TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: CryptoniteNXT

Contents

Partner Information

Partner information	
Date	July 19, 2019
Partner Name	CryptoniteNXT
Web Site	www.cryptonitenxt.com
Product Name	CryptoniteNXT
Partner Contact	Justin Yackoski, CTO, jyackoski@cryptonitenxt.com, 301-294-5266
Support Contact	www.cryptonitenxt.com/support or 301-294-5244
Partner Product for Integration	CryptoniteNXT
Product Description	Zero-trust network segmentation and moving target defense

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

- Protection of traffic and endpoints within a Layer 2 subnet
    - CryptoniteNXT provides an additional layer of protection prior to reaching a next-generation firewall located at a Layer 3 routing location
    - CryptoniteNXT allows granular policy control within and between Layer 2 subnets
    - CryptoniteNXT prevents network-based reconnaissance and contains attacks
    - CryptoniteNXT provides alerts on attempts to misuse or manipulate the network
    - CryptoniteNXT stops attacks on network services and infrastructure
- Collection and conveyance of endpoint and user identify
    - CryptoniteNXT automatically collects identity including available 2-factor authentication and support for endpoints outside of Active Directory. Identity is securely forwarded to Palo Alto to provide single sign-on and avoid captive portal use.
    - CryptoniteNXT cryptographically authenticates packets end-to-end to prevent spoofing.

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	CryptoniteNXT versions tested
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW	Complete	PAN-OS 8.x and 9.0	2.5 and higher
Panorama			
Prisma Access			
Prisma Public Cloud			
Prisma SaaS			
Traps			
VM-Series			
WildFire			

Other			

Integration Benefits

- Single sign-on for users, optionally using 2-factor authentication
- Endpoint and user identity is automatically collected and provided to allow policy enforcement and monitoring using a single consistent IP and identity for each endpoint
- Identity information without requiring Active Directory support
- Reduced need for portal-based authentication

Integration Diagram

This section illustrates the general flow of a User authenticating to the CryptoniteNXT protected enclave, and then extending this User identity and associated egress NAT IP address to the Palo Alto Next-Gen firewall, in order to facilitate end-to-end access control. While this document assumes users authenticate with the CryptoniteNXT Web Portal, the diagram below shows an example further integration with Aruba ClearPass for user/computer identity to avoid the use of a portal. The Palo Alto User-ID API is used to provide data from CryptoniteNXT (or indirectly from other sources) to the Palo Alto Next-Gen firewall. Palo Alto acts on this information as it would with the same data from other sources (for policy enforcement, monitoring, etc.). Compared to other sources, the data provided by CryptoniteNXT can be more highly trusted and a CryptoniteNXT-protected network can be configured to ensure man-in-the-middle and/or spoofing attacks are prevented.

