SAE 41: Sécuriser un système d'information

Par Nelson THOMAS et Marin LEVEIL

A l'attention de Mme LABAT et M. FARGEAS

Année Universitaire 2024-2025

Sommaire

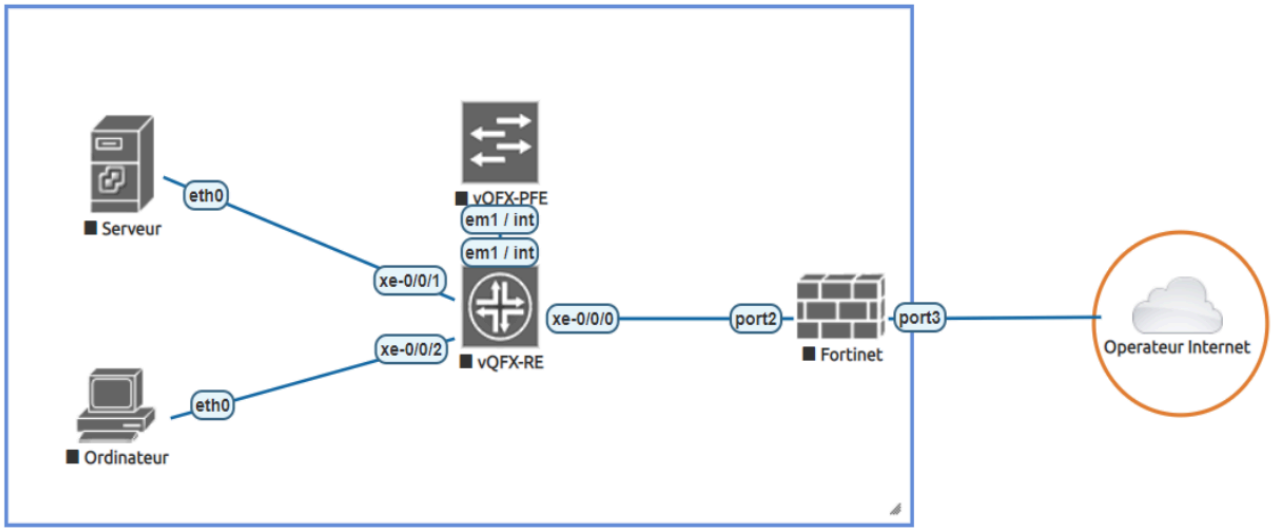
I. Contexte

A. Introduction

Dans le cadre du projet SAÉ 41, nous incarnons une Entreprise Nationale Multi-Sites devant implémenter une infrastructure réseau sécurisée. L'objectif principal est de concevoir et d'assurer la sécurisation du système d'information tout en permettant la communication efficace entre les différents sites via un réseau WAN interconnecté par un tunnel IPSec. Ce projet vise à reproduire des architectures et des solutions réseau réellement utilisées dans les entreprises aujourd'hui, offrant ainsi une expérience directement transposable au monde professionnel.

B. Topologie Technique

Chaque site comprend au minimum :



C. Objectifs du Projet

L'entreprise dispose de plusieurs sites, chacun devant implémenter une architecture réseau comprenant par exemple:

- Un réseau LAN sécurisé avec des VLANs distincts pour les postes clients et les serveurs.
- Un cloisonnement des VLANs à l'aide de VRF pour isoler le trafic des utilisateurs et des serveurs.
- Un routage inter-VLAN et inter-VRF assuré par un switch de niveau 3 et un firewall fortinet.
- Un routage dynamique entre le firewall et le switch de niveau 3.
- Une interconnexion IPSec entre sites distants, pouvant adopter une architecture Hub & Spoke ou Site-to-Site.
- Une éventuelle implémentation d'un SD-WAN utilisant deux opérateurs différents.
- Une Gestion avancée des firewalls avec un affinement des règles et de l'optimisation des performances.
- Implémentation d'éléments de dépannage réseau, diagnostic et correction des problèmes de connectivité et de performances.

D. Les différents éléments centraux

L'un des principaux intérêts de cette SAÉ était de nous faire découvrir des équipements de marques autre que Cisco afin de mieux comprendre les réelles utilisations dans le monde professionnel et de mesurer dans une certaine l'uniformité et des similitudes des commandes de configuration entre les équipements Cisco que nous utilisons dans notre cursus et d'autres marque comme par exemple les switchs Arista utilisés dans le monde professionnel.

Switch de niveau 3 Arista:

- Adoption en entreprise: Arista est un acteur clé dans les data centers et réseaux cloud, concurrençant Cisco et Juniper.

- Performance et automatisation: Son OS (EOS) est basé sur Linux, supporte l'automatisation (Python, Ansible) et optimise le routage et la QoS.

- Opportunités professionnelles: Compétence recherchée avec des certifications (ACE-A), ouvrant la porte à des postes bien rémunérés en réseau et cloud.

Firewall fortinet:

Fortinet est largement utilisé en entreprise

- C'est l'un des leaders du marché des firewalls, utilisé dans les PME, grandes entreprises et administrations.

- Très présent dans les SOC, datacenters et infrastructures cloud/hybrides.

- Reconnu pour son bon rapport qualité/prix et ses performances optimisées.

Facilité de gestion et automatisation

- Interface web intuitive et gestion centralisée avec FortiManager.

- Possibilité d'automatiser la sécurité avec des politiques dynamiques et FortiAnalyzer.

- Intégration facile avec d'autres solutions Fortinet (FortiSwitch, FortiAP, FortiAuthenticator).

Sécurité avancée et protection en temps réel

- IPS, filtrage web, sandboxing et inspection SSL pour bloquer les menaces.

- Gestion des VPN, segmentation réseau (VRF/VLAN) et détection des attaques.

- Intégré aux SOC et SIEM pour une surveillance proactive des incidents.

E. Informations de connexion

Lien pour l'accès à pnetlab :

https://185.15.27.134:15444/

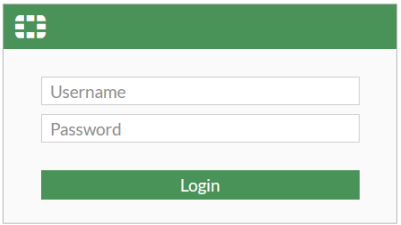
Login et mot de passe que nous avons utilisé :
Groupe1B/admIUTTeam01B

Configuration pour l'accès à l'interface graphique du fortinet :

Dans notre projet, il fallait accéder à l'interface graphique du Fortinet en configurant une des interfaces de ce dernier. Vous trouverez ci-dessous la configuration que nous avons utilisé.

```
config system interface
edit port1
set mode static
set ip 172.31.0.25/24
config router static
edit 1
set dst 0.0.0.0/0
set gateway 172.31.0.254
set device port1
```

Dans la configuration ci-dessus, nous modifions l'interface port1 du fortinet afin de lui attribuer l'ip externe 172.31.0.25 statiquement. Par la suite, il faut indiquer la passerelle 172.31.0.254. Cette configuration permet maintenant au fortinet de répondre à la requête de connexion vers le serveur de pnetlab (185.15.27.134). Il faut préciser un numéro de port qui nous a été affecté (10025).

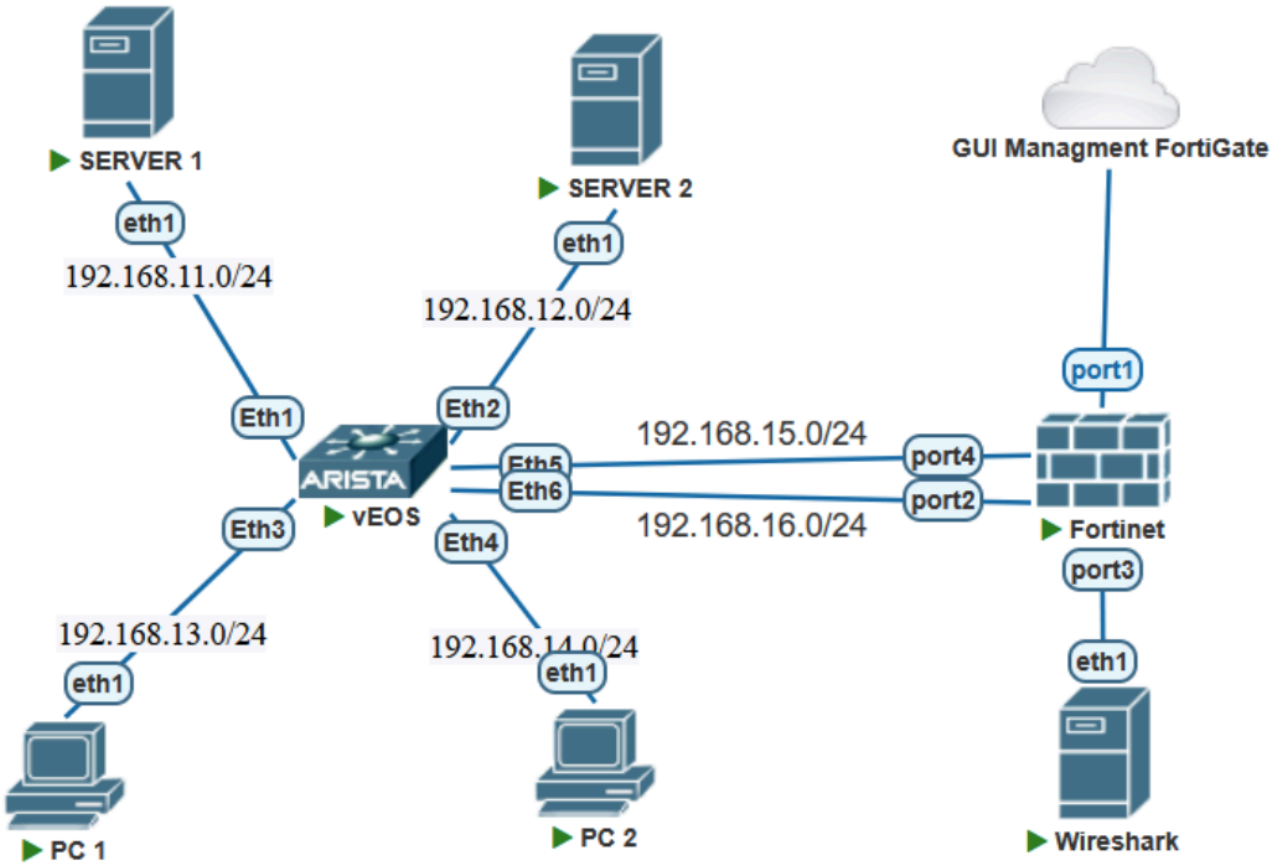


Après cela, nous avions accès à l'interface d'administration du fortinet.

interface externe sur le réseau pnetlab : 172.32.0.25/24

	Login	MDP
Arista (vEOS)	admin	Ø
Fortinet	admin	Ø (Pas de MDP pour la connexion) admin

II. Architecture



Cette section du compte rendu détaille les différentes composantes de notre architecture réseau. Et leur utilité dans un contexte d'entreprise.

