Oracle® SD-WAN Aware
Features Guide

Release 8.2
F29162-01
Jan 2020

Oracle SD-WAN Aware Features Guide, Release 8.2

F29162-01

Copyright © 2014, 2020, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or “commercial computer software documentation” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About This Guide

My Oracle Support vii

Revision History

1 Release 2.0 Features

Virtual Routing and Forwarding (VRF) 1-1
Cloud for Amazon Web Services 1-3
IPSec Tunnel Monitoring 1-4

2 Release 2.1 Features

About This Product 2-1
- Oracle SD-WAN Aware 2-1

New Features in Oracle SD-WAN Aware 2.1 2-1
- Oracle Virtual Appliance VT800 Support 2-1
- Alarm System 2-1
- Customizable Web Console 2-3
- DHCP Relay 2-5

Notification Enhancements 2-6
Multiple Netflow Collectors 2-6
- Summary 2-7

3 Oracle SD-WAN Aware 2.2 New Features Guide

About This Product 3-1
- Oracle SD-WAN Aware 3-1

New Features in Oracle SD-WAN Aware 2.2 3-1
- Support for 550 Sites 3-1
- Firewall Logs to Syslog 3-1
- DHCP Relay & DHCP Server 3-2

DHCP Relay 3-2
DHCP Server 3-3
Standby WAN Link (VSAT) 3-6
Adaptive Bandwidth Detection 3-9
SNMPv3 Polling and Trap Capability 3-10
Eligibility for IPsec Non-Conduit Routes 3-11
Routing Enhancements 3-12
Summary 3-12

4 Release 3.0 Features

Application/Packet Filtering 4-1
Applications 4-1
Apply The Application to Firewall Policies 4-1
Apply The Application to QoS Rules 4-2
Tracking Based on Firewall Policy 4-3
Tracking Based on QoS Rule 4-3
VRF Firewall Enhancements 4-4
Configuration using Templates 4-6
Basic Configuration Mode 4-8

5 Release 3.1 Features

Oracle SD-WAN Edge as an Autonomous System (eBGP) 5-1
Configure Trusted Virtual IP Address 5-1
Import Filters 5-3
WAN Link Template – Broadband, MPLS, and Private Intranet 5-4
Application Identification: DNS Proxy 5-7
Enabling DNS Proxy 5-8
Persistent Path Traffic Steering 5-9
Service Override Traffic Steering 5-10

6 Release 3.1 GA P2 Features

New Features in 3.1 GA P2 6-1
Additional Features in Aware 3.1 GA P2 6-5

7 Release 4.0 Features

WAN Optimization 7-1
Session Capacity for Supported Models 7-1
Configuring WAN Optimization via Aware 7-1

Verification 7-2
Zscaler Integration 7-3
Configuration via Aware 7-4
Verification 7-5
Customer Edge (CE) Router Replacement Within the Edge 7-6
Installation Summary 7-6
BGP Configuration via Aware 7-8
Neighbors 7-8
Import and Export Filters 7-9
Static Routes File 7-10
BGP Verification and Troubleshooting 7-10
BGP Troubleshooting Enhancements 7-12
E100 as an NCN 7-13
Capacity Report for the E100 NCN 7-14
NetFlow (Support for Version 9 and IPFIX) 7-15

8 Release 4.1 Features

WAN Optimization on Virtual Appliances 8-1
E1000 Hardware Options 8-1
10G Fiber (2 Port) Expansion Card 8-2
Fail to Wire Copper (4 Port) Expansion Card 8-3

9 Release 4.2 Features

Enhanced DHCP Relay 9-1
Client Private Subnet Reuse for Untrusted Segment 9-1
Palo Alto GlobalProtect Cloud Integration 9-2
Private Cloud Path Enhancement 9-2
Additional Features in Aware 4.2 GA 9-4

10 Release 4.3 Features

Enhanced Application Identification 10-1

11 Release 8.0 Features

12 Release 8.1 Features

13 Release 8.2 and later

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**.

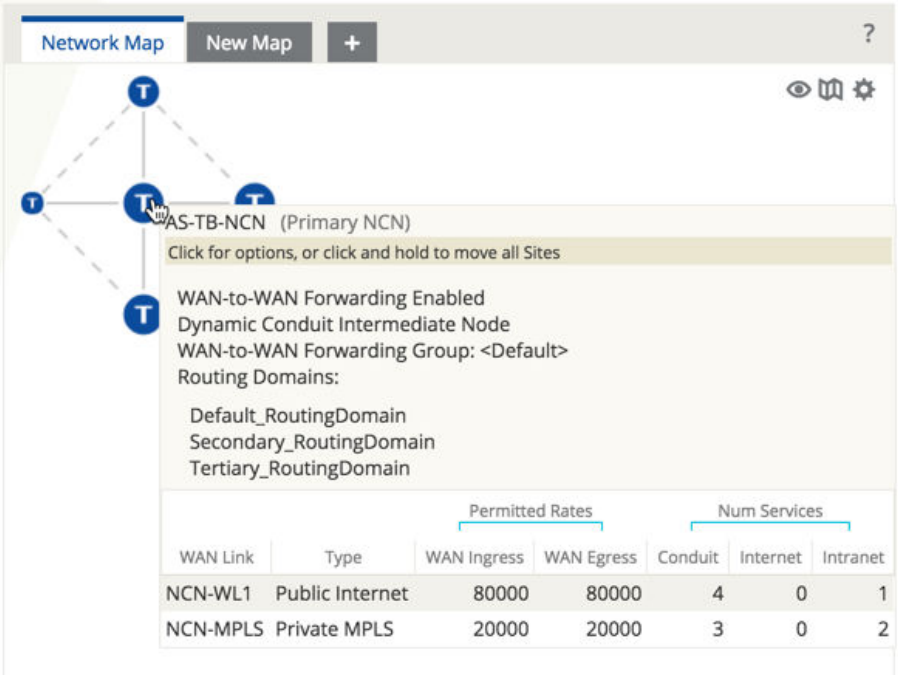


Figure 1: Network Map Elements Including Routing Domains

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.

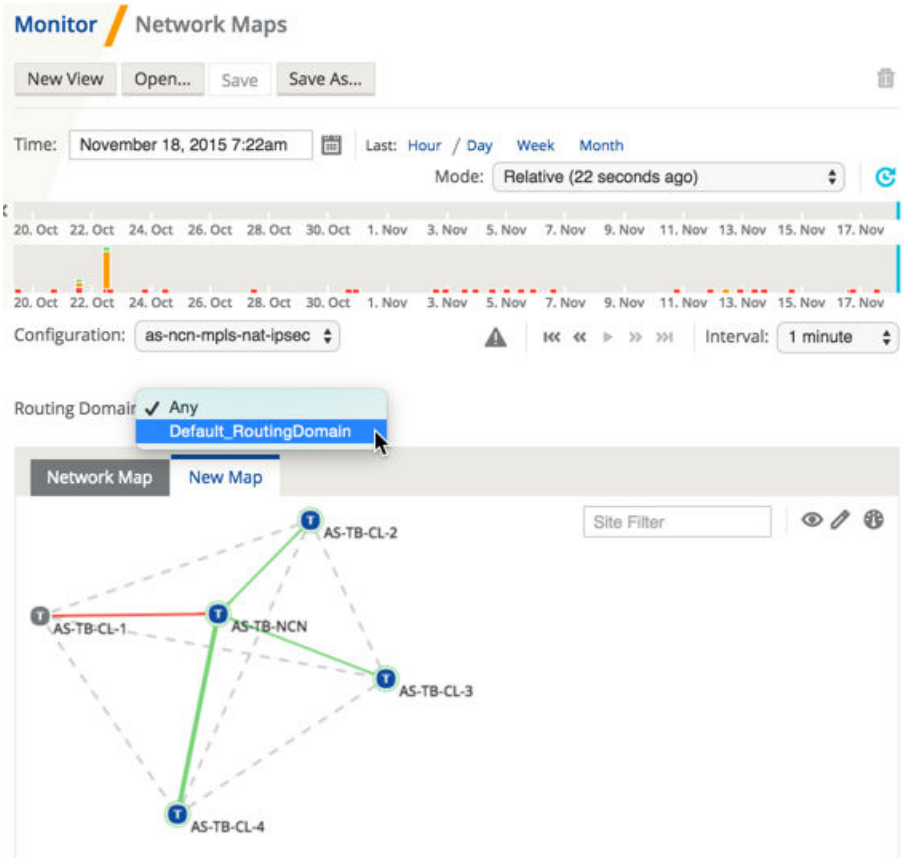


Figure 2: Network App Elements Filtered by Routing Domain

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.

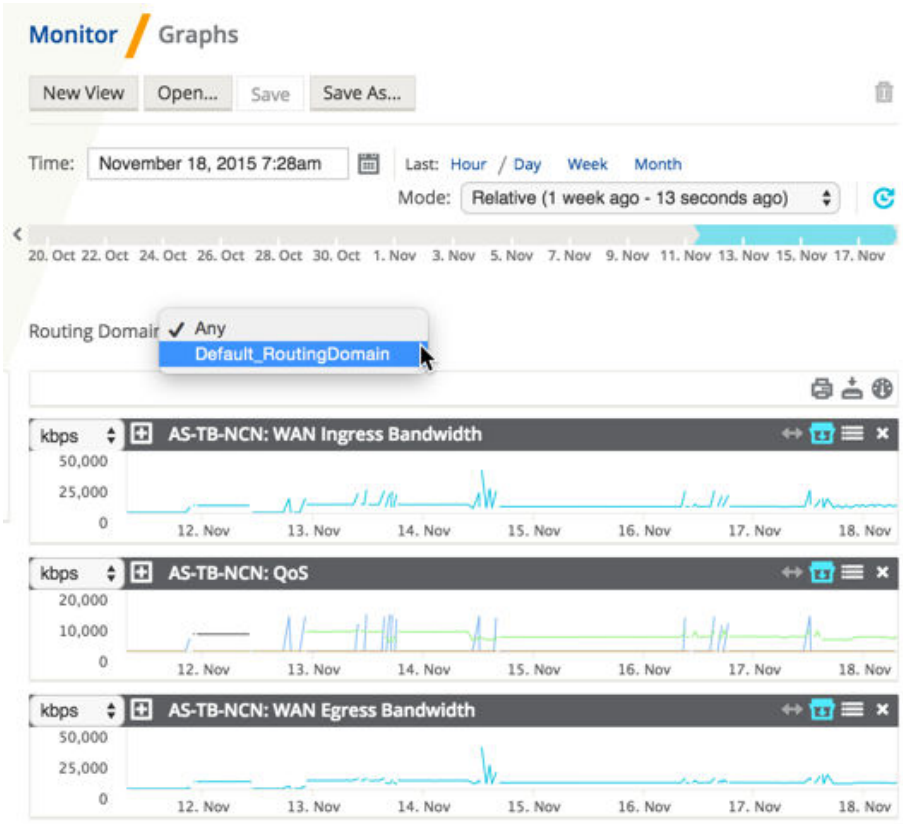


Figure 3: Graph Objects Filtered by Routing Domain

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

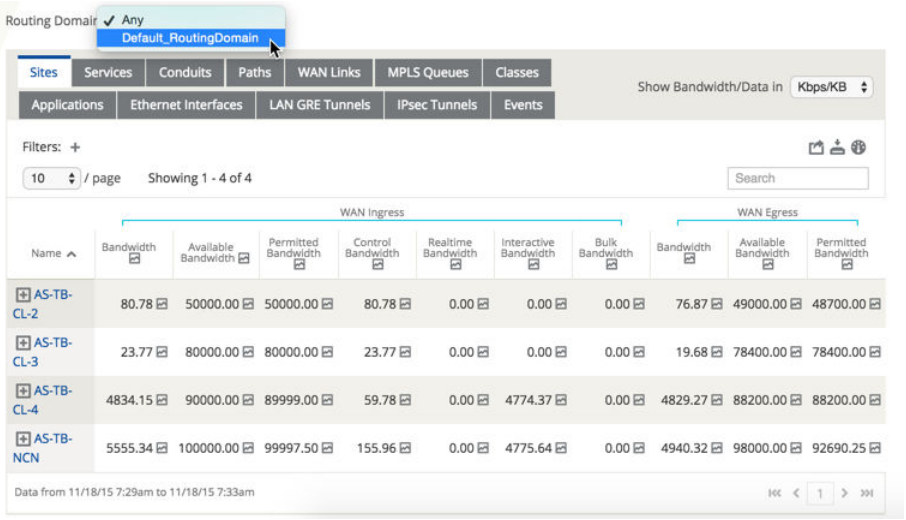


Figure 4: Reports Filtered by Routing Domain

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

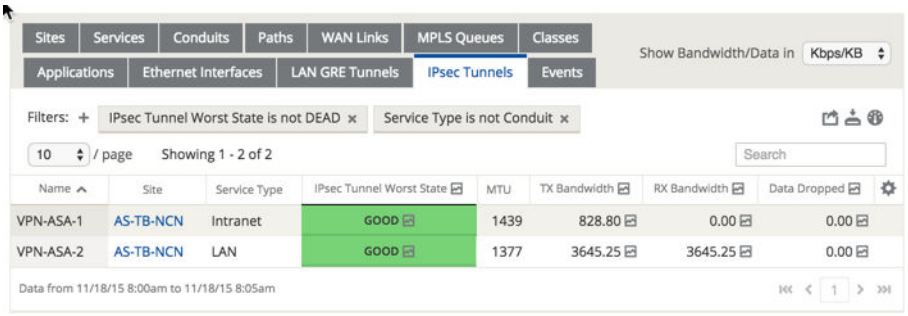


Figure 5: IPsec Tunnel Report

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

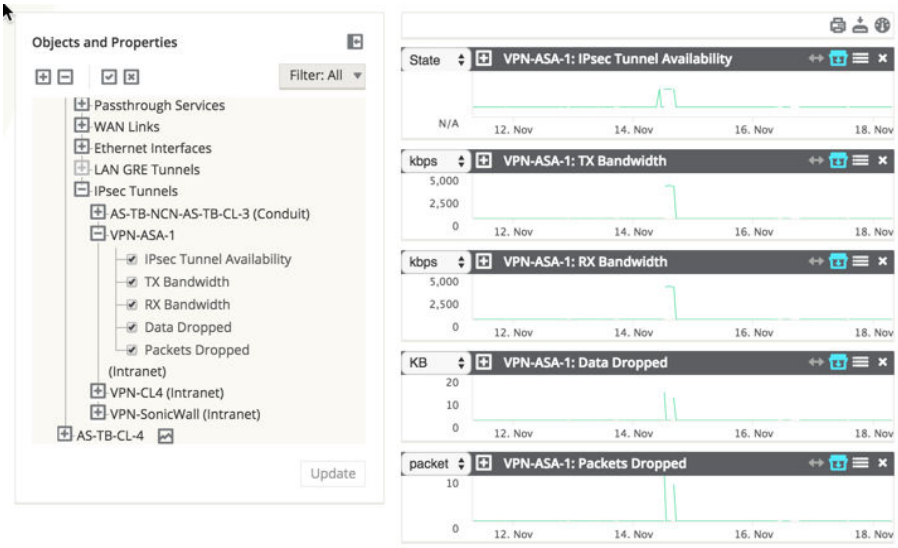


Figure 6: IPsec Tunnel Graphs

2
Release 2.1 Features

This chapter includes features and enhancements released in 2.0.

About This Product

Oracle SD-WAN Aware

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 SD-WAN Aware 2.1

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

Oracle Virtual Appliance VT800 Support

Oracle SD-WAN 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. Oracle SD-WAN Aware 2.1 provides the same configuration, monitoring, reporting, security and diagnostic capabilities for the VT800 that it provides for the VT500.

Alarm System

Oracle SD-WAN Edge 5.1 introduces a new Alarm System that streamlines the configuration and number of severity-based alerts for network administrators. Oracle SD-WAN 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.

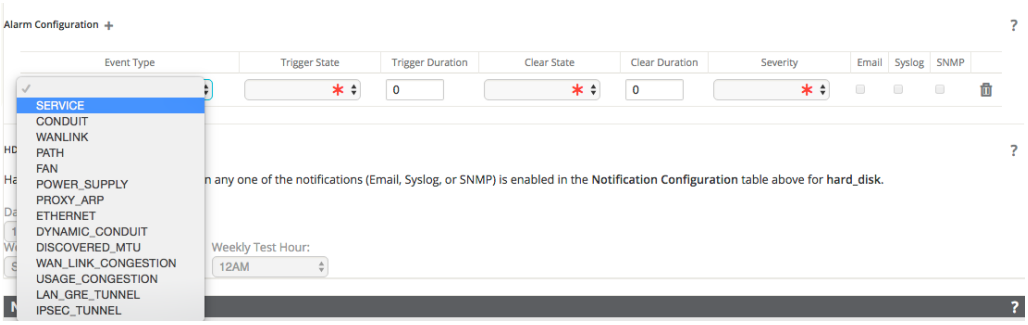


Figure 1: Select Event Type

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.

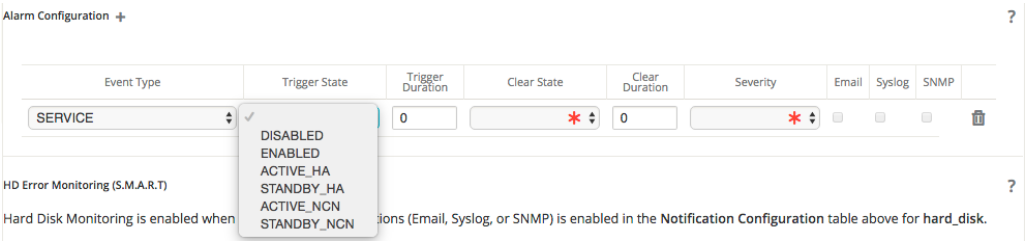


Figure 2: Select Trigger State

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.

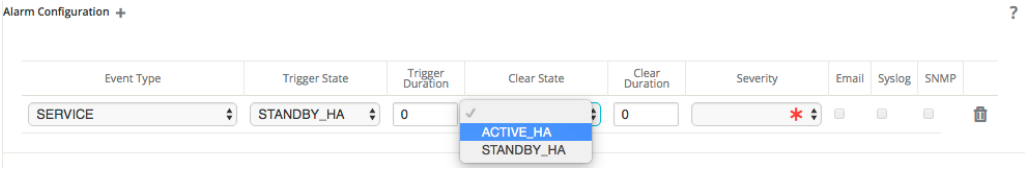


Figure 3: Select a Clear State

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.

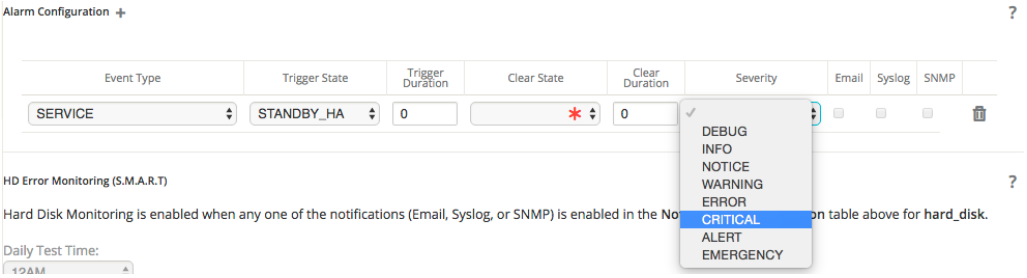


Figure 4: Choose a Severity

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 Oracle SD-WAN Edge 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

Oracle SD-WAN 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 Oracle SD-WAN 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.

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.

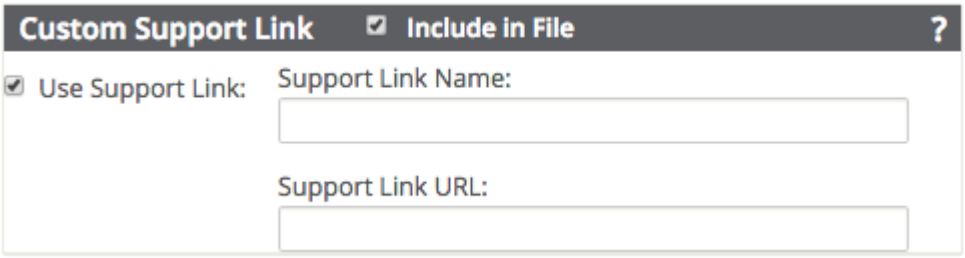


Figure 6: Custom Support URL

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 Oracle SD-WAN Aware.

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

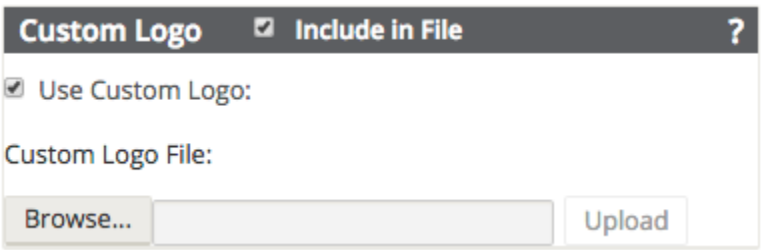


Figure 7: Custom Logo

When you are done, click **Save** to save the Alarm to the Oracle SD-WAN Edge 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.

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.

