

PROMEO FORMATION – BTS SIO SISR

Projet Personnel Encadré 2 - Netelia

Sécurisation d'une architecture réseau multisite grâce à des
Firewalls Stormshield.

Brice GAZEUX
2024-2026

Sommaire

1) Présentation du Projet

- a) Généralités et Objectif
- b) Contextualisation
- c) Contraintes

2) Étude et Conception

- a) Besoins
- b) Architecture réseau

3) Mise en œuvre de l'infrastructure

- a) Informations et organisation générale
- b) Mise en place de la DMZ
- c) Mise en place des serveurs internes
- d) Mise en place des réseaux LAN

4) Configuration pare-feu Stormshield

- a) Configuration minimale de fonctionnement
- b) Configuration Réseau
- c) Traduction d'adresses (NAT)
- d) Règles de Filtrage
- e) VPN

5) Tests et Validation

⌈!⌋ Ce document est à but d'information et de démonstration, les configurations présentées ne suivent pas les recommandations de sécurité, et ne représentent pas l'intégralité des configurations réelles pour éviter les doublons d'informations. ⌈!⌋

1) Présentation du Projet

a) Généralités et Objectif

Dans le cadre du PPE-2 du BTS SIO SISR, ce projet vise à réaliser la simulation d'une architecture réseau multisite à l'aide de firewall Stormshield. L'objectif est de concevoir la structure des différents sites, et de configurer les firewalls pour répondre aux besoins de communication et de sécurité inter-sites d'une entreprise.

Ce PPE vise à mettre en pratique des compétences acquises au cours du BTS, développer une autonomie de travail et réaliser, par une approche minimaliste, une architecture réseau sécurisée grâce à l'utilisation de firewalls Stormshield.

b) Contextualisation

L'entreprise Netelia souhaite relier trois de ses sites dans les Hauts-de-France, respectivement à Clermont, Beauvais et Amiens. Après avoir missionné plusieurs équipes pour traiter les aspects légaux, financiers et organisationnels, un pôle informatique voit le jour avec pour objectif de relier les différents sites tout en garantissant la sécurité des réseaux internes.

Pour cela une toute première maquette est créée, avec deux firewalls situés aux sites de Beauvais et Amiens.

La zone primaire d'Amiens supportera le LAN local ainsi que les serveurs internes de l'entreprise. De l'autre, le site de Beauvais disposera également de son propre LAN, et accueillera en plus une DMZ, ainsi qu'une liaison secondaire vers Clermont, un site tertiaire nécessitant des accès, mais de manière plus limitée.

c) Contraintes

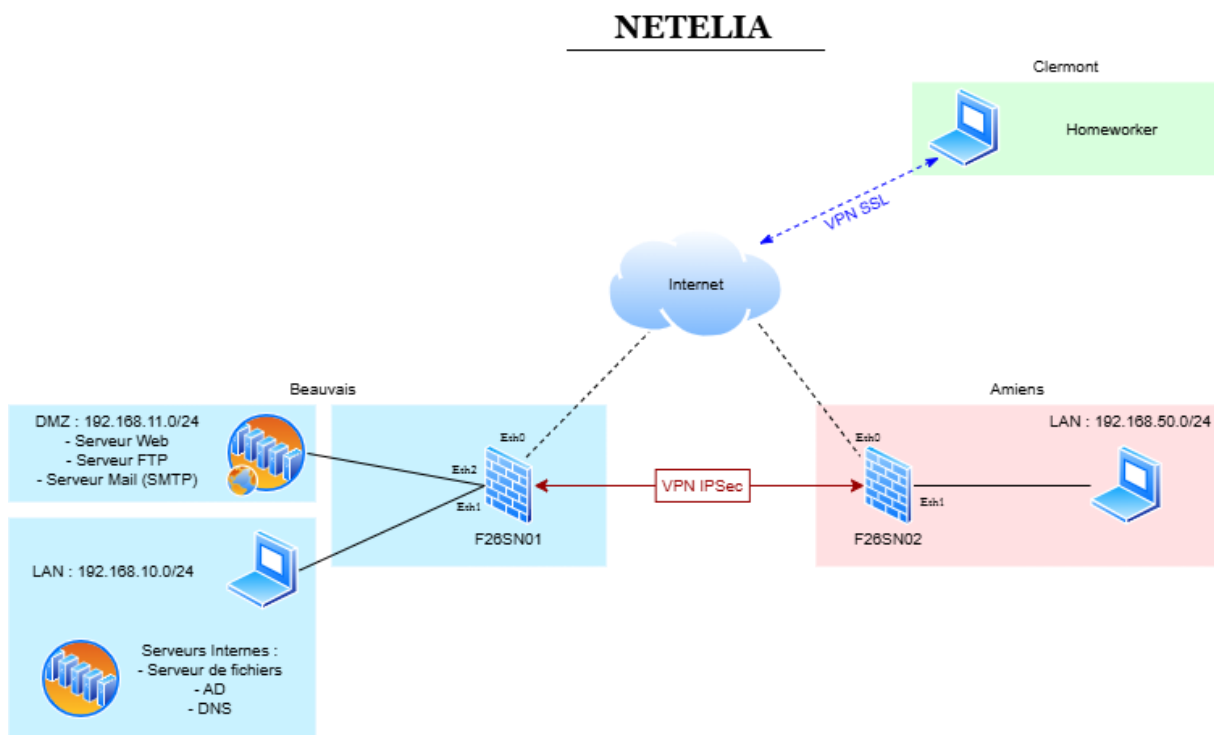
La distance entre les sites très éloignés de Beauvais et Amiens sera supporté par une liaison VPN dédiée. D'autres contraintes de la maquette concernent la mise en place d'une architecture réseau simple comprenant deux firewalls Stormshield, trois réseaux LAN, une DMZ, des serveurs internes isolés, ainsi qu'un tunnel VPN permettant d'assurer une communication sécurisée entre les différents sites.