<u>Du côté du switch Arista :</u>

- Connexion des périphériques finaux (PC, serveurs).

Cette connexion est essentielle pour assurer la communication entre les équipements informatiques de l'entreprise, permettant aux employés d'accéder aux ressources nécessaires.

- Connexion au firewall Fortinet.

Le firewall agit comme une barrière de sécurité entre le réseau interne et l'extérieur, filtrant le trafic et protégeant l'entreprise contre les menaces.

- Mise en place de 4 VLANs : un dédié à chaque serveur et un autre pour les postes clients.

L'utilisation des VLANs permet d'organiser le réseau en segments logiques, améliorant la sécurité et la gestion des flux tout en limitant la propagation des éventuels incidents.

- Communication inter-VLAN via un routage interne, permettant aux VLANs de communiquer entre eux.

Cette communication est indispensable pour permettre aux différents départements de l'entreprise d'échanger des données tout en maintenant une séparation logique.

- Mise en place de VRF (Virtual Routing and Forwarding) pour segmenter les tables de routage et limiter les communications inter-VLAN (isolation des PC et des serveurs).

L'isolement des flux entre les utilisateurs et les serveurs renforce la sécurité et optimise la gestion des accès en limitant les échanges inutiles.

<u>Du côté du firewall Fortinet :</u>

- Mise en place d'OSPF entre le switch et le firewall pour assurer le routage dynamique.

OSPF permet une gestion efficace et automatisée des routes réseau, assurant une connectivité optimale et une adaptation rapide aux changements d'infrastructure.

- Filtrage du trafic inter-VRF via le firewall, avec des règles spécifiques (exemple : autorisation du trafic FTP).

Cette segmentation permet de mieux contrôler les communications entre les différentes zones du réseau et de limiter les accès aux seules ressources nécessaires.

- Contrôle des flux entrants et sortants, en restreignant les accès aux services nécessaires (HTTP(S), DNS).

Ce filtrage empêche les connexions non autorisées, réduisant ainsi les risques d'attaques externes et de fuites de données.

- Port mirroring pour analyser le trafic réseau en temps réel avec Wireshark (sniffing), soit directement sur le switch.

Cette fonction est utile pour la surveillance et le dépannage du réseau, permettant d'identifier rapidement les anomalies ou menaces potentielles.

- Mise en place de l'IPS afin de contrôler automatiquement les trames inter-VRFs. Cela apporte une sécurité en plus pour les serveurs.

Un IPS détecte et bloque les activités suspectes en temps réel, renforçant ainsi la protection contre les cyberattaques et intrusions.

- Interconnexion avec les autres étudiants via un VPN IPsec.

L'utilisation d'un VPN IPsec permet de chiffrer les communications entre sites distants, garantissant la confidentialité et l'intégrité des données échangées.

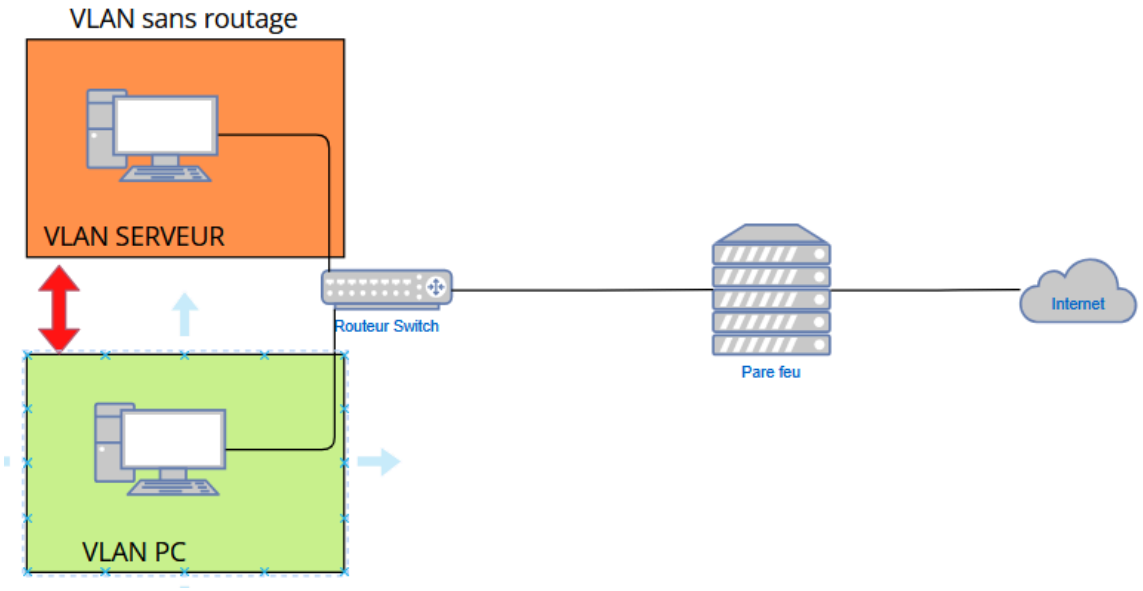
III. Les services implémentés

A. Switch Arista

1. VLANs, Routage inter-VLANs et DHCP

VLANS :

Un VLAN (Virtual Local Area Network) est un réseau logique qui segmente un réseau physique en plusieurs sous-réseaux indépendants. Il améliore la sécurité, la gestion du trafic et l'efficacité du réseau en isolant les communications entre groupes d'utilisateurs.



Objectif de cette partie :

Cette partie concerne l'adressage des VLAN connectés au switch/routeur arista. Le routage n'est pas activé sur ce dernier ce qui empêche les deux VLAN's de communiquer entre eux. Donc : Configuration DHCP.

Création:

```
vlan 11
   name SERVEUR1
!
vlan 12
   name SERVEUR2
!
vlan 13
   name PC1
!
vlan 14
   name PC2
```

Attribution des ip sur les VLANs :

```
interface Vlan11
   ip address 192.168.11.254/24
!
interface Vlan12
   ip address 192.168.12.254/24
!
interface Vlan13
   ip address 192.168.13.254/24
!
interface Vlan14
   ip address 192.168.14.254/24
```

Attribution des VLANs aux interfaces :

```
interface Ethernet1
   switchport access vlan 11
!
interface Ethernet2
   switchport access vlan 12
!
interface Ethernet3
   switchport access vlan 13
!
interface Ethernet4
   switchport access vlan 14
```

Configuration DHCP :

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui attribue automatiquement des adresses IP et des paramètres de configuration aux appareils d'un réseau. Il simplifie la gestion des adresses IP et évite les conflits d'adressage.

Création des pools :

```
dhcp server
  subnet 192.168.11.0/24
    range 192.168.11.50 192.168.11.70
    name POOL_SERVER_1
    dns server 8.8.8.8
    default-gateway 192.168.11.254
  !
  subnet 192.168.12.0/24
    range 192.168.12.50 192.168.12.70
    name POOL_SERVER_2
    dns server 8.8.8.8
    default-gateway 192.168.12.254
  !
  subnet 192.168.13.0/24
    range 192.168.13.50 192.168.13.70
    name POOL_PC_1
    dns server 8.8.8.8
    default-gateway 192.168.13.254
  !
  subnet 192.168.14.0/24
    range 192.168.14.50 192.168.14.70
    name POOL_PC_2
    dns server 8.8.8.8
    default-gateway 192.168.14.254
```

Activation DHCP sur les serveurs avec dhcp server ipv4 :

```
interface Vlan11
   ip address 192.168.11.254/24
   dhcp server ipv4
!
interface Vlan12
   ip address 192.168.12.254/24
   dhcp server ipv4
!
interface Vlan13
   ip address 192.168.13.254/24
   dhcp server ipv4
!
interface Vlan14
   ip address 192.168.14.254/24
   dhcp server ipv4
```

Test de ping entre les VLANs :

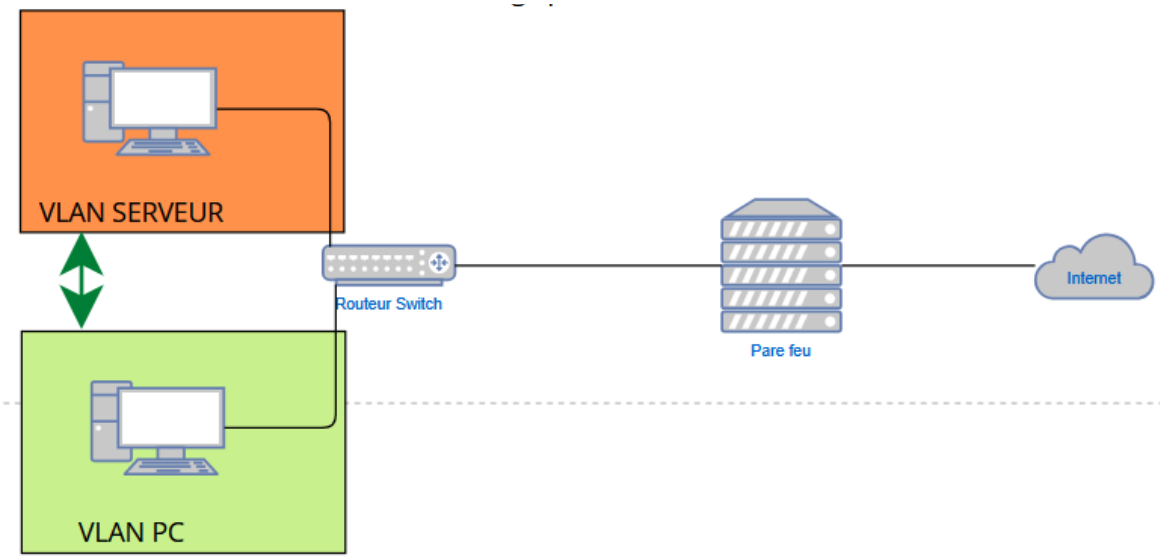
```
root@PC2:/home# ping 192.168.11.50
PING 192.168.11.50 (192.168.11.50) 56(84) bytes of data.
^C
--- 192.168.11.50 ping statistics ---
27 packets transmitted, 0 received, 100% packet loss, time 26618ms

root@PC2:/home#
```

Cela ne fonctionne pas car le routage n'est pas activé sur le switch Arista.

