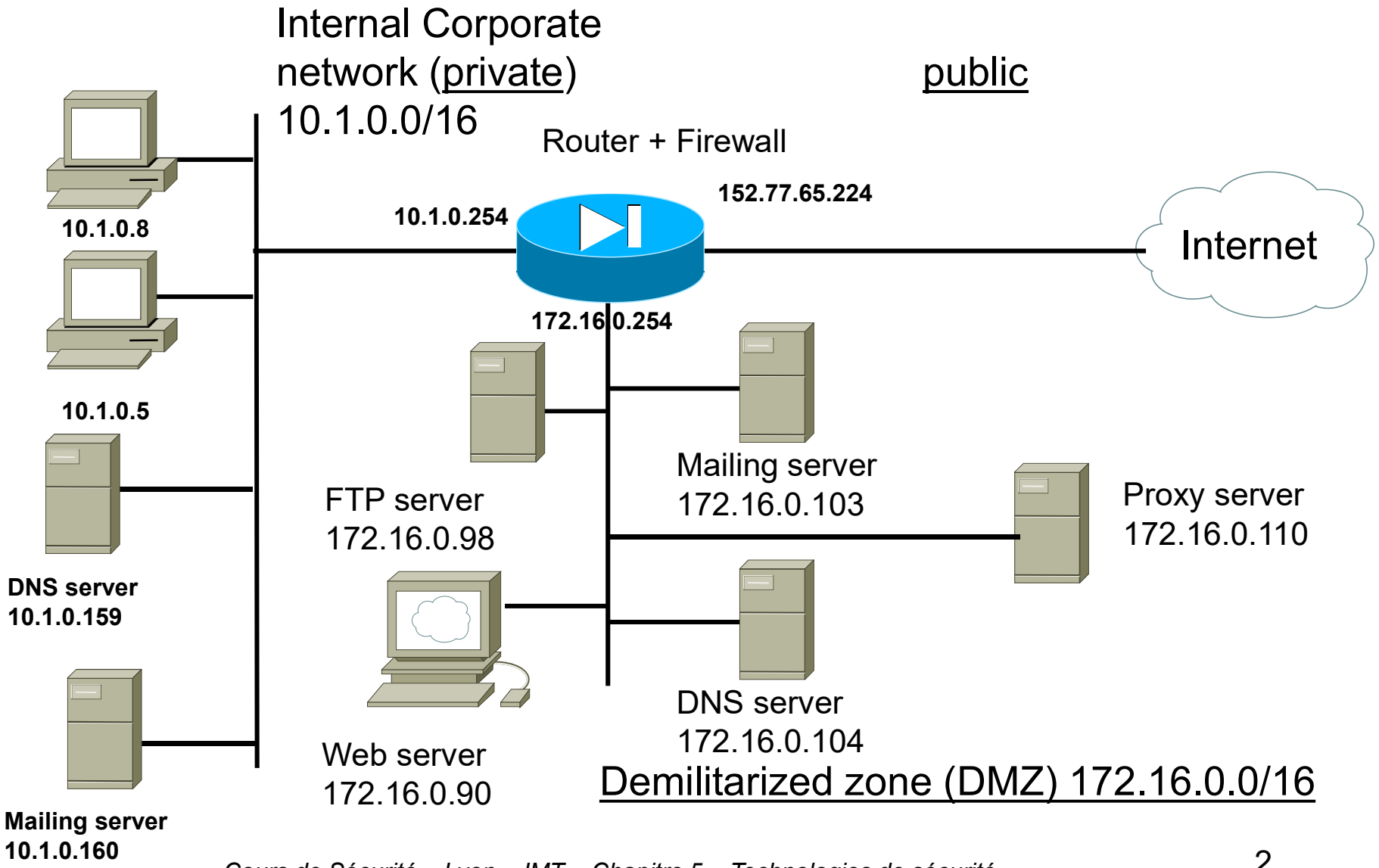
Cours de sécurité
5. Les technologies de sécurité
(sécurité des infrastructures)

A network…


Internal Corporate
network (private)
10.1.0.0/16
public
Router + Firewall
10.1.0.254
152.77.65.224
Internet
172.16.0.254
10.1.0.8
10.1.0.5
DNS server
10.1.0.159
Mailing server
10.1.0.160
FTP server
172.16.0.98
Web server
172.16.0.90
Mailing server
172.16.0.103
Proxy server
172.16.0.110
DNS server
172.16.0.104
Demilitarized zone (DMZ) 172.16.0.0/16

Operation: inspection of each packet

- Source Address
- Destination Address
- Ports

- The decision to authorize or not depends on each inspected point
- Note: fast data processing
- Example of standard ACL on a Cisco router
  - To authorize the packets (permit)
  - To prohibit the packets (deny)

```
access-list 10 permit any 192.168.10.0
access-list 10 permit any 192.168.20.0
access-list 10 deny any 192.168.30.0
```

Pare-feu sans état (*stateless firewall*)

Filtrage de paquets au moyen de règles/listes ACL (Access Control Lists)

- Les données TCP/IP segmentées en paquets
  - Couche 3 du modèle TCP/IP
- Examen du contenu des paquets et application de certaines règles
  - Transmission du paquet
  - Suppression du paquet
- Technologie très répandue au début d'internet
  - Première ligne de défense
- Très utilisée encore dans les routeurs
- Première ligne de défense, combinée à d'autres technologies de pare-feux

Exemples de règles de pare-feu (stateless)

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	Any	Any	192.168.1.0	> 1023	Allow	Rule to allow return TCP Connections to internal subnet
2	192.168.1.1	Any	Any	Any	Deny	Prevent Firewall system itself from directly connecting to anything
3	Any	Any	192.168.1.1	Any	Deny	Prevent External users from directly accessing the Firewall system.
4	192.168.1.0	Any	Any	Any	Allow	Internal Users can access External servers
5	Any	Any	192.168.1.2	SMTP	Allow	Allow External Users to send email in
6	Any	Any	192.168.1.3	HTTP	Allow	Allow External Users to access WWW server
7	Any	Any	Any	Any	Deny	"Catch-All" Rule - Everything not previously allowed is explicitly denied

Pare-feu à états (*stateful firewall*): Les ACL dynamiques

- Filtrage dynamique
  - **Stateful inspection firewall**: les filtres des paquets prennent en considération la couche 4 (TCP, UDP) et vérifient que les paquets sont conformes à la connexion en cours
  - conformité des paquets à une connexion TCP en cours.
  - Entrées dynamiques pour les flux de réponses des connexions TCP, UDP, ICMP
  - Non nécessité de laisser des ports ouverts de manière statique (les ports restent ouverts uniquement le temps de la session)
- Suivi des numéros de séquence TCP
  - Surveillance des numéros de séquence des paquets entrants et sortants pour suivre les flux de communication
  - Protection contre les attaques « man in the middle » et les piratages de session

