

Oracle® SD-WAN

Security Guide



Release 8.2
F26388-01
November 2019

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle SD-WAN Security Guide, Release 8.2

F26388-01

Copyright © 2013, 2019, Oracle and/or its affiliates. All rights reserved.

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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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	v
	Revision History	
1	Security Overview	
2	Security Features	
3	IPsec VPN Termination	
4	Feature Configuration	
	Changing a Password	4-13
5	Oracle SD-WAN Firewall Configuration	
	Firewall Use Case Examples	5-12
	Firewall Configuration	5-31
6	Glossary	

List of Figures

5-1	Firewall Zones	5-2
5-2	Interface Groups	5-2
5-3	Zone Diagram	5-3
5-4	Zone Inheritance	5-3
5-5	Firewall Policies	5-4

About This Guide

The purpose of this document is to provide the reader with an understanding of current security methods within the Oracle SD-WAN solution. The reader of this document is expected to be a network architect or a network administrator.

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
September 2019	• Initial release

1

Security Overview

Oracle SD-WAN is a QoS and WAN virtualization device. It can terminate IPsec tunnels that are external from the Talari Conduit. The number of tunnels an appliance can terminate is dependent on the appliance model.

However, because of the encapsulating nature of Conduits between two APNA endpoints, Oracle is able to provide end-to-end security for intra-network traffic. The rich set of security features provided by the APN solution allows customers to reduce costs by eliminating VPN appliances and services between Sites in the APN.

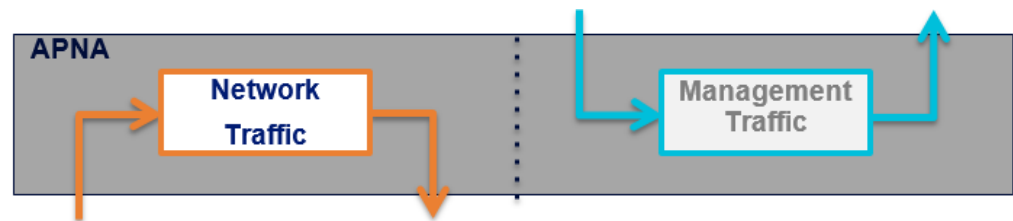
2

Security Features

Separation of Management and Network Traffic

The Oracle SD-WAN explicitly segregates all management and network traffic. This affords the appliance the ability to use known hardened applications to protect the appliance's management and configuration features without concern for collisions with Talari technologies.

This division also means that the Oracle SD-WAN data path cannot be compromised through management applications with known or unknown exploits or through standard probing techniques as the data path is not required to monitor, respond to, or forward management application traffic.



Security Zones

Oracle SD-WAN configuration allows for the explicit designation of network interfaces as Trusted or Untrusted.

A Trusted interface is a port that connects to a network where security is provided or is unnecessary. An example of this would be a link to an MPLS network or to a router that manages network-to-network security via a VPN infrastructure. Generally speaking, it is expected that a Trusted network segment is firewalled. Paths on a trusted interface can be configured as encrypted or non-encrypted.

An Untrusted interface is a port that connects to a network where no security/firewall is provided. An example of this would be a link to the public Internet, such as a DSL or Cable Internet connection. Paths on an untrusted interface can only be configured as encrypted. The Oracle SD-WAN does not allow non-encapsulated traffic to be forwarded from an Untrusted to a Trusted interface but does allow for PING and ARP requests.

Path Encryption

All Paths within a Conduit can be independently configured to encrypt or not encrypt their data between Sites. The method of encryption is configured globally for the entire Oracle SD-WAN. Path encryption is performed as follows:

- AES Encryption with 128bit or 256bit key (key length configured globally)
- Cipher Block Chaining (CBC) Mode
- Per-protocol sequence numbers included in every encrypted packet to help ensure message indistinguishability
- Per-session symmetric encryption keys negotiated using Elliptic Curve Diffie-Hellman exchange

- Optional: Periodic encryption key rotation using Elliptic Curve Diffie-Hellman exchange
- Optional: Use of an Initialization Vector, known as the Extended Packet Encryption Header
- Optional: Use of additional message authentication information, known as the Extended Packet Authentication Trailer

Per-Session Encryption Keys and Encryption Key Rotation

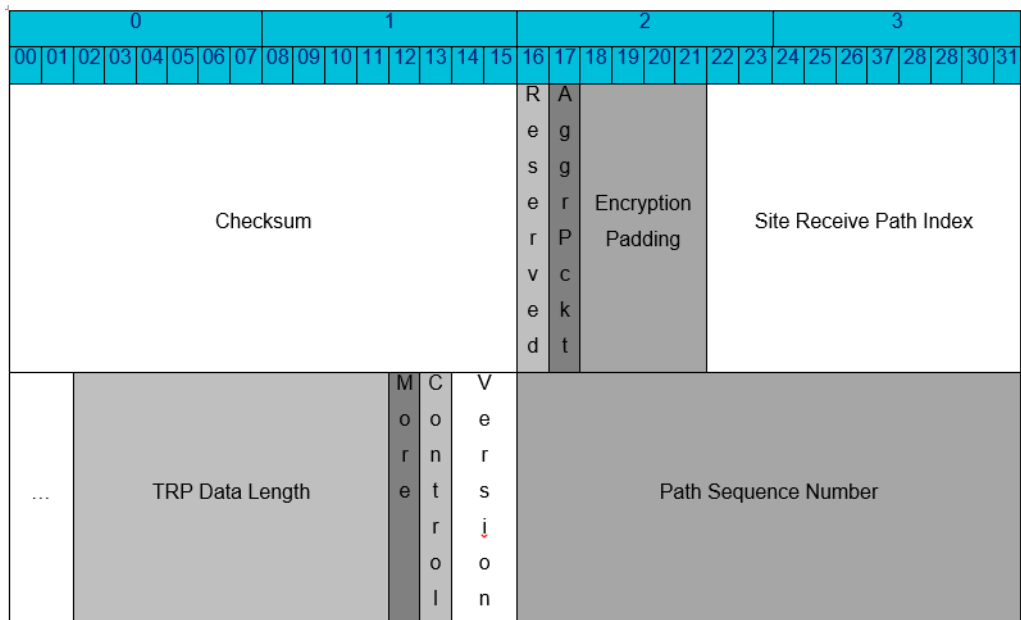
Per-session encryption keys are generated and automatically rotated (when Encryption Key Rotation is enabled) using an Elliptic Curve Diffie-Hellman algorithm. This provides the following benefits:

- Forward Secrecy
- Frequency Analysis from one session to another becomes a cryptographically hard problem since the session start and sequence number wrapping events are not immediately known
- A compromised encryption key does not automatically compromise the entire system and an Oracle SD-WAN reboot or encryption rekey re-secures the entire Oracle SD-WAN

Use of the Encryption Key Rotation feature is configured globally for the entire Oracle SD-WAN. It is enabled by default and Oracle strongly recommends that it remain enabled during normal operation. Disabling this feature may be relevant for certain troubleshooting scenarios. When enabled, Conduit encryption keys will be renegotiated on a random interval between 10 and 15 minutes.

Peer Message Authentication

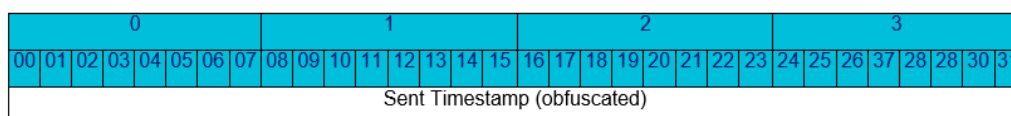
The Oracle SD-WAN encrypts a checksum of the Talari Reliable Protocol (TRP) header as part of each outgoing message. After decryption is complete on the receiving end, the checksum is validated. Since the checksum was encrypted with the message, the Oracle SD-WAN assumes that a trusted party sent the message, provided that the encryption key is secure.



Users can also enable the Extended Packet Authentication Trailer, which greatly strengthens message authentication. This feature is described below.

Replay Attack Protection

In the Oracle SD-WAN, the NCN maintains a network time to which all Clients must sync. This gives the Oracle SD-WAN a uniquely accurate method to protect against replay attacks without the need for sequence number synchronization. The Oracle SD-WAN obfuscates a sent timestamp in the TRP trailer of each outgoing message. If the sent timestamp of an arriving packet isn't within a certain range of the current network time, the packet is unlikely to be needed by users in the network and is also unlikely to be valid for processing. The Oracle SD-WAN will discard the packet.



The timestamp is sent with microsecond resolution and is 32 bits in length, which yields a ~4300 second (72 minute) range of protection. Encryption key rotation (which is configurable, but enabled by default) causes encryption keys to be renegotiated at intervals not to exceed 15 minutes, which means that there is never a long term window in which a replayed packet could be successful. Additionally, packet and flow sequence numbers ensure that short term replayed packets are treated as duplicates and dropped accordingly.

Secure Key Regeneration

In the same sense that it is not possible to eliminate the security ramifications of leaked VPN passwords, it is not possible to eliminate the ramifications of leaked Secure Keys. To that end, the Secure Key for a Site or for all Sites in the Oracle SD-WAN can be quickly regenerated via the Oracle SD-WAN web console. Regenerating Secure Keys is a non-resetting configuration change and will not affect Oracle SD-WAN operations.

Secure Key Protection

In both Oracle SD-WAN Software and Oracle SD-WAN Aware, Secure Keys are removed from all diagnostic information and no information is provided in diagnostic information that would allow Secure Keys to be reverse engineered.

Message Indistinguishability

- **Sequence Number Size**—The encryption key rotation window has been defined to guarantee that sequence numbers don't wrap before the next key rotation. In order to balance the need for indistinguishability against the potential performance impact of key rotation, the rotation window and the size of various sequence numbers have been tuned against one another to extend the roll over time.
- **Initial Sequence Number**—All sequence numbers, except for the internal TRP Flow sequence number, are seeded with a cryptographically random initial value to reduce the risk of Frequency Analysis. This eliminates the predictable nature of first packets having identical content.

Extended Packet Encryption Header (Optional)

An Initialization Vector (IV) is often used to provide very high unpredictability of the first encrypted block in a cipher block chain. However, using Initialization Vectors has some drawbacks:

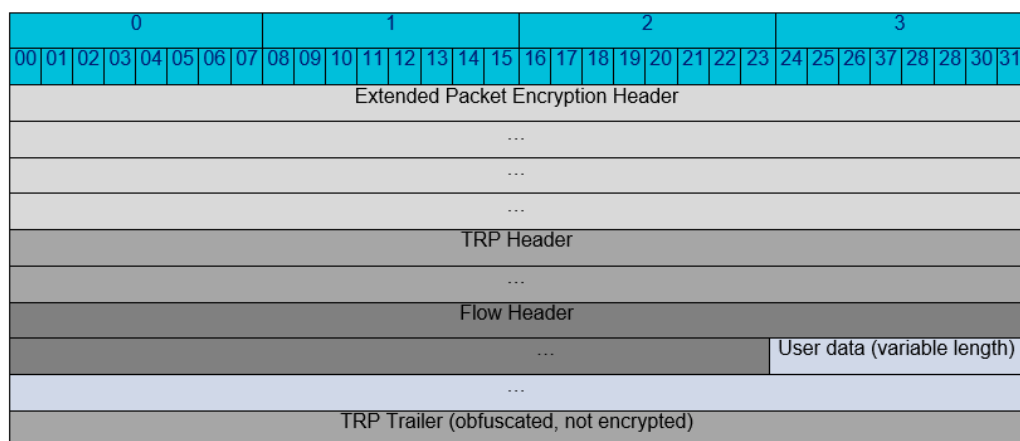
- A static IV is no more protective than a NULL IV.

- While an IV need not be secured in the encrypted message, it must be known to both sides of the encryption. Typically, this means the IV is sent along side the encrypted message.
- If an IV becomes predictable, much of the security it provides is compromised. There are known attacks to exploit this problem.

An alternative to rotating an IV in a cryptographically secure way is to seed the first cipher block of data with a large counter that is seeded with a cryptographically random initial value. After encryption, the counter is essentially a random block of data deterministic only with the encryption key. This method is proven to provide the same security as an IV, without incurring the process overhead of randomly generating an IV for each packet and guaranteeing that each IV is unique. See Appendix C of the NIST doc, which directly reference this methodology: <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>.

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 be prefixed inside the encrypted payload to act as a rotating, cryptographically random Initialization Vector.

This counter is known as the Extended Packet Encryption Header. Use of the Extended Packet Encryption Header is configured globally for the entire Oracle SD-WAN. It is disabled by default.

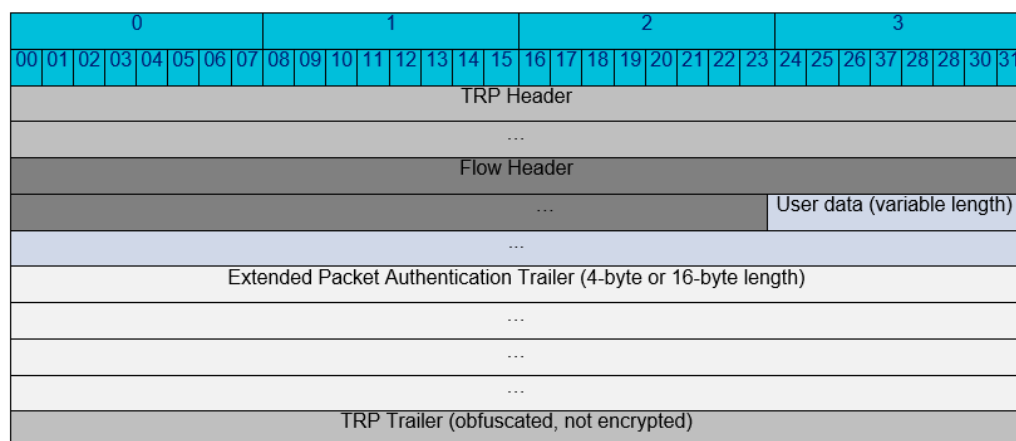


Extended Packet Authentication Trailer (Optional)

To provide users with the ability to have strong message authentication, an optional trailer inside the encrypted payload can 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. Because the checksum is over unencrypted data and is itself encrypted, there is a very high statistical likelihood that any change made to the packet will lead to either an incomprehensible packet or a mismatching checksum.

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. (Note: When used as an authenticating HMAC, the result of the SHA-256 function is truncated to 16 bytes.) Use of a standard HMAC, though cryptographically more secure, significantly decreases forwarding performance.

This trailer is known as the Extended Packet Authentication Trailer. Use of the Extended Packet Authentication Trailer is configured globally for the entire Oracle SD-WAN. It is disabled by default.



Database Security

It is recommended, for security reasons, to limit access to the Aware database in order to protect the configuration and metric data. To accomplish list, remove external access to the database so that only the Aware application can access the database.

3

IPsec VPN Termination

Oracle SD-WAN software allows Conduit based IPsec tunnels, as well as third party devices to terminate IPsec VPN tunnels on the LAN or WAN side of Oracle Appliances. Now you can secure site-to-site IPsec tunnels terminating on a Oracle Appliance using a FIPS Level 1 certified IPsec cryptographic binary. The supported number of tunnels is based on the appliance type.

