TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Teridion

Contents

Partner Information

Partner information	
Date	October 7, 2019
Partner Name	Teridion
Web Site	www.teridion.com
Product Name	Teridion for Enterprise
Partner Contact	Yarden Horev, Product Manager, yhorev@teridion.com, 5107074173
Support Contact	Support@teridion.com, 1-844-837-4346
Product Description	Teridion provides an enterprise WAN service built on the public cloud. Just like you have come to expect from cloud computing, Teridion's public cloud WAN service provides lightning-fast setup, global coverage, unbounded bandwidth and horizontal scale. The Teridion network is powered by Teridion Curated Routing, which fuses proven WAN acceleration techniques with metrics-driven route optimization. This gives enterprises: ● Secure, accelerated site-to-site performance ● Fast, consistent access to enterprise SaaS applications including superior low-loss, low-latency routing for voice and video ● SLA backed, cost-effective replacement for MPLS ● Full support for multi-cloud strategies with fast access to cloud workloads running in any cloud provider ● Simple and intuitive but powerful monitoring and analytics ● All this at a fraction of the price of carrier-grade and direct access circuits

Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform

- **Secured Site-to-Site Acceleration**
  Secure, Cost-effective, high-performance, SLA- backed service to replace legacy MPLS, with protocol acceleration and route optimization via broadband.

- **Multi-Cloud Optimization**
  Fast and reliable connectivity between each branch and cloud workloads located with any provider, globally, with a 'Zero Trust' approach.

- **SaaS Onramp**

Circuit-like reliability and protocol acceleration across broadband for SaaS applications that are backed by application level security policies.

Taking the action to route traffic directly from the branch via Teridion ensures great performance, eliminating commonly faced challenges, such as:-

- The requirement for backhauling traffic via the HQ with an MPLS circuit to guarantee secure access to enterprise workloads and cloud applications

- Remote Desktop/VDI Performance
    - RDP over TCP - Packet loss and inherent inefficiencies of TCP causing slow or choppy RDP performance
    - PCoIP - packet loss causing choppiness and screen freezes.

- Voice and Video Performance
    - Video - Packet loss causing screen glitching, out of sync audio, and frozen or dropped video calls.
    - Voice - Packet loss causing audio glitching, robotic sounding audio, and dropped calls.

- File Transfer and Backups Performance
    - Packet loss and TCP inefficiencies slowing file transfers and strangling overall throughput, despite a high bandwidth broadband or DIA connection.

Palo Alto Networks Products for Integration

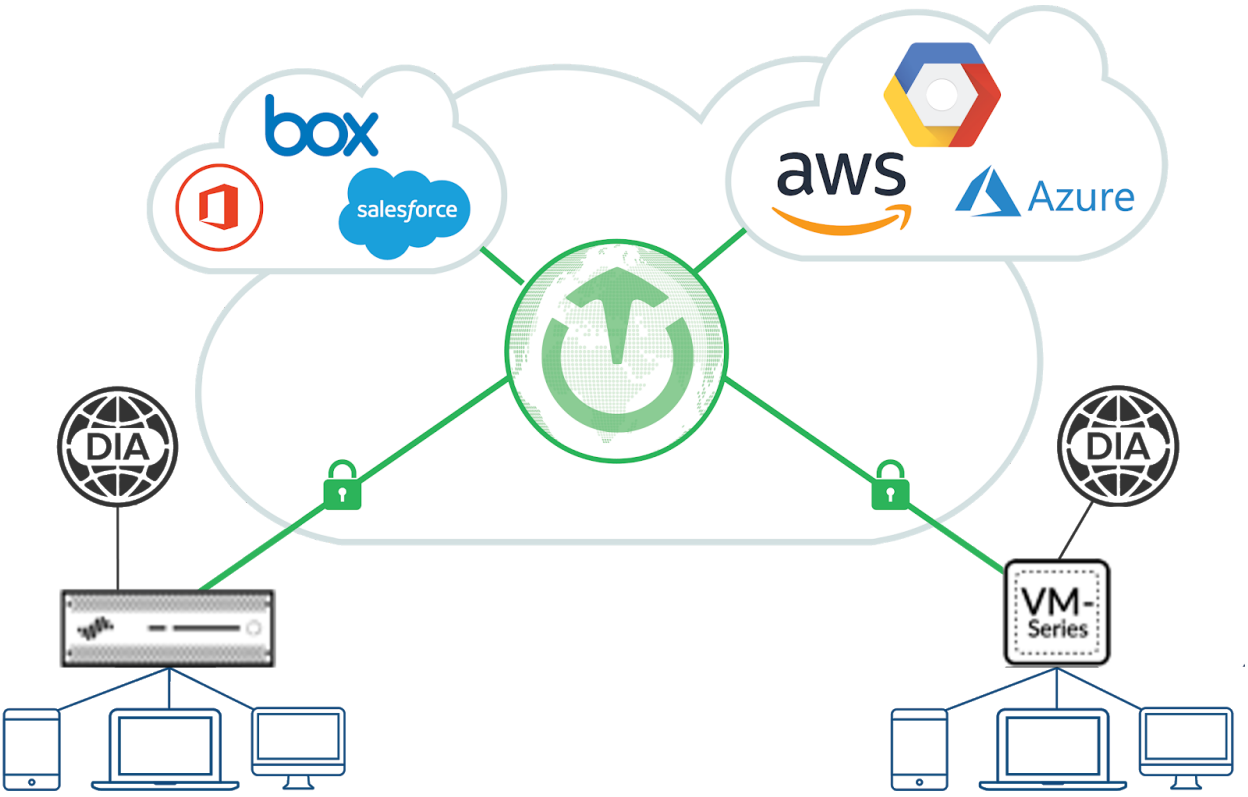
Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Teridion versions tested
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW	Validated	9.0.1	June 2019
Panorama			
Prisma Access			
Prisma Public Cloud			
Prisma SaaS			
Traps			
VM-Series	Validated	9.0.1	

