

---

# Lab 5 – Filtrage

## Table des matières :

1. Accès interne vers la DMZ.....	2
2. Navigation Internet restreinte (blocage géographique).....	3
3. Blocage d'un site spécifique par FQDN.....	5
4. Accès FTP sortant.....	6
5. Interdiction FTP pour un poste spécifique.....	7
6. Autorisation Ping sortant.....	8
7. Accès SSH vers d'autres firewalls.....	9
8. Restriction DNS sortant au seul serveur interne.....	10
9. Envoi de mails par le serveur SMTP.....	11
10. Accès entrant Web et FTP tracé.....	12
11. Réception d'e-mails entrants.....	13
12. Ping externe sur interface OUT + alarme mineure.....	14
13. Accès SSH et Web sur le firewall + alarme majeure.....	15
14. Vérification et tests des flux.....	16

# 1. Accès interne vers la DMZ

- Dans cette étape, je configure des règles de filtrage pour autoriser le réseau interne 192.168.y.0/24 à accéder aux serveurs de la DMZ (DNS, WEB — ports 80 et 808 pour le webmail — FTP et SMTP).

internal traffic IN to DMZ (contient 6 règles, de 1 à 6)						
1						
2						
3						
5						
6						

## 2. Navigation Internet restreinte (blocage géographique)

- Je configure une règle permettant l'accès HTTP et HTTPS à Internet, tout en bloquant les connexions vers les sites situés en République de Corée (ex. www.visitkorea.or.kr).

EDITION DE LA RÈGLE N° 1

Général  
Action  
Source  
Destination  
Port / Protocole  
Inspection

**DESTINATION**

GENERAL   **GEOLOCALISATION / REPUTATION**   CONFIGURATION AVANCEE

Général

Machines destinations:

+ Ajouter   x Supprimer

internet

EDITION DE LA RÈGLE N° 1

Général  
Action  
Source  
Destination  
Port / Protocole  
Inspection

**DESTINATION**

GENERAL   **GEOLOCALISATION / REPUTATION**   CONFIGURATION AVANCEE

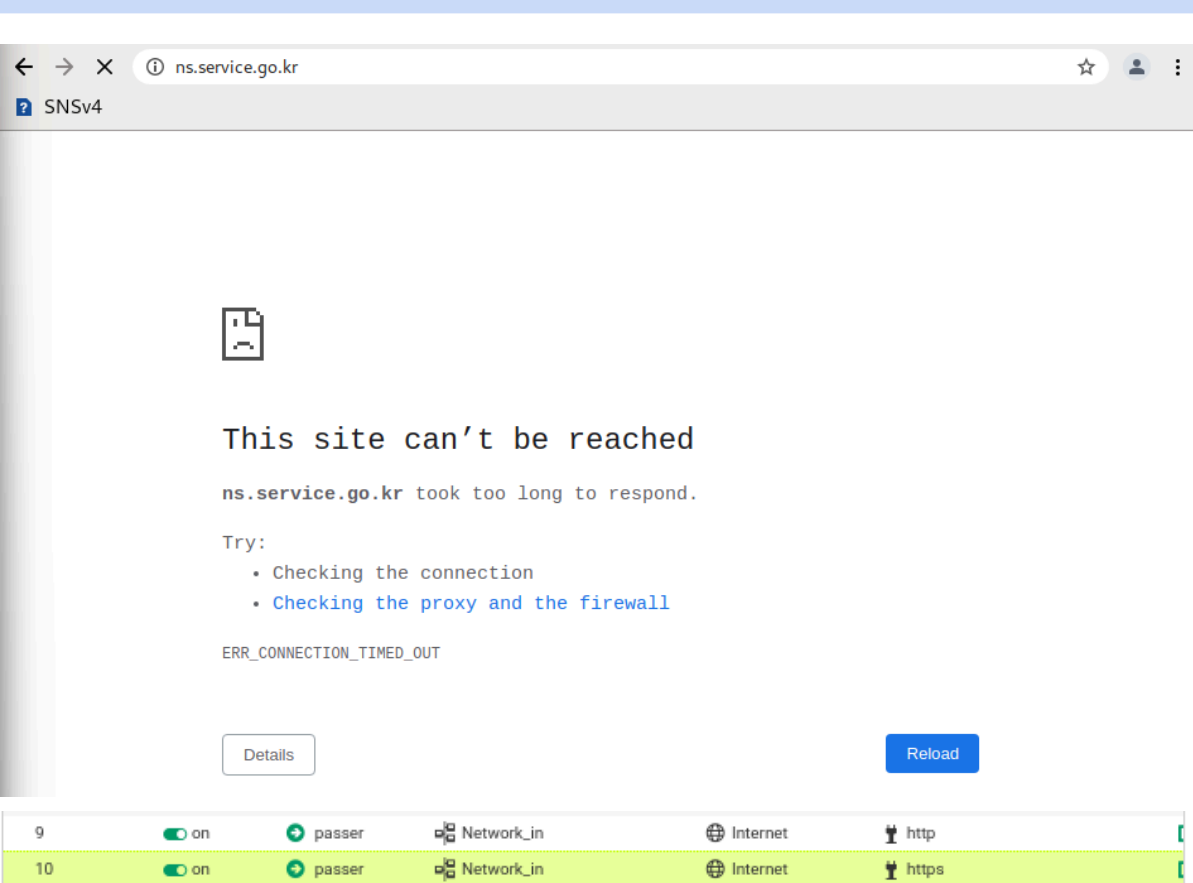
Géolocalisation

Sélectionnez une région: Corée du Sud





Réputation des adresses IP publiques





Sélectionnez une catégorie de réputation:

1   on   bloquer   Network\_in   Internet geo Corée du Sud   http https



The screenshot shows a web browser window with the address bar containing "ns.service.go.kr". The page displays an error message: "This site can't be reached" followed by "ns.service.go.kr took too long to respond." Below this, it says "Try:" and lists two suggestions: "Checking the connection" and "Checking the proxy and the firewall". The error code "ERR\_CONNECTION\_TIMED\_OUT" is visible. At the bottom of the page, there are two buttons: "Details" and "Reload".

9  on  passer  Network\_in  Internet  http

10  on  passer  Network\_in  Internet  https

### 3. Blocage d'un site spécifique par FQDN

- Je mets en place une règle qui empêche l'accès au site <https://www.cnn.com> depuis le réseau interne, en utilisant un objet FQDN.

**PROPRIÉTÉS**

Nom de l'objet:

Adresse IPv4 par défaut:

Commentaire:

---


2  on  bloquer  Network\_in  www.cnn.com  http  https

---

VMSNSX09K0639A9@19 x www.cnn.com x +

← → X ⓘ cnn.com ☆ 👤 ⋮

SNSv4



**This site can't be reached**

www.cnn.com took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR\_TIMED\_OUT

## 4. Accès FTP sortant

- Je permets aux postes internes de se connecter aux serveurs FTP sur Internet.



## 5. Interdiction FTP pour un poste spécifique

- Je bloque l'accès FTP pour la machine du stagiaire (192.168.y.200) tout en laissant les autres postes accéder au FTP.

internal traffic IN to DMZ (contient 2 règles, de 1 à 2)						
1				Network_in	srv_ftp_priv_A	ftp
2				pc_200	Any	ftp

## 6. Autorisation Ping sortant

- Je configure le firewall pour autoriser le ping (ICMP) vers Internet.

