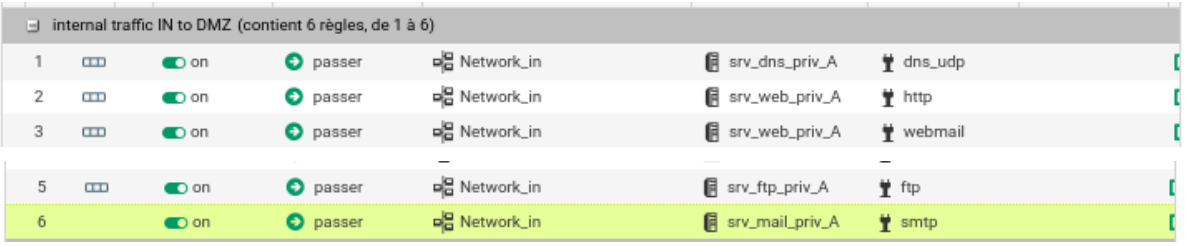
Lab 5 – Filtrage

Table des matières :

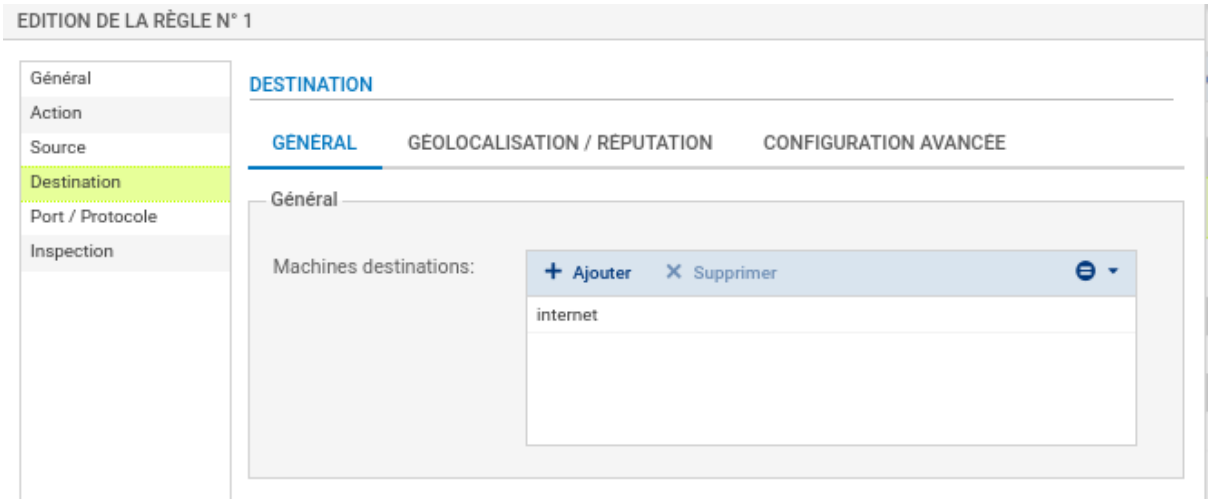
1. Accès interne vers la DMZ

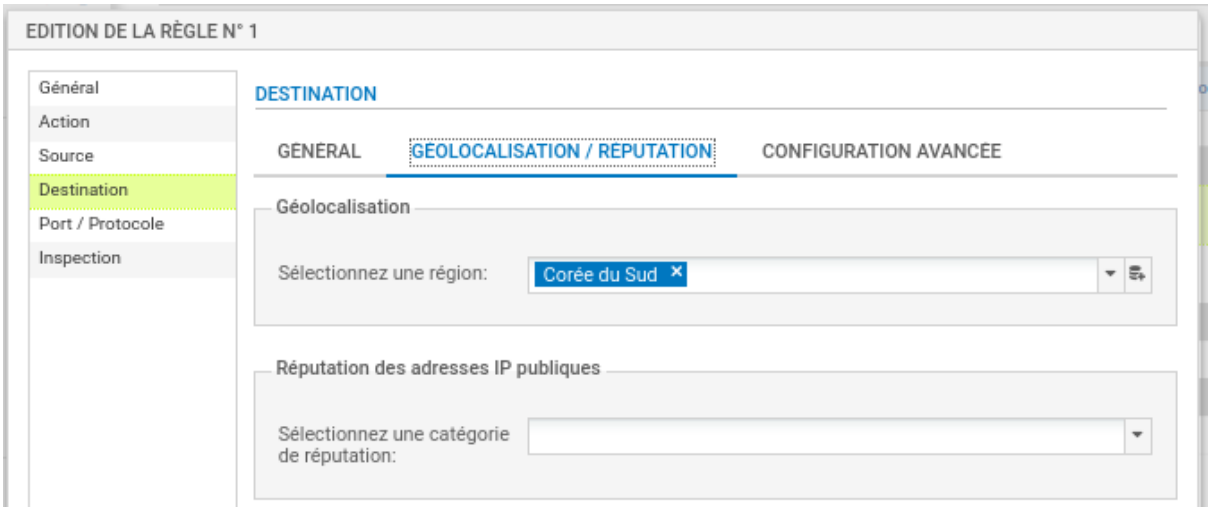
▪ Dans cette étape, je configure des règles de filtrage pour autoriser le réseau interne 192.168.y.0/24 à accéder aux serveurs de la DMZ (DNS, WEB — ports 80 et 808 pour le webmail — FTP et SMTP).