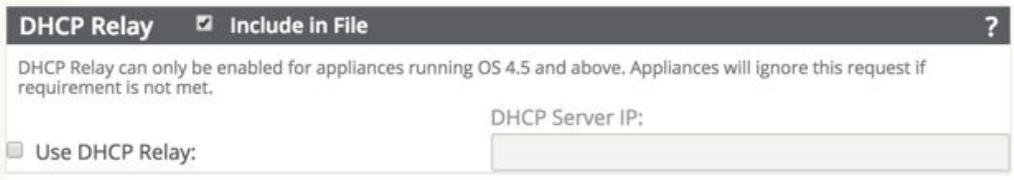


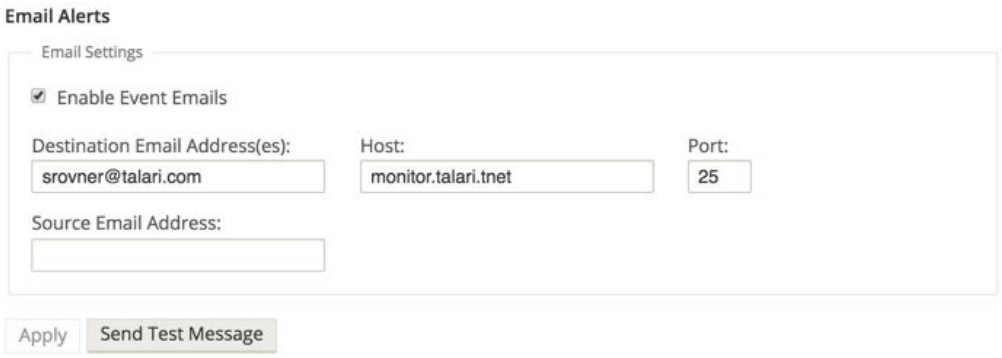
Figure 9: Enable DHCP Relay

When you are done, click **Save** to save the Alarm to the Oracle SD-WAN Edge 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 Oracle SD-WAN Aware 2.1:

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



The following notification enhancements were introduced on the **Manage**, and then **APN Appliance Settings** screen in Oracle SD-WAN 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.

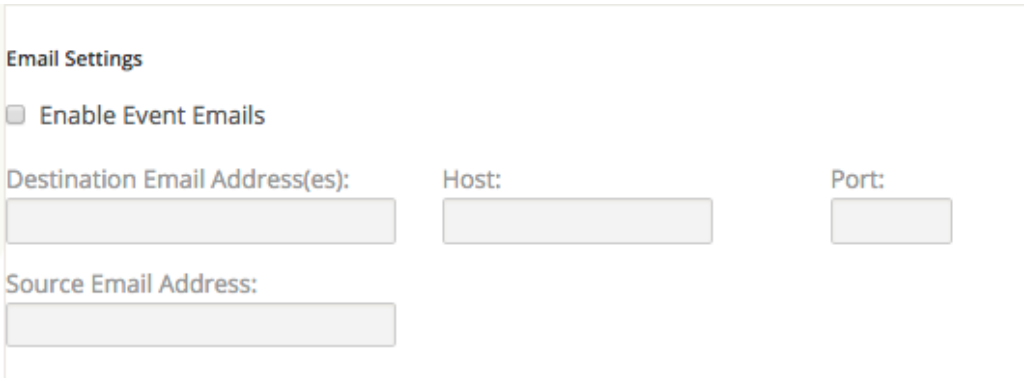


Figure 10: Configure Email Alerts

Multiple Netflow Collectors

Oracle SD-WAN 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.

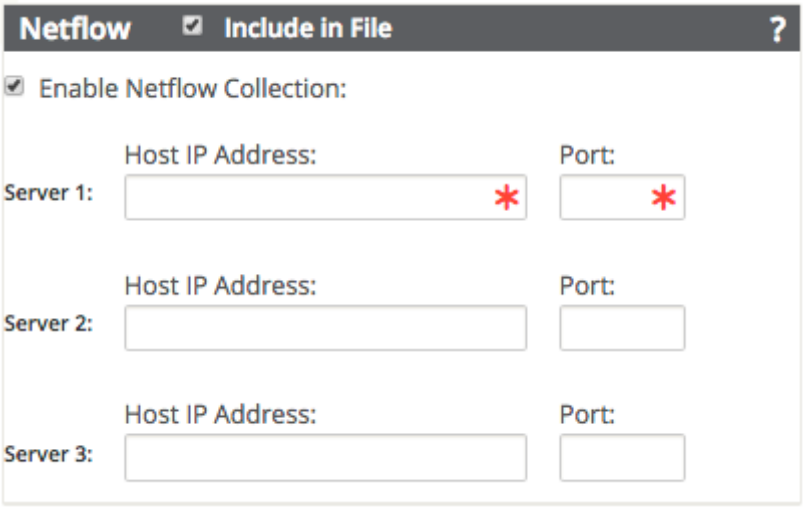


Figure 11: Multiple Netflow Hosts

When you are done, click **Save** to save the Alarm to the Oracle SD-WAN Edge 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 Oracle SD-WAN 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 SD-WAN Aware 2.2 New Features Guide

About This Product

Oracle SD-WAN Aware

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 SD-WAN Aware 2.2

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

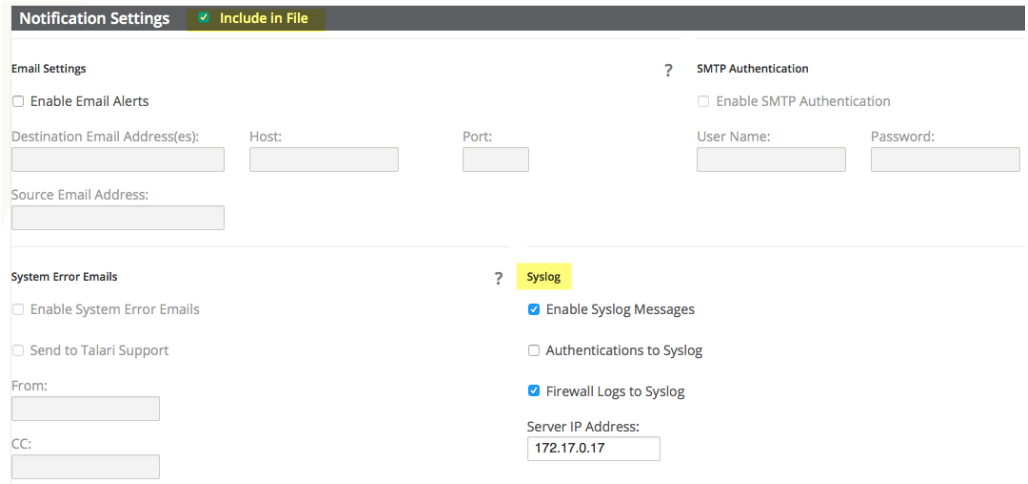
Support for 550 Sites

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

Firewall Logs to Syslog

Oracle SD-WAN Edge 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 Oracle SD-WAN 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.



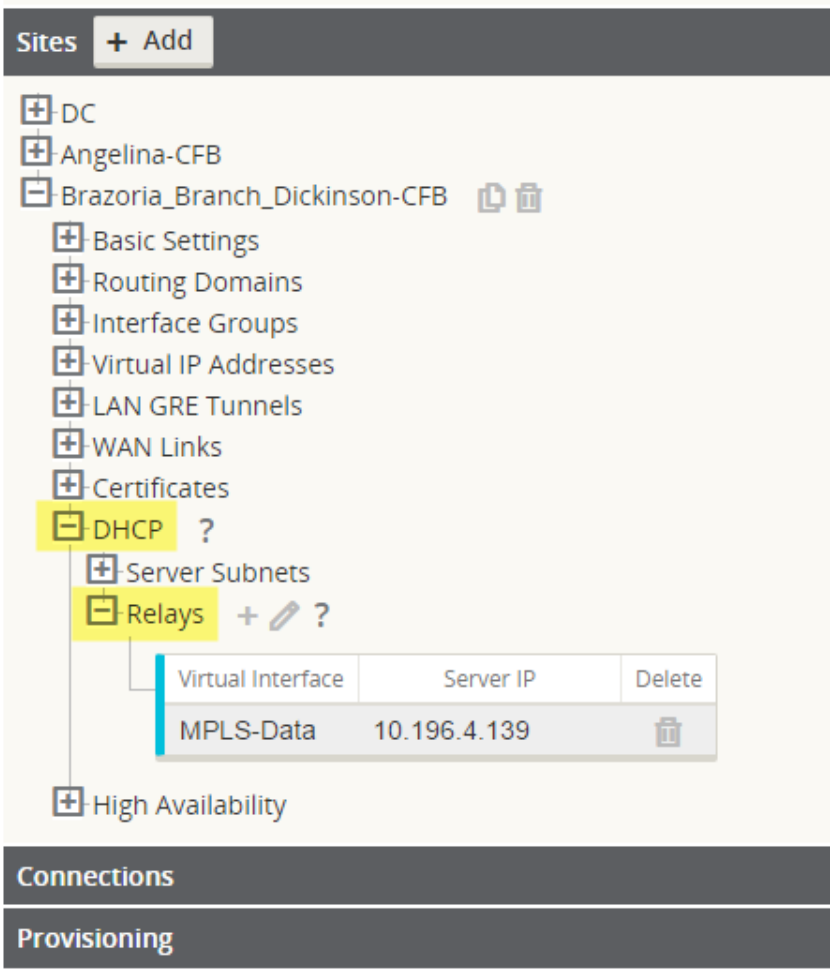
DHCP Relay & DHCP Server

As of Oracle SD-WAN Edge 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 Oracle SD-WAN 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.



DHCP Server

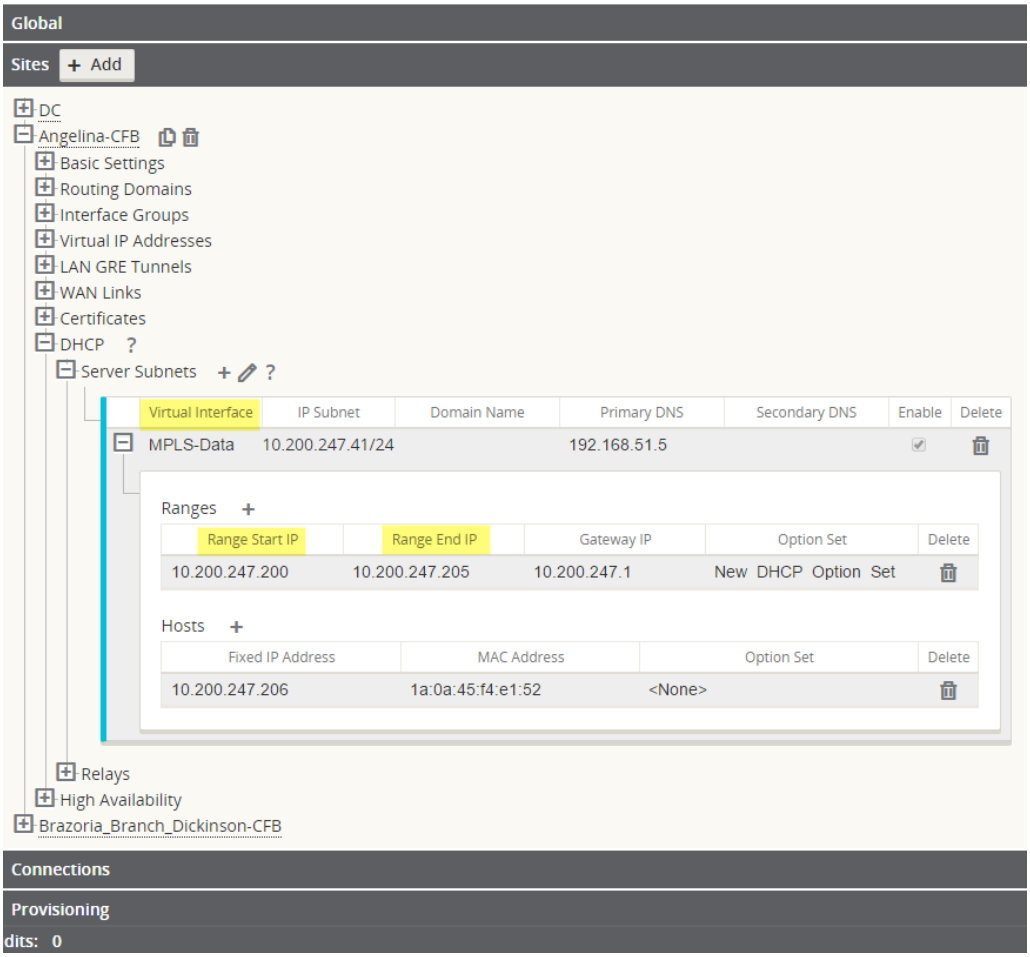
Network administrators can now also use the DHCP Server feature on data ports of Appliances to allow local hosts to acquire dynamic or static IP addressing directly from the Appliance.

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.

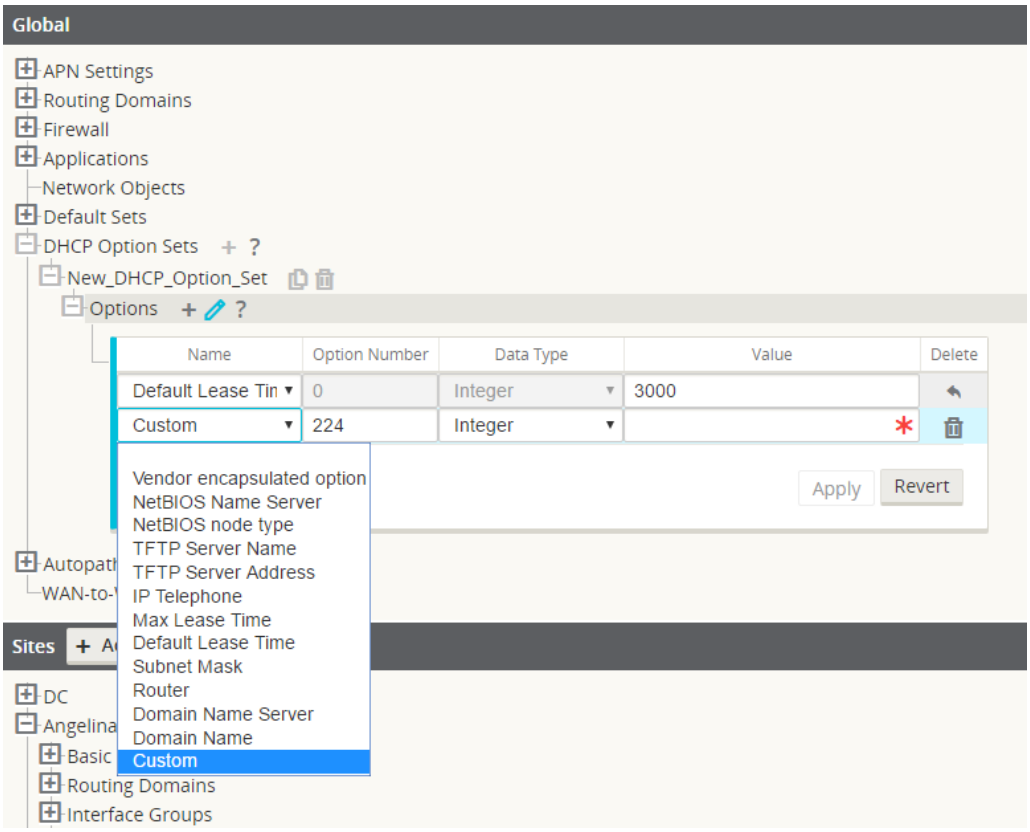
Users may also choose to enter additional information in this section that hosts will then be configured with as well, such as gateway IP, DNS, and an Option Set (described below).

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

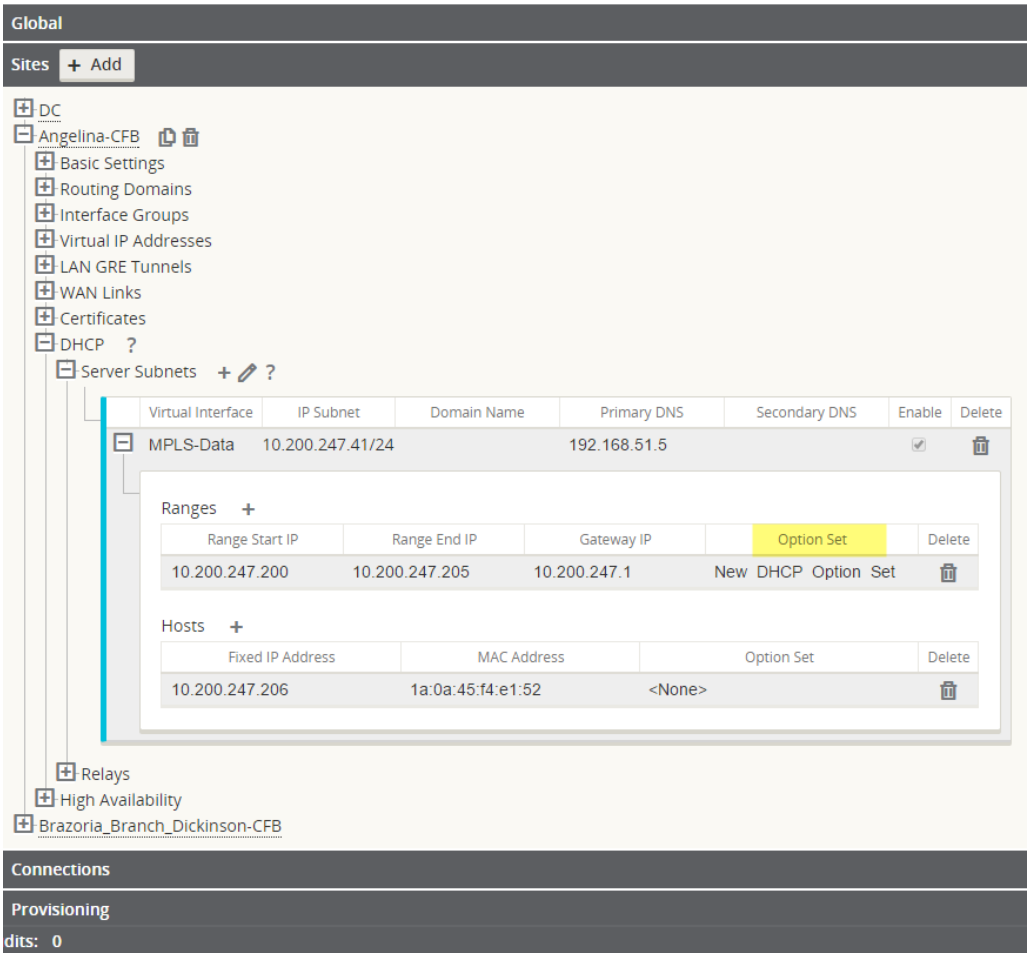


> **Note:**
>
> The following feature is optional, not required.

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**.



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.

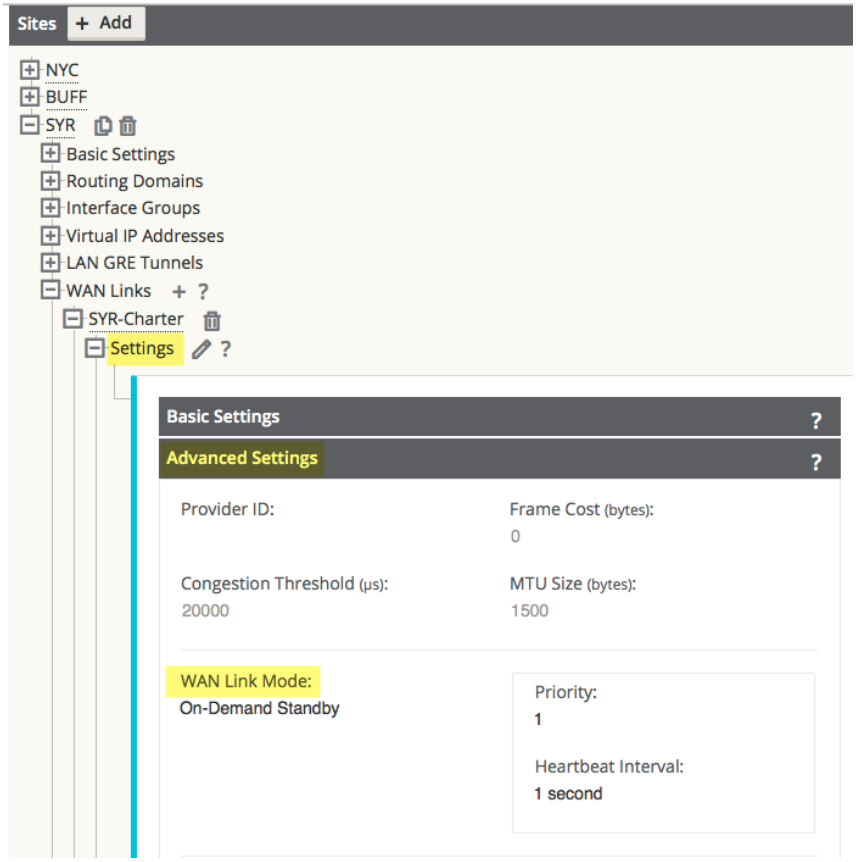


Standby WAN Link (VSAT)

Introduced in Oracle SD-WAN Edge 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 Oracle SD-WAN 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.**

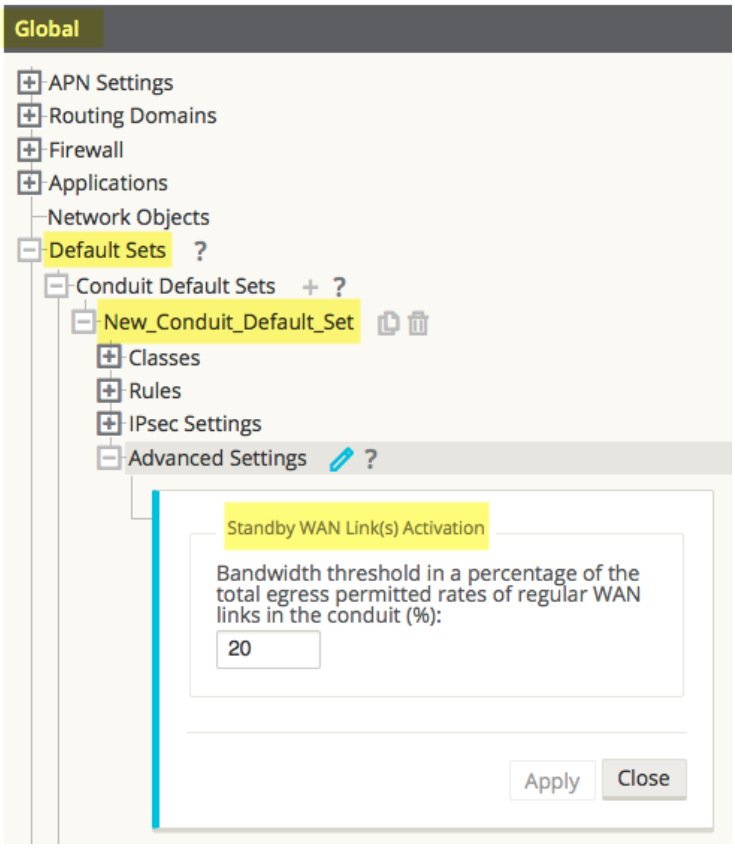


The **Priority** option is a value to indicate which Standby WAN Link will be activated in which order and the **Heartbeat Interval** can either be set or disabled.

