Oracle® SD-WAN

Firewall Configuration Guide

Original Publication Date: Nov 1, 2019

Table of Contents

About This Document

This document describes how to implement the Talari Firewall Feature set. It includes Filter Policies and NAT examples to help the user understand how to configure the firewall in certain topologies and configurations.

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.

References

The following document is available: Talari APN 5.2 Configuration File Reference

Talari Firewall Overview

Beginning in APN 5.2 GA, Talari provides a stateful firewall built into the Talari application. The firewall allows policies between user-defined zones and Talari APN 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 Talari APN services within a zone.
- Filter traffic between Talari APN services that reside in different zones.
- Define filter policies to allow, deny, and reject flows.
- Filter traffic between Talari 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

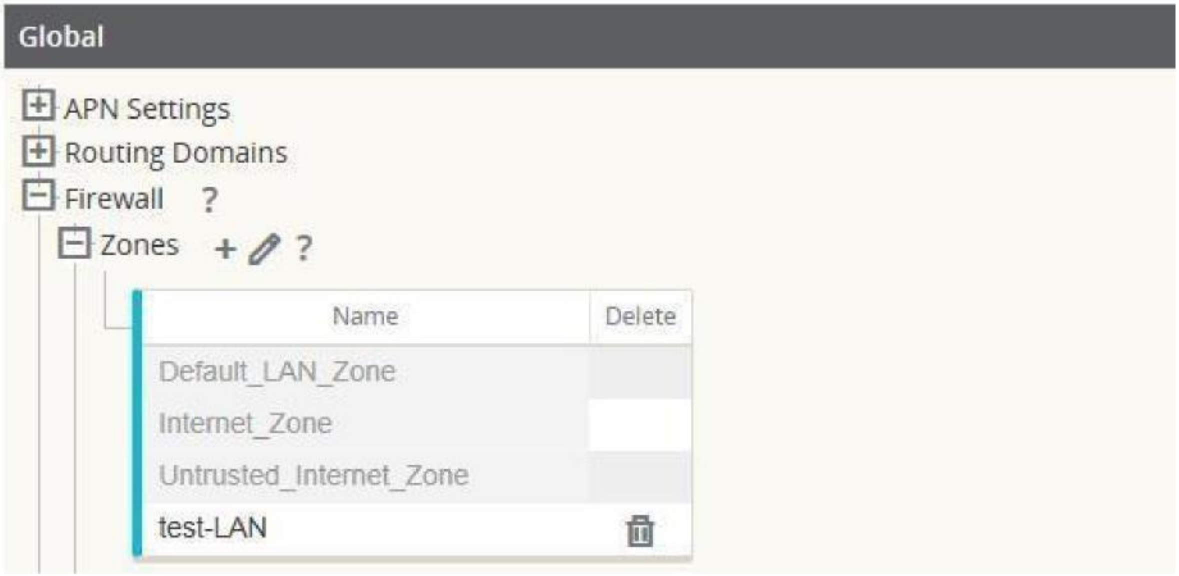
The user can configure zones in the network and define policies to control how traffic enters and leaves zones. By default, the system creates and automatically applies the following zones:

- **Internet Zone**
  - Applies to traffic to or from an Internet service using a Trusted interface.
- **Untrusted_Internet_Zone**
  - Applie **Zone**
    s to traffic
    to or from an Internet service using an Untrusted interface.
- **Default_LAN _**
  - 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

Figure 1 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 Talari Appliance.

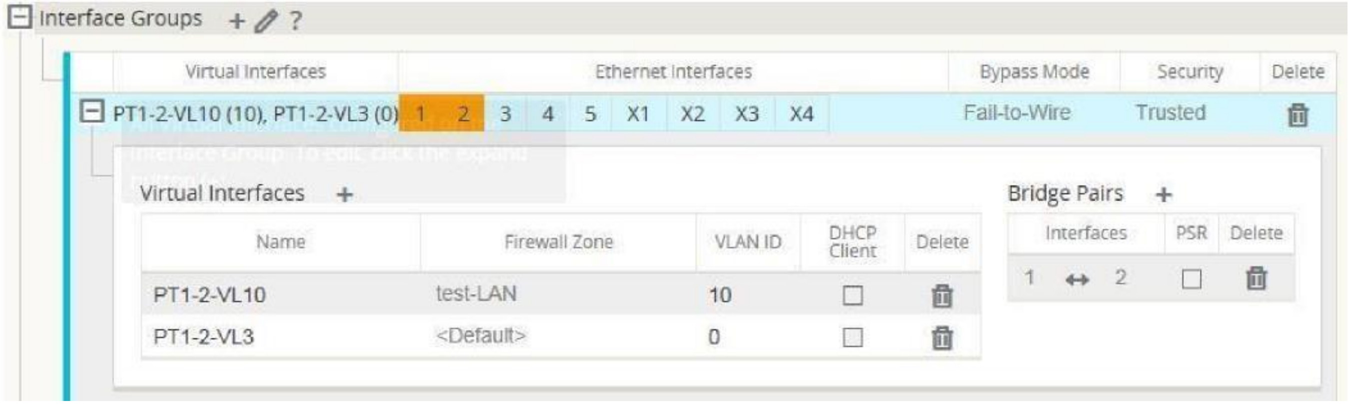


Name	Delete
Default_LAN_Zone	
Internet_Zone	
Untrusted_Internet_Zone	
test-LAN	🗑

Figure 1

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 polices 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".



Virtual Interfaces	Ethernet Interfaces	Bypass Mode	Security	Delete
PT1-2-VL10 (10), PT1-2-VL3 (0)	1 2 3 4 5 X1 X2 X3 X4	Fail-to-Wire	Trusted	🗑

Virtual Interfaces +

Name	Firewall Zone	VLAN ID	DHCP Client	Delete
PT1-2-VL10	test-LAN	10	□	🗑
PT1-2-VL3	<Default>	0	□	🗑

Bridge Pairs +

Interfaces	PSR	Delete
1 ↔ 2	□	🗑

Figure 2

The destination zone of a packet is determined based on the destination route match. As a Talari 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 Talari 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 Figure 3. In the example below, we have Zone_A and Zone_B, each of which has a LAN VNI.

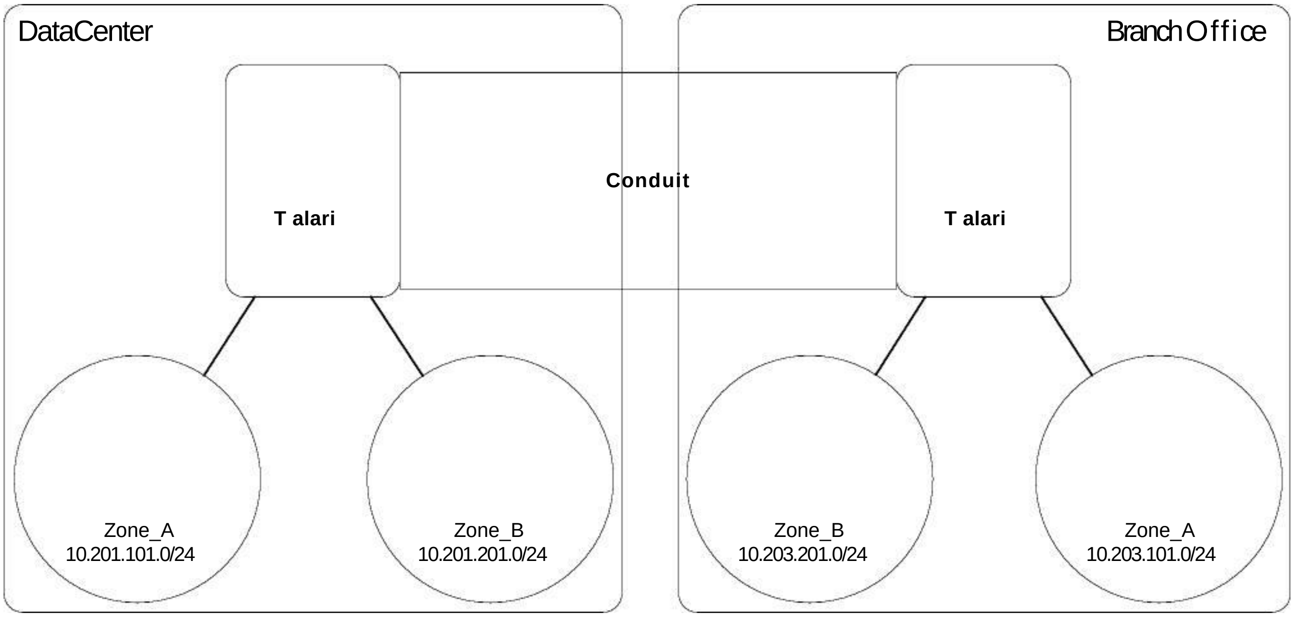
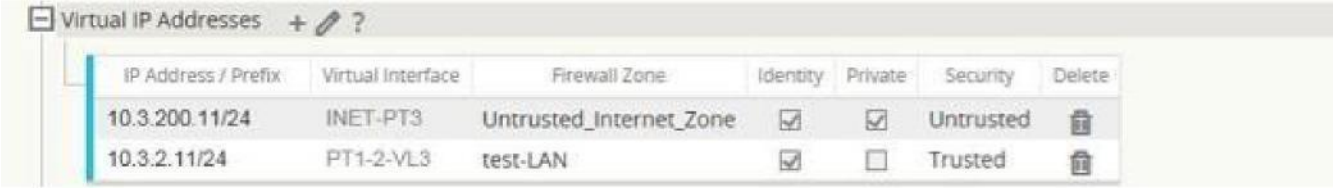


Figure 3

Figure 4 displays the inheritance of zone for a VIP from its assigned VNI.



IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
10.3.200.11/24	INET-PT3	Untrusted_Internet_Zone	☑	☑	Untrusted	🗑
10.3.2.11/24	PT1-2-VL3	test-LAN	☑	☐	Trusted	🗑

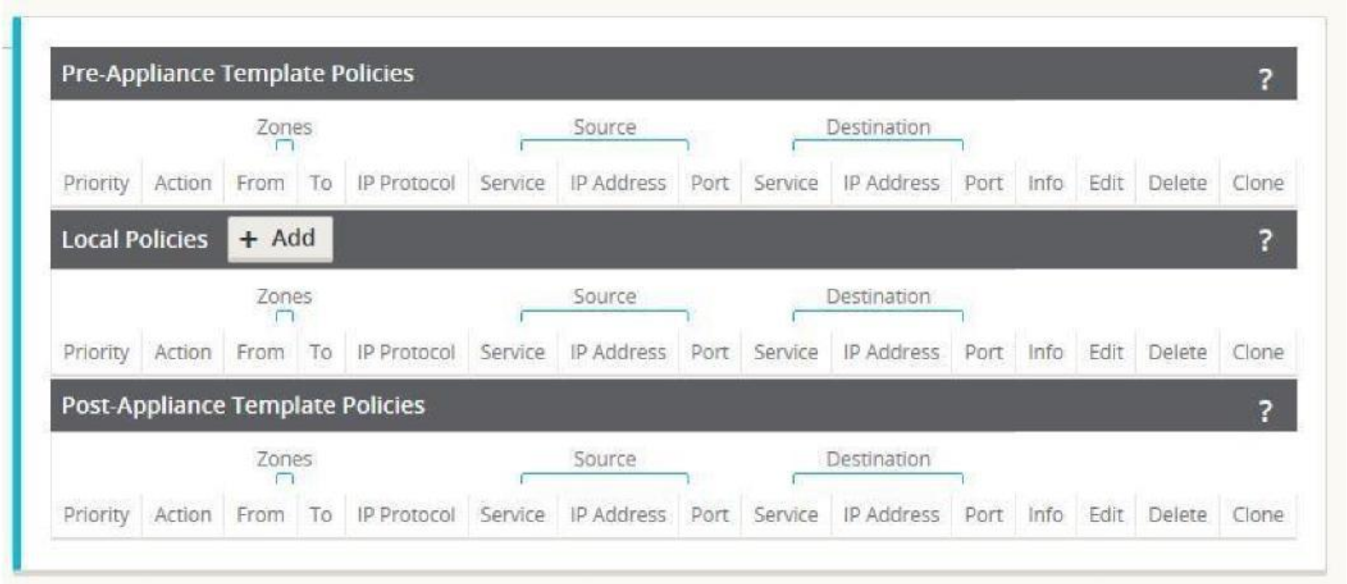
Figure 4

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 PostAppliance 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.



Pre-Appliance Template Policies ?

		Zones			Source			Destination						
Priority	Action	From	To	IP Protocol	Service	IP Address	Port	Service	IP Address	Port	Info	Edit	Delete	Clone

Local Policies + Add ?

		Zones			Source			Destination						
Priority	Action	From	To	IP Protocol	Service	IP Address	Port	Service	IP Address	Port	Info	Edit	Delete	Clone

Post-Appliance Template Policies ?

		Zones			Source			Destination						
Priority	Action	From	To	IP Protocol	Service	IP Address	Port	Service	IP Address	Port	Info	Edit	Delete	Clone

Figure 5

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 t**emplate “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.

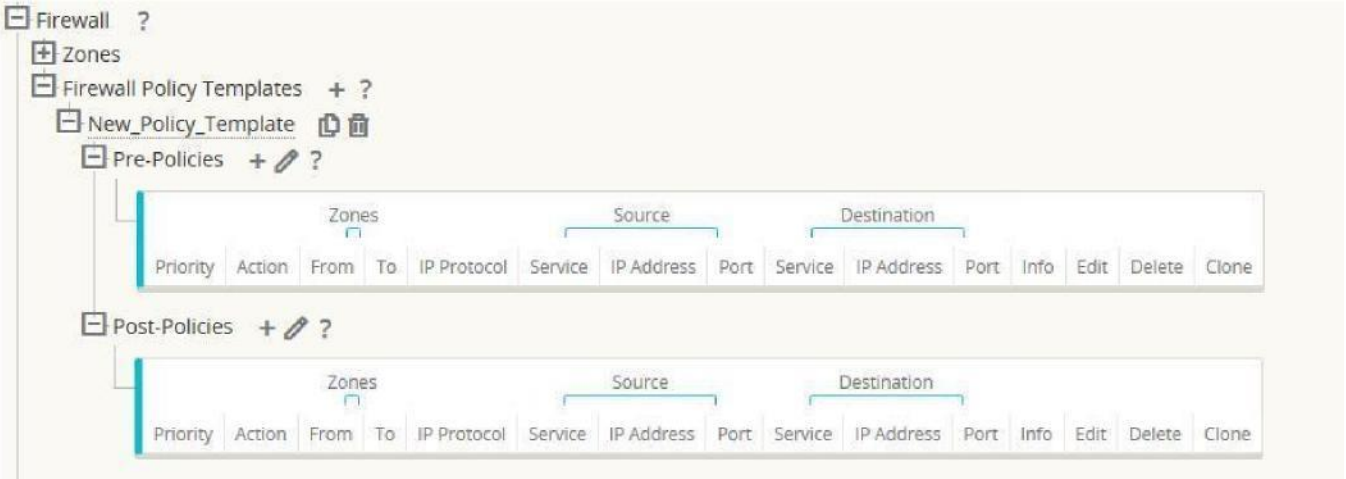
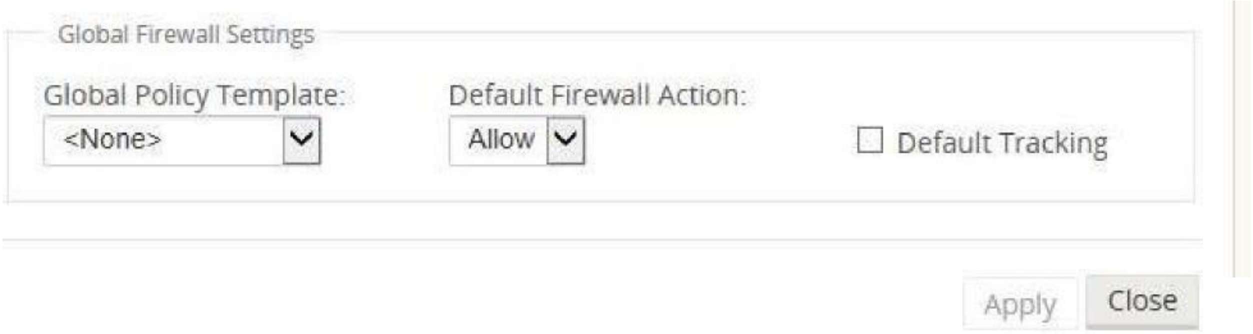


Figure 6

Figure 6 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 (see Figure 7). At the site level, the user can add more policy templates, as well as create site specific policies.