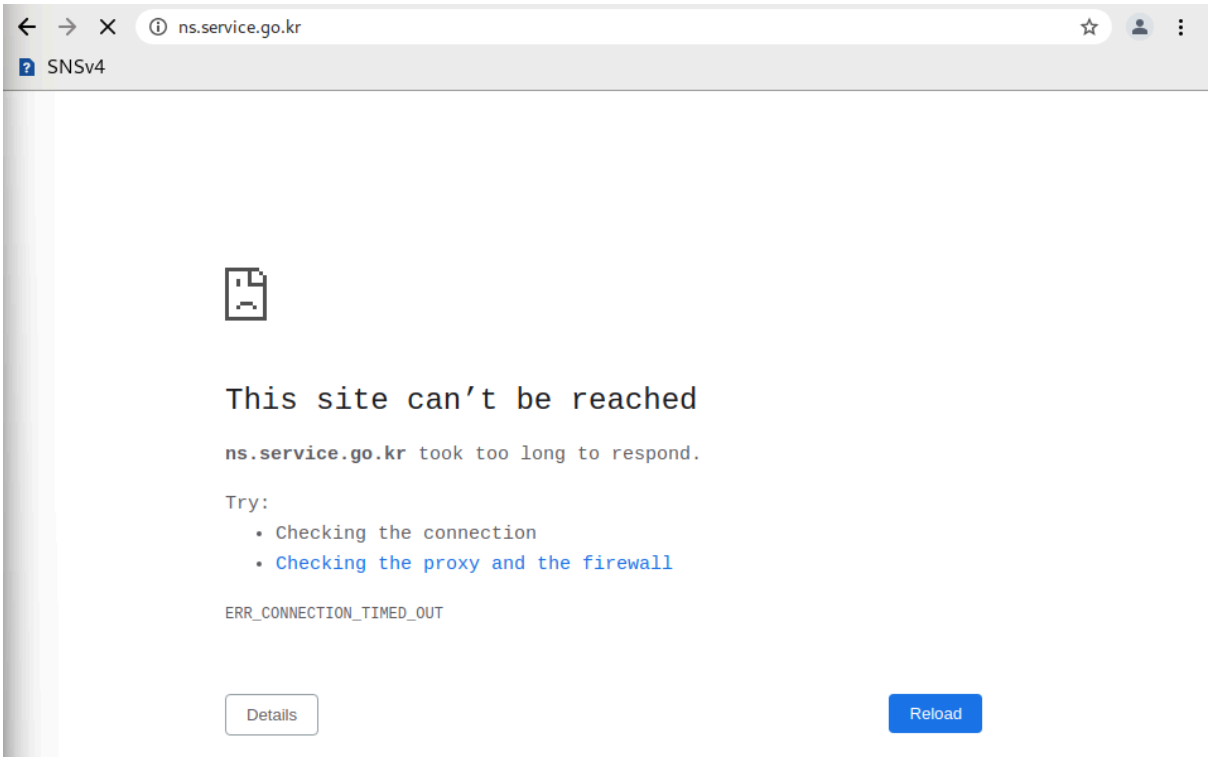


2. Navigation Internet restreinte (blocage géographique)

▪ 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).