IPsec – FIPS Capability

The Talari software supports a FIPS solution for IPsec traffic that is terminated within the Talari application. This is accomplished with the use of an external library licensed from Mocana. This library is FIPS Level 1 certified. This only applies to the Oracle application and NOT any related management based applications. Since the management based applications do not use the FIPS libraries, the overall system is not FIPS certified.

 **Note:**

The Mocana certification number of NIST is certification number 1878. Additional web links can be provided upon request.

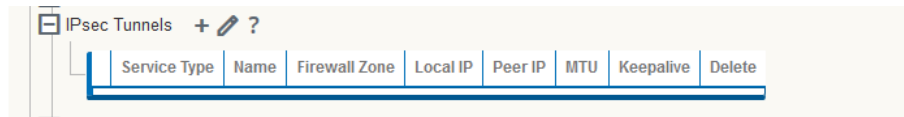
4

Feature Configuration

LAN and Intranet IPsec tunnel Configuration

IPsec is a common encryption protocol for IP communications. It has the capability to use multiple types of encryption for data confidentiality as well as multiple hash algorithms to ensure data integrity. However, generally speaking, IPsec is a statically configured protocol and relies on other systems to negotiate security parameters. The most common protocol used is Internet Key Exchange (IKE). IKE negotiates one set of security parameters to secure its own information exchange, then negotiates an independent set of security parameters for the IPsec tunnel.

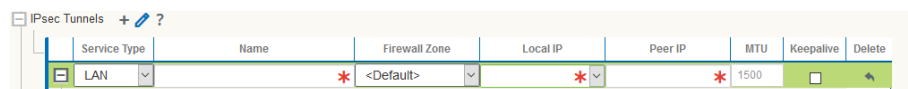
Access the IPsec configuration elements by selecting **Advanced** and then **Connections**. Use the plus symbol to add a new element and use the pencil marker symbol to edit an existing record.



Select a value for the **Service Type** parameter.

- Intranet
- LAN
- Palso Alto
- Zscalar

The default value is Intranet.



Fill in the following parameters:

- Name
 - If the service type is **Intranet**, select the auto-generated name appended with "Intranet_Service".
 - If the service type is **LAN**, type in the text in the name box.
- Firewall Zone—Select an entry from drop down list.
- Local IP—Dropdown list of Virtual IPs
- Peer IP—The other end of the component for which IP Sec tunnel needs to be established.
- MTU—The default value is 1500 bytes
- Keepalive—Is a check box, if enabled the appliance will trigger IKE and IPsec rekey

IKE Settings

Version

The IKE version used to initiate the ISAKMP. Values:

- IKEv1 (default)
- IKEv2

Mode

Phase 1 parameter exchange in Main mode or Aggressive mode. Values:

- Main (default)
- Aggressive

Identity

Identity of the IKE interface. Values:

- Auto (default)—IP address for PSK authentication, Certificate DN for certificate authentication
- IP Address— IP address of the appliance from which IKE interacts.

Authentication

The mode in which peer can authenticate the appliance. Values:

- pre-shared key (default)
- certificate

Pre-shared Key

This field appears only if the authentication method is pre-shared key, this field is for secret key of the peer.

Certificate

This field appears only if the authentication method is certificate, an entry should be selected from any of the the pre-configured certificate name which appears in the drop down list. Values: select an entry from the drop down list menu.

Validate Peer Identity

Validate the identity of the peer, which can come in the form of IP or FQDN. Values: Check box not ticked (default).

DH Group

Supported DH groups in the appliance MUST select one from the drop down list. Values:

- Group 1 – (Modp768)
- Group 2 – (Modp1024) (default)
- Group 5 – (Modp1536)

Hash Algorithms

Supported hashing algorithms in the appliance MUST select one from the drop down list.

Values:

- SHA1 (default)
- MD5
- SHA256

Encryption Mode

Encryption algorithms used for encryption in phase2 of ISAMKP. Values:

- AES 128-bit (default)
- AES 192-bit
- AES 256-bit

Integrity Algorithm

This field is specific to IKEv2 version. Values:

- SHA1 (default)
- MD5
- SHA256

Lifetime

Proposed IKE SA lifetime value in seconds for the IKE SA established during IKE phase 1 negotiation. Values:

- Min: 0
- Max: 86400
- Default: 3600

Lifetime Max

Maximum IKE SA lifetime accepted for IKE SA lifetime during IKE phase 1 negotiation. Values:

- Min: 0
- Max: 86400
- Default: 3600

DPD Timeout

Timer value in seconds when to send DPD message to peer. Values:

- Min: 0
- Max: 86400
- Default: 300

IPSec Settings

The screenshot shows the 'IPsec Settings' configuration window. It includes the following fields and values:

- Tunnel Type:** ESP
- PFS Group:** <None>
- Encryption Mode:** AES 128-Bit
- Lifetime (s):** 28800
- Lifetime (s) Max:** 86400
- Lifetime (KB):** 0
- Lifetime (KB) Max:** 0
- Network Mismatch Behavior:** Drop

Tunnel Type

Type of IPsec child SAs that can be established in phase 2. Values:

- ESP (Encapsulating Security Payload) (default)
- ESP + Auth
- AH (Authentication Header)
- ESP - NULL

PFS Group

DH group exchange used for Perfect Forward Secrecy. Values:

- <None> (default)
- Group 1 (MODP768)
- Group 2 (MODP1024)
- Group 5 (MODP1536)

Encryption Mode

Encryption algorithms used in IPsec SAs. Values:

- AES 128-bit (default)
- AES 192-bit
- AES 256-bit

Lifetime

Proposed IPsec SA lifetime value in seconds for the IPsec SA established during IKE phase 2 negotiation. Values:

- Min: 0
- Max: 86400
- Default: 28800

Lifetime Max

Maximum IPsec SA lifetime accepted for IPsec SA lifetime during IKE phase 2 negotiation. Values:

- Min: 0

- Max: 86400
- Default: 3600

Lifetime (KB)

Amount of data, in kilo bytes for an IPSec SA to exist. Values:

- Min: 0
- Max: 4194303
- Default: 0

Network Mismatch Behavior

Choose an action to take if a packet does not match the IP Sec tunnel's protected network. Values:

- Drop (default)
- Send unencrypted
- Use Non-IPSec Route

IPsec Protected Networks

The allowable set of IP addresses to use IPSec tunnels.

IPsec Protected Networks		+ Add	?
Source IP/Prefix	Destination IP/Prefix	Delete	
0.0.0.0/0	0.0.0.0/0	↩	

Source IP/Prefix

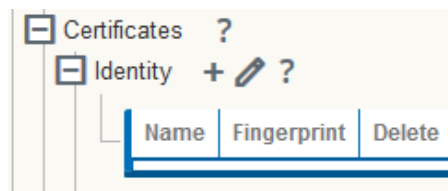
The source IP address which is allowed to use IPSec tunnels

Destination IP/Prefix

The destination IP address which is allowed to use IPSec tunnels

Certificate Configuration

In order to support IKE certificate authentication, an ability to define Identity and Trusted certificates will be created in the configuration editor. To add certificates, click **Advanced**, and then **Sites**, and then **Certificates**. Use the plus symbol to add a new element and use the pencil symbol to edit the existing records.



To create a new entry click on the plus symbol, enter a certificate name, and paste the public and private keys.

Add Identity Certificate ✕


Certificate Name:

*

Base64 Certificate:

*

Add trusted certificates who signed the certificates of the appliance.

Trusted +  ?		
Name	Fingerprint	Delete

The trusted certificate name and public key should be entered here.

Add Trusted Certificate ✕

Certificate Name:

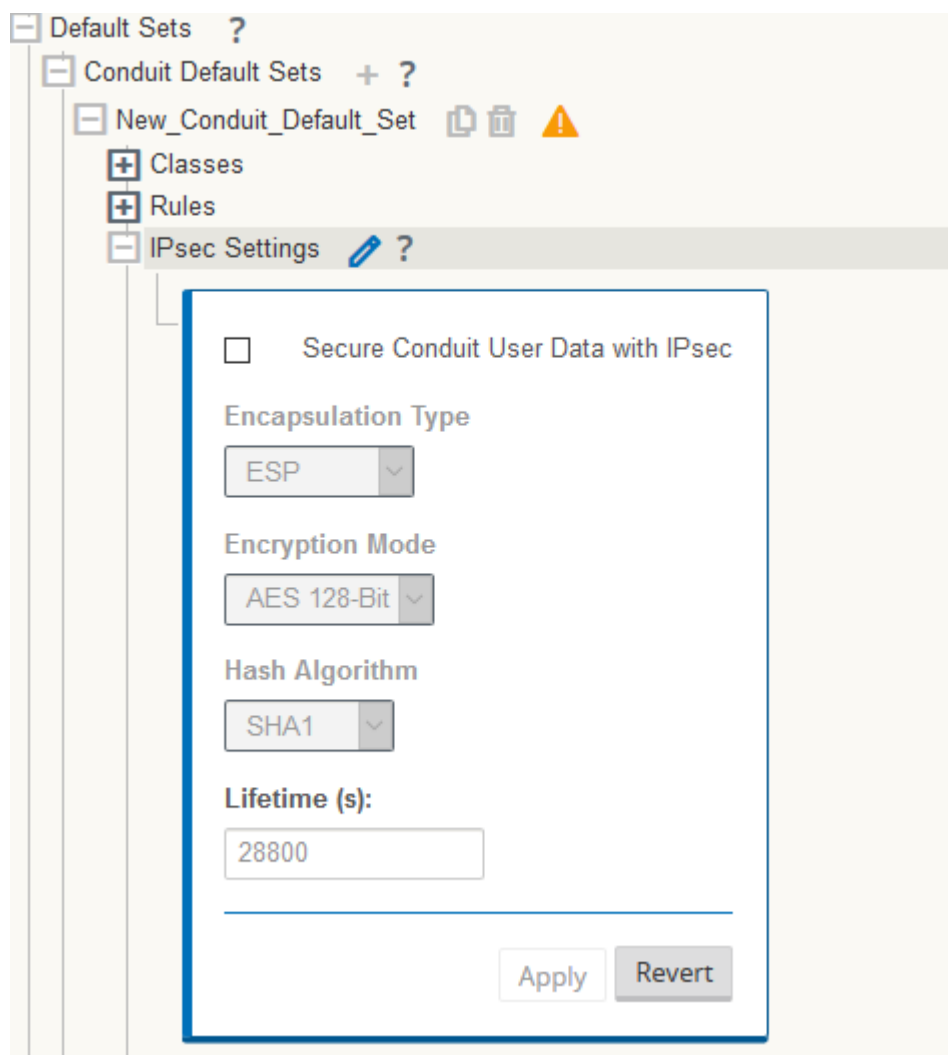
*

Base64 Certificate:

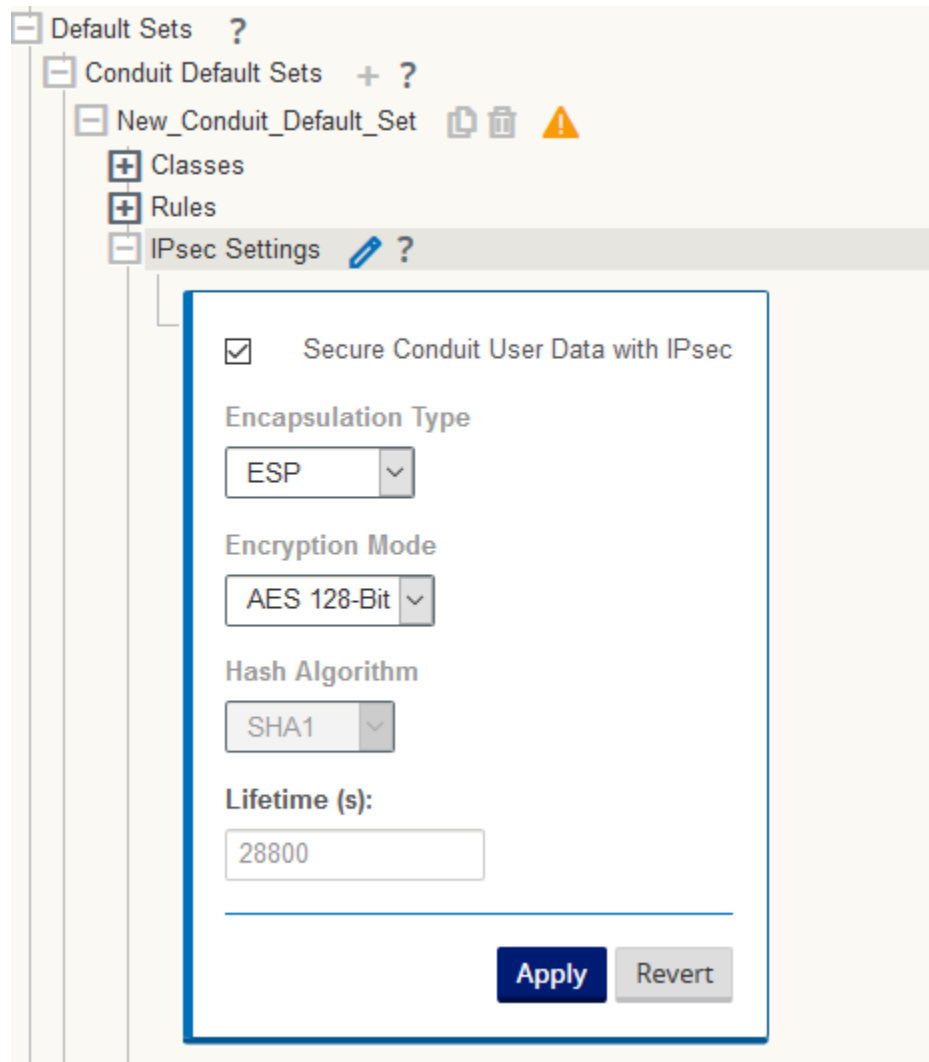
*

IPSec protected Conduits

For conduit scenario the IPSec SAs can be statically configured between two appliances, again for the establishment of IPSec tunnels IKE protocol is used. This section will allow users to configure the following information required for tunnel creation.



On selecting the check box for secure conduit user data with IPsec, there will be an option to select encapsulation type, encryption mode and the IPsec SA lifetime.



Tunnel Mode

Type of IPsec child SAs that can be established in phase 2. Values:

- ESP (default)
- ESP + Auth
- AH

Encryption Mode

Encryption algorithms used in IPsec SAs. Values:

- AES 128-bit
- AES 256-bit

Lifetime

Proposed IPsec SA life time in seconds for and IPsec SA during IKE phase 2 negotiation. Values:

- Min: 0
- Max: 86400

- Default: 28800

Dynamic Conduit IPSec

If there is no conduit configured between two sites CL1-E50 and CL2-E50 as shown in the below diagram, the data can be transferred between these two sites via WAN-to-WAN forwarding. The intermediate site (NCN-E100) must have WAN-to-WAN forwarding enabled. Traffic has to go through two hops to get to the destination site. This puts lots of burden on the intermediate site and there might be delay if the sites are in different geographical locations. The dynamic conduit feature can solve these problems as the dynamic conduits can be created on the fly when it is needed, and removed when it's no longer needed. There is a limitation on the maximum conduits can be configured per site based on the hardware type.