Routage inter-VLANs

Le routage inter-VLAN permet la communication entre VLANs via un routeur ou un switch de niveau 3. Ce dernier est la solution la plus rapide et efficace pour interconnecter les VLANs.



Objectif de cette partie :

Activation du routage sur l'Arista ce qui permet aux deux VLANS de communiquer ensemble.

Activation du routage sur le switch :

```
ip routing
```

Test de ping entre les VLANs :

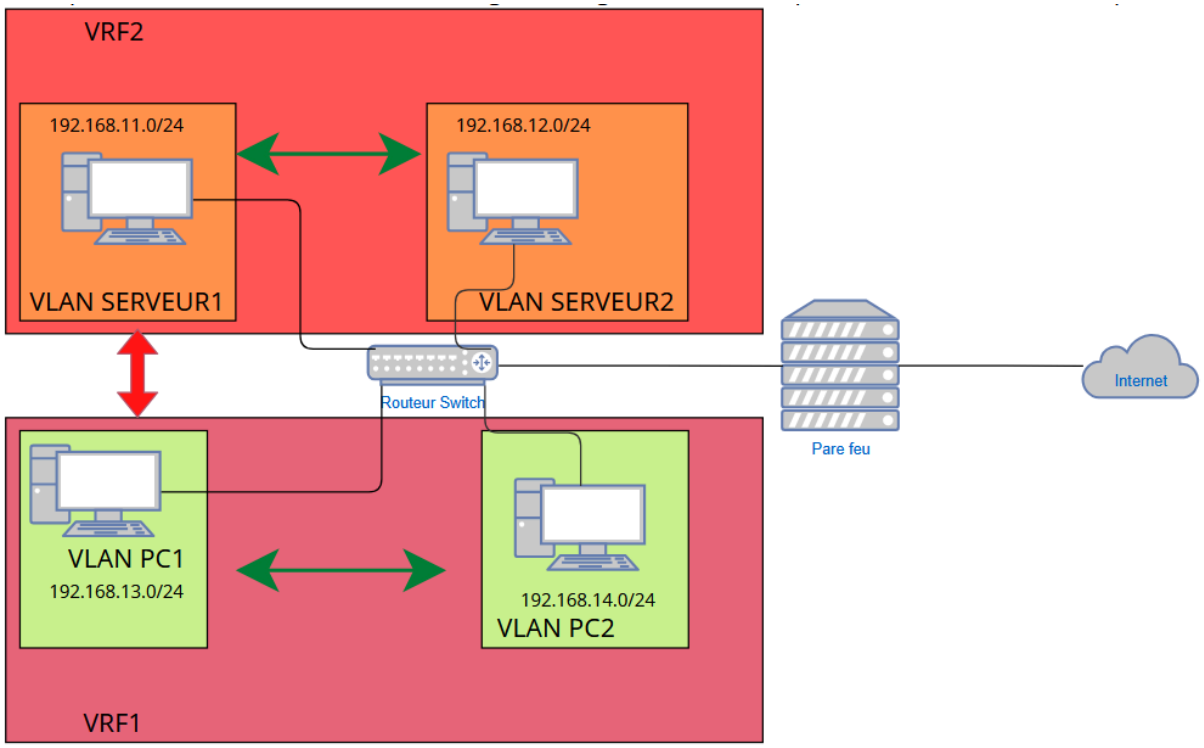
```
root@PC2:/home# ping 192.168.11.50
PING 192.168.11.50 (192.168.11.50) 56(84) bytes of data.
64 bytes from 192.168.11.50: icmp_seq=1 ttl=63 time=14.9 ms
64 bytes from 192.168.11.50: icmp_seq=2 ttl=63 time=4.19 ms
64 bytes from 192.168.11.50: icmp_seq=3 ttl=63 time=2.42 ms
64 bytes from 192.168.11.50: icmp_seq=4 ttl=63 time=4.59 ms
64 bytes from 192.168.11.50: icmp_seq=5 ttl=63 time=5.54 ms
^C
--- 192.168.11.50 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 2.420/6.323/14.877/4.394 ms
root@PC2:/home#
```

Nous pouvons voir que le problème de la partie précédente est maintenant résolu.

2. VRFS et OSPF

VRF

VRF (Virtual Routing and Forwarding) est une technologie de virtualisation du routage qui permet à un routeur de maintenir plusieurs tables de routage distinctes. Cela permet d'isoler le trafic entre différents clients ou services sur un même équipement réseau.



Mise en place de VRF pour cloisonner les tables de routage. Le routage devient impossible entre les machines de différentes VRF mais toujours possible entre les machines de la même VRF.

Création des VRFs :

```
vrf instance VRF_PC
!
vrf instance VRF_SERVER
```

Attribution des VRF dans les VLANs :

```
interface Vlan11
   vrf VRF_SERVER
   ip address 192.168.11.254/24
   dhcp server ipv4
!
interface Vlan12
   vrf VRF_SERVER
   ip address 192.168.12.254/24
   dhcp server ipv4
!
interface Vlan13
   vrf VRF_PC
   ip address 192.168.13.254/24
   dhcp server ipv4
!
interface Vlan14
   vrf VRF_PC
   ip address 192.168.14.254/24
   dhcp server ipv4
```

Attention, il faut refaire les conf ip et dhcp sur les interfaces.

Activation du routage intra VRF :

```
ip routing vrf VRF_PC
ip routing vrf VRF_SERVER
```

Test du routage :

Routage intra VRF (doit fonctionner) (PC2 vers PC1):

```
root@PC2:/home# ping 192.168.13.51
PING 192.168.13.51 (192.168.13.51) 56(84) bytes of data.
64 bytes from 192.168.13.51: icmp_seq=1 ttl=63 time=8.22 ms
64 bytes from 192.168.13.51: icmp_seq=2 ttl=63 time=3.72 ms
64 bytes from 192.168.13.51: icmp_seq=3 ttl=63 time=2.35 ms
^C
--- 192.168.13.51 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.348/4.764/8.222/2.508 ms
root@PC2:/home#
```

Cela fonctionne comme prévu.

Routage inter VRF (ne doit pas fonctionner) (PC2 vers SERVER1):

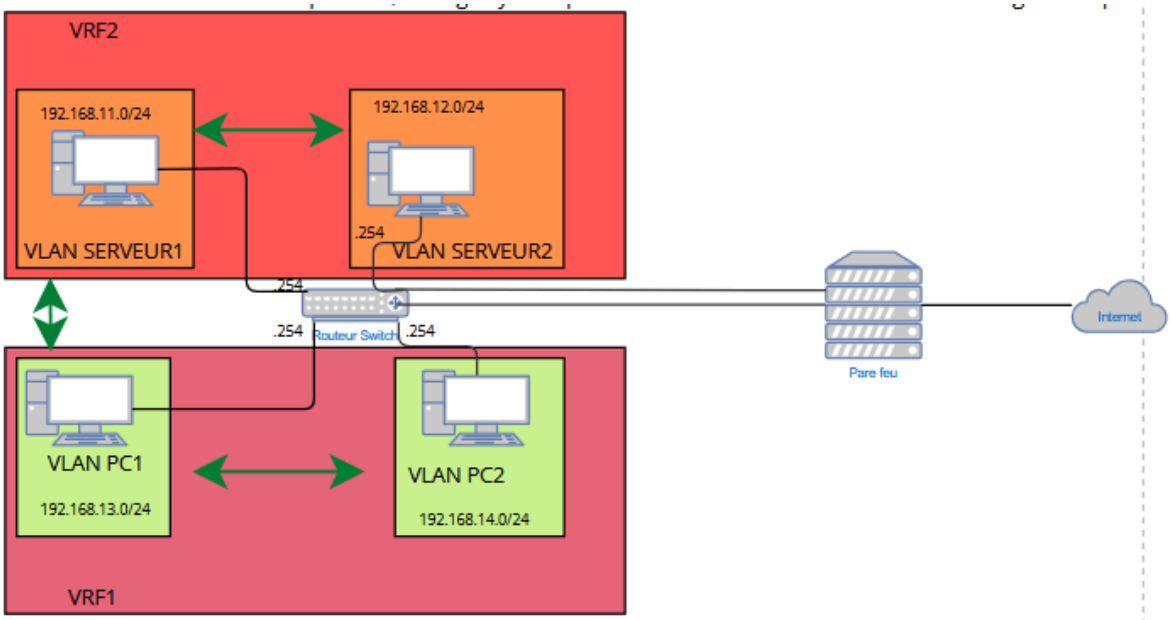
```
root@PC2:/home# ping 192.168.11.50
PING 192.168.11.50 (192.168.11.50) 56(84) bytes of data.
From 192.168.14.254 icmp_seq=1 Destination Net Unreachable
From 192.168.14.254 icmp_seq=2 Destination Net Unreachable
From 192.168.14.254 icmp_seq=3 Destination Net Unreachable
^C
--- 192.168.11.50 ping statistics ---
4 packets transmitted, 0 received, +3 errors, 100% packet loss, time 3005ms

root@PC2:/home#
```

Comme prévu, cela ne fonctionne pas.