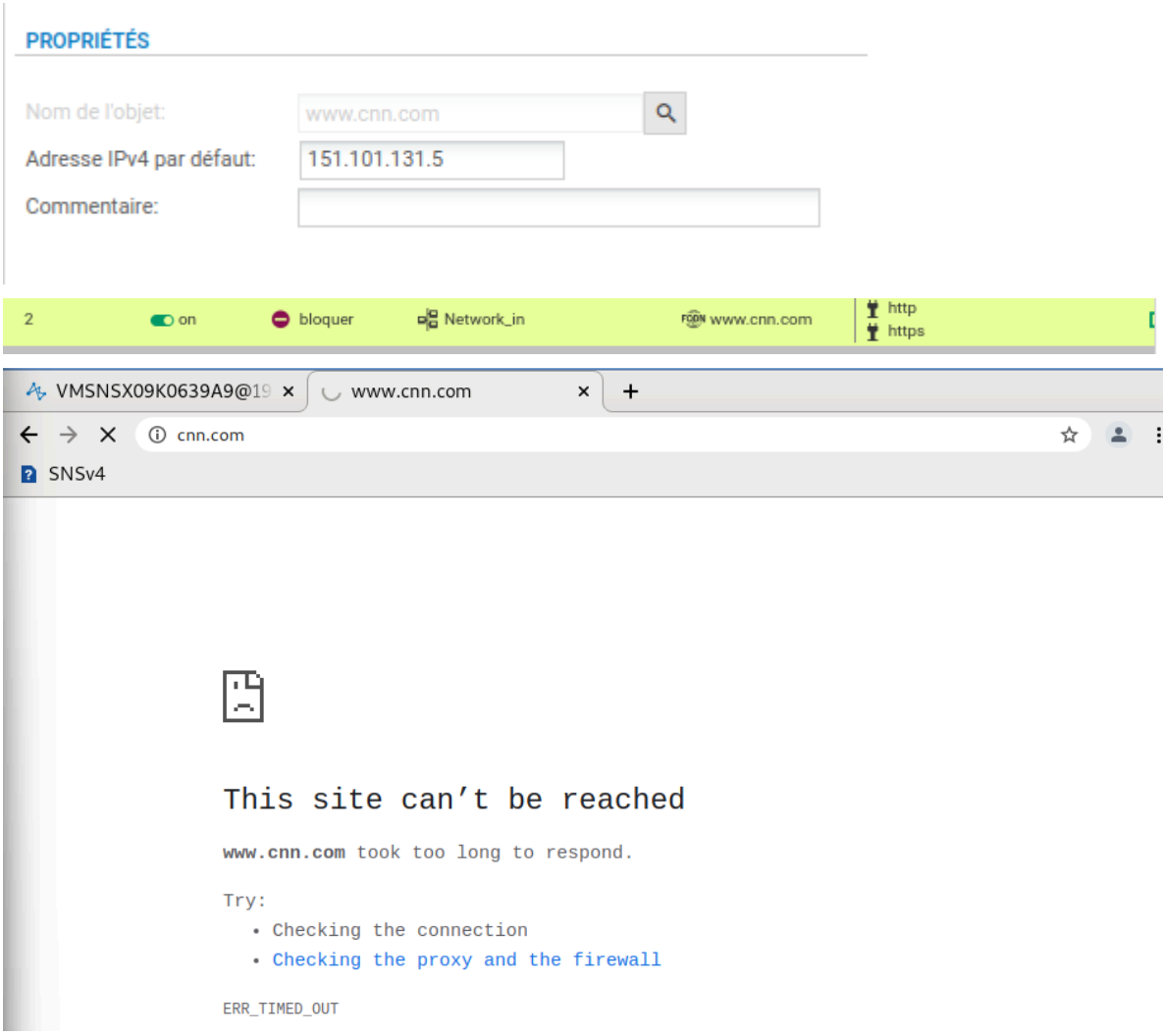




9	on	passer	Network_in	Internet	http	
10	on	passer	Network_in	Internet	https	

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.



4. Accès FTP sortant

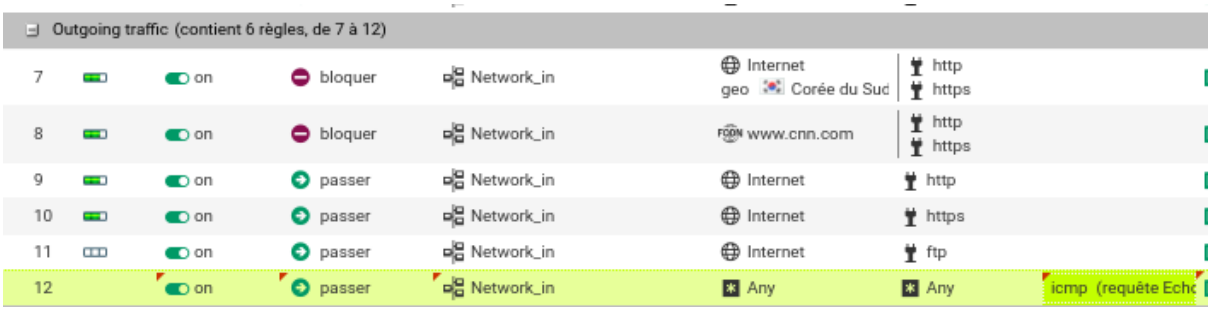
- Je permets aux postes internes de se connecter aux serveurs FTP sur Internet.

