TP Stormshield SNS EVA

Déploiement & Configuration d'un Pare-feu en environnement virtualisé

Gaston MEDJO

VMware Workstation · SNS EVA v4.3.11

1. Présentation & Objectifs

Ce guide détaille pas à pas le déploiement d'un pare-feu Stormshield Network Security (SNS) EVA en environnement virtualisé VMware Workstation. Il s'adresse à un public de techniciens et administrateurs réseau ayant des bases en cybersécurité.

Objectifs du TP

- Déployer une appliance SNS EVA v4.3.11 dans VMware Workstation
- Configurer les réseaux virtuels VMware (VMnet) pour les 3 zones
- Configurer les interfaces WAN, LAN et DMZ du firewall
- Mettre en place les règles de filtrage et NAT (masquerade)
- Administrer via l'interface Web SMA et la Console CLI
- Valider la connectivité Internet depuis les zones LAN et DMZ

Architecture réseau cible

L'architecture repose sur trois zones de sécurité distinctes :

Zone / Interface	VMnet	Réseau	IP Firewall	Rôle
WAN · em0	Bridged (VMnet0)	192.168.1.0/24	192.168.1.201	Sortie Internet (Bridge VMware)

LAN · em1	VMnet2 (Host-only)	10.15.1.0/24	10.15.1.254	Réseau LAN interne
DMZ · em2	VMnet5 (Host-only)	10.20.1.0/24	10.20.1.254	Zone démilitarisée

2. Préparation de l'Environnement VMware Workstation

Avant de démarrer la VM Stormshield, il faut préparer les réseaux virtuels VMware. Cette étape est fondamentale : une mauvaise configuration VMnet empêchera les interfaces du firewall de communiquer.

Étape 1 — Créer VMnet2 : Interface LAN (Host-only, 10.15.1.0/24)

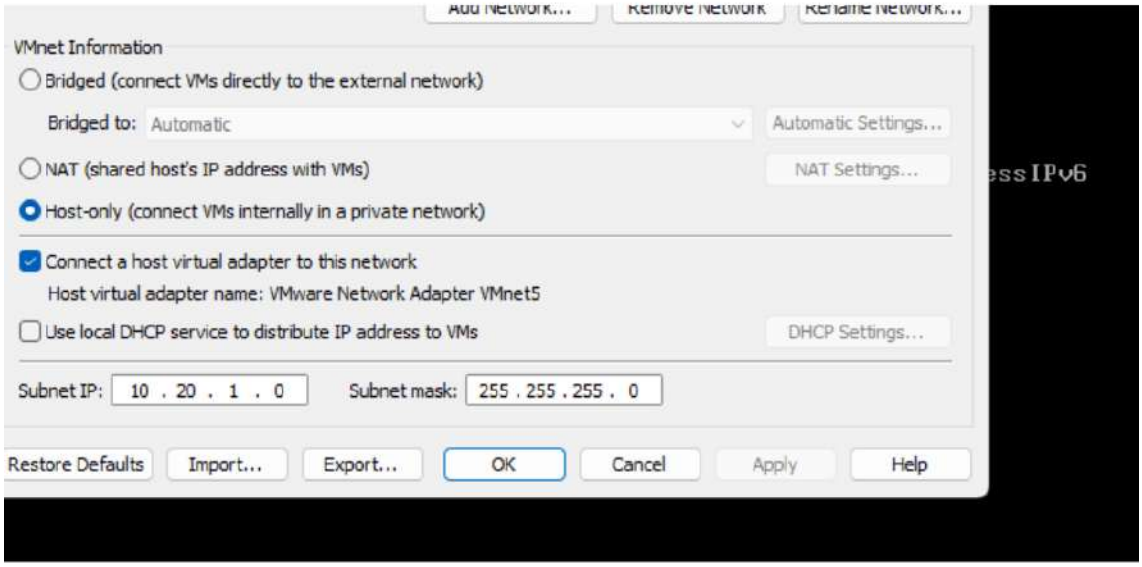
Cliquez sur "Add Network" et choisissez VMnet2. Configurez-le en Host-only avec le subnet 10.15.1.0/24 et SANS DHCP (les IP seront statiques). Ce réseau correspond au LAN interne.

Étape 2 — Configurer VMnet0 : Interface WAN (Bridged)

VMnet0 est le réseau Bridged de VMware. Il sera connecté à l'interface WAN du firewall.

Étape 3 — Créer VMnet5 : Interface DMZ (Host-only, 10.20.1.0/24)

Même démarche : ajoutez VMnet5 en mode Host-only avec le subnet 10.20.1.0/24, sans DHCP. Ce réseau sera connecté à l'interface DMZ du firewall (em2).

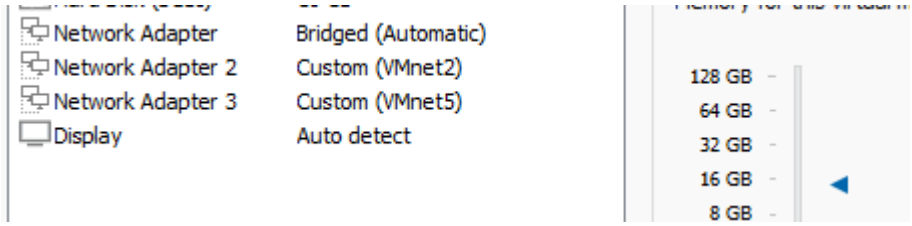


VMnet2	Host-only	-	Connected	-	10.15.1.0
VMnet5	Host-only	-	Connected	-	10.20.1.0

Étape 4 — Configurer les adaptateurs réseau de la VM SNS

Ouvrez les paramètres de la VM SNS EVA (clic droit > Settings). Ajoutez 3 adaptateurs réseau et assignez-les aux VMnet correspondants :

