LAB RÉSEAU – INTERCONNEXION DES DEUX SITES DISTANTS AVEC FORTIGATE

DOCUMENTATION TECHNIQUE

Concepteur : **Nelson Bandos**

Email : **nelson.bandos@proton.me**

Date : **Janvier 2026**

Version : **1**

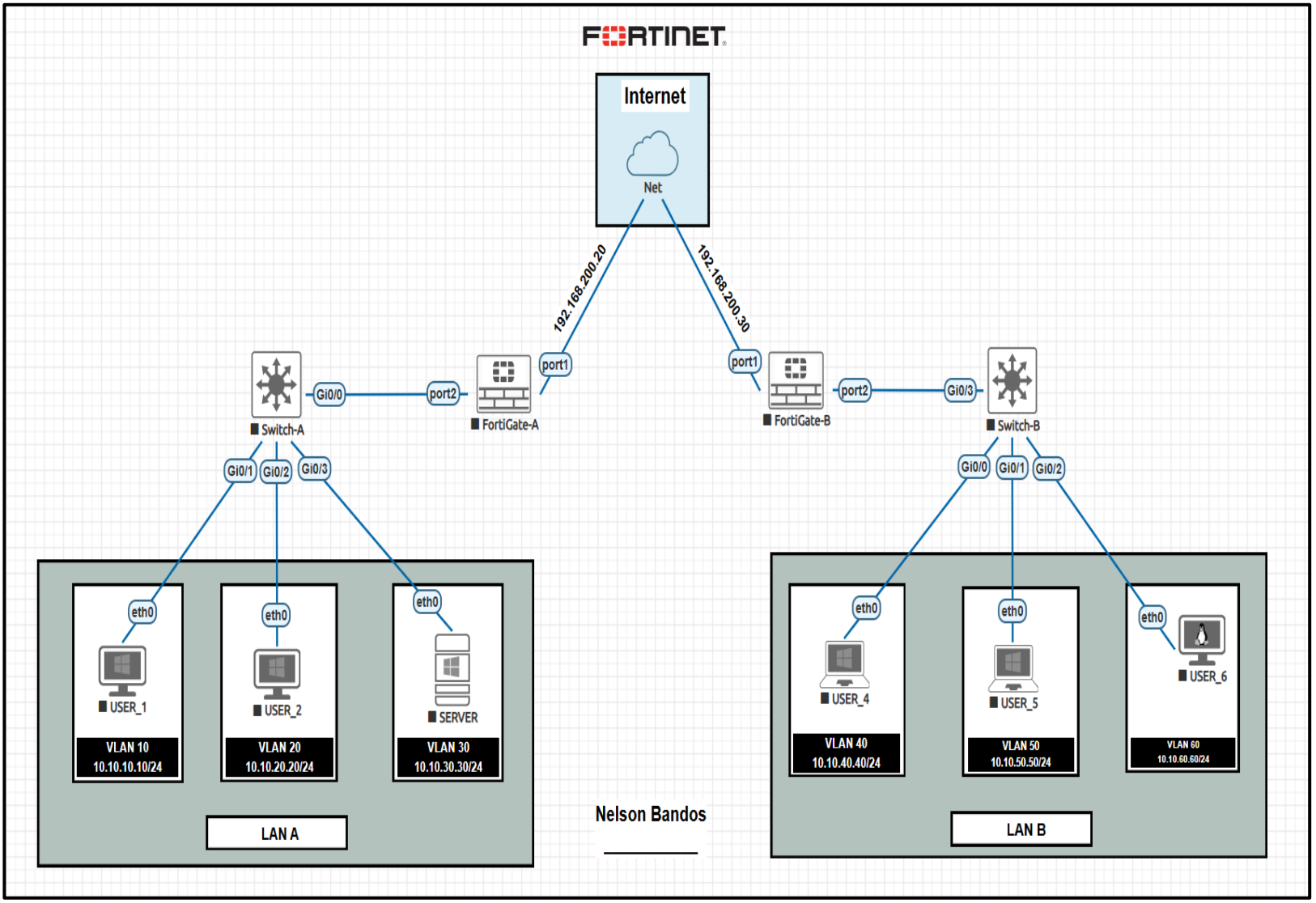

TABLE DES MATIÈRES

I. Introduction

Ce document constitue un guide technique d'implémentation pour le déploiement d'un laboratoire réseau sous EVE-NG, basé sur des pare-feux FortiGate. Il décrit de manière structurée l'architecture, les principes de conception et les choix techniques retenus afin de mettre en place une interconnexion sécurisée entre deux réseaux distants via un VPN site-to-site.

Ce guide se concentre volontairement sur la logique d'architecture, les mécanismes réseau et les bonnes pratiques. Les commandes de configuration sont volontairement exclues et sont disponibles dans le dépôt GitHub associé au projet.

