Oracle® SD-WAN Edge

Features Guide

Release 8.1
F26787-01
Jan 2020

ORACLE

Oracle SD-WAN Edge Features Guide, Release 8.1

F26787-01

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 x

Revision History

1 Release 2.3 Features

Geographic Redundancy 1-1
GRE Support 1-3
GRE Header Inspection Support 1-3
GRE Header Compression 1-4
Oracle Route Support 1-4
Multiple Intranet Services Defined 1-4
Route Learning via SNMP 1-5
SNMPv2 Route Polling Configuration 1-6
Include/Exclude rules 1-6
Included Routes 1-6
Excluded Routes 1-7
Intranet & Internet Enhancements 1-7
Intranet Name Support 1-7
Rule and Class Improvements 1-7
Default Classes: 1-8
Default Rules per Conduit: 1-8
WAN Link and Path Enhancements 1-13
Reserve Minimum Bandwidth for Conduit WAN Links 1-13
Configurable Congestion Control per WAN Link 1-14
Path Eligible Setting for Traffic Types 1-15
Reporting Enhancements 1-16
Availability Report 1-16
QoS Reports 1-17
Usage Report 1-17
Periodic Status Reports 1-18

Double Event Triggers 1-19
Observed Protocols 1-19
Enhanced Network Change Management 1-20
The Change Management Workflow 1-21

2 Release 2.4 Features

Network Functionality and Deployability 2-1
route_eligibility_based_on_path =Boolean 2-2
route_eligibility_to_wan_link_name =Text 2-2
L2 MAC Learning for Multiport Bridging 2-2
Design Considerations 2-3
udp_port_num =Number (2156) 2-4
udp_port_num_alt =Number (2156) 2-4
udp_port_switch_interval_minutes =Number (1440) 2-4
Network Topology 2-4
Support for Serial High Availability Appliances 2-5
Oracle Serial HA 2-6
Design Considerations: 2-7
Multiple VLAN Segment on Common WAN link 2-7
Design Considerations: 2-9
Path MTU Discovery 2-9
Design Considerations: 2-11
Usability 2-11
The Site Cloning Process 2-11
Next Steps in the Site Cloning Process 2-13
Improved Site WAN Link Provisioning 2-13
WAN Link Rates 2-14
Provisioning Groups 2-14
The Concept of Using Shares 2-15
Services 2-16
Shares of Group 2-16
Glossary 2-16

3 Release 2.5 Features

Oracle Hardware Support 3-1
Introducing the T5000 Appliance 3-1

4 Release 3.0 Features

Dynamic Conduits 4-1

Design Considerations 4-1
Dynamic Conduit Configuration 4-2
Dynamic Conduit Configuration Creation 4-3
WAN To WAN Forwarding Enhancements 4-6
Routing Enhancements 4-7
Intranet or Internet Fallback Routes 4-7
Additional Enhancements 4-7

5 Release 3.1 Features

Default Configuration Parameter Change 5-1
Oracle SD-WAN Edge Configuration Editor 5-1
Oracle SD-WAN Edge Configuration Editor and Oracle SD-WAN Edge Aware 5-2

6 Release 4.0 Features

256-Site Adaptive Private Networks 6-1
Changes to Data Storage on Oracle SD-WAN Edge Appliances 6-2
Changes to Local Route Scale 6-2

7 Release 4.1 Features

Oracle Virtual Appliance CT800 7-1
MOS Estimation 7-1
How to Configure 7-2
How to View 7-3
Security Enhancements 7-3
Summary 7-3
How to Configure 7-4
SNMP Polling for ARP Table 7-4
Appliance Settings from Aware 7-4

8 Release 4.2 Features

Non-Resetting Configuration Updates 8-1
Configuration Updates 8-1
Impact of Common Configuration Updates 8-2
Software Updates 8-3

9 Release 4.3 Features

Configure Private MPLS WAN Links 9-1

Add Private MPLS WAN LINK 9-2
Define WAN Link Basic Properties (Private MPLS) 9-3
Assign Autopath Group to Conduit-WAN Link 9-4
Verify Autopath Creation 9-4
View Permitted Rate and Congestion for WAN Links 9-5
View Permitted Rate 9-5
View Congestion 9-5
Configuration Versioning 9-7
Support for Installing User-Generated Certificates on Appliances 9-7

10 Release 4.4 Features

LAN GRE Tunnels 10-1
Monitor LAN GRE Tunnels 10-2
IPsec Encryption in Conduit 10-2
Monitoring IPsec 10-3
Path State Configurability and Monitoring 10-4
Monitor Statistics 10-5
Availability Reports 10-7
Additional Enhancements 10-9
Appliance T5200 Support 10-10
Oracle Virtual Appliance VT500 Support 10-10

11 Release 5.0 Features

Enhanced Match Criteria for Rules 11-1
Virtual Routing and Forwarding (VRF) 11-1
Monitoring 11-6
Dynamic Routing 11-8
Virtual IP Address Identity 11-8
Open Shortest Path First (OSPF) Routing Protocol 11-8
Interior Border Gateway Protocol (IBGP) 11-10
Filters 11-12
Network Objects 11-13
Monitoring 11-14
WAN Link IP Address Learning (DHCP Client) 11-14
Monitoring 11-16
IPsec VPN Termination 11-16
Monitoring 11-20
Standby WAN Links 11-21

Monitoring 11-22

12 Release 5.1 Features

Virtual Appliance VT800 12-1
Alarm System 12-1
Diagnose Alarms 12-3
Route Export Filters 12-3
Operating System Patching 12-4
Customizable Web Console 12-4
DHCP Relay and DHCP Server 12-6

13 Release 5.2 Features

Support for 550 Sites 13-1
Stateful Firewall 13-1
DHCP Relay & DHCP Server 13-1
Standby WAN Link (VSAT) 13-5
Adaptive Bandwidth Detection 13-8
Active Bandwidth Testing 13-9
SNMPv3 Polling and Trap Capability 13-11
Eligibility for IPsec Non-Conduit Routes 13-11
Additional Enhancements 13-12
    Routing Enhancements 13-12

14 Release 6.0 Features

Application Packet Filtering 14-1
Applications 14-1
Apply the Application to Firewall Policies 14-1
Apply the Application to QoS Rules 14-2
Tracking Based on Firewall Policy 14-3
Tracking Based on QoS Rule 14-3
VRF Firewall Enhancement 14-4
Easy First Install Simplified Appliance Installation 14-6
Configuration using Templates 14-7
    WAN Link Templates 14-7
    Basic Configuration Mode 14-8
    Service Chaining 14-13

15 Release 6.1 P2 Features

Site Templates 15-1
Additional Features in Edge 6.1 GA P2 15-4

16 Release 7.0 Features

WAN Optimization 16-1
Zscaler Integration 16-3
Customer Edge (CE) Router Replacement Within the APN 16-7
E100 as an NCN 16-14
Capacity Report for the E100 NCN 16-16
NetFlow (Support for Version 9 and IPFIX) 16-16
Additional Features in 7.0 GA 16-17

17 Release 7.1 Features

E1000 Hardware Options 17-1
Interactive Dashboard 17-3
WAN Optimization on Virtual Appliances 17-6
WAN Optimization Reporting Enhancements 17-7
Additional Features in 7.1 GA 17-8

18 Release 7.2 Features

User Interface Enhancements 18-1
WAN Optimization Dashboard and Reporting Enhancements 18-5
Enhanced DHCP Relay 18-10
Client Private Subnet Reuse for Untrusted Segment 18-11
Palo Alto GlobalProtect Cloud Integration 18-11
Private Cloud Path Enhancement 18-12
Additional Features in 7.2 GA 18-13

19 Release 7.2 P3 Features

Configuration Versioning and Comparison 19-1

20 Release 7.3 Features

Enhanced Application Identification 20-1
E500 Appliance (7.3 GA P3) 20-3
Private Registration Server (7.3 GA P3) 20-3

Threshold Alerting (7.3 GA P4) 20-3
Additional Features in 7.3 20-5

21 Release 8.0 Features

22 Release 8.1 Features

23 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 Edge Release Notes	Contains information about added features, resolved issues, requirements for use, and known issues in the latest Oracle SD-WAN Edge release.
Oracle SD-WAN OS Release Notes and Upgrade Guide	Contains information about inserting an OS Partition Image or OS Patch on an appliance in order to migrate to a new OS version or apply fixes to an existing version.
Oracle SD-WAN Security Guide	Contains information about security methods within the Oracle SD-WAN solution.
Oracle SD-WAN Edge Features Guide	Contains feature descriptions and procedures for all incremental releases of Oracle SD-WAN Edge. 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 2.3 Features

This chapter includes features and enhancements released in 2.3.

Geographic Redundancy

Currently, an Oracle Adaptive Private Network supports the concept of a single Network Control Node (NCN), which can be deployed in a High Available (HA) configuration. This allows for local redundancy, meaning that both appliances are deployed locally. With Edge g2.3 and the new Geographic Redundancy feature, the NCN and secondary NCN will not reside at the same location; they will reside in two separate data centers or locations. Typically, the second site would be some form of a disaster recovery facility. In the event of a primary data center failure, the backup data center should be operational and the secondary Oracle appliance would act as the NCN for Oracle SD-WAN Edge. There are a number of considerations to be aware of with this design:

- Oracle SD-WAN Edge supports a primary and secondary NCN
- HA is supported at primary and secondary NCN sites
- A secondary appliance will function as a client appliance when configured for Geographic Redundancy
- The active NCN is the clock source for the Oracle SD-WAN Edge
- The active NCN is the administration point for the Oracle SD-WAN Edge
- The active NCN will synchronize its database with the secondary NCN
- All client sites **MUST** have a conduit to the active and secondary NCNs
- Extra precautions must be taken when configuring routes
- The secondary NCN site should have static IP's for public Internet links
- If WAN-to-WAN forwarding is enabled on the Geographic Redundancy Oracle, the route cost will be the same for both NCN and Geographic Redundant NCN appliances. This can impact Oracle SD-WAN Edge routes and should be reviewed.

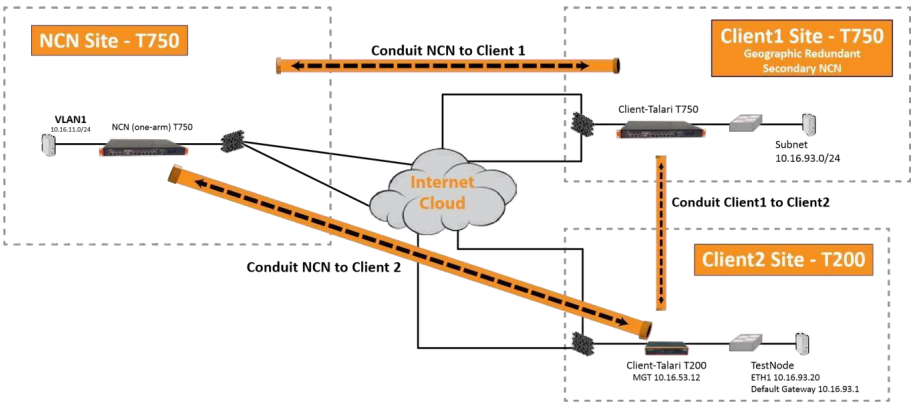


Figure 1

In Figure 1, we have the NCN site and two client sites, Client1 and Client2. Client1 is the Geographic Redundancy NCN site. As depicted in Figure 1, there must be a conduit between all client sites and the NCN site, as well as the Secondary NCN site. With this design, there are a number of recommendations:

- Design the redundant NCN site first and then design the routes
- Plan the Oracle SD-WAN Edge configuration file before deployment using the Oracle SD-WAN Edge configuration editor
- There must be enough WAN capacity for the required conduits
- Geographic NCN appliance requirements support hardware T3000 or T750 platforms only
- Be aware of the number of Oracle clients required, this will dictate NCN hardware requirements
- Be aware of failover times if local HA is deployed
- Since multiple conduits are now built from client sites, UDP hole punching may not work properly on all firewalls or NAT devices (two conduits)

The commands required to enable the Geographic Redundancy capability are provided below.

With the Geographic, Redundant NCNs, a new command was required to differentiate Oracle appliances. The new command is “appliance_mode,” and is described in detail below. The NCN primary would be configured with the following options:

```
add appli                                          model=t750
{
ance name=NCN
set appliance_properties
secure_key=0xacbf1332
enable_wan_to_wan_forwarding=yes
appliance_mode=primary_ncn;
```

The Oracle Client configuration would be configured as:

```
add applia                                         model=t750
{
nce name=Client1
set appliance_properties
secure_key=0xacbf1332
enable_wan_to_wan_forwarding=yes
appliance_mode=secondary_ncn;
```

appliance_mode = Text

Specifies the appliance's role in the Oracle SD-WAN Edge. It can be set as “primary_ncn“, “secondary_ncn,” or “client.” The Primary NCN would be set to primary, the secondary NCN would be set to secondary and a traditional client would be set to client.

GRE Support

In Oracle SD-WAN Edge release 2.3, Oracle is adding support for Generic Routing Encapsulation (GRE) header inspection and GRE header compression. GRE header inspection allows the appliance to look inside the IP GRE header and determine the protocol that resides inside the frame (inner protocol). Based on the inner protocol, Oracle APN will apply any defined rule and classify traffic accordingly. This capability simplifies the Oracle deployment within an infrastructure where IP GRE tunneling is currently in use.

GRE Header Inspection Support

Oracle SD-WAN Edge release 2.3 supports the ability to inspect IP GRE frames, and apply the corresponding rule and class based on the inner IP datagram. This support is based on RFC 2784 (Generic Routing Encapsulation). This capability eliminates the complexities of configuring external DSCP or ToS reflection for IP datagrams at the endpoint of the

IP GRE tunnel. Eliminating these complexities simplifies the Oracle's implementation process and requires user to only define the appropriate rules and classes in the configuration file. Certain WAN optimization devices also use IP GRE to encapsulate their traffic. This allows the APNA to identify certain WAN optimization flows that utilize the GRE encapsulation and classifying that traffic type. There are a few design considerations when implementing this feature:

- GRE uses IP protocol 47
- Does not support (Oracle) TCP termination
- Available on all Oracle appliances
- Supports only the inner IP datagram
- Supports GRE Header checksums

The GRE header inspection is enabled by default. The user must define the rules to map the inner protocol to a specific class. To monitor this capability the user should be aware of any IP GRE that exists in their infrastructure. The appliance will automatically identify these flows and display them in the flow table. Based on the Inner protocol, the appliance may apply any configured rule or the flow may default to an existing default rule. Figure 2 illustrates the flow page of an appliance where a GRE flow has been identified.

Figure 2 illustrates a flow that is encapsulated in a GRE tunnel. From the flow displayed, the IP Protocol (IPP) field is defined as GRE/TCP. This indicates that this is a GRE encapsulated flow and an inner IP field (protocol 1, ICMP). If the inner IP protocol was telnet, for example, the system would display GRE/TCP, and 23 would be under the destination port column. Now that the application is known, an existing rule for TCP telnet can be applied. This defined rule would classify the flow as an interactive flow, which would map to the Interactive class (Class 11).

In previous releases, the user would only see IPP 47. Any rules used to classify the traffic would require the traffic to be marked by either ToS or DSCP. The GRE header inspection now simplifies the deployment of the Oracle appliance when GRE tunneling is used within an infrastructure. This eliminates the need for marking the GRE frames based on the inner IP protocol.

GRE Header Compression

Oracle SD-WAN Edge release 2.3 provides GRE header compression support, allowing for less additional overhead per packet when the customer uses the GRE protocol through the Oracle SD-WAN Edge. When compression is enabled, the GRE header compression will reduce the GRE overhead of packets from 24 bytes per packet to 7 bytes per packet. GRE header compression is performed by default, and is supported with and without GRE checksums.

Oracle Route Support

Oracle has provided enhancements to the existing route support within the Oracle SD-WAN Edge. This has been expanded to include the following enhancements:

- Route learning via SNMPv2
- Multiple Intranet defined services and gateways
- Intranet/Internet Route Failover based on path state

Each of these new features will be described in detail below with a focus on Route learning via SNMPv2.

Multiple Intranet Services Defined

In prior releases (2.2 and prior) Oracle only supported a single defined Intranet service. This is a WAN service the APNA could be configured to use if traffic was not conduit based. The Intranet services were defined on a WAN link to be either the primary WAN link or the secondary WAN link. The new enhancement now allows a user the flexibility to configure up to 32 Intranet services.

Each service may have a primary and a secondary defined WAN link. When adding routes to the Oracle SD-WAN Edge configuration file, the user can assign a route to a defined Intranet service if multiple Intranet services exist. A single WAN link can have multiple Intranet services defined. The commands required for this capability are provided below:

Service definition would use the following commands:

```
add intranet_service name=Intranet-1

{

} add intranet_service name=Intranet-0

{

}
```

Adding the service to a specific wan link would use the following commands:

```
add net_usage      intranet_service_name=Intranet-0
                   service_type=intranet
                   wan_egress_rate_pct=10
                   wan_ingress_rate_pct=10;
```

If a route was added for the service, it would appear like the following:

```
add route     net=192.168.80.0/24
              intranet_service_name=Intranet-0
              cost=6 service=INTRANET;
```

These commands could be repeated for the individual routes and services as required.

Route Learning via SNMP

In Oracle SD-WAN Edge release 2.3, the APNA allows a user to define routers so that they can be polled for routes using SNMPv2. Once the routes have been learned by the APNA, the user can define rules which will include or exclude the routes from the

APNA route table. These routes will then be advertised or propagated to other APNAs within the Oracle SD-WAN Edge. Additional capabilities include the ability to continue polling the router for routes and, if a route is removed from the routing table of the router, propagate the topology change across the Oracle SD-WAN Edge. The polling intervals supported are “poll now,” “every 30 seconds,” “every minute,” or “every 5 minutes.” If the router that is probed is not reachable, the APNA can also be configured to purge the learned routes or maintain them. When using this capability, care must be taken when adding the routes. The user must define the routes properly to avoid any routing loop or problems. Routes included must be assigned to the correct Oracle SD-WAN Edge service; if Intranet(Internet) service is selected it must match the service defined in the configuration. This capability has the following design considerations:

- Currently only support for SNMPv2 is provided
- Probes the interface using the MIB: RFC 2096 IP Forwarding Table MIB and RFC1213-MIB
- Uses specific intervals to poll the router
- Router must support (configured) the MIB defined above (some routers do not)
- Can purge routes if router is not reachable
- Can include or exclude routes as required, excluded by default
- When defining the include/exclude rule, a user must assign a route to the correct service – local, intranet etc.
- Routes are local to each appliance, so the process is performed per appliance
- If no community string is defined, “public” is used
- Static routes learned from a polled router are displayed with the unknown interface
- Community string only supports alphanumeric characters
- Only Local routes are propagated via the Oracle SD-WAN Edge

- The polling takes place through the APNA management interface
- All straddle segments are added to the Oracle's route table by default

Log into the web console of the appliance and proceed to **Manage Network -> SNMP Route Learning**. Shown in Figure 3 are four sections to the web page: **Configuration**, **Include/Exclude Rules**, **Included Routes**, **Excluded Routes.**

SNMPv2 Route Polling Configuration

The first step is to complete the configuration section of the web page. First, define the router and community string under the configurations section of the page. The configuration section allows the user to perform the following:

- Add a router to poll
- Include the Community string
- Purge routes if the router is unreachable
- Polling time frame
- If Propagate Routes is set to YES, add routes to Oracle SD-WAN Edge route table
- Add multiple routes if required

The router that is typically added would be the LAN-side router. Subnets learned from this router would typically be local routes from a Oracle appliance perspective. The user must know which subnets are local subnets and which subnets are Intranet or Internet routes.

Include/Exclude rules

The user must then create a rule set which defines rules that would either include routes or exclude routes from the APNA route table. Once the rule is defined the user would hit the apply button to filter the corresponding routes and add them to the include route table. These routes could then be propagated to the Oracle SD-WAN Edge routing table, if desired. To propagate the routes, the user would have to have the option “Propagated routes” option set to “yes”. Defining include routes requires knowledge of the network infrastructure. Any route included must be assigned to the correct service for proper Oracle SD-WAN Edge routing.

When adding routes to include in the Oracle SD-WAN Edge routing table, there is significance to the order of the defined rule. The rules are processed in a top-down method. With that in mind, the user must be aware of the defined rules for including/ excluding routes. The preferred procedure would be to have more general rules defined first with more specific rules defined later in the rules list.

Included Routes

The Included Routes section displays the included routes. These are routes that will be propagated across the Oracle SD-WAN Edge from the local appliance. The local appliance will propagate these routes to all other appliances with which it maintains a conduit. These routes are then reachable from the conduit.

Excluded Routes

Excluded Routes are routes not included in the Oracle SD-WAN Edge route table, and are not propagated to other APNAs. By default, all routes learned from SNMP are Excluded Routes. The user must define Include Rules to add any Learned Route to the Oracle SD-WAN Edge route table.

Intranet & Internet Enhancements

Intranet/Internet Route Failover Based on Path State

In previous releases when there was a WAN link failure of the Intranet service, the appliance would forward traffic based on the WAN link defined for the Intranet service. There was no searching through the route table to determine if there was an alternate route to reach the destination. In release 2.3, an added enhancement now allows the appliance to continue searching through the Oracle SD-WAN Edge route table for a second route in the event of a WAN link failure.

For example, if there are two WAN links, WAN Link A and WAN link B, WAN link A is the MPLS circuit/WAN link while WAN link B is the Internet circuit. If the Intranet service is defined for WAN link A and that router becomes unreachable, the appliance will now continue searching the Oracle SD-WAN Edge route table for an alternative route when there is a new flow. If the user defined a second route to be a conduit route, the flow could traverse the conduit in the event of an Intranet WAN link failure. This provides a backup route in the event of a WAN link failure.

Intranet Name Support

In Oracle SD-WAN Edge release 2.2 and prior there is the concept of a single Intranet service. This single service was defined and all Intranet routes used this defined WAN link and gateway. There was also the ability to have a primary and secondary WAN link defined for the Intranet service. In Edge 2.3 the number of Intranet services has been increased to 32, allowing a user to define up to 32 separate Intranet services. The user would define separate services in the case where they had multiple MPLS routers each supporting specific subnets. The user could then define the separate Intranet service and point a specific route/subnet to the corresponding service. This allows a much more flexible solution when supporting Intranet traffic.

Rule and Class Improvements

In Oracle SD-WAN Edge release 2.2 and prior releases, the typical Oracle configuration file supported the concept of a single default class. This default class was designed to support all different traffic flows without a specific advantage to a certain traffic type – Real-time verses Interactive Verses Bulk, for example. Any traffic type that did not have a user defined rule would match the default class 9. The default rules have now been enhanced to support different rules and classes for the most common traffic flows seen on networks today. Before a user implements the Oracle SD-WAN Edge, they must review the current rule set to understand what is enabled by default. The rules and classes are not all encompassing, but do cover a wide range of

application and traffic flows. If the user has a custom application that is critical to the success of the deployment, they should define the application characteristics to a Oracle representative. The representative can then discuss the options with the user to define the correct rule set (class) for the customer application.

Shown below are the new default rules and classes as of Edge release 2.3:

Default Classes:

Class 0-9:

- User settable class
- Default: Bulk class
- Default: 1% share

Class 10 (*udp_ef_realtime_class*):

- Default class for user-defined UDP rules
- Realtime class
- 50% share

Class 11 (*control_tcp_ack_af11_int_class*):

- Default class for TCP Standalone ACK traffic.
- Interactive class
- 50% share

Class 12 (*ssh_telnet_interactive_class*):

- Interactive class
- 30% share

Class 13 (*gre_tcp_other_interactive_class*):

- Interactive class
- 20% share

Class 14 (*http_https_interactive_class*):

- Interactive class
- 10% share

Class 15 (*cifs_bulk_class*):

- Bulk class
- 45% share

Class 16 (*ftp_bulk_class*):

- Bulk class 45% share

Default Rules per Conduit:

- ICMP

(*Assigned to class 11*)

1. protocol_str=ICMP
2. class_name=control_tcp_ack_af11_int_class
3. transmit_mode=PERSISTENT_PATH
4. resequence_packets=YES
5. resequence_holdtime_ms=set rule_default
6. nontcp_resequence_holdtime_ms
7. class_tail_drop_small_packet_ms=350
8. class_tail_drop_small_packet_bytes=30000

- SSH

(*Assigned to class 12*)

1. protocol_str=SSH
2. class_name=ssh_telnet_interactive_class
3. transmit_mode=LOAD_BALANCE_PATHS
4. retransmit_lost_packets=YES
5. resequence_packets=YES
6. resequence_holdtime_ms=set rule_default tcp_resequence_holdtime_ms
7. class_tail_drop_small_packet_ms=350
8. class_tail_drop_small_packet_bytes=65000
9. reassign_flow_if_packet_exceeds_size_bytes=512 // for SCP
10. reassign_flow_if_packet_exceeds_size_class_name=ftp_bulk_class // for SCP
11. reassign_class_tail_drop_small_packet_bytes=(*~1/2 second based on WAN ingress bandwidth for the conduit*)

- Telnet

(*Assigned to class 12*)

1. protocol_str=TELNET
2. class_name=ssh_telnet_interactive_class
3. transmit_mode=LOAD_BALANCE_PATHS
4. retransmit_lost_packets=YES
5. resequence_packets=YES
6. resequence_holdtime_ms=set rule_default tcp_resequence_holdtime_ms
7. class_tail_drop_small_packet_ms=350
8. class_tail_drop_small_packet_bytes=65000

- HTTP

(*Assigned to class 14*)

1. protocol_str=HTTP
2. class_name=http_https_interactive_class
3. transmit_mode=LOAD_BALANCE_PATHS

4. retransmit_lost_packets=YES
5. resequence_packets=YES
6. resequence_holdtime_ms=set rule_default tcp_resequence_holdtime_ms
7. class_tail_drop_small_packet_ms=350
8. class_tail_drop_small_packet_bytes=100000

- HTTPS

(*Assigned to class 14*)

1. protocol_str=HTTPS
2. class_name=http_https_interactive_class
3. transmit_mode=LOAD_BALANCE_PATHS
4. retransmit_lost_packets=YES
5. resequence_packets=YES
6. resequence_holdtime_ms=set rule_default tcp_resequence_holdtime_ms
7. class_tail_drop_small_packet_ms=350
8. class_tail_drop_small_packet_bytes=100000

- CIFS

(*Assigned to class 15*)

1. protocol_str=CIFS
2. class_name=cifs_bulk_class
3. tcp_standalone_ack_class_name=control_tcp_ack_af11_int_class
4. tcp_standalone_ack_class_tail_drop_small_packet_ms=350
5. tcp_standalone_ack_class_tail_drop_small_packet_bytes=30000
6. transmit_mode=LOAD_BALANCE_PATHS
7. retransmit_lost_packets=YES
8. resequence_packets=YES
9. resequence_holdtime_ms=set rule_default tcp_resequence_holdtime_ms
10. class_tail_drop_small_packet_bytes=(*~2 seconds based on WAN ingress bandwidth for the conduit*)

- FTP

(*Assigned to class 16*)

1. protocol_str=FTP
2. class_name=ftp_bulk_class
3. tcp_standalone_ack_class_name=control_tcp_ack_af11_int_class
4. tcp_standalone_ack_class_tail_drop_small_packet_ms=350
5. tcp_standalone_ack_class_tail_drop_small_packet_bytes=30000
6. transmit_mode=LOAD_BALANCE_PATHS
7. retransmit_lost_packets=YES

8. resequence_packets=YES
9. resequence_holdtime_ms=set rule_default tcp_resequence_holdtime_ms
10. class_tail_drop_small_packet_bytes=(*~2 seconds based on WAN ingress bandwidth for the conduit*)

- GRE_EF

(*Assigned to class 10*)

1. protocol_str=GRE
2. dscp_tag=ef
3. class_name= udp_ef_realtime_class
4. gre_header_compression_enabled=YES
5. transmit_mode=LOAD_BALANCE_PATHS
6. retransmit_lost_packets=YES
7. resequence_packets=YES
8. resequence_holdtime_ms=set rule_default nontcp_resequence_holdtime_ms
9. class_tail_drop_small_packet_ms=100
10. class_tail_drop_small_packet_bytes=15000

- GRE_AF11

(*Assigned to class 11*)

1. protocol_str=GRE
2. dscp_tag=af11
3. class_name=control_tcp_ack_af11_int_class
4. gre_header_compression_enabled=YES
5. transmit_mode=LOAD_BALANCE_PATHS
6. retransmit_lost_packets=YES
7. resequence_packets=YES
8. resequence_holdtime_ms=set rule_default nontcp_resequence_holdtime_ms
9. class_tail_drop_small_packet_ms=350
10. class_tail_drop_small_packet_bytes=65000

- GRE

(*Assigned to class 13)*

1. protocol_str=GRE
2. class_name=gre_tcp_other_interactive_class
3. gre_header_compression_enabled=YES
4. transmit_mode=LOAD_BALANCE_PATHS
5. retransmit_lost_packets=YES
6. resequence_packets=YES
7. resequence_holdtime_ms=set rule_default nontcp_resequence_holdtime_ms

8. class_tail_drop_small_packet_ms=350
9. class_tail_drop_small_packet_bytes=200000
    - EF

(*Assigned to class 10*)

1. protocol_str=*
2. dscp_tag=ef
3. class_name=udp_ef_realtime_class
4. transmit_mode=DUPLICATE_PATHS
5. resequence_packets=YES
6. resequence_holdtime_ms=set rule_default nontcp_resequence_holdtime_ms
7. class_tail_drop_small_packet_ms=100
8. class_tail_drop_small_packet_bytes=15000
    - AF11

(*Assigned to class 11*)

1. protocol_str=*
2. dscp_tag=af11
3. class_name=control_tcp_ack_af11_int_class
4. transmit_mode=PERSISTENT_PATH
5. resequence_packets=YES
6. resequence_holdtime_ms=set rule_default nontcp_resequence_holdtime_ms
7. class_tail_drop_small_packet_ms=350
8. class_tail_drop_small_packet_bytes=30000
    - UDP

(*Assigned to class 10*)

1. protocol_str=UDP
2. class_name=udp_ef_realtime_class
3. transmit_mode=PERSISTENT_PATH
4. resequence_packets=YES
5. resequence_holdtime_ms=set rule_default nontcp_resequence_holdtime_ms
6. class_tail_drop_small_packet_ms=100
7. class_tail_drop_small_packet_bytes=15000
    - TCP

(*Assigned to class 13)*

1. protocol_str=TCP
2. class_name=gre_tcp_other_interactive_class
3. tcp_standalone_ack_class_name=control_tcp_ack_af11_int_class

4. tcp_standalone_ack_class_tail_drop_small_packet_ms=350
5. tcp_standalone_ack_class_tail_drop_small_packet_bytes=30000
6. transmit_mode=LOAD_BALANCE_PATHS
7. retransmit_lost_packets=YES
8. resequence_packets=YES
9. resequence_holdtime_ms=set rule_default tcp_resequence_holdtime_ms
10. class_tail_drop_small_packet_ms=350
11. class_tail_drop_small_packet_bytes=300000
    - Other

(*Assigned to class 13*)

1. protocol_str=*
2. class_name=gre_tcp_other_interactive_class
3. transmit_mode=PERSISTENT_PATH
4. resequence_packets=NO
5. class_tail_drop_small_packet_ms=350
6. class_tail_drop_small_packet_bytes=200000

When the upgrade is performed, the Oracle SD-WAN Edge editor and compiler will automatically assign a percentage of the available bandwidth to each class. This will eliminate any potential issues when upgrading if there are many rules defined in an existing configuration file.

WAN Link and Path Enhancements

In Oracle SD-WAN Edge release 2.3, WAN link enhancements include a number of configurable options that were classified as “debug options” in previous releases, and were used at a number of customer installations. These options are now easily accessible by all customers, and include reserving minimum bandwidth for a conduit link, and congestion control per WAN link. These options may be configured in the Oracle SD-WAN Edge configuration editor, or as specific configuration options. These will be defined in more detail below.

Reserve Minimum Bandwidth for Conduit WAN Links

Certain network conditions cause congestion on a defined WAN link or path. When this congestion occurs, the appliance would reduce the amount of conduit data being forwarded on that WAN link. The appliance would reduce the usage rate down to its lowest defined rate (in certain cases) which was 80 kbps. When this occurred, there could be a performance impact to user data that was inside the conduit. For instance, 80 kbps would typically not even support a typical VoIP phone call. This unforeseen state could be caused by some external WAN-facing router that is oversubscribed with no configuration options of guarantying the appliance its defined usable rate. To overcome this issue, Oracle SD-WAN Edge release 2.3 allows the user to define a WAN link minimum rate - which is the lowest usage rate a WAN link will use during times of congestion. This will guarantee the appliance will continue to send no less than this defined value on the WAN link.

There are a number of design considerations to be aware of for this capability:

- Can be applied to a specific conduit on a WAN link only
- Must consider defined usage rates
- If congestion is consistent, the user should resolve the congestion issue on the router or firewall

An example of defining this minimum usage rate:

```
add virtual_wan_link name=Client-1-Link2

{

set properties

                virtual_interface_name=CL1VL11
                virtual_ip_addr=10.1.20.12
                gw_ip_addr=10.1.20.5
                wan_ingress_physical_rate_kbps=3000
                wan_egress_physical_rate_kbps=3000
                wan_ingress_permitted_rate_kbps=3000
                wan_egress_permitted_rate_kbps=3000
                enable_public_ip_learning=true
                tracking_ip_addr=10.1.20.15; add conduit_usage
                remote_site_name=NCN-Site
                wan_egress_rate_pct=100.0
                wan_ingress_rate_pct=100.0
}               minimum_reserved_bandwidth_kbps=400;
```

minimum_reserved_bandwidth_kbps = Number (80

The minimum amount of bandwidth that this usage will be reduced to during on demand scheduling. The default value for conduit links in shown above.

As we can see from the above configuration example, this option is applied under the WAN link and conduit usage. Once the specific WAN link is defined, the user can proceed to the conduit usage section where the minimum bandwidth option can be defined.

Configurable Congestion Control per WAN Link

The congestion threshold defines the period of time the appliance determines the WAN link is congested – if there is congestion for the defined period, it will then proceed into a congestion avoidance state. This is accomplished by reducing the amount of data sent on a WAN link. Sending less conduit data on a WAN link should result in the probability of the congested state clearing itself. The default value for this configuration option is 20 ms. (20000- value – default).

If the user chooses to change this value, it is recommended they contact a Oracle representative for specific values to use. If they decide to change the value to avoid the appliance from acting on a congestion state, the user would increase the value for example, if the value is increased to 2000000 – this would instruct the appliance that congestion must occur for a period of 2 seconds before the congestion avoidance algorithm is invoked. In traditional networks, 2 seconds of congestion would not

happen. Since congestion is not detected the congestion avoidance algorithm is not enabled and the appliance continues sending data up to the defined usable rate.

```
add virtual_wan_link name=Client-1-Link2

{

set properties

virtual_interface_name=CL1VL11

virtual_ip_addr=10.1.20.12

gw_ip_addr=10.1.20.5

wan_ingress_physical_rate_kbps=3000

wan_egress_physical_rate_kbps=3000

wan_ingress_permitted_rate_kbps=3000

wan_egress_permitted_rate_kbps=3000

enable_public_ip_learning=true

congestion_threshold_us_per_s_us=200000
tracking_ip_addr=10.1.20.15; .

.

.

}
```

With the congestion avoidance algorithm disabled, the Oracle will send data up to the configured usage rate. There could be a negative impact to other data flows within the network infrastructure depending on bandwidth allocation. The Oracle assumes that the defined usage rate is a guaranteed rate and attempts to send data at that defined rate as required. Users must consider this when using this new parameter.

Path Eligible Setting for Traffic Types

The Path Eligible/Ineligible options allow users to specify a certain traffic class to be eligible or ineligible for a specific WAN link. By default, all WAN links are eligible for all traffic classes. When a WAN link is ineligible for a traffic class internally, the appliance will add 150 ms latency to the defined WAN link. Depending on the WAN links in the configuration, this may only reduce the use of that WAN link under normal conditions. When traffic is queued up, the WAN link could be used by the appliance for the ineligible class if circumstances dictate.

The configuration parameters are shown below:

```
set properties

virtual_interface_name=CL4VL44

virtual_ip_addr=10.4.50.12

gw_ip_addr=10.4.50.5

wan_ingress_physical_rate_kbps=10000
```

```
wan_egress_physical_rate_kbps=10000

wan_ingress_permitted_rate_kbps=10000
wan_egress_permitted_rate_kbps=10000
wan_ingress_realtime_eligible=true
wan_ingress_interactive_eligible=true
wan_egress_realtime_eligible=true
wan_egress_interactive_eligible=true
wan_ingress_bulk_eligible=true

wan_egress_bulk_eligible=true;
```

This configuration example displays the default option. When reviewing a standard configuration with all paths eligible, these options will not appear in the configuration file.

They are displayed above so the user can understand what commands to use for these options. To verify the settings, the user can use the Oracle SD-WAN Edge QoS reports to view and verify that a specific WAN link is limiting a traffic class from that WAN link. Users should consult a Oracle representative if they believe they need this feature enabled for a specific WAN link.

Reporting Enhancements

Oracle SD-WAN Edge release 2.3 now has additional reports that assist the user in understanding the availability of the Oracle SD-WAN Edge and quantifying the value of the Oracle SD-WAN Edge. These new reports provide data on Oracle SD-WAN Edge availability, QoS usage, periodic network status, and a method to reduce outdated information using double triggers for event notification. The following table correlates the old reports with the new reports in 2.3.

Edge Release 2.2 Reports	Edge Release 2.3 Reports
Reports	Performance Reports
Appliance Graphs	Appliance Reports
n/a	QoS Reports
n/a	Usage Reports
n/a	Availability Reports
n/a	Periodic Status Reports

Table 2

Availability Report

The Network availability report provides comprehensive data regarding uptime, goodtime, badtime, downtime and incidents per WAN link, conduit, and path. This data is available on a per site basis at the NCN and at any of the client sites. The client site report is based on that client's conduits and WAN links. Here is an example of a client site report:

The definition of availability report terms follows:

Term	Definition
Oracle SD-WAN Edge Object	A path, conduit or WAN Link.
Incidents	A counter for the number of periods of downtime.
Goodtime	The total amount of time that an object has been in a good state.
Badtime	The total amount of time that an object has been in a bad state.
Uptime	The total amount of time that an object has been in a state that is greater than dead.
Downtime	The total amount of time that an object has been in a dead state.

Table 3

The report displays up to 24 hours of data by default. Other display options are available including, 1 hour, 24 hours, 7 days, or “All Available Data.” To access this report, login into the web console and select **Monitor –> Availability Reports** from the pull-down menu.

QoS Reports

In prior release of Edge, the user did not have insight into the application classes that traverse a specific conduit, WAN link or path. There were only generic counters that could be used which displayed traffic on a per class basis. This data was provided as counters for total traffic only. In the Edge release 2.3, the appliance now provides class statistics based one of the following options: WAN link, Conduit, Path, and Site.

The Report will look like the following:

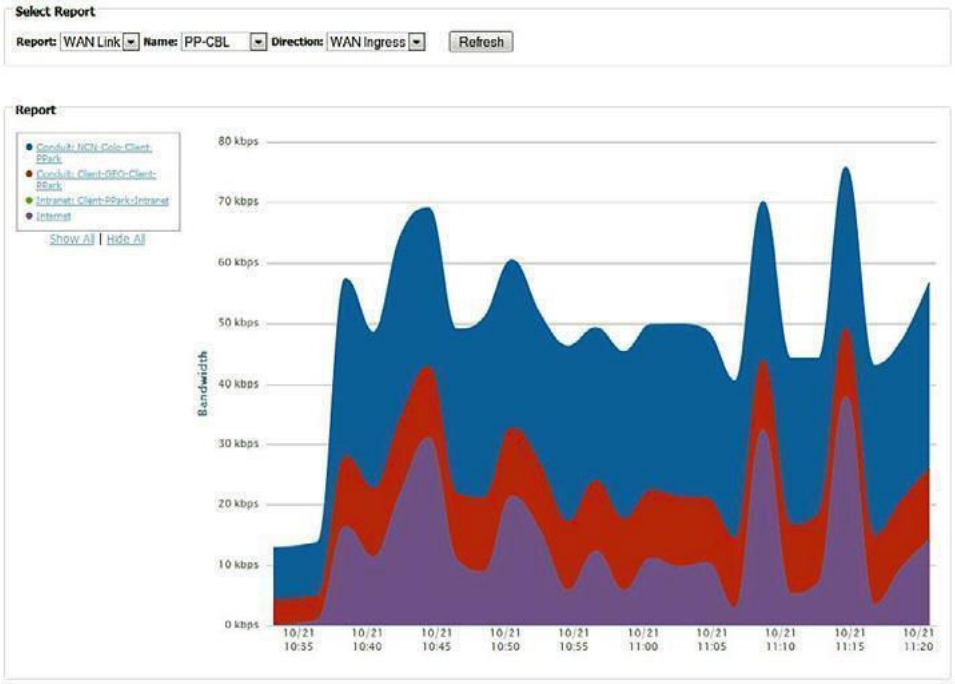
From the above screen capture we can see the different classes of traffic on the path

“PPCBL→Colo-L3. From the screen capture we can see the applications classified as Realtime (blue), Interactive (green) and Bulk (red). Traditionally, Realtime is VoIP or time sensitive traffic, Interactive is http/https/telnet and Bulk is any type of file transfer application (ftp). From this report the user can determine which traffic class was using what portion of the bandwidth on a conduit or WAN link. To view this report log in into the web console of the appliance and proceed to **Monitor -> QoS Reports**. Insight into this type of data allows the network administrator to plan accordingly for WAN link and bandwidth usage, and potential WAN link expansion.

Usage Report

The Oracle SD-WAN Edge Usage report allows the user to display usage for services that include Conduit, Intranet, and Internet. By default, this report displays all conduit and services information in a stacked fashion. The user can then disable conduit statistics from being displayed and only view Intranet and Internet traffic, if desired. This data can be displayed for a site or a WAN link, ingress direction or egress direction. To view this report login into the web console and proceed to **Monitor ->**

Usage Reports. The default graph for the Oracle SD-WAN Edge Usage report is shown below.



This screen capture is displaying usage for a specific WAN link (PP-CBL) in Oracle ingress direction (LAN to WAN). The different colors represent the conduits, as well as Internet and Intranet services provisioned on the PP-CBL WAN link. The user also has multiple options on time frame for data that is to be displayed, as well as the ability to display any available archived database. To view this report login into the web console of the appliance and proceed to **Monitor -> Usage Reports**

Periodic Status Reports

The Periodic Status reports are provided to the user automatically, once configured. These reports provide details regarding the status of the underlying network. The underlying network is considered to be the wide area network – MPLS cloud or ISP (internet) cloud, as seen from a Oracle appliance perspective. By default, the status report is not sent. To configure these reports, the user would login to the web console and proceed to **Integrate -> Periodic Status Reports** page. Configurable options include: details can be turned off or on for each individual Site, WAN link, Conduit, Path, Internet service, and intranet service.

To simplify the configuration process, the “Select All” option may be used, or just select individual items as appropriate. Once defined, the user can preview the report before the actual update is emailed. The email can be sent based on the user defined time criteria

(every day, specific days) as well as defining a specific time of day. There is also a “Send Now” option that can be used to test the capability. For this to work properly, the user must have the “Email Alerts” defined properly in the web console **Integrate**, and then **Configure Events and Alerts** section of the web console.

Once emailed, the report would look like Figure 7 below (depending on properties selected).

Double Event Triggers

In previous releases, the appliance would send a notification immediately after an event occurred under any circumstances. To enhance this capability and reduce the number of event notifications that users receive, a double event trigger capability has now been added to the appliance. This allows certain event emails to only be sent when they persist over a user-defined period of time. For example, a conduit is dead - and is dead for a certain period of time. Once the pre-defined time limit is reached and the conduit is still dead, the event notification would be sent to the defined email address. This will reduce the number of emails sent when a conduit goes down and comes back up immediately. Typically, path state change events generate more state changes which result in more email notifications. The double event trigger capability reduces the number of notifications dramatically while still allowing the user the ability to monitor any path state changes. This capability is disabled by default. The user has the following options when configuring this capability:

Supports Event Types: Timeframe in seconds:

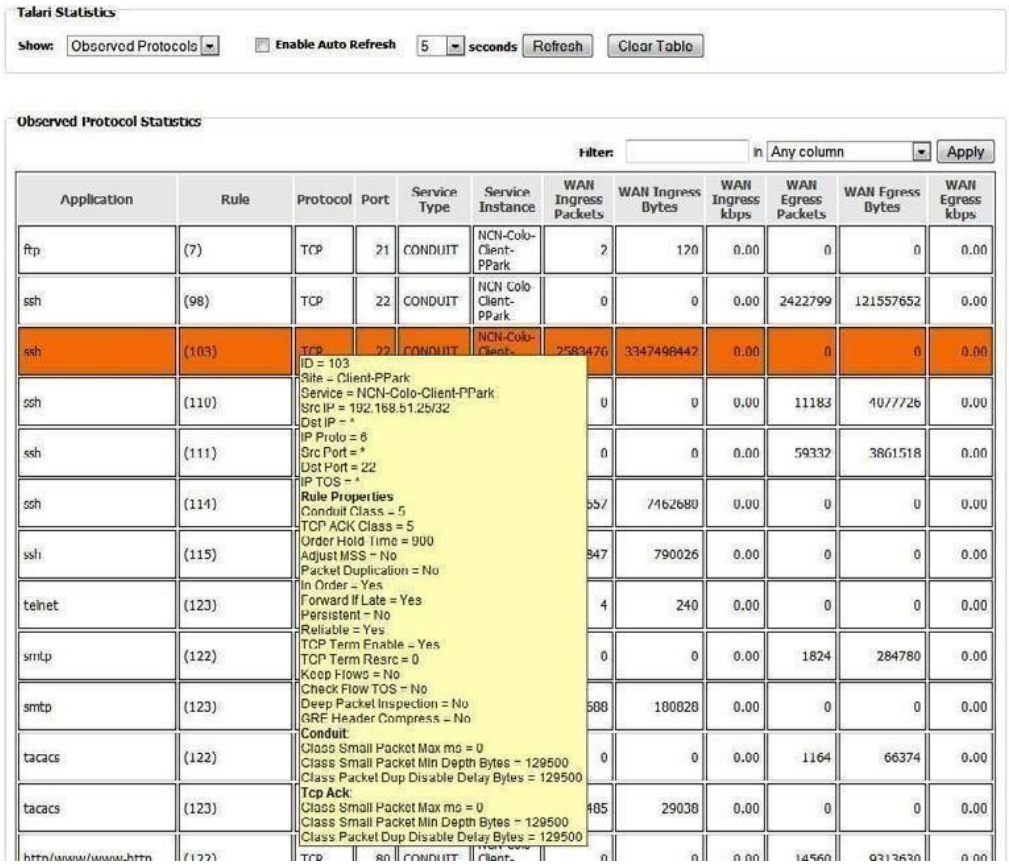
SERVICE	2
CONDUIT	5
WANLINK	10
PATH	30
	60

To configure this capability, log in to the web console of the appliance and proceed to

Integrate -> Configure Events and Alerts. Scroll down to the “General Event Configuration” section and look for the section labeled “Alert if State Persists.” By default, the user will see the behavior set to “Alert Immediately”, this pull-down supports the timeframe options shown above. Once all options are configured select the “Apply Settings” to complete any changes.

Observed Protocols

In Oracle SD-WAN Edge release 2.3, Oracle now provides users with a list of protocols that are traversing the Oracle appliance. The protocols are displayed to assist the user in verifying the correct rule set is applied, as well as learn what protocols may not be IANA-based protocols that reside within their infrastructure. The following screen shot illustrates this data within the Oracle appliance.

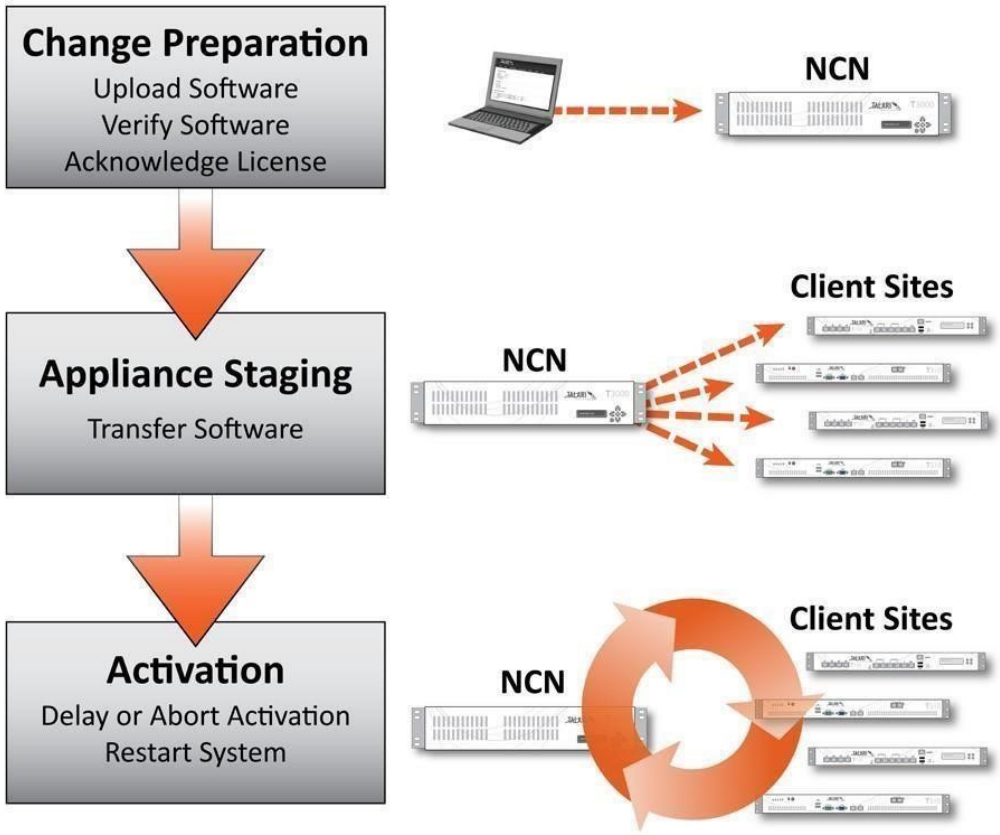


To view the observed protocols within the web console of the appliance, log in and proceed to **Monitor-> Statistics**. From the pull-down list "**Show**" select the "Observed Protocols" option. Depending on the data flow through the Oracle, the table may take a few second to populate. The table will display known and unknown protocols. This data displayed will provide which rule the flow is matching on, as well as other data regarding the flow.

Enhanced Network Change Management

The enhanced network change management process allows a user to upload a new file package to the Oracle SD-WAN Edge. This new package can be a software update, or a configuration update, or both. The three-step workflow is a set of checks and processes that ensure that configuration changes and software updates are applied to the network in a reliable, fail-safe way. Go to **Manage Network -> Change Management** to access this utility.

The Change Management Workflow



In addition to using change management for network software distribution and activation, a twostep local change management utility has been introduced as well, allowing for an easier and more intuitive process for updating software and configuration files on individual appliances. Local change management is located at the **Manage Appliance -> Local Change Management** page.

2

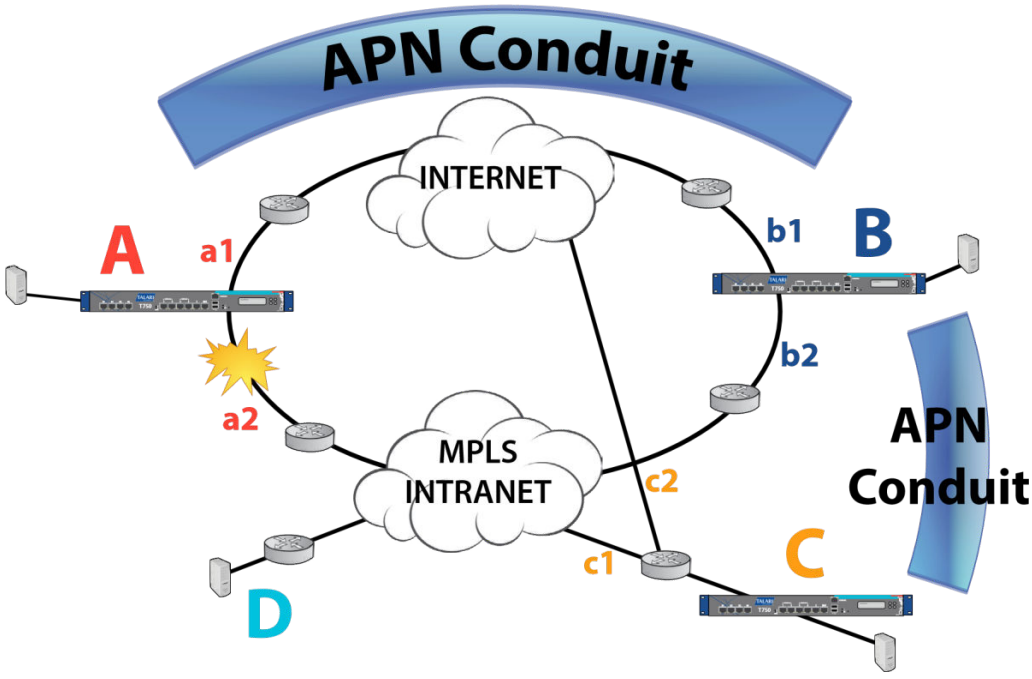
Release 2.4 Features

This chapter includes features and enhancements released in 2.4.

Network Functionality and Deployability

Intranet Route Eligibility Determined by Path State

A new feature has been added in Oracle SD-WAN Edge Release 2.4 to determine Intranet route eligibility by path state as opposed to WAN link state. In the past, a route was ineligible if the WAN link was down, but there were cases where the WAN link was only down at one site. This caused the Intranet data to not flow between sites. To resolve this issue the Oracle appliance now can make a path eligible/ineligible decision based on path state and not just WAN link state. The "**Route Eligible Path**" is a path whose status is used to determine whether a route is eligible to be used when making routing decisions.



As shown in Figure 1 above, there are four sites in a sample prior release network. There is a conduit from A to B and a conduit from B to C. WAN links a2 and b2 are also configured with intranet service. When a2 fails, all paths using a2 are dead, so a2 is in WAN link DEAD state. Intranet traffic going from site A to site B will then skip the intranet route and use the available conduit route. At site B, since b2 is used for a path for the B-C conduit, it remains in a GOOD state. Intranet traffic from site B to site A will continue to use the intranet route that enters the network on the b2 link and exits the network on the a2 link. This traffic will fail to reach the destination since a2 is down.

To solve this problem, this new feature allows a user to add an eligible path to the intranet route. When doing a route lookup, the intranet route is now skipped if the eligible path is DEAD.

One Route Eligible Path can be configured for each dynamic and/or user-configured static intranet route but there is no limit on the number of intranet routes that can be configured to use a Route Eligible Path. The configuration editor allows a path to be configured as a Route Eligible Path for user's static intranet routes. Adding, deleting, or changing the Route Eligible Path on an intranet route does not require a reset of the

Oracle SD-WAN Edge (please see Figure 2). For more information on the Oracle SD-WAN Edge Configuration Editor, please see the Oracle SD-WAN Edge Configuration Editor User's Guide.

Route Eligible Path can also be set by editing the configuration file itself. The command line options would include the following:

```
add route

net=10.0.0.0/8 intranet_service_name=Intranet-1
route_eligibility_based_on_path=true

route_eligibility_from_wan_link=a2

route_eligibility_to_wan_link=b2 service=INTRANET;
```

route_eligibility_based_on_path =*Boolean*

This feature allows a user to add an eligible path to the Intranet route. For Intranet Services, enable the Intranet route failover feature. Route eligibility will be based on the state of an associated path.

route_eligibility_from_wan_link_name = *Text* The “from” WAN link name for the path that determines whether to mark this route as ineligible, based on the state of the specified path.

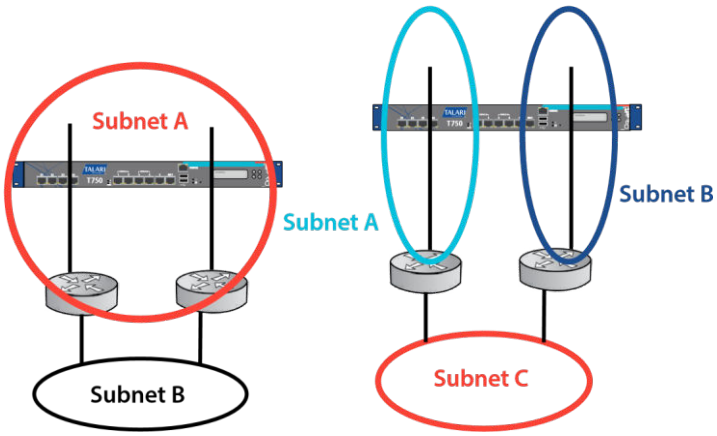
route_eligibility_to_wan_link_name =*Text*

The “to” WAN link name for the path that determines whether to mark this route as ineligible, based on the state of the specified path.

As defined above, the configuration requires the user to specify the WAN links and to enable the feature. For more information on the Oracle SD-WAN Edge configuration file, please see the *APN Configuration Reference*.

