

Sécurité des réseaux – ENSIBS Cybersécurité du Logiciel – 4^e année

CAHIER DE PROCÉDURES « Sécurité des réseaux »

Projet réalisé par

CHAPRON Lucas
DENOUE Enzo

Projet encadré par

CHARTON Philippe

Table des matières

I. Introduction	3
1. Contexte	3
2. Prévision de travail.....	3
II. Configuration et prise en main du réseau.....	4
1. Configuration du pare-feu et du réseau	4
2. Mise en place d'un partenariat avec VPN IPSec	5
3. Mise en place d'une connexion à l'application avec un VPN SSL	6
4. Mise en place d'un tunnel SSH.....	7
5. Mise en place d'une solution NIDS/NIPS	8
III. Conclusion.....	8
IV. Identifiants	8

Table des figures

Figure 1 : Architecture du réseau	3
Figure 2 : Réseau exemple adressage IP	4
Figure 3 : Règle LAN internet.....	5
Figure 4 : Règle DMZ internet et communication LAN/WEB	5
Figure 5 : Phases VPN IPSec	6
Figure 6 : Règles LAN IPSec	6
Figure 7 : Règles DMZ IPSec.....	6
Figure 8 : Règle IPSec.....	6
Figure 9 : Paramètres du serveur VPN SSL	7
Figure 10 : Site inaccessible à l'utilisateur sur un réseau public.....	7
Figure 11 : Connexion possible à l'application web	7

I. Introduction

1. Contexte

L'ancien administrateur réseau à démissionner de l'entreprise et le réseau de l'entreprise n'est plus opérationnel et à besoin d'une plus forte sécurisation.

L'architecture dont on dispose est la suivante :

