Cours
Présentation d'un pare-feu Stormshield

1 – Présentation de Stormshield

Stormshield est une filiale d'AIRBUS qui propose des firewalls "hautes performances" pour sécuriser les infrastructures réseaux des entreprises, des organisations, … (Certifié ANSII).
Trois catégories de pare-feu :

- Protection des réseaux informatiques et industriels : SNS - **Stormshield Network Security**.
- Protection des postes et serveurs : SES - **Stormshield Endpoint Security**.
- Protection des données : SDS - **Stormshield Data Security.**

Nous nous limiterons à l'étude du SNS - **Stormshield Network Security** – qui correspond à la protection des réseaux informatiques et industriels.

2 – Comment choisir son pare-feu Stormshield

Les solutions proposées par Stormshield sont liées à la taille de l'entreprise.

Exemple pour de petites entreprises

SN160 SN210 SN310

	SN160(W)	SN210(W)	SN310
Nombre d'interfaces 10/100/1000	1 + 4 ports (switch)	2 + 6 ports (switch)	8
Débit IPS (Gbps)	1	1.6	2.4
Débit VPN IPSec (Mbps AES)	200	350	600
Connexions simultanées	150 000	200 000	300 000
Slot pour carte SD	Oui	Oui	Oui
Disque Dur	-	-	-

Exemple pour de grandes entreprises

	SN1100	SN2100	SN3100	SN6100
Nombre d'interfaces 10/100/1000	8/24	2-26	2-26	8-64
Nombre d'interfaces fibre 1/10/40Gb	0-16/2-10	0-24/0-12/0-6	0-24/0-12/0-6	0-64/0-34/0-16
Débit IPS (Gbps)	18	35	55	68
Débit VPN IPSec (Gbps AES)	7,5	10	10	20,5
Connexions simultanées	1 800 000	2 500 000	5 000 000	20 000 000
Disque Dur	512 Go SSD	256 Go SSD (option raid 1)	256 Go SSD (raid 1)	512 Go SSD (raid 1)
Alimentation redondante	(option)	(option)	Oui	oui

La gamme EVA - Elastic Virtual Appliance

Elle est conçue pour répondre aux besoins spécifiques de protection :

- Des environnements virtualisés.
- Des infrastructures cloud (privé, public ou hybride).

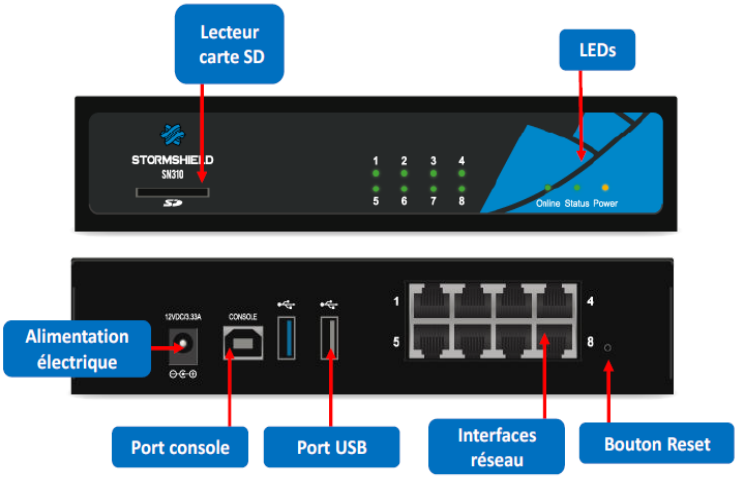
Idéal pour des solutions hébergées sur AWS (Amazon) ou Microsoft Azure, s'intègre facilement avec des hyperviseurs (VMWare, Hyper-V, …).

	EVA1	EVA2	EVA3	EVA4	EVAU
Nombre de connexions simultanées	200 000	400 000	1 000 000	1 500 000	5 000 000
Nombre d'interfaces VLANs 802.1q	128	256	512	512	1024
Nombre de tunnels	200	500	750	5 000	10 000
Clients VPN SSL Simultanés	100	150	200	250	500
Nombre max de vCPU/mémoire (Go)	1 / 2	2 / 3	4 / 6	4 / 8	16 / 64