L2 MAC Learning for Multiport Bridging

Mac address learning allows a user to define three ports in a bridge group. This simplifies many deployments by allowing the user to connect an MPLS router and a Firewall directly to the appliance without requiring a switch. Figure 3 provides two examples. The new bridging capability in Oracle SD-WAN Edge R2.4 reduces the need for infrastructure changes when deploying Oracle SD-WAN Edge appliances.



Multiple LAN Routers in Same LAN Subnet Multiple LAN Routers in Different LAN Subnet

MAC address learning for multiport bridging stores the source MAC address of each received packet so that future packets destined for that address can be forwarded only to the port on which that address is located. Packets destined for unrecognized addresses are forwarded out of every port. There are no options to configure this command. When three or more ports are configured in an Interface group this feature is enabled.

Design Considerations

- Oracle does not support user spanning tree with this feature. The infrastructure must therefore be designed accordingly
- This feature is enabled by default

Port Switching

Some WAN service providers do not allow long duration UDP sessions and block them in the Cloud. To avoid such issues, the Oracle SD-WAN Edge R2.4 introduces a new feature allowing the user to specify an alternate UDP port for the Oracle SD-WAN Edge conduit packets. UDP Port Switching is a preventative measure to change the source UDP port at specified intervals. The Alternate UDP port number and the port switch interval are user settable. Port Switching can be set using the Oracle SD-WAN Edge Configuration Editor (Figure 4, below). For more information on the Oracle SD-WAN Edge Configuration Editor, please see the *APN Configuration Editor User's Guide*.

Port Switching can also be set by editing the configuration file itself. The command line options would include the following:

```
add conduit_usage

remote_site_name=NCN-Site wan_egress_rate_fair_share=800000
wan_ingress_rate_fair_share=800000 service_group_name=Default
udp_port_num=2156

udp_port_num_alt=2157
```

```
udp_port_switch_interval_minutes=1500;
```

udp_port_num =*Number* (2156)

This will be used as the source UDP port for all WAN ingress packets sent from this link. The Oracle SD-WAN Edge will also only accept WAN Egress packets at this link with dst_port set to this port number.

udp_port_num_alt =*Number* (2156)

This will be used as the alternate source UDP port for all WAN ingress packets sent from this link. The Oracle SD-WAN Edge will also only accept WAN Egress packets at this link with dst_port set to this port number, or the udp_port_num_alt value.

udp_port_switch_interval_minutes =*Number* (1440)

if udp_port_num and udp_port_num_alt are both set and are not equal)

Interval in minutes to be used when switching between the two values of udp_port_num and udp_ port_num_alt. Allowed values are from 1 minute to 8640 minutes (6 days).

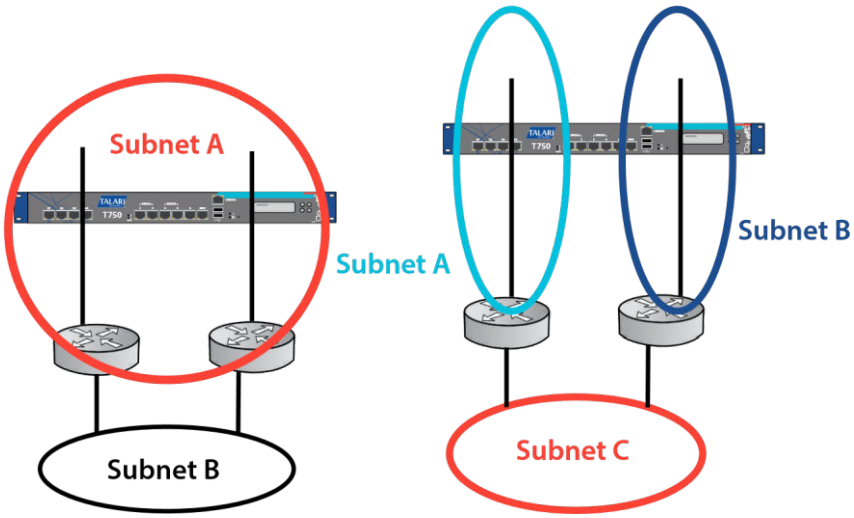
For more information on the Oracle SD-WAN Edge configuration file, please see the *APN Configuration Reference* available from the Oracle support site.

Network Topology

Support for Multiple Routers on LAN-side Subnets

With Oracle SD-WAN Edge Release 2.4, the local routes selection process allows the user to configure the local route to be eligible only when the gateway is reachable. If the gateway is unreachable, the route will be skipped and the next available route will be selected to forward the traffic.

With previous releases, the selection process for local routes only allows for the selection of the route with the lowest cost. Even if this local route's gateway is unreachable, and there are other routes available to get to the local network, this local route will still be selected, causing the traffic to the local network to be dropped. The new feature supports multiple LAN routers in the same or different subnets as shown in Figures 5 and 6 below.



Multiple LAN Routers in Same LAN Subnet Multiple LAN Routers in Different LAN Subnet

Figure 5 Figure 6

This feature is disabled by default but can optionally be enabled once the routes are added, using the Oracle SD-WAN Edge Configuration Editor as shown in Figure 7 on the following page.

Multiple routers on LAN-side subnets can also be set by editing the configuration file itself. The command for this feature is:

```
add route
net=10.3.50.0/24
gw_ip_addr=10.3.10.65
cost=6
route_eligible_on_gw=true
service=LOCAL;
```

route_eligible_on_gw = *Boolean* (NO)

Enabling this option will cause a route to only be valid if the gateway specified in this route is reachable. This parameter is for use in local routes only.

For more information on the Oracle SD-WAN Edge configuration file, please see the *APN Configuration Reference*.

Support for Serial High Availability Appliances

In Release 2.4, Oracle has enhanced its HA support by expanding it to support the Serial Inline HA Topology. This allows a simple Fail-to-Wire based serial HA option that simplifies deployments for end users. The Serial Inline HA feature also includes

supporting additional Fail-to-Block groups or nonHA traffic on the control segment. Figure 8 (below) shows an example of how Serial Inline HA could be configured.

Oracle Serial HA

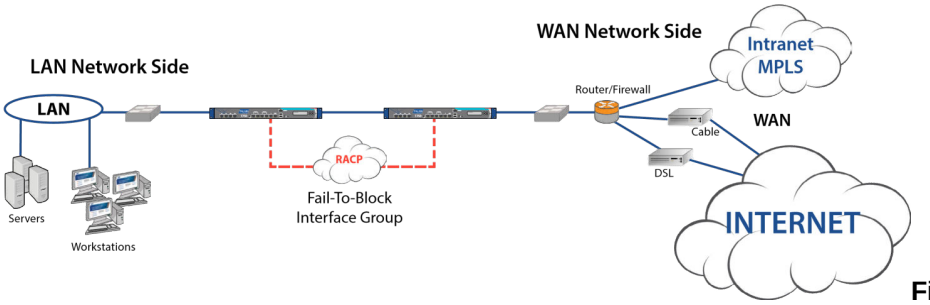


Figure 8

Serial Inline HA can be enabled in the Oracle SD-WAN Edge configuration file using the Oracle SD-WAN Edge

Configuration Editor GUI (shown in Figure 9 below). For more information on the Oracle SD-WAN Edge Configuration Editor, please see the *APN Configuration Editor User's Guide*.

The Serial Inline HA feature may also be set in the Oracle SD-WAN Edge configuration file manually, using the use_ serial_ha parameter. The user would configure the HA in the standard method but select the option for “use_serial_ha.” This feature can also be added to the configuration manually. A sample of the configuration setting is shown below:

```
Define site name=NCN1
{
add appliance name=ncn1
{
...
} add ha_appliance name=ncn1
- HA; { add ha_service set properties
primary_appliance_name=ncn1
HA secondary_appliance_name=ncn1 primary_reclaim=false
use_serial_ha=true; add interface_group
{
set interface_properties viprimary_ip_addr=10.40.10.13
rtual_interface_name=VLAN1
secondary_ip_addr=10.40.10.14; }
}
}
```

For more information on the Oracle SD-WAN Edge configuration file, please see the *APN Configuration Reference*.

Design Considerations:

- Keepalives must be configured on a Fail-To-Block (FTB) interface group
- FTB interface can be directly connected between appliances
- Supports untrusted interface groups for conduit traffic
- Link health not used for HA priority
- Must have a Fail to Wire bypass group defined for conduit traffic
- Standby appliance allows packet to pass through
- Spanning tree must be considered when deploying this topology
- Sends HA protocol across the FTB HA interface group only
- Configuration updates traverse the FTB HA interface group from active to backup appliance

Multiple VLAN Segment on Common WAN link

Oracle SD-WAN Edge Release 2.4 allows multiple VLANs and gateways to be configured on the same WAN link by supporting multiple Access Interfaces. Each “Access_Interface” will support a name, a VIP address, a gateway and the option to enable Proxy ARP. An example of these topologies is shown in Figure 10, below, where with the addition of this new feature Access Interfaces have been configured for VLANs g and b and Edge can perform Proxy ARP for routers g and b.

In previous Edge releases, the WAN link and WAN link gateway were on a single VLAN, causing problems for customers that segmented traffic (e.g. Intranet vs. Internet) on different VLANs for security reasons. Additionally, if Proxy ARP was enabled on a WAN link, it would only work properly for hosts that resided on the corresponding VLAN segment. If the WAN link was assigned to VLAN A and the gateway went down, the users on VLAN A would have connectivity but those on other VLAN would not.

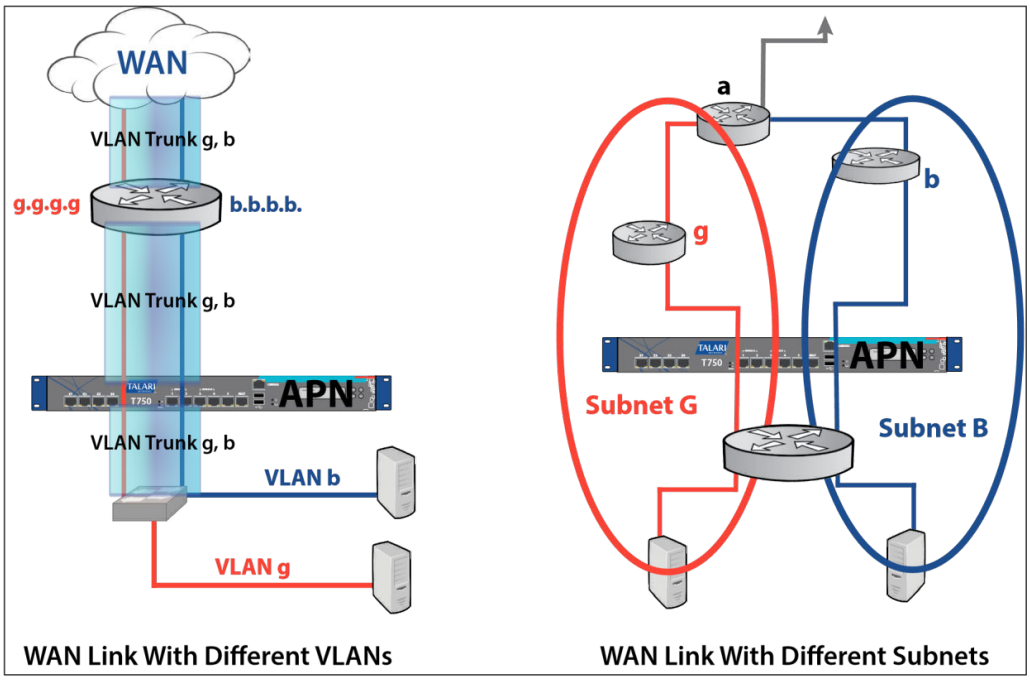


Figure 10

This feature may be set in the Configuration Editor, as shown in Figure 11 below. Note that the first configured WAN link access interface is set to be the Primary by default and additional access interfaces are defined to be excluded. The user would then be expected to verify the primary access interface link, as well as any interfaces to be configured as secondary. When the primary access interface gateway is not reachable, the appliance would use the access interface configured as secondary.

For more information on the Oracle SD-WAN Edge Configuration Editor, please see the *APN Configuration Editor User's Guide*.

These interfaces are used to define which gateway the appliance would use to forward conduit frame for the corresponding WAN link. These options are defined under the WAN link, Set Properties field of a WAN link definition.

To edit the configuration manually, the options associated with this feature are included below:

```
add access_interface name=CL3_WL0_access_interface_1
```

```
                virtual_interface_name=CL3VL0                    virtual_ip_addr=10.3.10.12
        gw_ip_addr=10.3.10.2

                        enable_proxy_arp=true;

set properties

                        primary_conduit_access_interface=Cogent-NS_175Federal-AutoAI-0
                        wan_ingress_physical_rate_kbps=2000
                        wan_egress_physical_rate_kbps=2000
                        wan_ingress_permitted_rate_kbps=2000
                        wan_egress_permitted_rate_kbps=2000
```

The Proxy ARP capability is configured under the Access Interface and is shown above. “True” would indicate Proxy ARP is enabled and “false” would indicate that the feature is disabled for the Access Interface. Proxy ARP needs to be enabled for local side subnets.

primary_conduit_access_interface = Text

The name of the access interface to be used as the primary access interface for this WAN Link. Mandatory.

secondary_conduit_access_interface = Text

The name of the access interface to be used as the secondary access interface for this WAN Link.

For more information on the Oracle SD-WAN Edge configuration file, please see the *APN Configuration Reference*.

Design Considerations:

• Enable Proxy ARP for local side subnets

Path MTU Discovery

Path MTU discovery allows the sender of IP packets to discover the Maximum Transmission Unit (MTU) of packets that it is sending to a given destination. The MTU is the largest packet that can be sent through the network along a path without requiring fragmentation. Previous releases supported ICMP to adjust the conduit MTU.

To overcome these limitations, Oracle SD-WAN Edge Release 2.4 introduces a new path MTU discovery method that will actively probe each sending path of each conduit to find out the current MTU, and adjust the conduit MTU accordingly. This feature must be enabled by the user and will then probe each path within a conduit every 10 minutes.

This feature can be configured in the Oracle SD-WAN Edge Configuration Editor (See Figure 12, below). Additionally, the Oracle SD-WAN Edge Web Console and CLI will display the current MTU that is being used by each WAN Ingress path on the conduit (See Figure 13 for an example) For more information on the Oracle SD-WAN Edge Configuration Editor, please see the *APN Configuration Editor User's Guide*. For more

information on using the Oracle SD-WAN Edge Web Console, please refer to the *APN Appliance Operation Guide*.

Figure 12. Active MTU Discovery in the Oracle SD-WAN Edge Configuration Editor.

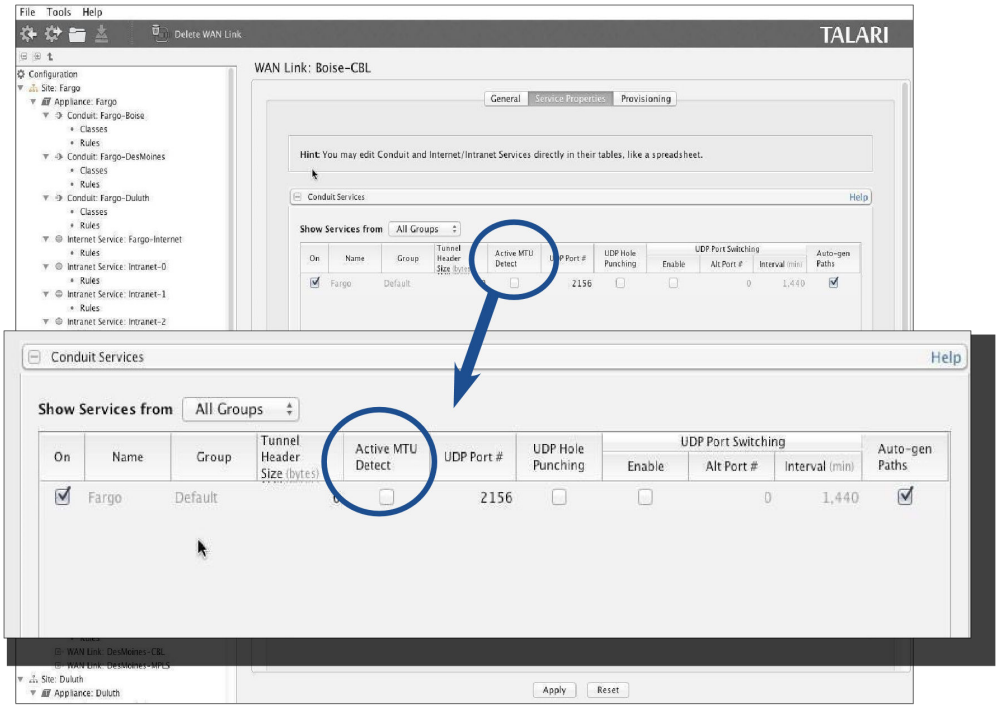
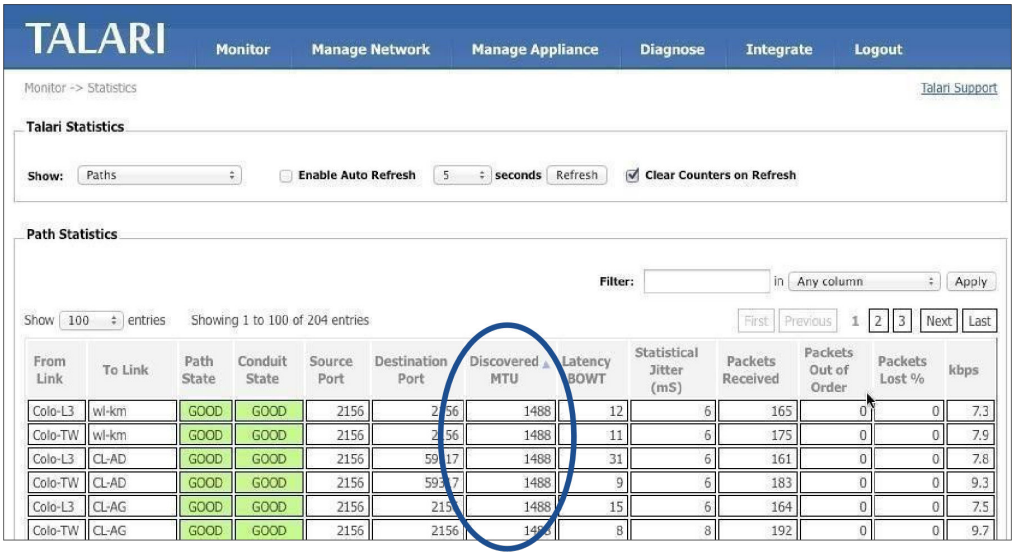


Figure 13. Active MTU Discovery Shown in the APN Web Console



If editing the configuration file manually, the command options for this capability in the configuration file are enabled under the WAN link, conduit services:

```
add conduit_usage  remote_site_name=Client-test1
                   wan_egress_rate_fair_share=100000
                   wan_ingress_rate_fair_share=100000
                   service_group_name=Default udp_port_num=2156
                   active_path_mtu_discovery_enable=true;
```

For more information on the Oracle SD-WAN Edge configuration file, please see the *APN Configuration Reference*.

Design Considerations:

• Currently if a lower MTU is detected, MTUs of all paths of the corresponding WAN link are reduced

Usability

Clone Site Configuration Wizard

To make it easier to add a new client site to a configuration, Oracle SD-WAN Edge Configuration Editor now allows the user to clone a pre-existing site's configuration as a new site.

To clone an existing site using the Configuration Editor, select the site that you would like to clone, and click the **Clone Site** button. This will bring up a dialog screen containing the cloned site information that must be changed before being allowed to save the new site information. See Figure 14 below. For more information on the Oracle SD-WAN Edge Configuration Editor, please see the *APN Configuration Editor User's Guide*.

The Site Cloning Process

A new cloned site must contain its own valid site configuration. In other words, the existing information from the site being cloned (presented on the screen in red) must be changed before the new site can be created. As you make the needed changes, the text will change from red to black. Any particular portion of the site being cloned that is unneeded in the new cloned site may be excluded by clicking on that line item and then clicking the **Exclude** button, and graying out the unneeded information. Please see Figure 15 below.

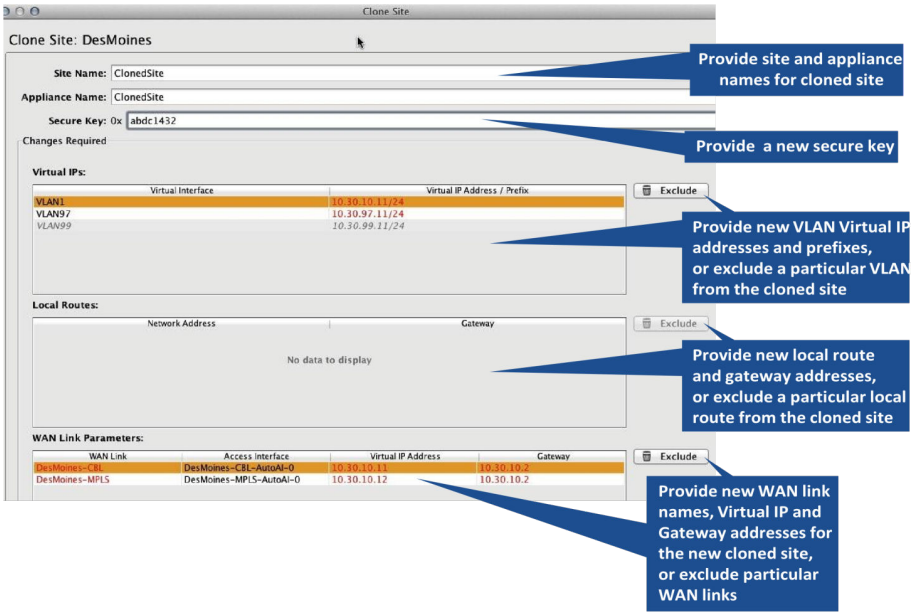


Figure 15

Once you have edited the screen making sure that all fields are valid and unique from their original values, the OK button will be enabled (Figure 16). Clicking the OK button will allow an audit of the new site to make sure the information will be valid for your configuration. If any errors are found, you will receive an error message pointing out that needs to be corrected.

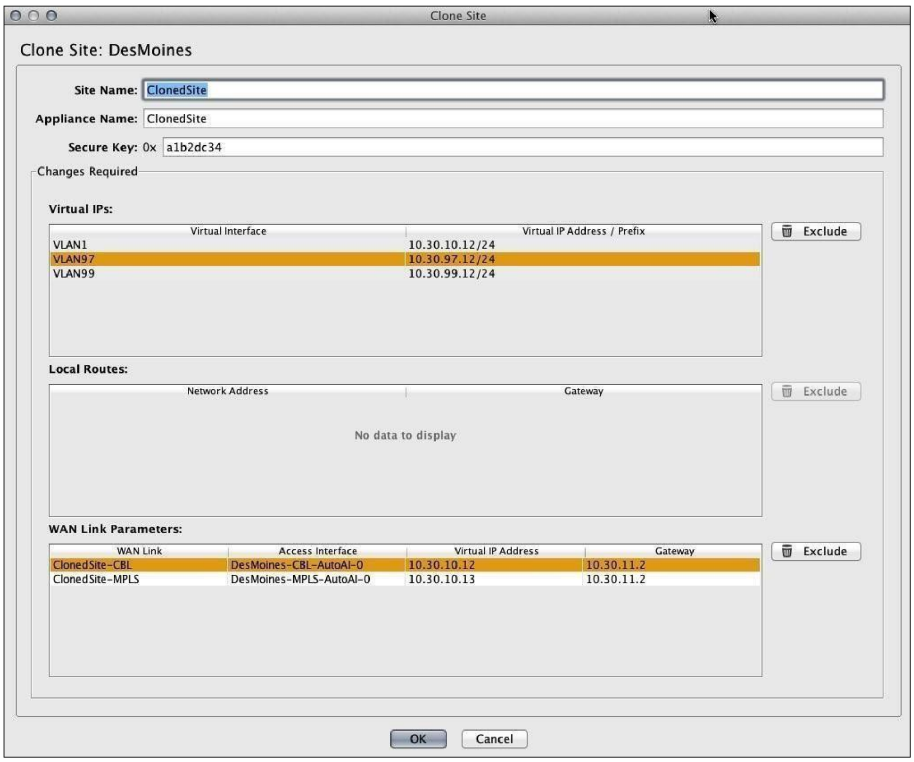


Figure 16. New te ready for audit.

If the audit succeeds, you will be presented with a screen detailing the next steps that need to be performed in making your new site functional in your network (see Figure 17).

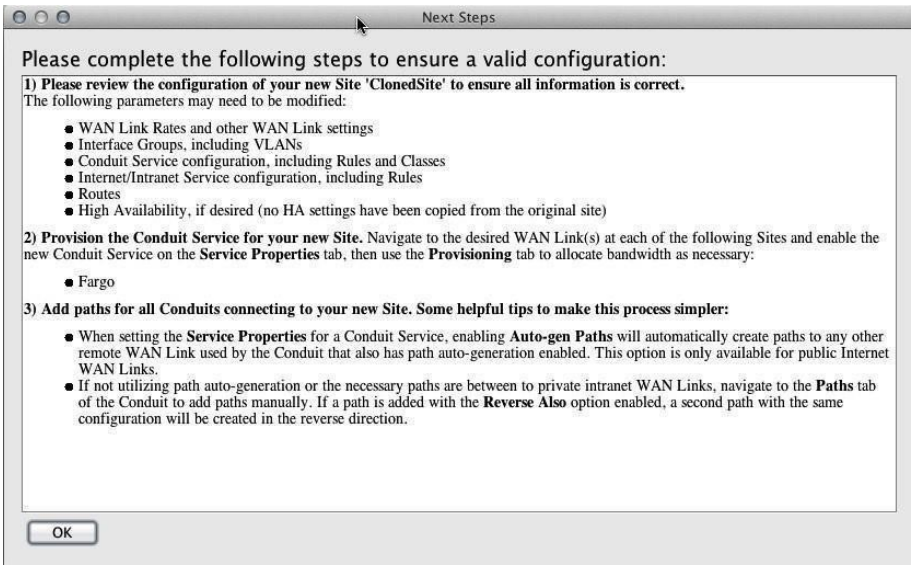


Figure 17: Next steps in the site cloning process message

Next Steps in the Site Cloning Process

Sample Next Steps for the newly created client site called “ClonedSite:”

1. **Please review the configuration of your new Site ‘ClonedSite' to ensure all information is correct.**

The following parameters may need to be modified:

- WAN Link Rates and other WAN Link settings
- Interface Groups, including VLANs
- Conduit Service configuration, including Rules and Classes
- Internet/Intranet Service configuration, including Rules
- Routes
- High Availability, if desired (no HA settings have been copied from the original site) **Provision the Conduit Service for your new Site.** Navigate to the desired WAN Link(s) at each of the following Sites and enable the new Conduit Service on the **Service Properties** tab, then use the **Provisioning** tab to allocate bandwidth as necessary:
- Fargo

1. **Add paths for all Conduits connecting to your new Site.** Some helpful tips to make this process simpler:
    - When setting the **Service Properties** for a Conduit Service, enabling **Auto-gen Paths** will automatically create paths to any other remote WAN Link used by the Conduit that also has path auto-generation enabled. This option is only available for public Internet WAN Links.
    - If not utilizing path auto-generation or the necessary paths are between to private intranet WAN Links, navigate to the Paths tab of the Conduit to add paths manually. If a path is added with the **Reverse Also** option enabled, a second path with the same configuration will be created in the reverse direction.

More detailed information on the elements of these steps is available in the *APN Configuration Editor User's Guide*.

Improved Site WAN Link Provisioning

An Overview of Provisioning

Provisioning allows for the automatic bidirectional (Ingress/Egress) distribution of bandwidth for a

WAN link among the various services associated with that WAN link. Using the Oracle SD-WAN Edge

Configuration Editor, the user can enter the values in the text fields and directly into the cells of the table like a spreadsheet. The Provisioning page is shown below in Figure 18. There are three steps to Provisioning that provide for this bandwidth distribution in a simple and effective way:

1. WAN Link Rates (Setting the WAN link physical and permitted rates)

2. Provisioning Groups (Create and edit groups of shares of bandwidth)
3. Services (View and edit services for groups or individual site WAN links)

With Oracle SD-WAN Edge Release 2.4, we introduce the concept of Fair Shares to the provisioning process. Shares are used to distribute the permitted bandwidth between the provisioning groups. The bandwidth calculated is based on the shares allocated for a particular group, divided by the total shares for all groups. A separate pool of shares is used for both Ingress and Egress traffic.

This area allows the user to set both the WAN link

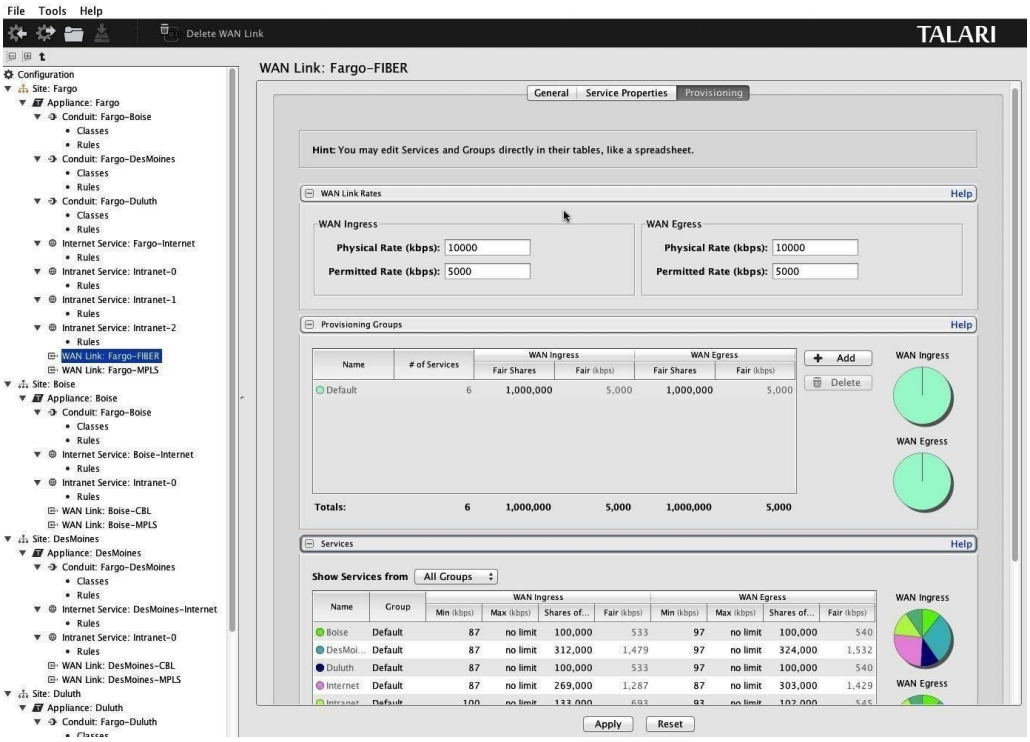


Figure 18

WAN Link Rates

Physical Rate (the raw bit rate for the incoming/ outgoing traffic), and the WAN link Permitted Rate (the available rate for incoming/outgoing traffic). Please see Figure 19 on the next page.

Provisioning Groups

A Provisioning Group contains a collection of WAN Link bandwidth usages for any given WAN Link. This allows the user to allocate and distribute the shares of bandwidth among a smaller set of services at a high level before drilling down to the individual services for finetuning. They also provide a boundary for the automatic redistribution of bandwidth within the child Services of the Provisioning Group.

In the **Provisioning Groups** table, shares are used to distribute the WAN Ingress/ Egress eligible bandwidth, which is the **Permitted Rate** minus the total **Min** reserved bandwidth of all Services on the WAN Link. All Services are initially assigned to a “Default” Group that is allocated all the eligible bandwidth. The user can create

additional Groups and allocate bandwidth to its members by giving that Group a number of **Fair Shares**. The resulting total bandwidth for all Services in the Group is then shown in the **Fair (kbps)** column. Please see Figure 20 for a view of the Provisioning Groups section.

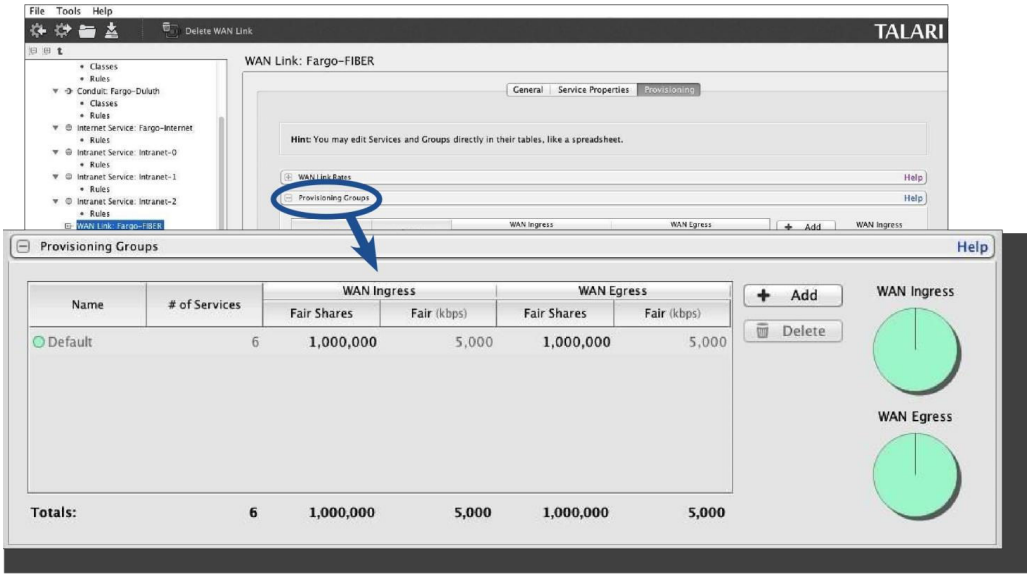


Figure 20

To create a Provisioning Group:

- Click the **Add** button

- Provide a Group name
- Provide the number of WAN Ingress and WAN Egress **Fair Shares** required for the new group
- Reassign Services to the new Group using the **Group** column in the **Services** table

Provisioning Groups are available to simplify the provisioning process and are not required if they are not needed.

The Concept of Using Shares

When provisioning bandwidth for Oracle SD-WAN Edge with a large number of sites, using percentages does not allow for enough granularity as the site count increases.

Oracle has instituted the use of shares for each of the Services or Groups of Services within the WAN Link. The total number of shares is up to the user, allowing any amount of granularity or precision when allocating bandwidth among the different Services. There are two distinct pools of these shares: WAN Ingress and WAN Egress.

> **Note:**
>
> All Services receive their Min Reserved Bandwidth before Fair distribution, which could result in Groups with equal Fair Shares having disparate Fair Rates. Fair Rates can also be affected by Service Maximums, if defined.

Services

The services definition for a WAN link are determined in this section (see Figure 21 below). For conduit services, the user would define the fair shares allocated to a client site. By default, all sites are placed in the “Default” group with the fair shares divided evenly. Services for individual site WAN links are shown and may be edited here.

- Display desired Provisioning Group or all groups by using the pull-down menu Add individual services to a Provisioning Group by selecting the service name and choosing the desired Group
- Set the desired WAN Ingress and Egress minimum and maximum rates, and Group shares for the service by double-clicking the cell to change the rate or number of shares
- To set an unlimited maximum rate, enter “0” or “no limit” into the cell
- Click the **Apply** button to save the settings

Shares of Group

On this table, the shares are used in the same way as above, but in this case, it is a new pool of shares within each group used. These shares are used to divide up the bandwidth among the members of a group based on the ratio of the current service divided by the total number of shares for the group in which it is a member. The Minimum rate acts as a base bandwidth allocation for each service, and the amount of bandwidth available for fair allocation is based on the total permitted for the group minus the sum of the minimums for each service in the group.

Glossary

- Adaptive Private Networking (Oracle SD-WAN Edge)

As used in this guide, the name for the whole network that includes the Adaptive Private Networking Appliances, the Wide Area Network, the conduits between peer APNAs, as well as other network application services. Oracle SD-WAN Edge is configured from a single APNA, which is the Network Control Node (NCN).

- Adaptive Private Networking Appliance (APNA)

The general name for a specific Oracle network appliance, also occasionally referred to as a Appliance.

- Client Node (Client)

A Oracle Client Node is an Oracle SD-WAN Edge appliance that is located across the Oracle network from the NCN. Although an NCN may potentially have multiple clients, each client has only one NCN.

- Conduit Service

The Conduit service is a logical combination of one or more paths, and is the typical mode for enterprise site-to-site intranet traffic, utilizing the full value of the Oracle's

Adaptive Private Networking. In this mode, depending on configuration, the traffic is actively managed across multiple WAN links to create an end to end conduit.

- Ethernet Interface

A physical or configurable interface of the APNA. For example, the T730 has nine userdefined Ethernet Gigabit interfaces, plus a predefined Management interface.

- Flow

A flow is a stateful instance (memory) used to track and treat application traffic from its source to its destination across Oracle SD-WAN Edge. The properties of a particular flow are derived from the routes, rules, and service that the traffic flow matches.

- Internet Network Service

The Internet Service is for traffic between an enterprise user and sites on the public Internet. Traffic of this type is not encapsulated. During times of congestion, Oracle SD-WAN Edge does actively manage bandwidth by rate-limiting Internet traffic relative to the conduit and intranet traffic as per the configuration established by the administrator.

- Intranet Network Service

The Intranet Service is for any portion of enterprise Intranet traffic that has not been defined for transmission across an Oracle SD-WAN Edge conduit. As with Internet traffic, it remains unencapsulated, and Oracle SD-WAN Edge manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Note that under certain conditions, and if configured for Intranet Fallback on the Conduit, traffic between a pair of APNAs that ordinarily travels via a conduit may instead be treated as Intranet to maintain network reliability.

- Network Control Node (NCN)

The NCN is the central APNA that acts as the master controller of Oracle SD-WAN Edge, as well as the central point of administration for the client nodes. The NCN's primary purpose is to establish and utilize a conduit with one or more Oracle Client Nodes across the network for enterprise site-tosite communications. A particular NCN can administer and have conduits to multiple Client Nodes.

- Network Service

A logical set of operations performed on the traffic as it uses Oracle SD-WAN Edge. The set of services supported are Bypass, Passthrough, Internet, Intranet, and Conduit.

- Passthrough Network Service

Traffic directed to the Passthrough service includes broadcasts, ARPs and other nonIPv4 traffic, as well as traffic on the APNA's local subnet, specifically configured subnets, or rules applied by the network administrator. The APNA does not delay, shape or modify

this traffic. Because the Oracle service does not hinder this traffic, the network administrator must be sure that Passthrough traffic does not consume substantial resources on the WAN links which the APNA is configured to use for other services. Example: Passthrough may be used if a host is located on the WAN side of the APNA, but access to the host does not impact the APNA's specific WAN links. Think of the special management IP of the WAN link router as a typical example of a proper explicit use of Passthrough.

- Redundant Oracle SD-WAN Edge Control Protocol (RACP)

The protocol developed by Oracle to provide functionality for two high availability (HA)

APNA's to communicate availability information.

- Rule

A Oracle Networking Service equivalent of a typical router access control list or filter mask. A rule defines match criteria and properties for IP flows. Flows that match those criteria use the service with which the rule is associated.

- Oracle Path Oracle Conduit Class

A Oracle Path is a logical link between two Oracle Virtual IP addresses (VIP). A Class is a queued service point into a Oracle conduit. The Class to which traffic is assigned determines its share of the conduit bandwidth, permitted queue depth, and its priority, relative to other traffic, for Oracle Network resources.

- **TCP Termination**

TCP termination provides the ability to split a single TCP connection into three separate TCP connections all managed and maintained by the Oracle SD-WAN Edge. TCP termination is only used for conduit traffic.

- Traffic Service Types

Traffic Service Types apply while the system is in the Active state noted above.

- Trust Relay Points (TRP)

A Cisco Systems software function implemented in voice over IP networks that provides multiple voice capabilities, such as transversing trusted firewalls.

- Trusted WAN Port

Appliance port processing network traffic that is protected by a firewall, performing as if it were a traditional WAN port.

- Untrusted WAN Interface

Appliance interface processing network segment traffic that is not being protected by a firewall. Non-conduit traffic from the WAN is unable to communicate to any network interface inside of the appliance. The segment is entirely isolated from the rest of the network with the exception of the APNs own 128 bit AES encrypted paths.

- WAN Link

The general term for an enterprise's connection to a WAN. These WAN links are typically connected to router ports. Some examples of WAN Links are T1, DSL, or Frame Relay.

3
Release 2.5 Features

This chapter includes features and enhancements released in 2.5.

Oracle Hardware Support

Oracle SD-WAN Release 2.5 incorporates the T5000 seamlessly into the entire family of appliances offered by Oracle. Basic Oracle SD-WAN Edge appliances platform capabilities are listed below.

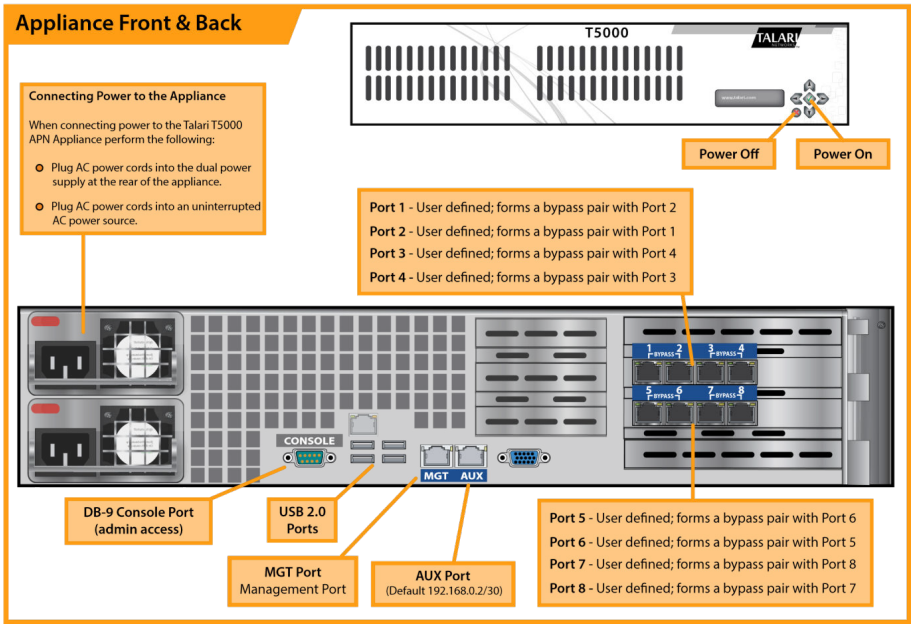
Appliance Model	Conduits	WAN Ingress Paths	WAN Egress Paths	Flows	Flows with TCP Termination
T5000	128	576	576	256,000	16,000
T3000	128	576	576	256,000	16,000
T750	32	216	216	64,000	8,000
T730	16	72	72	64,000	4,000
T510	8	36	36	32, 000	500

Table 1

Table 1 provides a detailed view of the supported hardware maximum capabilities. The number of conduits can be used to derive the number of sites if used as an NCN or as a client in a meshed configuration. If any of the appliances are used as a client device, the hardware can still support the number of conduits defined, but will be dependent on the Oracle SD-WAN Edge architecture deployed. Table 1 is provided so users understand the conduits supported by all platforms in Edge release 2.5.

Introducing the T5000 Appliance

Designed to bring WAN reliability and higher bandwidth to large data centers and call centers, the 2U rack-mountable Mercury T5000 appliance affordably delivers up to 3.0 Gbps uplink/3.0 Gbps downlink (6 Gbps total) across up to 8 WAN connections. T5000 appliance can easily communicate with other Oracle appliances such as the Mercury T510, T730, T750, and T3000 models. T5000 runs the same software as other Oracle appliances while taking performance and scalability to the next level, supporting gigabits of WAN bandwidth across the union of private WAN links and public Internet connections and providing support for up to 128 branch connections.



For information on installing the T5000, please reference the Oracle SD-WAN Edge T5000 Getting Started Guide and the Oracle SD-WAN Edge T5000 Hardware Guide.

4
Release 3.0 Features

This chapter includes features and enhancements released in 3.0.

Dynamic Conduits

The dynamic conduit is a conduit between two Oracle SD-WAN Edge client sites that is not predefined in the Oracle SD-WAN Edge configuration file, but is created on-demand based on network traffic. From a user perspective, the advantage of a conduit between client sites is that traffic can flow directly from one client Oracle SD-WAN Edge site to a second client site without having to traverse the NCN or two conduits. In addition, the conduit is built and removed dynamically based on user defined traffic thresholds. These thresholds are defined in either packets per second (pps) or bandwidth (kbps). From a configuration perspective, the Dynamic Conduit requires some up front configuration time. Another benefit of the Dynamic conduit is the ability for the any client to dynamically build a conduit to any other client.

This allows a dynamic full Mesh configuration for customer traffic flows. Once a threshold for the Dynamic Conduit is reached and the dynamic conduit is created, the appliances test the dynamic conduit before making full use of it in the following manner:

- Send Bulk data if any exists and verify no loss, then
- Send Interactive data and verify no loss, then
- Send Real Time data after the Bulk and Interactive data are considered stable (no loss or acceptable levels)
- If there is no Bulk or interactive data send Real Time Data after the conduit has been stable for a period of time

If the user data falls below the configured thresholds for a user defined period of time, the dynamic conduit is torn down.

Design Considerations

Based on the above traffic flows as well as the nature of dynamic conduits the user should be aware of certain Design considerations. These considerations are as follows:

- For voice traffic across the Dynamic Conduit be aware of WAN link limitations/ quality
  - Loss
  - Latency of the WAN link
- In certain cases WAN link may not be recommended as a path for a Dynamic Conduit if there is a high loss or latency that would impact certain traffic types. In this case, do not configure the WAN link as part of the Dynamic Conduit
- How often a WAN link transitions from good to bad

- Ideally there is traffic between the Oracle SD-WAN Edge sites that is non-voice traffic Bulk or Interactive before Voice
- WAN link thresholds are based on all traffic on a WAN link, including conduit, Intranet, and Internet
- In this release Dynamic Conduits support a single “Dynamic Conduit Default set” for rules and classes.
- When using Dynamic conduits, the user should have consisted rules for the following options: Header compression and TCP Termination.

Adding a site to the Dynamic Conduit is a service reset for all site participating in the Dynamic Conduit.

Dynamic Conduit Configuration

Dynamic Conduits have the concept of an Intermediate site; this site could be an

NCN site. If the NCN site has two client sites connected, Client A and Client B, with WAN-To-WAN forwarding enabled Client A would communicate with Client B through the NCN site (Intermediate). Any site configured as the Intermediate site monitors traffic flowing through sites that are configured to support Dynamic Conduits. In this example the NCN site is monitoring traffic levels between Client A and Client B. Once the configured threshold is reached through the Intermediate site the Dynamic Conduit is built between Client A and Client B.

The other high level design consideration is related to WAN-To-WAN Forwarding

Groups. By default, all Oracle SD-WAN Edge sites reside in the default forwarding group. When WAN-To-WAN forwarding is enabled all routes from all sites are known throughout the Oracle SD-WAN Edge. This may not be desired. Because of this, the concept of WAN-To-WAN Forwarding Groups was added in the 3.0 release. The user now has the ability to create multiple WAN-To-WAN Forwarding Groups that do not share routes. In this release the Intermediate Oracle will forward between WAN-To-WAN Forwarding Groups. In future software, a user will have an option to forward between WAN-To-WAN Forwarding Group or not.

A high-Level description of the configuration process follows.

The process for configuring a Dynamic Conduits is as follows:

- Identify intermediate Site
  - Enable intermediate site (use default WAN-To-WAN Forwarding Group)
  - Enable WAN to WAN forwarding at intermediate site
- Identify Client sites for Dynamic Conduits Enable dynamic conduits at the clients site
- Enable the Dynamic conduit service (WAN Link – Service properties)
  Provision WAN Link resources for the Dynamic Conduit (shares)
  - Identify threshold used for Dynamic Conduit Creation Define using Dynamic Conduit Default Set
    Define threshold at Intermediate Site WAN Link

Dynamic Conduit Configuration Creation

For the Dynamic Conduits to be created the user would define a site, typically the NCN (site but not required to be the NCN site), to act as the intermediate node for the client sites. These options are configured at the appliance level. At this site the user would enable “WAN-To-WAN forwarding”, as well as select the “Intermediate site” option, see figure 1.

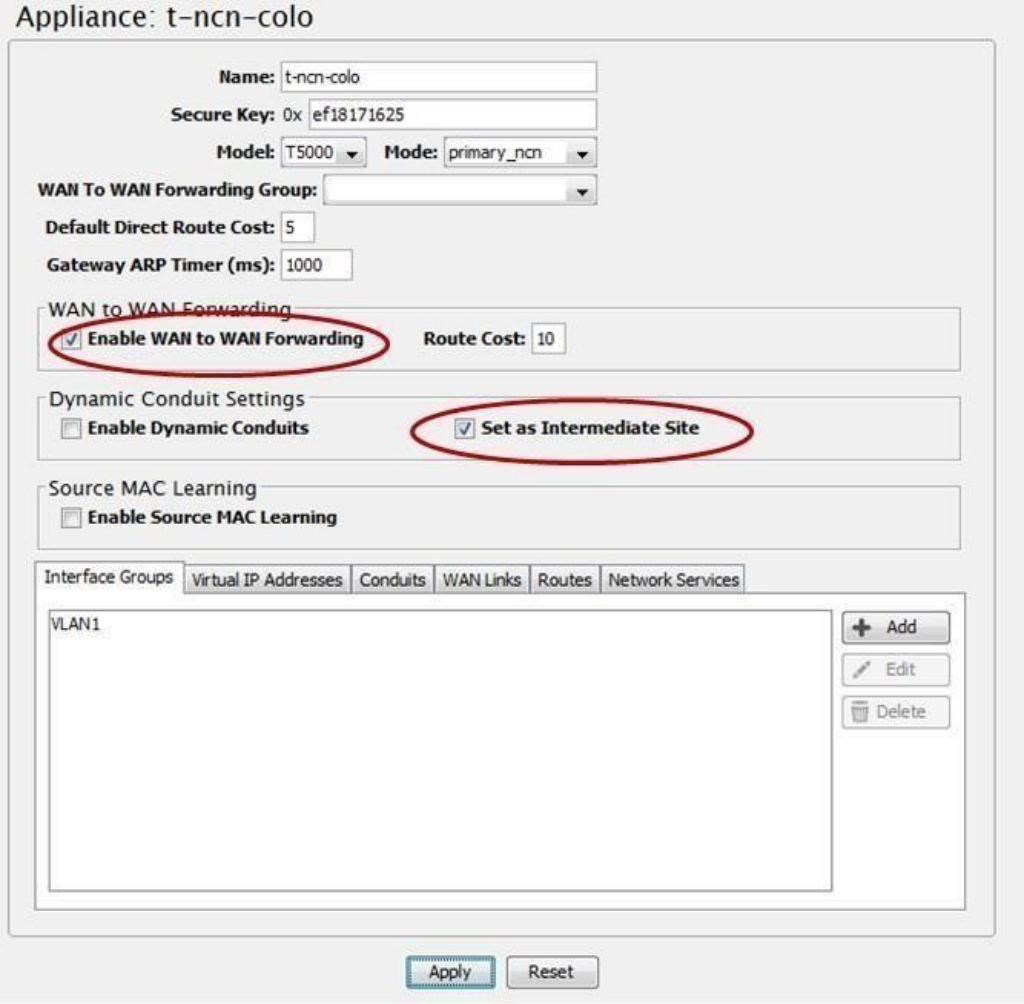


Figure 1

In this example the NCN with the WAN-To-WAN option enabled will forward all routes to all client appliances within a WAN-To-WAN Forwarding Group. By default, all sites reside in the default WAN To-WAN Forwarding Group. The user can also define additional WAN-To-WAN Forwarding Groups as required. The groups are defined at the Global configuration level. The intermediate site will monitor the traffic flow between Client Sites to determine if the traffic level reaches the user defined threshold. If the traffic flow reaches the defined threshold, the Intermediate node will instruct the client nodes to establish a Dynamic Conduit. The sample thresholds will be described later in this document.

At the client node, the user would enable the dynamic conduits option at the appliance level.

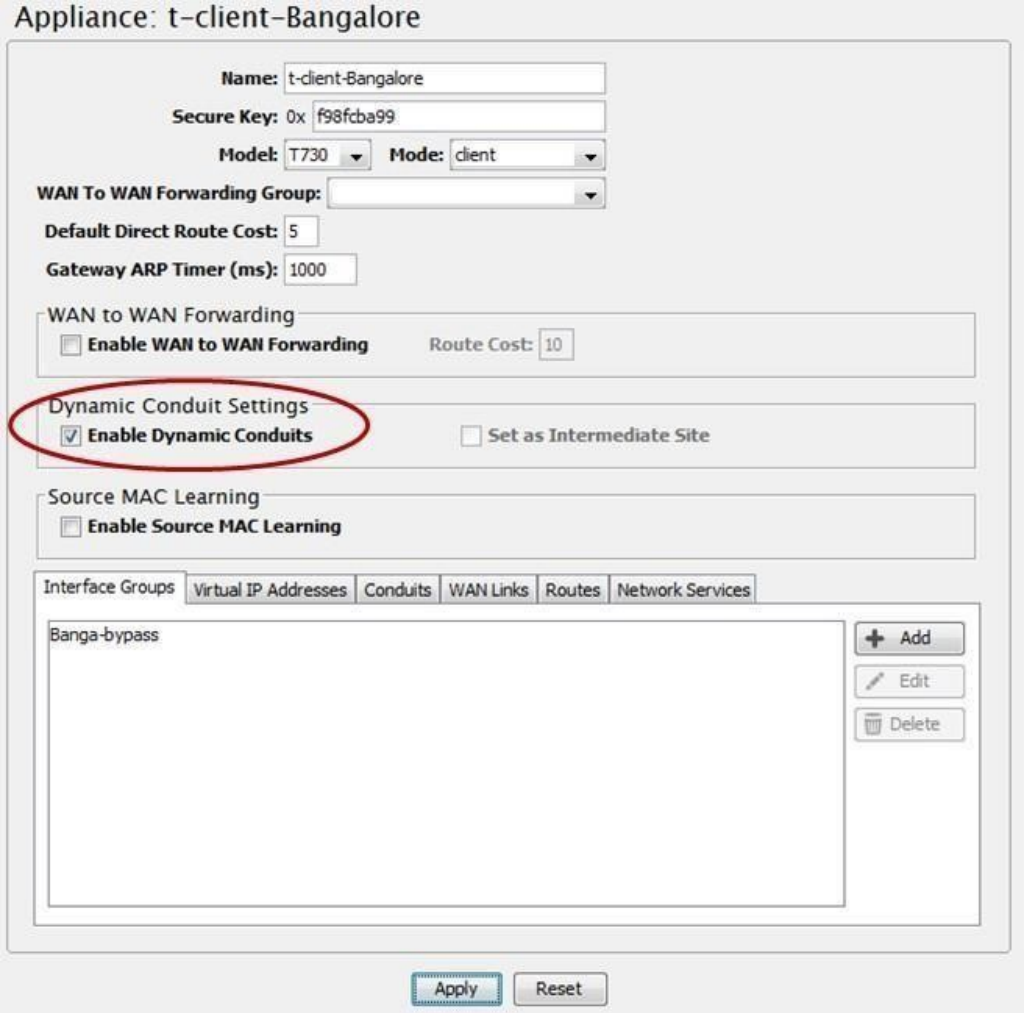


Figure 2

There are two methods for configuring thresholds for a dynamic conduit. The Dynamic Conduit will be created if any of the configured values (thresholds) are reached. The options can be configured at a global level or based on a WAN Link configured at the Intermediate node. If the user does not want to match on the WAN link they would only have to configure the thresholds at the global level. Currently if configured at the WAN link level all traffic accounted for is counted as the threshold value, so conduit traffic, intranet traffic and Internet traffic are all count towards the WAN link threshold. Examples of these options are defined below:

Option 1:

The advantage of this option is to offload bandwidth on one of the intermediate node WAN links. As clients communicate to each other through the intermediate node there may be a requirement to remove this traffic from one (or multiple) of its local WAN links. This can be accomplished by defining a threshold on the local WAN link. If one of the thresholds is reached the Dynamic Conduit will be established between client sites. The key design point when using the WAN link threshold option is that this is total traffic on the WAN link. This includes conduit, internet, and intranet traffic, not just client to client traffic. The option is defined under the appliance – WAN Link – General-Property's tab. Figure 3 displays the options to configure the available threshold options.

Figure 3

Option 2:

Once the Dynamic Conduit is enabled at a client site there is a Dynamic Conduit

Default Set defined. Within this default set is a properties tab which includes

"creation limits". The values for the conduit create are Sample time in seconds (default value 10 seconds), Throughput in kbps (default value 250 kbps), and Throughput in pps (default value 10 pps).

From the global level once a client site has “Dynamic Conduits” enabled look for “Dynamic Conduit Default Set: Default”. Figure 4 displays these settings.

