 1, 2
- **Mode:** Fail-to-Wire , Trusted
- **Bridged Interfaces:** 1 <--> 2
- **VLANS:** 0 (10.30.30.11/24)

Ethernet Port 3
- **Mode:** Fail-to-Block , Trusted
- **VLANS:** 0 (10.30.33.11/24)

Figure 5

Observe Branch_TemplateA now appears on the Network view page.



Sites Using This Template:

Interfaces:

Ethernet Ports: 1, 2

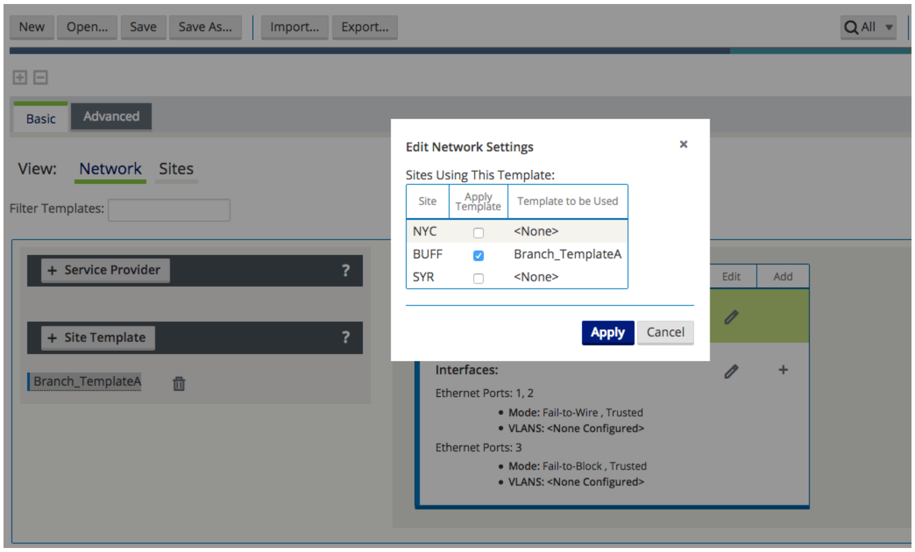
- **Mode:** Fail-to-Block , Trusted
- **VLANS:** <None Configured>

Ethernet Ports: 3

- **Mode:** Fail-to-Block , Trusted
- **VLANS:** <None Configured>

Figure 6

Assign the new template to a site. In the example below, Branch_TemplateA has been assigned to branch site “BUFF”.



Edit Network Settings

Sites Using This Template:

Site	Apply Template	Template to be Used
NYC	☐	<None>
BUFF	☑	Branch_TemplateA
SYR	☐	<None>

Interfaces:

Ethernet Ports: 1, 2

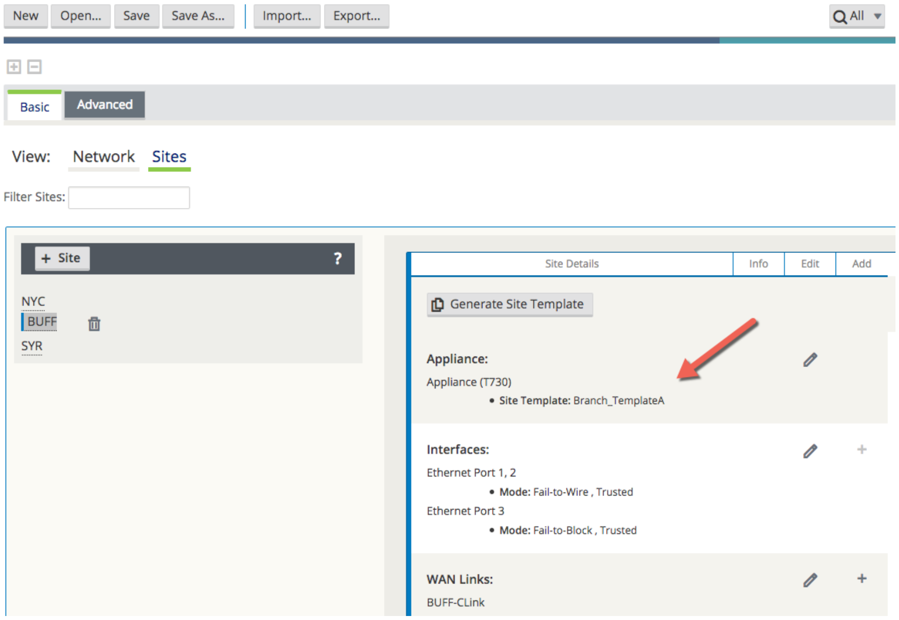
- **Mode:** Fail-to-Wire , Trusted
- **VLANS:** <None Configured>

Ethernet Ports: 3

- **Mode:** Fail-to-Block , Trusted
- **VLANS:** <None Configured>

Figure 7

Back on the Sites view, site “BUFF” shows it has been assigned to Site Template Branch_TemplateA.



Appliance:
Appliance (T730)
- **Site Template:** Branch_TemplateA

Interfaces:
Ethernet Port 1, 2
- **Mode:** Fail-to-Wire , Trusted

Ethernet Port 3
- **Mode:** Fail-to-Block , Trusted

WAN Links:
BUFF-CLink

Figure 8

Additional Features in Aware 3.1 GA P2

Additional features included in Aware 3.1 GA P2 include Service Provider – Aware (SP-Aware), OpenDaylight API for service provider configuration, and Restful APIs for service provider network Change Management.

7

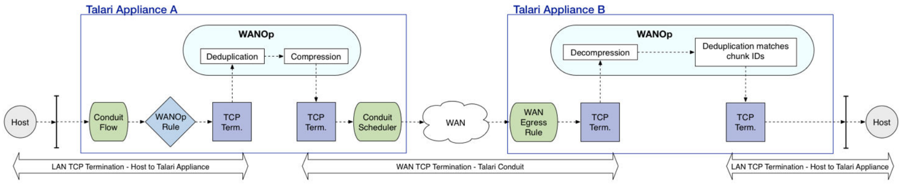
Release 4.0 Features

This chapter includes features and enhancements released in 4.0.

WAN Optimization

Edge 7.0 GA introduces the capability to perform WAN Optimization on TCP flows, allowing users to simplify branch network infrastructure by consolidating SD-WAN and WAN Optimization services on a single device. WAN Optimization (WANOp) increases efficiency across the WAN for bulk file-transfer traffic, specifically for data requested by more than one user at the same location.

When WAN Optimization is enabled for a flow, TCP Termination is automatically enabled as well. This feature splits a single TCP connection into 3 separate TCP connections, all managed and maintained by the Oracle, in to offer maximum throughput and reliable transfer across the WAN via the Oracle conduit. The diagram below shows an example WANOp flow between two Edge sites.



WAN Optimization is supported on the E100, T3010v2, T5000v2, and T5200 Appliance models.

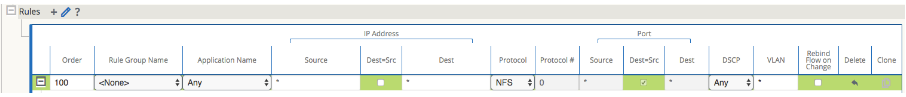
Session Capacity for Supported Models

Appliance Model	Number of Sessions
E100	8000
T3010v2	8000
T5000v2	16000
T5200	16000

The Oracle WANOp solution is configured on a per-rule basis and performs deduplication and compression on TCP Conduit traffic.

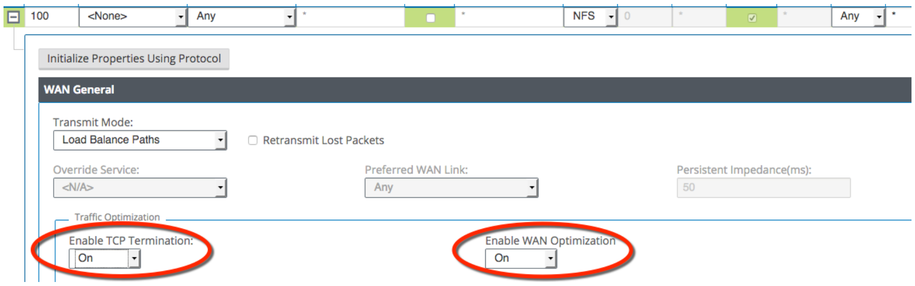
Configuring WAN Optimization via Aware

Using the web UI for Aware, navigate to **Manage > Configuration** and **Import** the current configuration file from the Active NCN. On the **Advanced** tab, under **Global > Default Sets > Conduit Default Sets > [Conduit Default Set] > Rules**, click the **(+)** icon to create a rule for the type of traffic to be optimized.



			IP Address					Port							
Order	Rule Group Name	Application Name	Source	Dest=Src	Dest	Protocol	Protocol #	Source	Dest=Src	Dest	DSCP	VLAN	Rebind Flow on Change	Delete	Clone
100	<None>	Any	*	□	*	NFS	0	*	☑	*	Any	*	□		

Expand the rule properties. WAN Optimization is enabled via a dropdown menu under the **WAN General** section. When WANOp is enabled, TCP Termination is also enabled by default.



Transmit Mode: Load Balance Paths

□ Retransmit Lost Packets

Override Service: <N/A>

Preferred WAN Link: Any

Persistent Impedance(ms): 50

Enable TCP Termination: On

Enable WAN Optimization: On

> **Note:**
>
> When WANOp is enabled, TCP Termination is enabled for WAN Optimization to function as designed. If desired, the user can also enable TCP Termination independently from the WAN Optimization capability, as shown above.

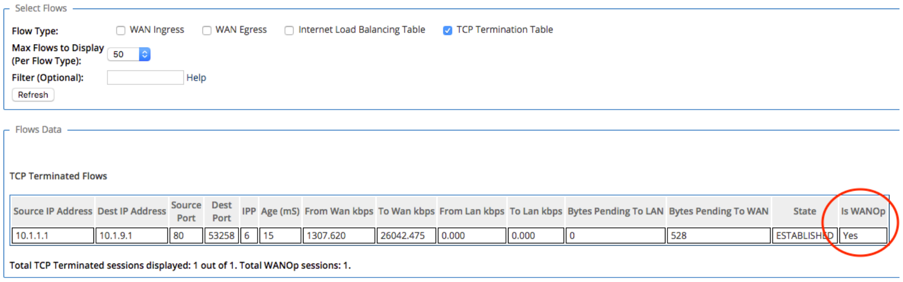
A reciprocal rule enabling WANOp will be generated automatically at the remote site of the selected Conduit.

Once your configuration is complete, **Export** it to the **Change Management inbox** and follow the prompts through the Change Management process until the new configuration has been Activated.

Verification

To verify that traffic flow is being optimized, navigate to the **Monitor** > **Flows** page on the NCN. Uncheck the WAN Ingress and WAN Egress Flow Types, and check TCP Termination, then click the refresh button to display only TCP Terminated flows.

