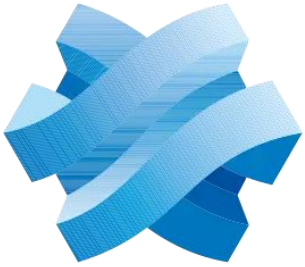
Documentation : Configuration des règles de sécurité et NAT

1. Présentation générale

- Objet : Règles de filtrage et de NAT/PAT mises en place pour sécuriser le réseau tout en permettant un accès contrôlé à Internet.

- Contexte : Configuration réalisée dans un pare-feu Stormshield pour protéger les ressources internes contre les menaces extérieures, contrôler le trafic, et permettre un accès sécurisé à Internet.

- Structure :
    - Règles de filtrage (entrantes/sortantes, par protocole).
    - Règles NAT/PAT.

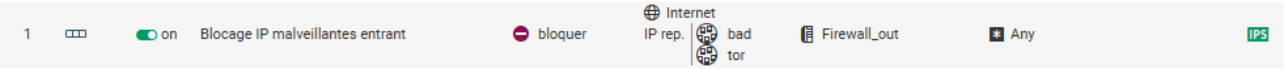


STORMSHIELD

2. Règles de filtrage

Règle 1 : Blocage IP malveillantes entrantes

- Description : Bloque tout trafic provenant d'IP ayant une mauvaise réputation (bad, tor).
- Source : Internet (IP répertoriées comme malveillantes).
- Destination : Firewall_out (interface internet)
- Action : Bloquer.
- Protocole : Tout.



Règle 2 : Blocage IP malveillantes sortantes

- Description : Bloque tout trafic sortant vers des IP malveillantes depuis le réseau interne.
- Source : Network_internals.
- Destination : IP malveillantes.
- Action : Bloquer.
- Protocole : Tout.

Règle 3 et 4 : Blocage RFC 5735

- Description : Bloque les plages d'adresses non routables spécifiées par la RFC 5735.
- Source : Internet ou Network_internals
- Destination : RFC 5735.
- Action : Bloquer.
- Protocole : Tout.

3	on	Blocage IP RFC 5735	bloquer	Internet	rfc5735	Any	IPS
4	on	Blocage IP RFC 5735 depuis reseau local	bloquer	Network_internals	rfc5735	Any	IPS

