

# SAE 4 Cyber.01

Lecomte Jessy  
Lengrand Léo  
Lamy Edgar  
Henocq Flavien  
Marchand Flavien  
Demars Victor

<b>Configuration ip du réseau.....</b>	<b>2</b>
Côté R1 :.....	2
Côté R2 :.....	2
Schéma Draw.io.....	3
<b>Configuration des équipements réseaux :.....</b>	<b>4</b>
R1 :.....	4
R2 :.....	4
R3 (vers vlan 800):.....	5
Config SW1 :.....	6
Config SW2 (droite). ....	7
<b>Sécurisation DNS.....</b>	<b>9</b>
Configuration d'un server DNSSEC:.....	9
<b>Tunnel VPN :.....</b>	<b>11</b>
Tunnel VPN pfsense2:.....	12
Tunnel VPN pfsense1:.....	13
<b>Sécurisation d'un autre service au choix.....</b>	<b>16</b>
Dhcp sécurisé :.....	16
<b>Test de sécurité.....</b>	<b>16</b>
Nmap.....	16
Config ciscoasa.....	17
<b>Sécurisation WEB.....</b>	<b>20</b>
Site Web (NGINX).....	20
HTTPS.....	20
Nginx.....	20
En-têtes.....	21
Test de connexion.....	26
<b>Recommandations ANSSI.....</b>	<b>27</b>

Travaille a effectué :

- Sécurisation DNS (Flavien M, Edgar et Victor)
- Sécurisation WEB (Flavien M, Flavien H et Léo)
- Sécurisation d'un autre service au choix. (Flavien H, Jessy et Léo)

- Tests de sécurité. (Jessy, Edgar et Victor)
- Recommandations ANSSI (Flavien M et Léo)
- Tunnel. (Jessy et Edgar)
- Pare-Feux.
- PfSense (Victor et Flavien H)
- Ciscoasa (Flavien M)

## Configuration ip du réseau

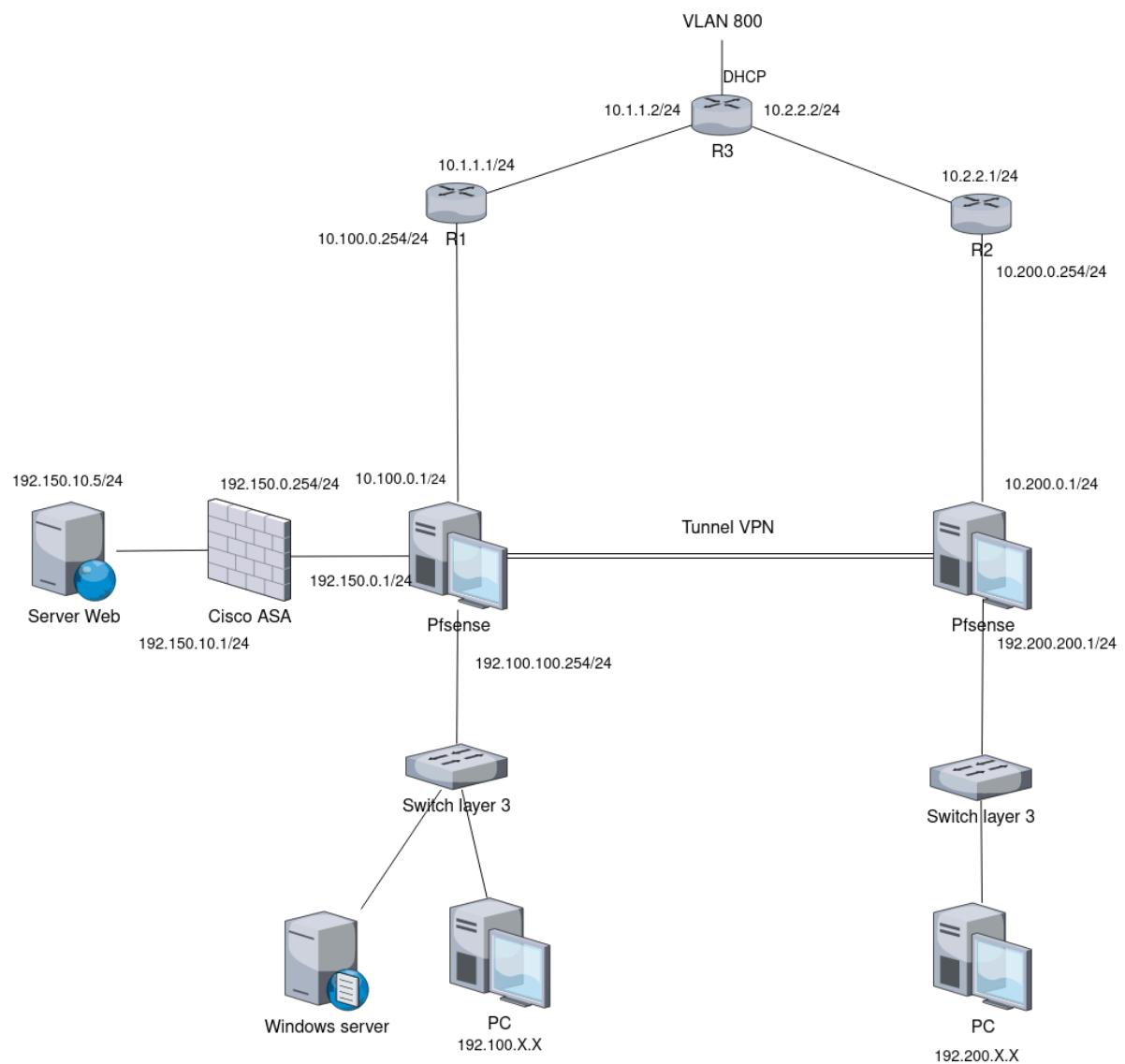
Côté R1 :

VLAN ID	Adresse réseaux	Masque de Sous-réseau	Passerelle Défaut
10 (Administration)	192.100.10.0	255.255.255.0	192.100.10.1
20 (Service)	192.100.20.0	255.255.255.0	192.100.20.1
30 (Production)	192.100.30.0	255.255.255.0	192.100.30.1
100 (Pare-feu)	192.100.100.0	255.255.255.0	192.100.100.1

Côté R2 :

VLAN ID	Adresse réseaux	Masque de Sous-réseau	Passerelle Défaut
10 (Administration)	192.200.10.0	255.255.255.0	192.200.10.1
20 (Service)	192.200.20.0	255.255.255.0	192.200.20.1
30 (Production)	192.200.30.0	255.255.255.0	192.200.30.1
100 (Pare-feu)	192.200.100.0	255.255.255.0	192.200.100.1

## Schéma Draw.io



## **Configuration des équipements réseaux :**

**R1 :**

```
hostname R1-Rome
enable secret daBsom
interface GigabitEthernet0/0
ip address 10.100.0.254 255.255.255.0
no shut

router ospf 1
redistribute static subnets
network 10.1.1.0 0.0.0.255 area 0
network 10.100.0.0 0.0.0.255 area 0

int g0/1
no shut
ip address 10.1.1.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 10.1.1.2
ip route 192.100.0.0 255.255.0.0 10.100.0.1
```