2) Schématisation de la Situation

a) Besoins

- Plan d'adressage IP
- Deux firewall Stormshield
- Serveurs DMZ : FTP, SMTP / Serveurs Internes : Fichiers, AD, DNS
- Appareils finaux
- NAT, Filtrage, DHCP, VPN

b) Architecture réseau



3) Mise en œuvre de l'infrastructure

a) Informations et organisation générale

Tableau d'adressage :

Équipement	Port	Adresse IP	Masque de Sous Réseau	Description
F26SN01	Eth0	172.18.204.104	/24	Internet
	Eth1	192.168.10.1	/24	LAN Beauvais
	Eth2	192.168.11.1	/24	DMZ
	X	192.168.100.1	/24	VPN SSL TCP
	X	192.168.101.1	/24	VPN SSL UDP
F26SN02	Eth0	172.18.204.204	/24	Internet
	Eth1	192.168.50.1	/24	LAN Amiens
N201P0 ?	Ethernet	192.168.11.10	/24	Hyperviseur
V26DB01	Bridge	192.168.11.11	/24	Web
V26DB02	Bridge	192.168.11.12	/24	FTP
V26DB03	Bridge	192.168.11.13	/24	Mail (SMTP)
N205P04	Ethernet	192.168.10.10	/24	Hyperviseur
V26WN01	Bridge	192.168.10.11	/24	Fichiers
V26WN02	Bridge	192.168.10.12	/24	AD, DNS
N201P0?	Ethernet	DHCP	DHCP	PC
N201P0?	Ethernet	DHCP	DHCP	PC
N201P0?	Ethernet	DHCP	DHCP	PC

b) Mise en place de la DMZ

Hyperviseur : VMWare sur Windows 11 (N201P0?)

VMs - Debian 13 :

- root : P@sswOrd

- user : P@sswOrd

- VMnet10 Bridge Intel® Ethernet

VM	Adresse IP	Package Tool	Utilisation
V26DB01	192.168.11.11	Apache2	Serveur Web HTTP / TCP:80
V26DB02	192.168.11.12	vsftpd	Serveur FTP FTP / TCP:21

V26DB03	192.168.11.13	postfix	Serveur Mail SMTP / 25
---------	---------------	---------	---------------------------

Vérifications :

- Serveur Web : Moteur de recherche → 192.168.11.11 → Ouverture page web
- Serveur FTP : ftp 192.168.11.12 → Message accès ftp
- Serveur Mail : Activer telnet dans « optionalfeatures » → telnet 192.168.11.13 25 → Message accès postfix

c) Mise en place des serveurs internes

Hyperviseur : VMWare sur Windows 11 (N205P04)