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

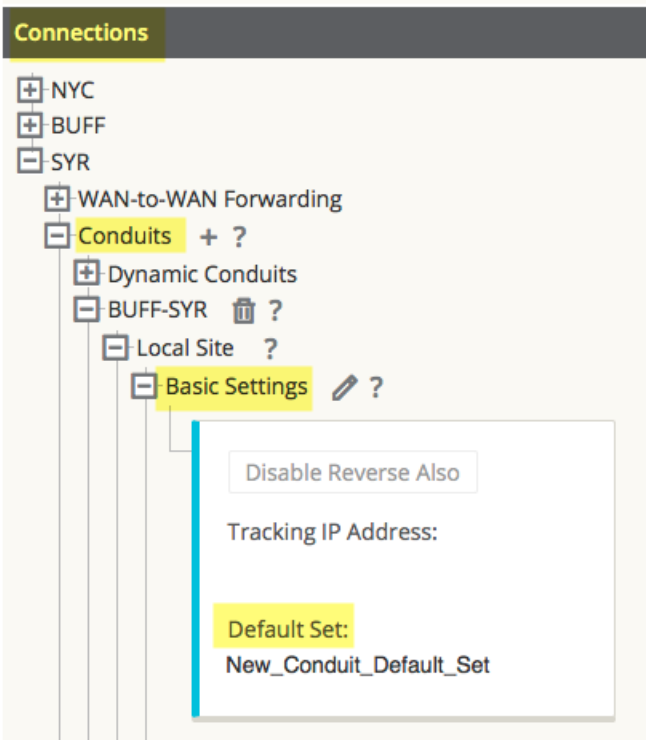
> **Note:**
>
> A WAN Link configured in Standby mode can not have Internet or Intranet Services enabled on it, this will result in a Configuration Audit Error.

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



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.**



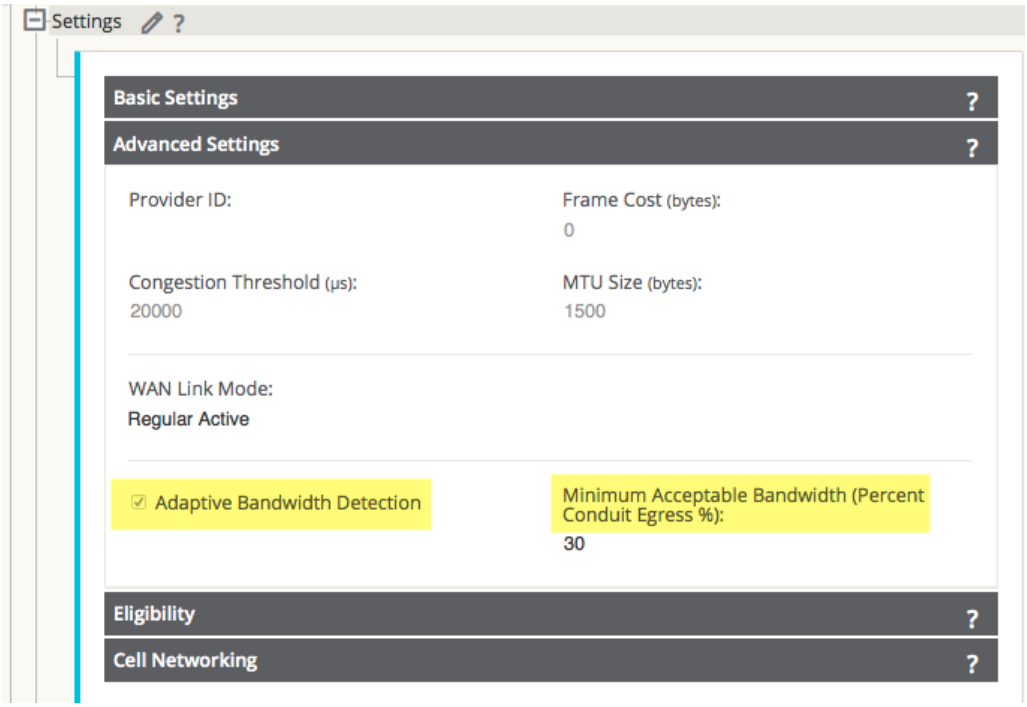
> **Note:**
>
> Step 2 is only required when choosing the On-Demand Standby option and is not applicable for Last-Resort Standby WAN Links.

Adaptive Bandwidth Detection

This feature is introduced in Oracle SD-WAN Edge 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 Oracle SD-WAN 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.**



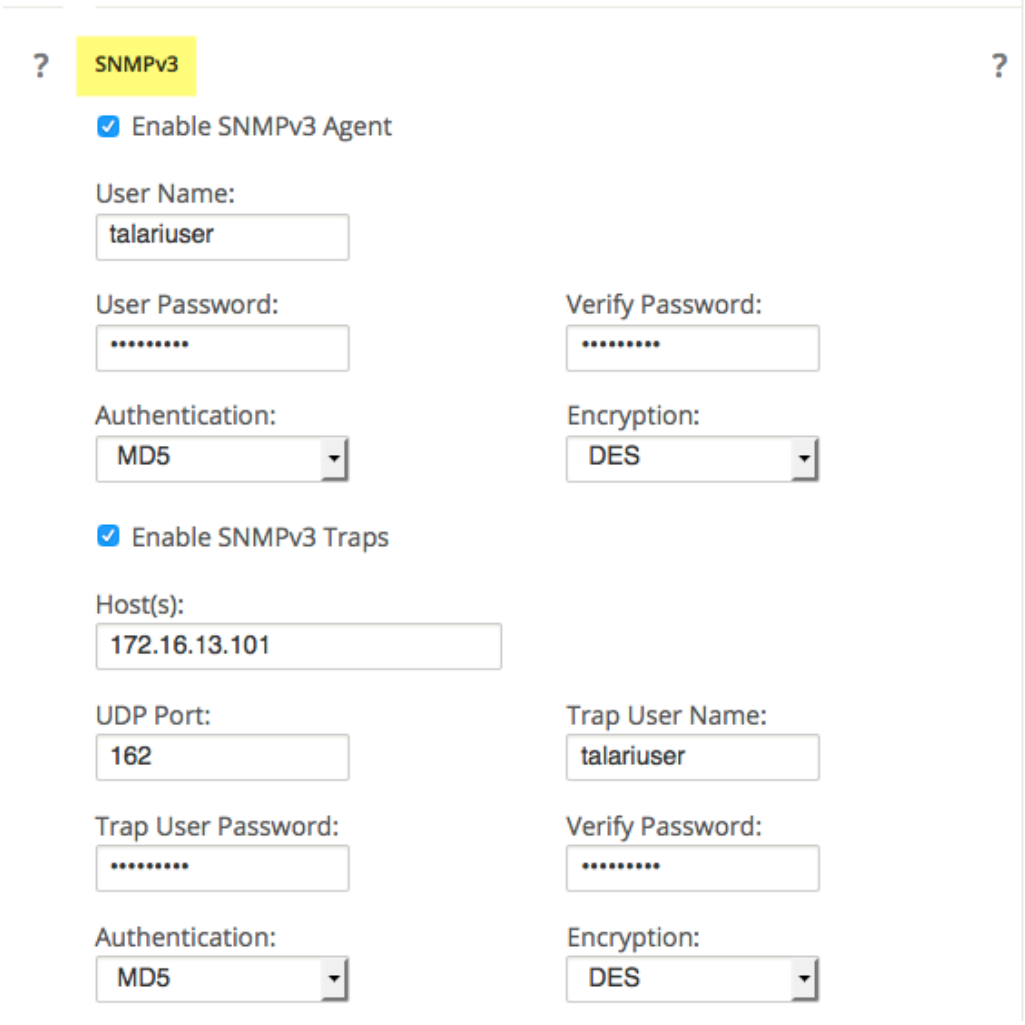
> **Note:**
>
> There is no specific logging or event alerts for this feature, but users may refer to **Monitor > Reports > WAN Links** for a historical trend in bandwidth rates.

SNMPv3 Polling and Trap Capability

> **Note:**
>
> Oracle only supports a single user account for each SNMPv3 capability.

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

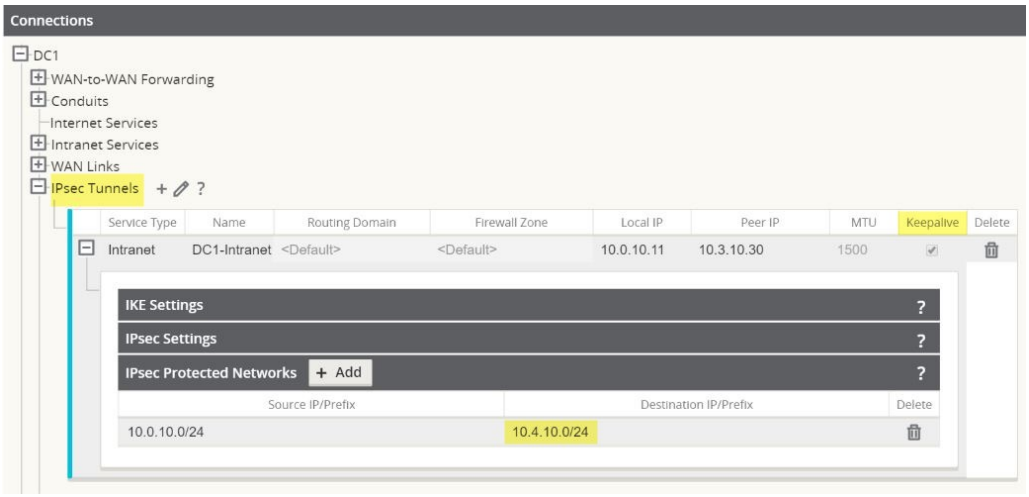
To configure SNMPv3 using Oracle SD-WAN Aware, navigate to **Manage > APN Appliance Settings** and check the box that says **Include in File** in the **Notification Settings** section. Then fill out the SNMPv3 settings as required.



Eligibility for IPsec Non-Conduit Routes

Prior to Oracle SD-WAN Edge 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 Oracle SD-WAN 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.



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 Oracle SD-WAN 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 Oracle SD-WAN Aware 2.2 are done from the web UI under **Manage > APN Configuration.**

Summary

Oracle's Oracle SD-WAN Aware 2.2 software introduces support for polling of up to 550 Oracle SD-WAN Edge 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 Oracle SD-WAN 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.

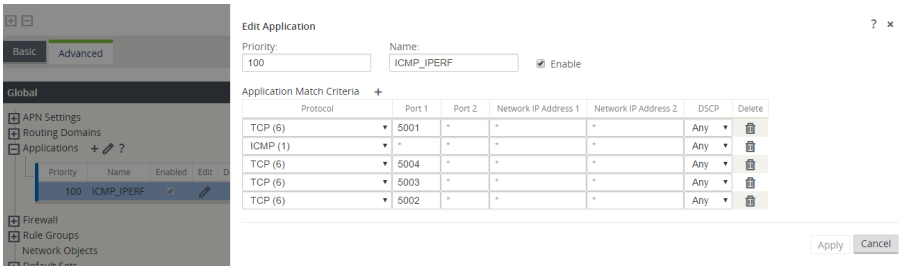


Figure 1: Add a new Application

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.

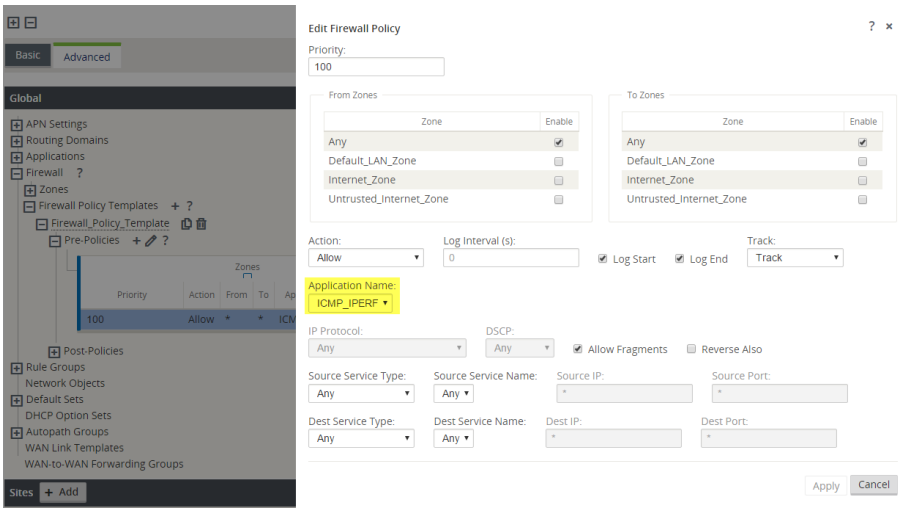


Figure 2: Associating a Firewall Policy with an Application

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

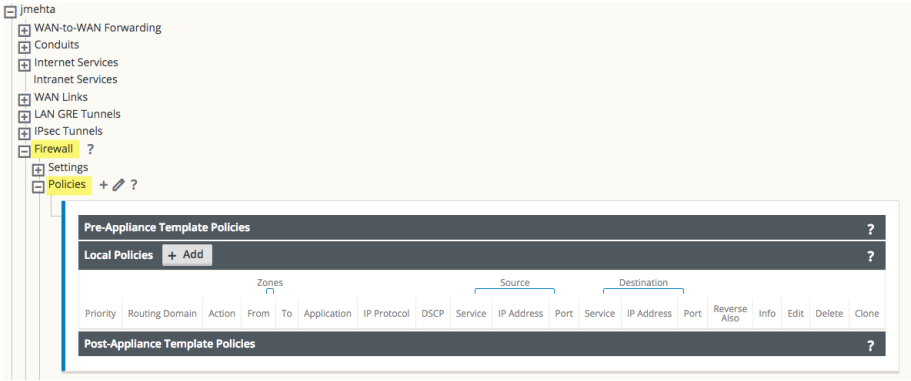


Figure 3: Associating a Firewall Policy with an Application at the Site Level

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**.

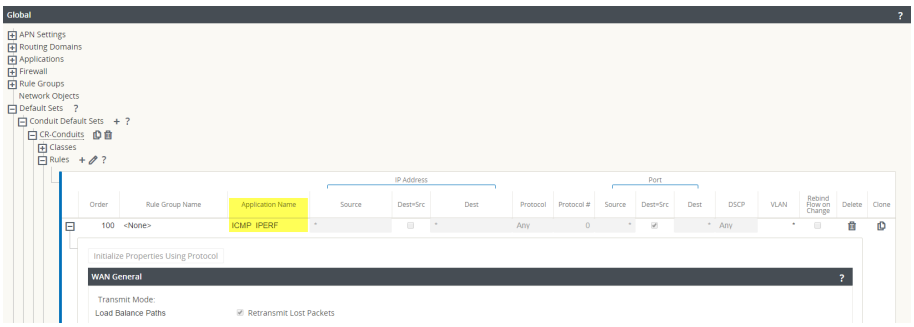


Figure 4: Adding Application to a global QoS Rule

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.

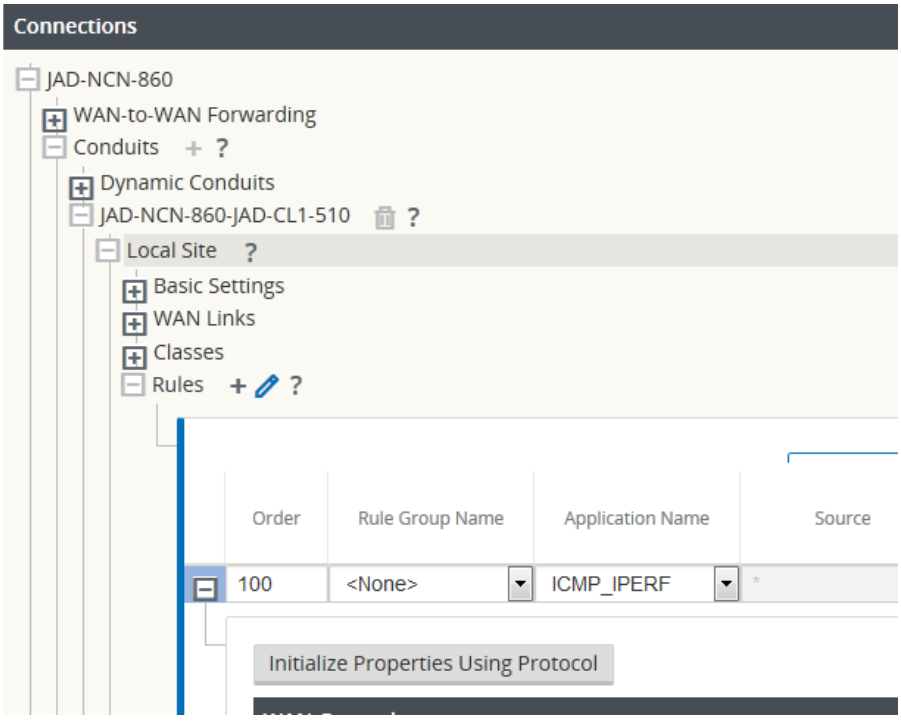


Figure 5: Adding Application to a Local QoS Rule

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.

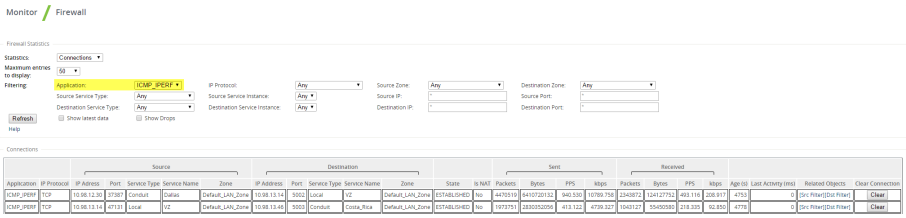


Figure 6: Filtering Firewall statistics by Application

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.

