TECHNOLOGY PARTNER PROGRAM USE CASE DOCUMENTATION

Table 1: Partner Information	
Date	January 9, 2020
Partner Name	RedSeal, Inc.
Web Site	https://www.redseal.net
Product Name	RedSeal cyber terrain analytics platform
Partner Contact	Noam Syrkin Sr. Technical Marketing Engineer **nsyrkin@redseal.net** (408) 990-3749
Support Contact	Support Portal: https://www.redseal.net/services/#customer-support Email: **support@redseal.net** Phone: US/Canada: 1-888-845-8169 UK: +44-2035140704
Partner Product for Integration	RedSeal cyber terrain analytics platform
Product Description	RedSeal's cyber terrain analytics platform shows customers what's on their network, how it's connected, and the associated risk. It unifies public cloud, private cloud, and physical network environments into one interactive model. Customers see how (or if) data can move within and between environments. RedSeal overlays host and endpoint information along with identified vulnerabilities. Risk and compliance managers can see if their network is set up as intended and get alerts if anything changes. Incident investigators can speed their investigation and containment with the network situational awareness RedSeal supplies. Network security personnel can validate and manage their segmentation and test changes to see if they'll violate any policies. Organizations use RedSeal's Digital Resilience Score to measure and improve their risk and resilience.

Use Cases for Integration with the Palo Alto Networks Security Operating Platform

Large, complex networks require the implementation and management of thousands of access rules. It can be difficult to determine the devices and rules that are responsible for unwanted access. Unwanted open access paths that contain vulnerabilities can leave organizations open to attack and allow an intruder to gain access to critical data systems.

To increase operational efficiency and reduce risk, Palo Alto Networks and RedSeal have partnered to ensure uniform visibility, defense, and ongoing management of an organization's entire firewall and network device infrastructure.

RedSeal's cyber terrain analytics platform shows you what's on your network, how it's connected, and the associated risk—across public cloud, private cloud, and physical environments. You'll be able to discover network devices automatically and verify your inventory, including endpoints. RedSeal will verify that your network devices are securely configured, comparing them with industry standards such as Standard Technical Implementation Guides (STIGs) and Center for Internet Security (CIS) security controls. RedSeal validates your network segmentation policies and continuously verifies that you remain in compliance with regulations and policies. Furthermore, it will prioritize mitigation based on the risk to your network from each vulnerability.

There are two major areas of integration:

- Cyber terrain modeling and mapping:
  - Model and understand hybrid environments—complete network inventory and how the devices (regardless of form factor) are connected.
  - Model access policies across physical, SDN, and cloud networks—where can a particular indicator of compromise (IOC) propagate within the network (blast radius)? How can it be contained?
- Risk and compliance audits:
  - Evaluate device configurations, compare to industry best practices, and harden them accordingly.
  - Model access policies across physical, SDN, and cloud networks.
  - Continuously monitor all L3 device access rules and configurations.
  - Analyze security impact: do security policy changes violate network segmentation policies?

Table 2: Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested	RedSeal Versions Tested
AutoFocus			
Cortex XDR			
MineMeld			
Next-Generation Firewall	Completed	PAN-OS 4.x, 5.x, 6.x, 7.x, 8.x, 9.x	RedSeal 8.5.0 – 9.3.2
Panorama	Completed	Version 5.x – 9.x	RedSeal 8.5.0 – 9.3.2
Prisma Access			
Prisma Cloud			
Prisma SaaS			
Traps			
VM-Series	Completed	PAN-OS 7.x, 8.x, 9.x	RedSeal 8.5.0 – 9.3.2
WildFire			
Other			

Integration Benefits

- Unify network understanding including your public cloud, private cloud, and physical networks, which helps you:
  - Identify any misconfigurations and assess device security posture (weak passwords or protocols).
  - Dynamically model all access paths based on Layers 2–4 and Layer 7 and across the public cloud and SDN to understand where an application can reach, anywhere within your network.
  - Validate network segmentation based on Layers 2–4 and Layer 7 and across public cloud and SDN.
  - Pinpoint weaknesses with end-to-end network visibility, including hosts.
  - Assess policy-change exposure and impact.
- See firewall rules in their entirety—including Layers 2–4 and Layer 7.