Outgoing traffic (contient 6 règles, de 7 à 12)							
7		on	bloquer	Network_in	Internet geo Corée du Sud	http https	
8		on	bloquer	Network_in	www.cnn.com	http https	
9		on	passer	Network_in	Internet	http	
10		on	passer	Network_in	Internet	https	
11		on	passer	Network_in	Internet	ftp	
12		on	passer	Network_in	* Any	* Any	icmp (requête Ech

- Test du bon fonctionnement :

```
user@client-training:~$ ping www.ac-nice.fr
PING www.ac-nice.fr.cdn.cloudflare.net (141.101.90.107) 56(84) bytes of data.
64 bytes from 141.101.90.107 (141.101.90.107): icmp_seq=1 ttl=56 time=98.9 ms
64 bytes from 141.101.90.107 (141.101.90.107): icmp_seq=2 ttl=56 time=63.1 ms
64 bytes from 141.101.90.107 (141.101.90.107): icmp_seq=3 ttl=56 time=47.1 ms
```

---

## 7. Accès SSH vers d'autres firewalls

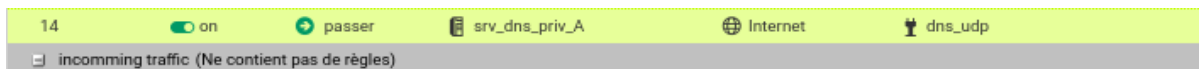
- Je permets aux postes internes d'établir des connexions SSH vers les firewalls distants.



---

## 8. Restriction DNS sortant au seul serveur interne

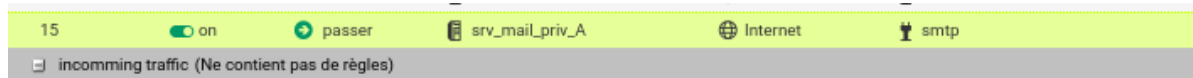
- Seul le serveur DNS interne (172.16.y.10) peut effectuer des requêtes DNS vers l'extérieur.



---

## 9. Envoi de mails par le serveur SMTP

- J'autorise le serveur de messagerie interne à envoyer des mails vers l'extérieur.




## 10. Accès entrant Web et FTP tracé

- J'autorise les réseaux externes à joindre les serveurs Web et FTP internes, et je configure le traçage de ces événements.

incomming traffic (contient 2 règles, de 16 à 17)						
16		<input checked="" type="checkbox"/> on	passer	Internet	Firewall_out	http
17		<input checked="" type="checkbox"/> on	passer	Internet	srv_ftp_pub_A	ftp

## 11. Réception d'e-mails entrants

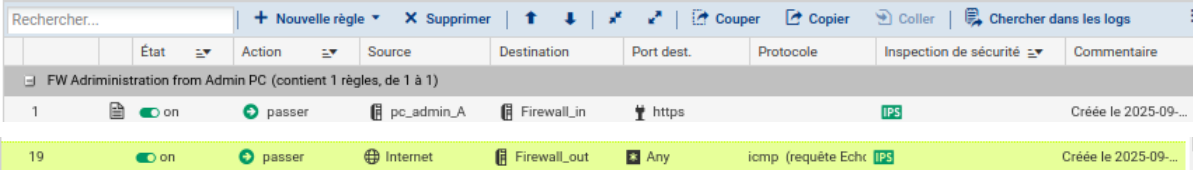
- J'autorise les serveurs de messagerie externes à transmettre des e-mails vers le serveur interne.



incomming traffic (contient 3 règles, de 16 à 18)							
16							
17							
18							

## 12. Ping externe sur interface OUT + alarme mineure

- J'autorise le ping depuis l'extérieur vers l'interface OUT du firewall, avec génération d'une alarme mineure.



Rechercher...	+ Nouvelle règle	X Supprimer	↑ ↓ ↶ ↷	Couper	Copier	Coller	Chercher dans les logs	
État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire	
FW Administration from Admin PC (contient 1 règles, de 1 à 1)								
1	on	passer	pc_admin_A	Firewall_in	https	IPS	Créée le 2025-09-...	
19	on	passer	Internet	Firewall_out	Any	icmp (requête Echx IPS)	Créée le 2025-09-...	