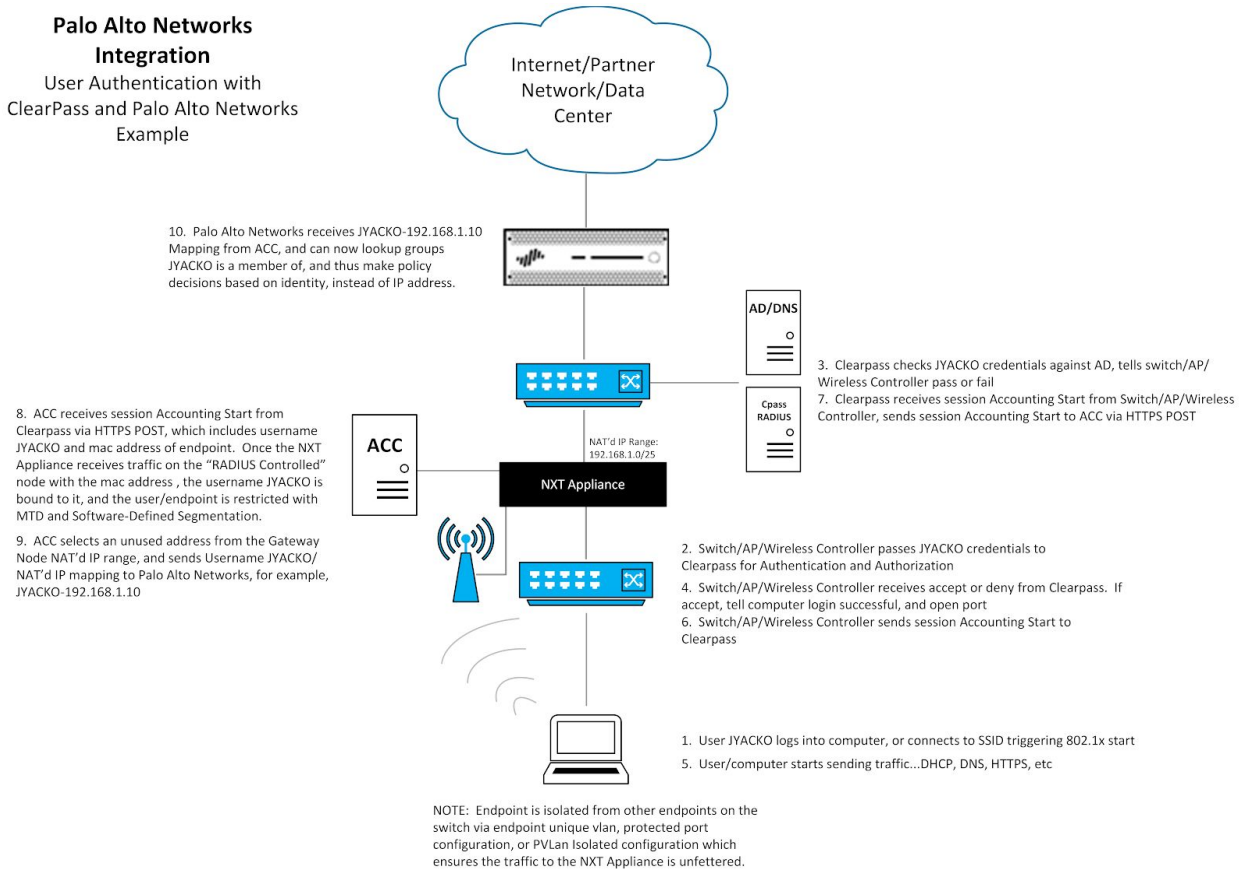


Figure 1: High-Level Flow

Before you begin

The following prerequisites must be met before configuring the integration:

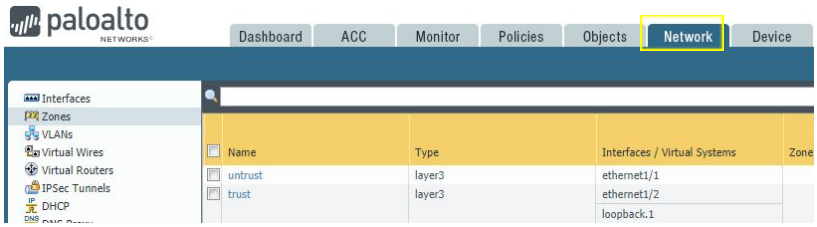
- General understanding of networking, Palo Alto, and CryptoniteNXT
- Users and Endpoints must be known to CryptoniteNXT (Automatic Onboarding in future release)
- CryptoniteNXT release 2.5+
- Palo Alto Next-Gen Firewall release 8.x or 9.x
- CryptoniteNXT Version 2.5+ environment configured for basic operations and a Gateway Egress IP Range configured
- Palo Alto environment configured for basic operations
- Connectivity verified between the CryptoniteNXT Administrative Control Center (ACC) and the Palo Alto Next-Gen Firewall.