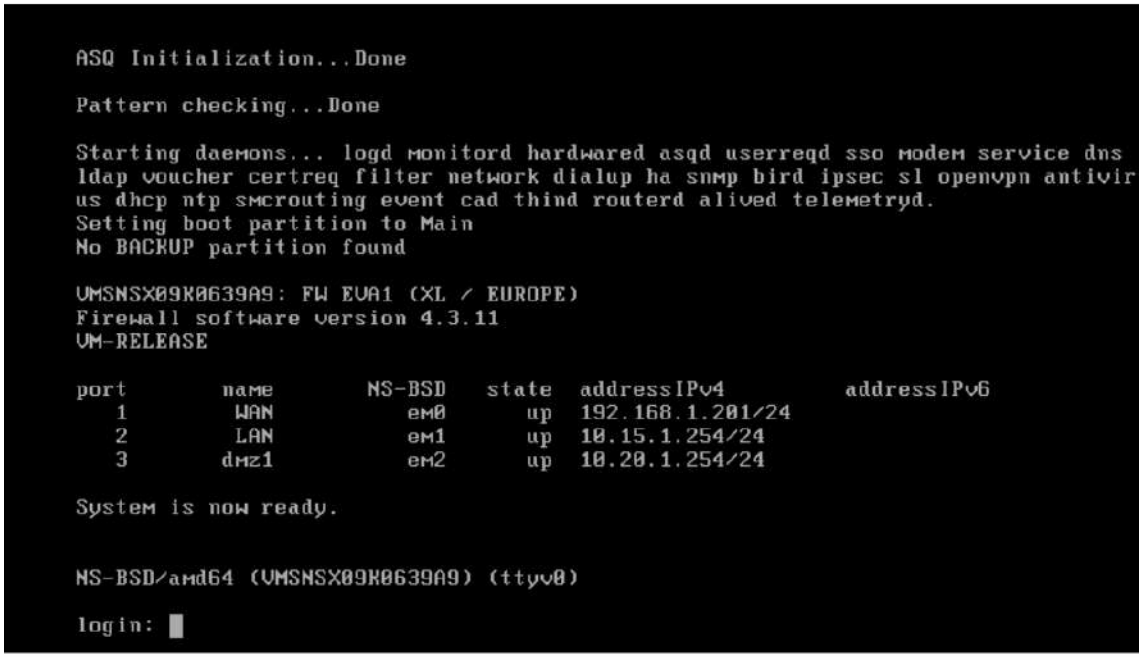
- Network Adapter 1 → Bridged ou VMnet8 (NAT) → future interface WAN (em0)
- Network Adapter 2 → Custom VMnet2 → future interface LAN (em1)
- Network Adapter 3 → Host-only (VMnet5) → future interface DMZ (em2)



3. Démarrage Initial du Firewall SNS

Étape 5 — Démarrer la VM et vérifier les interfaces

Une fois la VM configurée, démarrez-la. La console Stormshield s'affiche et montre l'état des interfaces réseau et les adresses IP assignées. C'est depuis cette console que l'on peut effectuer une configuration réseau de base avant d'accéder à l'interface Web.

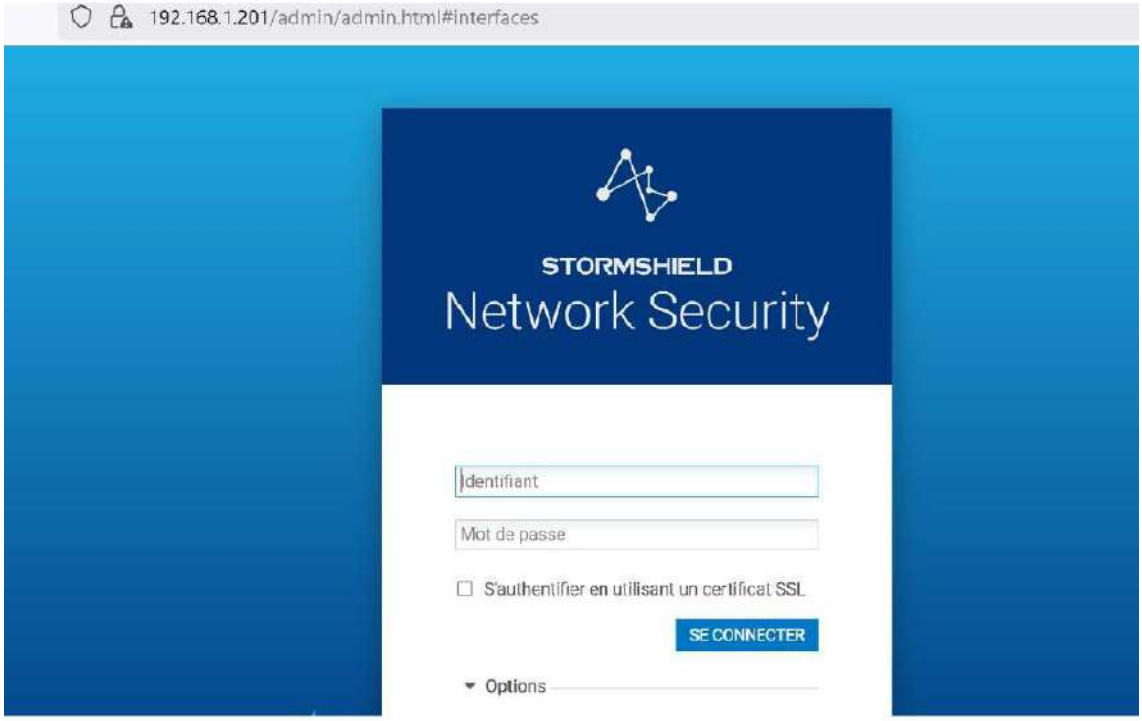


4. Accès à l'Interface Web d'Administration (SMA)

L'interface SMA (Stormshield Management Application) est le principal outil de configuration graphique. Elle est accessible via HTTPS depuis n'importe quel poste ayant une route vers l'IP WAN ou LAN du firewall.