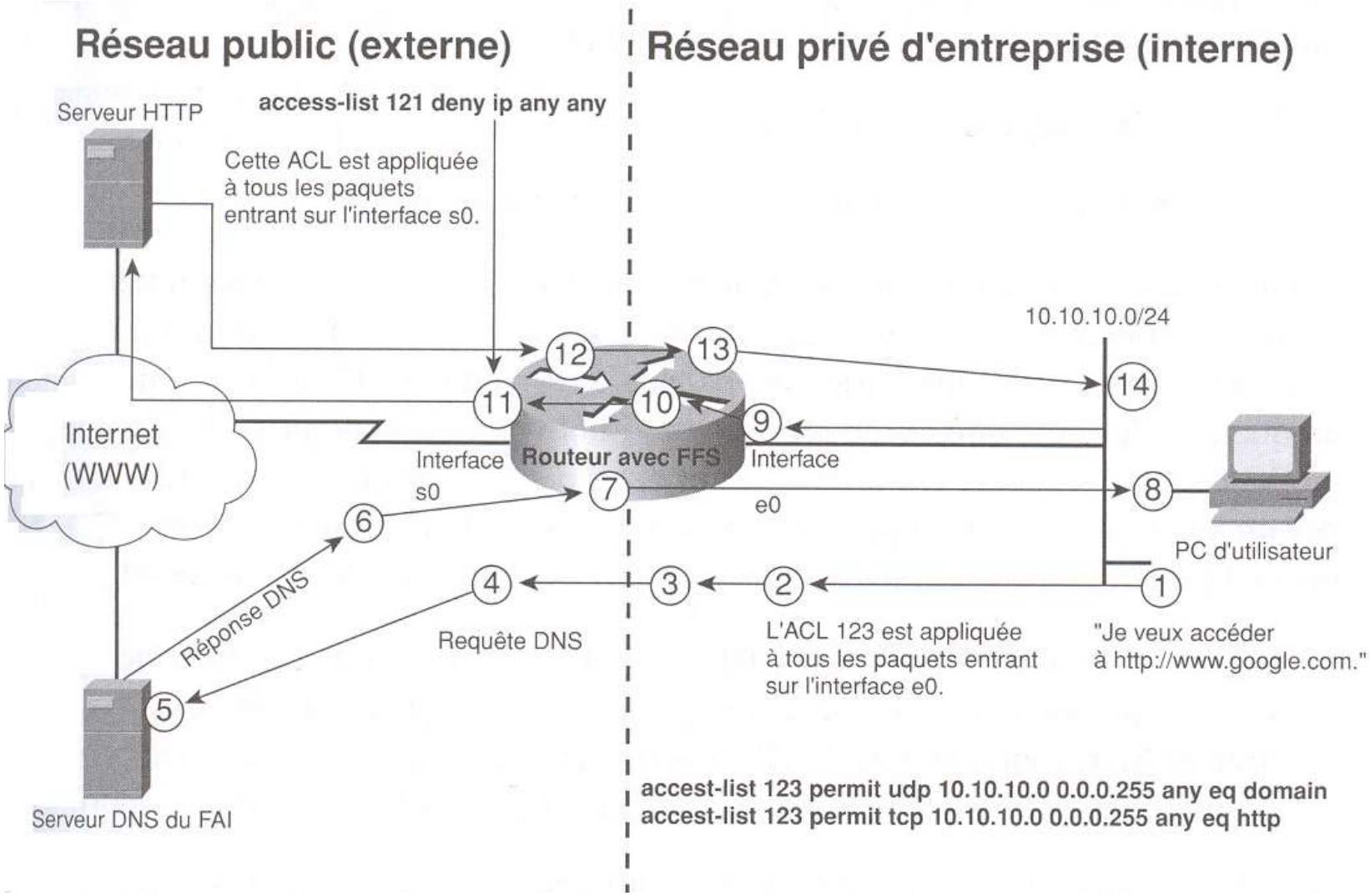
Les ACL dynamiques

- Suivi d'applications spécifiques (exemple de protocoles)
  - CU-SeeMe (port 7648): visioconférence PTP
  - FTP (port 21)
  - H.323 (port 1720): communication multimedia (VoIP, vidéo, audio)
  - ICMP: dépannage de problèmes (administrateur) + utilisé par les pirates => ne laisser passer que les messages ICMP générés à l'intérieur du réseau
  - MCGP (Media Control Gateway Protocol, port 2427) : VoIP
  - MSRPC (Microsoft Remote Procedure Call Protocol, port 135) : communication de processus inter-systèmes

Les ACL dynamiques

- NetShow (port 1755): streaming Microsoft
- R-EXEC (port 512) : commandes distantes (Unix)
- R-SHELL (port 514): shell distant (Unix)
- RTSP (Real-Time Streaming Protocol, port 544): streaming et VoIP
- SMTP (Simple Mail Transfer Protocol, port 25): courrier
- SQLNet (port 1521): Communications clients-BdD
- Stream Works (port 1558): Streaming de Real Networks
- Real Audio (port 7070): Streaming de Real Networks
- TFTP (Trivial File Transfer Protocol, port 69): transfert de fichiers clients-serveurs
- VDOlive (port 7000) : streaming

Exemple (1/5)


Réseau public (externe)
Réseau privé d'entreprise (interne)
Serveur HTTP
access-list 121 deny ip any any
Cette ACL est appliquée à tous les paquets entrant sur l'interface s0.
10.10.10.0/24
Internet (WWW)
Interface s0
Routeur avec FFS
Interface e0
PC d'utilisateur
Réponse DNS
Requête DNS
L'ACL 123 est appliquée à tous les paquets entrant sur l'interface e0.
"Je veux accéder à http://www.google.com."
Serveur DNS du FAI
accest-list 123 permit udp 10.10.10.0 0.0.0.255 any eq domain
accest-list 123 permit tcp 10.10.10.0 0.0.0.255 any eq http

- ACL
- Access-list 121 Permit TCP/UDP 10.10.10.0/24 any http
- Access-list 121 Permit TCP/UDP 10.10.10.0/24 DNS_SERVER dns

- Access-list 121 Permit TCP/UDP 10.10.10.0/24 any 80
- Access-list 121 Permit TCP/UDP 10.10.10.0/24 DNS_SERVER 53

Exemple (2/5)

- 1. L'utilisateur saisit www.google.fr
  - Le PC émet une requête de résolution de nom DNS pour obtenir l'adresse IP de l'URL
- 2. Le paquet de requête DNS (un datagramme UDP) arrive sur l'interface Ethernet interne du routeur
  - Il est comparé à la liste 123 (filtrage)
  - Il est transmis si autorisé ou supprimé
- 3. Le paquet autorisé est soumis au CBAC (Context-Based Access Control => contrôle d'accès contextuel)
  - Inspection
  - Consignation des informations dans la table d'états
    - Adresse IP source et numéro de port
    - Adresse IP destination, numéro de port et protocole
- 4. Création d'une instruction `permit` temporaire sur la liste 121
  - Autorisation du trafic en réponse par l'hôte de destination (serveur DNS)
  - Instruction temporaire placée devant les instructions statiques de l'ACL

Exemple (3/5)

- 5. Le paquet de requête DNS (port UDP 53) est transmis au serveur DNS
  - Réponse du serveur DNS
  - Entrée ACL dynamique maintenue 5 secondes
- 6. Arrivée du paquet de réponse DNS
  - Comparaison à l'ACL 121
  - Autorisé puisqu'appartenant à une session établie
- 7. Inspection du paquet de réponse DNS
  - Conservation des informations d'état jusqu'à expiration du temporisateur par défaut de maintien des sessions UDP
- 8. Arrivée de la réponse DNS sur le PC utilisateur et initiation par le PC d'une session HTTP avec google
  - HTTP s'appuie sur TCP, donc le premier paquet comporte le bit SYN (synchronisation) activé pour entamer le processus de négociation en trois temps de TCP

Exemple (4/5)

- 9. Le paquet HTTP est autorisé
  - liste 123 autorisant le port HTTP 80
- 10. Inspection du paquet sortant et consignation des info dans la table d'états
  - Adresse IP source et port
  - Adresse IP destination, port et protocole
- 11. Création d'une instruction `permit` temporaire sur la liste 121
  - Autorisation du trafic en réponse par l'hôte de destination (serveur HTTP)
  - Instruction temporaire placée devant les instructions statiques de l'ACL
  - Maintien de l'entrée pendant 30 secondes (le temps de recevoir un paquet SYN-ACK, synchronisation-acquittement, de la part du serveur web)
- 12. Réception du paquet provenant du serveur web
  - Autorisé par la liste 121 (car appartenant à une session établie)

Exemple (5/5)

- 13. Inspection du paquet provenant du serveur web
  - Elimination du paquet si violations de protocoles spécifiques
- Dans le cas de HTTP et autres protocoles nécessitant plusieurs sessions
  - Mise à jour continuelle de la table d'états
  - Mise à jour continuelle de l'ACL
- Délais de suppression des entrées ACL temporaires
  - ICMP et UDP, à expiration d'un temporisateur de durée configurable
  - TCP, cinq secondes après l'échange de paquets FIN

Pare-feux applicatifs

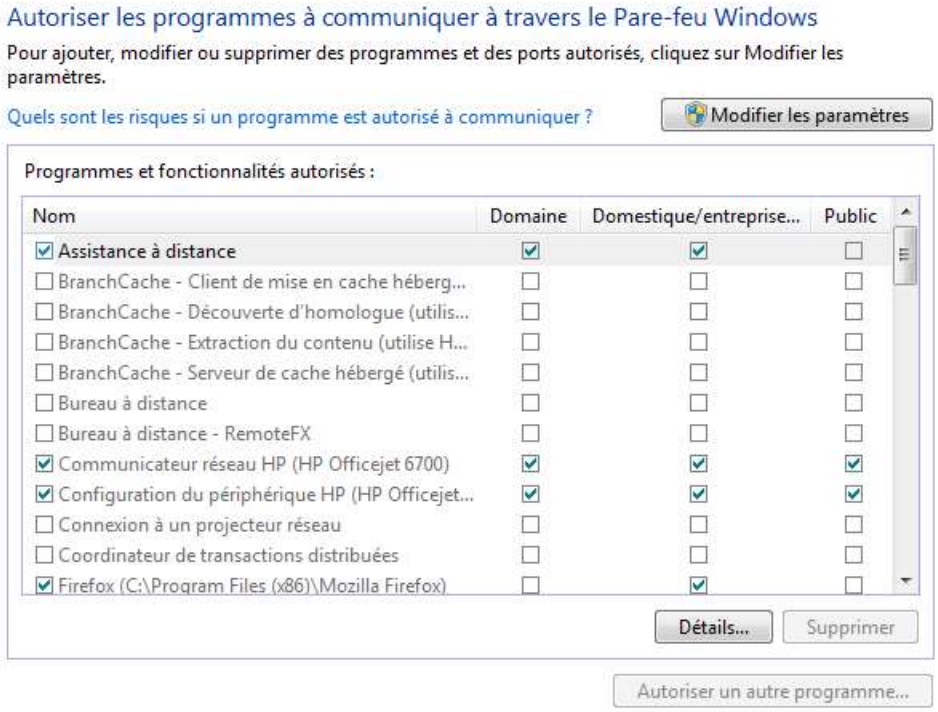
- Dernière génération de pare-feu
- Complète conformité du paquet à un protocole attendu
- Ex : protocole HTTP uniquement sur le port TCP 80
- Gourmand en temps de calcul
- Problématiques de certains protocoles (FTP par exemple) dits « sales » (car ne respectant pas strictement le modèle en couches (passage d'infos niveau IP (adresses) ou TCP (ports) au niveau applicatif)