Palo Alto Networks Configuration

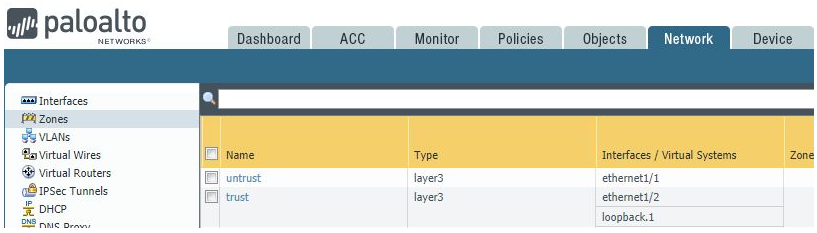
This section explains how to configure Palo Alto for integration with CryptoniteNXT. It assumes Palo Alto is already operational. This is a very basic setup – for detailed implementation guide, please review the link below.

Source: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/enable-user-id for PAN OS 9.x or https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/enable-user-id for PAN OS 8.x

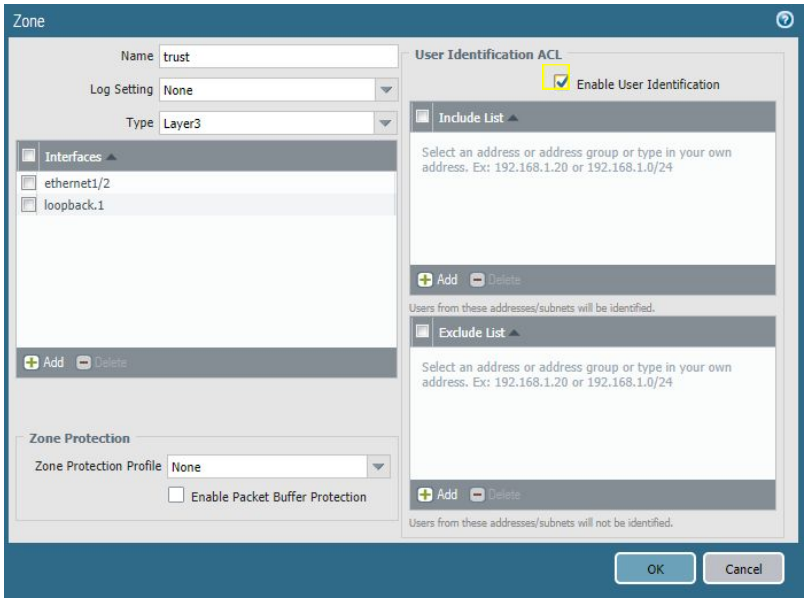
Click *Network* tab, then *Zones*



Click the *Zone Name* where users require user-based access controls. In this example, *Trust.*