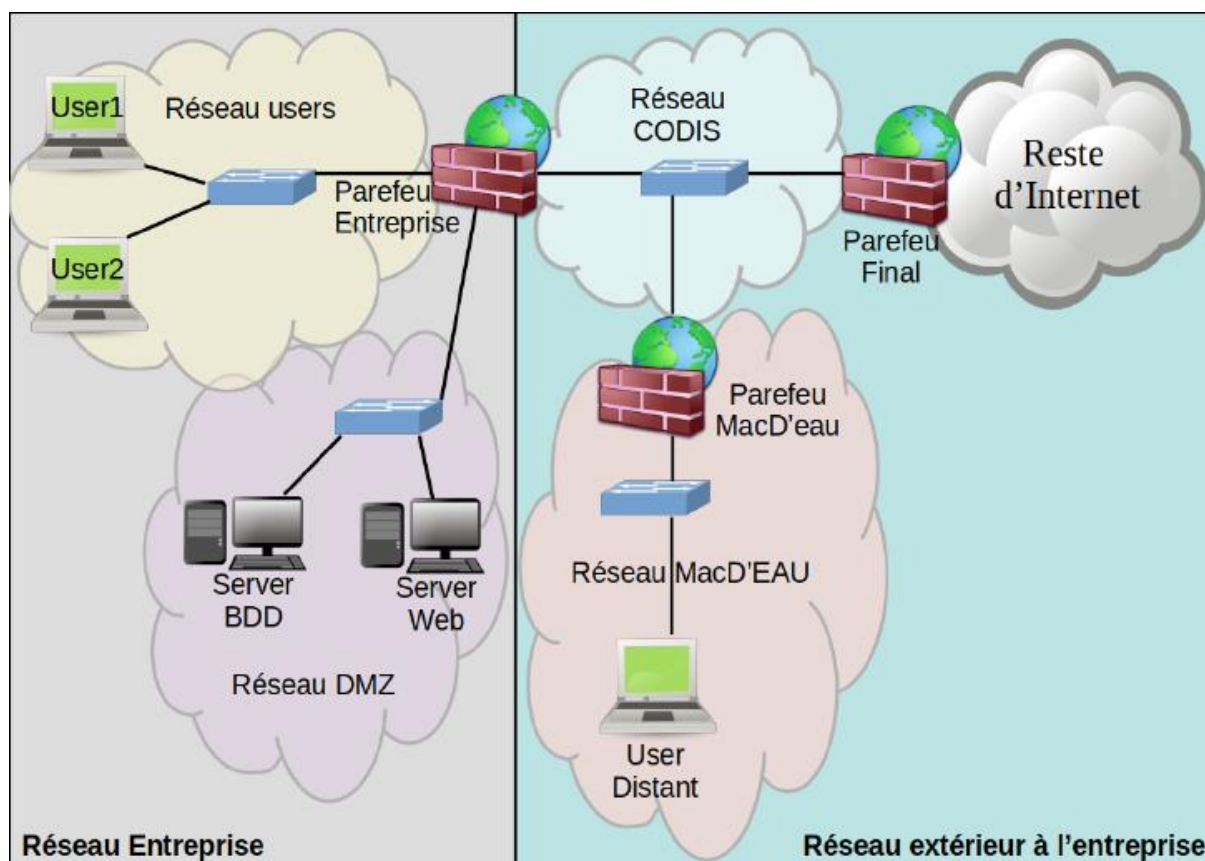


Figure 1 : Architecture du réseau

On ne peut paramétrer que les machines du réseau Entreprise.

2. Prévision de travail

Dans le cadre de notre travail dans l'entreprise, notre groupe de travail (groupe 21) composé de CHAPRON Lucas et DENOÛÉ Enzo avons pour objectif de remettre en état de marche le réseau de l'entreprise et de le sécuriser en mettant en place plusieurs solutions. Ces solutions seront : la mise en place d'un parefeu (Pfsense), la configuration des serveurs de l'entreprise, la mise en place d'un partenariat avec l'entreprise partenaire (groupe 2) avec un VPN IPSec, le déploiement d'un accès VPN SSL et SSH et la mise en place d'une solution NIDS/NIPS. **Tous les exemples présent dans le cahier de procédures ont été réalisé avec un parefeu Pfsense mais il existe de nombreux autres possibilités c'est pour cela que vous ne trouverez pas de lignes de commandes ou autres, seulement la méthode à suivre qui sera à adapter en fonction des cas.**

II. Configuration et prise en main du réseau

1. Configuration du pare-feu et du réseau

Au vu de l'architecture, il faut configurer 3 interfaces pour les 3 sous-réseaux connectés au pare-feu de l'entreprise.

- Pour ces 3 interfaces, il faut leur donner un nom et une adresse ip qui définira la plage d'adresse ip possible (utiliser un masque de sous-réseau le plus grand possible pour avoir le moins d'adresse ip possible).
- Il faut configurer le pare-feu pour qu'il puisse servir de passerelle et de serveur DNS pour les autres machines (se référer à la documentation de son pare-feu)
- Il faut maintenant définir une adresse ip à chaque machine du réseau entreprise en fonction du sous-réseau auquel elles appartiennent. On obtient alors un réseau tel que :

