UGA
Université
Grenoble Alpes

Security of information systems

http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/miscit/miscit_en.html

Jean-Marc THIRIET

jean-marc.thiriet@univ-grenoble-alpes.fr

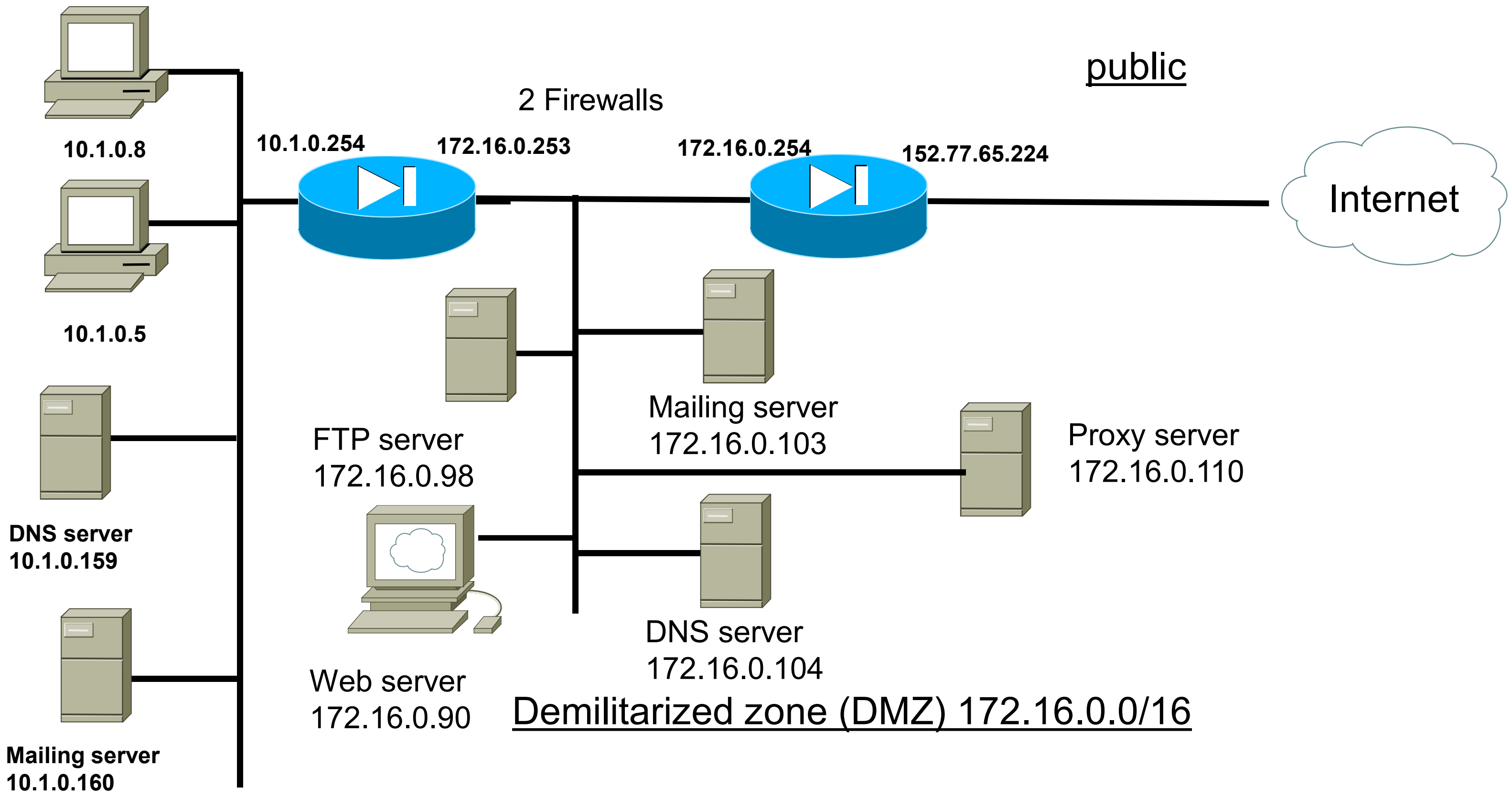
Université Grenoble Alpes

Course on “security of information systems”