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.

6. Autorisation Ping sortant

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



▪ Test du bon fonctionnement :

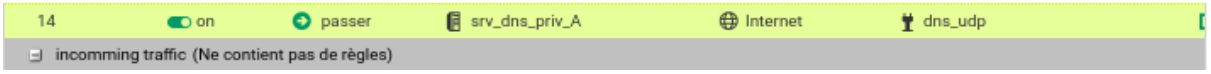
```
user@client-training:~$ ping www.ac-nice.fr
PING www.ac-nice.fr.cdn.cloudflare.net (141.101.90.107) 56(84) bytes of data.
64 bytes from 141.101.90.107 (141.101.90.107): icmp_seq=1 ttl=56 time=98.9 ms
64 bytes from 141.101.90.107 (141.101.90.107): icmp_seq=2 ttl=56 time=63.1 ms
64 bytes from 141.101.90.107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

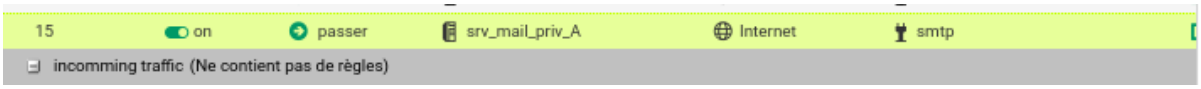
8. Restriction DNS sortant au seul serveur interne

