Palo Alto Next Gen Firewall Integration – XML API

This document covers the API integration between the Nile Access Service and Palo Alto Networks (PAN) Next Generation Firewalls (NGFW) to provide secure campus networks through dynamic and granular segmentation.

Overview

This document covers the API integration between the Nile Access Service and Palo Alto Networks (PAN) Next Generation Firewalls (NGFW) to provide secure campus networks through dynamic and granular segmentation. The Nile Service Block (NSB) inside the Nile Access Service communicates with PAN?OS® through XML API calls to provide the NGFW with mappings of client IP addresses to their dot1x user identity and group. The dynamic exchanges enable organizations to apply granular segmentation policies based on the organization security strategies.
pana

Components required

- Nile Access Service
- PAN NGFW with PAN?OS® version 9.1 and higher
- HTTPS (TCP port 443) connection to PAN firewall for API communication
- RADIUS server

icon

NOTE

Note: The tests conducted in this guide used PAN-OS® 10.2.3-h4 and ClearPass. Although Clearpass is shown in this guide, any RADIUS server will work.

Feature flow

1. A dot1x user authenticates to a Nile Enterprise SSID.
2. The associated RADIUS server returns a ‘Filter-Id’ VSA holding the user group with the ‘Access-Accept’
3. The NSB maps the username, acquired client DHCP IP address and the user group and sends via XML API to the PAN NGFW.

4. The PAN firewall identifies the group as a configured tag with an associated dynamic group with a security policy that implements the desired access control on the user traffic.

Required steps

1. Setting up RADIUS to return ‘Filter-Id’ VSA
2. Setting up PAN NGFW to identify information sent from NSB
3. Setting up the Nile Access Service to communicate with PAN NGFW
4. Validate the integration

A. Setting up RADIUS to return 'Filter-Id' VSA

The screenshots below provide examples of the Enforcement Policy and associated Profiles necessary to display the ‘Filter-ID’ attribute returned by ClearPass. It is based on the Active Directory ‘memberOf’ attribute:
Enforcement Policy
enforce
Enforcement Profile
pa

icon

NOTE

Note: This guide shows ClearPass being used as a server, but any RADIUS server can be used. The ‘Nile Dot1x ClearPass Integration’ document should be reviewed for the complete ClearPass Policy Manager setup.

A. Setting up RADIUS to return 'Filter-Id' VSA

1. API Access

To create an administrator account, there are 2 steps that must be followed:

1. Create an Admin Role Profile. The screenshot below shows an example of profile named ‘nile-xml-role’
2. Add an administrator account and attach the Admin Role Profile created in step a. The screenshot below shows an example of the account created named ‘ nile-admin’ attaching to the Admin Role Profile named ‘nile-xml-role’

a. New Admin Role

1. Navigate to **Device > Admin Roles,** and click on the **Add** button

2. Enter the name “nile-xml-role”
3. Under the **Web UI** tab, disable all options
4. Under the **XML API** tab, disable all options except **User-ID Agent**
5. Click on **Ok** to complete the role addition

pap
b. New Administrator Account

1. Navigate to **Device > Administrators,** and click on the **Add** button
2. **Name:** Enter the name “nile-admin”
3. **Password:** Enter a password and confirm it
4. **Administrator Type:** Role Based
5. **Profile:** Select the “nile- xml-role” profile
6. Click on **Ok** to complete to new account creation

pi

2. Tags and Dynamic Address Group

Tags are identifiers that can be used to create Dynamic Address Groups. PAN?OS® utilizes those groups to form tag-based security policies.

For the API integration to work, Tags and Dynamic Address Groups are required. .The **Staff** and **Student** Group seen below illustrate how to create Tags. The Tags will be mapped with the user group information sent by the NSB. Subsequently, those two tags are used to configure two PAN-OS® dynamic Address Groups: **Staff-role** and **Student-role**.

Create two Tags

1. Navigate to **Objects > Tags**, and click on the **Add** button
2. Add two Tags named Staff and Student

ps
ps
pe

Create two Dynamic Address Groups

1. Navigate to **Objects > Address Groups**, and click on the **Add** button
2. Add two Address Groups Staff-role and Student-role of type **Dynamic** matching respectively the Staff and Student

pnine
pten

3. Security policies

This guide assumes that the Nile NSB is connected to the Palo Alto Networks firewall through two ports that are both assigned to a newly created security zone called NSB.

To illustrate an example usage of security policies based on the Dynamic Address Groups created in the previous section, two security policies are created to allow all traffic matching the ‘Staff’ Tag, and deny access to the ‘wargaming.net’ and ‘traceroute’ for traffic matching the ‘Student’ Tag:
pele

4. Loopback address

Since the NSB connects to the PAN firewall through two Equal Cost Multi-Path (ECMP) interfaces, it is recommended to configure a loopback IP address that the NSB can use to connect to the firewall, no matter which interface the XML API traffic flows through.

For illustration purposes, the following loopback setting is shown below:

ptwel

c. Setting up the Nile Access Service to communicate with PAN NGFW

The following screenshots shows an example on how to accomplish that on the Nile Portal:

1. DHCP – Set the DHCP server and subnets for the user groups

pthor

2. Authentication – Set the RADIUS server parameters

pfor

3. Segments – Map the DHCP server and authentication method to the user segment

pfif

4. Wireless – Set up the SSID and attach user segment(s)

psix

d. Validate the integration

The validation steps below show what to look for when validating asuccessful dot1x authentication, returning the correct user group/tag through the ‘Filter-id’ attribute from ClearPass Policy Manager.

1. RADIUS server

Validate that the RADIUS server has assigned the appropriate role with the correct “FilterId’. The example below demonstrates ClearPass assigned the correct role to ‘**student1**’ through the returned attribute ‘Filter-Id’ with the value ‘**Student**’:
pseven
peight
A second validation for the user ‘**staff1**’ is shown below:
pnine
ptwenty

1. RADIUS server

Automatic correlation of IP to User-ID

Inside the PAN management dashboard, validate that there is correct mapping between IP and User-ID. The image below demonstrates the correct mapping between the users ‘student1’ and ‘staff1’ to their respective IP addresses 172.16.14.14 and 172.16.14.15:
pto

Automatic correlation of IP to User-ID

Inside the PAN management dashboard, validate that there is correct mapping between IP addresses and tags. The image below demonstrates the correct mapping betweenIP addresses to their respective tags:
ttw

Traffic Flow

Inside the PAN management dashboard, validate that traffic logs are available with the right flow. The image below demonstrates that security policies created did enforce as intended. The traffic log shows that ‘wargaming.net’ and ‘traceroute’ were denied for the user ‘student1’ with IP address 172.16.14.14, when it was allowed for user ‘staff1’ with IP address 172.16.14.15:
ptthe
tf

icon

NOTE

Note: It is recommended to create a dedicated administrator account inside the management console with the purpose of handling XML API communication initiated by ClearPass. Note: Nile recommends contacting a Nile Operator to assist for backend setup. Before contacting a Nile Operator, make sure to create an enterprise (dot1x) SSID.

Note: Nile recommends contacting a Nile Operator to assist for backend setup. Before contacting a Nile Operator, make sure to create an enterprise (dot1x) SSID.