TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Citrix Systems

Contents

Partner Information

Partner information	
Date	September 1, 2019
Partner Name	Citrix Systems
Web Site	https://www.citrix.com/
Product Name	Citrix SD-WAN
Partner Contact	Elisa Caredio, Principal Product Manager, elisa.caredio@citrix.com
Support Contact	+1 800 424 8749
Partner Product for Integration	Citrix SD-WAN 1100 appliance
Product Description	Citrix SD-WAN 1100 appliance

Use cases for integration into Palo Alto Networks Next-Generation Firewall

- VM-Series VM-50 and VM-100 running on Citrix 1100 appliance and integrated in virtual wire mode
- Traffic can be redirected to VM-50/VM-100 via Citrix SD-WAN policies on Citrix SD-WAN Center or Citrix Orchestrator
- VM-50/VM-100 inspects traffic based on the active security policies on the firewall
- LAN-to-LAN, LAN-to-WAN and LAN-to-Internet and Zone to Zone traffic protection

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Citrix Systems versions tested
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
GlobalProtect			
MineMeld			
NGFW			
Panorama	Validated	VM-50, VM-100, PAN-OS 9.0.1 and Panorama 9.0.1 (equal or higher to the PAN-OS version)	Citrix SD-WAN 11.0.2
Prisma Access			
Prisma Public Cloud			
Prisma SaaS			
Traps			

VM-Series	Validated	VM-50, VM-100, PAN-OS 9.0.1 Panorama – 9.0.1 and up. (Panorama needs to be equal or higher to the PAN-OS version)	Citrix SD-WAN 11.0.2
WildFire			
Other			

Integration Benefits

Integration of Palo Alto Networks VM-Series on Citrix 1100 appliance provides consolidation of SD-WAN and advanced security into a single branch device while maintaining separation of networking and security policies:

- Ability to run VM-50 and VM-100 hosted on Citrix 1100 appliance, therefore reducing the number of devices at the branch
- Ability to inspect and apply policy on the VM-Series which is hosted on Citrix 1100 appliance for any traffic that – based on topology and SD-WAN policies – flows LAN-to-LAN, LAN-to-WAN and LAN-to-Internet
- Have a complete on-premises SD-WAN + NGFW solution which blocks threats close to the entry point and allows customers to adopt local internet break-out at the branch with ease.
- Easy integrated workflow via SD-WAN Orchestrator and SD-WAN Center that simplifies provisioning, bring up and lifecycle management of the hosted VM-Series, while maintaining clear separation between networking and security policy management