Global Firewall Settings

Global Policy Template: <None>

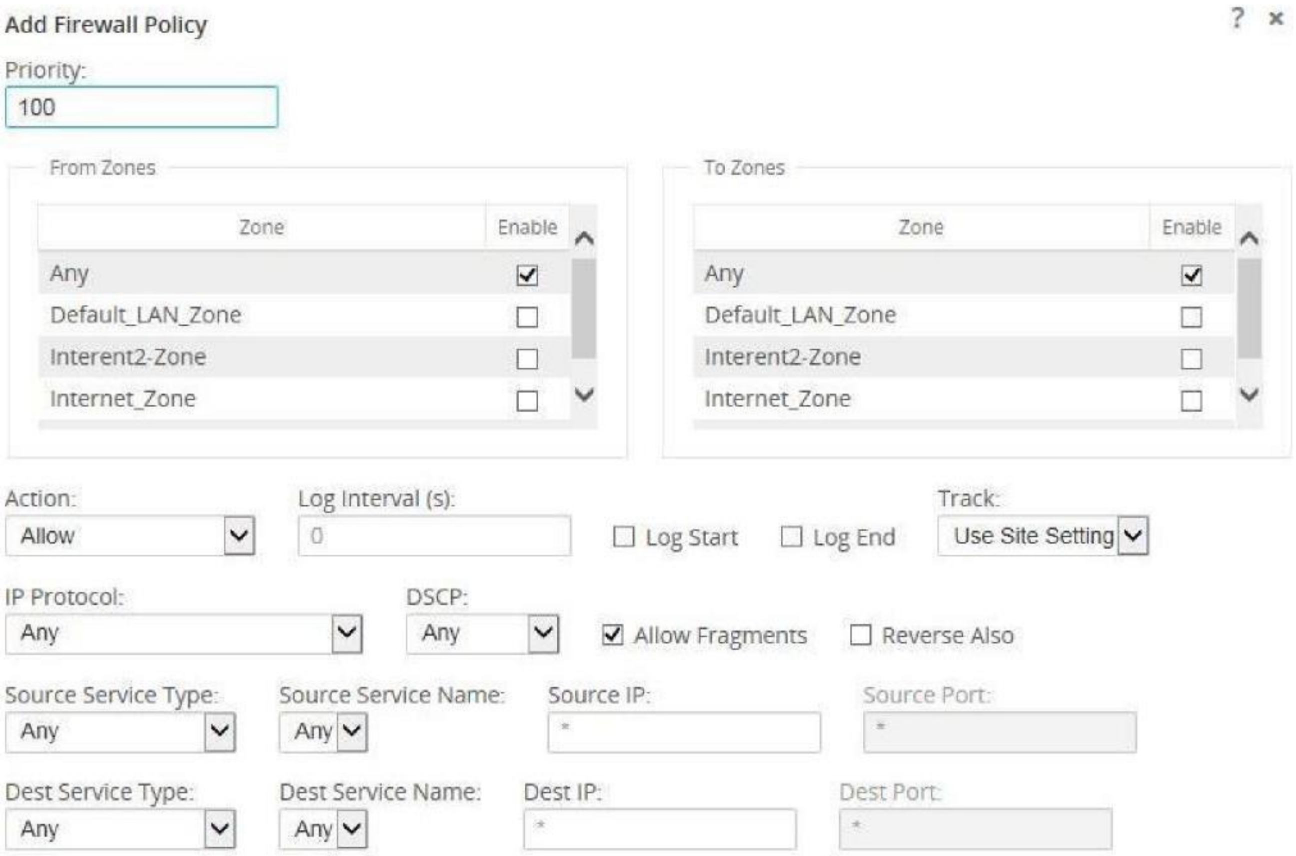
Default Firewall Action: Allow

□ Default Tracking

Figure 7

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

Note: Ports configured for Talari Reliable Protocol (UDP 2156, or a user-defined TRP port) are automatically permitted to prevent user-configurable polices from blocking a Conduit from establishing.



Add Firewall Policy

Priority: 100

From Zones

Zone	Enable
Any	☑
Default_LAN_Zone	□
Interent2-Zone	□
Internet_Zone	□

To Zones

Zone	Enable
Any	☑
Default_LAN_Zone	□
Interent2-Zone	□
Internet_Zone	□

Action: Allow

Log Interval (s): 0

□ Log Start

□ Log End

Track: Use Site Setting

IP Protocol: Any

DSCP: Any

☑ Allow Fragments

□ Reverse Also

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: Any

Dest IP: *

Dest Port: *

Figure 8

Policy Attributes

Priority – order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority polices.

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 Talari 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 Talari application. For example, running a ping from the Web UI of the Talari results in a packet sourced from a Talari 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 Talari 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 Talari 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

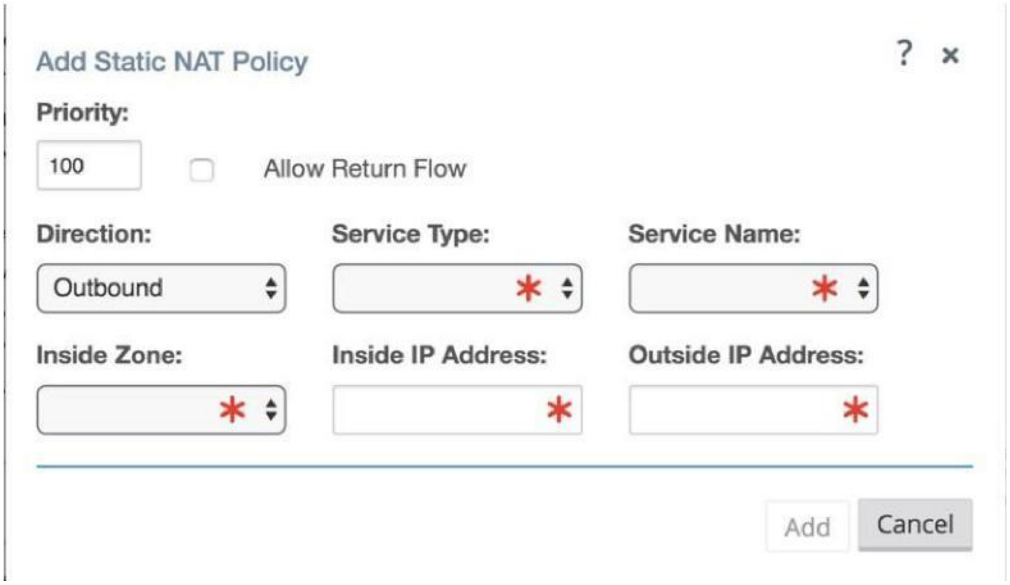
Note: At this time, the NAT capability can only be configured at the site level; there is no global configuration (templates) for NAT. All NAT policies are defined from a Source-NAT (“SNAT”) translation prespective. Corresponding Destination-NAT (“DNAT”) rules are created automatically for the user.

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

Priority: 100

□ Allow Return Flow

Direction: Outbound

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 polices.

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 Talari 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.

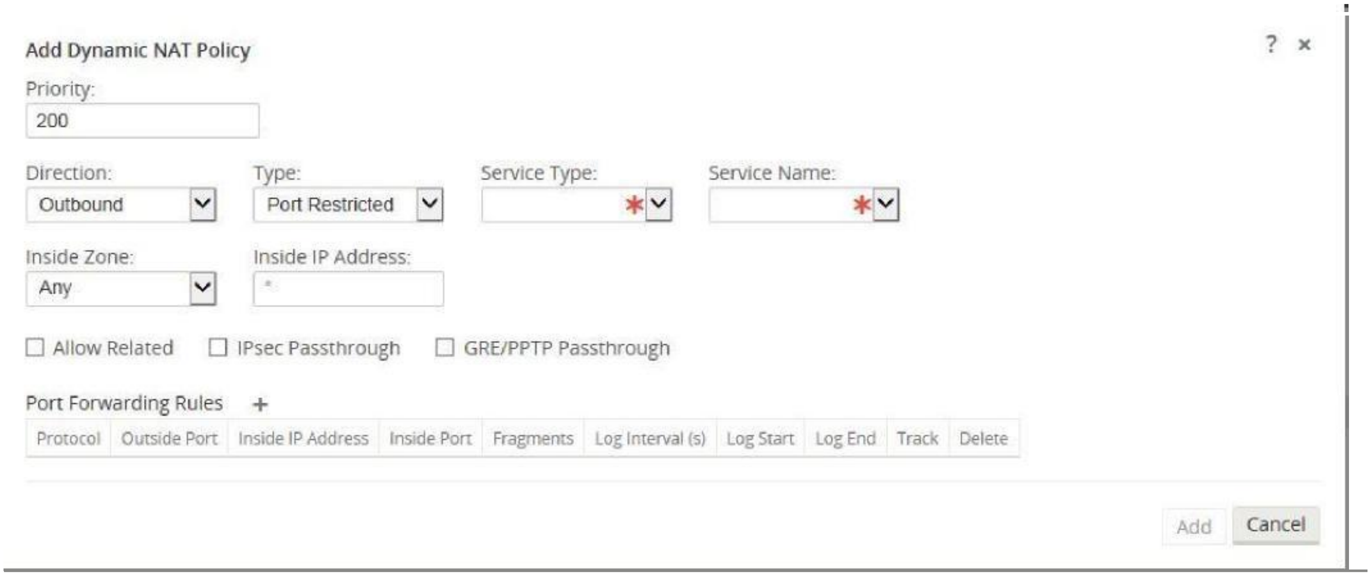
Inside IP address – source IP address and mask of the direction selected above.

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.



Add Dynamic NAT Policy

Priority: 200

Direction: Outbound

Type: Port Restricted

Service Type:

Service Name:

Inside Zone: Any

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

Figure 10

Priority – the order the policy will be applied within all the defined policies. Lower priority policies are applied before higher priority polices.

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 Talari 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.

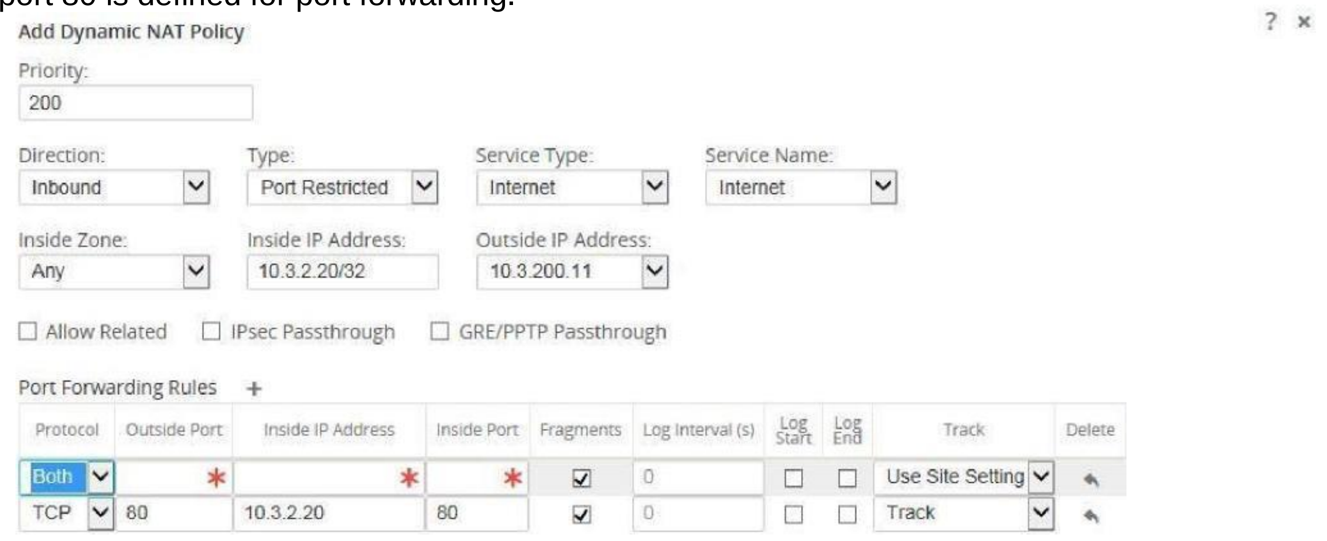
Allow Related – allow traffic related to the flow matching the rule. For example, ICMP redirection related to the specific flow that matched the policy, if there was some type of error related to the flow.

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

Priority: 200

Direction: Inbound

Type: Port Restricted

Service Type: Internet

Service Name: Internet

Inside Zone: Any

Inside IP Address: 10.3.2.20/32

Outside IP Address: 10.3.200.11

□ 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
Both	*	*	*	☑	0	□	□	Use Site Setting	
TCP	80	10.3.2.20	80	☑	0	□	□	Track	

Figure 11 **Protocol**

– TCP, UDP, or both.

Outisde 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).

Known Caveats

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 Talari 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 Talari 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.

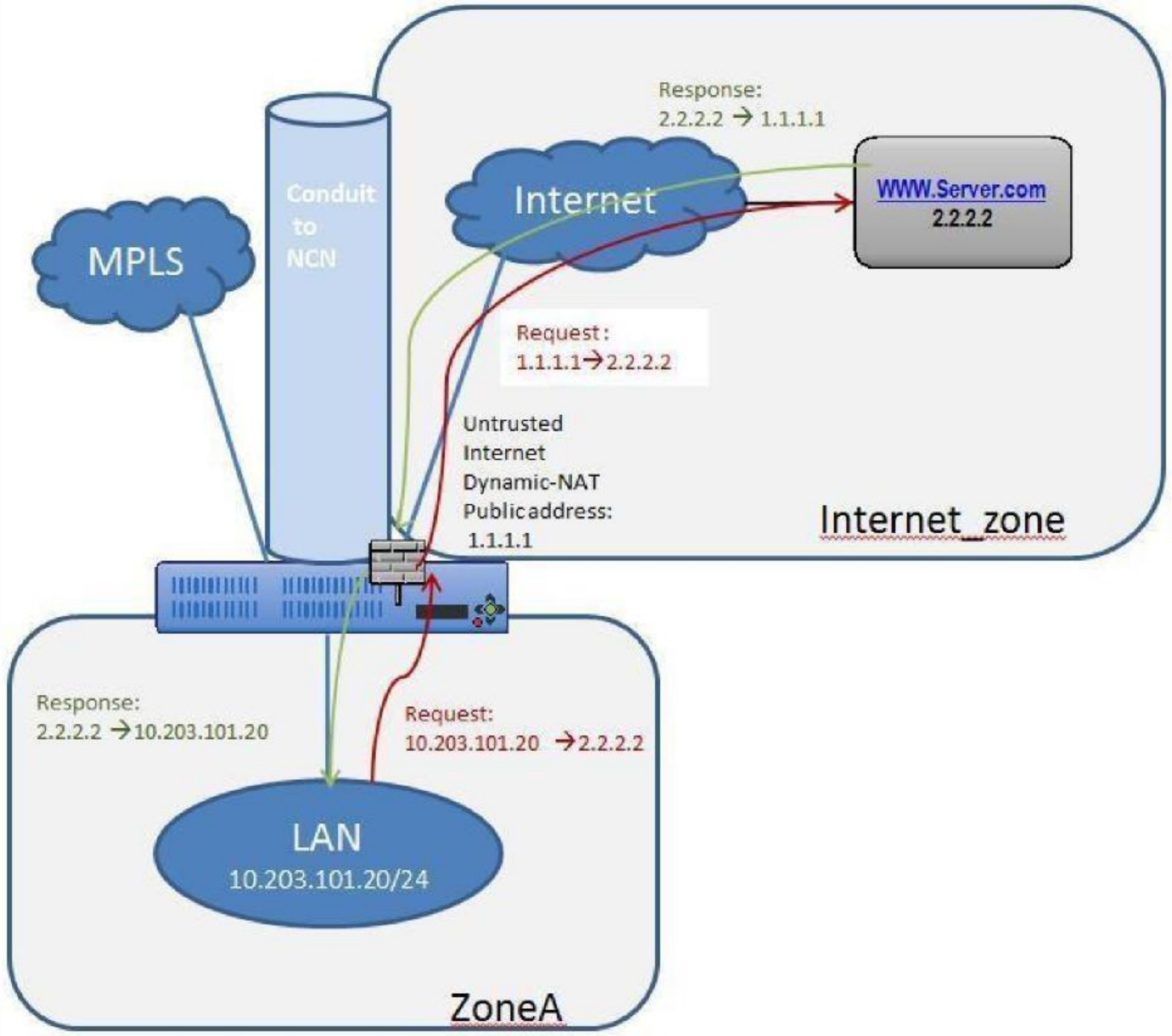


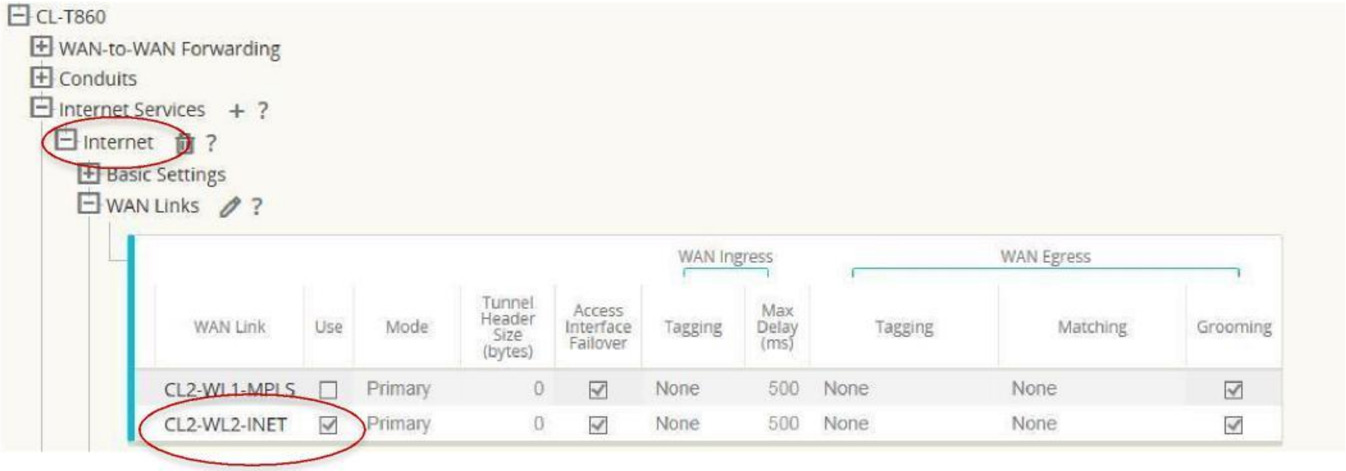
Figure 12

The configuration process to enable this capability is as follows, assuming the Talari 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).
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** it to **Change Management**.