The flows table will show detailed information about all TCP Terminated flows, including their WANOp state, as shown below:



Flow Type: □ WAN Ingress □ WAN Egress □ Internet Load Balancing Table ☑ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

Filter (Optional):

TCP Terminated Flows

Source IP Address	Dest IP Address	Source Port	Dest Port	IPP	Age (mS)	From Wan kbps	To Wan kbps	From Lan kbps	To Lan kbps	Bytes Pending To LAN	Bytes Pending To WAN	State	Is WANOp
10.1.1.1	10.1.9.1	80	53258	6	15	1307.620	26042.475	0.000	0.000	0	528	ESTABLISHED	Yes

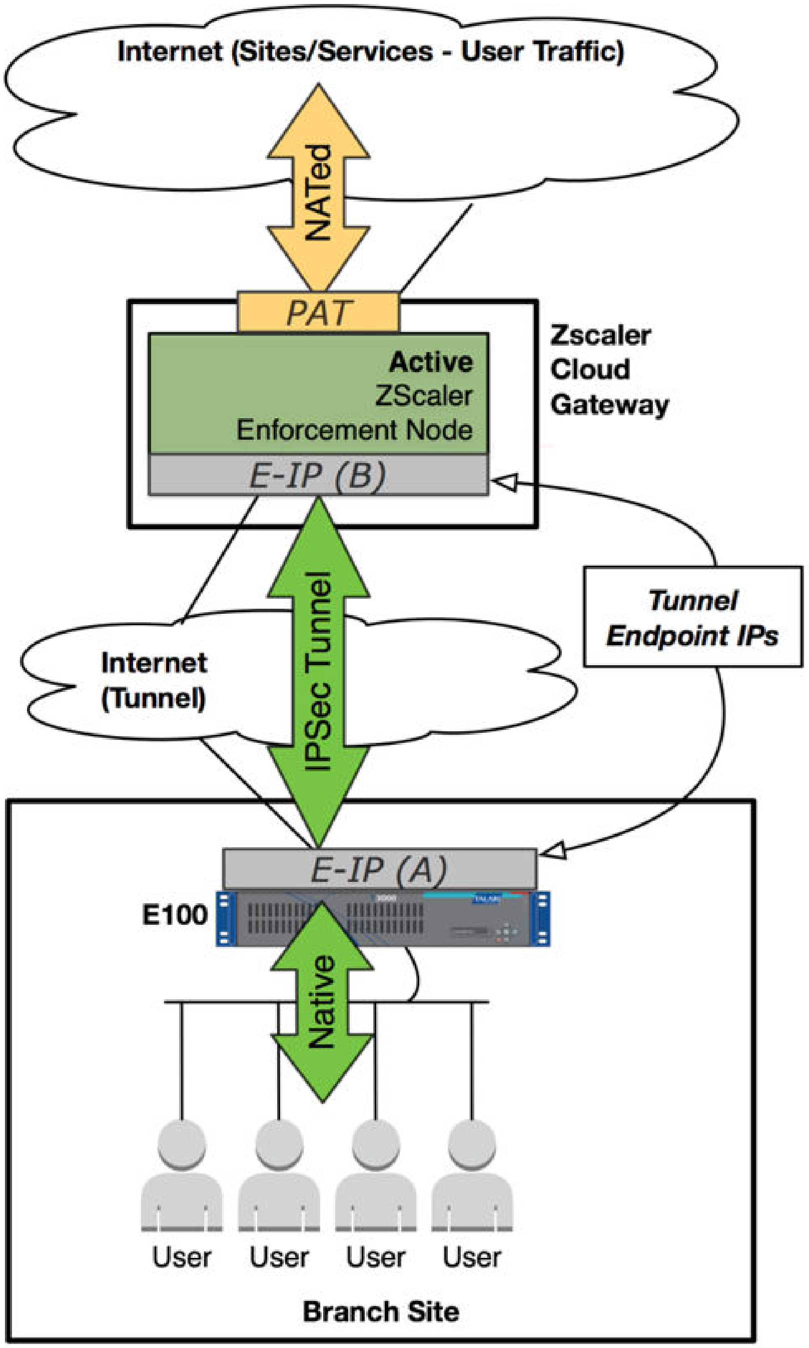
Total TCP Terminated sessions displayed: 1 out of 1. Total WANOp sessions: 1.

For more information on the Oracle WAN Optimization solution, including more detailed capabilities, performance, and monitoring options, please see the Oracle WAN Optimization Guide.

Zscaler Integration

Zscaler is a Cloud Security Provider (CSP) that delivers many of the most desirable Next Generation Firewall features including Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Data Loss Prevention (DLP), Sandboxing, and others.

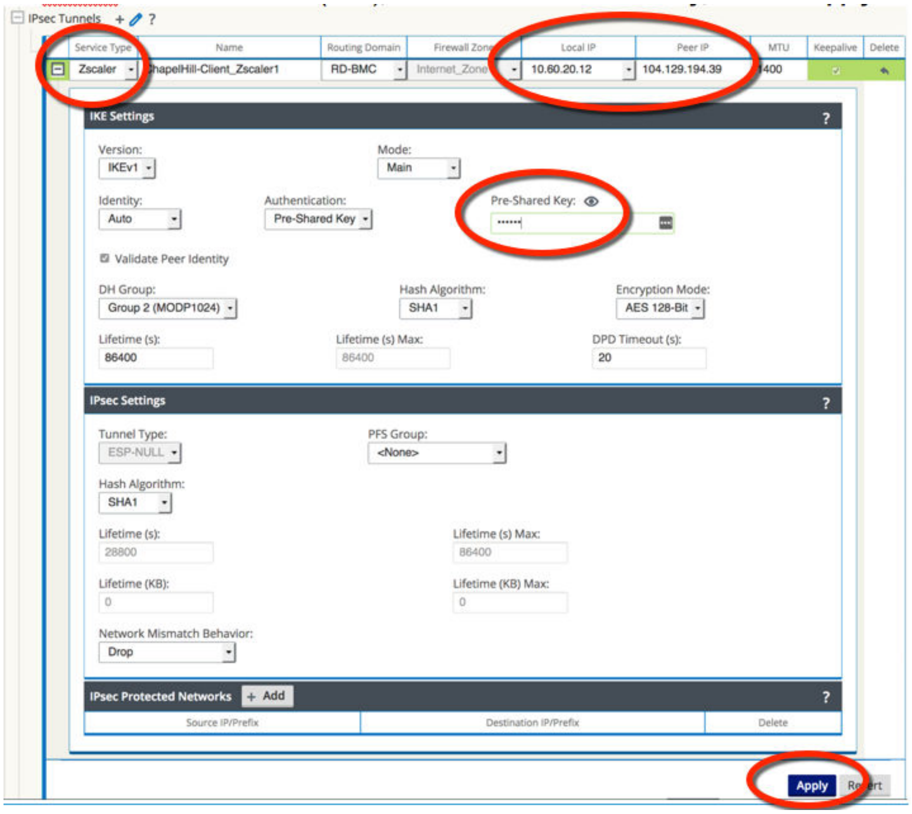
Introduced in Oracle SD-WAN Edge R7.0 GA, users can now integrate a branch office Appliance with the Zscaler Cloud Security Gateway via IPSec tunneling, for the purposes of tunneling Internet-destined traffic to Zscaler for cloud-hosted filtering and security services.



Configuration via Aware

To configure a Zscaler IPSec tunnel using Aware, navigate to **Manage > Configuration** and **Import** the current configuration file from the Active NCN. Click on the **Advanced** tab, expand **Connections > [Site Name] > IPSec Tunnels** and click the **(+)** icon.

Select Zscaler as the **Service Type**, select the **Local IP** address, fill in the **Peer IP** address of the Zscaler Enforcement Node (ZEN), enter the IKE **Pre-Shared Key**, and click **Apply**.



Service Type	Name	Routing Domain	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
Zscaler	hapelHill-Client_Zscaler1	RD-BMC	Internet_Zone	10.60.20.12	104.129.194.39	1400	☑	

IKE Settings

Version: IKEv1
Mode: Main
Identity: Auto
Authentication: Pre-Shared Key
Pre-Shared Key: ••••••
☑ Validate Peer Identity
DH Group: Group 2 (MODP1024)
Hash Algorithm: SHA1
Encryption Mode: AES 128-Bit
Lifetime (s): 86400
Lifetime (s) Max: 86400
DPD Timeout (s): 20

IPsec Settings

Tunnel Type: ESP-NULL
PFS Group: <None>
Hash Algorithm: SHA1
Lifetime (s): 28800
Lifetime (s) Max: 86400
Lifetime (KB): 0
Lifetime (KB) Max: 0
Network Mismatch Behavior: Drop

IPsec Protected Networks + Add

Source IP/Prefix	Destination IP/Prefix	Delete

> **Note:**
>
> When you add an IPSec tunnel with a Service Type of **Zscaler**, the following default configurations will be applied that are not applied when selecting **LAN** or **Intranet Service Types.**

- Firewall – Adds a Deny policy from Default_LAN_Zone to Untrusted_Internet_Zone.
- NAT – Deletes the default outbound PAT policy, if one exists.
- Routing – Adds a 0.0.0.0/0 route over the Zscaler tunnel and a /32 host-route of the tunnel Peer IP to the gateway.

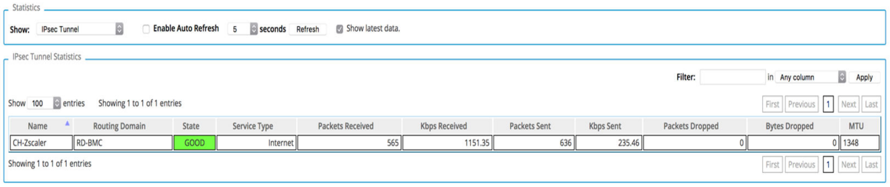
Save the configuration and **Export** it to the **Change Management inbox** of the NCN. Follow the Change Management process to **Stage** and **Activate** the new configuration.

Verification

Once the new configuration is running, follow the steps below to verify functionality.

1. Generate Internet traffic from a host on the LAN to a URL that has been blocked by Zscaler.

2. Verify the Zscaler IPSec Tunnel status in the web UI of the Appliance under **Monitor**, and then **Statistics**, and then **IPSec Tunnel**.



Show: IPsec Tunnel □ Enable Auto Refresh 5 seconds ☑ Show latest data.

