



DOSSIER DE SPECIFICATIONS TECHNIQUES

DEPLOIEMENT STORMSHIELD

SOMMAIRE

1	INTRODUCTION	4
2	SPECIFICATIONS MATERIELLES	5
2.1	SN-160	ERREUR ! SIGNET NON DEFINI.
3	DEPLOIEMENT DU SN-160	6
3.1	DESCRIPTION	6
3.2	VERSION DE STORMSHIELD	6
3.3	CONVENTION DE NOMMAGE	6
3.4	CONNECTIQUE	7
3.5	ARCHITECTURE DE NIVEAU 2	9
3.6	ARCHITECTURE DE NIVEAU 3	9
3.7	CONFIGURATION GENERALE	ERREUR ! SIGNET NON DEFINI.
4	POLITIQUE DE SECURITE	ERREUR ! SIGNET NON DEFINI.
4.1	PROFILS DE SECURITE	ERREUR ! SIGNET NON DEFINI.
4.2	REGLES	ERREUR ! SIGNET NON DEFINI.



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	28/08/2019	Zakaria EL HARTI	Modifications et ajouts
V0.3	10/09/2019	Zakaria EL HARTI	Version finale(corrections, ..)



1 Introduction

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.

2 Spécifications matérielles

2.1 SN-160



Référence	SN-160
Firewall throughput (App-ID)	1 Gbps
Threat Prevention throughput	800 Mbps
Antivirus throughput	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

3 Déploiement du SN-160

3.1 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

3.2 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.

