

PROMEO FORMATION – BTS SISR

Projet Personnel Encadré 2

Sécurisation d'une architecture réseau multisite grâce à des
Firewalls StormShield

Kenan MOORE
2024-2026

PPE 2

Sécurisation d'une architecture réseau multisite grâce aux firewalls Stormshield

1. Présentation du contexte

L'entreprise **DataPlus**, PME de 50 salariés, possède deux sites :

- Un site principal situé à Beauvais (siège)
- Un site secondaire situé à Amiens

Les deux sites communiquent via Internet pour accéder aux ressources internes (serveur de fichiers, applications métiers).

Cependant, l'infrastructure actuelle ne dispose pas de solution de sécurité centralisée avancée. Les échanges intersites ne sont pas suffisamment sécurisés et les accès distants ne sont pas correctement contrôlés.

La direction souhaite donc renforcer la sécurité du réseau en s'appuyant principalement sur les fonctionnalités offertes par les firewalls **Stormshield**.

2. Problématique

Comment sécuriser efficacement une architecture réseau multisite en s'appuyant sur les fonctionnalités d'un firewall Stormshield (filtrage, NAT, VPN) ?

3. Objectifs du projet

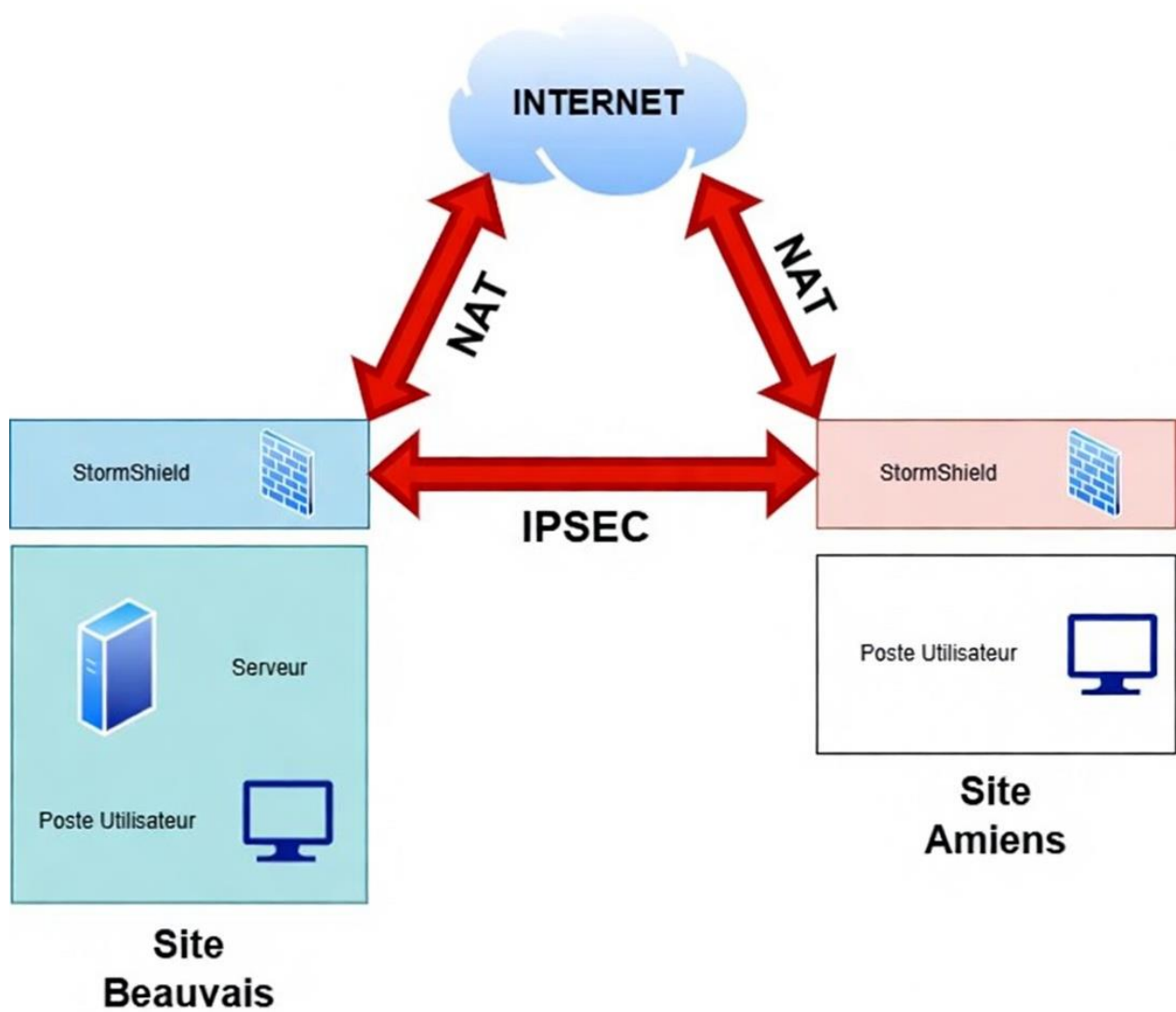
Le projet consiste à mettre en place une solution de sécurité basée sur deux firewalls Stormshield (un par site) afin de :

- Sécuriser la communication entre les deux sites via un VPN IPsec
 - Appliquer une politique de filtrage restrictive
 - Appliquer une translation NAT
-

