

Dossier de spécifications techniques

Déploiement Stormshield

Description : si:COMMUN SI:_CREATION:NOMIOS:NOMIOS_15_refonte_logotype:Nomios_Logo HD CMJN.eps

SOMMAIRE

[1 Introduction 4](#_Toc5696073)

[2 Spécifications matérielles 5](#_Toc5696074)

[2.1 PA-5260 5](#_Toc5696075)

[2.2 Panorama 5](#_Toc5696076)

[3 Déploiement du cluster de PA-5260 7](#_Toc5696077)

[3.1 Description 7](#_Toc5696078)

[3.2 Version de Panos 7](#_Toc5696079)

[3.3 Convention de nommage 7](#_Toc5696080)

[3.4 Connectique 8](#_Toc5696081)

[3.5 Architecture de Niveau 2 12](#_Toc5696082)

[3.6 Architecture de Niveau 3 17](#_Toc5696083)

[3.7 Mise en cluster 30](#_Toc5696084)

[3.8 Configuration générale 31](#_Toc5696085)

[3.9 NSX 31](#_Toc5696086)

[3.10 User ID 31](#_Toc5696087)

[4 Panorama 32](#_Toc5696088)

[4.1 Eléments de configuration 32](#_Toc5696089)

[4.2 Matrice de flux Panorama 32](#_Toc5696090)

[5 Politique de sécurité 34](#_Toc5696091)

DIFFUSION

|  |
| --- |
| Organisme ou Entreprise |
| Nom des destinataires | Support Nomios |
| Pour action | x |
| Pour Information | x |

SUIVI DES VERSIONS

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | NOM DU REDACTEUR | NATURE DE LA MODIFICATION |
| V0.1 | 12/08/2019 | Zakaria EL HARTI | Création document |
| V0.2 | 12/08/2019 | Zakaria EL HARTI | Modification et ajout |
| V0.3 | xx/xx/2019 | Zakaria EL HARTI | Version finale(corrections, ..) |

# Description : si:COMMUN SI:_CREATION:NOMIOS:NOMIOS_15_refonte_logotype:Nomios_Logo HD CMJN.epsIntroduction

Ce Dossier de Spécifications Détaillées référence les éléments de configuration qui seront utilisés dans le déploiement d’un Stormshield SN160 et de ses fonctionnalités.

Ce Firewall UTM NextGen sera entouré d’équipements réseaux variés afin de proposer une architecture complète autour de ce Firewall.

# Spécifications matérielles

## SN-160



|  |  |
| --- | --- |
| Référence | SN-160 |
| Firewall throughput (App-ID) | 1 Gbps |
| Threat Prevention throughput | 800 Mbps |
| Antivirus troughput | 100 Mbps |
| New sessions per second | 6,000 |
| Max sessions | 150,000 |
| Filtering rules (Max) | 4,096 |
| Interfaces supported NPC option | (5) 10/100/1000 |
| Power supply | 100-240V 60-50Hz 1,5-0,8A |

# Déploiement du SN-160

## Description

L’équipement SN-160 sera déployé en mode de fonctionnement seul. La mise en cluster n’étant possible qu’entre équipements physiques.

L’activité du Firewall interviendra sur les couches 4 à 7 du modèle OSI.

Le projet est composé de plusieurs étapes :

* Etape 1 : Mise en place du Firewall dans le LAB de l’entreprise (Configuration réseaux, interfaces, VLANs..)
* Etape 2 : Création d’un PC client et tests de règles de filtrage(URL, SSL..)
* Etape 3 : Mise en place de l’architecture complète autour du Firewall et tests finaux

## Version de Stormshield

Le Firewall Stormshield est déployé en version 3.7.5, il s’agit de la version actuelle communément utilisée chez les clients de Nomios.

## Convention de nommage

|  |  |
| --- | --- |
| Equipement | Description |
| SN160-STMD | Equipement Firewall SN160 Stormshield |

## Connectique

### Schéma physique existant

Une image contenant texte

Description générée automatiquement

Le schéma ci-dessous correspond au câblage des interfaces :

Une image contenant capture d’écran

Description générée automatiquement

### Câblage

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Equipement | Port | Equipement | Port | Type | Description |
| PA 3050 |  | SRX 1500 | ge-0/0/8 | 10G | Liaison simple |
| SRX 1500 |  | EX1 | ge-0/0/1 | 4G | Liaison simple |
| SRX |  | EX1 | ge-0/1/1 | 4G | Agrégat |
| EX 2200(EX1) |  | EX | ge-0/1/0 | 4G | Agrégat |
| EX |  | SN 160 | eth1 | 1G | Interface IN |
| EX |  | SN 160 | eth0 | 1G | Interface OUT |

## Architecture de Niveau 2

### Schéma niveau 2 cible

Une image contenant capture d’écran

Description générée automatiquement

### Interface VLAN

|  |  |  |  |
| --- | --- | --- | --- |
| Interface SN-160 | 802.1Q | VLAN ID | Description |
| IN | N/A | 1773 | eth1 – Interface LAN/DMZ |
| OUT | N/A | 1873 | eth0 – Interface WAN |