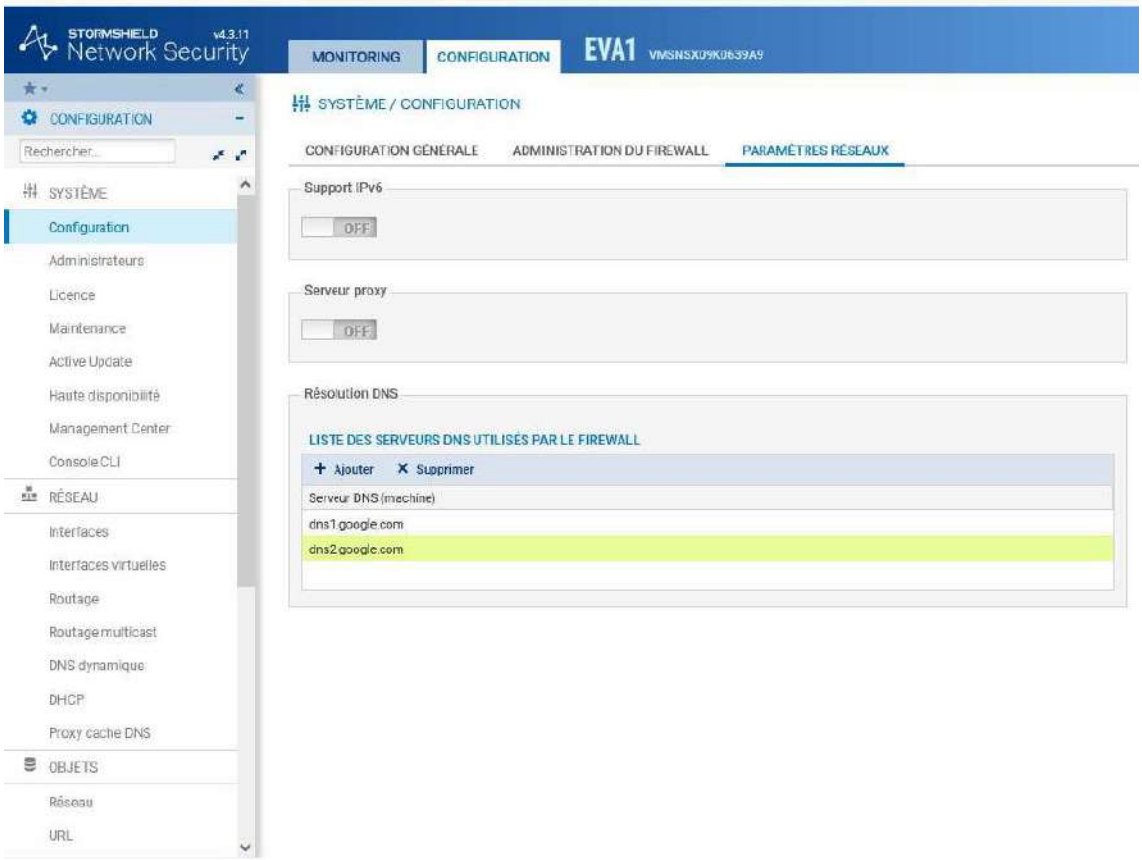
Étape 6 — Se connecter à la SMA

Ouvrez un navigateur web et accédez à l'URL HTTPS de l'interface d'administration. L'URL correspond à l'adresse IP de l'interface WAN du firewall, sur le port 443 :



Étape 7 — Découvrir l'interface SMA : Système / Configuration

Une fois connecté, l'interface SMA présente le menu latéral complet. La bannière supérieure affiche le nom du firewall (EVA1), son numéro de série (VMSNSX09K0639A9), la version (v4.3.11) et le mode de session (Écriture ou Lecture).



5. Configuration des Interfaces Réseau dans la SMA

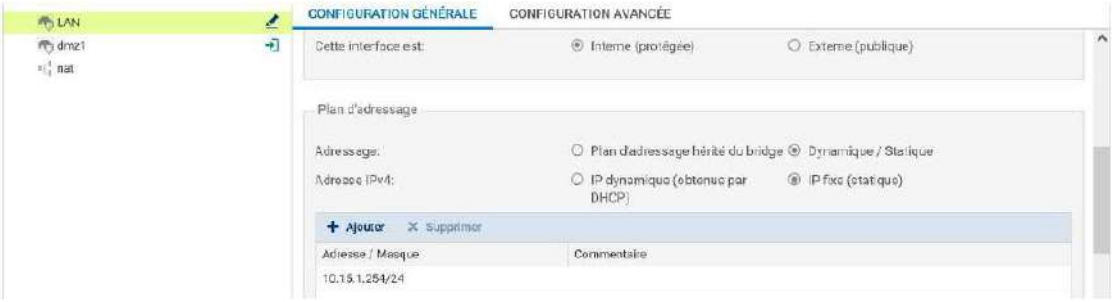
La configuration des interfaces se fait dans Réseau > Interfaces. Chaque interface physique (em0, em1, em2) est représentée et peut être configurée en termes de type (interne/externe), d'adressage IP et de VLAN.

Étape 8 — Configurer l'interface WAN (em0 — Externe)

L'interface WAN est de type Externe (publique). Elle reçoit l'IP statique de l'interface de sortie vers Internet. Dans notre lab, c'est l'IP sur le sous-réseau NAT VMware (192.168.78.0/24) ou sur le réseau 192.168.1.0/24.

Étape 9 — Configurer l'interface LAN (em1 — Interne)

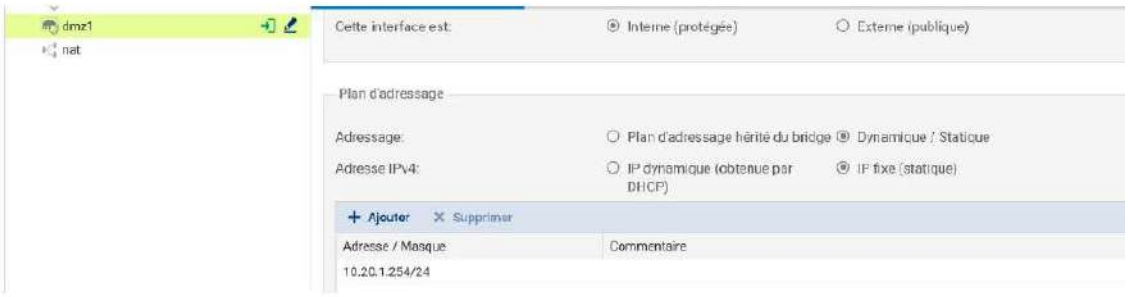
L'interface LAN est de type Interne (protégée). Elle constitue la gateway par défaut de toutes les machines du réseau 10.15.1.0/24. Son adresse IP est 10.15.1.254.



Interface LAN : type "Interne (protégée)", IP fixe 10.15.1.254/24, plan d'adressage statique

Étape 10 — Configurer l'interface DMZ (em2 — Interne)

La DMZ est également de type Interne. Elle reçoit l'adresse 10.20.1.254/24, gateway de toutes les machines en zone DMZ. L'interface em2 correspond à VMnet5 dans VMware.