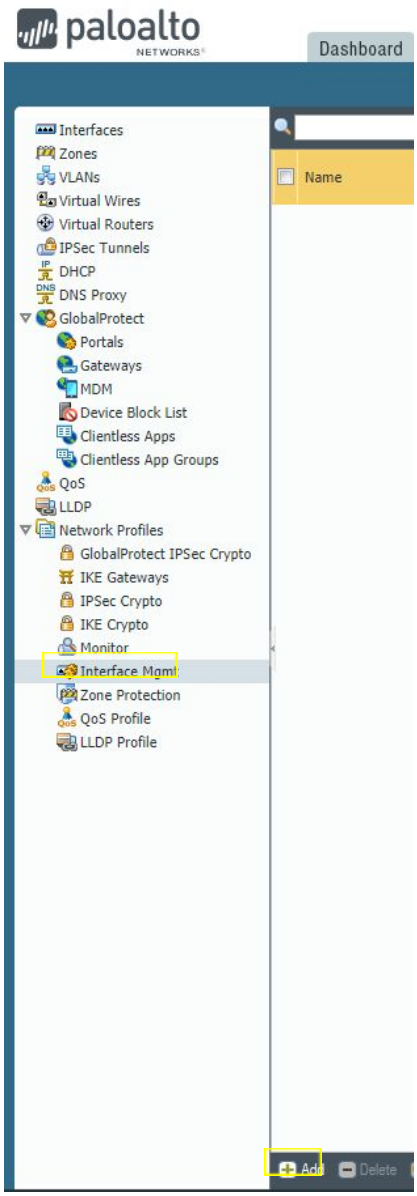


Check *Enable User Identification,* Click *OK*

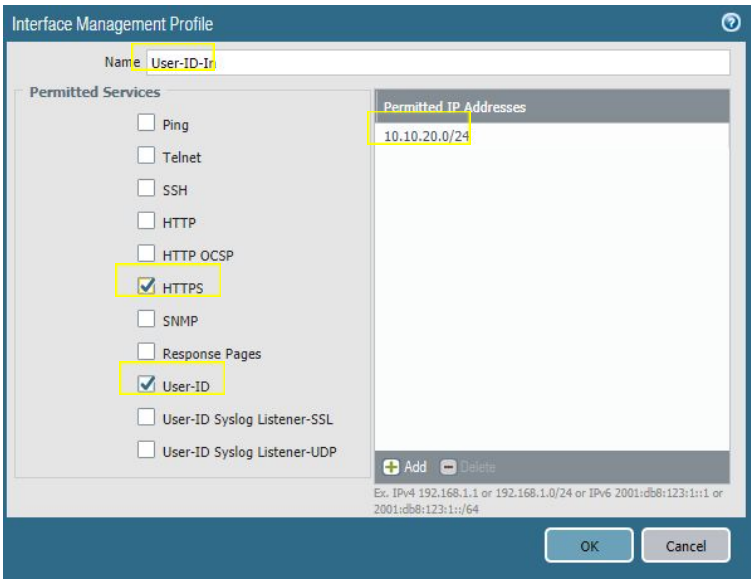

Zone
Name
trust
Log Setting
None
Type
Layer3
Interfaces
ethernet1/2
loopback.1
Add
Delete
Zone Protection
Zone Protection Profile
None
Enable Packet Buffer Protection
User Identification ACL
Enable User Identification
Include List
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add
Delete
Users from these addresses/subnets will be identified.
Exclude List
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Add
Delete
Users from these addresses/subnets will not be identified.
OK
Cancel

***Note**: In this example we are integrating NXT appliance on the Trust Interface/Zone to push User-to-IP mappings via API, since most enterprise networks will have separate management network for the management interface.*

Click the *Network Profiles, Interface MGMT, Add*



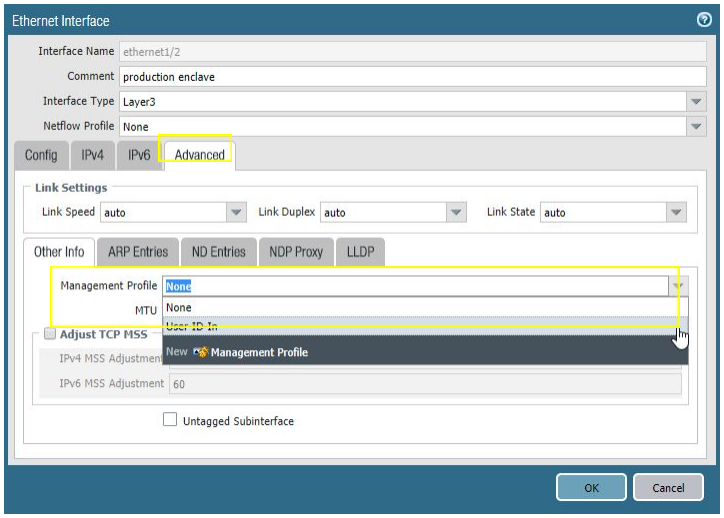
Give the Interface Management Profile a *Name,* then check *HTTPS* and *User-ID*. Add the CryptoniteNXT NAT'd Egress IP Range to *Permitted IP Addresses.* Click *OK.*