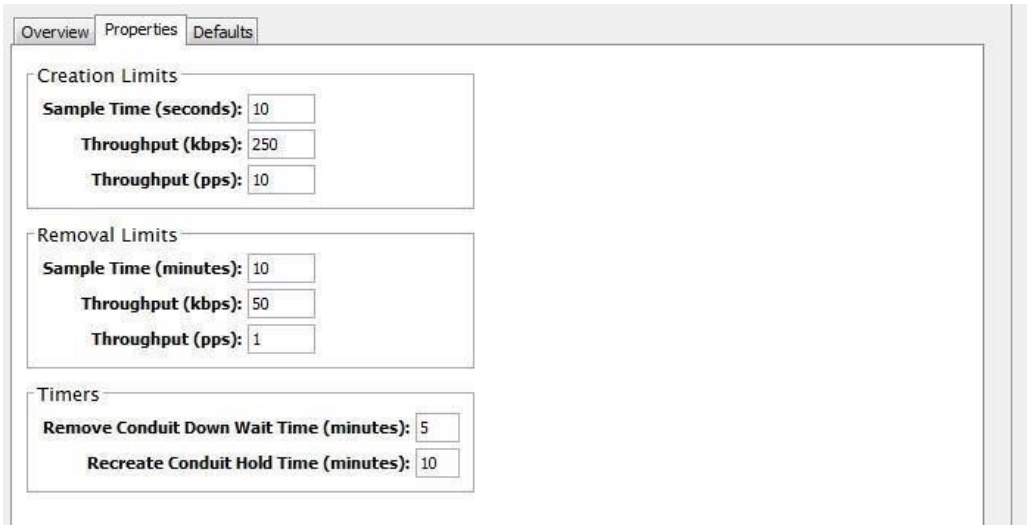


Figure 4

Once the intermediate site is defined, and WAN To WAN forwarding is enabled and Client sites have dynamic conduits enabled if any Creation limit is reached the dynamic Conduit is created. Again, this can be pps or kbps.

For each client site the user would also have to provision the Bandwidth shares for the Dynamic Conduit. These provisioned Fair shares per WAN link are used by all dynamic conduits on that WAN link. The allocated minimum reserve shares are per Dynamic Conduit for the WAN Link. Figure 5 shows and exampled of enabling the service on a WAN Link:

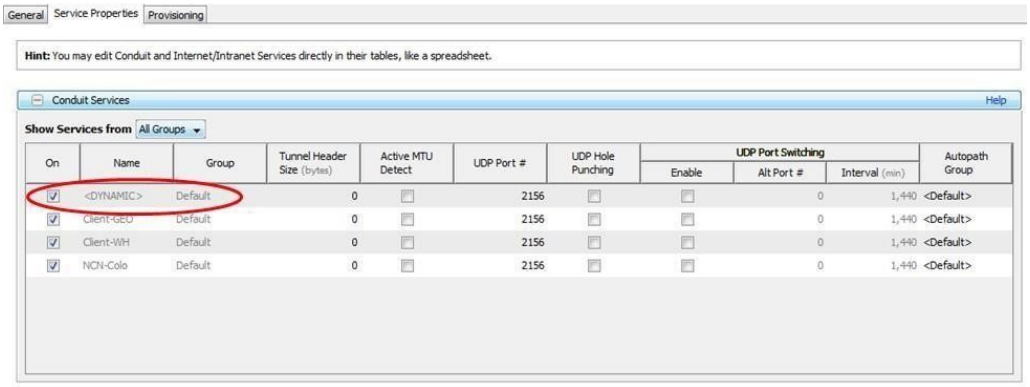


Figure 5

While Figure 6 shows how to define the shares for a WAN Link once the service is enabled.

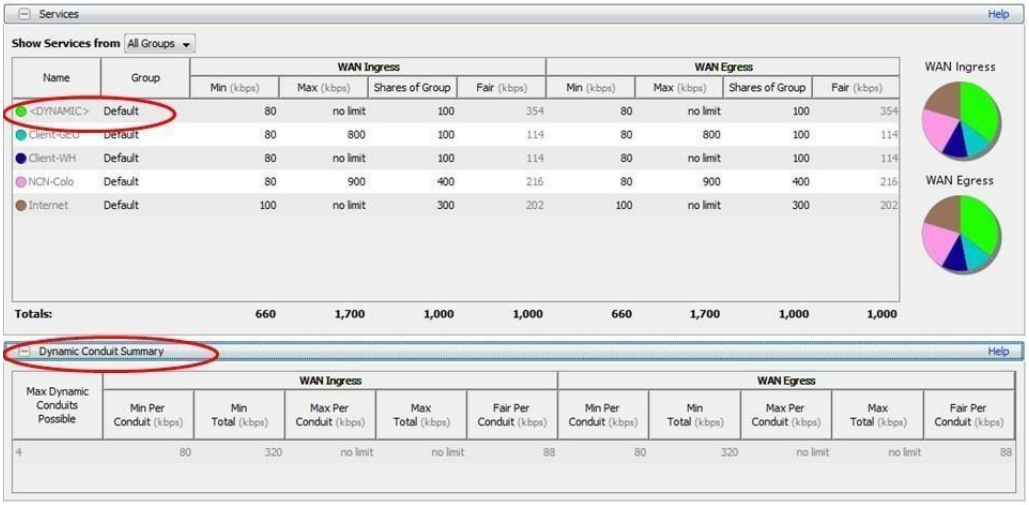


Figure 6

There is also dynamic conduit remove settings that are user definable. In addition to the above, the web console allows the user to delete a dynamic conduit or Freeze a dynamic conduit. The freeze option allows the user to keep the conduit up and ignore the remove conduit. This feature would be used for testing a dynamic conduit as well as for troubleshooting purposes. These options reside under the Manage Network Dynamic Conduits tab in the web console.

WAN To WAN Forwarding Enhancements

To provide the flexibility required for Dynamic Conduits to operate, WAN-to-WAN forwarding was enhanced to allow for multiple groups. All sites that are part of a WANTo-WAN Forwarding Group with WAN-To-WAN forwarding enabled have a common

routing table. The routing table consists of routes to all other sites in the group. Many customers in the past did not enable WAN-To-WAN forwarding because of this fact. By default, all APNA's are applied to the default group. If the requirement is for only certain sites to support dynamic Conduits the user would define a new WAN-To-WAN

Forwarding Group, then at the appliance level assign the appliance to the correct WAN-To-WAN Forwarding Group.

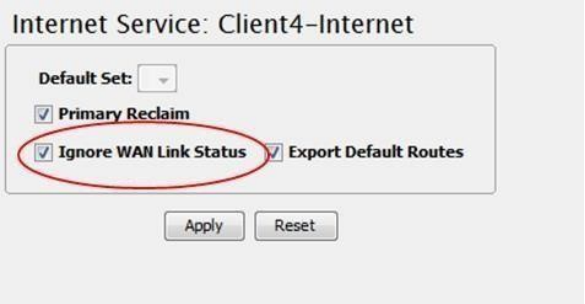
In addition, APNA's in one group will not have direct routes of an APNA that resides in another WAN-To-WAN Forwarding Group. The user also has the flexibility in allowing or excluding Internet routes and Intranet routes in the routing table. The

Internet/Intranet routes are considered local routes from a WAN-To-WAN forwarding perspective and included in the routing table unless otherwise configured. When configuring or planning to deploy Dynamic Conduits contact your Oracle representative for any additional information.

Routing Enhancements

Intranet or Internet Fallback Routes

There were certain configurations when route eligibility was used that a Conduit Fallback route was not hit because the conduit was down, but the gateway was still reachable. When this occurred, the traffic would hit a pass-through route which in certain designs was then dropped by the Oracle. To eliminate Oracle from dropping frames the user can now select Intranet/Internet fallback routes such that if the conduit fails the Oracle will forward traffic to the defined Intranet router/gateway. See figure 7 for details.



From figure 5 we can see that this option is configured under “Appliance – Internet Service – Ignore WAN link Status”. The same option exists under Intranet service and is enabled via the check box.

Additional Enhancements

- Auto-Path Groups for WAN Links
  In previous releases the user would have to create a manual path and then edit the advanced attributes for the path for private WAN links. Because there was no auto-path for private (intranet) WAN links the user was forced to define the paths and attributes for the path. This new feature allows a user to define an “Auto-Path-group” at the global level and assign attributes to the group.

  An “Auto-Path-group” defines a set of WAN links in the Oracle SD-WAN Edge that are reachable to each other. Figure 8 displays the options for the group.

Figure 8

The options other than the group name are standard Oracle options:

- DSCP setting for the path
- Encryption enabled or disabled
- Bad loss sensitivity
- Instability Sensitive

Once the group is defined it can be applied to as many WAN Links as needed reducing the configuration time.

Figure 9 displays where to apply this option.

The group is applied at the WAN link – Service properties – Conduit Level, under the Autopath group pull down menu.

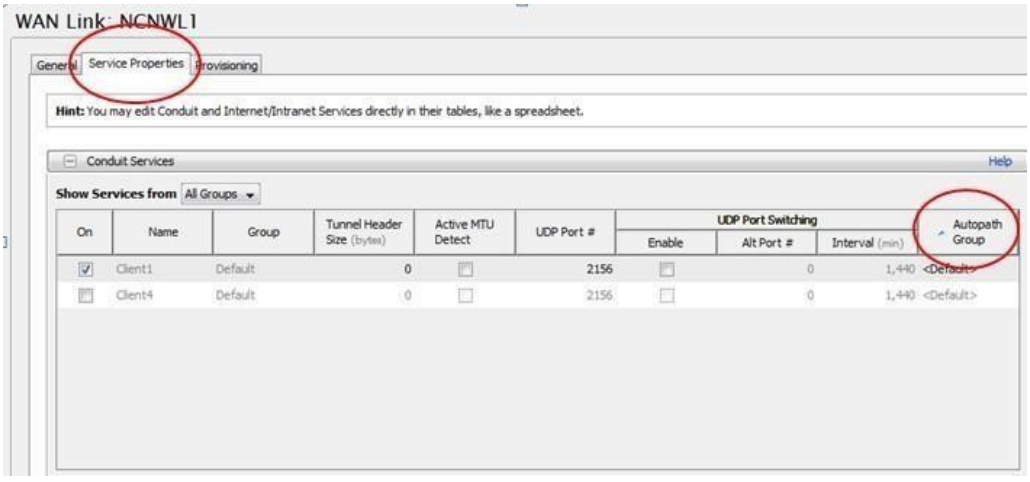


Figure 9

- SNMP
  Within the Oracle SNMP MIB there were enhancements and bug fixes added to the Oracle MIB. These changes include the following:
  - Add a Last updated date for the MIB
  - OracleNumEvents is now a gauge with events being clean up after 30 days
  - When in standby mode for HA counters are now accurate
  - All rule statistics types have changed from counters (64) to gauge
  - Dynamic Conduit statistics table is a separate table as there is only data when the conduit is in use
  - The appliance serial number is viewable from SNMP
  - The MIB now allows customers to define a “Contact”, “Location”, and or Description for an appliance. This is configured under Integrate >>Configure Events and Alerts in the web console of the appliance
  - tnStatsRuleTable now reports data correctly and will match the web console displayed data for rule statistics
  - tnStatsConduitEntry –now records BOWT (Best One Way Time), Jitter, Packets
    Lost uni- directionally
  - The ability to query Oracle version information was added to the MIB, including APNware version, OS version etc.
  - tnstatsConduitClassType values now match the web console classes as expected
  - Cisco NetFlow MIB is no longer supported
    * ARP Timeout Setting

    In the past this option was set-able through a debug level. This has now been moved to a user configurable parameter. Any previously configured ARP timeout value set using the debug level will be lost and must now be configured using the Gateway ARP Timer setting in the Configuration Editor. It defines the amount of time between ARPs for a Oracle WAN link gateway.

    This option is changed when devices do not handle the 1 second ARP value used by default in the Oracle appliance. The user can now define the number of seconds for ARP on an appliance at the global level. Figure 8 displays where to define this option.

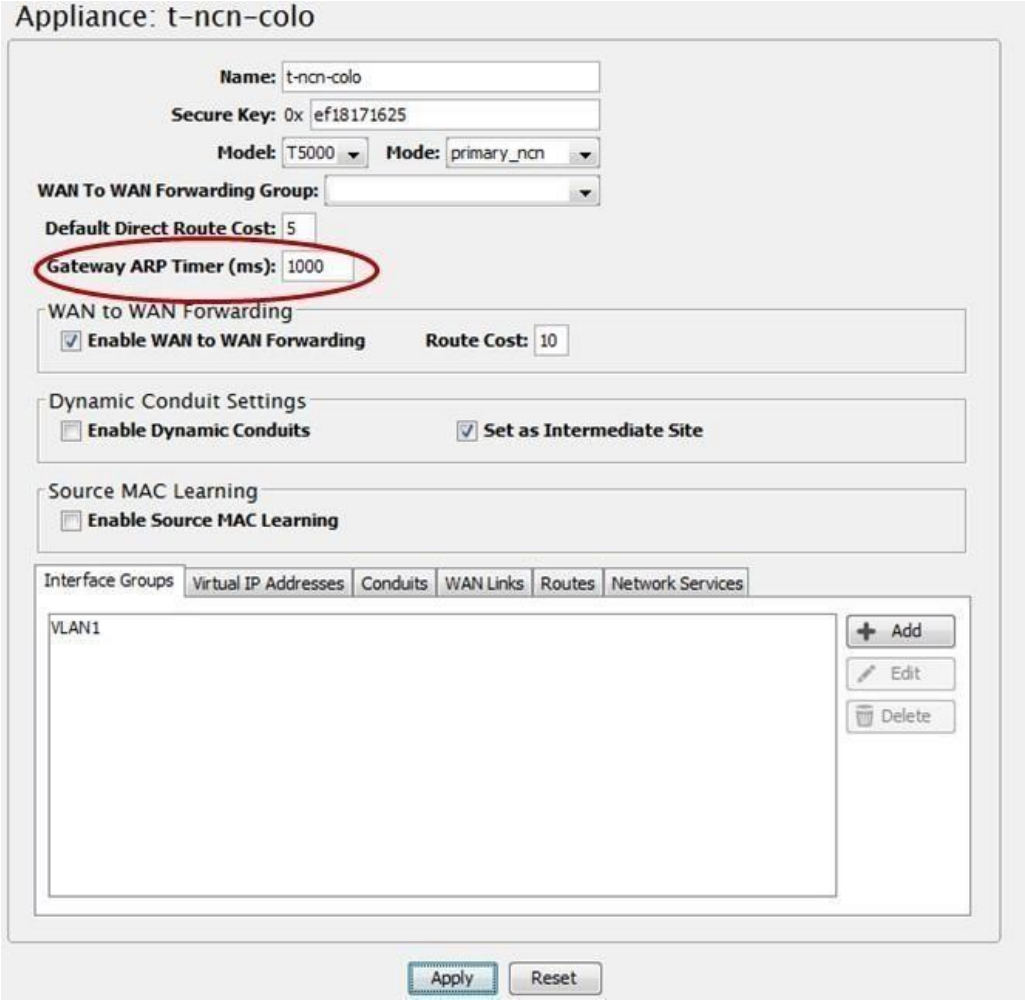


Figure 10

- WAN Link Disable Paths Option

In previous releases, a user wishing to prevent traffic from using a WAN link would have to individually disable each path that used the WAN link. Based on user requests, this has been enhanced to allow a user to select a WAN link to disable, which will automatically disable all paths on that WAN link.

- Ping Enhancements

Ping has now been enhanced to include the following new options:

- Ping count
- Packet size

In the past the system would only ping 5 times and the user could not define the size of a ping frame. This has been enhanced for troubleshooting purposes.

- Security Enhancements

Certain security enhancements are now included in APNware 3.0. These are listed below.

- Within the web console or the CLI the admin level user can now change the root level password if they know the current root password.

- Users accessing the appliance from SSH now can be authenticated by RADIUS or TACACS (Release 3.0P1)
- Additional RADIUS and TACACS server are now configurable, if the first server fails then the next server in the list will be used to authenticate the user. (release 3.0P1)

5

Release 3.1 Features

This chapter includes features and enhancements released in 3.1.

Default Configuration Parameter Change

In the Oracle SD-WAN Edge Software Release 3.1 there has been a change to a default configuration parameter. In previous software releases the Oracle SD-WAN Edge configuration editor/compiler would add in a bridge pair when configured for Fail-to-Wire (FTW) or provide a warning message that no bridge pair had been configured. Typically, the user would then add in the bridge pair definition if required. This would lead to a configuration file having the following entry for a bridge pair (as an example):

```
add bridge_pair device_one=1 device_two=2
```

This allows the Oracle appliance to bridge traffic between ports 1 and port 2, which also creates a FTW pair. The change is that now the system will NOT automatically add into the configuration file the above bridge commands. Instead the following warning will be provided to the user during validation of creating a configuration file:

```
* ---> WARNING: EC329: in define site 'Client---Test' ---> add
appliance ---> add interface_group: Interfaces in this interface
group are not part of a bridge pair. Devices connected to these
interfaces will not be reachable without the aid of an external
device.
```

To resolve the configuration warning the user should identify the site with the configuration issue and perform one of the following:

- Add in the bridge pair
- Enable Source MAC Learning

If the issue is not resolved, traffic that is considered pass--- through will not flow between port 1 and port 2. This may be required behavior, which is the reason for the default configuration change.

When upgrading from a previous release the user should not receive these warnings, but there are always exceptions. If the user does receive the warning message and has questions please contact support for clarifications on the message, configuration assistance and help in resolving the warning message.

Oracle SD-WAN Edge Configuration Editor

The new Oracle SD-WAN Edge Configuration Editor is a web--- based tool incorporated with Oracle SD-WAN Edge

Software that delivers Oracle SD-WAN Edge configuration editing capabilities, configuration compiling, and the ability to create and edit network maps. The Configuration Editor operates on Configuration Packages, which consist of an Oracle SD-WAN Edge configuration and one or more optional network maps. These

Configuration Packages can be saved, re--- opened, exported, or imported from the Configuration Editor. Unlike the legacy Configuration Editor, this new tool works without Java, making it a more secure choice for network development.

You will find the Configuration Editor on the web interface by navigating to **Manage Network**, and then **Configuration Editor**.

Once inside the Configuration Editor, you can select “New” to start building your Configuration Package or you can select “View Tutorial” to be guided through an introduction of the new tool.

The Configuration Tree (located in the left--- side pane of the Configuration Editor) is where you can add sites, define connections between those sites, and perform provisioning activities. Figure 3 illustrates an example of the Configuration Tree expanded to edit the Basic Settings for a site. All items denoted with “+” can be expanded to show more detail.

After building the network configuration, a Network Map can be customized by clicking & dragging individual sites onto the map, or by auto populating the map with all sites. Every new

Configuration Package has a default map called “Network Map” associated with it. This map can be re-named and additional maps can be created using the “+” tab.

To further customize your map, you can also add backgrounds to it. Click the gear symbol on the map and select “Set Background”. As shown in the example below, you can then place your Sites on the background where you wish. (See figure 5)

Oracle SD-WAN Edge Configuration Editor and Oracle SD-WAN Edge Aware

Oracle SD-WAN Aware is a new network management system to be release in 2014. In order to deploy Oracle SD-WAN Aware in an Adaptive Private Network, each Oracle *Mercury* Oracle SD-WAN Edge Appliance in the network must have its software updated to R3.1 or higher. The new Oracle SD-WAN Edge Configuration Editor is the

foundation of the configuration model that will allow an Oracle SD-WAN Aware Node to perform Management and Monitoring functions for the entire Oracle SD-WAN Edge. For more information on Oracle SD-WAN Aware and its implementation please contact your local Oracle representative.

6
Release 4.0 Features

This chapter includes features and enhancements released in 4.0.

256-Site Adaptive Private Networks

> **Note:**
>
> This feature is only supported for APNs in which Oracle SD-WAN Aware R1.0 GA P1 (or later) has been deployed. See *APN Software R4.0 GA Release Notes* for more details.

In Oracle SD-WAN Edge Software R4.0, a feature has been added to enable a single T5000, configured as an NCN, to create up to 256 static conduits. This doubles the previously supported scale. This will, in the general case, enable a T5000 NCN to govern an Oracle SD-WAN Edge with up to 256 Client Sites.

The T5000 can now also support a greater number of WAN Paths and Flows. See the below table for details on supported capacity for each NCN-capable appliance model:

Appliance Model	T750	T3000	T3010	T5000 (w/o Aware)	T5000 (w/ Aware)
Max Static Conduits	32	128	128	128	256
Max Dynamic Conduits	16	32	32	32	32
Max WAN Ingress Paths	216	576	576	576	1152
Max WAN Egress Paths	216	576	576	576	1152
Max Flows (TCP Term off)	64,000	256,000	256,000	256,000	512,000
Max Flows (TCP term on)	8,000	16,000	16,000	16,000	16,000
Max Public WAN Links	8	8	8	8	8
Max Private WAN Links	32	32	32	32	32

Configuration Editor

In Oracle SD-WAN Edge Software R4.0, the user will continue to be able to create and edit Oracle SD-WAN Edge configuration files from the NCN web interface via **Manage Network -> Configuration Editor**. However, the Oracle SD-WAN Edge Configuration Editor on the NCN will only support creating and editing Oracle SD-WAN Edge configuration files for APNs with up to 128 Client Sites. To scale past 128 Clients, the

Oracle SD-WAN Edge configuration file must be managed from Oracle SD-WAN Aware.

Changes to Data Storage on Oracle SD-WAN Edge Appliances

> **Note:**
>
> The following changes apply to all APNs, regardless of Oracle SD-WAN Aware deployment.

In Oracle SD-WAN Edge Software R4.0, it is guaranteed that each APNA participating in a worst-case typical 256-Site Oracle SD-WAN Edge will be able to store at least 7 days of statistical and event data.

Previously, 30 days of statistical storage was guaranteed on each APNA in an Oracle SD-WAN Edge. With the introduction of Oracle SD-WAN Aware, storage of statistical data on the APNAs is not the preferred method for network monitoring. An Oracle SD-WAN Edge equipped with Aware can offload statistics from the APNAs to the Aware Node and accumulate up to a year's worth of network-wide data.

Changes to Local Route Scale

> **Note:**
>
> The following changes apply to all APNs, regardless of Oracle SD-WAN Aware deployment.

In Oracle SD-WAN Edge Software R4.0, support for unique local routes was increased for all Oracle SD-WAN Edge appliances. Previously, unique local route scale was capped at 128 for all appliances models. See the below table for details on increased capacity for each appliance model:

Appliance Model	T510	T750	T750	T3000	T3010	T5000
Max Unique Local Routes	512	512	512	512	2048	2048

7

Release 4.1 Features

This chapter includes features and enhancements released in 4.1.

Oracle Virtual Appliance CT800

Oracle SD-WAN Edge Software R4.1 supports the deployment of a Oracle Virtual Appliance CT800 within Amazon Web Services (AWS). This feature allows the user to provide Conduit connectivity to the AWS cloud. Using the Oracle CT800 solution, users will be able to leverage the typical Oracle features providing a more reliable and secure connection to the AWS cloud. The solution also allows users to take advantage of the quality of service offering provided today by Oracle Conduit. As cloud demands grow, users can leverage Oracle Conduits to allocate WAN bandwidth to more critical applications when demand dictates.

Oracle CT800 features within AWS:

- Supports up to 100 Mbps of Conduit throughput
- Supports Static and Dynamic Conduits
- Supports Internet and AWS Direct Connect WAN services
- Supports typical FTB configurations
- Supports configuration of WAN/LAN/Management ports as needed

Oracle CT800 requirements within AWS:

- AWS EC2 Instance Type: c3.2xlarge
- # of vCPUs: 8
- RAM: 15 GB
- Storage: 160 GB
- # Network Interfaces: 2[1]

For installation details, see the *Oracle Virtual Appliance CT800 Getting Started Guide*.

As your cloud services grow, deploy the Oracle CT800 for a more robust and secure connection from your enterprise network to services in the AWS cloud.

MOS Estimation

In conjunction with Oracle SD-WAN Aware 1.1, Oracle SD-WAN Edge Software R4.1 supports the ability to provide Mean Opinion Score (MOS) estimates for defined applications traversing the WAN via a Oracle Conduit. This will assist the user in problem isolation for voice or other critical traffic flowing across the Conduits.

[1] At minimum, the Oracle CT800 requires 2 Network Interfaces (1 for MGT and 1 for LAN/WAN). However, the CT800 can support up to 4 Network Interfaces.

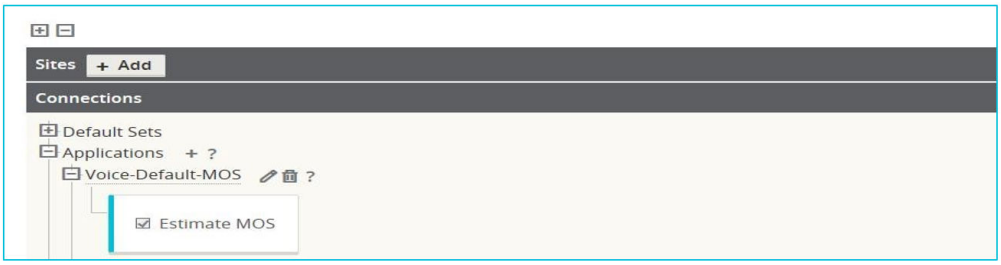
It is important to note that Oracle MOS estimation is based on WAN Egress flow processing. As traffic matching a defined rule is received at the WAN Egress side of the Conduit, the values for calculating the MOS are saved in the database file for reporting in Oracle SD-WAN Aware. The MOS calculation is based on the E-Model or ITU-T G.107. The following describes how a user would enable the MOS capability in the Oracle SD-WAN Edge Configuration Editor, then view calculated MOS values in Oracle SD-WAN Aware.

How to Configure

1. Create an Application with "Estimate MOS" Enabled

In the NCN web console, under **Manage Network**, and then **Configuration Editor**:

- Open a configuration to edit (or create a new configuration)
- Navigate to **Connections -> Applications** and select the "+" to add a new application
- Give the new application a name and make sure that "Estimate MOS" is enabled



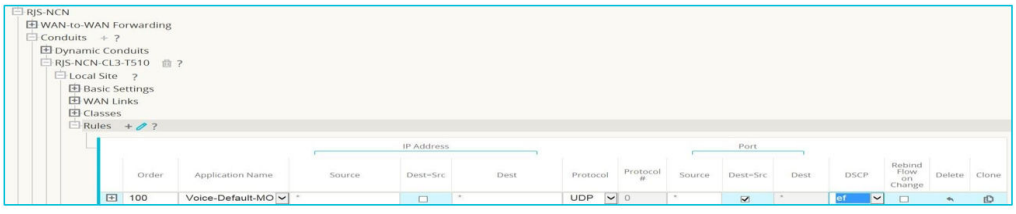
1. Add the Application to a Rule for a Static Conduit

In the NCN web console, under **Manage Network -> Configuration Editor**:

- Open a configuration to edit (or create a new configuration)
- Navigate to **Connections -> [Site Name] -> Conduits -> [Conduit Name] -> Local Site**

Under the **Rules** section, add a new rule with the previously-defined Application Name.

> **Note:**
>
> The rule can be added to a Default Set or to a specific Conduit.



3. Verify the Traffic Matches the Defined Rule

In the web console, under **Monitor -> Flows**:

- Review relevant traffic flows to ensure they are matching the defined rule

How to View

Once an application has been configured with "Estimate MOS" enabled, calculated MOS values for the application can be viewed in Oracle SD-WAN Aware. MOS values are calculated over one-minute intervals. The user can view both Average Oracle SD-WAN Edge MOS and Lowest Oracle SD-WAN Edge MOS for each interval.

- **Average APN MOS:** Calculated using the average latency for packets observed on WAN Egress that match the application over one minute, and an average loss percentage (sampled every second) for all flows matching the application over multiple minutes.
- **Lowest APN MOS:** Calculated using the average latency for packets observed on WAN Egress that match the application over one minute, and an average loss percentage (sampled every second) for all flows matching the application over multiple minutes.

To generate a graph of MOS values, in the Oracle SD-WAN Aware web console navigate to **Monitor > Graphs -> [Site Name] -> Conduits -> Applications -> Application Name -> [Average APN MOS | Lowest APN MOS]**.

To generate a report of MOS values, in the Oracle SD-WAN Aware web console navigate to **Monitor > Reports -> Applications**.

Security Enhancements

Oracle SD-WAN Edge Software R4.1 supports several security enhancements. Although not required for deployments, these features are available for environments that require an additional level of encryption or security in general.

Summary

A summary of these features is provided below. See *APN Security Technical Paper* for more details. Each feature is configurable at a global level, for the entire Adaptive Private Network (Oracle SD-WAN Edge).

256-bit AES Encryption

256-bit AES Encryption is now supported, in additional to the previously supported 128-bit AES Encryption. 256-bit AES Encryption is *not* enabled by default.

Enhanced Encryption Key Generation/Rotation

Per-session encryption keys are generated and automatically rotated (when Encryption Key Rotation is enabled) using an Elliptic Curve Diffie-Hellman algorithm. Encryption Key Rotation is enabled by default.

Extended Packet Authentication Trailer

To provide users with the ability to have strong message authentication, an optional trailer inside the encrypted payload can now be enabled. By default, this optional trailer is composed of a 4-byte checksum of the unencrypted packet data, which acts like a standard Hashed Message Authentication Code (HMAC). While a standard

HMAC would impact performance significantly, this checksum trailer provides a similar benefit while minimizing processing overhead. If use of a standard HMAC is required, the optional trailer can be configured to use a 16-byte SHA-256 HMAC in place of the 4-byte packet checksum.

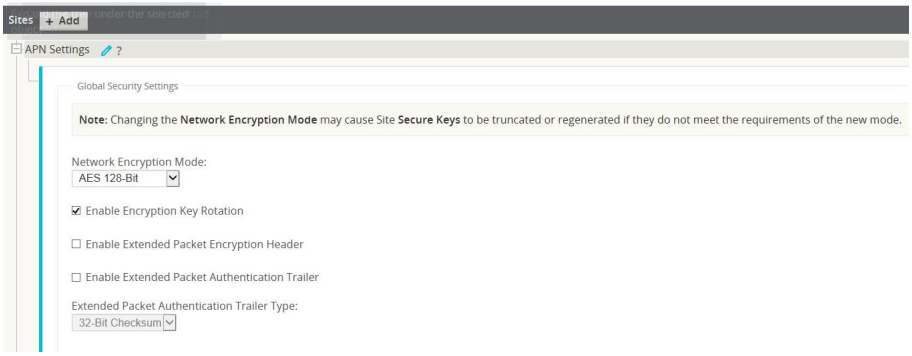
Extended Packet Encryption Header

To provide users with the ability to have the highest level of packet uniqueness and protection against Frequency Analysis, an optional 16-byte counter can now be prefixed inside the encrypted payload to act as a rotating, cryptographically random Initialization Vector.

How to Configure

In the NCN web console, under **Manage Network -> Configuration Editor**:

- Open a configuration to edit (or create a new configuration)
- Navigate **Sites -> Settings**



> **Note:**
>
> Enabling some of the enhanced security options could impact performance. Contact your Oracle Sales representative or Oracle Support for help in understanding the potential performance impact.

SNMP Polling for ARP Table

Oracle SD-WAN Edge Software R4.1 supports retrieval of ARP entries and associated statistics via SNMP polling. Polling will retrieve the data for existing ARP table entries, along with associated interfaces and statistics for each entry. The data for this SNMP entry is updated once a minute on the Oracle SD-WAN Edge Appliance.

For more data on this specific MIB enhancement please review the Oracle MIB and from the Oracle SD-WAN Edge Appliance web console under **Integrate -> Download/ View Oracle MIB**.

Appliance Settings from Aware

In conjunction with Oracle SD-WAN Aware R1.1, Oracle SD-WAN Edge Software R4.1 supports the ability to configure appliance settings from Oracle SD-WAN Aware.

Appliance settings include options associated with DNS, NTP, Time Zone, User Authentication, FTP server configuration, Notification settings,

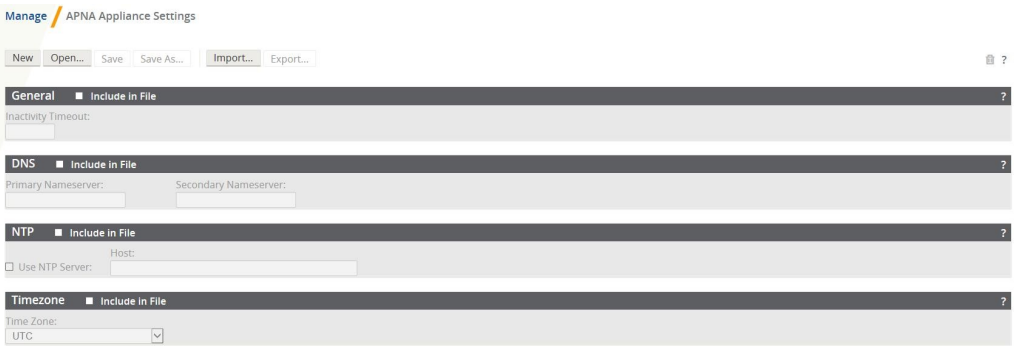
Netflow, etc. These options are not governed by the Oracle SD-WAN Edge Configuration Editor. With Oracle SD-WAN, Aware R1.1, these settings can now be pushed from Oracle SD-WAN Aware to any user-selected group of Oracle SD-WAN Edge Appliances in the network. Additionally, templates of appliance settings can be created, edited, and saved on Oracle SD-WAN Aware to streamline future Oracle SD-WAN Edge Appliance installs.

From a deployment perspective, the following should be considered:

- Settings defined locally will override settings that were previously pushed from Oracle SD-WAN Aware
- Settings pushed from Oracle SD-WAN Aware will override settings that were previously defined locally
- Settings pushed from Oracle SD-WAN Aware will take effect once received on the target Oracle SD-WAN Edge Appliance(s)
- Settings pushed from Oracle SD-WAN Aware are received on the target Oracle SD-WAN Edge Appliance(s) via the management interface
- Settings can only be pushed from Oracle SD-WAN Aware to those Oracle SD-WAN Edge Appliances that are reachable
  (i.e. displayed on the **Manage -> Discovery** screen)
- Blank settings in a template will not be pushed to the Oracle SD-WAN Edge Appliance(s)

In the Oracle SD-WAN Aware web console, under **Manage -> Appliance Settings**:

- Select "New" to create a new Appliance Settings template
- For each section, select "Include in File" to edit the options in that section
- Once all desired options have been set, select "Save" to save the template
- Select "Export" to export the template to the desired Oracle SD-WAN Edge Appliance(s)



8
Release 4.2 Features

This chapter includes features and enhancements released in 4.2.

Non-Resetting Configuration Updates

Oracle SD-WAN Edge Software R4.2 now supports all network configuration updates as non-resetting updates. This process change is inherent in all configuration updates and does not require any specific command to be enabled. When a new Oracle SD-WAN Edge Configuration is applied to the network via Change Management, the Oracle Service will not be forced to restart for any combination of configuration parameter changes. In addition, the web interface will provide detailed information on the time required for a staged configuration update to be performed on the network, allowing the user to understand the potential impact of an update to their Appliances and to their network as a whole.

Configuration Updates

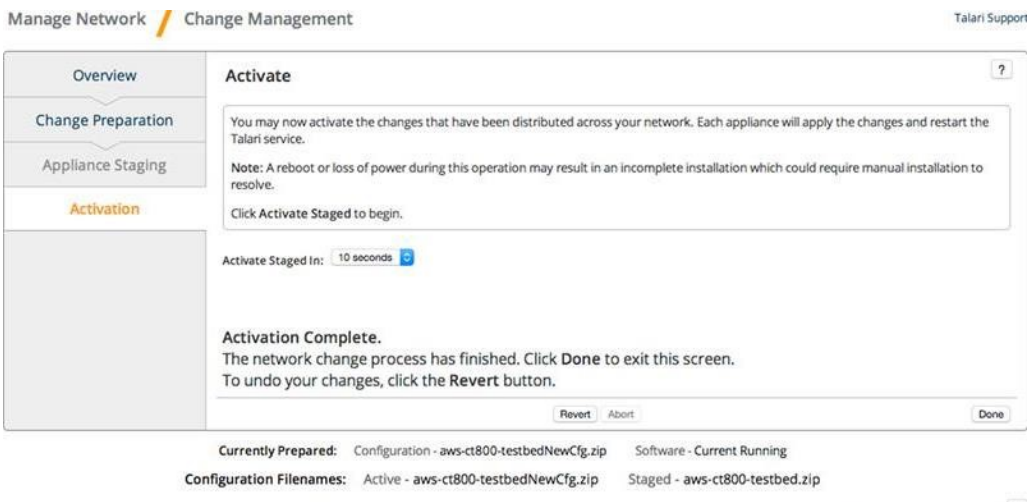
Under **Manage Network -> Change Management** on the web interface of the Network Control Node (NCN), there are two new columns, *Traffic Interruption - Expected* and *Traffic Interruption - Actual*. These columns display values that indicate the following for each Site in the Oracle SD-WAN Edge:

Traffic Interruption - Expected: The expected worst traffic interruption time for the Site, based on the difference between the active and staged configurations. For more detail on the impact to each Conduit, refer to APN_traffic_impact.log.

- 0 sec - No service interruption for this Site
- <1 sec - Traffic interruption time will be less than 1 second
- <1 min - Traffic interruption time will be less than 1 minute
- <3 min - Traffic interruption time will be less than 3 minutes (only relevant for software updates, which still require a restart of the Oracle Service)
- Loc Chg Mgt - Package must be applied via that Site's local change management

Traffic Interruption - Actual: The time it took to perform a configuration or software update at the Site. This does not include the time it took for full network convergence during an update. Updates to Sites may occur in parallel.

- *N* ms/s - Actual traffic interruption time at the Site when the update was performed
- Err - An error occurred when performing the update



Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
NCN-ct800-ncn	CT800		R4_2_QA_D1_11132014	21:52 on 11/21/14	R4_2_QA_D1_11132014	19:31 on 11/21/14	0 sec	0 ms	active / staged
AU-ct800-AU	CT800		R4_2_QA_D1_11132014	21:52 on 11/21/14	R4_2_QA_D1_11132014	19:31 on 11/21/14	0 sec	0 ms	active / staged
BRA-ct800-BRA	CT800		R4_2_QA_D1_11132014	21:52 on 11/21/14	R4_2_QA_D1_11132014	19:31 on 11/21/14	0 sec	0 ms	active / staged
Client-ct800-client	CT800		R4_2_QA_D1_11132014	21:52 on 11/21/14	R4_2_QA_D1_11132014	19:31 on 11/21/14	0 sec	0 ms	active / staged
GEO-ct800-GEO	CT800		R4_2_QA_D1_11132014	21:52 on 11/21/14	R4_2_QA_D1_11132014	19:31 on 11/21/14	0 sec	0 ms	active / staged
IRL-ct800-IRL	CT800		R4_2_QA_D1_11132014	21:52 on 11/21/14	R4_2_QA_D1_11132014	19:31 on 11/21/14	0 sec	0 ms	active / staged
SNG-ct800-SNG	CT800		R4_2_QA_D1_11132014	21:52 on 11/21/14	R4_2_QA_D1_11132014	19:31 on 11/21/14	0 sec	0 ms	active / staged

From the above, the expected traffic interruption time for the configuration update was 0 seconds (i.e. no expected interruption) for each Site, and that the actual interruption time met this expectation. Certain configuration updates will impact traffic for a period of time. When this is the case, the expected traffic interruption time will show the maximum interruption time that can be expected in the form of <1 sec, <1 min, or <3 min. Prior to activating a staged configuration update, the user can use the expected traffic interruption time for the staged configuration to determine if a maintenance window is required for the update. Please note that an appliance with traffic load may require more time to complete the update process.

Impact of Common Configuration Updates

The expected traffic interruption times for various common configuration changes are outlined below. These are estimates; the actual interruption times may be less and will be displayed in the web interface and logged for help with future planning.

No Interruption:

- NCN mode (primary, secondary) is changed
- Gateway ARP Timer is changed or Proxy ARP is enabled/disabled
- WAN-to-WAN Forwarding is enabled/disabled
- Intermediate Node attribute is enabled/disabled
- The attributes of a Route, Rule, Class or Autopath are changed
- Maximum Dynamic Conduits is changed or Dynamic Conduit Thresholds are changed
- WAN Link Conduit, Intranet, or Internet usage is changed (but not added/removed)
- Remote Site that has no Conduit to the local Site is added/removed
- Encryption key is changed or key rotation is enabled/disabled

Interruption of Less Than 1 Second:

- Site is added/removed or Site name is changed
- Conduit is added/removed/changed
- WAN Link or WAN Path is added/removed/changed
- Appliance Name is changed
- HA attributes are changed
- Interface Group is added/removed/changed
- WAN-to-WAN Forwarding Group is changed
- Dynamic Conduits are enabled/disabled
- WAN Link Conduit, Intranet, or Internet usage is added/removed
- Source MAC Learning is enabled/disabled
- Extended Packet Encryption Header is enabled/disabled
- Extended Packet Authentication Trailer is enabled/disabled or Trailer Type is changed

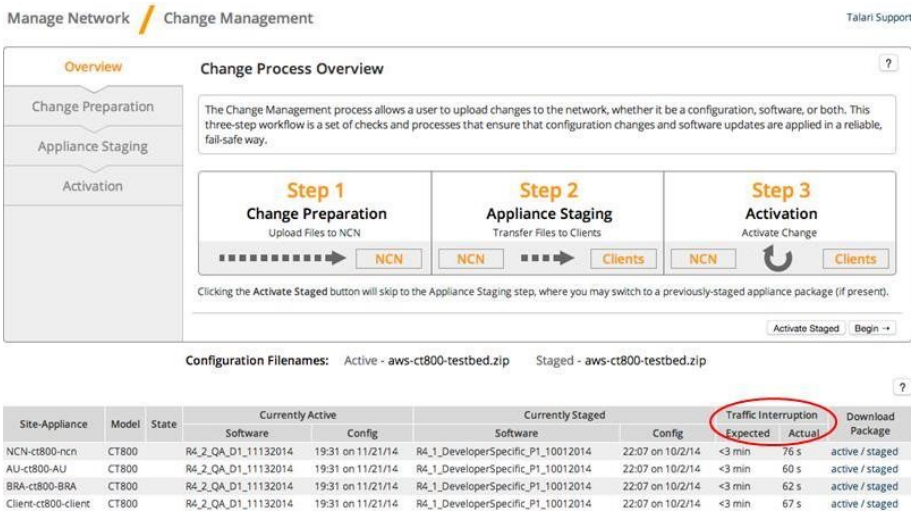
Interruption of Less Than 1 Minute:

- Encryption mode for the Oracle SD-WAN Edge is changed
- Any routing table update change when Local Route Eligibility is enabled at a site.

WAN Path Encryption is enabled/disabled

Software Updates

As in previous releases, software updates will require a restart of the Oracle Service. The new display will instruct the user of the expected traffic interruption time. The following screen shows the expected and actual traffic interruption times for a software update:



Site-Appliance	Model	State	Currently Active		Currently Staged		Traffic Interruption		Download Package
			Software	Config	Software	Config	Expected	Actual	
NCN-ct800-ncn	CT800		R4_2_QA_D1_11132014	19:31 on 11/21/14	R4_1_DeveloperSpecific_P1_10012014	22:07 on 10/2/14	<3 min	76 s	active / staged
AU-ct800-AU	CT800		R4_2_QA_D1_11132014	19:31 on 11/21/14	R4_1_DeveloperSpecific_P1_10012014	22:07 on 10/2/14	<3 min	60 s	active / staged
BRA-ct800-BRA	CT800		R4_2_QA_D1_11132014	19:31 on 11/21/14	R4_1_DeveloperSpecific_P1_10012014	22:07 on 10/2/14	<3 min	62 s	active / staged
Client-ct800-client	CT800		R4_2_QA_D1_11132014	19:31 on 11/21/14	R4_1_DeveloperSpecific_P1_10012014	22:07 on 10/2/14	<3 min	67 s	active / staged

From the above, the expected traffic interruption time for the software update was less than 3 minutes for each Site, but that the actual interruption time was less than 100 ms. The user traffic would have been impacted for a bit longer than this as Conduits

between the Sites must be operational or in the “GOOD” state before user traffic can flow across them.

9
Release 4.3 Features

This chapter includes features and enhancements released in 4.3.

Configure Private MPLS WAN Links

This feature simplifies creating Oracle SD-WAN Edge configurations when adding a Multiprotocol Layer Switching (MPLS) WAN Link. Previously, users created a WAN Link for each MPLS queue. Each WAN Link required a unique Virtual IP Address (VIP) to create the WAN Link and a unique Differentiated Services Code Point (DSCP) tag corresponding to the provider's queuing scheme. Once users defined a WAN Link for each MPLS queue, they defined the Intranet Service to map to a specific queue.

In Oracle SD-WAN Edge 4.3, a new MPLS specific WAN Link definition (i.e., Access Type) is available. Once the user selects the new Access Type, **Private MPLS,** they can define MPLS queues associated with the WAN Link. This allows users to define a single VIP with multiple DSCP tags that correspond to the provider's queuing implementation for the MPLS WAN Link. This also allows users to map the Intranet Service to multiple MPLS Queues on a single MPLS WAN Link.

> **Note:**
>
> If you have existing MPLS configurations and would like to implement the **Private MPLS** Access Type, please contact Oracle Support for assistance.

The high-level steps to configure this enhancement from within the Oracle SD-WAN Edge Configuration Editor are:

1. Define the WAN Link Access Type as **Private MPLS.**
2. Define the MPLS Queues corresponding to the Service Provider MPLS queues.
3. Enable the WAN Link for Conduit Service (enabled by default for Private MPLS WAN Links).
4. From **Conduit WAN Link**, assign an Autopath group.

> **Note:**
>
> If the Autopath Group is assigned from the WAN Link level, Oracle SD-WAN Edge will build paths automatically between the NCN and Client MPLS Queues based on matching DSCP tags. If the Autopath Group is assigned from the MPLS Queue level, Oracle SD-WAN Edge will build paths automatically regardless of whether the DSCP tags match.

1. Ensure that the same Autopath Group is configured at the NCN and Client.

2. Verify that the Paths for the WAN Link are built automatically.
3. Assign Intranet Service to a specific queue if needed.

> **Note:**
>
> The Oracle configuration may not have a one-to-one mapping for provider-based queues. This is based on specific deployment scenarios.

> **Note:**
>
> You cannot create Autopath Groups between different Private Access Types. For instance, you cannot create Autopath Groups between a Private Internet Access Type and a Private MPLS Access Type.

Add Private MPLS WAN LINK

In the Oracle SD-WAN Edge Configuration Editor, once users click **+ (Add)** under **Sites [Site Name] WAN Links**, the **Add WAN Link** pop-up appears.

Figure 1 illustrates how to configure the new WAN Link Access Type of **Private MPLS**.

Selecting a WAN Link Access Type of **Private MPLS** defines the Basic Settings for the WAN Link. The configurable settings include the physical (permitted) rate for WAN Ingress and WAN Egress. The MPLS Queues cannot exceed the physical (permitted) rate values. There are also no Audit errors if the sum of all MPLS Queues is below the WAN Link physical rates. See Figure 2 for a screen shot of the defined MPLS Queues.

Figure 2: Defined MPLS Queues

Figure 2 illustrates the Basic Settings for a Private MPLS WAN Link. Under the Basic Settings, there is now a new MPLS Queues Tab. Users click **+ Add** to add specific MPLS Queues. These should correspond with the queues defined by the Service Provider.

Users must define the following attributes for the MPLS Queues option:

- **MPLS Queue Name**
- **DSCP Tag:** This setting should correspond to the Service Provider's DSCP tag setting for the queue.
- **Unmatched:** When enabled, any frames arriving that do not match defined tags within the configuration file are mapped to this queue and the bandwidth defined for this queue.

- **WAN Ingress Permitted Rate:** The amount of bandwidth that Oracle devices are permitted to use for upload, which cannot exceed the defined physical upload rate of the WAN Link.
- **WAN Egress Permitted Rate:** The amount of bandwidth that Oracle devices are permitted to use for download, which cannot exceed the defined physical download rate of the WAN Link.

When users expand the MPLS Queue definition (by clicking the **+**), additional options appear.

These options include:

- **Tracking IP Address**: WAN Link tracking address
- **Congestion Threshold:** The defined amount of time for congestion (in microseconds) after which the MPLS Queue will throttle packet transmission to avoid additional congestion. When congestion exceeds the set Threshold, Oracle will back off the sending rate.
- **Eligibility:** The MPLS Queue's eligibility to process specific classes of traffic. When eligibility is disabled for a specific class of traffic, that class of traffic is unlikely to route through the MPLS Queue unless network conditions require it.

Users should configure the MPLS Queues that correspond to the existing Service Provider WAN Link queue definitions.

Since this is a new WAN Link Access Type, any existing MPLS WAN Links that are configured prior to Oracle SD-WAN Edge 4.3 are not impacted. Users should discuss migrating to the 4.3 features if desired, but migration is not required. Please contact your implementation team or support for additional recommendations when migrating to the new WAN Link Access Type.

Define WAN Link Basic Properties (Private MPLS)

Once the Private MPLS WAN Link with its MPLS Queues is defined, users should assign an Autopath Group to the WAN Link under a specific Conduit definition. Go to **Connections**

[Site Name] WAN Links [MPLS WAN Link Name] Conduits [Conduit Name] [Local Site] WAN Links and click Edit (✎). Click the **Autopath Group** drop-down menu and choose from the available groups. By default, MPLS Queues inherit the Autopath Group assigned to the MPLS WAN Link. You may choose to set the individual MPLS Queues to **Inherit** the chosen **Autopath Group** or choose an alternate from the **Autopath Group** dropdown menu for each MPLS Queue. Figure 3 illustrates this process.

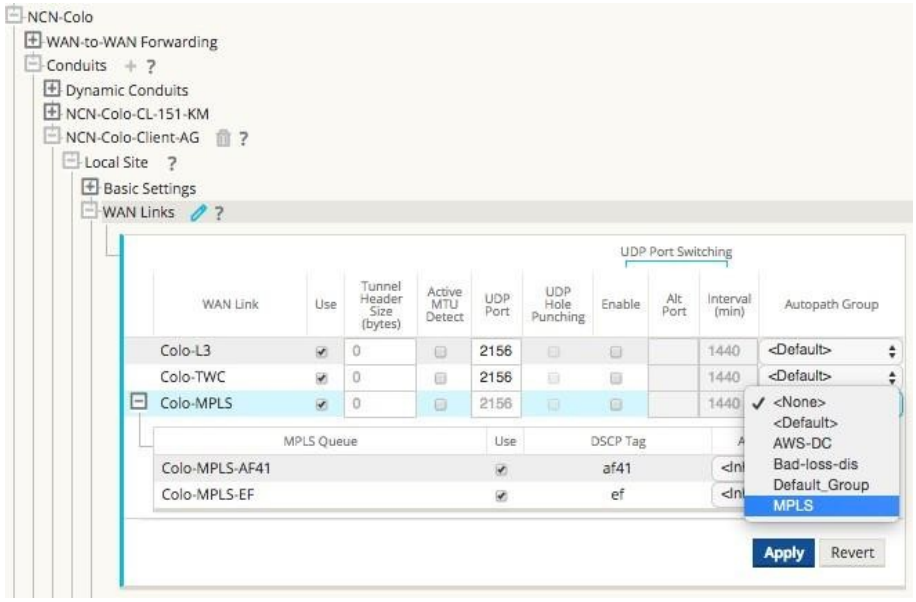


Figure 3: Conduit WAN Link Autopath Group Drop-Down Menu

> **Note:**
>
> If there is not a one-to-one mapping, based on DSCP tag, between queues at the local site and the remote site, users must map MPLS Queues to specific Autopath Groups. Inheriting an Autopath Group from the MPLS WAN Link will only automatically generate paths between queues with matching DSCP tags.

Assign Autopath Group to Conduit-WAN Link

Figure 4 and Figure 5 illustrate that the Autopath Group defined is the same for the NCN and Client appliance. This allows the system to build the Paths automatically. Figure 5 displays the NCN and Client settings. At the NCN site users can also expand the WAN Link associated with the conduit.

Verify Autopath Creation

Once users build the Path, the configuration is complete and they can follow the Change Management procedure to activate the configuration. Figure 6 illustrates the automatically generated paths.

View Permitted Rate and Congestion for WAN Links

In Oracle SD-WAN Edge 4.3, the Web console now allows users to view the permitted rate for WAN Links and WAN Link Usages and whether a WAN Link, Path, or Conduit may be in a congested state. In past Oracle SD-WAN Edge releases, this information was typically only available in Oracle SD-WAN Edge log files and via CLI-based commands. These options are now available in the Web console to assist users in problem isolation and troubleshooting.

View Permitted Rate

Permitted Rate is the amount of bandwidth that a particular WAN Link, Conduit Service, Intranet Service, or Internet Service is permitted to use at a given point in time. The permitted rate for a WAN Link is static, and is defined explicitly in the Oracle SD-WAN Edge configuration. The permitted rate for a Conduit Service, Intranet Service, or Internet Service will fluctuate over time, in response to congestion, user demand, and Fair Shares, but will always be greater than or equal to the Minimum Reserved Bandwidth for the Service.

Go to **Monitor Statistics** and select **WAN Link Usage** from the **Show** drop-down menu to display the page in Figure 7 including the **Permitted Kbps** information.

Under **Local WAN Links** users can see the configured permitted rates for each WAN Link defined at the local site. For example, RJS-NCN-WL2 has a configured permitted rate of 100Mbps. The **Usages and Permitted Rates** table displays the actual, real-time permitted rates for each Service that the WAN Link is used for (individual Conduit Services and combined Internet-Intranet Services). This information can assist users in troubleshooting a specific WAN Link problem or throughput associated with a WAN Link.

View Congestion

Oracle SD-WAN Edge 4.3 enhances the Web console to display a WAN Egress congestion state if it occurs within the site. There are three states associated with congestion:

- **UNKNOWN**: The WAN Link, Path, or Conduit is down so there is no congestion state
- **NO**: The WAN Link, Path, or Conduit is not congested
- **YES**: The WAN Link, Path, or Conduit is congested

In addition to the Web console displaying a congested state, there are also event notifications that users can enable and that the appliance generates when the congested state occurs. The event options include:

- **WAN_LINK_CONGESTION**: A WAN Link has become congested or un-congested
- **USAGE_CONGESTION**: A Conduit has become congested or un-congested

> **Note:**
>
> Congestion is detected if packets in the WAN are delayed more than 100ms from the expected time of arrival.

To view congestion on a WAN Link, go to **Monitor Statistics** and choose **WAN Link Usage** from the **Show** drop-down menu. See Figure 8 for a screen capture of a congested WAN Link. The congested WAN Link is highlighted in red with the Congestion state as **YES**.

To view congestion on a Path, go to **Monitor Statistics** and choose **Paths** from the **Show** drop-down menu. See Figure 9 for a congested Path.

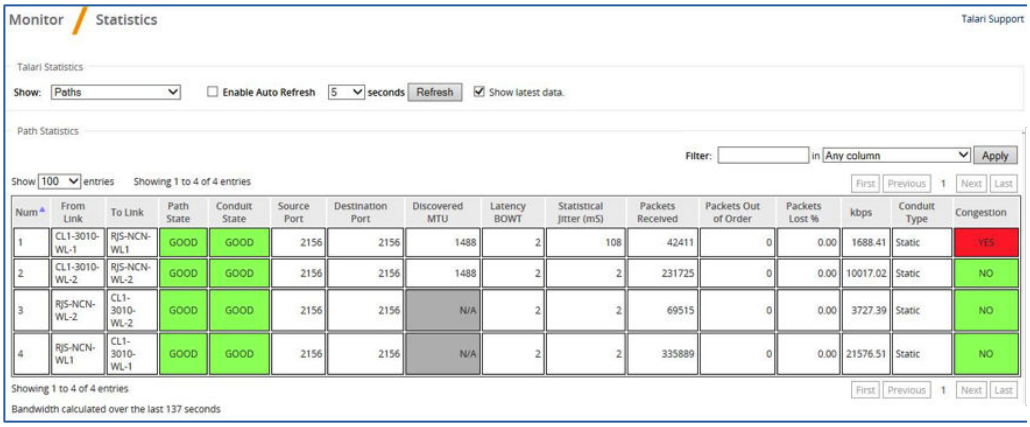


Figure 9: Congested Path

As illustrated in Figure 9, congestion can occur in one direction of a Path. In the above Oracle SD-WAN Edge, congestion is occurring from CL1-3010-WL1 RJS-NCNWL1. So, congestion (WAN Egress) is occurring from the Client site to the NCN site. Figure 9 was taken at the Client site. The Oracle NCN uses Oracle encapsulation to notify the Client appliance that it has congestion on the defined Path above. With this information, the Client appliance can also display that congested state.

To view congestion on a Conduit, go to **Monitor Statistics** and choose **Conduit** from the **Show** dropdown menu.

> **Note:**
>
> If a WAN Link, Path, or Conduit is congested, the Web console will display this state while the congestion persists and for an additional 15 seconds after the congestion clears. This is to provide users the ability to troubleshoot the event when it occurs.

Configuration Versioning

To reduce the chance of an Oracle SD-WAN Edge misconfiguration from multiple users exporting changes from the Configuration Editor in Oracle SD-WAN Edge, Oracle introduced Configuration Versioning in release 4.3.