5. Security technologies (security of the infrastructures)

DMZ

Internal Corporate
network (private)
10.1.0.0/16



public

2 Firewalls

10.1.0.8

10.1.0.5

DNS server
10.1.0.159

Mailing server
10.1.0.160

10.1.0.254

172.16.0.253

172.16.0.254

152.77.65.224

Internet

FTP server
172.16.0.98

Mailing server
172.16.0.103

Proxy server
172.16.0.110

Web server
172.16.0.90

DNS server
172.16.0.104

Demilitarized zone (DMZ) 172.16.0.0/16

Operation: inspection of each packet

- Source Address
- Destination Address
- Ports

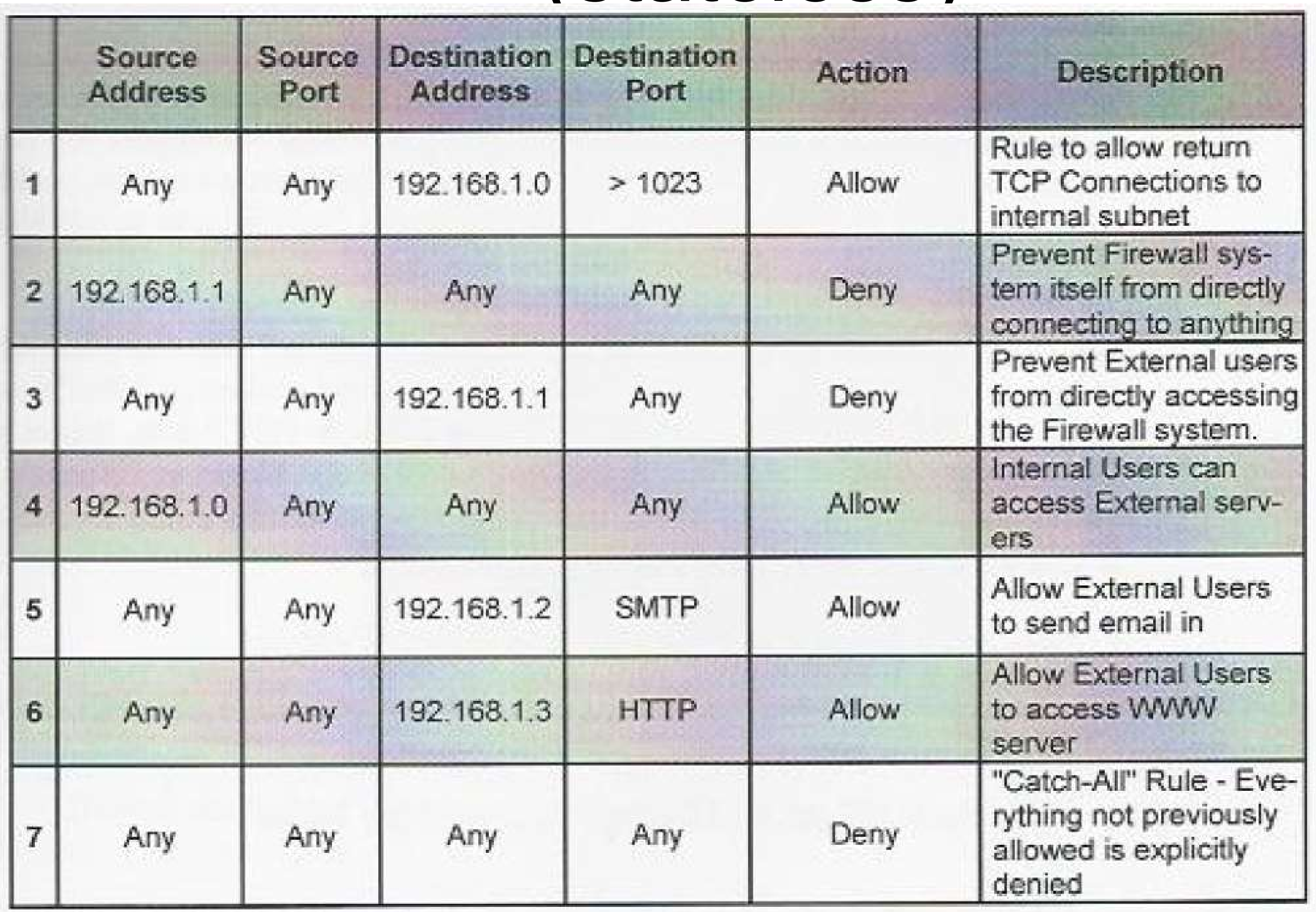
- The decision to authorize or not depends on each inspected point
- Note: fast data processing
- Example of standard ACL on a Cisco router
  - To authorize the packets (permit)
  - To prohibit the packets (deny)

```
                         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
```

Stateless firewall: Filtering of packets by means of ACL (Access Control Lists)

- TCP/IP Data segmented in packets
  - Layer 3 of the TCP/IP model
- Examination of the contents of the packets and application of certain rules
  - Transmission of the packet
  - Removal of the packet
- Very widespread technology at the beginning of Internet
  - First line of defense
- Very much still used in the routers
- First line of defense, combined with other firewalls technologies

Examples of firewall lists (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

Stateful firewall: Dynamic ACL

- Dynamic filtering
  - **Stateful inspection firewall**: packet filters that take into consideration OSI-layer 4 (particularly TCP) => if a connection is authorized, every packet within this exchange will be implicitely accepted
  - Dynamic entries for responses to the TCP, UDP, ICMP requests
  - Does not require to keep open the static ports (the ports remain open only during the time of the session)
- Follow-up/monitoring of the TCP sequence numbers
  - Monitoring of the sequence numbers of the input and output packets to follow-up communication flows
  - Protection against “man in the middle” attacks and session hackings

