

# R509 - TP Stormshield

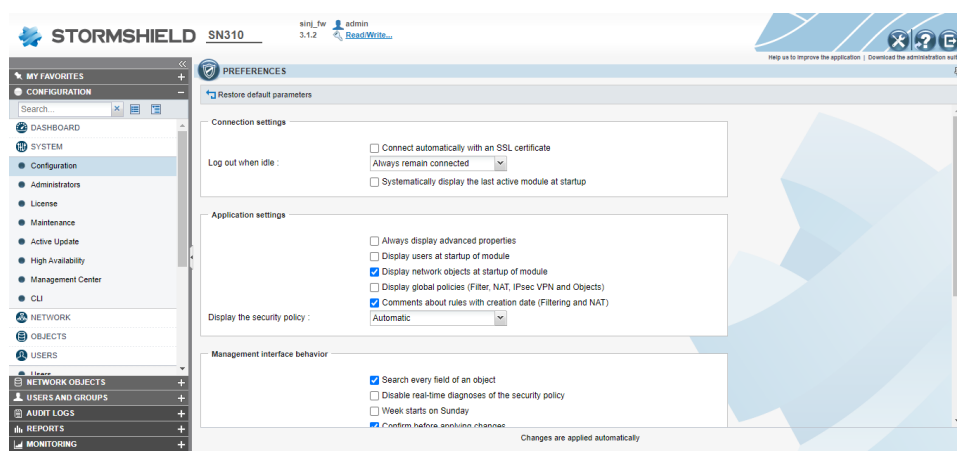
Par Fabiano, Gihed et Mussa

## Prise en main du Firewall

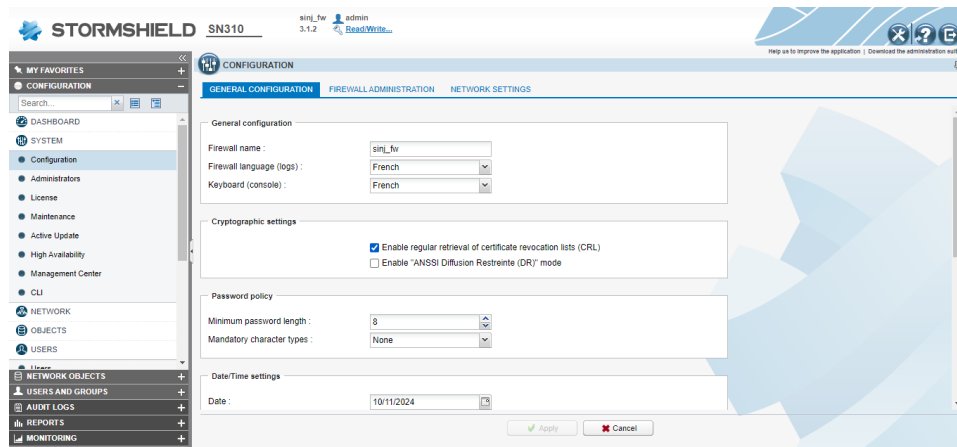
Pour configurer le pare-feu Stormshield, on se connecte à l'interface d'administration web



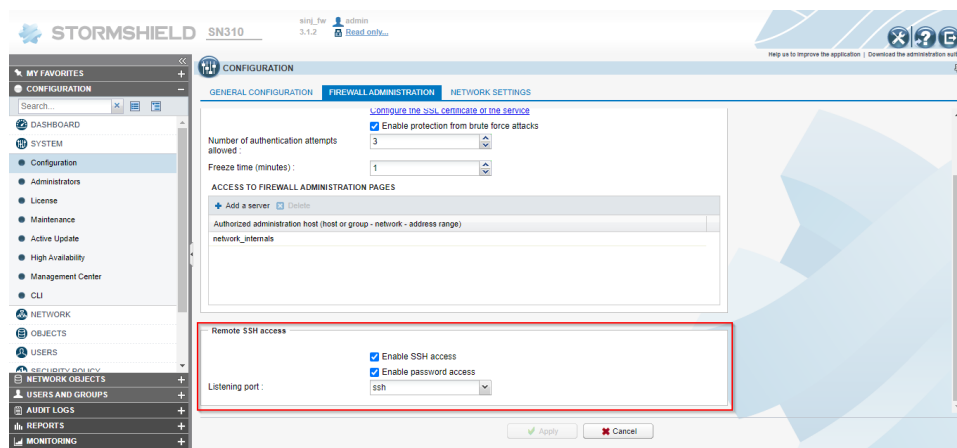
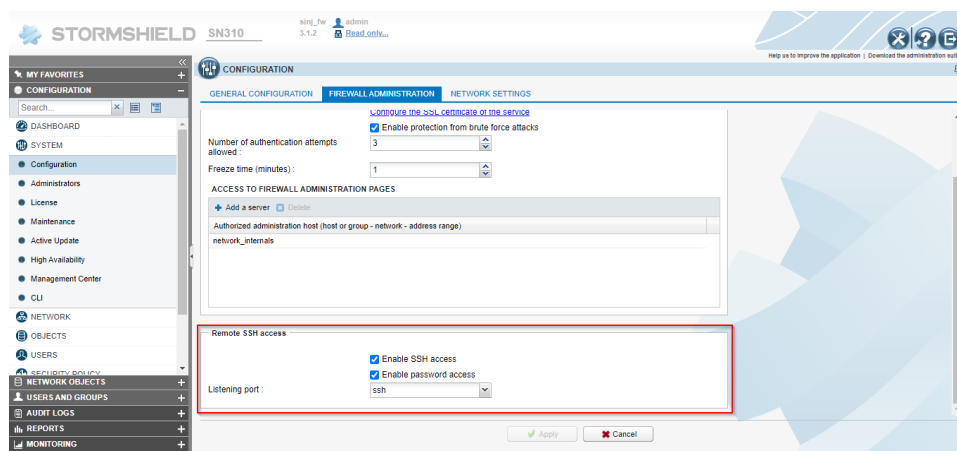
Dans les préférences, on choisit l'option de ne jamais être déconnecté en cas d'inactivité



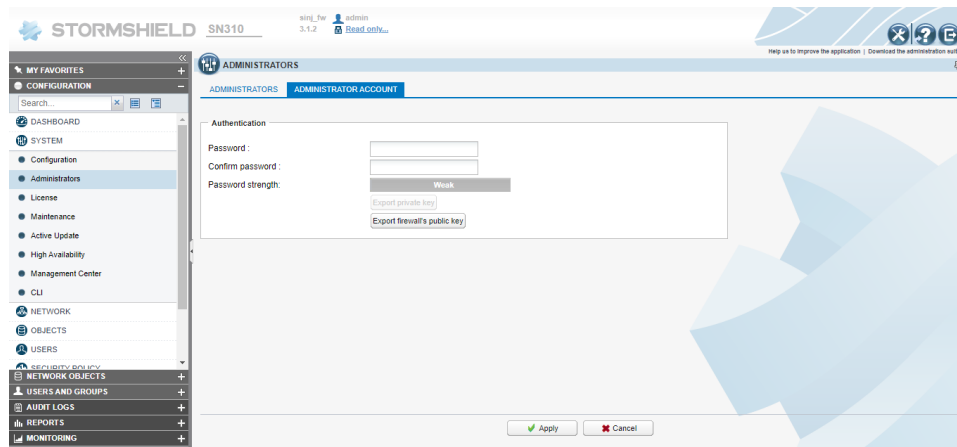
On configure ensuite le nom de notre pare-feu, la langue des logs ainsi que celui du clavier.