Steps 1 & 2 - Adding the Internet service and assigning it to a WAN Link.



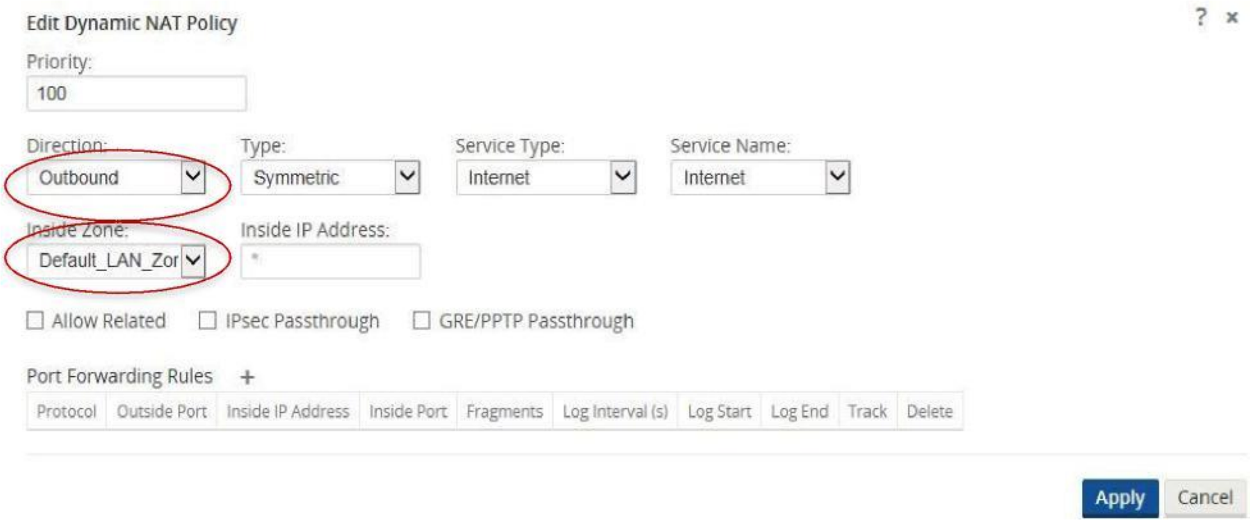
					WAN Ingress		WAN Egress		
WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Failover	Tagging	Max Delay (ms)	Tagging	Matching	Grooming
CL2-WL1-MPLS	□	Primary	0	☑	None	500	None	None	☑
CL2-WL2-INET	☑	Primary	0	☑	None	500	None	None	☑

Figure 1 3

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**.



Edit Dynamic NAT Policy

Priority: 100

Direction: Outbound

Type: Symmetric

Service Type: Internet

Service Name: Internet

Inside Zone: Default_LAN_Zor

Inside IP Address: *

☐ Allow Related ☐ IPsec Passthrough ☐ GRE/PPTP Passthrough

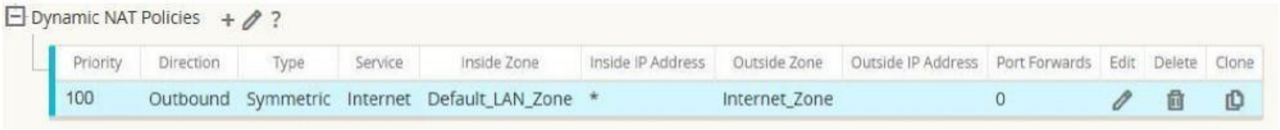
Port Forwarding Rules +

Protocol	Outside Port	Inside IP Address	Inside Port	Fragments	Log Interval (s)	Log Start	Log End	Track	Delete

Figure 1 4

Define the dynamic NAT policies (PAT rule):

a. Direction: Outbound
b. Type: Symmetric (Firewall can change the source port)
c. Service Type: Internet
d. Service Name: Internet
e. Inside Zone: Default_LAN_Zone
f. Inside IP address: * (default)
g. Outside zone: Internet_Zone (because of defined service type this is known) The completed Dynamic NAT Policy will be displayed as follows:



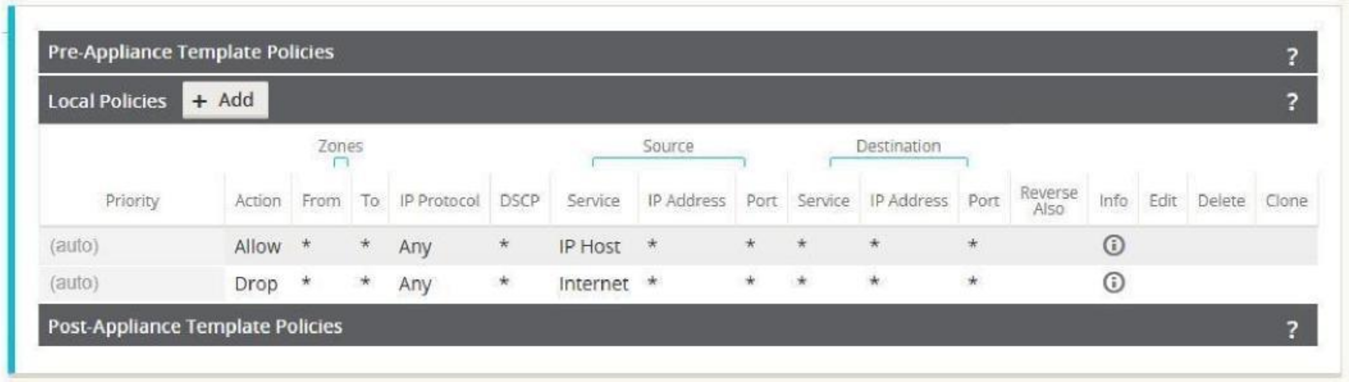
Dynamic NAT Policies + ?

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 Talari 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 ?

		Zones				Source			Destination							
Priority	Action	From	To	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone
(auto)	Allow	*	*	Any	*	IP Host	*	*	*	*	*		ⓘ			
(auto)	Drop	*	*	Any	*	Internet	*	*	*	*	*		ⓘ			

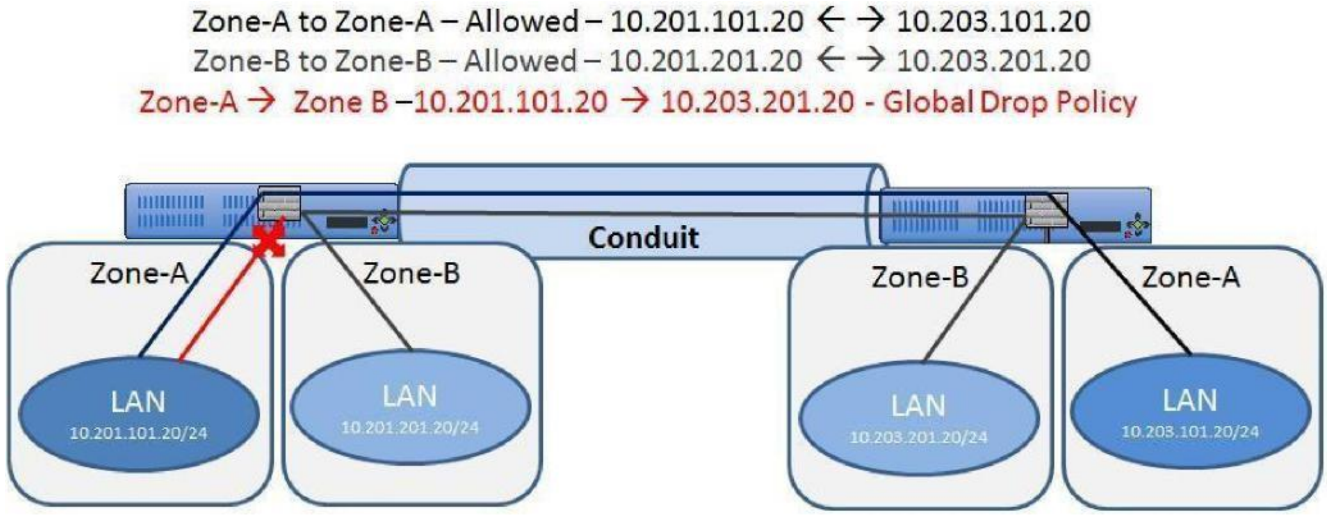
Post-Appliance Template Policies ?

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.



Zone-A to Zone-A – Allowed – 10.201.101.20 ← → 10.203.101.20

Zone-B to Zone-B – Allowed – 10.201.201.20 ← → 10.203.201.20

Zone-A → Zone B –10.201.101.20 → 10.203.201.20 - Global Drop Policy

Figure 17

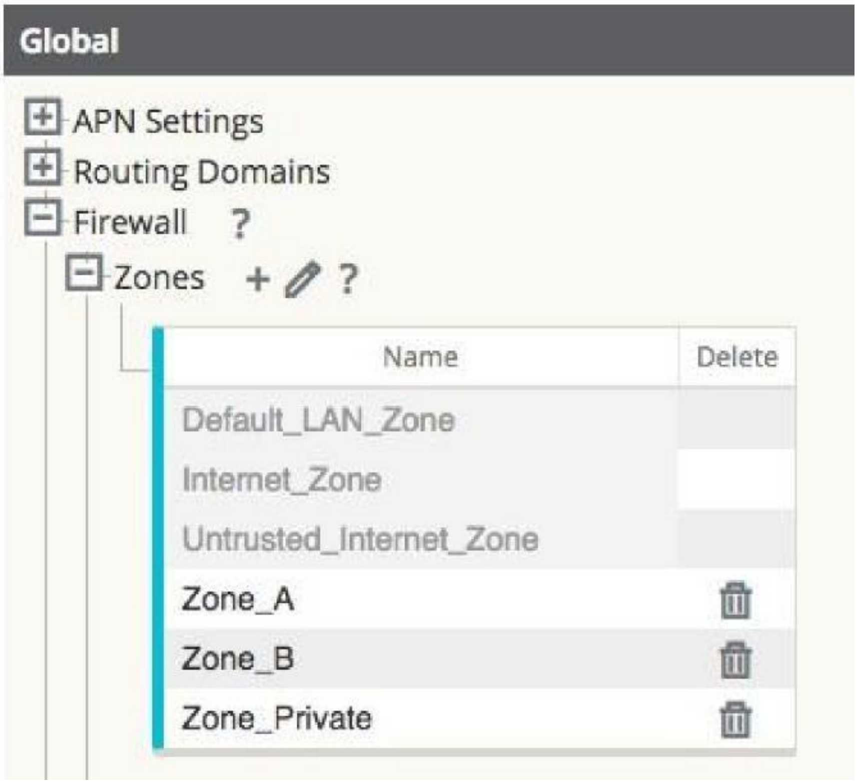
The configuration process to enable this capability is as follows, assuming the Talari Client site is currently up and operational.

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.

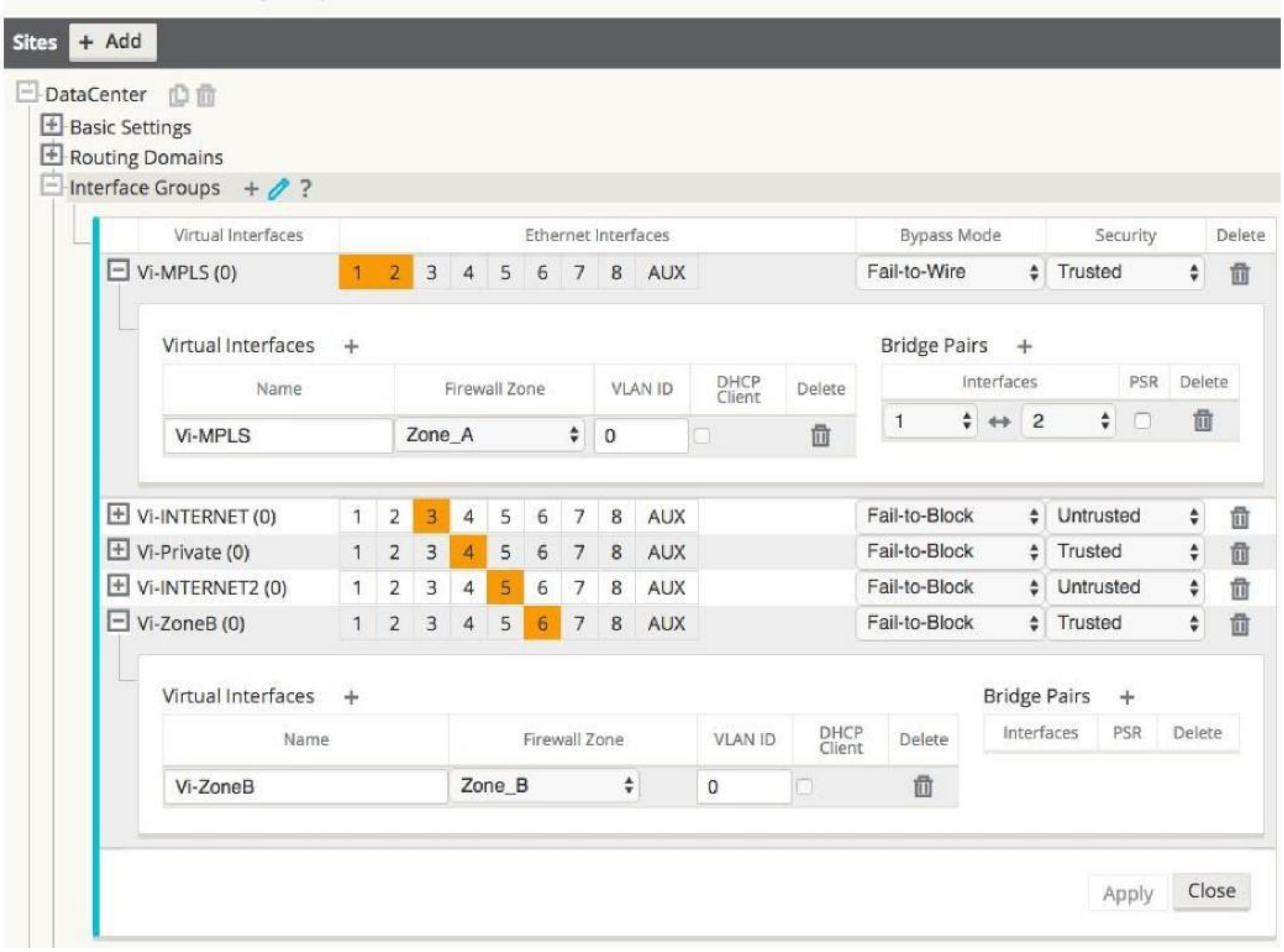


Name	Delete
Default_LAN_Zone	
Internet_Zone	
Untrusted_Internet_Zone	
Zone_A	🗑
Zone_B	🗑
Zone_Private	🗑

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 Talari Appliance.