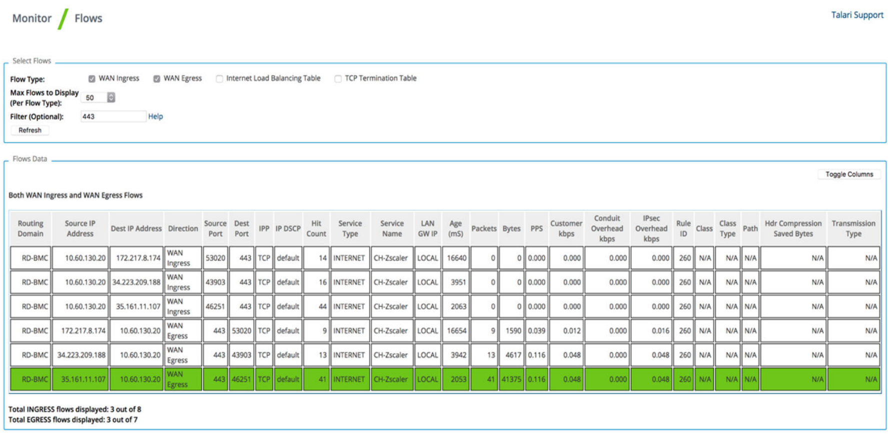
Filter: in Any column

Show 100 entries Showing 1 to 1 of 1 entries

Name	Routing Domain	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropped	MTU
CH-Zscaler	RD-BMC	GOOD	Internet	565	1151.35	636	235.46	0	0	1348

Showing 1 to 1 of 1 entries

3. Verify the flow of the generated traffic through the Appliance via **Monitor**, and then **Flows.** Once you have identified the flow, confirm the Service Type as INTERNET.



Flow Type: ☑ WAN Ingress ☑ WAN Egress □ Internet Load Balancing Table □ TCP Termination Table

Max Flows to Display (Per Flow Type): 50

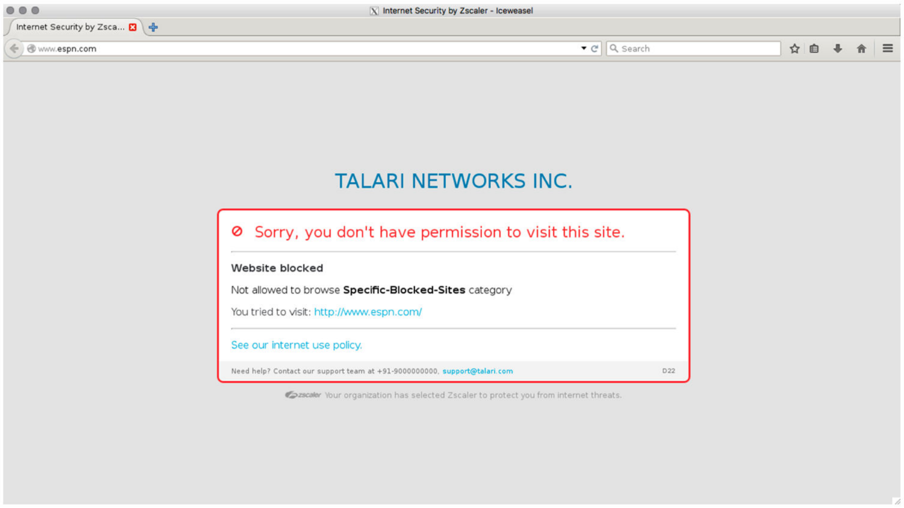
Filter (Optional): 443

Both WAN Ingress and WAN Egress Flows

Routing Domain	Source IP Address	Dest IP Address	Direction	Source Port	Dest Port	IPP	IP DSCP	Hit Count	Service Type	Service Name	LAN GW IP	Age (mS)	Packets	Bytes	PPS	Customer kbps	Conduit Overhead kbps	IPsec Overhead kbps	Rule ID	Class	Class Type	Path	Hdr Compression Saved Bytes	Transmission Type
RD-BMC	10.60.130.20	172.217.8.174	WAN Ingress	53020	443	TCP	default	14	INTERNET	CH-Zscaler	LOCAL	16640	0	0	0.000	0.000	0.000	0.000	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	10.60.130.20	34.223.209.188	WAN Ingress	43903	443	TCP	default	16	INTERNET	CH-Zscaler	LOCAL	3951	0	0	0.000	0.000	0.000	0.000	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	10.60.130.20	35.161.11.107	WAN Ingress	46251	443	TCP	default	44	INTERNET	CH-Zscaler	LOCAL	2063	0	0	0.000	0.000	0.000	0.000	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	172.217.8.174	10.60.130.20	WAN Egress	443	53020	TCP	default	9	INTERNET	CH-Zscaler	LOCAL	16654	9	1590	0.039	0.012	0.000	0.016	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	34.223.209.188	10.60.130.20	WAN Egress	443	43903	TCP	default	13	INTERNET	CH-Zscaler	LOCAL	3942	13	4617	0.116	0.048	0.000	0.048	260	N/A	N/A	N/A	N/A	N/A
RD-BMC	35.161.11.107	10.60.130.20	WAN Egress	443	46251	TCP	default	41	INTERNET	CH-Zscaler	LOCAL	2053	41	41375	0.116	0.048	0.000	0.048	260	N/A	N/A	N/A	N/A	N/A

Total INGRESS flows displayed: 3 out of 8
Total EGRESS flows displayed: 3 out of 7

4. Verify Zscaler is blocking the traffic.



Internet Security by Zscaler - Iceweasel
Internet Security by Zsca...
www.espn.com
Search

TALARI NETWORKS INC.

Sorry, you don't have permission to visit this site.

Website blocked

Not allowed to browse **Specific-Blocked-Sites** category

You tried to visit: http://www.espn.com/

See our internet use policy.

Need help? Contact our support team at +91-9000000000, support@talari.com D22

zscaler Your organization has selected Zscaler to protect you from internet threats.

In the event the IPSec Tunnel between the Appliance and the Zscaler ZEN goes down, the 0.0.0.0/0 route through the tunnel will become unreachable and pulled from the Oracle's routing table. Traffic will hit the next available, reachable 0.0.0.0/0 route out to the Internet. Route reachability can be verified in the Appliance's web UI under **Monitor > Statistics > Routes**.

Note:

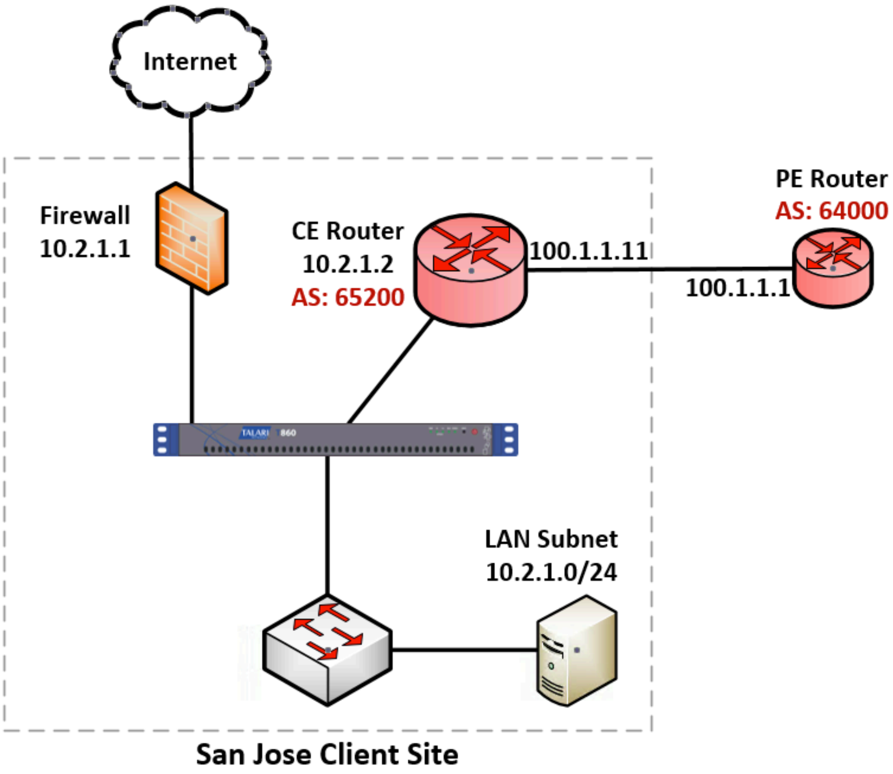
R7.0 GA only supports a single VRF/routing domain for Zscaler.

Customer Edge (CE) Router Replacement Within the Edge

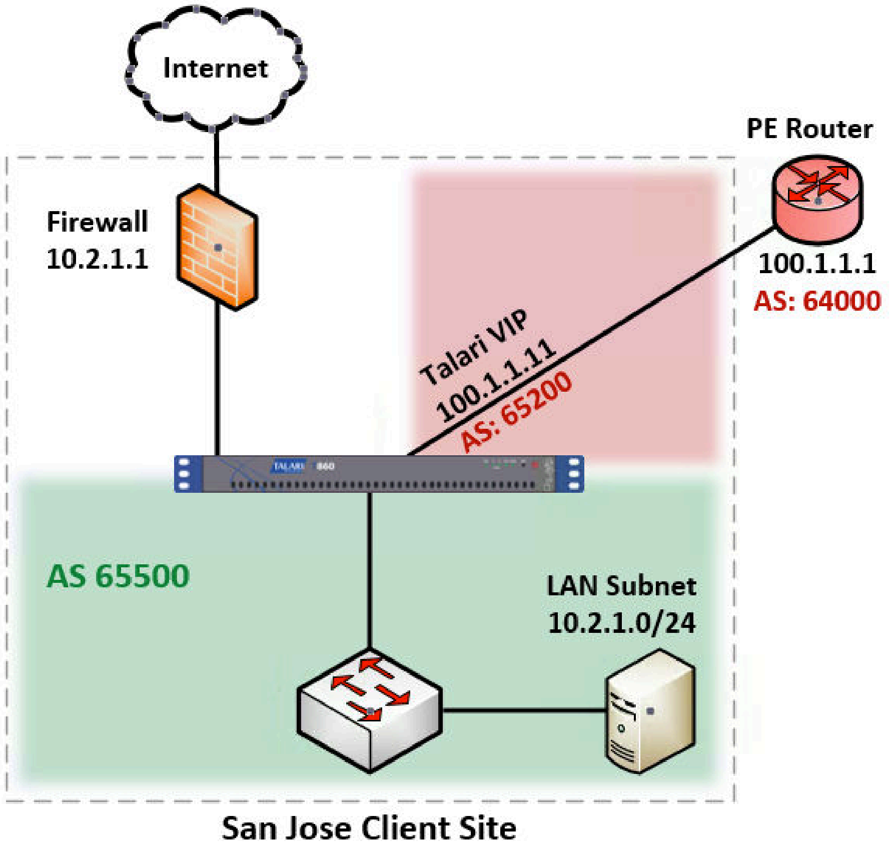
Oracle SD-WAN Edge 7.0 introduces the ability to replace a Customer Edge Router with a Oracle Adaptive Private Network Appliance. This is accomplished by leveraging the Oracle APNA's ability to masquerade its Local Autonomous System (AS) number (on a per-neighbor basis) so that it can peer with a Provider Edge (PE) Router in the same way that a Customer Edge (CE) Router does. The Oracle APNA can peer with other BGP neighbors as well, using either its true Local AS number or a masqueraded AS number.

Installation Summary

Sample Oracle SD-WAN Edge site before replacing the CE Router with the Oracle APNA.



Sample Oracle SD-WAN Edge site after replacing the CE Router with the Oracle APNA.