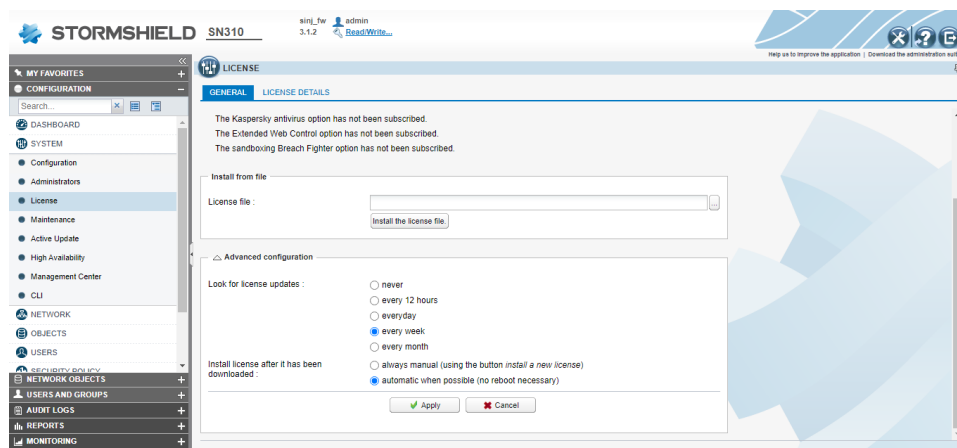
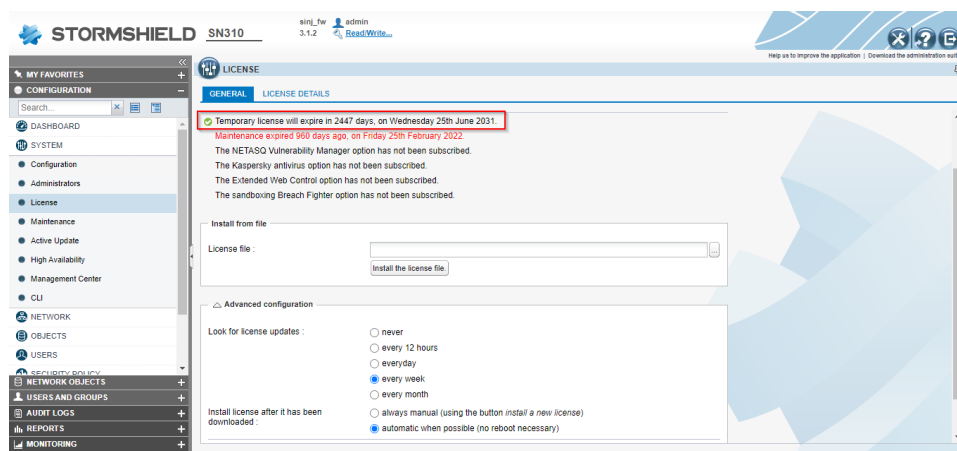
Viens ensuite l'activation du service SSH avec l'authentification par mot de passe.



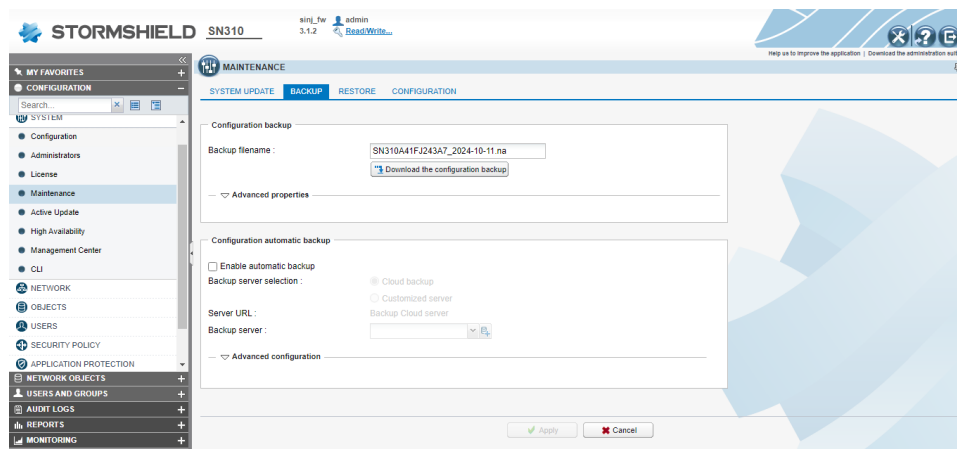
pour le mot de passe, on a pris Sinj1234@



la licence est pour l'instant encore valable. On configure par la même occasion la mäj automatique avec une vérification hebdomadaire.



Et on fait une backup de la configuration.



La même configuration est à faire pour l'autre entreprise.

## Les Objets

On va désormais créer les objets, dans ce rapport, on retrouvera les configurations faites sur la machine de l'entreprise A (=1). On devra donc configurer les machines de l'entreprise B (=2)

On va donc créer l'objet ainsi que le réseau pour l'autre compagnie :

- Fw\_B en 192.36.253.20
- Lan\_in\_B en 192.168.2.0 / 255.255.255.0

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name:

Fw\_B

IPv4 address:

192.36.253.20

MAC address:

01:23:45:67:89:ab (optional)

Resolution

None (static IP)

Automatic

Comments:

CREATE AN OBJECT

Host  
DNS name (FQDN)  
**Network**  
IP address range  
Router  
Group  
IP Protocol  
Port  
Port group  
Region group  
Time object

Object name:   
IPv4 address  
Network IP address:   
*Example 192.168.0.0/16 or 192.168.0.0/255.255.0.0*  
Comments:

On crée ensuite un service 'webmail' basé sur TCP fonctionnant sur le port 808.

CREATE AN OBJECT

Host  
DNS name (FQDN)  
Network  
IP address range  
Router  
Group  
IP Protocol  
**Port**  
Port group  
Region group  
Time object

Object name:   
☒ Port  
Port:   
☐ Port range  
From:   
To:   
Protocol:   
Comments:

Et on crée ensuite différents objets pour notre entreprise, respectivement :

- pc\_admin = 192.168.1.2
- srv\_dns\_priv = 172.16.1.10
- srv\_web\_priv = 172.16.1.11
- srv\_ftp\_priv = 172.16.1.12
- srv\_mail\_priv = 172.16.1.13

## CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses IP

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

pc\_admin

Adresse IPv4:

192.168.1.2

Adresse MAC:

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

Résolution

☒ Aucune (IP statique)

☐ Automatique

Commentaire:

## CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses IP

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

srv\_dns\_priv

Adresse IPv4:

172.16.1.10

Adresse MAC:

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

Résolution

☒ Aucune (IP statique)

☐ Automatique

Commentaire:

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses IP

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

srv\_web\_priv

Adresse IPv4:

172.16.1.11

Adresse MAC:

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

Résolution

☒ Aucune (IP statique)

☐ Automatique

Commentaire:

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses IP

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

srv\_ftp\_priv

Adresse IPv4:

172.16.1.12

Adresse MAC:

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

Résolution

☒ Aucune (IP statique)

☐ Automatique

Commentaire:

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses IP

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

Adresse IPv4:

Adresse MAC:

Résolution

☒ Aucune (IP statique)
 ☐ Automatique

Commentaire:

On va créer ensuite un groupe qui contiendra les 4 serveurs qu'on viens de créer, on le nommera '4\_Serv\_Sinj'.

