Palo Alto Network’s Next-Generation Firewall

This document is designed to assist with integrating Palo Alto Network Next-Generation Firewall in High Availability to allow traffic to be received from the Nile Service Block or send traffic into the NSB.

Overview

The Nile Service Block (NSB) connects to one or two upstream Palo Alto Next Generation Firewall (NGFW) appliances, over point-to-point layer 3 links, and pushes all client traffic (north-south or east west) to the NGFW appliance. Such design puts the customer in full control of the NSB traffic, to implement the desired security policies.

This document purpose is to assist with the seamless integration between the Nile NSB and the Palo Alto NGFW appliance.

Requirements

- Administrator rights to the Nile Portal.
- **NSB IP pool**:
  This is the IP pool used for the management plane of the NSB Elements to communicate with the Nile Cloud.
- **Sensor IP pool**:
  This is the IP pool used for the management plane of the Nile Sensors to communicate with the Nile Cloud.
- **Four /30 subnets**:
  These are the four (4) Equal Cost Multi-Path (ECMP) L3 links between the Nile gateways and the Palo Alto NGFW appliance, to achieve a High-Definition and Always-On service.
- **Client subnets**:
  These are the subnets defined on the Nile Portal and used by wired and wireless devices connected to the Nile Service.
- **Servers Addresses**:
  These are the IP addresses of the customer DHCP, DNS, and RADIUS servers that are to be defined on the Nile Portal.

Topology Diagram

pan topology diagram

icon

NOTE

Note: It is important to diagram the interface IP assignments. For illustration purposes, this document uses the following interfaces and IP subnets:

Uplink subnets:

PA-1 to GW-1 link: 172.16.7.0/30

PA-1 to GW-2 link: 172.16.7.4/30

PA-2 to GW-1 link: 172.16.7.8/30

PA-2 to GW-2 link: 172.16.7.12/30

PAN Interfaces:

ethernets: 1/1 to 1/4 NSB uplinks (only two are needed for a single PAN)

ethernet1/5 LAN (on-prem Servers network)

ethernet1/6 High Availability (HA2)

ethernet1/7 WAN1

ethernet1/8 WAN2

Mgmt HA1

Setup

Multiple sections need to be set up on the Palo Alto Next Generation Firewall:

1. Zones
2. Profiles
    1. Management
    2. LLDP
3. Interfaces
    1. NSB Interfaces
    2. WAN Interfaces
    3. LAN Interface
4. Routing
    1. Static (WAN)
    2. OSPF or Static (NSB)
5. Firewall Rules
6. NAT Rules

7. High Availability (Active – Passive)

Before starting, log into the administrator web page of your Palo Alto NGFW appliance.

A. Single/Active Firewall

1. Zones

To define the Internet, LAN and NSB zones, go to **Network g Zones:**

network g zones
Figure 1

NSB

Click on **+Add** button (at the bottom of the Zone screen) to create a new zone:

1. **Name:** NSB
2. **Log Setting:** SNMP traps or syslog could be defined as needed.

(drop down menu)

1. **Type:** Layer3 (drop down menu)
2. **Interfaces:** Add the NSB assigned interfaces 1/1 to 1/4.

(**+ Add** button at bottom of Interfaces panel for each.)

1. **Zone Protection Profile:** Define to match your environment.

NSB
Figure 2

Internet

Click on **+Add** button (at the bottom of the Zone screen) to create another new zone:

1. **Name:** Internet
2. **Log Setting:** SNMP traps or syslog could be defined as needed.
3. **Type:** Layer3
4. **Interfaces:** Add the WAN interfaces 1/7 and 1/8.
5. **Zone Protection Profile:** Define to match your environment.

internet
Figure 3

LAN
Repeat the Add Zones step to create the LAN zone and add the assigned interface 1/5 to it:

LAN
Figure 4

Once the above setup steps are complete, the Zones page looks like this:

figure 5
Figure 5

2. Profiles

Management Profile

Go to **Network ? Network Profiles ? Interface Mgmt**:

Click on **+ Add** button, and enable the desired services with security concerns in mind.
The following screenshots illustrate two profiles: NSB and WAN:

figure 6
Figure 6

figure 7
Figure 7

LLDP Profile

Go to **Network ? Network Profile ? LLDP Profile**
Click on the **+ Add** button:

