Stormshield SN710

Administration : les bases

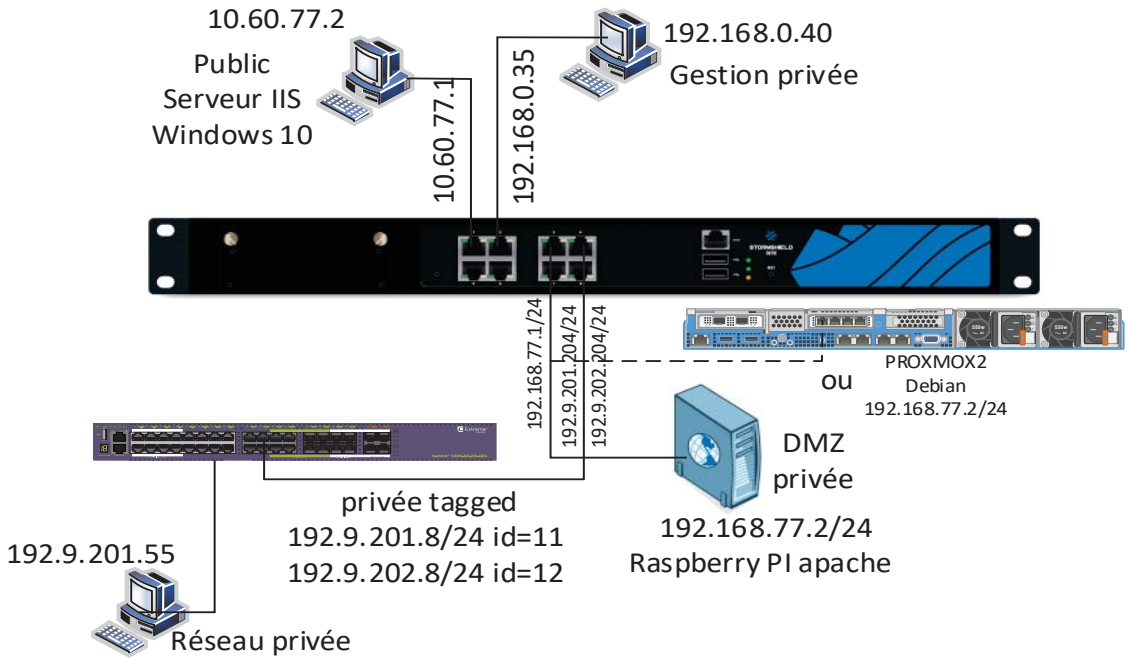


Table des matières

1 Infrastructure de la salle 4
2 Le cahier des charges 4
3 La configuration réseau 6
3.1 Les interfaces 6
3.1.1 L'interface out 6
3.1.2 L'interface DMZ1 7
3.1.3 L'interface IN 8
3.1.4 L'interface DMZ2 8
3.1.5 Test du serveur public par cli 11
3.1.6 La passerelle par défaut 11
3.2 La page d'administration 12
3.3 Les serveurs DNS 12
4 La configuration réseau du client privée d'administration 13
5 Le filtrage et le NAT sans VPN 14
5.1 Les configurations 14
5.2 Les échanges sur le NAT 17
6 Configuration de PC publique 20
7 Vérification des échanges du PC privée vers DMZ et publique 22
8 Mise en place du VPN SSL sur le SN710 pour un client publique 23
8.1 Authentification par un annuaire LDAP Microsoft AD 25
8.2 Un annuaire interne 26
8.3 La politique d'authentification 30
8.4 Les accès au VPN 31
8.5 L'activation du VPN SSL 34
8.6 Paramétrage du client VPN publique pour un annuaire externe 35
8.7 Paramétrage du client VPN publique pour un annuaire interne LDAP 40
8.8 Le filtrage et le NAT pour le VPN SSL client publique 43
9 Mise en place du VPN IPSEC sur le SN710 pour un client publique 47
9.1 Prérequis 47
9.2 Création d'un correspondant nomade 47
9.3 Création du réseau virtuel VPN IPSEC 50
9.4 La politique de chiffrement 50
9.5 L'identification 51
9.6 Les droits d'accès au VPN 53

