OPNSENSE

Installation - Configuration – FireWalling – DHCP - DMZ – Portail captif – NAT&Redirection – Unbound DNS – Antivitus (Clamav) - Proxy (http&https) – Certificats - VPN

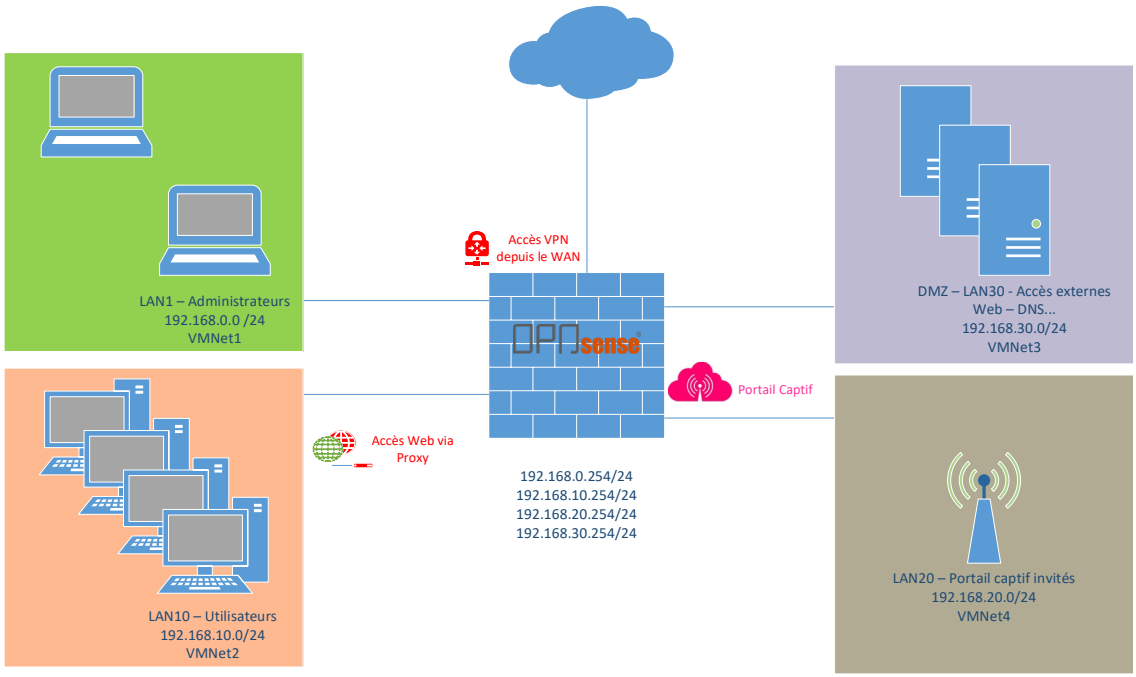
01 OCTOBRE 2023

BTS SIO

PARTIE 1 – INSTALLATION ET CONFIGURATION DE LA SOLUTION

1 PREPARATION DE LA MACHINE VIRTUELLE

SEQUENCE 1



2 PREMIER LANCEMENT A PARTIR DE L'ISO

SEQUENCE 2

3 PREINSTALLATION

SEQUENCE 3

4 AFFECTATION DES INTERFACES

SEQUENCE 4

5 CONFIGURATION DES INTERFACES

SEQUENCE 5

6 TEST DE CONFIGURATION DES INTERFACES

SEQUENCE 6

7 INSTALLATION DES VMWARE TOOLS (PILOTES OU DRIVERS DE LA MACHINE VIRTUELLE)

SEQUENCE 7

8 CONFIGURATION D'UN CLIENT ET CONNEXION A L'INTERFACE DE GESTION

SEQUENCE 8

9 L'ASSISTANT DE CONFIGURATION (WIZARD) - PREMIERE CONFIGURATION GRAPHIQUE

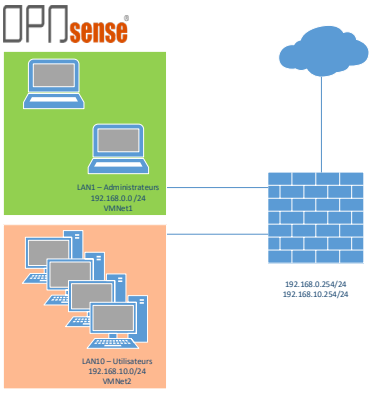
SEQUENCE 9

10 MISE A JOUR D'OPNSENSE ET SECURISATION DE L'ADMINISTRATION WEB

SEQUENCE 10

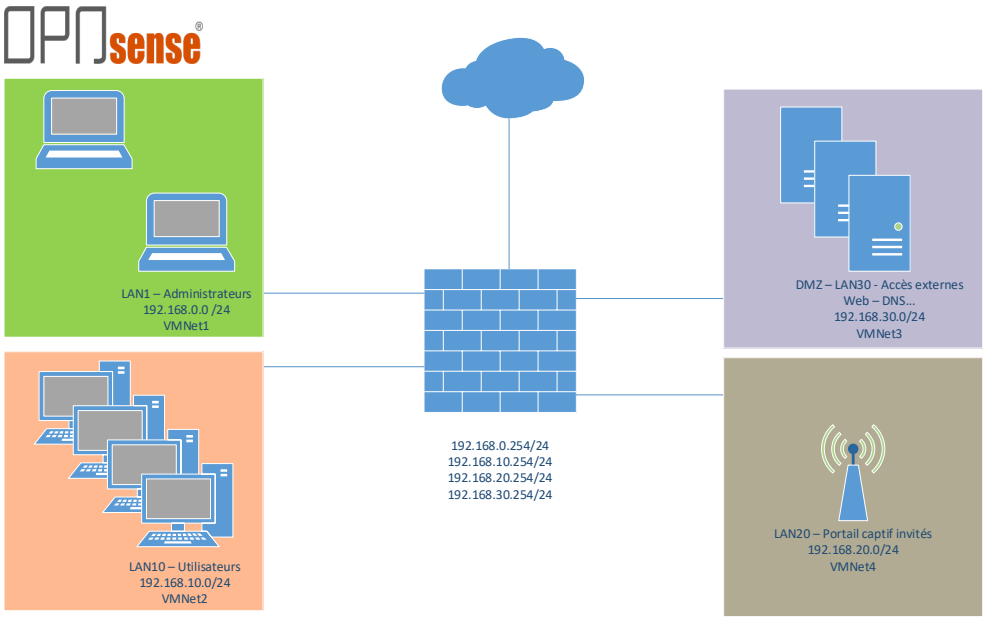