6. Configuration du Routage

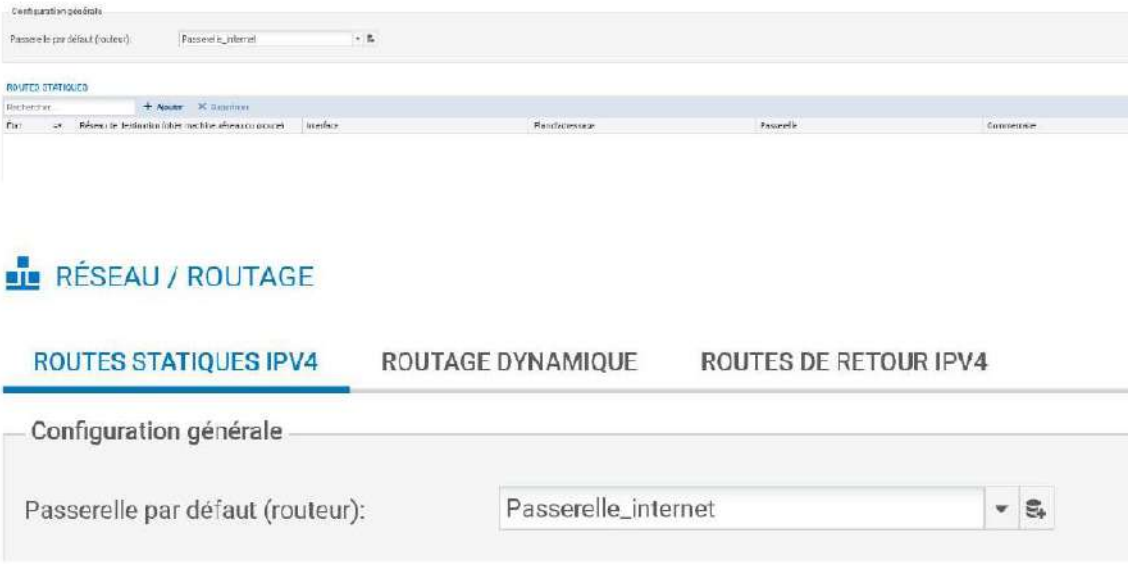
Le routage est configuré depuis Réseau > Routage. Une route par défaut (0.0.0.0/0) est nécessaire pour que le firewall puisse acheminer le trafic sortant vers Internet via la gateway WAN.

Étape 11 — Vérifier le routage avant la configuration

Au départ, la section routage est vide : aucune route statique, aucune passerelle par défaut définie. C'est pourquoi le firewall ne peut pas encore accéder à Internet.

Étape 12 — Définir la passerelle par défaut

Dans SNS, la passerelle par défaut est un objet de type Machine. Il faut d'abord créer l'objet "Passerelle_internet" (IP : 192.168.1.254) dans Objets > Réseau, puis l'assigner dans Routage > Configuration générale.



7. Configuration DNS du Firewall

Le firewall lui-même a besoin d'une résolution DNS pour ses propres opérations : Active Update (mises à jour de signatures), NTP, Sandboxing Stormshield, support technique. La configuration DNS se fait dans Système > Configuration > Paramètres réseaux.

Étape 13 — Configurer les serveurs DNS du firewall

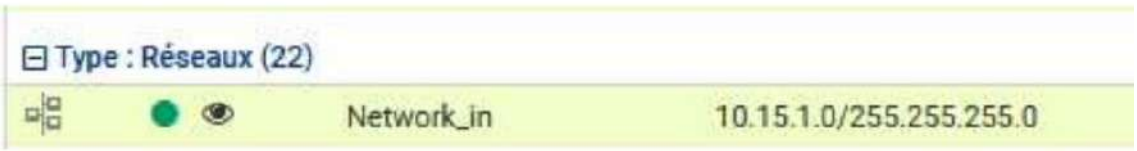
Dans l'onglet "Paramètres réseaux", section "Résolution DNS", ajoutez les serveurs DNS que le firewall lui-même utilisera. Ici, nous utilisons les DNS publics Google (8.8.8.8 et 8.8.4.4).

8. Création des Objets Réseau

Dans Stormshield, les règles de filtrage et NAT référencent des objets réseau plutôt que des adresses IP brutes. Cette approche améliore la lisibilité, la cohérence et la maintenabilité de la politique de sécurité.

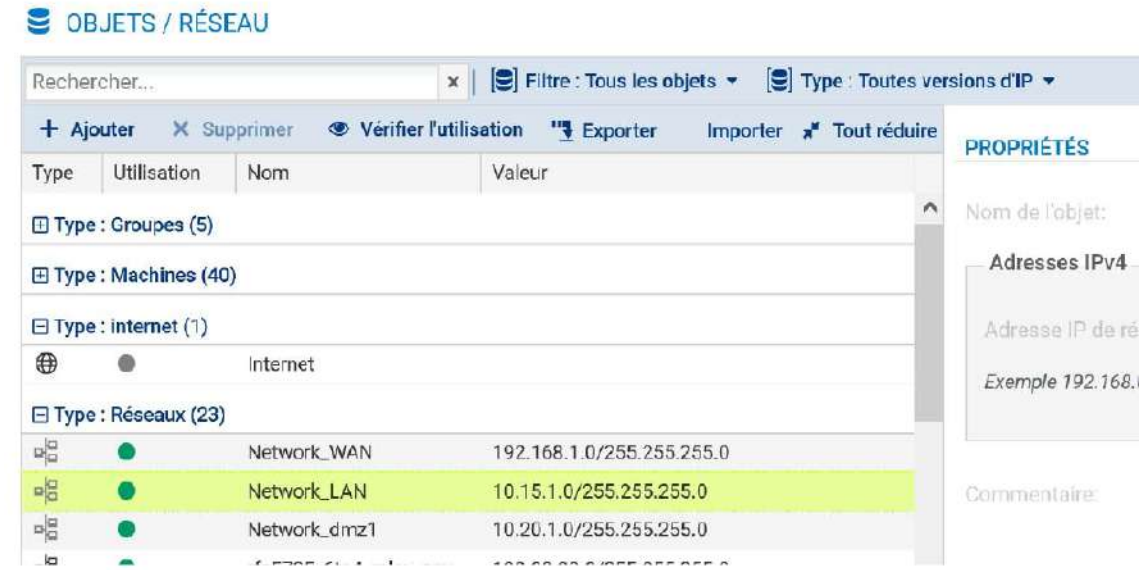
Étape 14 — Créer l'objet Network_in (phase initiale LAN)