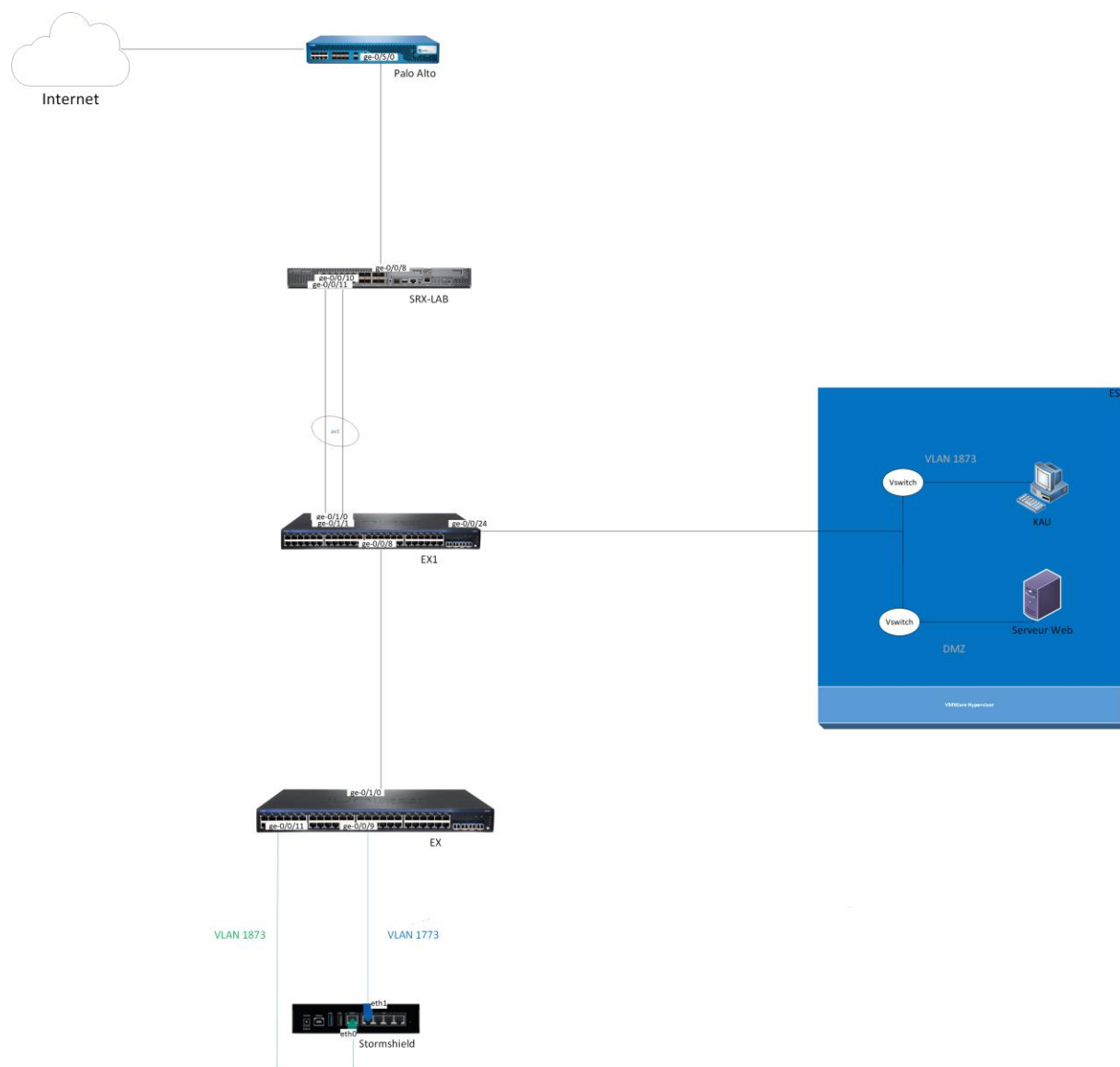
3.3 Convention de nommage

Equipement	Description
SN160-STMD	Equipement Firewall SN160 Stormshield



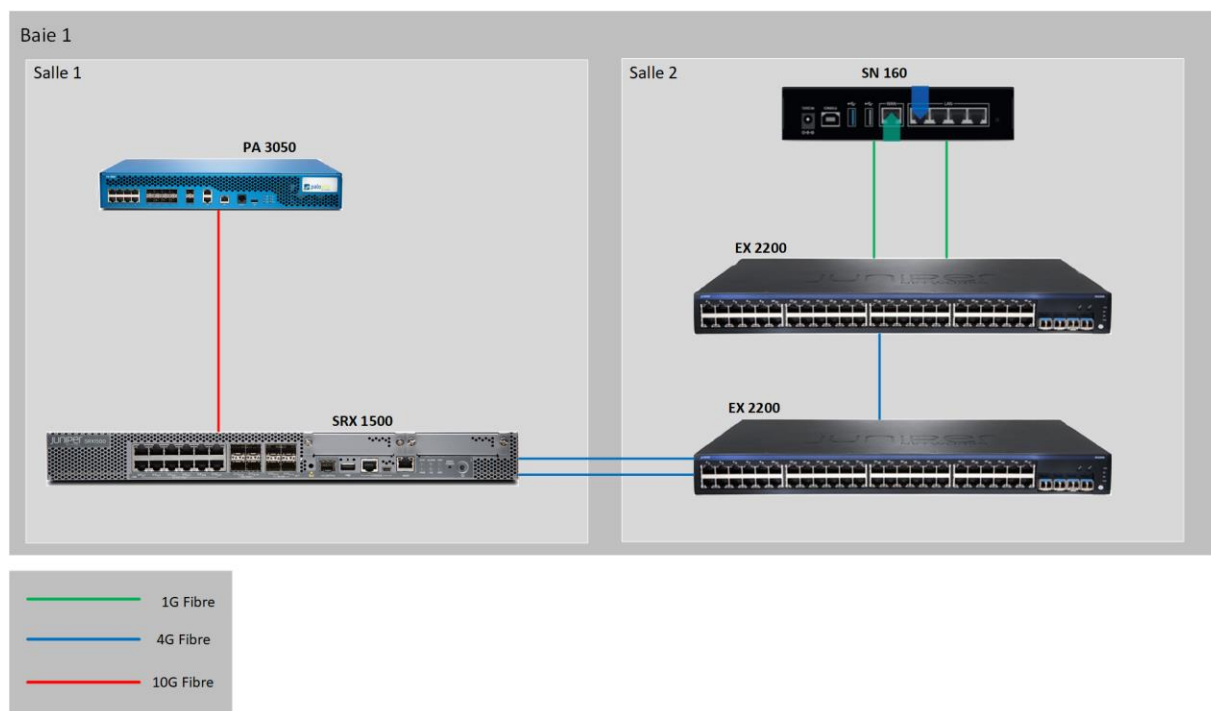
3.4 Connectique

3.4.1 Schéma physique existant



DOSSIER DE SPECIFICATIONS TECHNIQUES DETAILLEES

Le schéma ci-dessous correspond au câblage des interfaces :