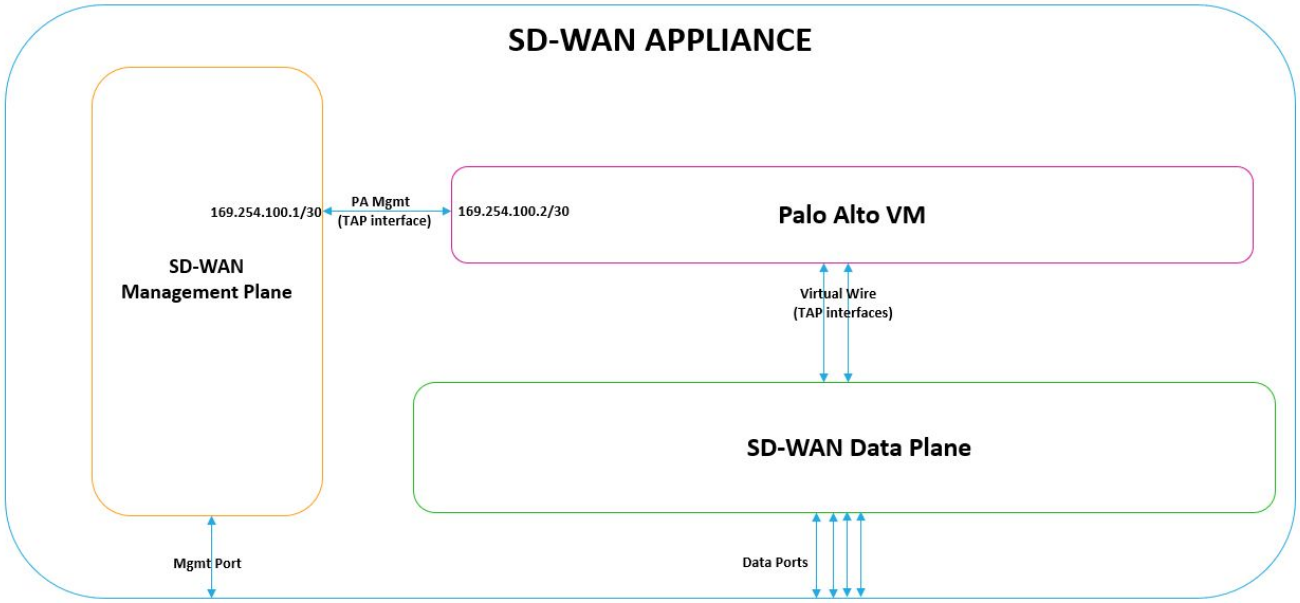
Integration Diagram

Following are the high-level details about the integration.

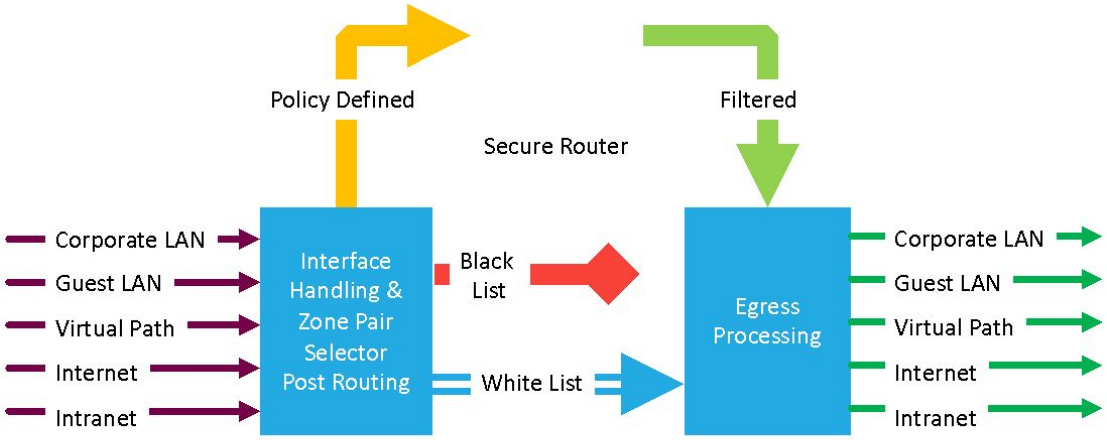
- Palo Alto Networks VM-Series is deployed in Virtual Wire mode
- All external management and data interfaces are managed by SD-WAN. TAP (Virtual Network Adaptor) interfaces are used for communication with Palo Alto Networks VM-Series. There is one management TAP interface and two data TAP interfaces are connected to Palo Alto Networks VM-Series which is operating in vwire mode (virtual wire).
- Palo Alto Networks VM-Series is assigned with following IP address, gateway and DNS on management interface
    - IP/Prefix: 169.254.100.2/30
    - Gateway: 169.254.100.1
    - DNS: 169.254.100.1
- Management access to Palo Alto Networks VM-Series is provided through SD-WAN management IP address
    - Source NAT operation will be performed for all outgoing management traffic
    - GUI access to Palo Alto Networks VM-Series is provided on <SD-WAN Mgmt IP>:4100 port

- CLI access to Palo Alto Networks VM-Series is provided on <SD-WAN Mgmt IP>:4101 port

Data Traffic redirection to Palo Alto Networks VM-Series can be controlled from SD-WAN configuration



Policy integration model



Before you begin

- Dependencies:
  - Customer needs to obtain the Auth codes and VM Image from the PA Support Portal
  - Optional Panorama authentication key can be added during the bootstrap process
  - Customer needs to have a 1100-SE appliance deployed

- Customer needs to have a SD-WAN Center appliance or a SD-WAN Orchestrator service entitlement
- Network connectivity between the MCN, SD-WAN Center or Orchestrator and the 1100-SE Branch device