- 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

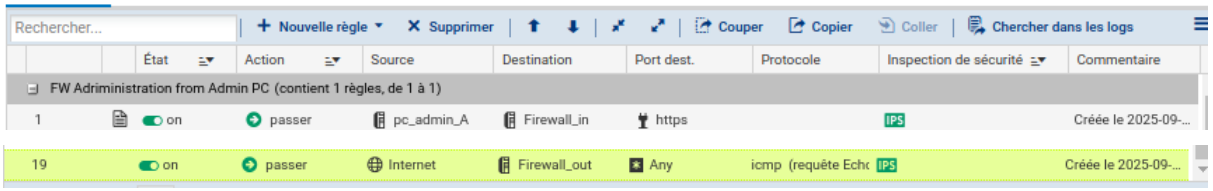
▪ J’autorise les réseaux externes à joindre les serveurs Web et FTP internes, et je configure le traçage de ces événements.

11. Réception d’e-mails entrants

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

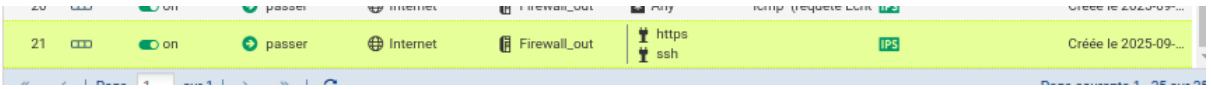
12. Ping externe sur interface OUT + alarme mineure

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



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

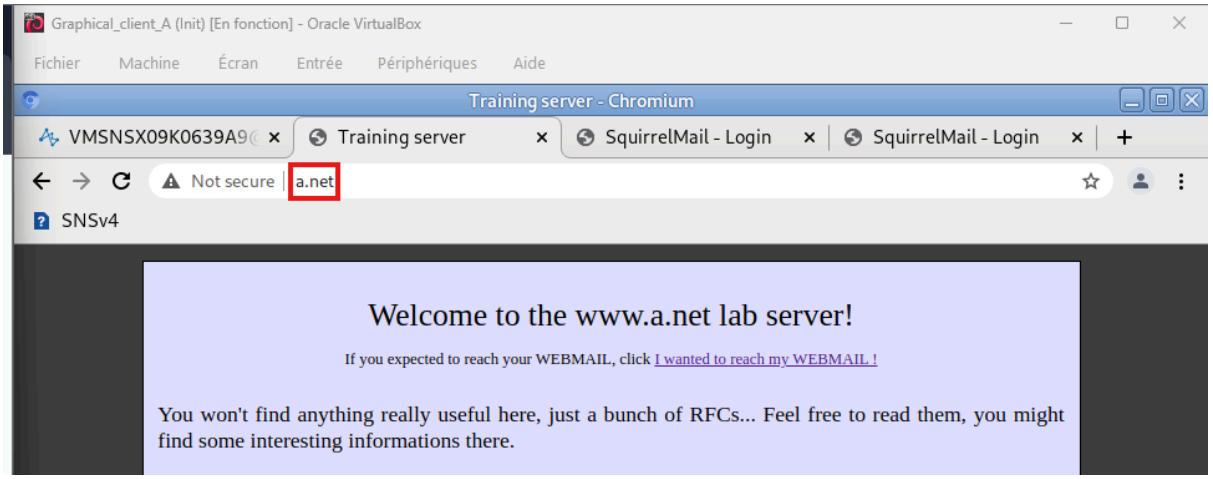
▪ Les réseaux externes peuvent accéder au firewall via l'interface Web et en SSH, avec levée d'une alarme majeure.