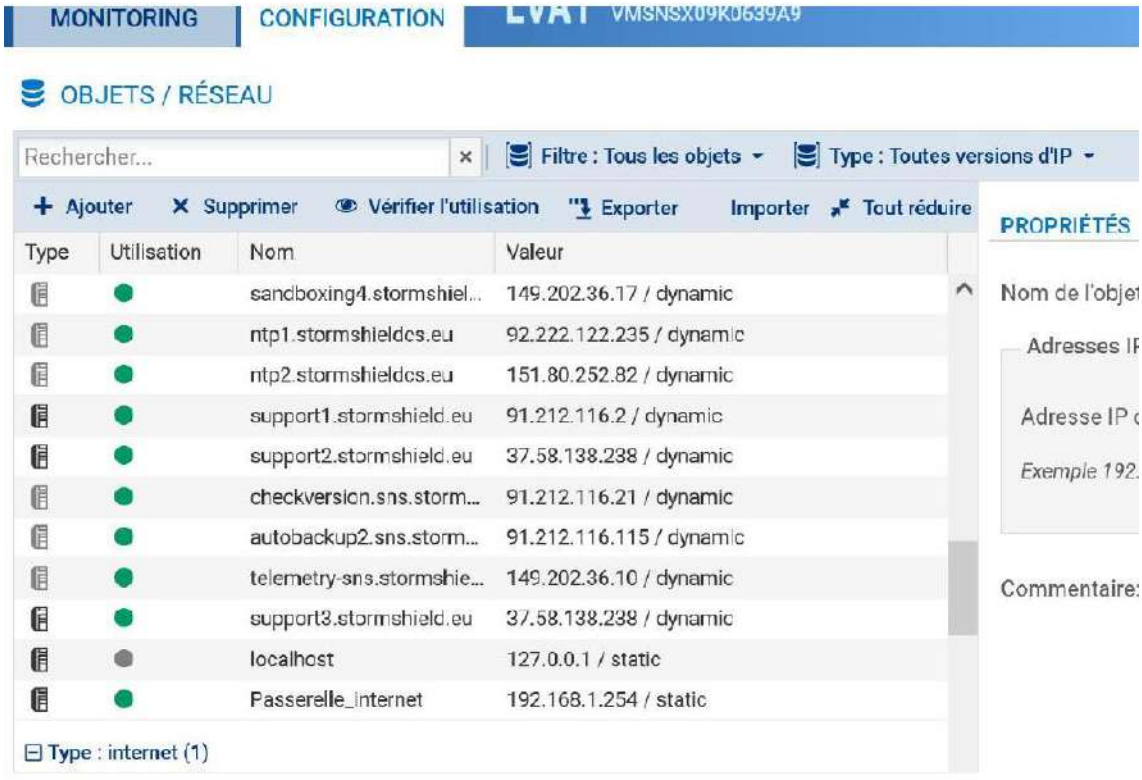
Dans la première phase du TP (architecture à 2 zones), l'objet représentant le réseau interne s'appelait "Network_in". Il correspond au sous-réseau 10.15.1.0/24.



Étape 15 — Vue complète des objets réseau : Architecture 3 zones

Avec l'architecture complète, les objets réseau créés sont : Network_WAN, Network_LAN, Network_dmz1. Des objets machines Stormshield sont automatiquement créés par SNS (NTP, sandboxing, support, etc.).





Étape 16 — Objet Network_LAN dans la base d'objets

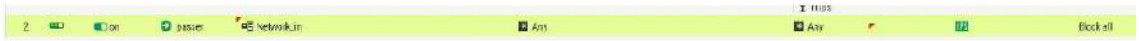
L'objet Network_LAN (renommé depuis Network_in) est visible dans la liste des réseaux. Le point vert indique qu'il est utilisé dans au moins une règle de sécurité.

9. Politique de Sécurité — Filtrage

La politique de filtrage SNS définit quels flux sont autorisés ou bloqués. Elle est accessible via Politique de sécurité > Filtrage et NAT. Les règles sont évaluées de haut en bas, et le firewall applique un blocage implicite (default deny) sur tout trafic non matché.

Étape 17 — Règle de filtrage n°2 : LAN vers Internet (phase initiale)

Dans la configuration initiale à 2 zones, la règle 2 autorise le trafic sortant du réseau interne (Network_in) vers n'importe quelle destination. Le trafic est filtré en HTTPS uniquement dans un premier temps.



Étape 18 — Règle NAT masquerade dans la liste (phase initiale)

La règle 4 dans la politique de filtrage initiale correspond à la règle NAT + filtrage combinée : passer Network_in vers Network_nat (interface WAN masquerade), destination Any.

Étape 19 — Règle n°1 : Règle NAT dans la politique (phase initiale)

La première règle NAT de la politique initiale est visible dans l'onglet NAT. Elle correspond à la règle de masquerade créée automatiquement lors de la configuration du réseau interne.

Étape 20 — Édition d'une règle de blocage : Action "bloquer"

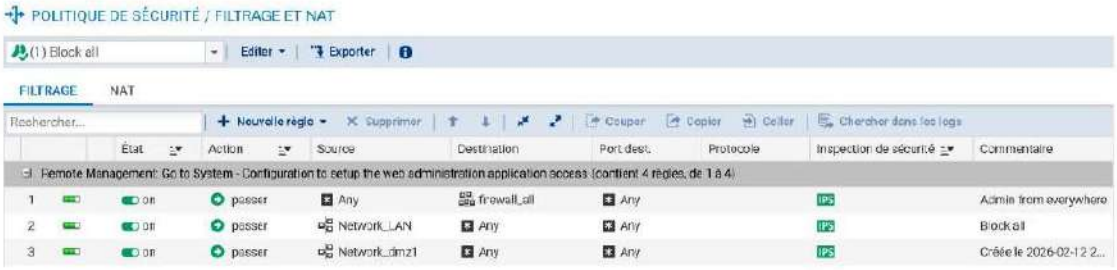
Lors de la création d'une règle de blocage explicite, l'interface d'édition de règle permet de configurer l'action, le niveau de trace (journalisation) et une éventuelle programmation horaire.

Étape 21 — Politique de filtrage Remote Management : Architecture 3 zones

Avec l'architecture tri-zones, SNS crée automatiquement une politique système "Remote Management" contenant les règles permettant l'accès à l'interface d'administration. Cette politique contient 4 règles.

Étape 22 — Politique de filtrage finale : 3 règles actives

La politique de filtrage finale (hors Remote Management) contient 3 règles principales autorisant le trafic des zones LAN et DMZ vers Internet, avec inspection de sécurité IPS activée.



10. Politique de Sécurité — NAT

Le NAT (Network Address Translation) de type masquerade permet aux machines des zones internes d'accéder à Internet en se cachant derrière l'IP publique de l'interface WAN du firewall. Les règles NAT se configurent dans l'onglet NAT de la politique de sécurité.

Étape 23 — Vue d'ensemble des règles NAT : LAN + DMZ

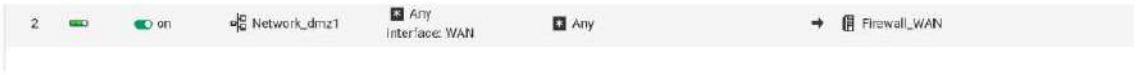
Deux règles de masquerade sont créées : une pour Network_LAN et une pour Network_dmz1. Elles traduisent le trafic sortant (interface WAN) vers l'adresse de l'objet Firewall_WAN.