OSPF

OSPF (Open Shortest Path First) est un protocole de routage à état de liens utilisé dans les réseaux IP pour calculer le chemin le plus court entre les routeurs. Il fonctionne de manière hiérarchique et utilise l'algorithme de Dijkstra pour mettre à jour dynamiquement les routes.



Interconnexion entre le switch Arista et le pare feu Fortinet. Routage dynamique et autorisation du flux entre les deux VRF grâce au pare-feu fortinet.
Communication intra et inter vlan possible.

Configuration des VRF et de l'ospf entre les équipements :

Création des VLAN 15 et 16 :

```
vlan 15
   name ROUTAGE_SERVEURS
!
vlan 16
   name ROUTAGE_PC
```

Configuration des VLAN 15 avec ip et VRF :

```
interface Vlan15
   vrf VRF_SERVER
   ip address 192.168.15.1/24
!
interface Vlan16
   vrf VRF_PC
   ip address 192.168.16.1/24
```

Attribution des interfaces eth5 et eth6 dans les VLAN 15 et 16 :

```
interface Ethernet5
   switchport access vlan 15
!
interface Ethernet6
   switchport access vlan 16
```

Routage dynamique :

Ajout de routes par défaut dans les VRF du switch/routeur :

```
ip route vrf VRF_PC 0.0.0.0/0 192.168.16.2
ip route vrf VRF_SERVER 0.0.0.0/0 192.168.15.2
```

OSPF sur l'Arista :

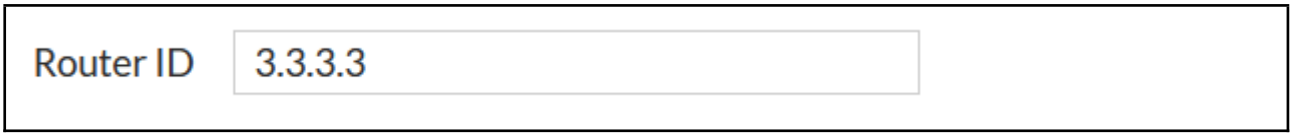
```
router ospf 1 vrf VRF_SERVER
   router-id 1.1.1.1
   passive-interface Ethernet1
   passive-interface Ethernet2
   network 192.168.11.0/24 area 0.0.0.0
   network 192.168.12.0/24 area 0.0.0.0
   network 192.168.15.0/24 area 0.0.0.0
   max-lsa 12000
!
router ospf 2 vrf VRF_PC
   router-id 2.2.2.2
   passive-interface Ethernet3
   passive-interface Ethernet4
   network 192.168.13.0/24 area 0.0.0.0
   network 192.168.14.0/24 area 0.0.0.0
   network 192.168.16.0/24 area 0.0.0.0
   max-lsa 12000
!
end
```

Configuration de l'ospf sur le fortinet :

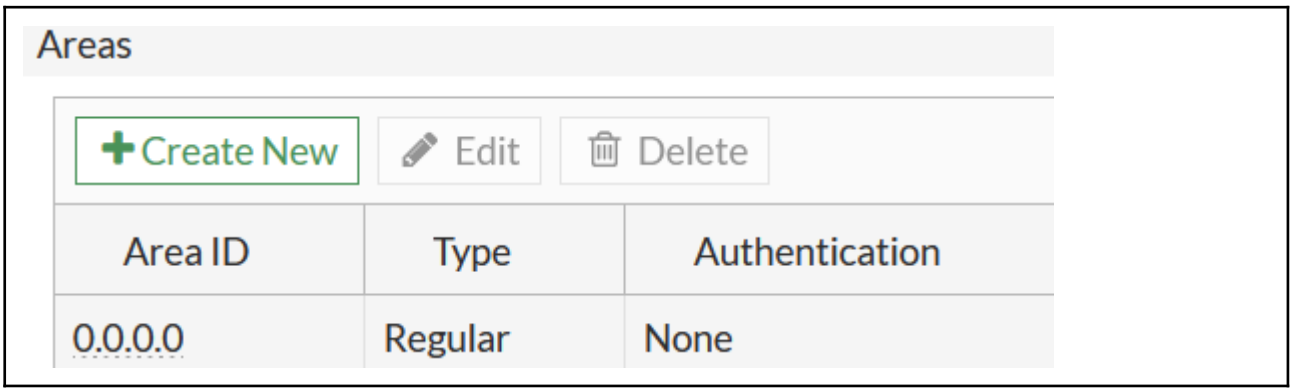
```
config router ospf
    set router-id 3.3.3.3
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "port2"
            set interface "port2"
        next
        edit "port4"
            set interface "port4"
        next
    end
    config network
        edit 1
            set prefix 192.168.15.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.16.0 255.255.255.0
        next
    end
    config redistribute "connected"
    end
    config redistribute "static"
        set status enable
    end
end
```

Il faut aussi faire les règles sur le pare-feu fortinet pour laisser les réseaux communiquer entre eux. (voir partie Firewall Fortinet: Filtrage)

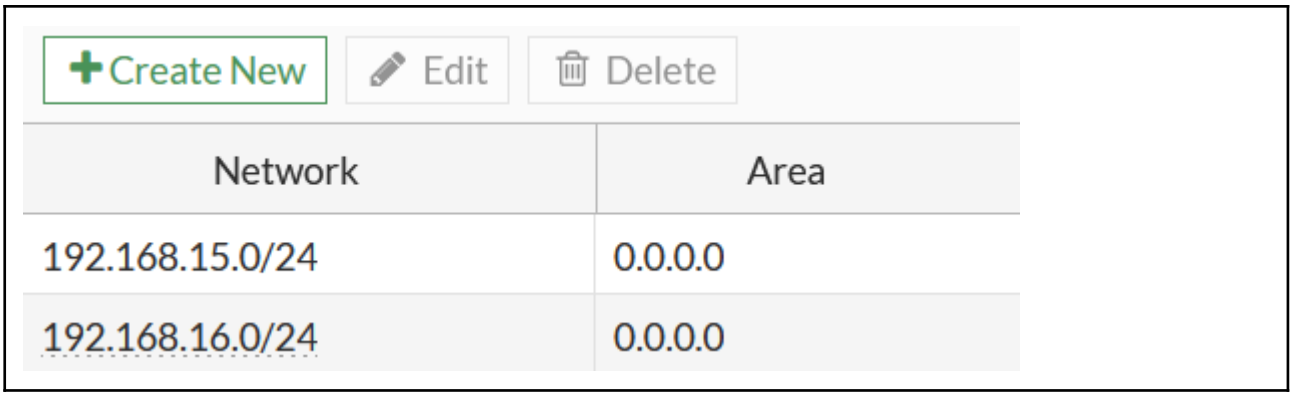
Configuration graphique OSP :



On configure un router ID. Ici nous utilisons 3.3.3.3 car 1.1.1.1 et 2.2.2.2 sont déjà prises pour les VRF.



On configure l'area 0 (backbone area) sur laquelle vont transiter les différentes informations de routage. On spécifie l'area 0 car OSP peut utiliser des zones de routage virtuelles.



On spécifie les différents réseaux à annoncer, ici ce sont les réseaux directement connectés du fortinet.

Affichage de la table de routage du ARISTA :

```
localhost#show ip route vrf VRF_SERVER

VRF: VRF_SERVER

Gateway of last resort:
 S       0.0.0.0/0 [1/0]
         via 192.168.15.2, Vlan15

 C       192.168.11.0/24
         directly connected, Vlan11
 C       192.168.12.0/24
         directly connected, Vlan12
 O       192.168.13.0/24 [110/21]
         via 192.168.15.2, Vlan15
 O       192.168.14.0/24 [110/21]
         via 192.168.15.2, Vlan15
 C       192.168.15.0/24
         directly connected, Vlan15
 O       192.168.16.0/24 [110/11]
         via 192.168.15.2, Vlan15
```

Les routes dynamiques sont bien présentes.

Ping dans la VRF :

SERVER1 vers SERVER2 (sensé fonctionner) :

```
root@SERVER 2:/home# ping 192.168.11.51
PING 192.168.11.51 (192.168.11.51) 56(84) bytes of data.
64 bytes from 192.168.11.51: icmp_seq=1 ttl=63 time=12.1 ms
64 bytes from 192.168.11.51: icmp_seq=2 ttl=63 time=2.26 ms
64 bytes from 192.168.11.51: icmp_seq=3 ttl=63 time=2.00 ms
^C
--- 192.168.11.51 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.001/5.455/12.101/4.700 ms
```

```
root@SERVER 2:/home#
```

Cela fonctionne comme prévu

Ping entre les VRF:

SERVER1 vers PC1 (Sensé fonctionner) :

```
root@SERVER 1 :/home# ping 192.168.13.51
PING 192.168.13.51 (192.168.13.51) 56(84) bytes of data.
64 bytes from 192.168.13.51: icmp_seq=1 ttl=61 time=13.2 ms
64 bytes from 192.168.13.51: icmp_seq=2 ttl=61 time=5.94 ms
64 bytes from 192.168.13.51: icmp_seq=3 ttl=61 time=6.76 ms
64 bytes from 192.168.13.51: icmp_seq=4 ttl=61 time=4.93 ms
^C
--- 192.168.13.51 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 4.932/7.700/13.167/3.221 ms
```