1. Objectifs du projet

Les objectifs principaux de ce déploiement sont les suivants :

- Mettre en place une interconnexion sécurisée entre deux sites distants à l'aide d'un VPN site-to-site
- Permettre la communication bidirectionnelle entre plusieurs VLANs répartis sur deux réseaux distincts
- Centraliser les fonctions de routage, de sécurité et de services réseau sur les pare-feux FortiGate
- Simplifier et structurer les politiques de sécurité grâce à l'utilisation de zones logiques
- Simuler un environnement d'entreprise réaliste dans EVE-NG
- Approfondir la maîtrise des concepts FortiGate (VLAN, routage inter-VLAN, DHCP, VPN)

2. Environnement et prérequis

a. Environnement de virtualisation

- Plateforme de lab : EVE-NG
- Hyperviseur sous-jacent : selon l'infrastructure (VMware, Proxmox, etc.)

b. Équipements virtuels

- Routeur/Pare-feu : 2 × FortiGate (v7)
- Switch L2 : 2 × Switch Ethernet L2
- Hôtes de test : postes virtuels (VPCS ou machines virtuelles)

c. Compétences requises

- Notions de base en réseaux IP
- Compréhension des VLANs et du routage inter-VLAN
- Connaissances fondamentales des VPN site-to-site
- Familiarité avec l'interface FortiGate

II. Architecture globale

Le laboratoire est composé de deux réseaux géographiquement distincts :

- Réseau A
- Réseau B

Chaque réseau dispose :

- D'un pare-feu FortiGate assurant les fonctions de routage, de sécurité, de DHCP et de VPN.
- D'un switch Ethernet assurant la commutation de niveau 2
- De plusieurs hôtes finaux répartis par VLAN

Les deux pare-feux sont interconnectés via leurs interfaces WAN et établissent un tunnel VPN site-to-site de type route-based.

1. Segmentation réseau et VLAN

a. Principes généraux

Chaque site est segmenté en plusieurs VLANs afin d'isoler logiquement les flux réseau selon les rôles des utilisateurs et des services. Le lien entre le pare-feu FortiGate et le switch est configuré en mode trunk 802.1Q, permettant le transport de plusieurs VLANs sur une seule interface physique.

Le pare-feu FortiGate agit comme passerelle par défaut pour l'ensemble des VLANs et assure le routage inter-VLAN.

b. Réseau A

VLAN ID	Nom	Réseau IP	Passerelle
10	NetAdmin	10.10.10.0/24	10.10.10.254
20	SysAdmin	10.10.20.0/24	10.10.20.254
30	NetDev	10.10.30.0/24	10.10.30.254

c. Réseau B

VLAN ID	Nom	Réseau IP	Passerelle
40	Testeurs	10.10.40.0/24	10.10.40.254
50	Managers	10.10.50.0/24	10.10.50.254
60	Contributors	10.10.60.0/24	10.10.60.254

III. Segmentation logique par zones (FortiGate)

Afin d'améliorer la lisibilité et la scalabilité des politiques de sécurité, les interfaces VLAN sont regroupées au sein de zones logiques sur les pare-feux FortiGate.

2. Principe des zones

Une zone FortiGate est un regroupement logique d'interfaces partageant un même rôle fonctionnel. Les règles de sécurité sont définies entre zones plutôt qu'entre interfaces individuelles.

3. Zones mises en œuvre

- Zone LAN : regroupe l'ensemble des VLANs d'un site
- Zone WAN : regroupe l'interface connectée à Internet
- Zone VPN : regroupe l'interface du tunnel IPsec

4. Avantages

- Simplification des politiques de sécurité
- Meilleure lisibilité de l'architecture
- Facilitation des évolutions futures (micro-segmentation, nouveaux VLANs)

IV. Sécurité de niveau 2 (L2)

Les switches du laboratoire sont volontairement limités à un rôle de niveau 2. Plusieurs mécanismes de sécurité L2 sont pris en compte afin de protéger le réseau contre des attaques locales ou des erreurs de configuration.

- Les mesures de sécurité envisagées incluent :
- Limitation du nombre d'adresses MAC par port (Port Security)
- Protection contre les serveurs DHCP non autorisés (DHCP Snooping)
- Protection contre l'empoisonnement ARP (Dynamic ARP Inspection)
- Prévention des boucles accidentelles (BPDU Guard)
- Ces mécanismes permettent de renforcer la sécurité du réseau sans complexifier l'architecture.

V. Interconnexion VPN site-to-site

1. Principe général

Le VPN site-to-site permet de créer un réseau privé logique unique malgré la séparation physique des sites. Le tunnel VPN est établi entre les interfaces WAN des pare-feux FortiGate.

2. Routage et flux

Les sous-réseaux VLAN des deux sites sont transportés à travers le tunnel VPN. Le routage est assuré par les pare-feux FortiGate et aucun mécanisme de NAT n'est appliqué au trafic inter-site.

VI. Services réseau

1. DHCP

Chaque VLAN dispose de son propre pool DHCP. Les paramètres réseau (adresse IP, masque, passerelle et DNS) sont distribués automatiquement par le pare-feu FortiGate.

2. DNS

Les serveurs DNS sont définis au niveau du service DHCP. Des serveurs publics ou internes peuvent être utilisés selon les besoins.

VII. Tests et validation

Les tests réalisés permettent de valider :

- L'attribution correcte des adresses IP sur chaque VLAN
- La communication inter-VLAN au sein d'un même site
- La communication inter-site via le tunnel VPN
- L'accès à Internet pour l'ensemble des VLANs

VIII. Limites et évolutions possibles

Ce laboratoire constitue une base fonctionnelle et évolutive. Certaines fonctionnalités avancées ne sont volontairement pas implémentées à ce stade, notamment :

- Supervision SNMP centralisée
- Authentification réseau 802.1X
- Micro-segmentation avancée entre VLANs
- Ces évolutions peuvent être intégrées ultérieurement sans remise en cause de l'architecture existante.

IX. Conclusion

Cette architecture fournit une base solide pour la mise en œuvre d'un laboratoire réseau professionnel sous EVE-NG. Elle permet de simuler un environnement d'entreprise réaliste tout en restant lisible, modulaire et évolutif.