Oracle® SD-WAN Chaining with Palo Alto Networks NGFW

Installation Guide

Original Publication Date: Nov 1, 2019

Table of Contents

About This Document

The purpose of this document is to provide the reader with an understanding of how to install a Talari Appliance with Virtual Palo Alto Networks NGFW. The Palo Alto Networks NGFW will be installed using the Service Chaining capability of the Talari E100 or Talari E1000 platform.

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 documents are available:

- *Talari Service Chaining UI Installation GUI*
- *Talari 6.1 New Feature Guide*

Introduction

In this installation guide, we will explore how to integrate a native Talari and the Palo Alto Networks NGFW (Next Generation Firewall) as a Guest VM on a Talari Appliance. The hypervisor being used for this Service Chaining is the KVM hypervisor. The Talari solution is a next-generation SD-WAN architecture which supports the Service Chaining capability. This capability allows the Talari Application to run natively while also supporting a Guest VM. The combined next-generation security with SD-WAN and branch office network simplification solution will provide a virtual service chained architecture which delivers the highest performance required by networks today, while also increasing reliability, performance, and security.

Talari has expanded support for service chaining from the E100 appliance to a higher performance appliance, the Talari E1000. For larger sites, Talari recommends that customers use the E1000 appliance. Contact your Talari representative for conduits performance levels for these platforms. Configuration of the E100 appliance and the E1000 appliance is the same from a user perspective. The two Talari Models have the following properties from a resource and OS perspective:

Model	VCPUs	Memory Maximum	QEMU Version	Libvirt Version
E100	2	10GB	2.1.2	1.2.9
E1000	2	16GB	2.1.2	1.2.9

Note: Talari OS 5.0 and OS 5.1 support the above QEMU and libvirt versions. These are compatible with the Palo Alto Next Generation Firewall requirements.

Interaction Between the Talari Appliance and Palo Alto Networks NGFW

The Talari SD-WAN is a two-ended solution. The Talari Appliances use a proprietary encrypted encapsulation (Talari Reliable Protocol - TRP) for data traversal between appliances, which enables a unique per-packet routing feature across multiple WAN Links simultaneously.

The Palo Alto Networks Solution brings next-generation security through its one-of-akind, multi-layered defense model, preventing threats at each stage of the attack life cycle.

The data shared between the Talari Appliance and Palo Alto Networks NGFW will be dependent on the customer requirement.

Here we will go over two example solutions. In Customer Solution #1, branch office

Internet-bound traffic uses the Internet WAN Link local to the site. The Internet traffic needs to be secure. The user traffic will be received first by the Talari Appliance and then by the Palo Alto Networks NGFW.

In Customer Solution #2, the user needs to inspect and secure all data from the branch prior to sending data via the Private or Public WAN. The user traffic is received by the Palo Alto Networks NGFW then forwarded (based on security parameters) to the Talari Appliance.