Cela fonctionne comme prévu

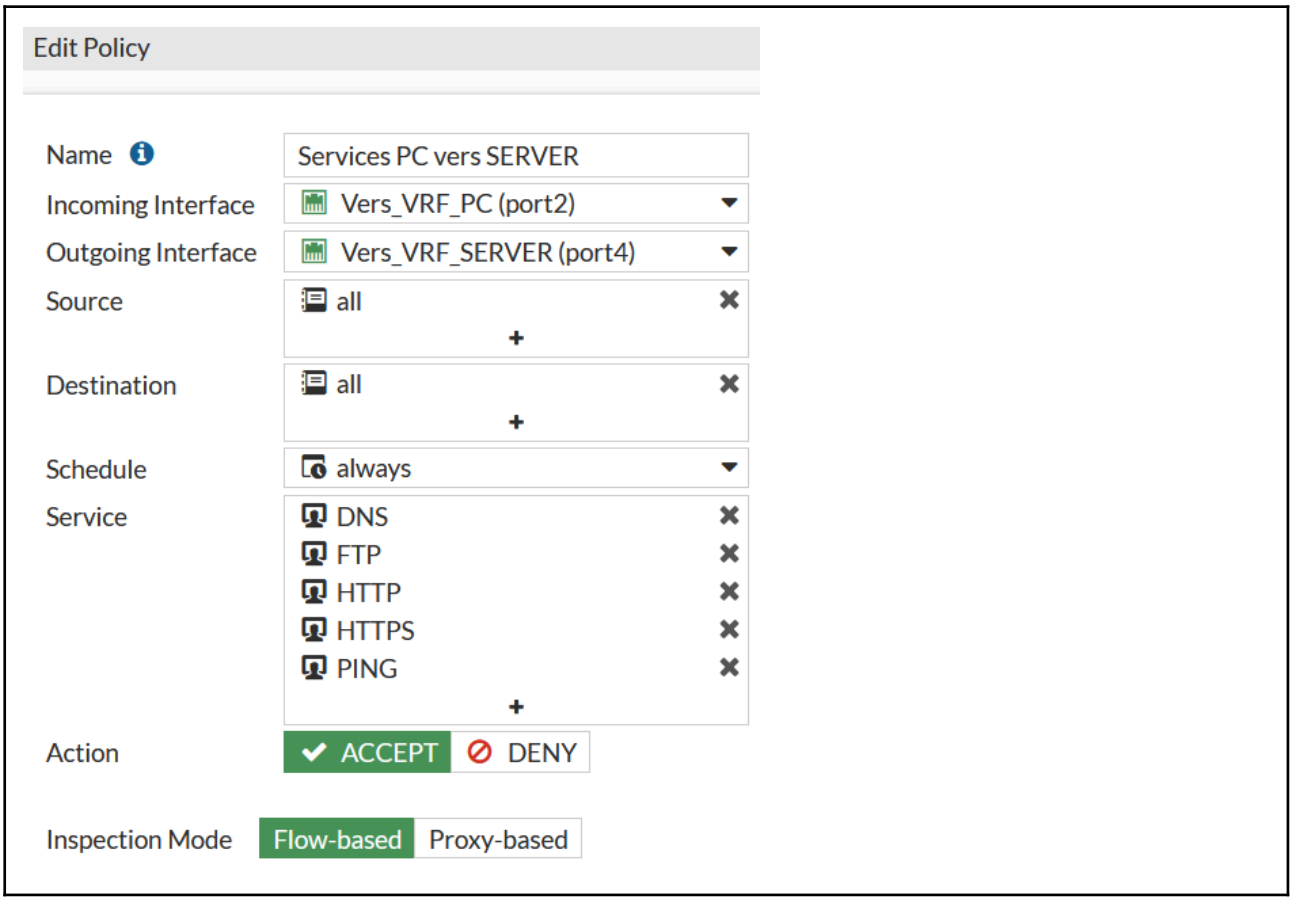
B. Firewall Fortinet

1. Filtrage

Les règles de filtrage sur un firewall Fortinet assurent la sécurité, la performance et la conformité du réseau. Elles contrôlent les accès, bloquent les cyberattaques (scans, intrusions, malwares) et optimisent le trafic pour éviter la surcharge. Enfin, elles garantissent le respect des normes de cybersécurité comme l'ISO 27001 ou le RGPD.

- Interdire tous les flux, puis autoriser ceux qui nous intéressent
- Filtrage pour laisser passer internet:
  - DNS
  - HTTP/S
- Filtrage pour laisser les Pcs faire des échanges de fichiers via les serveurs
  - FTP

Configuration d'une politique :



Politiques de filtrage sur le fortinet :

Name	Source	Destination	Schedule	Service	Action
Vers_VRF_PC (port2) → Vers_VRF_SERVER (port4) 2					
Services PC vers SERVER	all	all	always	DNS FTP HTTP HTTPS PING	ACCEPT
PC_vers_SERVER	all	all	always	ALL	DENY
Vers_VRF_SERVER (port4) → Vers_VRF_PC (port2) 2					
Services SERVER vers PC	all	all	always	DNS FTP HTTP HTTPS PING	ACCEPT
SERVER_Vers_PC	all	all	always	ALL	DENY
Implicit 1					
Implicit Deny	all	all	always	ALL	DENY

2. IPS

L'IPS (Intrusion Prevention System) sur un firewall Fortinet protège le réseau en détectant et bloquant les menaces en temps réel. Il empêche les attaques connues (exploits, malwares, scans réseau) grâce à une base de signatures, et analyse le comportement du trafic pour stopper les attaques inconnues (zero-day, brute-force). De plus, il renforce la sécurité entre VLANs/VRFs, limitant la propagation des infections et des intrusions internes.

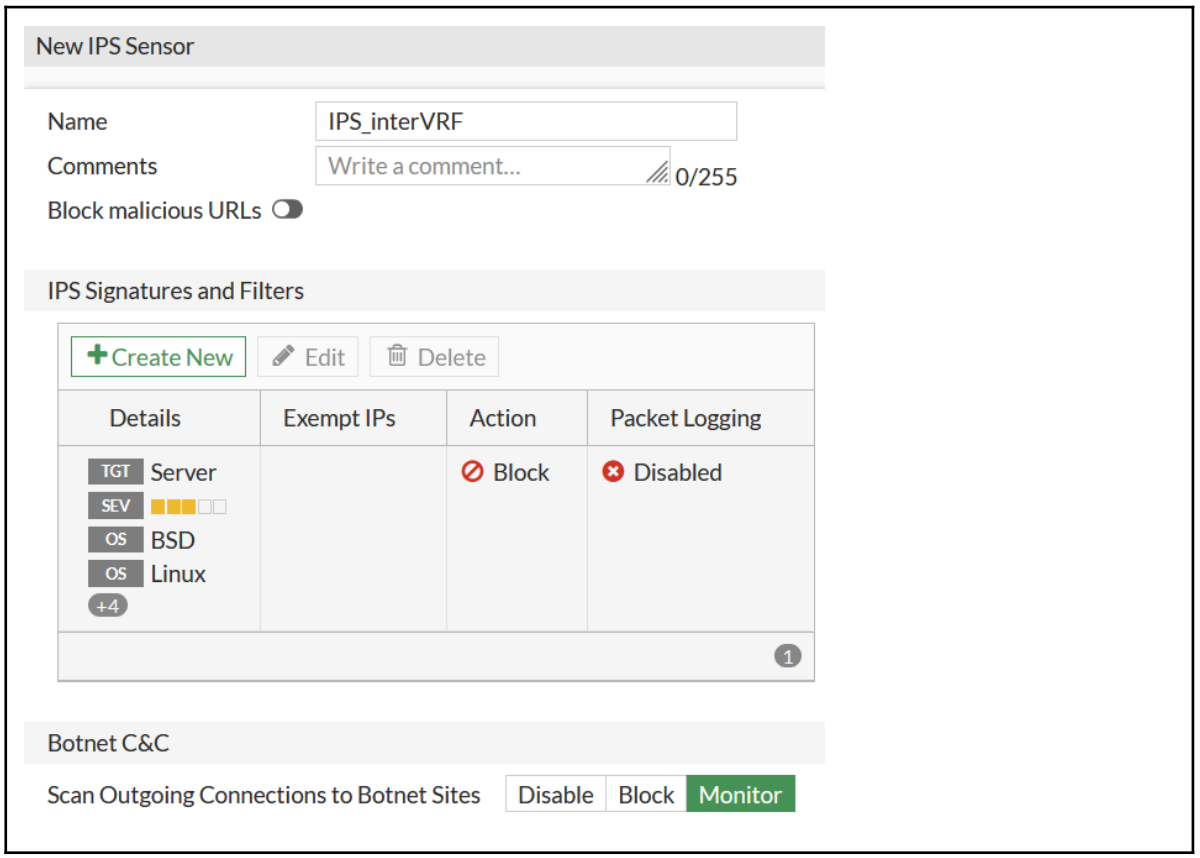
- Activer l'IPS (Intrusion Prevention System)
    - détecter et bloquer les menaces inter-VRF (pc infecté)

Onglet System > Feature visibility

Activation de l'IPS.

Configuration profil IPS :

Security Profiles > Intrusion Prevention



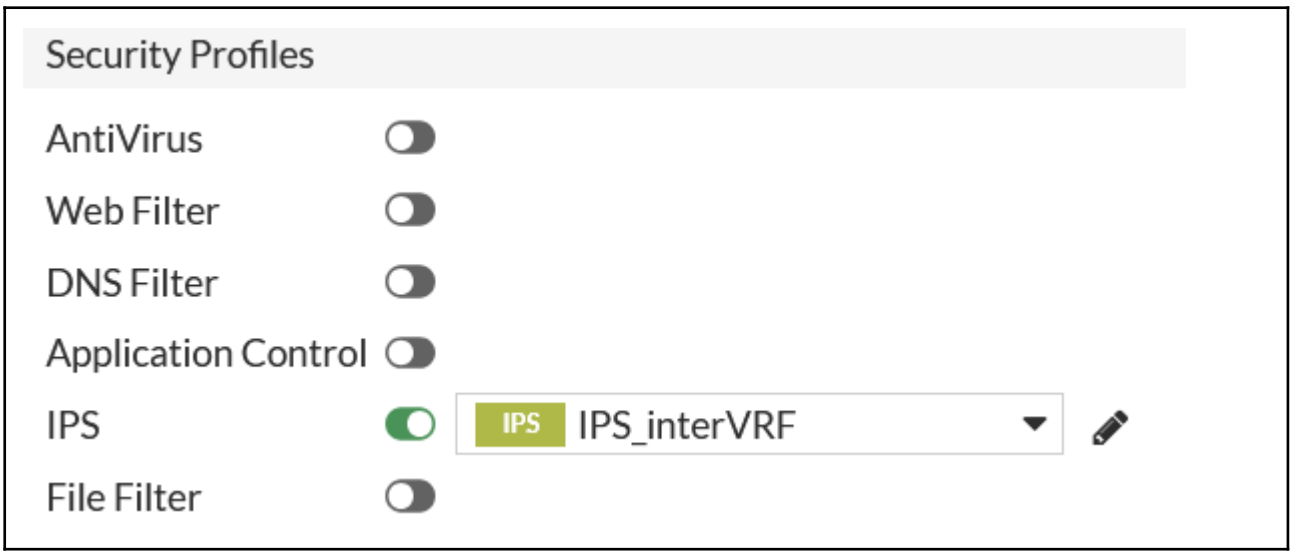
Ici, nous configurons un profil IPS avec des signatures afin de bloquer le trafic ciblant des serveurs, une sévérité jugée comme moyenne et provenant de tout type d'OS.