VMs – Windows Serveur 2019 :

- Adminsitrateur : P@ssw0rd ou rien
- AdminPPE : P@ssw0rd
- UserPPE : P@ssw0rd
- VMnet 10 Intel® Ethernet

VM	Adresse IP	Rôles et fonctionnalités	Utilisation
V26WN01	192.168.10.11	Service de fichier > Serveur de fichier	Partage de fichiers
V26WN02	192.168.10.12	AD DS, DNS	Accès Domaine Résolution DNS

Vérifications :

- Active Directory : Joindre un poste au domaine depuis le site d'Amiens
- DNS : Résolution DNS de 192.168.11.11 en web.ppe2.local

4) Configuration pare-feu Stormshield

a) Configuration minimale de fonctionnement

Changement du nom du Firewall, de la langue du clavier et synchronisation NTP :

Configuration > Système > Configuration > Configuration Générale

Rechercher...

SYSTÈME

Configuration

Administrateurs

Licence

Maintenance

CONFIGURATION GÉNÉRALE ADMINISTRATION DU FIREWALL PARAMÈTRES RÉSEAUX

Configuration générale

Nom du firewall F26SN01-Brice

Langue du Firewall (traces) Anglais

Clavier (console) Français

Paramètres de date et d'heure - 18/03/2026 15:53:05

☐ Saisie manuelle

☐ Synchroniser avec votre machine - 18/03/2026 16:54:52

☒ Maintenir le firewall à l'heure (NTP)

Fuseau horaire Europe/Paris

LISTE DES SERVEURS NTP

+ Ajouter × Supprimer

Serveur NTP (machine ou groupe - plage d'adresses) (15 max.) Identifiant de cl...

ntp1.stormshieldcs.eu

ntp2.stormshieldcs.eu

Activation SSH :

Configuration > Système > Configuration > Configuration Générale

Accès distant par SSH

☒ Activer l'accès par SSH !

☒ Autoriser l'utilisation de mot de passe

☐ Utiliser le shell nsrpc pour les administrateurs autres que le compte admin

Port d'écoute ssh

Mise en place mot de passe sur le compte admin :

Configuration > Système > Administrateurs > Compte Admin

CONFIGURATION

Rechercher...

SYSTÈME

Configuration

Administrateurs

Licence

Maintenance

Active Update

Haute disponibilité

Management Center

Console CLI

RÉSEAU

ADMINISTRATEURS COMPTE ADMIN GESTION DES TICKETS

Authentification

Ancien mot de passe

Nouveau mot de passe

Confirmer le mot de passe

Bon

Exports

Clé privée de l'administrateur Exporter la clé privée

Clé publique du firewall Exporter la clé publique

Création des objets (exemple avec le Lan de la DMZ) :

Configuration > Objets > Réseau > +Ajouter

CRÉER UN OBJET

Machine
Nom DNS (FQDN)
Réseau
Plage d'adresses
Routeur
Groupe
Protocole IP

Nom de l'objet : Lan_DMZ

Adresses IPv4

Adresse IP de réseau : 192.168.11.0/24
Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire : DMZ site Beauvais

b) Configuration Réseau

Configuration des interfaces physiques (exemple avec l'interface out) :

Configuration > Réseau > Interfaces

bridge
dmz2
dmz3
dmz4
dmz5
dmz6
out
in
dmz1

CONFIGURATION GÉNÉRALE CONFIGURATION AVANCÉE

État : ON

Paramètres généraux

Nom : out

Commentaire :

Cette interface est : ☐ Interne (protégée) ☒ Externe (publique)

Plan d'adressage

Adressage : ☐ Plan d'adressage hérité du bridge ☒ Dynamique / Statique

Adresse IPv4 : ☐ IP dynamique (obtenue par DHCP) ☒ IP fixe (statique)

Adresse / Masque	Commentaire
172.18.205.104/24	Adresse IP Publique, sortie dans LAN Promeo N205

out
in
dmz1

1 Ethernet, 1 Gbit/s
2 Ethernet, 1 Gbit/s
3 Ethernet, 1 Gbit/s

172.18.205.104/24
192.168.10.1/24
192.168.11.1/24

DHCP sur le site de Beauvais :