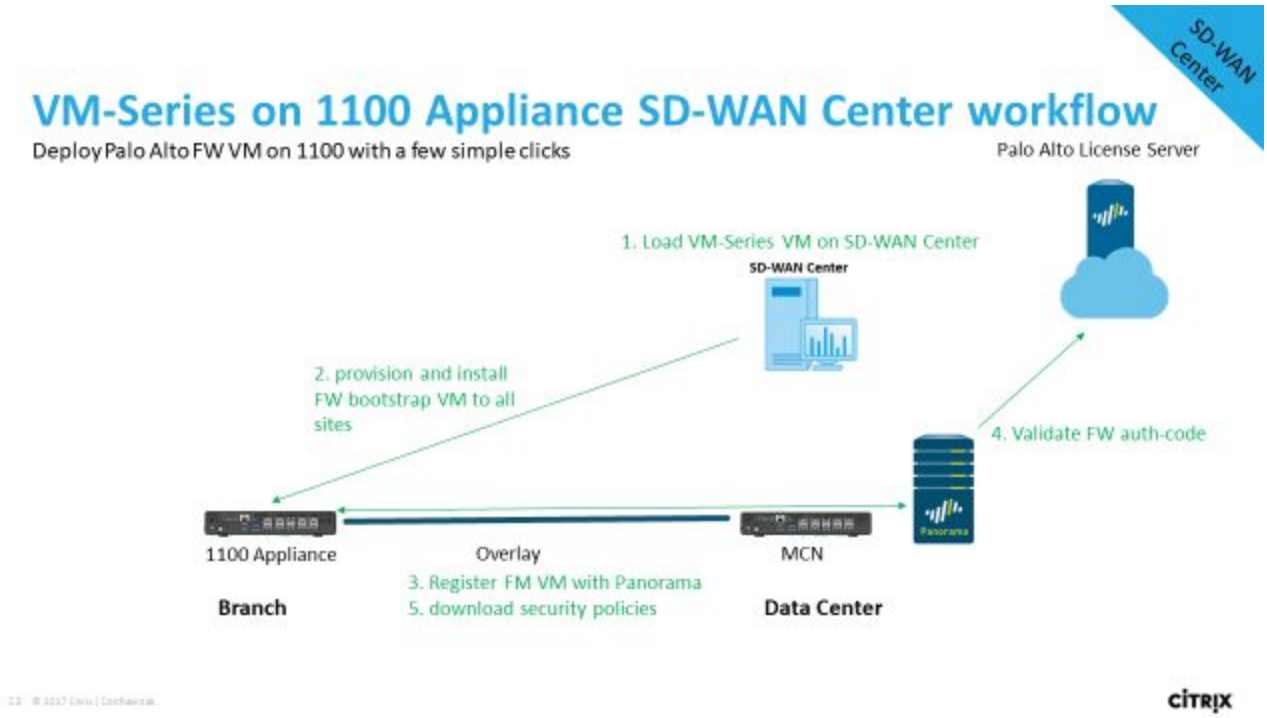
- Requirements for a successful integration:
  - The Advanced Security Virtual Appliance is deployed in a Virtual Wire mode
- Dependencies on OS Versions:
  - Citrix 1100 appliance running software version 11.0.2 and above
  - Supports only PAN-OS Version 9.0.1 and above.

Palo Alto Networks Configuration

Palo Alto Networks VM 50 and VM 100 can be easily integrated into Citrix SD-WAN 1100 appliance with a few easy steps via SD-WAN Management:

1. Upload Palo Alto Networks VM-Series software on Citrix SD-WAN Management platform
2. Citrix SD-WAN Management platform provisions the Palo Alto Networks VM-Series software to all the Citrix SD-WAN 1100 appliances in the deployment
3. Each appliance brings up the Palo Alto Networks VM-Series in bootstrap mode
4. Palo Alto Networks VM-Series connects to Panorama

A more detailed diagram of the workflow is depicted below:



Configuring the Palo Alto Networks VM-Series on the SD-WAN 1100 appliance:

1. Login to the Palo Alto Networks VM-Series with the default username and password, or use the Panorama UI to start configuring the appliance
2. Create a VLAN tagged sub-interface on Ethernet port Eth1 and Eth2 and configure them as a virtual wire. Note that Eth1 interface maps to the Inside network and the Eth2 maps to the Outside Interface. Note down the value of the VM
3. If required, apply appropriate Zone information to the Virtual Wire interfaces
4. From the policy tab, create an appropriate filtering policy for this virtual wire