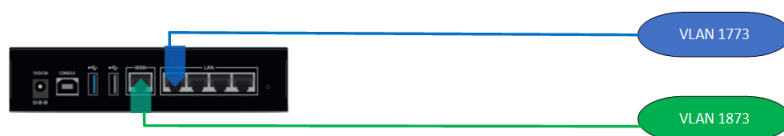


3.4.2 Câblage

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

3.5 Architecture de Niveau 2

3.5.1 Schéma niveau 2 cible



3.5.2 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

3.5.3 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

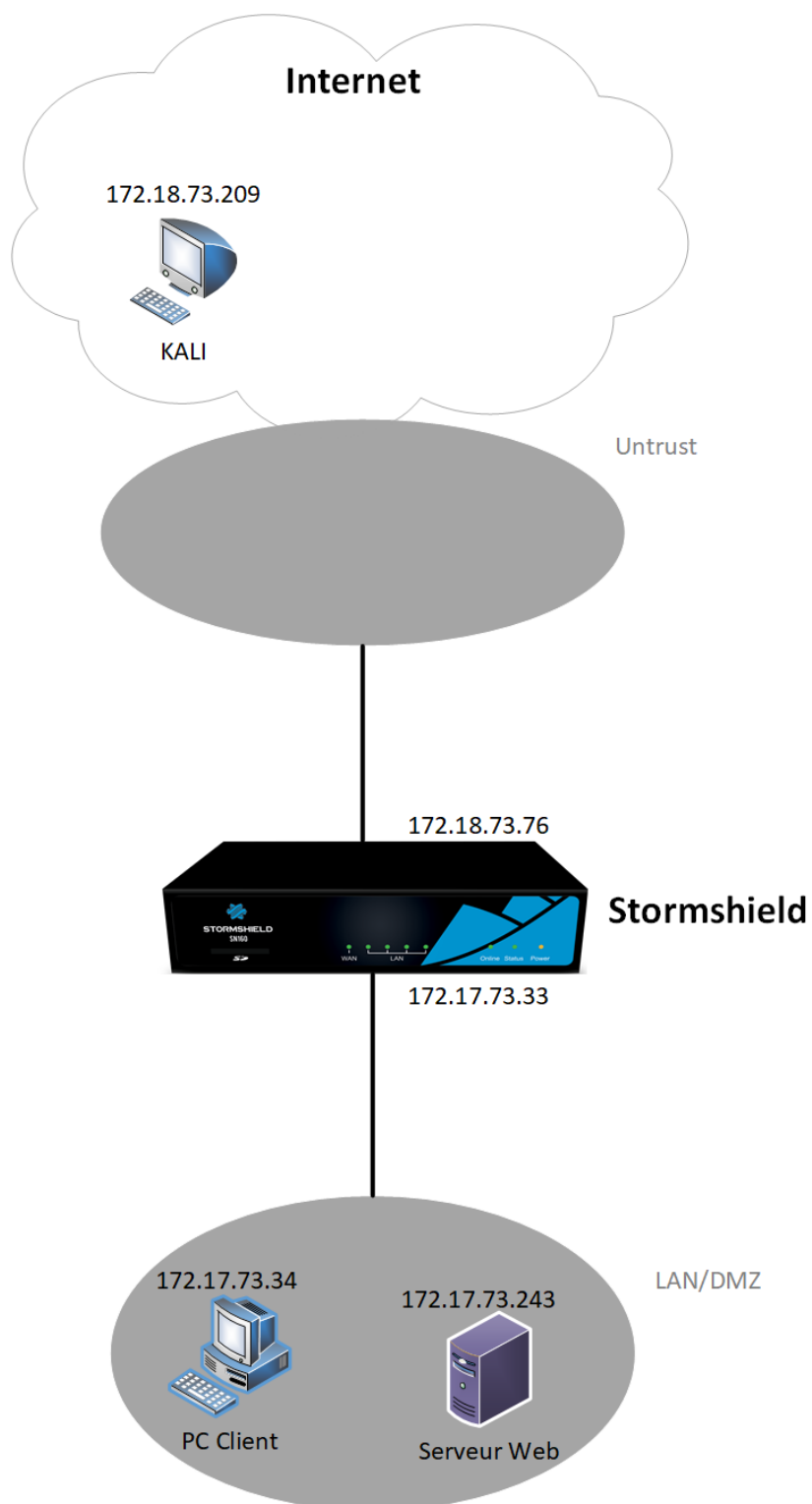
3.6 Architecture de Niveau 3

3.6.1 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 :



3.6.2 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

3.6.3 Routage

3.6.3.1.1.1 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

3.7 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	

3.7.1 Active Directory

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

Paramètres de la configuration :

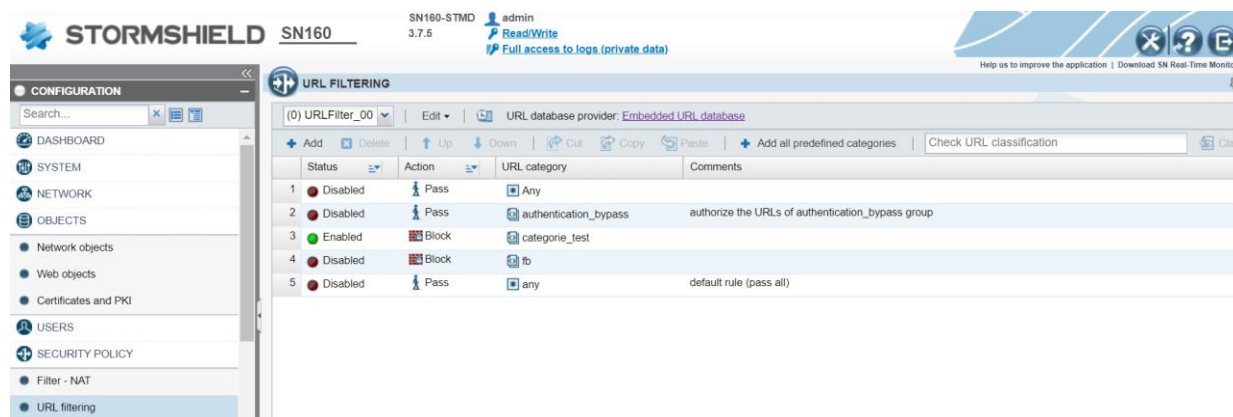
	Valeur	Description
Microsoft Active Directory		Authentification des utilisateurs
Nom de domaine	Infra-lab.nms.lab	
Serveur	Server_adlab	172.16.0.219
Format/Type	Annuaire LDAP	LDAP externe