The Oracle SD-WAN Edge Configuration Editor applies versioning metadata to configuration packages when the user saves a configuration or exports a configuration to Change Management. Upon export to Change Management, Oracle SD-WAN Edge detects whether the configuration the user is attempting to export is derived from the running configuration. If the configuration is not derived from the current, running configuration, Oracle SD-WAN Edge presents the warning illustrated in Figure 10.

Figure 10: Export Configuration Dialog with Warning Message

The user can choose to proceed and overwrite the running configuration or cancel the Export.

Support for Installing User-Generated Certificates on Appliances

Currently, all major browsers present a warning screen to users when they attempt to access the Web console of an appliance for the first time stating that the SSL certificate is invalid. Some browsers allow the user to add an exception to avoid the warning in the future, but the exception is specific to the appliance, the workstation, and the browser. The certificate is invalid for two reasons:

- The identity on the certificate does not match the URL of the appliance (typically an IP address).

- An authority trusted by the user's system did not sign the certificate.

Oracle SD-WAN Edge 4.3 allows users to upload generated certificates to the Web console of the appliance.

The user should generate the certificate for the appliance's IP address and the appropriate Certificate Authority should sign the certificate prior to installation. If the certificate is generated properly, it will be trusted by the systems on the user's network.

> **Note:**
>
> For User-Generated certificates, there is also a root certificate that is loaded into the user's Web browser.

To upload the certificate, log into the appliance and proceed to **Manage Appliance HTTPS Certificate**. Users can upload a certificate and key file as required. There is no procedure to delete a certificate that was uploaded, but the user can regenerate a Oracle certificate by selecting **Regenerate HTTPS Certificate** as illustrated in Figure 11.

Figure 11: HTTPS Certificate

10

Release 4.4 Features

This chapter includes features and enhancements released in 4.4.

LAN GRE Tunnels

Oracle SD-WAN Edge 4.4 introduces LAN GRE Tunnels and allows you to configure Appliances to terminate GRE

Tunnels on the LAN. For example, in certain environments it may be advantageous to create a GRE Tunnel between a Appliance and a LAN side Linux host or router. This allows the Appliance to pass Conduit traffic into a GRE Tunnel terminated on the host or router for forwarding or processing. LAN GRE Tunnels can be used in the AWS environment where no Layer 2 support is available to simplify the deployment process.

To configure a LAN GRE Tunnel:

1. Log into your Appliance's web console.
2. Click on **Manage Network**, and then **Configuration**.
3. Open **Sites** → **[Site Name]**, and then **LAN GRE Tunnels** and click **+** to add a new tunnel.
4. Enter a **Name** and select a **Source IP** from the list of configured Virtual IPs.
5. Enter the tunnel's **Destination IP** and prefix (e.g., 10.4.0.20).
6. Click the **Checksum** checkbox if a checksum in the header is required.
7. Enter the **Keepalive Period** in seconds.

> **Note:**
>
> If the Keepalive Period is set to **0**, no keepalive packets will be sent, but the tunnel will stay up even if the other end of the tunnel is unreachable.

1. Enter the number of **Keepalive Retries**.

> **Note:**
>
> This is the number of times that the Appliance sends keepalive packets without a response before it brings the tunnel down.

1. Click **Apply**.

> **Note:**
>
> If the packet size including the GRE header exceeds the MTU and if "don't fragment" is set in the IP header, the packet will be dropped, but if "don't fragment" is **not** set in the IP header, the packet will be fragmented.

Figure 1: Create a LAN GRE Tunnel

Monitor LAN GRE Tunnels

To monitor configured LAN GRE Tunnels, go to **Monitor**, and then **Statistics** and choose **LAN GRE Tunnel** from the **Show** drop-down menu.

Figure 2: LAN GRE Statistics

IPsec Encryption in Conduit

Oracle SD-WAN Edge 4.4 introduces the ability to secure Conduit user data with IPsec encapsulated by the Oracle Reliable Protocol (TRP). This is executed using a 140-2 Level 1 FIPS-certified IPsec cryptographic library using Suite B algorithms and 256-bit ECP.

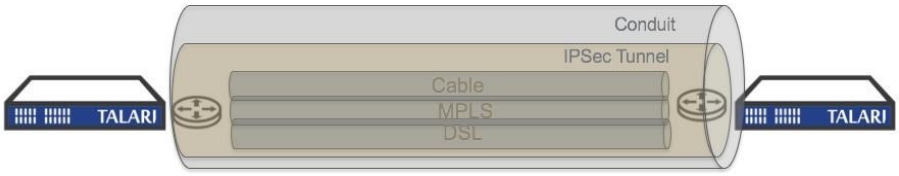


Figure 3: IPsec Encryption in a Conduit To implement IPsec Encryption on a Conduit:

1. Log into your Appliance's web console.
2. Click on **Manage Network**, and then **Configuration**.
3. Open **Connections** → **Default Sets** → **Conduit Default Sets** → **[Site Name]**, and then **IPsec Settings**.
4. Click the edit icon (▬) and click the checkbox next to **Secure Conduit User Data with IPsec** to enable IPsec on the conduit.
5. Choose **ESP**, **ESP+Auth**, or **AH** from the **Tunnel Mode** drop-down menu.
6. If the Tunnel Mode is ESP or ESP+Auth, choose **AES 128-bit** or **AES 256-bit** from the **Encryption Mode** drop-down menu.
7. If the Tunnel Mode is AH, choose **SHA1** or **SHA-256** from the **Hash Algorithm** drop-down menu.
8. Click **Apply**.

Figure 4: Configure IPsec on a Conduit

Monitoring IPsec

To monitor Conduits secured with IPsec go to **Monitor**, and then **Statistics** and choose **Conduit** from the **Show** drop-down menu. The **IPsec Tunnel State** column indicates whether a Conduit's IPsec tunnel state is **GOOD**, **DEAD**, or **NEG** (tunnel is being negotiated).

Figure 5: IPsec Tunnel State

Path State Configurability and Monitoring

Oracle SD-WAN Edge 4.4 allows users to control when a Path is marked bad and how long a bad Path is kept on probation. It also gives users greater visibility into why a bad or dead Path is in its current state.

1. Oracle SD-WAN Edge 4.4 gives you greater control of the Bad Loss Sensitivity feature with the ability to manually configure the threshold for loss before a Path is marked BAD.
2. Now you can manually configure Silence Period, or the time that must elapse before a Path is marked BAD after packets are determined to be overdue.
3. Now you can also manually configure the Path Probation Period, or the time that must elapse before a Path is marked GOOD, after the symptom (e.g., loss or silence) clears.

The following new attributes are configurable:

- **Bad Loss Sensitivity**: The Path state transitions from **GOOD** to **BAD** when a specified amount of loss is observed. When set to **On**, loss is evaluated based on an internal formula. When set to **Custom**, loss is evaluated based on user-defined threshold. When set to **Off**, loss does not affect Path state.
- **Percent Loss Over Time**: Designate the Percent Loss (via drop-down menu) that is tolerable Over Time (via drop-down menu). Together these attributes establish what percentage of loss is tolerable over a specified period of time. Once exceeded, the Path State transitions from GOOD to BAD.
- **Silence Period (ms)**: The Path state transitions from **GOOD** to **BAD** when no packets are received within the specified amount of time.
- **Path Probation Period (ms)**: The probation period before changing the Path state from **BAD** to **GOOD**, after the symptom (e.g., loss or silence) clears.

To configure Bad Loss Sensitivity:

1. Log into your Appliance's web console.
2. Click on **Manage Network**, and then **Configuration**.
3. Open **Connections → Autopath Groups → [Autopath Group Name]**.

4. Click the edit icon and choose **Custom** from **the Bad Loss Sensitivity** drop-down menu

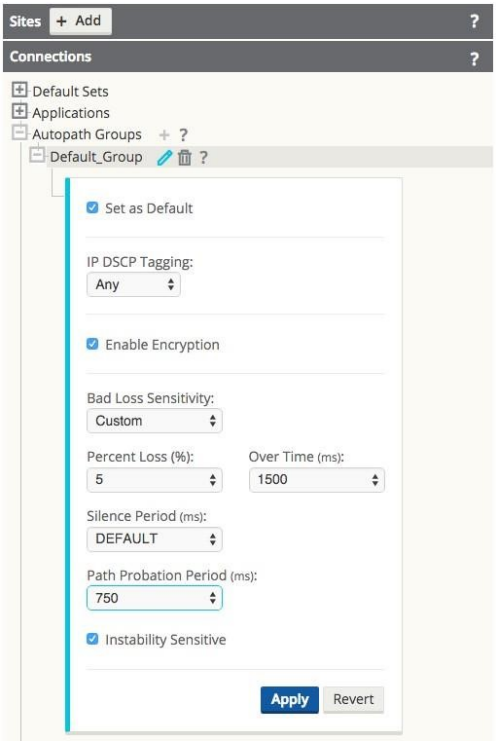


Figure 6: Configuring New Bad Loss Sensitivity Attributes

1. Choose a **Percent Loss** and a corresponding **Over Time** amount from their respective dropdown menus to establish a threshold for loss over time before the Path state will transition from GOOD to BAD.
2. Define a **Silence Period** (in milliseconds) from the drop-down menu. If no packets are received within the Silence Period you designated, the Path state will transition from GOOD to BAD.
3. Define a **Path Probation Period** (in milliseconds) from the drop-down menu. After the symptom (e.g., loss or silence) clears, the Path state will transition from BAD to GOOD once the Path Probation Period you designate here elapses.
4. Click the checkbox next to **Instability Sensitive** if you want latency penalties and spikes considered in the Path scoring algorithm.
5. Click **Apply**.

Monitor Statistics

The **Monitor**, and then **Statistics** default **Paths** screen was updated and renamed to increase usability. The **Source Port**, **Destination Port**, **Discovered MTU**, **Packets Received**, and **Packets Out of Order**, columns were moved to the new **Paths (Advanced)** screen (see Figure 8) to save space. Thus, the new, default **Paths (Summary)** screen is streamlined and easier to read.

Figure 7: Paths (Summary) Screen

On the new **Monitor**, and then **Statistics**, and then **Paths (Advanced)** screen, some column headings have been condensed to make the screen more readable.

The following header names have changed:

- Congestion is now **Cong**
- Source Port is now **Src Port**
- Destination port is now **Dst Port**
- Discovered MTU is now **MTU**
- Statistical Jitter (mS) is now **Jitter (mS)**
- Packets Out of Order is now **OOO**

Figure 8: New Paths (Advanced) Screen

The following new columns were also added to the **Paths (Advanced)** screen:

- **Reason**: This column indicates why a Path is marked BAD or DEAD.

- **Path State Duration**: This column indicates how long a Path has been in its current state.

Figure 9: Reason and Duration

Availability Reports

The Availability Reports screen (**Monitor**, and then **Availability Reports**) was reorganized and updated for both usability and readability.

Figure 10: Availability Reports

The **Incidents** column was enhanced to include a cluster of sub-columns that convey the following information:

- **Total**: The number of times a Path or Conduit has transitioned to a BAD or DEAD state.
- **Loss**: The number of times a Path has been marked BAD due to packet loss.
- **Silence**: The number of times a Path has been marked BAD or DEAD due to packet silence (i.e., no packets are received).
- **Peer**: The number of times a Path has been marked BAD or DEAD because the remote site indicated it was BAD or DEAD.

The **Badtime** column was enhanced to include a cluster of sub-columns that convey the following information:

- **Total**: The total time a Path or Conduit has been in a BAD state.
- **Loss**: The total time a Path has been marked BAD due to packet loss.
- **Silence**: The total time a Path has been marked BAD due to packet silence (i.e., no packets are received).
- **Peer**: The total time a Path has been marked BAD because the remote site indicated it was BAD.

The **Downtime** column was enhanced to include a cluster of sub-columns that convey the following information:

- **Total**: The total time a Path or Conduit has been marked DEAD.
- **Silence**: The total time a Path has been marked DEAD (i.e., no packets are received).

- **Peer**: The total time a Path has been marked DEAD because the remote site indicated it was DEAD.

Additional changes to Availability Reports:

- Path and Conduit information in Availability Reports is also included in the Periodic Status Reports when they are configured to include the Path or the Conduit in the report.

Additional Enhancements

The following enhancements were also rolled into Oracle SD-WAN Edge 4.4:

- Perform Diagnostic Dumps on Remote Client Appliances from the NCN

If you can still reach a Client via the NCN but cannot access that Client via its management port, the new `background_diagnostics` command allows administrators to perform a diagnostic dump on the remote Client via the NCN command line. When administrators execute the `tcon debug` command then execute the `remote_cmd [Remote`

`Site] ‘‘tcon background_diagnostics''` (e.g., `remote_cmd Omaha-CL1 ‘‘tcon`

`background_diagnostics''`) command from a debug shell, a diagnostic dump will be started as a background process at the remote site specified.

Administrators can track the execution of the current remote diagnostics operation and avoid spawning separate diagnostic dumps using `remote_cmd [Remote Site] ‘‘tcon`

`background_diagnostics_status''` (e.g., `tcon remote_cmd Omaha_CL1 ‘‘tcon background_diagnostics_status''`). This way administrators will know when the remote

diagnostic dump is complete.

> **Note:**
>
> The `background_diagnostics` and `background_diagnostics_status` commands can only be executed from within the debug shell.

- Export Authentication Logs to Syslog

When syslog is available for an appliance, administrators can now navigate to **Integrate** →

Configure Events and Alerts and click the **Authentications to Syslog** checkbox to forward user login events to a remote syslog server.

Figure 11: Syslog Settings

- Route Serviceability Enhancements

The **Routes** screen under **Monitor**, and then **Statistics** now displays the **Maximum allowed routes** as well as the routes in use. It also houses a new **Purge dynamic routes** button that you can use to clear dynamic routes and refresh the route table if you suspect it is corrupted.

Figure 12: Changes to Routes Screen

Appliance T5200 Support

Oracle SD-WAN Edge 4.4 introduces support for the new Appliance T5200. The T5200 is the first Appliance with 10G fiber connectivity. The 2U rack-mountable T5200 delivers up to 3Gbps across eight public and 32 private WAN Links and connects up to 256 sites, all of which you can manage through the Oracle SD-WAN Edge 4.4 interface. Refer to the *Appliance T5200 Hardware Guide* for additional details.

Oracle Virtual Appliance VT500 Support

Oracle SD-WAN Edge 4.4 introduces support for the new Oracle Virtual Appliance VT500. The VT500 is the first Oracle Virtual appliance built to run on VMware's vSphere virtual server environment. It delivers up to 40Mbps across three public and 32 private WAN Links and connects up to eight sites that you can manage through the Oracle SD-WAN Edge 4.4 interface. Refer to the *Oracle Virtual Appliance VT500 Getting Started Guide* for additional details.

11
Release 5.0 Features

This chapter includes features and enhancements release in 5.0.

Enhanced Match Criteria for Rules

In support of the new Virtual Routing and Forwarding (VRF) feature set, Edge 5.0 has significantly enhanced the criteria for Rule matching. The VLAN ID and the newly introduced Routing Domain may be used as match criteria for Rules in addition to the previously supported match criteria.

- Routing Domain: You can now choose one of the available, configured Routing Domains from the drop-down menu when creating a new Rule.

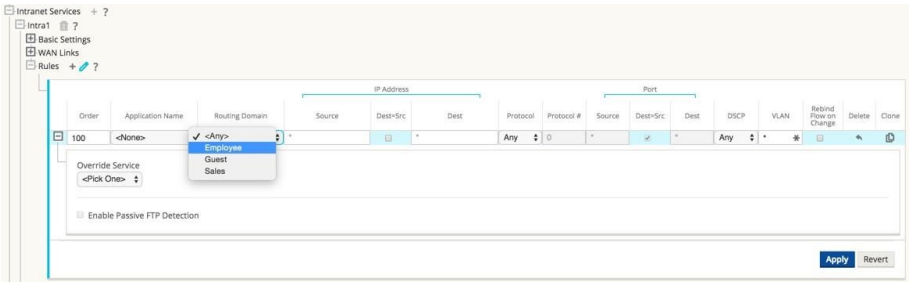


Figure 1: Routing Domain Drop-Down Menu

- VLAN ID: You can now enter one of the configured VLAN IDs in the VLAN ID field when creating a new Rule.

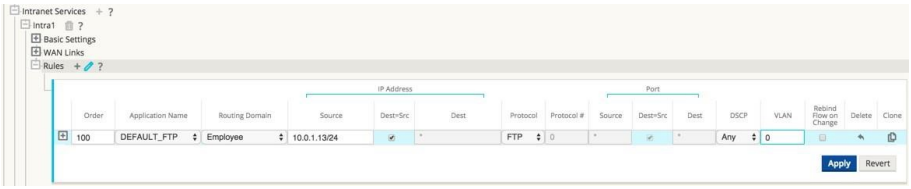


Figure 2: VLAN ID Field

Virtual Routing and Forwarding (VRF)

Edge 5.0 introduces Virtual Routing and Forwarding (VRF) to empower network administrators by giving them tools to segment their network for additional security and manageability. You can now separate guest network traffic from employee traffic, create distinct routing domains to segment large corporate networks, support multiple tenants at a Client Site, and segment traffic to support multiple customer networks.

Here are the touch points in Edge 5.0 to add, configure, and use Routing Domains to control and segment network traffic. Routing Domains can be used with both the Open Shortest Path First (OSPF) and Interior Border Gateway Protocol (IBGP) protocols.

In the Configuration Editor under **Global**, and then **Routing Domains** click Add (+) and enter a Name for your new Routing Domain. If you want to default to this Routing Domain, click the Default checkbox. Click Apply to save the changes. If you plan to implement a single Routing Domain, no explicit configuration is required. All new configurations are automatically populated with a default Routing Domain.

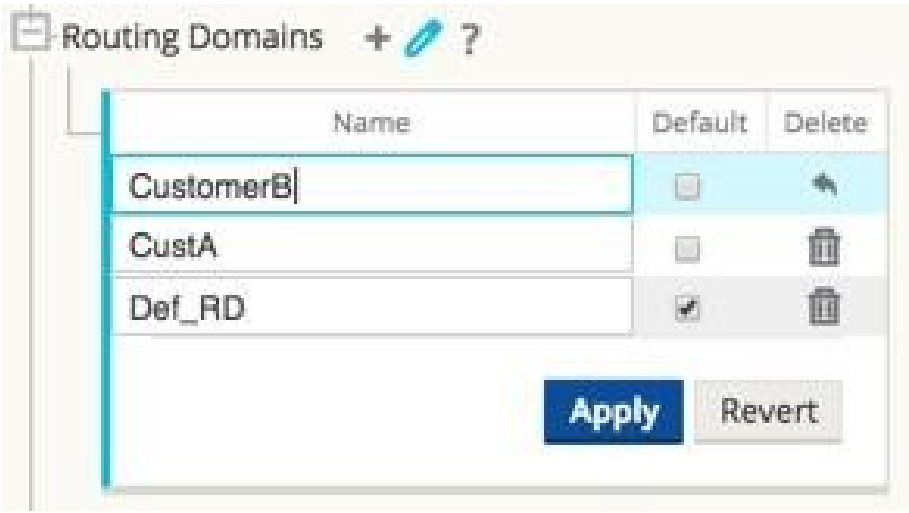


Figure 3: Add a Routing Domain

Under **Sites**, and then **[Client Site Name]**, and then **Routing Domains** click the Enable checkbox to enable a configured Routing Domain for the Site. Click the Default checkbox to make that Routing Domain the default for the Site. Click Apply to save the changes.

Note: Unchecking Enable for a Routing Domain will make it unavailable for use at the Site.

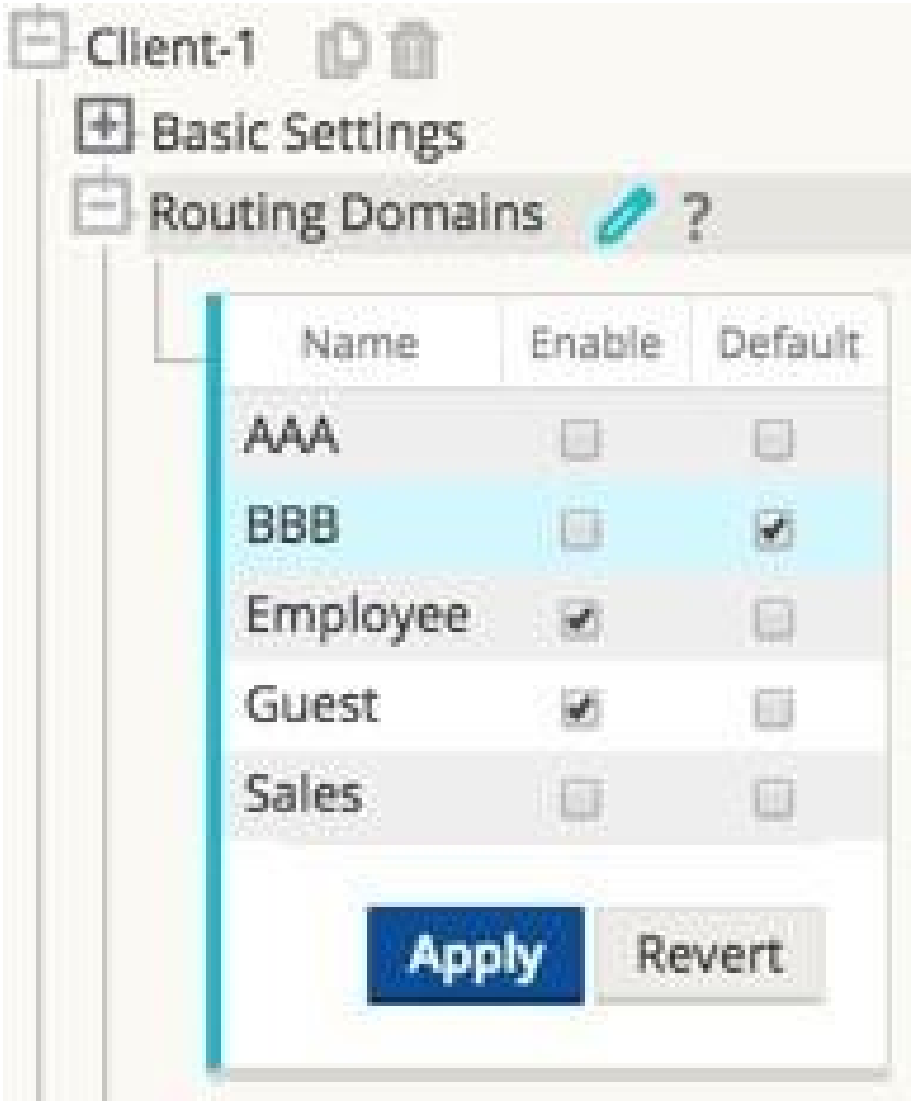


Figure 4: Site Level Routing Domain Management

Under **Sites**, and then **[Client Site Name]**, and then **Interface Groups** choose a Routing Domain from the drop-down menu when configuring Virtual Interfaces.

Note: Once Virtual Interfaces are associated with a specific Routing Domain, only those interfaces will be available when using that Routing Domain.

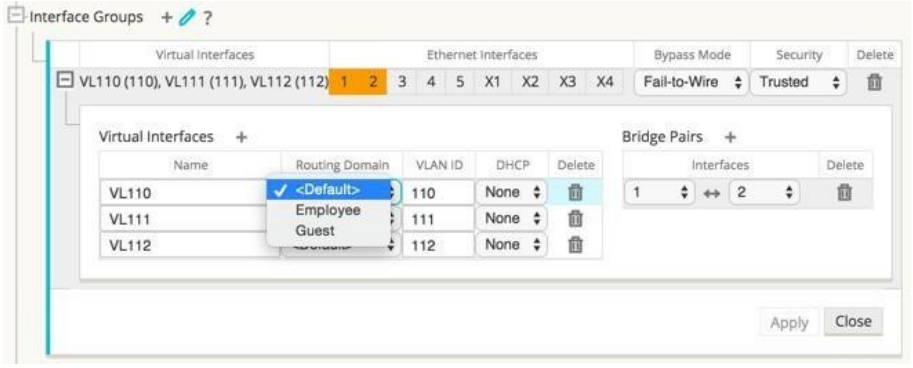


Figure 5: Configuring Interface Groups

From **Sites**, and then **[Client Site Name]**, and then **Virtual IP Addresses** choose a Routing Domain from the dropdown menu when configuring Virtual IP Addresses. The Routing Domain you choose determines which Virtual Interfaces are available from the drop-down menu.

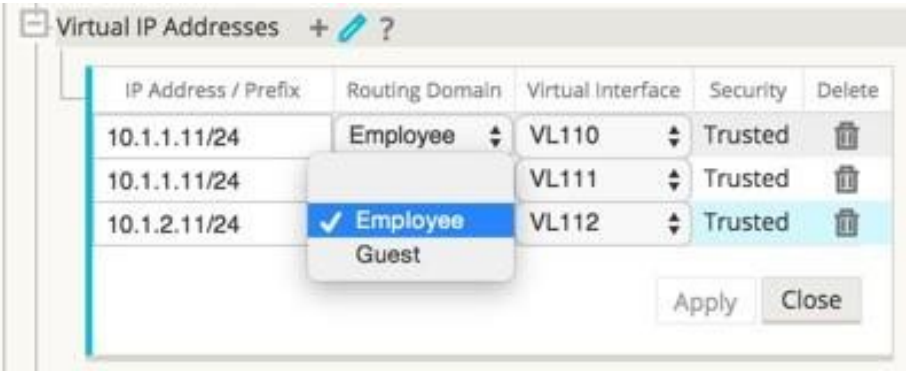


Figure 6: Configure Virtual IP Addresses

Under **Sites**, and then **[Client Site Name]**, and then **LAN GRE Tunnels** choose a Routing Domain from the drop-down menu when configuring a LAN GRE Tunnel. The Routing Domain you choose determines which Source IP Addresses are available from the drop-down menu.

Figure 7: Configure a LAN GRE Tunnel

From **Sites**, and then **[Client Site Name]**, and then **WAN Links**, and then **[WAN Link Name]**, and then **Access Interfaces** choose a Routing Domain from the drop-down menu when configuring an Access Interface. The Routing Domain you choose determines which Virtual Interfaces are available from the drop-down menu.

Figure 8: Configure an Access Interface

Under **Connections**, and then **[Site Name]**, and then **Intranet Services**, and then **[Intranet Service Name]**, and then **Basic Settings** click the Edit (✎) icon. Choose a Routing Domain from the drop-down menu.

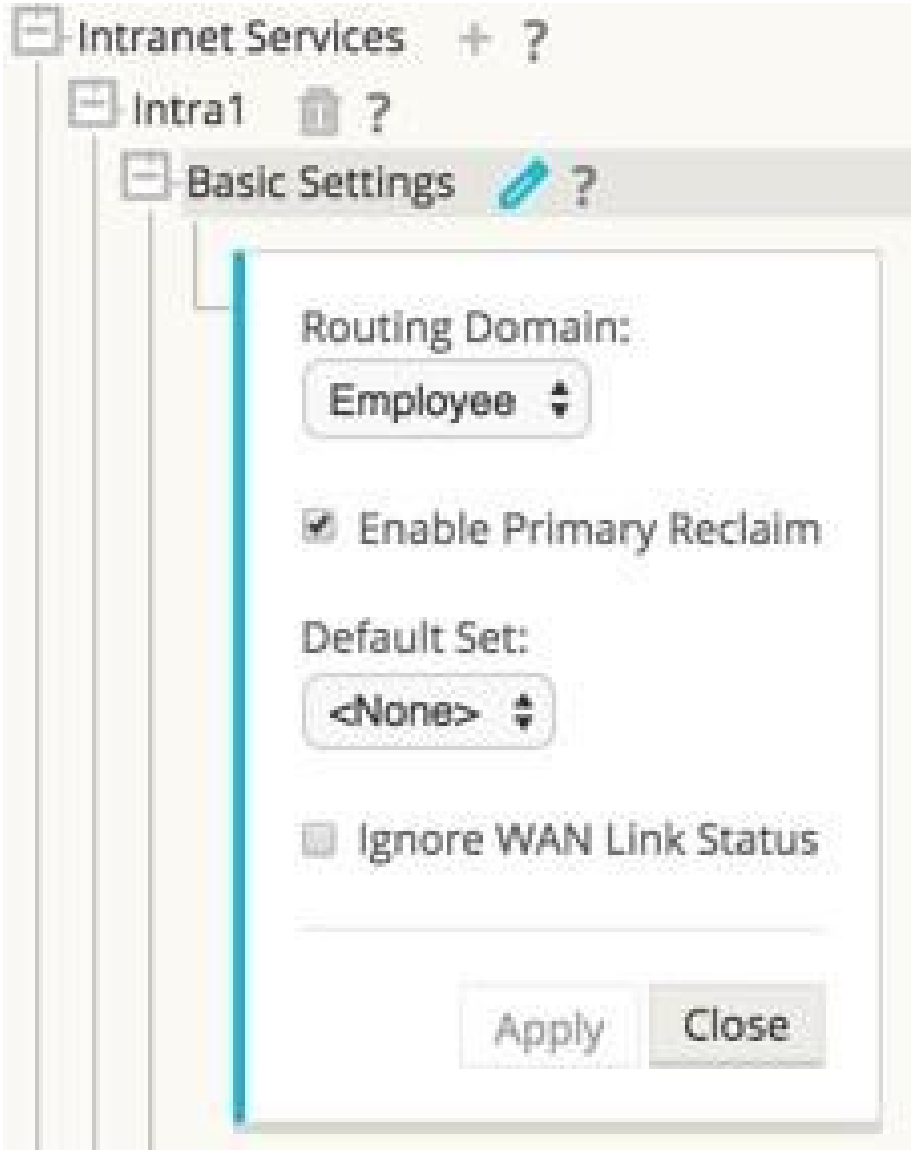


Figure 9: Select Routing Domain for Intranet Service

From **Connections**, and then **[Site Name]**, and then **Intranet Services**, and then **[Intranet Service Name]**, and then **Rules** choose a Routing Domain from the drop-down menu.

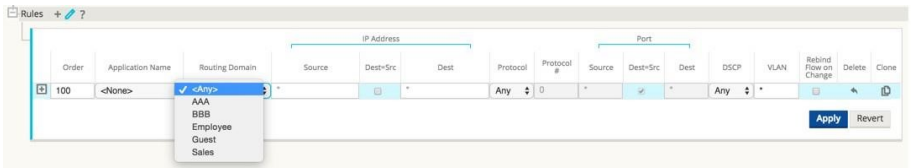


Figure 10: Configure a Rule

From **Connections**, and then **[Site Name]**, and then **IPsec Tunnels** when you choose LAN as the Service Type, choose a Routing Domain from the drop-down menu. The Routing Domain will determine which Local IP Addresses are available.

Note: If the Service Type is Intranet, the Routing Domain is pre-determined by the chosen Intranet Service.

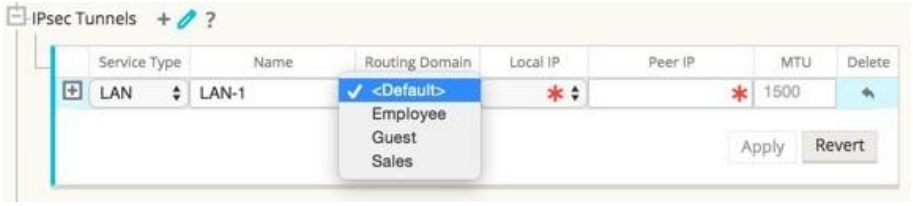


Figure 11: Configure IPsec Tunnel

From **Connections**, and then **[Site Name]**, and then **Routes** choose a Routing Domain from the drop-down menu. New Routes are automatically associated with the default Routing Domain.

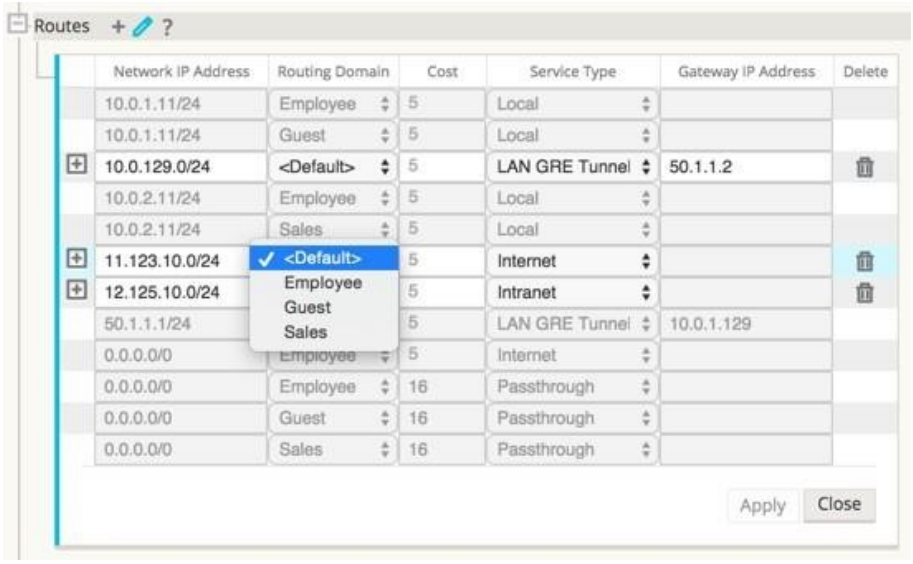


Figure 12: Configure a Route

Monitoring

From the Oracle Talari Appliance's home page, Routing Domain names are displayed in the System Status area of the screen.

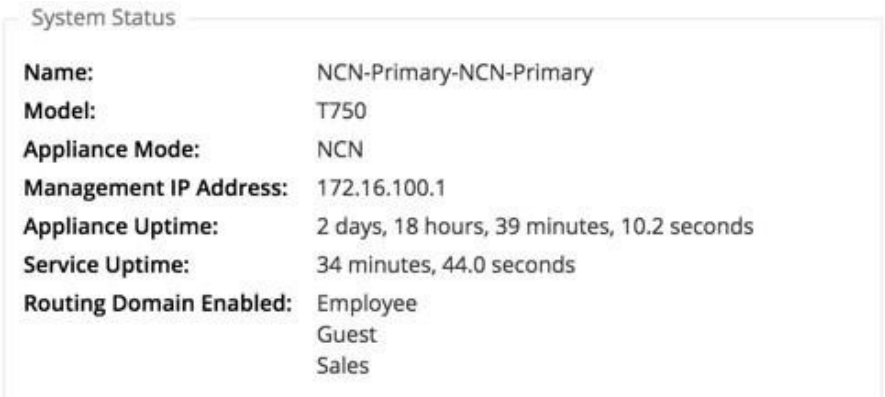


Figure 13: Appliance Home Page

Under **Monitor**, and then **Statistics**, Routing Domain information is displayed, and results can be filtered by Routing Domain for the following criteria:

- Access Interfaces
- WAN Links
- MPLS Queues
- Intranet Services
- ARP
- LAN GRE
- Tunnels
- IPsec
- Routes
- Flows

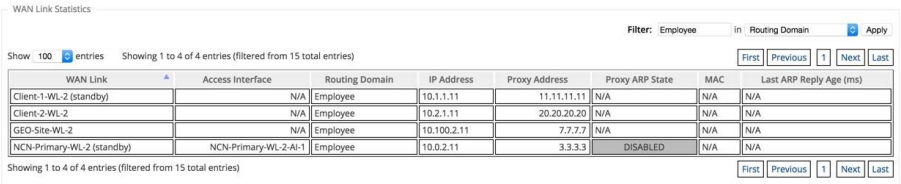
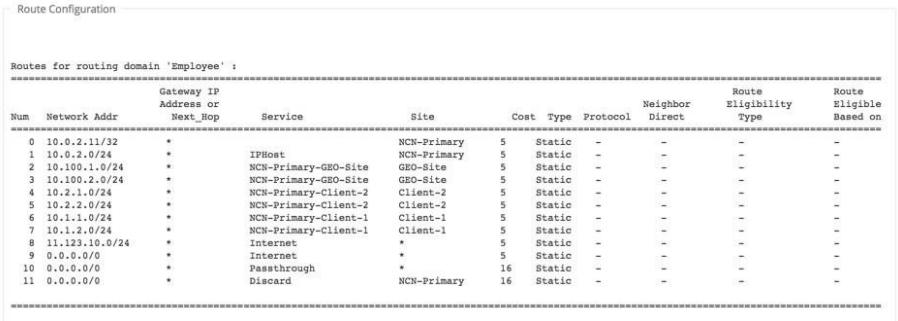


Figure 14: WAN Link Statistics Filtered by Employee Routing Domain

Under **Manage Network**, and then **View Configuration**, wherever configuration information for the following attributes is displayed, the Routing Domain is also displayed:

- Sites
- WAN Links
- Intranet Services
- LAN GRE
- Tunnels
- IPsec
- Routes
- Flows



Dynamic Routing

Edge 5.0 introduces support for Dynamic Routing protocols. This feature enables your Oracle Talari Appliance to discover LAN subnets, advertise Conduit routes, work more seamlessly within networks using the Interior Border Gateway Protocol (IBGP) and Open Shortest Path First (OSPF) protocols, potentially eliminate redundant equipment (branch routers), and support graceful router failover.

Note: Edge 5.0 uses Interior BGP (IBGP) and OSPF as an Interior Gateway Protocol (IGP).

Virtual IP Address Identity

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.

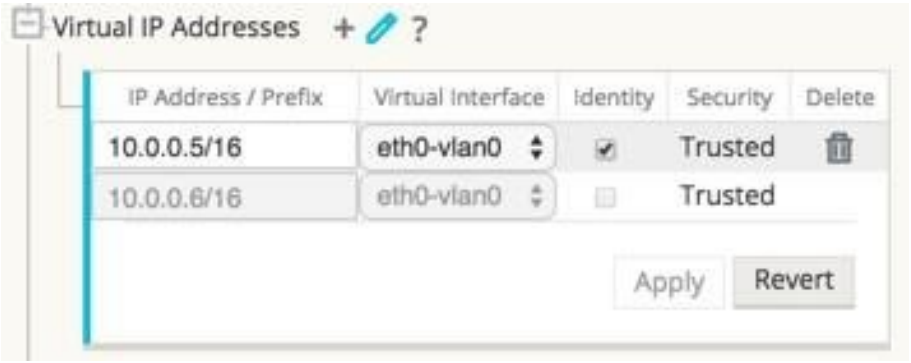


Figure 15: Virtual IP Address Identity

Open Shortest Path First (OSPF) Routing Protocol

OSPF is an interior routing protocol that uses a link state algorithm to exchange routing information between routers within a single routing domain (i.e., autonomous system). You can now configure Oracle Talari Appliances to learn routes and advertise routes using OSPF.

To configure OSPF:

1. Under **Connections**, and then **[Site Name]**, and then **Route Learning**, and then **OSPF**, and then **Basic Settings** click the Edit ( ) icon.
2. Click the Enable checkbox, enter an optional Router ID, click the Advertise APN Routes checkbox if you wish to advertise Routes, and click Apply to enable OSPF.

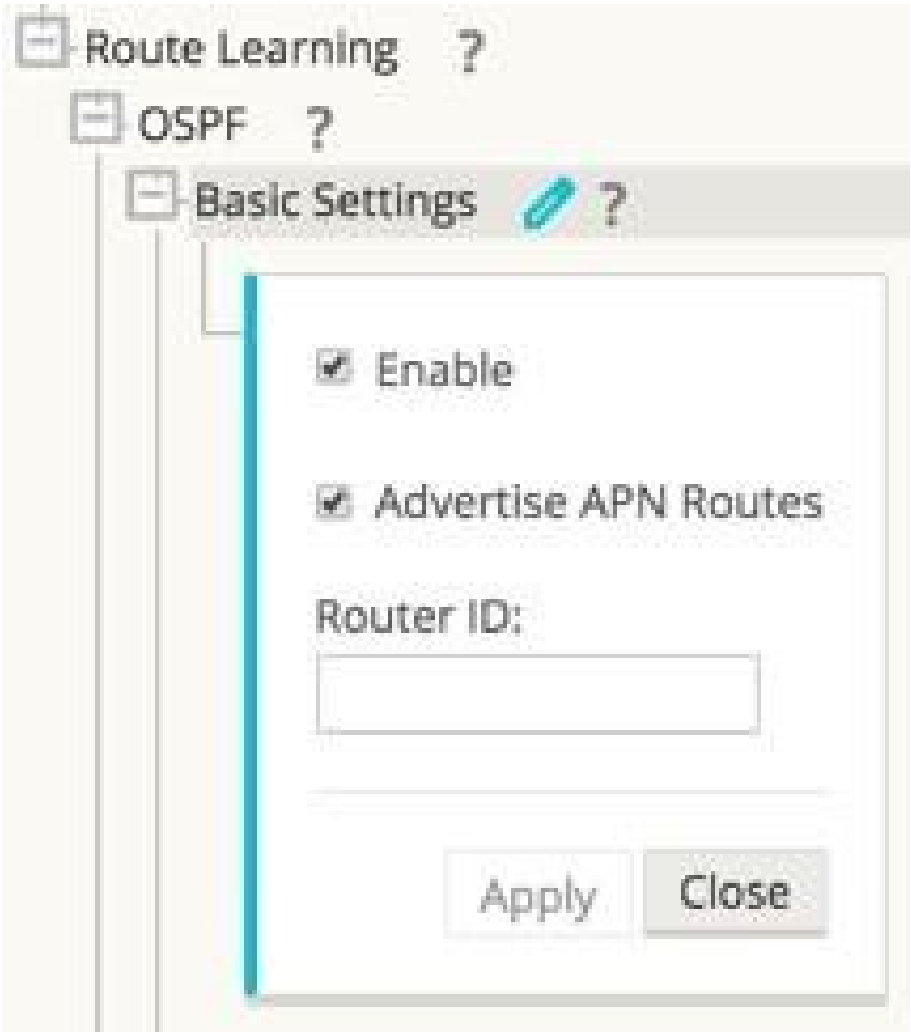


Figure 16: Enable OSPF

3. Expand **OSPF > Areas** and click the Edit icon.

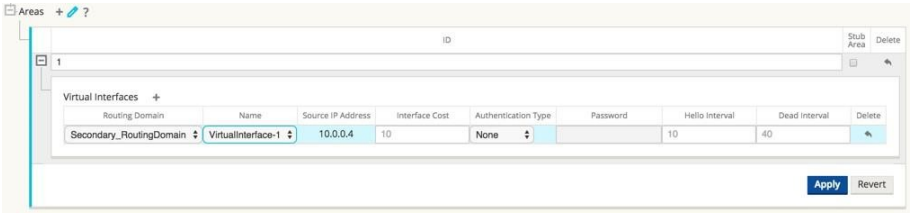


Figure 17: Configuring OSPF

1. Enter an area ID to learn from and advertise to.
2. For sites with multiple Routing Domains, under Virtual Interfaces choose a Routing Domain from the drop-down menu as illustrated in Figure 17. The Routing Domain determines which Virtual Interfaces are available.

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.

1. Choose one of the available Virtual Interfaces from the Name drop-down menu. The Virtual Interface will determine the Source IP Address.
2. Enter the Interface Cost (10 is the default).
3. Choose an Authentication Type from the drop-down menu.
4. If you chose Password or MD5 in step 8, enter the Password associated text field.
5. In the Hello Interval field, enter the amount of time to wait between sending Hello protocol packets to directly connected neighbors (10 seconds is the default).
6. In the Dead Interval field, enter the amount of time to wait to receive a Hello protocol packet before marking a router as dead (40 seconds is the default).
7. Click Apply to save your changes.

Interior Border Gateway Protocol (IBGP)

Interior BGP (IBGP) is an exterior routing protocol designed to exchange routing information between routing domains (i.e., autonomous systems). However, BGP may be used for routing within a domain. In this application, it is referred to as Interior BGP. You can now configure Oracle Talari Appliances to learn routes and advertise routes using Interior BGP.

To configure Interior BGP (IBGP):

1. Under **Connections**, and then **[Site Name]**, and then **Route Learning**, and then **IBGP**, and then **Basic Settings** click the Edit (✎) icon.
2. Click the Enable checkbox, click the Advertise APN Routes checkbox if you wish to advertise Routes, enter an optional Router ID, and enter the number of the Local Autonomous System to learn routes from and advertise routes to in the Local Autonomous System field. Click Apply to enable IBGP.

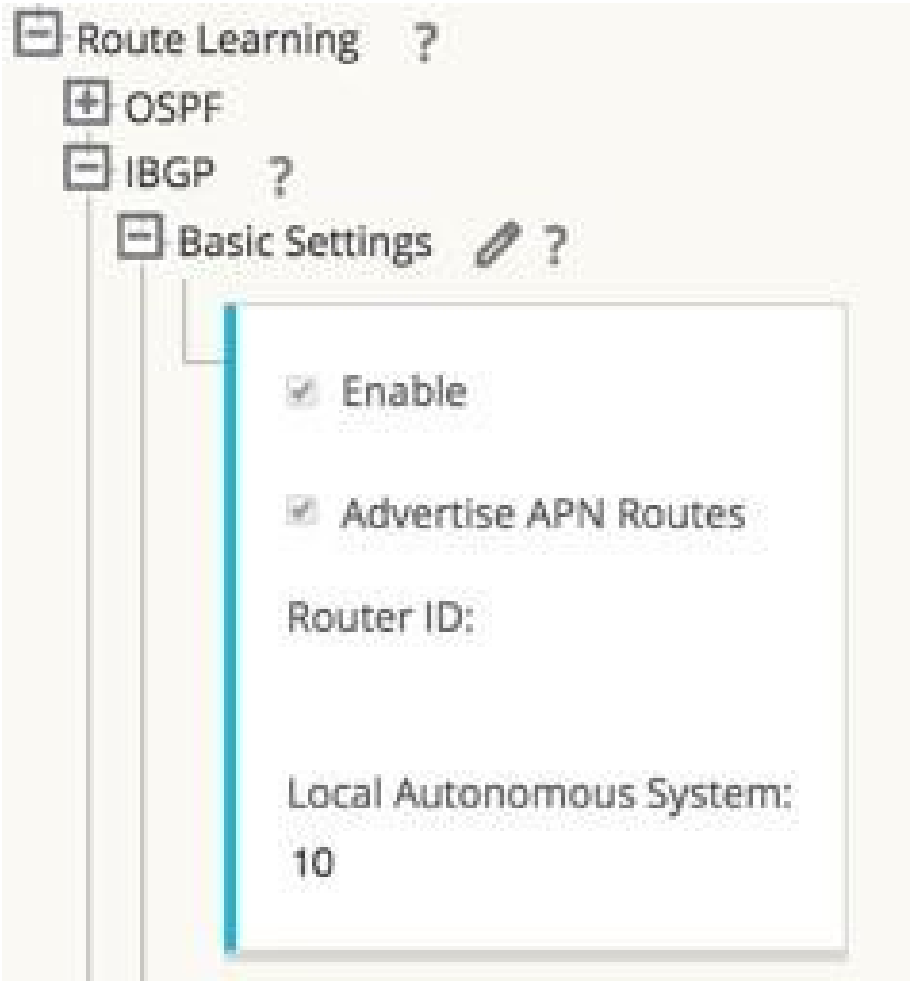


Figure 18: Enable IBGP

1. Expand **IBGP**, and then **Basic Settings**, and then **Neighbors** and click the Add (+) icon.

Figure 19: Add a Neighbor to a Site with a Single Routing Domain

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

1. For Sites with multiple Routing Domains, choose a Routing Domain from the drop-down. The Routing Domain determines which Virtual Interfaces are available.
2. Choose a Virtual Interface from the drop-down menu. The Virtual Interface will determine the Source IP Address.
3. Enter the IP Address of the IBGP Neighbor router in the Neighbor IP field.

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

Filters

Filters are used to import or exclude routes learned via OSPF and IBGP based on specific match criteria.

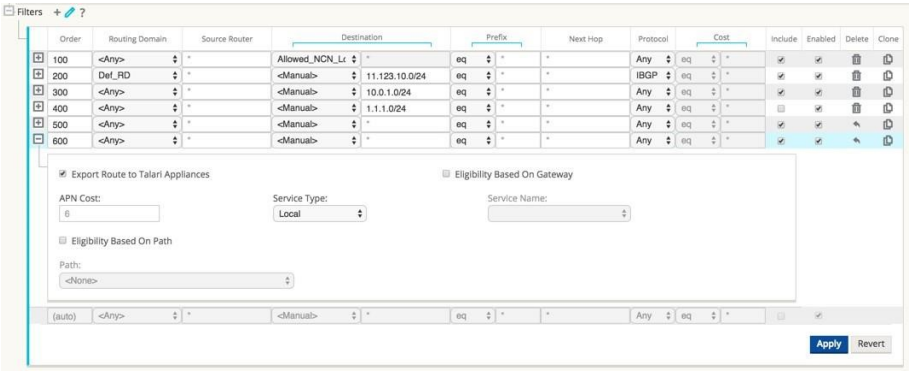


Figure 20: Add a Filter on a Site with Multiple Routing Domains

1. Expand **Route Learning**, and then **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. You can use the following criteria to construct each Filter that you create.

- Order: The Order in which filters are prioritized. The first filter that a route matches to will be applied to that route.
- Routing Domain: To match routes from a specific routing domain, choose one of the configured Routing Domains from the drop-down menu.
- Source Router: To match routes from a specific source router, enter the IP address of the Source Router.
- Destination: To match routes by destination, choose Manual from the drop-down menu and enter an IP Address and Netmask in the adjacent field or choose from the list of available Network Objects.
- Prefix: To match routes by prefix, choose a match predicate from the drop-down menu and enter a Route prefix in the adjacent field.
- The predicates are:
  - Eq: Equal to
  - lt: Less than

  - le: Less than or equal to
  - gt: Greater than
  - ge: Greater than or equal to
- Next Hop: To match routes by next hop, enter the IP address of the Next Hop.
- Protocol: To match routes by protocol, choose the protocol from the drop-down menu (Any, OSPF, or IBGP) 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 Oracle Talari Appliances: Click the checkbox to export matching routes to Oracle Talari 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.
- Cost: Enter the cost that the Oracle Talari 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.

4. Once you have configured your filter, click Apply.

Network Objects

Edge 5.0 introduces Network Objects, a new option under the Global section in the Configuration Editor. Now you can group multiple subnets together, and reference a single Network Object when defining a Route Filter rather than creating a filter for each subnet.

1. If you plan to use Network Objects, navigate to **Global**, and then **Network Objects** click Add (+).
2. Click Add (+) under Networks.
3. Enter the IP Address and Subnet of the new Network Object.
4. Click Apply to save the settings.
5. To edit the Network Object's name, double-click on the name of the Network Object and enter a new name.

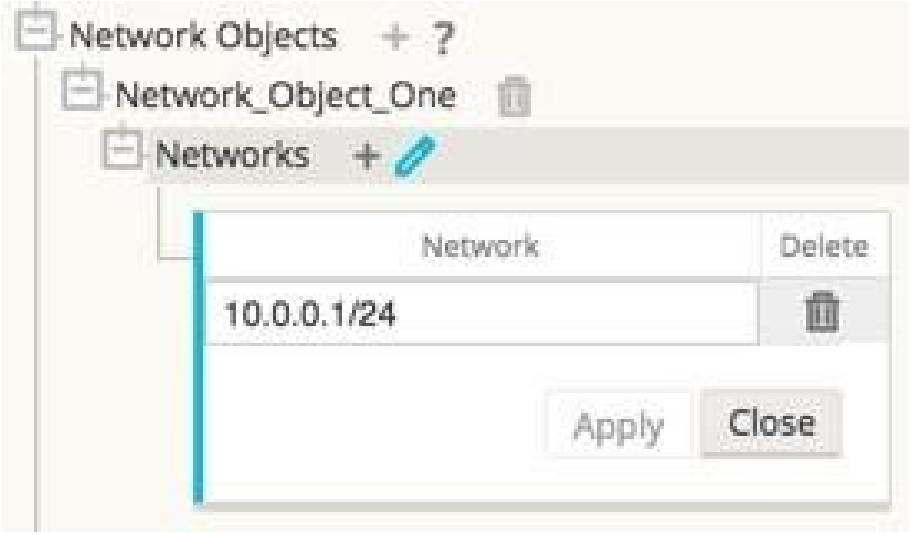


Figure 21: New Network Object

Monitoring

Under **Monitor**, and then **Statistics** all functions for Routes supported in Edge 4.4 are supported in Edge 5.0 regardless of whether a Route is Dynamic or Static.

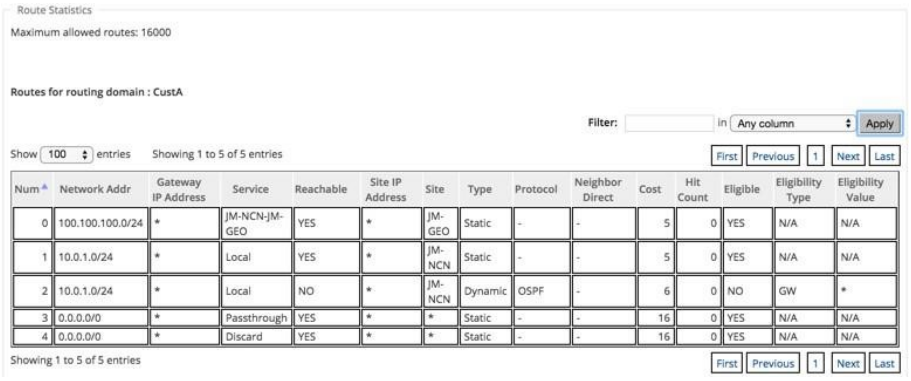


Figure 22: Route Statistics for Dynamic and Static Routes

WAN Link IP Address Learning (DHCP Client)

Edge 5.0 introduces WAN Link IP Address Learning via DHCP Clients. This functionality reduces the amount of manual configuration to deploy Oracle Talari Appliances and reduces customers' ISP costs by eliminating the need to purchase

static IP Addresses. Now Oracle Talari Appliances can obtain dynamic IP Addresses for WAN Links on untrusted interfaces eliminating the need for an intermediary WAN router to perform this function or a static IP.

Note: DHCP Client can only be configured for Oracle Talari Appliances configured as Client Nodes.

To Configure DHCP for an Untrusted Virtual Interface, choose Client from the DHCP dropdown menu under **Sites**, and then **[Client Name]**, and then **Interface Groups**, and then **Virtual Interfaces**.

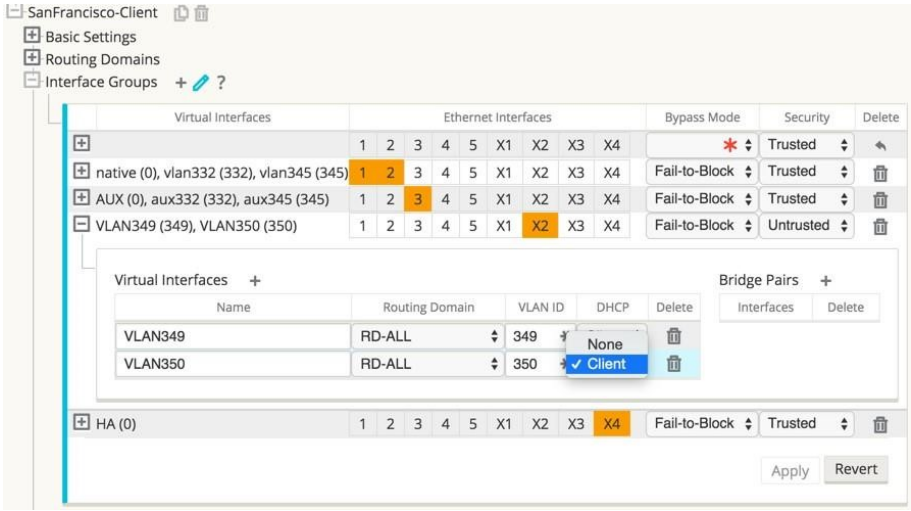


Figure 23: Enable DHCP for a Virtual Interface

Under **WAN Links**, and then **[WAN Link Name]**, and then **Settings**, and then **Basic Settings** click the **Autodetect Public IP** checkbox to enable the Network Control Node (NCN) to detect the Public IP Address to be used by the Public Internet WAN Link.

Note: This is required when DHCP Client mode is configured for the WAN Link.

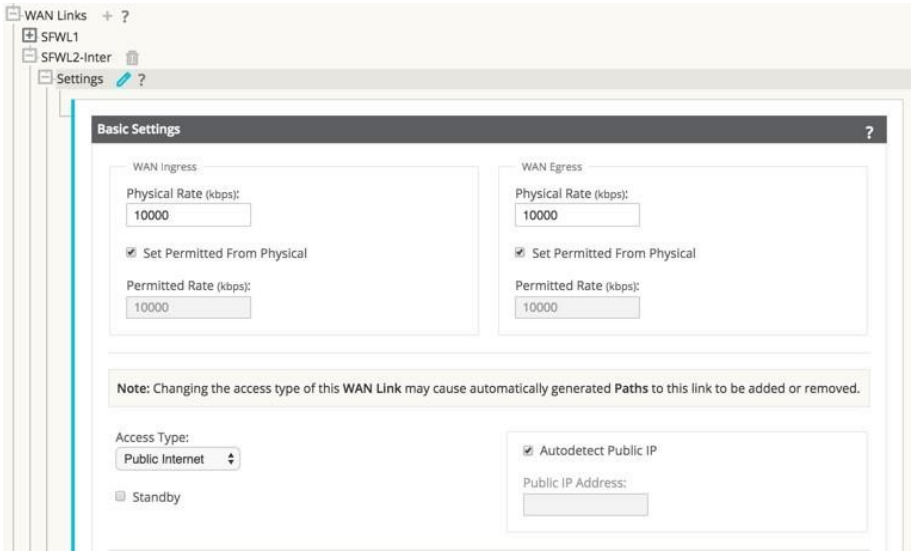


Figure 24: Autodetect Public IP

Monitoring

The runtime Virtual IP Address, Subnet Mask, and Gateway settings are logged as in 4.4. Events are generated when Dynamic Virtual IPs are learned, released, or expired; when there is a communication issue with the learned Gateway or DHCP server; or when duplicate IPs are detected. If duplicate IPs are detected at a Site, Dynamic Virtual IPs are released and renewed until all Virtual Interfaces at the site have unique Virtual IP Addresses.