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses IP

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

Commentaire:

srv

Type	Nom de l'objet
	srv_dns_priv
	srv_web_priv
	srv_ftp_priv
	srv_mail_priv

Créer un objet

Type	Objets dans ce groupe
	srv_mail_priv
	srv_ftp_priv
	srv_web_priv
	srv_dns_priv

Pour le dns, on remplace les deux dns de google par celui du réseau Nat dans le cas de la machine virtuelle.



CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses IP

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

Default\_Gw

Adresse IPv4:

192.36.253.1

Adresse MAC:

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

Résolution

☒ Aucune (IP statique)
☐ Automatique

Commentaire:

Résolution DNS

LISTE DES SERVEURS DNS UTILISÉS PAR LE FIREWALL

+ Ajouter	✕ Supprimer
Serveur DNS (machine)	
Default_Gw	

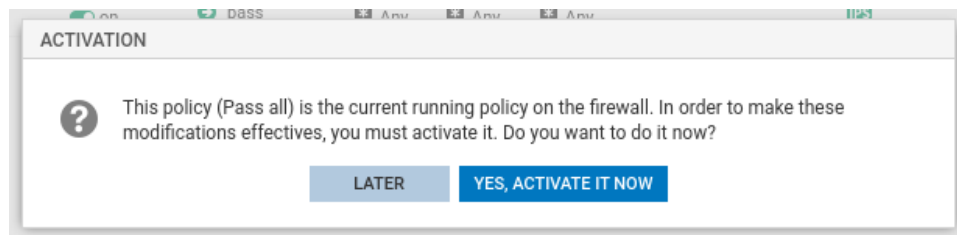
L'entreprise B, quant à lui, aura les objets suivants :

- Fw\_A = 192.36.253.10
- Lan\_in\_A = 192.168.1.0 / 255.255.255.0
- Pc\_admin = 192.168.2.2
- Srv\_dns\_priv = 172.16.2.10
- Srv\_web\_priv = 172.16.2.11
- Srv\_ftp\_priv = 172.16.2.12
- Srv\_mail\_priv = 172.16.2.13

Avec un groupe pour les 4 serveurs et le dns si machine virtuelle.

## Configuration réseau

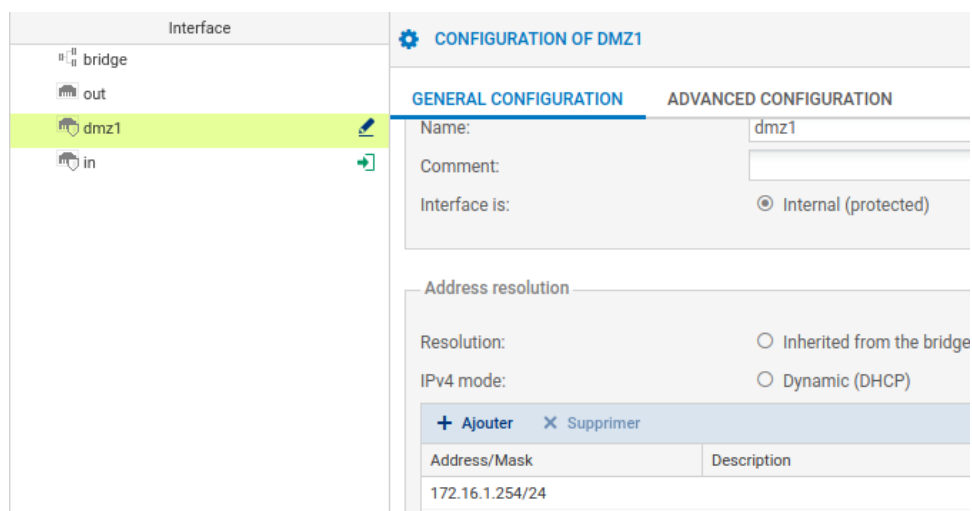
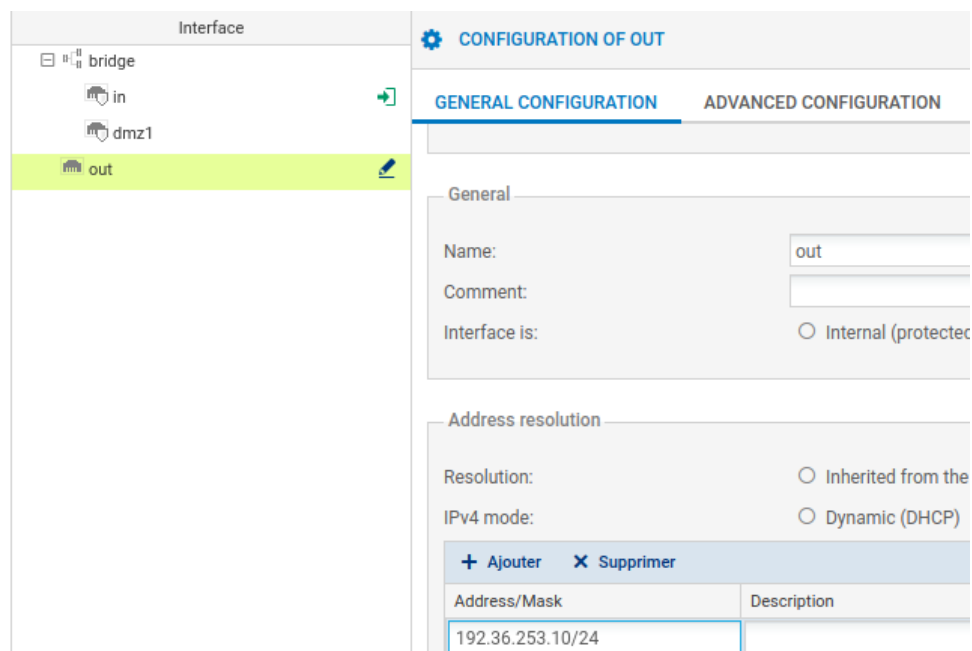
On va sélectionner la politique de filtrage Pass all qui autorisera tous les trafics traversant ou à destination du firewall