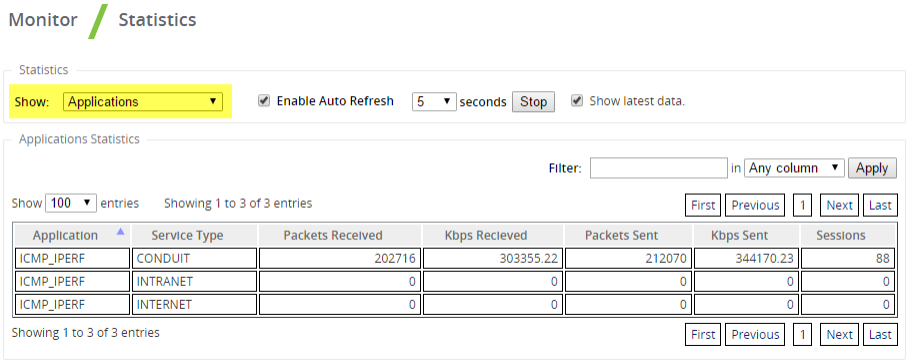


Figure 7: Tracking QoS by Application

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.**

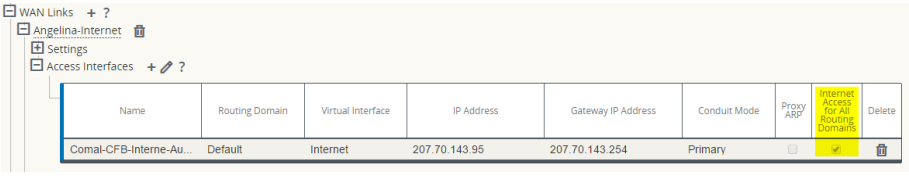


Figure 8: Enabling Internet access for All Routing Domains

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**

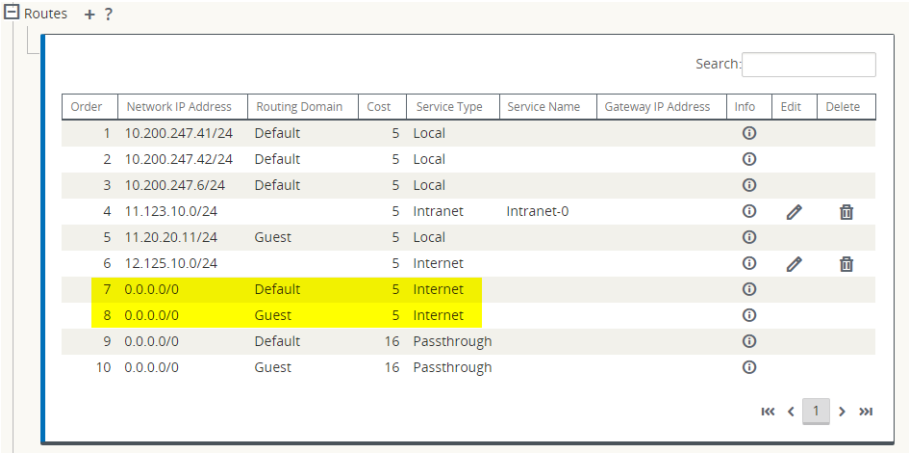


Figure 9: Verifying Routes Added for Each Routing Domain

> **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:

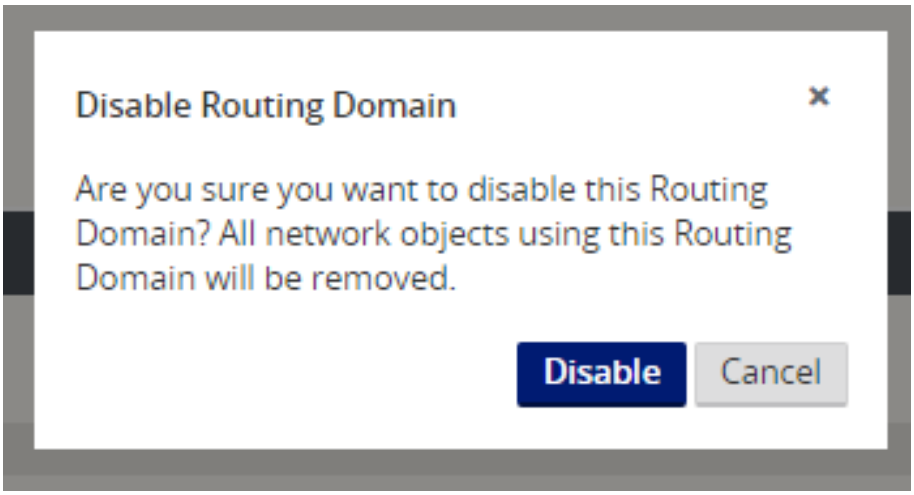


Figure 10: Removing a Routing Domain

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

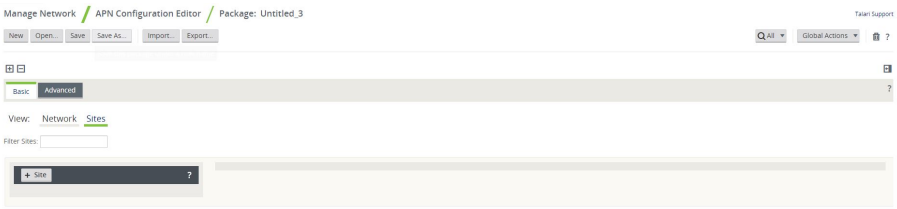
3.0 GA also supports the ability to configure the new Templates that are introduced In Oracle SD-WAN Edge 6.0 GA. New customers with five or more basic sites to setup for the first time will enjoy time savings while setting up new sites and WAN Links. With the use of templates, users may configure certain 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.

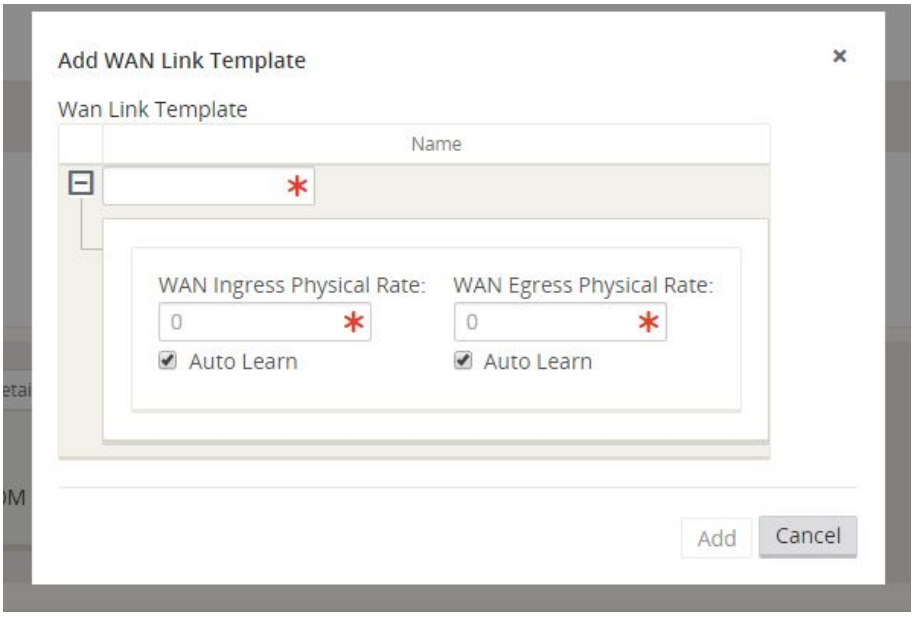
Below are the steps to use this feature through the Basic configuration mode:

Manage Network > APN Configuration Editor > New > Basic.

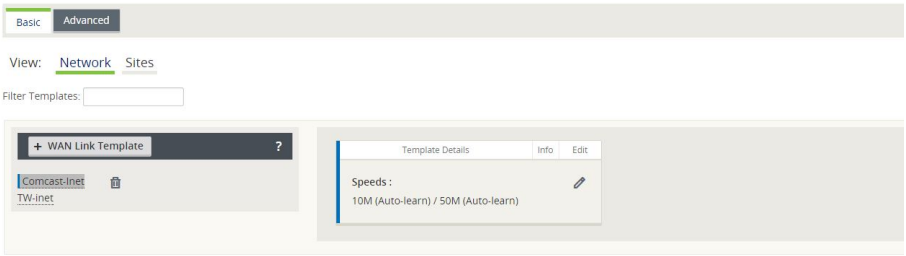


Click Network to change from the (default) Sites view to Network view.

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



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 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.

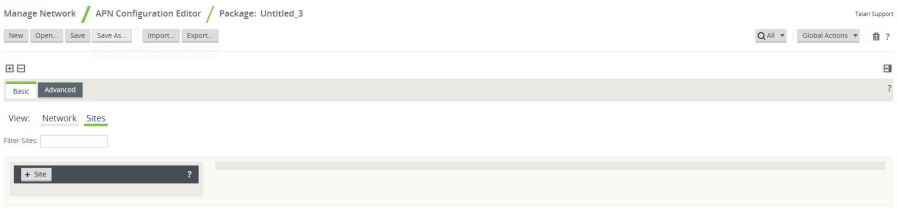
The concept of the **Basic > Sites** view is to simplify the configuration process to allow the user to create a configuration file, which will generate a Conduit between the defined sites. The required configuration properties for a Conduit between sites include:

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

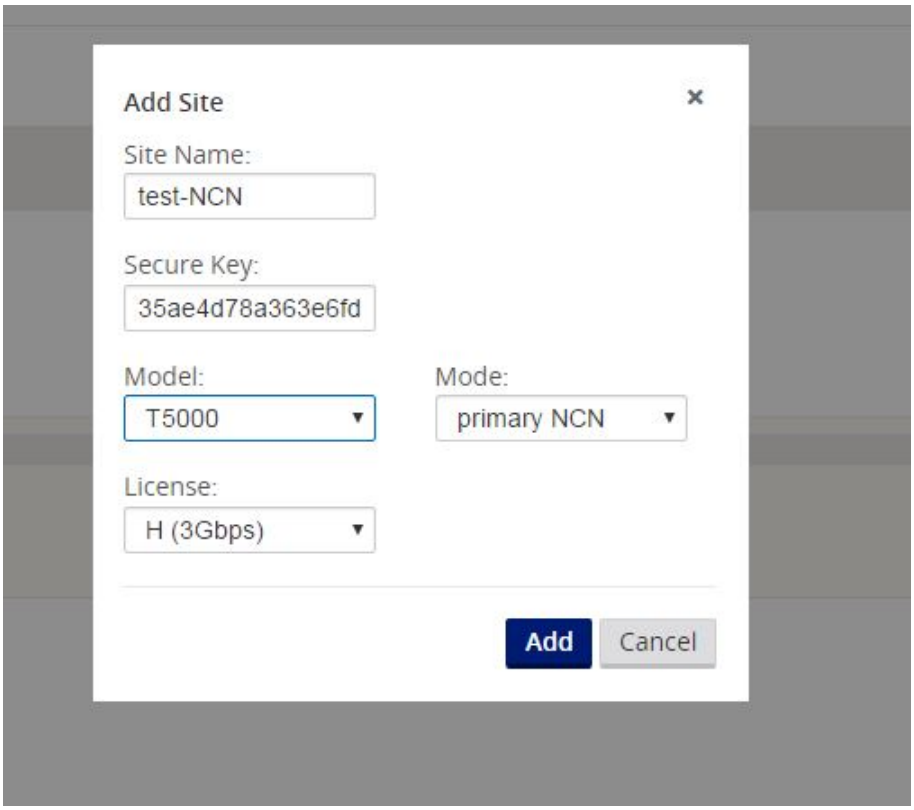
Existing users will observe that one configuration change on the Basic mode view may in fact modify or change more than one setting in Advance mode. Basic mode does allow the Import of existing configurations, and allows the user to move between Basic and Advanced modes.

Below are the steps to use the Basic configuration mode.

Manage Network > Configuration Editor > New > Basic.



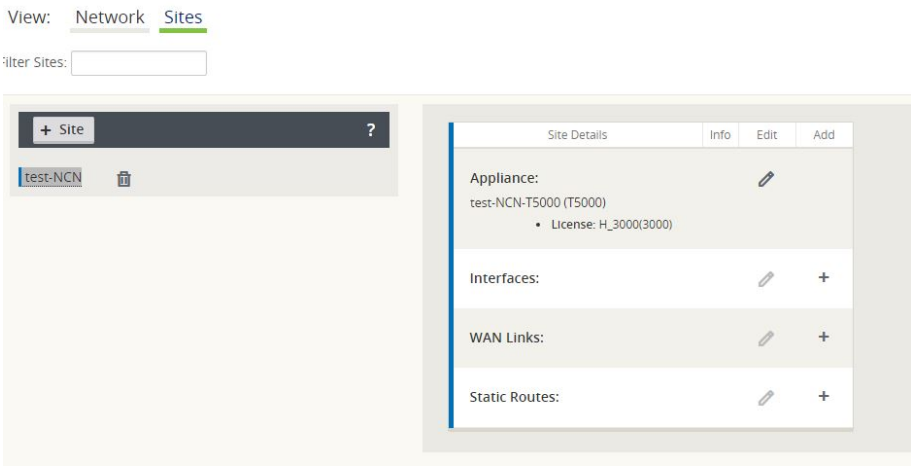
Click **+ Site** and enter basic site details.



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.

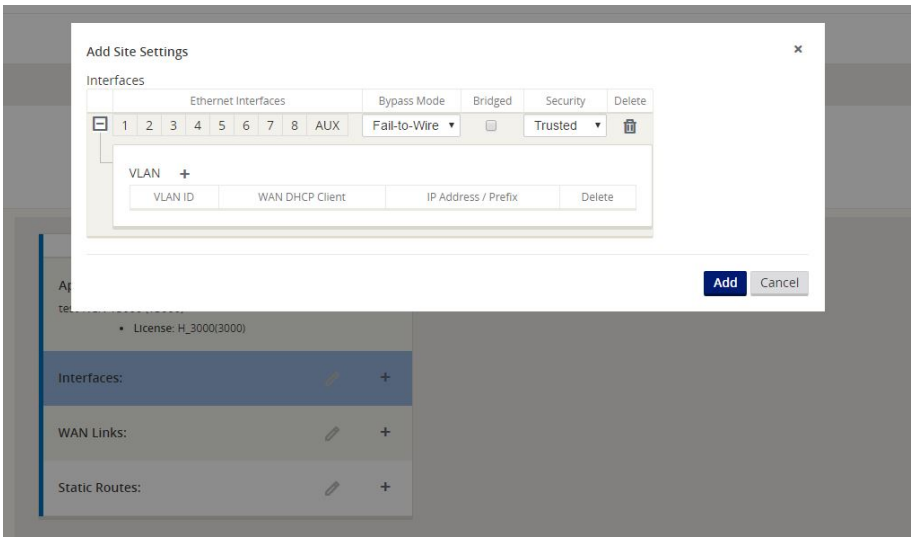
Appliance

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.



Interfaces

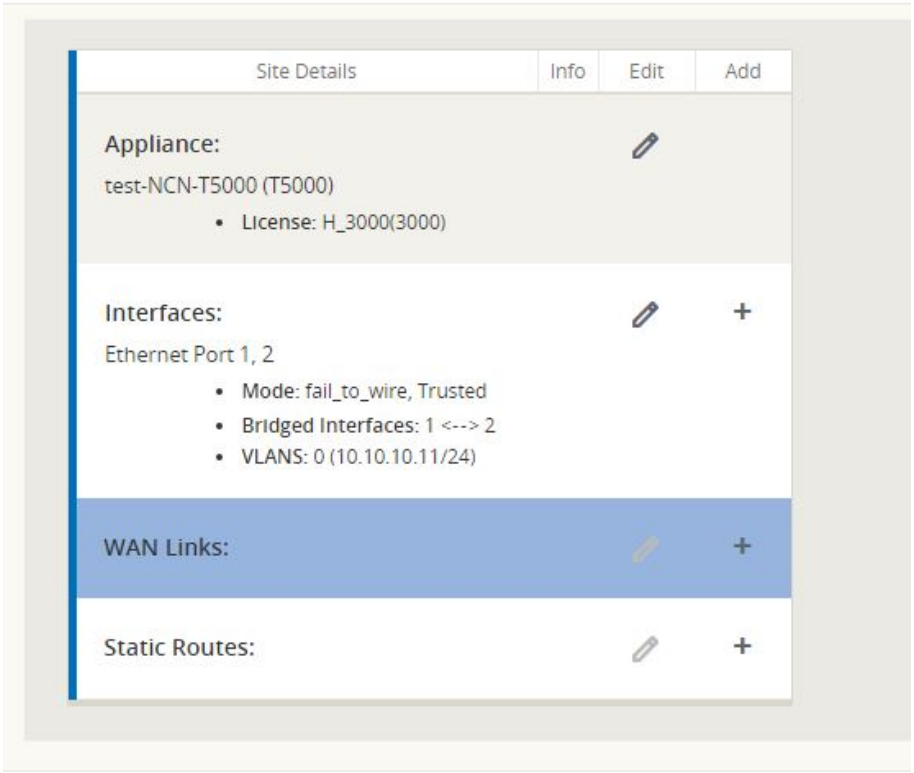
Clicking the Add / Edit Icon to the right of the Interfaces summary view shown for the site will provide the ability to add, edit, and delete Interfaces.



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.

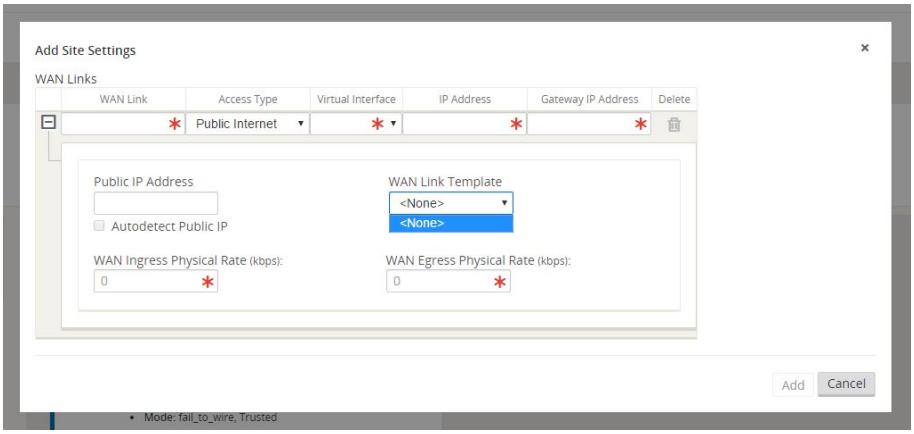
WAN Links

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.

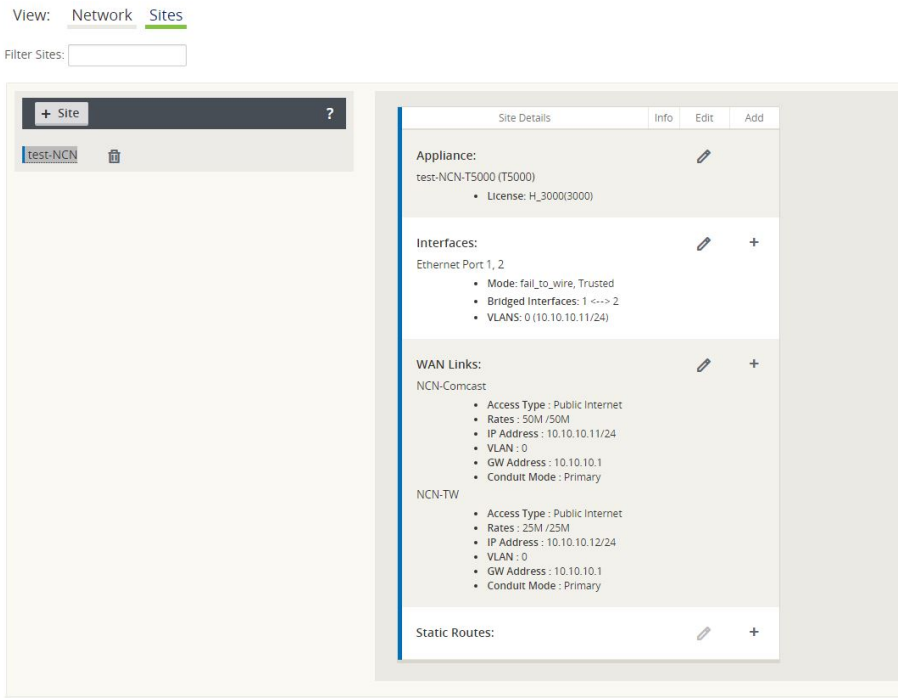


While Adding / Editing a WAN Link, the option to use a WAN Link Template is provided. After selecting a WAN Link Template, the WAN Link will be configured using

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.

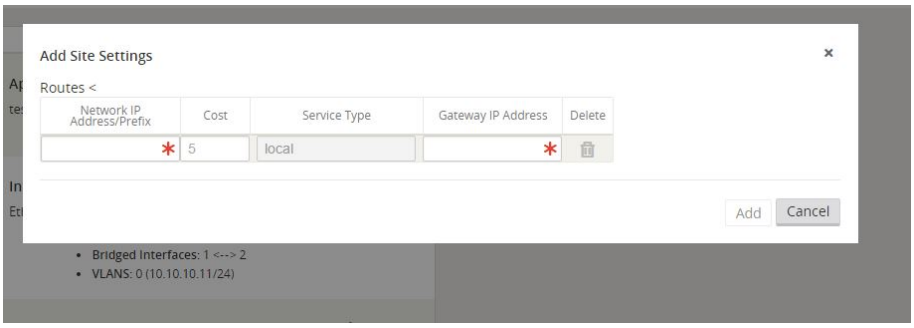


A summary view of WAN Links is then displayed in Basic mode after the initial configuration is complete.