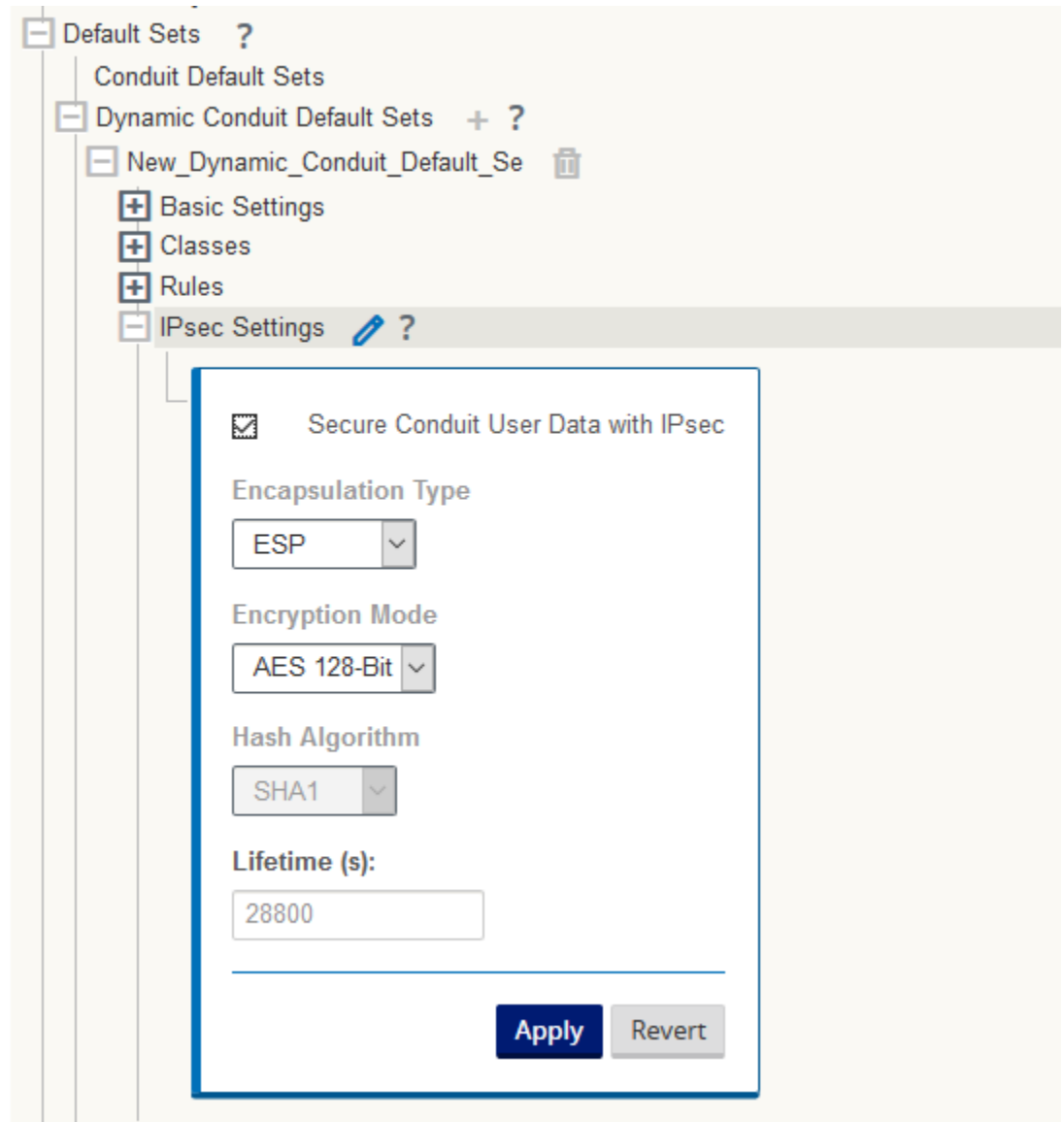
On NCN side, the check box enable WAN-to-WAN Forwarding should be enabled and also the Enable Site as Intermediate Node should be enabled.

The screenshot shows the configuration interface for the 'Connections' section of a site named 'NCN-E100'. Under the 'WAN-to-WAN Forwarding' settings, the following options are visible:

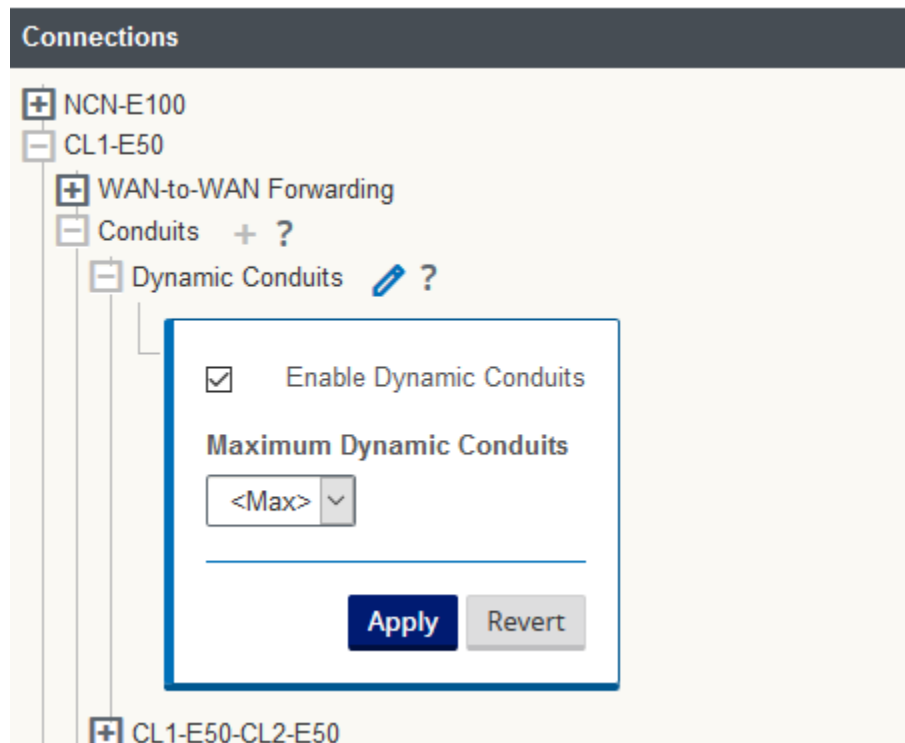
- Group:** A dropdown menu set to '<Default>'.
- Enable WAN-to-WAN Forwarding (Routes Export)**
- Enable Conduit-to-Conduit Forwarding**
- Enable Conduit-to-Internet/Intranet Forwarding**
- Route Cost:** A text input field containing the value '10'.
- Enable Site as Intermediate Node**

At the bottom right of the configuration panel, there are two buttons: 'Apply' (in blue) and 'Revert' (in grey).

The Dynamic IPSec has to be configured, it is under **Global->Default Sets->Dynamic Conduit Default Sets**.



The field **Enable Dynamic Conduits** under **connections** table should be enabled for each of the client nodes (APNAs) between whom dynamic conduits needs to be setup.



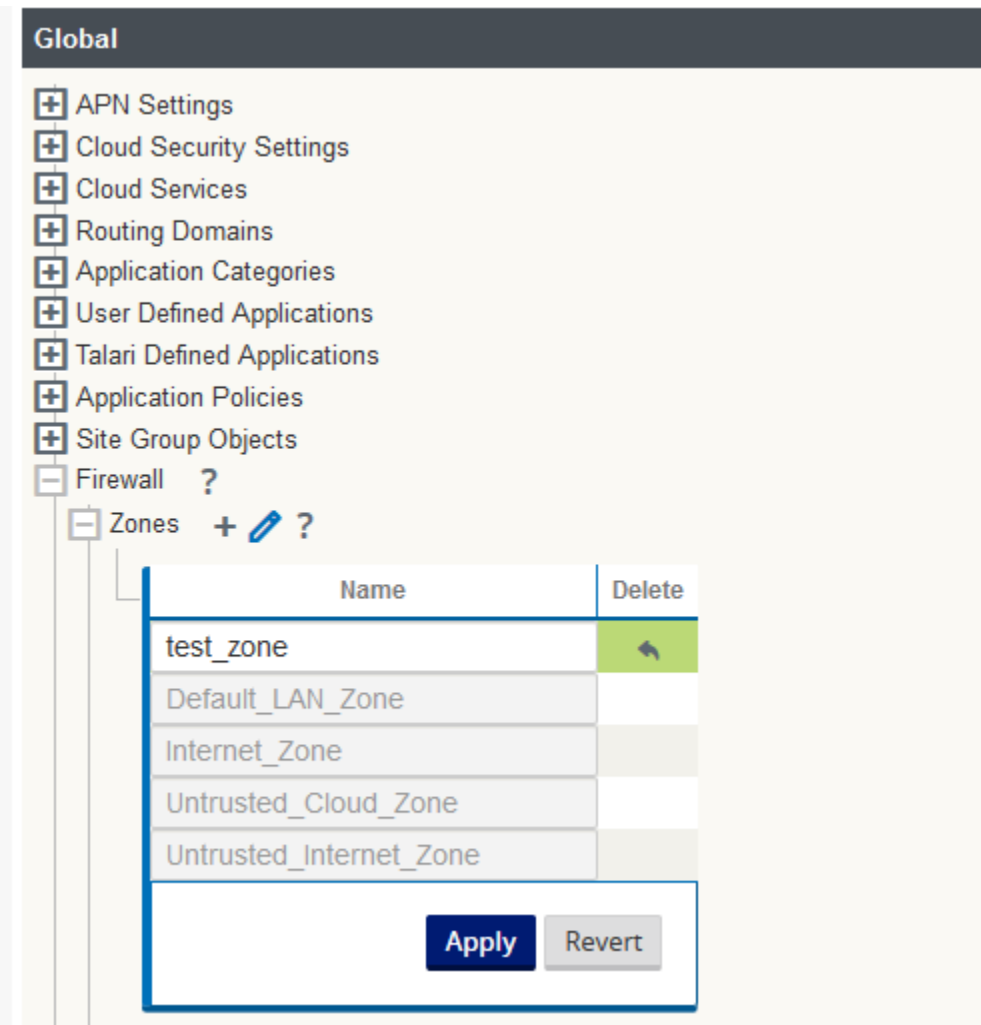
There shouldn't be any static conduits configured between the client nodes for which dynamic conduits

Set the "Autopath Group" to "default_group"

Conduit Service	Use	Tunnel Header Size (bytes)	Active MTU Detect	UDP Port	UDP Hole Punching	UDP Port Switching			Autopath Group
						Enable	Alt Port	Interval (min)	
<DYNAMIC>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	2156	<input type="checkbox"/>	<input type="checkbox"/>		1440	<None>
CL1-E50-CL2-E50	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	2156	<input type="checkbox"/>	<input type="checkbox"/>		1440	<Default>
NCN-E100-CL1-E50	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	2156	<input type="checkbox"/>	<input type="checkbox"/>		1440	<Default>

Firewall

The Firewall is a way of applying a set of security policies during the route lookup processing phase. The Talari Firewall does connection tracking so that policies can block inbound traffic that is not a result of an outbound session initiation. The Firewall application is integrated so that it knows about the different services (Conduit, Intranet, Internet, Local vs WAN, Zones) that SDWAN provides. This allows the Firewall policies to reference services, which an external firewall device would not be able to do. An external firewall has no ability to look inside SDWAN's encapsulated conduit traffic to apply policies, which the integrated inbuilt SDWAN Firewall can do.



Changing a Password

To change the local user password:

1. Click **Manage SD-WAN Edge** and then **Users/Authentication**.

The screenshot shows the 'Users / Authentication' page. The main heading is 'Users / Authentication'. Below it is the section 'Change Local User Password'. The form contains the following fields:

- User Name:
- Current Password:
- New Password:
- Confirm New Password:

At the bottom of the form is a 'Change Password' button.

2. Enter the current password.
3. Enter a new password.
4. Confirm the new password.
5. Click **Change Password**.

5

Oracle SD-WAN Firewall Configuration

The Oracle SD-WAN Firewall includes Filter Policies and NAT examples to help the user understand how to configure the firewall in certain topologies and configurations.

Oracle SD-WAN Firewall Overview

Beginning in APN 5.2 GA, Oracle provides a stateful firewall built into the Oracle SD-WAN application. The firewall allows policies between user-defined zones and Oracle SD-WAN Edge services. The firewall also supports Static NAT and Dynamic NAT (PAT & Port-Forwarding). Additional firewall capabilities include:

- Filter traffic flows between zones.
- Filter traffic between Oracle SD-WAN APN services within a zone.
- Filter traffic between Oracle SD-WAN APN services that reside in different zones.
- Define filter policies to allow, deny, and reject flows.
- Filter traffic between Oracle SD-WAN APN services at a site.
- Track flow state for selected flows.
- Global Filter Policy Templates.
- Provide Static Network Address Translation (Static NAT).
- Provide Dynamic Network Address Translation (Dynamic NAT):
- Port Address Translation (PAT).
- Port-Forwarding.

To simplify the configuration process, the firewall policies can be created at a Global level. The Global configuration consists of Pre-Appliance and Post-Appliance site Policy Templates. These templates can be applied to all sites in the APN globally. This document will provide a detailed explanation of these capabilities as well as specific configuration examples for the most commonly used Firewall topologies.

Zones

The user can configure zones in the network and define policies to control how traffic enters and leaves zones. By default, the system creates and automatically applies the following zones:

- `Internet_Zone`—Applies to traffic to or from an Internet service using a Trusted interface.
- `Untrusted_Internet_Zone`—Applies to traffic to or from an Internet service using an Untrusted interface.
- `Default_LAN_Zone`—Applies to traffic to or from an object with a configurable zone, where the zone has not been set.

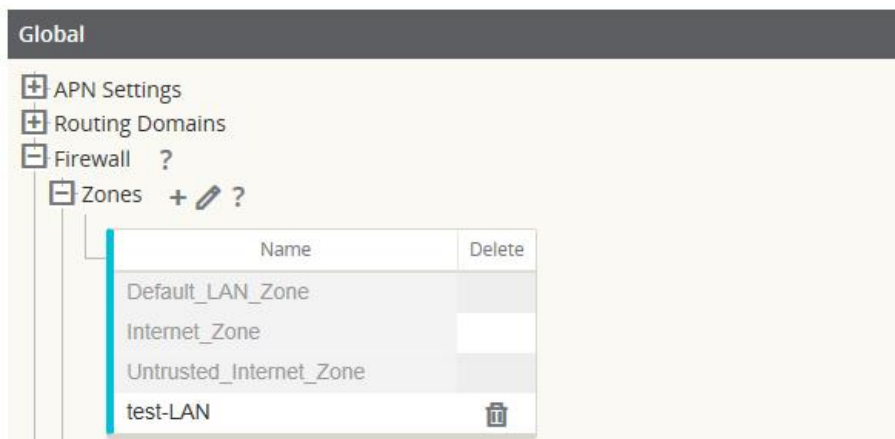
Users can create their own zones and assign them to the following types of objects:

- Virtual Network Interfaces (VNI)
- Intranet Services

- LAN GRE Tunnels
- LAN IPsec Tunnels

The following figure shows that there are three zones pre-configured for the user. Additionally, users can create their own zones as required. In this example, the zone “test-LAN” was a user created one. It is assigned to the Virtual Interface of the bypass segment (ports 1 and 2) of the Oracle SD-WAN Appliance.