Customer Solution #1

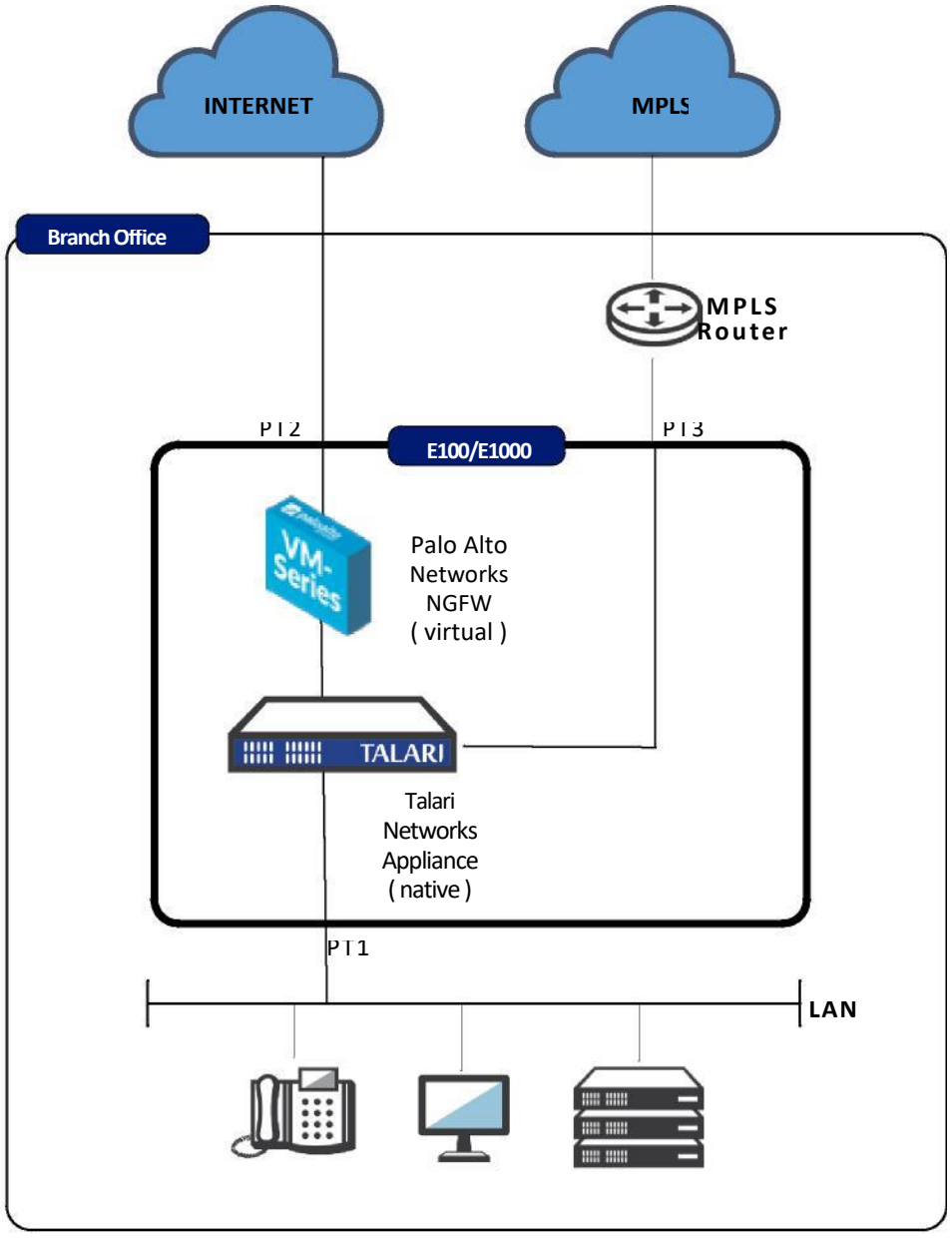

Figure 1

The Talari Appliance will send Internet-bound data packets (Salesforce, Dropbox, etc.) to the Palo Alto Networks NGFW for NAT and other security features to create secure, direct Internet access. The Palo Alto Networks NGFW will also be providing NAT for the encrypted encapsulated Talari Reliable Protocol packets traversing the Internet link to other Talari sites.

In the configuration defined above, the Talari Appliance will operate in Fail-to-Block mode. This will provide additional security in the event there is a Talari Appliance failure and not allow Internet traffic to reach the LAN segment. The Talari Appliance will have an IP address and port assigned to the Internet WAN Link, and the Palo Alto Networks NGFW will have an interface, IP address, and zone assigned for the LAN. The Palo Alto Networks NGFW LAN port and Talari WAN port will reside on the same Layer 3 subnet and the ports will connect via Linux bridge commands.

From the Talari Appliance perspective, the Palo Alto Networks NGFW LAN interface is configured as the gateway for the Internet link. All traffic that must be routed to the Internet WAN Link will be sent to the Palo Alto Networks NGFW as the next-hop gateway. Within the Talari Appliance configuration, we have also turned on Auto-Detect Public IP for the branch site, so the Public IP is disseminated to other connected Talari Appliances for TRP exchange.

From the Palo Alto Networks NGFW perspective, the Talari Appliance is the LAN gateway next-hop. All traffic to be routed to the LAN must be sent to the Talari Appliance's IP address representing the Internet link. The Talari Appliance acts as a next-hop router.

As packets are flowing from the LAN to the WAN the Talari Appliance is making perpacket routing decisions based upon application and link quality (loss, latency, jitter, and bandwidth) for LAN traffic destined for Talari-enabled sites. Between Talari sites, the customer is now able to duplicate voice packets and send them on separate WAN Links to increase reliability, mitigate loss by tracking individual packet transmits and arrivals while resending lost packets, use latency-aware Load Balancing so a large packet flow such as a data backup can use multiple links simultaneously, and perform sub-second failover to avoid black-outs and brown-outs. The Palo Alto Networks NGFW brings peace of mind knowing the Internet bound traffic has next-generation security in place keeping a watchful eye on packets, ensuring secure transmission.

Customer Solution #2

The data path flow will be different when the user needs to inspect and secure all data from the branch prior to sending data via the MPLS or Internet WAN Links. In this scenario, the user must secure all LAN traffic, regardless of destination.

The Palo Alto Networks NGFW is the default gateway for the LAN. Traffic will be inspected by the firewall and, based on the policies defined, it will either be permitted or denied from entering the network. Traffic to the Private WAN will be forwarded to the Talari Appliance. The Talari Appliance will then make the per-packet routing decision by sending the encrypted encapsulated data packet either through the MPLS WAN Link or back towards the Palo Alto Networks NGFW to be forwarded on through the Internet WAN Link.