- **Name:** LLDP Enable
- **Mode:** transmit-receive
- **Optional TLVS:** Enable all 4 options (Port Description, System Name, System Description, System Capabilities)

figure 8
Figure 8

3. Interfaces

To set up Interfaces,
go to **Network ? Interfaces ? Ethernet:**

NSB Interfaces

Two interfaces (2) are needed for a single firewall, and four (4) for an Active-Passive set of two firewalls. This document is using Ethernet1/1 to Ethernet1/4 as the four uplinks to the NSB:

Ethernet1/1:

Click the Interface ethernet1/1, and set the following:

1. **Comment:** Link to Nile GW-1

2. **Interface type:** Layer3
3. **Config** tab:
    1. **Virtual Router:** default
    2. **Security Zone:** NSB

nine
Figure 9

4. **IPv4** tab:

a. **Type:** Static

b. **IP:** 16.7.1/30

ten
Figure 10

5. **Advanced** tab:

a. **Management Profile:** Select the NSB profile.

ele
Figure 11

a. **LLDP**: Enable LLDP and Select the ‘LLDP enable’ profile

twe
Figure 12

Repeat the same procedure for Ethernet1/2 through Ethernet1/4:

Ethernet1/2: 172.16.7.5/30
Ethernet1/3: 172.16.7.9/30
Ethernet1/4: 172.16.7.13/30

This completes the setup for the four uplink interfaces to the NSB.

WAN Interfaces

In this document, the firewall(s) is/are connected to two ISPs through interfaces Ethernet1/7 and Ethernet1/8, for redundancy purposes.

Ethernet1/7:

Click the Interface ethernet1/7, and set the following:

1. **Comment:** Link to Nile ISP1
2. **Interface type:** Layer3
3. **Config** tab:
    1. **Virtual Router:** default
    2. **Security Zone:** Internet

4. **IPv4** tab:
    1. **Type:** Static
    2. **IP:** 1.251.236/27
5. **Advanced** tab:
    1. **Other Info:**
        1. **Management Profile:** WAN

figure 13
Figure 13

Ethernet1/8:

Click the Interface ethernet1/8, and set the following:

1. **Comment:** Link to Nile ISP2
2. **Interface type:** Layer3
3. **Config** tab:
    1. **Virtual Router:** default
    2. **Security Zone:** Internet
4. **IPv4** tab:
    1. **Type:** Static
    2. **IP:** 1.252.236/27
5. **Advanced** tab:
    1. **Other Info:**
        1. **Management Profile:** WAN

figure 14
Figure 14

LAN subnet

This setting specifies the interface to a directly-attached server farm, or the core network. It is shown here for completion purposes:

figure 15
Figure 15

3. Routing

To set up routing on the PAN firewall, go to **Network ? Virtual Routers**.

figure 16
Figure 16

The virtual router **default** is used in this document, and all interfaces have already been added in the previous section. Click on “default” link to see the settings:

figure 17
Figure 17

WAN Routing (static)

Static routing is used on the WAN with two (2) default routes added, for ISP1 and ISP2. ISP1 is the primary and receives a metric of 10. ISP2 acts as a backup with a metric of 100.

Click the '**Static Routes**' selector in the Virtual Router panel.

figure 18
Figure 18

Click the '**+ Add**' button in the pop-up to add 2 static routes as follows:

ISP1:

- **Name:** Default Route
- **Destination:** 0.0.0/0
- **Interface:** ethernet1/7
- **Next Hop:** IP Address – 10.1.251.225
- **Metric:** 10
- **Route Table:** Unicast
- **Path Monitoring:**
    - **Failure Condition:** Any
    - **Path Monitoring Destination:**
        - **Name:** Pri-Default-GW
        - **Enable**
        - **Source IP:** 1.251.236/27
        - **Destination IP:** 1.251.225
        - **Ping Interval:** 3
        - **Ping Count:** 5

figure 19
Figure 19

ISP2:

- Name: Backup Default Route
- Destination: 0.0.0/0
- Interface: ethernet1/8
- Next Hop: IP Address – 10.1.252.225
- Metric: 100
- Route Table: Unicast

figure 20
Figure 20

NSB Routing

Important:
For the Nile service to operate correctly, it is critical that the following subnets are routed back by the PAN firewall to the NSB gateways:

- NSB subnet

- Sensor subnet
- All client subnets
- Servers (DHCP, Radius, DNS) hosts/subnets

Two routing options to the Nile NSB are supported: **static** or **dynamic (OSPF)**

Option 1: Static routing with ECMP

In this document, the following subnets:

- NSB subnet: 16.8.0/24
- Sensor subnet: 16.9.0/24
- Client subnets: 16.10.0/24 – 172.16.15.0/24

Therefore, four (4) static routes are added to the aggregated subnet: 172.16.8.0/21, one for each of the downlinks to the Nile Gateways.