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



Virtual Interfaces	Ethernet Interfaces	Bypass Mode	Security	Delete
Vi-MPLS (0)	**1** **2** 3 4 5 6 7 8 AUX	Fail-to-Wire	Trusted	🗑
Vi-INTERNET (0)	1 2 **3** 4 5 6 7 8 AUX	Fail-to-Block	Untrusted	🗑
Vi-Private (0)	1 2 3 **4** 5 6 7 8 AUX	Fail-to-Block	Trusted	🗑
Vi-INTERNET2 (0)	1 2 3 4 **5** 6 7 8 AUX	Fail-to-Block	Untrusted	🗑
Vi-ZoneB (0)	1 2 3 4 5 **6** 7 8 AUX	Fail-to-Block	Trusted	🗑

Vi-MPLS (0) – Virtual Interfaces +

Name	Firewall Zone	VLAN ID	DHCP Client	Delete
Vi-MPLS	Zone_A	0	□	🗑

Bridge Pairs +

Interfaces	PSR	Delete
1 ↔ 2	□	🗑

Vi-ZoneB (0) – Virtual Interfaces +

Name	Firewall Zone	VLAN ID	DHCP Client	Delete
Vi-ZoneB	Zone_B	0	□	🗑

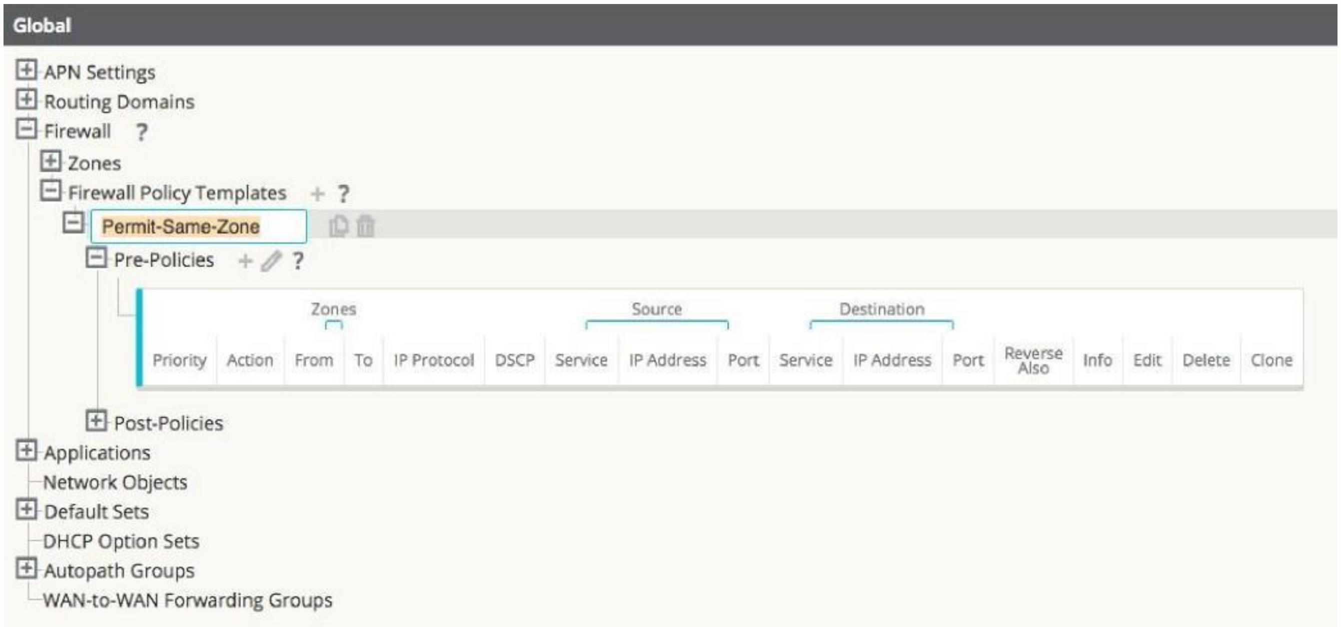
Bridge Pairs +

Interfaces	PSR	Delete

Figure 19

Step 2 - Create a filter-policy template to:

c. Permit Zone_A > Zone_A traffic.
d. Permit Zone_B > Zone_B traffic.

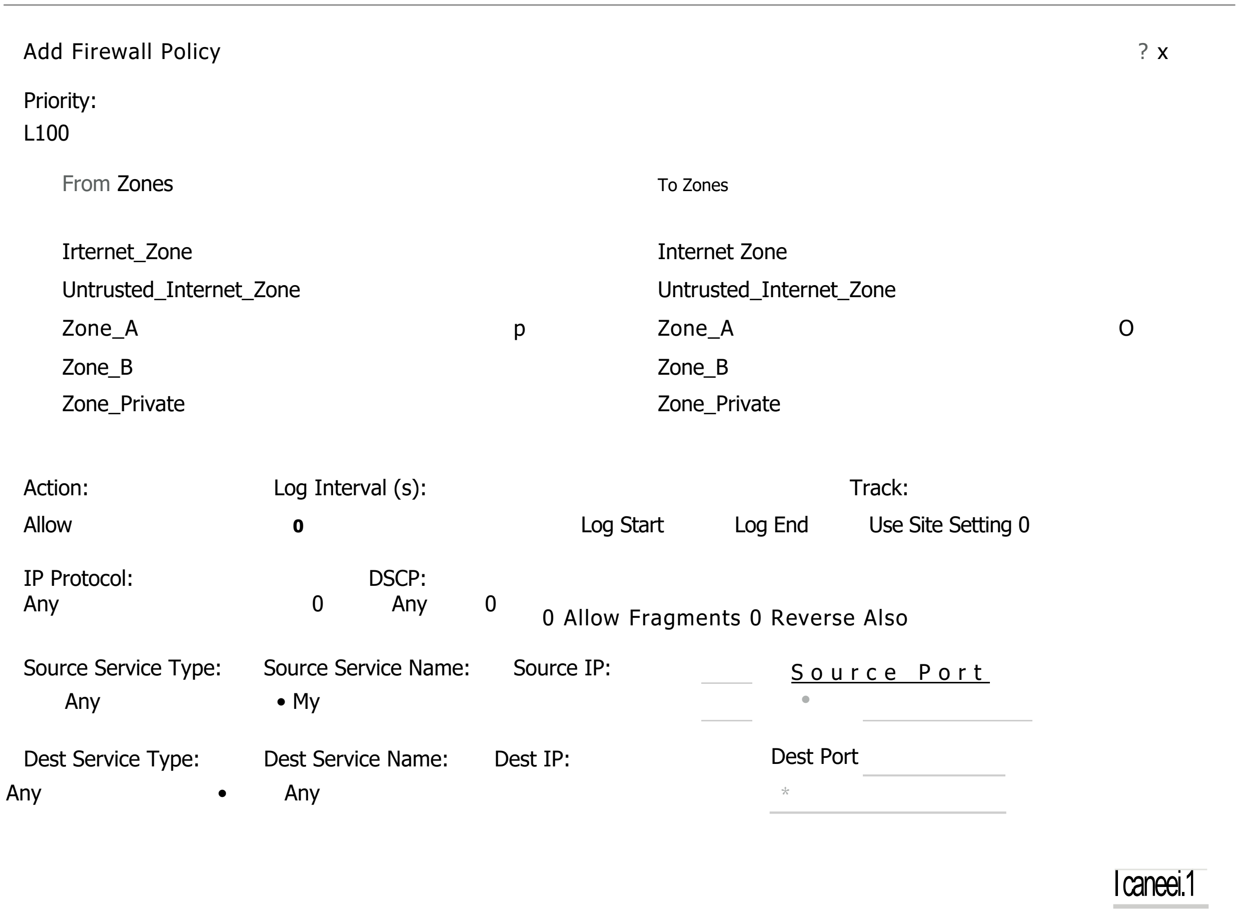


		Zones				Source			Destination							
Priority	Action	From	To	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone

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:
L100

From Zones		To Zones	
Irternet_Zone		Internet Zone	
Untrusted_Internet_Zone		Untrusted_Internet_Zone	
Zone_A	p	Zone_A	O
Zone_B		Zone_B	
Zone_Private		Zone_Private	

Action: Allow

Log Interval (s): **0**

Log Start Log End

Track: Use Site Setting 0

IP Protocol: Any 0

DSCP: Any 0

0 Allow Fragments 0 Reverse Also

Source Service Type: Any

Source Service Name: • My

Source IP:

Source Port •

Dest Service Type: Any •

Dest Service Name: Any

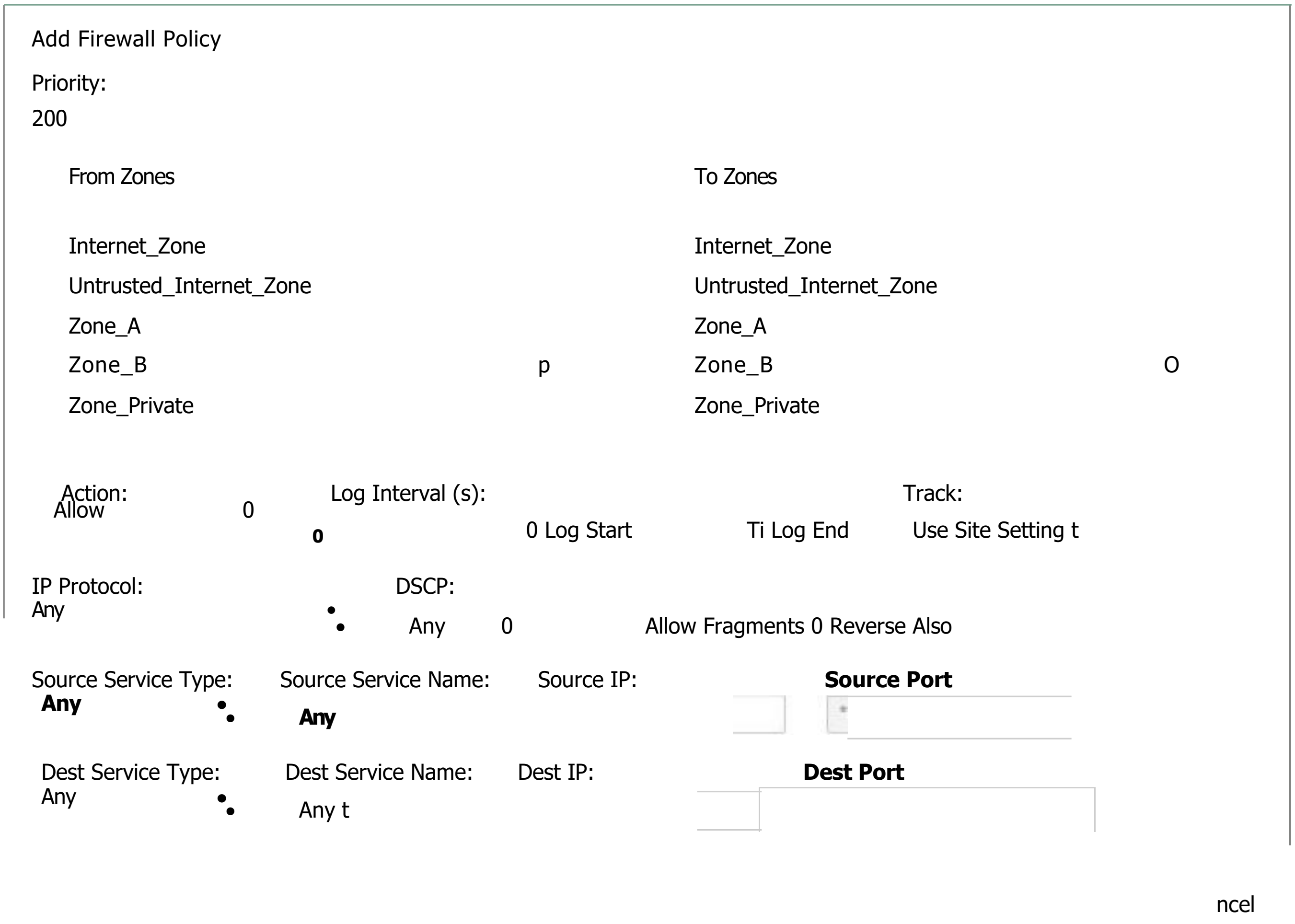
Dest IP:

Dest Port *

Icaneei.1

Figure 21

Repeat the process for Zone_B policies.



Add Firewall Policy

Priority:
200

From Zones		To Zones	
Internet_Zone		Internet_Zone	
Untrusted_Internet_Zone		Untrusted_Internet_Zone	
Zone_A		Zone_A	
Zone_B	p	Zone_B	O
Zone_Private		Zone_Private	

Action:
Allow 0

Log Interval (s):
0

0 Log Start

Ti Log End

Track:
Use Site Setting t

IP Protocol:
Any

DSCP:
Any 0

Allow Fragments 0 Reverse Also

Source Service Type:
Any

Source Service Name:
Any

Source IP:

Source Port

Dest Service Type:
Any

Dest Service Name:
Any t

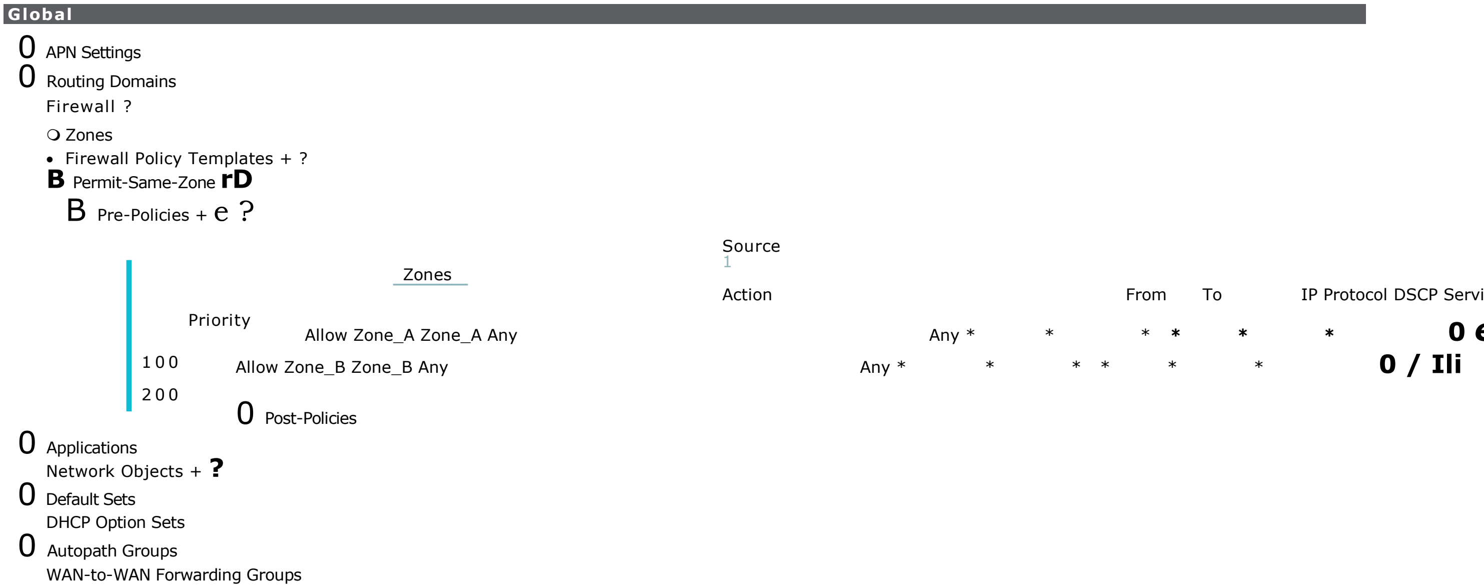
Dest IP:

Dest Port

ncel

Figure 22

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



Global

0 APN Settings
0 Routing Domains
Firewall ?
❍ Zones
- Firewall Policy Templates + ?
B Permit-Same-Zone rD
B Pre-Policies + e ?