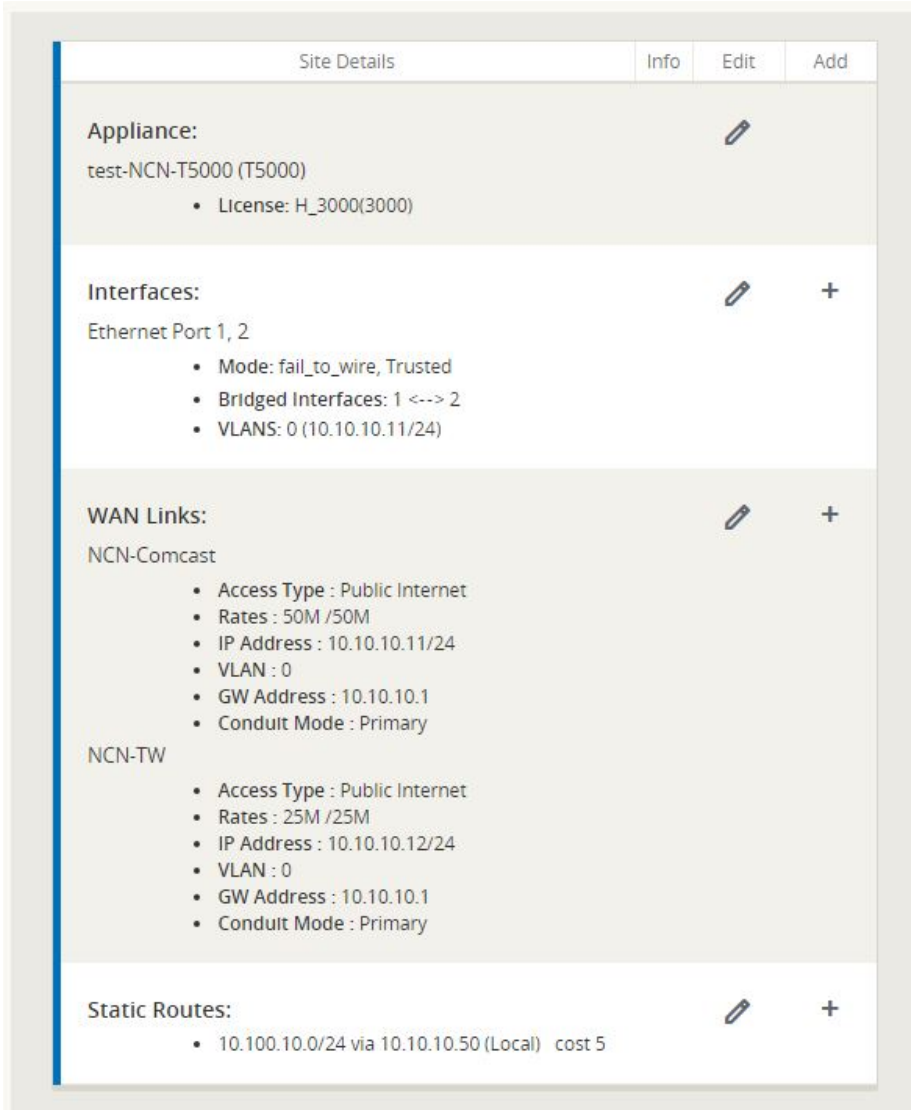


Static Routes

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.



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.



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.

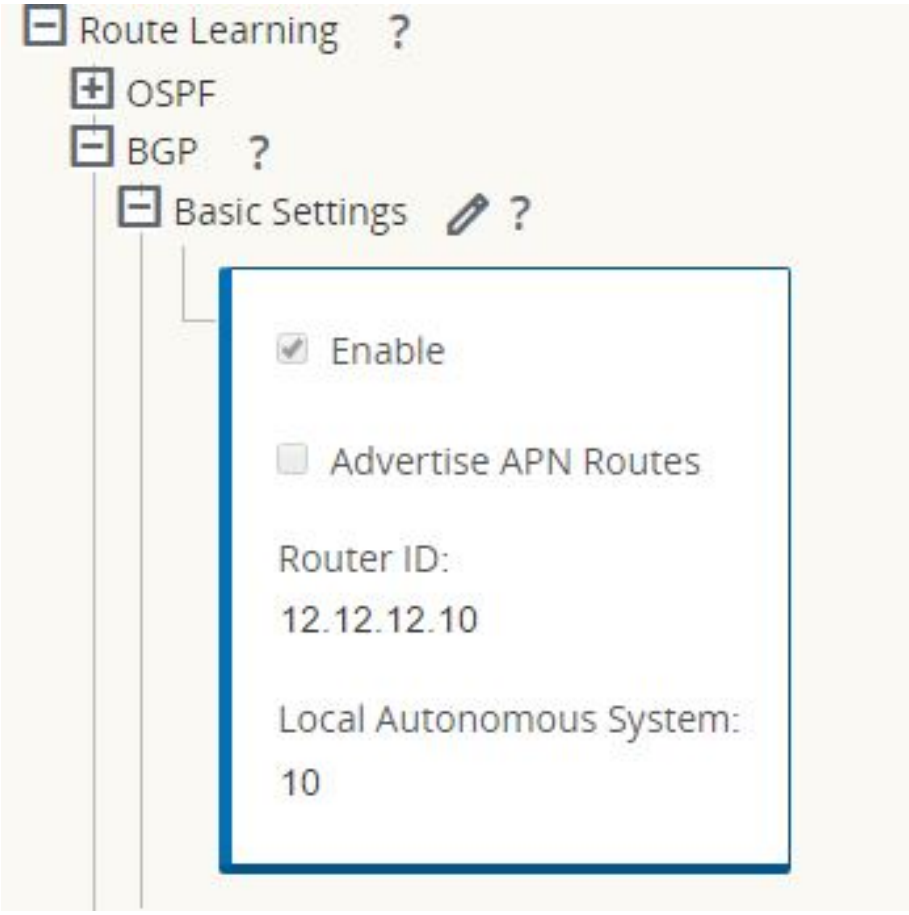
Configure Trusted Virtual IP Address

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

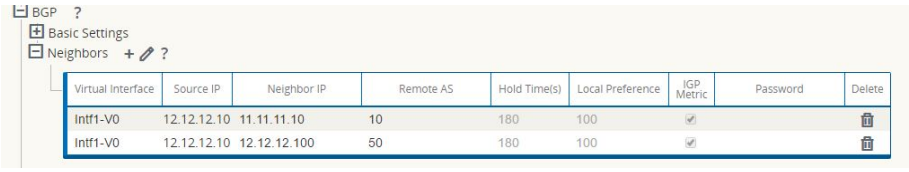
To use a Virtual IP Address for Dynamic Routing, go to **Sites**, and then **[Site Name]**, and then **Virtual IP Addresses**. Click the **Identity** checkbox for a Virtual IP Address to use it for IP services.

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.



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



> **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.

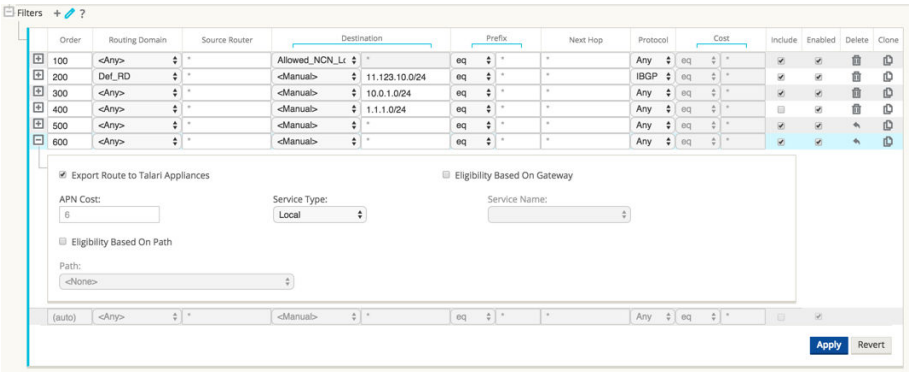
1. Choose a **Virtual Interface** from the drop-down menu. The Virtual Interface will determine the **Source IP Address**.

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**.**



> **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, **e**nter 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.

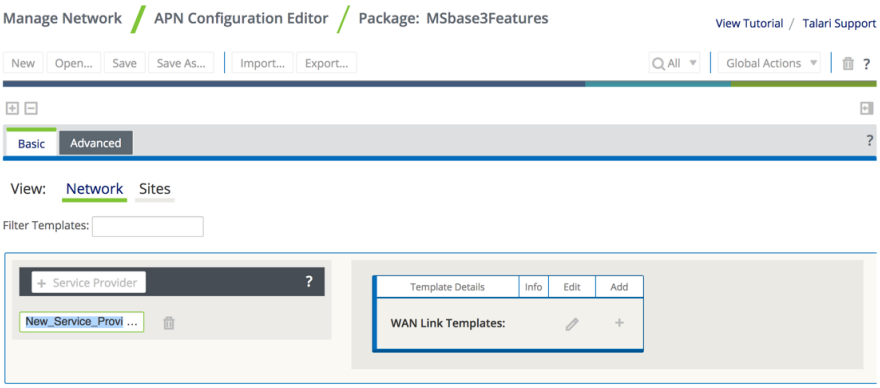
Oracle SD-WAN Edge 6.1 now supports BGP attribute manipulation for ingress and egress per peer. Please contact your Oracle Representative for additional information on this topic.

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

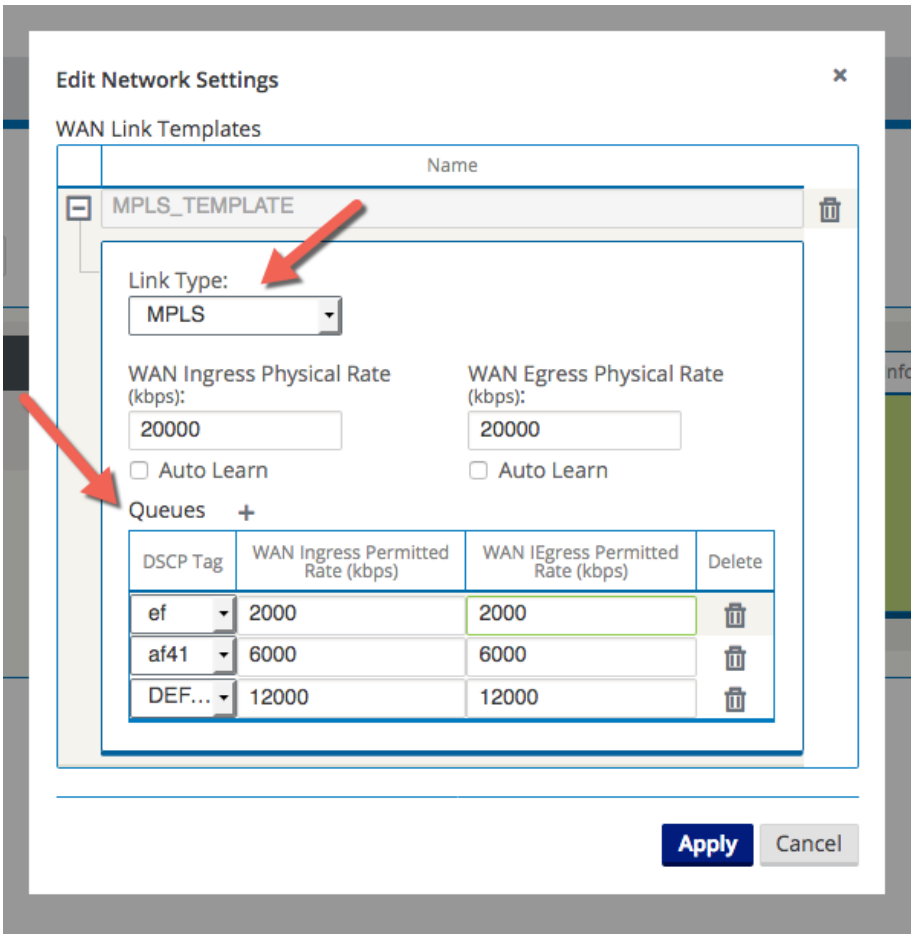
WAN Link Template for newly created sites, as well as an easier way to clone branch locations with similar Service Provider attributes.

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.**

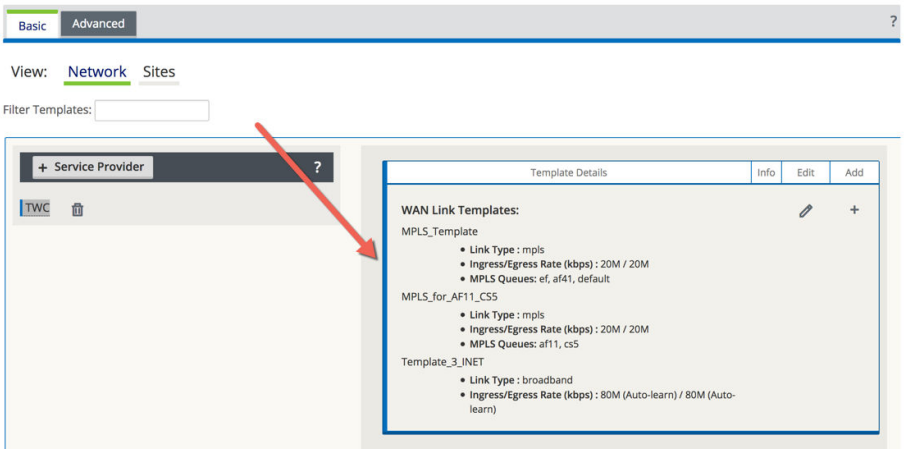


A New_Service_Provider option will appear, click inside this box to change the name, then click the **+** icon to create a new WAN Link Template.

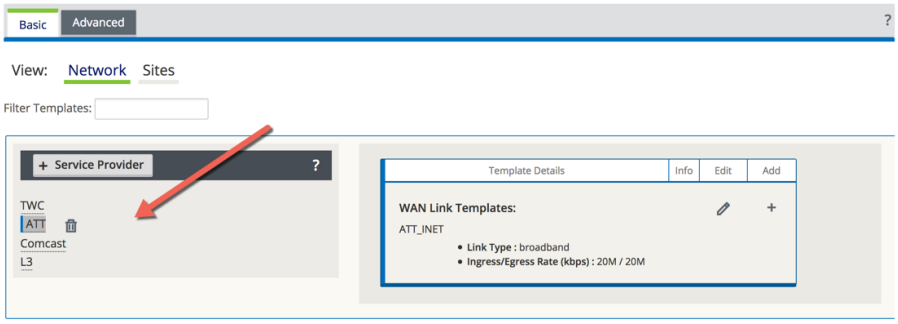
Select the Link Type from the drop down and enter the WAN Ingress and Egress bandwidth rates. If your WAN Link is an MPLS link, you will have the ability to enter up to 8 queues based on DSCP Tag.



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.

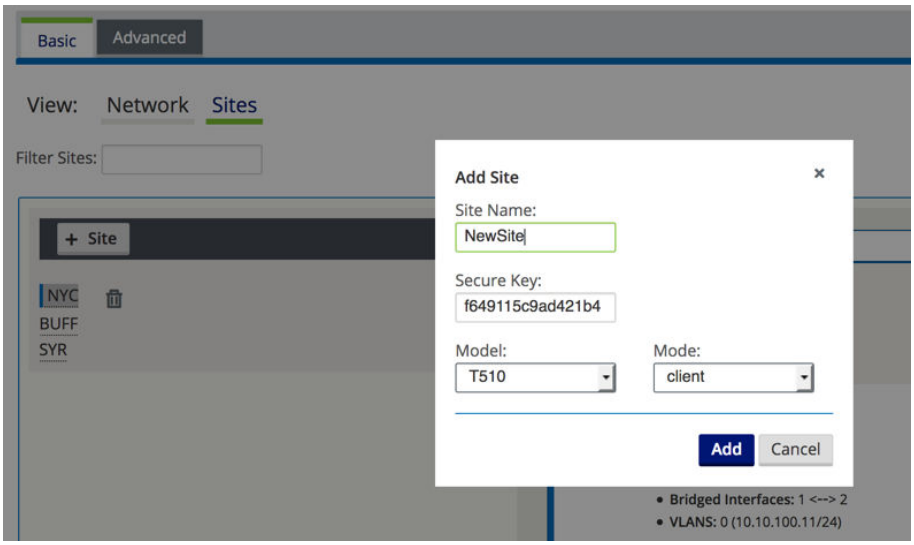


The user may also define up to twenty Service Providers, although only four are shown in this example.



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.



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.

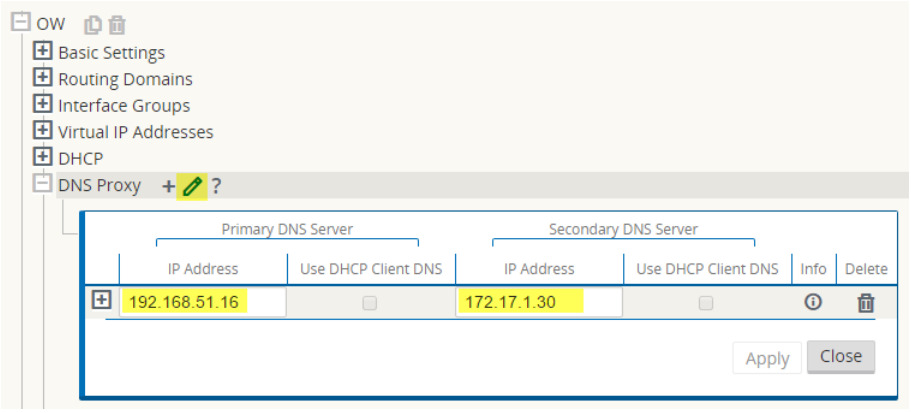
Application Identification: DNS Proxy

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

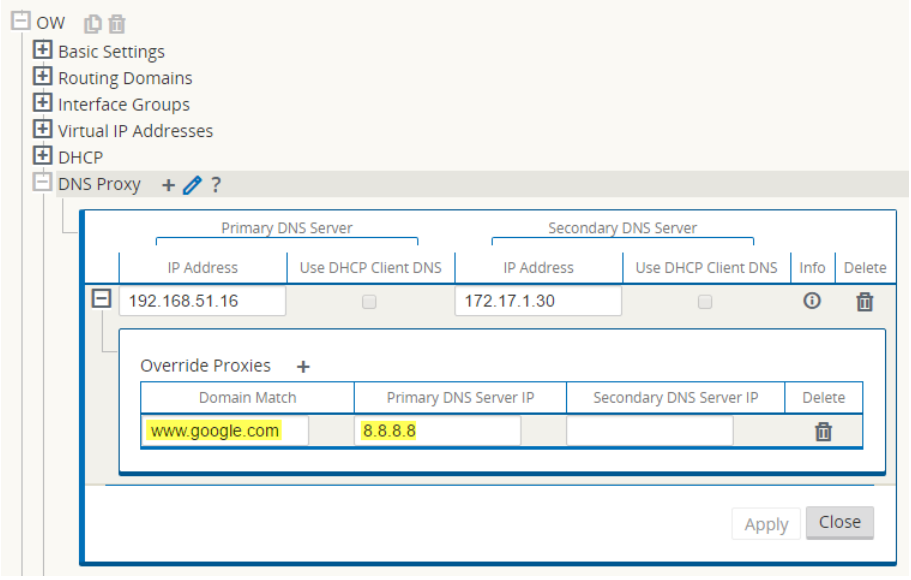
certain web sites sent out the local Internet circuit verses backhauling these sites through the Conduit to the NCN site.

Enabling DNS Proxy

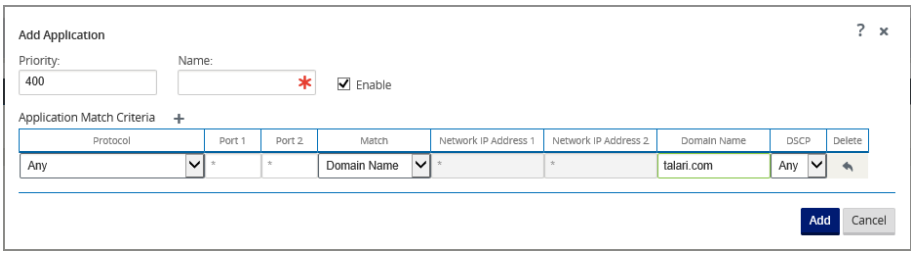
From Aware, navigate to **Manage > Configuration** and **Import** the current configuration file from the Active NCN. On the Advanced view tab, navigate to **Sites > [Site Name] > DNS Proxy**. Users can manually configure the Primary and Secondary DNS server IP addresses to be used, or select the **Use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



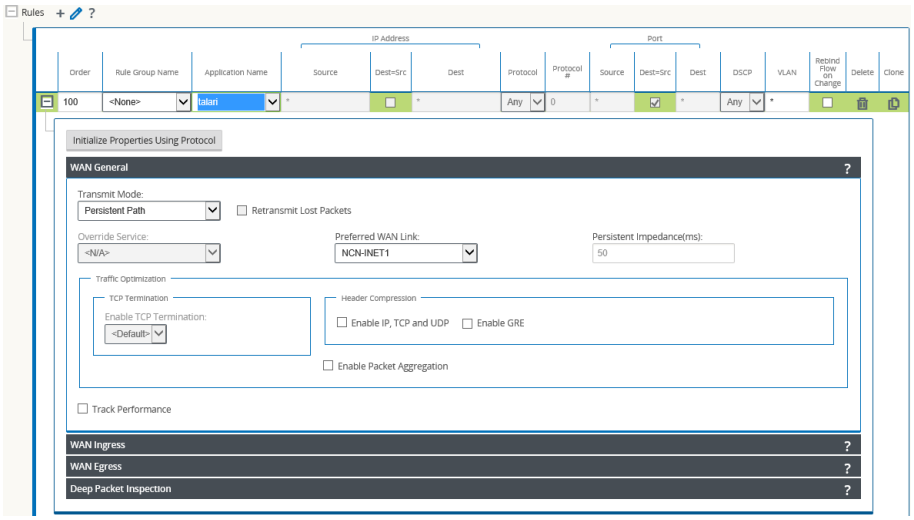
Click the **(+)** icon to expand and configure Override Proxies for DNS requests matching certain domain names.