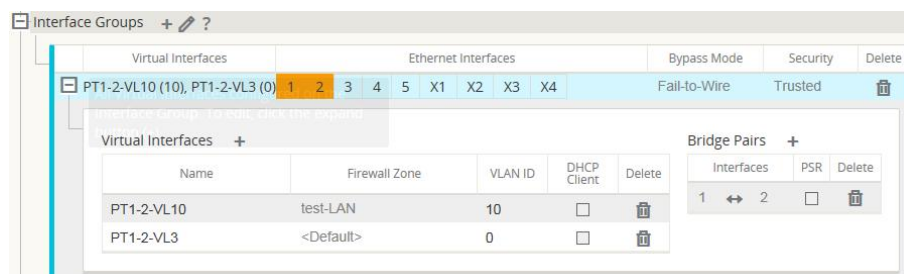
Figure 5-1 Firewall Zones



The source zone of a packet is determined by the service or VNI a packet is received on. The only exception to this is Conduit traffic. When traffic enters a Conduit, packets are marked with the zone that originated the traffic and that source zone is carried through the Conduit. This allows the receiving end of the Conduit to make a policy decision based on the original source zone before it entered the Conduit.

For example, a network administrator may want to define policies so that only traffic from VLAN 30 at Site A is allowed to enter VLAN 10 at Site B. The administrator can assign a zone for each VLAN and create policies that permit traffic between these zones and blocks traffic from other zones. Figure 2 shows how a user would assign the "test-LAN" zone to VLAN 10. In this example, the "test-LAN" zone was previously defined by the user in order to assign it to Virtual Interface "PT1-2-VL10".

Figure 5-2 Interface Groups



The destination zone of a packet is determined based on the destination route match. As a Oracle SD-WAN Appliance looks up the destination subnet in the route table, the packet will match a route, which has a zone assigned to it.

To state this information again:

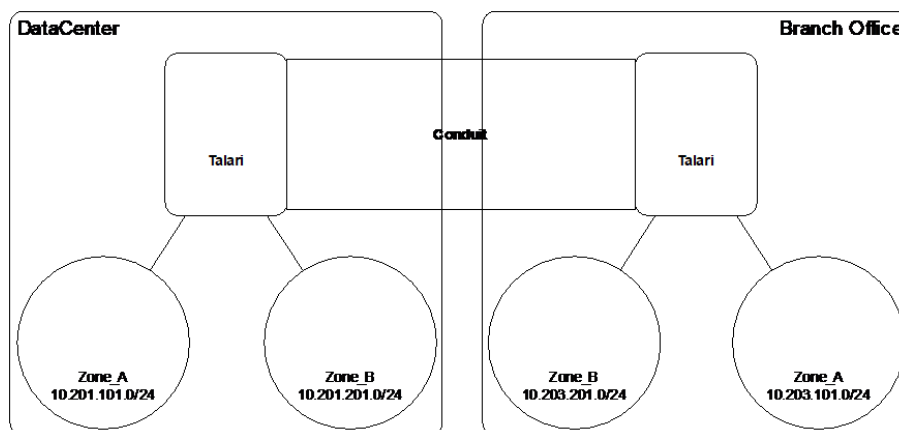
- Source zone
 - Non-Conduit: Determined via the VNI packet was received on.
 - Conduit: Determined via source zone field in packet flow header. (VNI the packet was received on at source site)
- Destination zone
 - Determined via destination route lookup of packet.

Routes shared with remote sites in the APN maintain information about the destination zone, including routes learned via a dynamic routing protocol (BGP, OSPF). Using this mechanism, zones gain global significance in the APN and allow end-to-end filtering within the APN.

The use of zones provides a network administrator an efficient way to segment network traffic based on customer, business unit, or department.

The capability of the Oracle SD-WAN firewall allows the user to filter traffic between services within a single zone, or to create policies that can be applied between services in different zones, as shown in the following figure. In the example below, we have Zone_A and Zone_B, each of which has a LAN VNI.

Figure 5-3 Zone Diagram



The following figure displays the inheritance of zone for a VIP from its assigned VNI.

Figure 5-4 Zone Inheritance

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.3.200.11/24	INET-PT3	Untrusted_Internet_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Untrusted	
10.3.2.11/24	PT1-2-VL3	test-LAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	

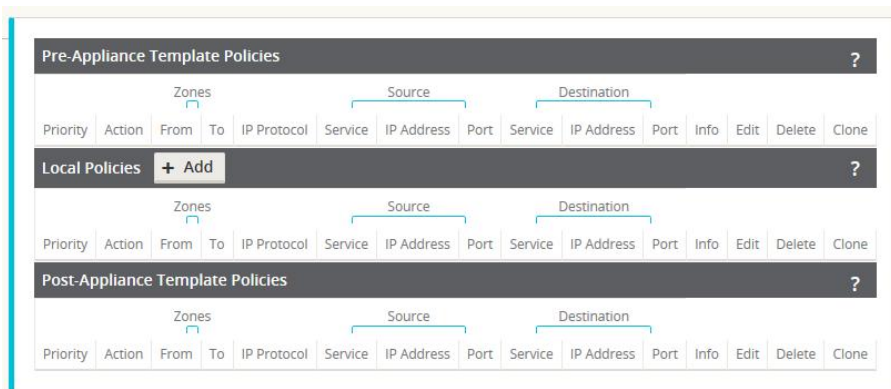
Policies

Policies provide the ability to allow, deny, reject, or count and continue specific traffic flows. Applying these policies individually to each site would be difficult as the APN grows in size. To resolve this issue, groups of firewall filters can be created with a Firewall Policy Template.

A Firewall Policy Template can be applied to all sites in the APN or only to specific sites, as required. These policies are ordered as either Pre-Appliance Template Policies or Post-Appliance Template Policies. Both APN-wide Pre-Appliance and Post-Appliance Template Policies are configured at the Global level (refer to Figure 6 on Page 7).

Local policies are configured at the site level under **Connections** and apply only to that specific site.

Figure 5-5 Firewall Policies



Pre-Appliance Template Policies are applied before any local site policies. Local site policies are applied next, followed by Post-Appliance Template Policies. The goal is to simplify the configuration process by allowing a user to apply global policies while still maintaining the flexibility to apply site-specific ones.



Note:

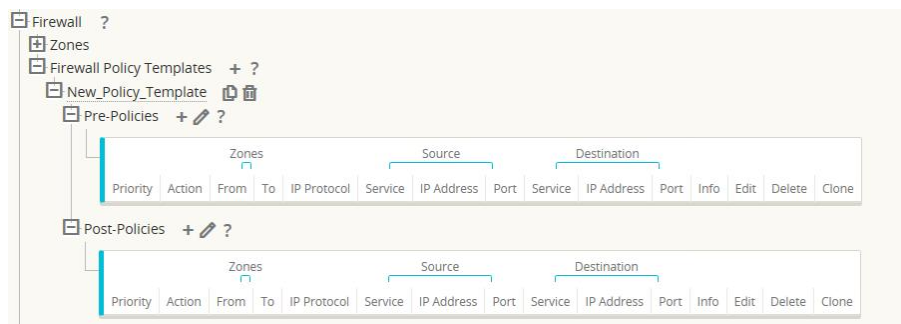
See the Filter Policy Evaluation Order below for specific information on how the system processes these policies.

Filter Policy Evaluation Order

1. Pre-Templates – compiled policies from all template “PRE” sections.
2. Pre-Global – compiled policies from Global “PRE” section.
3. Local – appliance-level policies.
4. Local Auto Generated – automatically local generated policies.
5. Post-Templates – compiled policies from all template “POST” sections.
6. Post-Global – compiled policies from Global “POST” section.

Policy definitions - Global and Local (site)

The user will configure Pre-Appliance and Post-Appliance Template Policies at a global level. Local policies are applied at the site level of an appliance.



The above figure shows the policy template that would apply to the APN globally. To apply a template to all sites in the APN, navigate to **APN Settings > Global Policy Template** and select a specific policy. At the site level, the user can add more policy templates, as well as create site specific policies.



The specific configurable attributes for a policy are displayed in Figure 8. These are the same for all policies.

Note:

Ports configured for Oracle SD-WAN Reliable Protocol (UDP 2156, or a user-defined TRP port) are automatically permitted to prevent user-configurable policies from blocking a Conduit from establishing.

Add Firewall Policy ? x

Priority:

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Interent2-Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Interent2-Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>

Action: Log Interval (s): Log Start Log End Track:

IP Protocol: DSCP: Allow Fragments Reverse Also

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

Policy Attributes

- **Priority** – order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.
- **Zone** – flows have a source zone and destination zone.
- **From Zone** – source zone for the policy.
- **To Zone** – destination zone for a policy.
- **Action** – action to perform on a matched flow.
- **Allow** – permit the flow through the Firewall.
- **Drop** – deny the flow through the firewall by dropping the packets.
- **Reject** – deny the flow through the firewall and send a protocol specific response. TCP will send a reset, ICMP will send a redirect.
- **Count and Continue** – count the number of packets and bytes for this flow, then continue down the policy list.
- **Log Interval** – time in seconds between logging the number of packets matching the policy to a syslog server.
- **Log Start** – selected when a log file is created for new flow.
- **Log End** – log the data for a flow when the flow is deleted.
- **Note:** The default Log Interval value of 0 means no logging.
- **Track** – allows the firewall to track the state of a flow and display this information in the **Monitor > Firewall > Connections** table. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under **Firewall > Settings > Advanced > Default Tracking**.
- **No Track** – flow state is not enabled.

- **Track** – displays the current state of the flow (which matched this policy).
- **IP Protocol** – define an IP protocol. Options include ANY, TCP, UDP or ICMP.
- **DSCP** – allow the user to match on a DSCP tag setting.
- **Allow Fragments** – allow IP fragments that match this filter policy.
- **Note:** The firewall does not reassemble fragmented frames.
- **Source Service Type** – in reference to a Oracle SD-WAN service – Local (to the appliance), Conduit, Intranet, IPhost, or Internet are examples of Service Types.
- **IPhost Option** - This is a new service type for the Firewall and is used for packets that are generated by the Oracle SD-WAN application. For example, running a ping from the Web UI of the Oracle SD-WAN results in a packet sourced from a Oracle SD-WAN Virtual IP address. Creating a policy for this IP address would require the user to select the IPhost option.
- **Note:** Please refer to the Dynamic NAT – LAN to Untrusted Internet use case as an example.
- **Source Service Name** – name of a service tied to the service type. For example, if Conduit is selected for Source Service type, this would be the name of the specific Conduit. This is not always required and depends on the service type selected.
- **Source IP address** – typical IP address and subnet mask the filter will use to match.
- **Source Port** – source port the specific application will use.
- **Destination Service Type** - in reference to a Oracle SD-WAN service – Local (to the appliance), Conduit, Intranet, IPhost, or Internet are examples of service types.

 **Note:**

See above for definition of IPhost service type.

- **Destination Service Name** - name of a service tied to the service type. This is not always required and depends on the service type selected.
- **Destination IP Address** - typical IP address and subnet mask the filter will use to match.
- **Destination Port** – destination port the specific application will use (i.e. HTTP destination port 80 for the TCP protocol).
- The track option provides much more detail about a flow. The state information tracked in the state tables is included below.

State Table for The Track Option

There are only a few states that are consistent:

- INIT: connection created, but the initial packet was invalid.
- O_DENIED: packets that created the connection are denied by a filter policy.
- R_DENIED: packets from the responder are denied by a filter policy.
- NOT_TRACKED: the connection is not statefully tracked but is otherwise allowed.
- CLOSED: the connection has timed out or otherwise been closed by the protocol.
- DELETED: the connection is in the process of being removed.

- The DELETED state will almost never be seen.

All other states are protocol specific and require stateful tracking be enabled.

TCP can report the following states:

- SYN_SENT: first TCP SYN message seen.
- SYN_SENT2: SYN message seen in both directions, no SYN+ACK (AKA simultaneous open).
- SYN_ACK_RDVD: SYN+ACK received.
- ESTABLISHED: second ACK received, connection is fully established.
- FIN_WAIT: first FIN message seen.
- CLOSE_WAIT: FIN message seen in both directions.
- TIME_WAIT: last ACK seen in both directions. Connection is now closed waiting for reopen.

All other IP protocols (notably ICMP and UDP) have the following states:

- NEW: packets seen in one direction.
- ESTABLISHED: packets seen in both directions.

Network Address Translation (NAT)

The Oracle SD-WAN firewall allows the user to configure static NAT and dynamic NAT for different use cases. The following configurations are supported for NAT:

- Static one-to-one NAT
- Dynamic NAT (PAT- Port Address Translation)
- Dynamic NAT with Port Forwarding rules

Note:

At this time, the NAT capability can only be configured at the site level; there is no global configuration (templates) for NAT. All NAT policies are defined from a Source-NAT (SNAT) translation perspective. Corresponding Destination-NAT (DNAT) rules are created automatically for the user.

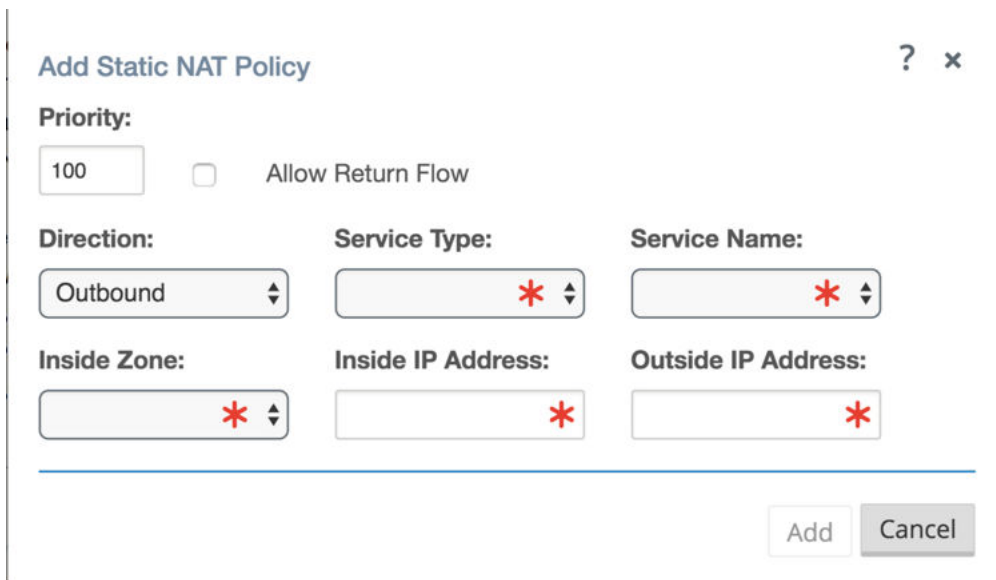
Basic configuration of each type will be defined below so the user has an idea of what is required to enable a static or dynamic NAT capability. Specific examples of the use cases for NAT are provided later in this document.

Static NAT Configuration Options

Static NAT allows the user to configure one-to-one NAT, where an inside IP address will match a public IP address. The configuration options are shown in Figure 9. The user must also define the filter policies to allow traffic back in for the static NAT configuration.

 **Note:**

Beginning in APN 7.2 P4, users have the option to enable the “Allow Return Flow” option to allow inbound connections as well as outbound connections without defining a second filter policy. Additional policies may still be required in some scenarios.