Application du profil sur une règle de pare-feu :

Policy & Objects > Firewall Policy

Dans notre scénario, nous souhaitons protéger les attaques des PC (infection potentielle) sur les serveurs.

Il faut retourner dans la politique de filtrage configurée dans la partie où nous autorisons uniquement le passage des ping, du dns, de FTP et HTTP(S). Nous éditons la politique Services PC vers SERVER.



Dans la section Security Profiles nous pouvons activer l'onglet IPS et choisir le profil IPS_interVRF défini précédemment.

L'IPS est maintenant actif entre nos deux VRF.

Nous pouvons voir les logs dans Log & Report > Events > Security Rating Events

À l'origine, nous voulions illustrer le fonctionnement en utilisant la commande NMAP pour scanner un serveur mais elle n'est pas disponible sur les machines du LAB.

3. Firewall policies

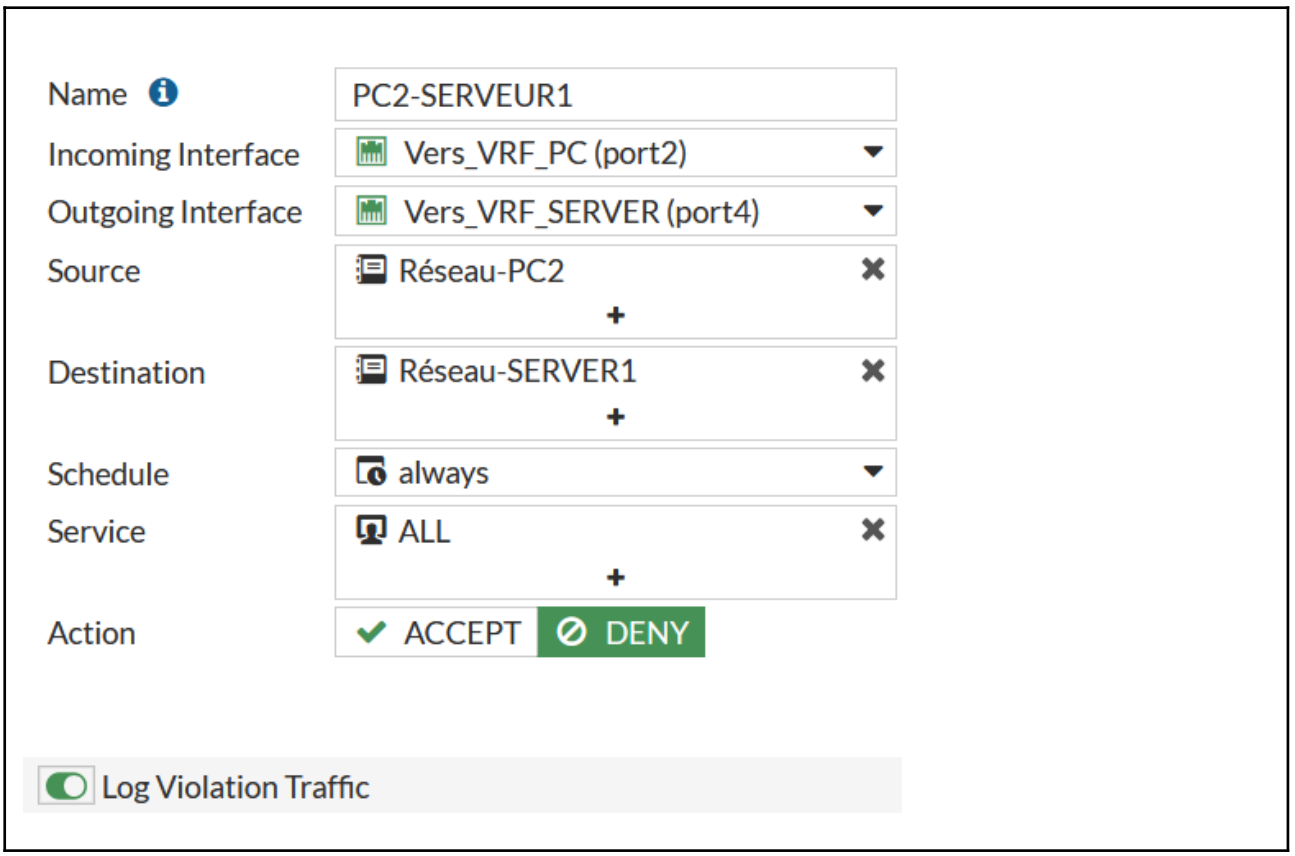
Les firewall policies permettent de définir et contrôler précisément le trafic autorisé ou bloqué entre différentes parties du réseau. Elles assurent la sécurisation en filtrant les flux entrants et sortants en fonction de critères comme l'adresse IP, le port, le protocole, ou l'interface. Ces politiques permettent également de segmenter le réseau, de protéger les ressources critiques et de garantir une gestion fine des accès. En appliquant des règles adaptées, elles préviennent les attaques et optimisent la performance du réseau en bloquant le trafic inutile.

Dans cette partie, nous allons créer une règle de pare-feu qui empêche au vlan PC2 d'accéder au vlan SERVER1.

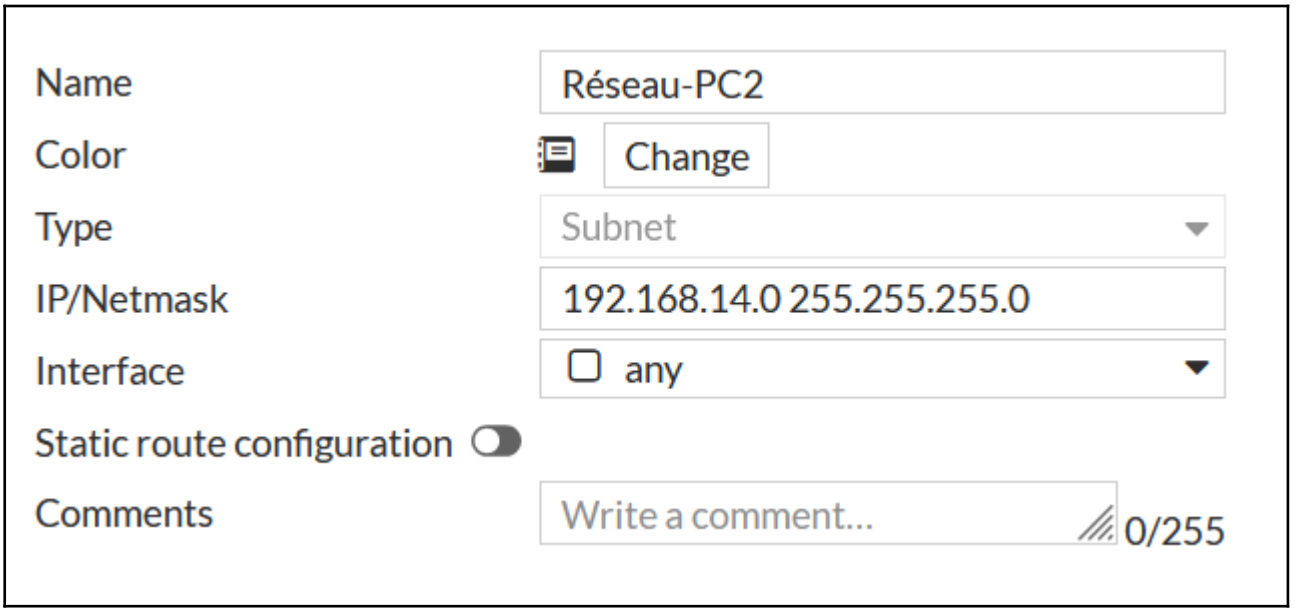
Ping PC2 vers SERVER1 :

```
root@PC 2 :/home# ping 192.168.11.51
PING 192.168.11.51 (192.168.11.51) 56(84) bytes of data.
64 bytes from 192.168.11.51: icmp_seq=1 ttl=61 time=8.86 ms
64 bytes from 192.168.11.51: icmp_seq=2 ttl=61 time=4.31 ms
64 bytes from 192.168.11.51: icmp_seq=3 ttl=61 time=3.96 ms
^C
--- 192.168.11.51 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.956/5.710/8.864/2.234 ms
root@PC 2 :/home#
```

Dans un premier temps, nous pouvons voir que PC2 à accès au serveur 1 (192.168.11.51).



Sur le Fortinet on configure une règle de filtrage qui refuse tout type de trafic du réseau de PC2 vers le réseau de SERVER1.



Voici la configuration de Réseau-PC2 vue dans la règle précédente.

Vers_VRF_PC (port2) → Vers_VRF_SERVER (port4) 3					
PC2-SERVEUR1	Réseau-PC2	Réseau-SERVER1	always	ALL	DENY
Services PC vers SERVER	all	all	always	DNS FTP HTTP HTTPS PING	ACCEPT
PC_vers_SERVER	all	all	always	ALL	DENY

Dans l'ordre de priorité, il faut bien placer la règle PC2-SERVEUR1 au-dessus car la règle Services PC vers SERVER autoriserait le trafic entre les deux VLAN.

```
root@PC 2 :/home# ping 192.168.11.51
PING 192.168.11.51 (192.168.11.51) 56(84) bytes of data.
^C
--- 192.168.11.51 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4085ms

root@PC 2 :/home#
```

Nous pouvons voir maintenant que le PC2 n'arrive plus à accéder au SERVER1.