Configuration > Réseau > DHCP

PLAGE D'ADRESSES

Rechercher...	+ Ajouter X Supprimer			
Plage d'adresses	Passerelle	DNS primaire	DNS secondaire	Nom de domaine
Dhcp_Lan_Beauvais	Firewall_in	VM_Srv_ADDNS_Priv	dns1.google.com	Domaine par défaut

Passerelle par défaut :

Configuration > Réseau > Routage

Configuration générale

Passerelle par défaut (routeur)

ROUTES STATIQUES

Rechercher [+ Ajouter](#) [X Supprimer](#)

Nom de l'objet	Gw_N205
Adresse IP	172.18.205.254
Commentaire	Gateway N205

c) Traduction d'adresses (NAT)

Création de NAT Statique Bimap (ftp, mail) et par port (http) pour les serveurs présents en DMZ.

NAT sur F26SN01 :

Configuration > Politique de sécurité > Filtrage et NAT > NAT

FILTRAGE NAT									
Rechercher...	+ Nouvelle règle	X Supprimer	↑	↓	↕	↕	Couper	Copier	Coller
								Chercher dans les logs	Chercher dans la s
	État	Nom	Trafic original (avant translation)			Trafic après translation			
			Source	Destination	Port dest.	Source	Port src.	Destination	Port dest.
NAT Statique (Bimap) (contient 4 règles, de 1 à 4)									
1	on	ftp_out	VM_Srv_FTP_	Any interface: out	ftp	Firewall_out			
2	on	ftp_in	Any interface: out	Firewall_out	ftp			VM_Srv_FTP_Priv	
3	on	mail_out	VM_Srv_Mail	Any interface: out	smtp smtps	Firewall_out			
4	on	mail_in	Any interface: out	Firewall_out	smtp smtps			VM_Srv_Mail_Priv	
NAT Dynamique (contient 1 règles, de 5 à 5)									
5	on	traffic_out	Network_inte	Internet interface: out	Any	Firewall_out	epheme	Any	
NAT Statique par port (contient 1 règles, de 6 à 6)									
6	on	http_in	Internet interface: out	Firewall_out	http	Any		VM_Srv_Web_Priv	

d) Règles de Filtrage

Entièrement des règles de filtrages mises en place sur le F26SN01 (y compris VPN).

FILTRAGE NAT									
Rechercher...									
	État	Nom	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
VPN IPsec Amiens (contient 1 règle, de 1 à 1)									
1	on	Amiens_to_In	passer	Lan_Amiens via Tunnel VPN IPsec	Network_internals	Any		IPS	Créé le 2026-03-20 16:20:38 par admin (192.168.10.50)
VPN SSL Homeworker (contient 2 règles, de 2 à 3)									
2	on	VPNSSL_to_In	passer	Lan_VPN_TCP Lan_VPN_UDP via Tunnel VPN SSL	Network_internals	Any		IPS	Créé le 2026-03-20 17:16:53 par admin (192.168.10.50)
3	on	VPNSSL_to_Internet	passer	Lan_VPN_TCP Lan_VPN_UDP via Tunnel VPN SSL	Internet	http https dns		IPS	Créé le 2026-03-20 17:21:26 par admin (192.168.10.50)
In to DMZ (contient 3 règles, de 4 à 6)									
4	on	in_http	passer	Network_internals	VM_Srv_Web_Priv	http		IPS	Créé le 2026-03-20 16:12:20 par admin (192.168.10.50)
5	on	in_mail	passer	Network_internals	VM_Srv_Mail_Priv	smtp smtps		IPS	Créé le 2026-03-20 16:13:19 par admin (192.168.10.50)
6	on	in_ftp	passer	Network_internals	VM_Srv_FTP_Priv	ftp		IPS	Créé le 2026-03-20 16:38:34 par admin (192.168.10.50)
Internal Servers (contient 2 règles, de 7 à 8)									
7	on	internals_to_dns	passer	Network_internals	VM_Srv_ADDNS_Priv	dns		IPS	Créé le 2026-03-20 16:37:19 par admin (192.168.10.50)
8	on	internals_to_ad	passer	Network_internals	VM_Srv_ADDNS_Priv	ldap ldaps		IPS	Créé le 2026-03-20 16:35:54 par admin (192.168.10.50)
Outgoing (contient 2 règles, de 9 à 10)									
9	on	allow_web	passer	Network_internals	Internet	http https		IPS	Créé le 2026-03-20 16:15:07 par admin (192.168.10.50)
10	on	allow_ping	passer	Network_internals	Internet	Any	icmp (requête Echo)	IPS	Créé le 2026-03-20 16:15:53 par admin (192.168.10.50)
Incoming (contient 1 règle, de 11 à 11)									
11	on	allow_internet_to_http	passer	Internet	Firewall_out	http		IPS	Créé le 2026-03-20 16:30:32 par admin (192.168.10.50)
Block ALL (contient 1 règle, de 12 à 12)									
12	on	block_all	passer	Any	Any	Any		IPS	

e) VPN

VPN site à site simple IPsec :