**R2 :**

```
hostname R2-Berlin
enable secret rodkuh
interface GigabitEthernet0/0
ip address 10.200.0.254 255.255.255.0
no shut
```

```
router ospf 1
 redistribute static subnets
 network 10.2.2.0 0.0.0.255 area 0
 network 10.200.0.0 0.0.0.255 area 0

int g0/2
no shut
ip address 10.2.2.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 10.2.2.2
ip route 192.200.0.0 255.255.0.0 10.200.0.1
```

### R3 (vers vlan 800):

```
hostname R3-Allemagne
enable secret bixde2
interface GigabitEthernet0/1
ip address 10.1.1.2 255.255.255.0
ip nat inside
no shut

int g0/0
no shut
ip add dhcp
ip nat outside
exit

access-list 1 permit any

interface GigabitEthernet0/2
ip address 10.2.2.2 255.255.255.0
ip nat inside
no shut

ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 10.16.0.1
```

```
router ospf 1
 redistribute connected subnets
 network 10.1.1.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.255 area 0
```

### Config SW1 :

enable secret Navfu8

*ip routing*

```
ip dhcp excluded-address 192.100.10.0 192.100.10.10
ip dhcp excluded-address 192.100.20.0 192.100.20.10
ip dhcp excluded-address 192.100.30.0 192.100.30.10
```

```
ip dhcp pool vlan10
 network 192.100.10.0 255.255.255.0
 default-router 192.100.10.1
 dns-server 192.100.10.2
```

```
ip dhcp pool vlan20
 network 192.100.20.0 255.255.255.0
 default-router 192.100.20.1
 dns-server 192.100.10.2
```

```
ip dhcp pool vlan30
 network 192.100.30.0 255.255.255.0
 default-router 192.100.30.1
 dns-server 192.100.10.2
```

```
interface range G0/1-7
 switchport mode access
 switchport access vlan 10
 no shut
```

```
interface range G0/8-15
 switchport mode access
 switchport access vlan 20
 no shut
```

```
interface range G0/16-23
```

```
switchport mode access  
switchport access vlan 30  
no shut
```

```
interface GigabitEthernet0/24  
no switchport  
ip address 192.100.100.253 255.255.255.0
```

```
interface Vlan10  
ip address 192.100.10.1 255.255.255.0
```

```
interface Vlan20  
ip address 192.100.20.1 255.255.255.0
```

```
interface Vlan30  
ip address 192.100.30.1 255.255.255.0
```

```
router ospf 1  
network 192.100.0.0 0.0.255.255 area 0  
exit  
ip route 0.0.0.0 0.0.0.0 192.100.100.254
```

```
ip dhcp snooping vlan 10-30  
int range g0/1-23  
ip dhcp snooping trust
```

## Config SW2 (droite)

```
enable secret xomsij  
ip dhcp excluded-address 192.200.10.0 192.200.10.10  
ip dhcp excluded-address 192.200.20.0 192.200.20.10  
ip dhcp excluded-address 192.200.30.0 192.200.30.10
```

```
ip dhcp pool vlan10  
network 192.200.10.0 255.255.255.0  
default-router 192.200.10.1  
dns-server 192.100.10.2
```

```
ip dhcp pool vlan20  
network 192.200.20.0 255.255.255.0
```

```
default-router 192.200.20.1
```

```
dns-server 192.100.10.2
```

```
ip dhcp pool vlan30
```

```
network 192.200.30.0 255.255.255.0
```

```
default-router 192.200.30.1
```

```
dns-server 192.100.10.2
```

```
ip routing
```

```
interface range G0/1-7
```

```
switchport mode access
```

```
switchport access vlan 10
```

```
no shut
```

```
interface range G0/8-15
```

```
switchport mode access
```

```
switchport access vlan 20
```

```
no shut
```

```
interface range G0/16-23
```

```
switchport mode access
```

```
switchport access vlan 30
```

```
no shut
```

```
interface G0/24
```

```
no switchport
```

```
ip address 192.200.200.253 255.255.255.0
```

```
interface Vlan10
```

```
ip address 192.200.10.1 255.255.255.0
```

```
interface Vlan20
```

```
ip address 192.200.20.1 255.255.255.0
```

```
interface Vlan30
```

```
ip address 192.200.30.1 255.255.255.0
```

```
router ospf 1
```

```
network 192.200.0.0 0.0.255.255 area 0
```

```
exit
```

```
ip route 0.0.0.0 0.0.0.0 192.200.200.1
```

```
ip dhcp snooping vlan 10-30
```

```
int range g0/1-23
```

ip dhcp snooping trust

Nous ajoutons des mots de passe sur chaque équipement. Les mot de passe sont complexes et chiffrés

mdp pfSense (10.100.0.1) : nexhYc-xihnyt

mdp pfSense (10.200.0.1) : gaccuh-godgek1

mdp windows server : zytkop-zubzyn-4Tunmu

mdp compte secrétaire : gewhyr-sicro6

## Sécurisation DNS

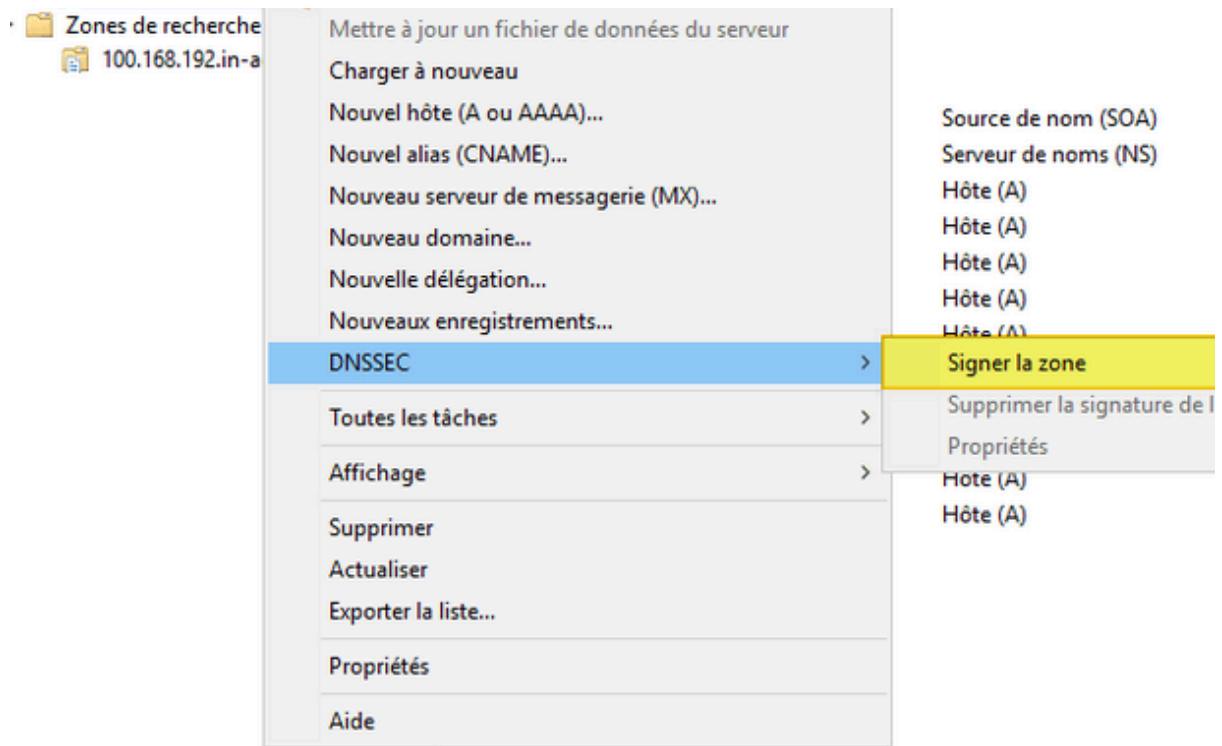
### Configuration d'un serveur DNSSEC:

Vérifier si le DNSSEC est bien actif:

PowerShell: (Get-DnsServerSetting).EnableDnsSec

```
Selection Administrateur : Windows PowerShell
PS C:\> (Get-DnsServerSetting).EnableDnsSec
True
PS C:\>
```

Depuis Windows Server 2016, le DNSSEC est activé par défaut, cependant il faut signer la zone:



Une fois les zones signées, voici notre zone de recherche directe DNSSEC:

Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[22], srv-societe1.dom-so...	statique
(identique au dossier parent)	Serveur de noms (NS)	srv-societe1.dom-societe1...	statique
(identique au dossier parent)	Hôte (A)	192.168.10.2	16/02/2024 13:00:00
(identique au dossier parent)	RR Signature (RRSIG)	[NSEC3PARAM][Inception(UTC);...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[DNSKEY][Inception(UTC);...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[A][Inception(UTC); 16/02...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[NS][Inception(UTC); 16/0...	statique
(identique au dossier parent)	RR Signature (RRSIG)	[SOA][Inception(UTC); 16/...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[257][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[257][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	DNS KEY (DNSKEY)	[256][DNSSEC][RSA/SHA-...	statique
(identique au dossier parent)	Next Secure 3 Parameter...	[SHA-1][0][50][C6C7413F8...	statique
12at2p3vcadlcnoal4u60ksl9...	RR Signature (RRSIG)	[NSEC3][Inception(UTC); 1...	statique
12at2p3vcadlcnoal4u60ksl9...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50]...	statique
26evgfnoteher605j3phq9fac...	RR Signature (RRSIG)	[NSEC3][Inception(UTC); 1...	statique
26evgfnoteher605j3phq9fac...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50]...	statique
2ufu8gtfh77cip6696v50vb7...	RR Signature (RRSIG)	[NSEC3][Inception(UTC); 1...	statique
2ufu8gtfh77cip6696v50vb7...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50]...	statique
4s7910gg8i531cf61mbkp4...	RR Signature (RRSIG)	[NSEC3][Inception(UTC); 1...	statique
4s7910gg8i531cf61mbkp4...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50]...	statique
58f8vfb1oc479u77b3c1oen2...	RR Signature (RRSIG)	[NSEC3][Inception(UTC); 1...	statique
58f8vfb1oc479u77b3c1oen2...	Next Secure 3 (NSEC3)	[SHA-1][NO Opt-Out][50]...	statique
60pqgjiik4t4q2bllh6hrb3jh...	RR Signature (RRSIG)	[NSEC3][Inception(UTC); 1...	statique

Une fois la configuration du DNSSEC terminée, voici comment vérifier la signature en utilisant la commande powershell suivante sur le serveur et le client:

Resolve-DnsName -Name srv-apps.it-connect.local -DnssecOk

```
C:\Users\admin> Resolve-DnsName -Name srv-societe1.dom-societe1.lan -DnssecOk
Name   Type    TTL   Section  IPAddress
-----  ---  ----  ---  -----
srv-societe1.dom-societe1.lan  A      3600  Answer   192.168.10.2

Name   Type    TTL   Section  IPAddress
-----  ---  ----  ---  -----
srv-societe1.dom-societe1.lan  AAAA  1200  Question  fe80::b43:e7b1:d884:5ea6
srv-societe1.dom-societe1.lan  A      1200  Question  192.168.10.2
```

Nous voyons que l'échange entre le serveur DNSSEC et le client se fait par le biais d'une signature DNSSEC

## Tunnel VPN :

**Custom Filter Options**

**Hint** All input is **space-separated**. When selecting a match that specifies "OR", at least two Types should be specified (such as Ethertype and Port). This will capture packets that match either Type instead of exclusively both.

**Untagged Filter** Filter options for packets without any VLAN tags.

include any of	UNTAGGED PACKETS		
all of	EXAMPLE: 10.1.1.0/24 192.168.1.1		
HOST IP ADDRESS OR SUBNET			
[IPsec]	EXAMPLE: 17 tcp	all of	EXAMPLE: 80 443
PROTOCOL		PORT NUMBER	
		ETHERTYPE	

**Tagged Filter** Filter options for packets that have a VLAN tag set. Specify a tag level to match stacked VLAN packets (such as QinQ).

exclude all	VLAN TAG	any of	EXAMPLE: 100 200	1
TAGGED PACKETS		HOST MAC ADDRESS		LEVEL
all of	EXAMPLE: 10.1.1.0/24 192.168.1.1	all of	EXAMPLE: 00:02 11:22:33:44:55:66	
HOST IP ADDRESS OR SUBNET		HOST MAC ADDRESS		
any of	EXAMPLE: 17 tcp	any of	EXAMPLE: arp 8100 0x8200	
PROTOCOL		PORT NUMBER		
		ETHERTYPE		

**Stop**

Running packet capture:  
`/usr/sbin/tcpdump -ni em0 -c 1000 -U -w -'((esp or (udp port 4500 and udp[8:4]!={})) and ((not vlan))'`

**Packet Capture Output: /tmp/packetcapture-em0-20240326095030.pcap**  Auto-scroll

```

09:51:28.690883 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x51), length 120
09:51:28.704579 IP 10.100.0.1 > 10.200.0.1: ESP(spi=0xcd232760,seq=0x22), length 120
09:51:29.415547 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x52), length 96
09:51:29.699334 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x53), length 120
09:51:29.705087 IP 10.100.0.1 > 10.200.0.1: ESP(spi=0xcd232760,seq=0x23), length 120
09:51:30.700824 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x54), length 120
09:51:30.706493 IP 10.100.0.1 > 10.200.0.1: ESP(spi=0xcd232760,seq=0x24), length 120
09:51:31.434283 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x55), length 96
09:51:31.701509 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x56), length 120
09:51:31.706113 IP 10.100.0.1 > 10.200.0.1: ESP(spi=0xcd232760,seq=0x25), length 120
09:51:35.492692 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x57), length 96
09:51:38.638959 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x58), length 104
09:51:38.638993 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x59), length 96
09:51:38.639019 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x5a), length 104
09:51:38.639043 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x5b), length 96
09:51:43.886085 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x5c), length 96
09:51:43.886123 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x5d), length 104
09:51:43.886393 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x5e), length 100
09:51:44.899863 IP 10.200.0.1 > 10.100.0.1: ESP(spi=0xc244c837,seq=0x5f), length 96