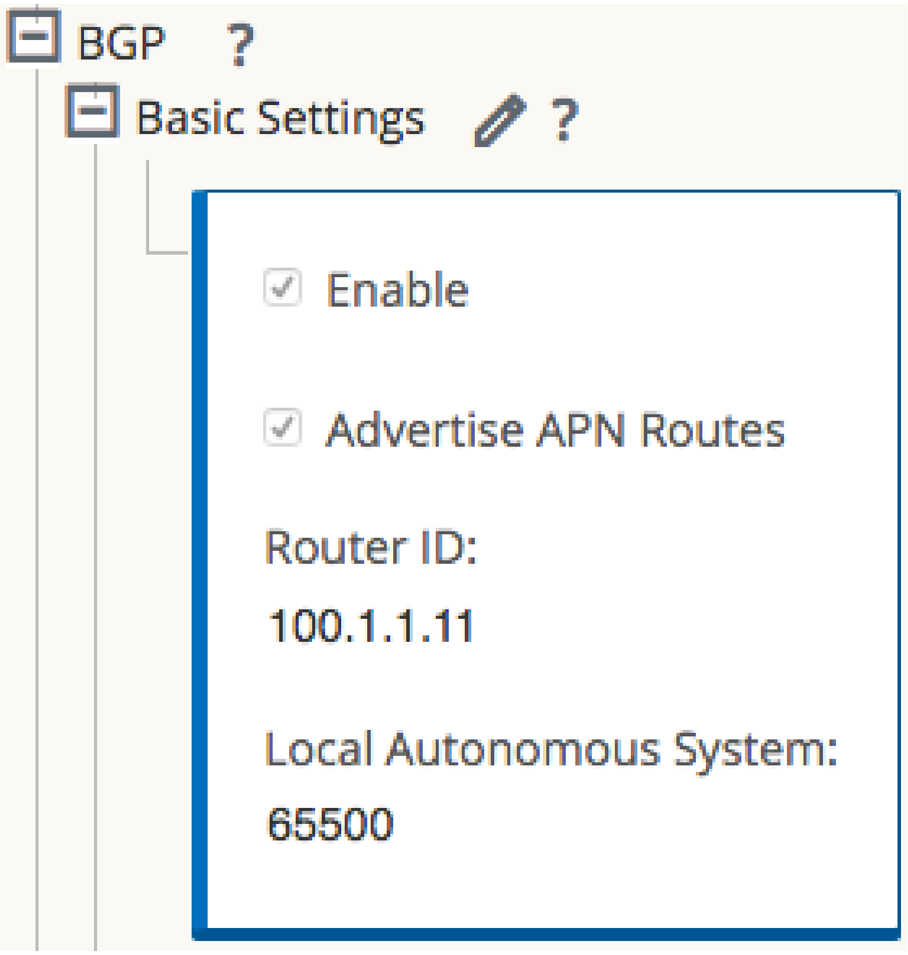


The CE router is removed and the Oracle APNA peers directly with the PE router via eBGP by masquerading its AS number as the replaced CE router's AS number (AS 65200). The APNA's actual Local AS number is 65500 and it can peer via iBGP with local routers in this AS.

If desired, APNAs can also peer with each other via iBGP over a Conduit. This allows Edge to act as an Autonomous System. The primary use-case intended for Edge as an Autonomous System consists of the primary NCN, and secondary NCN if required, are configured as Route-Reflectors, and Clients using an iBGP peering session to the NCN(s) for BGP reachability information.

BGP Configuration via Aware

Import the current configuration running on the Active NCN, then navigate to **Connections > [Site Name] > Route Learning > BGP > Basic Settings** and click the pencil icon to edit.



☑ Enable

☑ Advertise APN Routes

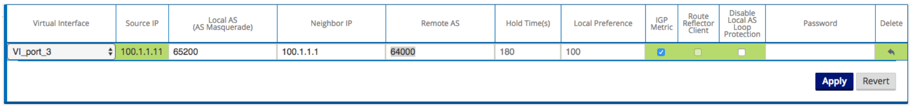
Router ID:
100.1.1.11

Local Autonomous System:
65500

Check the **Enable** box to enable BGP on the APNA. If it is desirable to advertise Edge routes to BGP peers, check the **Advertise Routes** box. Enter an optional **Router ID** and enter the **Local Autonomous System** number.

Neighbors

Use the **(+)** icon to the right of the **Neighbors** section to add BGP neighbor entries.



Virtual Interface	Source IP	Local AS (AS Masquerade)	Neighbor IP	Remote AS	Hold Time(s)	Local Preference	IGP Metric	Route Reflector Client	Disable Local AS Loop Protection	Password	Delete
VI_port_3	100.1.1.11	65200	100.1.1.1	64000	180	100	☑	□	□		↶

Choose the appropriate **Virtual Interface**, enter the **Local AS** number or enter an AS number to Masquerade the Local AS number as, and enter the **Neighbor IP** address.

Note: If the Local AS field in the **Neighbors** section is left blank, the default behavior is to use the Local AS defined in the previous step under **Basic Settings**. If no Local AS is defined in either of these sections, no AS number will be used.

The following options may also be set:

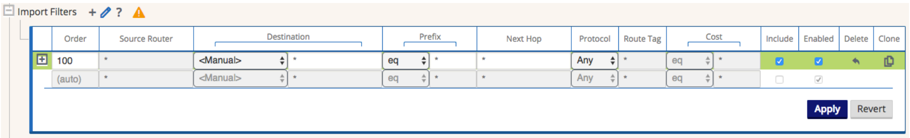
- **Hold Time(s)** - Time in seconds to wait before declaring a neighbor as DOWN.
- **Local Preference** - Sets the BGP attribute Local Preference for routes learned from the neighbor specified.

- **Route Reflector Client** - The Oracle APNA will act as a Route Reflector and the neighbor will be treated as a Route Reflection Client.
- **Disable Local AS Loop Protection** - By default, BGP routes learned that contain the APNA's Local AS number in the AS path will be rejected to guard against routing loops. This can be disabled for situations in which learned routes are prepended with the APNA's Local AS number for the purpose of influencing path selection in BGP.
- **Password** - Used if the BGP session requires MD5 authentication.

Import and Export Filters

Now that BGP is enabled and neighbors have been configured, the Import Filters can be configured under **Connections > [Site Name] > Route Learning > Import Filters.**

By default, no routes will be imported until Import Filters have been added, as the default filter rejects all route advertisements. Expand the Import Filters section and use the **(+)** icon to add a filter.



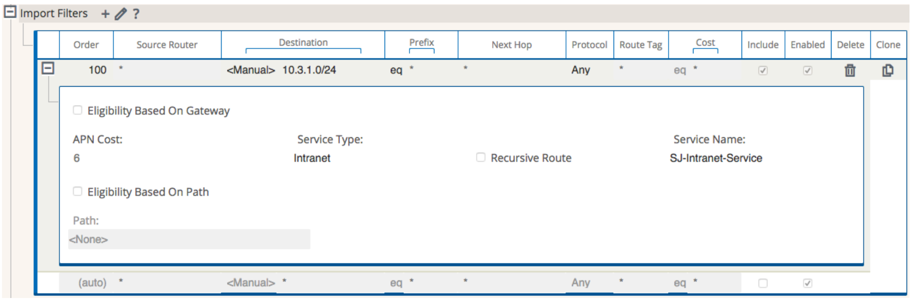
	Order	Source Router	Destination		Prefix		Next Hop	Protocol	Route Tag	Cost		Include	Enabled	Delete	Clone
⊞	100	*	<Manual>	*	eq	*	*	Any	*	eq	*	☑	☑	↶	⧉
	(auto)	*	<Manual>	*	eq	*	*	Any	*	eq	*	□	☑		

Note:

For each added filter, use any combination of the **Destination**, **Prefix**, and **Next Hop** fields to match desired BGP routes to learn. If these fields are left with their default value of **(*)**, all advertised BGP routes will be imported to the Oracle. Additionally, it is important to understand the impact of the **Include** and **Enabled** checkboxes. If **Include** is checked, routes that match the filter will be imported. On the same filter, if **Include** is not checked, then routes that match the filter will not be imported. The **Enabled** checkbox simply enables or disables the filter entirely.

Use the **(+)** icon to the left of the **Order** column to reveal Edge specific options. Click the **Service Type** dropdown box to expose the available options. Depending on the Service Type chosen, various additional options will be available and are listed below.

- **Export Route to Appliances:** If the Export Route to Appliances checkbox is enabled, the Appliance will communicate route data to Appliances at other sites if WAN-to-WAN forwarding is enabled. This functionality is enabled by default but only applies to the following Service Types: Local and LAN GRE Tunnel.
- **Eligibility Based on Gateway:** If the gateway becomes unreachable, this feature will ensure that traffic is not sent to matching routes.
- **Cost:** The cost will be applied to the matched routes when importing into the Appliance's route table. The default Edge Cost is 6.
- **Service Type:** Choose a Service Type from all the existing, supported Oracle Services.
- **Recursive Route:** When the Service Type is Conduit, check this option to find the Conduit name from an imported route's source router automatically.
- **Service Name:** The name of the service that matching routes will use.
- **Eligibility Based on Path:** If enabled, Path state becomes criteria for filters.



	Order	Source Router	Destination	Prefix	Next Hop	Protocol	Route Tag	Cost	Include	Enabled	Delete	Clone
⊟	100	*	<Manual> 10.3.1.0/24	eq *	*	Any	*	eq *	☑	☑	🗑	⧉
	(auto)	*	<Manual> *	eq *	*	Any	*	eq *	□	☑		