11 AJOUTER UN SEGMENT RESEAU SUPPLEMENTAIRE ET ACTIVER LE SERVICE DHCP SUR CE SEGMENT

SEQUENCE 11



12 AJOUTER PLUSIEURS SEGMENTS RESEAU (AVEC DHCP) - TEST DU ROUTAGE INTER-SEGMENTS

SEQUENCE 12



PARTIE 2 – MISE EN PLACE DES REGLES DE FIREWALLING

13 AVANT D'ALLER PLUS LOIN... SAUVEGARDER VOTRE CONFIGURATION !!!

SEQUENCE 13

14 MISE EN PLACE DE UNBOUND (PHASE 1)

SEQUENCE 14

15 LES ALIAS (OBJECTS) DE CONFIGURATION DU PAREFEU

SEQUENCE 15

16 LES REGLES DE PAREFEU : PREMIERE APPROCHE

SEQUENCE 16

Interfaces	Destination →	Admin0		DMZ30		Utilisateurs10		Invités20		VPN		WAN			Type d'accès
	Source ↓	Addr	Net	Addr	Net	Addr	Net	Addr	Net	Addr	Net	Addr	Net	Internet	
Admin0	Admin0 Net	any	any	any	any	any	any	any	any	any	any	any	any	any	Total
DMZ30	any	any	any	DNS	any	any	any	any	any	any	any	any	any	any	Mise à jour
Utilisateurs10	any	any	any	any	3128	3128	any	any	any	any	any	any	any	Via 3128	Proxy
Invités20	any	any	any	any	any	any	any	DNS	any	any	any	any	any	any	Portail captif
WAN	any	ssh	any	any	any	any	any	any	any	vpn	any	any	any	vpn	VPN & SSH