5. Commit the configuration

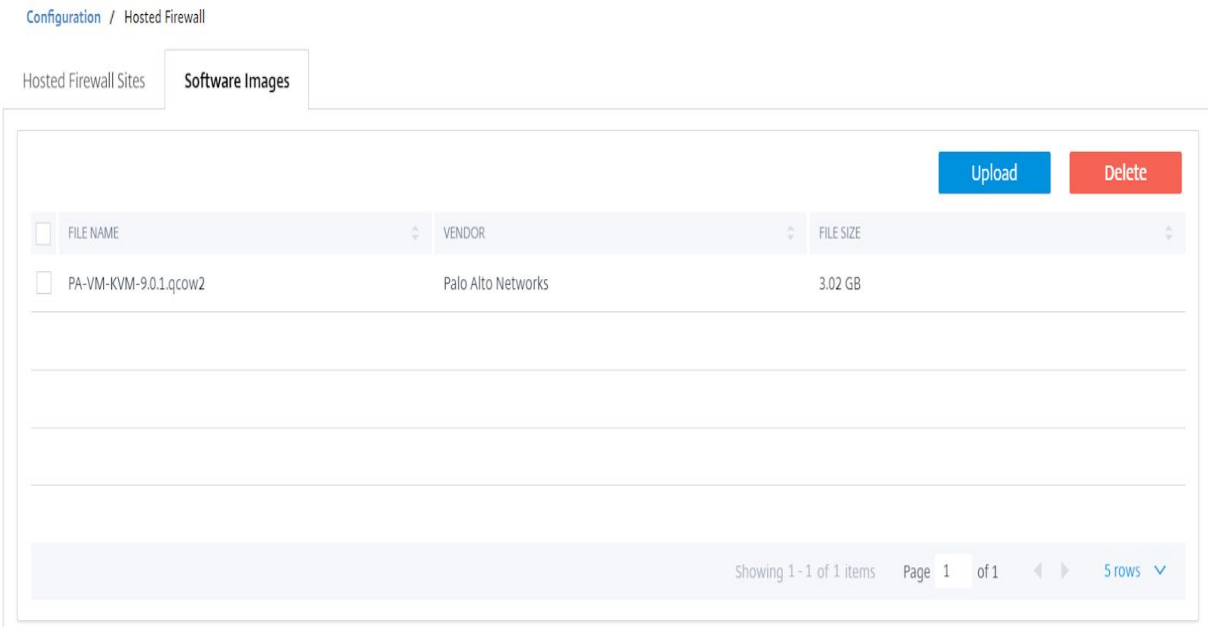
Configuring the SD-WAN 1100 Appliance for ADVANCED security services:

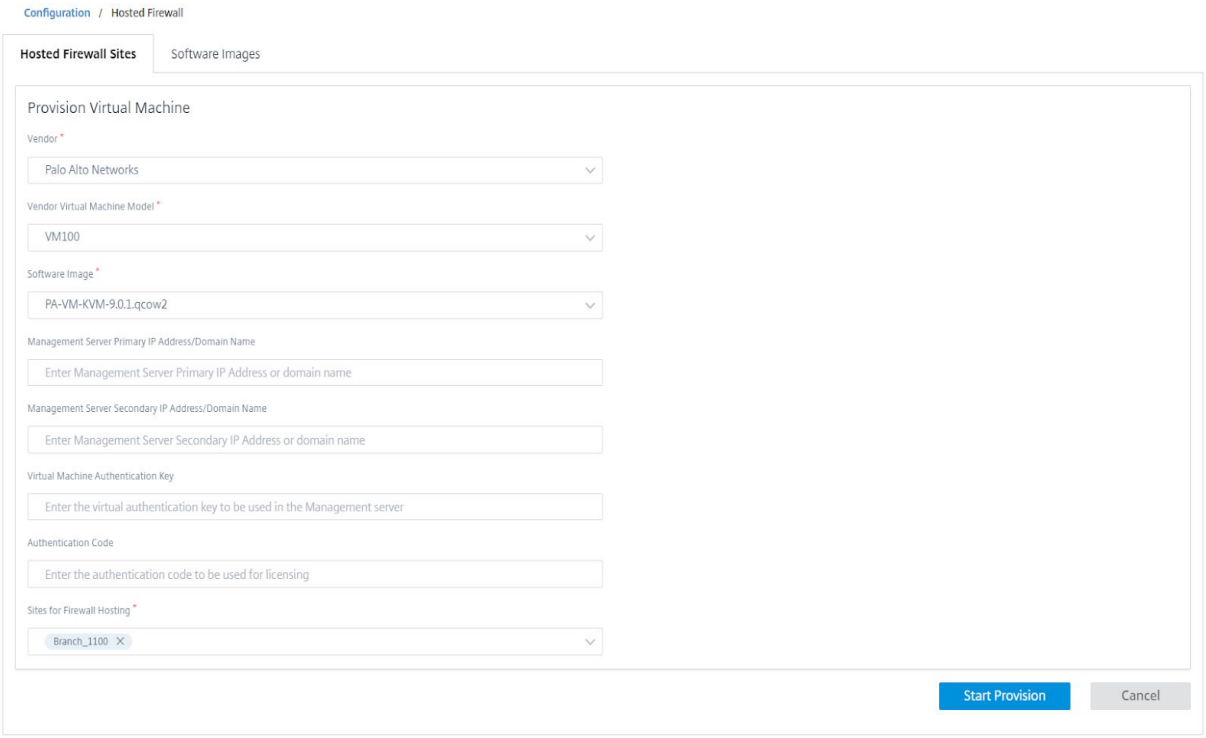
1. From the global UI create an Advanced Security template. Create a VLAN ID for redirecting traffic between a pair of zones to the Palo Alto Networks VM-Series. This VLAN value must be the same as the one defined in the appliance from the previous step
2. From the site-specific firewall configuration UI, configure the source and destination zone pair and apply a redirect policy with the template value from the previous step.
3. Apply the changes to the network. The specific sites with the PA VM Firewall will now have a redirection policy that will enforce the security filtering using the PA VM instance on that appliance

For more advanced configuration options, refer to the documentation from Palo Alto Networks and Citrix Systems

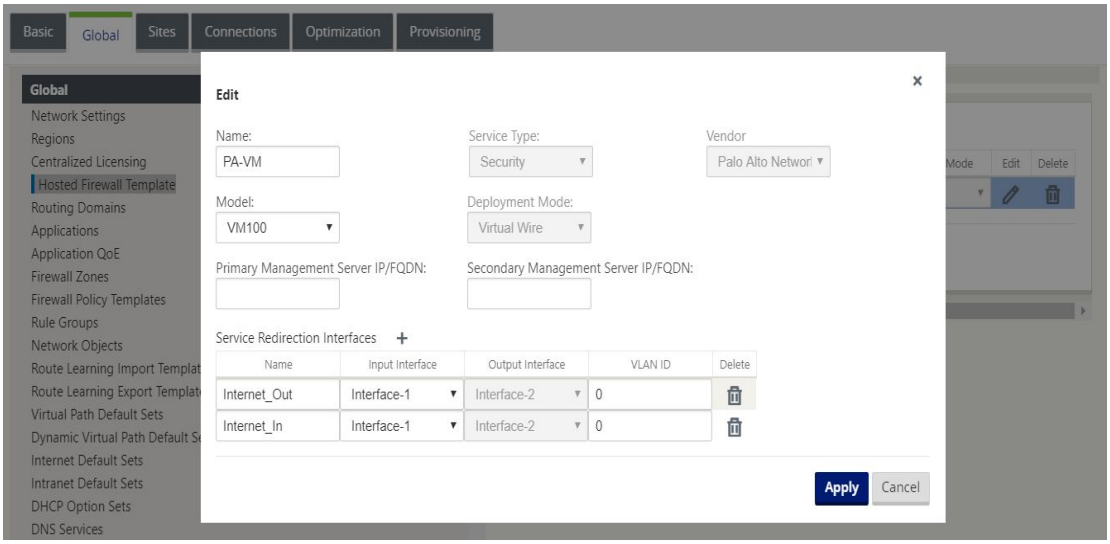
Partner Product Configuration

- Customer can provision and configure traffic redirection to the Palo Alto Networks VM-Series via Citrix SD-WAN Management. There are two parts to it:
    - Provisioning of the Palo Alto Networks software to all SD-WAN 1100 appliances in the deployment (Configuration -> Hosted Firewall)