Essai d'accès à une adresse non routable (RFC 5735) :

```
C:\Users\morgan.mathis>ping 192.0.2.0

Envoi d'une requête 'Ping'  192.0.2.0 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

Résultat dans les logs du pare-feu :

09/12/2024 15:09:12	Bloquer	172.16.3.249	192.0.2.0
09/12/2024 15:09:07	Bloquer	172.16.3.249	192.0.2.0
09/12/2024 15:09:02	Bloquer	172.16.3.249	192.0.2.0

DÉTAILS DE LA LIGNE DE LOG	
Configuration	
Protocole	icmp
Protocole Internet	icmp
Règle N°	4
Nom de la règle	Blocage IP RFC 5735 depuis reseau l
Profil IPS (ID)	01
Niveau règles	Locale
Dates	
Enregistré à	09/12/2024 15:16:45
Date et heure	09/12/2024 15:16:44
Décalage GMT	+0100
Destination	
Nom de destination	192.0.2.0
Destination	192.0.2.0
Interf. dest.	out
Interf. dest. (ID)	Ethernet0
Divers	
Journaux	filter
Action	Bloquer

Correspondance avec la regle N° 4

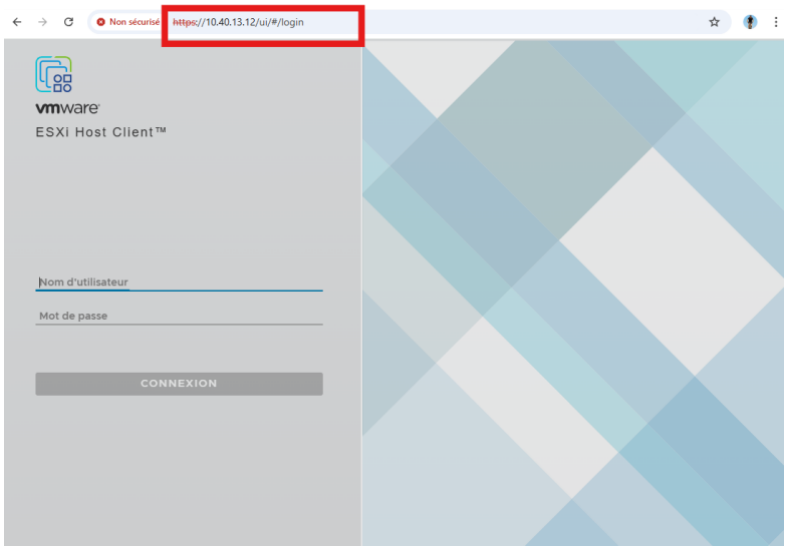
Adresse IP ping depuis le reseau local

Ping bloquer avec la regle N° 4

Règle 5 : Accès HTTP/HTTPS au réseau LAN spécifique

- Description : Permet l'accès HTTP et HTTPS au réseau 10.40.0.0.
- Source : Network_internals.
- Destination : LAN_SIO (10.40.0.0)
- Action : Passer
- Protocole : https / http

Simulation d'accès HTTP/HTTPS au réseau LAN_SIO en se connectant au ESXI (10.40.13.12)



Résultat dans les logs du pare-feu :

09/12/2024 15:45:24 Autoriser 172.16.3.249 10.40.13.12 https

DÉTAILS DE LA LIGNE DE LOG	
Configuration	
Protocole	ssl
Protocole Internet	tcp
Règle N°	5
Nom de la règle	Accès HTTP HTTPS au réseau 10.40.
Profil IPS (ID)	01
Niveau règles	Locale
Dates	
Enregistré à	09/12/2024 15:45:24
Date et heure	09/12/2024 15:45:23
Décalage GMT	+0100
Destination	
Nom de destination	10.40.13.12
Destination	10.40.13.12
Destination orig.	10.40.13.12
Nom du port dest.	https
Port destination	443
Port destination orig.	443
Interf. dest.	out
Interf. dest. (ID)	Ethernet0
Divers	
Journaux	connection
Action	Autoriser

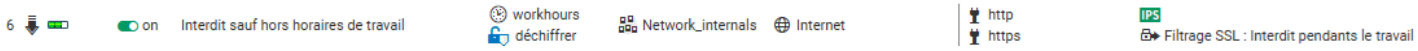
Correspondance avec la regle N° 5