Pare-feux identifiants

- Identification des connexions passant à travers le filtre IP.
- Règles de filtrage par utilisateur et non plus par adresse IP ou adresse MAC
- Possibilité de suivre l'activité réseau par utilisateur
- Règles dynamiques basée sur l'authentification d'un utilisateur (ex Kerberos), l'identité de son poste ainsi que son niveau de sécurité (présence d'antivirus, de patches particuliers)

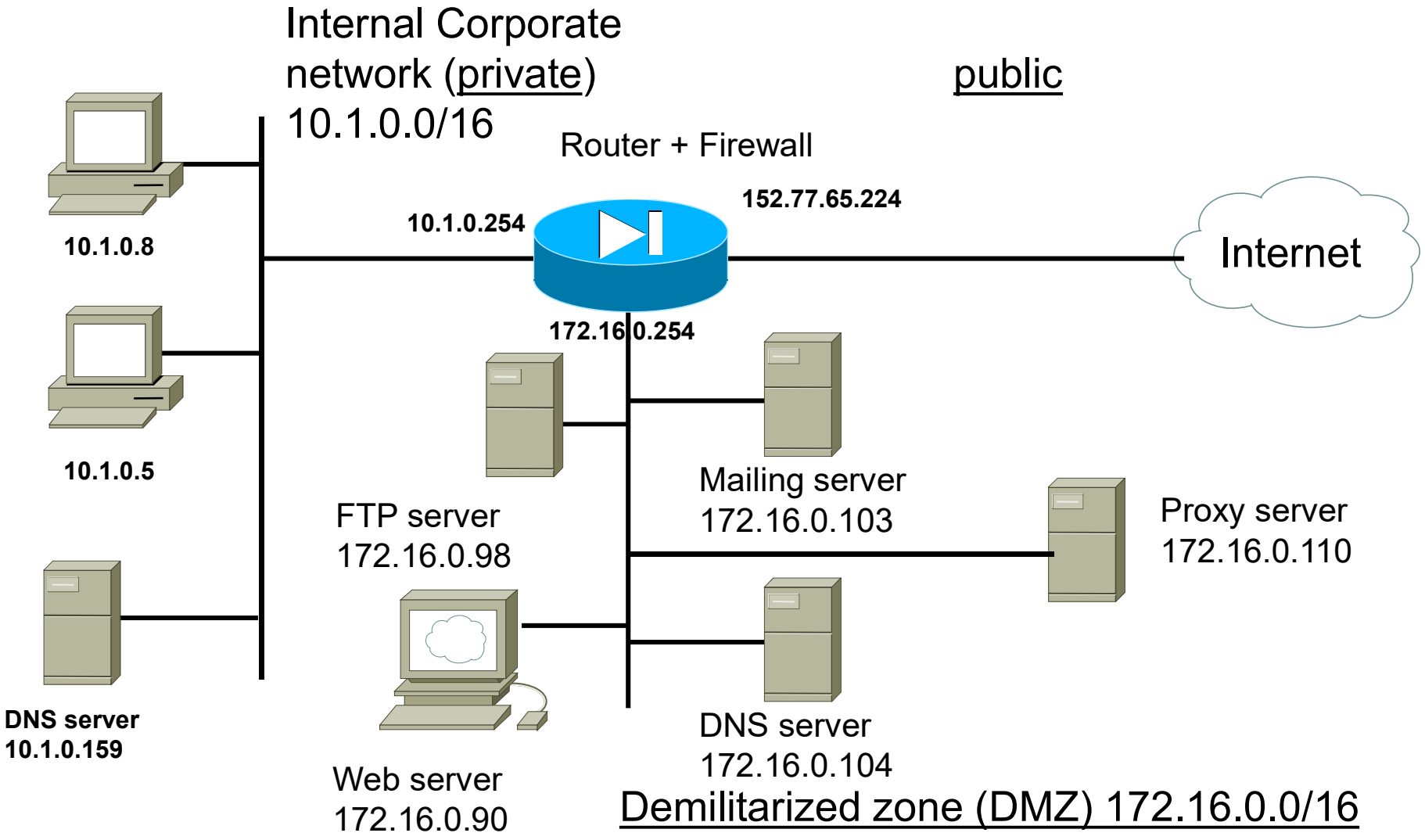
Pare-feux personnels

- Elément important d'une stratégie de sécurité en profondeur
- Pare-feu personnel
  - Peut être intégré au système (Windows, Mac…)
  - Ex : panneau de configuration