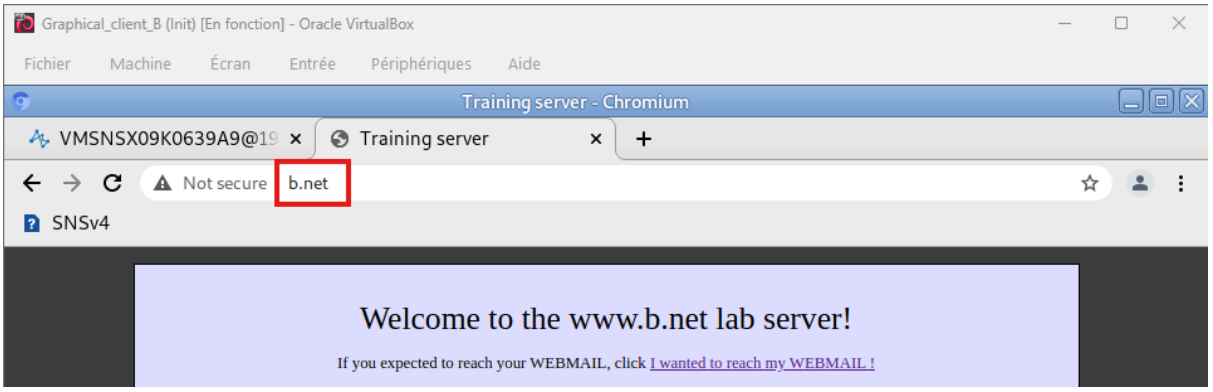


14. Vérification et tests des flux

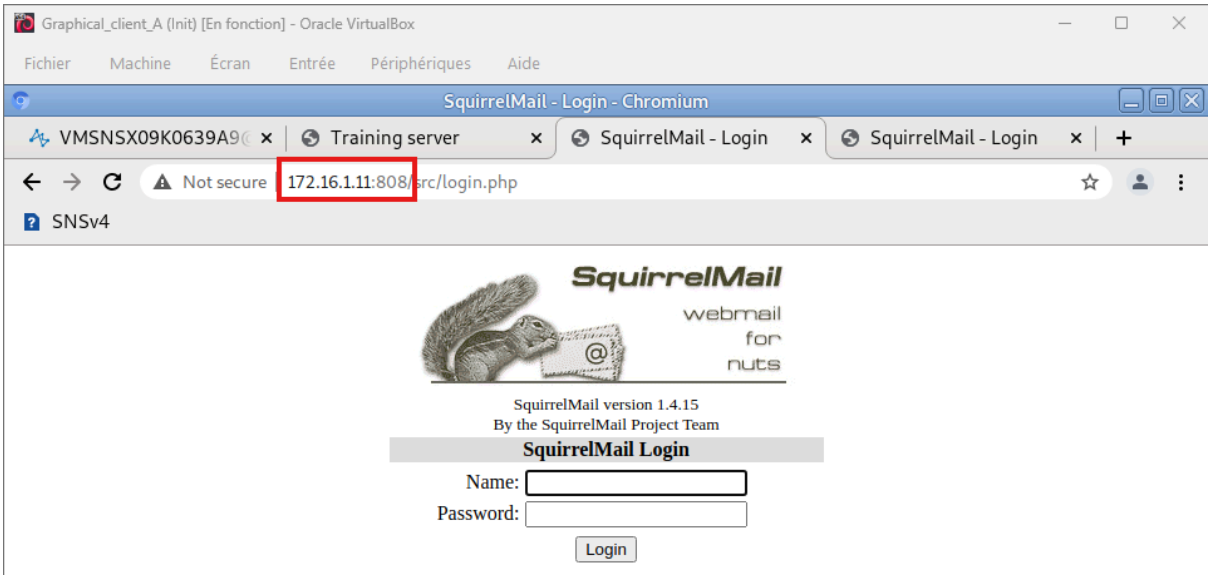
▪ Je teste tous les trafics sortants et fais tester les trafics entrants par des pairs. Ensuite, je consulte les logs pour confirmer :

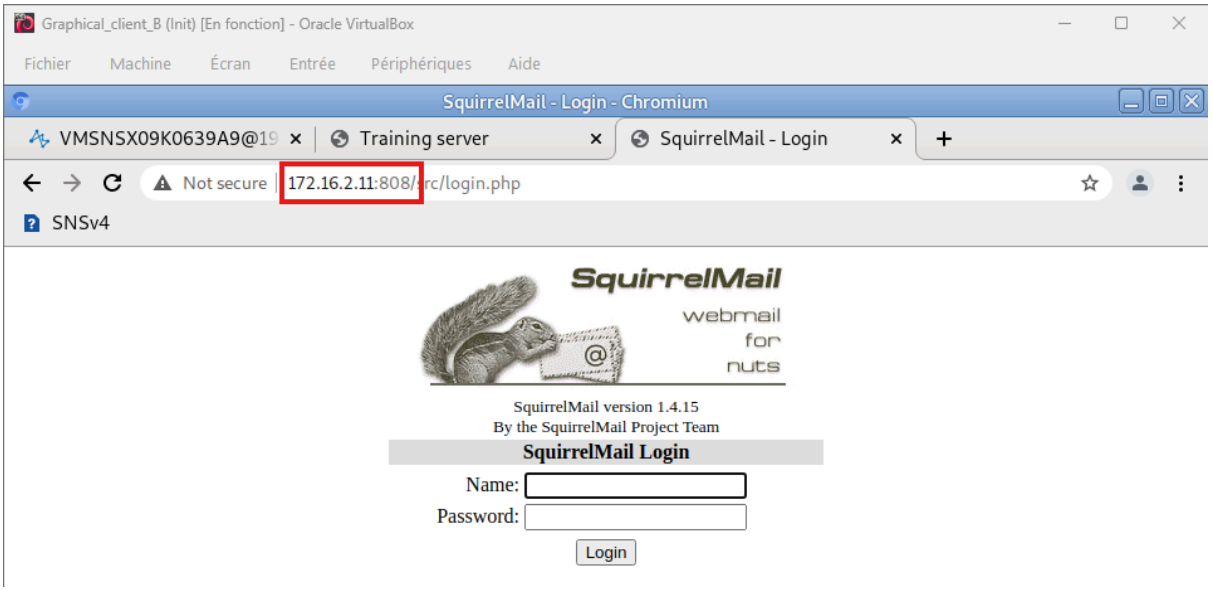
- que chaque flux passe bien par la règle correspondante,
- que les événements sont bien tracés,
- que les alarmes se lèvent correctement.



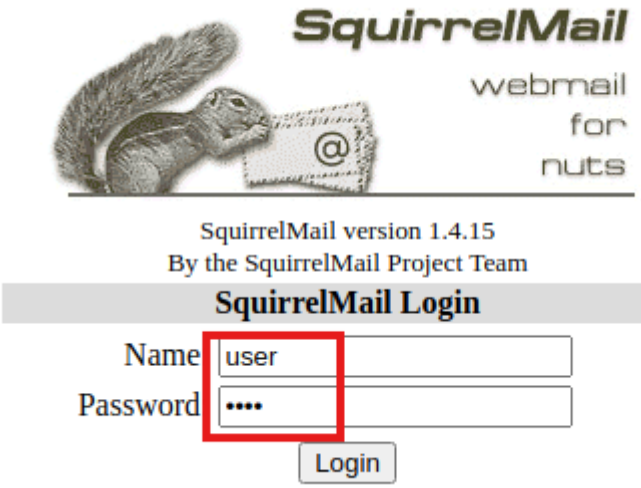


• Accès au webmail : http://172.16.y.11:808





- Utilisateur : user
- Mot de passe : user



• Adresses email : user@x.net