Source
1
Zones
Action From To IP Protocol DSCP Servi
Priority
Allow Zone_A Zone_A Any Any * * * * * * 0 e
100 Allow Zone_B Zone_B Any Any * * * * * * 0 / Ili
200
0 Post-Policies

0 Applications
Network Objects + ?
0 Default Sets
DHCP Option Sets
0 Autopath Groups
WAN-to-WAN Forwarding Groups

Figure 23

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

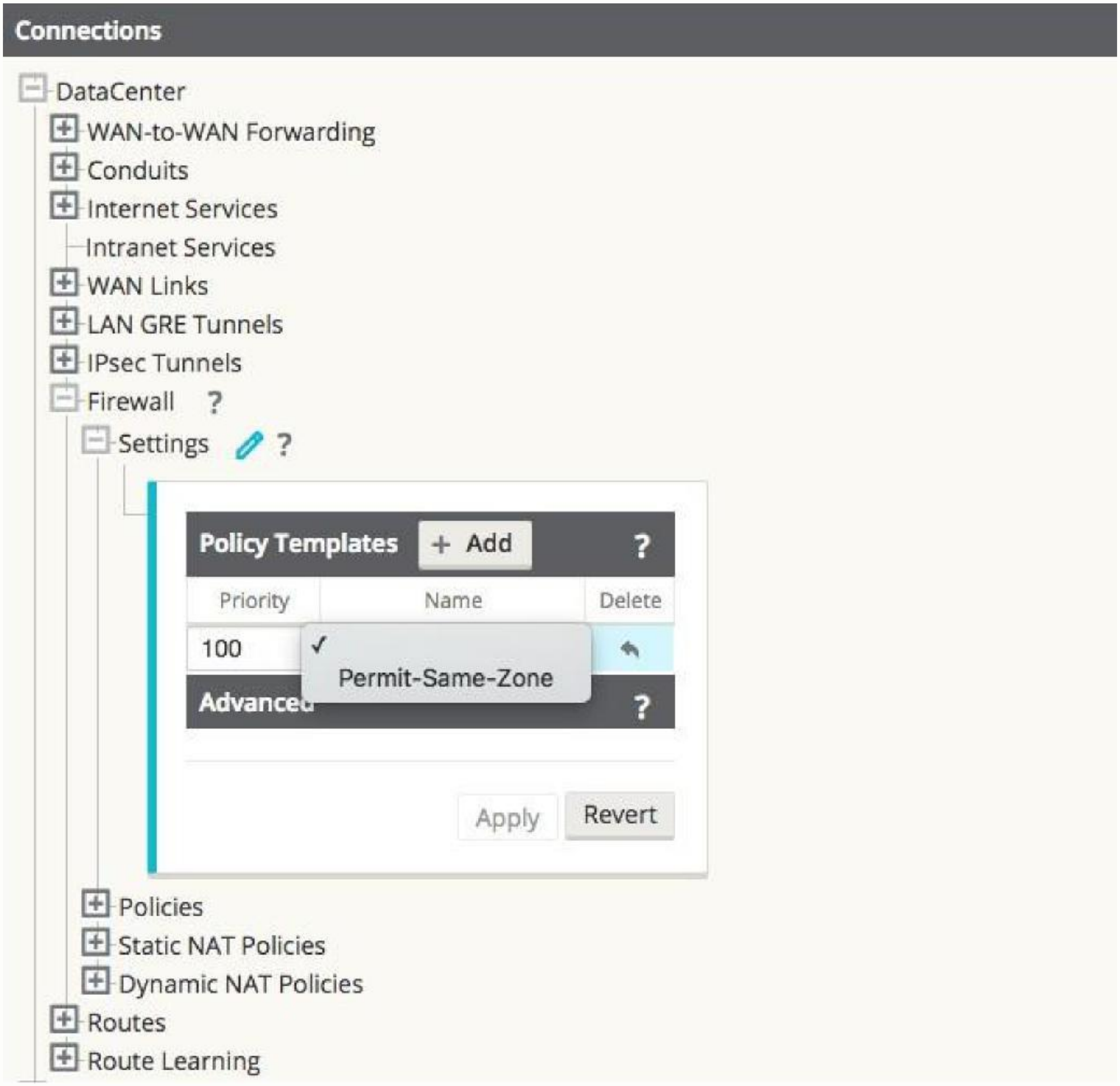
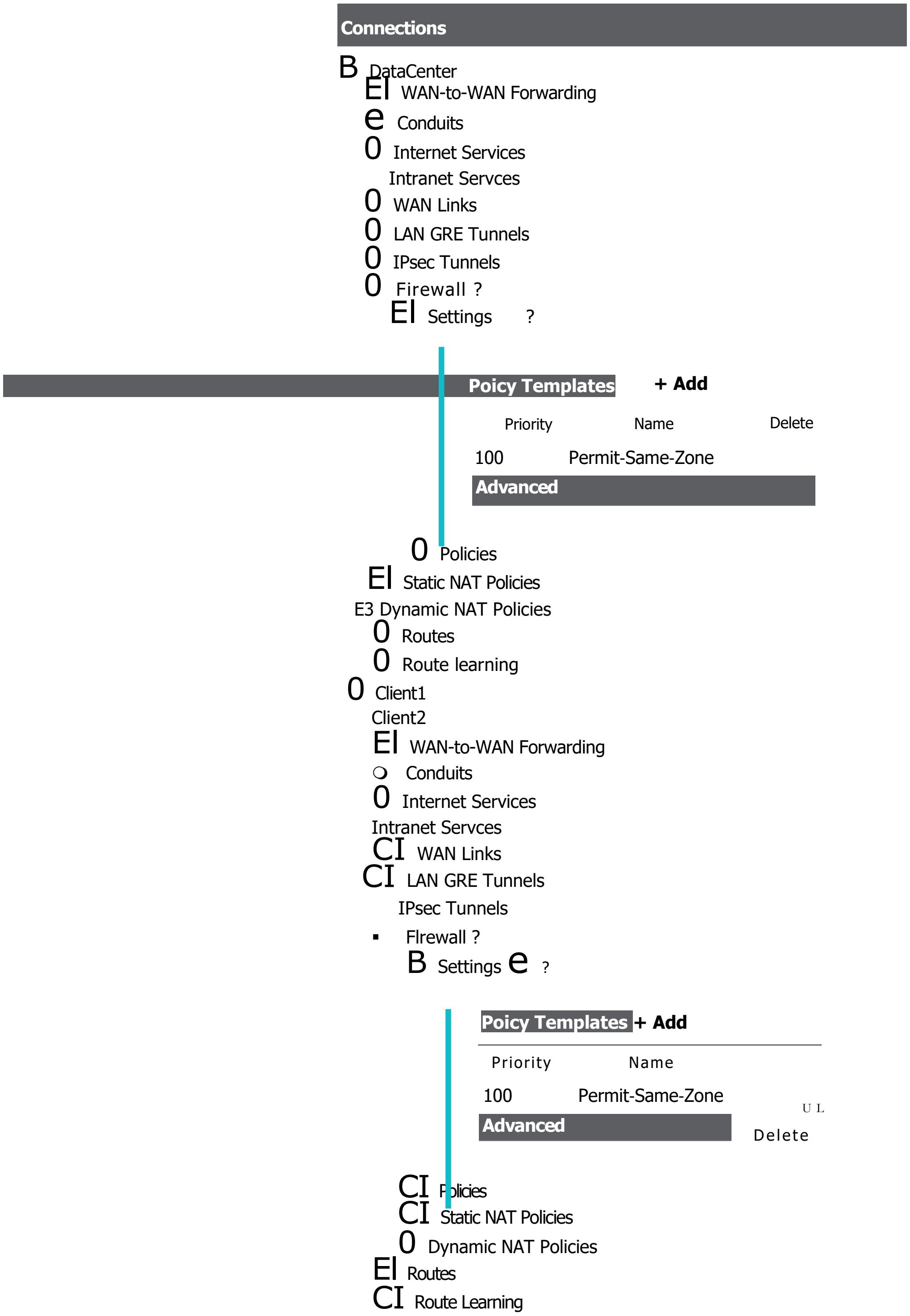


Figure 24

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

B DataCenter
El WAN-to-WAN Forwarding
e Conduits
0 Internet Services
Intranet Servces
0 WAN Links
0 LAN GRE Tunnels
0 IPsec Tunnels
0 Firewall ?
El Settings ?

Poicy Templates + Add

Priority	Name	Delete
100	Permit-Same-Zone	

Advanced

0 Policies
El Static NAT Policies
E3 Dynamic NAT Policies
0 Routes
0 Route learning
0 Client1
Client2
El WAN-to-WAN Forwarding
❍ Conduits
0 Internet Services
Intranet Servces
CI WAN Links
CI LAN GRE Tunnels
IPsec Tunnels
▪ FIrewall ?
B Settings e ?

Poicy Templates + Add

Priority	Name	
100	Permit-Same-Zone	U L

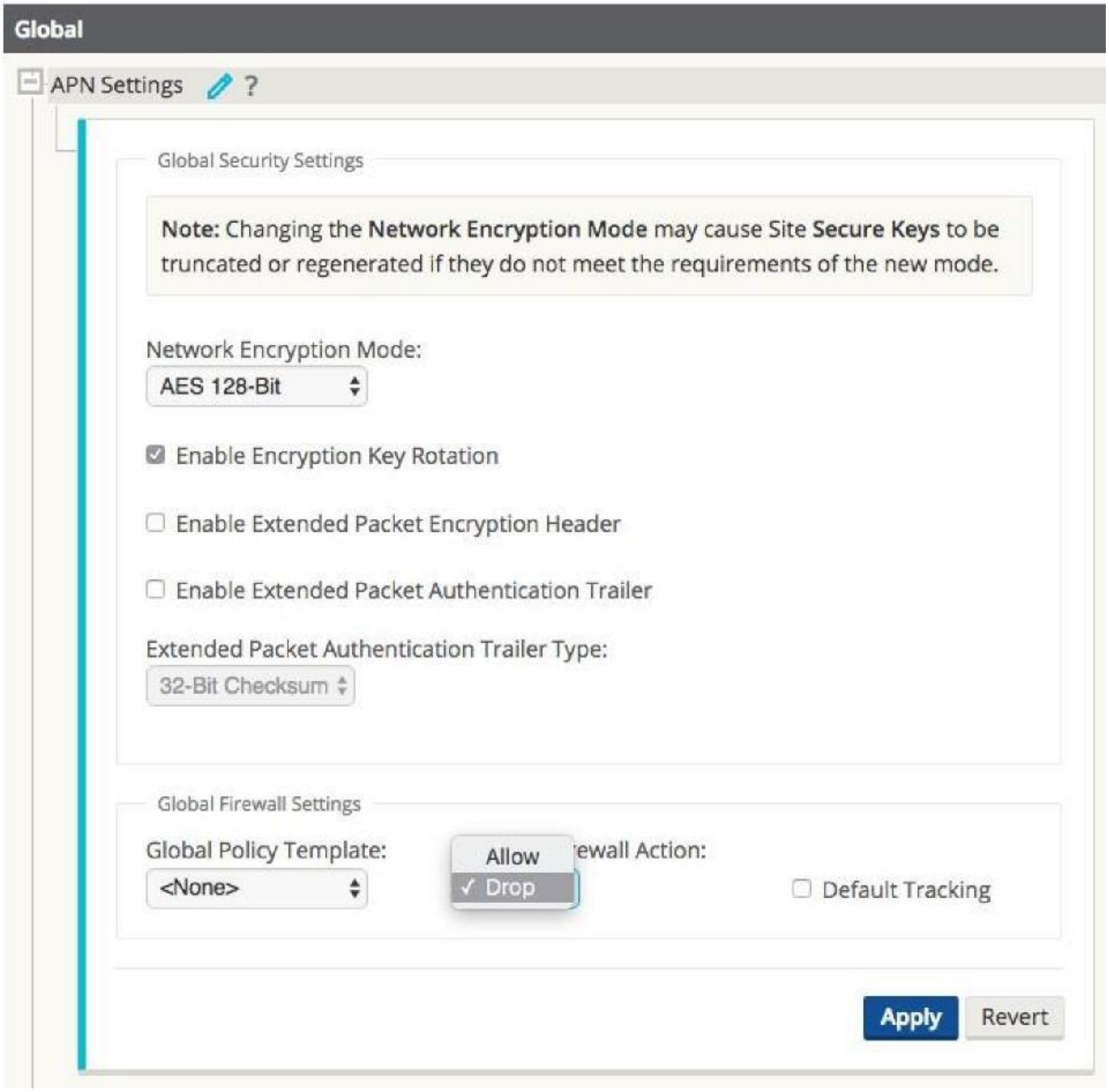
Advanced

Delete

CI Policies
CI Static NAT Policies
0 Dynamic NAT Policies
El Routes
CI Route Learning

Figure 25

Step 4 - Configure the default global behavior to **Drop**.



Global Security Settings

Note: Changing the **Network Encryption Mode** may cause Site **Secure Keys** to be truncated or regenerated if they do not meet the requirements of the new mode.

Network Encryption Mode: AES 128-Bit

☑ Enable Encryption Key Rotation

□ Enable Extended Packet Encryption Header

□ Enable Extended Packet Authentication Trailer

Extended Packet Authentication Trailer Type: 32-Bit Checksum

Global Firewall Settings

Global Policy Template: <None>

ewall Action: ✓ Drop

□ Default Tracking

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.

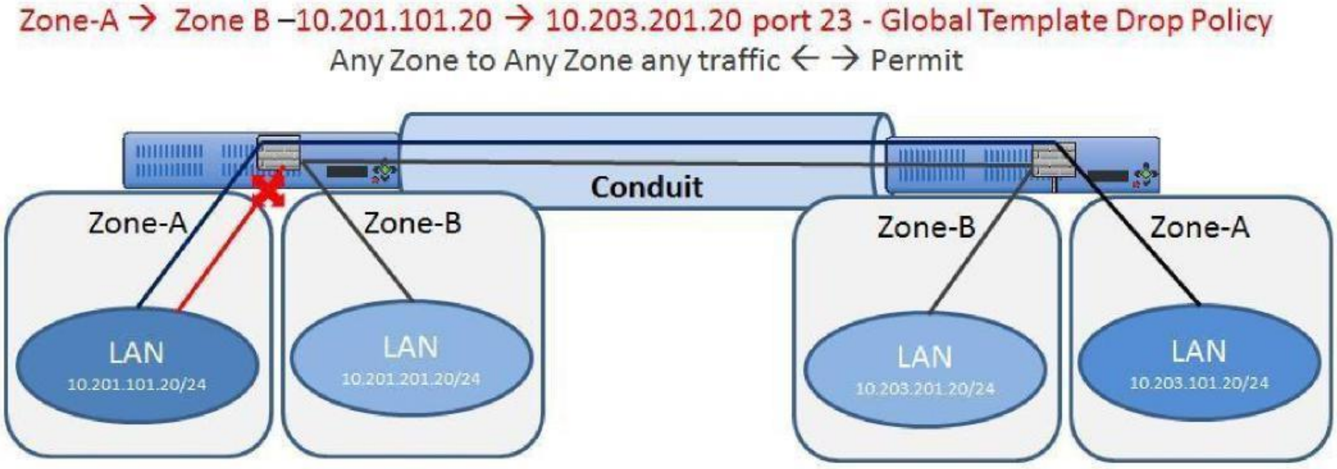
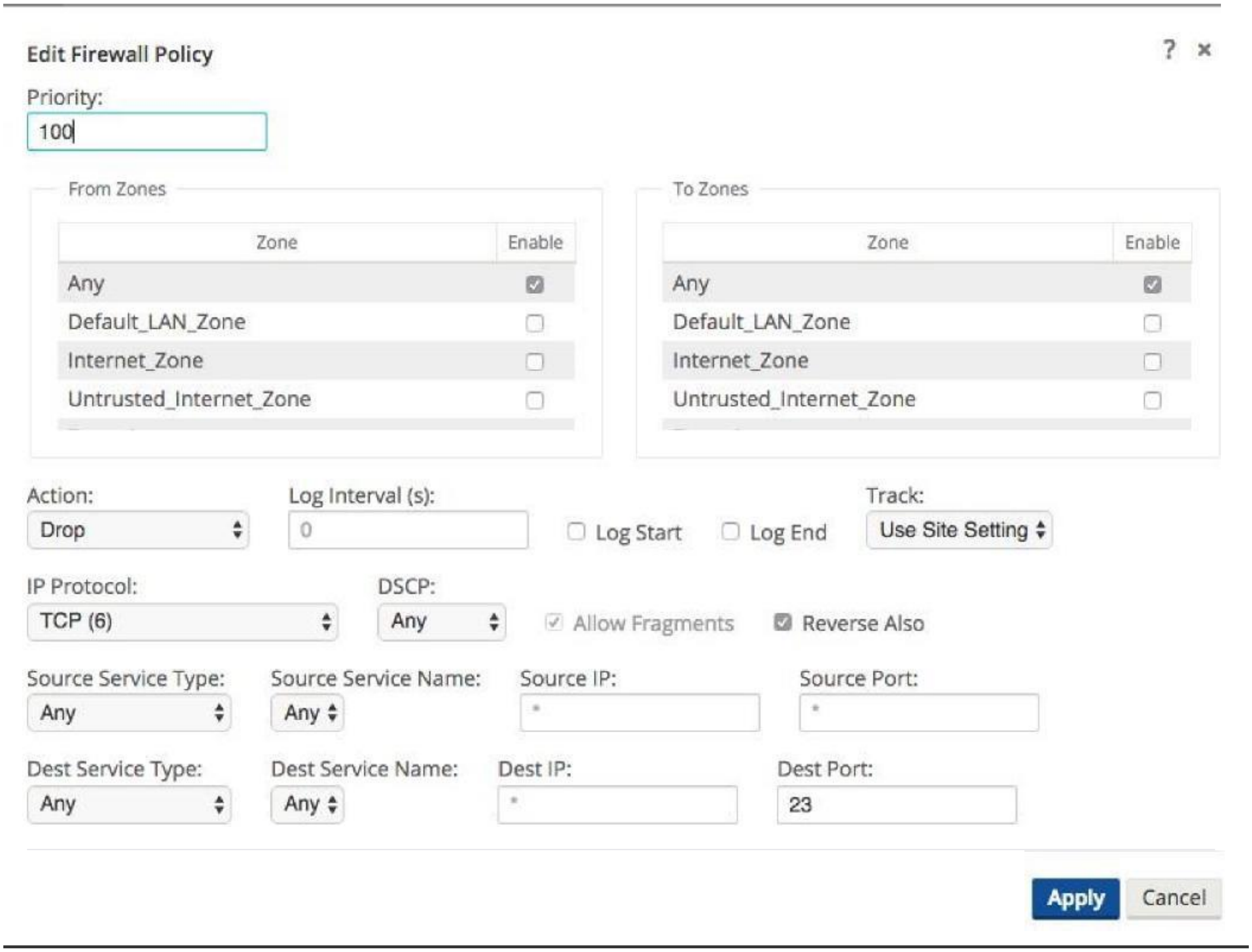