Under **Manage Network** > **Enable/Disable/Purge Flows** the DHCP Client WAN Links table provides the status of learned IPs. From here you can request to Renew the IP, which will refresh the lease time. You can also choose to **Release & Renew**, which will get a new IP address with a new lease.

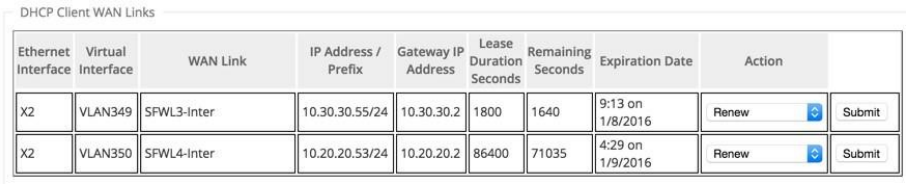


Figure 25: DHCP Client WAN Links

IPsec VPN Termination

Expanding on the IPsec in Conduit feature introduced in 4.4, Edge 5.0 release allows third party devices to terminate IPsec VPN Tunnels on the LAN or WAN side of Oracle Talari Appliances. Now you can secure site-to-site IPsec Tunnels terminating on an Oracle Talari Appliance using a 140-2 Level 1 FIPS certified IPsec cryptographic binary.

Note: Bandwidth provisioning is not available for LAN side IPsec VPN termination.

If you plan to implement Certificates for IKE negotiation, navigate to **Sites**, and then **Certificates** and add any necessary certificates.

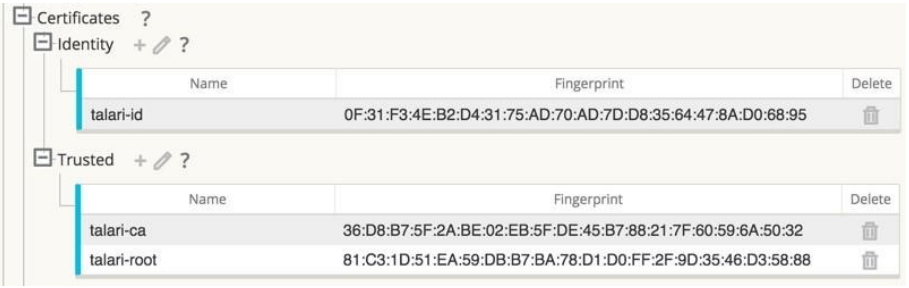


Figure 26: Certificates for IKE Negotiation

Navigate to **Connections**, and then **[Site Name]**, and then **IPsec Tunnels** to create an IPsec Tunnel.

You can configure the following criteria, and click Apply to save your settings:

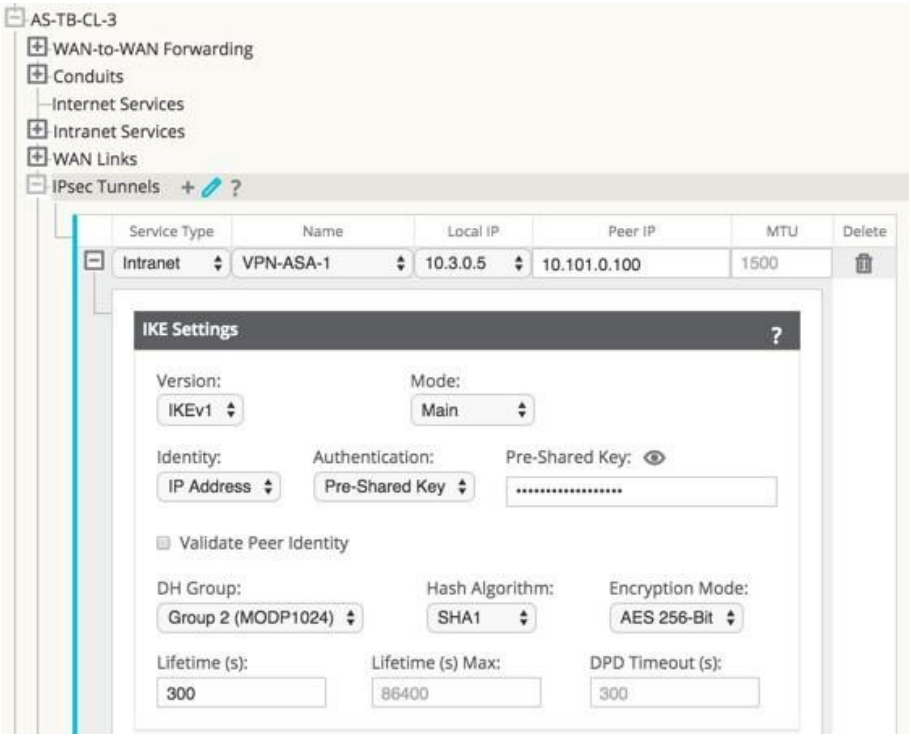


Figure 27: IPsec IKEv1 Settings

- Service Type: Choose either Intranet or VPN from the drop-down menu.
- Name: If the Service Type is Intranet, choose from the list of configured Intranet Services in the drop-down menu. If the service type is LAN, enter a unique Name.
- Local IP: Choose the Local IP address of the IPsec Tunnel from the drop-down menu of available Virtual IP Addresses configured at this Site.
- Peer IP: Enter the Peer IP address of the IPsec Tunnel.
- MTU: The default is 1500, but you can enter a different value.
- IKE Settings
  - Version: Choose either IKEv1 or IKEv2 from the drop-down menu.
  - Mode: For IKEv1, choose either Main or Aggressive from the Mode drop-down menu.
  - Identity: Choose either Auto or IP Address from the Identity drop-down.
  - Authentication: Choose either Pre-Shared Key or Certificate from the Authentication drop-down menu.
    * Pre-Shared Key: If you are using a Pre-Shared Key, copy and paste it into this field. Click on the Eyeball ( ) icon to view the Pre-Shared Key.
    * Certificate: If you are using an Identity Certificate, choose it from the drop-down menu.
  - Validate Peer Identity: Click the Validate Peer Identity checkbox to validate the

IKE's Peer Identity. If the peer's ID type is not supported, do not enable this feature.

- DH Group: Choose the Diffie–Hellman group (Group 1, Group 2, or Group 5) to use for IKE key generation from the drop-down menu.

- Hash Algorithm: Choose MD5, SHA1, or SHA-256 from the drop-down menu to authenticate IKE messages.
- Encryption Mode: Choose AES 128-bit, AES 192-bit, or AES 256-bit as the Encryption Mode for IKE messages from the drop-down menu.
- Lifetime (s): Enter the preferred duration, in seconds, for an IKE security association to exist. The default is 3600 seconds.
- Lifetime Max (s): Enter the maximum preferred duration, in seconds, to allow an IKE security association to exist. The default is 86400 seconds.
- DPD Timeout (s): Enter the Dead Peer Detection timeout, in seconds, for VPN connections. The default is 300 seconds.
- IKEv2 Settings

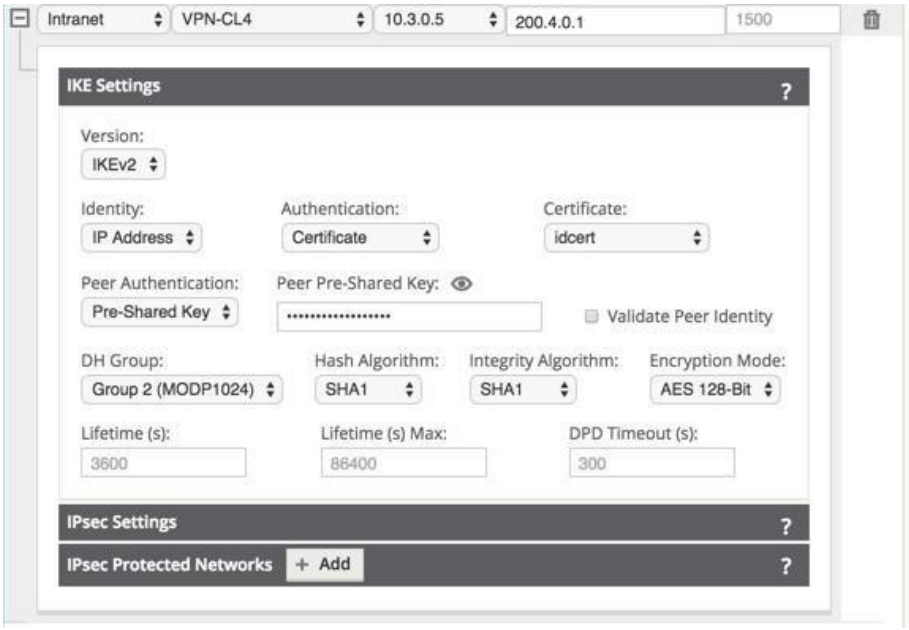


Figure 28: IPsec IKEv2 Settings

- Peer Authentication: Choose Mirrored, Pre-Shared Key, or Certificate Peer Authentication from the drop-down menu.

Peer Pre-Shared Key: Paste the IKEv2 Peer Pre-Shared Key into this field for authentication. Click on the Eyeball ( ) icon to view the Pre-Shared Key.

- Integrity Algorithm: Choose MD5, SHA, or SHA-256 as the hashing algorithm to use for HMAC verification from the drop-down menu.
- IPsec Settings

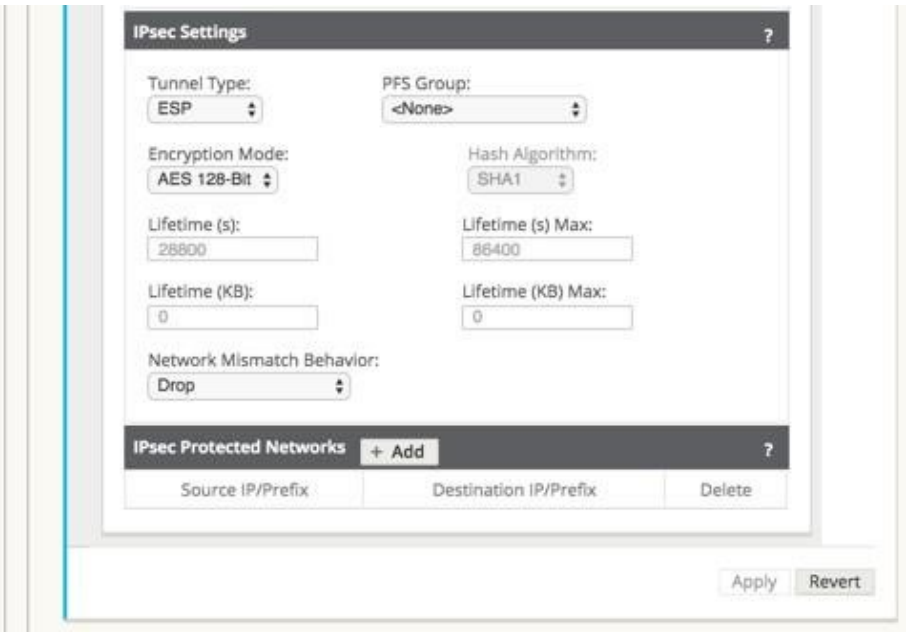


Figure 29: IPsec Settings and IPsec Protected Networks

- Tunnel Type: Choose ESP, ESP+Auth, or AH as the Tunnel Type from the dropdown menu.
- PFS Group: Choose the Diffie–Hellman group (Group 1, Group 2, or Group 5) to use for perfect forward secrecy key generation from the drop-down menu.
- Encryption Mode: If you chose ESP or ESP+ Auth, choose AES 128-bit, AES 192bit, or AES 256-bit as the Encryption Mode for IPsec messages from the drop-down menu.
- Hash Algorithm: If you chose ESP+Auth or AH as the Tunnel Type, choose MD5, SHA1, or SHA-256 from the Hash Algorithm drop-down menu to use for HMAC verification.
- Lifetime (s): Enter the amount of time, in seconds, for an IPsec security association to exist. The default is 28800 seconds.
- Lifetime Max (s): Enter the maximum amount of time, in seconds, to allow an IPsec security association to exist. The default is 86400 seconds.
- Lifetime (KB): Enter the amount of data, in kilobytes, for an IPsec security association to exist.
- Lifetime Max (KB): Enter the maximum amount of data, in kilobytes, to allow an IPsec security association to exist.
- Network Mismatch Behavior: Choose Drop, Send Unencrypted, or Use Non-IPsec Route as the desired action for your Talari WAN to take if a packet does not match the IPsec Tunnel's Protected Networks from the drop-down menu.
- IPsec Protected Networks
  - Source IP/Prefix: After clicking the Add (+ Add) button, enter the Source IP and Prefix of the network traffic the IPsec Tunnel will protect.
  - Destination IP/Prefix: Enter the Destination IP and Prefix of the network traffic the IPsec Tunnel will protect.

Monitoring

Under **Monitor**, and then **Statistics** when you choose IPsec Tunnel from the Show drop-down menu, you can see the following criteria:

- Tunnel Name
- State
- Service Type
- Packets Received
- Packets Sent
- Kbps Received
- Kbps Sent
- Packets Dropped
- Bytes Dropped
- MTU

Figure 30: IPsec Tunnel Monitoring

Under **Manage Network**, and then **View Configuration** when you choose IPsec Tunnel from the Show dropdown menu, you can view the IPsec Tunnel configuration:

IPsec Tunnel Configuration

```
================================================================================
Name: VPN-ASA-1
================================================================================
        ipsec_service_type=intranet
        ike_local_ip_addr=10.0.0.6
        ike_remote_ip_addr=10.101.0.100
        network_mtu=1500
        ike_version=2
        ike_auth=psk
        ike_identity=auto
        ike_peer_auth=cert
        ike_validate_peer_identity=1
        ike_hash_algorithm=sha256
        ike_integ_algorithm=sha256
        ike_encryption_mode=aes256
        ike_dhgroup=group2
        ike_lifetime_s=300
        ike_lifetime_s_max=86400
        ike_dpd_s=300
        ipsec_tunnel_mode=tunnel
        ipsec_tunnel_type=esp_auth
        ipsec_encryption_mode=aes128
        ipsec_hash_algorithm=sha
        ipsec_pfsgroup=none
        ipsec_lifetime_s=28800
        ipsec_lifetime_s_max=86400
        ipsec_lifetime_kb=0
        ipsec_lifetime_kb_max=0
        ipsec_mismatch_behavior=drop
        Protected Networks:
                [1] 10.0.0.0/16 -> 10.101.0.0/16
                [2] 10.4.0.0/16 -> 10.101.0.0/16
                [3] 10.3.0.0/16 -> 10.101.0.0/16
                [4] 10.2.0.0/16 -> 10.101.0.0/16
                [5] 10.1.0.0/16 -> 10.101.0.0/16
================================================================================
```

Figure 31: IPsec Tunnel Configuration

Standby WAN Links

Edge 5.0 introduces Standby WAN Links, which you can configure so user traffic will only be transmitted on that WAN Link when all other available WAN Links are dead or disabled. This feature can *only* be configured for Private Intranet and Public Internet Access Types. Simply click the Standby checkbox when you configure a Private Intranet or Public Internet WAN Link in the Configuration Editor.

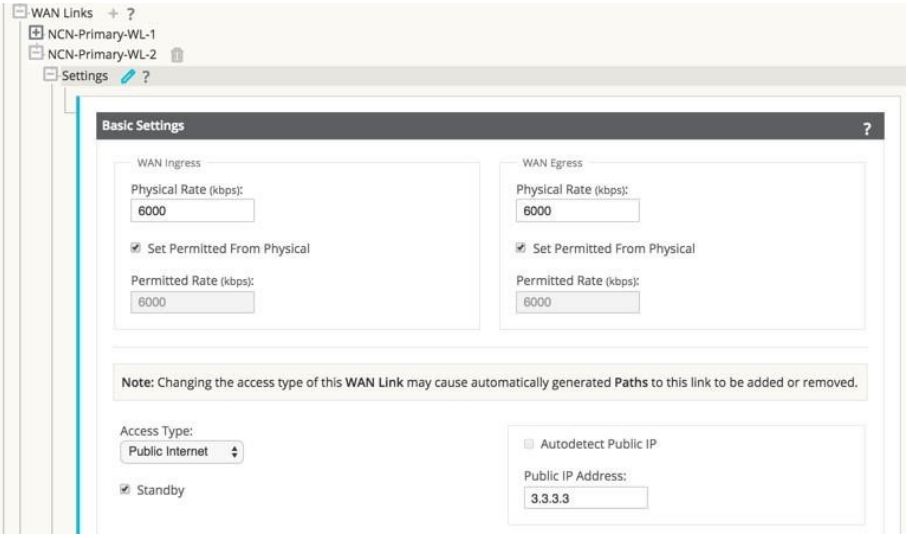


Figure 32: Standby WAN Link on Public Internet Connection

Monitoring

A Path that has at least one Standby WAN Link as an endpoint is considered a backup Path. Under **Monitor**, and then **Statistics** all functions for Paths are supported regardless of whether a Path is configured as a backup Path in Edge 5.0.

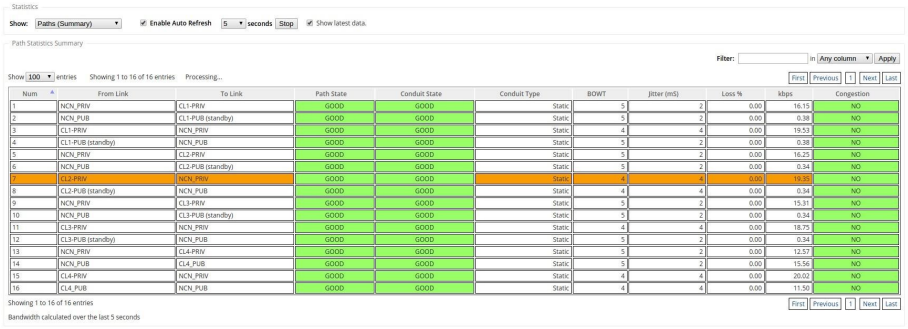


Figure 33: Paths (Summary) Including Standby WAN Links

Figure 34: Paths (Summary) Including Standby WAN Links Filtered

12

Release 5.1 Features

This chapter includes features and enhancements released in 5.1.

Virtual Appliance VT800

Edge 5.1 introduces support for the new 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.

Alarm System

Edge 5.1 introduces a new Alarm System that streamlines the configuration and number of severity based alerts for network administrators. Now you can configure contextually-based alarms with specific criteria for triggering and clearing alarm states. To configure an Alarm:

1. Under **Integrate Configure Alarms**, click the **Add Alarm** button.
2. Select an **Event Type** from the drop-down menu.

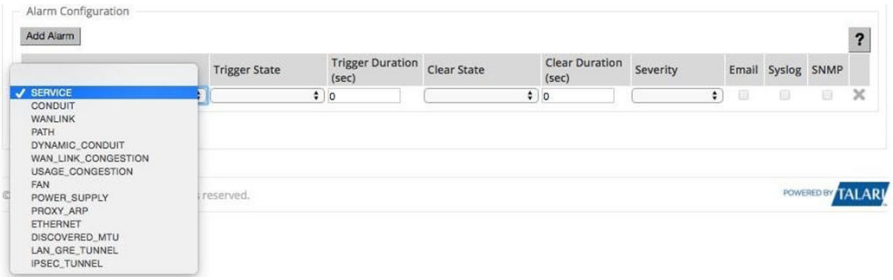


Figure 1: Select Event Type

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.

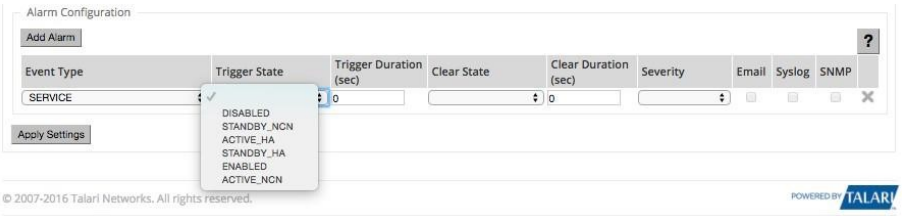


Figure 2: Select Trigger State

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 dropdown menu are determined by the Trigger State.

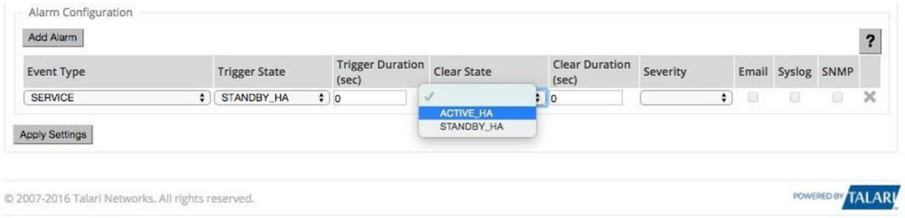


Figure 3: Select a Clear State

1. Enter the amount of time (in seconds) in the **Clear Duration** field that the Event Type must remain in the Clear State to clear 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 and is also displayed with the Alarm under **Diagnose View/Clear Alarms**.

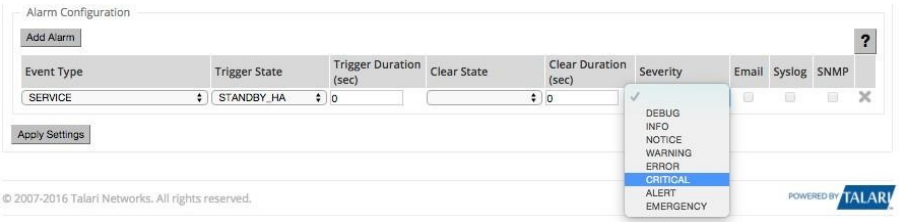


Figure 4: Choose a Severity

1. Select the alert delivery method by clicking the **Email, Syslog,** and **SNMP** checkboxes. You can select multiple delivery methods, however, even if you do not choose a delivery method, an alarm is produced that you can view on the **View/Clear Alarms** page.
2. Click **Apply** to save the alarm.
3. Repeat steps 1 through 8 to add additional Alarms.

Diagnose Alarms

To diagnose network issues based on current Alarms, you can use the Diagnose Alarm page to see a list of all current Alarms. Click **Diagnose**, and then **View/Clear Alarms** to sort and filter the list of Alarms, or clear them by clicking the **Clear Action** checkbox at the end of an Alarm row then clicking the **Clear Checked Alarms** button near the top of the page. Click the **Clear All Alarms** button to clear all current alarms.

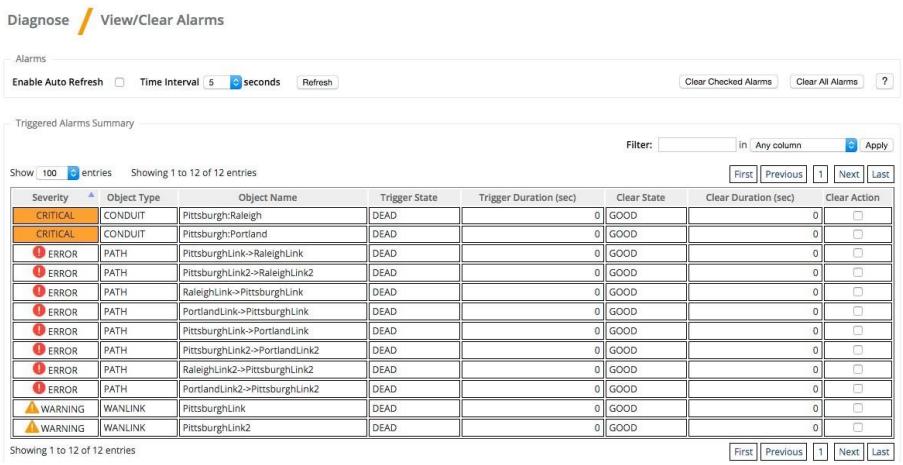
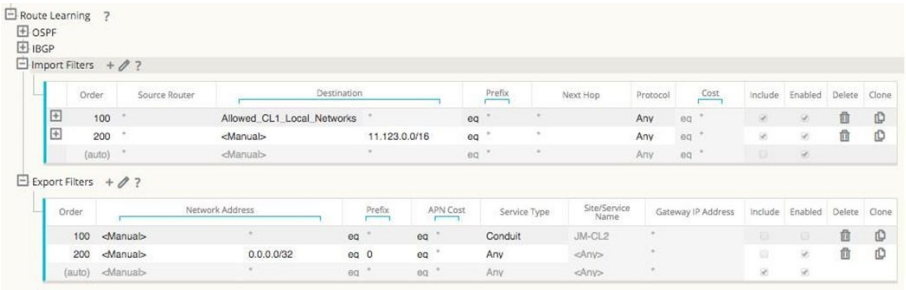


Figure 5: View or Clear Alarms

Route Export Filters

For networks in which Route Learning has been enabled, Edge 5.1 provides more fine grained control over which Edge routes are advertised to routing neighbors rather than advertising all or no routes. Export Filters are used to include or exclude routes for advertisement via OSPF and IBGP based on specific match criteria.

Under **Connections**, and then **(Site Name)**, and then **Route Learning** in the Configuration Editor, **Import Filters** are separate and distinct from **Export Filters.** You may configure up to 32 Export Filters.



You can use the following criteria to construct each Export Filter that you create:

- **Order:** The Order in which filters are prioritized. The first filter that a route matches to will be applied to that route.
- **Service Type:** To match filters from a specific routing domain, choose one of the configured Routing Domains from the drop-down menu.

- **Network Address:** Enter the IP Address and Netmask or configured Network Object that describes the route's network.
- **Prefix:** To match routes by prefix, choose a match predicate from the drop-down menu and enter a Route prefix in the adjacent field.
- **APN Cost:** The method (predicate) and the APN Route Cost that are used to narrow the Selection of routes exported.
- **Service Type:** To match routes by Service Type, select the Service Type (e.g., Local, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel, or Passthrough) from a list of existing, supported Services.
- **Site/Service Name:** If you select a Service Type, you may also need to select a specific Site or Service Name
- **Gateway IP Address:** If you choose LAN GRE Tunnel as the Service Type, enter the Gateway IP for the tunnel.
- **Include:** Click the checkbox to **Include** routes that match this filter. Otherwise matching routes are ignored.
- **Enable:** 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.

Operating System Patching

To facilitate the expeditious distribution of Debian patches to customers, those patches will now be bundled in new OS patches that are separate from Edge Software updates and full OS updates. OS patches can be independently uploaded and installed to the active OS partition on Oracle Talari Appliances running OS 4.1 or later and each patch builds on the previously uploaded patch.

To see the Currently Installed Patch Level, navigate to **Manage Appliance OS Partitions.** To upload new OS patches, scroll down to the **OS Patch Network Upload** area of the page.

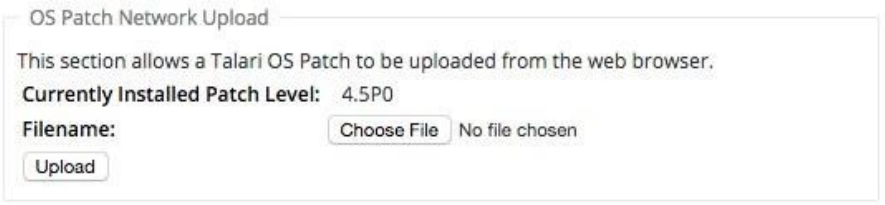


Figure 7: OS Patch Network Upload

Once you download a new patch to your local machine, click the **Choose File** button to select the file you downloaded and click **Upload** to install the patch to the active OS partition on your Oracle Talari Appliance. For a more in depth explanation of OS patching, please refer to the *OS Partition Update Guide.*

Customizable Web Console

Now you can customize the look and feel of your Oracle Talari Appliance's Web Console. Edge 5.1 allows network administrators to add a Custom Login Message, a Custom Support Link, and Upload a Custom Logo to brand their Oracle Talari Appliances' web interfaces.

From the **Manage Appliance HTTPS Settings** in the **Custom Login Message** area, 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. When you are done, click the **Save Login Message** button to save the message.

Figure 8: Custom Login Message

In the **Custom Support Link** area of the **HTTPS Settings** screen enter a **Support Link Name** and your organization's **Support Link URL** to create a link on the appliance login page.

Figure 9: Custom Support URL

From the **Upload Custom Logo** section on the **HTTPS Settings** screen, you can upload a logo to replace the Talari logo on your appliance. Click the **Choose File** button, choose the logo image you want to upload, and click **Upload Custom Logo.** If you need to remove the logo you updated, click **Remove Custom.**

Figure 10: Custom Logo

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

Figure 11: Customized Web Console

DHCP Relay and DHCP Server

Edge 5.1 introduces the ability to use your Oracle Talari Appliances as either DHCP Servers or DHCP Relay Agents to simplify your network's configuration. Now you can use your Oracle Talari Appliances to issue IP Addresses via DHCP or forward DHCP packets between clients and servers where necessary.

> **Note:**
>
> DHCP Relay and DHCP Server require appliances to be running OS 4.5 or later.

Management Interface DHCP Server

From the **Manage Appliance Local Network Settings** screen you can now configure the **Management Interface DHCP Server**. Click the **Enable DHCP Server** checkbox to start the server, then enter the **Lease Time** (in minutes), the **Domain Name**, and define the IP Address range by entering a **Start IP Address** and an **End IP Address.**

Figure 12: Configure DHCP Server

Click the **Change Settings** button to finish configuring the DHCP Server. Click the **Show Clients** button to view the current DHCP clients, and click the **Clear Clients** button to release the current DHCP Client Leases.

> **Note:**
>
> If you plan to use DHCP Server on an Oracle Talari 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.

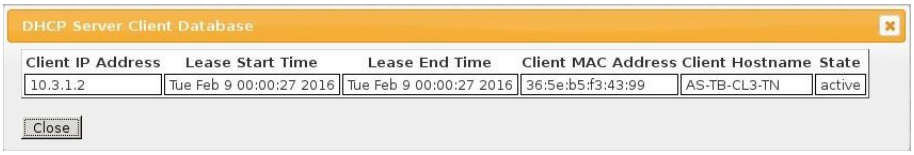


Figure 13: DHCP Server Client Database

DHCP Relay

Network administrators can use the DHCP Relay service on the management port of Oracle Talari 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 Oracke Talari Appliances as DHCP Replay Agents.*

From the **Manage Appliance Local Network Settings** Screen you can configure the **Management Interface DHCP Relay.** Click the **Enable DHCP Relay** checkbox to enable the service. Enter the **DHCP Server IP Address** and click the **Change settings** button to begin using your appliance as a DHCP Relay Agent.

> **Note:**
>
> If you plan to use DHCP Relay on an Oracle Talari 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.

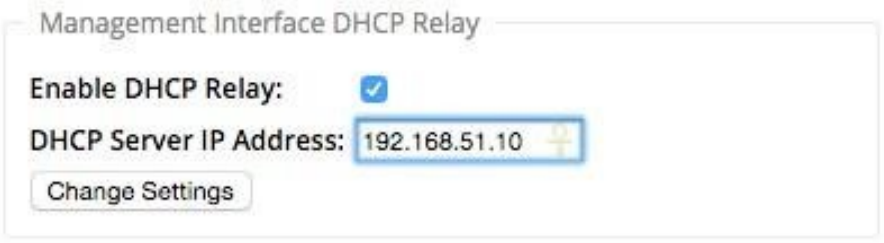


Figure 14: Enable DHCP Relay

13

Release 5.2 Features

This chapter includes features and enhancements released in 5.2.

Support for 550 Sites

Edge 5.2 supports the ability for a T5200, functioning as an NCN, to create up to 550 static Conduits without loss of performance and with full support for all previously existing features, including up to 16,000 Routes. The user also gains the ability to have up to 23,000 WAN Paths, 11,000 WAN Links, 512,000 Flows, and 200,000 Rules.

Stateful Firewall

Edge 5.2 provides a firewall built into the Oracle Talari Application. The firewall allows Policies between Services and Zones, and supports Static NAT, Dynamic NAT (PAT), and Dynamic NAT with Port Forwarding. Additional firewall capabilities include:

- Filtering traffic flows between Zones
- Filtering traffic between services within a Zone
- Filtering traffic between services that reside in different Zones
- Filtering traffic between services at a site
- Defining Filter Policies to Allow, Deny, or Reject flows
- Tracking flow state for selected flows
- Applying Global Policy Templates
- Support for Port Address Translation for traffic to the Internet on an untrusted port, as well as port forwarding inbound and outbound

To simplify the configuration process, firewall Policies are created at the Global level. This Global configuration consists of Pre-Appliance and Post-Appliance site Policy Templates that can be applied to all sites within Edge. For a more in-depth explanation of the Stateful Firewall feature in Oracle SD-WAN Edge 5.2 GA, please refer to *SD-WAN Firewall Configuration Guide.*

DHCP Relay & DHCP Server

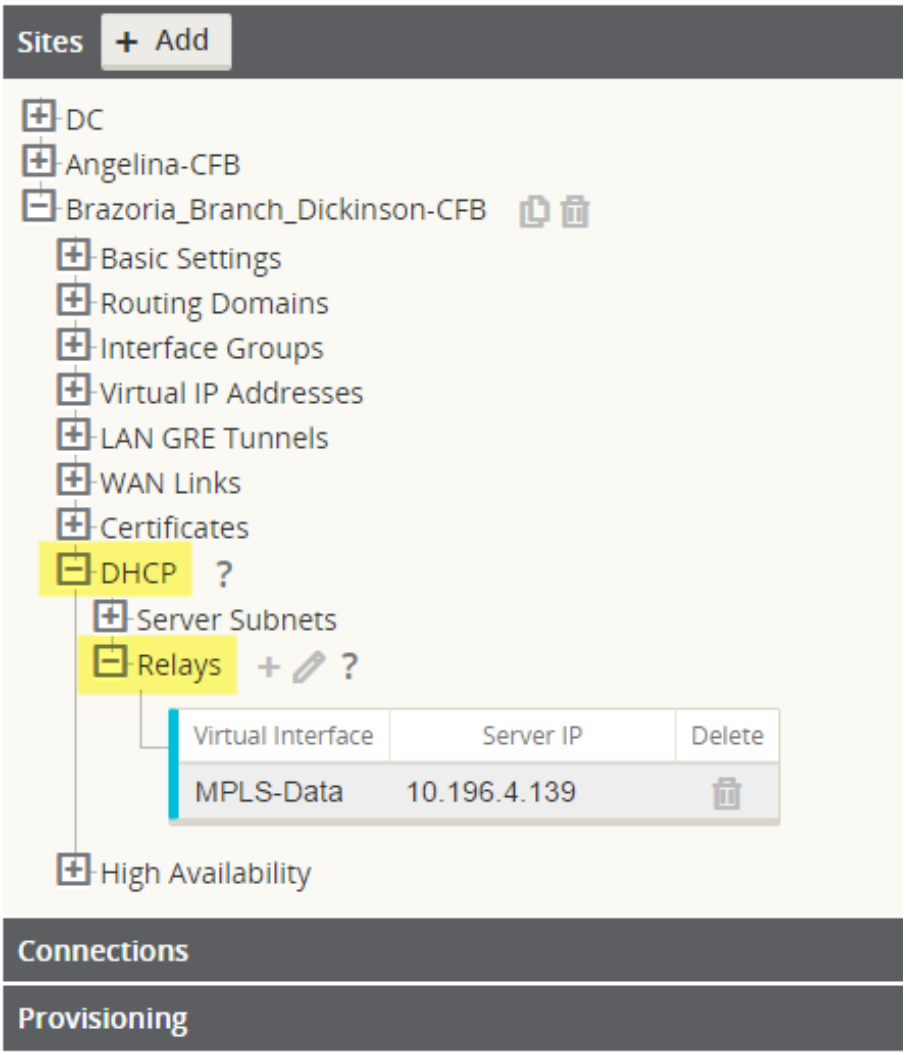
Devices on the same network as the Oracle Talari Appliance's LAN/VLAN interface may now use the DHCP Relay & DHCP Server features to provide those devices with their IP configuration. These features help to simplify the client site network by reducing the amount of equipment necessary.

- DHCP Relay

Network administrators can now use the DHCP Relay service on data ports of Oracle Talari 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 **Manage Network > Configuration Editor > Sites > [Site Name] > DHCP.** Expand **Relays** then specify the data ports to be used and the Server IP address.



- DHCP Server

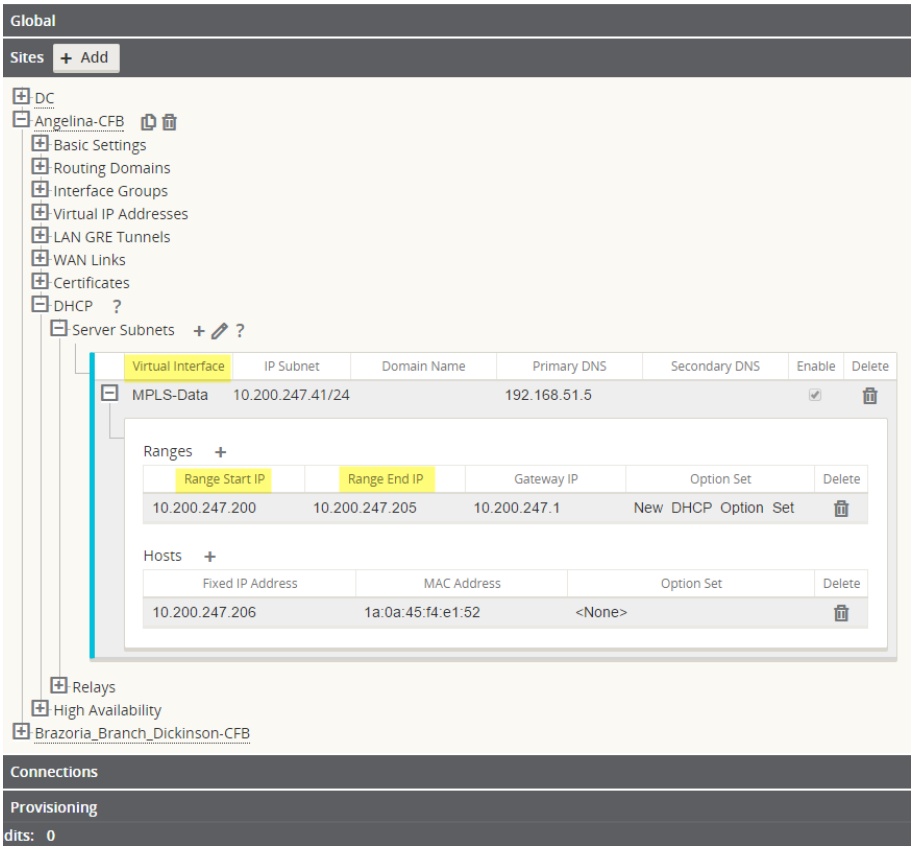
Network administrators can now also use the DHCP Server feature on data ports of Oracle Talari Appliances to allow local hosts to acquire dynamic or static IP addressing directly from the Oracle Talari Appliance.

To configure DHCP Server:

1. Navigate to **Manage Network > Configuration Editor > 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.

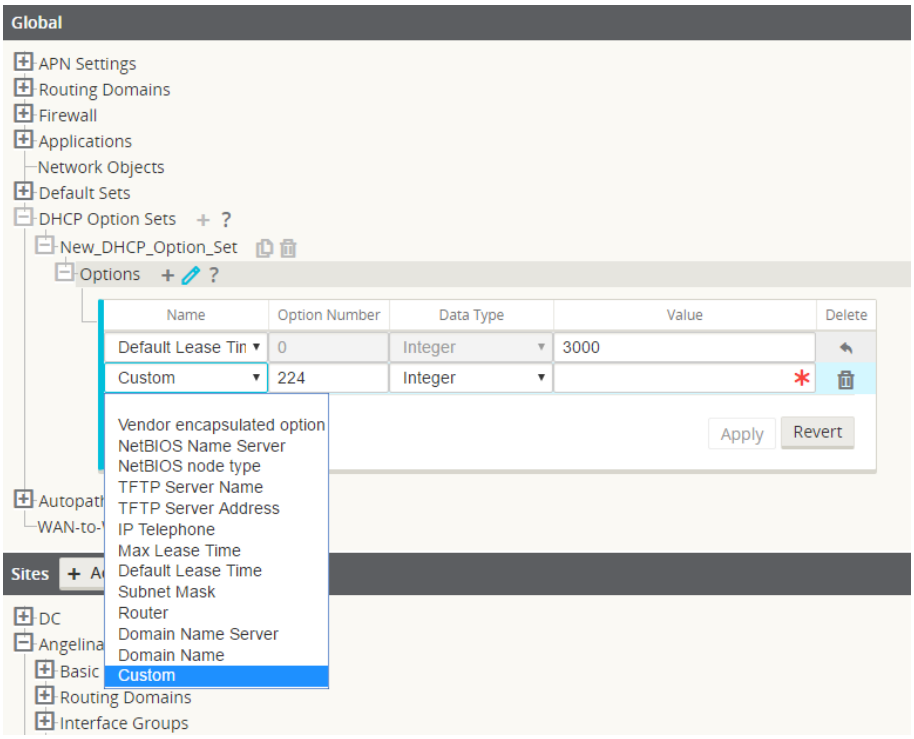
Users may also choose to enter additional information in this section that hosts will then be configured with as well, such as gateway IP, DNS, and an Option Set (described below).

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

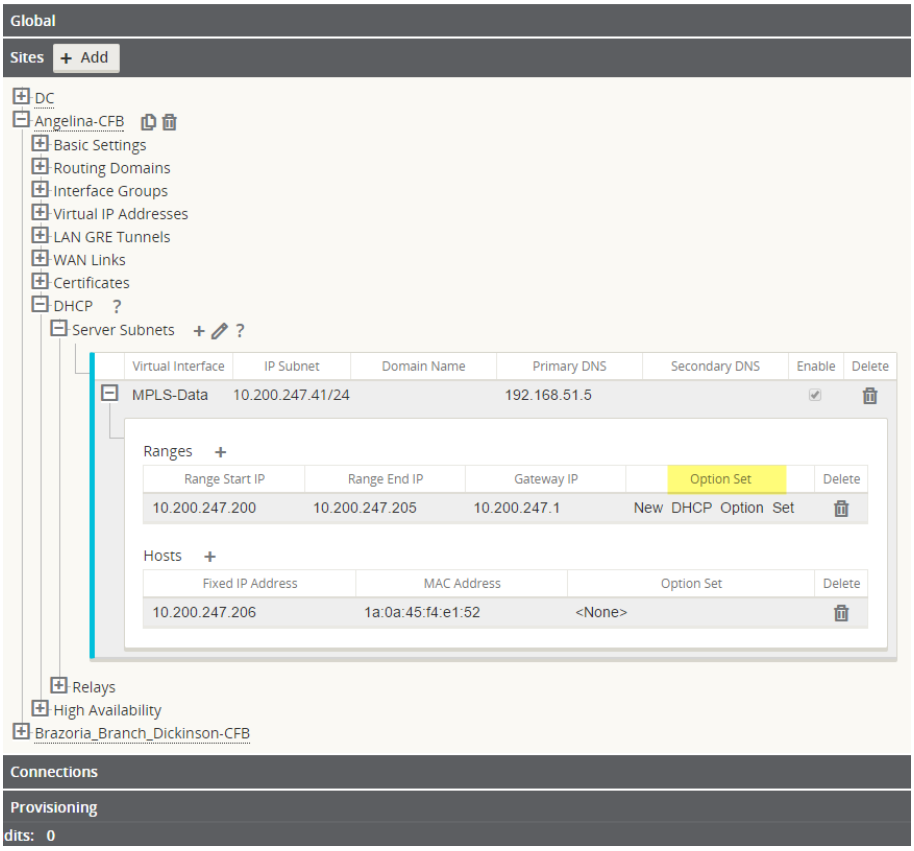


> **Note:**
>
> The following feature is optional, not required.

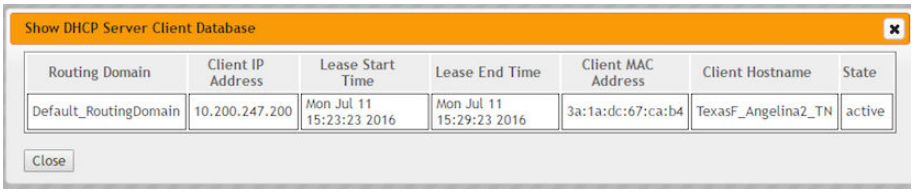
DHCP Option Sets are a group of DHCP settings or paramters that can be applied to inidividual IP address ranges. To create DHCP Option Sets, navigate to the **Global** section of the configuration and expand **Options**. Enter the required settings you would like to include in the set, then click **Apply**.



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.



To view a list of Clients from the DHCP Server Database, navigate to **Monitor > DHCP** from the web UI.

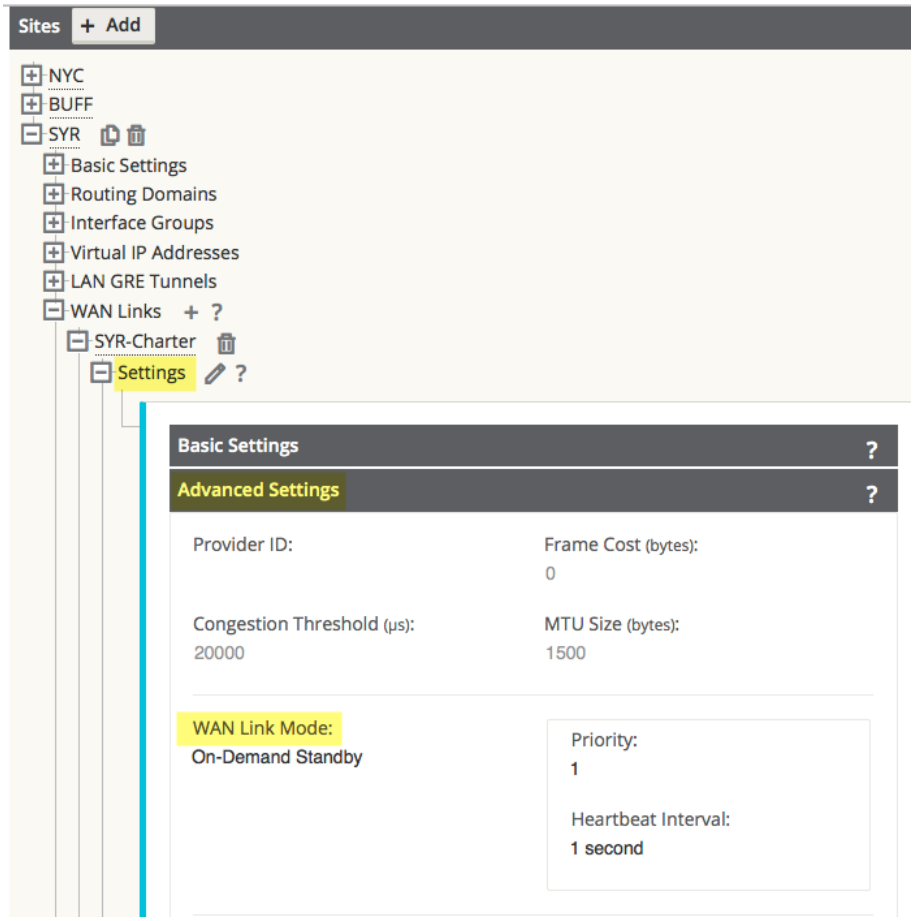


Standby WAN Link (VSAT)

Introduced in 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).

Below are steps to enable this feature. This example chooses the On-Demand Standby option:

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

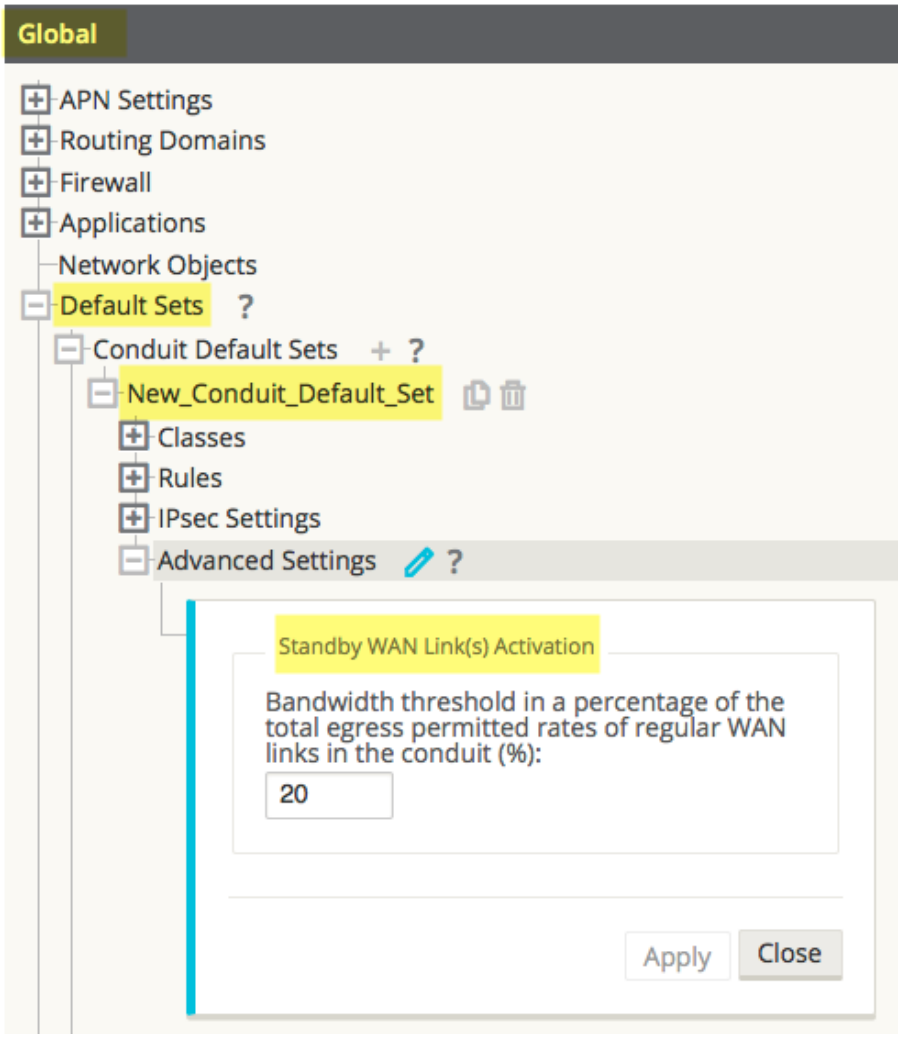


The **Priority** option is a value to indicate which Standby WAN Link will be activated in which order and the **Heartbeat Interval** can either be set or disabled.

> **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.

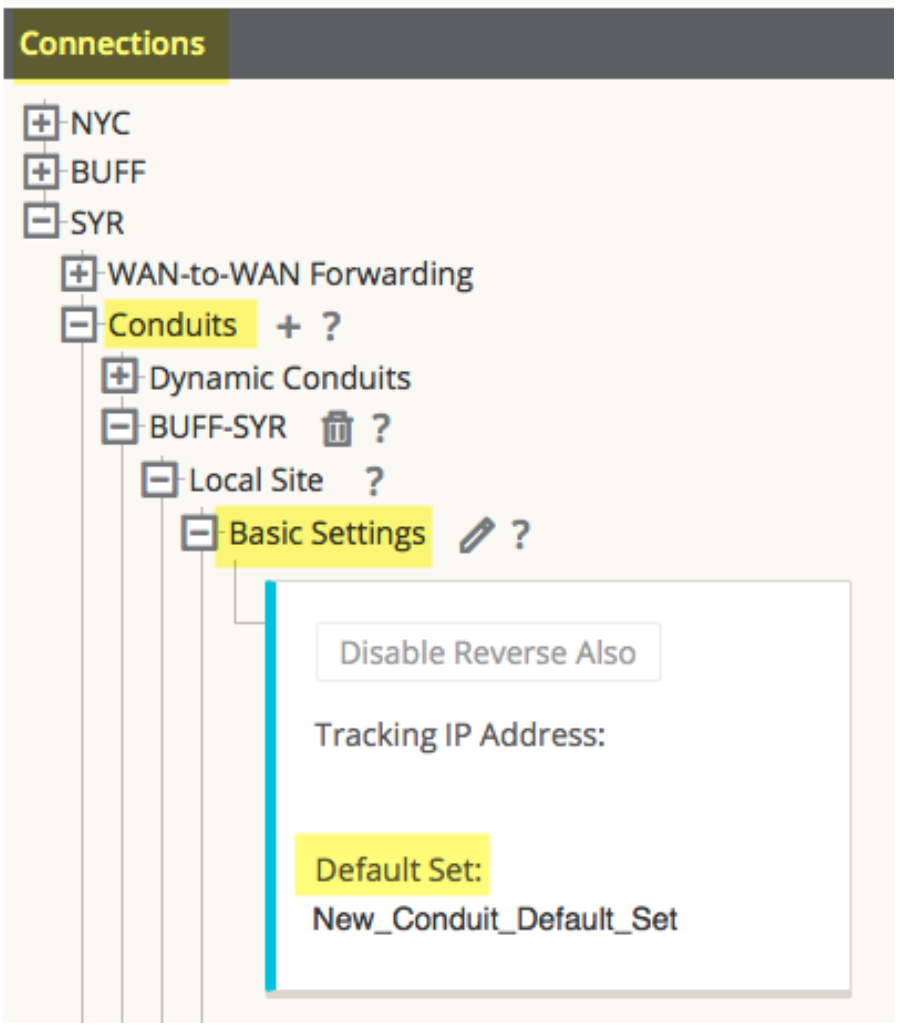
2. Create a Default Set in the **Global** section that will be used for Conduits using the Standby WAN Link.



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

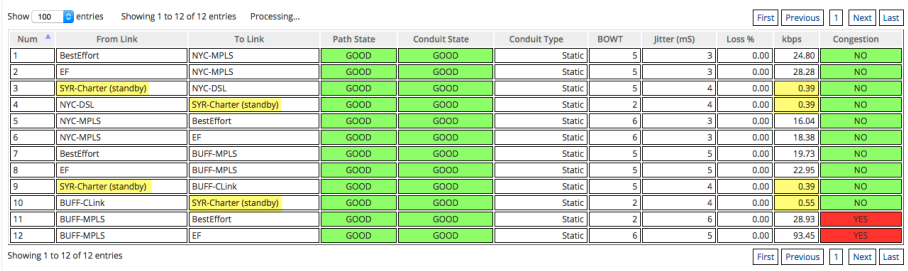
available bandwidth provided by the regular WAN Links in the conduit falls below this bandwidth threshold, On-Demand Standby WAN Links in the Conduit will be activated to supplement bandwidth.

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.

Output from the **Monitor > Statistics** page of the web UI will let you know which WAN Links are in Standby mode. The user will observe minimal amounts of traffic traversing such links, depending on how the Heartbeat Interval and Activation thresholds have been configured.