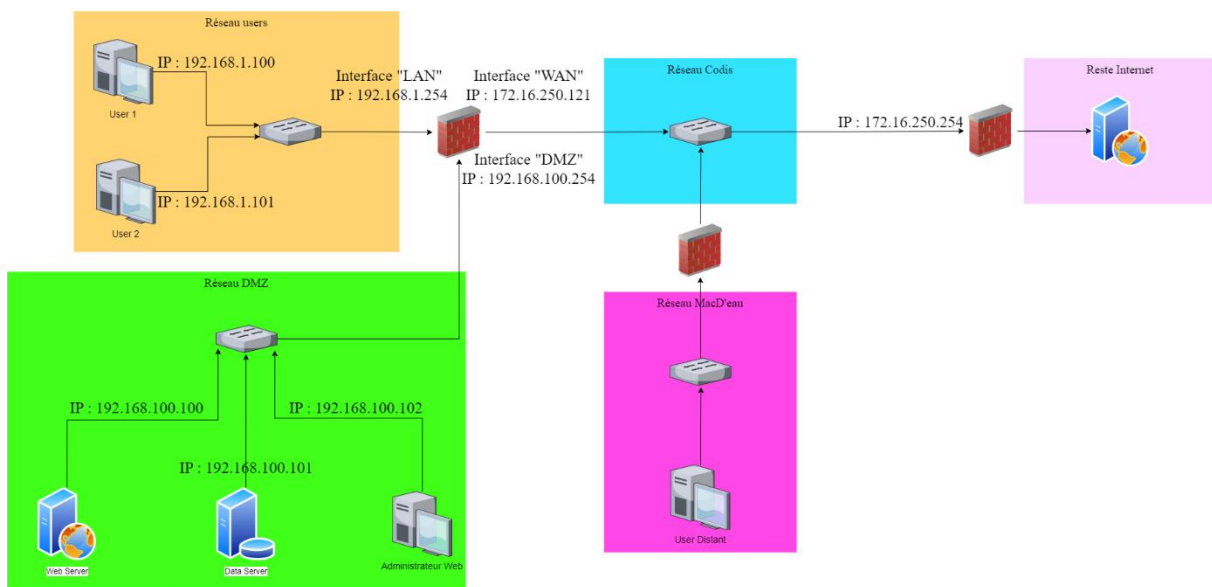


Figure 2 : Réseau exemple adressage IP

Il faut maintenant configurer les gateways des machines pour savoir où envoyer les paquets.

- Pour les 2 machines users, la gateway est l'adresse du côté de l'interface LAN du pare-feu de l'entreprise soit dans notre exemple : 192.168.1.254.
- Pour le pare-feu de l'entreprise, la gateway est l'interface « visible » du pare-feu connecter au reste d'internet ici : 172.16.250.254
- Pour les serveurs et machine du réseau DMZ, la gateway est l'interface DMZ du pare-feu de l'entreprise soit : 192.168.100.254

À présent il faut ajouter le DNS à contacter, au vu de notre architecture les adresses DNS seront les mêmes que les gateways pour nos machines.

- Pour les 2 machines users, le DNS est l'adresse du côté de l'interface LAN du pare-feu de l'entreprise soit dans notre exemple : 192.168.1.254.
- Pour le pare-feu de l'entreprise, le DNS est l'interface « visible » du pare-feu connecter au reste d'internet ici : 172.16.250.254
- Pour les serveurs et machine du réseau DMZ, le DNS est l'interface DMZ du pare-feu de l'entreprise soit : 192.168.100.254

Maintenant, sauf exception de configuration de pare-feu spécifique, vos machines ont accès à internet. Les machines ont accès à internet mais elles sont très vulnérables actuellement car le pare-feu ne bloque rien. En effet un attaquant peut communiquer avec nos machines avec n'importe quel protocole sur n'importe quel port. C'est pour cela qu'il faut configurer des règles sur le pare-feu de l'entreprise pour que ceci ne soit plus d'actualité et protéger au maximum les attaques les plus basiques.

Il est possible de configurer ces règles indépendamment sur chaque interface. On a besoin d'un accès internet (HTTP/HTTPS/DNS). Il ne faut laisser que les protocoles UDP/TCP et leurs ports associés soit le port 80,443 et 53.

Du côté de l'interface LAN, on configure les règles suivantes :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2 / 34.47 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	5 / 801.99 MiB	IPv4 TCP/UDP	LAN net	*	*	80 (HTTP)	*	none		Connexion HTTP	
<input type="checkbox"/>	9 / 112.53 MiB	IPv4 TCP/UDP	LAN net	*	*	443 (HTTPS)	*	none		Connexion HTTPS	
<input type="checkbox"/>	5 / 455 KiB	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		Connexion DNS	

Figure 3 : Règle LAN internet

Du côté de l'interface DMZ, on instaure la règle :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	1 / 65.45 MiB	IPv4 TCP/UDP	DMZ net	*	*	443 (HTTPS)	*	none		Connexion HTTPS	
<input type="checkbox"/>	0 / 3.76 MiB	IPv4 TCP/UDP	DMZ net	*	*	80 (HTTP)	*	none		Connexion HTTP	
<input type="checkbox"/>	2 / 154 KiB	IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)	*	none		Connexion DNS	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	LAN net	*	192.168.100.100	80 (HTTP)	*	none		LAN vers WEB	

Figure 4 : Règle DMZ internet et communication LAN/WEB

Dès lors vos machines ont internet et l'accès à elles sont un peu plus limités.