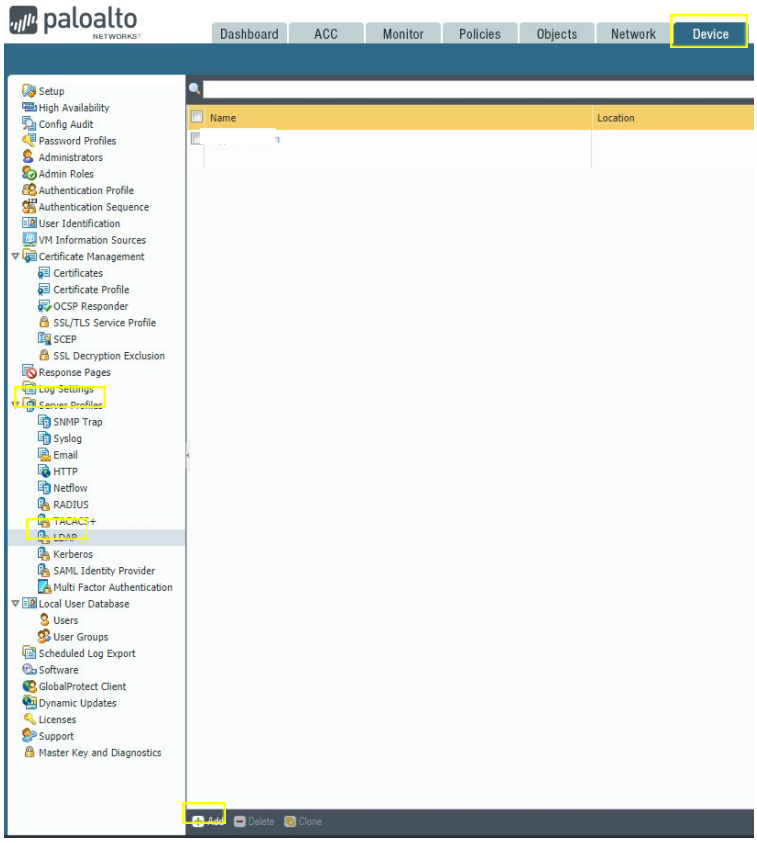
Associate Interface Management Profile with Interface in *Trust* Zone that will receive XML API POSTS from CryptoniteNXT ACC. Browse to *Network*, *Interfaces,* Click the *Interface.* In this example, *ethernet 1/2*.

Click *Advanced* tab, then select from *Management Profile* the Interface Management Profile created earlier.