Since Nile traffic to the PAN firewall uses flow based ECMP routing through both Nile Gateways, it is important to enable ECMP on the firewall:

1.1 ECMP setup:

Go to **Virtual-Router g default g Router Settings g ECMP**
Select the following:

- **Enable**
- **Max Path:** 4
- **Load Balance Method:** Weighted Round Robin
- Add all interfaces to the NSB, namely ethernet1/1 to ethernet1/4

figure 21 1
Figure 21

1.2 Static routes:

Add four (4) **equal cost** static routes for the aggregated subnet in this example:

figure 22
Figure 22

1.3 Route validation

Inspect the routing table and forwarding table to validate the static routes to the aggregate subnet 172.16.8.0/21, by clicking **More Runtime Stats** under **Network g Virtual Routers:**

figure 23
Figure 23

Routing table:

figure 24
Figure 24

Forwarding table:

figure 25
Figure 25

Option 2: Dynamic routing (OSPF)

2.1 ECMP setup:

The setup is the same as has been defined in the static routing section.

2.2 OSPF setup:

Go to **Network g Virtual Routers g default g OSPF**
Set the following:

- **Enable:** checked
- **Reject Default Route:** unchecked
- **Router ID:** 0.0.1 in this example (unique IP address)

figure 26
Figure 26

Add the interfaces connected to the NSB (ethernet1/1 to ethernet1/4), one by one:

- **Areas:** Click **+ Add**
  - **Area ID:** 0.0.0
  - **Type:** Normal
  - **Interface:** click **+ Add**

figure 27
Figure 27

- Select the Interface (ethernet1/1 – ethernet1/4)
- **Link Type**: Broadcast (from the pull-down list)
- **Timing** section:
  - **Hello Interval**: 1 (for faster convergence)
  - Other timers: default values
- **Metric/Priority:** defaults
- **Auth Profile:** None (from the pull-down list)

figure 28
Figure 28

- Repeat the above for the other three (3) interfaces.

figure 29

Figure 29

- **Export Rules:**

    - Click the '**Export Rules**' tab
    - **Allow Redistribute Default Route:** checked

figure 30
Figure 30

- Click **+ Add**
    - **Name:** 0.0.0/0
    - **New Path Type:** Ext 1 (radio button)
    - **Metric:** 10

figure 31
Figure 31

A summary of the virtual router 'default' setup is illustrated below:

figure 32
Figure 32

icon

NOTE

If no aggregation is used, then four (4) equal-cost routes are needed for the NSB, sensors, and client subnets.

4. Firewall Rules

By default, Palo Alto Next Gen firewall allows intrazone (within the same zone) traffic and denies / blocks interzone (between two different zones) traffic.

As three zones were created in this document – (1) Internet, (2) NSB and (3) LAN – rules are needed to allow traffic from the LAN and NSB zones to the Internet zone, and between the NSB and LAN zones.

figure 33
Figure 33

4.1 LAN/NSB Access to the Internet

Go to **Policies g Security**
Click on **+ Add** to create the policy as follows:

- **Name:** LAN-NSB to Internet
- **Rule Type:** Universal
- **Source** column set:
    - **Source Zone:** LAN and NSB
    - **Source Address:** Any
    - **Source User:** Any
    - **Source HIP Profile** Any
- **Destination** column set:

    - **Destination Zone:** Internet
    - **Destination Address:** Any
- **Application:** Any
- **Service/URL Category:** Any
- **Action:** Allow

4.2 NSB/LAN Access

Go to **Policy g Security**
Click on **+ Add** to create the policy as follows:

- **Name:** NSB-LAN
- **Rule Type:** Universal
- **Source:**
    - **Source Zone:** LAN and NSB
    - **Source Address:** Any
    - **Source User:** Any
    - **Source HIP Profile** Any
- **Destination:**
    - **Destination Zone:** LAN and NSB
    - **Destination Address:** Any
- **Application:** Any
- **Service/URL Category:** Any
- **Action:** Allow

icon

NOTE

The above rules are provided as an example; it is up to customers to change them according to the requirements of their security policies.

5. NAT Rules

By default, the Palo Alto Next Gen Firewall does not NAT traffic. Source NAT rules are needed for internal traffic using private addresses to reach the Internet.