WildFire			
Other			

Integration Benefits

- Secure, accelerated site-to-site performance
- Fast and consistent access to enterprise SaaS applications
- Superior low-loss, low-latency routing for voice and video
- SLA backed, cost-effective replacement for MPLS
- Full support for multi-cloud strategies with fast access to cloud workloads running in any cloud provider
- Simple and intuitive but powerful monitoring and analytics
- All this at a fraction of the price of carrier-grade and direct access circuits

Integration Diagram



- Customer's internet/ site-to-site traffic is being routed from the Palo Alto NGFW to the Teridion network. This traffic can be anything from voice calls, file sharing between enterprise sites, RDP, HTTPS traffic to SaaS apps, and more.
- An IPSec tunnel is created between the Palo Alto NGFW and the Teridion Cloud Router (TCR) that is dedicated to the site where the FW resides.
- For resiliency two tunnels can be created, one to a Primary-TCR and another to a Secondary-TCR from each site.

- Once the tunnel is created, the customer can choose which traffic to route via Teridion, and get optimized performance for that traffic: Lower loss, lower latency and higher throughput to other enterprise sites, cloud workloads and SaaS applications.

Before you begin

- Requirements for successful integration:
    - The customer to have a broadband/ DIA connectivity on the site.
    - IPSEC VPN tunnel to the Teridion Cloud Router with appropriate routing at the source to send relevant interesting traffic through the tunnel.

Palo Alto Networks Configuration

Create IPSec VPN tunnels to the Teridion Cloud Routers following the steps below.

Step	Description	Configuration Changes
1	**Creating New IKE Crypto Key** On the main tab go to: Network => Network-Profiles => IKE Crypto => Add Fill in the Phase-1 IKE information in the "IKE Crypto Profile" window (Same configuration on both sides) and click "ok".	**"Name":** Enter the name of the "IKE Crypto Profile". **"DH Group":** Select the DH Group. **"Authentication"**: Select authentication method. **"Encryption":** Select encryption method. **"Key-Lifetime":** Select the lifetime key in seconds (Also should be the same value as configured on Teridion's Network).