```

La commande `tcpdump` nous permet d'observer les communications passant par le tunnel VPN

```

R3-Allemagne(config-router)#do debug ip nat
IP NAT debugging is on
R3-Allemagne(config-router)#exit
R3-Allemagne(config)#
*Mar 26 16:14:53.903: NAT*: s=10.2.2.1->10.16.18.51, d=8.8.8.8 [10]
*Mar 26 16:14:55.899: NAT*: s=10.2.2.1->10.16.18.51, d=8.8.8.8 [11]
*Mar 26 16:14:57.899: NAT*: s=10.2.2.1->10.16.18.51, d=8.8.8.8 [12]
*Mar 26 16:14:59.899: NAT*: s=10.2.2.1->10.16.18.51, d=8.8.8.8 [13]
*Mar 26 16:15:01.899: NAT*: s=10.2.2.1->10.16.18.51, d=8.8.8.8 [14]

```

## Tunnel VPN pfSense2:

Tunnels IPsec										
	ID	IKE	Passerelle distante		Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
	1	Disable	V2	WAN 10.100.0.1		AES (128 bits)	SHA256	14 (2048 bit)	VPN to 10.100.0.1	
	ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description	Actions P2	
	1	Disable	tunnel	192.200.0.0/16	192.100.0.0/16	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	LAN PfSense2	
	2	Disable	tunnel	192.200.0.0/16	192.150.0.0/24	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	VPN to DMZ	
			Ajouter P2							

État IPsec							
ID	Description	Local	Distant	Rôle	Chrono	Algo	État
con1 #1	VPN to 10.100.0.1	ID: 10.200.0.1  Host: 10.200.0.1:500 SPI: fa1f0450746e09aa	ID: 10.100.0.1 Host: 10.100.0.1:500 SPI: ada37b51ade0331f	IKEv2 Initiator	Rekey: 24167s (06:42:47) Reauth: Désactivé	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established Il y a 82 secondes (00:01:22)
ID	Description	Local	SPI(s)	Distant	Temps	Algo	Statistiques
con1: #4	Multiple	192.200.0.0/16	Local: c1e22b7e Distant: cc105f46	192.100.0.0/16 192.150.0.0/24	Rekey: 2834s (00:47:14) Life: 3518s (00:58:38) Install: 82s (00:01:22)	AES_GCM_16 (128) IPComp: Aucun	Octets entrants: 0 (0 B) Paquets entrants: 0 Octets sortants: 9,060 (9 KiB) Paquets sortants: 75

Routes IPv4						
Destination	Passerelle	Drapeaux	Uses	MTU	Interface	Expire
default	10.200.0.254	UGS	7	1500	em0	
10.100.0.1	10.200.0.254	UGHS	6	1500	em0	
10.200.0.0/24	link#1	U	1	1500	em0	
10.200.0.1	link#5	UHS	3	16384	lo0	
127.0.0.1	link#5	UH	2	16384	lo0	
192.100.10.2	10.200.0.254	UGHS	6	1500	em0	
192.200.10.0/24	192.200.200.253	UGS	8	1500	em1	
192.200.20.0/24	192.200.200.253	UGS	8	1500	em1	
192.200.30.0/24	192.200.200.253	UGS	8	1500	em1	
192.200.200.0/24	link#2	U	4	1500	em1	
192.200.200.1	link#5	UHS	5	16384	lo0	

## Tunnel VPN pfSense1:

État IPsec																																			
ID	Description	Local	Distant	Rôle	Chrono	Algo	État																												
con1 #4		ID: 10.100.0.1 Host: 10.100.0.1:500 SPI: 818de014a31038cb	ID: 10.200.0.1 Host: 10.200.0.1:500 SPI: f819c28f1028d22a	IKEv2 Initiator	Rekey: 23044s (06:24:04) Reauth: Désactivé	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established Il y a 301 secondes (00:05:01)																												
Show child SA entries (3 Connected)																																			
Tunnels IPsec																																			
ID	IKE	Passerelle distante	Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions																											
1	V2	WAN 10.200.0.1		AES (128 bits)	SHA256	14 (2048 bit)																													
<table border="1"> <thead> <tr> <th>ID</th><th>Mode</th><th>Sous-réseau local</th><th>Sous-réseau distant</th><th>Protocole P2</th><th>Transformations P2</th><th>Méthodes d'authentification P2</th><th>Description P2</th><th>Actions P2</th></tr> </thead> <tbody> <tr> <td>  1</td><td>tunnel</td><td>192.100.0.0/16</td><td>192.200.0.0/16</td><td>ESP</td><td>AES (128 bits), AES128-GCM (128 bits)</td><td>SHA256</td><td></td><td> </td></tr> <tr> <td>  2</td><td>tunnel</td><td>OPT1</td><td>192.200.0.0/16</td><td>ESP</td><td>AES (128 bits), AES128-GCM (128 bits)</td><td>SHA256</td><td></td><td> </td></tr> </tbody> </table>									ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description P2	Actions P2	1	tunnel	192.100.0.0/16	192.200.0.0/16	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256			2	tunnel	OPT1	192.200.0.0/16	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256		
ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description P2	Actions P2																											
1	tunnel	192.100.0.0/16	192.200.0.0/16	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256																													
2	tunnel	OPT1	192.200.0.0/16	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256																													
Ajouter P2																																			

## Diagnostics / Packet Capture

?

Packet Capture Options		
Capture Options	IPsec (enc0)	Everything
	Interface to capture packets on.	Filter preset.
Max number of packets to capture (default 1000).	1000	0
	Max bytes per packet (default 0). Enter 0 (zero) for no limit.	<input checked="" type="checkbox"/> Promiscuous Mode
		Capture all traffic seen by the interface. Disable this option to only capture traffic to and from the interface, including broadcast and multicast traffic.
View Options	Normal	<input type="checkbox"/> Name Lookup
	The level of detail shown when viewing the packet capture.	Perform a name lookup for port, host, and MAC addresses when viewing the packet capture. This can cause significant delays due to reverse DNS lookups.
Last capture start	March 26th, 2024 10:56:21 am.	
Last capture stop	March 26th, 2024 10:56:40 am.	
<input type="button" value="Start"/> <input type="button" value="View"/> <input type="button" value="Download"/> <input type="button" value="Clear Captures"/>		