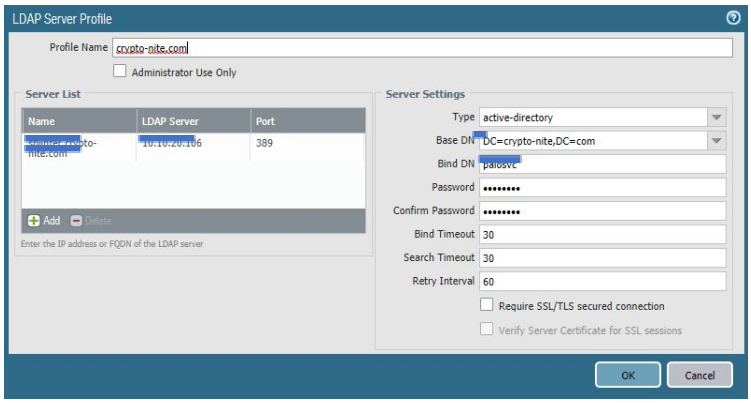
Click *OK.*



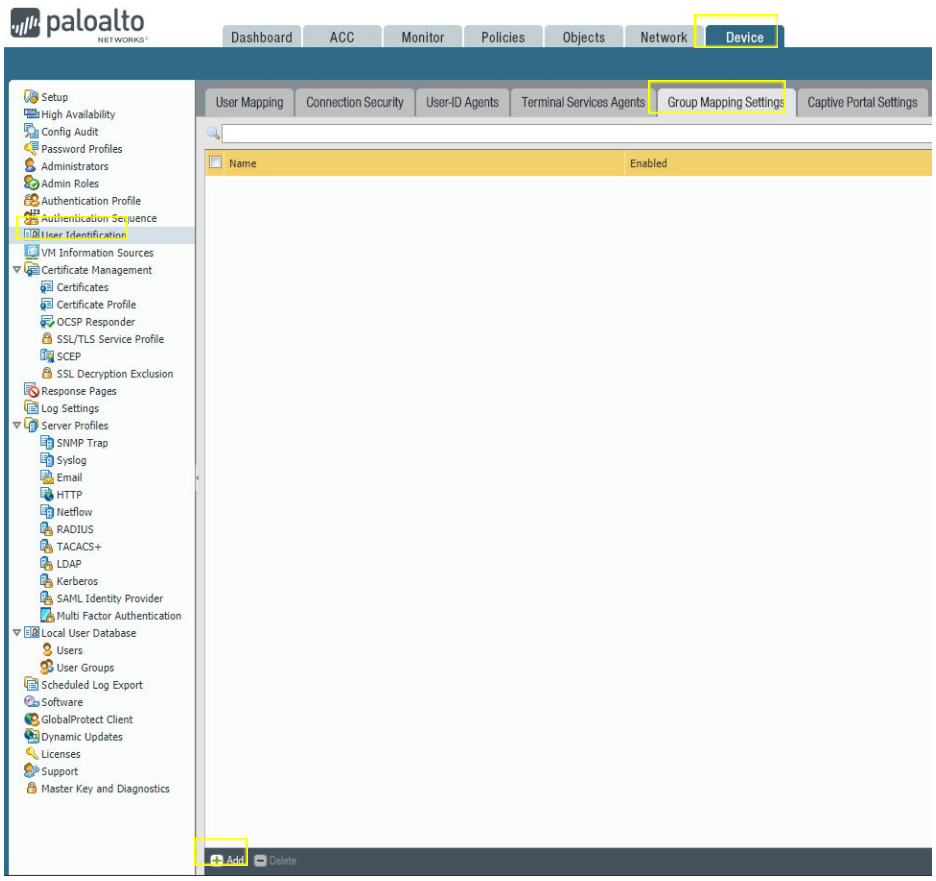
Click *Device* tab, *Server Profiles, LDAP, Add*



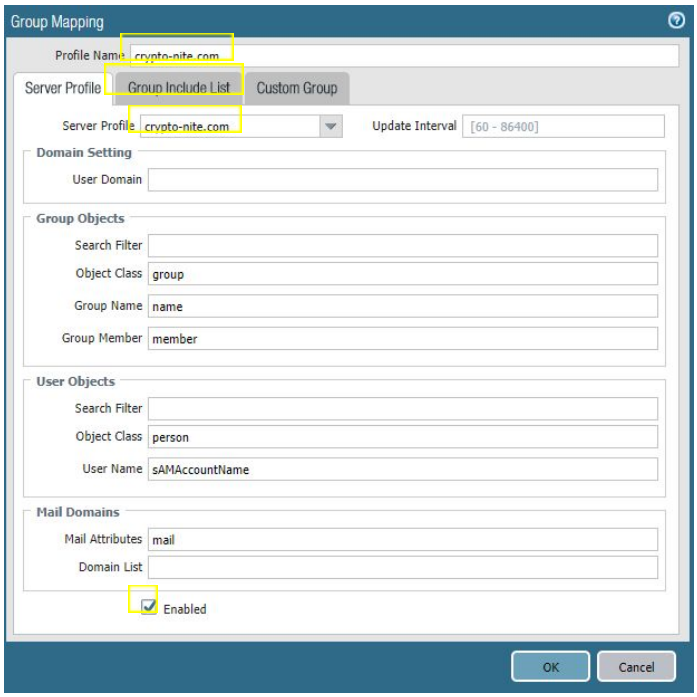
Enter information to connect to your organization's Active Directory.