Zone-A → Zone B –10.201.101.20 → 10.203.201.20 port 23 - Global Template Drop Policy
Any Zone to Any Zone any traffic ← → Permit
Conduit
Zone-A
Zone-B
Zone-B
Zone-A
LAN
10.201.101.20/24
LAN
10.201.201.20/24
LAN
10.203.201.20/24
LAN
10.203.101.20/24

Figure 27

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

4. Create filter-policy template to deny TCP with destination port 23 traffic.
5. Assign filter-policy template to sites.
6. **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

Priority: 100

From Zones

Zone	Enable
Any	☑
Default_LAN_Zone	□
Internet_Zone	□
Untrusted_Internet_Zone	□

To Zones

Zone	Enable
Any	☑
Default_LAN_Zone	□
Internet_Zone	□
Untrusted_Internet_Zone	□

Action: Drop

Log Interval (s): 0

□ Log Start □ Log End

Track: Use Site Setting

IP Protocol: TCP (6)

DSCP: Any

☑ Allow Fragments ☑ Reverse Also

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

Dest Service Name: Any

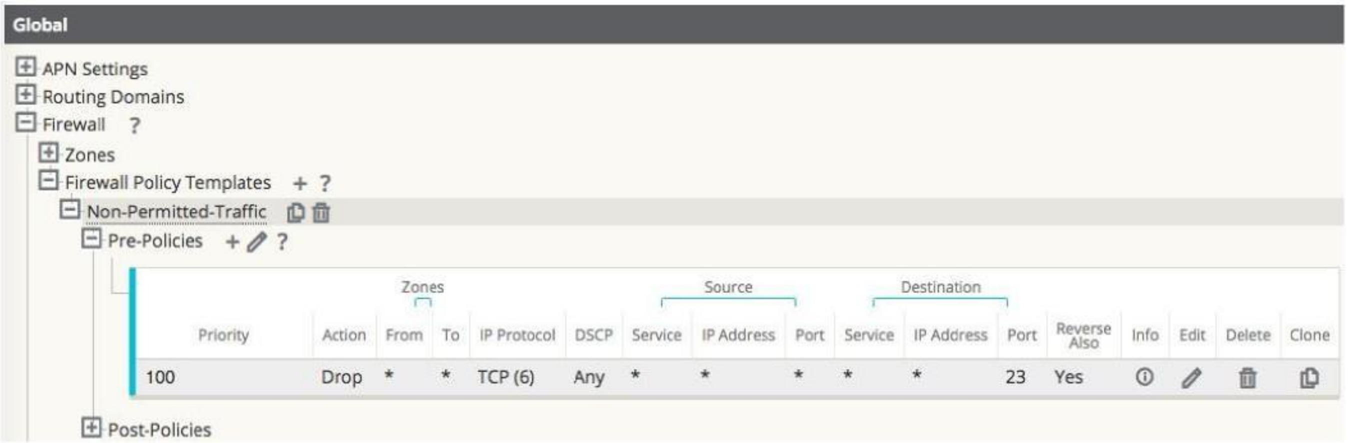
Dest IP: *

Dest Port: 23

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.

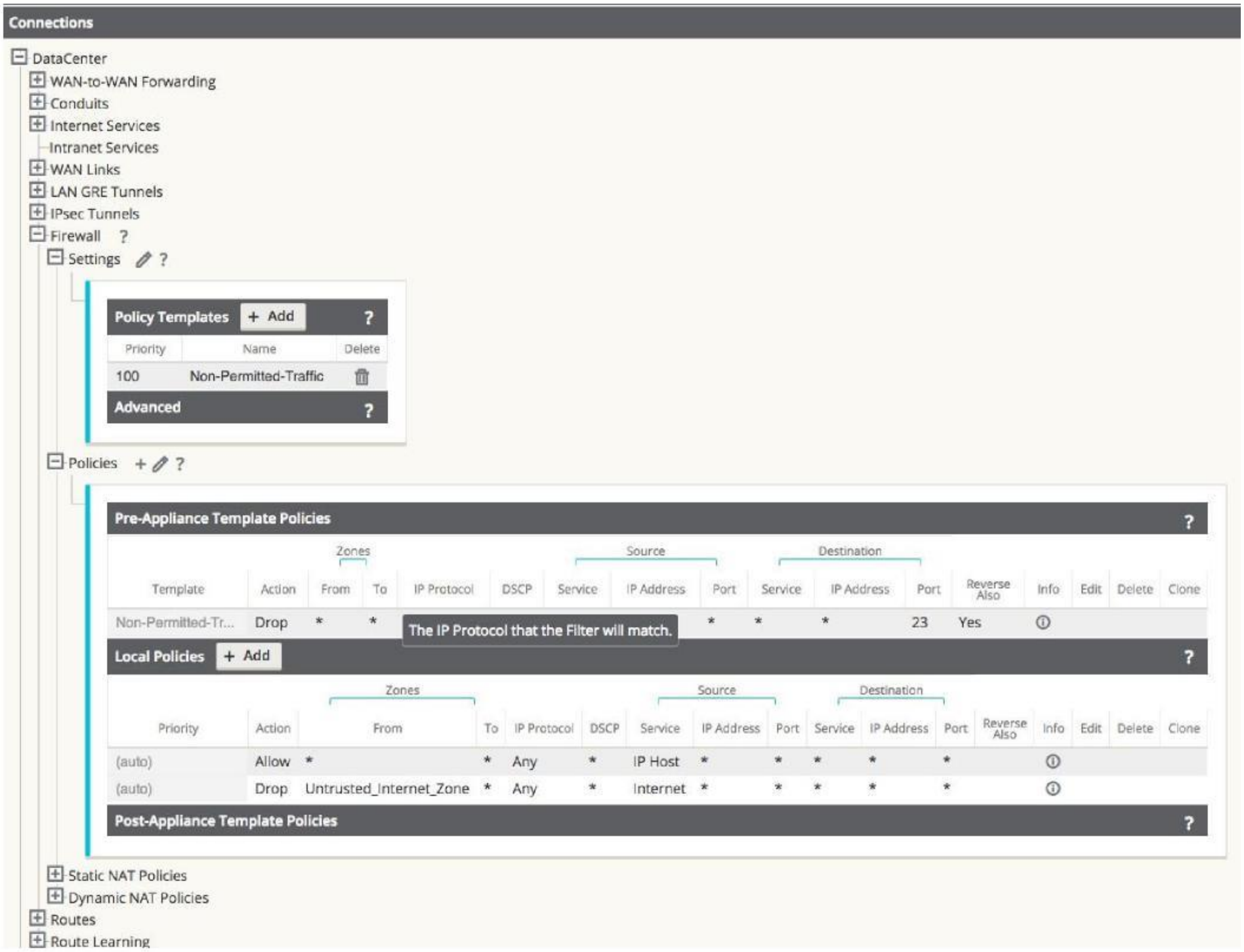
The user also has the option to make this policy Pre-Appliance, Post-Appliance, or site specific. The screen shot below displays that the user has chosen to make this policy a Global Pre-Appliance Policy.



		Zones				Source			Destination							
Priority	Action	From	To	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone
100	Drop	*	*	TCP (6)	Any	*	*	*	*	*	23	Yes	ⓘ	✎	🗑	⧉

Figure 29

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



Connections

- DataCenter
  - 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	Non-Permitted-Traffic	🗑

Advanced ?

- Policies + ?

Pre-Appliance Template Policies ?

		Zones				Source			Destination							
Template	Action	From	To	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone
Non-Permitted-Tr...	Drop	*	*					*	*	*	23	Yes	ⓘ			

The IP Protocol that the Filter will match.

Local Policies + Add ?

		Zones				Source			Destination							
Priority	Action	From	To	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone
(auto)	Allow	*	*	Any	*	IP Host	*	*	*	*	*		ⓘ			
(auto)	Drop	Untrusted_Internet_Zone	*	Any	*	Internet	*	*	*	*	*		ⓘ			

Post-Appliance Template Policies ?

- Static NAT Policies
- Dynamic NAT Policies
- Routes
- Route Learning

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.

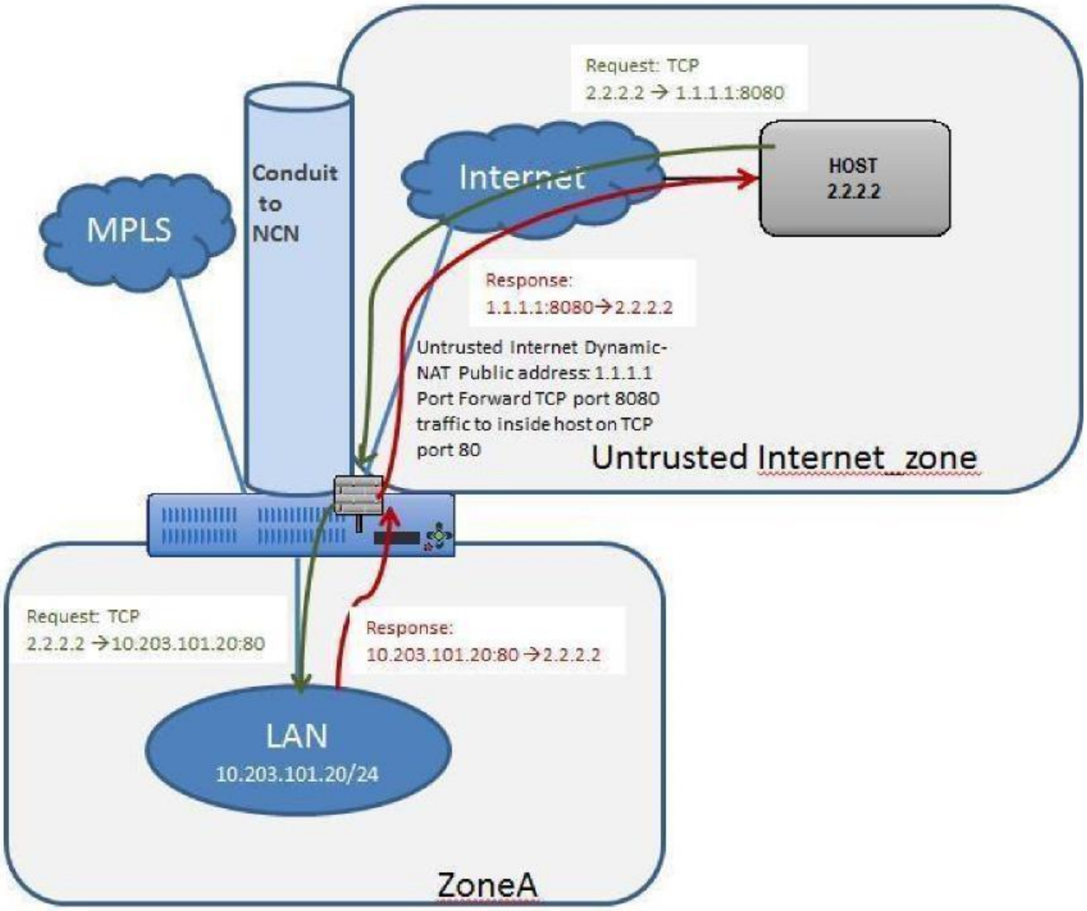


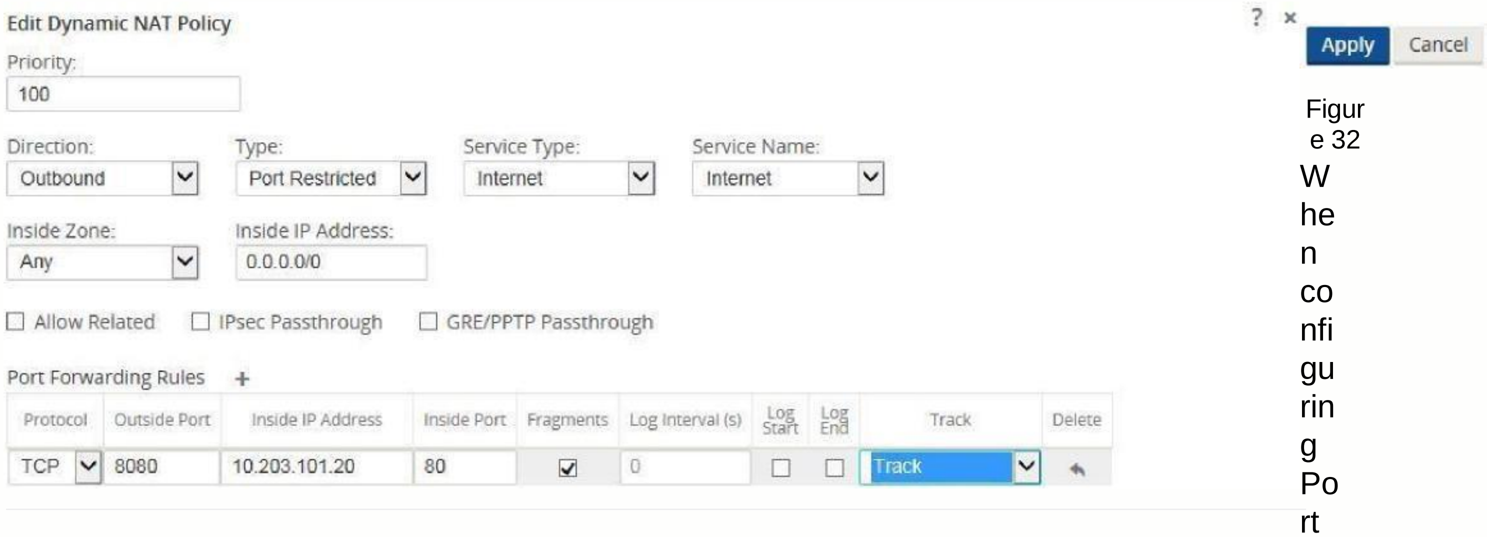
Figure 31

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

7. Define the dynamic NAT policies (PAT rule).
8. The system will add policies to allow traffic in and out for this NAT statement.
9. **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.**

e. Direction: Outbound
f. Type: Port-Restricted (Firewall can change the source port)
g. Service: Internet
h. Inside Zone:* (default)
i. Inside IP Address: * (default)
j. Outside Zone: Untrusted_Internet_Zone
k. Outside IP Address: blank
l. Port Forwards: 1
m. Outside: TCP/8080, Inside: 10.203.101.20 TCP/80



Edit Dynamic NAT Policy

Priority: 100

Direction: Outbound

Type: Port Restricted

Service Type: Internet

Service Name: Internet

Inside Zone: Any

Inside IP Address: 0.0.0.0/0

□ Allow Related □ IPsec Passthrough □ GRE/PPTP Passthrough

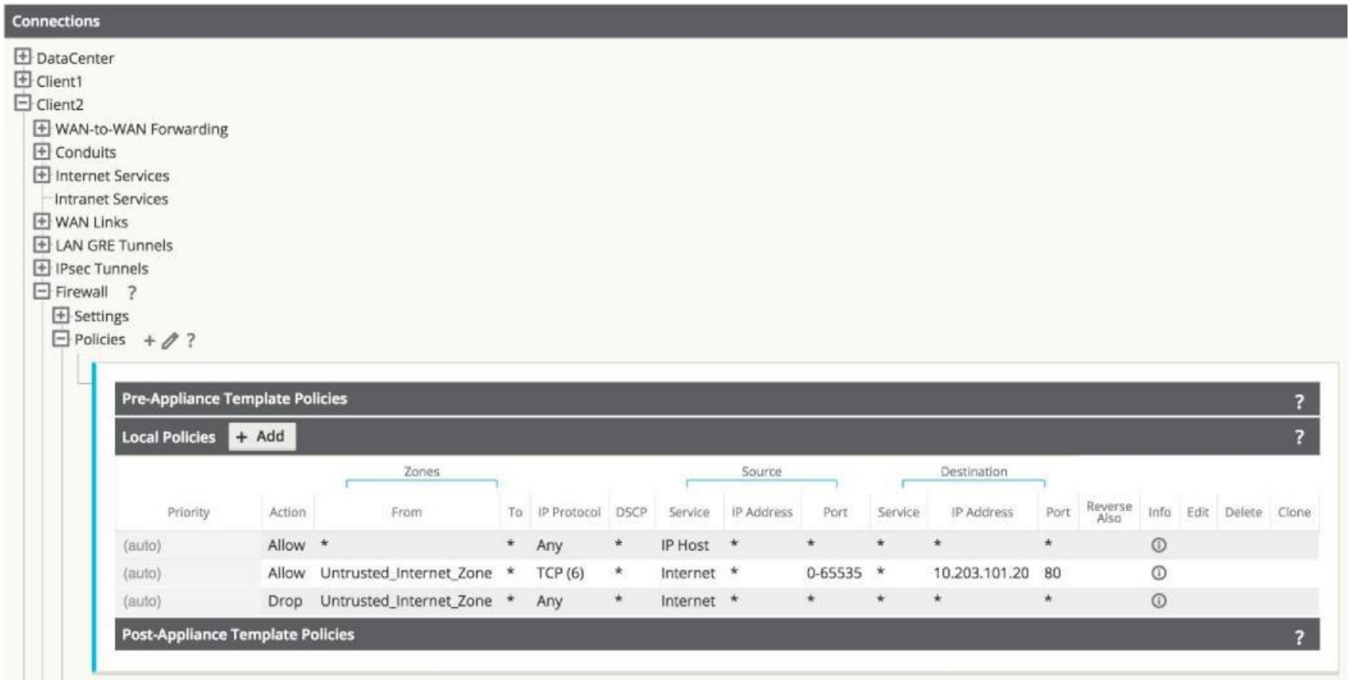
Port Forwarding Rules +

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	☑	0	□	□	Track	

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 10.203.10.20 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 Forwading Policy and should be verified by the end user under the **Policies** section.