### Packet Capture Output: /tmp/packetcapture-enc0-20240326105621.pcap

```

10:56:23.263540 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.56924 > 192.100.10.2.53: tcp 0
10:56:24.265339 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12 > 192.100.10.11: ICMP echo request, id 13, seq 1, length 64
10:56:24.271359 (authentic,confidential): SPI 0xc4d915f2: IP 192.100.10.12 > 192.200.10.12: ICMP echo reply, id 13, seq 1, length 64
10:56:25.266044 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.10.12 > 192.100.10.11: ICMP echo request, id 13, seq 2, length 64
10:56:25.273279 (authentic,confidential): SPI 0xc4d915f2: IP 192.100.10.12 > 192.200.10.12: ICMP echo reply, id 13, seq 2, length 64
10:56:26.266668 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12 > 192.100.10.11: ICMP echo request, id 13, seq 3, length 64
10:56:26.271257 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.46270 > 192.100.10.2.53: UDP, length 42
10:56:26.271359 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.41149 > 192.100.10.2.53: UDP, length 48
10:56:26.271414 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.37976 > 192.100.10.2.53: UDP, length 42
10:56:26.271491 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.51815 > 192.100.10.2.53: UDP, length 46
10:56:26.271559 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.10.12.58963 > 192.100.10.2.53: UDP, length 34
10:56:26.271669 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.59832 > 192.100.10.2.53: UDP, length 48
10:56:26.271713 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.52785 > 192.100.10.2.53: UDP, length 34
10:56:26.271762 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12.57161 > 192.100.10.2.53: UDP, length 46
10:56:26.272239 (authentic,confidential): SPI 0xc4d915f2: IP 192.100.10.11 > 192.200.10.12: ICMP echo reply, id 13, seq 3, length 64
10:56:27.267446 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12 > 192.100.10.11: ICMP echo request, id 13, seq 4, length 64
10:56:27.272995 (authentic,confidential): SPI 0xc4d915f2: IP 192.100.10.11 > 192.200.10.12: ICMP echo reply, id 13, seq 4, length 64
10:56:28.267795 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12 > 192.100.10.11: ICMP echo request, id 13, seq 5, length 64
10:56:28.274385 (authentic,confidential): SPI 0xc4d915f2: IP 192.100.10.11 > 192.200.10.12: ICMP echo reply, id 13, seq 5, length 64
10:56:29.269037 (authentic,confidential): SPI 0xcc27b3c1: IP 192.200.18.12 > 192.100.10.11: ICMP echo request, id 13, seq 6, length 64

```

## Routes IPv4

Destination	Passerelle	Drapeaux	Uses	MTU	Interface	Expire
default	10.200.0.254	UGS	7	1500	em0	
10.100.0.1	10.200.0.254	UGHS	6	1500	em0	
10.200.0.0/24	link#1	U	1	1500	em0	
10.200.0.1	link#5	UHS	3	16384	lo0	
127.0.0.1	link#5	UH	2	16384	lo0	
192.100.10.2	10.200.0.254	UGHS	6	1500	em0	
192.200.10.0/24	192.200.200.253	UGS	8	1500	em1	
192.200.20.0/24	192.200.200.253	UGS	8	1500	em1	
192.200.30.0/24	192.200.200.253	UGS	8	1500	em1	
192.200.200.0/24	link#2	U	4	1500	em1	
192.200.200.1	link#5	UHS	5	16384	lo0	

**pfSense COMMUNITY EDITION**

**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

## Diagnostics / Packet Capture

### Packet Capture Options

Capture Options	IPsec (enc0)	Custom Filter
Interface to capture packets on.		
Max number of packets to capture (default 1000). Enter 0 (zero) for no limit.	Max bytes per packet (default 0). Enter 0 (zero) for no limit.	<input checked="" type="checkbox"/> Promiscuous Mode
The level of detail shown when viewing the packet capture.		<input type="checkbox"/> Name Lookup
Force the captured traffic to be interpreted as a specified type.		Perform a name lookup for port, host, and MAC addresses when viewing the packet capture. This can cause significant delays due to reverse DNS lookups.

### Custom Filter Options

Hint	All input is <b>space-separated</b> . When selecting a match that specifies "OR", at least two Types should be specified (such as EtherType and Port). This will capture packets that match either Type instead of exclusively both.
Untagged Filter	Filter options for packets without any VLAN tags.
include any of UNTAGGED PACKETS all of EXAMPLE: 10.1.1.0/24 192.168.1.1 HOST IP ADDRESS OR SUBNET any of EXAMPLE: 17 tcp PROTOCOL all of EXAMPLE: 80 443 PORT NUMBER any of EXAMPLE: arp 8100 0x8200 ETHERTYPE	
Tagged Filter	Filter options for packets that have a VLAN tag set. Specify a tag level to match stacked VLAN packets (such as QinQ).
exclude all TAGGED PACKETS all of EXAMPLE: 10.1.1.0/24 192.168.1.1 HOST IP ADDRESS OR SUBNET any of EXAMPLE: 17 tcp PROTOCOL all of EXAMPLE: 80 443 PORT NUMBER any of EXAMPLE: 100 200 VLAN TAG 1 LEVEL all of EXAMPLE: 00:02:11:22:33:44:55:66 HOST MAC ADDRESS any of EXAMPLE: arp 8100 0x8200 ETHERTYPE	

Running packet capture:  
 /usr/sbin/tcpdump -ni enc0 -c 1000 -U -w -

### Packet Capture Output: /tmp/packetcapture-enc0-20240327074351.pcap

Auto-scroll

```

07:44:22.139050 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 133, length 64
07:44:23.139276 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 134, length 64
07:44:23.141421 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 134, length 64
07:44:24.138933 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 135, length 64
07:44:24.140573 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 135, length 64
07:44:25.140476 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 136, length 64
07:44:25.142217 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 136, length 64
07:44:26.141138 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 137, length 64
07:44:26.143037 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 137, length 64
07:44:27.142925 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 138, length 64
07:44:27.145749 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 138, length 64
07:44:28.142724 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 139, length 64
07:44:28.145132 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 139, length 64
07:44:29.143686 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 140, length 64
07:44:29.145807 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 140, length 64
07:44:30.144289 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 141, length 64
07:44:30.146409 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 141, length 64
07:44:31.144786 (authentic,confidential): SPI 0xc1c83cc9: IP 192.200.10.12 > 192.100.10.2: ICMP echo request, id 1, seq 142, length 64
07:44:31.148541 (authentic,confidential): SPI 0xc864e02c: IP 192.100.10.2 > 192.200.10.12: ICMP echo reply, id 1, seq 142, length 64
  
```

## Sécurisation d'un autre service au choix.

Dhcp sécurisé :

```
ip dhcp snooping vlan 10-30
interface GigabitEthernet0/1-23
ip dhcp snooping trust
```

## Test de sécurité

Nmap

IP Router → Vlan 800

```
(kali㉿kali)-[~]
└─$ nmap 10.16.18.51
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 04:06 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 4.50% done; ETC: 04:06 (0:00:42 remaining)
Nmap scan report for 10.16.18.51
Host is up (0.0024s latency).
All 1000 scanned ports on 10.16.18.51 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 9.24 seconds
```

IP PfSense 2

```
(kali㉿kali)-[~]
└─$ nmap 10.200.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 04:09 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
```

IP PfSense 1

```
(kali㉿kali)-[~]
└─$ nmap 10.100.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 04:09 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
```

Ses règles de base suffisent à bloquer les pings venant du WAN et le scan de ports.