Adresse IP d'accès HTTP depuis le reseau local

Connexion HTTP / HTTPS autoriser avec la regle N° 5

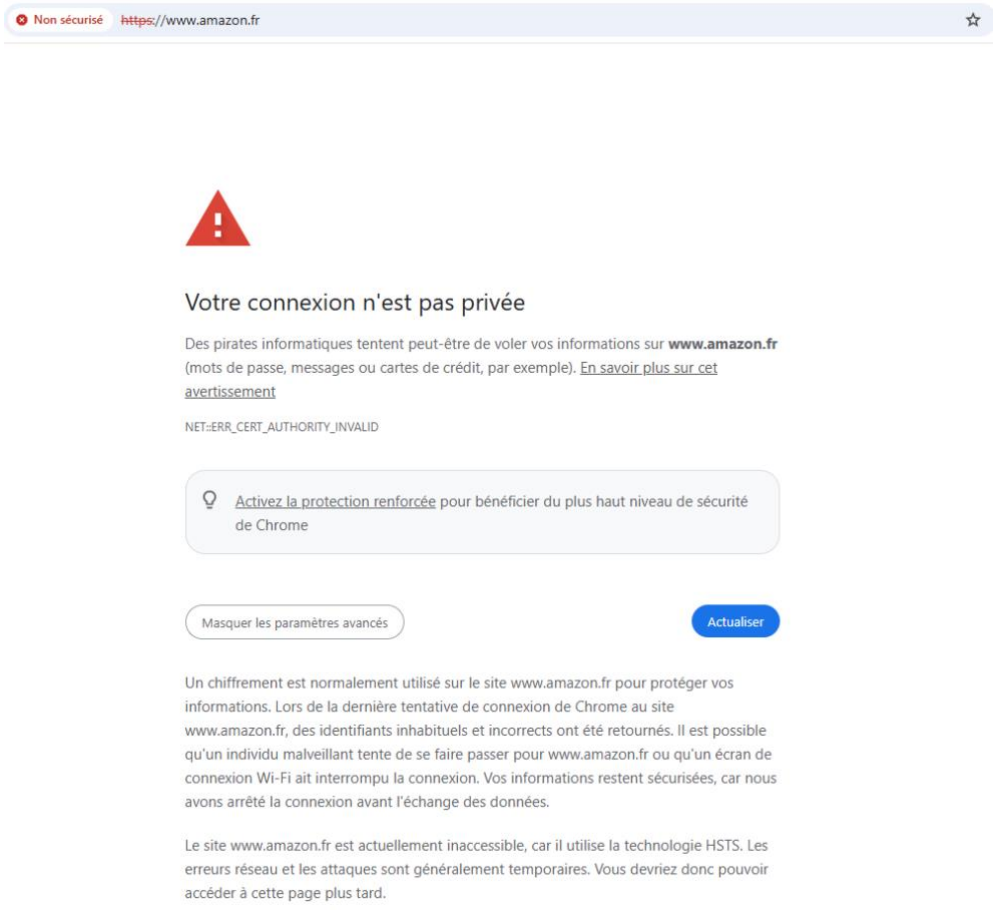
Règle 6 : Interdiction hors horaires de travail

- Description : Bloque l'accès HTTP/HTTPS vers Internet en dehors des horaires de travail.
- Source : Network_internals.
- Destination : Internet.
- Action : Bloquer en déchiffrant le trafic SSL.



1	on	Passer sans déchiffrer	proxyssl_by...	don't decrypt some specific ssl servers
2	on	Bloquer sans déchiffrer	shopping	
3	on	Bloquer sans déchiffrer	ads	
4	on	Bloquer sans déchiffrer	entertainment	
5	on	Bloquer sans déchiffrer	news	
6	on	Passer sans déchiffrer	any	default rule (decrypt all)

Simulation d'accès HTTP/HTTPS pendants les horaires de travail (catégorie shopping : Amazon)



Résultat dans les logs du pare-feu :

09/12/2024 16:20:01	Bloquer	172.16.3.249	www.amazon.fr	https
09/12/2024 16:20:00	Bloquer	172.16.3.249	www.amazon.fr	https
09/12/2024 16:20:00	Bloquer	172.16.3.249	www.amazon.fr	https
09/12/2024 16:20:00	Bloquer	172.16.3.249	www.amazon.fr	https

DÉTAILS DE LA LIGNE DE LOG

Configuration	
Protocole	ssl
Règle N°	6
Nom de la règle	Interdit sauf hors horaires de trav
Profil IPS (ID)	1
Niveau règles	Locale
Dates	
Enregistré à	09/12/2024 16:20:00
Date et heure	09/12/2024 16:19:59
Décalage GMT	+0100
Destination	
Pays destination	
Continent destination	
Nom de destination	www.amazon.fr
Destination	3.162.34.54
Destination orig.	3.162.34.54
Nom du port dest.	https
Port destination	443
Port destination orig.	443
Divers	
Journaux	ssl
Action	Bloquer

Correspondance avec la regle N° 6

Accès site web amazon

Connexion HTTPS / HTTP bloquer avec la regle N° 6

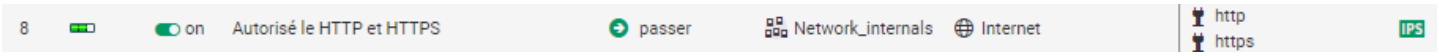
Règle 7 : Blocage permanent de certains sites (pornography, illégal, warez) et exception pour le trafic bancaire

- Description : Cette règle bloque l'accès à certains sites classés comme nuisibles, illégaux ou à contenu inapproprié (par exemple, sites pornographiques, illégaux, ou warez). Cependant, elle permet le passage du trafic bancaire sans déchiffrement SSL pour garantir la confidentialité de ces échanges.