2	**Creating Two New IKE-Gateways, one for each VPN connection (Phase-1)** On the main tab go to: "Network" => "Network-Profiles" => "IKE Gateways" => "Add" On the new window fill in the information for Phase-1 negotiation. (In this step we configure two different IKE-Gateways for each TCR VPN connection).	**"General" Tab** **"Name":** Enter the name of the "IKE Gateway". **"Version":** IKE Version, its recommended to select "IKEv2 Preferred Mode" **"Interface":** The outgoing physical interface from which the tunnels will be formed. **"Local IP Address":** The IP Address of the outgoing physical interface from which the tunnels will be formed. **"Peer IP Address Type":** In our case the type will be IP. **"Peer IP Address":** IP Address of the remote TCR (On this stem we configure two IKE Gateways, one for the Primary-TCR and another for the Secondary-TCR). **"Authentication":** Select the authentication method, in this case we will use "Pre-Shared Key" for Phase-1 authentication. **"Pre-Shared Key":** Fill in the Pre-Shared Key for phase-1 authentication. **"Local-Identification":** That IP Address will be used as identification that is sent to the TCR, it is recommended to use the local site's public IP address for identification (For devices behind NAT, if your device is the edge device of the network it will use its public IP address, if not it will use its internal IP address as its identification ID.) **"Peer-Identification":** The TCR sends its public IP address as identification, fill in the remote TCR's IP address. **"Advanced-Options" Tab** **IKEv1 Configuration** **"IKE Crypto Profile":** Select the IKE Crypto Profile we created in step number 1. **"Dead-Peer-Detection":** Check the left side Check-box and fill in the sample interval.

		• **Check that the "Enable Passive Mode" checkbox is unchecked!**
3	**Creating New Crypto-Key for Phase-2 Negotiation** On the main tab go to: "Network" =>"Network Profiles" => "IPSec Crypto" => "Add" Fill in the Phase-2 Crypto information in the new "IPSec Crypto Profile" window.	**"Name":** Enter the name of the "IPSec Crypto Profile". **"DH Group":** Select the DH-Group. **"Authentication"**: Select authentication method. **"Encryption":** Select encryption method. **"Lifetime":** Select the lifetime in seconds (Also should be the same value as configured on Teridion's Network).

4	**Creating two new tunnel interfaces, one for each VPN connection (Phase-2)** On the main tab go to: "Network" => "Interfaces" => go to "Tunnel" Tab => "Add" On the new window fill in the information for the new tunnel interface. (In this step we configure two different tunnel interfaces for each TCR VPN connection).	**"Config" Tab** • **Select the number of the "Tunnel Interface".** **"Comment":** Enter the description of the "Tunnel Interface" **'Virtual-Router":** Select the relevant routing table for the tunnel interface. **"Security-Zone":** Select the relevant security zone for the tunnel interface. **"IPv4" Tab** **"IP Address":** Create new "/32" internal IP Address which will be used for the purpose of monitoring the tunnel for fail-over situation (Configure a different "/32" address for each tunnel interface). **"Advanced" Tab** **"MTU":** Select "1400" for the tunnel MTU.

5	**Creating two new IPSec Tunnel interfaces, one for each VPN connection (Phase-2)** On the main tab go to: "Network" => "IPSec Tunnels" => "Add" (In this step we configure two different IPSec Tunnels for each TCR VPN connection).	**"General" Tab** **"Name":** Enter the name of the "IPSec Tunnel". **"Tunnel Interface"** Select the tunnel interface created in step number 4. **"Type":** Select "Auto Key" or enter a "Manual Key". **"Address Type":** Select "IPv4" for "Address Type". **"IKE Gateway":** Select the IKE-Gateway created in step number 2. **"IPSec Crypto Profile":** Select the IPSec-Crypto-Profile created in step number 3. ● **Check the "Show Advanced Options" Check-box.** ● **Check the "Tunnel Monitor" Check-box.** **"Destination IP":** Enter the destination IP Address of the TCR to monitor the IPSec-Tunnel. (The monitor IP address of the Primary-TCR is 169.254.50.29/32 and the monitor IP address of the Secondary-TCR is 169.254.50.30/32, we will add a new route in the routing table in the following steps). **"Proxy IDs" Tab** **"IPv4" Tab** **Add Proxy-ID IP Address:** The Proxy-ID is actually an "Access-List" to the traffic that goes through the tunnel. Every line represents a rule that defines which "Local" subnet is permitted to reach the selected remote subnet. In this case the **"Local"** subnet will be the LAN subnets which we would like to communicate with other sites or to go out to the internet through Teridion's network. The **"Remote"** subnet will be "0.0.0.0/0" since Teridion's TCRs can be used as a Default-Gateway to the internet and to the other sites connected to Teridion's network.

		• It is also mandatory to add to this "Access-List" the local Tunnel-Interface Addresses that was created in step number 4 to enable monitoring through the tunnels.