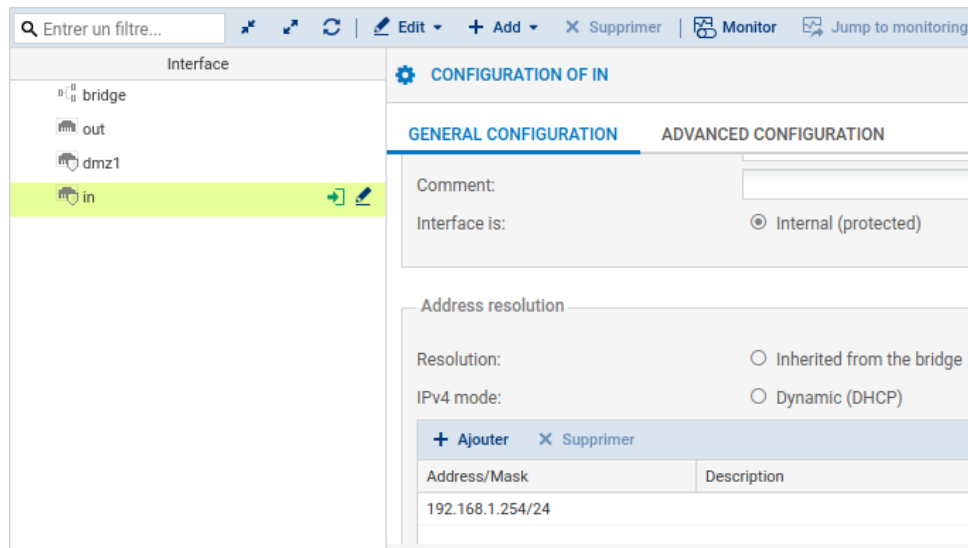


## Configuration des interfaces

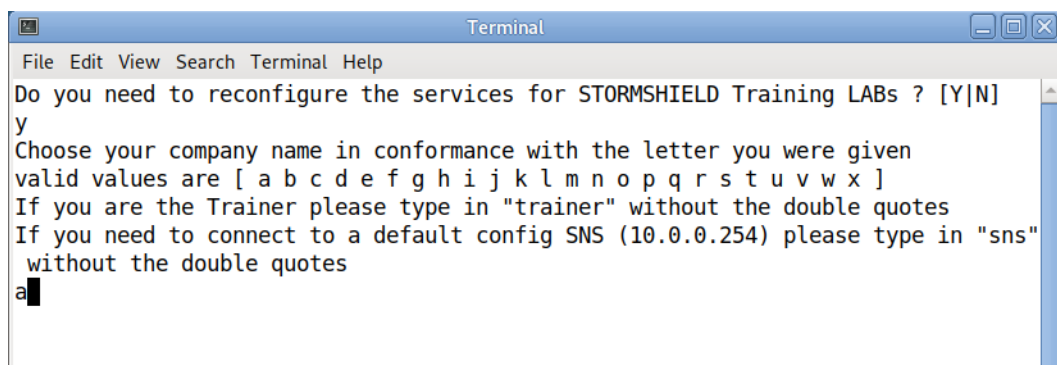
On configure ensuite les interfaces OUT, DMZ1 et IN, respectivement :

- 192.36.253.10/24
- 172.16.1.254/24
- 192.168.1.254/24





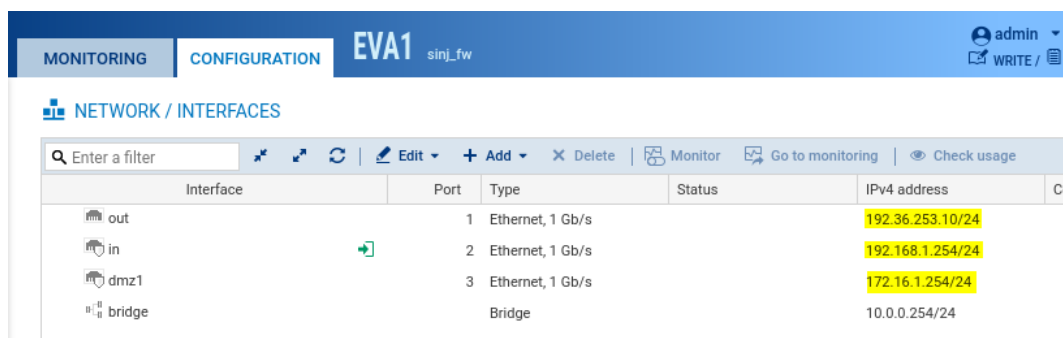
Dans le cas de l'utilisation de la VM, on double-clique sur network\_config.sh et on choisit la lettre de notre entreprise (a ou b).



avec la commande `ip a`, on vérifie l'adresse attribuée :

```
user@client-training:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
t 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
group default qlen 1000
    link/ether 08:00:27:44:b1:5c brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe44:b15c/64 scope link
        valid_lft forever preferred_lft forever
```

Après reconnexion sur l'interface de notre pare-feu, on vérifie la bonne adressage de nos interfaces.



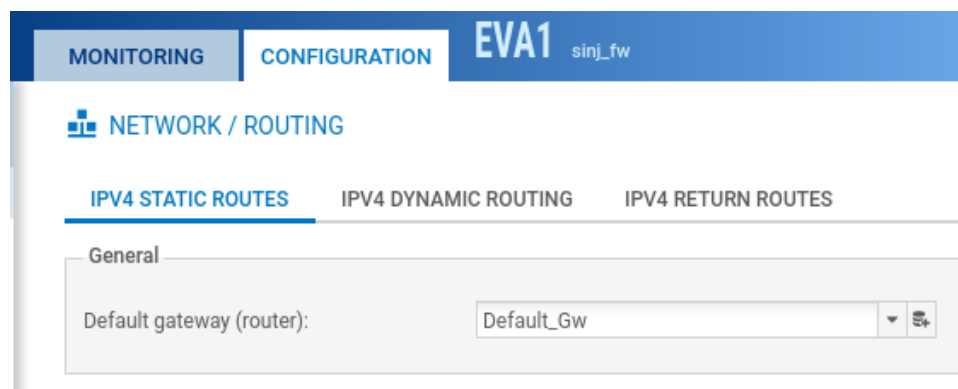
Interface	Port	Type	Status	IPv4 address
out	1	Ethernet, 1 Gb/s		192.36.253.10/24
in	2	Ethernet, 1 Gb/s		192.168.1.254/24
dmz1	3	Ethernet, 1 Gb/s		172.16.1.254/24
bridge		Bridge		10.0.0.254/24

Pour l'entreprise B, les configuration des interfaces seront :

- OUT : 192.36.253.20/24
- DMZ1 : 172.16.2.254/24
- IN : 192.168.2.254/24

## Configuration du routage

On va désormais configurer la passerelle par défaut de notre firewall.



MONITORING CONFIGURATION EVA1 sinj\_fw

NETWORK / ROUTING

IPV4 STATIC ROUTES IPV4 DYNAMIC ROUTING IPV4 RETURN ROUTES

General

Default gateway (router): Default\_Gw

On crée ensuite une route statique pour permettre de rejoindre Lan\_in\_B depuis notre machine.