2. Mise en place d'un partenariat avec un VPN IPSec

Notre entreprise a vraiment besoin de communiquer avec un partenaire qui a aussi son entreprise. Afin de pouvoir partager nos services et donner un lien sécurisé à notre partenaire, il va falloir créer un lien VPN IPsec entre les deux réseaux entreprise. Il faut pour cela créer ce qu'on appelle phases. Il y en a 2. Une pour la connexion de nos machines utilisateurs au serveur web du partenaire et une pour la connexion de leurs machines utilisateurs à notre serveur web. Pour les créer, il faut se mettre d'accord sur le protocole de chiffrement utilisé ainsi qu'une clé commune. Dans l'exemple

IPsec Tunnels									
	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	Disable	1	V2	WAN	AES (256 bits)	SHA256	2 (1024 bit)	Partenariat entreprise 22	
			172.16.250.122						
	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/>	Disable	1	tunnel	DMZ	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	Entreprise22 -> Entreprise21	
<input type="checkbox"/>	Disable	2	tunnel	LAN	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	Entreprise21 -> Entreprise22	
Add P2									

Figure 5 : Phases VPN IPsec

Il faut également limiter cette porte que l'on vient d'ouvrir avec de nouvelles règles de pare-feu :

Floating

WAN

LAN

DMZ

IPsec

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 / 1.29 GiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP/UDP	LAN net	*	192.168.2.11	80 (HTTP)	*	none		Groupe21 -> Groupe22	

Figure 6 : Règles LAN IPsec

Floating

WAN

LAN

DMZ

IPsec

OpenVPN

Rules (Drag to Change Order)

States

Protocol

Source

Port

Destination

Port

Gateway

Queue

Schedule

Description

Actions

✓

0 / 0 B

IPv4

192.168.3.0/24

*

192.168.100.100

80

*

none

Groupe22 vers

Groupe21

TCP/UDP

(HTTP)

Figure 7 : Règles DMZ IPsec

Floating

WAN

LAN

DMZ

IPsec

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 TCP/UDP	192.168.3.0/24	*	DMZ net	80 (HTTP)	*	none		Groupe22 -> Groupe21	<div> <div></div> <div></div> <div></div> <div></div> </div>

Figure 8 : Règle IPsec

3. Mise en place d'une connexion à l'application avec un VPN SSL

Afin de mettre à disposition des membres de l'entreprise l'application de comptabilité, et ce où qu'ils soient (i.e. sur un réseau public par exemple), nous avons mis en place une connexion VPN SSL.

Il faut ensuite configurer le VPN SSL tel quel pour avoir une sécurisation de la connexion et des échanges (l'exemple est avec OpenVPN) :




OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 4000 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-128-GCM, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	Accès Distant OpenVPN	  

Figure 9 : Paramètres du serveur VPN SSL

Un utilisateur ne pourra pas directement se connecter au serveur web en étant sur un réseau public.

Ce site est inaccessible

http://192.168.100.100/ est inaccessible.

ERR_ADDRESS_UNREACHABLE

Figure 10 : Site inaccessible à l'utilisateur sur un réseau public

Pour palier ce problème, l'utilisateur doit démarrer une connexion avec le VPN SSL. Il peut alors entrer les identifiants connu seulement des membres de l'entreprise pour établir la connexion.

L'utilisateur peut alors accéder à l'application web en entrant l'adresse du serveur web dans la barre d'adresse.