6	**Add the new tunnel interfaces to the relevant "Virtual Router" and create new routes trough Teridion's network** On the main tab go to: "Network" => "Virtual-Router" => Click on the relevant Routing-Table To add the new tunnel interfaces to the relevant "Virtual Router" go to: "Router Settings" => "General" => "Add" and the new tunnel interfaces created in step number 4. To create new routes to the remote sites go to: "Static Routes" => "IPv4" Tab => "Add" In this step we are going to configure new routes to the remote sites subnets and to the TCRs monitor addresses that will go through the tunnels. Also on each route (Except the routes to the TCRs monitor address 169.254.50.29 - 30) we will enable "Path-Monitoring" to be able to detect route failure, when the Pah-Monitor check fails the best route automatically moves to the second route with the highest metric value.	**"Name":** Enter the name of the new route (Description). **"Destination":** Enter the remote site subnet or the TCR monitoring address. **"Interface":** Enter the interface which the traffic will go through (For each remote site subnet will have two routes with different metrics, the route to the primary tunnel will get lower metric for better priority and the route to the secondary tunnel will get higher metric for lower priority). **NOTE** ***The monitoring address of the primary TCR (169.254.50.29/32) will be routed only through the primary tunnel and the monitoring address of the secondary TCR (169.254.50.30/32) will be routed only to the secondary tunnel!*** ***"Next Hop":*** Since the type of VPN we are using is a "Policy Based VPN", there is no need to select "Next Hop IP Address", so we will select "None" for the "Next Hop". **"Metric":** Enter the metric of the route (For the primary route enter lower metric for higher priority and for the secondary route enter higher metric for lower priority). **"Path Monitoring"** **"Source IP":** Select the relevant tunnel interface address for path monitoring. **"Destination IP":** Select the relevant TCR monitoring address for path monitoring (For routes going through the primary tunnel select 169.254.50.29/32 and for routes going through the secondary tunnel select 169.254.50.30/32)

7	**Commit the changes** To commit the changes click on the "Commit" button on the upper right side.	
8	**Tunnel Status Validation** To see if the formation of the tunnel succeeded and to check the status of the tunnels go to: "Network" => IPSec Tunnels" and see if the status of the "Tunnel" , "IKE Gateway" and "Tunnel Interface" is green.	

General reference for IPSec configuration on PAN-OS:-

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/vpns/set-up-site-to-site-vpn.html

Partner Product Configuration

To create your Teridion network, log into the Teridion portal (my.teridion.com) using the credentials provided in your welcome email.

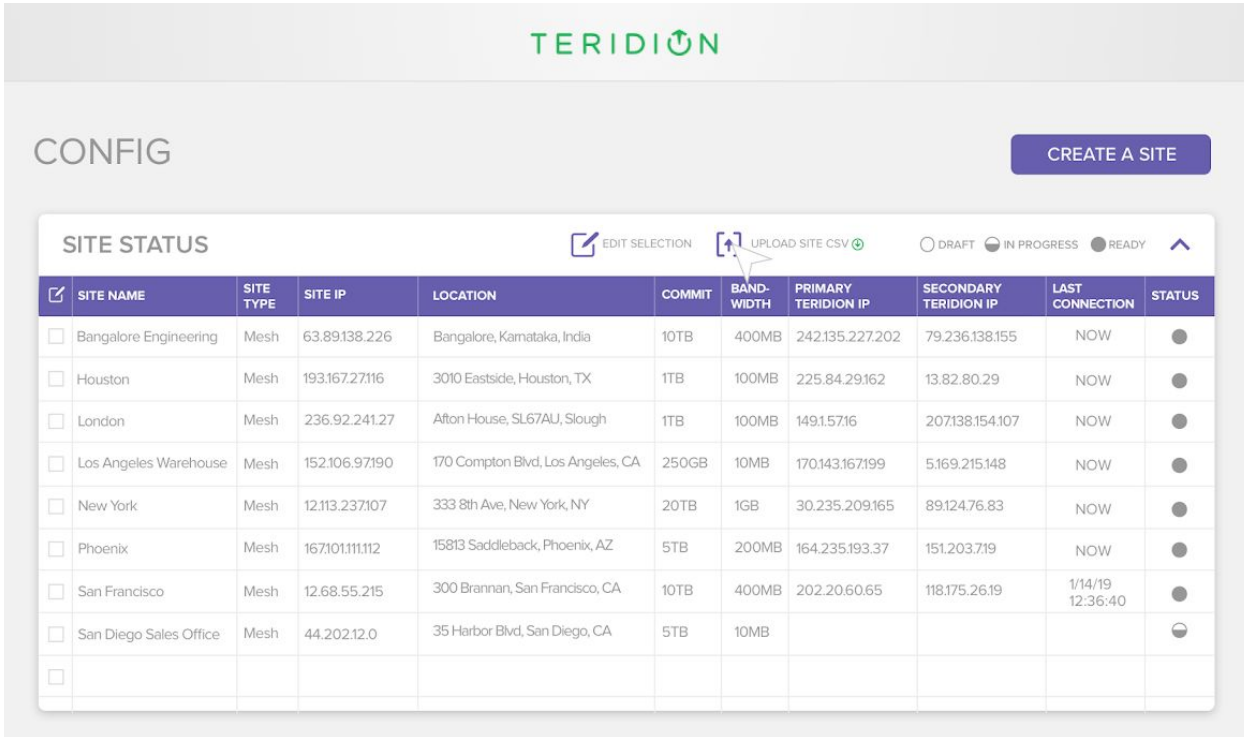
Each site created in the Teridion Portal will have three sequential statuses:

Draft- After clicking 'Save' for a site, the site will be in draft mode. Draft mode is like a "waiting room" where sites are kept until you're ready to commit the entire job for configuration. While sites are in draft mode, you can freely edit them, and no configuration adds or changes are pushed to Teridion.

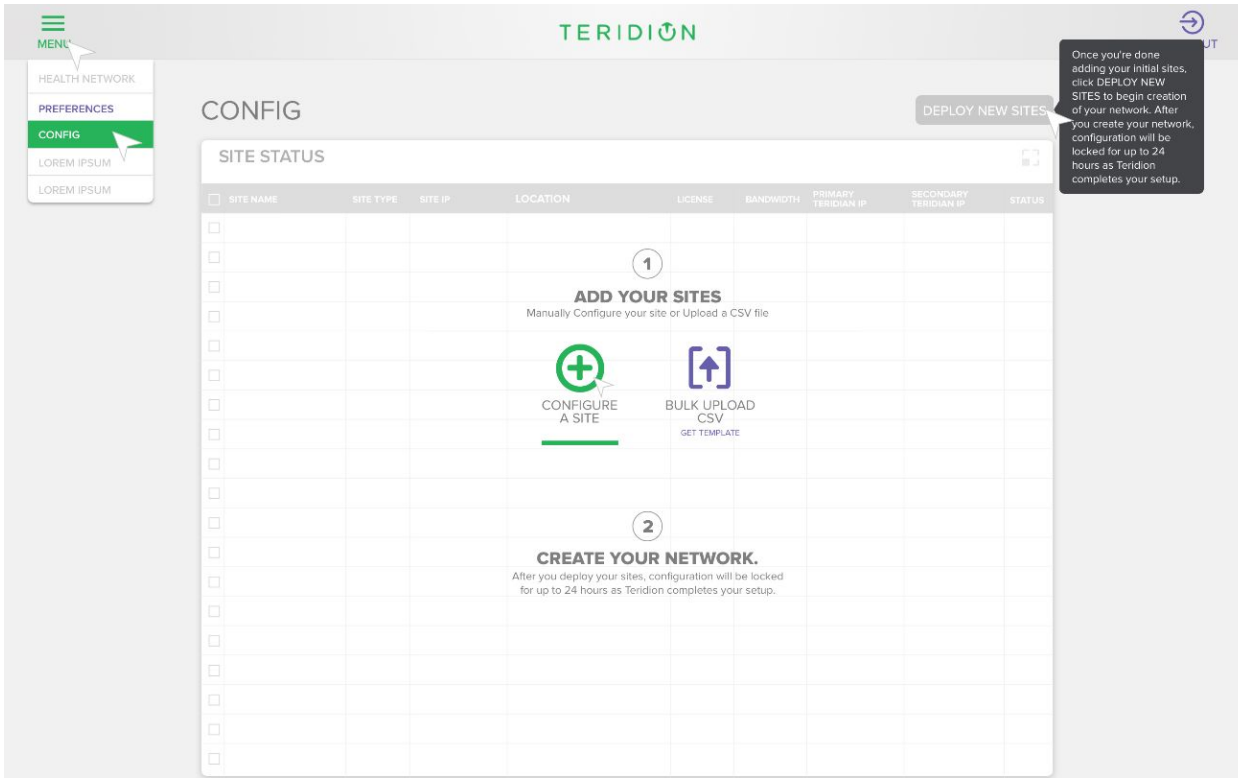
In-progress- After saving all required sites in draft mode, select 'Deploy New Sites'. This will send all site information to Teridion to create the network and change all sites' status to 'In-progress'.