MONITORING CONFIGURATION EVA1 sinj\_fw admin WRITE /

NETWORK / ROUTING

IPv4 STATIC ROUTES IPv4 DYNAMIC ROUTING IPv4 RETURN ROUTES

General

Default gateway (router): Default\_Gw

STATIC ROUTES

Searching... + Add X Delete

Status	Destination network (ho...	Interface	Address range	Gateway	C
on	Lan_in_B	out	192.168.2.0/24	Fw_B	

même manipulation chez l'entreprise B

IPv4 STATIC ROUTES IPv4 DYNAMIC ROUTING IPv4 RETURN ROUTES

General

Default gateway (router): Default\_Gw

STATIC ROUTES

Searching... + Add X Delete

Status	Destination network (host, net...	Interface	Address range	Gateway
on	Lan_in_A	out	192.168.1.0/24	Fw_A

## Configuration du proxy cache DNS :

MONITORING CONFIGURATION EVA1 sinj\_fw

NETWORK / DNS CACHE PROXY

ON

LIST OF CLIENTS ALLOWED TO USE THE DNS CACHE

Searching... + Add X Delete

DNS client [host, network, range, group] ↑

srv\_dns\_priv

On peut voir après un test de Ping de la machine de l'entreprise A vers celui de la machine B que les routes fonctionnent.

```

user@client-training:~$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=26.8 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=14.9 ms
^C
--- 192.168.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 10ms
rtt min/avg/max/mdev = 14.871/20.841/26.812/5.972 ms
user@client-training:~$ █

```

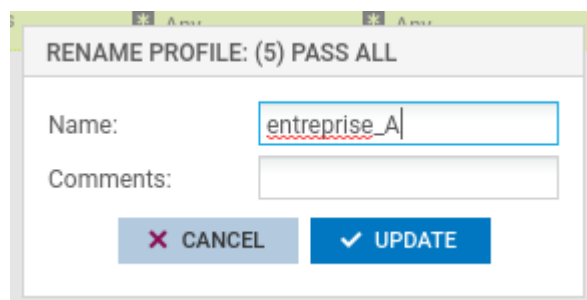
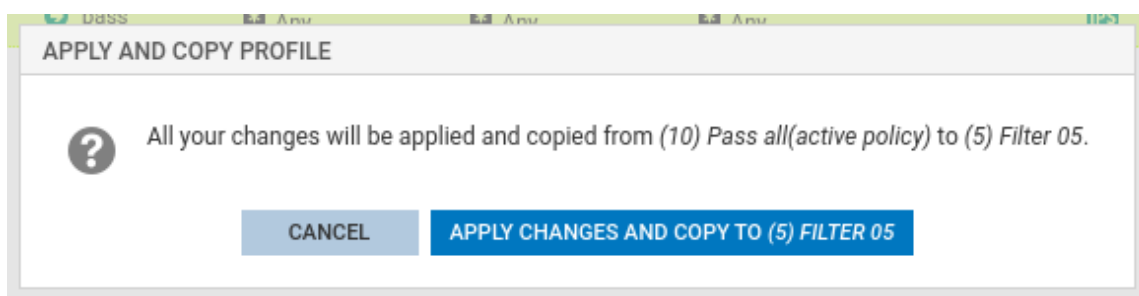
## Translation d'adresses

On désactive les routes statiques

**STATIC ROUTES**

Status	Destination network (ho...	Interface	Address range	Gateway
off	Lan_in_B	out	192.168.2.0/24	Fw_B

On copie la politique Pass all et on renomme ensuite la copie.



On fait, dans l'ordre de ces questions : (Non, pas dans l'ordre, voir plus en bas la raison)

3. Ajoutez une règle de NAT afin que les machines de vos réseaux internes puissent accéder au réseau externe sans que leur IP privée n'y soit vue. Ensuite, testez l'accès au réseau externe et l'accès à internet depuis votre poste (l'accès à internet est possible via la passerelle 192.36.253.1 si la translation est correctement configurée).
4. Vous disposez de 2 adresses IP publiques supplémentaires « 192.36.253.x2 » et « 192.36.253.x3 » réservées respectivement à vos serveurs FTP et MAIL situés en DMZ. Ajoutez les règles de NAT qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.
5. Ajouter une règle de NAT afin que votre serveur WEB situé en DMZ soit joignable grâce à une redirection de port via l'adresse IP publique portée par votre firewall « 192.36.253.x0 ».

On a alors :

			Original traffic (before translation)			Traffic after translation			
			Source	Desti...	Dest. port ↑	Source	Src. port	Destination	Dest. port
1			Network_in	Inte interface	Any	Firewall_out	ephemeral_fw	Any	

Pour la question 4, on crée d'abord les objets srv\_mail\_pub et srv\_ftp\_pub

Object name:	srv_ftp_pub	
IPv4 address:	192.36.253.12	
MAC address:	01:23:45:67:89:ab (optional)	

Object name:	srv_mail_pub	
IPv4 address:	192.36.253.13	
MAC address:	01:23:45:67:89:ab (optional)	

puis la règle

STATIC NAT WIZARD

Objective: Map a private IP address to a public (virtual) IP address.  
For example, map 1 to 1 between a local server and a public IP address.

General

PRIVATE IP ADDRESS

Private host(s):

srv\_ftp\_priv

VIRTUAL (PUBLIC) IP ADDRESS

Virtual host(s):

srv\_ftp\_pub

Only on the interface:

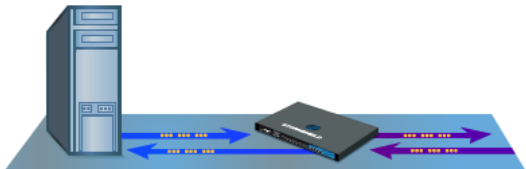
out

ces deux règles ont été crée automatiquement

		Sta...	Original traffic (before translation)			Traffic after translation			
			Source	Desti...	Dest. port	Source	Src. port	Destination	Dest. port
1			Network_ir	Inte interface	Any	Firewall_out	ephemeral_fw	Any	
2			srv_ftp_pri	Any interface	Any	srv_ftp_pub			
3			Any interface: out	srv_	Any			srv_ftp_pri	

pareil pour l'autre serveur public

STATIC NAT WIZARD



Objective: Map a private IP address to a public (virtual) IP address.  
For example, map 1 to 1 between a local server and a public IP address.

General

PRIVATE IP ADDRESS

Private host(s):

VIRTUAL (PUBLIC) IP ADDRESS

Virtual host(s):

Only on the interface:

puis la question 5

5			Network_ir	Inte interface	Any	Firewall_out	ephemeral_fw	Any	
NAT par PORT - Question 5 (contains 1 rules, from 6 to 6)									
6			Internet interface: out	Fire	http	Any		srv_web_priv	