Add Static NAT Policy ? x

Priority:
 Allow Return Flow

Direction: **Service Type:** **Service Name:**

Inside Zone: **Inside IP Address:** **Outside IP Address:**

Figure 9

- **Priority** - the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.
- **Direction** – the direction, from the perspective of the virtual interface or service, that the translation will operate.
- **Outbound** – the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.
Example: LAN service to Internet service – for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.
- **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.
Example: Internet service to LAN service – For packets received on the Internet service, the source IP address is translated. For packets transmitted on the Internet service, the destination IP address is translated.
- **Service Type** – in reference to a Oracle SD-WAN service. For static NAT, these include Local (to the appliance), Intranet, and Internet.
- **Service Name** – specific service name that corresponds to the defined Service Type above.
- **Inside Zone** – one of the existing inside zones configured on the appliance.
- **Inside IP address** – source IP address and mask of the direction selected above.
- **Outside IP address** – the outside IP address and mask of packets that are translated to.

Dynamic NAT Configuration Options

Dynamic NAT is used when the user would want to forward traffic from a LAN segment to the Internet on an untrusted port. In this case, the user would configure the NAT in an outbound direction, as well as make sure the corresponding filter policies are defined to allow traffic back in. By default, once the dynamic NAT has been configured the system will add in two filter policies. These policies will:

- allow Any IPhost route, Any zone, Any source and destination.
- drop all other traffic from the source zone to the destination zone (zone specific).

Figure 10 provides the configuration options for the dynamic NAT configuration.

Figure 10

- **Priority** – the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority policies.
- **Direction** – the direction from the virtual interface or service perspective the translation will operate.
- **Outbound** – the destination address for a packet will be translated for packets received on the service. The source address will be translated for packets transmitted on the service.
Example: LAN service to Internet service – for packets outbound, (LAN to Internet) the source IP address is translated. For packets inbound or received (Internet to LAN) the destination IP address are translated.
- **Inbound** - the source address for a packet will be translated for packets received on the service. The destination address will be translated for packets transmitted on the service.
Example: Internet service to LAN service – for packets received on the Internet service the source IP address is translated. For packets transmitted on the Internet service, the destination IP address is translated.
- **Type** – the type of dynamic NAT to perform.
- **Port-Restrictive** - Port-Restricted NAT is what most consumer grade gateway routers use. Inbound connections are generally disallowed unless a port is specifically forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port (this is known as endpoint independent mapping). This requirement limits a Port-Restricted NAT firewall to 65535 simultaneous sessions, but facilitates an often used internet technology known as hole punching.
- **Symmetric** – Symmetric NAT is sometimes known as enterprise NAT because it allows for a much larger NAT space and enhances security by making translations less predictable. Inbound connections are generally disallowed unless a port is specifically

forwarded to an inside address. Outbound connections allow return traffic from the same remote IP and port. Connections from the same inside IP and port need to map to the same outside IP and port (this is known as endpoint dependent mapping). This mode explicitly prevents hole punching.

- **Service Type** – in reference to a Oracle SD-WAN service. For static NAT these include Local (to the appliance), Intranet, Internet.
- **Service Name** – the specific service name that corresponds to the defined Service Type above.
- **Inside Zone** – select the inside zone for the packets that require NAT.
- **Inside IP address** - define an IP host address or a subnet based on traffic that requires NAT. This should be an IP address that resides in the Inside Zone.
- **Allow Related** – allow traffic related to the flow matching the rule. For example, ICMP redirection related to the specific flow that matched the policy, if there was some type of error related to the flow.
- **IPsec Passthrough** – allow IPsec traffic to passthrough unchanged.
- **GRE/PPTP Passthrough** – allow GRE or IPsec to passthrough unchanged.

Dynamic NAT with Port Forwarding Configuration Options

Dynamic NAT with port forwarding allows the user to port forward specific traffic to a defined IP address. This is typically used for inside hosts like web servers. Once the dynamic NAT is configured the user would define the port forwarding policy. From the example in Figure 11, we can see that dynamic NAT is configured for a specific IP host address. The NAT example will map an inside IP host to an outside IP host. Port forwarding can then be configured which will define a specific inside and outside port mapped to an inside IP address. In this example, HTTP port 80 is defined for port forwarding.

Add Dynamic NAT Policy ? x

Priority:

Direction: Type: Service Type: Service Name:

Inside Zone: Inside IP Address: Outside IP Address:

Allow Related IPsec Passthrough GRE/PPTP Passthrough

Port Forwarding Rules +

Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Track	Delete
<input type="text" value="Both"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Use Site Setting"/>	<input type="text"/>
<input type="text" value="TCP"/>	<input type="text" value="80"/>	<input type="text" value="10.3.2.20"/>	<input type="text" value="80"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Track"/>	<input type="text"/>

- **Protocol** – TCP, UDP, or both.
- **Outside Port** – outside port the user will port forward into the inside address.
- **Inside IP address** – inside address to forward matching packets.
- **Inside Port** – map the packet to the same, or a different, inside port.
- **Fragments** – allow the forwarding of fragmented packets.

- **Log Interval** – time in second between logging the number of packets matching the policy to a syslog server.
- **Log Start** – selected when a log file is created for new flow.
- **Log End** – log the data for a flow when the flow is deleted.

 **Note:**

The default Log Interval value of 0 means no logging.

- **Track** – allows the firewall to track the state of a flow and display this information in the **Monitor > Firewall > Connections** table. If the flow is not tracked, the state will show NOT_TRACKED. See the table for the state tracking based on protocol below. Use the setting defined at the site level under **Firewall > Settings > Advanced > Default Tracking**.
- **No Track** – flow state is not enabled.
- **Track** – displays the current state of the flow (which matched this policy).

Filter Policies

When filtering using zones, traffic that is using a Conduit route that was manually configured in the **Routes** section does not know the **To Zone** until the traffic arrives at the remote site. Filter Policies for this traffic must be configured at the remote site.

When filtering using zones, traffic from a private VIP may only be filtered at the local site using the zone for the private VIP. Similarly, if the source IP address for a packet is translated using NAT, the original **Inside Zone** can only be filtered locally. Remote appliances must use the **Outside Zone**.

Static & Dynamic NAT Policies

NAT translations are not permitted if the Inside and Outside Zones are the same.

While both inbound and outbound translations can be configured simultaneously for a service, only the first to match will be used. Multiple translations may occur if a rule exists on the service a packet is received on and the service a packet is sent on.

Note: Dynamic NAT translations allow all reciprocal traffic for sessions initiated from the inside network. To filter these connections, add filter policies for the outbound traffic. Static NAT translations allow reciprocal traffic for sessions initiated from inside the network only on policies with the “Allow Return Flow” option enabled.

Firewall Use Case Examples

Dynamic NAT – LAN to Untrusted Internet

In this example, the firewall will allow the local users Internet access at a Client site. The Internet access will utilize the firewall to NAT the traffic to the Internet while providing policies to limit or deny any traffic that did not originate from the inside LAN segment. If configured, the Oracle SD-WAN will also now provision the Internet usages on this WAN Link. In the past, this was not possible because an untrusted port would only allow ICMP, ARP, and TRP packets, while all other traffic was blocked. A diagram of the Client site is included in Figure 12.

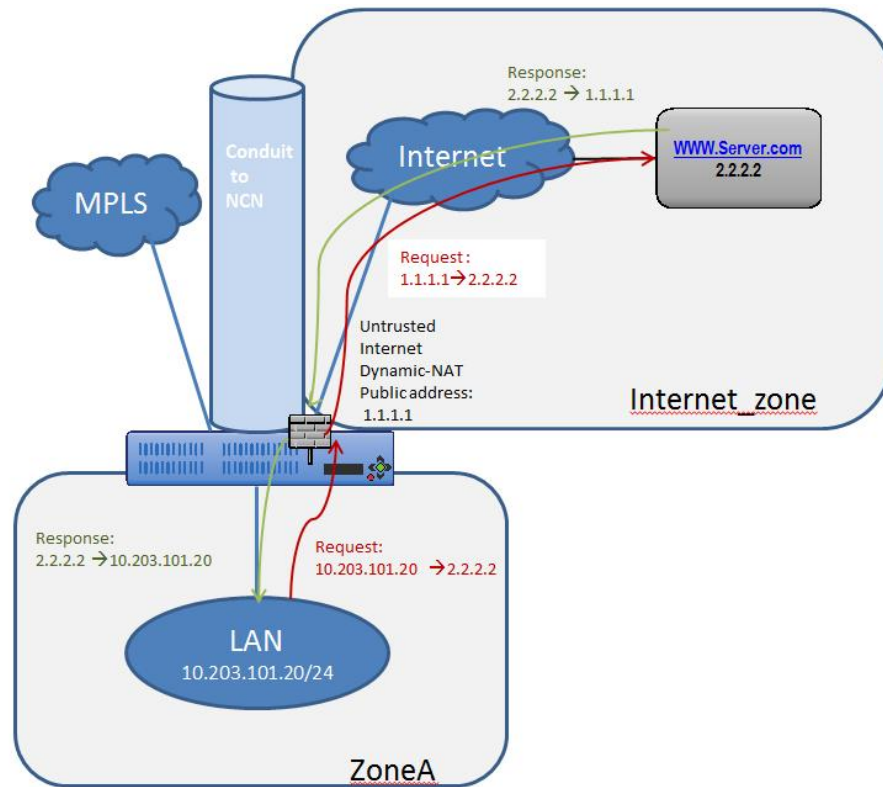


Figure 12

The configuration process to enable this capability is as follows, assuming the Oracle SD-WAN Client site is currently up and operational.

1. Add the Internet service to the site.
 2. Assign it to the WAN Link (even though the WAN Link is untrusted).
 3. Define the dynamic NAT policies (PAT rule).
 4. The system will add policies to allow traffic in and out for this NAT statement.
 5. Save the configuration and Export it to **Change Management**.
- Steps 1 & 2 - Adding the Internet service and assigning it to a WAN Link.

CL-T860

- WAN-to-WAN Forwarding
- Conduits
- Internet Services + ?
 - Internet ?
 - Basic Settings
 - WAN Links ?

WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Failover	WAN Ingress		WAN Egress		
					Tagging	Max Delay (ms)	Tagging	Matching	Grooming
CL2-WL1-MPLS	<input type="checkbox"/>	Primary	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>
CL2-WL2-INET	<input checked="" type="checkbox"/>	Primary	0	<input checked="" type="checkbox"/>	None	500	None	None	<input checked="" type="checkbox"/>

Figure 13

The Internet service was added to the site with service name “Internet”. Once added, the service was applied to WAN Link “CL2-WL2-INET”. By default, the bandwidth allocated to the new Internet service is 1000 shares. If more bandwidth is required, the user should review the

Provisioning section in the Configuration Editor under **Provisioning > [Site Name] > WAN Links > CL2-WL2-INET > Services > Internet**.

Once the Internet service has been added and assigned to a WAN Link, the user can then configure the dynamic NAT function. Since this use case only requires dynamic NAT, there are no global policies to apply. All required policies can be added locally to the site. Figure 14 provides a screen capture of how the user should configure the dynamic NAT capability.

Navigate to **Connections > [Site Name] > Firewall > Dynamic NAT Policies > Add**.

Figure 14

Define the dynamic NAT policies (PAT rule):

1. Direction: Outbound
2. Type: Symmetric (Firewall can change the source port)
3. Service Type: Internet
4. Service Name: Internet
5. Inside Zone: Default_LAN_Zone
6. Inside IP address: * (default)
7. Outside zone: Internet_Zone (because of defined service type this is known)

The completed Dynamic NAT Policy will be displayed as follows:

Priority	Direction	Type	Service	Inside Zone	Inside IP Address	Outside Zone	Outside IP Address	Port Forwards	Edit	Delete	Clone
100	Outbound	Symmetric	Internet	Default_LAN_Zone	*	Internet_Zone		0			

Figure 15

In addition to the NAT policy, the system will add two default policies. The first policy allows traffic outbound from a Oracle SD-WAN Virtual IP address (IP Host) and the NAT process. The second rule will deny all other inbound traffic from the Internet_Zone . System added rules are marked with a priority of (auto) and the user can add policies with a higher priority if necessary.

Note: The rule that allows this traffic outbound is the default rule defined at the global level to Allow all firewall traffic. If the default policy is set to **Drop**, the user must add a more specific policy that allows all LAN traffic outbound to the Internet.

Pre-Appliance Template Policies														?			
Local Policies														+	Add	?	
Priority	Action	Zones		IP Protocol	DSCP	Service	Source			Destination			Reverse Also	Info	Edit	Delete	Clone
		From	To				IP Address	Port	Service	IP Address	Port						
(auto)	Allow	*	*	Any	*	IP Host	*	*	*	*	*	*					
(auto)	Drop	*	*	Any	*	Internet	*	*	*	*	*	*					
Post-Appliance Template Policies														?			

Figure 16

Once the configuration is complete, the user will Export the configuration to **Change Management** to apply the changes.

Policies Between Zones

In this example, the firewall will allow traffic only to the same zone as it originated (Zone_A > Zone_A). Traffic destined to a different zone will be blocked (Zone_A > Zone_B). The filtering affects both APN (WAN) as well as appliance-local traffic (L3 interface to L3 interface). A topology diagram is included in Figure 17.

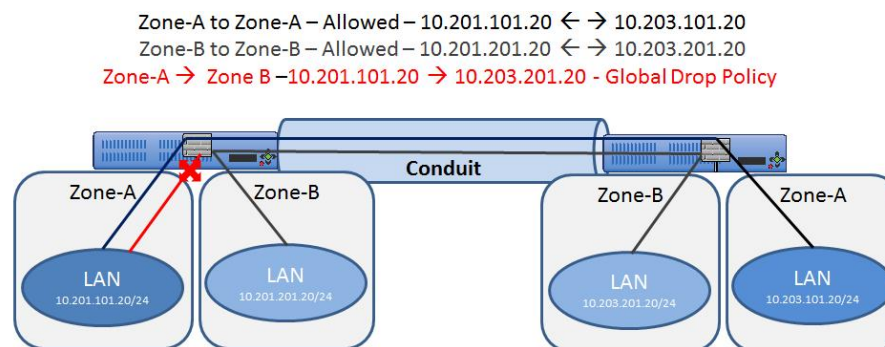


Figure 17

The configuration process to enable this capability is as follows, assuming the Oracle SD-WAN Client site is currently up and operational.

1. Create and assign zones (Zone_A & Zone_B) to interfaces.
2. Create filter-policy template to:
 - a. Permit Zone_A > Zone_A traffic.
 - b. Permit Zone_B > Zone_B traffic.
3. Assign filter-policy template to sites.
4. Configure default global behavior as drop.
5. Save the configuration and Export to **Change Management**.

Note: Step 4 may also be done locally if required.

Step 1- Create and assign zones (Zone_A & Zone_B) to interfaces.