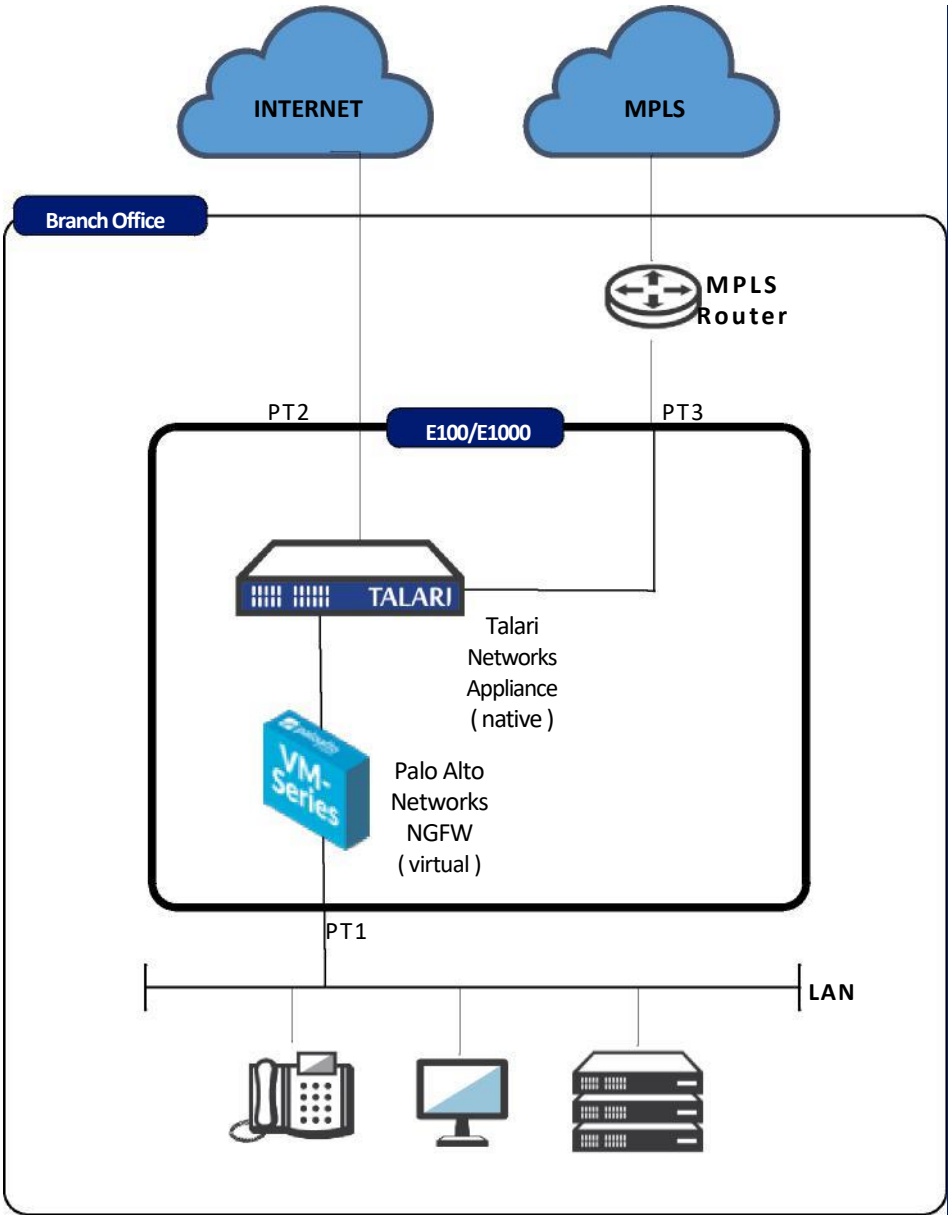

Figure 2

The Talari Appliance will have an IP address and port assigned to the Internet WAN Link and MPLS Link. The Talari Internet WAN Link port will connect to the Palo Alto Networks NGFW. The Palo Alto Networks NGFW will have an interface and IP address assigned for the LAN traffic. There will also be separate interfaces, IP addresses, and zones assigned for the external facing Internet port and the port connected to the Talari Appliance (for outbound and inbound Private WAN traffic), as well as for the encapsulated encrypted TRP packets sourced and destined for the Internet from the Talari Appliance. The Palo Alto Networks NGFW and Talari Appliance ports' IP addresses will reside on the same Layer 3 subnet and the ports will connect via a Linux bridge created within the installation of the Guest VM.

From the Talari Appliance perspective, the Palo Alto Networks NGFW Private WAN interface IP address is configured as the gateway for the Internet WAN Link and the gateway for LAN traffic. Within the Talari Appliance configuration, we have also turned on Auto-Detect Public IP for the branch site so the Public IP is disseminated to other connected Talari Appliances for TRP exchange.