Show 100 entries Showing 1 to 12 of 12 entries Processing... First Previous 1 Next Last

Num	From Link	To Link	Path State	Conduit State	Conduit Type	BOWT	Jitter (mS)	Loss %	kbps	Congestion
1	BestEffort	NYC-MPLS	GOOD	GOOD	Static	5	3	0.00	24.80	NO
2	EF	NYC-MPLS	GOOD	GOOD	Static	5	3	0.00	28.28	NO
3	SYR-Charter (standby)	NYC-DSL	GOOD	GOOD	Static	5	4	0.00	0.39	NO
4	NYC-DSL	SYR-Charter (standby)	GOOD	GOOD	Static	2	4	0.00	0.39	NO
5	NYC-MPLS	BestEffort	GOOD	GOOD	Static	6	3	0.00	16.04	NO
6	NYC-MPLS	EF	GOOD	GOOD	Static	6	3	0.00	18.38	NO
7	BestEffort	BUFF-MPLS	GOOD	GOOD	Static	5	5	0.00	19.73	NO
8	EF	BUFF-MPLS	GOOD	GOOD	Static	5	5	0.00	22.95	NO
9	SYR-Charter (standby)	BUFF-CLink	GOOD	GOOD	Static	5	4	0.00	0.39	NO
10	BUFF-CLink	SYR-Charter (standby)	GOOD	GOOD	Static	2	4	0.00	0.55	NO
11	BUFF-MPLS	BestEffort	GOOD	GOOD	Static	2	6	0.00	28.93	YES
12	BUFF-MPLS	EF	GOOD	GOOD	Static	6	5	0.00	93.45	YES

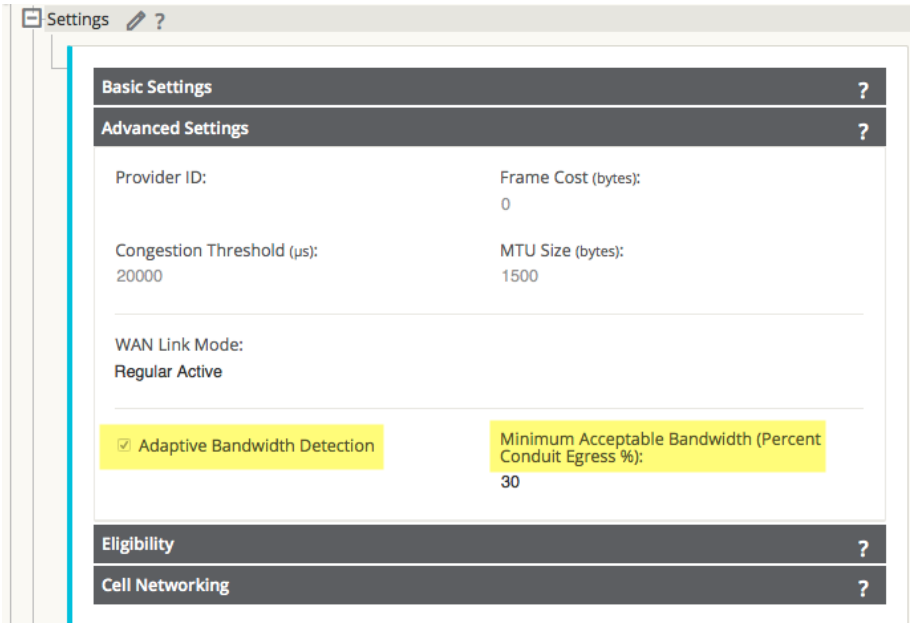
Showing 1 to 12 of 12 entries First Previous 1 Next Last

Adaptive Bandwidth Detection

This feature is introduced in 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 Oracle Talari 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:

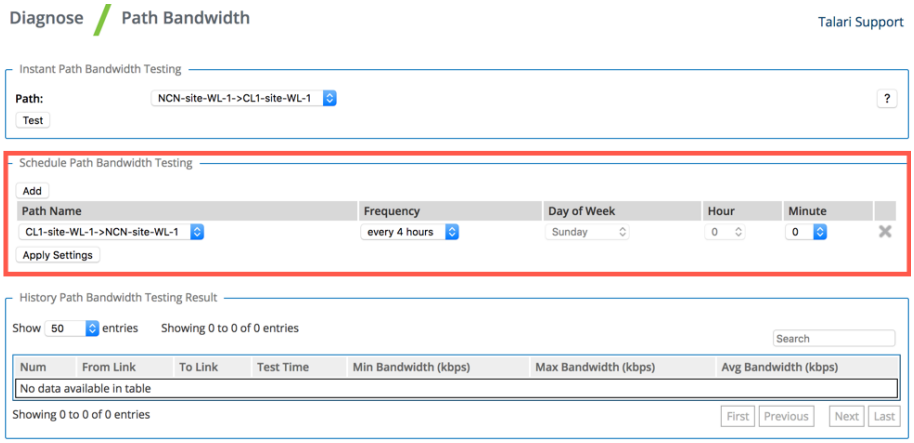
1. In the Configuration Editor, navigate to **Sites > [Site Name] > WAN Links > [WAN Link Name] > Settings > Advanced Settings.**
2. Check the **Adaptive Bandwidth Detection** box and enter in the **Minimum Acceptable Bandwidth.**



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

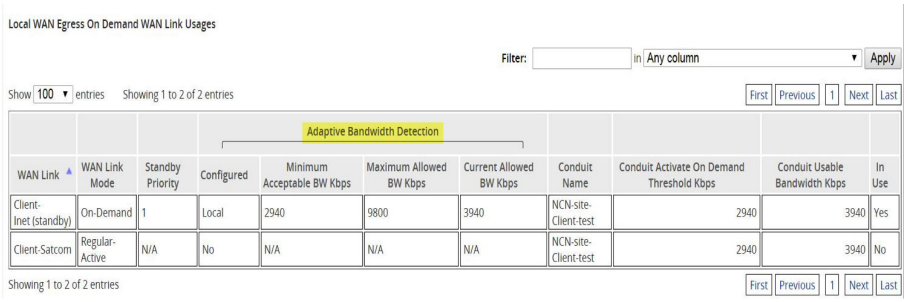
To schedule recurring bandwidth tests after enabling Adaptive Bandwidth Detection:

1. Navigate to **Diagnose > Path Bandwidth**.
2. Under **Schedule Path Bandwidth Testing**, click the Add button. Select the Path Name to test on, Frequency, Day of Week (if applicable), Hour (if applicable), and Minute, then click Apply Settings.



> **Note:**
>
> If Adaptive Bandwidth Detection is configured but recurring bandwidth testing is not scheduled, the bandwidth test will run once and the Oracle Talari appliance will use that one-time result. Recurring bandwidth testing is required for Adaptive Bandwidth Detection to function as intended.

Users may monitor the bandwidth detected on these links from the web UI under **Monitor > Statistics > WAN Link Usage > Local WAN Egress On Demand WAN Link Usages.**



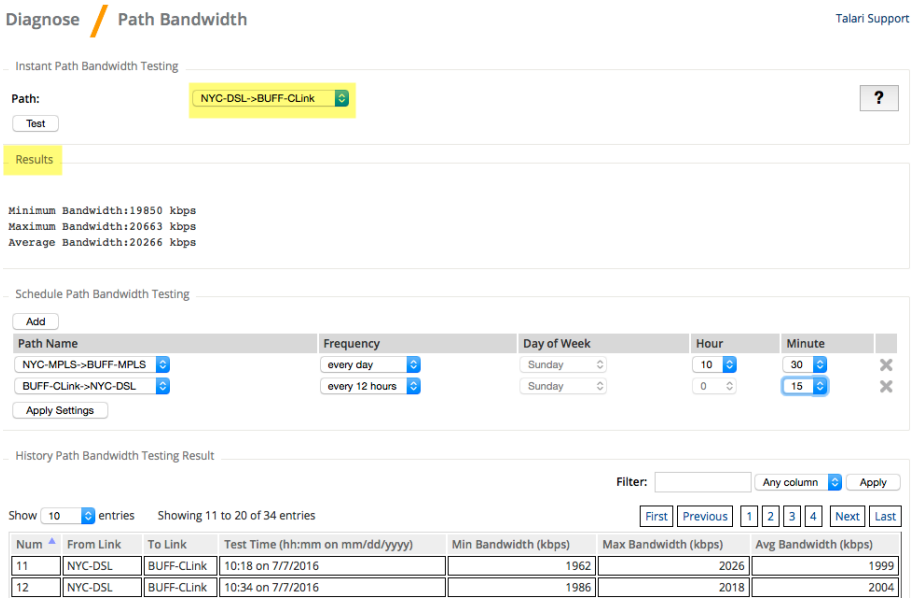
Active Bandwidth Testing

Edge 5.2 provides users the ability to issue an instant path bandwidth test, or to schedule such testing to be completed at specific times on a recurring basis. This feature will be useful for demonstrating how much bandwidth the user has between two locations during new and existing installations, also for testing paths to determine the outcome of setting and confirmation changes, such as adjusting DSCP tag settings or bandwidth Permitted Rates.

To use this tool:

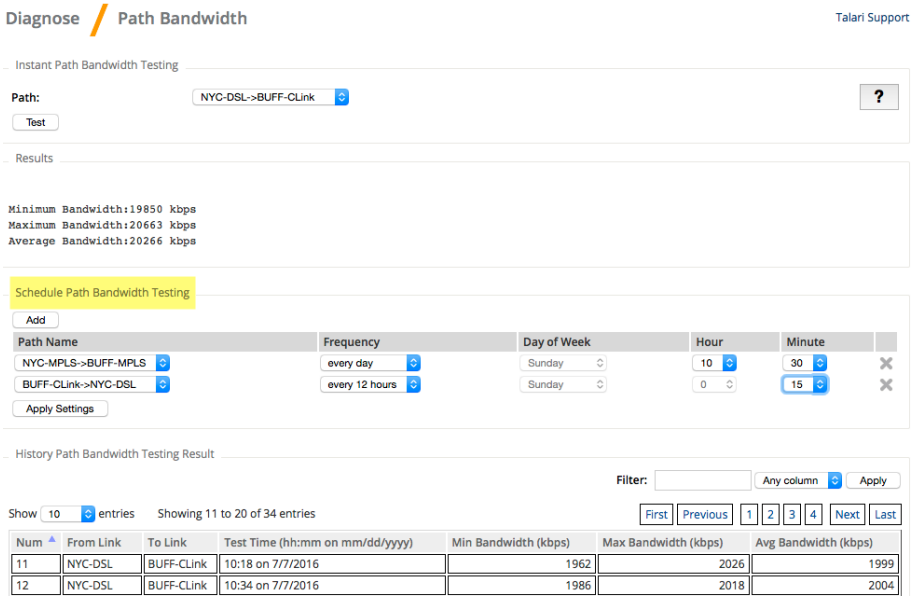
1. Navigate to **Diagnose > Path Bandwidth.**

2. Select the desired Path and click **Test.**



The output will display the minimum, maximum, and average bandwidth results of the test. Along with the ability to test the bandwidth, the user can now change the configuration file to use the learned bandwidth. This is accomplished via the Auto Learn option is under **Site > [Site Name] > WAN Links > [WAN Link Name] > Settings** and if enabled, the system will use the learned bandwidth.

Users may also schedule reoccurring tests of path bandwidth in weekly, daily, or hourly intervals.

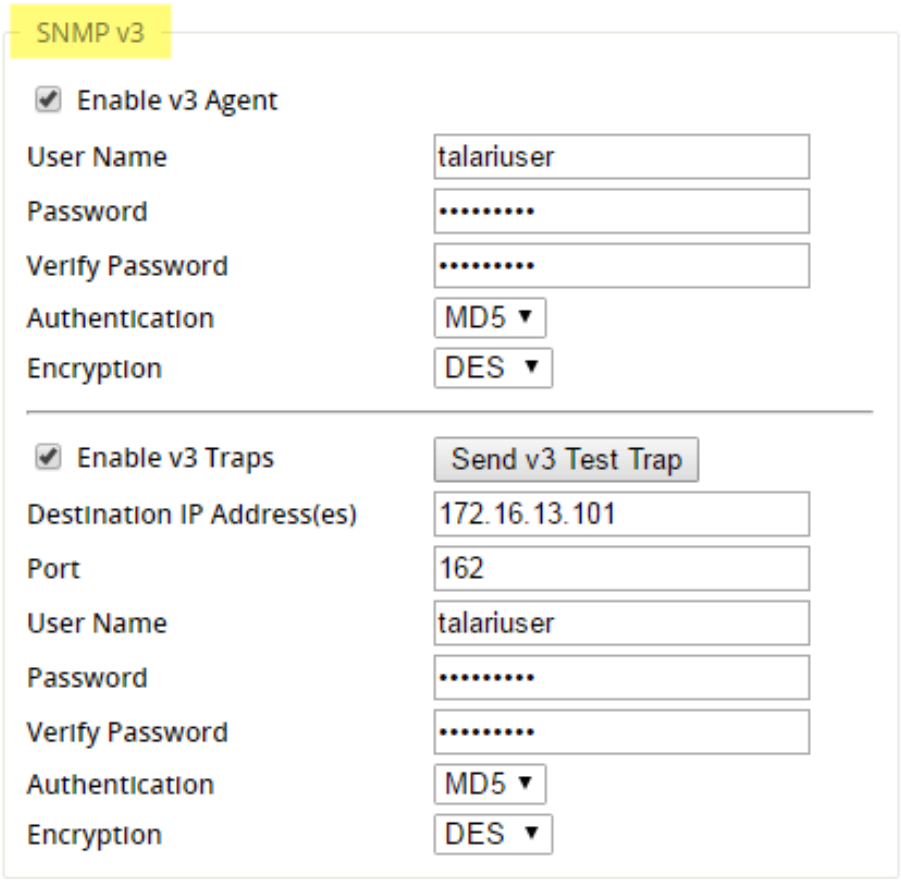


> **Note:**
>
> A history of the path bandwidth testing results will be displayed at the bottom of this page and results will archive every 7 days.

SNMPv3 Polling and Trap Capability

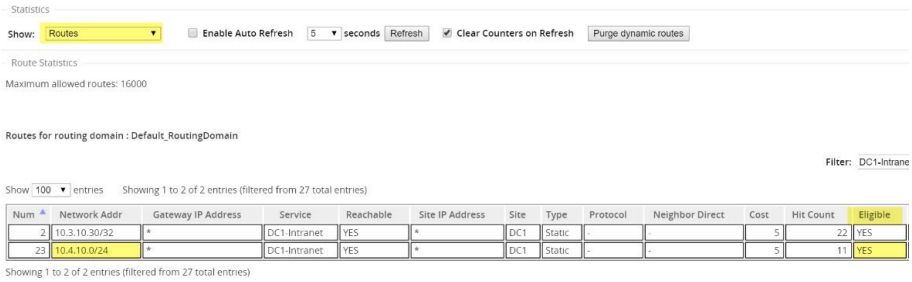
> **Note:**
>
> The platform only supports a single user account for each SNMPv3 capability.

To configure SNMPv3 Polling and Traps, navigate to the SNMPv3 section of the **Integrate > Configure Events and Alerts** page and fill in the fields as required.



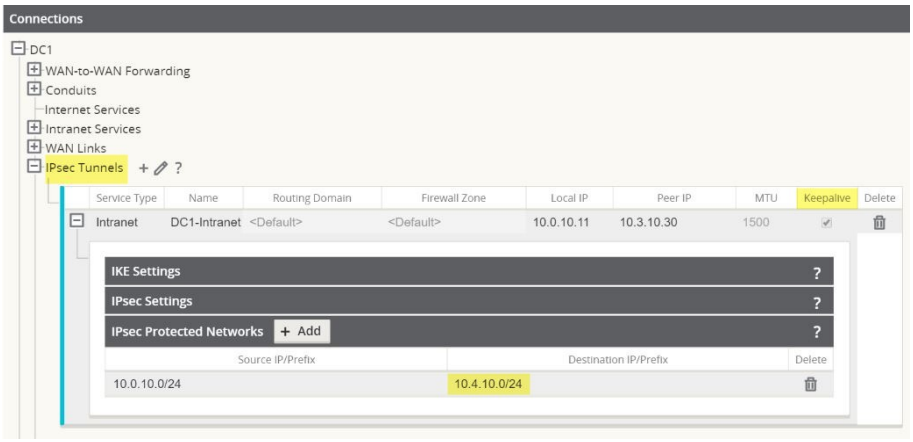
Eligibility for IPsec Non-Conduit Routes

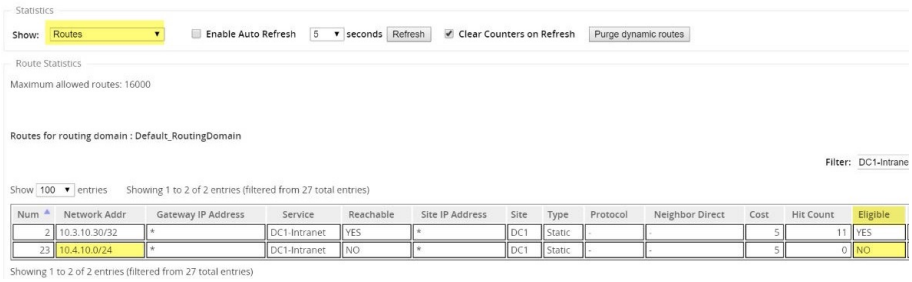
Prior to Edge R5.2, IPsec tunnel routes would remain in the route table even if the tunnel became unavailable.



Routing Table Example A

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 Table Example B

Additional Enhancements

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.

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

Users may now configure a 0.0.0.0/0 route to hairpin 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. Enabling WAN-to-WAN Forwarding to accomplish this is no longer necessary.

14

Release 6.0 Features

This chapter includes features and enhancements released in 6.0.

Application Packet Filtering

> **Note:**
>
> Prior to Edge 6.0 GA, the objects that perform MOS scoring were originally called “Applications” but have been renamed “Rule Groups” in this, and future, releases.

In Edge 6.0 GA, 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

In the Configuration Editor under **Advanced > Global > Applications,** click **Add (+)** to create a new Application that will allow for multiple different criteria.

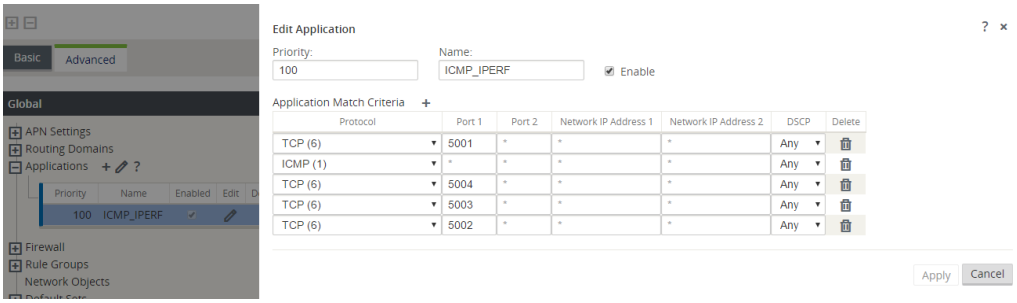


Figure 1: Add a new Application

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.

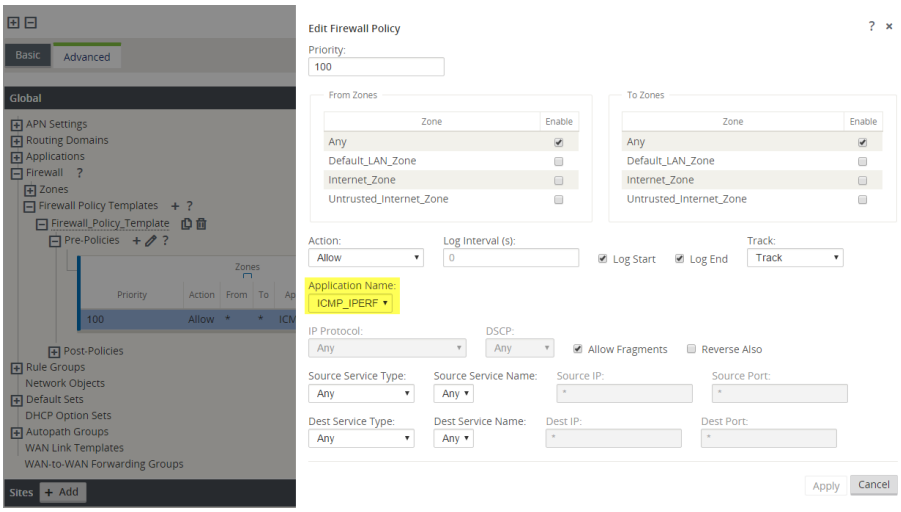


Figure 2: Associating a Global Firewall Policy with an Application

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

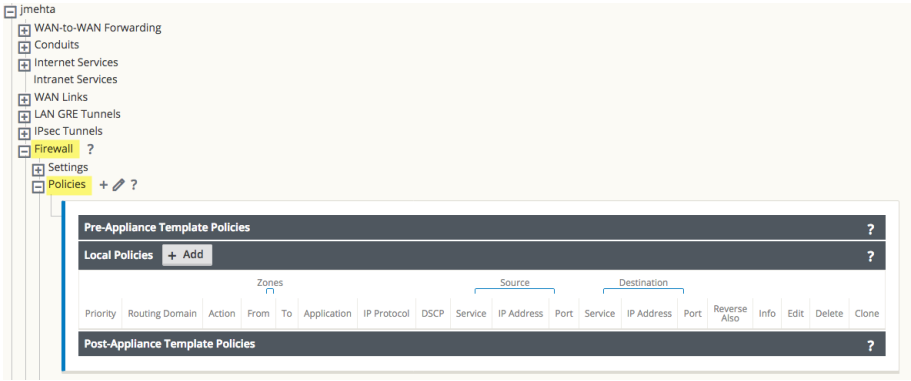


Figure 3: Associating a Firewall Policy with an Application at the Site Level

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**.

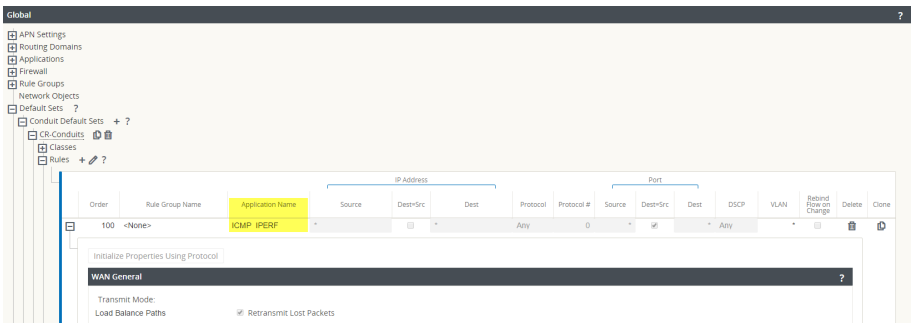


Figure 4: Adding Application to a Global QoS Rule

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.

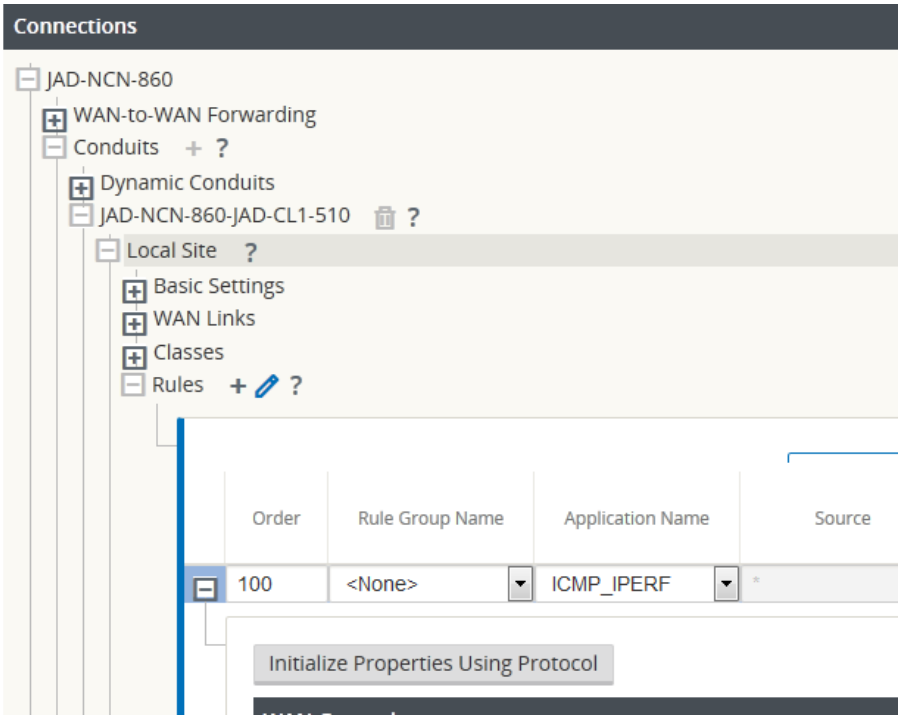


Figure 5: Adding Application to a Local QoS Rule

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.

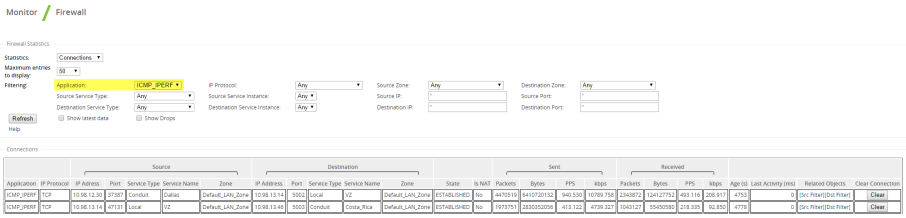


Figure 6: Filtering Firewall statistics by Application

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.

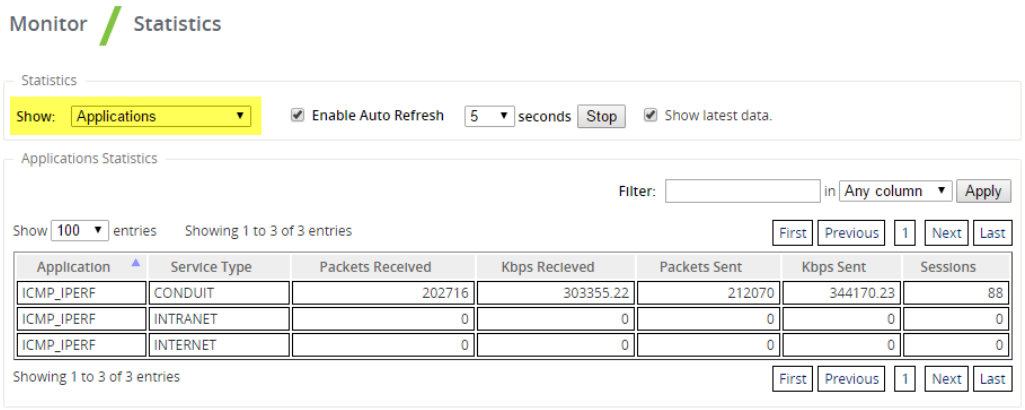


Figure 7: Tracking QoS by Application

VRF Firewall Enhancement

Edge 6.0 GA introduces VRF Firewall enhancements to allow for multiple VRFs, each having access to the Internet. 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 Edge 5.0 *New Features Guide.*

Below are the steps to configure this option:

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 Edge 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.**

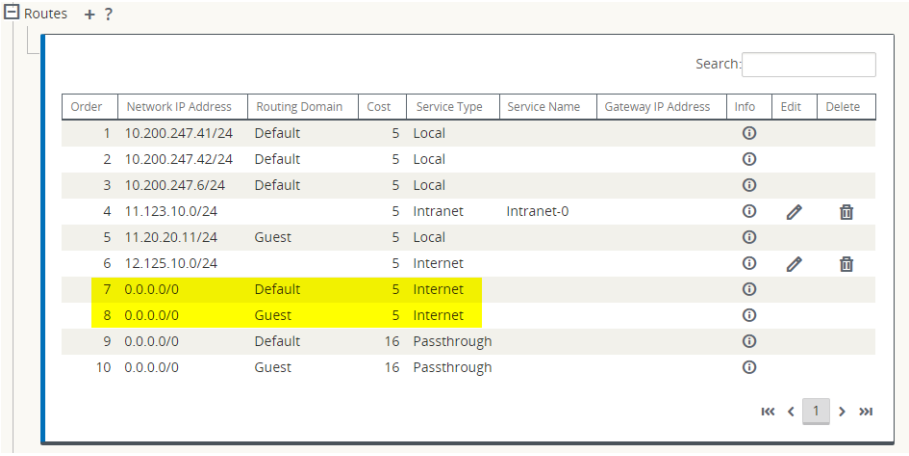


Figure 9: Verifying Routes Added for Each Routing Domain

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

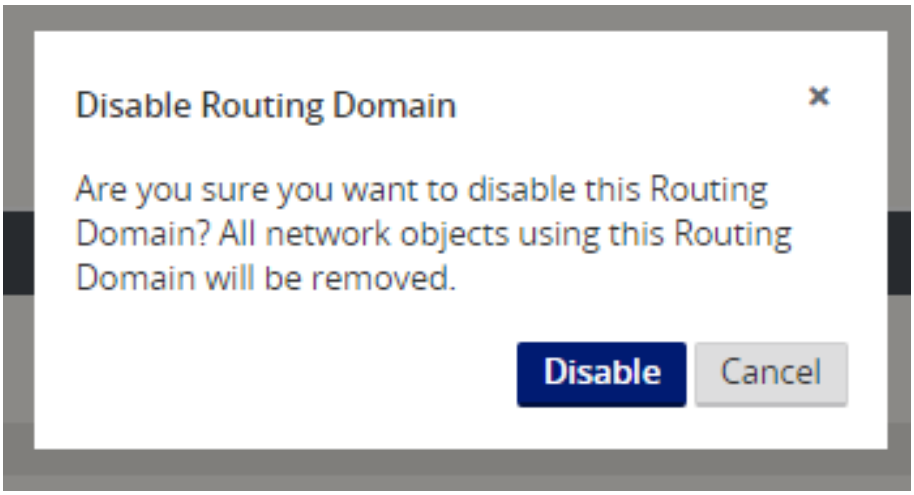


Figure 10: Removing a Routing Domain

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

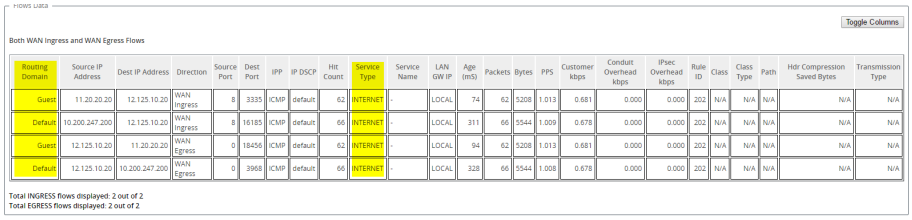


Figure 11: Flows in Routing Domains

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

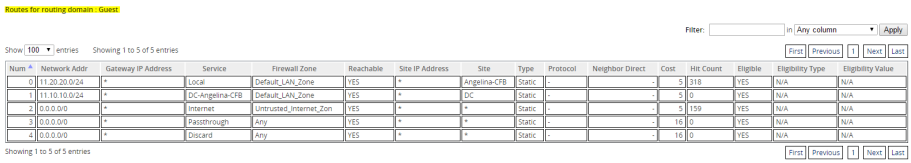


Figure 12: Flows for a Routing Domain

Easy First Install Simplified Appliance Installation

Oracle Talari Appliances going into new sites and RMA replacement appliances going into existing site can now be implemented with ease. A new Edge can now be connected and powered on by a non-technical person. A Network Administrator can add a new site, configure it at the NCN, and upload the software and configuration package to a registration server. This registration server will reside in the cloud. The Client Appliance is then installed and will acquire an IP address from DHCP. Once the Client Appliance has a valid IP address it will contact the registration server, and based on its serial number, download the corresponding package. Once the package is downloaded, it is activated automatically and the site will become operational.

Configuration using Templates

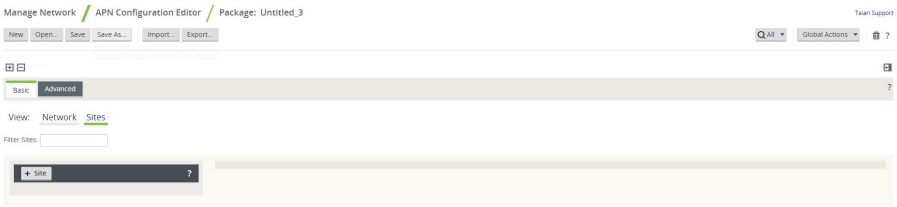
In Edge 6.0 GA, new customers with five or more basic sites to setup for the first time will enjoy time savings while setting up new sites and WAN Links. With the use of templates, users may configure certain settings one-time and then duplicate the settings across more than one site as needed. This 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 Edge 6.0 GA.

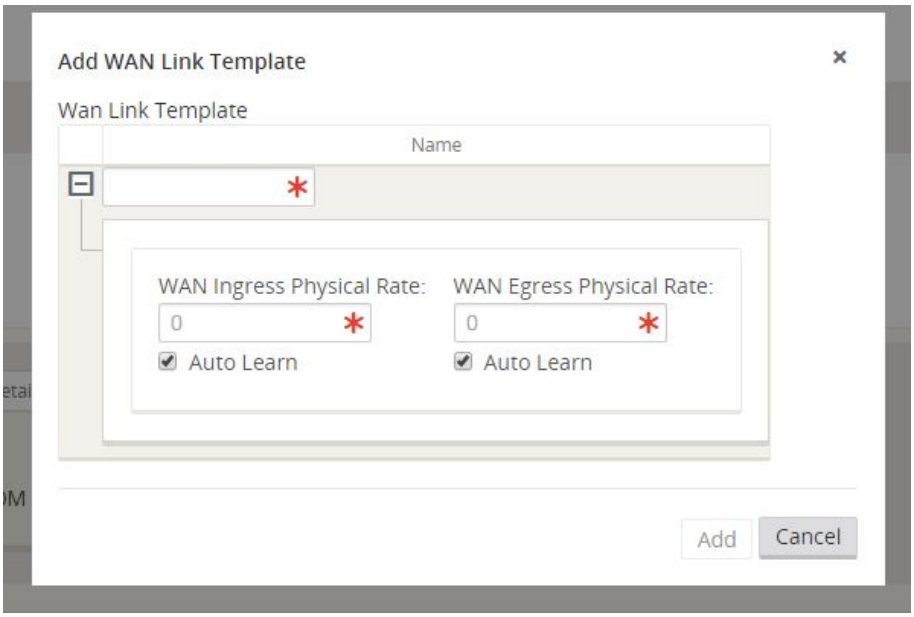
Below are the steps to use this feature through the Basic configuration mode:

Manage Network > Configuration Editor > New > Basic.

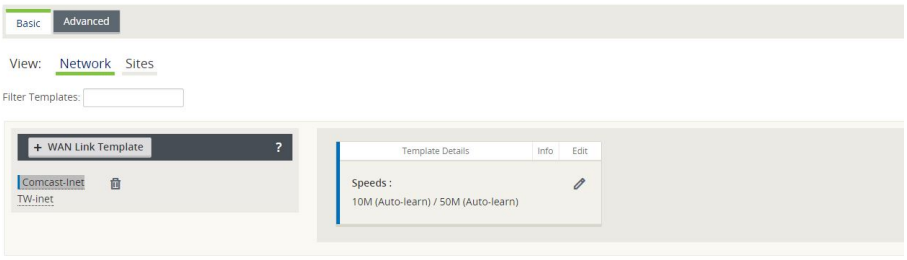


Click Network to change from the (default) Sites view to Network view.

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

Edge 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.

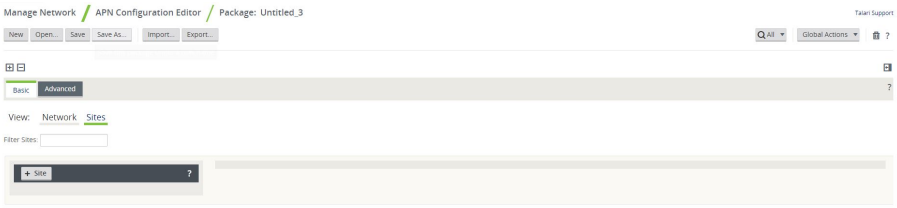
The concept of the **Basic > Sites** view is to simplify the configuration process to allow the user to create a configuration file, which will generate a Conduit between the defined sites. The required configuration properties for a Conduit between sites include:

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

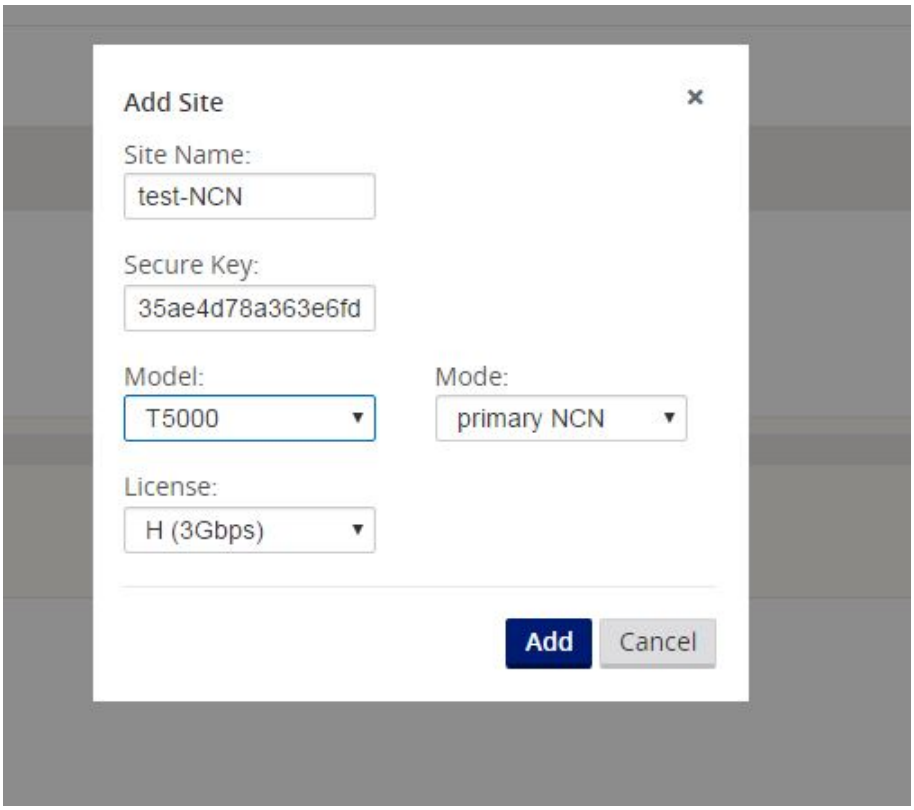
Existing users will observe that one configuration change on the Basic mode view may in fact modify or change more than one setting in Advance mode. Basic mode does allow the Import of existing configurations, and allows the user to move between Basic and Advanced modes.

Below are the steps to use the Basic configuration mode.

Manage Network > Configuration Editor > New > Basic.



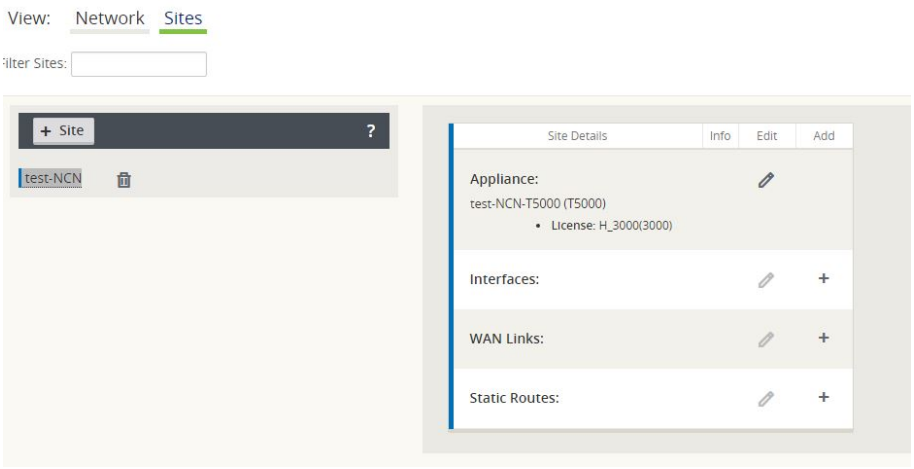
Click **+ Site** and enter basic site details.



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.

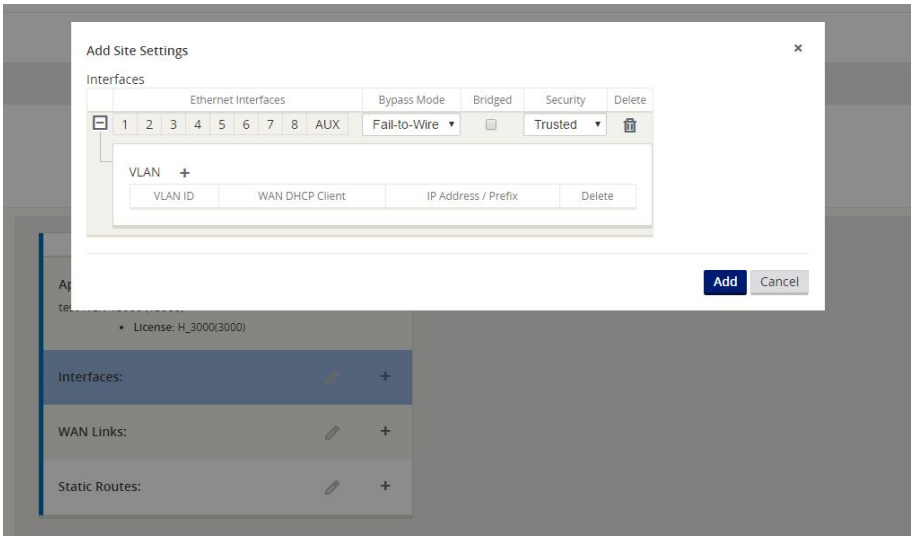
Appliance

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

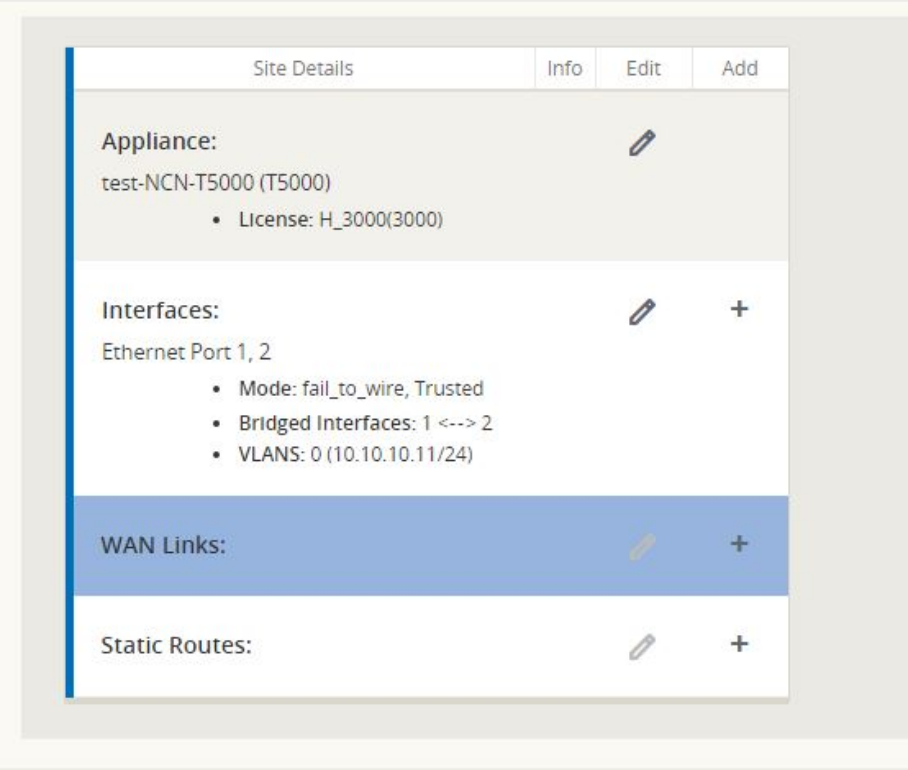
Clicking the Add / Edit Icon to the right of the Interfaces summary view shown for the site will provide the ability to add, edit, and delete Interfaces.



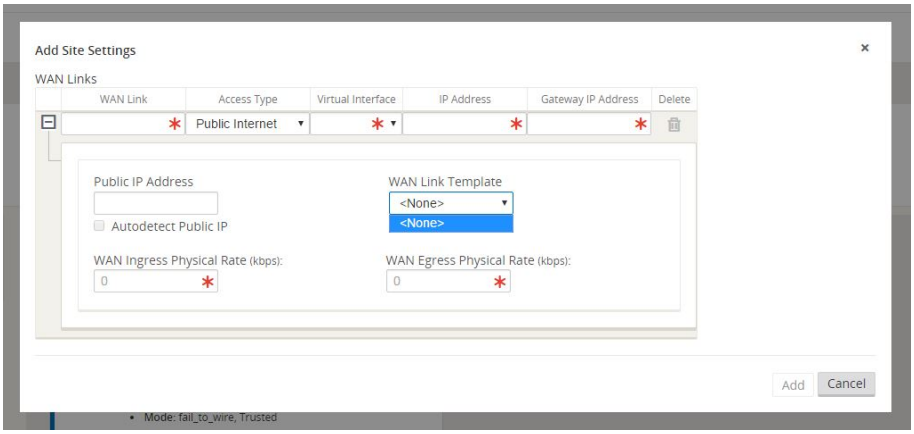
The Interface option allows the user to define the physical topology of the site, such as the ports, logical VLANs and security level for the physical ports. At this level, the user can also define if the WAN interface will use DHCP for an IP address, or they may statically assign an IP address. This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

WAN Links

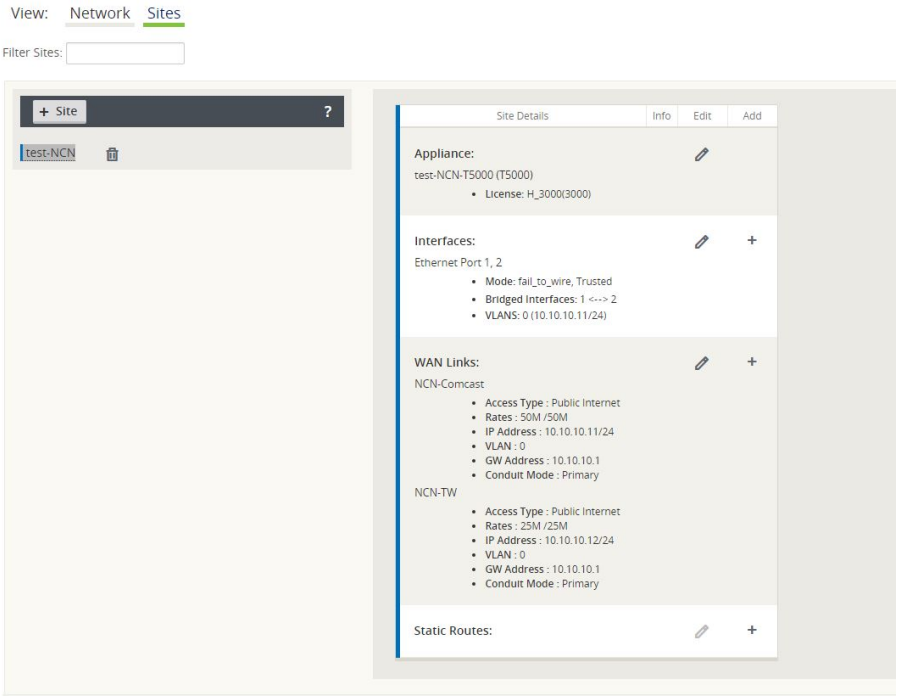
Clicking the Edit Icon to the right of the WAN Links summary view shown for the site will provide the ability to add, edit, and delete WAN Links.



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.

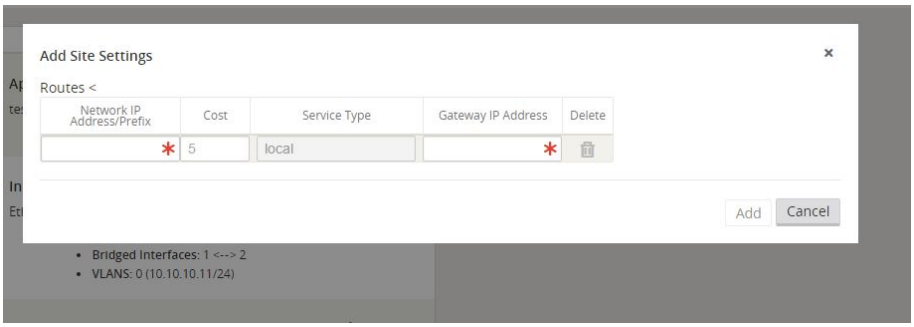


A summary view of WAN Links is then displayed in Basic mode after the initial configuration is complete.

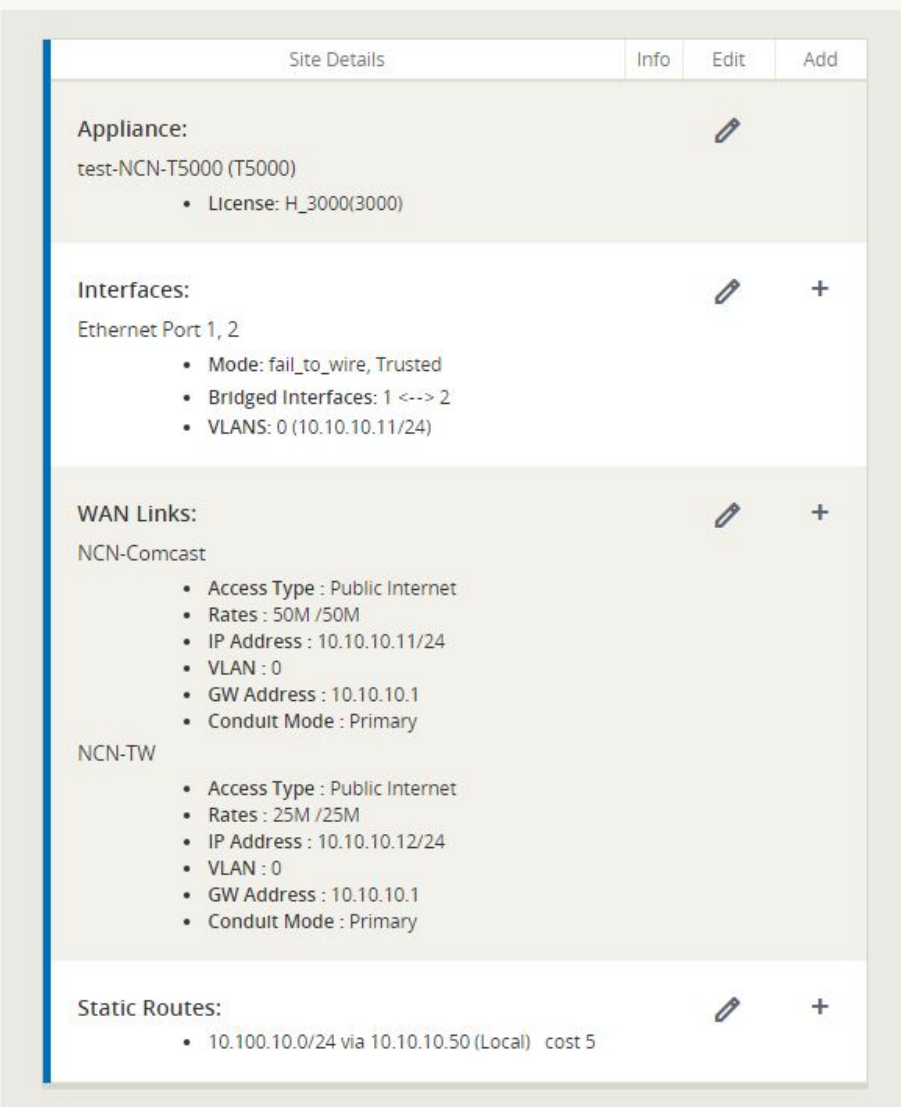


Static Routes

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.

Service Chaining

Edge 6.0 GA now provides support for service chaining on the T860 Appliance with OS 5.0. This capability allows the T860 Appliance to run the application natively and support a Guest VM via KVM. This capability is intended for sophisticated partners. For more information on this capability please contact your representative.

15

Release 6.1 P2 Features

This chapter includes features and enhancements released in 6.1 P2.

Site Templates

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

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

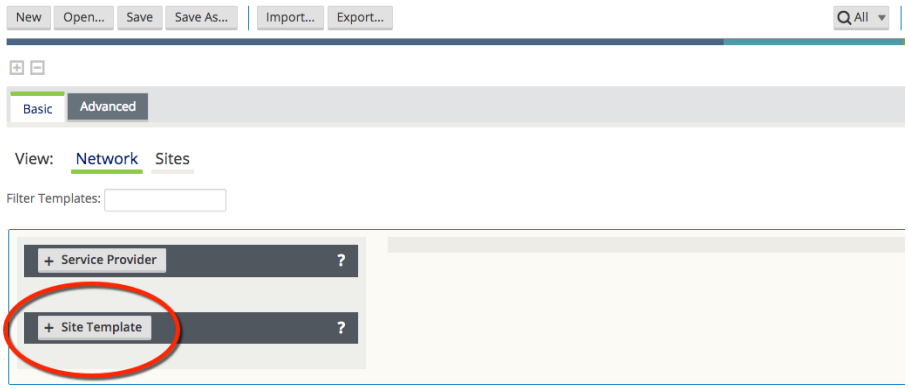


Figure 1

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 that 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.

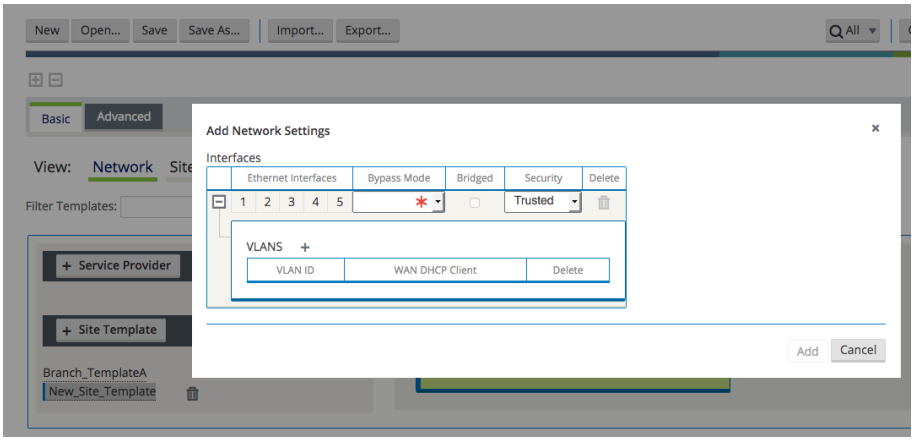


Figure 2

The user will then select which sites should use the template.

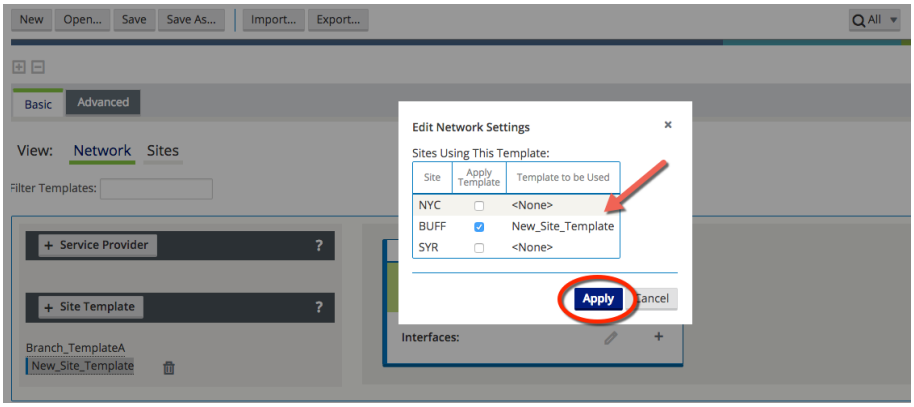


Figure 3

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.**

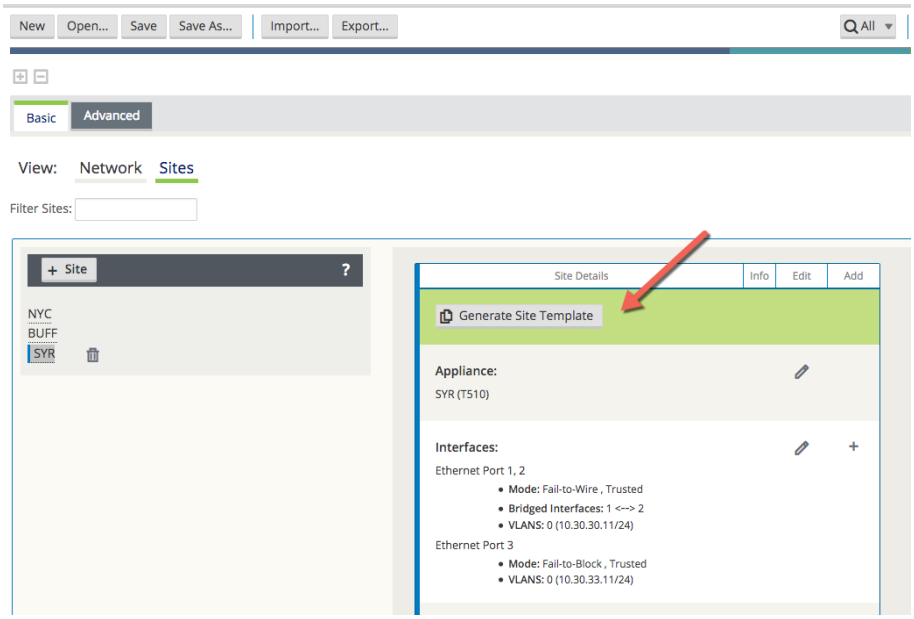


Figure 4

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

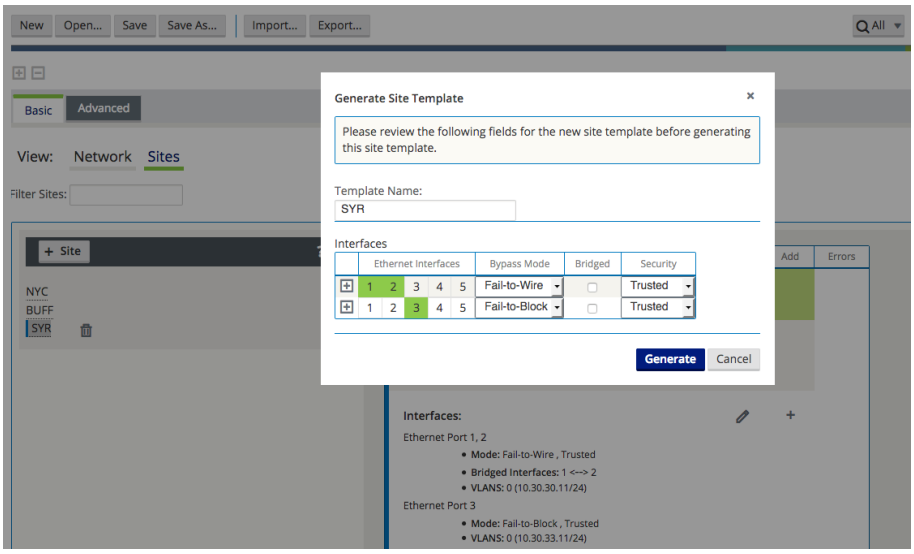


Figure 5

Observe that Branch_TemplateA now appears on the Network view page.