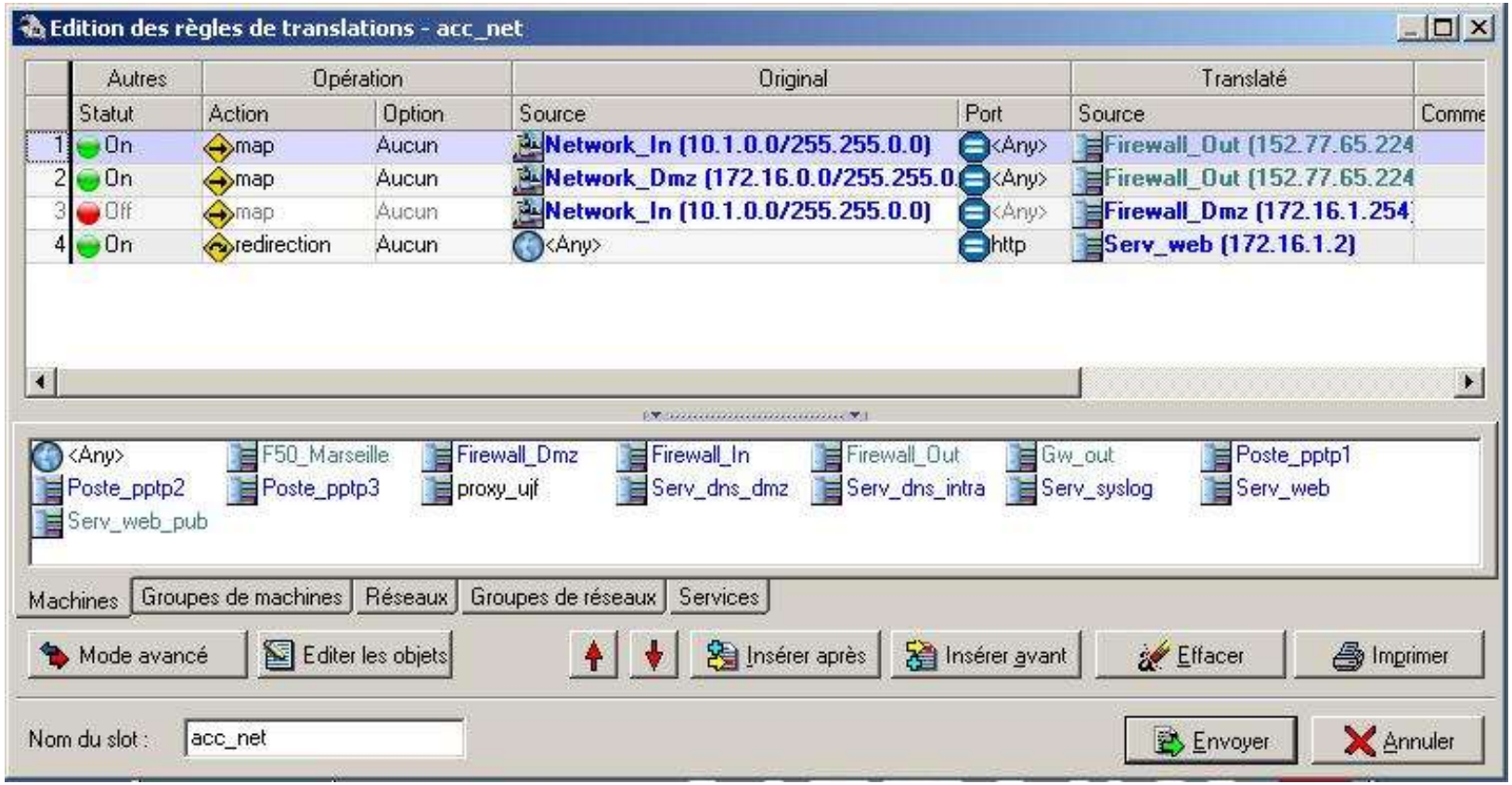


Type de pare-feux

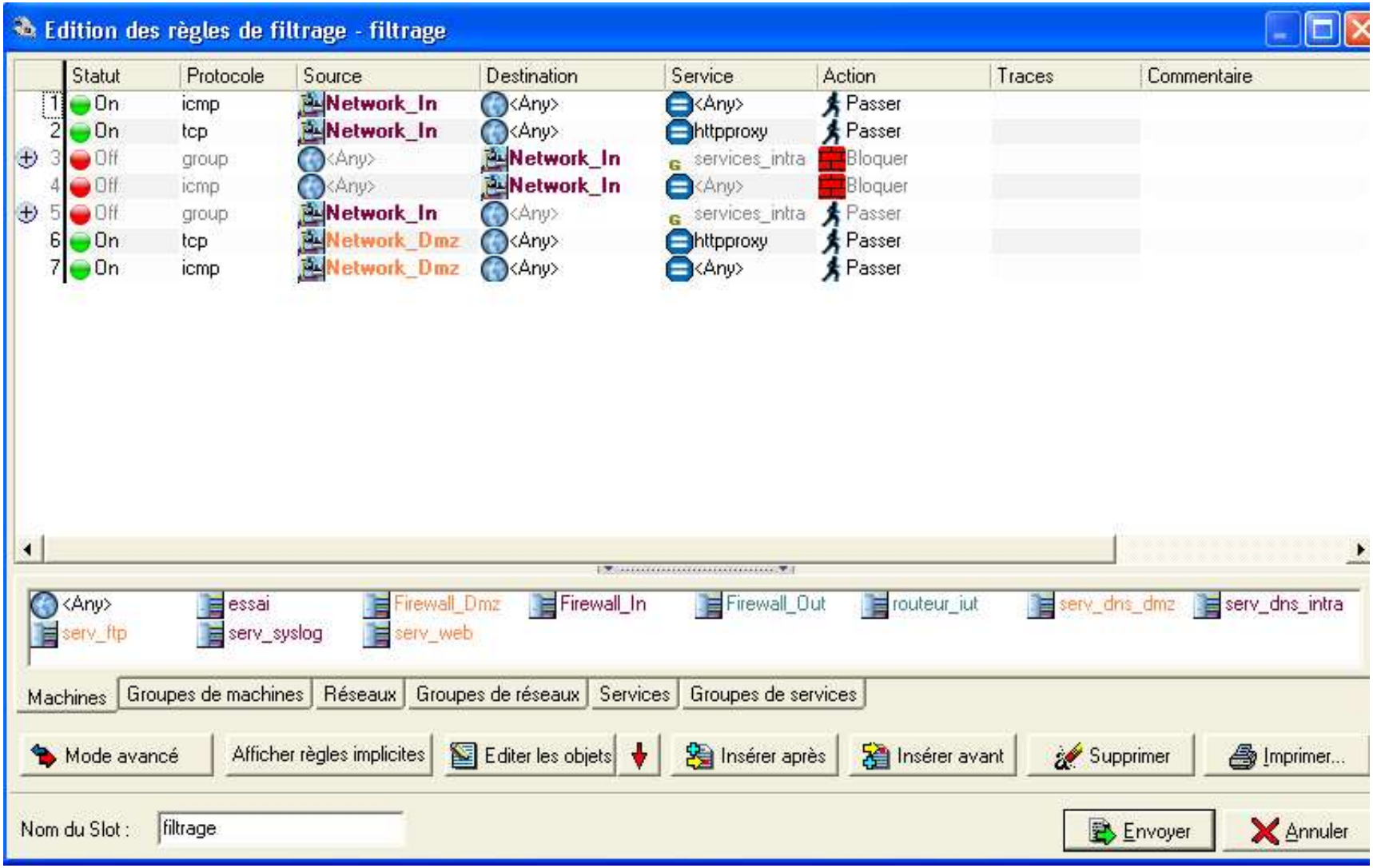
Un réseau…


Internal Corporate
network (private)
10.1.0.0/16
public
Router + Firewall
152.77.65.224
10.1.0.254
Internet
10.1.0.8
10.1.0.5
172.16.0.254
FTP server
172.16.0.98
Mailing server
172.16.0.103
Proxy server
172.16.0.110
DNS server
10.1.0.159
Web server
172.16.0.90
DNS server
172.16.0.104
Demilitarized zone (DMZ) 172.16.0.0/16

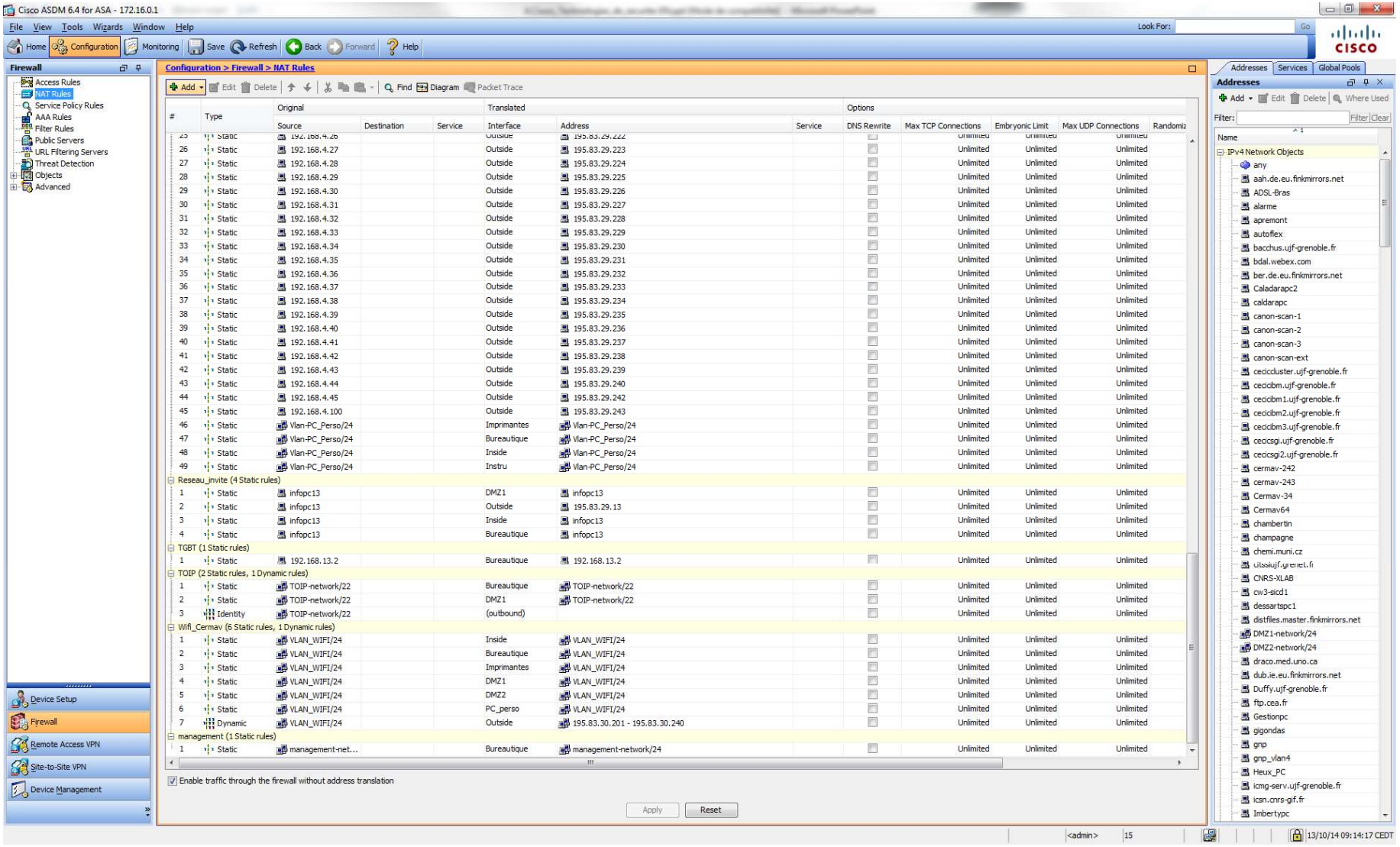
Translation (Netsacq)