The screenshot shows a 'Firewall / Rules / WAN' interface. At the top, there are tabs for 'Floating', 'WAN' (which is selected), 'LAN', and 'IPsec'. Below the tabs is a table titled 'Rules (Drag to Change Order)'. The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are two rows in the table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/1000 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

A yellow banner at the bottom of the table area states: 'No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.'

At the bottom right of the interface are several buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

## Config ciscoasa

ASA Version 9.0(1)

!

hostname ciscoasa

enable password 8Ry2Yjlyt7RRXU24 encrypted

passwd 2KFQnbNIdI.2KYOU encrypted

names

!

interface Ethernet0/0

switchport access vlan 2

!

interface Ethernet0/1

switchport access vlan 2

!

interface Ethernet0/2

switchport access vlan 3

!

interface Ethernet0/3

!

interface Ethernet0/4

!

interface Ethernet0/5

!

interface Ethernet0/6

!

interface Ethernet0/7

!

**interface Vlan1**

nameif inside

security-level 100

**ip address 192.150.0.254 255.255.255.0**

```

!
interface Vlan2
  nameif dmz
  security-level 50
  ip address 192.150.10.1 255.255.255.0
!
  ftp mode passive
object network obj_any
  subnet 0.0.0 0.0.0
object network INSIDE
  subnet 192.168.1.0 255.255.255.0
object network obj-net-192_150_0_0
  subnet 192.150.0.0 255.255.255.0
object network obj-web-server
  host 192.150.10.5
access-list inside_access_in extended permit tcp 192.100.0.0 255.255.0.0 host 192.150.0.5 eq www
access-list inside_access_in extended permit tcp 192.200.0.0 255.255.0.0 host 192.150.0.5 eq www
access-list inside_access_in extended permit tcp 192.100.0.0 255.255.0.0 host 192.150.0.5 eq https
access-list inside_access_in extended permit tcp 192.200.0.0 255.255.0.0 host 192.150.0.5 eq https
  pager lines 24
  logging enable
  logging buffered debugging
  logging asdm informational
  mtu inside 1500
  mtu dmz 1500
  icmp unreachable rate-limit 1 burst-size 1
  no asdm history enable
  arp timeout 14400
  no arp permit-nonconnected
!
object network obj_any
  nat (inside,dmz) dynamic interface
object network obj-net-192_150_0_0
  nat (inside,dmz) dynamic interface
object network obj-web-server
  nat (dmz,inside) static 192.150.0.5
route inside 0.0.0.0 0.0.0.0 192.150.0.1 1
  timeout xlate 3:00:00
  timeout pat-xlate 0:00:30
  timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
  timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
  timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
  timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
  timeout tcp-proxy-reassembly 0:01:00

```

```
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.150.10.0 255.255.255.0 inside
http 192.150.0.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh timeout 5
console timeout 0

dhcpd auto_config
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
```

```
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:04286640aa7ac3a0f7ba56869ba268b6
: end
```

## Sécurisation WEB

### Site Web (NGINX)

```
apt update
apt install nginx
apt install certbot python3-certbot-nginx
```

### HTTPS

#### Génération d'une clef et d'un certificat auto-signé :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl/selfsigned.key -out
/etc/nginx/ssl/selfsigned.crt
```

### Nginx

***sudo nano /etc/nginx/sites-available/societe1 :***

```
server {
    listen 80;
    server_name societe1.fr www.societe1.fr;
    return 301 https://$host$request_uri;
}

server {
    listen 443 ssl;
    server_name societe1.fr www.societe1.fr;

    ssl_certificate /etc/nginx/ssl/selfsigned.crt;
    ssl_certificate_key /etc/nginx/ssl/selfsigned.key;

    root /var/www/societe1.fr;
    index index.html;

    location / {
        try_files $uri $uri/ $uri.html =404;
    }
}
```

***nano /var/www/societe1.fr/index.html :***

```

<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <title>Société 1</title>
</head>
<body>
    <h1>Société 1</h1>
    <a href="page1">Page 1</a>
</body>
</html>

```

**nano /var/www/[societe1.fr/page1.html](#) :**

```

<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <title>Page 1</title>
</head>
<body>
    <h1>Page 1</h1>
    <a href="/">Retour à l'accueil</a>
</body>
</html>

```

**lien symbolique entre sites-available/societe1 et sites-enabled :**

*In -s /etc/nginx/sites-available/societe1 /etc/nginx/sites-enabled/*

**vérifier l'orthographe :**

*nginx -t*

**redémarrer nginx**

*systemctl restart nginx*

## En-têtes

On ajoute les différents en-têtes de sécurité :

```

server {
    listen 80;
    server_name _;
    return 301 https://$host$request_uri;
}

server {

```

```

listen 443 ssl;
server_name _;

ssl_certificate /etc/nginx/ssl/selfsigned.crt;
ssl_certificate_key /etc/nginx/ssl/selfsigned.key;

root /var/www/societe1.fr;
index index.html;

location / {
    try_files $uri $uri/ $uri.html =404;
}

add_header Strict-Transport-Security 'max-age=31536000; includeSubDomains; preload';
add_header Content-Security-Policy "default-src 'self'; font-src *;img-src * data:; script-src *; style-src *";
add_header X-XSS-Protection "1; mode=block";
add_header X-Frame-Options "SAMEORIGIN";
add_header X-Content-Type-Options nosniff;
add_header Referrer-Policy "strict-origin";
add_header Permissions-Policy
"geolocation=(),midi=(),sync-xhr=(),microphone=(),camera=(),magnetometer=(),gyroscope=(),fullscreen=(self),payment=()";
}

```

Les en-têtes vu sur le navigateur :

②	<a href="#">Connection:</a> keep-alive
②	<a href="#">Content-Encoding:</a> gzip
②	<a href="#">Content-Security-Policy:</a> default-src 'self'; Font-src *;img-src * data:; script-src *; style-src *
②	<a href="#">Content-Type:</a> text/html
②	<a href="#">Date:</a> Fri, 29 Mar 2024 12:05:59 GMT
②	<a href="#">ETag:</a> W/"65f04d39-ac"
②	<a href="#">Last-Modified:</a> Tue, 12 Mar 2024 12:40:25 GMT
	<a href="#">Permissions-Policy:</a> geolocation=(),midi=(),sync-xhr=(),microphone=(),camera=(),magnetometer=(),gyroscope=(),fullscreen=(self),payment=()
②	<a href="#">Referrer-Policy:</a> strict-origin
②	<a href="#">Server:</a> nginx/1.18.0 (Ubuntu)
②	<a href="#">Strict-Transport-Security:</a> max-age=31536000; includeSubDomains; preload
②	<a href="#">Transfer-Encoding:</a> chunked
②	<a href="#">X-Content-Type-Options:</a> nosniff
②	<a href="#">X-Frame-Options:</a> SAMEORIGIN
②	<a href="#">X-XSS-Protection:</a> 1; mode=block

Pour les voirs on fait [Clic Droit] > Inspecter > Réseau > **(On recharge la page)** > 200 GET localhost / > En-têtes :

The screenshot shows the Network tab of the developer tools. A context menu is open at the top left, with the 'Inspecter' option highlighted with a red box. The Network tab has a red border around its header. The 'En-têtes' section is also highlighted with a red box. The response for the GET request to 'localhost /' is shown, with the status 200 OK and various headers listed.