4 Politique de sécurité

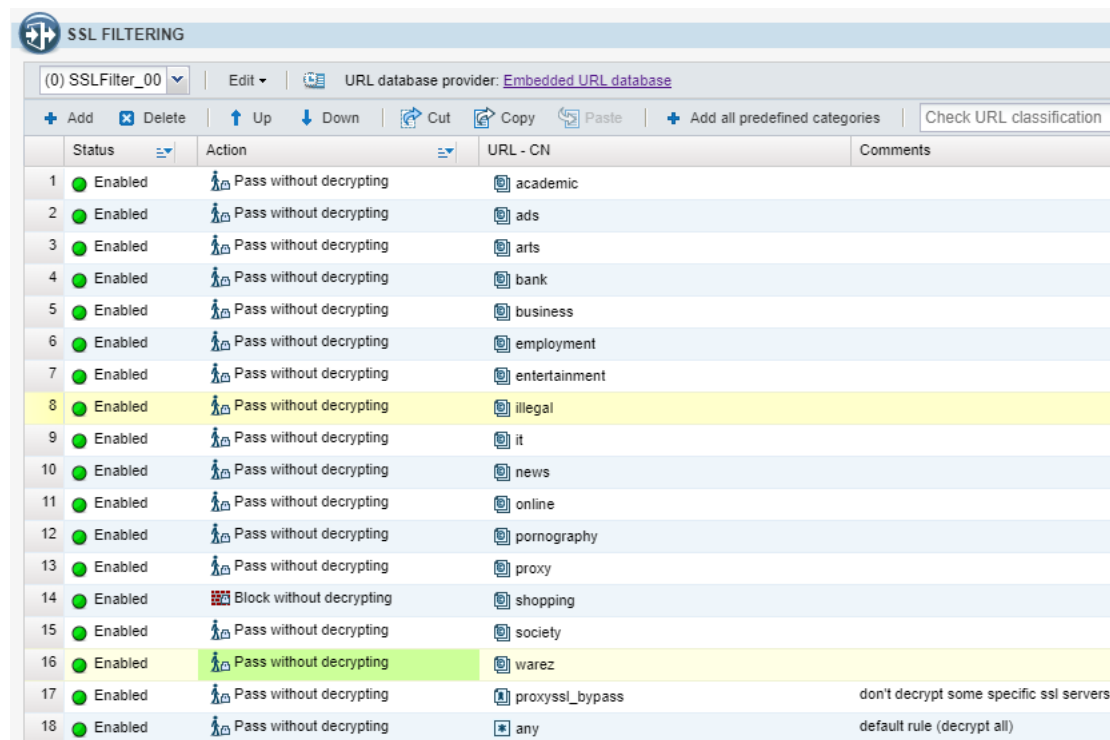
4.1.1 Profils de sécurité

Les profils URL et SSL 00(par défaut) seront configurés dans un premier temps.

Profil URL

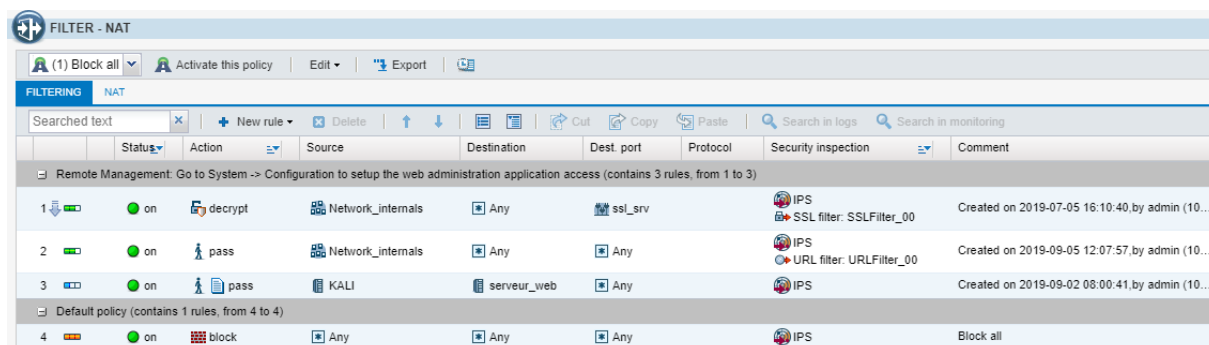


Profil SSL



4.1.2 Règles

Nous avons ici les différentes règles de filtrage mises en place pour le projet.



	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comment
Remote Management: Go to System -> Configuration to setup the web administration application access (contains 3 rules, from 1 to 3)								
1	on	decrypt	Network_internals	Any	ssl_srv		IPS SSL filter: SSLFilter_00	Created on 2019-07-05 16:10:40, by admin (10...
2	on	pass	Network_internals	Any	Any		IPS URL filter: URLFilter_00	Created on 2019-09-05 12:07:57, by admin (10...
3	on	pass	KALI	serveur_web	Any		IPS	Created on 2019-09-02 08:00:41, by admin (10...
Default policy (contains 1 rules, from 4 to 4)								
4	on	block	Any	Any	Any		IPS	Block all

- Règle 1 : Test PC Client blocage des sites catégories « Shopping »
- Règle 2 : Test PC Client blocage du site « neverssl »
- Règle 3 : Attaque du serveur par la machine KALI et enregistrement des logs
- Règle 4 : Règle par défaut « Block all »