From the perspective of the Palo Alto Networks NGFW, the Talari Appliance is the Private WAN gateway next-hop. All traffic to be routed to the Private WAN must be sent to the Talari Appliance's IP address representing the MPLS Link. The Talari Appliance acts as a next-hop router and will also be sending TRP packets to and from this zone to the Internet to send packets across the Internet Link.

The result of this solution is the Palo Alto Networks NGFW is providing full suite nextgeneration security measures to all data passing through the site's network. Fully secure packets are now flowing from the LAN to the WAN, and the Talari Appliance is making per-packet routing decisions based upon application and link quality (loss, latency, jitter, and bandwidth) for LAN traffic destined for remote Talari-enabled sites. Between Talari sites, the customer is now able to duplicate voice packets and send them on separate WAN Links to increase reliability, mitigate loss by tracking individual packet transmits and arrivals while resending lost packets, use latency-aware Load Balancing so a large packet flow such as a data backup can use multiple links simultaneously, and perform sub-second failover to avoid black-outs and brown-outs.

Packets destined for Public Internet will be inspected and have NAT performed, while packets destined for Private WAN will be forwarded from the firewall to the Talari Appliance and then encapsulated in the Talari Conduit. The Talari paths will utilize both the MPLS and the Internet WAN Links.

Functional Business Requirements

This solution is for users seeking to deploy Palo Alto Networks next-generation security with the addition of more bandwidth for less cost, improved performance, and exceptional reliability that a Talari SD-WAN and branch office network simplification solution brings to the table.

Note: Although the diagrams depict a Hybrid WAN environment, Talari can run on Internet only or MPLS only environments.

The use case can be tested within a lab environment by creating two distinct sites with the Talari E100 or E1000 and the Palo Alto Networks NGFW. Set up a WAN simulation tool between the two sites to represent the clouds and mimic the impact of loss, latency, jitter fluctuations, as well as black-out and brown-out conditions on the separate WAN Links. Create a VM to represent potential Internet traffic.

The use case can also be tested within real world environments.

Success is defined as providing a next-generation security to sites and communication across the WAN while increasing bandwidth, performance, and reliability.

Description of the Test Environment

The Talari Appliance E100 running Release 6.1 GA P2 has been proven to interoperate with the Palo Alto VM-300 Guest VM running 8.0 software. Because of the resources available on the Talari E100 the recommended Palo Alto Networks vm is the VM-200 or VM-100.The E1000 is a higher performance Talari appliance and can support the resource requirements of the Palo Alto Networks VM-300. The release running on the Talari E1000 Appliance is 7.0 GA P2.

The solution is running on the Talari Appliances with the Talari Application in native mode while the Palo Alto Networks NGFW is running as a Guest VM on KVM.

Upon installation, the Talari software will create the required bridge infrastructure for the appropriate connectivity.

Test Plan and Results

The test plan will cover reliability, performance, failover, and security. Test cases will require a minimum of 2 sites for the Talari solution to operate. The Palo Alto Networks NGFW only needs to be deployed at one site to show functionality, for example, just the branch office.

Success Criteria

1. Performance - If no traffic is running between sites, send a single data flow (iperf, FTP, etc.) to the other site. A single flow should generate 80% or greater of the combined WAN Links' bandwidth.
2. Reliability - Identify a flow and the WAN Link the flow is traversing (using the Talari GUI via **Monitor > Flows**) then pull the cable. The session should not drop.
3. Failover - Have a voice call running between sites and pull the cable of the WAN Link identified in the Flows Table. The voice call should not drop.
4. Security - Create a policy on the Palo Alto Networks NGFW to deny a certain traffic flow. Send this specific type of traffic flow and observe the flow should fail.

Steps for Integration

The E100 should be deployed with APN software 6.1 GA P2 or higher. The E1000 should be deployed with APN software 7.0 GA P2 or higher. At this point, the user can

configure and deploy the Service Chaining Guest VM. The Talari Service must be disabled to allow the user to deploy the Service Chaining Guest VM.

1. Download the Palo Alto Networks NGFW VM image for KVM (qcow2 image).
2. Download the Palo Alto Networks NGFW XML file. The files are labeled LAN or WAN in the file name to indicate what side of the Talari Application the user is installing the Palo Alto Networks NGFW.
3. Upload both the image file and XML through the Talari Service Chaining web page on the branch office appliance.
4. Access the console interface of the Palo Alto Networks NGFW to assign an IP address for GUI configuration.

Customer Solution #1 Installation

The branch office Internet bound traffic uses the Internet WAN Link local to the site. The customer needs to secure Internet traffic.