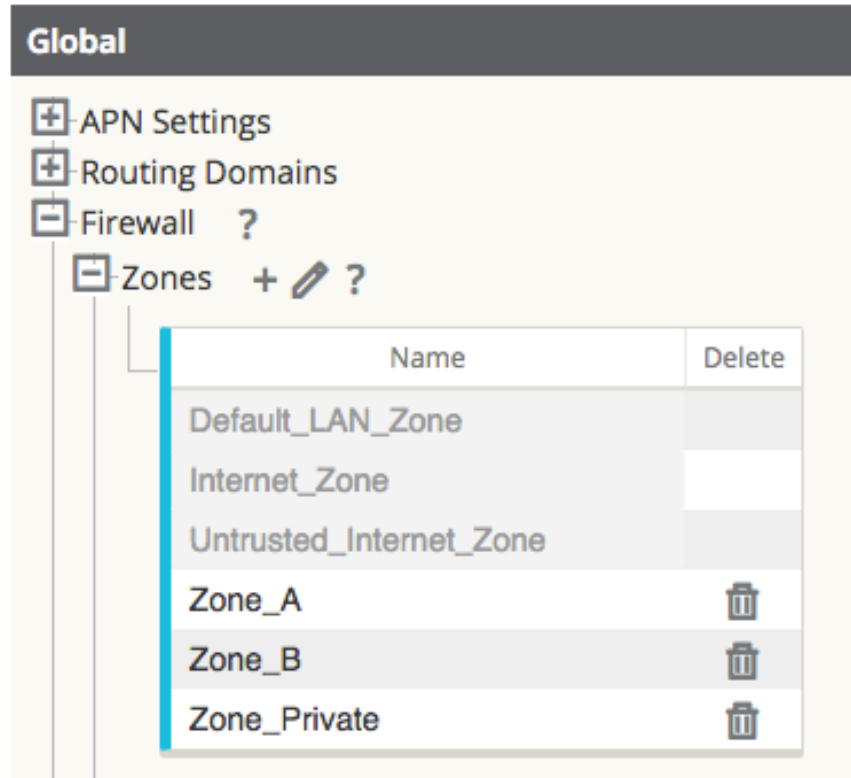


Figure 18

Figure 18 shows how the zone is added at the global level. Once the zone is created, it must be assigned to a logical interface within the Oracle SD-WAN Appliance.

Figure 19 provides an example of how the user assigns the zone to a VNI. Under **Site > [Site Name] > Interface Groups > Virtual Interface** the user can select an interface or interface pair, then assign a zone.

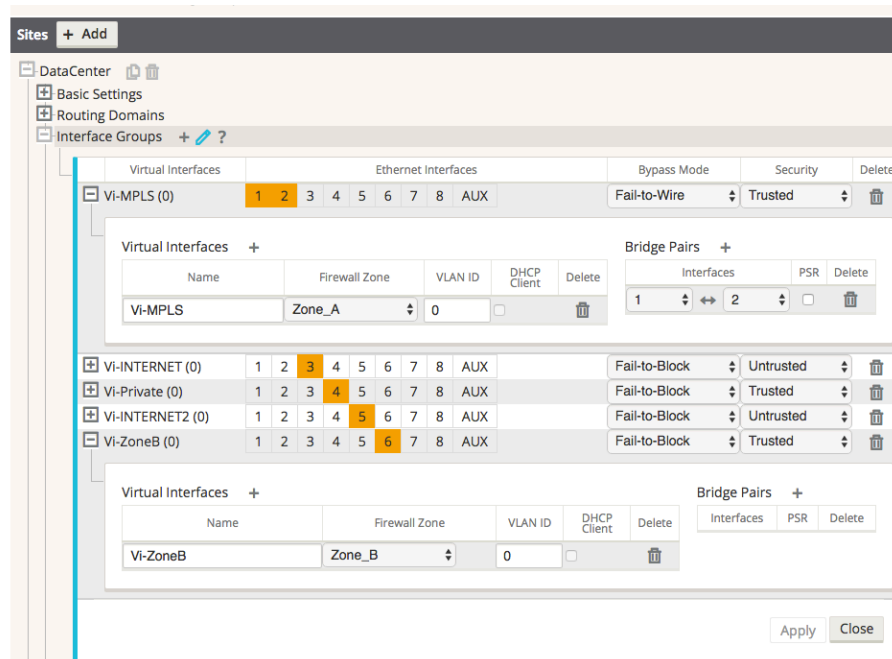


Figure 19

Step 2 - Create a filter-policy template to:

1. Permit Zone_A > Zone_A traffic.
2. Permit Zone_B > Zone_B traffic.

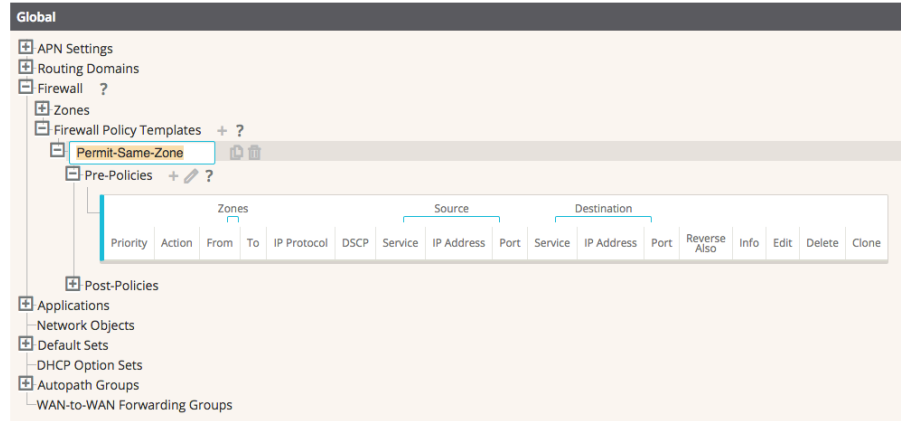


Figure 20

Note:

This template can then be applied to all appliances in the APN, if required.

Figure 21 shows the user how to configure Zone_A (source) and Zone B (destination). In this example, all other policy options are set to the Any or the * option, with more selective security options available if required.

Add Firewall Policy ? x

Priority:

From Zones

- Internet_Zone
- Untrusted_Internet_Zone
- Zone_A
- Zone_B
- Zone_Private

To Zones

- Internet_Zone
- Untrusted_Internet_Zone
- Zone_A
- Zone_B
- Zone_Private

Action: Log Interval (s): Log Start Log End

IP Protocol: DSCP: Allow Fragments Reverse Also

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

Figure 21

Repeat the process for Zone_B policies.

Add Firewall Policy ? x

Priority:

From Zones:

- Internet_Zone
- Untrusted_Internet_Zone
- Zone_A
- Zone_B
- Zone_Private

To Zones:

- Internet_Zone
- Untrusted_Internet_Zone
- Zone_A
- Zone_B
- Zone_Private

Action: Log Interval (s): Log Start Log End Track:

IP Protocol: DSCP: Allow Fragments Reverse Also

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

Figure 22

Once the policies are created to allow zone to zone traffic, they will be displayed as seen below.

Priority	Action	Zones		IP Protocol	DSCP	Source			Destination			Reverse Also	Info	Edit	Delete	Clone
		From	To			Service	IP Address	Port	Service	IP Address	Port					
100	Allow	Zone_A	Zone_A	Any	Any	*	*	*	*	*	*					
200	Allow	Zone_B	Zone_B	Any	Any	*	*	*	*	*	*					

Figure 23

Step 3 - Assign the filter-policy template to sites.

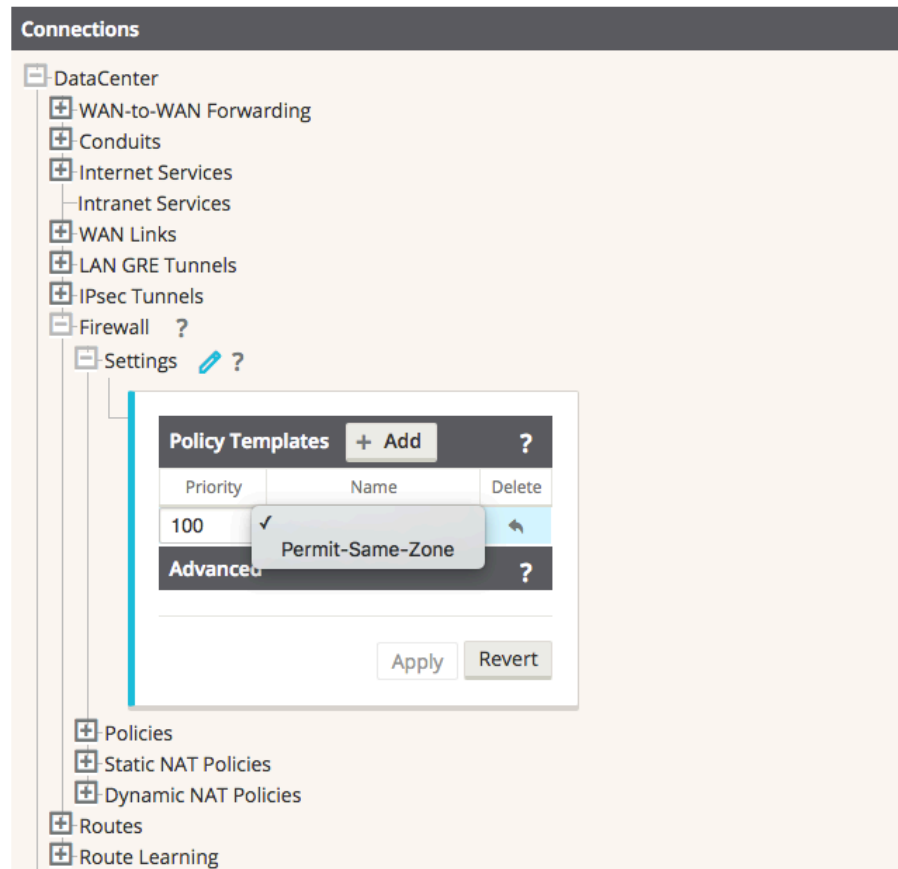


Figure 24

Assigning a Pre-Appliance policy to a site is done under **Connections > [Site Name] > Firewall > Settings > Policy Template > Add**.

Example of the applied Policy Template for NCN and Client Sites:

Connections

- [-] DataCenter
 - [+] WAN-to-WAN Forwarding
 - [+] Conduits
 - [+] Internet Services
 - Intranet Services
 - [+] WAN Links
 - [+] LAN GRE Tunnels
 - [+] IPsec Tunnels
 - [-] Firewall ?
 - [-] Settings ?
- [+] Policies
- [+] Static NAT Policies
- [+] Dynamic NAT Policies
- [+] Routes
- [+] Route Learning
- [+] Client1
- [-] Client2
 - [+] WAN-to-WAN Forwarding
 - [+] Conduits
 - [+] Internet Services
 - Intranet Services
 - [+] WAN Links
 - [+] LAN GRE Tunnels
 - [+] IPsec Tunnels
 - [-] Firewall ?
 - [-] Settings ?

Policy Templates + Add ?

Priority	Name	Delete
100	Permit-Same-Zone	

Advanced ?

Policy Templates + Add ?

Priority	Name	Delete
100	Permit-Same-Zone	

Advanced ?

Figure 25

Step 4 - Configure the default global behavior to Drop.

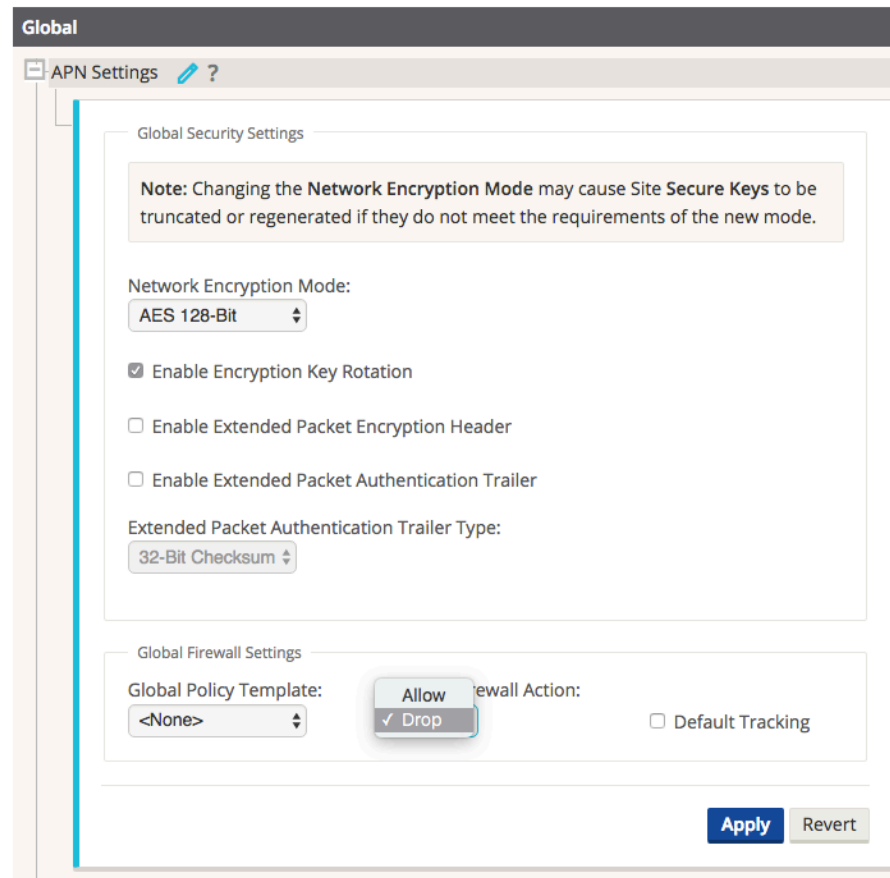


Figure 26

In this example, once the zone to zone policies are defined, the user elects to deny all other traffic. This configuration option is found under the **Global > APN Settings > Firewall Action > Drop**.

Note:

Use this option with caution, as all other traffic will now be dropped.

Once the configuration is complete in the Editor, the user will Export the configuration to **Change Management** to apply the changes.

LAN to Conduit Zone to Zone – Block/Allow Specific Traffic Types

In this example, the firewall will deny a specific sub-set of traffic (TCP with destination port 23) globally. The filtering affects both APN (WAN) as well as appliance-local traffic (L3 interface to L3 interface). A topology diagram is included in Figure 27.

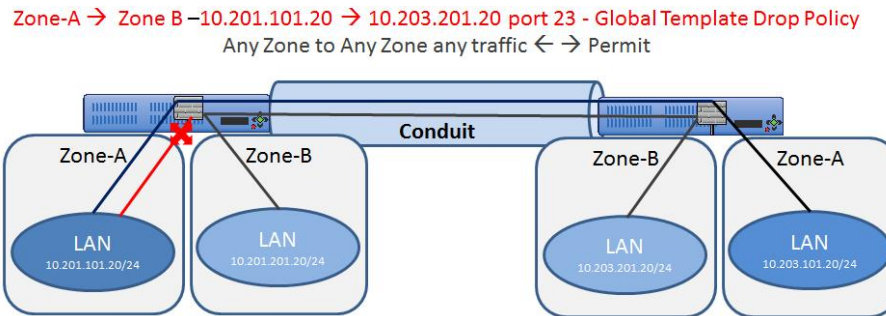


Figure 27

The configuration process to enable this capability is as follows, assuming the Oracle SD-WAN Client site is currently up and operational.

1. Create filter-policy template to deny TCP with destination port 23 traffic.
2. Assign filter-policy template to sites.
3. Save the configuration and Export to **Change Management**.

Step 1 - Create filter-policy template to deny TCP with destination port 23 traffic.