on a alors

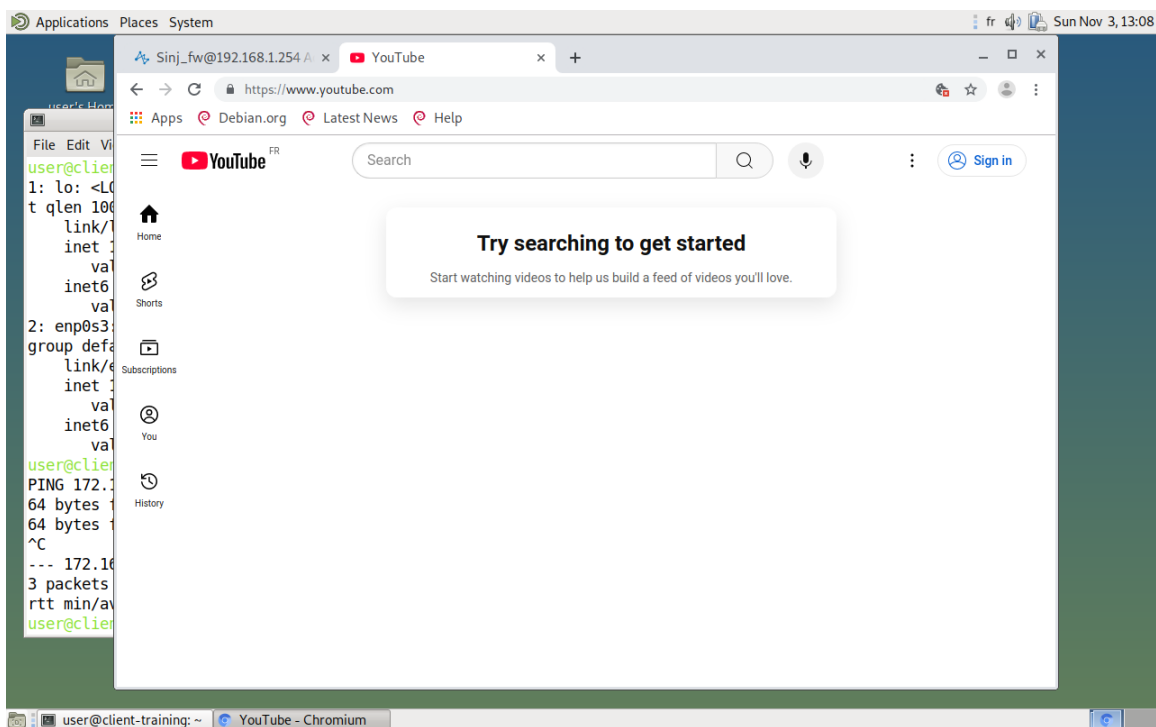
NAT STATIQUE (contains 4 rules, from 1 to 4)									
1			srv_ftp	Internet interface: out	Any	srv_ftp_f			
2			Interne interface: ou	Any	Any	srv_ftp_put		srv_ftp_	
3			srv_ma	Internet interface: out	Any	srv_mail			
4			Interne interface: ou	Any	Any	srv_mail_pi		srv_mai	NAT inside IPSe...
NAT DYNAMIQUE (contains 1 rules, from 5 to 5)									
5			Networ	Internet interface: out	Any	Firewall_out	ephemera	Any	
NAT STATIQUE PAR PORT (contains 1 rules, from 6 to 6)									
6			Interne	Firewall_out	Any	Any	http	srv_web	





En suivant l'ordre des questions, le filtrage NAT ne fonctionnait pas, j'ai donc recommencé en commençant d'abord par les filtres NAT STATIQUES de la question 4, puis le NAT DYNAMIQUE de la question 3 et enfin par celui de la question 5.

## Test d'accès à un site en https



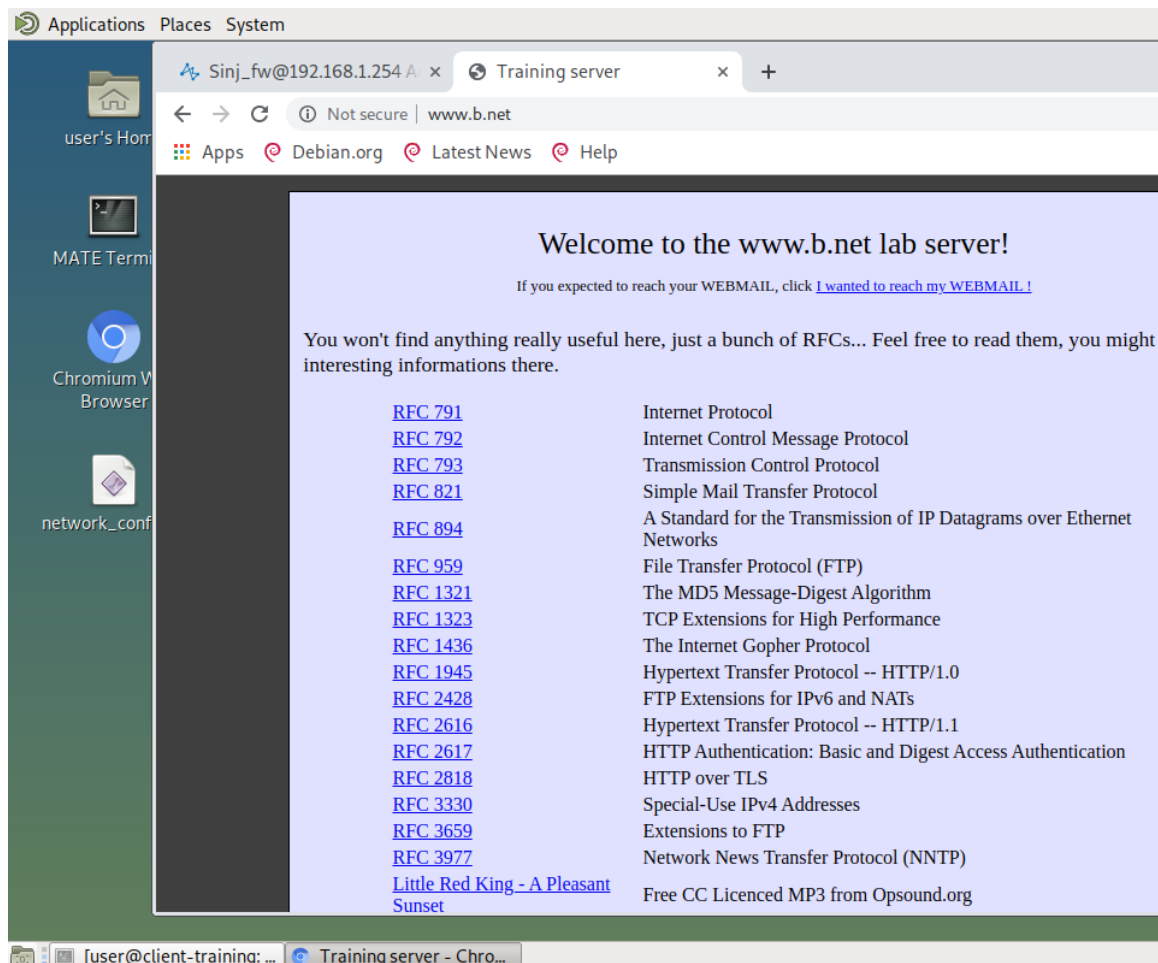
Test d'accès au serveur Web de l'entreprise B (lancer la VM Debian-Training-Webmail-DMZ1-X au préalable)

```
Debian-Training-Webmail-DMZ-A [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Stopping DNS forwarder and DHCP server: dnsmasq.
Starting DNS forwarder and DHCP server: dnsmasq.

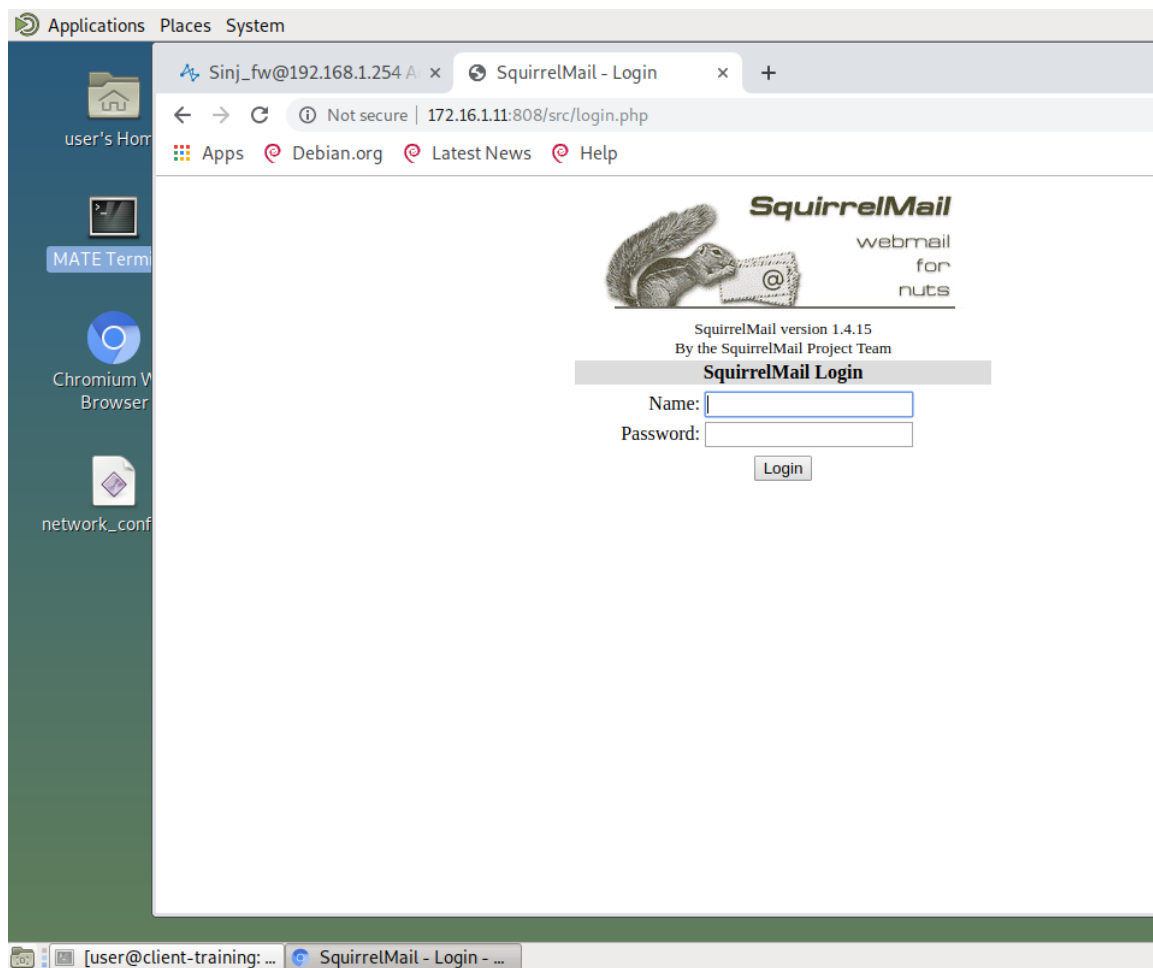
Your WEB server is "www.a.net" on 172.16.1.11
Your FTP server is "ftp.a.net" on 172.16.1.12
Your DNS server is on 172.16.1.10
Your DOMAIN NAME is a.net
Your MAIL server is "mail.a.net" on 172.16.1.13
Your WEBMAIL server is "webmail.a.net" on 172.16.1.11:808
Your USERNAME for mails is "user" and his password is "user"
The administrator of this server is "root" with password "root"

[ 324.023392] ip_tables: (C) 2000-2006 Netfilter Core Team
[ 324.031407] nf_conntrack version 0.5.0 (2048 buckets, 8192 max)

#####
# "kb [ fr us be de it ... ]" will remap your keyboard easily #
#####
*** IF YOU NEED TO CHANGE THE CONFIGURATION OF THIS VM, ***
*** PLEASE READ THE /root/README.conf.txt. ***
debianformation:~# kb fr
Loading /usr/share/keymaps/i386/azerty/fr.kmap.gz
debianformation:~#
debianformation:~# _
```