9.7 Les règles de filtrage et NAT pour le VPN IPSEC 53
9.8 Vérification des profils de chiffrement 54
9.9 La protection applicative 54
9.10 Le client publique VPN IPSEC 55
10 La licence sur le SN710 59
11 Filtrage par URL simple par FQDN (politique de filtrage par URL définie) 60
12 La protection applicative sur stormshield 61
13 La base URL embarquée 63
13.1 Filtrage par URL avec protection applicative par sonde IPS 64
13.2 Protection applicative avec sonde IPS en TLS 67

1 Infrastructure de la salle



2 Le cahier des charges

Créez quatre interfaces :

- ✓ Un réseau publique sur out avec comme adresse publique 10.60.77.1/24
- ✓ Une gestion privée du pare feu sur le port IN avec comme adresse 192.168.0.35
- ✓ Un réseau privée avec deux VLAN taggés VLAN1 192.9.201.24/24 un VLAN2 192.9.202.24/24 sur le port4 DMZ2 (id du VLAN1 11, ide du VLAN2 12)
- ✓ Un réseau DMZ avec un serveur DMZ privé sur le port 3 DMZ1. L'interface aura comme adresse IP 192.168.77.1/24

On créera un objet

- ➢ Machine pour le serveur DMZ
- ➢ Machine pour le serveur publique qui servira de passerelle par défaut
- ➢ Machine pour le service AD et DNS en 192.9.201.7/24
- ➢ Un port pour le service web https en port 8043

La route par défaut sera la passerelle sur le domaine publique 10.60.77.1
Le service DNS sera à l'adresse IP 192.9.201.7
L'administration du pare feu sera permise sur le réseau privé VLAN2 et la gestion privée 192.168.0.40

Les règles de NAT

Le VLAN2 pourra joindre le domaine publique 10.60.77.2 (id 11) en masquerading
Le réseau publique pourra joindre le service web DMZ en utilisant la passerelle publique 10.60.77.1

Les règles de filtrage

Le réseau privée VLAN2 pourra joindre le domaine publique en http et https

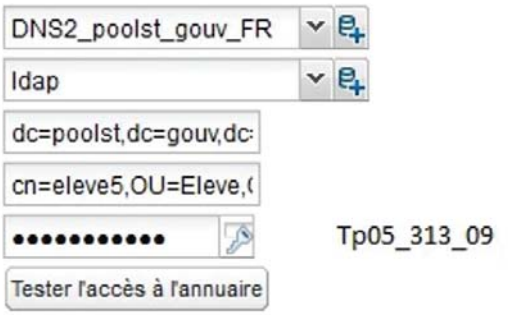
Le réseau publique via la passerelle publique 10.60.77.1 pourra joindre le service web DMZ
Le réseau privée VLAN2 pourra joindre le service web de la DMZ

Vérifiez si tous les accès sont autorisés :

Du client publique vers la DMZ en passant par le pare-feu
Du client privée du VLAN 2 vers la DMZ
Du client privée du VLAN 2 vers le client publique

Le VPN SSL

On mettra en place le VPN SSL avec une authentification par le serveur microsoft active directory. L'annuaire sera donc externe. On prendra l'eleve5 qui est disponible dans l'annuaire AD
Le pool VPN_SSL sera à l'adresse 192.168.100.0/24
Le client VPN SSL sera dans le **domaine publique**
Le serveur Microsoft active directory a comme configuration



Le client VPN pourra accéder à la DMZ mais aussi au réseau privé VLAN2. Il pourra utiliser les adresses privées car celles-ci seront chiffrées et non visibles dans le tunnel SSL vers le port out

Le VPN IPSEC

On mettra en place le VPN IPSEC IKEV1 type nomade avec une authentification par certificat. Les trois certificats autorité de certification, serveur et utilisateur eleve5 seront créés sur le firewall.

Le filtrage protocolaire

Créer une entrée DNS sur Windows server 2016

Nom de l'URL	Adresse IP	Type protocolaire
monsitepublique.poolst.gouv.fr	10.60.77.2	http
monsitedmz.poolst.gouv.fr	192.168.77.2	https

Mettre en place une politique de filtrage de blocage du client privée vers le site monsitepublique.poolst.gouv.fr en utilisant
Filtrage par URL simple par FQDN, Tester
Désactiver la politique précédente

Mettre en place une politique de filtrage de blocage du client privée vers le site monsitepublique.poolst.gouv.fr en utilisant
Un filtrage par URL avec protection applicative par sonde IPS

Mettre en place une politique de filtrage de blocage du client privée vers le site de la DMZ monsitedmz.poolst.gouv.fr
en utilisant Une protection applicative avec sonde IPS en TLS