Étape 24 — Règle NAT 1 : Masquerade du réseau LAN

La règle NAT 1 traduit tout le trafic provenant de Network_LAN sortant par l'interface WAN, en remplaçant l'IP source par celle de l'objet Firewall_WAN (l'IP de l'interface WAN du firewall).

Étape 25 — Règle NAT 2 : Masquerade du réseau DMZ

La règle NAT 2 est identique à la règle 1 mais s'applique au réseau DMZ. Toutes les machines de la DMZ accèdent à Internet avec l'IP WAN du firewall comme adresse source visible.



11. Console CLI — Administration en Ligne de Commande

Étape 26 — Syntaxe correcte : SYSTEM PING

La commande ping dans SNS s'utilise via la famille SYSTEM avec la syntaxe "SYSTEM PING host=<adresse_IP>". Le résultat affiche transmitted, received, packet_size et time de réponse.

> *Attention : les commandes standard Unix (ping, ifconfig...) ne fonctionnent pas dans la CLI SNS. Il faut utiliser la syntaxe propre à Stormshield.*

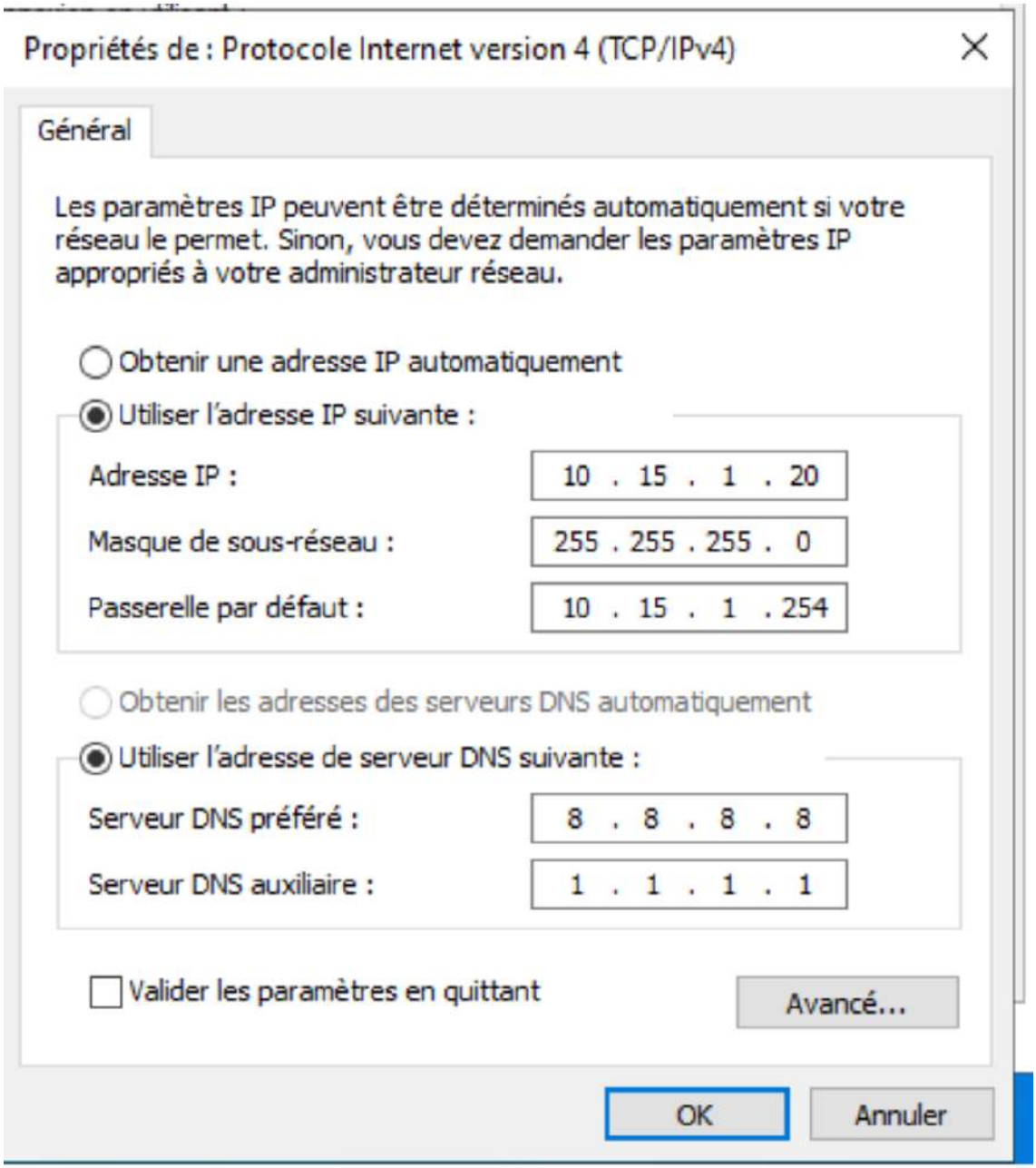
12. Configuration IP des Postes Clients

Les machines virtuelles Windows connectées aux réseaux LAN et DMZ doivent être configurées avec une IP statique dans la plage correspondante, avec la gateway pointant vers l'interface du firewall SNS.

Poste client réseau LAN (10.15.1.0/24)