Test d'accès au serveur webmail



## Filtrage

Création de règles de filtrage du Réseau In vers serveurs de la DMZ

(5) entreprise_A								
Edit Export								
FILTERING NAT								
Searching...								
+ New rule X Delete								
Status Action Source Destination Dest. port Protocol Security in								
In vers DMZ - Question 1 (contains 5 rules, from 1 to 5)								
1	on	pass	Network_in	srv_dns_priv	dns	IPS		
2	on	pass	Network_in	srv_web_priv	http	IPS		
3	on	pass	Network_in	srv_web_priv	webmail	IPS		
4	on	pass	Network_in	srv_ftp_priv	ftp	IPS		
5	on	pass	Network_in	srv_mail_priv	smtp	IPS		

On s'occupe dorénavant des traffics sortants :

2. Votre réseau interne, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (test avec [www.visitkorea.or.kr](http://www.visitkorea.or.kr)).
3. L'accès au site <https://www.cnn.com> doit être bloqué depuis le réseau interne, en utilisant un objet FQDN.
4. Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine (pc\_200) est 192.168.x.200.
5. Votre réseau interne doit pouvoir joindre les serveurs FTP et Web de l'autre entreprise.
6. Votre réseau interne doit pouvoir émettre un ping vers n'importe quelle destination.
7. Seul votre serveur DNS interne (172.16.x.10) est autorisé à résoudre vers l'extérieur.
8. Votre serveur de messagerie peut envoyer des mails vers le serveurs publié par l'autre entreprise.

2.

**DESTINATION**

GENERAL **GEOLOCATION / REPUTATION** ADVANCED PROPERTIES

Geolocation

Select a region: Corée du Sud

6	<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> block	Network_in	Internet geo Corée du Sud	http https	IPS
7	<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> pass	Network_in	Internet	http https	IPS

3. Création de l'objet FQDN, on appuie sur la loupe pour la résolution DNS.

**Host**

**FQDN DNS name (FQDN)**

**Network**

**IP address range**

Object name:

Default IPv4 address:

Comments:

8	<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> block	Network_in	FQDN www.cnn.com	https	
---	--	---	------------	------------------	-------	--

l'agencement des règles doit être fait de la manière suivante :

Traffics sortants (contains 3 rules, from 6 to 8)						
6			block	Network_in	Internet geo Corée du Sud	http https
7			block	Network_in	www.cnn.com	http
8			pass	Network_in	Internet	http https

les règles particulières avant les règles générales.

4. On crée d'abord l'objet pc\_200 (192.168.1.200)

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

IP address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name:

pc\_200

IPv4 address:

192.168.1.200

MAC address:

01:23:45:67:89:ab (optional)

Resolution

☒ None (static IP)

☐ Automatic

Comments:

on block pc\_200 Any ftp

5.

10 on pass Network\_in srv\_ftp\_b ftp

inutile de créer l'autre car la règle de la question 2, naviguer sur les sites web en https et http est active.

6.

EDITING RULE NO 10

General

Action

Source

Destination

Port - Protocol

Inspection

PORT AND PROTOCOL

Port

Destination port:

+ Add

✕ Delete

Any

Protocol

Protocol type: IP protocol

Application protocol: No applicative analysis

IP protocol: icmp

ICMP message: Echo request (Ping)

☒ Stateful tracking

10	<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> pass	Network_in	Any	Any	icmp (Echo req	IPS
----	--	--	------------	-----	-----	----------------	-----

7.

11	<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> pass	srv_dns_priv	Internet	dns_udp	dns	IPS
----	--	--	--------------	----------	---------	-----	-----

8.