Sur le Fortinet, dans l'onglet Log & Report > Forward Traffic :

Date/Time		Source
3 minutes ago		192.168.14.52
3 minutes ago		192.168.14.52
3 minutes ago		192.168.14.52
3 minutes ago		192.168.14.52
3 minutes ago		192.168.14.52

Destination	Application Name	Result	Policy ID
192.168.11.51		Deny: policy violation	PC2-SERVEUR1 (5)
192.168.11.51		Deny: policy violation	PC2-SERVEUR1 (5)
192.168.11.51		Deny: policy violation	PC2-SERVEUR1 (5)
192.168.11.51		Deny: policy violation	PC2-SERVEUR1 (5)
192.168.11.51		Deny: policy violation	PC2-SERVEUR1 (5)

Nous pouvons observer les log de filtrage des paquets qui passent au travers du fortinet.

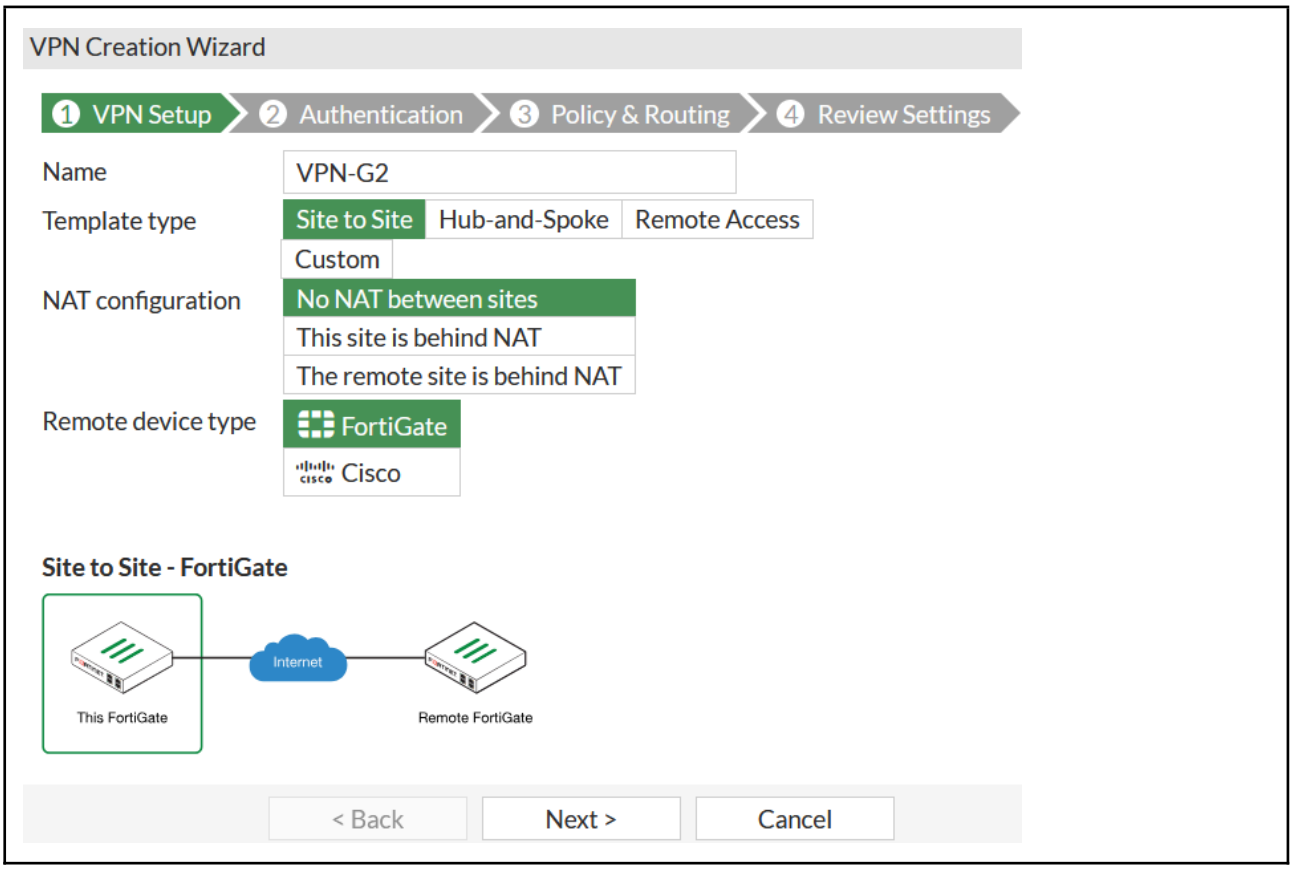
L'heure à laquelle elle s'est produite, l'adresse source et destination dans le paquet, l'état de refus pour cause de violation et la règle de filtrage qui a engendré le refus.

4. Interconnexion

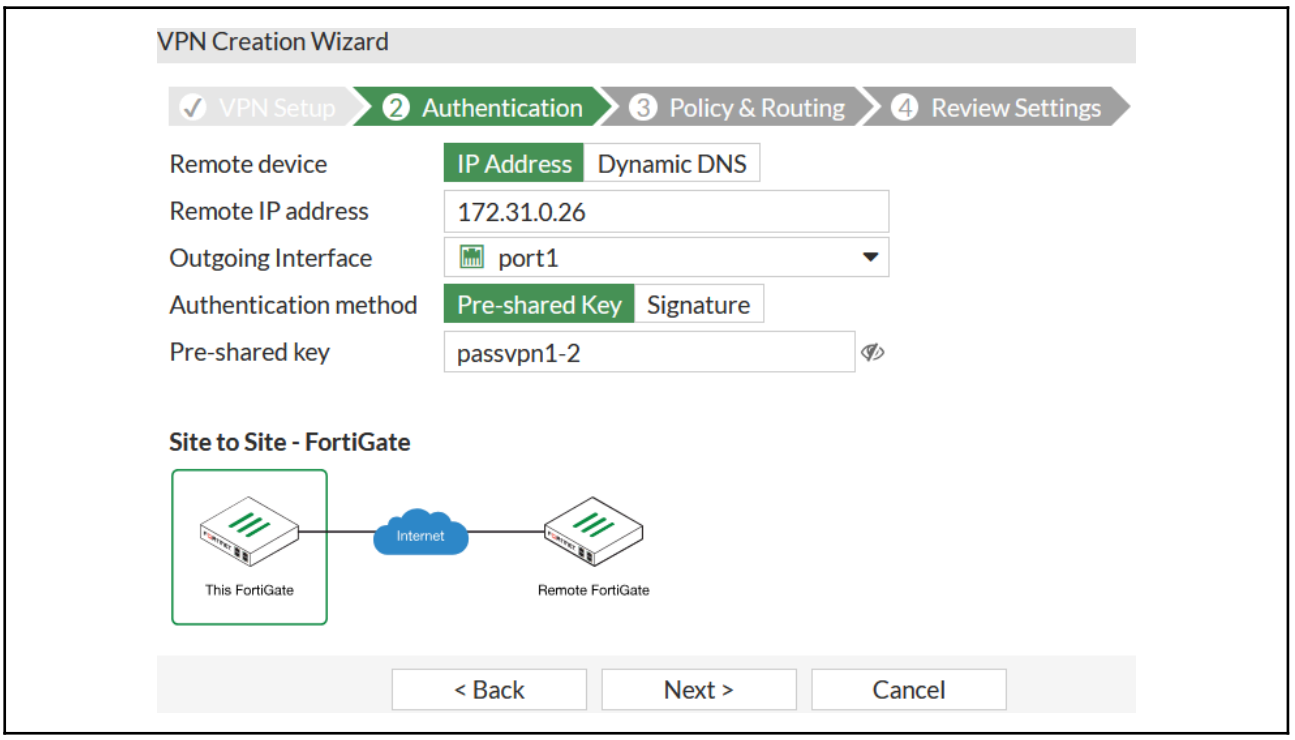
L'interconnexion via un VPN IPSec entre deux réseaux permet de sécuriser les communications en chiffrant les données qui transitent entre les sites distants. Cela garantit la confidentialité et l'intégrité des informations échangées, même sur des réseaux publics comme Internet. Le VPN IPSec permet également de connecter des sites géographiquement éloignés de manière sécurisée, en créant un tunnel privé entre eux. En outre, il réduit les risques d'interception et protège contre les attaques externes, tout en permettant aux utilisateurs distants d'accéder aux ressources internes du réseau de manière sécurisée.

VPN IPsec :

Même si nous n'avons pas pu nous mettre d'accord avec les autres groupes pour du VPN site à site, nous avons quand même essayé de configurer notre côté de la configuration VPN entre Fortinet.