Étape 27 — Configurer l'IP du poste LAN : 10.15.1.20

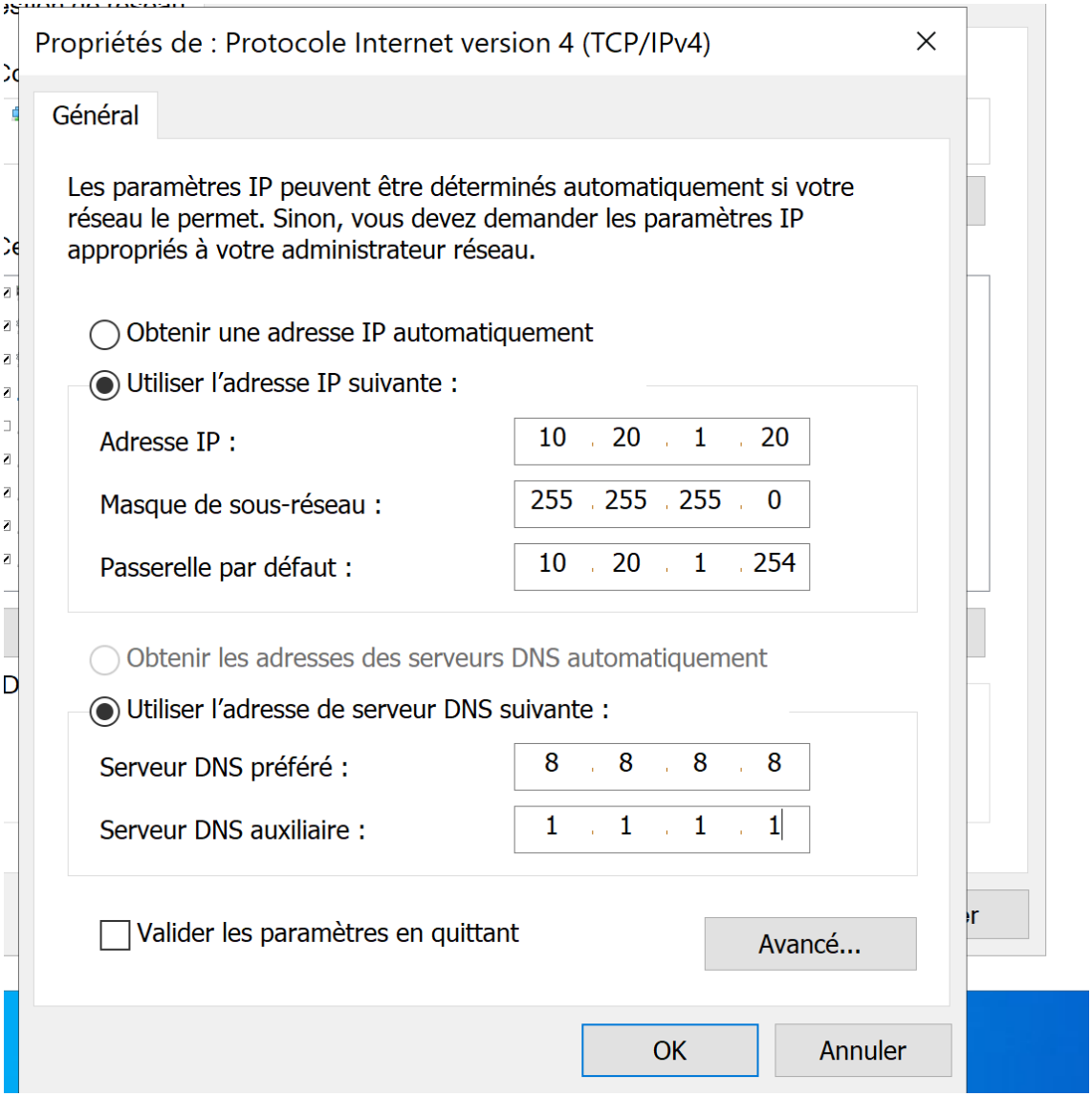
Le premier poste Windows du LAN est configuré avec l'adresse 10.15.1.20, masque /24, et la gateway 10.15.1.254 (interface LAN du firewall SNS). Les DNS publics Google sont utilisés.



Poste client réseau DMZ (10.20.1.0/24)

Étape 28 — Configurer l'IP du poste DMZ : 10.20.1.20 (via VMnet5)

Le poste Windows de la DMZ est connecté au VMnet5. Il reçoit l'IP 10.20.1.20, gateway 10.20.1.254 (interface DMZ du firewall), DNS Google.



Étape 29 — Vérifier la configuration IP du poste DMZ (ipconfig)

La commande ipconfig dans la console du poste DMZ confirme l'adresse 10.20.1.20 et la passerelle 10.20.1.254.

```
Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::cd26:27b0:344c:90ed%6
   Adresse IPv4. . . . . . . . . . . . . .: 10.20.1.20
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.20.1.254
```

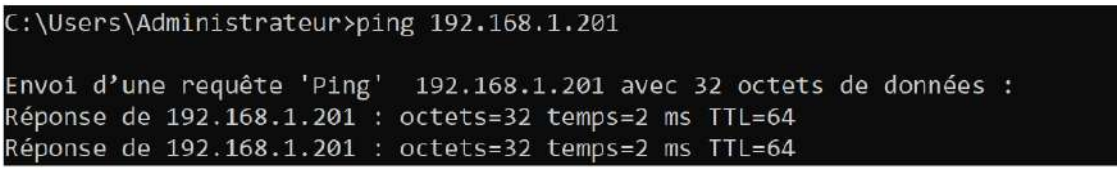
13. Tests de Validation & Connectivité

La phase de validation est la plus importante : elle confirme que l'ensemble de la chaîne (interfaces, routage, filtrage, NAT) fonctionne correctement. Les tests sont réalisés en ping depuis les postes clients LAN et DMZ.

Tests depuis le réseau LAN

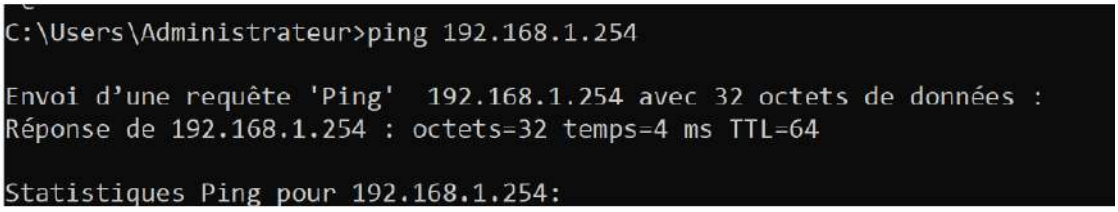
Étape 30 — Test 1 : Ping vers l'interface WAN du firewall (192.168.1.201)

Le premier test valide que le poste LAN peut joindre le firewall via son interface WAN. Ce test confirme le routage inter-zones LAN→WAN et que les règles de filtrage autorisent le ping.



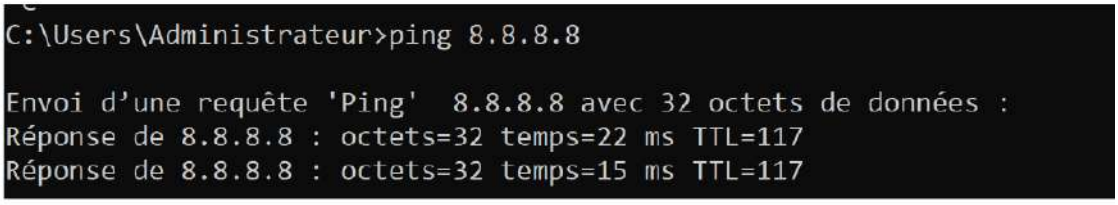
Étape 31 — Test 2 : Ping vers la gateway Internet (192.168.1.254)

Ce test valide que le trafic traverse bien le firewall et atteint la passerelle VMware NAT (192.168.1.254). Cela confirme que la route par défaut et le NAT sont correctement configurés.