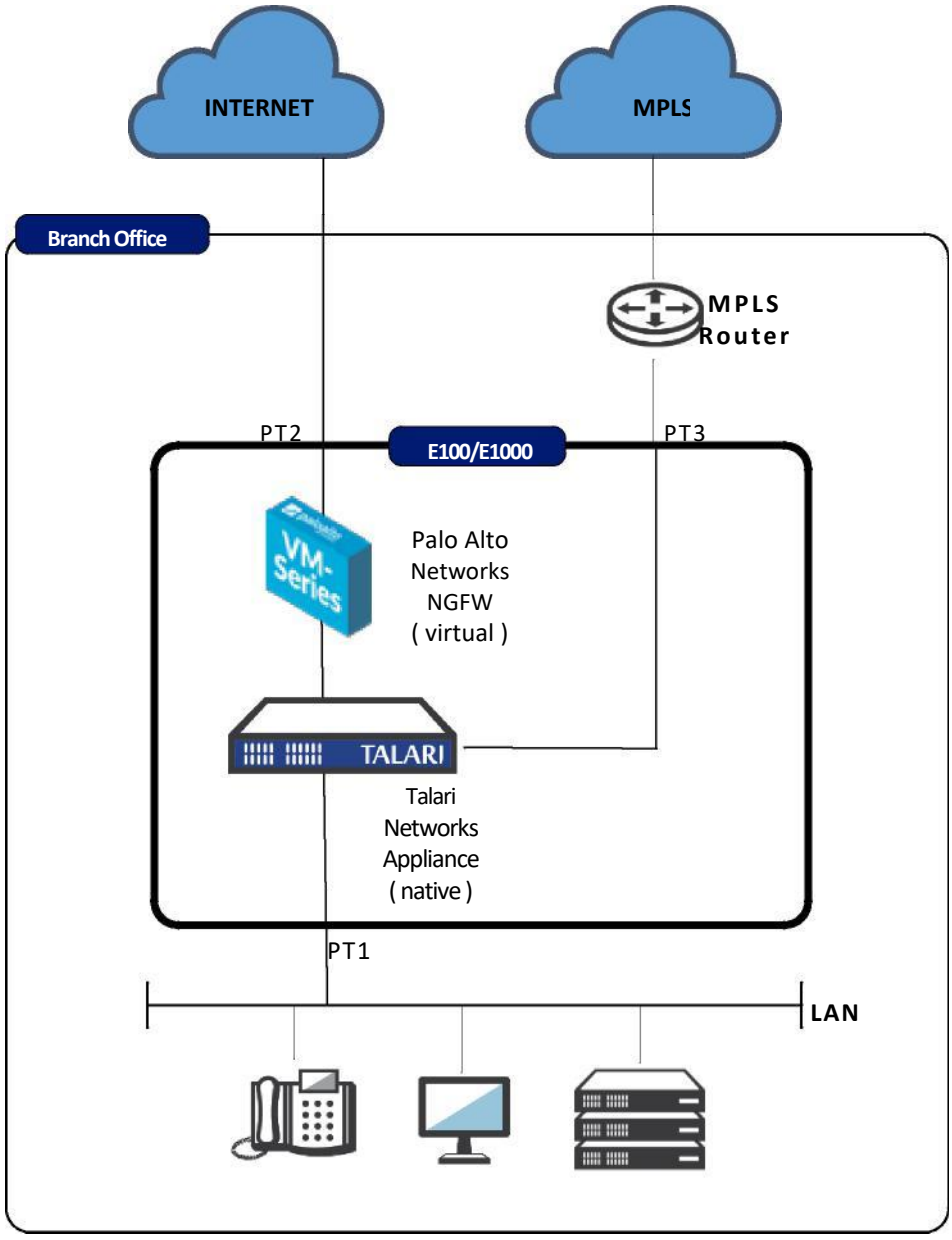

Figure 3

In this scenario, we will assume the Talari Appliance is configured and reachable via an IP address on the Management port. We can the log into the Web UI and install the Palo Alto Networks VM on the WAN side of the Talari Appliance.

Login into the appliance and go to **Integrate > Service Chaining** tab.