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



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



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

Persistent Path Traffic Steering

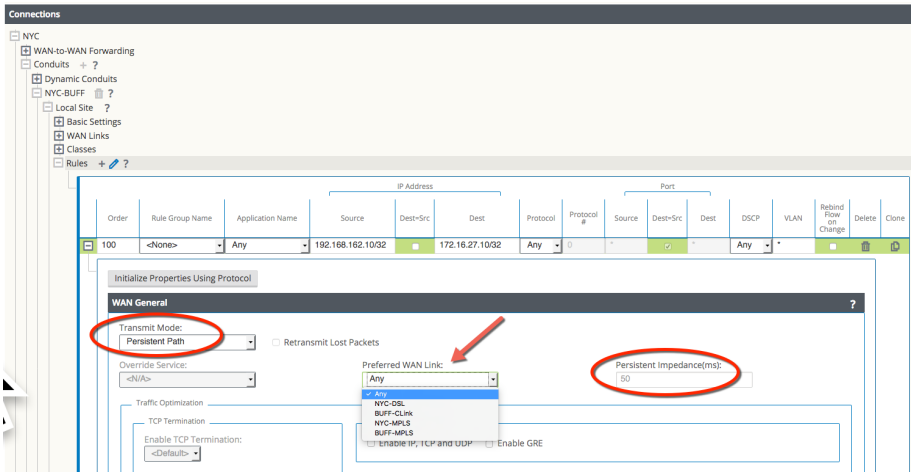
6.1 GA introduces Persistent and Conduit Path Steering providing users the option to select a favored WAN Link when creating a Conduit Rule using Persistent Path as the Transmit Mode. As an example, a user may now use Path Steering to direct voice traffic down the MPLS WAN Link.

> **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.

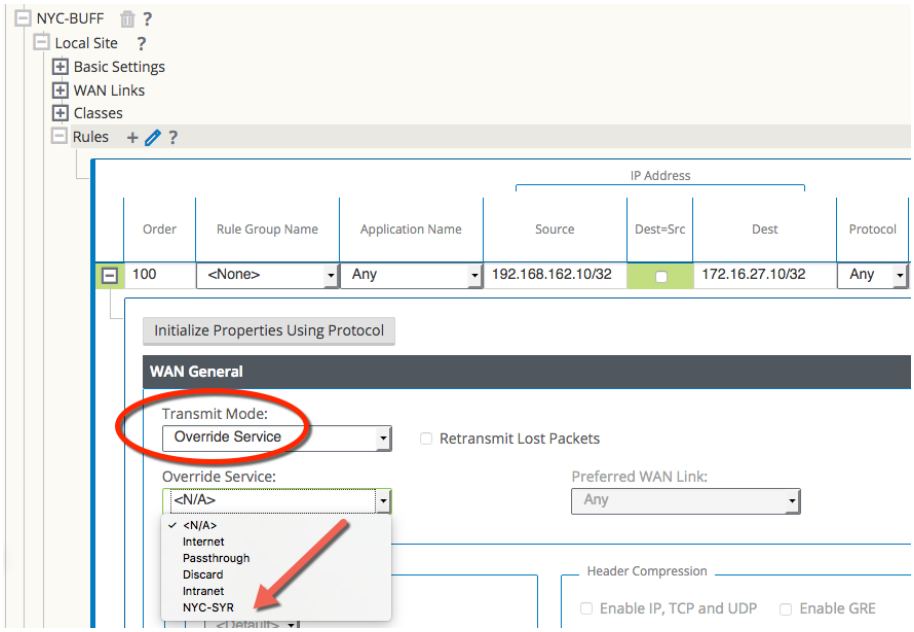
The chosen Path will be the one used for new flows matching this Rule as long as the queue depth is not above the user configurable Persistent Impedance value, which is

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.



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.



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.

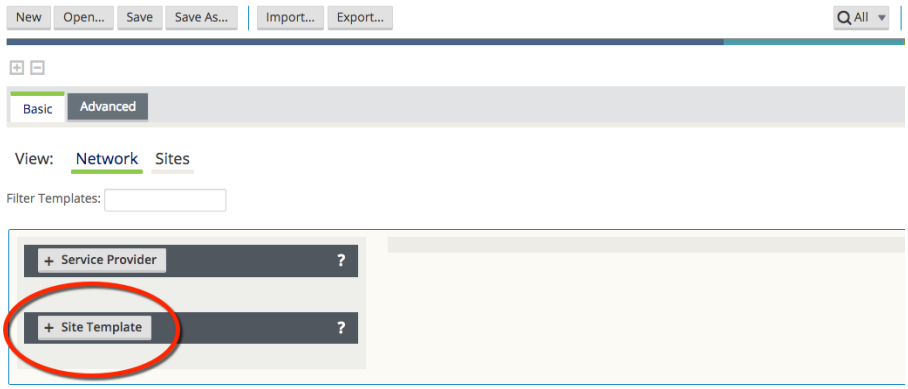


Figure 1

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.

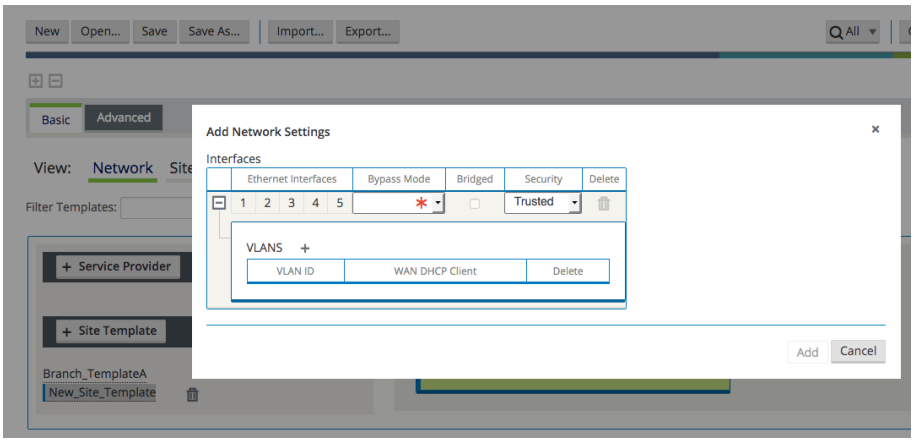


Figure 2

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

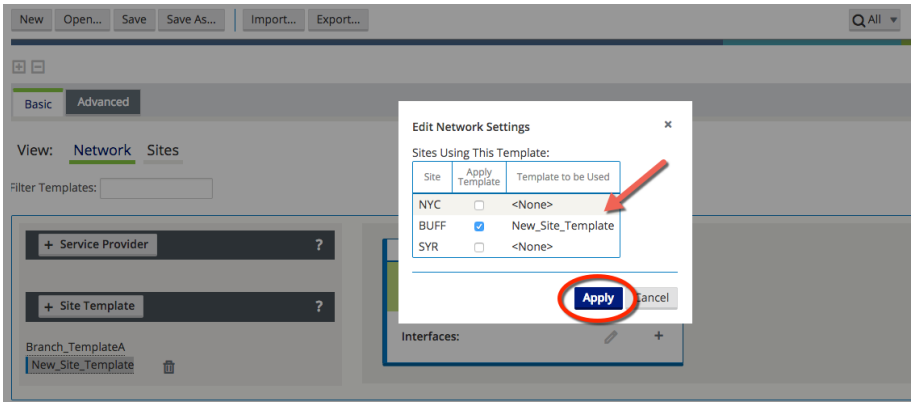


Figure 3

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.**

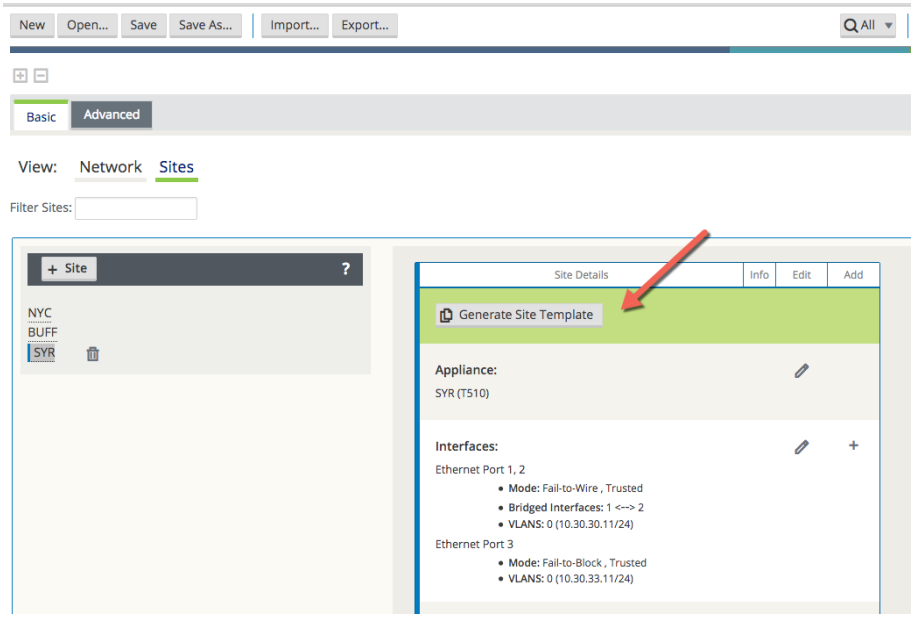


Figure 4

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.

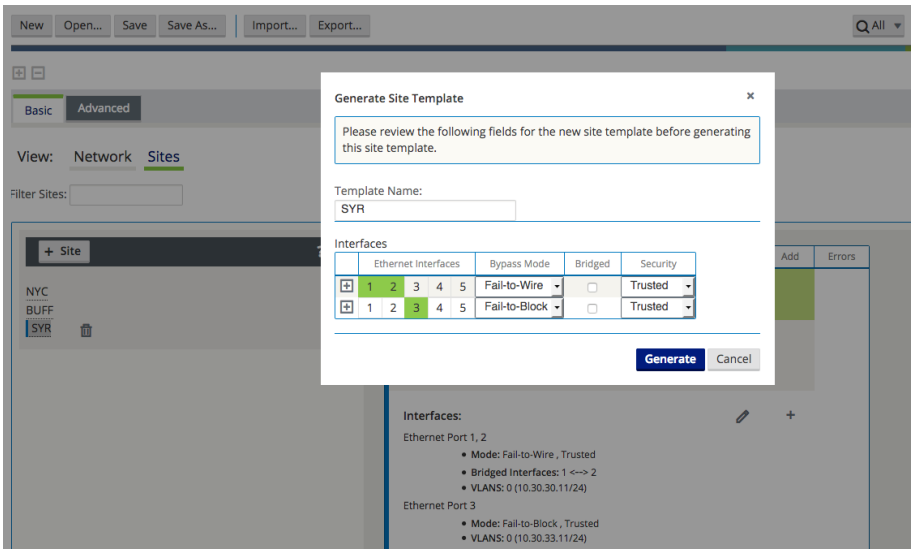


Figure 5

Observe Branch_TemplateA now appears on the Network view page.

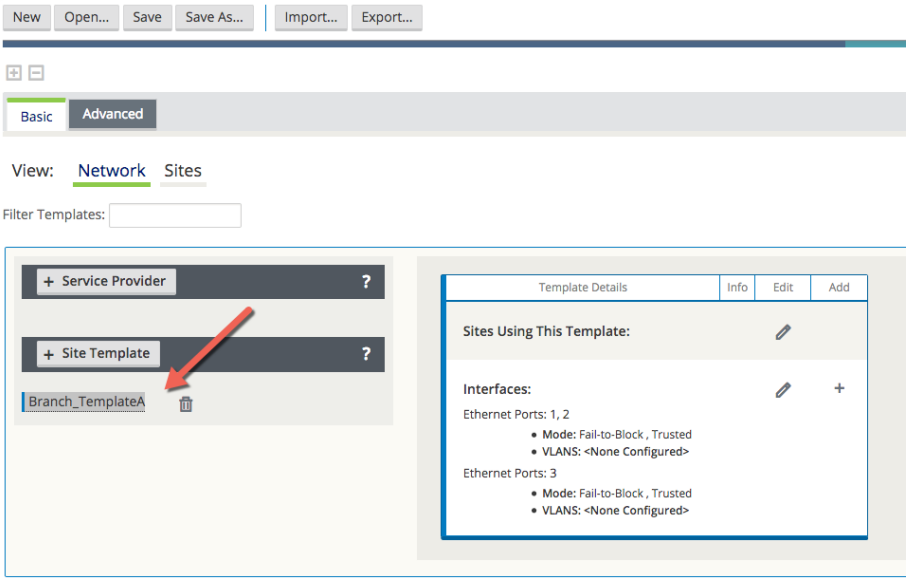


Figure 6

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

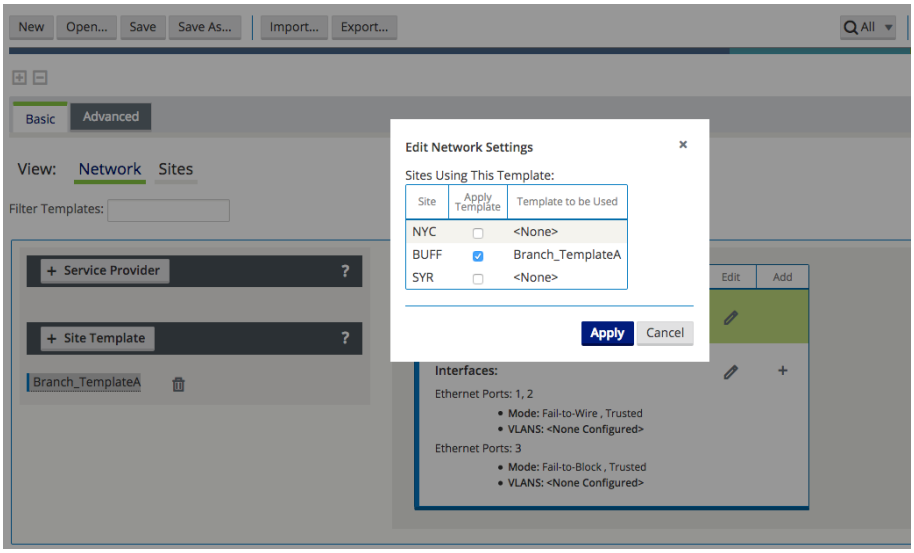


Figure 7

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

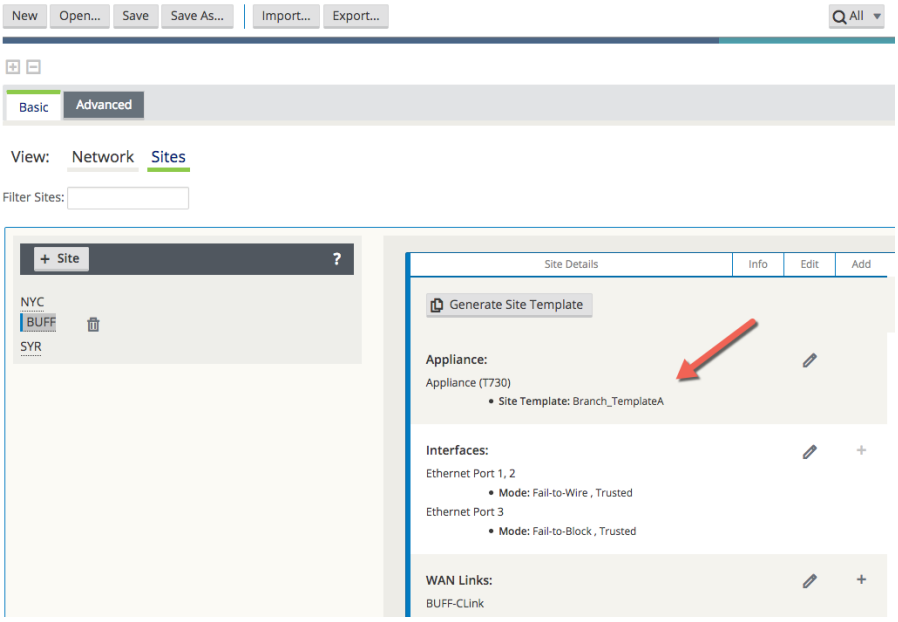


Figure 8

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

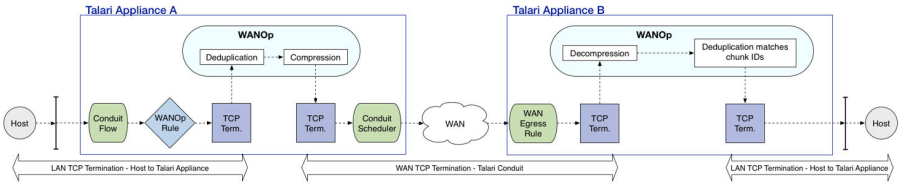
Release 4.0 Features

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.

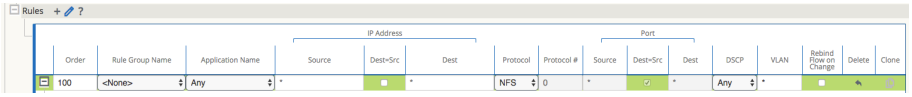
Session Capacity for Supported Models

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

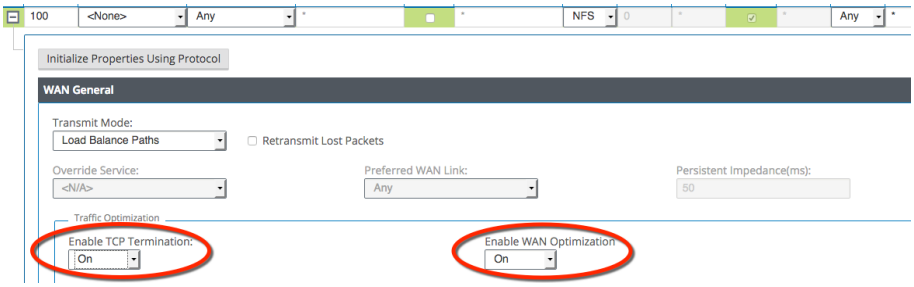
The Oracle WANOp solution is configured on a per-rule basis and performs deduplication and compression on TCP Conduit traffic.

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.



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.



> **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.

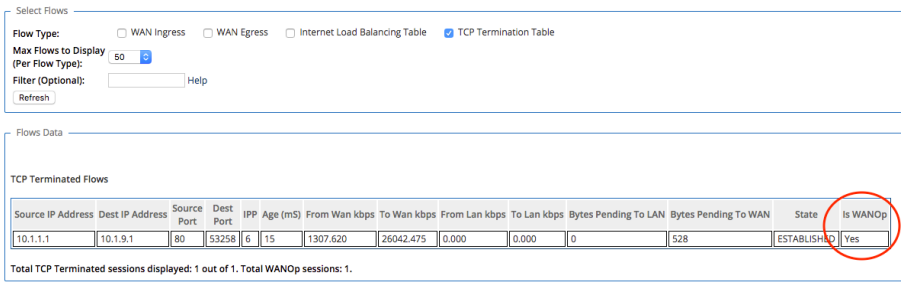
A reciprocal rule enabling WANOp will be generated automatically at the remote site of the selected Conduit.

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:

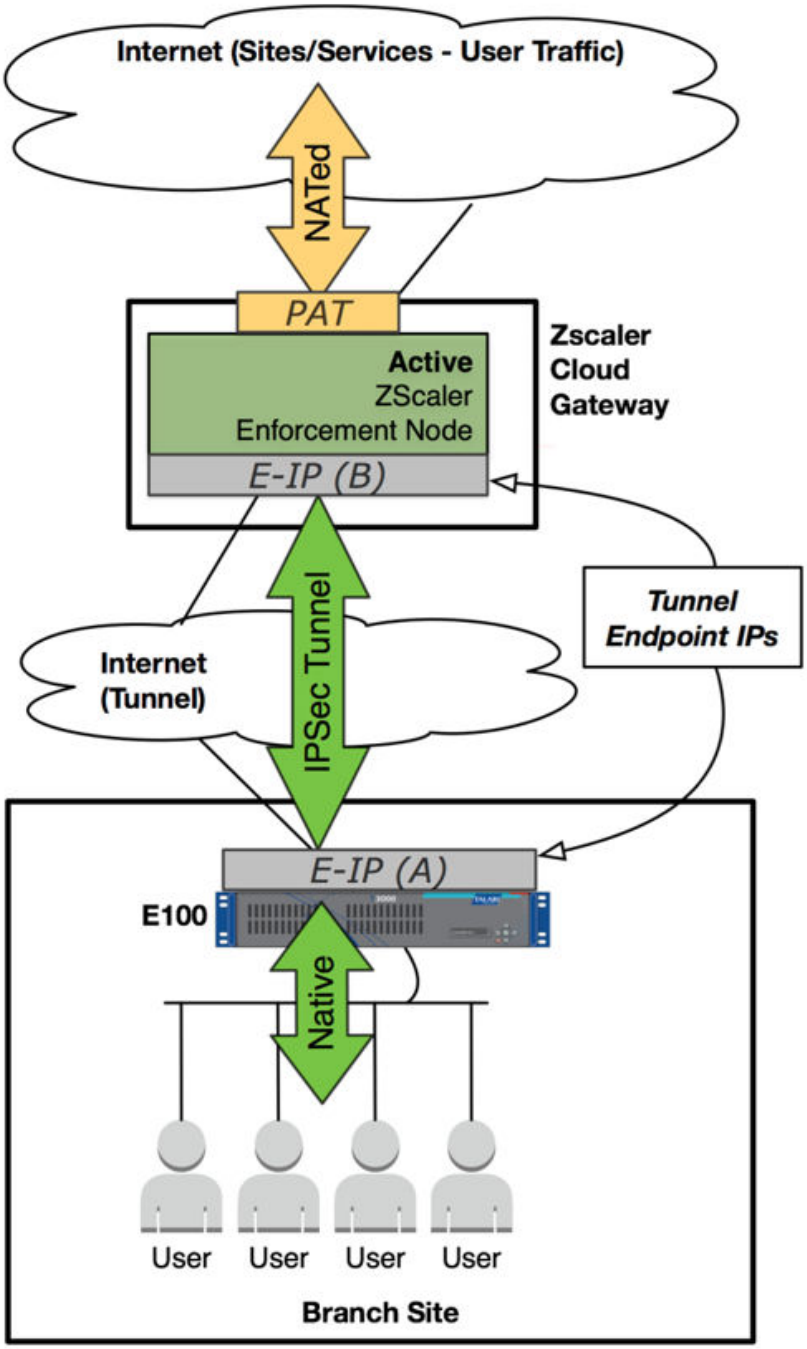


For more information on the Oracle WAN Optimization solution, including more detailed capabilities, performance, and monitoring options, please see the Oracle WAN Optimization Guide.