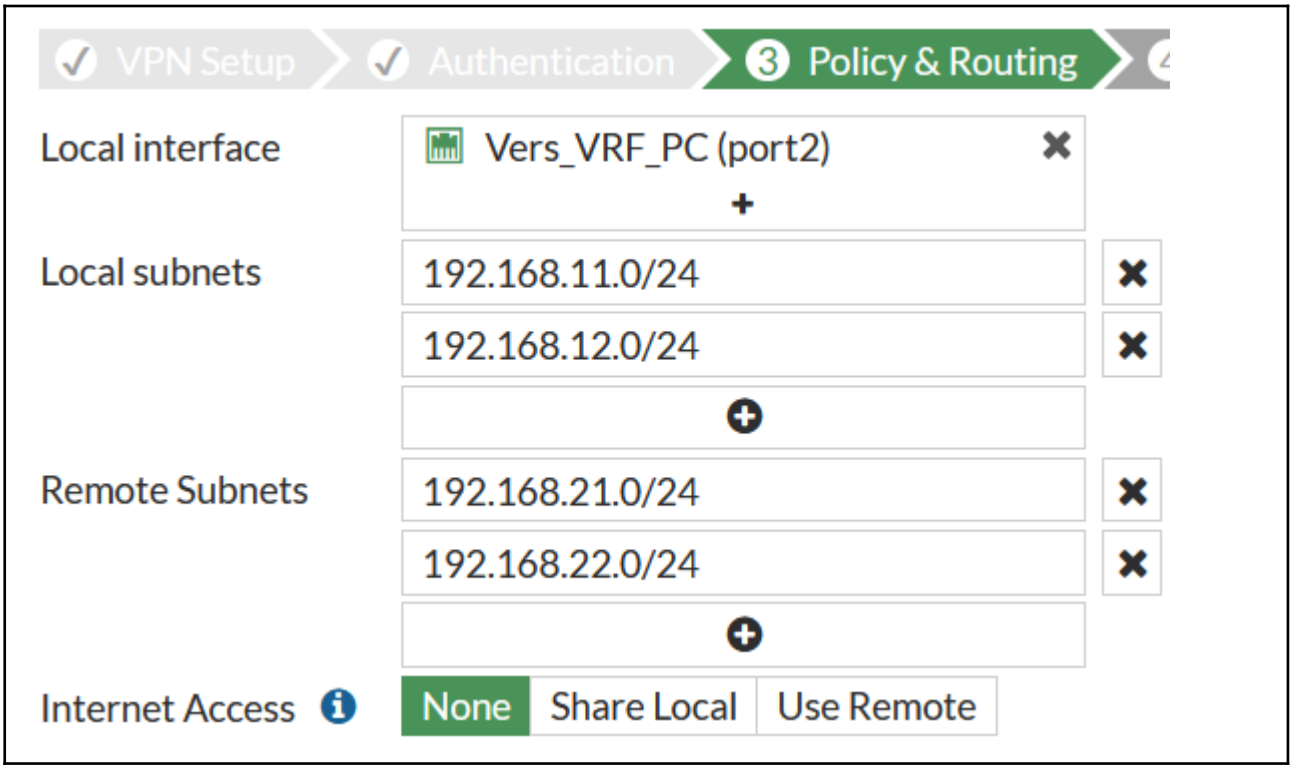


Nous voulons faire un VPN avec le groupe 2.



On indique l'adresse de l'interface distante, Fortinet du groupe 2 et l'interface locale afin de réaliser l'interconnexion entre nos fortinet.

Ensuite, on indique un mode de passe commun pour l'authentification sur le tunnel.



Par la suite, on configure quelle interface et quels réseaux ont le droit de communiquer sur le tunnel. Réseaux locaux et distants.

IV. Problèmes rencontrés/Solutions apportées

1. DHCP

Problème n°1:

- Les clients refusent les offres DHCP

```
root@PC 2 :/home# dhclient eth1 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3 (xid=0xb011953c)
DHCPOFFER of 192.168.14.51 from 192.168.14.254
DHCPREQUEST for 192.168.14.51 on eth1 to 255.255.255.255 port 67 (xid=0x3c9511b0)
DHCPACK of 192.168.14.51 from 192.168.14.254 (xid=0xb011953c)
/sbin/dhclient-script: 140: local: 2: bad variable name
DHCPDECLINE of 192.168.14.51 on eth1 to 255.255.255.255 port 67 (xid=0x3c9511b0)
```

Une erreur dans les clients poussait à refuser toutes les adresses proposées par le DHCP.

Solution:

Exécution d'une commande pour modifier le script gérant les messages DHCP

```
sed -i 's/^[[:space:]]*local[[:space:]]\+//g' /sbin/dhclient-script
```

```
root@PC 2 :/home# dhclient eth1 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
```

```
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3 (xid=0xa1e63662)
DHCPOFFER of 192.168.14.52 from 192.168.14.254
DHCPREQUEST for 192.168.14.52 on eth1 to 255.255.255.255 port 67 (xid=0x6236e6a1)
DHCPACK of 192.168.14.52 from 192.168.14.254 (xid=0xa1e63662)
bound to 192.168.14.52 -- renewal in 3250 seconds.
```

L'ip est maintenant acceptée par le client.

Problème n°2:

- Le DHCP ne fonctionne plus sur le switch arista après l'intégration des VRFs

```
root@Docker:/home# dhclient -v eth1
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/50:00:00:2d:00:01
Sending on   LPF/eth1/50:00:00:2d:00:01
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3 (xid=0x53dd2726)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 5 (xid=0x53dd2726)
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 5
^C
```

Après l'implémentation des VRF sur le Arista, le DHCP a cessé de fonctionner, les clients ne recevaient plus de DHCPOFFER.

Ceci est dû au fait que les pools ont auparavant été configurés dans le contexte global et non pas sur les VRF qui en sont isolées isolées.

Solution:

Configuration des pool DHCP dans les VRF :

```
dhcp server vrf VRF_PC
   subnet 192.168.13.0/24
```

```
    range 192.168.13.50 192.168.13.70
    name POOL_PC1
    default-gateway 192.168.13.254
  !
  subnet 192.168.14.0/24
    range 192.168.14.50 192.168.14.70
    name POOL_PC2
    default-gateway 192.168.14.254
!
```

En préfixant la configuration du DHCP avec une VRF, il était possible de créer les pools DHCP dans la VRF spécifiée.

```
Listening on LPF/eth1/50:00:00:d7:00:01
Sending on   LPF/eth1/50:00:00:d7:00:01
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3 (xid=0x97f5ec67)
DHCPOFFER of 192.168.11.51 from 192.168.11.254
DHCPREQUEST for 192.168.11.51 on eth1 to 255.255.255.255 port 67 (xid=0x67ecf597)
DHCPACK of 192.168.11.51 from 192.168.11.254 (xid=0x97f5ec67)
bound to 192.168.11.51 -- renewal in 3096 seconds.
```

Par la suite, les clients pouvaient à nouveau reçevoir des offres DHCP et les accepter.

2. Port mirroring

Nous avons essayé d'activer le port mirroring sur le fortinet puis sur le switch arista mais les commandes et les options n'étaient pas disponible sur la version fournie dans le lab.

problème n°1 Initialisation sur le Fortinet:

Configuration que nous aurions faite pour activer le port mirroring sur le fortinet :

```
config system interface
edit port2
set snmp-index 1
set span enable
set span-dest port3
next

edit port4
set snmp-index 1
set span enable
set span-dest port3
next
end
```

On active le SPAN (Switched Port Analyser) sur les port2 et port4 et on copie le trafic vers le port3.

Il est important de mettre les deux interfaces des VRF en miroir car il n'y a que le flux entrant sur les interfaces qui est copié ce qui nous donnerait accès uniquement à un côté du trafic.

problème n°2 Initialisation sur le switch arista :

Nous avons également essayé de configurer le mirroring sur le switch mais un message nous indiquant que le switch ne le supportait pas est apparu.

```
localhost(config)#monitor ses
  session  not supported on this hardware platform
```

```
configure
monitor session 1 source interface Ethernet5
monitor session 1 source interface Ethernet6
monitor session 1 destination interface Ethernet7
end
```

Voici néanmoins la configuration que nous aurions utilisé pour copier le trafic passant par les interfaces de routage des VRF sur le switch (Ethernet5 et Ethernet6) vers l'interface connectée au wireshark (ethernet7).

V. Annexes

Configuration Arista :

```
! Command: show running-config
! device: localhost (vEOS-lab, EOS-4.31.2F)
!
! boot system flash:/vEOS-lab.swi
!
no aaa root
!
dhcp server vrf VRF_PC
   subnet 192.168.13.0/24
      range 192.168.13.50 192.168.13.70
      name POOL_PC1
      default-gateway 192.168.13.254
   !
   subnet 192.168.14.0/24
      range 192.168.14.50 192.168.14.70
      name POOL_PC2
      default-gateway 192.168.14.254
!
dhcp server vrf VRF_SERVER
   subnet 192.168.11.0/24
      range 192.168.11.50 192.168.11.70
      name POOL_SERVER1
      default-gateway 192.168.11.254
   !
   subnet 192.168.12.0/24
      range 192.168.12.50 192.168.12.70
      name POOL_SERVER2
      default-gateway 192.168.12.254
!
dhcp server
!
transceiver qsfp default-mode 4x10G
!
service routing protocols model multi-agent
!
```

```
spanning-tree mode mstp
!
system l1
   unsupported speed action error
   unsupported error-correction action error
!
vlan 11
   name SERVER1
!
vlan 12
   name SERVER2
!
vlan 13
   name PC1
!
vlan 14
   name PC2
!
vlan 15
   name ROUTAGE_SERVEURS
!
vlan 16
   name ROUTAGE_PC
!
vrf instance VRF_PC
!
vrf instance VRF_SERVER
!
interface Ethernet1
   switchport access vlan 11
!
interface Ethernet2
   switchport access vlan 12
!
interface Ethernet3
   switchport access vlan 13
!
interface Ethernet4
   switchport access vlan 14
!
interface Ethernet5
```

```
   switchport access vlan 15
!
interface Ethernet6
   switchport access vlan 16
!
interface Ethernet7
!
interface Management1
!
interface Vlan11
   vrf VRF_SERVER
   ip address 192.168.11.254/24
   dhcp server ipv4
!
interface Vlan12
   vrf VRF_SERVER
   ip address 192.168.12.254/24
   dhcp server ipv4
!
interface Vlan13
   vrf VRF_PC
   ip address 192.168.13.254/24
   dhcp server ipv4
!
interface Vlan14
   vrf VRF_PC
   ip address 192.168.14.254/24
   dhcp server ipv4
!
interface Vlan15
   vrf VRF_SERVER
   ip address 192.168.15.1/24
!
interface Vlan16
   vrf VRF_PC
   ip address 192.168.16.1/24
!
ip routing
ip routing vrf VRF_PC
ip routing vrf VRF_SERVER
!
```

```
ip route vrf VRF_PC 0.0.0.0/0 192.168.16.2
ip route vrf VRF_SERVER 0.0.0.0/0 192.168.15.2
!
router ospf 1 vrf VRF_SERVER
   router-id 1.1.1.1
   passive-interface Ethernet1
   passive-interface Ethernet2
   network 192.168.11.0/24 area 0.0.0.0
   network 192.168.12.0/24 area 0.0.0.0
   network 192.168.15.0/24 area 0.0.0.0
   max-lsa 12000
!
router ospf 2 vrf VRF_PC
   router-id 2.2.2.2
   passive-interface Ethernet3
   passive-interface Ethernet4
   network 192.168.13.0/24 area 0.0.0.0
   network 192.168.14.0/24 area 0.0.0.0
   network 192.168.16.0/24 area 0.0.0.0
   max-lsa 12000
!
end
```