### Listes des VLANS

Le tableau ci-dessous liste l’ensemble des VLAN porté par le SN 160 :

|  |  |  |
| --- | --- | --- |
| VLAN ID | Network | Description |
| 1773 | 172.17.73.0/24 | VLAN interne – LAN/DMZ |
| 1873 | 172.18.73.0/24 | VLAN externe - Untrust |

## Architecture de Niveau 3

### Schéma logique cible

|  |  |  |
| --- | --- | --- |
| Interface | IP | Masque |
| IN | 172.17.73.33 | 255.255.255.0 |
| OUT | 172.18.73.76 | 255.255.255.0 |

Ci-dessous le schéma logique représentant les interconnexions du Firewall Stormshield :

Une image contenant texte

Description générée automatiquement

### Adressage IP

Le tableau ci-dessous regroupe l’ensemble des IPs dans les VLANs du SN 160.

|  |  |  |  |
| --- | --- | --- | --- |
| Machine | IP Address/Mask | Gateway | VLAN |
| KALI | 172.18.73.209/24 | 172.18.73.76 | 1873 |
| Serveur Web | 172.17.73.243/24 | 172.17.73.33 | 1773 |
| PC Client | 172.17.73.34/24 | 172.17.73.33 | 1773 |

### Routage

###### Routage Statique :

Ci-dessous la route par défaut qui a été implémentée sur le SN :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Destination | | | Interface | Next hop |
| 0.0.0.0/0 |  |  | OUT | 172.18.73.254 |

## Configuration générale

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Name | IP | Description |
| NTP Server | ntp1.stormshieldcs.eu | 92.222.122.235 |  |
| ntp2.stormshieldcs.eu | 151.80.252.82 |  |
| DNS Server | dns1.google.com | 8.8.8.8 |  |
| dns2.google.com | 8.8.4.4 |  |
| Administration | Firewall administration page | 172.18.73.76/admin |  |

### Active Directory

L’authentification des administrateurs est faite par le biais du serveur AD.

Paramètres de la configuration :

|  |  |  |
| --- | --- | --- |
|  | Valeur | Description |
| Microsoft Active Directory |  | Authentification des utilisateurs |
| Nom de domaine | Infra-lab.nms.lab |  |
| Serveur | Server\_adlab | 172.16.0.219 |
| Format/Type | Annuaire LDAP | LDAP externe |

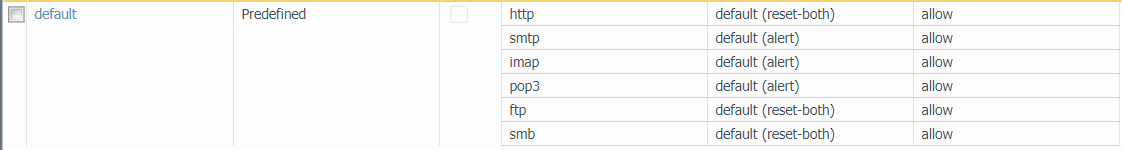
# Politique de sécurité

### Profils de sécurité/VPN

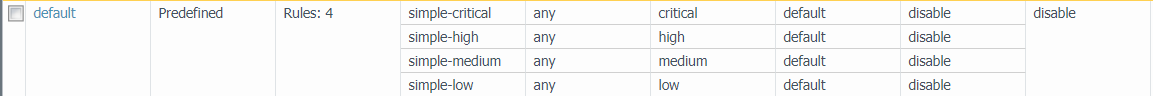
Les profile Antivirus, Antispyware et IPS associés à la licence Threat Prevention seront configurés par défaut dans un premier temps.

PROBTP ne dispose pas de licence TP.

Profil Antivirus



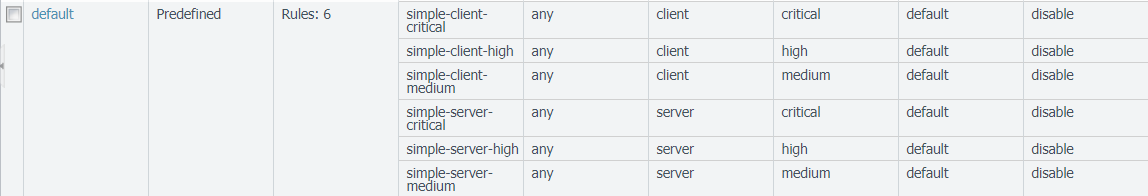
Profil Anti-spyware



L’action default correspond à l’action associée à la signature (drop, reset, reset-both,alert).

Le DNS sinkhole sera configuré

Profil IPS



L’action default correspond à l’action associée à la signature (drop, reset, reset-both,alert).

### Règles

Nous avons reporté les règles du Checkpoint la section OM et IA sur les Palo Alto Network.