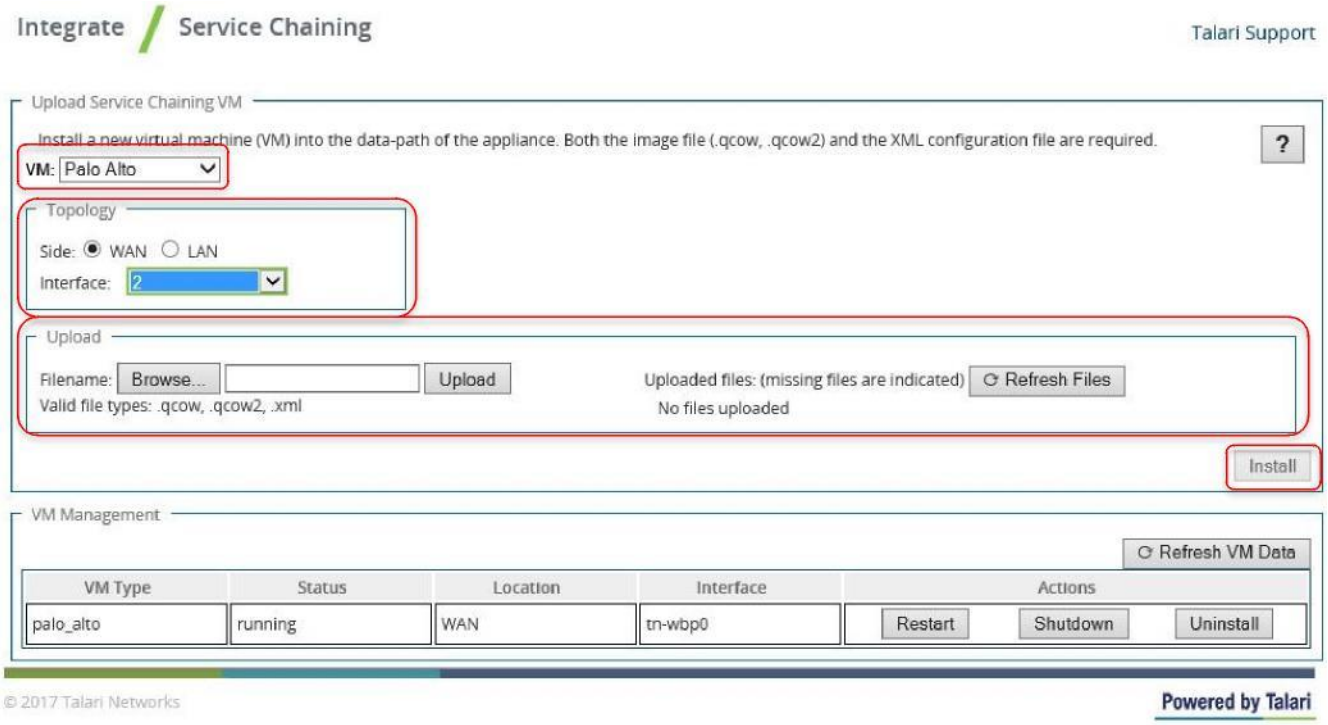

Figure 4

P erform the following:

- Select the VM
- Select the Topology ○ WAN
  - LAN
  - Select the Interface for the topology
- Upload the required files ○ Image
  - XML

The example in Figure 4 shows the user selecting the following options to install the Palo Alto Networks VM on the LAN side of the Talari Application.

- VM – Palo Alto
- Topology – WAN
- Interface – 2

Once the files have uploaded, select the install button. If the correct files have not been uploaded, the Install button is greyed out. Once the user selects the install button, the system will prompt the user with two questions:

- Insert the VM into the Data Path

- Setup management for the VM

Select OK to both questions and allow the system to install the Palo Alto Networks VM.

Once the VM is installed, the user can configure a Management IP address and complete the Palo Alto Networks configuration via the GUI interface.

Now that the Guest VM is up and operational, the user must configure it. Steps to gain access to the console interface are as follows.

- SSH into the Talari appliance using an X Windows interface, such as X11 forwarding, using these credentials:
  - Username: talariuser ○ Password: talari
- Issue the command **vncviewer**

Note: The Guest VM must be running for this step to work as expected.

- Once the VNC Viewer popup window appears, hit enter – no password is required.

Figure 5

The Guest VM
console will then appear in the X11 session window. The user may now configure the Palo Alto Networks IP management commands to access the Web interface of the Palo Alto Networks NGFW. To do this, login to the CLI of the Palo Alto Networks NGFW. Issue the following sequence of commands to assign an IP address, gateway, and DNS Server IP to the management interface of the Palo Alto Networks NGFW: admin@PA-VM>**configure** admin@PA-VM#**show** (to view the current configuration) admin@PA-VM# **set deviceconfig system ip-address 1.1.1.1 netmask 255.255.255.0 default-gateway 1.1.1.5 dns-setting servers primary 1.1.1.50**

IP address - 1.1.1.1

Gateway - 1.1.1.5

DNS server - 1.1.1.50

admin@PA-VM#**commit** (which allows the change to take effect) admin@PA-VM#**exit**

admin@PA-VM>**ping host 1.1.1.100** (a host on the external LAN network)

Once you have verified an external host is reachable, use the GUI interface of the Palo

Alto Networks NGFW to complete the configuration.

Note: When using Palo Alto Networks software 8.0 dhcp must be disabled on the management port. The command required is: set deviceconfig system type static

Customer Solution #2 Installation

The branch office Internet-bound traffic uses the Internet WAN Link local to the site. The user traffic is inspected by the Palo Alto Networks NGFW prior to any Talari Service (Conduit or Internet).