Edit Firewall Policy ? x

Priority:

From Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

To Zones

Zone	Enable
Any	<input checked="" type="checkbox"/>
Default_LAN_Zone	<input type="checkbox"/>
Internet_Zone	<input type="checkbox"/>
Untrusted_Internet_Zone	<input type="checkbox"/>

Action: Log Interval (s): Log Start Log End Track:

IP Protocol: DSCP: Allow Fragments Reverse Also

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

Figure 28

In Figure 28, the user creates a policy to Drop TCP traffic with destination port 23 with a source or destination of any IP address. The user can also select the **Track** option for such flows if complete TCP state monitoring is desired.

The user also has the option to make this policy Pre-Appliance, Post-Appliance, or site specific. The screen shot below displays that the user has chosen to make this policy a Global Pre-Appliance Policy.

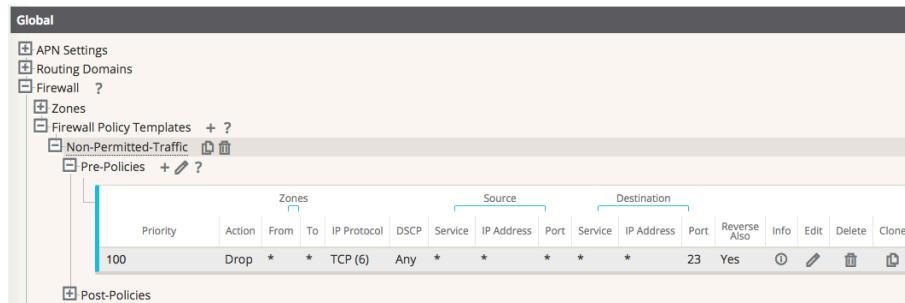


Figure 29

Step 2 - Assign the filter-policy template to sites.

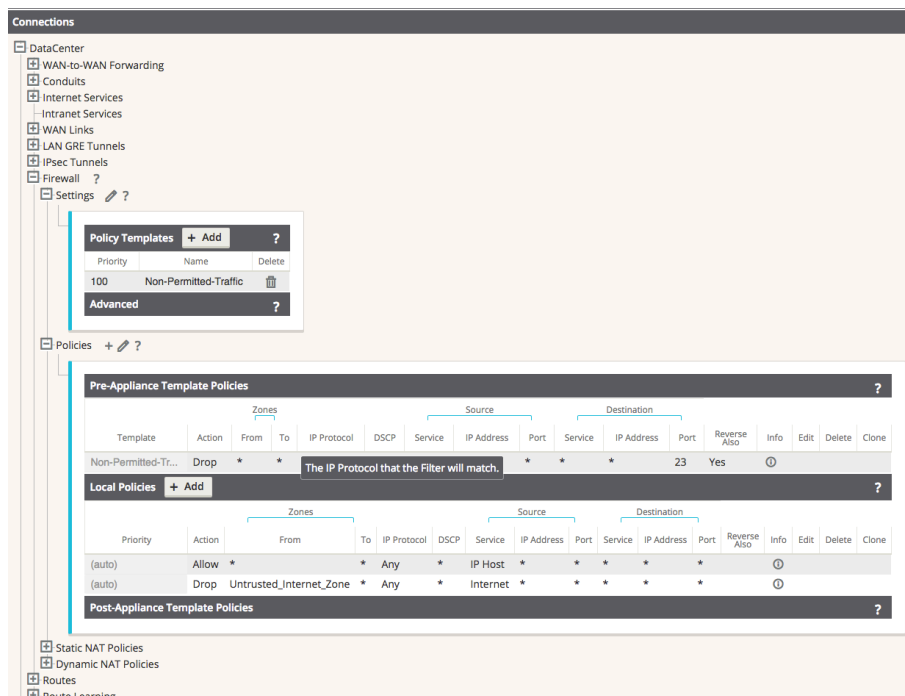


Figure 30

The template can be assigned to a specific site under **Connections > [Site Name] > Firewall > Settings**.

Save the configuration and Export to **Change Management**.

Internet (untrusted) Port Forwarding – DMZ

In this example, the firewall will port forward specific traffic arriving on an outside/untrusted Internet VIP (TCP/8080) to an inside/LAN host (TCP/80). A topology diagram is included in Figure 31.

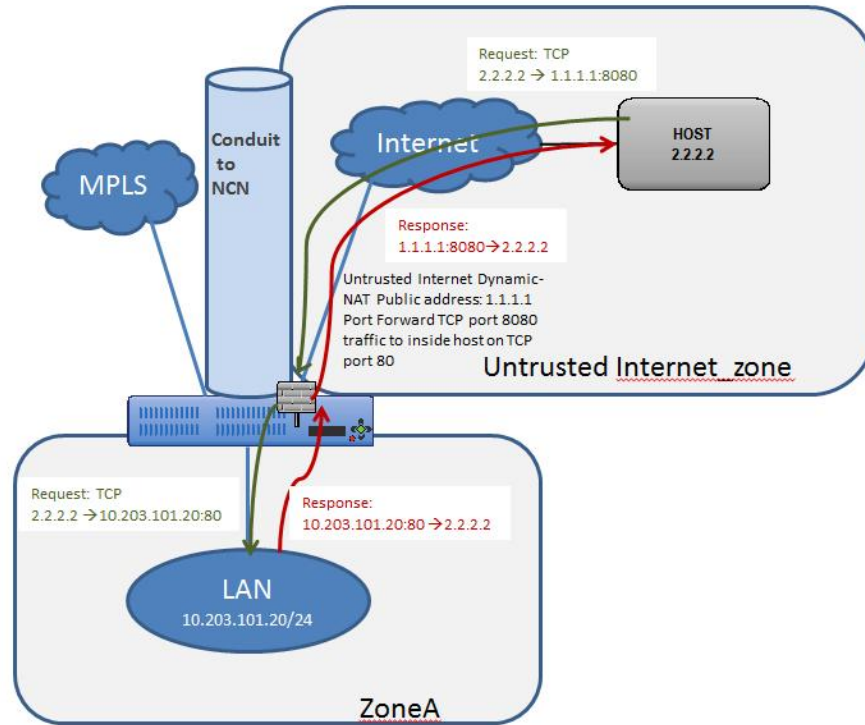


Figure 31

The configuration process to enable this capability is as follows, assuming the Oracle SD-WAN Client site is currently up and operational.

1. Define the dynamic NAT policies (PAT rule).
2. The system will add policies to allow traffic in and out for this NAT statement.
3. Save the configuration and Export to **Change Management**.

Step 1 - Define the dynamic NAT policies (PAT rule) under **Connections > [Site Name] > Firewall > Dynamic NAT Policies**.

1. Direction: Outbound
2. Type: Port-Restricted (Firewall can change the source port)
3. Service: Internet
4. Inside Zone: * (default)
5. Inside IP Address: * (default)
6. Outside Zone: Untrusted_Internet_Zone
7. Outside IP Address: blank
8. Port Forwards: 1
 - a. Outside: TCP/8080, Inside: 10.203.101.20 TCP/80

Edit Dynamic NAT Policy ? x

Priority:

Direction: Type: Service Type: Service Name:

Inside Zone: Inside IP Address:

Allow Related IPsec Passthrough GRE/PPTP Passthrough

Port Forwarding Rules +

Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Track	Delete
TCP	8080	10.203.101.20	80	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Track"/>	<input type="button" value="Delete"/>

Figure 32

When configuring Port Forwarding, the user must define the dynamic NAT (PAT) prior to enabling the specific **Port Forwarding Rules**. Figure 32 displays that dynamic NAT is enabled to the Internet Service Type, then the Port Forwarding Rule may be created. The requirements in this example are to port forward TCP port 8080 traffic inbound for host 10.203.101.20 on TCP port 80. The user will also **Track** the state of this connection.

Step 2 - The system will add policies to allow traffic in and out for this dynamic NAT statement and the Port Forwarding Policy and should be verified by the end user under the **Policies** section.

Connections

- DataCenter
- Client1
- Client2
- WAN-to-WAN Forwarding
- Conduits
- Internet Services
 - Intranet Services
- WAN Links
- LAN GRE Tunnels
- IPsec Tunnels
- Firewall ?
- Settings
- Policies + ?

Pre-Appliance Template Policies													?				
Local Policies + Add													?				
Priority	Action	Zones		IP Protocol	DSCP	Source			Destination			Reverse Also	Info	Edit	Delete	Clone	
		From	To			Service	IP Address	Port	Service	IP Address	Port						
(auto)	Allow	*	*	Any	*	IP Host	*	*	*	*	*	*					
(auto)	Allow	Untrusted_Internet_Zone	*	TCP (6)	*	Internet	*	0-65535	*	10.203.101.20	80						
(auto)	Drop	Untrusted_Internet_Zone	*	Any	*	Internet	*	*	*	*	*						
Post-Appliance Template Policies													?				

Figure 33

Figure 33 shows the rules automatically generated by the system. These rules will allow dynamic NAT to the Internet from an inside host, as well as to port forward any traffic from the Internet to that specific host on TCP port 80. This simplifies the configuration process for the end user.

Save the configuration and Export to **Change Management**.

Static One-to-One NAT - Internet to LAN/DMZ Host

In this example, the firewall will use static NAT for traffic from an outside host to a host residing on the LAN or DMZ segment. This is a one-to-one NAT so all traffic for the 1.1.1.1 destination address will NAT to the inside address of 10.203.101.20. The reverse NAT rule for traffic outbound is implied. All IP protocols (TCP, UDP, GRE etc.) are forwarded.

Note: The mask used in this example allows users to map to a specific inside host address.
A topology diagram is included in Figure 34.

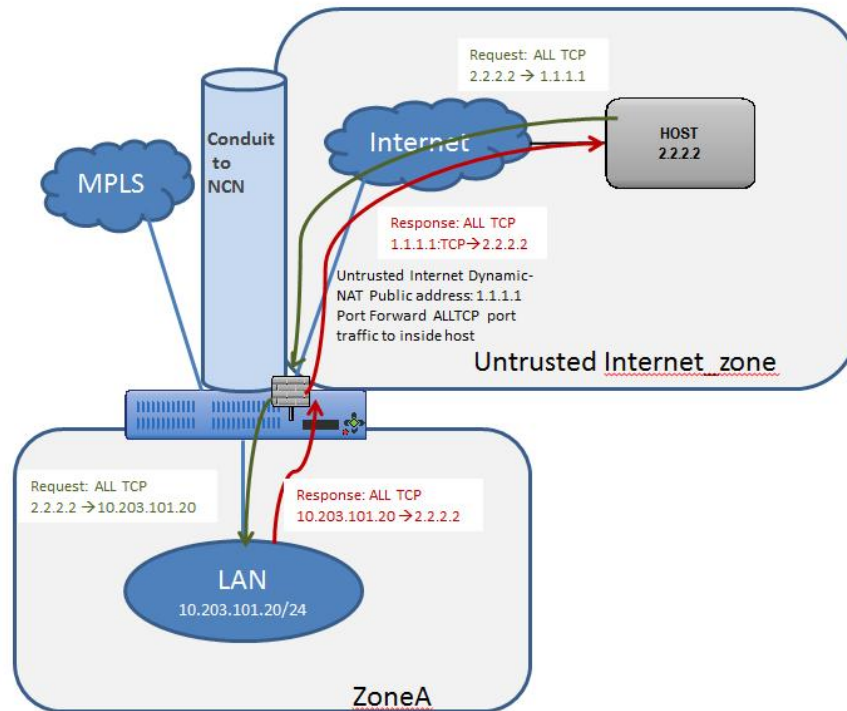


Figure 34

The configuration process to enable this capability is as follows, assuming the Oracle SD-WAN Client site is currently up and operational.

1. Define the static NAT policies (one-to-one rule).
2. Create filter policy to permit Untrusted_Internet_Zone traffic inbound.
3. Save the configuration and Export to **Change Management**.

Step 1 - Define the static NAT policies (one-to-one rule):

1. Direction: Outbound
2. Service: Internet
3. Inside Zone: Zone_A
4. Inside IP Address: 10.203.101.20/32
5. Outside Zone: Untrusted_Internet_Zone
6. Outside IP Address: 1.1.1.1/32

Add Static NAT Policy ? x

Priority:

Direction: Service Type: Service Name:

Inside Zone: Inside IP Address: Outside IP Address:

Figure 35

Users will navigate to **Connections > [Site Name] > Firewall > Static NAT Policies** to add a new policy. The figure above shows the options available to the user. Enabling the static NAT does not apply any automatic policies so the user must configure specific policies to allow or drop traffic. In the above policy, outside IP address 1.1.1.1 maps to inside IP address 10.203.101.20.

Step 2 - Create the filter policy to permit Untrusted_Internet_Zone traffic inbound.

Add Firewall Policy ? x

Priority:

From Zones: Any, Default_LAN_Zone, Internet_Zone, Untrusted_Internet_Zone (checked), Zone_A, Zone_B

To Zones: Default_LAN_Zone, Internet_Zone, Untrusted_Internet_Zone, Zone_A (checked), Zone_B, Zone_Private

Action: Log Interval (s): Log Start Log End

IP Protocol: DSCP: Allow Fragments Reverse Also

Source Service Type: Source Service Name: Source IP: Source Port:

Dest Service Type: Dest Service Name: Dest IP: Dest Port:

Figure 37

To configure traffic policies, the user must understand what traffic is going to be allowed or dropped. Figure 37 shows a sample policy allowing any traffic from the Untrusted_Internet_Zone (a pre-defined zone on the Oracle SD-WAN Appliance) to inside Zone_A (which is manually user-defined). The policy allows any IP protocol, with any source IP address and port through to the inside host address. The user may define more specific policies as required.

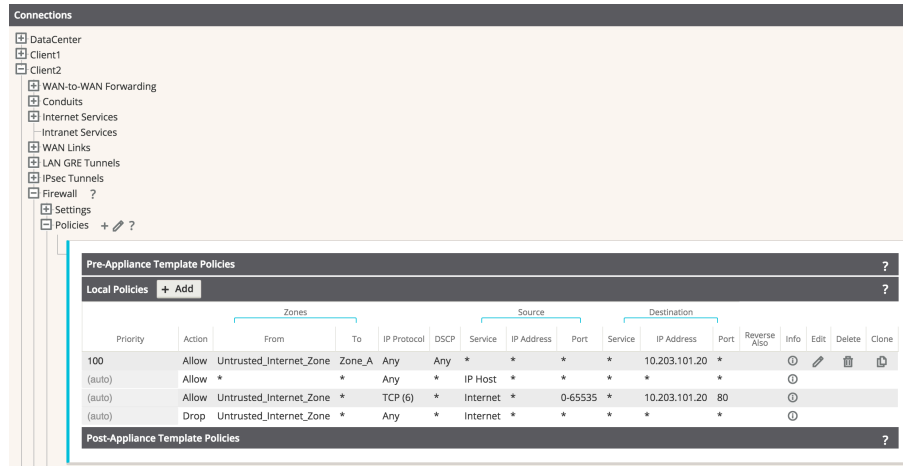


Figure 38

Once the policies are defined to allow the traffic, the user should expand the configuration out to review them and verify, as shown above.

Save the configuration and Export to **Change Management**.

Private LAN (VNI-NAT) into Conduit APN and Internet

In this example, the firewall will employ two separate NAT operations, an inbound static NAT and an outbound dynamic NAT (PAT). The reason for the inbound static NAT is the source network (192.168.0.0/24) is a non-unique network and exists at every network location; 192.168.0.0/24 will NAT to an APN-unique network to allow for overlap translation. The outbound dynamic NAT (PAT) is the standard for LAN to Internet traffic. A topology diagram is included in Figure 39.