4. Architecture mise en place

4.1 Déploiement des firewalls

Chaque site est équipé d'un firewall Stormshield :



Equipement :	IP :	Site :
StormShield	192.168.10.10/24	Beauvais
Poste Utilisateur	192.168.10.20/24	Beauvais
Serveur	192.168.10.1/24	Beauvais
StormShield	192.168.20.10/24	Amiens
Poste Utilisateur	192.168.20.20/24	Amiens

FW_Beauvais :

out		1	Ethernet, 1 Gbit/s	172.18.205.103/24
in		2	Ethernet, 1 Gbit/s	192.168.10.10/24

FW_Amiens :

out		1	Ethernet, 1 Gbit/s	172.18.205.103/24
in		2	Ethernet, 1 Gbit/s	192.168.20.10/24

4.2 Règles appliquées :

- Le réseau interne a accès à Internet en http et https
- Le réseau interne peut accéder aux serveurs internes
- Accès à Internet grâce au NAT
- Les sites pornographiques sont interdits

Règles :

Pass_Internet (contient 3 règles, de 2 à 4)							
2	on	HTTP_Pass	passer	Network_internals	Internet	http	Filtrage URL : PPE2
3	on	HTTPS_Déchiffre	déchiffrer	Network_internals	Internet	https	Filtrage SSL : PPE2
4	on	HTTPS_Pass	passer	Network_internals	Internet	https	
BlockAll (contient 1 règles, de 5 à 5)							
5	on		bloquer	Any	Any	Any	

Filtrage URL :

(0) PPE2

Editer

Fournisseur de base URL : [Base URL embarquée](#)

+ Ajouter

✕ Supprimer

↑ Monter

↓ Descendre

Couper

Copier

Coller

+ Ajouter

	État	Action	Catégorie d'URL	Commentaire
1	 on	 Bloquer	 pornography	
2	 on	 Bloquer	 compromise...	Block the URLs of Compromised URLs group
3	 off	 Passer	 authenticati...	authorize the URLs of authentication_bypass group
4	 on	 Passer	 *	any default rule (pass all)

Filtrage SSL :

(0) PPE2

Editer

Fournisseur de base URL : [Base URL embarquée](#)

+ Ajouter

✕ Supprimer

↑ Monter

↓ Descendre

✂ Couper

📄 Copier

📄 Coller

+ Ajouter tout

	État	Action	URL - CN	Commentaire
1	 on	 Bloquer sans déchiffrer	 pornography	
2	 on	 Bloquer sans déchiffrer	 compromise...	Block the URLs of Compromised URLs group
3	 on	 Passer sans déchiffrer	 proxysql_by...	don't decrypt some specific ssl servers
4	 on	 Passer sans déchiffrer	 *	default rule (decrypt all)

5. Mise en place du VPN site-to-site (IPSec)

Un tunnel VPN IPsec est configuré entre les deux firewalls Stormshield.

Caractéristiques :

- Chiffrement AES
- Authentification sécurisée
- Échange des réseaux internes nécessaires

Ce tunnel permet :

- L'accès aux ressources du siège depuis l'agence
- Une communication chiffrée entre les deux sites

VPN :

Beauvais :

État	Nom	Réseau local	Correspondant	Réseau distant	Profil de chiffrement
on	VPN_Amiens	Network_internals	Site_Amiens	LAN_Amiens	StrongEncryption

VPN (contient 1 règles, de 1 à 1)

1	on	VPN_Pass	passer	Firewall_out via Tunnel VPN IPsec	SRVAD	Any
---	----	----------	--------	-----------------------------------	-------	-----

Amiens :

État	Nom	Réseau local	Correspondant	Réseau distant	Profil de chiffrement
on	VPN_Beauvais	Network_internals	Site_FW_Beauvais	LAN_Beauvais	StrongEncryption

2	on	VPN_In	passer	SRVAD via Tunnel VPN IPsec	Network_internals	Any
3	on	VPN_Out	passer	Network_internals	SRVAD	Any

Objets créés :

PROPRIÉTÉS

Nom de l'objet: FW_Amiens

Adresse IPv4: 172.18.205.203

Adresse MAC: 01:23:45:67:89:ab (Facultatif)

Résolution: ☒ Aucune (IP statique) ☐ Automatique

Commentaire:

PROPRIÉTÉS

Nom de l'objet: SRVAD

Adresse IPv4: 192.168.10.1

Adresse MAC: 01:23:45:67:89:ab (Facultatif)

Résolution: ☒ Aucune (IP statique) ☐ Automatique

Commentaire:

PROPRIÉTÉS

Nom de l'objet: FW_Beauvais

Adresse IPv4: 172.18.205.103

Adresse MAC: 01:23:45:67:89:ab (Facultatif)

Résolution: ☒ Aucune (IP statique) ☐ Automatique

Commentaire:

Des tests ont été réalisés afin de valider le bon fonctionnement du tunnel. (Accès à l'AD)

6. NAT

Une translation NAT Dynamique a été mise en place sur les 2 StormShield comme ceci :

État	Nom	Trafic original (avant translation)			Trafic après translation		
		Source	Destination	Port dest.	Source	Port src.	Destination
on	NAT Dynamique	Network_in	Internet interface: out	Any	Firewall_out	ephemeral_fw	Any