```

    Headers for GET https://localhost/
    Status: 200 OK
    Headers:
    Connection: keep-alive
    Content-Encoding: gzip
    Content-Security-Policy: default-src 'self'; font-src *;img-src * data;; script-src *; style-src *
    Content-Type: text/html
    Date: Fri, 29 Mar 2024 12:05:59 GMT
    ETag: W/"65f04d39-ac"
    Last-Modified: Tue, 12 Mar 2024 12:40:25 GMT
    Permissions-Policy: geolocation=(),midi=(),sync-xhr=(),microphone=(),camera=(),magnetometer=(),gyroscope=(),fullscreen=(self),payment=()
    Referrer-Policy: strict-origin
    Server: nginx/1.18.0 (Ubuntu)
    Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
    Transfer-Encoding: chunked
    X-Content-Type-Options: nosniff
    X-Frame-Options: SAMEORIGIN
    X-XSS-Protection: 1; mode=block
  
```

Pour voir le certificat du site on clic sur le **cadenas** à côté de la barre de recherche :

The top screenshot shows a browser address bar with 'https://localhost'. A warning message 'Informations pour le site localhost' is displayed, stating 'Connexion non sécurisée' (Unsecured connection). The bottom screenshot shows a similar warning for 'https://localhost', with the message 'Sécurité de la connexion pour localhost' and 'Votre connexion à ce site n'est pas sécurisée.' (Your connection to this site is not secure). It also mentions 'Vous avez ajouté une exception de sécurité pour ce site.' (You have added a security exception for this site) and a button 'Supprimer l'exception' (Delete exception).

Informations sur la page - <https://localhost/>

 Général  Permissions  Sécurité

**Identité du site web**

Site web : localhost  
Propriétaire : Ce site web ne fournit pas d'informations sur son propriétaire.  
Vérifiée par : societe1.fr [Afficher le certificat](#)

**Vie privée et historique**

Ai-je déjà visité ce site web auparavant ? Oui, 74 fois  
Ce site web conserve-t-il des informations sur mon ordinateur ? Non [Effacer les cookies et les données de navigation](#)  
Ai-je un mot de passe enregistré pour ce site web ? Non [Voir les mots de passe enregistrés](#)

**Détails techniques**

Connexion chiffrée (clés TLS\_AES\_256\_GCM\_SHA384, 256 bits, TLS 1.3)  
La page actuellement affichée a été chiffrée avant d'avoir été envoyée sur Internet.  
Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

[Aide](#)

# Certificat

societe1.fr

## Nom du sujet

Pays	FR
État / Province	HDF
Localité	Bethune
Organisation	societe1.fr
Unité organisationnelle	societe1.fr
Nom courant	societe1.fr
Adresse électronique	societe1@societe1.fr

## Nom de l'émetteur

Pays	FR
État / Province	HDF
Localité	Bethune
Organisation	societe1.fr
Unité organisationnelle	societe1.fr
Nom courant	societe1.fr
Adresse électronique	societe1@societe1.fr

## Validité

Pas avant	Tue, 12 Mar 2024 11:59:07 GMT
Pas après	Wed, 12 Mar 2025 11:59:07 GMT

## Informations sur la clé publique

Algorithme	RSA
Taille de la clé	2048
Exposant	65537
Module	B6:5A:42:49:04:60:CA:F4:53:A1:C8:2E:4A:5D:A7:56:18:45:3E:D4:5B:B2:8D:D...

## Divers

Numéro de série	31:E1:2B:01:90:7C:5F:77:E2:0F:12:8D:1E:E6:E4:B6:F1:2D:3A:ED
Algorithme de signature	SHA-256 with RSA Encryption
Version	3
Télécharger	<a href="#">PEM (cert)</a> <a href="#">PEM (chain)</a>

Test de connexion

## Test de connexion au site depuis des machines du réseau local:

192.100.10.12/24 -> 192.150.0.5:



The screenshot shows a web browser window with the URL <https://site.dom-societe1.lan>. The page title is "Société 1". Below the title, there is a link labeled "Page 1".

```
root@rt-mv: /home/administrateur
root@rt-mv:/home/administrateur# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:49:14:fa brd ff:ff:ff:ff:ff:ff
    inet 192.100.10.12/24 brd 192.100.10.255 scope global dynamic noprefixroute
        valid_lft 80091sec preferred_lft 80091sec
    inet6 fe80::702b:9771:9dc4:2c5b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@rt-mv:/home/administrateur#
```

192.200.10.12/24 -> 192.150.0.5:



The screenshot shows a web browser window with the URL <https://site.dom-societe1.lan>. The page title is "Société 1". Below the title, there is a link labeled "Page 1".