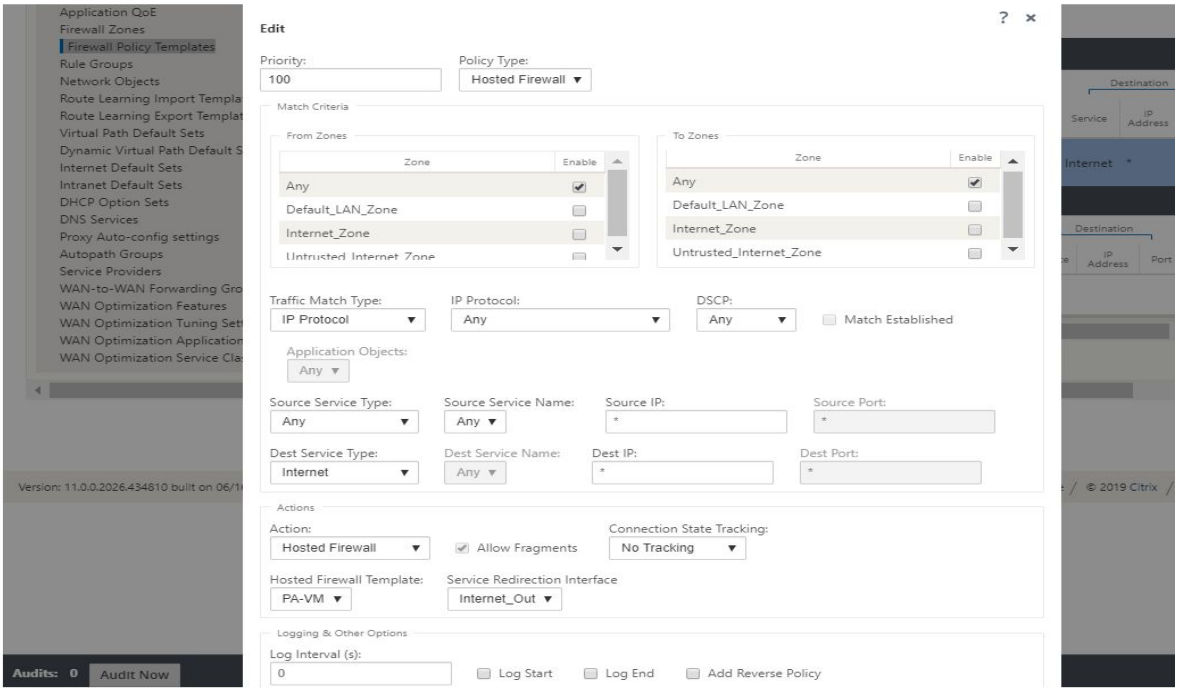




- Enable Traffic redirection to hosted Palo Alto Networks VM-Series in SD-WAN Configuration (Configuration -> Network Configuration)
  - Configure “Hosted Firewall Template” with the information that is required to traffic redirection to Palo Alto Networks VM-Series



- Configure “Firewall Policy Template” with the required traffic redirection rules
- Associate the Firewall Policy Template to the required sites



Common troubleshooting steps

- SD-WAN maintains connection table which tracks all the connections going through it, the only exception here is passthrough connections will not be part of connections table. SD-WAN connection table is listed under: “Monitoring ->Firewall”
- Connections that are redirected to Palo Alto Networks VM-Series also listed in SD-WAN connection table. For redirected connections, stats will be maintained to track number of packets sent to (or) received from Palo Alto Networks VM-Series
- SD-WAN firewall filter policies counts the packet hits and the maps the list of connections hitting the policy
- Palo Alto Networks VM-Series connections can also be viewed under the Monitor/Traffic tab. The Security Policies can also show the “Rule Usage” in Policies when troubleshooting which rule in the VM-Series is being utilized. This can be enabled by making the “Rule Usage” column available. To add this column, click the down arrow of a policy in the Policy Tab, then columns and select “Rule Usage.”