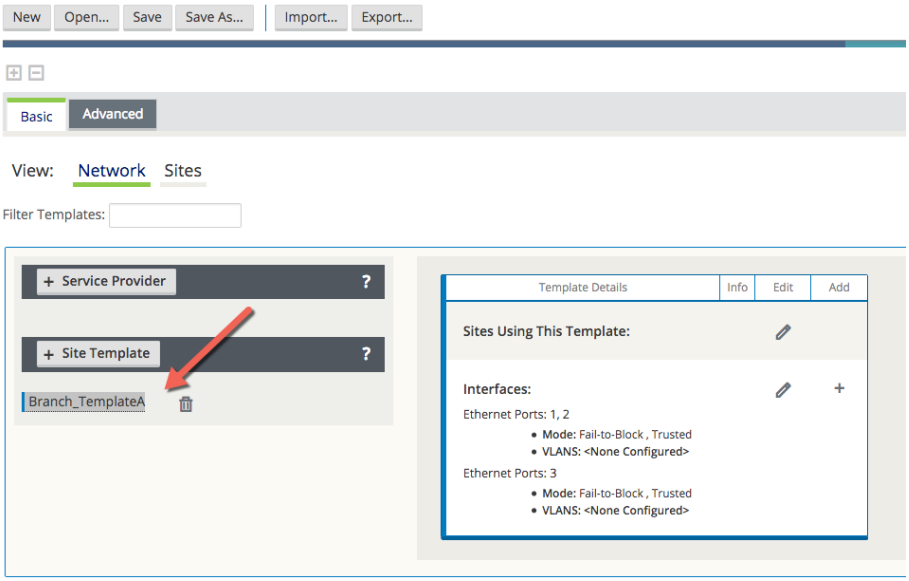


Figure 6

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

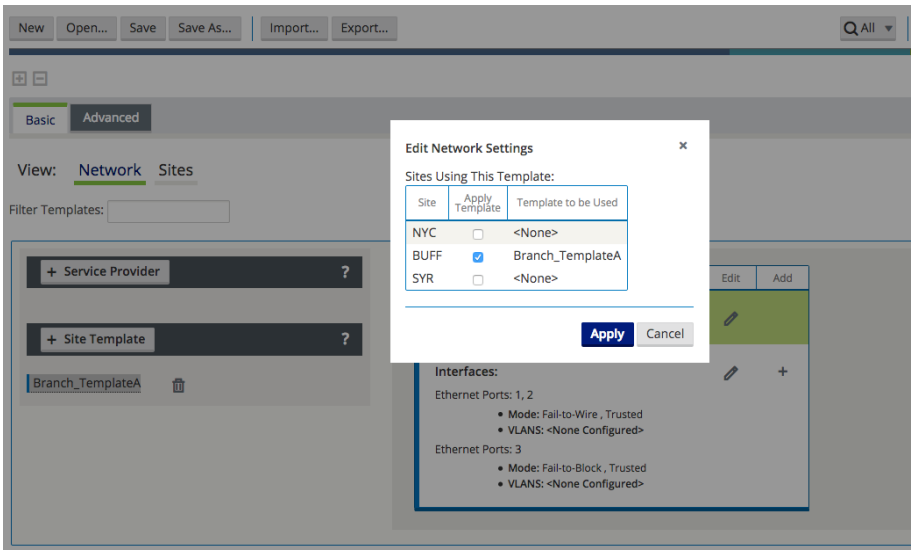


Figure 7

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

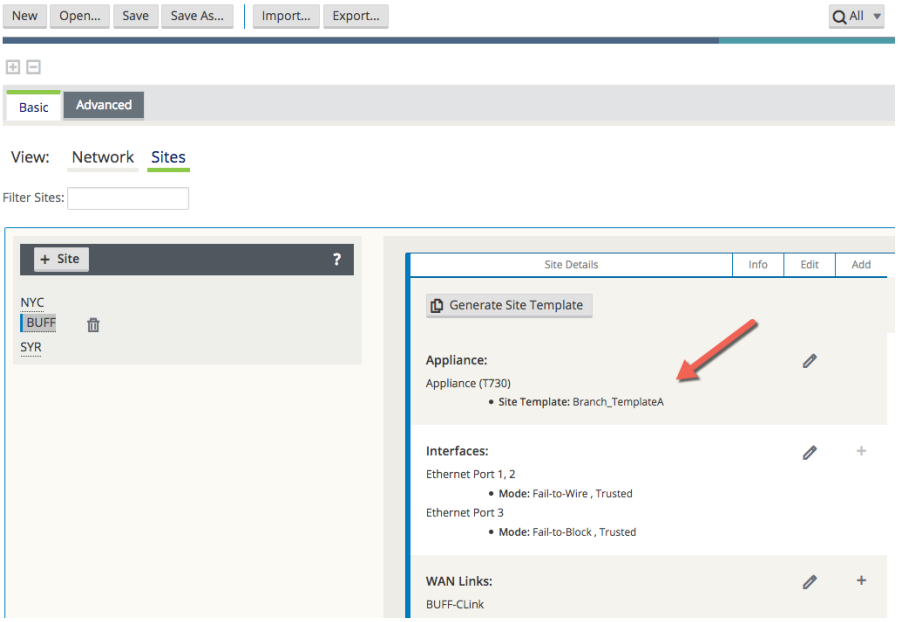


Figure 8

Additional Features in Edge 6.1 GA P2

Additional features included in Edge 6.1 GA P2 include Service Provider – Aware (SP-Aware), OpenDaylight API for service provider configuration, and Restful APIs for service provider network Change Management.

16

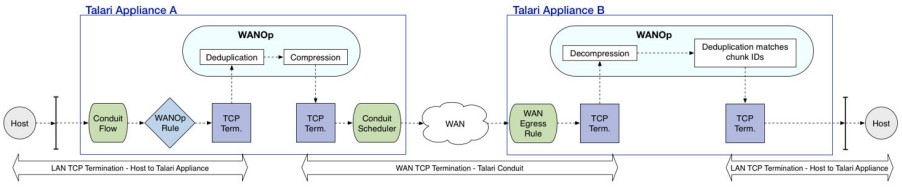
Release 7.0 Features

This chapter includes features and enhancements released in 7.0.

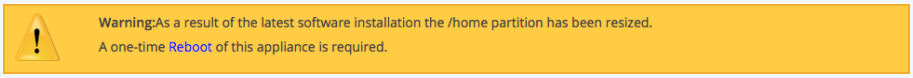
WAN Optimization

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 , in to offer maximum throughput and reliable transfer across the WAN via the conduit. The diagram below shows an example WANOp flow between two sites.



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

> **Note:**
>
> A one-time reboot is required on all WANOp-capable Oracle Talari Appliances after upgrading to 7.0. The following banner will be displayed if the reboot is necessary:
>
> 
>

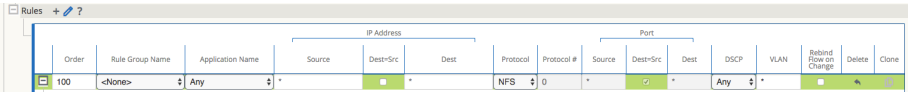
Session Capacity for Supported Models

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

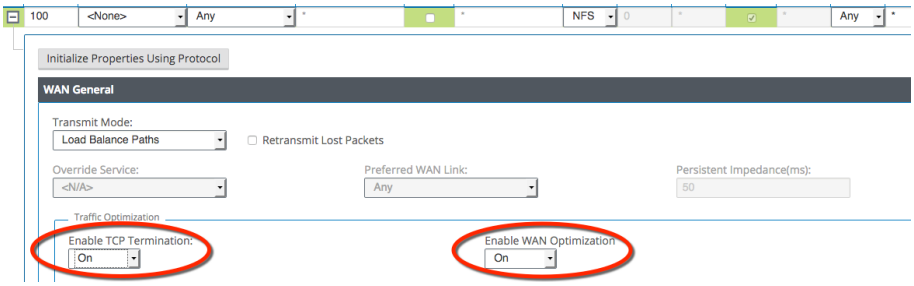
The WANOp solution is configured on a per-rule basis and performs deduplication and compression on TCP Conduit traffic.

Configuring WAN Optimization

Pull up the web UI for the NCN appliance, navigate to **Manage Network > APN Configuration Editor** and **Import** the current configuration file. 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.

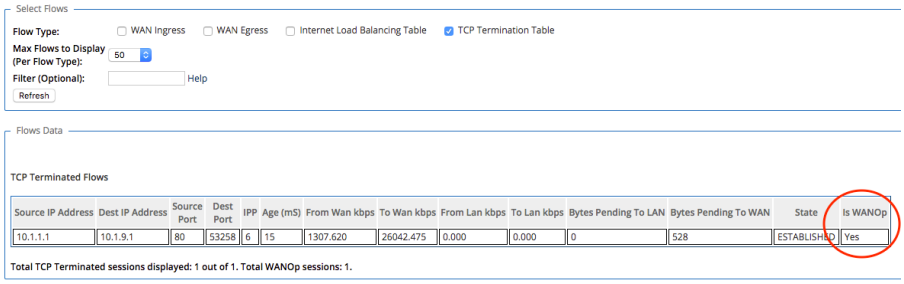
A reciprocal rule enabling WANOp will be generated automatically at the remote site of the selected Conduit.

Once your configuration is complete, **Export** it to **Change Management** 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:

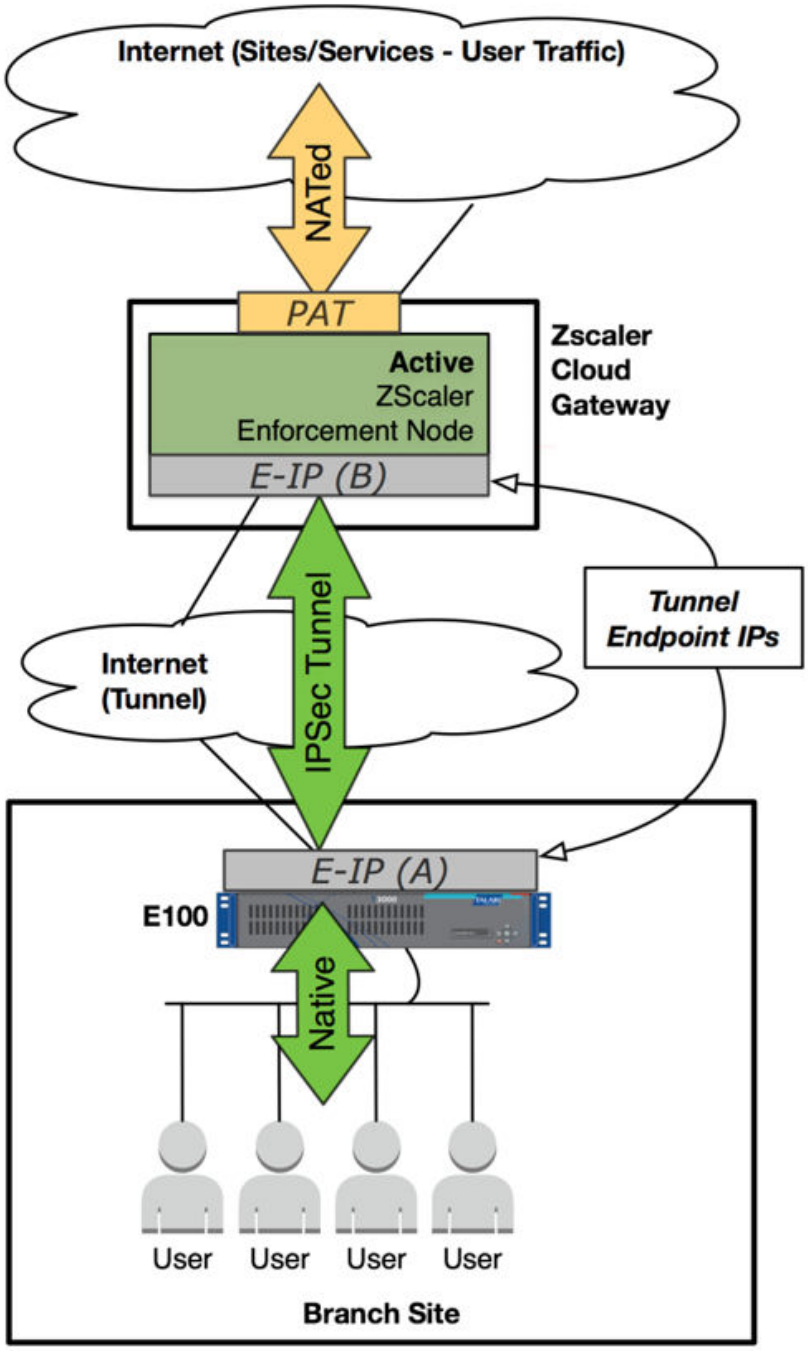


For more information on the WAN Optimization solution, including more detailed capabilities, performance, and monitoring options, please see the WAN Optimization Guide.

Zscaler Integration

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

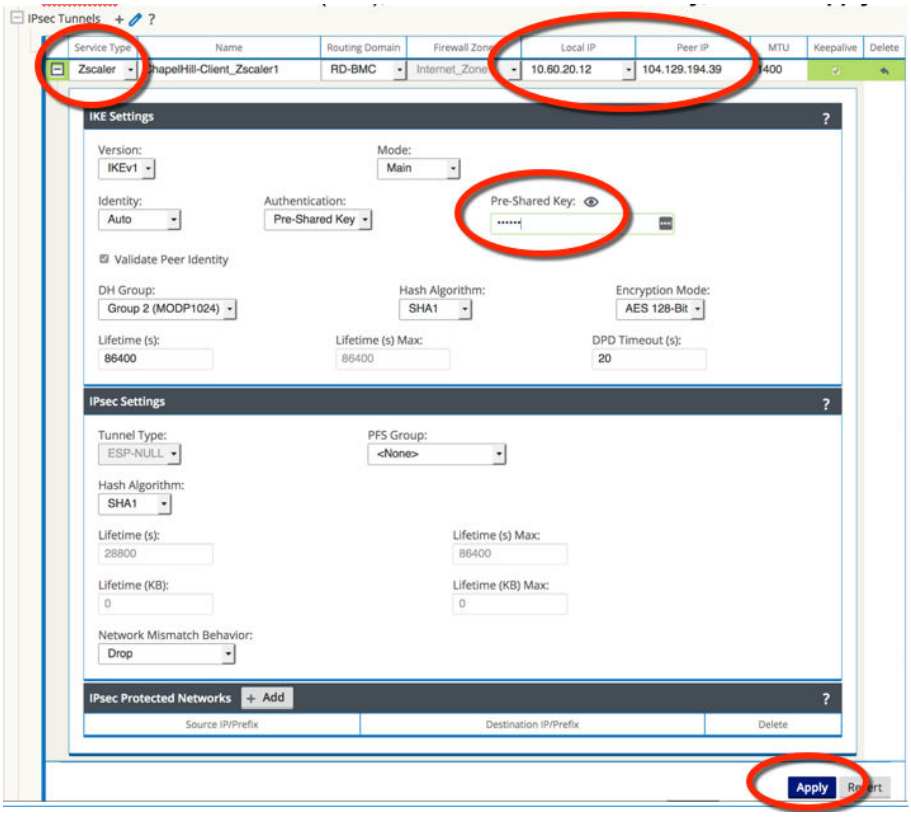
Introduced in APN R7.0 GA, users can now integrate a branch office Oracle Talari Appliance with the Zscaler Cloud Security Gateway via IPSec tunneling, for the purposes of tunneling Internet-destined traffic to Zscaler for cloud-hosted filtering and security services.



Configuration

To configure a Zscaler IPSec tunnel, navigate to **Manage Network > Configuration Editor** on the NCN and **Import** the current configuration file. 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.

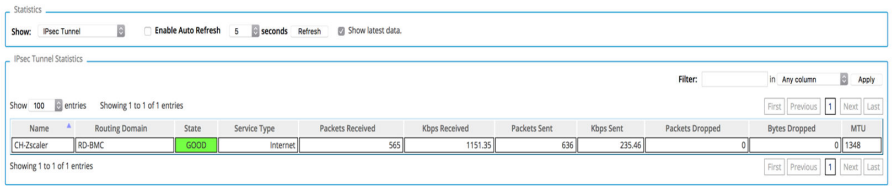
Save the configuration and **Export** it to **Change Management**. Follow the Change Management process to **Stage** and **Activate** the new configuration.

Verification

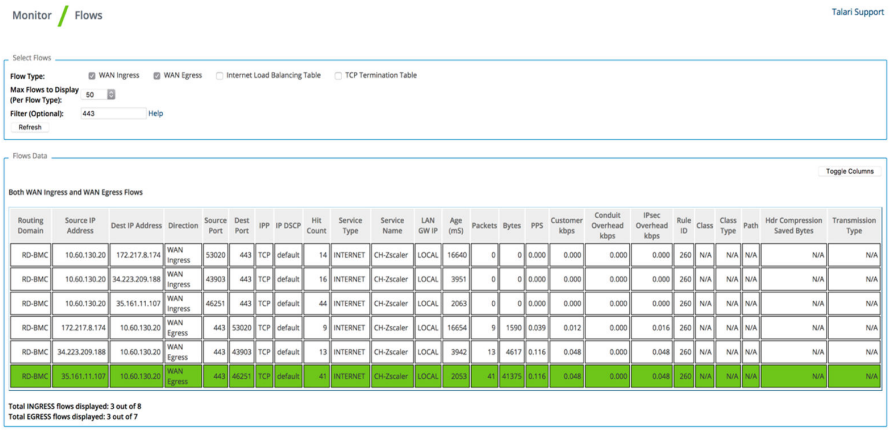
Once the new configuration is running, follow the steps below to verify functionality.

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

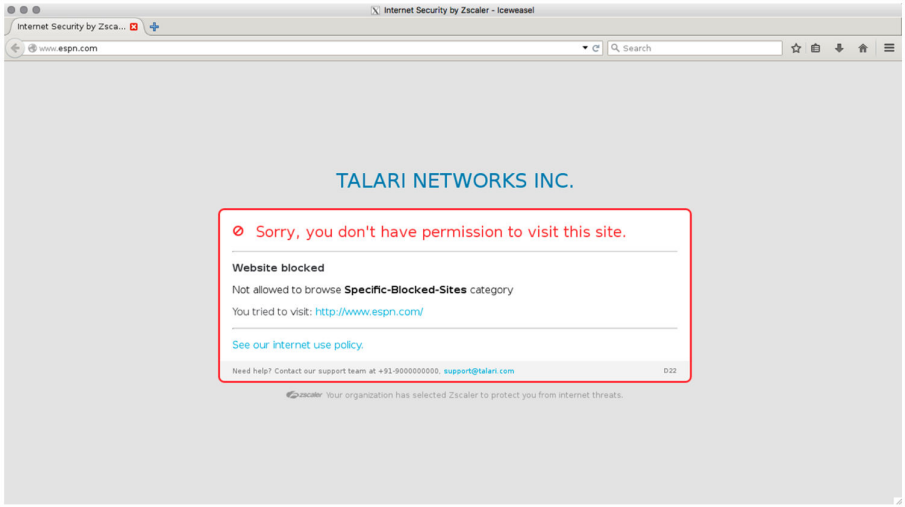
2. Verify the Zscaler IPSec Tunnel status in the web UI of the Oracle Talari Appliance under **Monitor > Statistics > IPSec Tunnel.**



3. Verify the flow of the generated traffic through the Oracle Talari Appliance via **Monitor > 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 Oracle Talari Appliance and the Zscaler ZEN goes down, the 0.0.0.0/0 route through the tunnel will become unreachable and pulled from the 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 Oracle Talari Appliance's web UI under **Monitor > Statistics > Routes**.

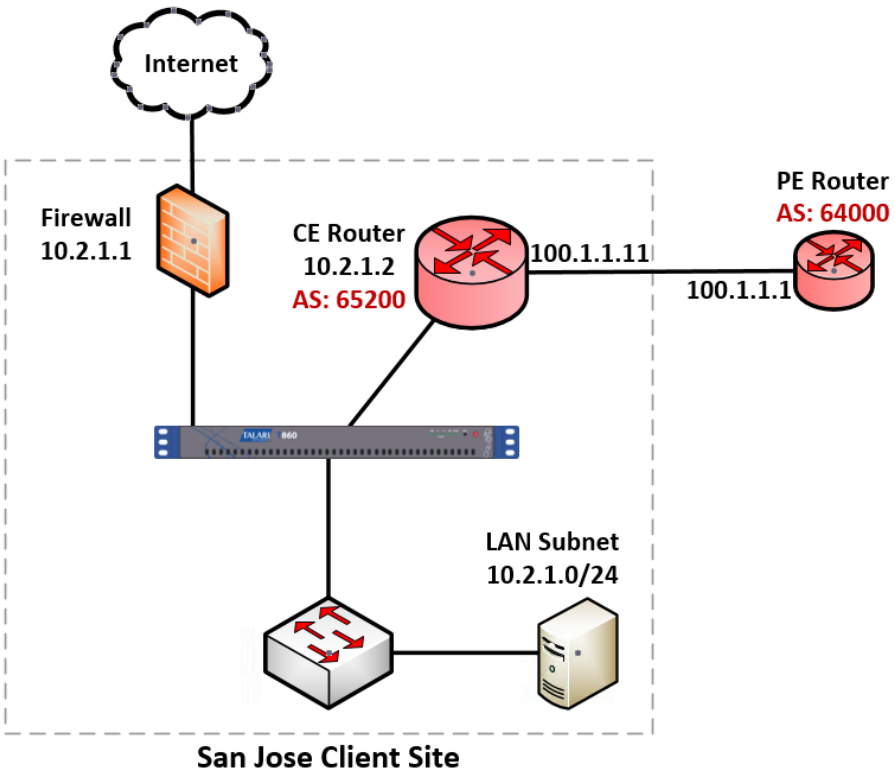
> **Note:**
>
> R7.0 GA only supports a single VRF/routing domain for Zscaler.

Customer Edge (CE) Router Replacement Within the APN

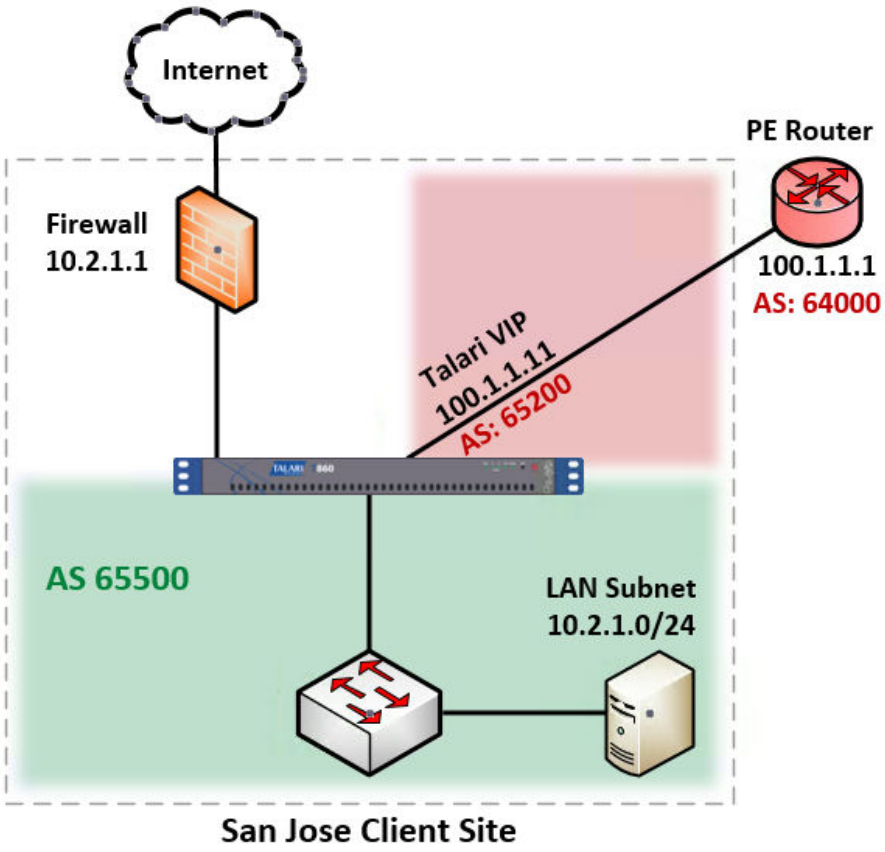
Oracle SD-WAN Edge 7.0 introduces the ability to replace a Customer Edge Router with a Adaptive Private Network Appliance. This is accomplished by leveraging the APNA's ability to masquerade its Local Autonomous System (AS) number (on a per-neighbor basis) so that it can peer with a Provider Edge (PE)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

Installation Summary

Sample APN site before replacing the CE Router with the APNA.



Sample Edge site after replacing the CE Router with the APNA.

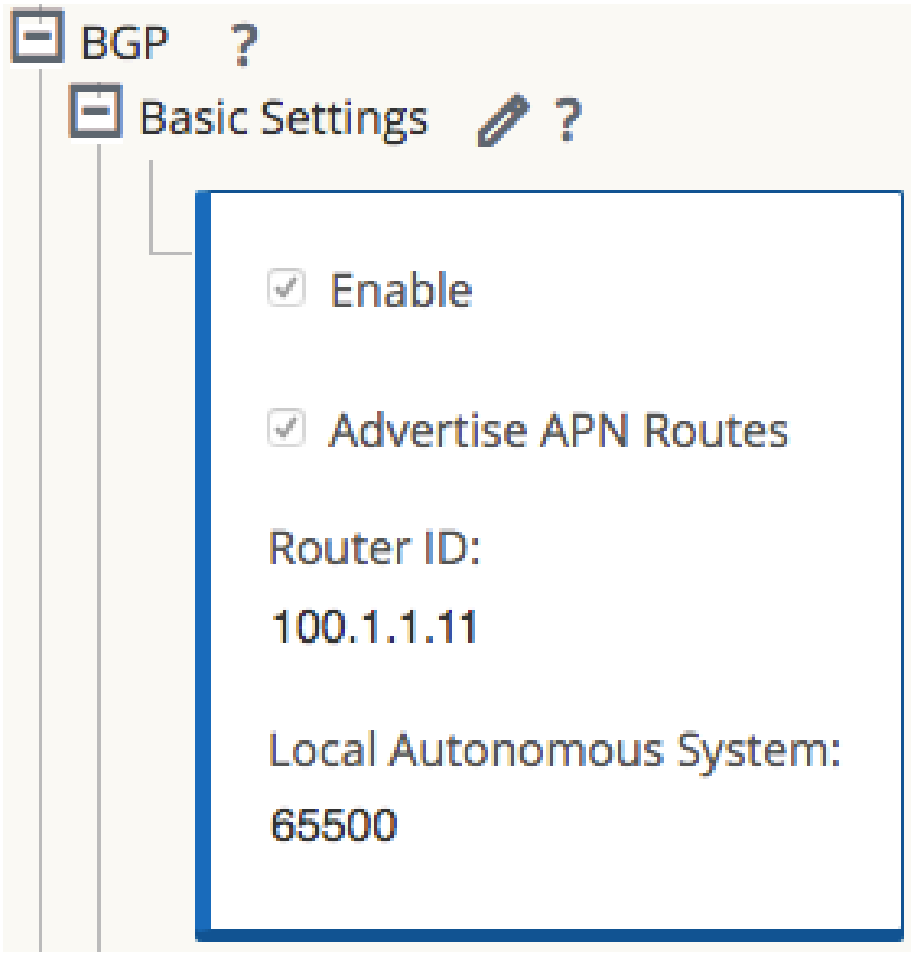


The CE router is removed and the APNA peers directly with the PE router via eBGP by masquerading its AS number as the replaced CE router's AS number (AS 65200). The APNA's actual Local AS number is 65500 and it can peer via iBGP with local routers in this AS.

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

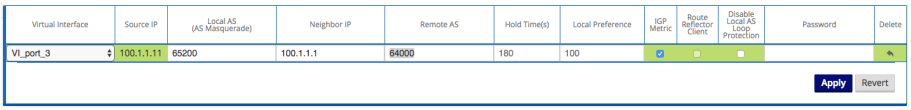
Using the Configuration Editor, navigate to **Connections > [Site Name] > Route Learning > BGP > Basic Settings** and click the pencil icon to edit.



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 **AS Masquerade number**, and enter the **Neighbor IP** address. In this example, we are using the **AS Masquerade** number 65200, to match the AS Number of the former CE Router.

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:

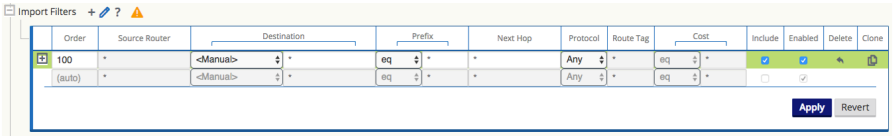
- **Hold Time(s)** - Time in seconds to wait before declaring a neighbor as DOWN.

- **Local Preference** - Sets the BGP attribute Local Preference for routes learned from the neighbor specified.
- **Route Reflector Client** - The 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 to influence 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.

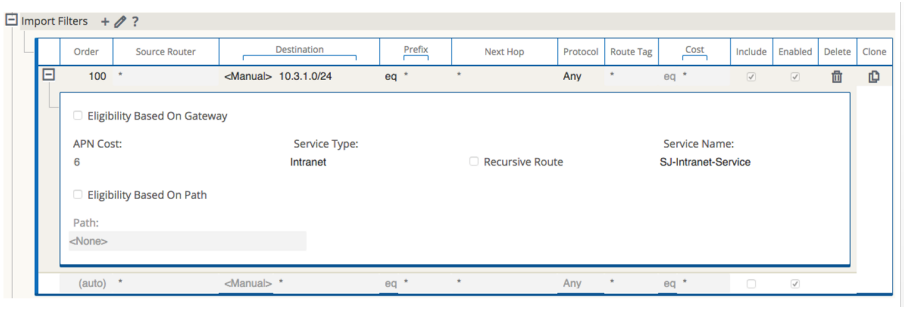


> **Note:**
>
> For each added filter, use any combination of the **Destination**, **Prefix**, and **Next Hop** fields to match desired BGP routes to learn. If these fields are left with their default value of **(*)**, all advertised BGP routes will be imported. Additionally, it is important to understand 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 Oracle Talari Appliances:** If the Export Route to Oracle Talari Appliances checkbox is enabled, the Oracle Talari Appliance will communicate route data to Oracle Talari 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.
- **APN Cost:** The cost will be applied to the matched routes when importing into the Oracle Talari Appliance's route table. The default APN Cost is 6.
- **Service Type:** Choose a Service Type from all the existing, supported 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.



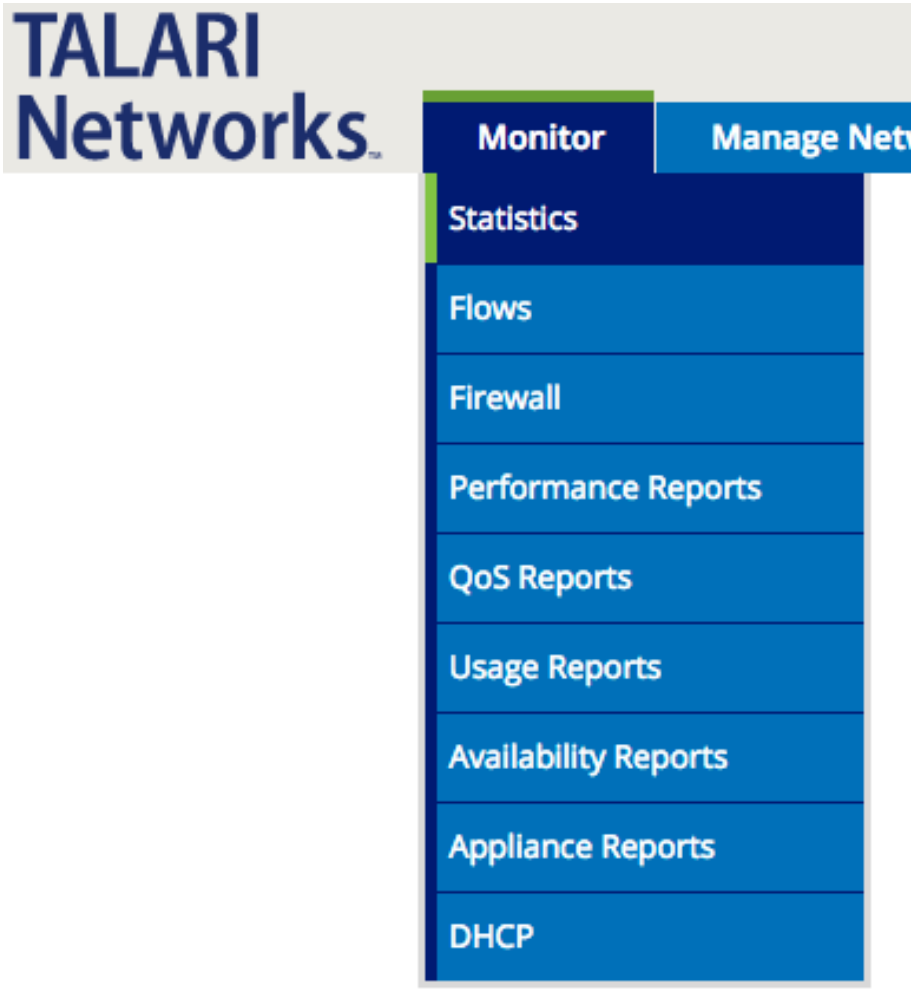
Once configuration of the APN is complete, the configuration should be saved and **Change Management** should be used to push the configuration changes to the APNAs.

Static Routes File

Oracle Talari Appliances provide a **Static Routes** file that can be edited to define routes that should persist through software and configuration changes made to the APN. This is used for inserting static routes into the dynamic routing table, not the APN 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 APN configuration. By default, static routes defined in this file will be advertised to all neighbors within the specified routing domain.

BGP Verification and Troubleshooting

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



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

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

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

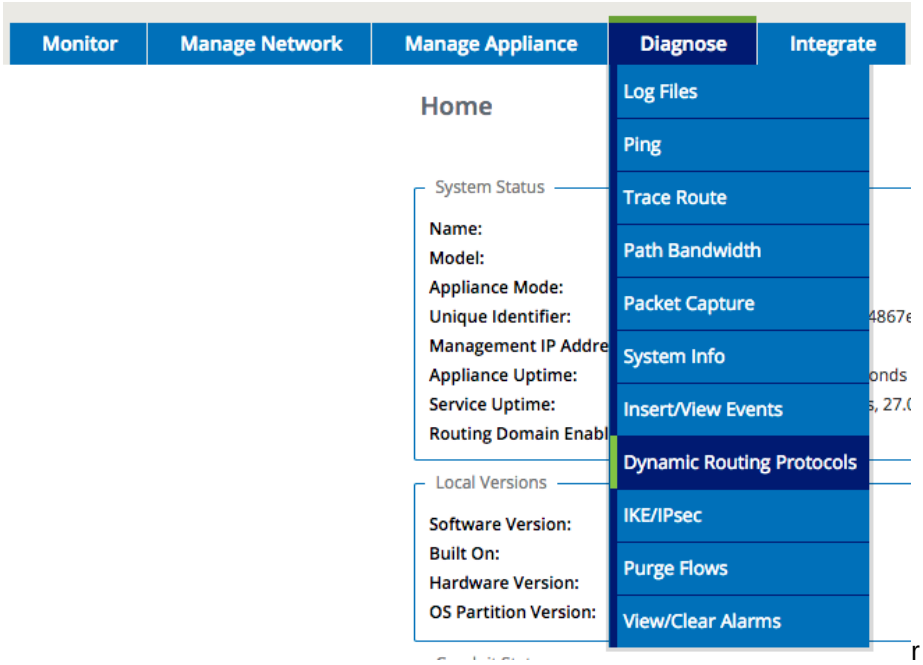
Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol
0	100.1.1.0/24	*	Local	Default_LAN_Zone	YES	*	SanJose-CLI	Static	-
1	10.2.1.0/24	*	Local	Default_LAN_Zone	YES	*	SanJose-CLI	Static	-
2	10.1.1.0/24	*	RAL-NCN-SanJose-CLI	Default_LAN_Zone	YES	*	RAL-NCN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

Note:

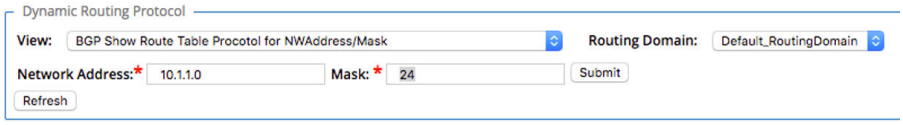
The route must also be considered reachable for it to be used.

BGP Troubleshooting Enhancements

The Oracle Talari 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. When a view allows filtering, enter the Network Address and Mask in the format shown below.



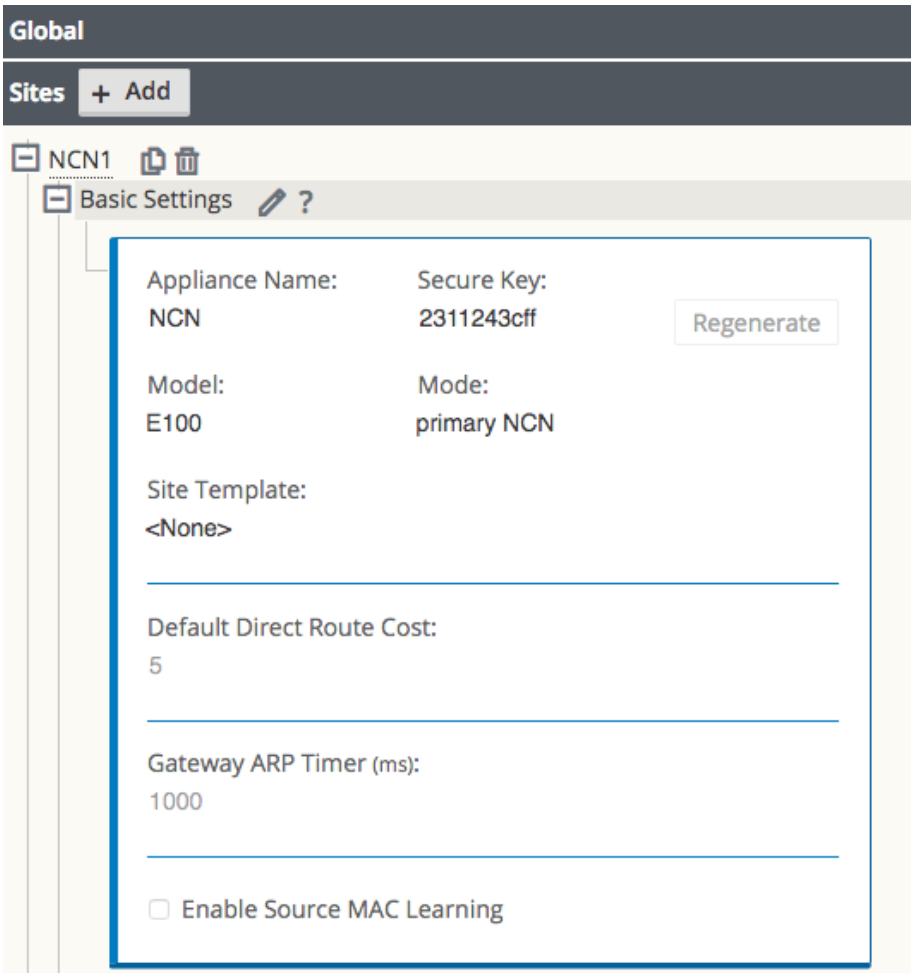
- **BGP State** - Shows an overview of the current state of each Dynamic Routing Protocol instance.
- **BGP Show Route Table Protocol** - Shows prefixes associated with each BGP instance/neighbor.
- **BGP Show Route NWAddress/Mask Table** – Shows prefixes associated with each BGP instance/neighbor and allows filtering for specific prefixes. Will provide APN and BGP routes.
- **BGP Show Route Table Protocol NWAddress/Mask -** Shows prefixes associated with each BGP instance/neighbor and allows filtering for specific prefixes. Provides BGP routes only.
- **BGP Show Route Export** - Shows routes being advertised from the Oracle Talari Appliance.
- **BGP Show Route Export (detailed)** - Shows routes being advertised from the Oracle Talari 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.
- **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 Route Count in Table** - Gives a count of all entries in the routing table (BGP and APN).
- **Show Protocol** - Outputs a list of routing protocols that are currently running and their states.
- **Talari Protocol Table -** Shows only the Edge routing table.
- **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.

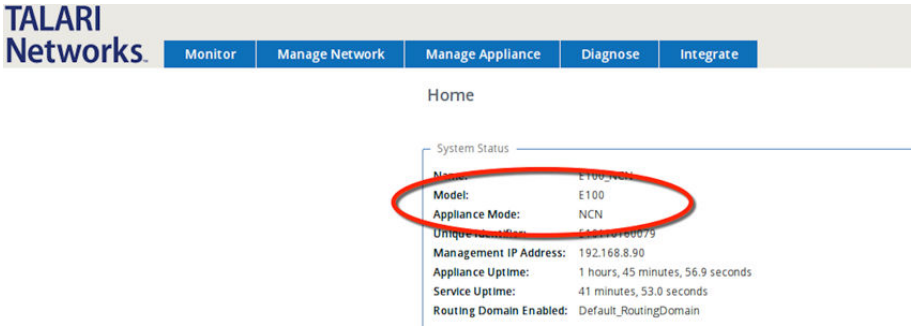
For additional information on this topic (including how to edit the Static Routes file) please refer to the CE Router Replacement Guide on the Support Portal section of our website under Documentation.

E100 as an NCN

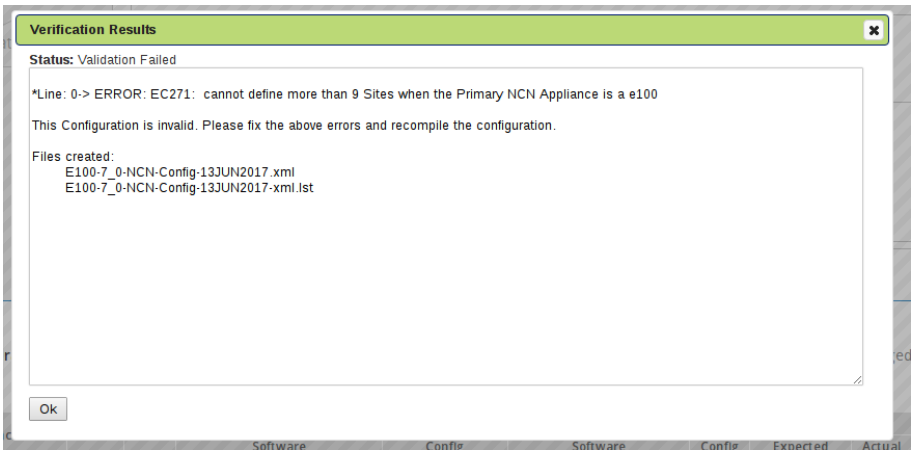
R7.0 GA now supports deployment of the E100 Oracle Talari Appliance as a primary and secondary NCN for up to 8 Client sites (9 total sites per-network). This is done in the Configuration Editor from the **Advanced** tab under **Sites > [Site Name] > Basic Settings** where the **Model** should be the E100 and the **Mode** can now be either primary NCN or secondary NCN.



After completing the configuration, the user will **Export** it to **Change Management** 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.



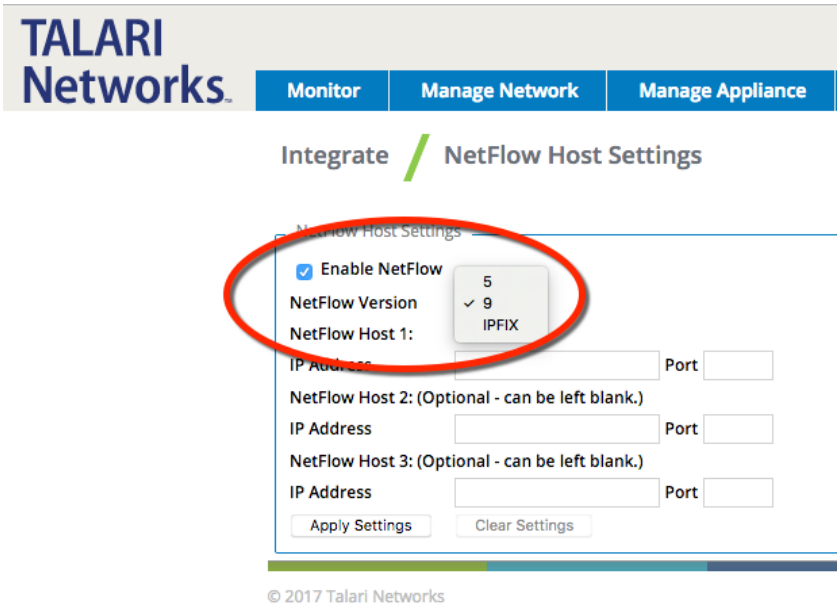
Capacity Report for the E100 NCN

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, navigate to **Integrate > NetFlow Host Settings** from the web UI of any Talari Appliance, click the **Enable NetFlow** button, then select the preferred version from the **NetFlow Version** drop down.



Note:

To complete the configuration, you must enter in a **NetFlow Host IP Address** and **Port** number, then click the **Apply Settings** button.

Additional Features in 7.0 GA

Additional features included in 7.0 GA include support for the VT800 at the data rate of 500Mbps through a Conduit on the Azure cloud and the VT800 at the data rate of 2Gbps for ESXi on the Intel Xeon E7-8870v4.

Appliance Model	Throughput 1400B at MOS score of 4.3 or Better
T510	2 x 40 Mbps
T730	2 x 80 Mbps
T750	2 x 120 Mbps
E100	2 x 200 Mbps
T860	2 x 800 Mbps
T3010	2 x1 Gbps
T5000	2 x 3 Gbps
T5200	2 x 5 Gbps
VT800 (ESXi)	2 x 2 Gbps
VT800 (Azure)	2 x 500 Mbps
VT800 (Hyper-V)	2 x 200 Mbps
CT800	2 x 100 Mbps

17

Release 7.1 Features

This chapter includes features and enhancements released in 2.3.

E1000 Hardware Options

7.1 introduces 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. To determine which expansion card (if any) is installed on the appliance, check the number of Ethernet interfaces under **Manage Appliance > Local Network Settings**:

Hardware Option	Ports
E1000 without expansion card	AUX, MGT, interfaces 1-8
E1000 with 10G expansion card	AUX, MGT, interfaces 1-10
E1000 with FTW expansion card	AUX, MGT, interfaces 1-12

Port Labelling for Expansion Cards

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. For an **E1000 with no expansion card**, only configure ports 1 – 8. For an **E1000 with the 10G fiber** expansion card, only configure ports 1 – 10; ports 9 and 10 should not be configured for FTW. For an **E1000 with the FTW** expansion card, all 12 ports may be configured.

If a configuration that does not match the available hardware is applied to an E1000, the Talari 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 service will start. Alternately, the appliance may be factory defaulted and a corrected configuration applied using the Easy 1st Install process. **The Talari 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*.

Interactive Dashboard

7.1 enhances the Oracle Talari Appliance Home page, providing users with an interactive dashboard which provides at-a-glance insight into the APN and quick access to areas of interest:

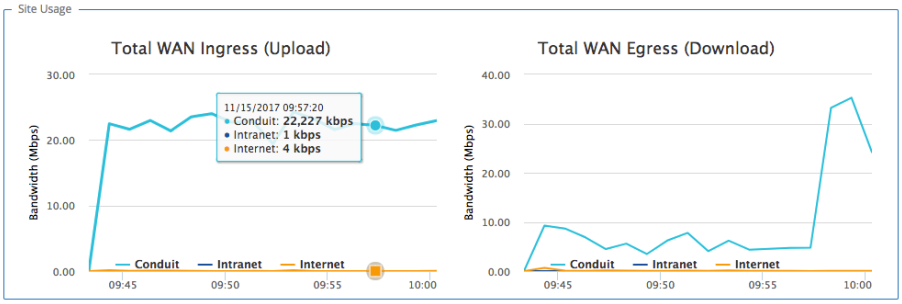
System Status and Quick Links

The new landing page moves the appliance name to the top of the page. Local system information has been consolidated under the System Status heading. Additional system information (including model, service uptime, and the build date for software) has been moved to the **Diagnose > System Info** tab.

Just below the System Status information, quick links are provided to commonly used screens:

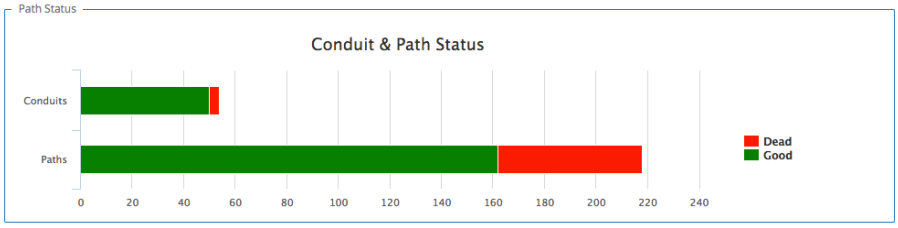
- The Paths Summary button takes users to the **Monitor > Statistics** Path Summary report.
- The Classes button takes users to the **Monitor > Statistics** Classes report, with the Conduit Filter pre-set to the first Conduit in the list.
- The WAN Link Usage button takes users to the **Monitor > Statistics** WAN Link Usage report.
- The Diagnose button takes users to the **Diagnose > Log Files** page.

Site Usage



The Site Usage graphs show an overview of the past 24 hours of WAN Ingress and WAN Egress bandwidth usage for the site, broken down by Conduit, Intranet, and Internet. Hover over a point on the graph to view a tooltip showing the date, time, and exact values for Conduit, Intranet, and Internet bandwidth at that time. These graphs are linked to the **Monitor > Usage Reports** page. Clicking on a graph will take users to the Usage Reports page to view the requested report in more detail.

Path Status

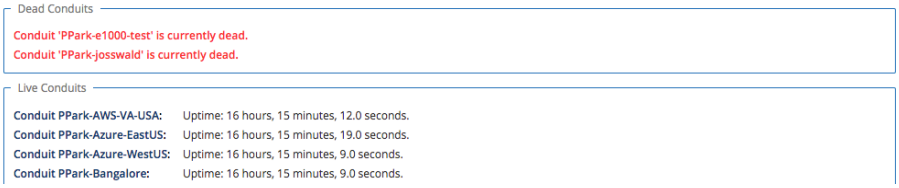


This bar chart provides a visual display of Conduit and Path states. Red (Dead) segments are clickable. A Dead Conduits segment links to **Monitor > Statistics > Conduits**, pre-filtered to show only dead Conduits. A Dead Paths segment links to **Monitor > Statistics > Paths (Summary)**, pre-filtered to show only dead Paths.

Recent Event Errors

Displays up to 10 recent errors, if any Events with an Event Type of “Error” are available to display.

Conduits



Any dead Conduits are displayed above the list of live Conduits. Clicking on a dead Conduit will take the user to **Monitor > Statistics > WAN Link Usage**, where the

Usage and Permitted Rates table will be automatically filtered based on the service name for the Conduit.

Live Conduits provide hyperlinks to the remote site (on the NCN only).

WAN Optimization on Virtual Appliances

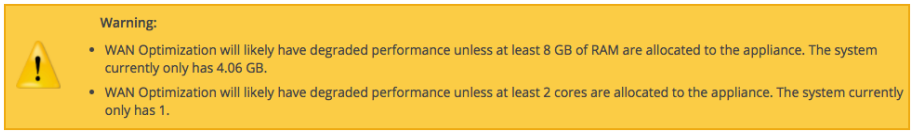
7.1 expands support for WAN Optimization to the VT800 and CT800 platforms. WAN Optimization is supported on these platforms at the following levels, with the following resources:

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:

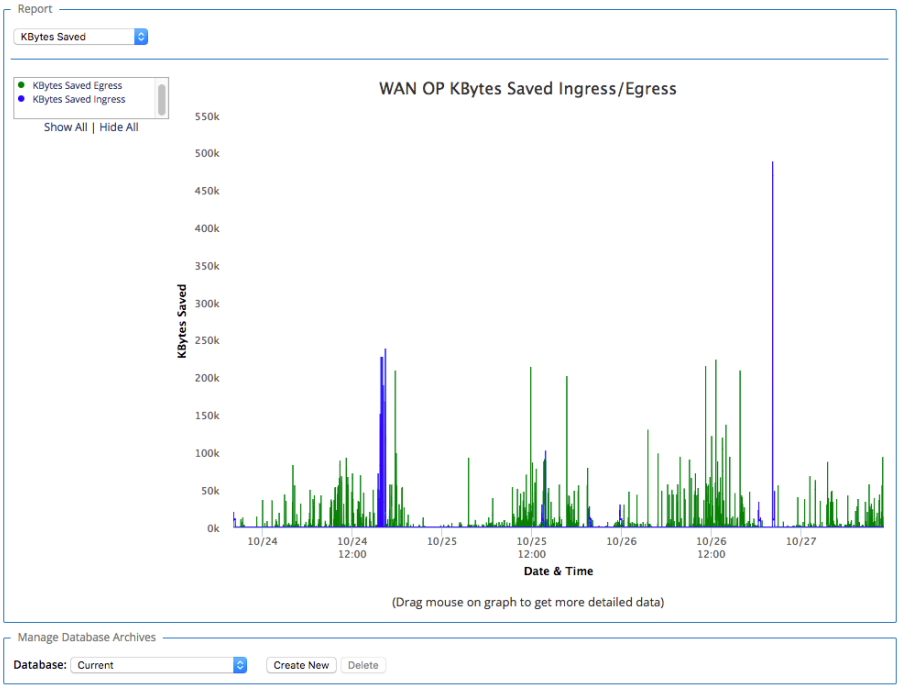
The maximum number of WANOp sessions is scaled based on available memory. If a virtual appliance has insufficient dedicated RAM, the maximum number of WANOp sessions will be lower. Provisioning a virtual appliance below recommended system specifications will not disable WANOp, but will impact WANOp performance.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

A warning banner will be displayed in the Web Console if WANOp is enabled on a VT800 or CT800 that does not meet the minimum recommended system specifications. An example is shown below, on a VT800 with insufficient RAM and VCPUs:



WAN Optimization Reporting Enhancements

7.1 enhances the existing WAN Optimization monitoring facilities with graphical reports to display key WANOp data over time. To view the reports, navigate to **Monitor > WAN Optimization**.

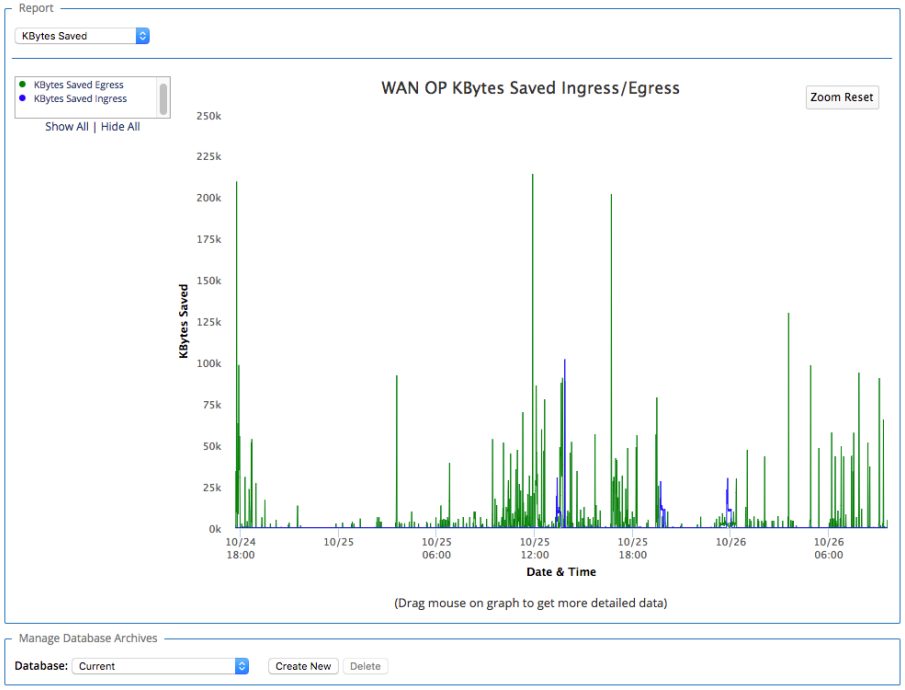


Different reports may be selected from the dropdown in the upper left-hand corner of the Report pane, and filtered using the criteria to the left of the graph. Available reports include:

- Kilobytes Saved (Egress/Ingress)
- Compression Ratio (Egress/Ingress)
- Deduplication Ratio (Egress/Ingress)
- Data Reduction Percentage (Egress/Ingress)
- Deduplication Cache Percentage (Hit/New)
- Deduplication Cache Count (Hit/New)
- Deduplication Cache Kilobytes (Hit/New)

For in-depth descriptions of the information provided in these reports, please see the *WANOp Setup and Configuration Guide*.