- Source : Network_internals (réseau interne).
- Destination : Internet.
- Action : Déchiffrement pour bloquer le trafic vers les sites inappropriés, tout en permettant le trafic bancaire sans déchiffrement.
- Exceptions : Sites bancaires.

1	on	Passer sans déchiffrer	proxyssl_by...	don't decrypt some specific ssl servers
2	on	Passer sans déchiffrer	bank	
3	on	Bloquer sans déchiffrer	pornography	
4	on	Bloquer sans déchiffrer	illegal	
5	on	Bloquer sans déchiffrer	warez	
6	on	Passer sans déchiffrer	any	default rule (decrypt all)

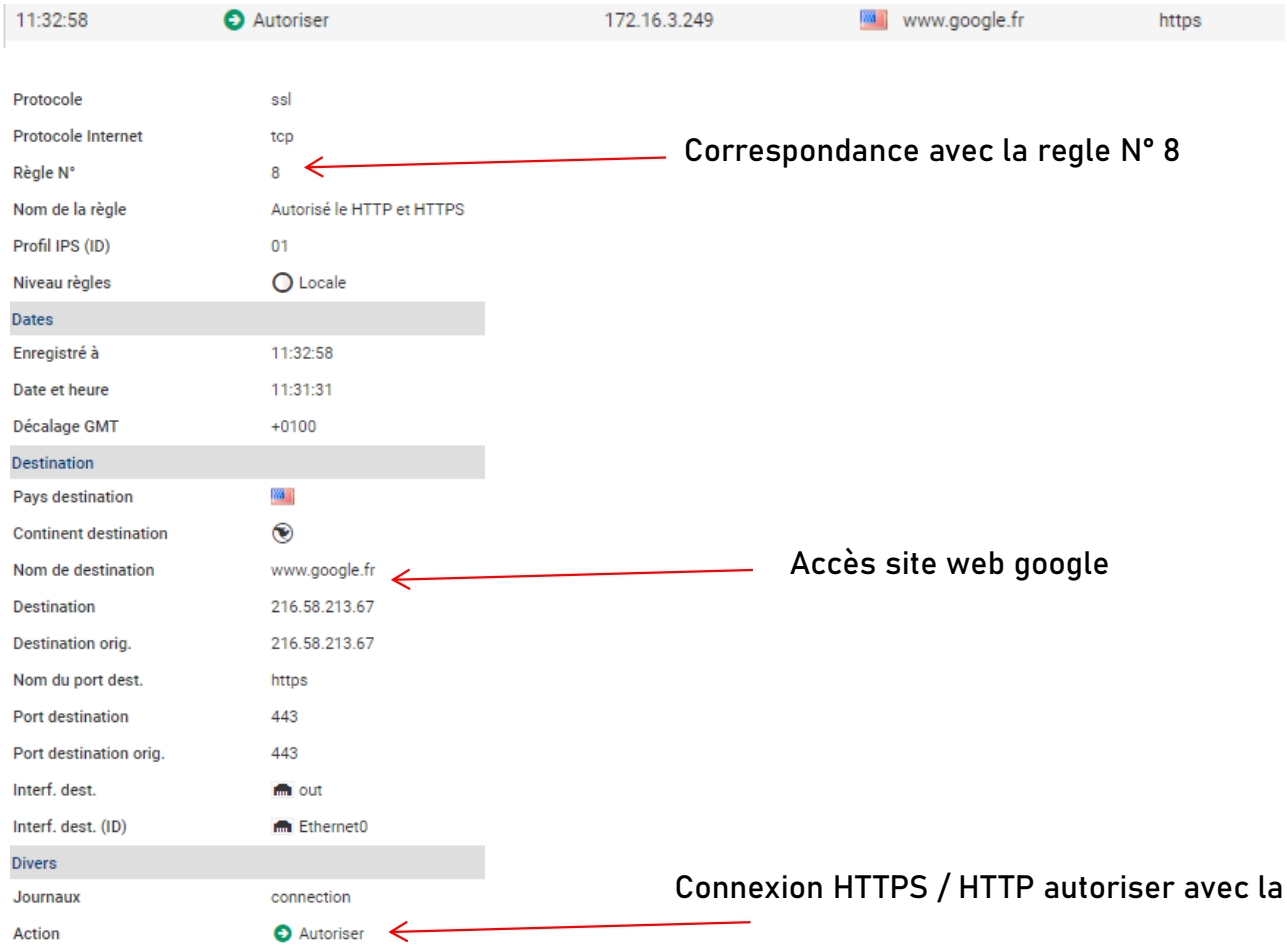
Règle 8 : Autorisation HTTP et HTTPS

- Description : Autorise tout le trafic HTTP/HTTPS vers Internet en l'absence de restrictions spécifiques.
- Source : Network_internals
- Destination : Internet
- Action : Passer



Tests : Vérifier un accès HTTPS (ex. www.google.com)

Résultat dans les logs du pare-feu :



Correspondance avec la regle N° 8

Accès site web google

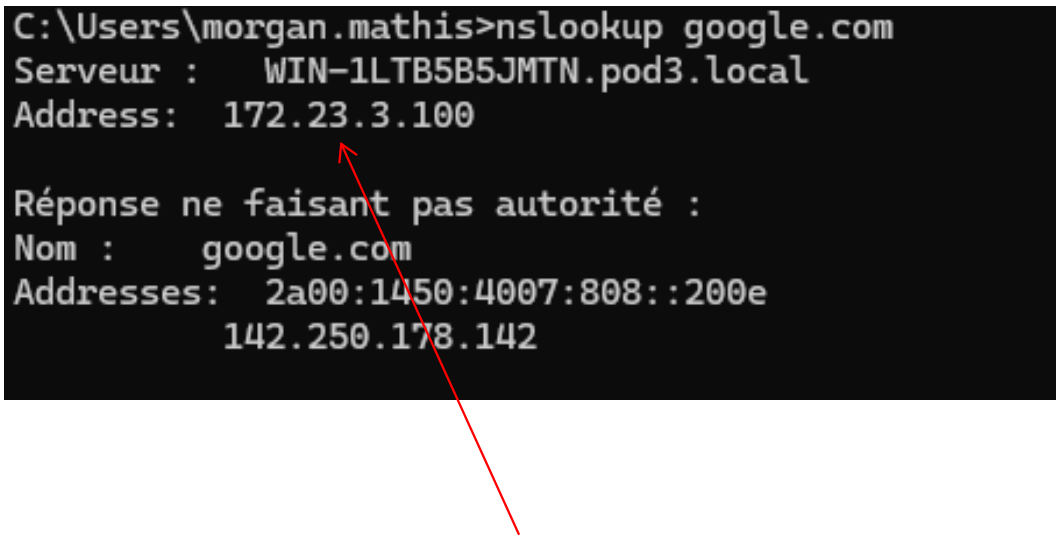
Connexion HTTPS / HTTP autoriser avec la règle N° 8

Règles 9 et 10 : DNS autorisé en entrée et DNS autorisé en sortie

- Description : Permettent la résolution DNS pour le réseau interne (entrée et sortie).
- Source : Network_internals ou DNS
- Destination : Network_internals ou DNS
- Action : Passer
- Potocole : DNS

9	on	DNS autorisé en entrée	passer	DNS_POD3 DNS_Lycée dns1.google.com	Network_internals	dns	IPS
10	on	DNS autorisé en sortie	passer	Network_internals	DNS_POD3 DNS_Lycée dns1.google.com	dns	IPS

Tests : résolution DNS depuis le réseau local avec « DNS_POD3 »



IP DNS_POD3

Règles 11, 12 et 13 : Règle ICMP

- Description : sécurisation ICMP intérieure et exterieure
- Source : Network_internals ou internet
- Destination : internet, firewall_dmz1, network_out
- Action : Passer ou bloquer
- Potocole : icmp

Tests : ping depuis le réseau local vers un réseau externe