- Automatically prioritize remediation based on exposure.
- Understand and prioritize vulnerabilities based on network and application access paths.

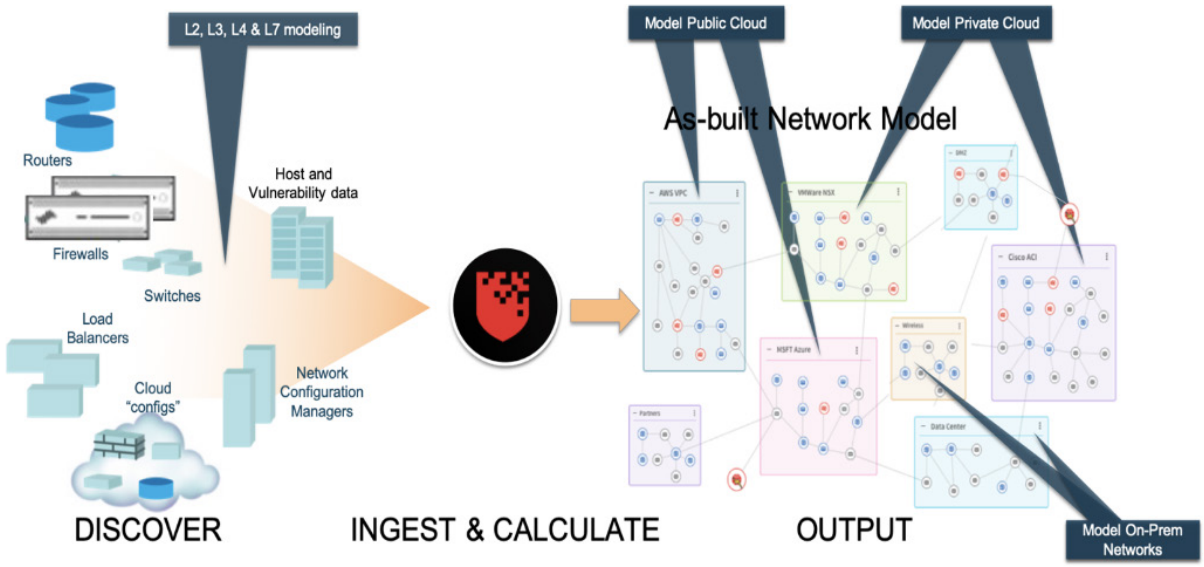


Figure 1: The RedSeal cyber terrain analytics platform—unified understanding of your network environments

RedSeal's integration with the Palo Alto Networks Next-Generation Firewall ensures uniform visibility, defense, and ongoing management of your entire firewall and network device infrastructure. The combination of Palo Alto Networks Next-Generation Firewall and RedSeal allows you to visualize your network topology, validate end-to-end access routes, import vulnerability scan data to prioritize remediation efforts, and continuously monitor and track changes to ensure ongoing compliance.