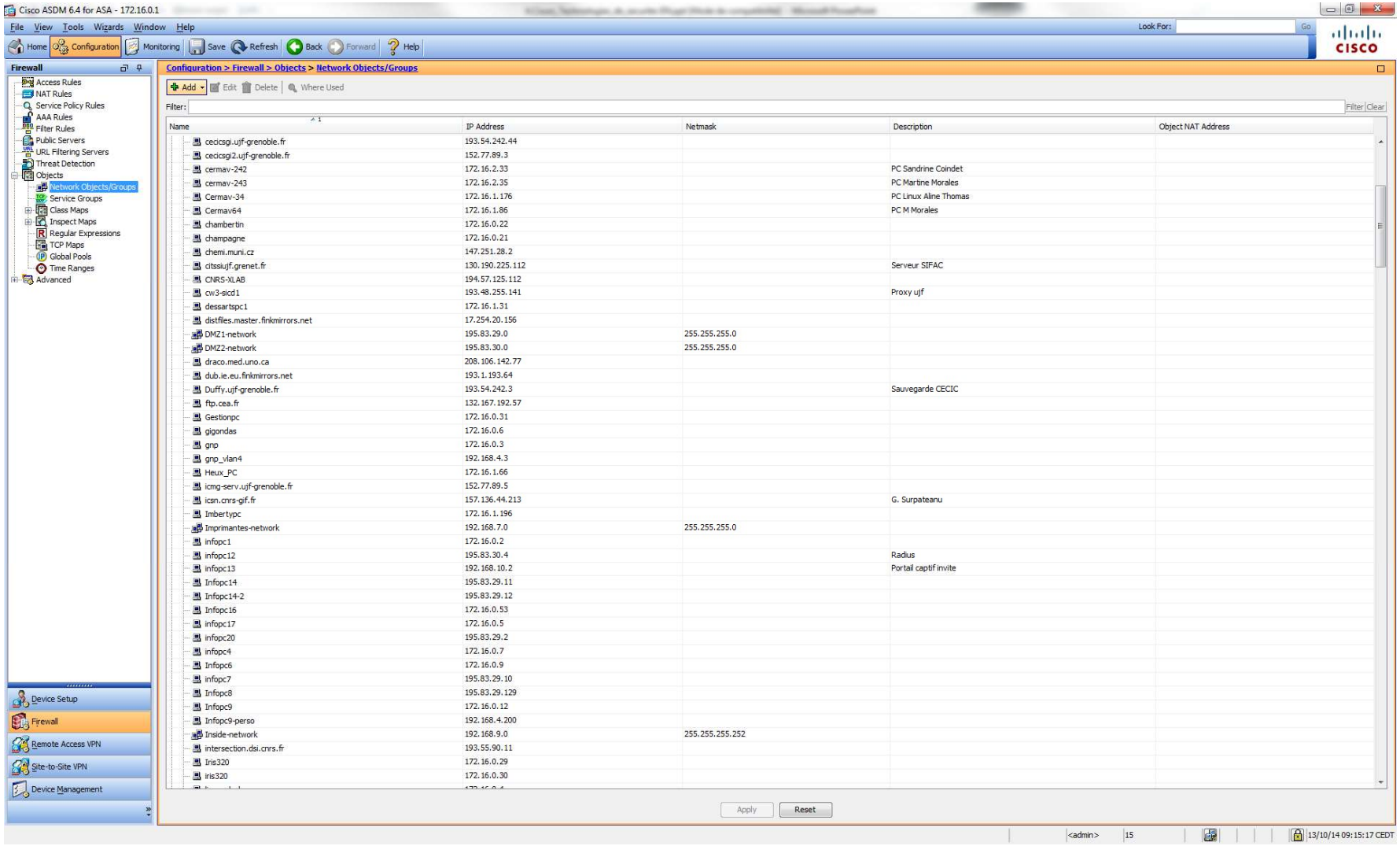
Règles de filtrage (Netascq)



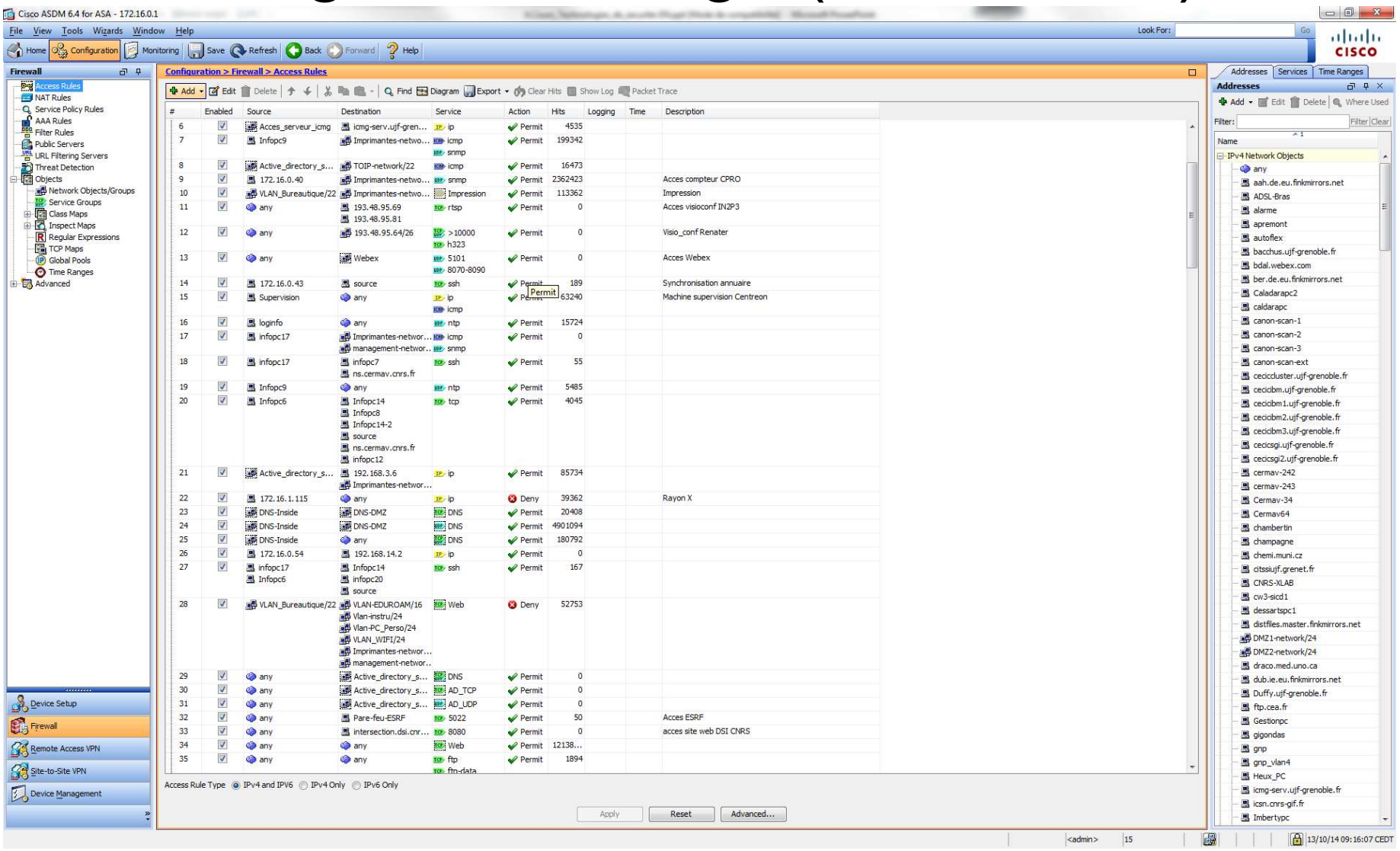
Translation (Cisco ASA)



Pare-feu Cisco ASA
Définition des machines (hôtes)



Règles de filtrage (Cisco ASA)



Software firewall

- Comportement par défaut à adopter avec un paquet entrant.
- Suppression de tous les paquets s'ils ne répondent à aucune condition :
- iptables --policy INPUT DROP
- iptables --policy OUTPUT DROP
- iptables --policy FORWARD DROP

Example of rules

- iptables --new local_net
- iptables -A local_net --proto udp --dport 53 -s 192.168.0.0/24 –j ACCEPT
- iptables -A local_net --proto tcp --dport 80 -s 192.168.0.0/24 –j ACCEPT
- iptables -A local_net --proto tcp --dport 443 -s 192.168.0.0/24 –j ACCEPT

Positionnement des pare-feu

- Où mettre des pare-feu ?
  - A l'endroit de la connexion réseau interne-internet
  - Entre diverses portions de réseau interne (grandes entreprises)

Limitations des pare-feu

- Ne peut empêcher des utilisateurs ou attaquants utilisant des modems d'accéder à l'intérieur du réseau
- Ne peut empêcher une mauvaise utilisation des mots de passe (nom respect de la stratégie de mots de passe par les utilisateurs)
- Concentration du trafic en un seul point = goulet d'étranglement = source de panne fatale

Critères de choix d'un pare-feu

- Nature, type d'applications (FTP, messagerie, SNMP, Audio, Vidéo),
- Répartition et équilibrage de charge (QoS)
- Type de filtrage (niveau réseau, niveau applicatif)
- Facilités d'enregistrement des actions à des fins d'audit
- Outils et facilités d'administration
- Capacité à supporter un tunnel chiffré (VPN)
- Outils de surveillance, alarmes, audit actif
- Vulnérabilités : intrusions => modification de la configuration, des accès, effacement ou modification des traces de journalisation, infection virale
- Evaluation : cf organisation des critères communs (www.commoncriteriaportal.org)

Principe de base pour la configuration d'un pare-feu

- Moindre privilège : ne pas accorder aux utilisateurs du réseau protégé par le pare-feu des droits dont ils n'ont pas la nécessité ; interdire par exemple le peer-to-peer dans le cadre d'une entreprise
- Interdiction par défaut : interdire par défaut tout transit à travers le pare-feu et ne laisser passer que celui qui est explicitement autorisé, évitant ainsi tout transit involontairement intercepté
- Défense en profondeur : utiliser les moyens de protection à tous les niveaux possibles, par exemple en analysant et filtrant tout ce qui peut l'être au niveau du pare-feu. Ce principe évite de laisser entrer dans le réseau des communications indésirables, même si un autre moyen de contrôle est utilisé plus en profondeur dans le réseau
- Goulet d'étranglement : toutes les communications entrant et sortant du réseau doivent transiter par le pare-feu. Il ne faut pas de points d'entrée ou de sortie du réseau non contrôlés, comme par exemple des modems sauvages
- Simplicité : les règles de filtrage du pare-feu doivent être les plus simples et les plus compréhensibles possibles afin d'éviter toute erreur de la part de l'administrateur ou de ses successeurs
- Participation des utilisateurs : les utilisateurs doivent être impliqués dans la mise en place du pare-feu. Ils doivent en effet exprimer leurs besoins et recevoir en échange les raisons et les objectifs de l'installation d'un tel dispositif ; les contraintes afférentes au pare-feu seront ainsi mieux acceptées.