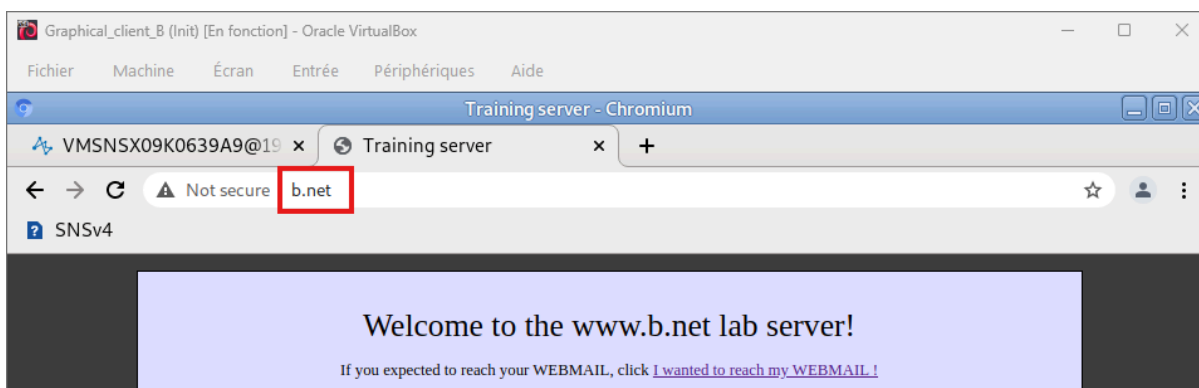
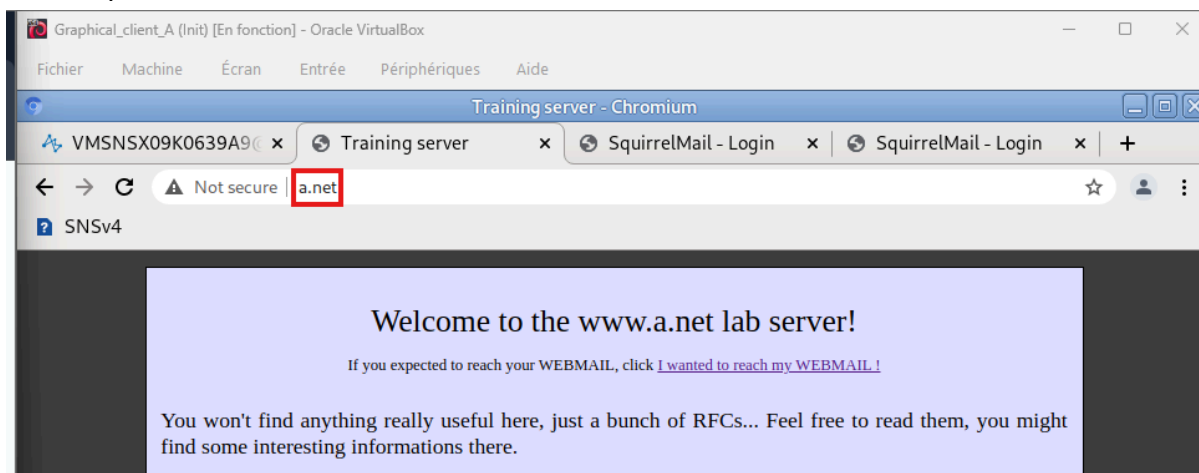
## 13. Accès SSH et Web sur le firewall + alarme majeure

- Les réseaux externes peuvent accéder au firewall via l'interface Web et en SSH, avec levée d'une alarme majeure.