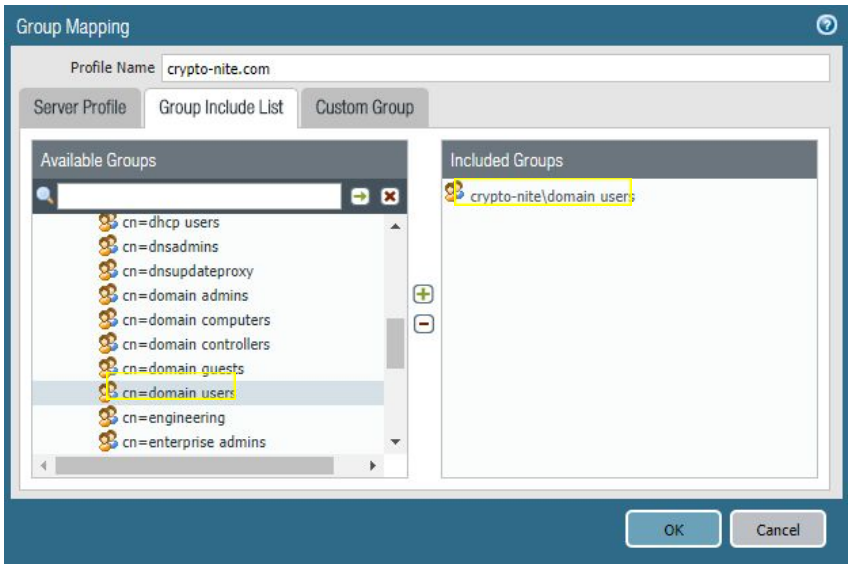
Click *Device* tab, *User Identification, Group Mapping Settings, Add*



Enter *Profile Name,* Select *Server Profile* (LDAP), Check *Enabled,* then Click *Group Include List*



Under *Available Groups*, browse the Active Directory for the Groups your organization would like to use in Access Control decisions, and add them to *Included Groups.* In this example, I will select *domain users.* Click OK.



Partner Product Configuration

This section explains how to configure the CryptoniteNXT ACC for integration with Palo Alto Next-Gen Firewall. These steps assume CryptoniteNXT system is operational.

From ACC GUI, click *Enable Editing*

Click *Integration*

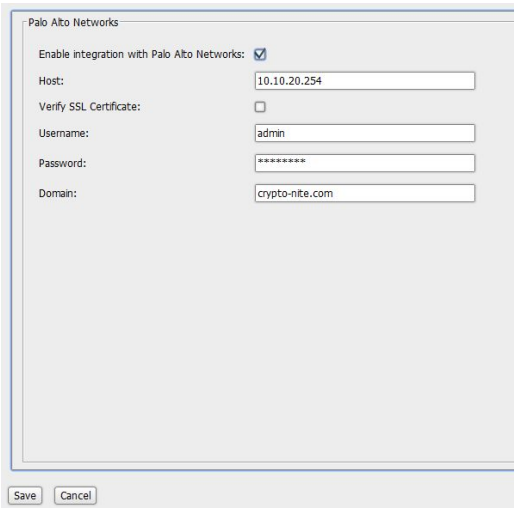
On the right side, Check Enable Integration with Palo Alto.

Host: IP address of Palo Alto interface to receive User-ID and HTTPS from ACC

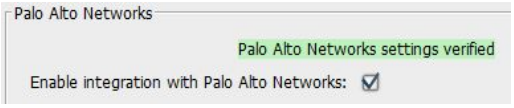
Username: Palo Alto Administrator user

Password: Palo Alto Administrator user password

Domain: Your org's domain name



Click Save. CryptoniteNXT will send test data to verify the credentials. Ensure Palo Alto Networks settings are displayed as verified in green.



Troubleshooting

This section explains how to verify the Palo Alto integration with CryptoniteNXT is working as expected.

Step 1 – Verify Credentials

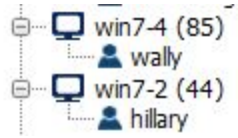
If the green verified message is not displayed after saving the Palo Alto integration settings within CryptoniteNXT, either the credentials are incorrect or basic network connectivity between the CryptoniteNXT ACC and the Palo Alto Next-Gen Firewall is not established. The CryptoniteNXT ACC GUI may provide additional information. Manually verify from the ACC or another CryptoniteNXT-protected endpoint that communication to port 443 of the Palo Alto Next-Gen Firewall is possible, using ping, netcat, wget, or similar connectivity diagnostic tools.