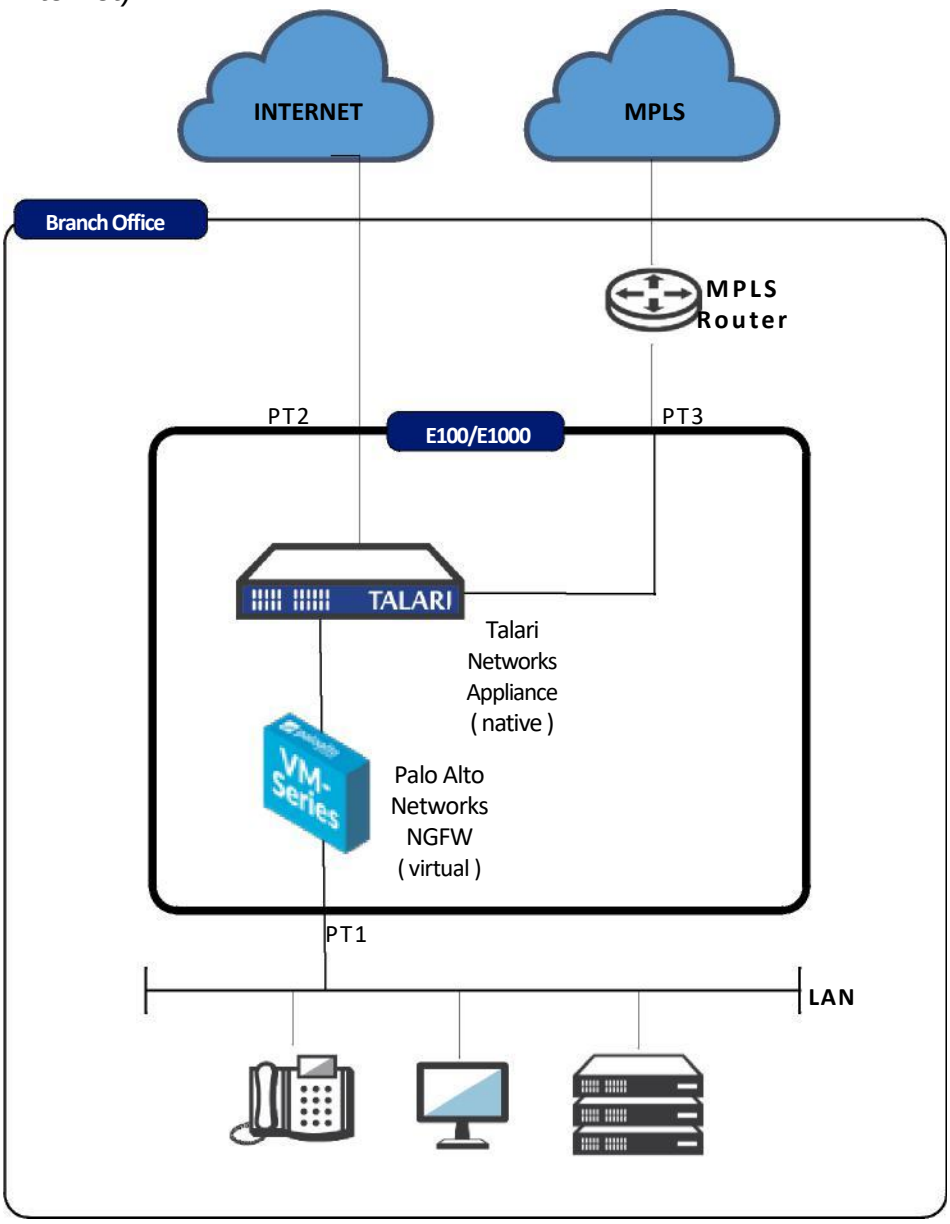

Figure 6

In this scenario, we will assume the Talari Appliance is configured and reachable via an IP address on the Management port. We can the log into the Web UI and install the Palo Alto Networks VM on the LAN side of the Talari Appliance.

Login into the appliance and go to **Integrate > Service Chaining** tab.