□ Eligibility Based On Gateway

APN Cost: 6

Service Type: Intranet

□ Recursive Route

Service Name: SJ-Intranet-Service

□ Eligibility Based On Path

Path: <None>

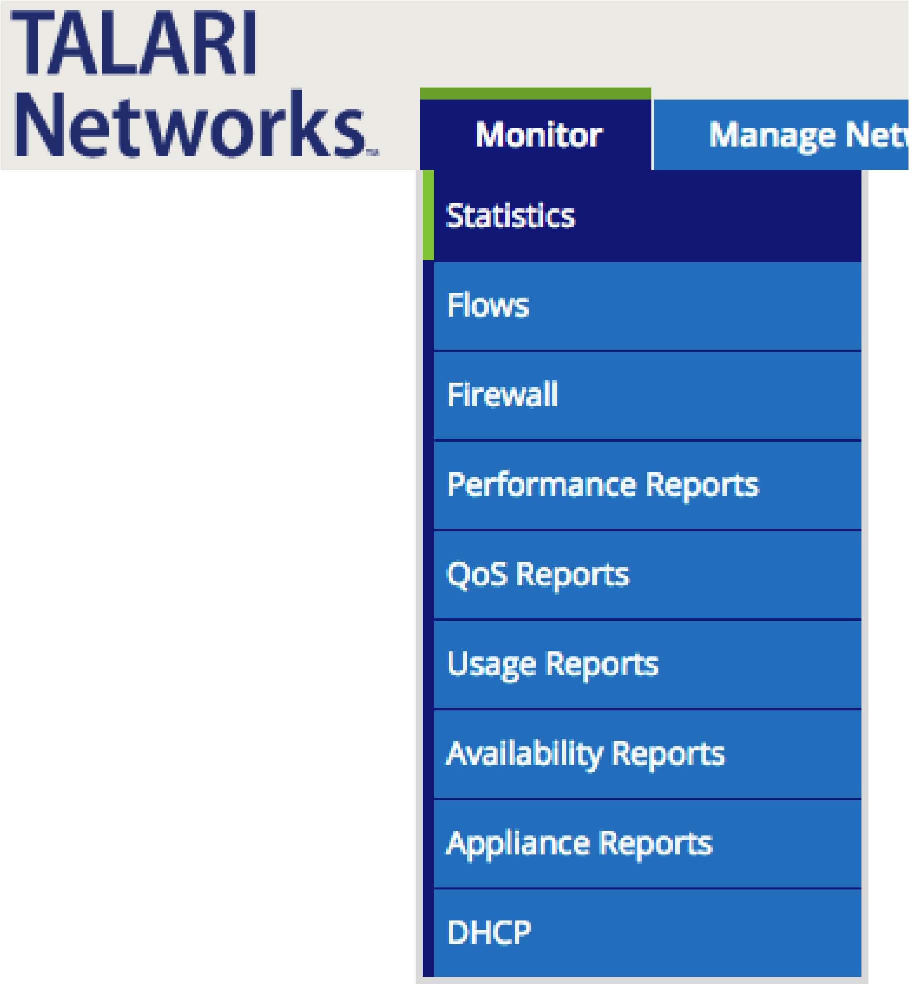
Once configuration of the Edge is complete, it should be saved and the **Change Management** process from the NCN should be used to push the configuration changes to the APNAs.

Static Routes File

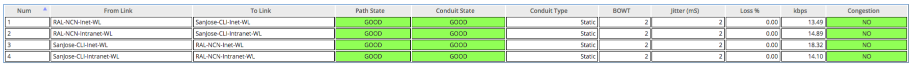
Appliances provide a **Static Routes** file that can be edited to define routes that should persist through software and configuration changes made to Edge. This is used for inserting static routes into the dynamic routing table, not the Edge routing table. It ensures that any necessary static routes are advertised to the PE router after the CE router replacement, regardless of changes to the Edge configuration. By default, static routes defined in this file will be advertised to all neighbors within the specified routing domain.

BGP Verification and Troubleshooting

After the replacement, login to the web UI of the APNA and navigate to **Monitor > Statistics** to verify that the change is successful.

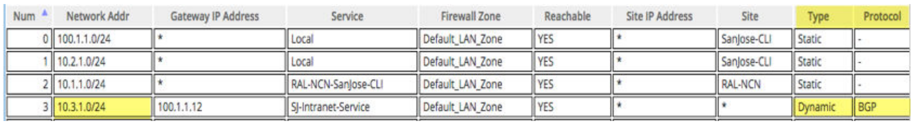


This will bring up the **Paths (Summary)** statistics page. Verify that **Path State** and **Conduit State** report GOOD for each WAN Link as shown in the image below.



Num	From Link	To Link	Path State	Conduit State	Conduit Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	RAL-NCN-Inet-WL	SanJose-CLI-Inet-WL	GOOD	GOOD	Static	2	2	0.00	13.49	NO
2	RAL-NCN-Intranet-WL	SanJose-CLI-Intranet-WL	GOOD	GOOD	Static	2	2	0.00	14.89	NO
3	SanJose-CLI-Inet-WL	RAL-NCN-Inet-WL	GOOD	GOOD	Static	2	2	0.00	18.32	NO
4	SanJose-CLI-Intranet-WL	RAL-NCN-Intranet-WL	GOOD	GOOD	Static	2	2	0.00	14.10	NO

Next, use the dropdown menu to select **Routes** to verify that the expected routes are properly being learned via BGP. In the example below, notice the 10.3.1.0/24 route shows **Type** as Dynamic and **Protocol** as BGP.



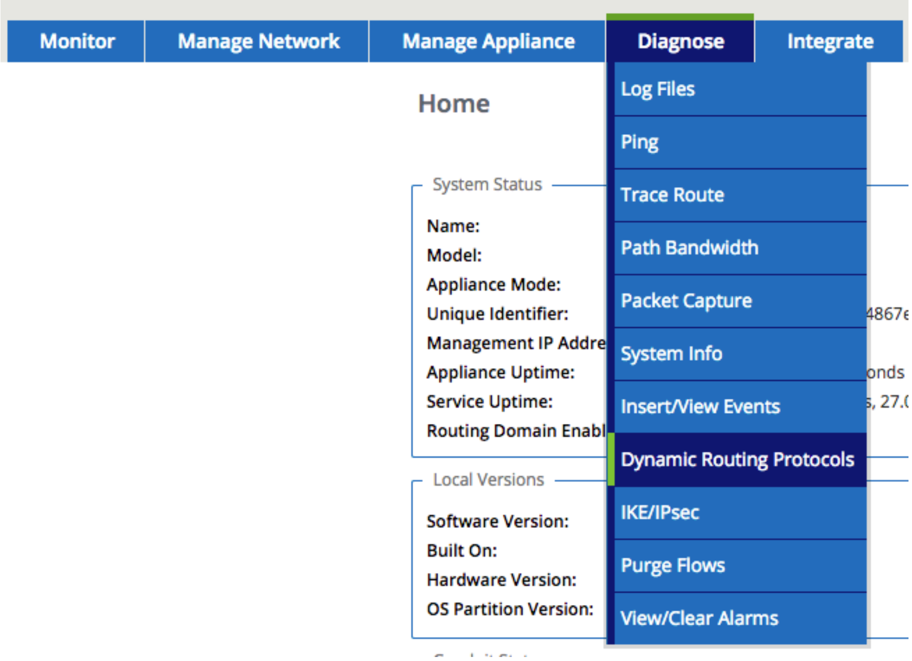
Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol
0	100.1.1.0/24	*	Local	Default_LAN_Zone	YES	*	SanJose-CLI	Static	-
1	10.2.1.0/24	*	Local	Default_LAN_Zone	YES	*	SanJose-CLI	Static	-
2	10.1.1.0/24	*	RAL-NCN-SanJose-CLI	Default_LAN_Zone	YES	*	RAL-NCN	Static	-
3	10.3.1.0/24	100.1.1.12	SJ-Intranet-Service	Default_LAN_Zone	YES	*	*	Dynamic	BGP

Note:

The route must also be considered reachable for it to be used.

BGP Troubleshooting Enhancements

The Appliance's web UI provides tools to gather information about the Dynamic Routing Protocols you have enabled. These tools can be found under **Diagnose > Dynamic Routing Protocols**.



Below are descriptions of each option.

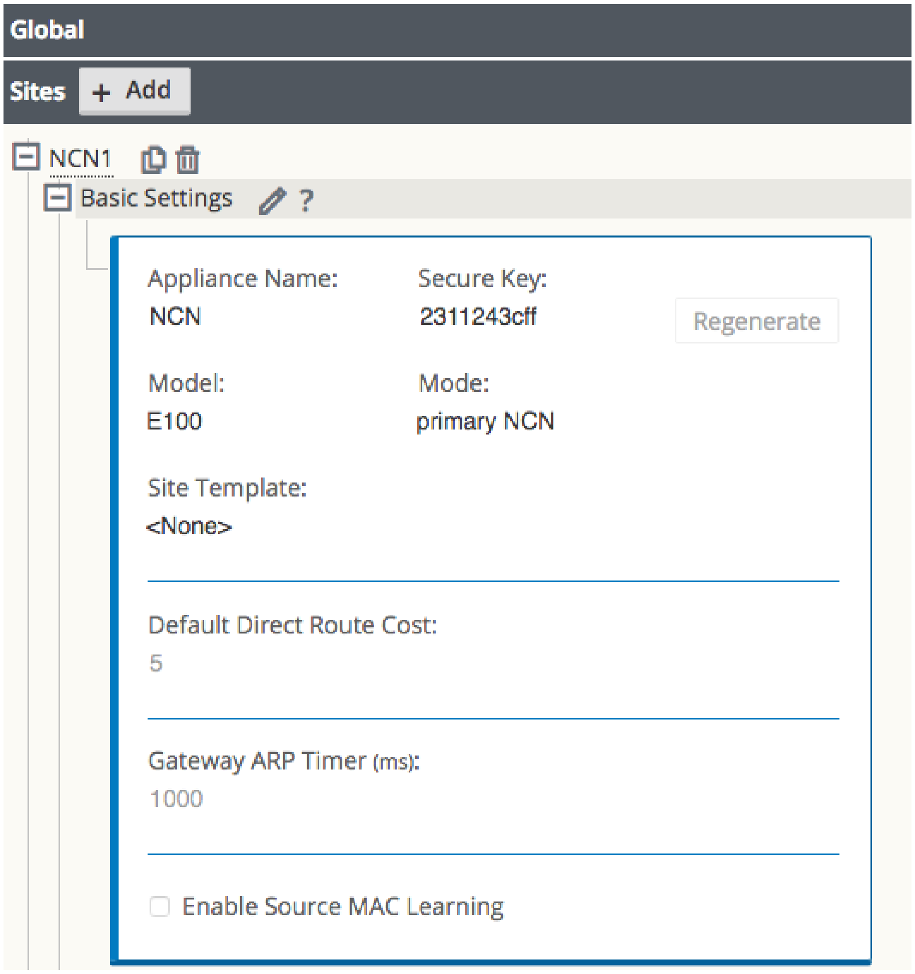
- **BGP State** - Shows an overview of the current state of each Dynamic Routing Protocol instance.
- **Show Route Table**- Provides an overview of each route prefix.
- **Show Route Table (detailed)** - Provides an overview of each route prefix and protocol-specific attributes such as Next Hop, Local Preference, AS Path, etc.
- **Show Protocol** - Outputs a list of routing protocols that are currently running and their states.
- **BGP Show Route Table Protocol** - Shows prefixes associated with each BGP instance/ neighbor.
- **BGP Show Route Table Protocol NWAddress/Mask Table -** Shows prefixes associated with each BGP instance/neighbor and allows filtering for specific prefixes.
- **Oracle Protocol Table -** Shows only the Edge routing table.
- **Show Route Count in Table** - Gives a count of all entries in the routing table (BGP and Edge).
- **BGP Show Route Export** - Shows routes being advertised from the Appliance.
- **BGP Show Route Export (detailed)** - Shows routes being advertised from the Appliance, as well as routing protocol attributes.
- **BGP Show Route Preexport** - Shows all applicable routes for advertisement.

- **BGP Show Route Preexport (detailed)** - Shows all applicable routes for advertisement, as well as routing protocol attributes.
- **Appliance ifconfig** - Shows the output of the "ifconfig" command to provide the user detailed information about each active interface port.
- **BGP Configure** - Reloads the advanced routing configuration.
- **BGP Restart** - Restarts all routing protocols.

For additional information on this topic (including how to edit the Static Routes file) please refer to the CE Router Replacement Guide.