DMZ, zone démilitarisée (concept de sécurité périmétrique)

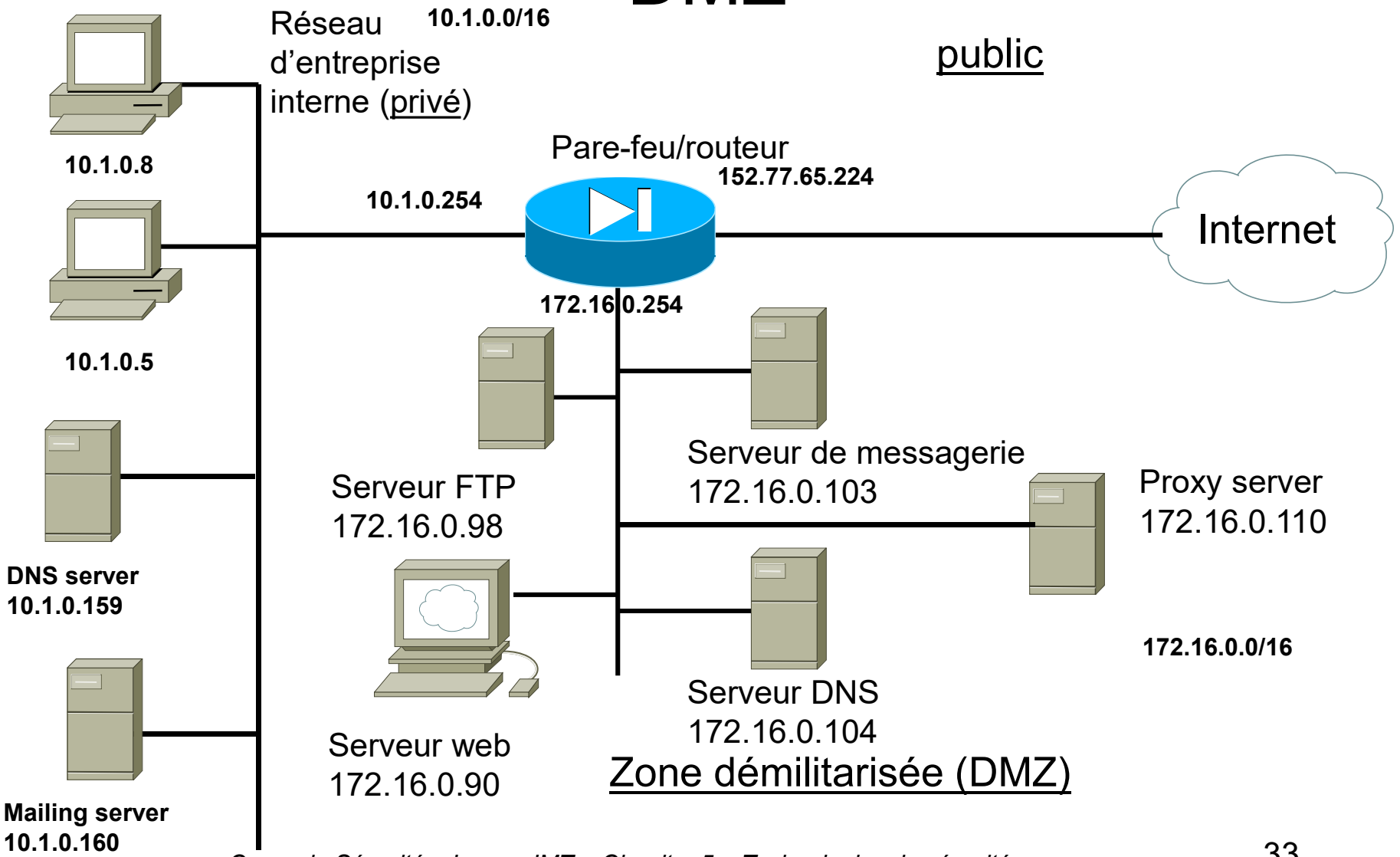
Zone démilitarisée (sécurité périmétrique) (DMZ, Demilitarized Zone)

- Zone du réseau interne isolée (entre la zone publique et la zone privée)
  - Serveur web
  - Serveur de messagerie
  - Serveur FTP
  - ...
- Cela permet au trafic venant d'internet d'aller dans cette zone, mais pas de pénétrer ailleurs sur le réseau interne
- Possibilité d'auditer le trafic échangé avec la DMZ
- Possibilité de placer un système de détection d'intrusion

DMZ : son rôle

- Proposer une zone
  - Recevant les demandes de l'extérieur
  - Ne communiquant pas avec le réseau local
  - Possédant son propre adressage
- Accès à la zone
  - Par le routeur depuis l'extérieur
  - Par le routeur + NAT depuis l'intérieur
- Réalise une zone tampon
  - Peut être corrompue
  - Ne révèle jamais la présence du réseau local

Ex : Architecture autour d'une DMZ



Exercice

- Soit une architecture autour d'un pare-feu à états
- On souhaite mettre en place :
  1. Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur.
  2. Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne.
  3. Toutes les machines de l'intérieur doivent pouvoir sortir en http ou https en passant par le proxy
  4. Le serveur DNS du réseau interne doit pouvoir joindre le DNS de la DMZ sur le port 53.
  5. Le serveur DNS de la DMZ doit pouvoir joindre un DNS externe (IP: 143.210.47.211).
- Actions à mener
  - Si besoin, mettre en place des règles de translation
  - Ecrire les règles de filtrage et les commenter
- Audit de notre stratégie de sécurité
  - Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur. Est-ce une bonne stratégie ? Pourquoi ?
  - Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne. Pourquoi cette stratégie ?

Exercise 1

- We use a stateful firewall
- The machines from the inside network should be able to reach any machine in the DMZ or outside (for the mail)
  - Access-list 1 permit mail 10.1.0.0/16 any eq 25
- The machines from the DMZ should be able to reach any machine in outside BUT NOT inside (for the mail)
  - Access-list 1 deny mail 172.16.0.0/16 10.1.0.0/16 eq 25 (should be before !)
  - Access-list 1 permit mail 172.16.0.0/16 any eq 25
- Concerning http
  - Any machine from inside should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - Access-list 1 permit tcp/udp 10.1.0.0/16 172.16.0.110 eq 3128
  - Any machine from the DMZ should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - No rule
  - The proxy should be able to reach any http server (port 80) everywhere
  - Access-list 1 permit tcp 172.16.0.110 any eq 80
- We should not forget the DNS aspects (port 53)
  - Access-list 1 permit tcp/udp 10.1.0.159 172.16.0.104 eq 53
  - Access-list 1 permit tcp/udp 172.16.0.104 a_specific_DNS_Server_outside eq 53
  - Access-list 1 deny any any any eq any

Exercice 2

- Soit une architecture autour d'un pare-feu à états
- On souhaite mettre en place :
  1. Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur.
  2. Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne.
  3. Toutes les machines de l'intérieur doivent pouvoir sortir en http ou https en passant par le proxy
  4. Le serveur DNS du réseau interne doit pouvoir joindre le DNS de la DMZ sur le port 53.
  5. Le serveur DNS de la DMZ doit pouvoir joindre un DNS externe (IP: 143.210.47.211).
- Actions à mener
  - Si besoin, mettre en place des règles de translation
  - Ecrire les règles de filtrage et les commenter
- Audit de notre stratégie de sécurité
  - Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur. Est-ce une bonne stratégie ? Pourquoi ?
  - Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne. Pourquoi cette stratégie ?

Exercise 2

- Let's consider an architecture around a stateful firewall
- We wish to set up :
  1. All the machines of the internal network must ping the DMZ or the outside.
  2. All the machines in the DMZ must be able to ping outside but not on the internal network.
  3. All the machines from the inside must be able to reach http or https servers through the proxy.
  4. The DNS server of the internal network must be able to reach the DNS of the DMZ on port 53.
  5. The DNS server of the DMZ must be able to reach an external DNS (IP: 143.210.47.211).
- Actions to be carried out If necessary,
  - set up translation rules
  - Write filter rules and comment on them
- Audit of our security strategy
  - All the machines in the internal network have to be connected to the DMZ or to the outside. Is this a good strategy? Why is it a good strategy?
  - All the machines in the DMZ must ping the outside but not the internal network. Why this strategy?