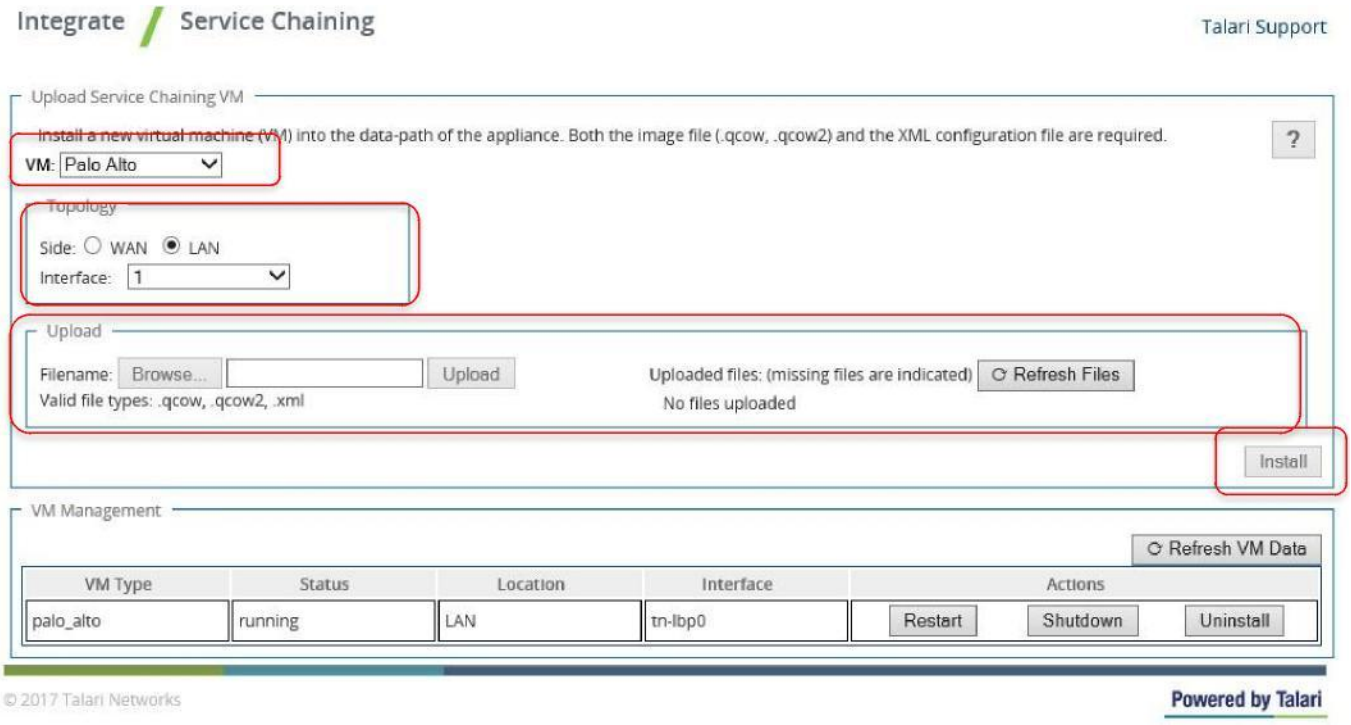

Figure 7

Perform the following:

- Select the VM
- Select the Topology ○ WAN
  - ○ LAN
  - ○ Select the Interface for the topology
- Upload the required files ○ Image ○ XML

The example in Figure 7 shows the user selecting the following options to install the Palo Alto Networks VM on the LAN side of the Talari Application.

- VM – Palo Alto
- Topology – LAN
- Interface – 1

Once the files have uploaded, select the install button. If the correct files have not uploaded, the install button is greyed out. Once the user selects the install button, the system will prompt the user with two questions:

- Insert the VM into the Data Path
- Setup management for the VM

The user should select OK to both questions and allow the system to install the Palo Alto Networks VM.

Once the VM is installed, the user can configure a Management IP address and complete the Palo Alto Networks configuration via the GUI interface.

Now that the Guest VM is up and operational, the user must configure it. Steps to gain access to the console interface are as follows.

- SSH into the Talari applaince using an X Windows interface, such as X11 forwarding, entering the credentials:
  - Username: talariuser ○ Password: talari
- Issue the command **vncviewer**

Note: The Guest VM (firewall) must be running for this step to work as expected.

- Once the VNC Viewer popup window appears, hit enter – no password is required.

Figure 8

The Guest VM console will then appear in the X11 session window. The user may now configure the Palo Alto Networks NGFW IP management commands to access the Web interface of the Palo Alto Networks NGFW. To do this, login to the CLI of the Palo Alto Networks NGFW. Issue the following sequence of commands to assign an IP address, gateway, and DNS Server IP to the management interface of the Palo Alto Networks NGFW: admin@PA-VM>**configure** admin@PA-VM#**show** (to view the current configuration).

admin@PA-VM# **set deviceconfig system ip-address 1.1.1.1 netmask 255.255.255.0 default-gateway 1.1.1.5 dns-setting servers primary 1.1.1.50**

IP address - 1.1.1.1

Gateway - 1.1.1.5

DNS server - 1.1.1.50

admin@PA-VM#**commit** (which allows the change to take effect) admin@PA-VM#**exit**

admin@PA-VM>**ping host 1.1.1.100** (a host on the external LAN network)

Note: When using Palo Alto Networks software 8.0 dhcp must be disabled on the management port. The command required is: set deviceconfig system type static

Once you have verified an external host is reachable, use the GUI interface of the Palo Alto Networks NGFW to complete the configuration.