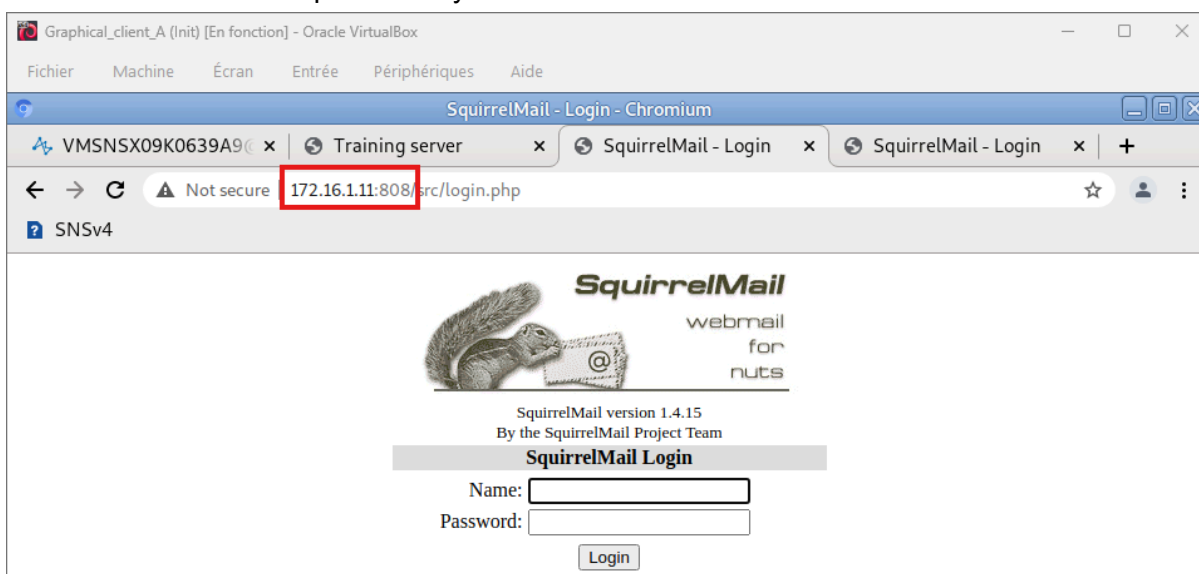


## 14. Vérification et tests des flux

- Je teste tous les trafics sortants et fais tester les trafics entrants par des pairs. Ensuite, je consulte les logs pour confirmer :
  - que chaque flux passe bien par la règle correspondante,
  - que les événements sont bien tracés,
  - que les alarmes se lèvent correctement.



- Accès au webmail : <http://172.16.y.11:808>



Graphical\_client\_B (Init) [En fonction] - Oracle VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

SquirrelMail - Login - Chromium

VMSNSX09K0639A9@19 x Training server x SquirrelMail - Login x +

Not secure 172.16.2.11:8080/src/login.php

SNSv4

**SquirrelMail**  
webmail  
for  
nuts

SquirrelMail version 1.4.15  
By the SquirrelMail Project Team

**SquirrelMail Login**

Name:

Password:

Login

- Utilisateur : user
- Mot de passe : user

**SquirrelMail**  
webmail  
for  
nuts

SquirrelMail version 1.4.15  
By the SquirrelMail Project Team

**SquirrelMail Login**

Name:

Password:

Login

**SquirrelMail**  
webmail  
for  
nuts

SquirrelMail version 1.4.15  
By the SquirrelMail Project Team

**SquirrelMail Login**

Name:

Password:

Login

- Adresses email : user@x.net

The image shows a webmail interface with two main sections. The top section is a composition form for an email. The bottom section is a message list and a preview of the selected email.

**Composition Form:**

- Current Folder: **INBOX** [Sign Out](#)
- Compose [Addresses](#) [Folders](#) [Options](#) [Search](#) [Help](#) [SquirrelMail](#)
- To:
- Cc:
- Bcc:
- Subject:
- Priority: **Normal**  On Read  On Delivery
- 
- Text area:

**Message List and Preview:**

Browser: [SNSv4](#) | Not secure | 172.16.2.11:808/src/webmail.php

Current Folder: **INBOX** [Sign Out](#)  
[Compose](#) [Addresses](#) [Folders](#) [Options](#) [Search](#) [Help](#) [SquirrelMail](#)

Message List | [Delete](#) | [Previous](#) | [Next](#) | [Forward](#) | [Forward as Attachment](#) | [Reply](#) | [Reply All](#)

**Subject:** lab 5 q14  
**From:** user@a.net  
**Date:** Mon, September 29, 2025 12:49 pm  
**To:** user@b.net  
**Priority:** Normal  
**Options:** [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#)

test au bon fonctionnement