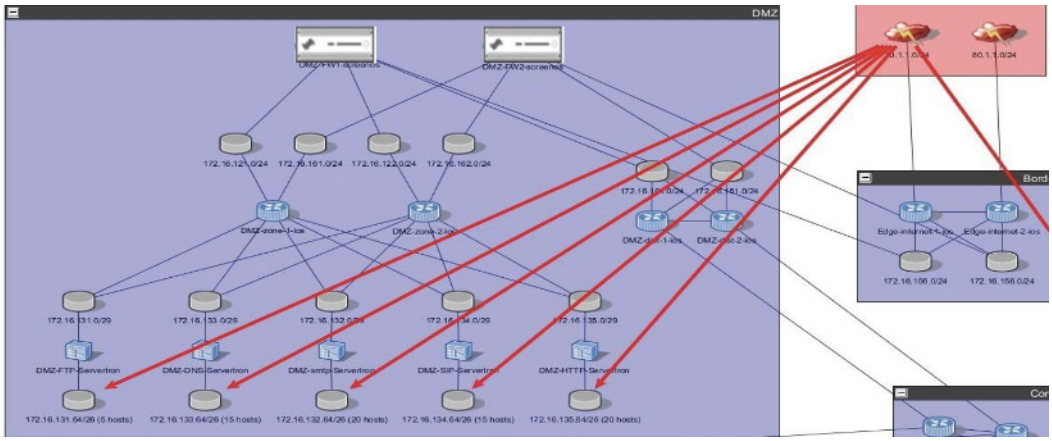


Figure 2: RedSeal details network access paths and prioritizes risks

From a suspect IP address, RedSeal can both identify all reachable targets—even several hops away—and prioritize which ones should be protected first.

What Data Is Shared?

What data is shared between RedSeal and Palo Alto Networks Next-Generation Firewalls? How is the data obtained? What actions are taken with the data?

RedSeal imports Next-Generation Firewall configurations. Device configurations can be gathered in the following ways:

- Directly from the device
- From Panorama™ network security management
- Via saved configuration files out of a CMDB

Once device configurations are collected, RedSeal normalizes the data, stores it in a database, and runs analytics to make sure device configurations comply with industry best practices (STIG/CIS) as well as your own standards; ensure that your network complies with corporate and industry policies (PCI, NERC-CIP); and verify that your network is segmented according to policies. RedSeal calculates access based on traditional routing algorithms as well as Layer 7 (App-ID) capabilities so users can see where an application can reach within the network.

Before You Begin

Successful integration requires the following:

1. Users must have "read only" access credentials to each Next-Generation Firewall or Panorama from which they want to import into RedSeal.
2. Alternatively, they can connect to a CMDB to import the configurations.
3. Users should ensure that the latest RedSeal plugin for Palo Alto Networks Next-Generation Firewalls is installed.

Palo Alto Networks Configuration

To begin configuration:

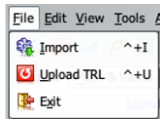
- Allow the RedSeal server access to the Palo Alto Networks Next-Generation Firewall or Panorama on TCP Port 22 (SSH).
- Create a dedicated read-only admin account RedSeal can use to log in to the Next-Generation Firewall or Panorama instance. This will be used to execute the commands specified in the Technical Details section later.
- Set up a firewall admin account and assign CLI privileges for RedSeal by following these steps.

Partner Product Configuration

Configure a data collection task to import Next-Generation Firewall configurations:

1. Log in to the RedSeal client.

2. Click on the sprocket icon or select File > Import.



3. The **Data Import** dialogue window open.
   Change to the **Data Collection** tab.

4. Click the New button to create a new data collection task.
5. In the Data Collection Task dialogue window select:
   1. Select "L2 & L3 Devices".
   2. Scroll down to "Palo Alto Networks PAN-OS" (applicable for both Next-Generation Firewall and Panorama).
   3. The **Communication Method** is SSH.
   4. Give this data collection task a name.
   5. Select existing login credentials or add new ones.
   6. Enter the hostname, IP address, or FQDN of the host to be collected. This host can be either a single Next-Generation Firewall or Panorama.
   7. If the host is Panoramas, you can optionally specify which firewalls to include in the collection.
   8. If the host is Panorama, you can optionally specify which firewalls to exclude in the collection.

Note: If the host is Panorama and you leave fields 7 and 8 empty, all Next-Generation Firewalls managed by the Panorama instance will be imported. This could potentially result in a data collection task that takes a long time to complete.