17 CONFIGURATION DES REGLES DE DNS

SEQUENCE 17

18 PORTAIL CAPTIF (APPROCHE RAPIDE)

SEQUENCE 18

19 DEMONSTRATION DE LA REDIRECTION DNS FORCEE

SEQUENCE 19

20 PROXY WEB (PHASE 1) - CONFIGURATION MINIMALE ET TEST

SEQUENCE 20

PARTIE 3 – SECURISATION DES ECHANGES DNS (UNBOUND)

21 UNBOUND COMME RESOLVEUR DNS SECURISE

SEQUENCE 21

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers

22 TEST DE LA CONFIGURATION SECURISEE

SEQUENCE 22

23 FILTRAGE AVEC UNBOUND ET REDIRECTIONS

SEQUENCE 23

Site de référence :

https://support.umbrella.com/hc/en-us/articles/115007472907-Block-Page-Bypass-or-Whitelist-Only-mode-Domains-to-Allow

https://support.umbrella.com/hc/en-us/articles/115007472907-Block-page-bypass

24 FILTRAGE AVEC UNBOUND ET REDIRECTIONS : TEST

SEQUENCE 24

PARTIE 4 – SECURISATION PAR PAREFEU

25 FILTRAGE PAR LISTES D'ALIAS

SEQUENCE 25

Sites de référence :

MALVEILLANTES

https://www.spamhaus.org/drop/drop.txt

https://www.spamhaus.org/drop/edrop.txt

https://rules.emergingthreats.net/blockrules/compromised-ips.txt

https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

RANSONWARES

- https://feodotracker.abuse.ch/downloads/ipblocklist.txt
- https://sslbl.abuse.ch/blacklist/sslipblacklist.txt

Blocage par pays :

MAXMIND (version 2024)

Configuration de MaxMind GeoIP

Créer un compte chez MaxMind :

Allez sur https://www.maxmind.com/en/geolite2/signup et créez votre compte.

Notez que l'adresse e-mail que vous fournissez sera utilisée pour vous envoyer le lien que vous devrez saisir dans OPNsense, alors assurez-vous qu'il s'agit d'un vrai compte.

Générer une clé de licence

Cliquez sur le lien « Ma clé de licence » et générez une clé.

Lorsqu'on vous demande si vous utilisez « geoipupdate », choisissez « non ».

Enregistrez l'ID de clé.

Il ne vous reste plus qu'à remplacer la partie « Ma clé de licence » du lien ci-dessous par votre clé de licence.

https://**AccountID:LicenseKey**@download.maxmind.com/geoip/databases/GeoLite2-Country-CSV/download?suffix=zip

Dans OPNsense, allez dans Pare-feu : Alias et sélectionnez l'onglet Paramètres GeoIP. Entrez l'URL que vous avez créée dans la zone URL et cliquez sur Appliquer.

PARTIE 5 - LE SERVICE PROXY (AVANCE)

SEQUENCE 30

31 PROXY - CONFIGURATION DES ACLS (ACCESS CONTROL LISTS)

SEQUENCE 31

https://www.oreilly.com/library/view/regular-expressions-cookbook/9780596802837/ch07s16.html

FILTRAGE DES ADRESSES IPV4 DANS LES URL

```
\b(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\b
```

Syntaxe OpnSense 23 : [0-9]+\.[0-9]+\.[0-9]+\.[0-9]+

FILTRAGE DES ADRESSES IPV6 DANS LES URL

```
\b(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4}\b
```

32 PROXY/PAREFEU - LE PROBLEME DU PING...

SEQUENCE 32

33 PROXY - MISE EN PLACE DES LISTES NOIRES D'URL - BLACKLISTS -

SEQUENCE 33

SITES CONTENANT DES LISTES NOIRES

~~https://dsi.ut-capitole.fr/blacklists/~~

http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz

https://urlhaus.abuse.ch/browse/

https://www.smoothwall.com/education/ (payante)

SITE DE TEST

https://www.eicar.org

34 MISE EN PLACE D'UN CLIENT VPN « ROADWARRIOR »

Les Road Warriors sont des utilisateurs distants qui ont besoin d'un accès sécurisé à l'infrastructure de l'entreprise. OPNsense utilise OpenVPN pour sa configuration SSL VPN Road Warrior et offre une intégration OTP (One Time Password) avec les tokens standard et Google Authenticator.