```
administrateur@rt-mv: ~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:00:01:43 brd ff:ff:ff:ff:ff:ff
    inet 192.200.10.12/24 brd 192.200.10.255 scope global dynamic noprefixroute
        valid_lft 80321sec preferred_lft 80321sec
    inet6 fe80::aec7:1da7:c0d9:d14d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
administrateur@rt-mv: ~$
```

# Recommandations ANSSI

Identifiant	Intitulé de la recommandation	Associée à une exigence d'une règle	Mesure retenue, exclue ou non applicable ?	Niveau de mise en œuvre
2	R1 Modifier les éléments de configuration par défaut	Oui	Retenue	Totalement mis en œuvre
3	R1- Paliere l'impossibilité de changer un élément par défaut	Non	Non retenue	n.a
4	R2 Installer uniquement les services ou fonctionnalités indispensables	Oui	Retenue	Totalement mis en œuvre
5	R2- Paliere l'impossibilité de désinstaller un service non indispensable	Oui	Retenue	Totalement mis en œuvre
6	R3 Définir et utiliser des configurations de référence	Non	Non retenue	n.a
7	R4 Établir un inventaire technique des éléments et des accès au SIE	Non	Non retenue	n.a
8	R5 Utiliser uniquement des équipements maîtrisés	Oui	Retenue	Totalement mis en œuvre
9	R6 Dédier aux SIE des supports amovibles identifiés	Oui	Retenue	Totalement mis en œuvre
10	R7 Décontaminer les supports amovibles avant leur utilisation	Oui	Retenue	Totalement mis en œuvre
11	R7+ Utiliser un équipement dédié à l'analyse des supports amovibles	Non	Non retenue	n.a
12	R8 Mettre en œuvre une traçabilité de l'utilisation des supports amovibles	Non	Non retenue	n.a
13	R8+ Mettre en œuvre un outil de protection contre l'exfiltration de données	Non	Non retenue	n.a
14	R9 Segmenter le SI en systèmes et sous-systèmes	Oui	Retenue	Totalement mis en œuvre
15	R10 Autoriser les interconnexions suivant le besoin de fonctionnement	Oui	Non retenue	n.a
16	R11 Mettre en place un cloisonnement physique	Oui	Non retenue	n.a
17	R11- Mettre en place un cloisonnement logique par le chiffre	Oui	Retenue	Totalement mis en œuvre
18	R11- Mettre en place un cloisonnement logique	Oui	Retenue	Totalement mis en œuvre
19	R12 Chiffrer les données en amont du stockage avec des secrets distincts	Non	Non retenue	n.a
20	R13 Contrôler le cloisonnement mis en place en cas d'externalisation	Oui	Non retenue	n.a
21	R14 Infrastructures numériques : cloisonner les services internes	Oui	Retenue	Totalement mis en œuvre
22	R15 Segmenter les SIE publics en au moins deux sous-systèmes	Oui	Non retenue	n.a
23	R16 Accès public : chiffrer et authentifier les flux au niveau applicatif	Oui	Retenue	Totalement mis en œuvre
24	R17 Accès public : authentifier les utilisateurs	Non	Retenue	Totalement mis en œuvre
25	R17+ Accès public : authentifier les utilisateurs avec deux facteurs	Non	Non retenue	n.a
26	R18 Accès nomade : mettre en place un tunnel chiffré et authentifié	Oui	Retenue	Totalement mis en œuvre
27	R19 Accès nomade : authentifier les utilisateurs avec deux facteurs	Oui	Non retenue	n.a
28	R20 Accès nomade : chiffrer intégralement le disque du poste	Oui	Non retenue	n.a
29	R21 Accès nomade : utiliser des filtres de confidentialité	Non	Non retenue	n.a
30	R22 Accès interne : mettre en place un tunnel chiffré et authentifié	Oui	Retenue	Totalement mis en œuvre
31	R23 Filtrer les flux aux interconnexions entre les systèmes et entre les sous-systèmes	Oui	Non retenue	n.a
32	R23+ Filtrer les flux aux extrémités des communications	Non	Retenue	Totalement mis en œuvre
33	R24 Définir les besoins de filtrage sur le SIE	Oui	Non retenue	n.a
34	R25 Formaliser les règles de filtrage	Oui	Non retenue	n.a
35	R26 Passer régulièrement en revue les règles de filtrage	Non	Non retenue	n.a
36	R27 Mettre en œuvre le filtrage grâce à des équipements spécialisés	Non	Retenue	Totalement mis en œuvre
37	R28 Bloquer tous les flux non explicitement autorisés	Oui	Non retenue	n.a
38	R29 Utiliser des comptes d'administration dédiés	Oui	Retenue	Totalement mis en œuvre
39	R29- Paliere l'absence de comptes dédiés à l'administration	Oui	Non retenue	n.a
40	R30 Utiliser par défaut des comptes d'administration individuels	Oui	Non retenue	n.a
41	R31 Attribuer les droits d'administration à des groupes	Non	Non retenue	n.a
42	R32 Protéger l'accès aux annuaires des comptes d'administration	Non	Retenue	Totalement mis en œuvre
43	R33 Renforcer l'authentification pour les comptes d'administration	Non	Non retenue	n.a
44	R34 Empêcher le stockage des secrets d'authentification dans les journaux	Oui	Non retenue	n.a
45	R35 Respecter le principe du moindre privilège dans l'attribution des droits d'administration	Oui	Non retenue	n.a
46	R36 N'utiliser que des équipements maîtrisés pour l'administration	Oui	Retenue	Totalement mis en œuvre
47	R37 Utiliser un poste d'administration dédié	Oui	Non retenue	n.a
48	R37- Accéder aux autres environnements de travail depuis le poste d'administration	Oui	Non retenue	n.a
49	R38 Renforcer la sécurité du poste d'administration	Oui	Non retenue	n.a
50	R39 Connecter les ressources d'administration sur un réseau physique dédié	Oui	Non retenue	n.a
51	R39- Connecter les ressources d'administration sur un réseau VPN IPsec dédié	Oui	Non retenue	n.a
52	R39- Paliere l'absence de chiffrement des flux d'administration	Oui	Non retenue	n.a
53	R40 Dédier une interface réseau physique d'administration	Non	Non retenue	n.a
54	R40- Dédier une interface réseau virtuelle d'administration	Non	Non retenue	n.a
55	R41 Cloisonner et filtrer le réseau d'administration	Non	Non retenue	n.a
56	R42 Utiliser des protocoles sécurisés pour l'administration	Non	Retenue	Totalement mis en œuvre
57	R43 Administrer des SI différents avec des serveurs outils différents	Non	Non retenue	n.a
58	R44 Utiliser des comptes individuels	Oui	Retenue	Totalement mis en œuvre
59	R44- Paliere l'absence de comptes individuels	Oui	Non retenue	n.a
60	R45 Désactiver les comptes inutilisés	Oui	Retenue	Totalement mis en œuvre
61	R46 Mettre en œuvre un mécanisme d'authentification pour chaque compte	Oui	Retenue	Totalement mis en œuvre
62	R47 Établir une politique de gestion des secrets d'authentification	Oui	Retenue	Totalement mis en œuvre
63	R48 Interdire le partage de secrets d'authentification	Oui	Non retenue	n.a
64	R48- Protéger les secrets d'authentification des comptes partagés	Oui	Non retenue	n.a
65	R49 Dédier un mot de passe à chaque compte privilégié	Oui	Retenue	Totalement mis en œuvre
66	R50 Stocker les mots de passe dans un coffre-fort de mots de passe	Non	Non retenue	n.a
67	R51 Renouveler régulièrement les secrets d'authentification	Oui	Non retenue	n.a
68	R51- Paliere l'impossibilité de modifier un secret d'authentification	Oui	Non retenue	n.a
69	R52 Contrôler le renouvellement et l'accès aux secrets d'authentification	Oui	Retenue	Totalement mis en œuvre
70	R53 Renouveler immédiatement des secrets d'authentification	Non	Retenue	Totalement mis en œuvre
71	R54 Définir une politique de gestion des droits d'accès	Oui	Non retenue	n.a
72	R55 Attribuer les droits d'accès suivant le principe du moindre privilège	Oui	Non retenue	n.a
73	R56 Définir une traçabilité des comptes privilégiés	Oui	Non retenue	n.a
74	R57 Faire une revue régulière des droits d'accès	Oui	Non retenue	n.a
75	R58 Documenter une politique de MCS	Oui	Non retenue	n.a
76	R59 Mettre en place une veille de sécurité	Oui	Non retenue	n.a
77	R60 Obtenir des mises à jour de sécurité officielles	Non	Non retenue	n.a
78	R61 Appliquer les mises à jour de sécurité	Oui	Retenue	Totalement mis en œuvre
79	R62 Utiliser des logiciels et des matériels supportés	Oui	Retenue	Totalement mis en œuvre
80	R62- Paliere l'utilisation de versions obsolètes de logiciels et de matériels	Oui	Non retenue	n.a