Étape 32 — Test 3 : Ping vers Internet, IP (8.8.8.8 — Google DNS)

Le ping vers 8.8.8.8 est le test de connectivité Internet par excellence. Les réponses reçues confirment que le NAT masquerade fonctionne et que le trafic atteint Internet.



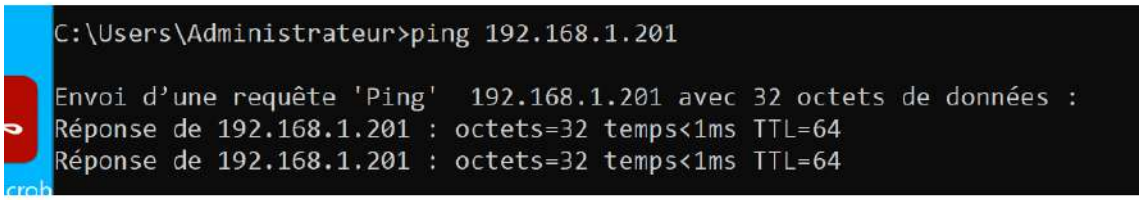
Étape 33 — Test 4 : Ping vers Internet, FQDN (google.fr)

Le ping vers google.fr valide la résolution DNS complète depuis le poste LAN. La réponse montre la résolution de google.fr en 142.251.142.67, puis les paquets ICMP retournés depuis Google.

Tests depuis le réseau DMZ

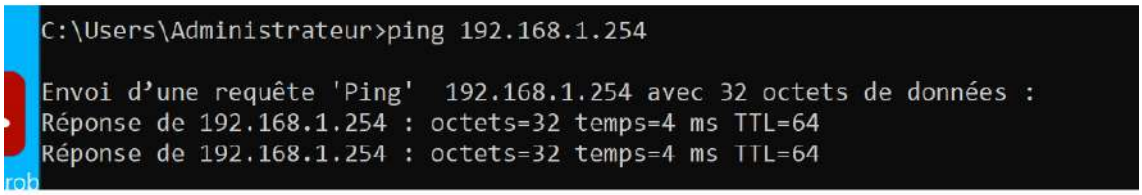
Étape 34 — Test 5 : Ping vers l'interface WAN du firewall depuis DMZ

Même test que depuis le LAN, mais réalisé depuis le poste de la DMZ (10.20.1.20). Le temps de réponse inférieur à 1ms est normal (réseau virtuel local).



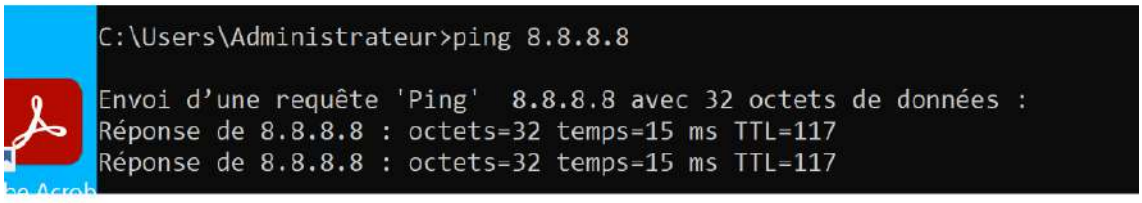
Étape 35 — Test 6 : Ping vers la gateway Internet depuis DMZ

Ce test confirme que le routage inter-zones fonctionne également depuis la DMZ. Le firewall route correctement le trafic de la DMZ vers le réseau WAN.



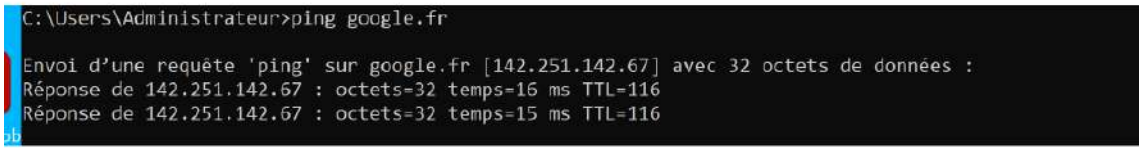
Étape 36 — Test 7 : Ping Internet (8.8.8.8) depuis DMZ

Connectivité Internet depuis la DMZ. Le TTL=117 est identique à celui obtenu depuis le LAN — le trafic emprunte le même chemin via le NAT masquerade du firewall.



Étape 37 — Test 8 : Ping FQDN (google.fr) depuis DMZ

Test final de validation DNS + Internet depuis la zone DMZ. Le résultat est identique à celui obtenu depuis le LAN : résolution DNS fonctionnelle et connectivité Internet opérationnelle.



14. Conclusion & Points Clés à Retenir

Ce TP a couvert l'intégralité du cycle de déploiement d'un firewall Stormshield Network Security : de la préparation VMware jusqu'à la validation de la connectivité Internet depuis les zones LAN et DMZ. Tous les objectifs initiaux ont été atteints avec succès.

Récapitulatif des étapes réalisées

- Préparation VMware : Virtual Network Editor, VMnet0 (Bridged/WAN), VMnet2 (LAN), VMnet5 (DMZ)
- Configuration matérielle de la VM : 3 adaptateurs réseau correctement mappés
- Premier démarrage console SNS : vérification des interfaces em0, em1, em2
- Accès SMA et découverte de l'interface graphique d'administration
- Configuration des interfaces WAN (Externe), LAN et DMZ (Internes)
- Configuration du routage : passerelle par défaut via objet Passerelle_internet
- Configuration DNS du firewall : dns1.google.com et dns2.google.com
- Création des objets réseau : Network_WAN, Network_LAN, Network_dmz1
- Politique de filtrage : règles autorisant LAN et DMZ vers Internet avec IPS
- Politique NAT : règles de masquerade pour LAN et DMZ via Firewall_WAN
- Console CLI SNS : syntaxe SYSTEM PING et commandes disponibles
- Configuration IP statique des postes Windows LAN (10.15.1.x) et DMZ (10.20.1.x)
- Tests de validation : ping WAN, gateway, 8.8.8.8 et google.fr depuis LAN et DMZ

Points techniques Stormshield essentiels

- Syntaxe CLI SNS : les commandes standard Unix ne fonctionnent pas (SYSTEM PING, pas "ping")
- Filtrage + NAT sont indépendants mais complémentaires — les deux sont requis pour l'accès Internet
- Default deny implicite : tout trafic non matché est bloqué, même sans règle explicite de blocage
- Les objets réseau centralisent l'adressage — jamais d'IP directe dans les règles
- Type d'interface (Interne/Externe) conditionne l'application des politiques de sécurité
- L'appliance EVA est fonctionnellement identique aux appliances physiques SNS de la gamme SN