Les fonctions standards d'un firewall Stormshield

- ✓ Routage dynamique, routage par politique ;
- ✓ Client DHCP ;
- ✓ Serveur/Relai DHCP ;
- ✓ Client DynDNS : ce service qui permet de mapper automatiquement une adresse IP dynamique (adresse IP qui change régulièrement) à un nom de domaine statique.
- ✓ Cache DNS ;
- ✓ Client NTP ;
- ✓ Agent SNMP ;
- ✓ Syslog
- ✓ Tunnels (VPN IPSec, VPN SSL, …) ;
- ✓ Moteur IPS : analyse des protocoles IP, ICMP, UDP, http, FTP, SIP, MODBUS, … ;
- ✓ Signatures contextuelles IPS : Une base de signatures d'attaque utilisée en complément de l'analyse protocolaire pour détecter rapidement les attaques connues.
- ✓ Antispam (analyse heuristique ou par réputation). Analyse Heuristique permet la qualification d'un email en SPAM en se basant sur un algorithme particulier qui détermine le degré de légitimité des emails.
- ✓ Antivirus standard ;
- ✓ Filtrage d'URL ;
- ✓ Système haute disponibilité : Assure la continuité de services en utilisant deux firewalls : un en mode actif et l'autre en mode passif. Dans le cas où le firewall actif n'est plus fonctionnel, le firewall passif bascule en mode actif pour assurer la transmission et la protection des données.

2 – Prise en main du firewall



Trois LEDs d'Etat

La première LED « orange » indique que le firewall est sous-tension (câble d'alimentation branché).

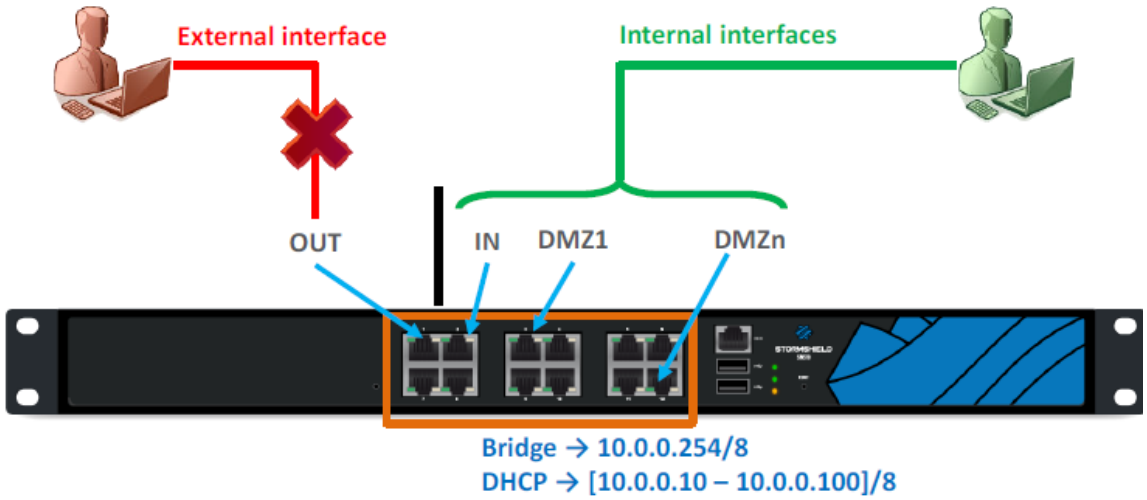
La deuxième LED « verte » indique que le système d'exploitation du firewall est fonctionnel.

La troisième LED « verte » indique que le firewall a fini de démarrer et qu'il est fonctionnel.

Restauration de la configuration usine

Maintenez le bouton Reset enfoncé 10 secondes.

Configuration d'usine



Lorsque vous recevez votre pare-feu ou après une réinitialisation, le firewall se trouve en configuration d'usine :

- La première interface du firewall est nommée "**OUT**", la seconde "**IN**" et les suivantes "**DMZx**".
- L'interface "**out**" est une interface externe, utilisée pour connecter le firewall à internet.
- Les autres interfaces sont internes et servent à connecter le firewall à des réseaux locaux.
- Toutes les interfaces sont incluses dans un bridge dont l'adresse est 10.0.0.254/8. Un serveur DHCP est actif sur toutes les interfaces du bridge et il distribue des adresses IP comprises entre 10.0.0.10 et 10.0.0.100.

Important

Avec la configuration usine, connecter une machine sur l'interface externe et ensuite sur une interface interne sera interprété par le firewall comme une tentative d'usurpation d'adresse IP sur le bridge et par conséquent, il bloquera tout le trafic généré par cette machine. Le redémarrage du firewall sera nécessaire pour débloquer cette situation.

Pour accéder à l'interface d'administration du firewall, vous devez connecter votre machine sur une interface interne.

Remarque

Pour les activités pratiques nous utiliserons une solution EVA intégrée dans une infrastructure virtuelle.