Configuration > VPN > VPN IPsec > Site à Site

SITE À SITE (GATEWAY-GATEWAY)				MOBILE - UTILISATEURS NOMADES	
Entrer un filtre...					
	État	Réseau local	Correspondant	Réseau distant	Profil de chiffrement
1	on	Network_internals	Site_F26SN02	Lan_Amiens	StrongEncryption

Ajout d'une règle dans le filtrage :

VPN IPsec Amiens (contient 1 règle, de 1 à 1)						
1	on	Amiens_to_In	passer	Lan_Amiens via Tunnel VPN IPsec	Network_internals	Any

VPN SSL :

Configuration > VPN > VPN SSL

VPN / VPN SSL

ON Activer le VPN SSL

PARAMÈTRES GÉNÉRAUX

VÉRIFICATION DES POSTES CLIENTS (ZTNA) (DÉSACTIVÉ)

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée 172.18.205.104

Réseaux ou machines accessibles Network_internals

Réseau assigné aux clients (UDP) Lan_VPN_UDP

Réseau assigné aux clients (TCP) Lan_VPN_TCP

Maximum de tunnels simultanés autorisés 40

Paramètres DNS envoyés au client

Nom de domaine ppe2.local

Serveur DNS primaire VM_Srv_ADDNS_Priv

Serveur DNS secondaire dns1.google.com

Créer un annuaire interne :

Configuration > Utilisateurs > Configuration des annuaires

UTILISATEURS / CONFIGURATION DES ANNUAIRES

ANNUAIRES CONFIGURÉS (5 MAXIMUM)

+ Ajouter un annuaire Action

Domain name

ppe2.local

Configuration

☒ Activer l'utilisation de l'annuaire utilisateur

Organisation ppe2

Domaine local

Identifiant cn=NetasqAdmin

Mot de passe

Confirmer

Robustesse du mot de passe

Accès au LDAP interne

☒ Activer l'accès non chiffré (PLAIN)☐ Activer l'accès en SSL

Certificat SSL présenté par le serveur Aucun certificat

Créer un utilisateur :

Configuration > Utilisateurs > Utilisateurs

UTILISATEURS / UTILISATEURS

Rechercher... Utilisateurs + Ajouter un utilisateur + Ajouter un groupe X Supprimer | Vérifier l'utilisation

Cn ↓

user@ppe2.local

user (user)

COMPTE CERTIFICAT MEMBRE DES GROUPES

Créer ou modifier le mot de passe [Droits d'accès](#)

Détails

Identifiant (login)	user
Nom	user
Prénom	
E-mail	
Téléphone	

Profil External sur le port out :

Configuration > Utilisateurs > Authentification > Portail Captif

UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES POLITIQUE D'AUTHENTIFICATION **PORTAIL CAPTIF** PROFILS DU PORTAIL CAPTIF

Portail captif

CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE

+ Ajouter X Supprimer

Interface	Profil	Méthode ou annuaire par défaut
out	External	Annuaire LDAP (ppe2.local)

Autoriser l'accès à tout le monde :

Configuration > Utilisateurs > Droits d'accès > Accès détaillé

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT **ACCÈS DÉTAILLÉ** SERVEUR PPTP

Rechercher... + Ajouter X Supprimer | Monter Descendre

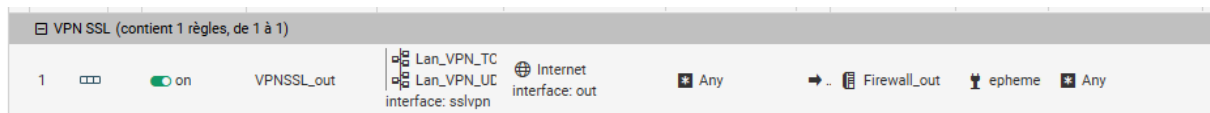
	Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage
1	Activé	Any user@ppe2.local	Interdire	Interdire	Autoriser	Interdire