Users can zoom in to view a period of time in greater detail by dragging on the graph to select the timeframe of interest:



To zoom out to the original graph data, click the Zoom Reset button in the upper right corner of the pane.

Users may also view reports for archived databases by selecting the report they wish to view, then scrolling down to the Manage Database Archives pane and selecting an archived database from the dropdown. Changing reports after selecting an archived database will reset the report to the current database.

Additional Features in 7.1 GA

Increased Maximum Bandwidth on AUX Port

7.1 increases the maximum WAN link bandwidth for interface groups including the AUX port to 500Mbps on the T3010, T5000, and T5200.

Monitor > Statistics Enhancements

7.1 introduces some slight changes to the Monitor > Statistics page in the Web Console:

- In the Paths (Summary) view, the Congestion column has been removed.
- In the Classes view, the Conduit Filter field has been replaced with a dropdown menu. Additionally, any entry in the Dropped Packets column with a value greater than 0 will be highlighted.
- In the ARP view, entries are automatically sorted by reply state.
- In the WAN Link Usage view, the Usage % column has been added to the “Local WAN Links” and “Usage and Permitted Rates” tables. The Usage % is Kbps/ Permitted Kbps.

WANOp Intelligent Cache

7.1 optimizes the performance of WANOp caching for items accessed multiple times, ensuring faster speeds for frequently accessed files.

18

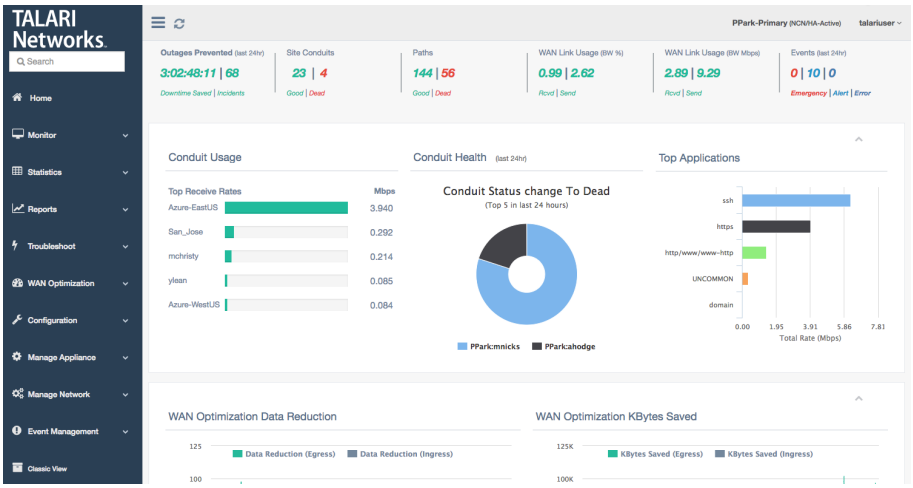
Release 7.2 Features

This chapter includes features and enhancements released in 7.2.

User Interface Enhancements

7.2 GA introduces a new and improved user interface, including a new landing dashboard and updated navigation. The new dashboard and all statistics screens are responsive for easier viewing on varying screen sizes.

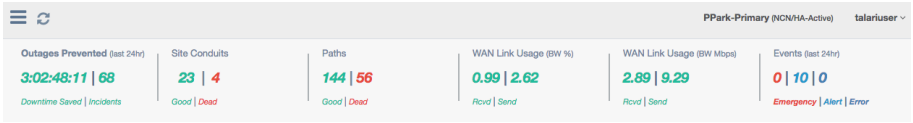
Navigation menus have been moved to the sidebar, and reorganized into logical groupings to make the navigation experience more intuitive. Additionally, users may quickly locate any navigation link using the Search bar at the top of the navigation sidebar.



New Landing Dashboard

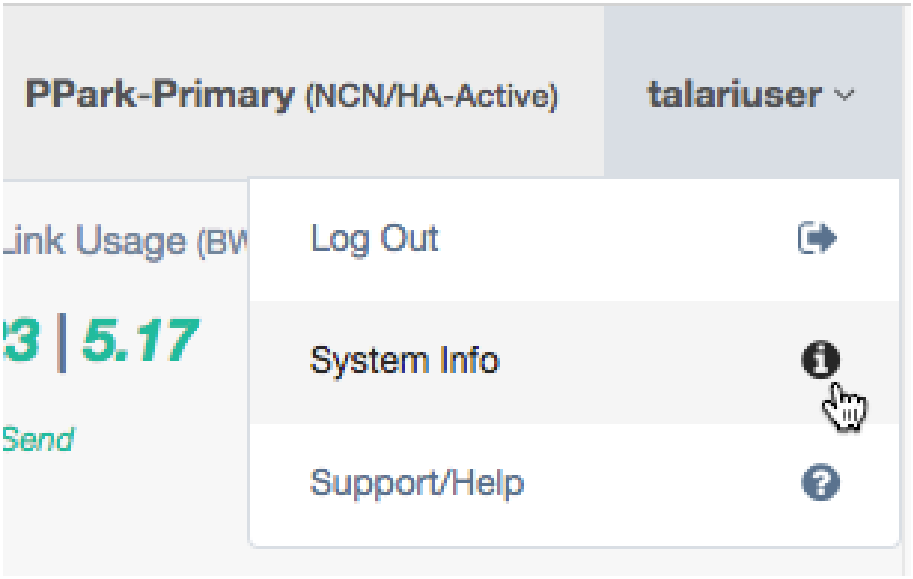
Landing Dashboard Components

The top bar will be visible on every page of the new User Interface:

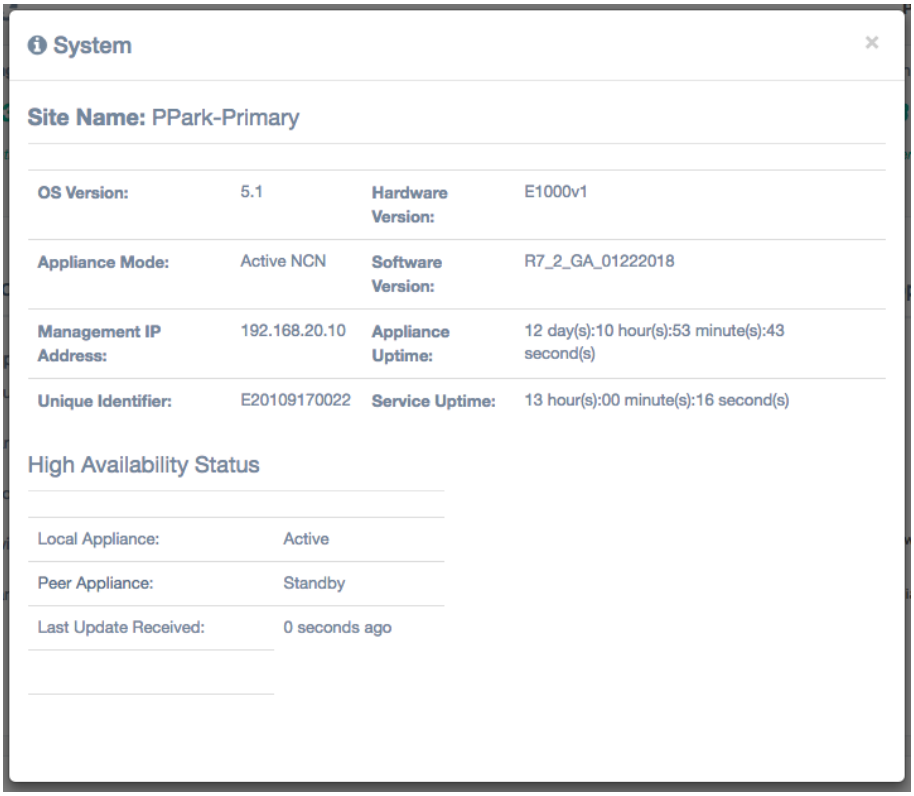


Toggle visibility of the navigation menu and refresh the current page using the buttons on the left-hand side of the top bar. On the right-hand side, the site name and logged-in username are displayed.

Click on the username to display a dropdown menu with links for logout, system information, and support:



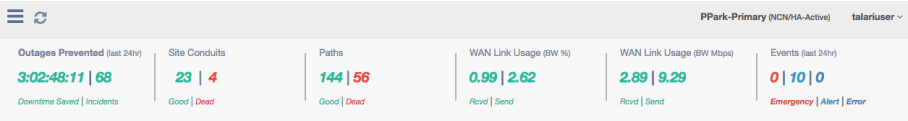
Click System Info in the dropdown to display the system status information, including OS Version, Hardware Version, Software Version, and Management IP:



Appliance alerts will also be shown in the top bar, if any exist:

Click the alert icon to display a popup listing all appliance alerts.

The first section of the new dashboard presents summary information about the health of the site:



Outages Prevented (Last 24 hours): The amount of downtime saved (calculated as time when Paths went dead but the Conduits stayed up) and number of incidents (times Paths went dead) detected in the last 24 hours. Links to **Reports > Availability**.

Site Conduits: The number of Good and Dead Conduits for the site. Each number links to **Statistics > WAN > Conduits**, filtered by the appropriate state.

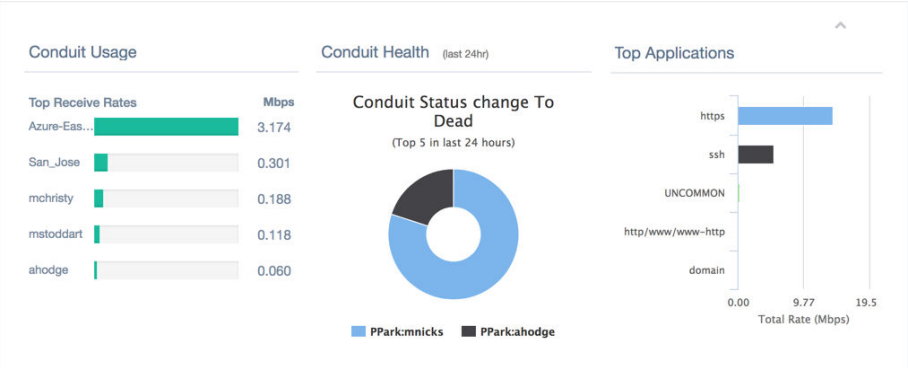
Paths: The number of Good and Dead paths for the site. Each number links to **Statistics > WAN > Paths (Summary)**, filtered by the appropriate state. Any Bad paths are included in the count of Good paths, as this is a transitory path state.

WAN Link Usage (BW %): The local WAN Link Usage by percentage of total permitted rate, for receive (download) and send (upload). Links to **Statistics > WAN > WAN Link Usage**.

WAN Link Usage (Mbps): The local WAN Link Usage by Mbps, for receive (download) and send (upload). Links to **Statistics > WAN > WAN Link Usage**.

Events (Last 24 hours): The number of emergency/alert/critical-level severity events in the last 24 hours. Links to **Event Management > Insert/View Events**.

The second section of the dashboard provides information about Conduit health:



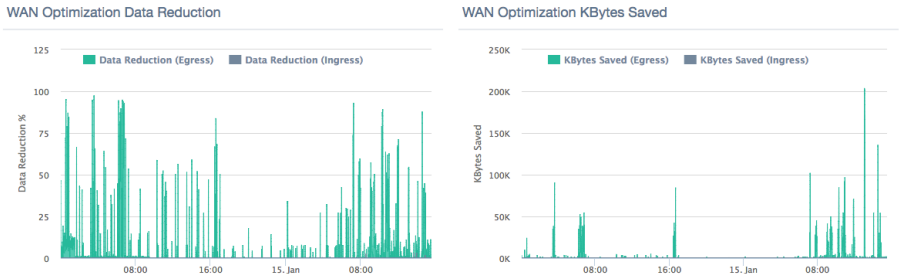
> **Note:**
>
> This section and all of the following sections can be collapsed and expanded using the **^** button in the upper right corner.

Conduit Usage: The top five receive rates in Mbps for the local site, sorted in descending order. The report title links to **Statistics > WAN > Conduits**.

Conduit Health: The five Conduits which have gone dead the most in the last 24 hours. If fewer than five Conduits have gone dead in the last 24 hours, only those which have gone dead will be shown. Users may hover over each section of the graph to see total state changes for that site within the last 24 hours. The report title links to **Statistics > WAN > Conduits**.

Top Applications: The top five observed protocols and the total rate for each. The report title links to **Statistics > QOS > Observed Protocols**.

The third section of the dashboard provides at-a-glance information about WAN Optimization, and will only be displayed on appliances that support WAN Optimization:

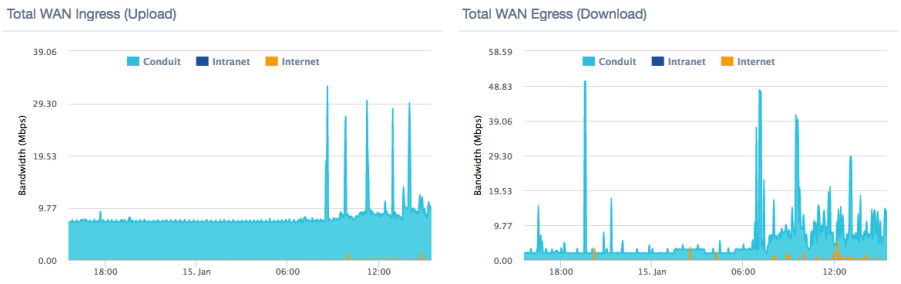


WAN Optimization Data Reduction: Report displaying data reduction percentages for WAN Egress and WAN Ingress WANOp traffic at the site on a per-minute basis. Users may hover over a point on the chart to display detailed data. Select the legend headers to turn data points off or on. The report title links to **WAN Optimization > Statistics**, with the data reduction report displayed.

WAN Optimization Kbytes Saved: Report displaying kilobytes saved using WAN Optimization for WAN Egress and WAN Ingress. Users may hover over a point on the chart to display detailed data. Select the legend headers to turn data points off or on. The report title links to **WAN Optimization > Statistics**, with the Kbytes Saved report displayed.

> **Note:**
>
> Data is only displayed if WAN Optimization is enabled. Otherwise, the section will report “No Data to Display”.

The fourth section of the dashboard presents site bandwidth reports:

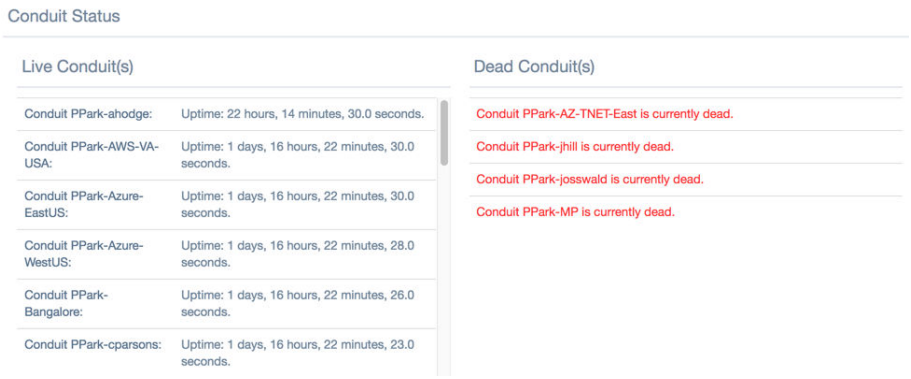


Total WAN Ingress (Upload): Report displaying total WAN Ingress bandwidth usage for Conduit, Intranet, and Internet services for the last 24 hours. Users may hover over a point on the chart to display detailed data. Select the legend headers to turn data points off or on. The report title links to **Reports > Usage**, with WAN Ingress pre-selected in the direction dropdown.

Total WAN Egress (Download): Report displaying total WAN Egress bandwidth usage for Conduit, Intranet, and Internet services for the last 24 hours. Users may hover over a point on the chart to display detailed data. Select the legend headers to

turn data points off or on. The report title links to **Reports > Usage**, with WAN Egress pre-selected in the direction dropdown.

The fifth and final section displays Conduit status information:



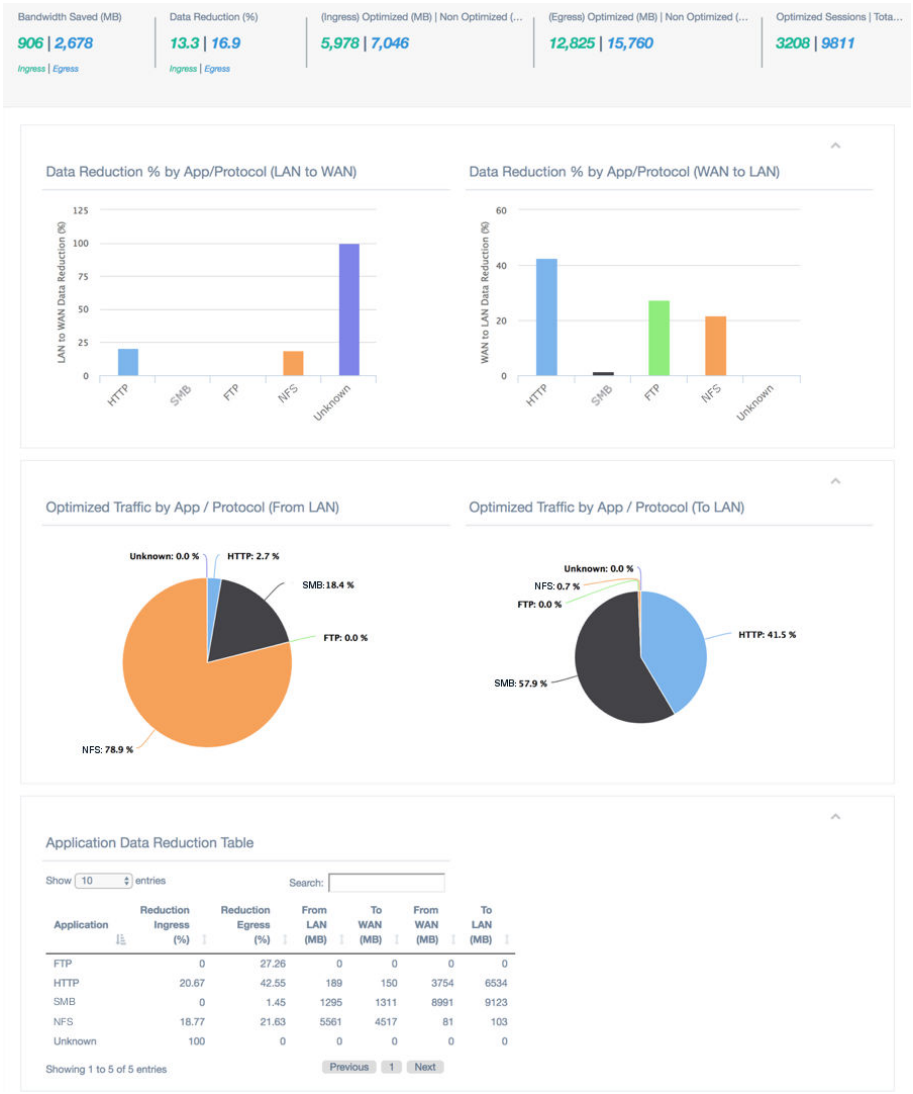
Live Conduits: A list of all live Conduits at the site. On the NCN, live conduits link to the remote site.

Dead Conduits: A list of all dead Conduits at the site. Dead Conduits link to **Statistics > WAN > Conduits**, filtered for dead conduits.

WAN Optimization Dashboard and Reporting Enhancements

7.2 provides a new at-a-glance dashboard for WAN Optimization with more detailed reports and more data about the protocols being optimized. The dashboard refreshes automatically every minute to provide up-to-date information. Additionally, all WANOp pages have been consolidated into the new WAN Optimization menu in the sidebar for ease of location. The WAN Optimization menus and dashboard will only be displayed on appliances that support WAN Optimization.

To view the WAN Optimization dashboard, navigate to **WAN Optimization > Dashboard**:



WAN Optimization Dashboard Overview

> **Note:**
>
> The new WAN Optimization dashboard takes advantage of the Application objects that can be defined in the Configuration (**Global > Applications**). Application Recognition was introduced in 6.1. Please see the 6.1 New Features Guide for configuration details.

If an application is defined in the configuration and used in policies or rules, individual WANOp statistics will be tracked for that application and tagged with the application name defined in the configuration.

WAN Optimization Dashboard Components

The first section of the WAN Optimization dashboard presents summary information about WAN Optimization function at the site:

Bandwidth Saved (MB): Total bandwidth saved using WAN Optimization in MB, for WAN Ingress and WAN Egress. Links to **WAN Optimization > Monitor WANOp** with the Kbytes Saved report pre-selected.

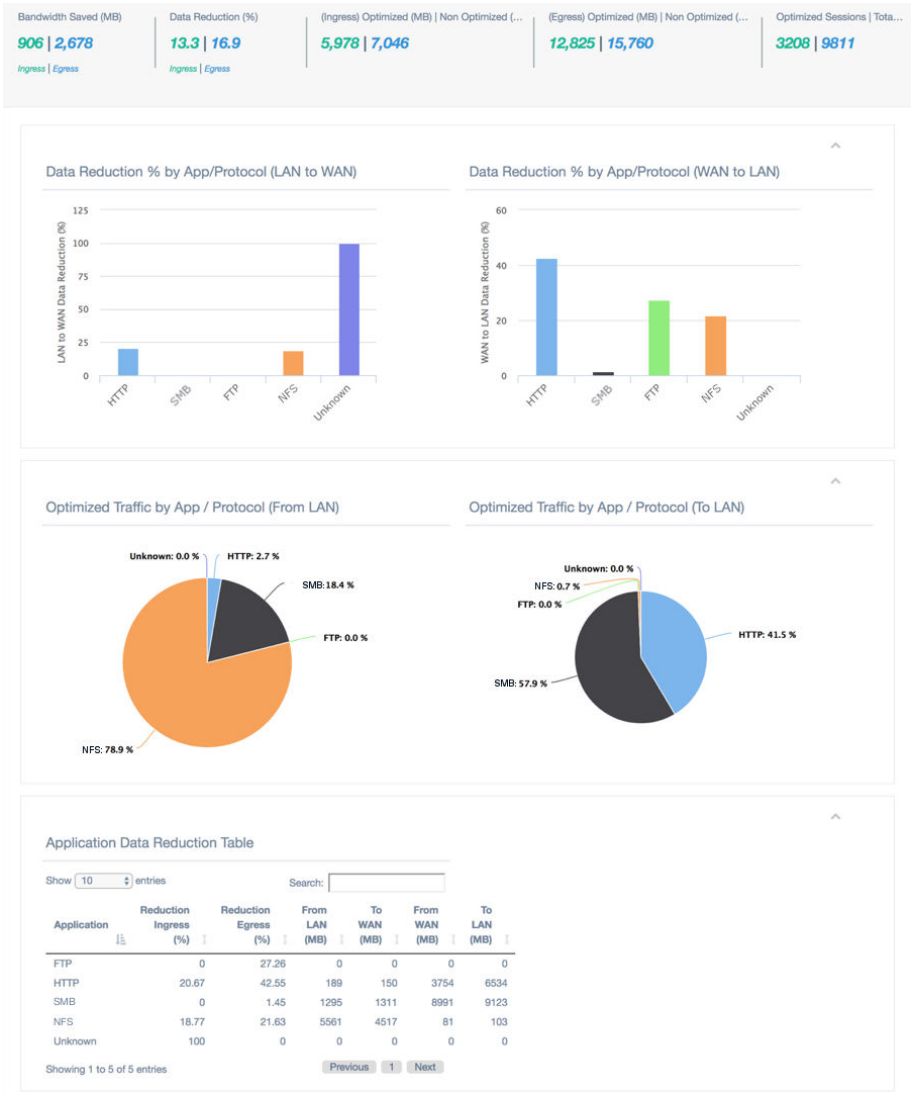
Data Reduction (%): Data reduction percentage using WAN Optimization, for WAN Ingress and WAN Egress. Links to **WAN Optimization > Monitor WANOp** with the Data Reduction % report pre-selected.

(Ingress) Optimized (MB) | Non Optimized (MB): Total WAN Ingress bandwidth optimized vs non-optimized, in MB. Links to **WAN Optimization > Statistics**.

(Egress) Optimized (MB) | Non Optimized (MB): Total WAN Egress bandwidth optimized vs non-optimized, in MB. Links to **WAN Optimization > Statistics**.

Optimized Sessions | Total Flows: Total number of active WAN Optimized sessions vs total active sessions. Links to **WAN Optimization > Flows**, with WAN Ingress, WAN Egress, and TCP Termination Table pre-selected.

The second section of the WAN Optimization dashboard provides data reduction reports by application/protocol:



Data Reduction % by App/Protocol (LAN to WAN): Data reduction percentage for each protocol or application (for applications defined in the configuration), for WAN Ingress (upload). Users may hover over each bar to see the exact percentage.

Data Reduction % by App/Protocol (WAN to LAN): Data reduction percentage for each protocol or application (for applications defined in the configuration), for WAN Egress (download). Users may hover over each bar to see the exact percentage.

The third section of the WAN Optimization dashboard provides information about optimized traffic by application/protocol:

Optimized Traffic by App/Protocol (From LAN): Chart displaying the percentage of total optimized upload/WAN Ingress traffic for each protocol or application (for applications defined in the configuration). Users may hover over each bar to see the exact percentage.

Optimized Traffic by App/Protocol (To LAN): Chart displaying the percentage of total optimized download/WAN Egress traffic for each protocol or application (for applications defined in the configuration). Users may hover over each bar to see the exact percentage.

The final section of the WAN Optimization dashboard is the **Application Data Reduction Table**:

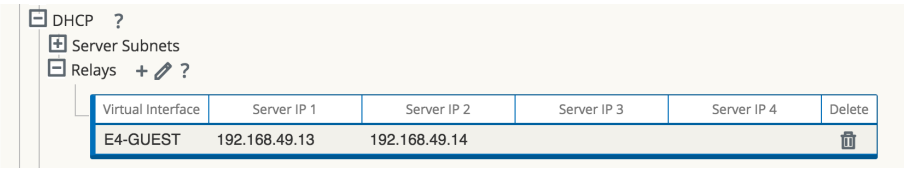
The Application Data Reduction table shows flow statistics for WAN Optimized sessions that match user-defined Application objects in the configuration, as well as WAN Optimized HTTP, HTTPS, FTP, SSH, and Telnet sessions that do not match a defined Application object.

For more information about WAN Optimization, please see the WAN Optimization Guide.

Enhanced DHCP Relay

7.2 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:

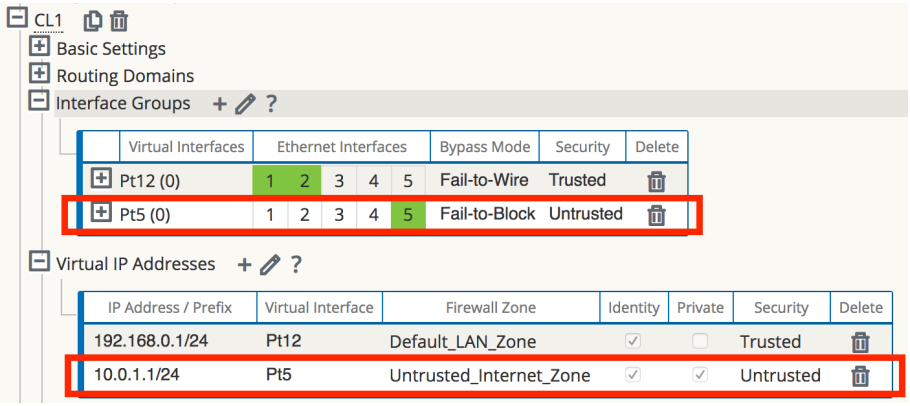


When configuring DHCP Relays, the Virtual Interface and Server IP 1 are required. Server IPs 2 through 4 are optional.

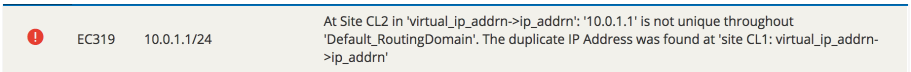
Monitoring information for DHCP Relay is available under **Monitor > DHCP**.

Client Private Subnet Reuse for Untrusted Segment

7.2 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.

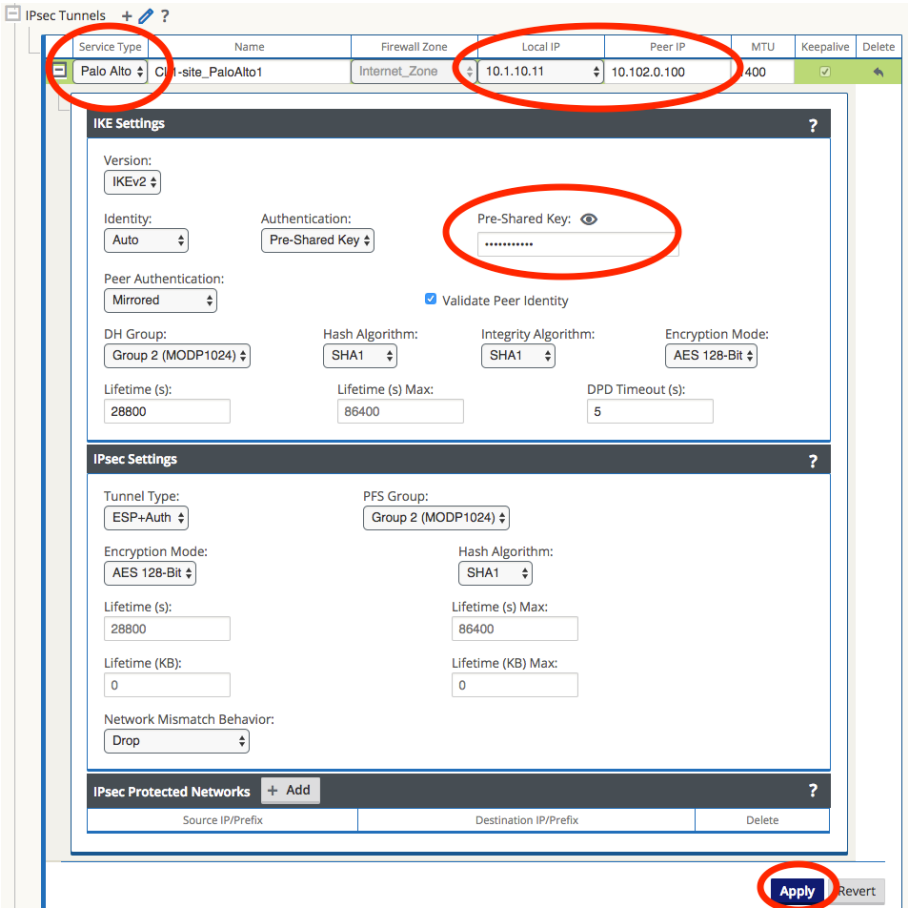


Palo Alto GlobalProtect Cloud Integration

7.2 adds support for integration of branch office Oracle Talari 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 **Configuration > Configuration Editor** on the NCN 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**.



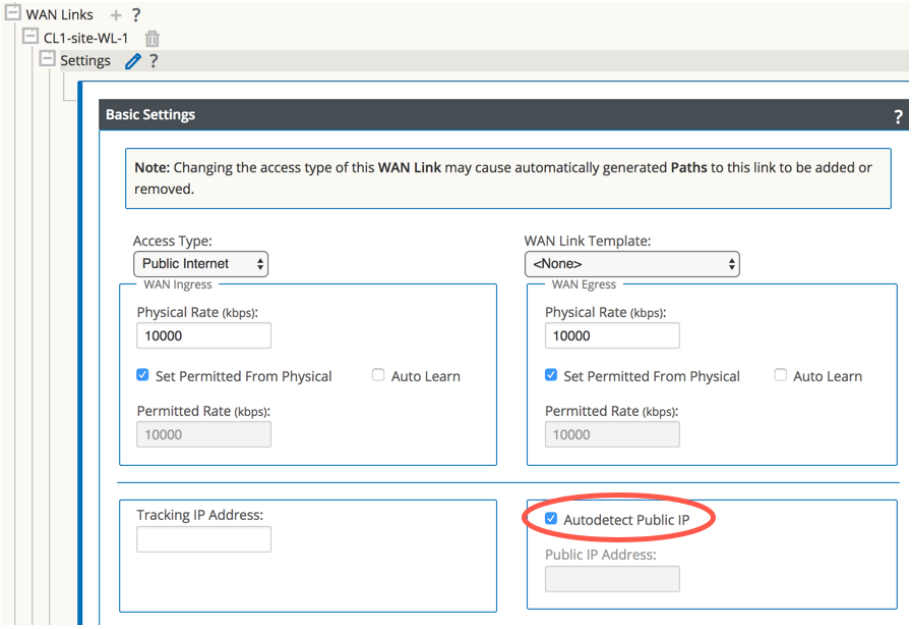
If no options are available in the Local IP dropdown, ensure Internet Service is enabled on at least one WAN link at the site under **Connections > [Site Name] > Internet Services**.

Private Cloud Path Enhancement

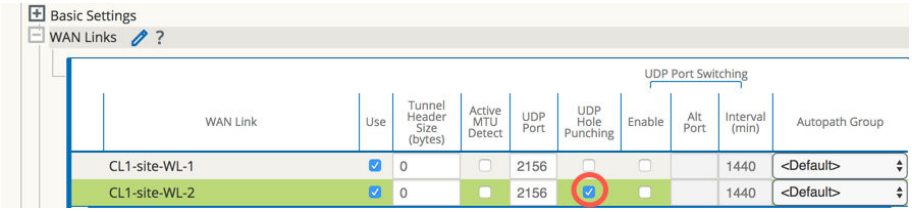
In certain cases, service providers have a private cloud which is separate from the public Internet. Within their environment they use PAT (Port Address Translation) to forward user traffic from their private cloud to the Internet. In these cases, the service provider will have a limited number of public IP address for NATing. When deployed for an enterprise customer, if they select one of these providers for multiple client sites, there is the possibility that multiple Client WAN links could be PATed/NATed to the same public IP address. Prior to 7.2, Talari 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 Path in the GOOD state. However, at the second Client site using the same public IP address, the Path would be in the DEAD state. To resolve this issue, 7.2 has been enhanced to use the source IP address and source port for path learning validation. With this enhancement Talari 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 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 7.2 GA

7.2 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.

19

Release 7.2 P3 Features

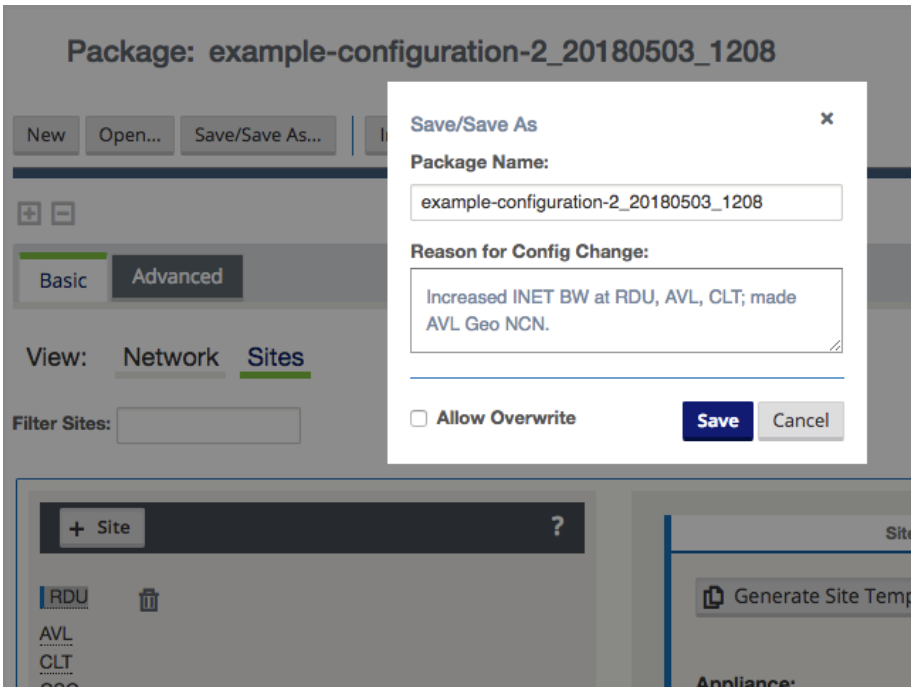
This chapter includes features and enhancements released in 7.2 P3.

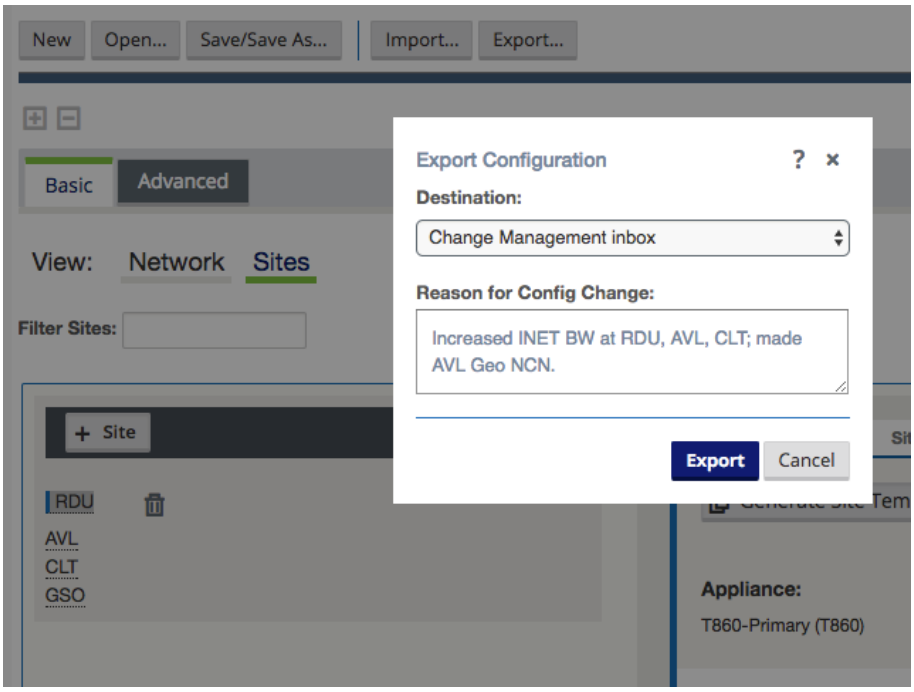
Configuration Versioning and Comparison

Configuration Versioning

Beginning in 7.2 GA P3, configurations will be versioned automatically whenever a change is applied via Change Management. Each new version contains additional metadata which allows network administrators to quickly audit changes to the configuration. The information collected includes: the user who edited the configuration and when the edit was made, the user who activated the configuration and when the configuration was activated, the name of the configuration, and a user-generated comment describing the reason for the change. All of the information except the user-generated comment will be collected automatically without any required action from the user or network administrator.

Whenever a configuration is saved or exported, the user will be prompted to add a comment, as shown below:





Note:

Adding or updating the user comment is not enforced by the configuration editor. Users may save or export a configuration with no added comment, or without updating the comment text.

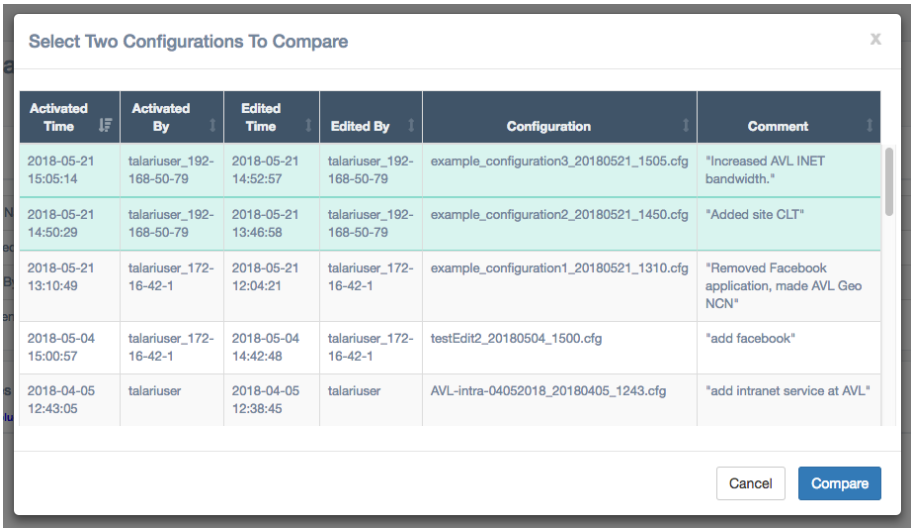
> **Note:**
>
> Adding a user comment when exporting a saved configuration will overwrite any user comment added when the configuration was previously saved.

Configuration Comparison

To review and compare configurations, navigate to **Configuration > Compare Archived Configurations** and click **Select Configurations to Compare**.

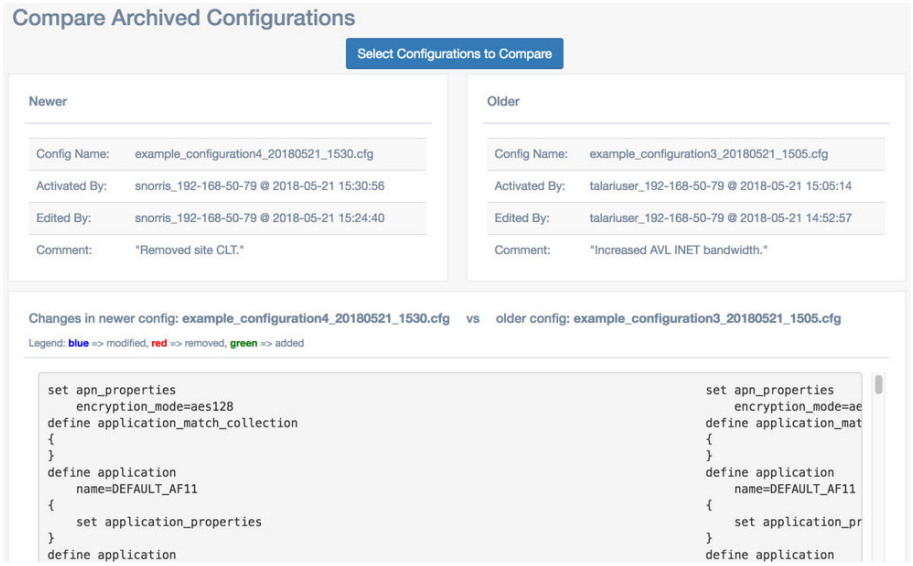
> **Note:**
>
> Only configurations which have already been activated via Change Management are available for comparison.

Click to select or deselect a configuration for comparison. Selected configurations will be highlighted. Click Compare to view the selected configurations.



> **Note:**
>
> More than two configurations may be selected, but only two configurations may be compared at a time. The Compare button will be greyed out until only two configurations are selected.

The newer configuration will be displayed on the left, and the older configuration will be displayed on the right. In addition to the configuration name and user-generated comment, the header for each configuration will show the activating/editing username, IP address, date, and time:



A side-by-side comparison of the configuration text file is displayed below the headers. Objects that have been removed will be highlighted in red and marked with a "-":

Objects that have been added will be highlighted in green and marked with a "+":

Objects that have been modified will be highlighted in blue and marked with a "<<":

20

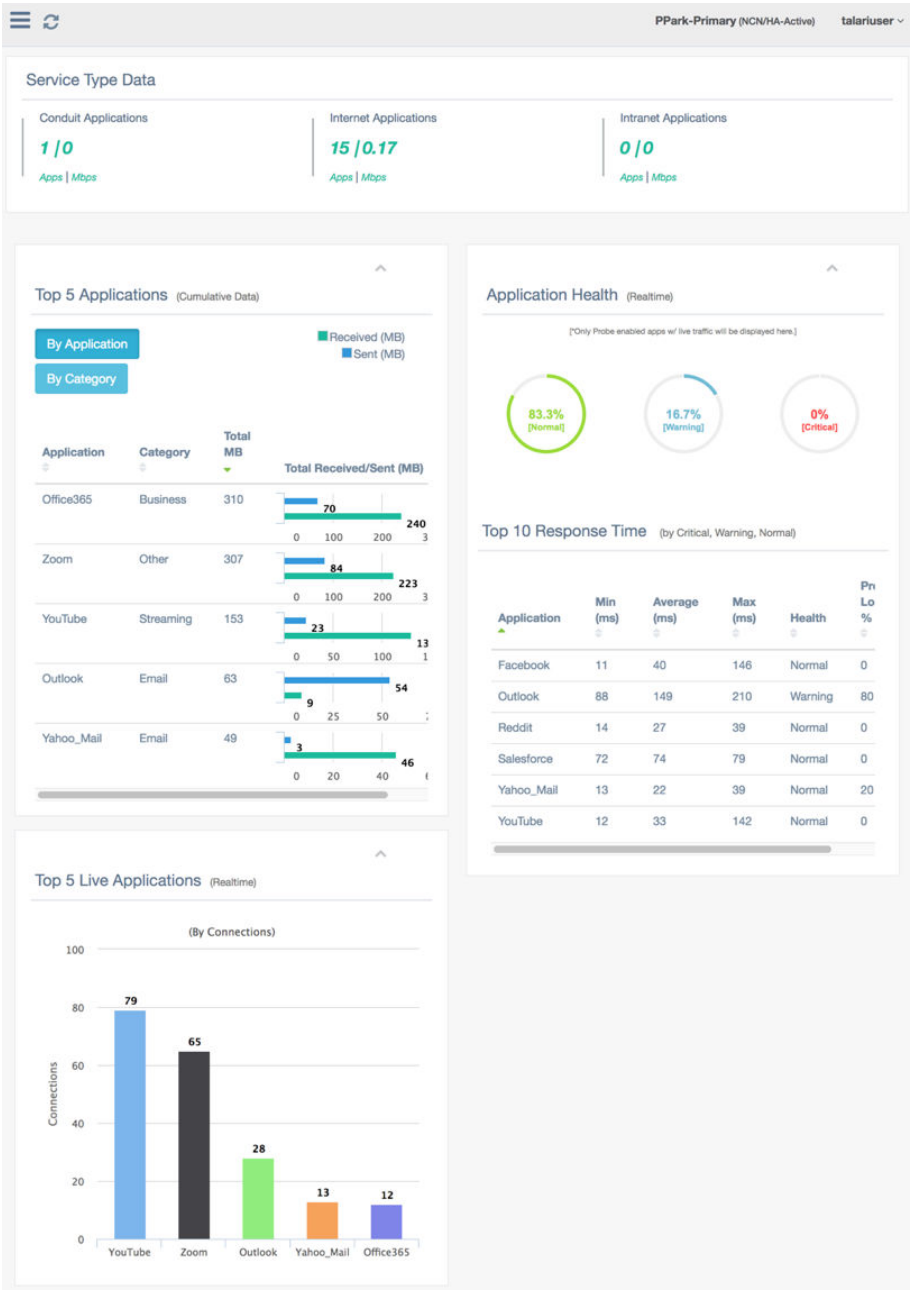
Release 7.3 Features

This chapter includes features and enhancements released in 7.3.

Enhanced Application Identification

7.3 GA introduces Enhanced Application Identification, which offers a significant improvement to how Oracle Talari 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 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. Talari will provide updates to the Application Signature Library moving forward based on customer feedback.
- A dedicated application dashboard which allows the user to view top cumulative and live applications, bandwidth usage by service, and application health information. This information helps administrators perform common tasks such as troubleshooting and capacity planning:



- Streamlined configuration elements that make creating an application policy fast and easy. The 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 *Enhanced Application Identification & Application Signatures Guide.*

E500 Appliance (7.3 GA P3)

7.3 GA P3 adds support for the E500 appliance. The E500 is an extension of the E-series of Oracle Talari Appliances. The E500 intended for use in mid-sized branch or regional offices that require higher performance and port density than the E100 provides. The E500 supports WAN Optimization and Easy 1st Install. For more information on this platform, please see the *E500 Installation Guide* and the *E500 Hardware Guide*.

Private Registration Server (7.3 GA P3)

Beginning in 7.3 GA P3, customers who do not wish to depend on the public Registration Server may host a Private Registration Server for use during the Easy 1st Install process. The private registration server may be deployed for access via an incumbent private intranet or for access via the public Internet, and may use either a static IP host or a DNS-resolvable Fully Qualified Domain Name (FQDN).

Once the Private Registration Server (PRS) is installed and operational, the high-level data flow for the Easy 1st Install process to complete properly is as follows:

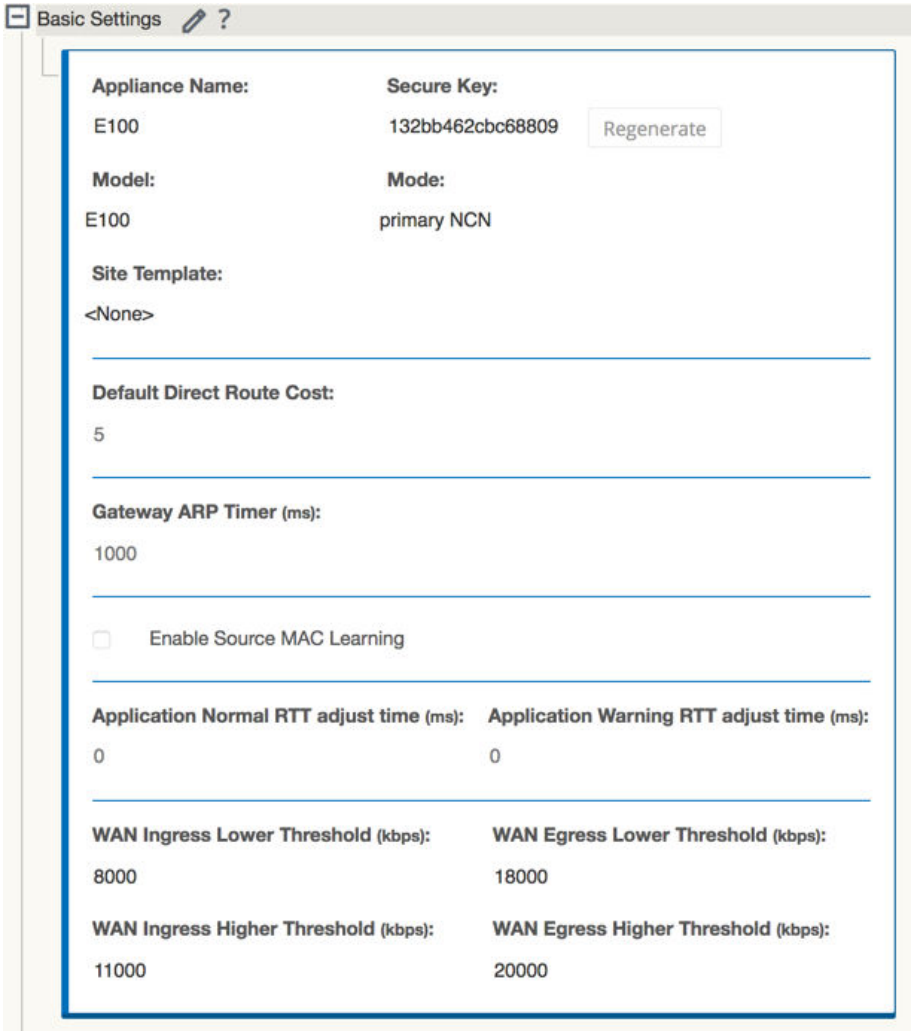
- User provides the serial number for the site being deployed to the NCN
- The NCN uploads package to the PRS
  - Connectivity must exist to the PRS from the NCN management port IP
  - The NCN pushes the client package to the PRS via HTTPS
- Once the client appliance is powered on and has an IP address/gateway/DNS for the management port, the following occurs:
  - The client will attempt to establish an HTTPS session via its management port to the PRS and provide its serial number
    - Once the serial number is validated via the HTTPS session, the PRS will provide a URL for the client to download the appliance package
  - The client appliance will establish a second HTTPS session to retrieve the appliance package based on the validated serial number

For detailed information on deploying and using a Private Registration Server, please see the *Private Registration Server Installation and Deployment Guide.*

Threshold Alerting (7.3 GA P4)

7.3 GA P4 introduces the ability to monitor WAN link usage and trigger an alert if a user-defined usage threshold is exceeded. Threshold Alerting can provide insight into situations wherein the failure of one WAN link in a Conduit would result in the remaining WAN link(s) being oversubscribed, allowing customers to resolve potential issues before they arise.

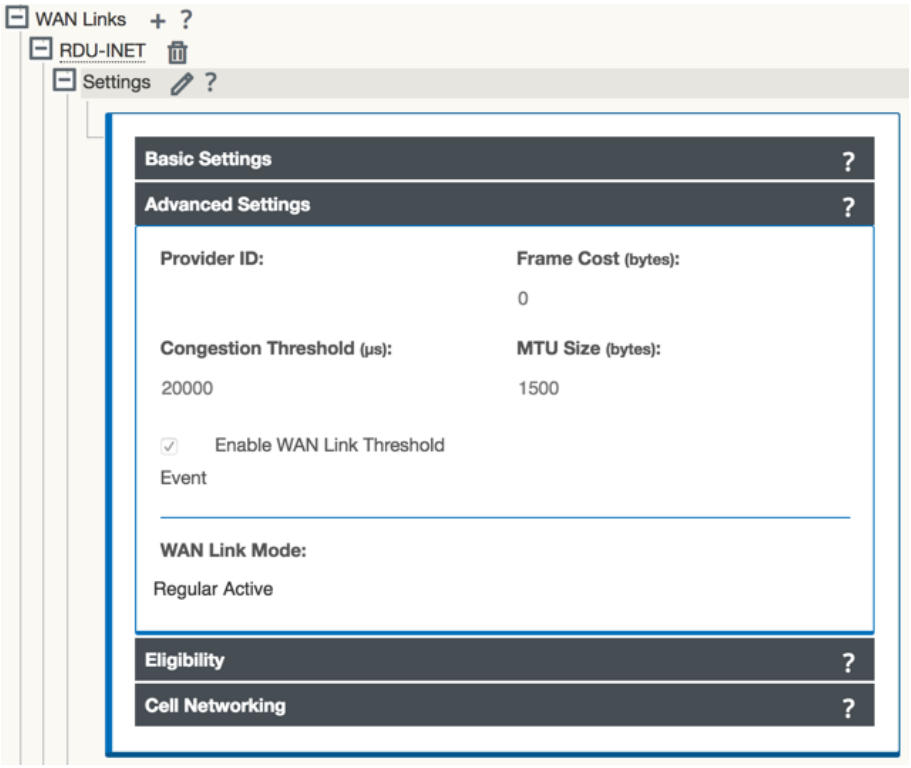
Threshold Alerting is configured using the Advanced view of the Configuration Editor, and is disabled by default. To enable Threshold Alerting at a site, go to **Sites > [Site] > Basic Settings** and enter a non-zero value for at least one threshold:



When a threshold is configured and the combined WAN link usage for the site exceeds the configured value, an event will be generated.

> **Note:**
>
> When the combined WAN link usage exceeds the Lower Threshold value, an event with a severity of “Notice” will be generated. When the combined WAN link usage exceeds the Higher Threshold value, an event with a severity of “Warning” will be generated.

By default, all WAN links at a site are used for threshold calculations. To exclude a WAN link from threshold calculations, go to **Sites > [Site] > WAN Links > [WAN Link] > Settings > Advanced Settings** in the Advanced view of the Configuration Editor and uncheck the “Enable WAN Link Threshold” box:



Additional Features in 7.3

- CT800-128 and VT800-128 Appliances (7.3 GA P4)
  7.3 GA P4 introduces support for the CT800-128 and the VT800-128. These new virtual appliances build on the CT800 and VT800 appliances to support up to 128 conduits in AWS, ESXi, Azure, and HyperV.
- Increased Throughput in AWS (7.3 GA P4)
  The CT800-128 supports a new maximum performance level of 500Mbps full-duplex for AWS.

21
Release 8.0 Features

This chapter includes features and enhancements released in 8.0.

ID	Description	Release
16569	Old log files are now compressed to permit longer retention.	8.0 GA
16551	8.0 GA introduces Cloud Connect, which allows customers to connect to participating Cloud Connect providers from the enterprise platforms via Cloud Conduits.	8.0 GA
19119	The licensing requirement for virtual appliances (VT800, VT800 - 128, CT800, and CT800 - 128) has been removed.	8.0 GA P1

22
Release 8.1 Features

This chapter includes features and enhancements released in 8.1.

ID	Description	Release
29989632 (19500)	User Names can now contain several special characters that were previously disallowed: @, /, and \ .	APN 8.1 P1
29989624 (19486)	T5200 CPU profile optimizations as well as general packet scheduler enhancements have been made to significantly improve performance and stability during heavy load across large networks. Advanced logging and alerting tools are included.	APN 8.1 P1
29989439 (19230)	When configuring email alerts with SMTP Authentication enabled, event emails may not be sent.	APN 8.1 P1
29989448 (19245)	8.1 introduces support for the D6000. The D6000 is the replacement appliance for the T5X00 series, with improved performance.	APN 8.1 GA
29989220 (18936)	8.1 introduces support for the D2000. The D2000 is the replacement appliance for the E1000.	APN 8.1 GA

23
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.