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.

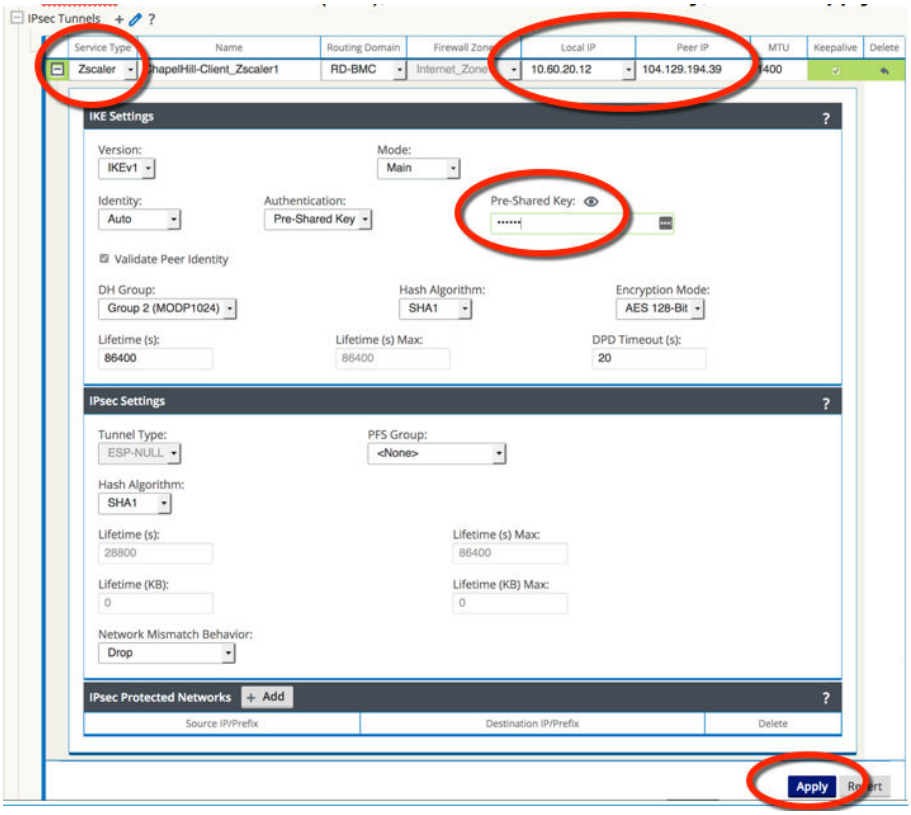
Introduced in Oracle SD-WAN Edge R7.0 GA, users can now integrate a branch office Appliance with the Zscaler Cloud Security Gateway via IPSec tunneling, for the purposes of tunneling Internet-destined traffic to Zscaler for cloud-hosted filtering and security services.



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**.



> **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.

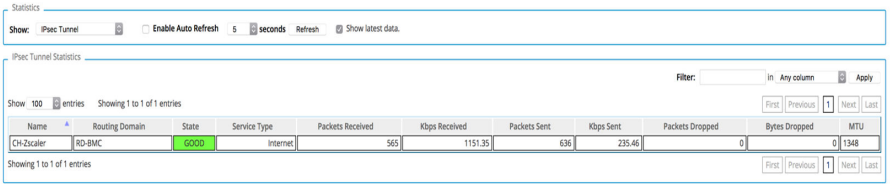
Save the configuration and **Export** it to the **Change Management inbox** of the NCN. Follow the Change Management process to **Stage** and **Activate** the new configuration.

Verification

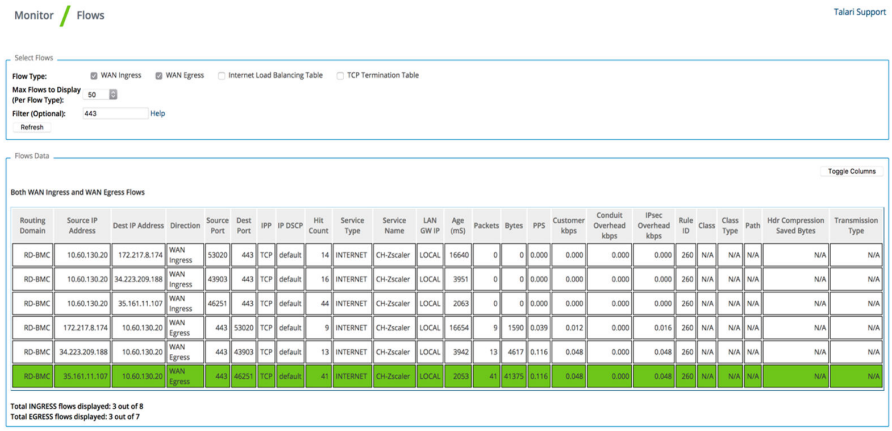
Once the new configuration is running, follow the steps below to verify functionality.

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

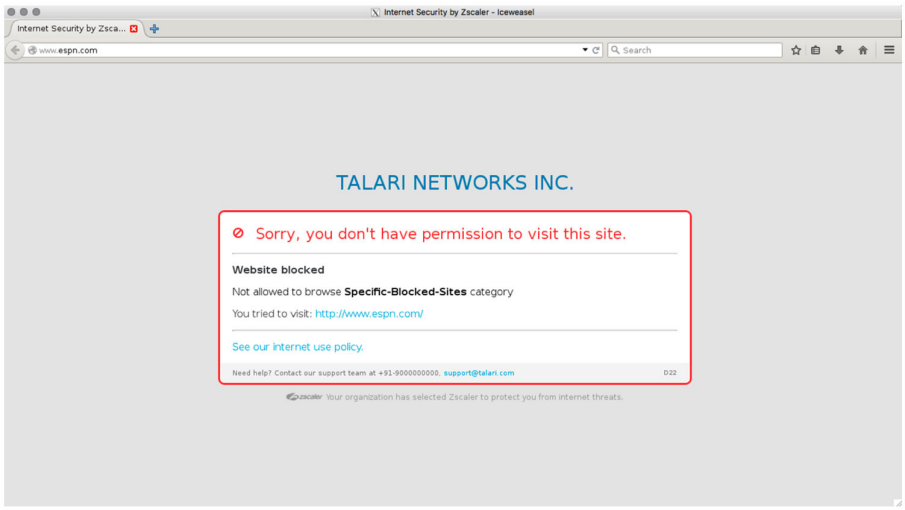
2. Verify the Zscaler IPSec Tunnel status in the web UI of the Appliance under **Monitor**, and then **Statistics**, and then **IPSec Tunnel**.



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.



4. Verify Zscaler is blocking the traffic.



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**.

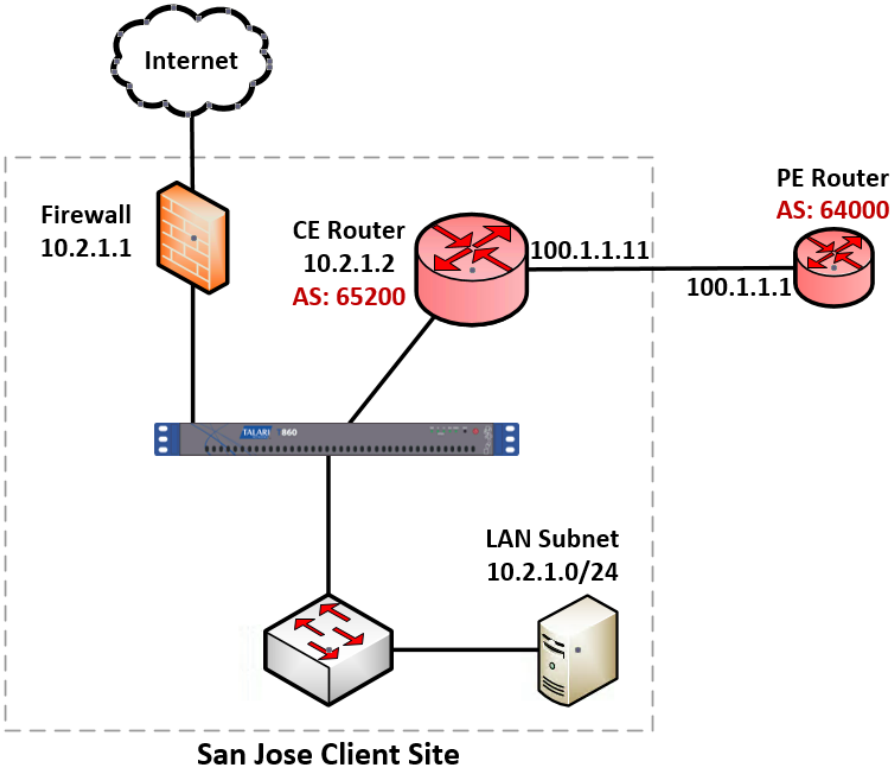
> **Note:**
>
> R7.0 GA only supports a single VRF/routing domain for Zscaler.

Customer Edge (CE) Router Replacement Within the Edge

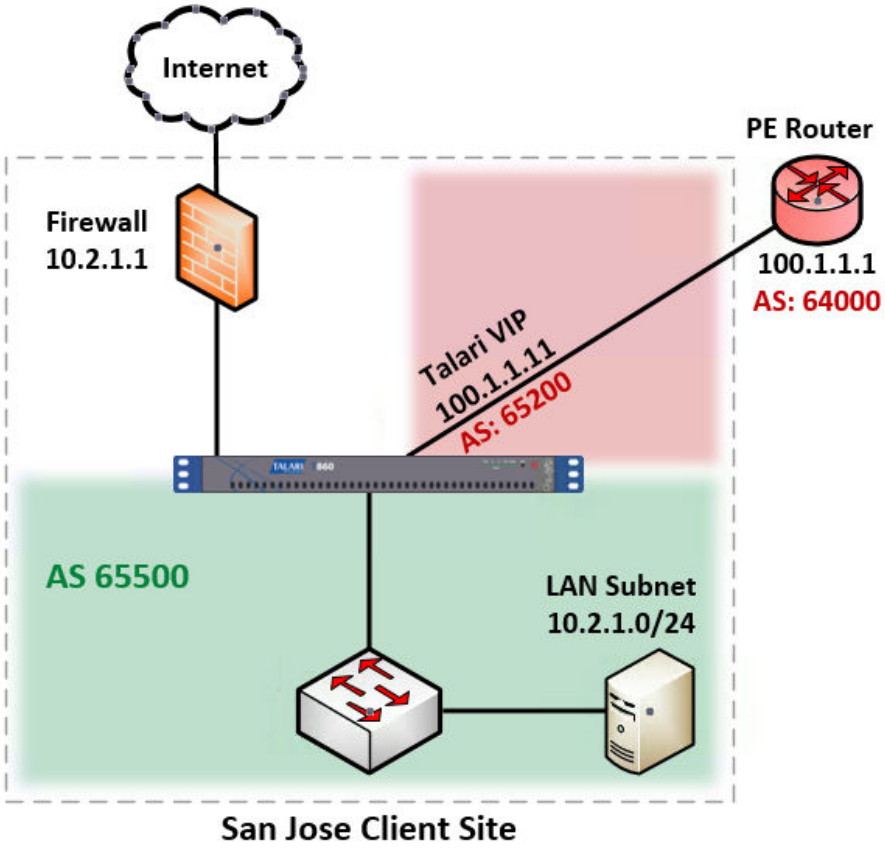
Oracle SD-WAN Edge 7.0 introduces the ability to replace a Customer Edge Router with a Oracle Adaptive Private Network Appliance. This is accomplished by leveraging the Oracle APNA's ability to masquerade its Local Autonomous System (AS) number (on a per-neighbor basis) so that it can peer with a Provider 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.

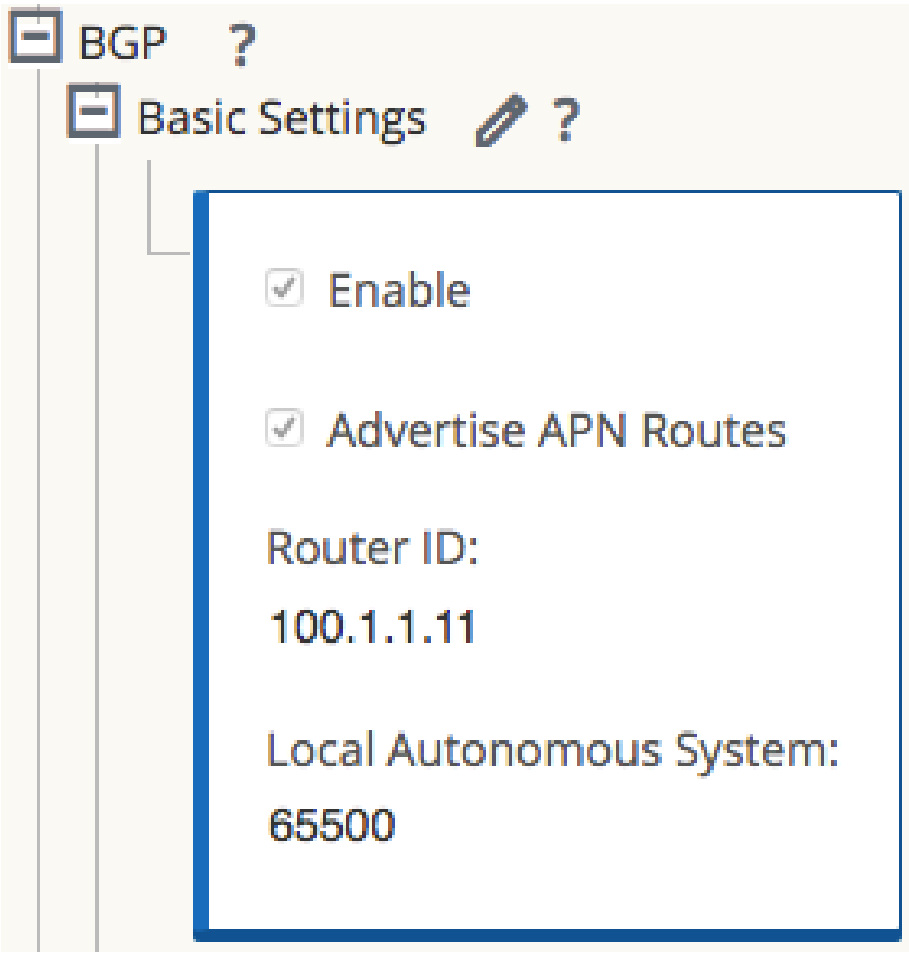


The CE router is removed and the Oracle APNA peers directly with the PE router via eBGP by masquerading its AS number as the replaced CE router's AS number (AS 65200). The APNA's actual Local AS number is 65500 and it can peer via iBGP with local routers in this AS.

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

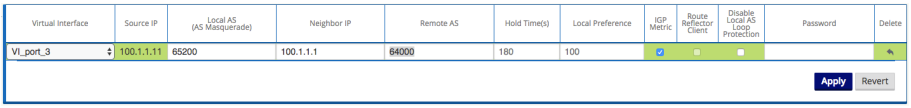
Import the current configuration running on the Active NCN, then navigate to **Connections > [Site Name] > Route Learning > BGP > Basic Settings** and click the pencil icon to edit.



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.



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.

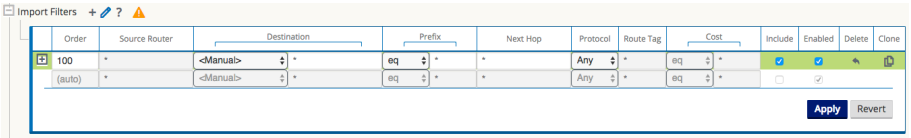
The following options may also be set:

- **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.

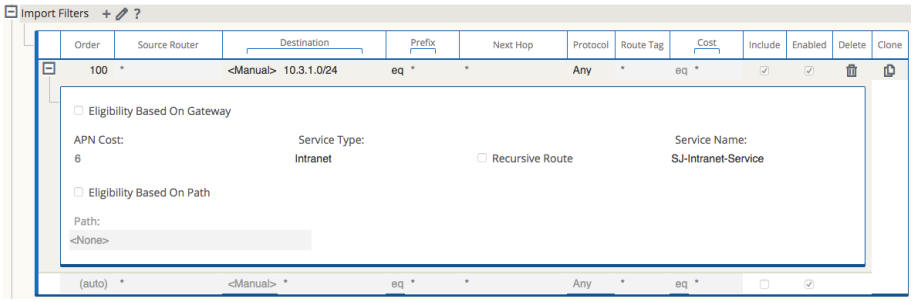


Note:

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.



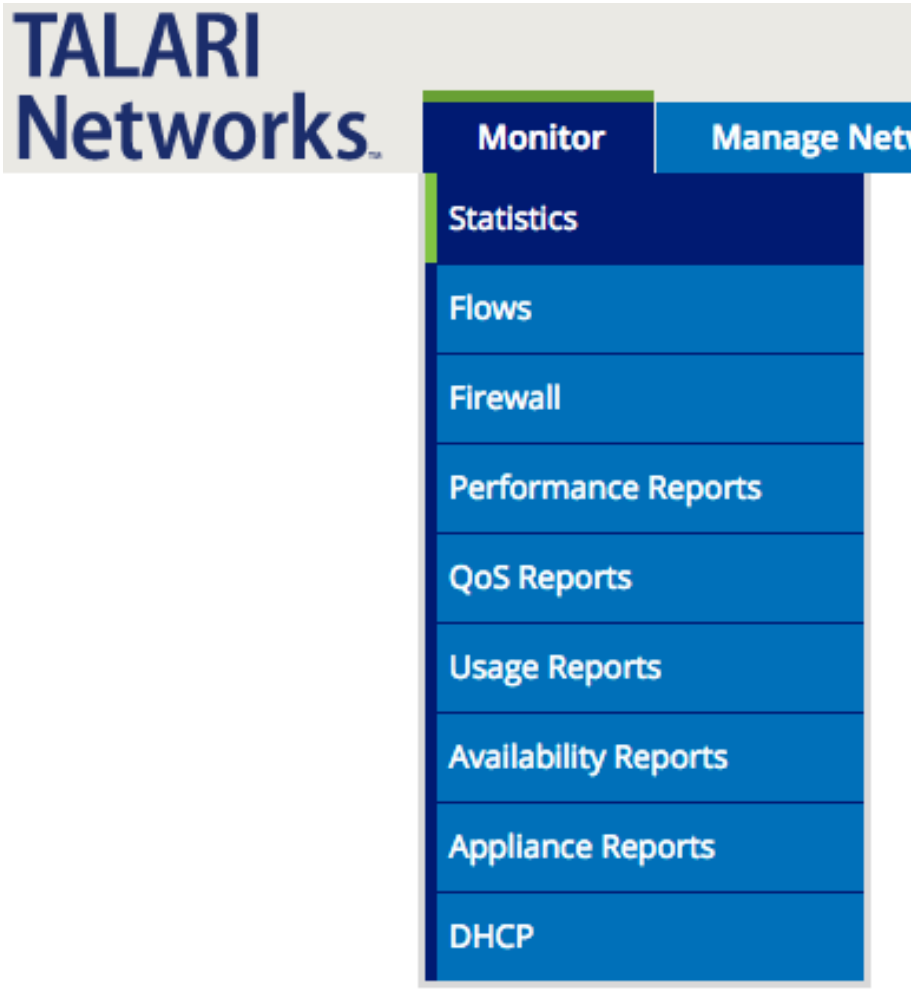
Once configuration of the Edge is complete, it should be saved and the **Change Management** process from the NCN should be used to push the configuration changes to the APNAs.

