TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: **CyberMDX Technologies**

Contents

Partner Information

Partner information	
Date	March 27, 2019
Partner Name	CyberMDX Technologies Inc.
Web Site	https://www.cybermdx.com
Product Name	MDefend
Partner Contact	Motti Sorani, CTO, +972-503890642, mottis@cybermdx.com
Support Contact	support@cybermdx.com; 1-646-794-4161
Partner Product for Integration	MDefend
Product Description	Visibility and Cybersecurity Platform for Medical Devices and Clinical Networks

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

- Comprehensive visibility – Enrich PAN with CyberMDX classification data, via auto-tagging the devices and creation of dynamic address groups by vendor and type.
    - The dynamic address groups are used in PAN policies to restrict the network traffic between different groups and external networks.

Palo Alto Networks Products for Integration

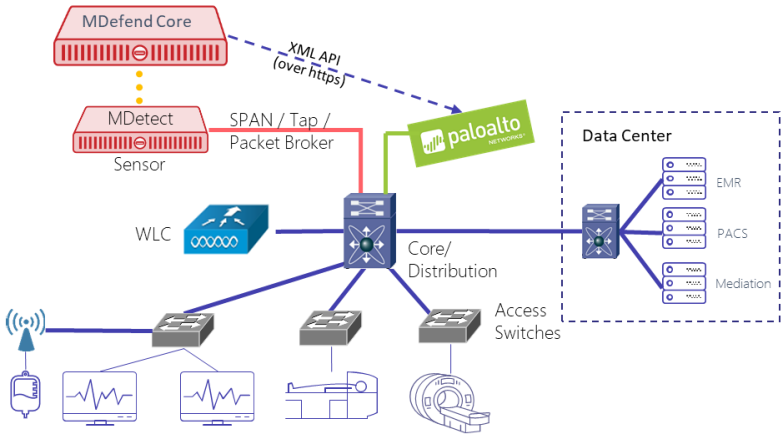
Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	CyberMDX versions tested
Aperture			
AutoFocus			
GlobalProtect			
GlobalProtect Cloud Service			
Cortex Data Lake			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW	Active	PanOS 9.0	MDefend 3.12
Panorama	Active	PanOS 9.0	MDefend 3.12
RedLock			
Traps			
VM-Series			
WildFire			
Other			

Integration Benefits

- Auto identify and classify devices in clinical networks.
- Automate the process of tagging the devices inside PAN.
- Leverage tags to enforce fine-tuned network access policies which reduce the attack surface, and hence the changes of a successful attack.

Integration Diagram

The diagram below illustrates how this integration works in a two layer network architecture and a stand-alone NGFW. (Please note that three layer architecture and distributed networks are also supported, as is integration with the Panorama management system).



- MDefend auto identify and classify devices in the network.
- MDefend shares this classification data by creating addresses for the devices inside PAN, and tagging them with vendor, type and a special flag for medical devices.
- A dynamic address group is created for every group of devices, defined by vendor and type
- Dynamic address groups can be used in policies to restrict network traffic between the groups and between a group and external networks.
- MDefend continuously updates the ip address of devices as they might change dynamically, and create address as new devices get on board.
- MDefend applies a housekeeping procedure to delete addresses for decommissioned devices.

Before you begin

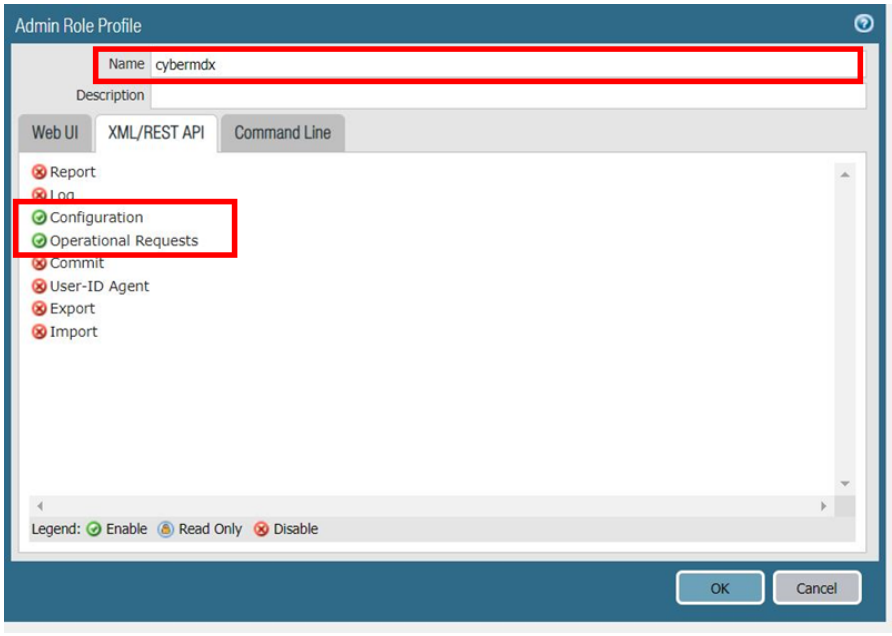
- Integration tested on Pan OS 9.0 with XML API enabled
- Minimal version of CyberMDX MDefend: 3.12