Règles de translation

- Elles sont nécessaires car nous avons utilisé des adresses privées
- 10.1.0.0/16 any 152.77.65.224 ; les machines du réseau interne sortent sur le réseau public en utilisant l'adresse publique unique 152.77.65.224
- 172.16.0.0/16 any 152.77.65.224 ; les machines de la DMZ sortent sur le réseau public en utilisant l'adresse publique unique 152.77.65.224

Règles de filtrage

Protocole	Source	Destination	Service (numéro port)	Action	Commentaire
ICMP	10.1.0.0/16	Any	Any	Pass	Réseau interne ping partout
ICMP	172.16.0.0/16	10.1.0.0/16	Any	Block	Pas de de DMZ vers réseau interne
ICMP	172.16.0.0/16	Any	Any	Pass	DMZ pingue partout
TCP	10.1.0.0/16	172.16.0.110	Httpproxy	Pass	Passage flux TCP réseau interne => proxy
TCP	172.16.0.110	Any	http, https	Pass	Passage flux TCP du proxy vers les serveurs http partout
TCP,UDP	10.1.0.159	172.16.0.104	Dns (port 53)	Pass	DNS Passe du réseau interne => DMZ
TCP,UDP	172.16.0.104	143.210.47.211	Dns (port 53)	Pass	DNS passe de DMZ vers DNS externe

Règles de translation

- Elles sont nécessaires car nous avons utilisé des adresses privées
- 10.1.0.0/16 any 152.77.65.224 ; les machines du réseau interne sortent sur le réseau public en utilisant l'adresse publique unique 152.77.65.224
- 172.16.0.0/16 any 152.77.65.224 ; les machines de la DMZ sortent sur le réseau public en utilisant l'adresse publique unique 152.77.65.224

Règles de filtrage

Protocole	Source	Destination	Service (numéro port)	Action	Commentaire
ICMP	10.1.0.0/16	Any	Any	Pass	Réseau interne ping partout
ICMP	172.16.0.0/16	10.1.0.0/16	Any	Block	Pas de de DMZ vers réseau interne
ICMP	172.16.0.0/16	Any	Any	Pass	DMZ pingue partout
TCP	10.1.0.0/16	172.16.0.110	Httpproxy	Pass	Passage flux TCP réseau interne => proxy
TCP	172.16.0.110	Any	http, https	Pass	Passage flux TCP du proxy vers les serveurs http partout
TCP,UDP	10.1.0.159	172.16.0.104	Dns (port 53)	Pass	DNS Passe du réseau interne => DMZ
TCP,UDP	172.16.0.104	143.210.47.211	Dns (port 53)	Pass	DNS passe de DMZ vers DNS externe

Quelques considération au sujet de la NAT

Network Address Translation

Fonction NAT, traduction d'adresse (network address translation)

- Adresses de l'internet (IPv4)
  - Théorie, 2^{32} adresses (~4,3 Mds d'adresse)
  - Pratique
    - Adresses publiques : ~3,2 Mds
    - Adresses réservées : test…
    - Adresses privées : réservées pour les réseaux internes (non accessibles de l'extérieur)
      - 10.0.0.0 à 10.255.255.255 (préfixe 10/8)
      - 172.16.0.0 à 172.31.255.255 (préfixe 172.16/12)
      - 192.168.0.0 à 192.168.255.255 (préfixe 192.168/16)
- NAT assure la conversion entre les adresses publiques et privées, entre le réseau interne et des ouvertures sur l'extérieur
  - pare-feu,
  - Quelques fois un routeur ou un ordinateur

NAT

- NAT statique
  - Même adresse IP publique à une adresse IP privée donnée
  - Ex : serveur WEB
- NAT dynamique
  - Associe à une adresse IP privée une adresse publique aléatoire tirée d'un groupe
- PAT (Port Address translation)
  - Associe une seule adresse publique à plusieurs adresses privées en utilisant divers ports
  - Rappel : 65 535 ports TCP sont supportés par adresse IP

Sécurité avec NAT

- Plus difficile pour un attaquant de :
  - Déterminer la topologie du réseau et le type de connectivité de l'entreprise cible
  - Identifier le nombre de systèmes qui s'exécutent sur le réseau
  - Identifier le type des machines et leurs systèmes d'exploitation
  - Réaliser des attaques de type déni de service (Ex : SYN Flood, scan de ports, injection de paquets)

Inconvénients de NAT

- Connexions UDP mal gérées
  - Estimation du temps où la connexion doit rester ouverte
- D'autres protocoles sont mal gérés
  - Kerberos, X Windows, rsh (remote shell), SIP (Session Initiation Protocol)
- Systèmes de chiffrement et d'authentification
  - Ces systèmes sont basés sur l'intégrité des paquets
  - Or NAT modifie ces paquets
- Journalisation compliquée
  - Mise en corrélation des journaux demande d'intégrer les traductions réalisées par NAT
- Problème de partage d'adresse avec PAT
  - Authentification auprès d'une ressource extérieure protégée (tous les utilisateurs partageant la même adresse risquent de pouvoir utiliser cette ressource)

Références bibliographiques

- Présentation de Eric WIESS
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Cours de Jean-Luc Noizette, ESSTIN, Nancy, 2005
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux* , 4ème édition – Dunod, 2013
- G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006.
- NIST, Guidelines on firewalls and firewall policy, J. Wack & al., 2002.
- The 60 minute network security guide (first stpes towards a secure network environment), 2006, SNAC

Autres exercices d’application

Exercice 37 : pool d'adresses

- Une entreprise pratique la translation d'adresses dynamique avec un pool de 3 adresses IP 193.49.96.60 à 62). Quatre stations A, B, C et D souhaitent accéder au site web dont l'adresse est 128.178.50.93. Les adresses internes des stations A, B, C et D sont respectivement 192.168.0.1 à 4. Les quatre machines utilisent le port source 3001.
- Compléter la table de translation du routeur pendant la connexion (plusieurs solutions correctes sont possibles)

Table de translation du pare-feu pendant la connexion							
Interne				externe			
Source	Port	Dest	Port	Source	Port	Dest	Port
192.168.10.1							
192.168.10.2							
192.168.10.3							
192.168.10.4							

Solution exercice 37 : pool d'adresses

- Il existe plusieurs réponses possibles. On considère ici que le routeur distribue dans un premier temps les adresses disponibles dans le pool. Puis, lorsqu'il n'y a plus d'adresses, il utilise une adresse disponibles mais change le port source. Nous pourrions également ne distribuer qu'une adresse IP avec plusieurs ports.

Table de translation du pare-feu pendant la connexion							
Interne				externe			
Source	Port	Dest	Port	Source	Port	Dest	Port
192.168.10.1	3001	128.178.50.93	80	193.49.96.60	3001	128.178.50.93	80
192.168.10.2	3001	128.178.50.93	80	193.49.96.61	3001	128.178.50.93	80
192.168.10.3	3001	128.178.50.93	80	193.49.96.62	3001	128.178.50.93	80
192.168.10.4	3001	128.178.50.93	80	193.49.96.62	3002	128.178.50.93	80

Exercice 42 : Principes de base de la configuration d'un pare-feu

- On considère les principes de base suivants : moindre privilège, interdiction par défaut, défense en profondeur, goulet d'étranglement, simplicité et participation des utilisateurs. Discuter chacun de ces principes dans le cadre de la configuration d'un pare-feu.

Solution exercice 42 : Principes de base de la configuration d'un pare-feu (1/2)

- Les principes de base à respecter sont les suivants :
  - **Moindre privilège** : ne pas accorder aux utilisateurs du réseau protégé par le pare-feu des droits dont ils n'ont pas la nécessité ; interdire par exemple le « peer-to-peer » dans le cadre d'une entreprise
  - **Interdiction par défaut** : interdire par défaut tout transit à travers le pare-feu et ne laisser passer que celui qui est explicitement autorisé, évitant ainsi tout transit involontairement accepté
  - **Défense en profondeur** : utiliser les moyens de protection à tous les niveaux possibles, par exemple en analysant et filtrant tout ce qui peut l'être au niveau du pare-feu. Ce principe évite de laisser entrer dans le réseau des communications indésirables, même si un autre moyen de contrôle est utilisé plus en profondeur dans le réseau (par ex sur le serveur de messagerie)

Solution exercice 42 : Principes de base de la configuration d'un pare-feu (2/2)

- **Goulet d'étranglement** : toutes les communications entrant ou sortant du réseau doivent transiter par le pare-feu. En effet, il ne faut pas de points d'entrée ou de sortie du réseaux non contrôlés, comme par exemple des « modems » sauvages, des réseaux VPN mal configurés, entrées de données par clés USB avec de mauvaises intentions…
- **Simplicité** : les règles de filtrage du pare-feu doivent être les plus simples et donc les plus compréhensibles possibles afin d'éviter toute erreur de la part de l'administrateur ou de ses successeurs
- **Participation des utilisateurs** : les utilisateurs doivent pouvoir être impliqués dans la mise en place du pare-feu. Ils doivent en effet exprimer leurs besoins et recevoir en échange les raisons et les objectifs de l'installation d'un tel dispositif ; les contraintes afférentes au pare-feu (et au-delà à l'ensemble de la stratégie de sécurité déployée) seront ainsi mieux acceptées

Exo 44 : règles de filtrage d'un pare-feu sans mémoire (stateless)

- On considère un pare-feu sans mémoire dont le critère de filtrage est fondé sur les paquets SYN (paquets dont le flag SYN est 1 et le flag ACK est 0). On souhaite que le serveur de messagerie (128.178.1.1) sur le réseau interne puisse recevoir et envoyer des messages de et vers internet. Ecrire les règles de filtrage du pare-feu dans le tableau ci-dessous

Source	Port	Dest	Port	Protocole	Paquet SYN	Action

Corrigé 44 : règles de filtrage d'un pare-feu sans mémoire (stateless) (1/2)

- On donne dans le tableau ci-dessous les règles de filtrage du pare-feu permettant au serveur de messagerie d'envoyer ou de recevoir des messages de ou vers internet.
- La première ligne de la table permet à n'importe quelle machine extérieure au réseau de se connecter sur le port 25 du serveur de messagerie ; tout paquet TCP est alors accepté : SYN, SYN-ACK et ACK.