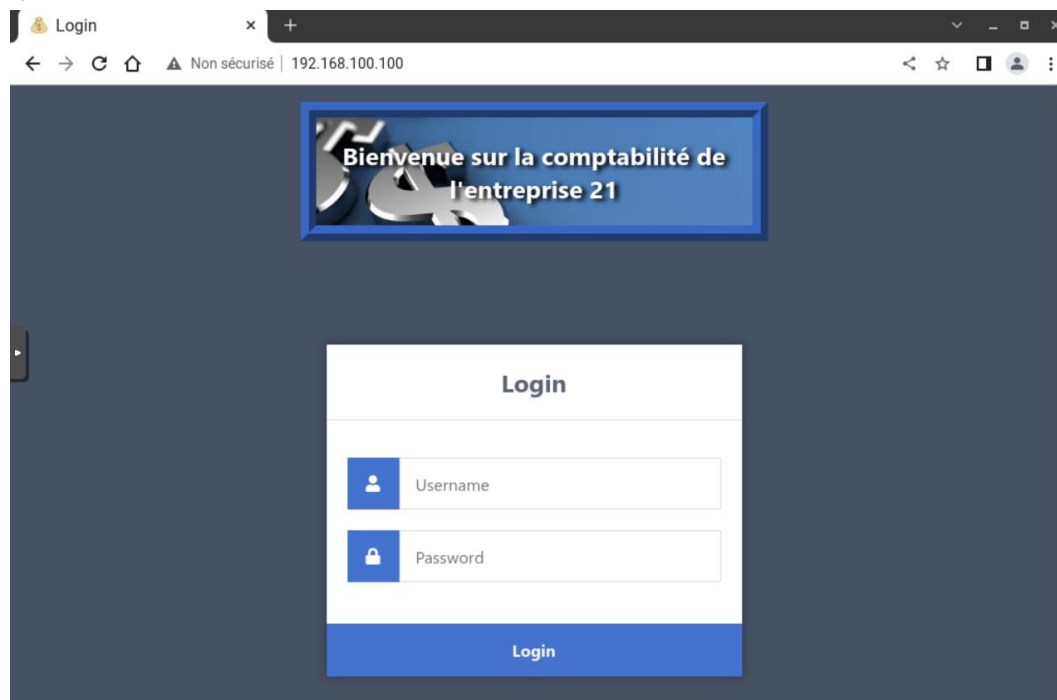


Figure 11 : Connexion possible à l'application web

4. Mise en place d'un tunnel SSH

Les administrateurs de l'entreprise ont besoin d'un accès ssh. Tout d'abord il faut générer une paire de clé pour l'authentification. Il faut mettre une passphrase pour plus de sécurité. Choisissez de préférence RSA ou ECDSA avec une longueur de clé assez conséquente 2048 bits (par exemple). On donne aux admins la clé privée et on garde la clé publique pour le pare-feu qui devra rediriger leur connexion. En supposant qu'ils ont déjà un compte spécifique pour leur connexion, il faut installer un serveur SSH aux endroits où ils doivent arriver avec leurs tunnels. Il faut également faire la redirection de port (NAT) au niveau du pare-feu pour que ce dernier sache où rediriger le tunnel. Pour plus de sécurité respectez au maximum les consignes de l'ANSII pour les mots de passes. Rajoutez une protection pour bannir les personnes qui tenteraient de bruteforce et empêchez les admins de

créer d'autre tunnel ssh que ceux qu'ils sont autorisé à faire avec permitopen au niveau de la clé publique.

5. Mise en place d'une solution NIDS/NIPS

Afin de sécuriser le réseau de l'entreprise, il est nécessaire d'analyser et filtrer les connexions car certaines peuvent être dues à des attaquants. Pour ceci il faut avoir une solution du type NIDS/NIPS qui écoute sur le réseau qui permet de lister, filtrer et stopper les connexions / tentatives de connexion douteuses. Il est installé au niveau du pare-feu car il regarde uniquement les attaques sur le réseau et non sur les machines.

III. Conclusion

Les solutions proposées ci-dessus permettent de sécuriser le réseau et les machines de l'entreprise contre certains types d'attaque peu évolués. En effet, n'ayant aucune possibilité de configuration du serveur web nous empêchent de le sécuriser contre des attaques du type escalades de privilège etc. De plus, effectuer des tests d'intrusion afin de mesurer la robustesse de la solution proposée est hautement nécessaire.

IV. Identifiants

Vous trouverez ci-après les mots de passes de nos machines :

- User1 : Lucasenzo56 !
- User2 : EnzoEsTuneFeignasse666
- Admin : m4kh4ck>4llCTFT34M
- Pfsense : pf3s3ns31sS3Cur3tk
- Mac d'eau : BURGERKING<DOMAC
- DataServer : pl34s3l3tourBDD
- WebServer : ahahahag00dluck

Pour le pare-feu, les identifiants sont :

- Username : admin
- Password : 580aEj1&p\$VuW0rdM3j

Pour le VPN SSL :

- ID : vpn.itconnect
- Password : Ensibs\$1379

Pour le compte admin du SSH :

- Login : Ronald
- Password : J41PLusd1nsp1p0url3smdP :(

Passphrase pour clé : azertyuiop