Step 2 – Verify Operation

Next verify that the system is functional by connecting to the part of the network that is integrated with CryptoniteNXT and Palo Alto – in this example we will connect a computer directly to a CryptoniteNXT Endpoint Node.

On the CryptoniteNXT ACC GUI, browse to *Display*

On the left panel, identify where a specific User is logged in. In this example, we are interested in Users Hillary and Wally, where we see Hillary logged in on Computer win7-2, and Wally logged in on Win7-4.

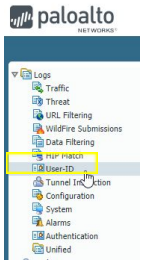


On the right panel, Select *Endpoints*, then *IPs*. We will then check to see an IP address has been allocated to the Computers that Hillary and Wally are logged into. These values will then be validated as the same in Palo Alto.

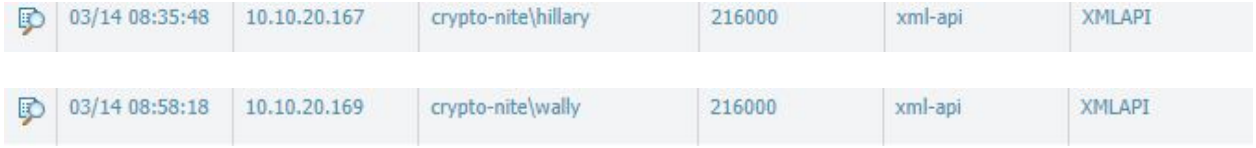
win7-1	58	cryp-54000001	☑	03/09/2018 17:35:17	10.10.20.143
win7-2	44	cryp-54000001	☑	03/09/2018 17:29:51	10.10.20.167
win7-3	206	cryp-54000001	☑	03/09/2018 17:23:58	10.10.20.153
win7-4	85	cryp-54000001	☑	03/09/2018 17:29:10	10.10.20.169
win7-5	11	cryp-54000001	☑	03/09/2018 17:32:19	10.10.20.151
win7-6	81	cryp-54000001	☑	03/09/2018 17:08:56	10.10.20.162
win7-7	221	cryp-54000001	☑	03/09/2018 17:34:17	10.10.20.164
win10-1	110	cryp-54000001	☑	03/09/2018 14:43:58	10.10.20.168
win10-2	37	cryp-54000001	☑	03/09/2018 14:43:54	10.10.20.159

On Palo Alto GUI, browse to *Monitor*

Select *Logs – User-ID*



Ensure user/computer identities are being mapped to an ip address, the Data Source is XMLAPI, and the associated identity/ip mapping aligns with the values seen in CryptoniteNXT ACC GUI. In the example below, Hillary is mapped to 10.10.20.167, and Wally is mapped to 10.10.20.169.



Technical Details

The integration between CryptoniteNXT and Palo Alto is via the User-ID API. See the following link for more details on this API:

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/enable-user-id for PAN OS 9.x or https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/enable-user-id for PAN OS 8.x

The integration operates the same regardless of whether CryptoniteNXT receives the user identity internally (e.g. via CryptoniteNXT's captive portal), via a CryptoniteNXT API, or via RADIUS. If a user is present on an endpoint, the username is provided. Otherwise, the endpoint's name is provided. If an endpoint is assigned separate ingress and egress IPs, User-ID entries for both IPs is automatically provided to Palo Alto.

Whenever CryptoniteNXT receives updated information to send to Palo Alto (e.g. on a new endpoint joining or a user logging in/out), the typical time for CryptoniteNXT to immediately push the new information is 100 ms. If CryptoniteNXT is unable to send data to Palo Alto after 3 consecutive attempts, re-sending will be attempted every few seconds until connectivity is restored. Since the Palo Alto Next-Gen Firewall loses any User-ID mappings on a reboot and to prevent any other potential de-synchronization of state, the full set of User-ID mappings are pushed to Palo Alto every 10 minutes.