		Zones				Source			Destination							
Priority	Action	From	To	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone
(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	*	*	*	*	*		ⓘ			

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.

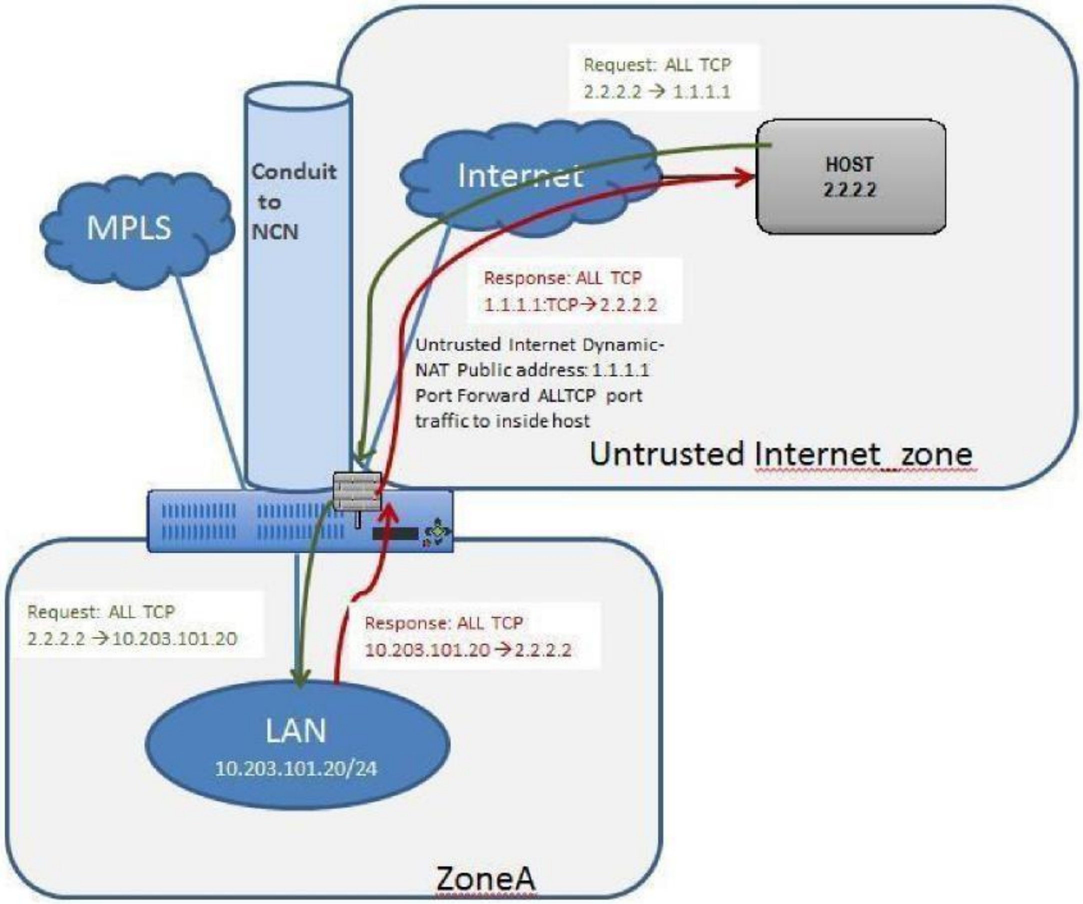


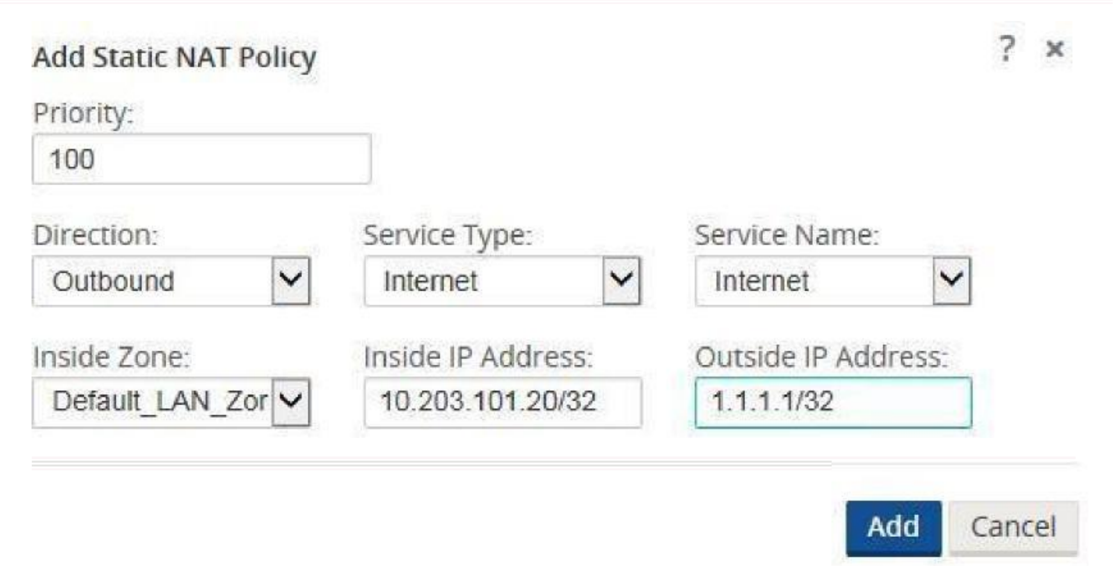
Figure 34

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

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

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

n. Direction: Outbound
o. Service: Internet
p. Inside Zone: Zone A
q. Inside IP Address: 10.203.101.20/32
r. Outside Zone: Untrusted_Internet_Zone
s. Outside IP Address: 1.1.1.1/32



Add Static NAT Policy

Priority: 100

Direction: Outbound

Service Type: Internet

Service Name: Internet

Inside Zone: Default_LAN_Zor

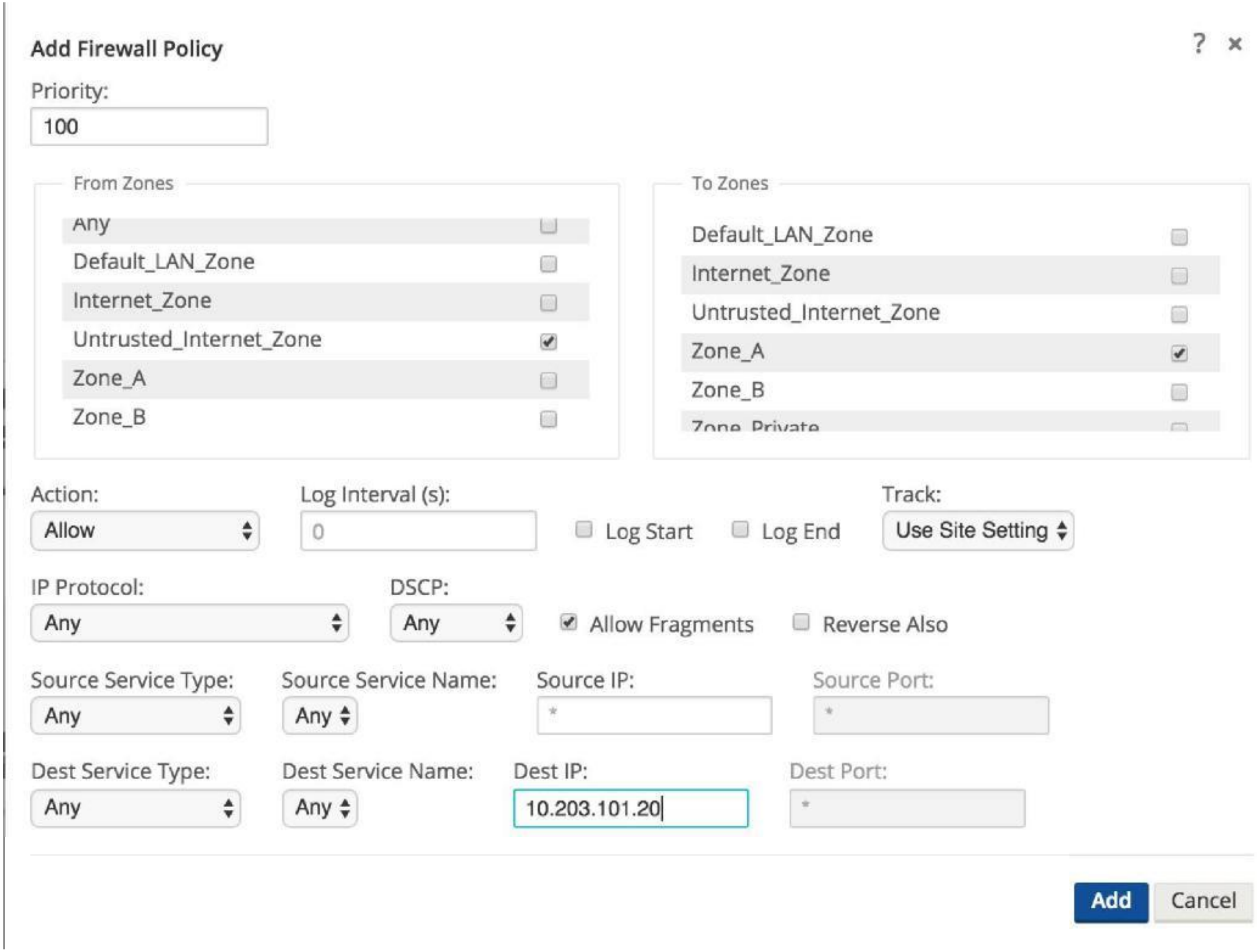
Inside IP Address: 10.203.101.20/32

Outside IP Address: 1.1.1.1/32

Figure 35

Users will nagivate 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

Priority: 100

From Zones

- Any ☐
- Default_LAN_Zone ☐
- Internet_Zone ☐
- Untrusted_Internet_Zone ☑
- Zone_A ☐
- Zone_B ☐

To Zones

- Default_LAN_Zone ☐
- Internet_Zone ☐
- Untrusted_Internet_Zone ☐
- Zone_A ☑
- Zone_B ☐
- Zone_Private ☐

Action: Allow

Log Interval (s): 0

☐ Log Start ☐ Log End

Track: Use Site Setting

IP Protocol: Any

DSCP: Any

☑ Allow Fragments ☐ Reverse Also

Source Service Type: Any

Source Service Name: Any

Source IP: *

Source Port: *

Dest Service Type: Any

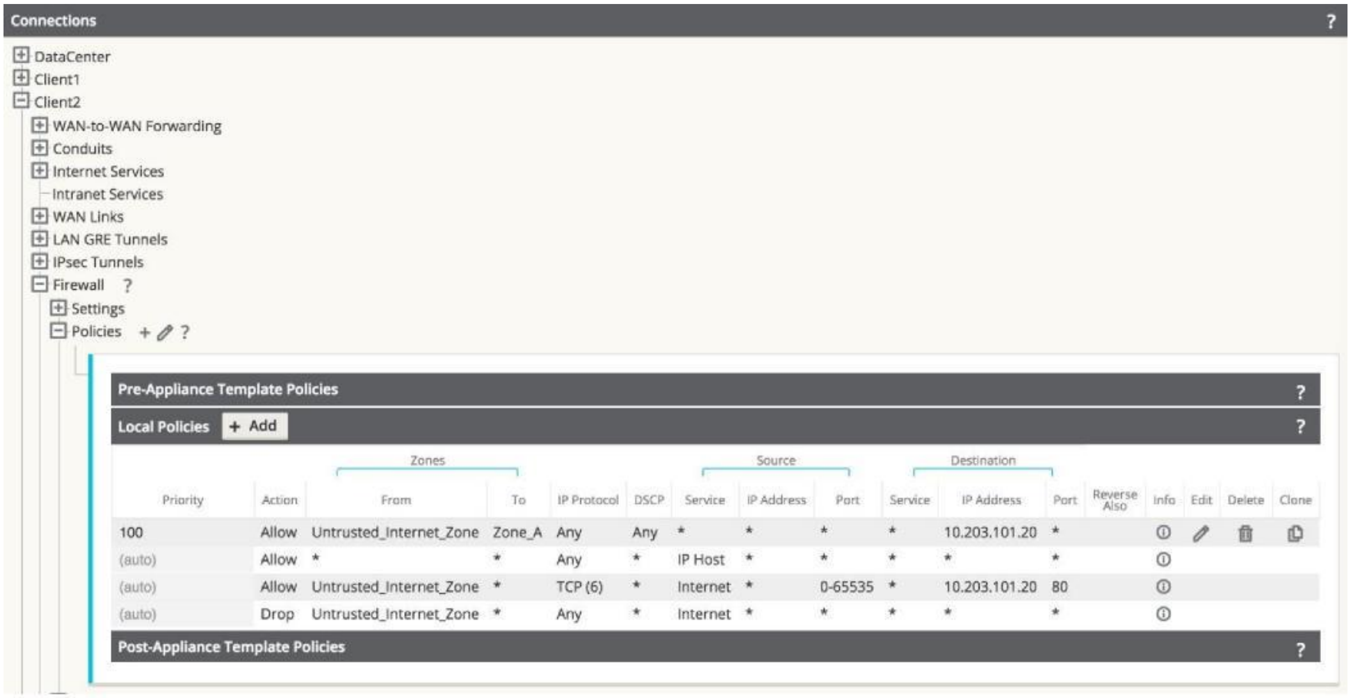
Dest Service Name: Any

Dest IP: 10.203.101.20

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 Talari 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.



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 ?

		Zones				Source			Destination							
Priority	Action	From	To	IP Protocol	DSCP	Service	IP Address	Port	Service	IP Address	Port	Reverse Also	Info	Edit	Delete	Clone
100	Allow	Untrusted_Internet_Zone	Zone_A	Any	Any	*	*	*	*	10.203.101.20	*		ⓘ	✎	🗑	⧉
(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 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.