Static Routes File

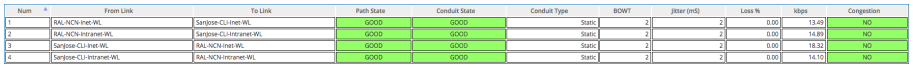
Appliances provide a **Static Routes** file that can be edited to define routes that should persist through software and configuration changes made to Edge. This is used for inserting static routes into the dynamic routing table, not the Edge routing table. It ensures that any necessary static routes 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	14.80	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

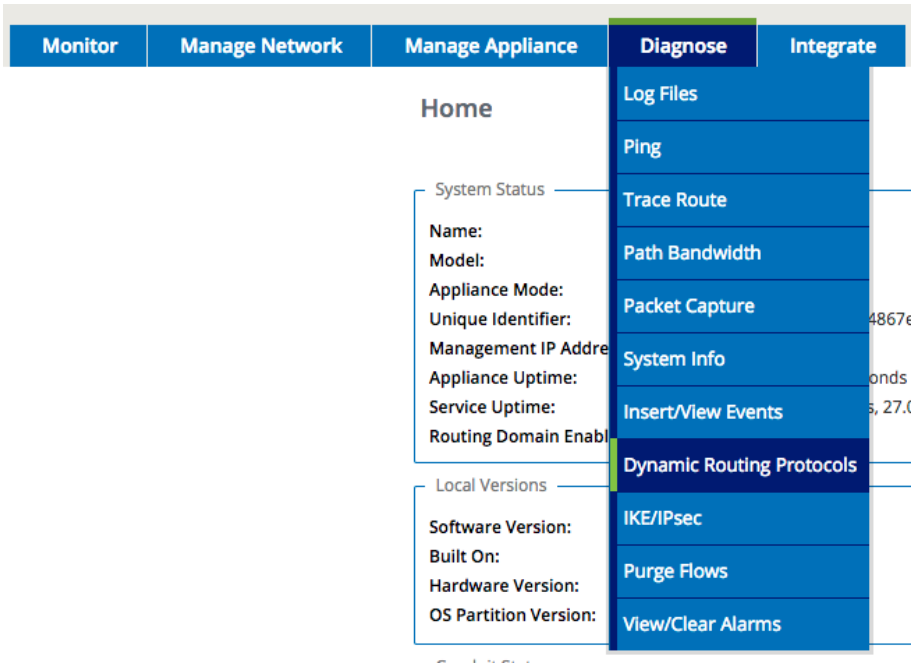
Next, use the dropdown menu to select **Routes** to verify that the expected routes are properly being learned via BGP. In the example below, notice the 10.3.1.0/24 route shows **Type** as Dynamic and **Protocol** as BGP.

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.

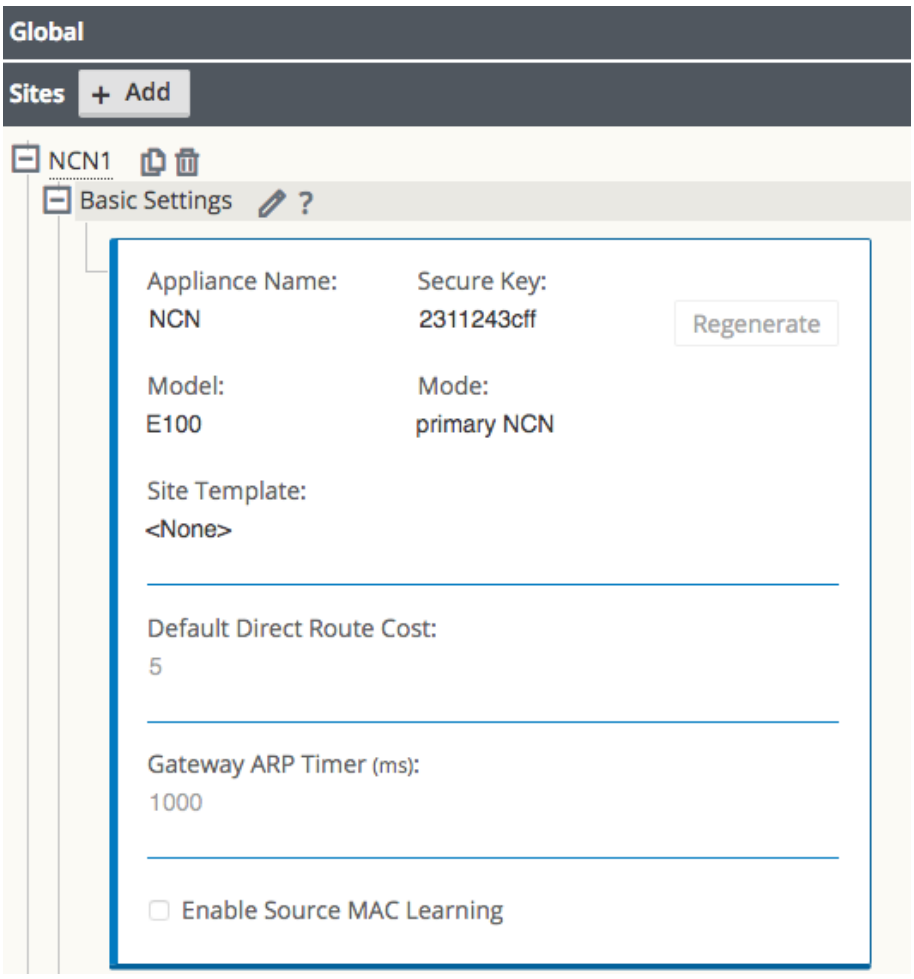
- **BGP State** - Shows an overview of the current state of each Dynamic Routing Protocol instance.
- **Show Route Table**- Provides an overview of each route prefix.
- **Show Route Table (detailed)** - Provides an overview of each route prefix and protocol-specific attributes such as Next Hop, Local 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.

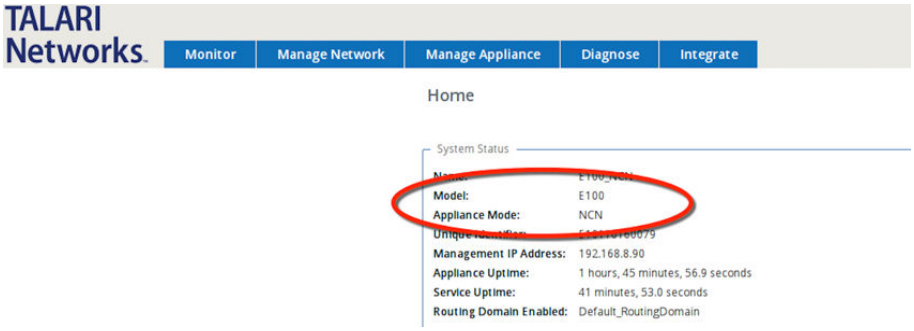
E100 as an NCN

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.



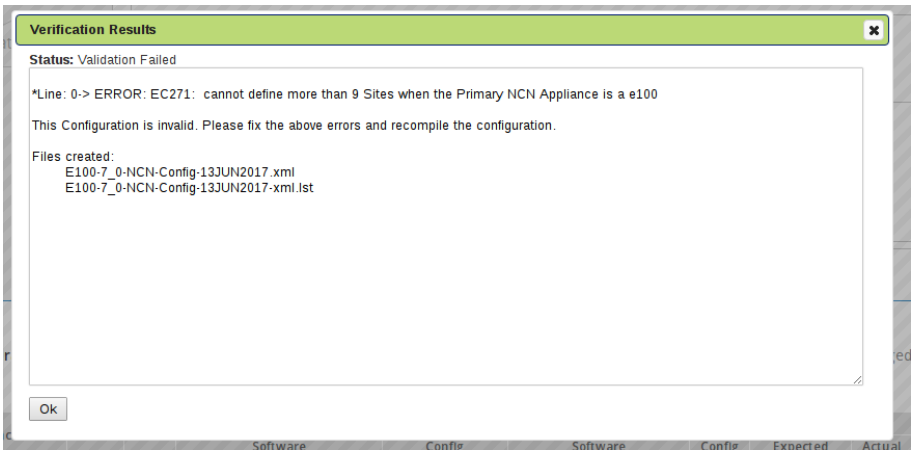
After completing the configuration, the user will **Export** it to the **Change Management inbox** of the NCN and follow the prompts to create a package for the E100 appliance.

Once you have uploaded the package to the E100, the Home Page will reflect that the E100 is functioning as the NCN Appliance.



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.



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

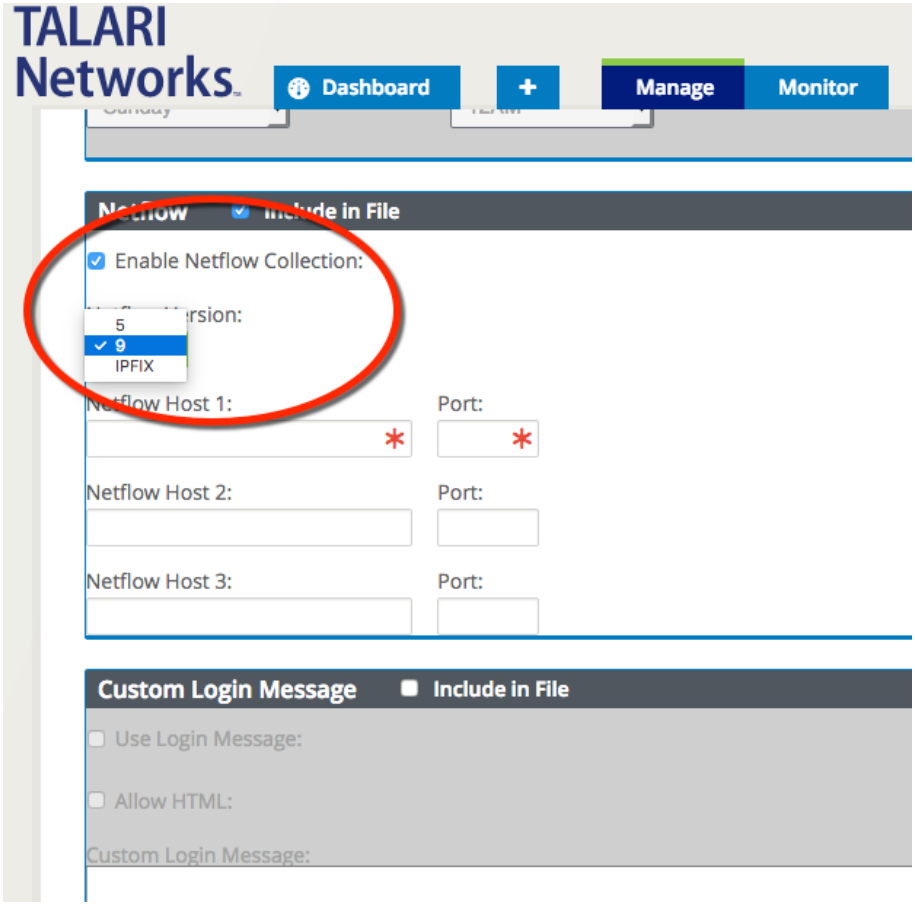
Max Public WAN Links	3	8	8	8	8	8	8	8
Max Private WAN Links	32	32	32	32	32	32	32	32
Max Routes (Static & Dynamic)	16,000	16,000	16,000	16,000	16,000	16,000	16,000	16,000
Max Recommended Routing Domains[1]	16	16	16	16	16	16	16	16

1

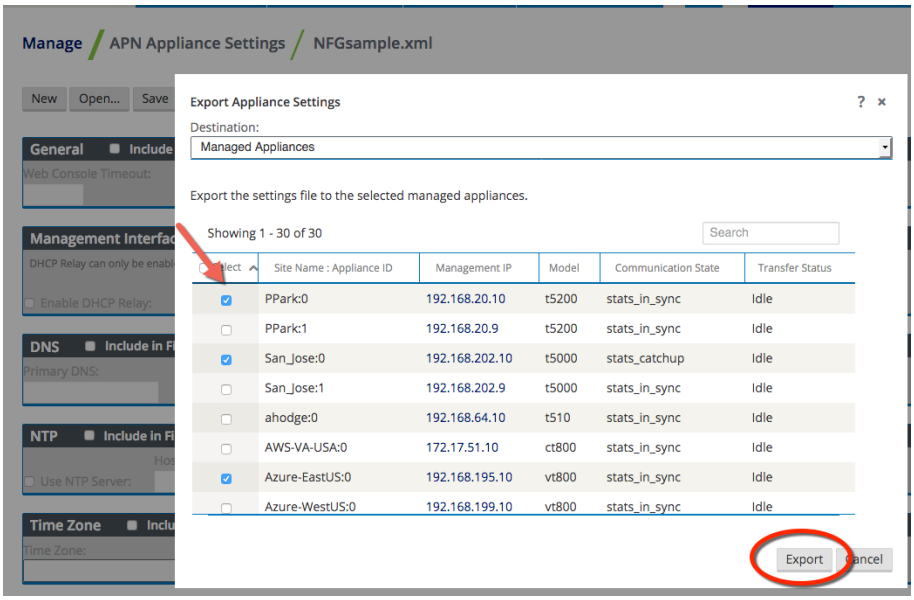
NetFlow (Support for Version 9 and IPFIX)

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.



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


Manage / APN Appliance Settings / NFGsample.xml
New
Open...
Save
General
Include
Web Console Timeout:
Management Interfac
DHCP Relay can only be enabl
Enable DHCP Relay:
DNS
Include in Fl
Primary DNS:
NTP
Include in Fl
Use NTP Server:
Time Zone
Incl
Time Zone:
Export Appliance Settings
Destination:
Managed Appliances
Export the settings file to the selected managed appliances.
Showing 1 - 30 of 30
Search
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
Export
Cancel

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

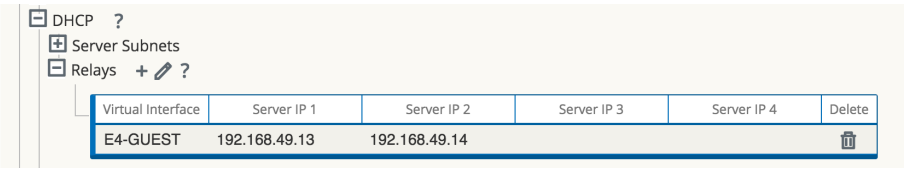
Release 4.2 Features

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.

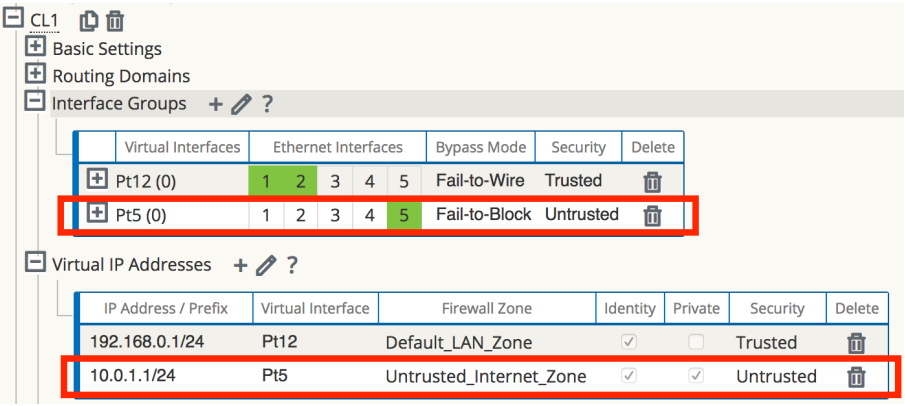
DHCP relays may be configured in the Advanced view of the Configuration Editor, under **Sites > [site name] > DHCP > Relays**, as shown below:



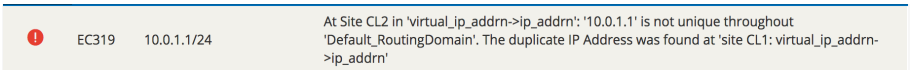
When configuring DHCP Relays, the Virtual Interface and Server IP 1 are required. Server IPs 2 through 4 are optional.

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.



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

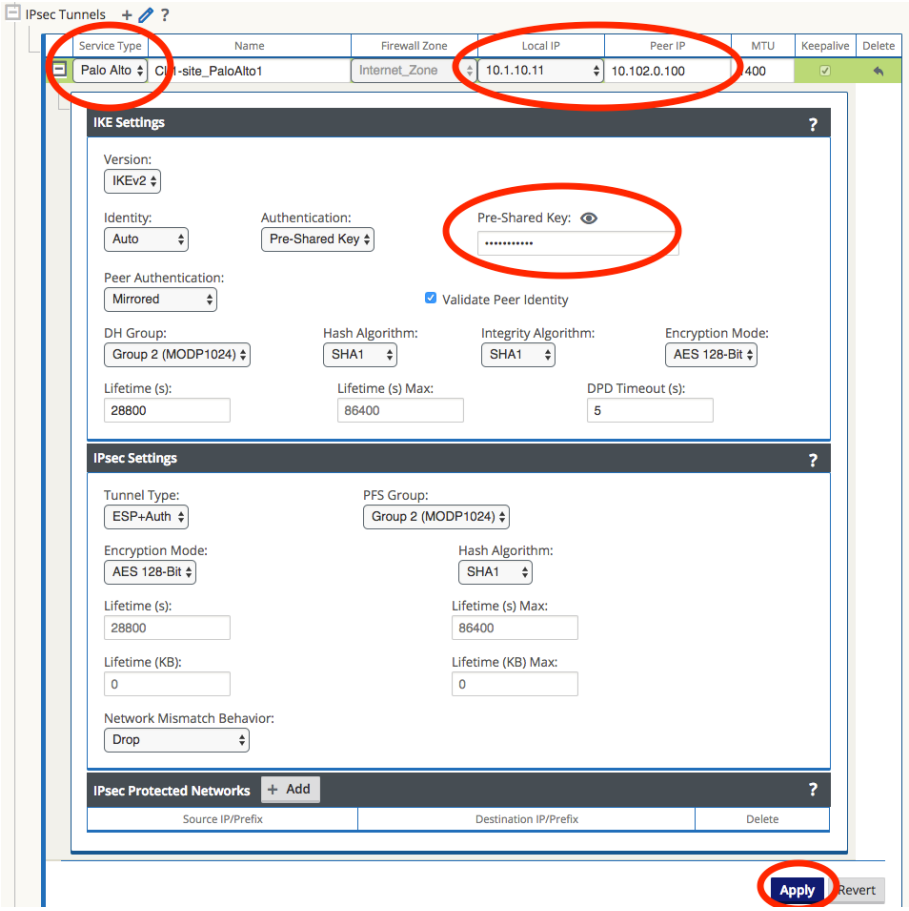


Palo Alto GlobalProtect Cloud Integration

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**.



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**.

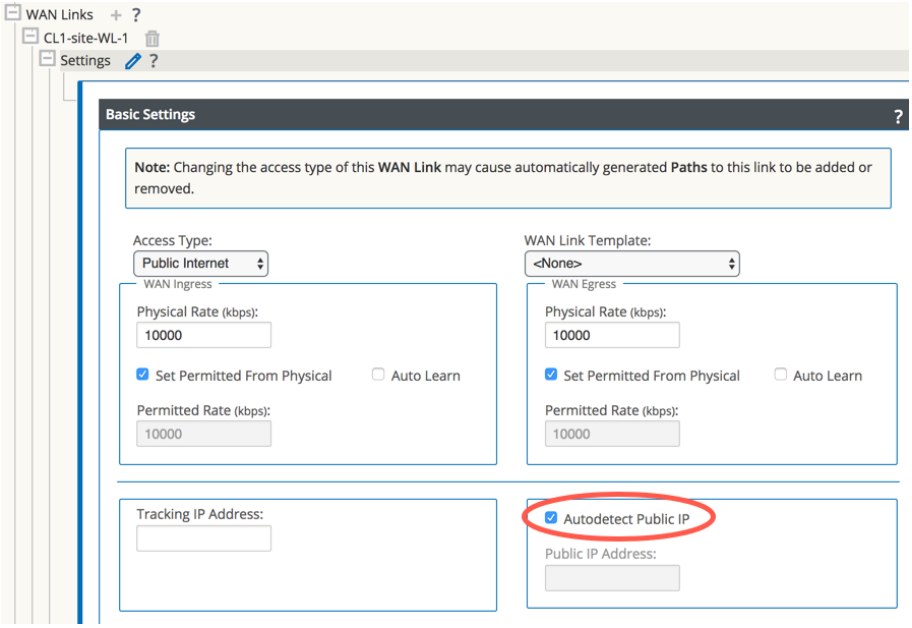
Private Cloud Path Enhancement

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

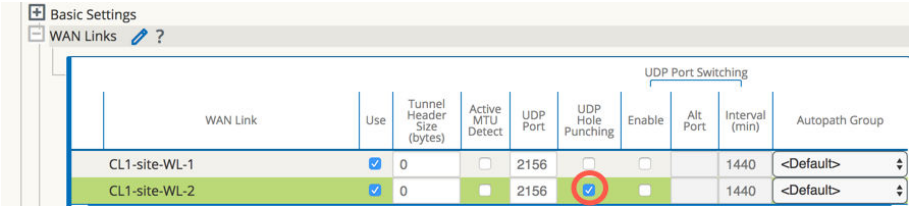
provider will have a limited number of public IP address for NATing. When Oracle is deployed for an enterprise customer, if they select one of these providers for multiple Oracle client sites, there is the possibility that multiple Oracle Client WAN links could be PATed/NATed to the same public IP address. 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:



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:



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.*

11

Release 8.0 Features

This chapter includes features and enhancements released in 8.0

ID	Issue Description
18848	Aware 8.0 introduces support for Cloud Conduits, including: • Display and filter cloud conduit type in the Monitor Conduit Report. • Add cloud conduit related events to the Monitor Event Report. • Add support to display and filter on Cloud WAN Link Usage in Monitor Graphs. • Add support to display cloud conduit usage data in Monitor WAN Links report.

12

Release 8.1 Features

This chapter includes features and enhancements released in 8.1.

Issue	Issue Description
29986230 (15145)	The special characters '/', ' \ ', and '@' are now permitted in Aware usernames.

13
Release 8.2 and later

Feature descriptions for release 8.2 and later are available in the documentation set that corresponds to each release. See the Release Notes for the release to see a description of the feature.