Source	Port	Dest	Port	Protocole	Paquet SYN	Action
any	any	128.178.1.1	25	tcp	any	permit
any	25	128.178.1.1	any	tcp	no	permit
128.178.1.1	any	any	25	tcp	any	permit
128.178.1.1	25	any	any	tcp	no	permit
any	any	any	any	any	any	deny,log

Corrigé 44 : règles de filtrage d'un pare-feu sans mémoire (stateless) (2/2)

- La seconde ligne permet à une machine extérieure de répondre à une demande de connexion (les paquets SYN sont donc refusés).
- La troisième ligne a pour objectif d'autoriser le serveur de messagerie à se connecter sur le port 25 d'une machine extérieure au réseau.
- La quatrième ligne a pour but de permettre au serveur de messagerie de répondre à une machine extérieure (les paquets SYN sont donc rejetés).
- La dernière ligne interdit tout autre type de trafic quels que soient les machines, ports et protocoles utilisés. Ce type de trafic est enregistré car la commande « log » est stipulé dans la table, ce qui permettra d'obtenir des informations en cas de problèmes.

Exo 45 : Règles de filtrage d'une pare-feu sans mémoire (bis)

- On considère un pare-feu sans mémoire qui abrite la machine 203.167.75.1. L'utilisateur de cette machine souhaite pouvoir naviguer sur le web, recevoir des connexions telnet provenant de l'extérieur du réseau interne, ainsi que recevoir et initier des connexions SSH de et vers internet. Sachant que les serveurs HTTP, telnet et SSH utilisent respectivement les ports 80, 23 et 22, écrire la table de filtrage du pare-feu en utilisant le critère de filtrage sur les paquets SYN (flag SYN à 1 et flag ACK à 0).

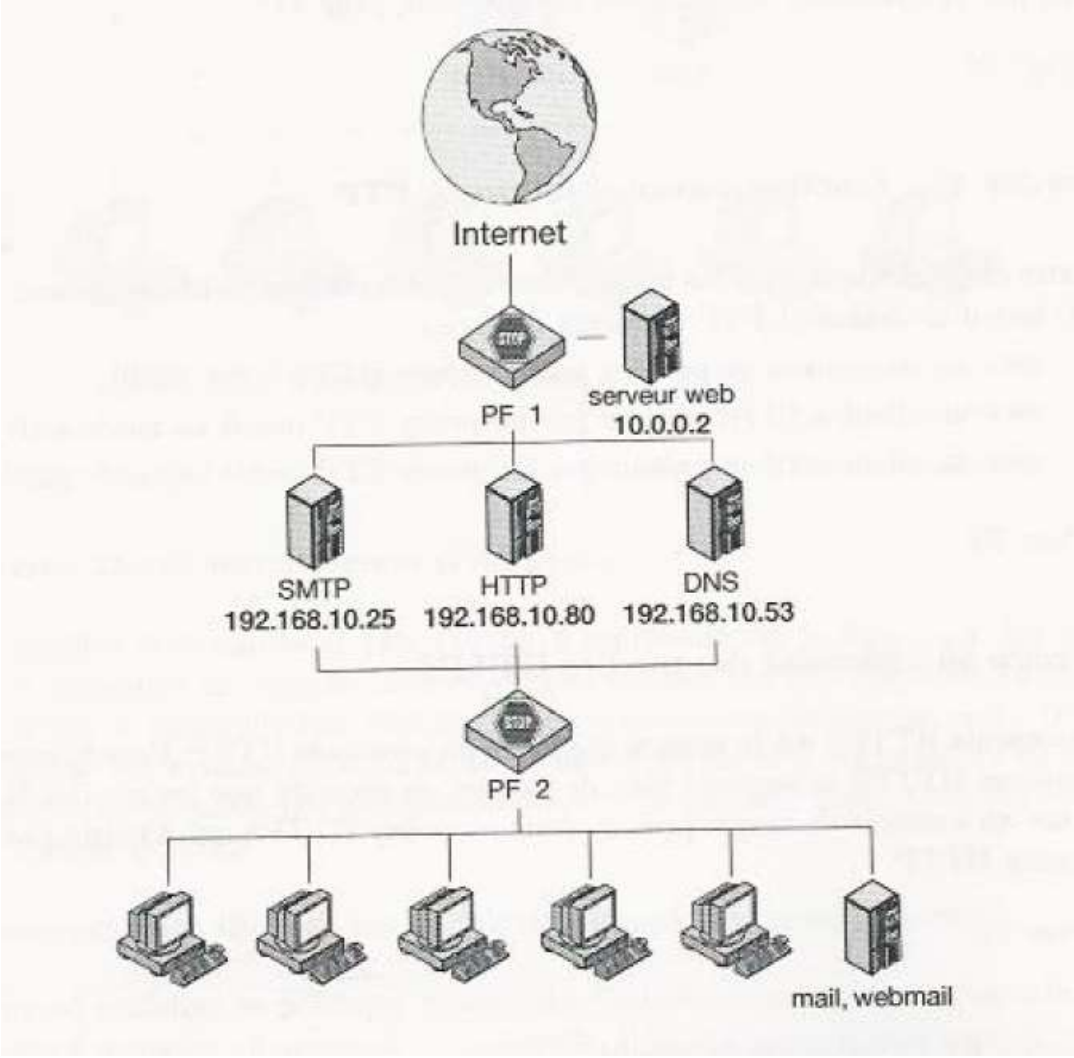
Corrigé 45 : Règles de filtrage d'une pare-feu sans mémoire (bis)

Source	Port	Dest	Port	Protocole	Paquet SYN	Action
any	any	203.167.75.1	22	tcp	any	permit
any	22	203.167.75.1	any	tcp	no	permit
any	80	203.167.75.1	any	tcp	no	permit
any	any	203.167.75.1	23	tcp	any	permit
203.167.75.1	any	any	22	tcp	any	permit
203.167.75.1	22	any	any	tcp	no	permit
203.167.75.1	any	any	80	tcp	any	permit
203.167.75.1	23	any	any	tcp	no	permit
any	any	any	any	any	any	deny,log

Ex 46 : Règles de filtrage d'un pare-feu avec mémoire

- On considère l'architecture diapo suivante. On suppose que l'adresse du serveur web est 10.0.0.2 et que les proxies SMTP, HTTP et DNS possèdent respectivement les adresses 192.168.10.25, 192.168.10.80 et 192.168.10.53. Les trois proxies sont utilisés en mode direct (donc vers internet) et inverse (donc depuis internet). Le serveur web doit aussi être accessible depuis le réseau interne. On désigne par dmz_proxy toutes les adresses de la zone des proxies et par dmz_web toutes les adresses de la zone du serveur web. Ecrire les règles de filtrage pour le pare-feu externe avec mémoire (PF1)

Architecture ex 46 et 47



Corrigé 46 : Règles de filtrage d'un pare-feu avec mémoire

Exercice 47

Exercice 47 : Vulnérabilités d'un pare-feu sans mémoire

Le pare-feu sans mémoire d'une université qui relie son réseau à Internet (via une ligne de 400 Mbps) a été configuré de la manière suivante : seules les connexions entrantes (initiées depuis l'extérieur de l'université) sur les ports 22 (SSH), 80 (HTTP) et 443 (HTTPS) sont permises ; plus précisément, les paquets `SYN` venant de l'extérieur à destination d'un port interdit sont jetés. En revanche, toutes les connexions sortantes (initiées depuis l'intérieur de l'université) sont permises.

1. Donner une raison plausible au fait que l'université ait choisi un pare-feu sans mémoire.

2. Expliquer comment un adversaire ne disposant pas d'un accès interne au réseau de cette université peut « cartographier » ce dernier en le scannant depuis l'extérieur.

- 3. Que faudrait-il changer pour améliorer la situation ?

Architecture ex 46 et 47