14	<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> pass	srv_mail_priv	Internet	smtp		IPS
----	--	--	---------------	----------	------	--	-----

Les traffics entrant désormais :

## Trafics entrants :

9. L'autre entreprise peut joindre vos serveurs Web et FTP ; ces événements doivent être tracés.
10. Le serveur mail de l'autre entreprise est autorisé à transmettre des e-mails à votre serveur de messagerie.
11. L'autre entreprise est autorisée à pinger l'interface externe de votre firewall; ce type d'événement doit lever une alarme mineure.
12. L'autre entreprise peut se connecter à votre firewall : via l'interface web et en SSH. Ce type d'événement doit lever une alarme majeure.

9. Pour le serveur web

Pour tracer les événements :

General  
**Action**  
Source  
Destination  
Port - Protocol  
Inspection

**ACTION**  
GENERAL QUALITY OF SERVICE ADVANCED PROPERTIES  
General  
Action: pass  
Log level: verbose  
Scheduling: standard (connection log)  
verbose (Filtering log)  
minor alarm  
major alarm  
Routing  
Gateway - router:

15 on pass Internet Firewall\_out http

Pour le serveur ftp

16 on pass Internet srv\_ftp\_pub ftp IPS

10.

17 on pass Internet srv\_mail\_priv smtp IPS

11.

## ACTION

### GENERAL

### QUALITY OF SERVICE

### ADVANCED PROPERTIES

#### General

Action:

Log level:

Scheduling:

Routing:

#### Gateway - router:

☐ on ☐ pass ☐ Internet ☐ Firewall\_out ☐ Any ☐ icmp (Echo request) ☐ IPS

12.

19 ☐ on ☐ pass ☐ Internet ☐ Firewall\_out ☐ ssh ☐ https ☐ IPS

Pour permettre à l'autre entreprise de se connecter via https

## SYSTEM / CONFIGURATION

### GENERAL CONFIGURATION

### FIREWALL ADMINISTRATION

### NETWORK SETTINGS

#### Access to the firewall's administration interface

Listening port:

☒ Allow the 'admin' account to log in

[Configure the SSL certificate of the service](#)

☒ Enable protection from brute force attacks

Number of authentication attempts allowed:

Freeze time (minutes):

#### ACCESS TO FIREWALL ADMINISTRATION PAGES

+ Add X Delete

Authorized administration host (host or group - network - address range)

network\_internals

Fw\_B

On a alors, au final :



IN vers DMZ - Question 1 (contains 6 rules, from 1 to 6)									
1				Network_in	srv_dns_priv	dns			IPS
2				Network_in	srv_web_priv	http			IPS
3				Network_in	srv_web_priv	webmail			IPS
4				pc_200	Any	ftp			IPS
5				Network_in	srv_ftp_priv	ftp			IPS
6				Network_in	srv_mail_priv	smtp			IPS

Traffics sortants (contains 8 rules, from 7 to 14)									
7				Network_in	Internet geo Corée du Sud	http https			IPS
8				Network_in	www.cnn.com	http			IPS
9				Network_in	Internet	http https			IPS
10				Network_in	srv_ftp_b	ftp			IPS
11				Network_in	srv_web_b	http https			IPS
12				Network_in	Any	Any	icmp (Echo request		IPS
13				srv_dns_priv	Internet	dns_udp dns			IPS
14				srv_mail_priv	Internet	smtp			IPS

Traffics entrants (contains 5 rules, from 15 to 19)									
15				Internet	Firewall_out	http			IPS
16				Internet	srv_ftp_pub	ftp			IPS
17				Internet	srv_mail_priv	smtp			IPS
18				Internet	Firewall_out	Any	icmp (Echo request		IPS
19				Internet	Firewall_out	ssh https			IPS

## Filtrage de contenu (HTTP et HTTPS)

On sélectionne la base de donnée embarquée

## OBJECTS / WEB OBJECTS

URL	CERTIFICATE NAME (CN)	GROUPS OF CATEGORIES	URL DATABASE
URL database provider :		Embedded URL database	
Embedded URL database			
Category	Comments		
academic	Université et Enseignement Supérieur		

www.facebook.com est classée dans la catégorie 'online'

»

★

⚙

🔍

👤

🔗

🛡

📺

📢

📁

👤

OBJECTS / WEB OBJECTS

URL

CERTIFICATE NAME (CN)

GROUPS OF CATEGORIES

URL DATABASE

Add a customized category

Remove

👁 Check usage

www.facebook.com

1

Classify

URL category

Comments

vpnsst\_owa

antivirus\_bypa...

authentication...

Authorized characters

Authorized characters: '\*' '?' ']' '[' '-' '.' [a-z] [A-Z] [0-9]

Example: www.google.com/\* or \*.yahoo.com/\*

URL CATEGORY: VPNSST\_OWA

Add a URL Remove

URL

schemas.microsoft.com/\*

www.w3.org/TR/\*

Page 1 of 1

URL categories: www.facebook.com

online

www.home.barclays est classée dans la catégorie 'bank' et www.mozilla.org dans la catégorie 'it'.

On a par la suite modifier la page de blocage de notre choix



Nous allons désormais créer une politique de filtrage URL et SSL qui nous permettre d'accéder à tous les sites web sauf ceux listé auparavant, tout en s'assurant de toujours pouvoir rejoindre le site [www.bbc.com](http://www.bbc.com)

On a donc créer une White List, où on va répertorier les sites joignables, [www.bbc.com](http://www.bbc.com) dans notre cas.

1

URL **CERTIFICATE NAME (CN)** GROUPS OF CATEGORIES URL DATABASE

Add a customized category Remove Check usage

Certificate name (CN) category	Comments
White_list	
proxyssl_bypass	

2

Authorized characters  
 ' ' [a-z] [A-Z] [0-9] and \* are allowed  
 The character \* is only valid if placed at the end followed by a dot.

3

WHITE\_LIST

Add a certificate name Remove

Certificate name (CN) ▲

\*.bbc.com

puis une Black List pour les sites web non voulu

## OBJECTS / WEB OBJECTS

URL **CERTIFICATE NAME (CN)** GROUPS OF CATEGORIES URL DATABASE

Add a customized category | Remove | Check usage

Certificate name (CN) category	Comments
Black_list	
White_list	
proxysl_bypass	

**Authorized characters**  
 ' ' [a-z] [A-Z] [0-9] and '\*' are  
 The character '\*' is only valid  
 followed by a dot.

**BLACK\_LIST**

Add a certificate name Remove

Certificate name (CN) ▲
*.mozilla.org
*.home.barclays
*.facebook.com

Sans oublier de toucher le filtrage SSL

### SECURITY POLICY / SSL FILTERING

(0) SSLFilter\_00 | Edit | URL database provider: [Embedded URL database](#)

+ Add | X Delete | Up | Down | Cut | Copy | Paste | + Add all predefined categories

	Status	Action	URL - CN	Comments
1	on	Pass without decrypting	White_list	
2	on	Block without decrypting	Black_list	
3	on	Block without decrypting	shopping	
4	on	Block without decrypting	news	
5	on	Pass without decrypting	Any	

On modifie également le filtrage URL

### SECURITY POLICY / URL FILTERING

(0) URLFilter\_00 | Edit | URL database provider: [Embedded URL database](#)

+ Add | X Delete | Up | Down | Cut | Copy | Paste | + Add all predefined categories

	Status	Action	URL category	Comments
1	off	Pass	authentificati...	authorize the URLs of authentication_bypass group
2	on	BlockPage_00	shopping	
3	on	BlockPage_00	news	
4	on	Pass	any	default rule (pass all)