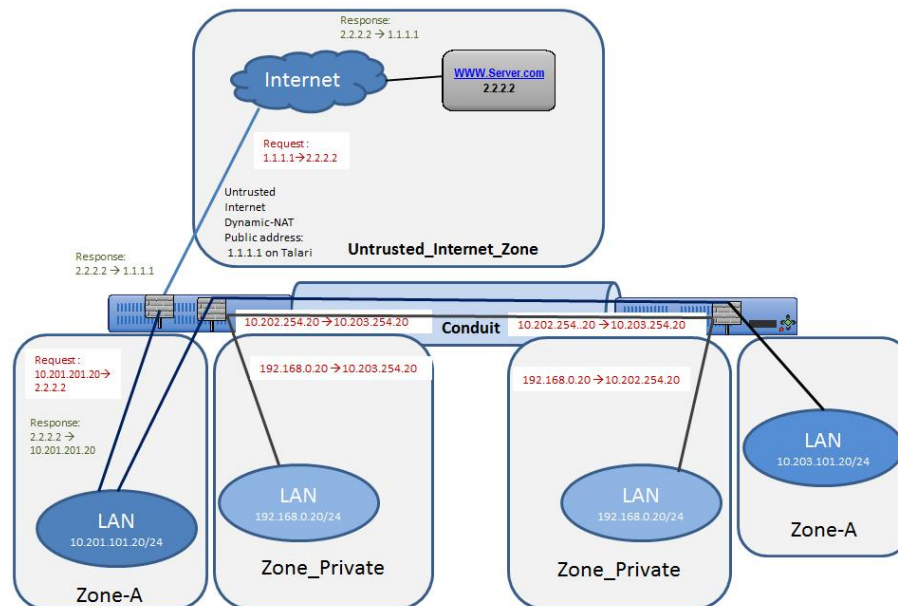


Figure 39

The configuration process to enable this capability is as follows, assuming the Oracle SD-WAN Client site is currently up and operational.

1. Set Private Zone interfaces as Private under VIP configuration.
2. Define the static NAT Policy (one-to-one) – Branch Office 1.
3. Define the static NAT Policy (one-to-one) – Branch Office 2.
4. Define the dynamic NAT Policy (PAT) – Both Offices.
5. Save the configuration and Export to **Change Management**.

Step 1 - Set Private Zone interfaces as Private by selecting the checkbox under VIP configuration and define local subnet 192.168.0.0/24. This route will have local significance only and is not advertised within the APN routing table.

The screenshot shows the 'Sites' configuration page with a '+ Add' button. It displays a tree view of configuration elements for 'DataCenter', including 'Client1' and 'Client3'. Under 'Client1', the 'Virtual IP Addresses' section is expanded, showing a table with the following data:

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
1.1.1.1/24	Vi-INTERNET	Untrusted_Internet_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Untrusted	
10.202.1.1/24	Vi-MPLS	Zone_A	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	
192.168.0.1/24	Vi-Private	Zone_Private	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Trusted	

Below this table, there are expandable sections for DHCP, WAN Links, Certificates, and High Availability. The same structure is repeated for 'Client3', with its 'Virtual IP Addresses' table containing:

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
1.1.3.1/24	Vi-INTERNET	Untrusted_Internet_Zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Untrusted	
10.204.1.1/24	Vi-MPLS	Zone_A	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted	

Figure 40

Step 2 - Define the static NAT Policy (one-to-one) – Branch Office 1.

1. Direction: Inbound
2. Service: Local
3. Inside Zone: Zone_Private
4. Inside IP Address: 192.168.0.0/24
5. Outside Zone: Zone_A
6. Outside IP Address: 10.202.254.0/24

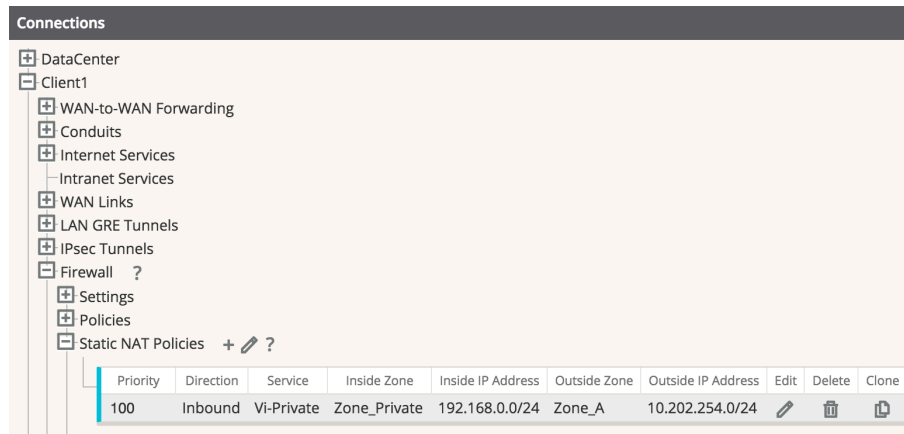


Figure 41

The user may add Static NAT Policies, but this will apply to the subnet. Host addresses within the subnet will match, for example, 192.168.0.20 will map to 10.202.254.20. The Service type selected is a local service called “Vi-Private” that corresponds to the private address space selected as Zone_Private. The above policy is an inbound statement stating that any LAN traffic from the private address space will NAT to the inside address space, and is then routed across the APN.

Repeat the process for Branch Office 2. Once Branch Office 2 is complete, the NAT for the private address space is complete. Next, the user will configure the dynamic NAT to the Internet.

Step 3 - Define the static NAT Policy (one-to-one) – Branch Office 2.

1. Direction: Inbound
2. Service: Local
3. Inside Zone: Zone_Private
4. Inside IP Address: 192.168.0.0/24
5. Outside Zone: Zone_A
6. Outside IP Address: 10.203.254.0/24

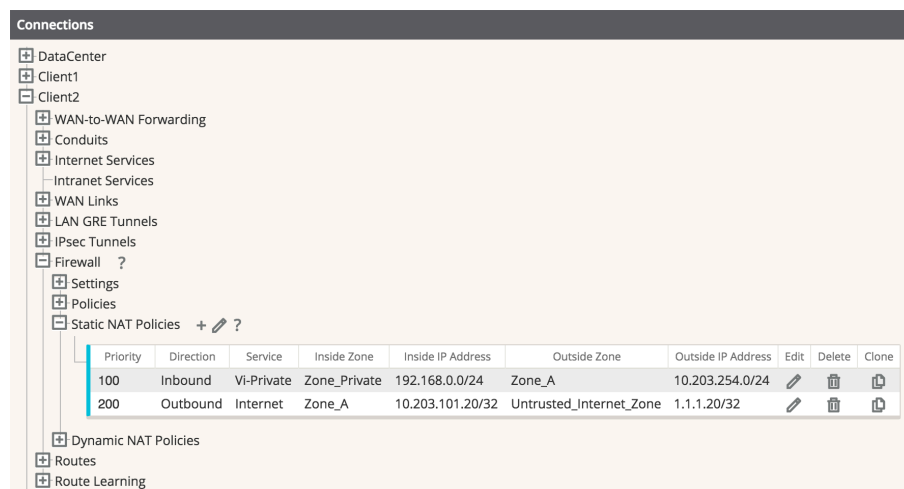
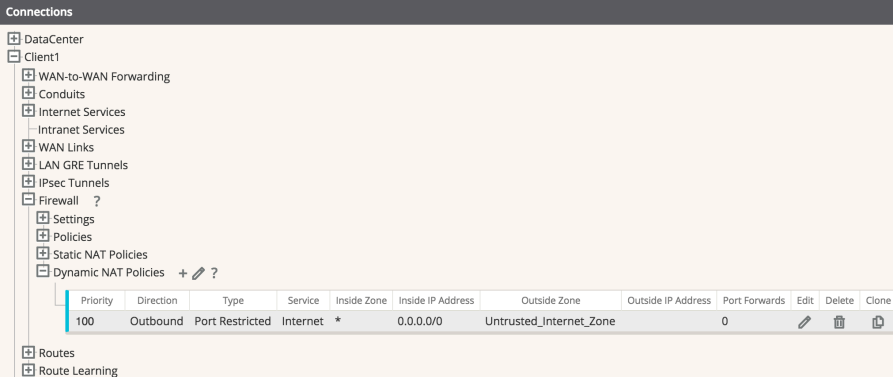


Figure 42

Step 4 - Define the dynamic NAT Policy (PAT) – Both Offices.

1. Direction: Outbound
2. Type: Port-Restricted (FW can change the source port)
3. Service: Internet
4. Inside Zone: * (default)
5. Inside IP Address: * (default)
6. Outside Zone: Untrusted_Internet_Zone
7. Outside IP Address: blank
8. Port Forwards: 0



The screenshot shows the 'Connections' configuration page in the Oracle SD-WAN management console. The left sidebar contains a tree view with categories like DataCenter, Client1, WAN-to-WAN Forwarding, Conduits, Internet Services, Intranet Services, WAN Links, LAN GRE Tunnels, IPsec Tunnels, Firewall, Settings, Policies, Static NAT Policies, and Dynamic NAT Policies. The 'Dynamic NAT Policies' section is expanded, showing a table with one policy configured.

Priority	Direction	Type	Service	Inside Zone	Inside IP Address	Outside Zone	Outside IP Address	Port Forwards	Edit	Delete	Clone
100	Outbound	Port Restricted	Internet	*	0.0.0.0/0	Untrusted_Internet_Zone		0			

Figure 43

Note:

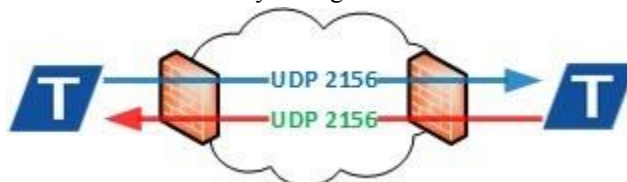
Figure 43 only represents one office, and does not show both.

The final step is to configure the dynamic NAT for Internet access. This is accomplished by selecting the inside zone to be any (or *) zone and the outside zone to be the Untrusted_Internet_Zone, as was configured in the first example. Since the inside zone and IP address space are both set to any, all local users will NAT to the Internet, including the private address space which NATs to the local inside address space.

Save the configuration and Export to **Change Management**.

Firewall Configuration

In a Oracle SD-WAN WAN, a WAN Path is a logical, one-way, UDP encapsulated flow of data between two Oracle SD-WAN Appliances and a constituent part of a Conduit. Conduits use Oracle SD-WAN Reliable Protocol (TRP) on UDP Port 2156 by default, but the UDP Port number can be manually configured for each Conduit.



UDP Port Mapping and Forwarding

When a Oracle SD-WAN Appliance is installed behind a firewall or NAT device it is necessary to ensure the TRP traffic is permitted in each direction and mapped to the corresponding internal WAN Link Virtual IP Address (VIP).

Firewall Access Rules

Firewall vendors often employ associative object-based components to create service rules for access to the private network. These guidelines are listed below, however, consult your firewall vendor documentation for specific configuration instruction.

1. **Service Object**—By default, TRP uses UDP 2156. If the port number is changed in the configuration, the service object should match.
2. **Host Object**—The WAN Link VIP as it appears to the firewall from the private network.
3. **NAT Policy**—Apply NAT to the outbound TRP traffic referencing the Service and Host Objects.
4. **Security Policy**—Allow inbound TRP traffic from the remote Oracle SD-WAN Appliance. Depending on the firewall make and model this may be implicitly allowed through the NAT Policy.

Objects and Policies	Properties
Service Object	UDP Port 2156
Host Object	WAN Link VIP
NAT Policy	NAT Host and Service
Security Policy	Permit or Forward UDP 2156 to WAN Link VIP



Troubleshooting

Incorrect firewall configuration may result in a DEAD Path in one or both directions. A Path is DEAD when no TRP packets are received for 1500ms or longer.

1. Verify that the firewall configuration matches the configured WAN Link VIPs and UDP ports.
2. Are TRP packets being received on the sending firewall from the LAN?
3. Inspect packet flow on the sending firewall:
 - a. Are TRP packets using the expected NAT Policy and have the correct public IP Address?

6

Glossary

Oracle SD-WAN Aware (Aware)

A software product that provides the services of a network management system (NMS) for the Oracle SD-WAN. Used to manage, monitor, and troubleshoot the Oracle SD-WAN.

Oracle SD-WAN Software

Oracle SD-WAN operating software.

Avalanche Effect

In cryptography, an encryption algorithm is said to have an avalanche effect when a small change in the clear text yields large changes in the encrypted text. An algorithm that exhibits the avalanche effect is mathematically more secure than others because it is very difficult to identify messages that are closely related.

Conduit Service (Conduit)

A service that is a logical combination of one or more paths. This is the typical service for Enterprise Site-to-Site Intranet traffic, utilizing the full value of the APN. With this service, depending on the configuration, traffic is actively managed across multiple WAN Links to create an end-to-end tunnel.

Cryptographically Random

In cryptography, a cryptographically random number is generated by a pseudo random number generating algorithm that is mathematically impossible to predict without knowing the initialization parameters. The US Government security certification, FIPS, maintains a list of approved number generators for cryptography.

Elliptic Curve Diffie-Hellman

A method of creating public/private key pairs for the purpose of establishing a shared secret over an insecure channel using elliptic curve parameters. ECDH is known to provide forward secrecy.

Frequency Analysis

In cryptography, frequency analysis is a method of studying the frequency of patterns in encrypted data in order to infer contents of the encrypted data over time. In its most basic form, frequency analysis is used to learn the contents of a simple substitution cipher based on knowledge of the occurrence of characters in the plain text lexicon. A similar approach can be applied to encrypted network packets to discern the meaning of a data stream.

Forward Secrecy

A property of encryption key exchange protocols that ensures that a session key will not be compromised if another session key or long term keying material becomes compromised in the future.

Indistinguishability

An encrypted message is said to be indistinguishable if an independent observer picking any other message of their choice is no more successful than random chance ($p=0.5$) when attempting to identify whether or not the contents of the two messages are identical.

Initialization Vector

In cryptography, an initialization vector (IV) is used to randomize the input to an encryption method in a way that can be easily undone after decryption. In a block mode encryption, the IV is typically the same size as the block and is XOR'ed with the first block of data prior to encryption. In block chaining, the output of each encrypted block is used as the IV for the next block thereby increasing the difficulty of understanding patterns in a particular message.

Network Control Node (NCN)

The central APNA that acts as the master controller of the APN, as well as the central point of administration for the Client Nodes. The NCN's primary purpose is to establish and utilize Conduits with one or more Client Nodes located across the APN for Enterprise Site-to-Site communications. A particular NCN can administer and have Conduits to multiple Client Nodes.

Secure Key

A unique value that identifies a Site within the APN. Secure Keys are used to generate unique encryption keys for each Conduit, which secures initial client peering and session key generation.

Talari Reliable Protocol (TRP)

A Talari protocol used for reliable transmission of traffic across a WAN between two APNAs. TRP packets are encapsulated in UDP using a default port of 2156.

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.

WAN Path (Path)

A logical, unidirectional connection between two WAN Links.