Since this document covers a dual ISP environment, two source NAT rules are needed for each ISP.

Go to **Policies g NAT**
Click on **+ Add** to create the Source NAT rules:

figure 34
Figure 34

4.2 NSB/LAN Access

- **General:**
    - **Name:** provide a name for the rule

    - **NAT Type:** ipv4
- **Original Packet** tab:

figure 35
Figure 35

- **Source Zone:** NSB and LAN (check boxes)
- **Destination Zone:** Internet (from pull-down list)
- **Destination Interface:** ethernet1/7 (from pull-down list)
- **Service:** Any (from pull-down list)
- **Source Address:** Any (check box)
- **Destination Address:** Any (check box)

- Translated Packet tab:

figure 36
Figure 36

- **Source Address Translation:**
    - **Translation Type:** Dynamic IP and Port (from drop-down list)
    - **Address Type:** Interface Address (from drop-down list)
    - **Interface:** ethernet1/7 (from drop-down list)
    - **IP Address:** 1.251.236/27 (from drop-down list)

4.2 NSB/LAN Access
Repeat the previous step using interface **ethernet1/8**, with the **Translated Packet** tab reflecting the following:

figure 37
Figure 37

B. Two firewalls

1. HA (Active-Passive)

It is important to abide by the Palo Alto prerequisites for Active/Passive HA (high availability), as detailed in the following URL:

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/set-up-activepassive-ha/prerequisites-for-activepassive-ha#id78977437-fe66-4204-9690-5a673fc8dd35

HA Ports

The HA ports could be dedicated or assigned based on the firewall model

In this document the following HA ports are utilized:

Control Link (HA1): Management
Data Link (HA2): ethernet1/6

Active Firewall

General Setup

Go to **Device ? High Availability ? General**
where the setup is divided into sections accessible through their own setup button.

figure 38
Figure 38

Click the config button within each section to access the settings, starting with the **Setup** section:

- **Setup** (config button)

figure 39
Figure 39

- - **Enable HA:** Check the box
  - **Group ID:** 10
  - **Mode:** Active-Passive (radio button)
  - **Enable Config Sync:** Check the box
  - **Peer HA1 IP Address:** 1 1.250.6 (peer management IP in this document)
- **Active/Passive Setting** (config button)

figure 40
Figure 40

- **Passive Link State:** Auto

- **Control Link (HA1)** (config button)
  - The management port is used in this document

- **Data Link (HA2)** (config button)

figure 41
Figure 41

- **Enable Session Synchronization:** Check the box
- **Port:** ethernet1/6
- **IPv4/IPv6 Address:** 168.224.1
- **Netmask:** 255.255.252
- **Transport:** ethernet (dropdown)
- **HA2 Keep-Alive:** Check the box
  - **Action:** Log Only

- **Election Settings** (config button)
  - Device Priority: 100 (HA Active with Peer set to 200)
  - Preemptive: leave unchecked in this document
  - HA Timer Settings: Recommended (in this document)

figure 42
Figure 42

Link and Path Monitoring

This setup defines the failover conditions and could use link and/or path monitoring to determine what causes a PAN firewall to fail over.

This document covers link monitoring of the NSB and WAN interfaces.

Two groups are defined: NSB and WAN

The NSB link monitoring comprises the active interfaces on each firewall, namely:

- Ethernet1/1 and ethernet1/2 on the Active firewall
- Ethernet1/3 and ethernet1/4 on the Passive firewall

The WAN link monitoring has both ISP1 and ISP2 interfaces (Dual ISP).

To set up HA link monitoring,
go to **Device ? High Availability ? Link and Path Monitoring**,
Define as shown:

figure 43
Figure 43

Passive Firewall

General Setup

Repeat the setup steps taken in the Active firewall section to define HA on the Passive firewall paying attention to the following:

- Same group ID: 10
- Peer HA1 IP Address Active firewall management port IP
- Higher Device priority in Election Settings
- Data Link (HA2) IP Address: 192.168.224.2

figure 44
Figure 44

Link and Path Monitoring

45b
Figure 45

Click the Commit button on each firewall to save the setup and make it operational.

Once synchronized, the High Availability widget on each firewall should reflect their state and that their setup is in sync:

figure 46
Figure 46
fs
Figure 47

icon

NOTE

1. The management ports of both firewalls have ip connectivity.
2. Ping is enabled and permitted on the management interface.
3. HA2 ports are connected via an ethernet cable.