Palo Alto Networks Configuration

Step 1: Inside PAN - Create a Role for CyberMDX

Go to: Device \ Admin Roles. Click “Add”

In the pop-up, enter a name for the role e.g. cybermdx, and inside the XML/REST API tab, check the following capabilities: Configuration, Operational Requests

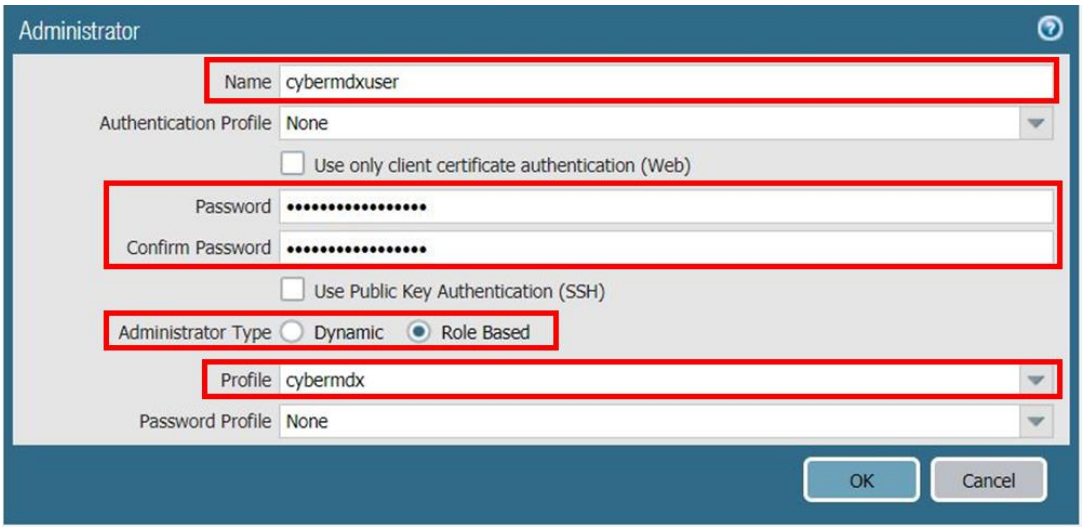


Step 2: Create a user and password for CyberMDX

Go to: Device \ Admin Roles. Click “Add”

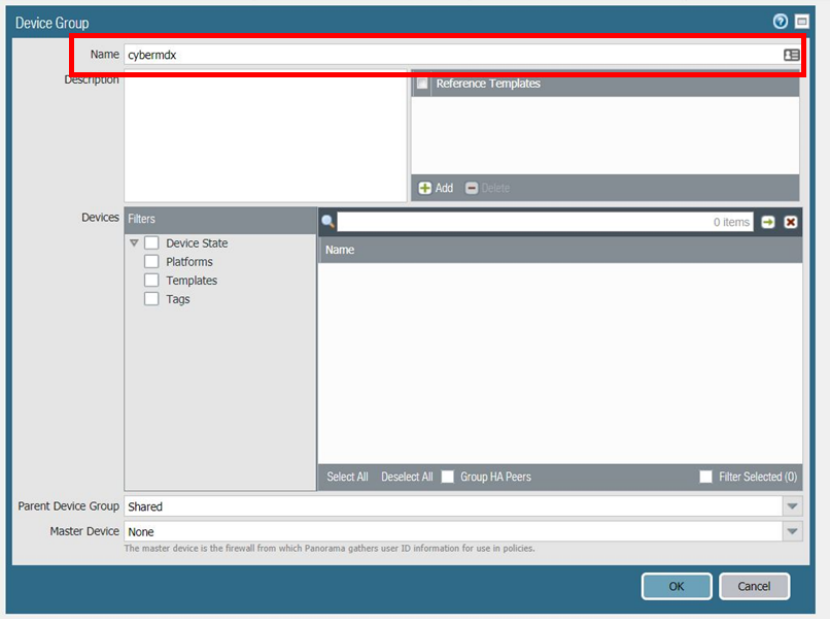
In the pop-up, enter a name for the user, a password, check “Role Based” administrator type and in the profile enter name chosen for the role in the former step

*Click on **Commit***



Step 3: For Panorama integration only – if no device group exists – create one

Inside Panorama Go to: Panorama \ Device Group, click on “Add”
In the pop-up, enter a name and choose the devices to include in the group



Partner Product Configuration

Step 4: Define PAN Endpoint in MDefend

Note: the endpoint could be Panorama management system or a stand-alone NGFW.