```
C:\Users\morgan.mathis>ping 10.40.3.23

Envoi d'une requête 'Ping'  10.40.3.23 avec 32 octets de données :
Réponse de 10.40.3.23 : octets=32 temps<1ms TTL=126
Réponse de 10.40.3.23 : octets=32 temps<1ms TTL=126
Réponse de 10.40.3.23 : octets=32 temps=1 ms TTL=126
Réponse de 10.40.3.23 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 10.40.3.23:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Réseau externe

Tests : ping depuis un réseau externe vers le réseau local

```
C:\Users\jimmy.menard>ping 172.16.3.109

Envoi d'une requête 'Ping'  172.16.3.109 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 172.16.3.109:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Réseau interne

Tests : ping depuis le réseau local vers le pare-feu

```
C:\Users\morgan.mathis>ping 172.16.3.250

Envoi d'une requête 'Ping'  172.16.3.250 avec 32 octets de données :
Réponse de 172.16.3.250 : octets=32 temps<1ms TTL=64
Réponse de 172.16.3.250 : octets=32 temps<1ms TTL=64
Réponse de 172.16.3.250 : octets=32 temps<1ms TTL=64
Réponse de 172.16.3.250 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.16.3.250:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

IP pare-feu (Firewall_dm

Règles 14 : Block All

- Description : block all
- Source : Any
- Destination : Any
- Protocole : Any
- Action : bloquer

La règle "Block All", configurée en dernière position dans la liste de mes règles de filtrage sur le Stormshield, permet de bloquer tout le trafic réseau qui n'est pas explicitement autorisé par les règles précédentes.

Cette règle repose sur le principe de "refus par défaut" (deny by default), une méthode éprouvée pour renforcer la sécurité des systèmes. En d'autres termes, toute communication ou connexion non définie de manière explicite est automatiquement interdite.

Objectif :
Garantir qu'aucun flux non contrôlé ou non anticipé ne puisse traverser le pare-feu, réduisant ainsi les risques de failles ou d'activités malveillantes.

Mécanisme :

- Toutes les règles spécifiques d'autorisation (ALLOW) sont placées avant la règle "Block All".
- La règle "Block All" est configurée avec une action de refus global pour tout trafic restant.