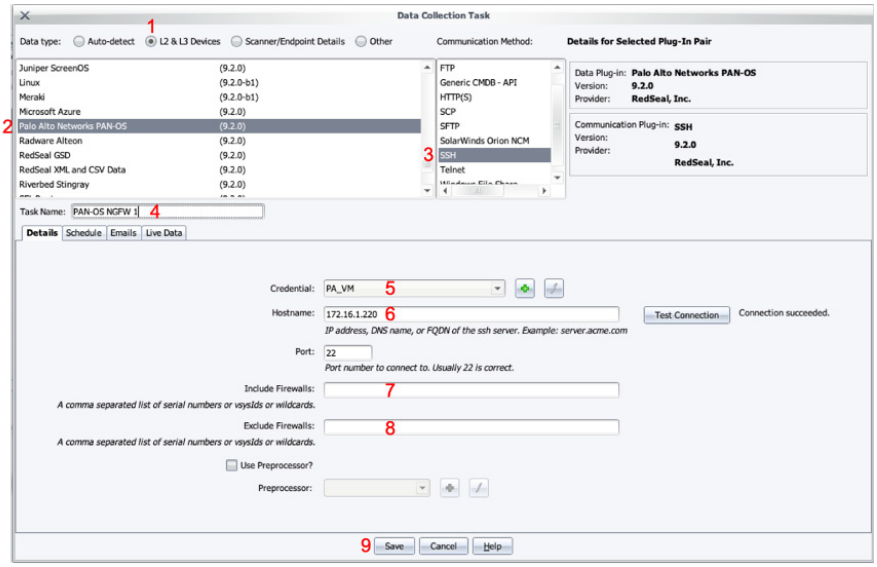


Figure 3: Data Collection Task window

9. Click the **Save** button.
10. The newly created task is run on demand. You can select the **Schedule** tab and add a run time schedule for it.

For more information, refer to the *RedSeal Data Import Plug-Ins Guide and RedSeal User Guide*.

Troubleshooting: Failure to Collect from Panorama

Troubleshooting this issue requires the RedSeal server debug log and the output of the SSH session as the user executes the commands directly on Panorama.

1. Collecting server debug log:
   1) Log in to the RedSeal Client UI.
   2) Navigate to Edit > System Setting > Logs:
      a) Change the server log to “DEBUG”.
   3) Re-run the data collection.
   4) Confirm the error messages shows failed to complete.
   5) Collect the server debug log once completed:
      a) Open a web browser and go to https://<RedSeal-IP>/data/system/log/server/all
      b) Download the server log.
2. Connect to Panorama:
   1) Use a SSH client.
   2) Change the SSH client setting to make sure it captures all readable output.
   3) Log in to Panorama using the same credentials configured in the data collection task.
   4) Execute the following commands:
      a) set cli pager off
      b) show system info
      c) show config running
      d) show config repo device ?
      e) show config repo device <serial#>
      f) show config repo device <serial#> version 100000
      g) show system setting url-database
   5) Verify each command completed successfully (if any failed, please work with your Palo Alto Networks administrator to make sure the user credentials have sufficient privileges).
   6) Terminate the session once all commands are executed.
   7) Upload the SSH session output manually for file-based import communication to confirm the results.
3. Please share the server debug log and the SSH client output with RedSeal Support:
   - Support Portal: https://www.redseal.net/services/#customer-support
   - Email: **support@redseal.net**
   - Phone: US/Canada: 1-888-845-8169
   - UK: +44-2035140704

Technical Details

Import data from a Palo Alto Networks firewall with the Palo Alto Networks PAN-OS® plugin.
The device must be able to respond to these commands depending on the type of data being collected.

Configurations:

```
- Pan-OS
  ◦ set cli pager off
  ◦ show system info
  ◦ show config merged
```

- show config pushed-shared-policy
- show config pushed-shared-policy vsys vsys<N>
- show running rule-use rule-base security
- type unused vsys vsys<N>
- show system setting url-database
- request system external-list show type ip name ?
- request system external-list show type ip name <EDL-name>

– Panorama
- set cli pager off
- show system info
- show config running
- show config repo device ?
- show config repo device <serial#>
- show config repo device <serial#> version 100000
- show system setting url-database

– Layer 2 connectivity data:
- show mac all
- show interface hardware
- show arp all
- how vlan all

– ORT data:
- show routing route

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

redseal-technology-partner-program-use-case-documentation-tpb-021020