E100 as an NCN

Edge 7.0 GA now supports deployment of the E100 Appliance as a primary and secondary NCN for up to 8 Client sites (9 total sites per-network). This configuration may be done using Aware by importing the configuration currently running on the Active NCN. From the **Advanced** tab under **Sites > [Site Name] > Basic Settings** where the **Model** should be the E100 and the **Mode** can now be either primary NCN or secondary NCN.



Appliance Name: NCN

Secure Key: 2311243cff

Model: E100

Mode: primary NCN

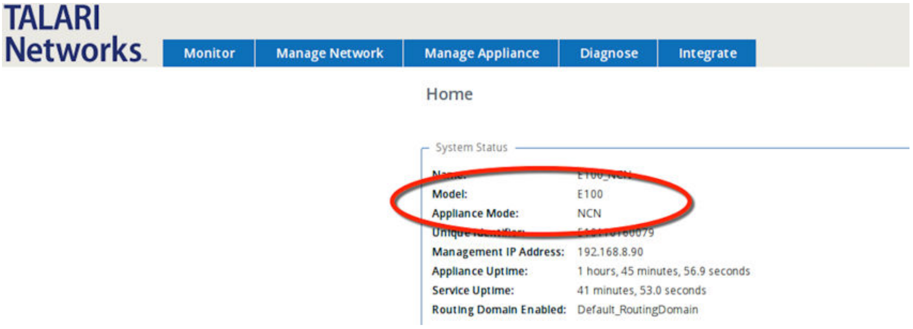
Site Template: <None>

Default Direct Route Cost: 5

Gateway ARP Timer (ms): 1000

□ Enable Source MAC Learning

After completing the configuration, the user will **Export** it to the **Change Management inbox** of the NCN and follow the prompts to create a package for the E100 appliance. Once you have uploaded the package to the E100, the Home Page will reflect that the E100 is functioning as the NCN Appliance.

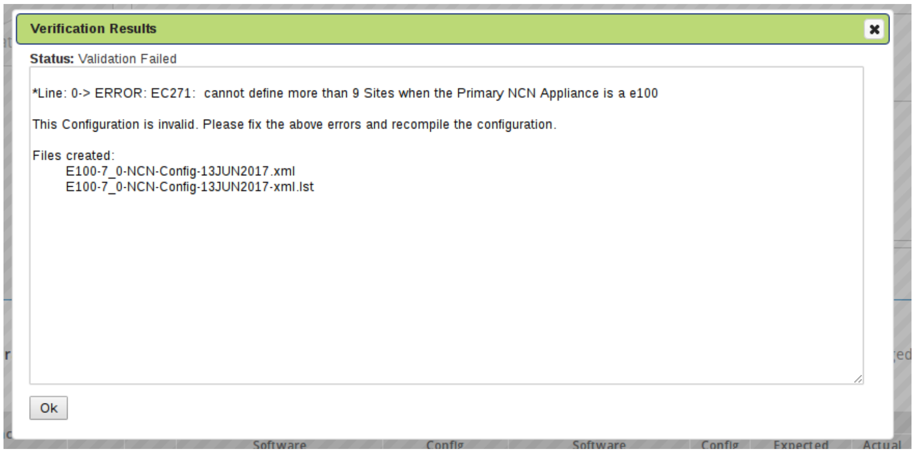


System Status

Name: E100_NCN
Model: E100
Appliance Mode: NCN
Unique Identifier: [illegible]
Management IP Address: 192.168.8.90
Appliance Uptime: 1 hours, 45 minutes, 56.9 seconds
Service Uptime: 41 minutes, 53.0 seconds
Routing Domain Enabled: Default_RoutingDomain

Note:

If you try to push a configuration through Change Management where the primary or secondary NCN is an E100 and you have defined more than 8 Client sites (resulting in more than 9 total sites per-network), the configuration will not pass the Validation Check.



Status: Validation Failed

```
*Line: 0-> ERROR: EC271:  cannot define more than 9 Sites when the Primary NCN Appliance is a e100

This Configuration is invalid. Please fix the above errors and recompile the configuration.

Files created:
      E100-7_0-NCN-Config-13JUN2017.xml
      E100-7_0-NCN-Config-13JUN2017-xml.lst
```

Capacity Report for the E100 NCN

Appliance Model	T510	T730	T750	T860	E100	T3010	T5000	T5200
Supported as NCN	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Max Client Sites as NCN	N/A	N/A	32	32	8	128	256	550
Max Static Conduits	8	16	32	32	32	128	256	550
Max Dynamic Conduits	4	8	16	16	16	32	32	32
Max WAN Ingress Paths	36	72	216	216	216	576	1152	5500
Max WAN Egress Paths	36	72	216	216	216	576	1152	5500
Max Flows (TCP Term off)	64,000	64,000	64,000	64,000	64,000	256,000	512,000	512,000
Max Flows (TCP term on)	500	4,000	8,000	8,000	8,000	16,000	16,000	16,000
Max Public WAN Links	3	8	8	8	8	8	8	8
Max Private WAN Links	32	32	32	32	32	32	32	32

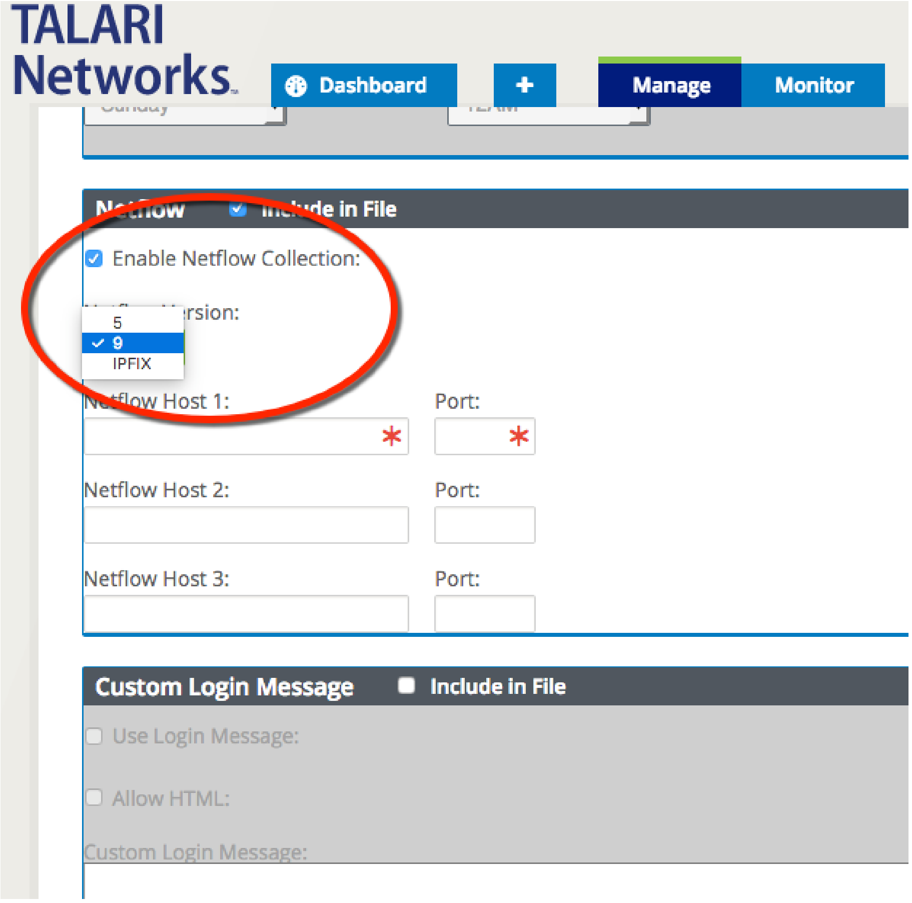
Max Routes (Static & Dynamic)	16,000	16,000	16,000	16,000	16,000	16,000	16,000	16,000
Max Recommended Routing Domains[1]	16	16	16	16	16	16	16	16

[1]

NetFlow (Support for Version 9 and IPFIX)

While NetFlow v5 is the default setting, users now have the ability to export flow information using NetFlow v9 and IPFIX. To enable NetFlow and select the version using Aware, navigate to **Manage > Appliance Settings** and scroll down to the **NetFlow** section. Click the **Include in File** option and **Enable NetFlow Collection**, then select the preferred version from the **NetFlow Version** drop down.

To complete the configuration, you must enter in a **NetFlow Host IP Address** and **Port** number.



Netflow ☑ Include in File

☑ Enable Netflow Collection:

Netflow Version: 5 / ✓ 9 / IPFIX

Netflow Host 1: * Port: *

Netflow Host 2: Port:

Netflow Host 3: Port:

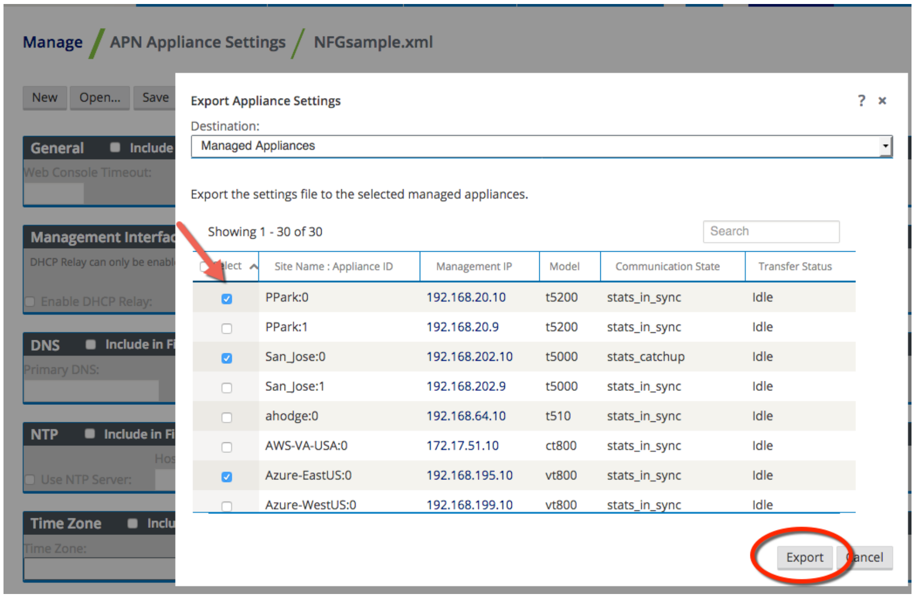
Custom Login Message □ Include in File

□ Use Login Message:

□ Allow HTML:

Custom Login Message:

Click **Save As** and **Export** the file to the desired Edge Appliances.



Export Appliance Settings

Destination:

Managed Appliances

Export the settings file to the selected managed appliances.