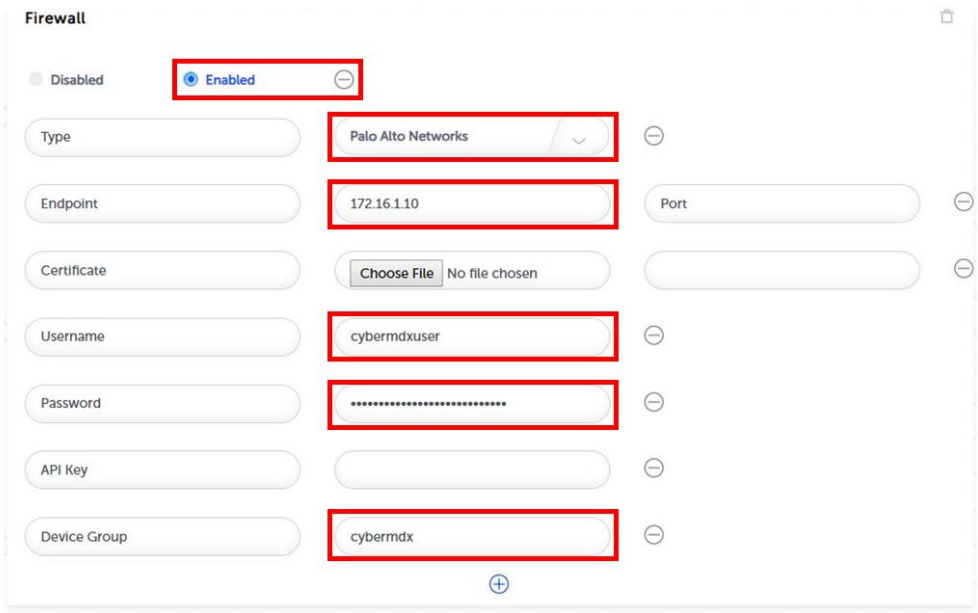
Inside MDefend, Go to: *Settings* \ *Integrations* \ *Firewall*

- Check “Enabled”
- Set Type to Palo Alto Networks
- Set Endpoint IP Address to Panorama or NGFW IP Address
- Leave ther port empty
- Set the user and password created for cybermdx user in step 2

In case of Panorama - set the device group name in “Device Group”.

In case of NGFW – leave this one empty

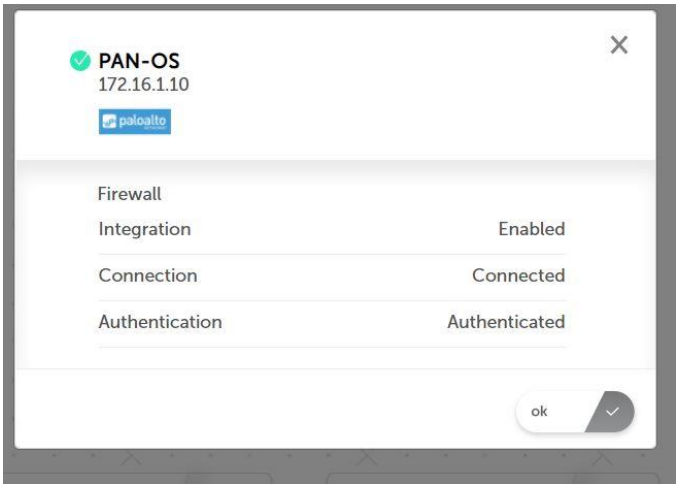
Press “Save”



Step 5: Verify the integration is working properly

Inside MDefend, Go to: *Status*

Click on the Palo Alto Networks box, and verify the integration is Enabled connected and authenticated.



Troubleshooting

- Refer to the status of the integration inside MDefend Status Screen.
    - In case of a connection problem – verify connectivity between MDefend and Panorama/NGFW
    - In case of authentication problem – verify the user allocated to cybermdx is valid, and repeat steps 1-5 of the integration setup if needed
    - Otherwise – contact CyberMDX Professional Services
      email: support@CyberMDX.com phone: 1-646-794-4161

Technical Details

The API calls that are being leveraged

- **system info**
  - cmd type: op
  - xml: <show><system><info></info></system></show>

- **tags**
  - cmd types: **set, del**
  - xapi
    - NGFW: **/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/tag/entry**
    - Panorama: **/config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='cybermdx']/tag/entry**
- **addresses**
  - cmd types: **set, del**
  - xapi
    - NGFW: **/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address/entry**
    - Panorama: **/config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='cybermdx']/address/entry**
  - o
- **address groups**
  - cmd types: **set**
  - xapi
    - NGFW: **/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address-group/entry**
    - Panorama: **/config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='cybermdx']/address-group/entry**