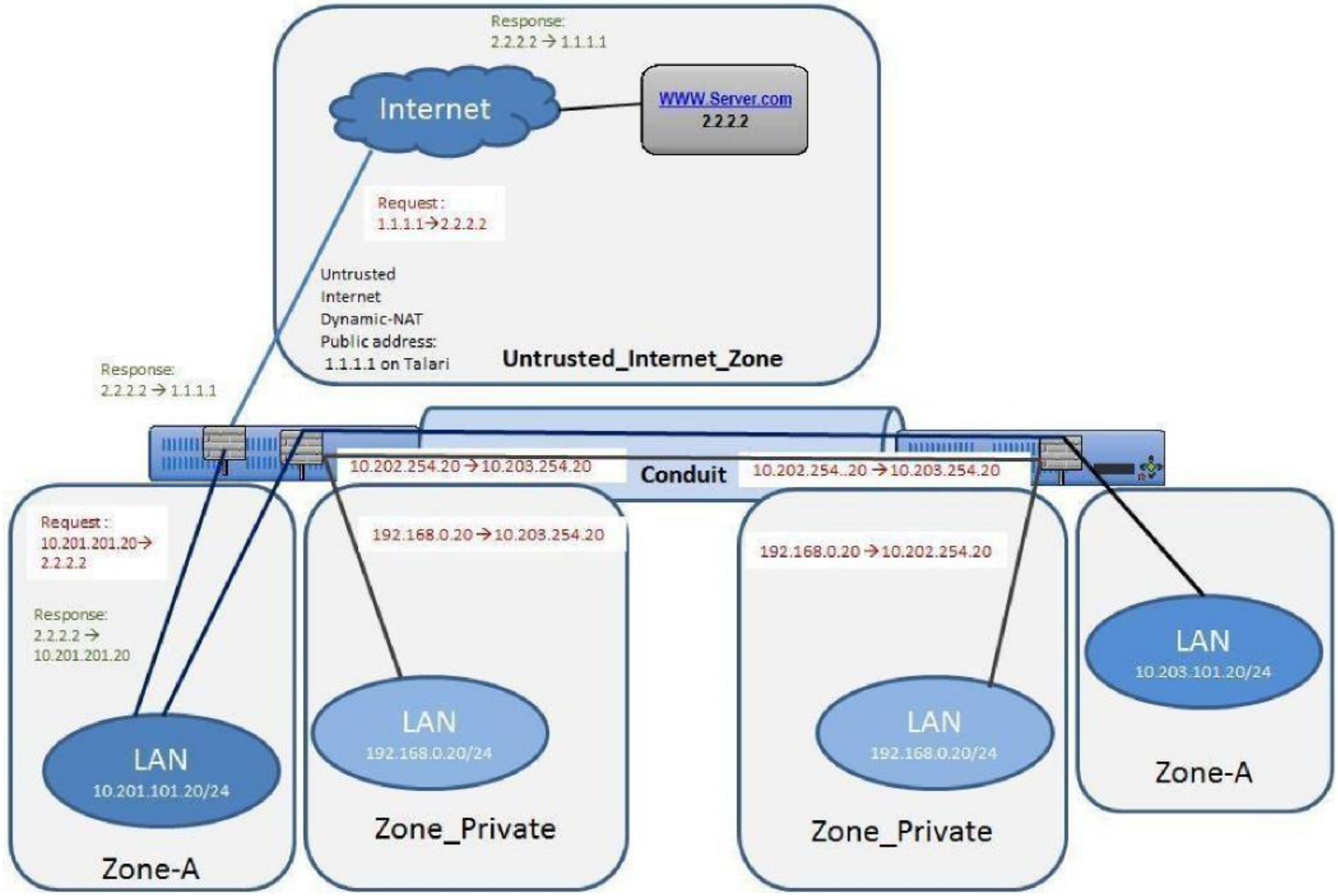
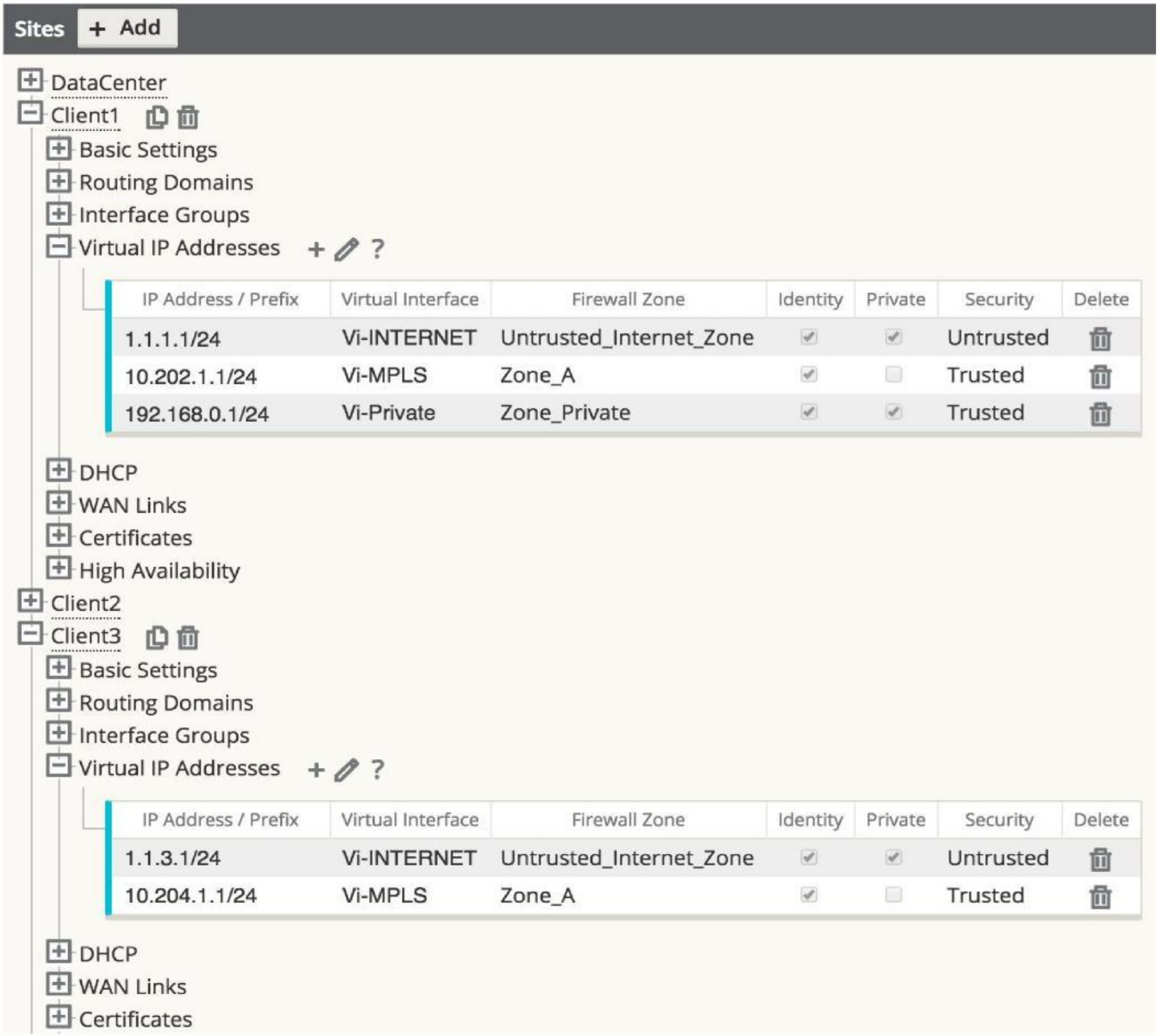


Figure 39

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

7. Set Private Zone interfaces as Private under VIP configuration.
8. Define the static NAT Policy (one-to-one) – Branch Office 1.
9. Define the static NAT Policy (one-to-one) – Branch Office 2.
10. Define the dynamic NAT Policy (PAT) – Both Offices.
11. **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.



Sites + Add

- ⊞ DataCenter
- ⊟ Client1
  - ⊞ Basic Settings
  - ⊞ Routing Domains
  - ⊞ Interface Groups
  - ⊟ Virtual IP Addresses + ?

IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
1.1.1.1/24	Vi-INTERNET	Untrusted_Internet_Zone	☑	☑	Untrusted	🗑
10.202.1.1/24	Vi-MPLS	Zone_A	☑	☐	Trusted	🗑
192.168.0.1/24	Vi-Private	Zone_Private	☑	☑	Trusted	🗑

  - ⊞ DHCP
  - ⊞ WAN Links
  - ⊞ Certificates
  - ⊞ High Availability
- ⊞ Client2
- ⊟ Client3
  - ⊞ Basic Settings
  - ⊞ Routing Domains
  - ⊞ Interface Groups
  - ⊟ Virtual IP Addresses + ?

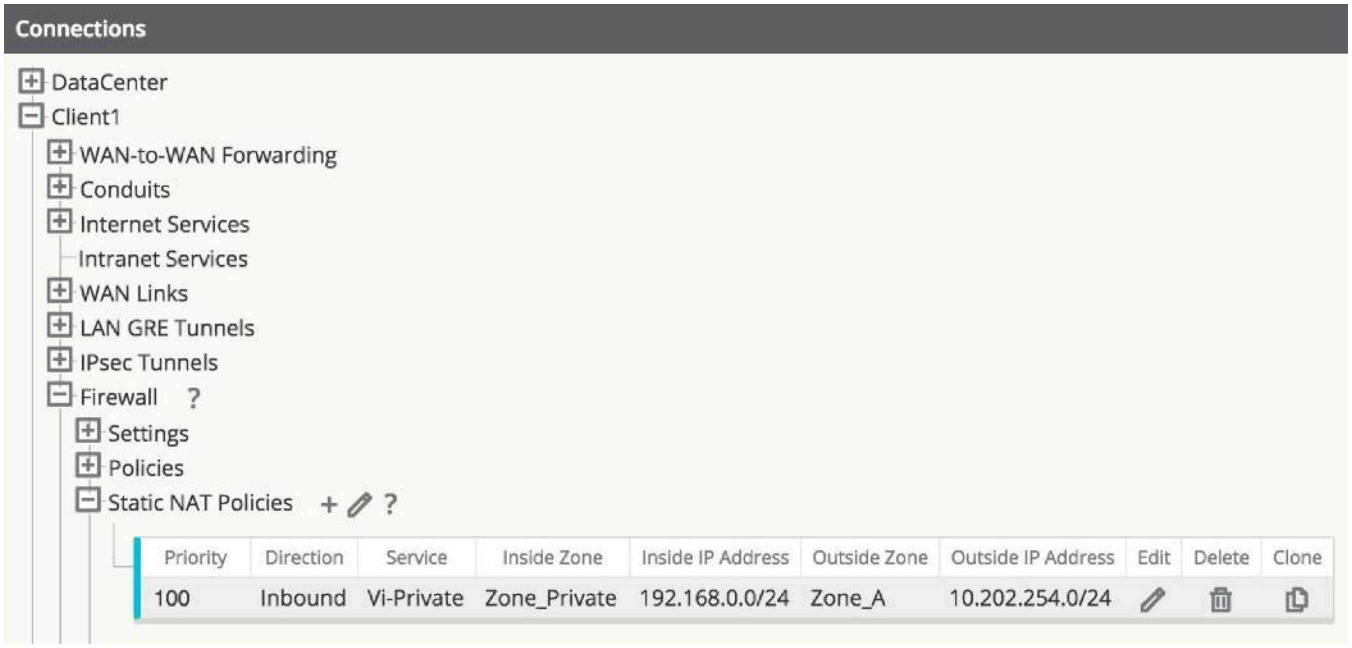
IP Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security	Delete
1.1.3.1/24	Vi-INTERNET	Untrusted_Internet_Zone	☑	☑	Untrusted	🗑
10.204.1.1/24	Vi-MPLS	Zone_A	☑	☐	Trusted	🗑

  - ⊞ DHCP
  - ⊞ WAN Links
  - ⊞ Certificates

Figure 40

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

t. Direction: Inbound
u. Service: Local
v. Inside Zone: Zone_ Private
w. Inside IP Address: 192.168.0.0/24
x. Outside Zone: Zone_A
y. Outside IP Address: 10.202.254.0/24



Connections

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

Priority	Direction	Service	Inside Zone	Inside IP Address	Outside Zone	Outside IP Address	Edit	Delete	Clone
100	Inbound	Vi-Private	Zone_Private	192.168.0.0/24	Zone_A	10.202.254.0/24	✎	🗑	⧉

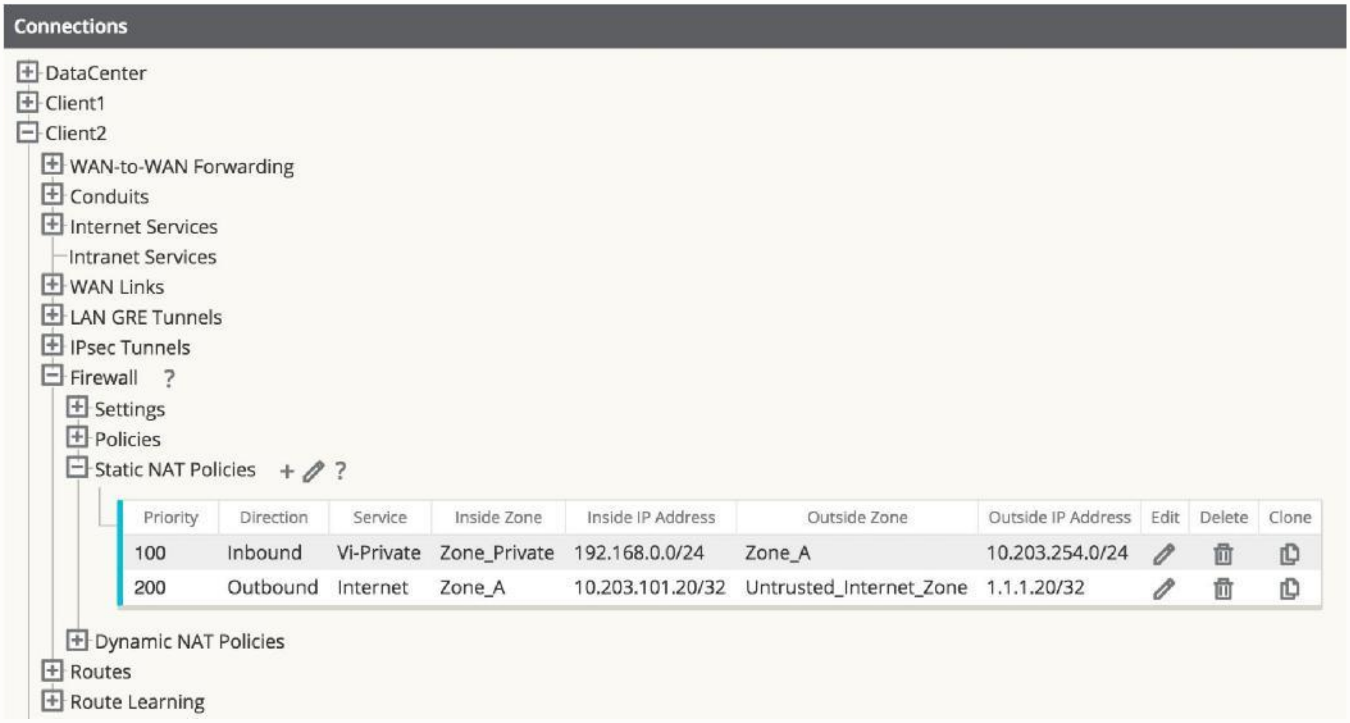
Figure 41

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.

z. Direction: Inbound
aa. Service: Local
bb. Inside Zone: Zone_ Private
cc. Inside IP Address: 192.168.0.0/24
dd. Outside Zone: Zone_A
ee. Outside IP Address: 10.203.254.0/24



Connections

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

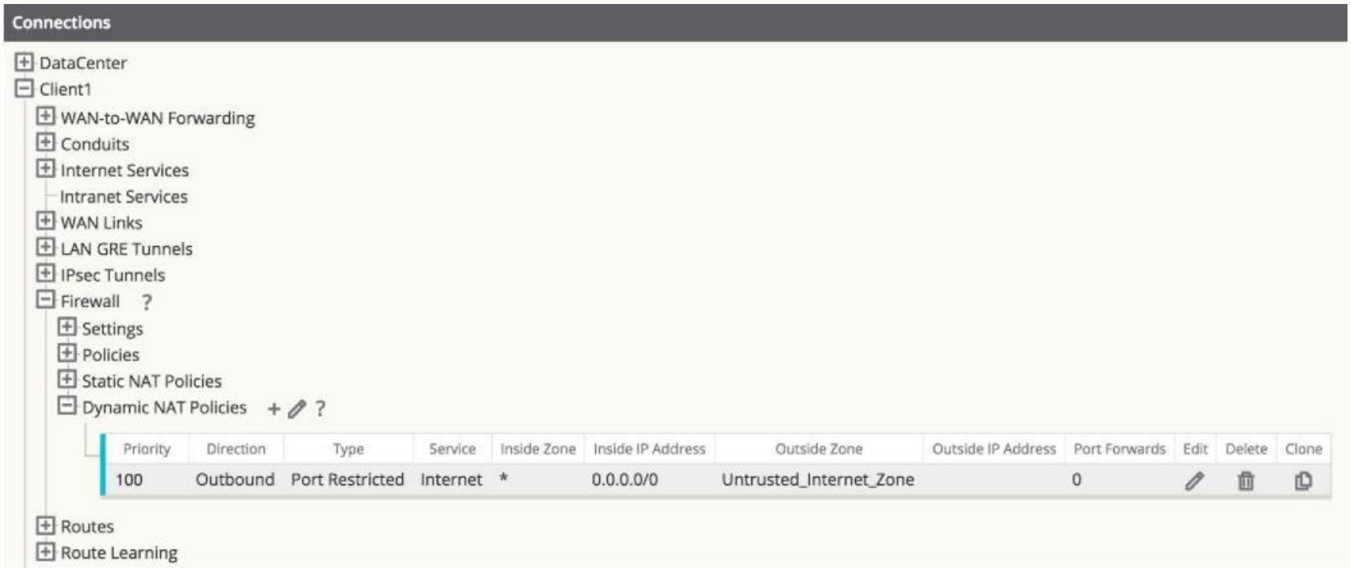
Priority	Direction	Service	Inside Zone	Inside IP Address	Outside Zone	Outside IP Address	Edit	Delete	Clone
100	Inbound	Vi-Private	Zone_Private	192.168.0.0/24	Zone_A	10.203.254.0/24	✎	🗑	⧉
200	Outbound	Internet	Zone_A	10.203.101.20/32	Untrusted_Internet_Zone	1.1.1.20/32	✎	🗑	⧉

- ⊞ Dynamic NAT Policies
- ⊞ Routes
- ⊞ Route Learning

Figure 42

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

ff. Direction: Outbound
gg. Type: Port-Restricted (FW can change the source port)
hh. Service: Internet
ii. Inside Zone:* (default)
jj. Inside IP Address: * (default)
kk. Outside Zone: Untrusted_Internet_Zone
ll. Outside IP Address: blank
mm. Port Forwards: 0



Connections

- ⊞ DataCenter
- ⊟ Client1
  - ⊞ 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 + ✎ ?

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	✎	🗑	⧉

- ⊞ Routes
- ⊞ Route Learning

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.**

Summary

The Talari Firewall Configuration Guide provides example configuration topologies that users can reference as a guide on how to configure the Talari firewall for defined topologies. This is not a exhaustive list of use cases, but they are the most common at the time this document was created. Additional use cases and topologies will be added in the future.