Showing 1 - 30 of 30

□ Select	Site Name : Appliance ID	Management IP	Model	Communication State	Transfer Status
☑	PPark:0	192.168.20.10	t5200	stats_in_sync	Idle
□	PPark:1	192.168.20.9	t5200	stats_in_sync	Idle
☑	San_Jose:0	192.168.202.10	t5000	stats_catchup	Idle
□	San_Jose:1	192.168.202.9	t5000	stats_in_sync	Idle
□	ahodge:0	192.168.64.10	t510	stats_in_sync	Idle
□	AWS-VA-USA:0	172.17.51.10	ct800	stats_in_sync	Idle
☑	Azure-EastUS:0	192.168.195.10	vt800	stats_in_sync	Idle
□	Azure-WestUS:0	192.168.199.10	vt800	stats_in_sync	Idle

8

Release 4.1 Features

This chapter includes features and enhancements released in 4.1

WAN Optimization on Virtual Appliances

4.1 expands support for WAN Optimization to the VT800 and CT800 platforms. WAN Optimization is supported on these platforms at the following levels, with the following resources:

Platform	License Level	WANOp Capacity	VCPUs	RAM	Max WANOp Sessions	Disk Size	Cloud Instance Type
VT800 for ESXi	20 Mbps	8 Mbps	2	8GB	1,500	160GB	
VT800 for ESXi	2 Gbps	200 Mbps	14 (2.10GHz)	16GB	10,000	160GB	
VT800 for Azure	20 Mbps	8 Mbps	4	28GB	10,000	160GB	DS12_v2
VT800 for Azure	500 Mbps	100 Mbps	8 (2.4GHz)	56GB	16,000	160GB	DS13_v2
VT800 for Hyper-V	20 Mbps	8 Mbps	2	8GB	1,500	160GB	
VT800 for Hyper-V	200 Mbps	100 Mbps	10 (2.10GHz)	10GB	5,000	160GB	
CT800 for AWS	20 Mbps	8 Mbps	8	15GB	5,000	160GB	c3.2xlarge
CT800 for AWS	200 Mbps	50 Mbps	8	15GB	5,000	160GB	c3.2xlarge

Note:

The maximum number of WANOp sessions is scaled based on available memory. If a virtual appliance has insufficient dedicated RAM, the maximum number of WANOp sessions will be lower. Provisioning a virtual appliance below recommended system specifications will not disable WANOp, but will impact WANOp performance. Provisioning a virtual appliance below the defined minimum specifications is not supported.

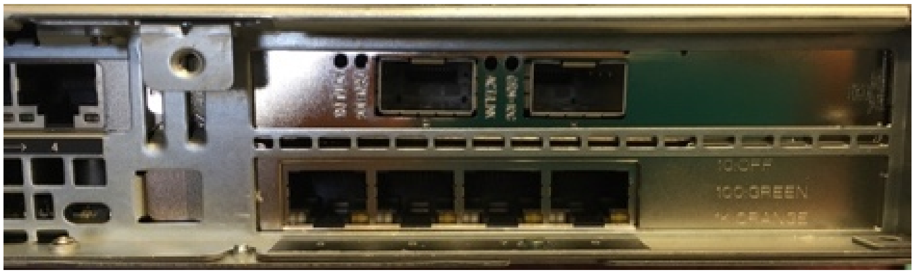
E1000 Hardware Options

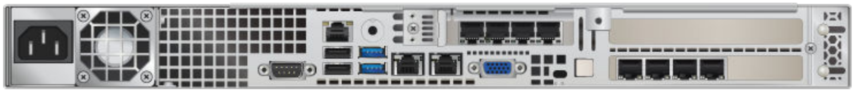
4.1 supports three hardware variations for the E1000 in the form of optional expansion cards. Customers may order either four additional fail-to-wire Gigabit Ethernet ports or two 10 Gigabit Ethernet fiber ports.

Port 9

Port 10

10G Fiber (2 Port) Expansion Card





The E1000 with 10G fiber expansion card does not ship with SFPs. The following modules are supported in conjunction with this card:

Description	Intel Part
Intel (**Short Range**) Dual Rate 10GBASE-SR/1000BASE-SX (Supplier Part FTLX8571D3BCVIT1 or AFBR-709DMZ-IN2)	E10GSFPSR
Intel (**Long Range**) Dual Rate 10GBASE-LR/1000BASE-LX (Supplier Part FTLX1471D3BCVI31)	E10GSFPLR
Intel Ethernet SFP+ 10GbE direct attach passive copper Twinaxial Cable (Available in 1 Meter, 3 Meter, and 5 Meter lengths)	1 Meter: XDACBL1M 3 Meter: XDACBL3M 5 Meter: XDACBL5M

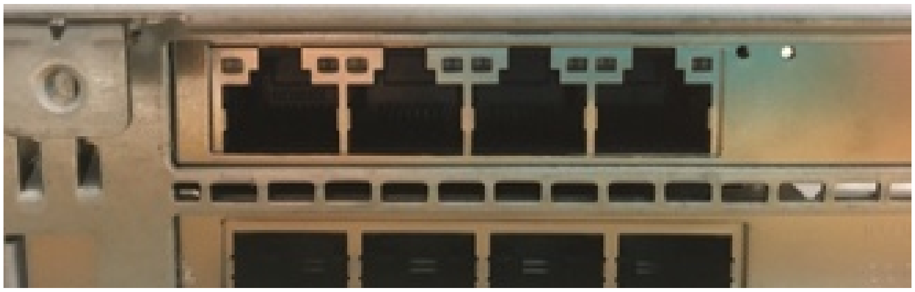
Port 9

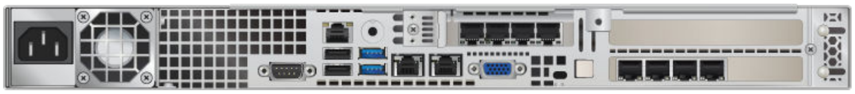
Port 12

Port 11

Port 10

Fail to Wire Copper (4 Port) Expansion Card





Note:

The configuration editor will not detect which expansion card (if any) is installed on an E1000, and will offer port 1 – 12 for *all* E1000s.

Before beginning configuration for an E1000, please verify the physical ports on the appliance. The following ports may be configured for each hardware option:

Hardware Option	Ports
E1000 without expansion card	AUX, interfaces 1-8
E1000 with 10G expansion card	AUX, interfaces 1-10 (ports 9 and 10 fail-to-block only)
E1000 with FTW expansion card	AUX, interfaces 1-12

If a configuration that does not match the available hardware is applied to an E1000, the Oracle service will be disabled. Once a mismatched configuration has been applied to an E1000, a corrected package must be applied through Local Change Management before the Oracle service will start. Alternately, the appliance may be factory defaulted and a corrected configuration applied using the Easy 1st Install process. **The Oracle service will be disabled until a corrected package is applied.**

For more information about the E1000, available hardware options, and special configuration considerations, please see the *E1000 Installation Guide* and the *E1000 Hardware Guide*.

9

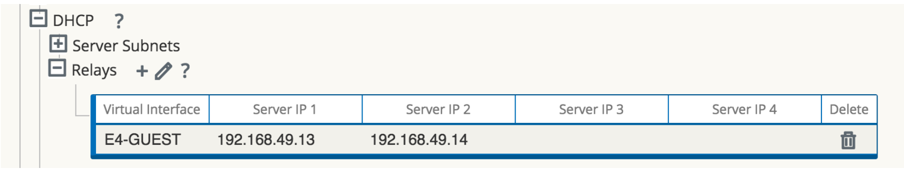
Release 4.2 Features

This chapter includes features and enhancements released in 4.2

Enhanced DHCP Relay

4.2 introduces the ability for users to configure up to four DHCP server relay addresses per virtual interface, allowing users with multiple DHCP servers at their NCN site to take advantage of increased redundancy.

DHCP relays may be configured in the Advanced view of the Configuration Editor, under **Sites > [site name] > DHCP > Relays**, as shown below:

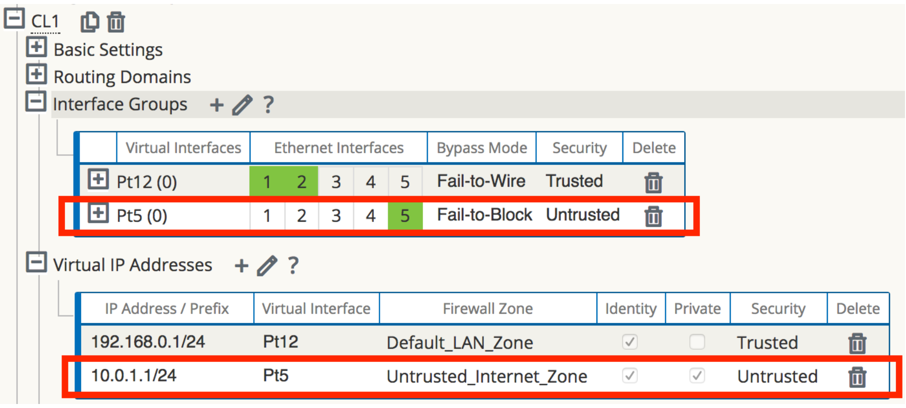


Virtual Interface	Server IP 1	Server IP 2	Server IP 3	Server IP 4	Delete
E4-GUEST	192.168.49.13	192.168.49.14			🗑

When configuring DHCP Relays, the Virtual Interface and Server IP 1 are required. Server IPs 2 through 4 are optional.

Client Private Subnet Reuse for Untrusted Segment

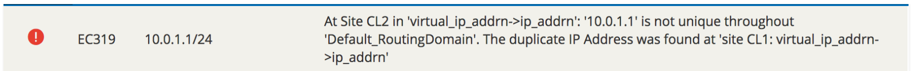
4.2 introduces the ability to set duplicate Virtual IPs at multiple sites when the Virtual IP Address is Private and the associated Interface Group is defined as Untrusted. This feature is intended for use is situations where multiple sites are being deployed with the same WAN link provider, with provider equipment pre-configured for the same IP address/subnet at every site.



Virtual Interfaces	Ethernet Interfaces	Bypass Mode	Security	Delete
Pt12 (0)	1 2 3 4 5	Fail-to-Wire	Trusted	🗑
Pt5 (0)	1 2 3 4 5	Fail-to-Block	Untrusted	🗑

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
192.168.0.1/24	Pt12	Default_LAN_Zone	✓	□	Trusted	🗑
10.0.1.1/24	Pt5	Untrusted_Internet_Zone	✓	✓	Untrusted	🗑

If one or more of the duplicate Virtual IPs is not private, an Audit Error will be displayed.