Règles de filtrage :

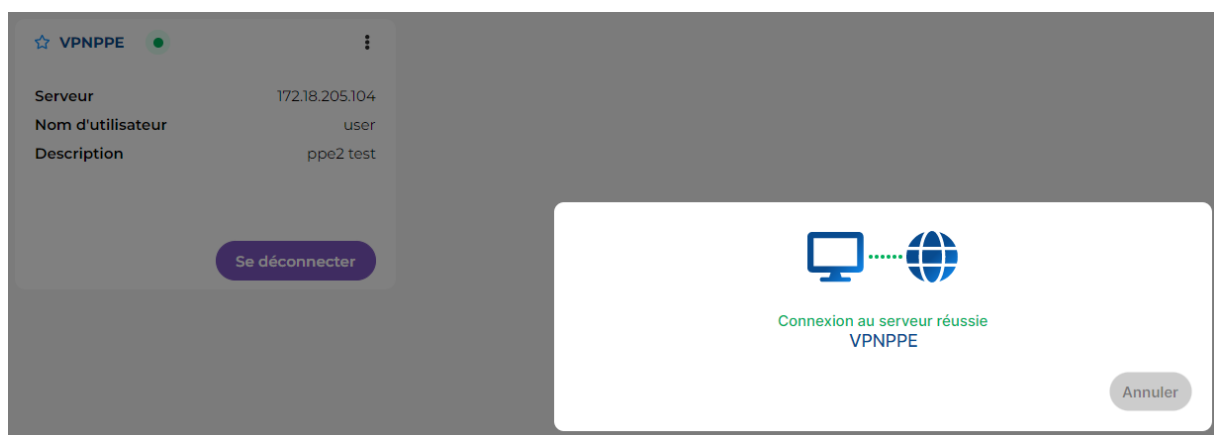
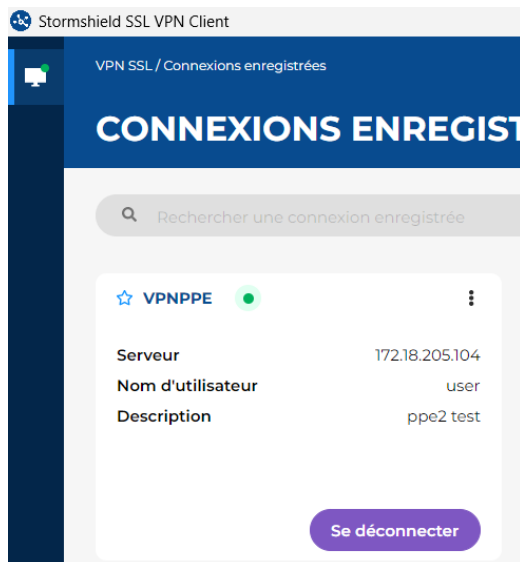
VPN SSL Homeworker (contient 2 règles, de 2 à 3)

2	on	VPNSSL_to_in	passer	Lan_VPN_TCP Lan_VPN_UDP via Tunnel VPN SSL	Network_internals	Any	IPS
3	on	VPNSSL_to_internet	passer	Lan_VPN_TCP Lan_VPN_UDP via Tunnel VPN SSL	Internet	http https dns	IPS

Règles NAT :



Utilisation de l'application « Stormshield SSL VPN Client » :



5) Tests et Validations

ICMP (Ping) :

- ✓ - Des LAN Beauvais, Amiens, VPN et DMZ vers Internet
- ✓ - Des LAN Beauvais, Amiens, VPN et DMZ entre eux

Serveurs :

- ✓ - Serveurs de la DMZ (Web, FTP et Mail) accessibles par tous
- ✓ - Serveurs internes (AD, DNS) depuis les réseaux internes

DHCP :

- ✓ - Des pare-feu pour les LAN de Beauvais, Amiens et VPN

NAT :

- ✓ - Redirection de l'interface out du pare-feu vers les serveurs en DMZ
- ✓ - NAT des réseaux internes en sortie vers internet

VPN :

- ✓ - IPSec entre les deux sites
- ✓ - SSL pour le Homeworker