> **Note:** Once you click 'Deploy New Sites', the network creation process begins, and all routes and Teridion Cloud Routers are deployed. This may take up to 24 hours, and during that time you won't be able to deploy any additional sites or make changes to the Teridion configuration.

Ready- Once the configuration is complete and the network is in service, the status will change to 'Ready'. At this point, the IPSec tunnels to the Teridion edge can be created.



1. Navigate to Menu-> Configuration. Add sites by choosing ‘Configure a site’ (if it’s the first site you’re creating) or ‘Create another site’ (for any sites after the initial site).

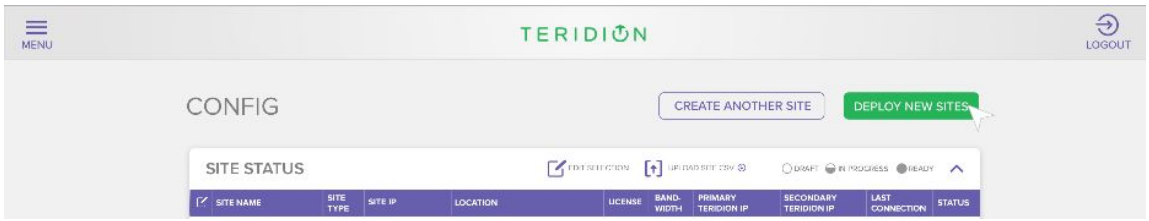


2. You'll connect each firewall to Teridion. For each appliance, you'll create a Teridion site. For each site, complete all the following fields and click 'save'.

    a. Site name - Provide a meaningful name to your site.
    b. Location- fill the city, state (if in US) and country of your site.
    c. Site bandwidth - These should be the rated upstream and downstream connection speeds for your broadband connection. Teridion will use these values to allow you to monitor your bandwidth usage.
    d. Site type: Spoke or Hub/Mesh- When selecting Hub/Mesh, the site will be connected to all other Hub/Mesh sites, and may also have spoke sites connected to it. For spoke sites, you'll need to assign a hub site to which it will connect.
    e. Site IP- Enter the public IP address of the site.
    f. Site ID- Enter the IP address assigned to the WAN interface (this value will default to the site IP). If the device is behind a NAT, the site ID will be the internal IP of the WAN interface. If the site has a static IP, the site ID will be the public IP of the site.
    g. Monitoring IP- Selecting a monitoring IP address will enable Teridion to present a complete view of network performance all the way to your site. The default value is the site IP, but it can be any other pingable public IP at the site.
    h. Site subnets - Insert all subnets behind the site that will use the IPSec tunnel (in CIDR notation, e.g. 192.168.120.0/24).
    i. CPE Support multiple tunnels (Yes/No) - Select 'Yes' if you would like to configure a redundant Teridion Cloud Router for your site for high availability.
    j. IPSec policies- Choose a template or fill custom policies for authentication, encryption, DH group and lifetime for phase 1 and phase 2.
    j. Pre-shared Secret - Choose a strong pre-shared secret. Remember to save it for configuring the tunnel on the NGFW; you won't be able to view the key in the Teridion Portal after you create it.

    Add more sites as needed. Remember, clicking 'Deploy New Sites' will 'lock' the portal until the network is created, so hold off until you finish saving all your required sites for this network.

3. When all sites are added, click 'Deploy New Sites'. Teridion will send an email notification to you once the network is ready.



4. Once the network is up, navigate to Menu-> Configuration. Find the Teridion endpoint IPs for each site in the 'Primary Teridion IP' column. These IPs will be used to configure the IPSec tunnel on the NGFW.

Troubleshooting

- Common troubleshooting steps
    - o Standard site-to-site IPSec troubleshooting

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clh5CAC&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail

- Contact information for support: Teridion has a 24x7 support and NOC teams. You can reach them by -
    - Support email: *support@teridion.com*
    - Phone: 1-844-837-4346
- Teridion is a TSA Net Member.

Technical Details

- The integration between Palo Alto Networks NGFW and Teridion network will include IPSec VPN from each site with Palo-Alto firewall to the Teridion Cloud Router, once the connection is formed, routes to the relevant subnets will point to the tunnel interface which connects to the Teridion-Cloud-Router over IPSec on each site.
- Route (Path) monitoring is recommended for each route that points to the tunnel.