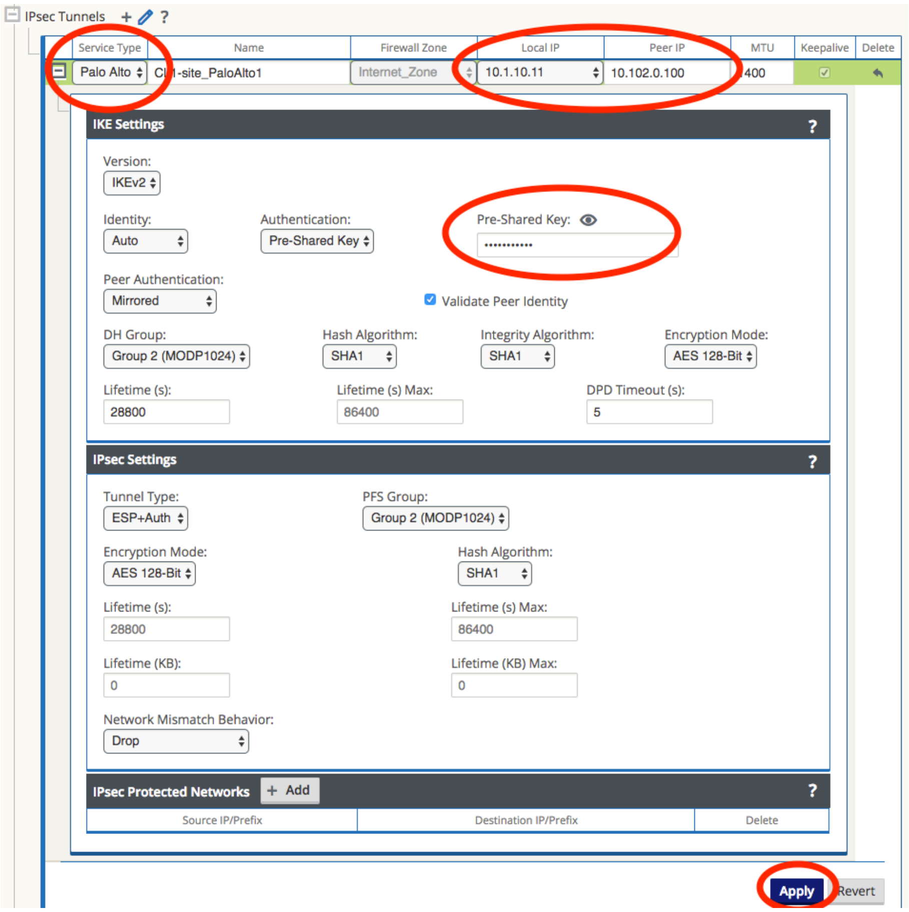
!	EC319	10.0.1.1/24	At Site CL2 in 'virtual_ip_addrn->ip_addrn': '10.0.1.1' is not unique throughout 'Default_RoutingDomain'. The duplicate IP Address was found at 'site CL1: virtual_ip_addrn->ip_addrn'

Palo Alto GlobalProtect Cloud Integration

Aware 4.2 adds support for integration of branch office Appliances with the Palo Alto GlobalProtect cloud service via IPsec tunneling, enabling users to tunnel Internet-destined traffic to GPCS for cloud-hosted filtering and security services.

To configure a Palo Alto GlobalProtect cloud IPSec tunnel, navigate to **Manage > Configuration** and **Import** the current configuration file. Click on the **Advanced** tab, expand **Connections > [Site Name] > IPSec Tunnels**, and click the **(+)** icon.

Select Palo Alto as the **Service Type**, select the **Local IP** address from the dropdown, fill in the **Peer IP** address of the GlobalProtect cloud service IKE Gateway, enter the IKE **Pre-Shared Key**, add the local Protected Networks for the IPsec tunnel, and click **Apply**.



IPsec Tunnels

Service Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Delete
Palo Alto	C[illegible]1-site_PaloAlto1	Internet_Zone	10.1.10.11	10.102.0.100	[illegible]400	☑	

IKE Settings

Version: IKEv2

Identity: Auto
Authentication: Pre-Shared Key
Pre-Shared Key: ••••••••••••

Peer Authentication: Mirrored
☑ Validate Peer Identity

DH Group: Group 2 (MODP1024)
Hash Algorithm: SHA1
Integrity Algorithm: SHA1
Encryption Mode: AES 128-Bit

Lifetime (s): 28800
Lifetime (s) Max: 86400
DPD Timeout (s): 5

IPsec Settings

Tunnel Type: ESP+Auth
PFS Group: Group 2 (MODP1024)

Encryption Mode: AES 128-Bit
Hash Algorithm: SHA1

Lifetime (s): 28800
Lifetime (s) Max: 86400

Lifetime (KB): 0
Lifetime (KB) Max: 0

Network Mismatch Behavior: Drop

IPsec Protected Networks

Source IP/Prefix	Destination IP/Prefix	Delete

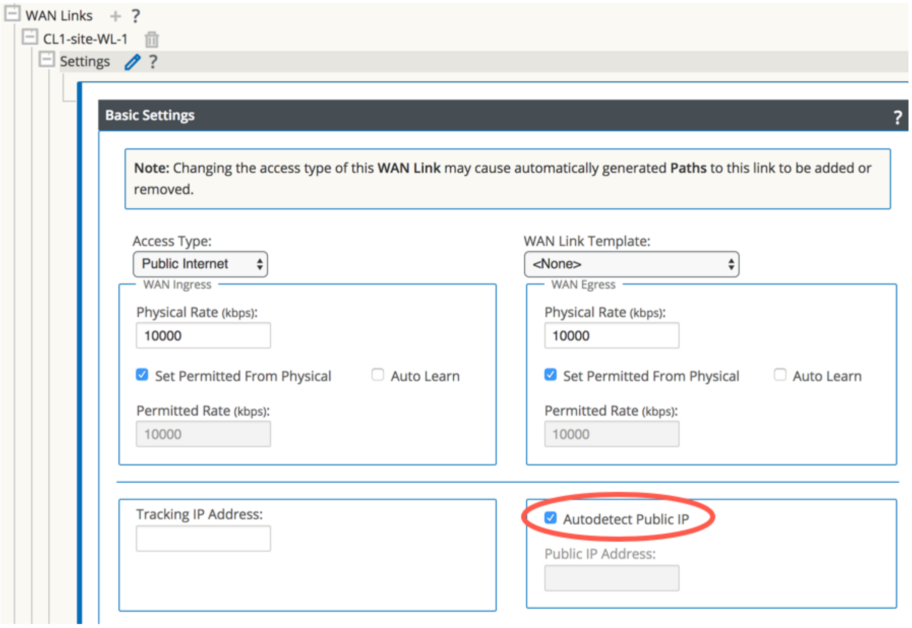
If no options are available in the Local IP dropdown, ensure Internet Service is enabled on at least one WAN link at the site under **Connections > [Site Name] > Internet Services**.

Private Cloud Path Enhancement

In certain cases, service providers have a private cloud which is separate from the public Internet. Within their environment they use PAT (Port Address Translation) to forward user traffic from their private cloud to the Internet. In these cases, the service provider will have a limited number of public IP address for NATing. When Oracle is deployed for an enterprise customer, if they select one of these providers for multiple Oracle client sites, there is the possibility that multiple Oracle Client WAN links could be PATed/NATed to the same public IP address. Previously, Oracle would validate/learn a path based on the source IP address of the received frame (at the NCN for example). The end result is that the first site brought online would function as expected, with a Oracle Path in the GOOD state. However, at the second Oracle Client site using the same public IP address, the Oracle Path would be in the DEAD state. To resolve this issue, this release has been enhanced to use the source IP address and source port for path learning validation. With this enhancement Oracle has expanded its ability to interoperate with multiple additional Service Provider WAN environments.

> **Note:**
>
> Conduits between Client sites with the same shared public IP are not supported at this time.

All WAN links which may reside behind the same public IP must have Autodetect Public IP enabled in the configuration under **Sites > [Site Name] > WAN Links > [WAN Link] > Settings > Basic Settings**, as shown below:



Note: Changing the access type of this **WAN Link** may cause automatically generated **Paths** to this link to be added or removed.

Access Type: Public Internet

WAN Link Template: <None>

WAN Ingress

Physical Rate (kbps): 10000

☑ Set Permitted From Physical □ Auto Learn

Permitted Rate (kbps): 10000

WAN Egress

Physical Rate (kbps): 10000

☑ Set Permitted From Physical □ Auto Learn

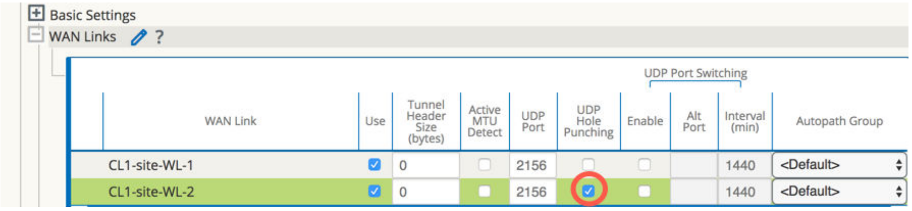
Permitted Rate (kbps): 10000

Tracking IP Address:

☑ Autodetect Public IP

Public IP Address:

Remote sites other than the NCN will not be able to bring up paths on to a client using a shared public IP unless UDP Hole Punching is enabled in the configuration under **Connections > [Site Name] > Conduits > [Conduit] > Local Site > WAN Links** at the client sites which share the public IP, as shown below:



						UDP Port Switching			
WAN Link	Use	Tunnel Header Size (bytes)	Active MTU Detect	UDP Port	UDP Hole Punching	Enable	Alt Port	Interval (min)	Autopath Group
CL1-site-WL-1	☑	0	□	2156	□	□		1440	<Default>
CL1-site-WL-2	☑	0	□	2156	☑	□		1440	<Default>

Additional Features in Aware 4.2 GA

Aware 4.2 introduces the following additional features:

- Configuration Editor:

A note has been added in the Configuration Editor at all locations where a Rule may be configured to clarify that Drop Limit and Disable Limit values in milliseconds are not valid for Bulk Classes. These values will automatically be set to 0. Drop Depth (bytes) and Disable Depth (bytes) values should be used for Bulk Classes instead.

10

Release 4.3 Features

This chapter includes features and enhancements released in 4.3.

Enhanced Application Identification

4.3 GA introduces the ability to configure Enhanced Application Identification, which offers a significant improvement to how Appliances identify and forward applications. This release introduces the following new application identification enhancements:

- DNS snooping, a less intrusive application identification technique when compared to our existing DNS proxy or manual six-tuple identification mechanisms.
- Simplified application policy configuration, with a default signature library (the Oracle Application Signature Library) with over 100 application entries included. Preset application signatures are modular and can be downloaded and upgraded independently of software packages via the regular Change Management process. Oracle will provide updates to the application Oracle Application Signature Library moving forward based on customer feedback.
- Streamlined configuration elements that make creating an application policy fast and easy. Oracle's Enhanced Application Identification is extensible and supports the addition of user-defined categories and applications.
- Applications are assigned to a pre-defined application category, or users may configure additional application categories as required.

By combining all of these capabilities, users can create granular application policies such as steering a single application (e.g., Microsoft Office 365) out the local internet service while forwarding all other SaaS application(s) back to the data center or NCN site. The user can also define the scope of the application policy which could include a single location, all Edge sites or a subset of sites depending on user needs. Traditional QOS services are applied for conduit services where the user can map an application to a pre-defined classification or select their own classification from a pre-defined list.

For information on configuring and monitoring Enhanced Application Identification, please see the *Oracle Enhanced Application Identification & Oracle Application Signatures Guide.*