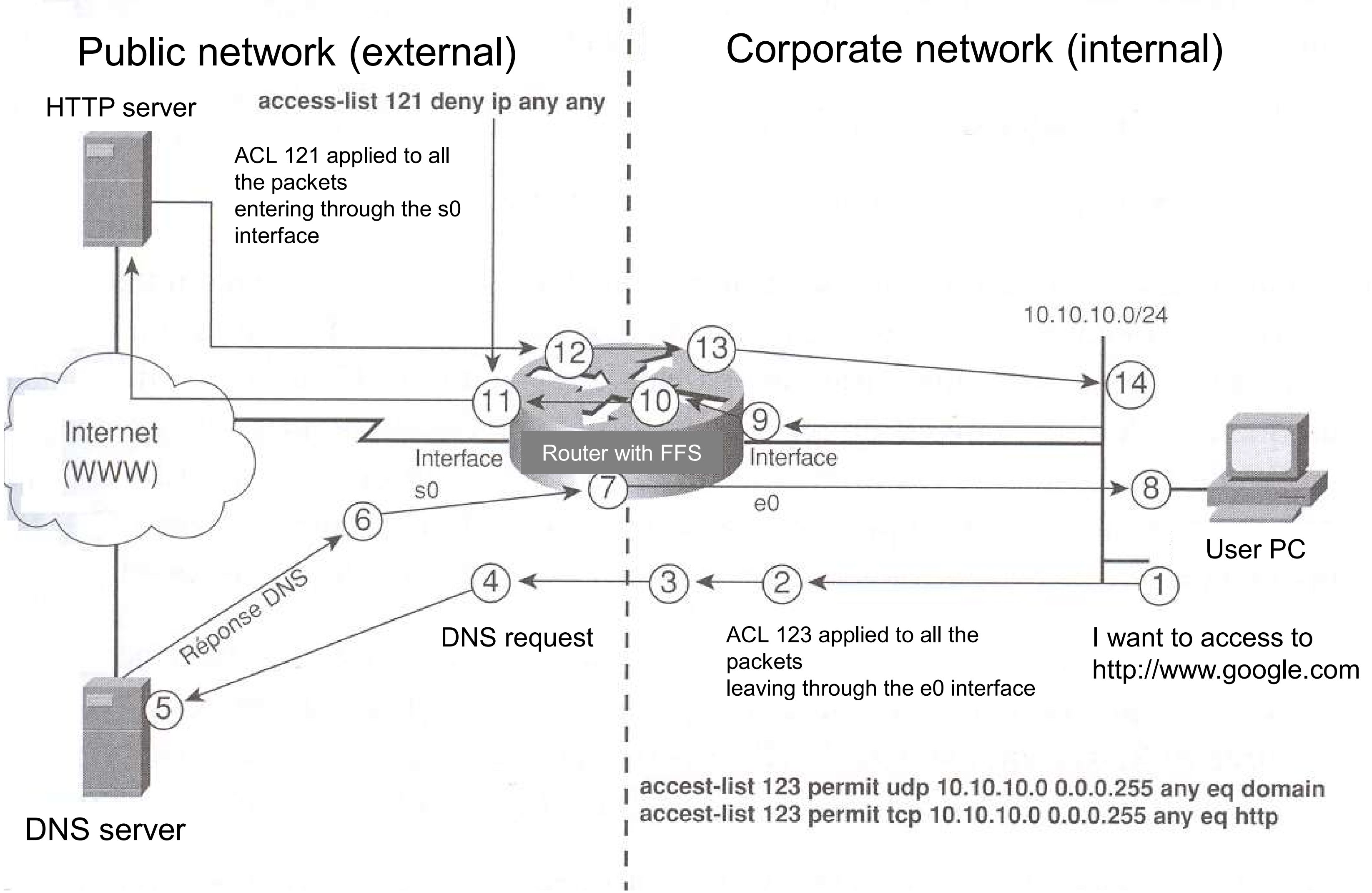
Dynamic ACL

- Follow-up of specific applications (example of protocols)
  - Cu-SeeMe (port 7648): PTP videoconference
  - FTP (port 21)
  - H.323 (port 1720): multi-media communication (VoIP, video, audio)
  - ICMP: repairing of problems (administrator) + used by the pirates => to let pass only ICMP messages generated inside the network
  - MCGP (Media Control Gateway Protocol, port 2427): VoIP
  - MSRPC (Microsoft Remote Procedure Call Protocol, port 135): communication of inter-systems process

Dynamic ACL

- NetShow (port 1755): Microsoft streaming
- R-EXEC (port 512): distant controls (Unix)
- R-SHELL (port 514): distant Shell (Unix)
- RTSP (Real-Time Streaming Protocol, port 544): streaming and VoIP
- SMTP (Simple Mail Transfer Protocol, port 25): mail
- SQLNet (port 1521): Communications clients-database
- Stream Works (port 1558): Real Networks Streaming
- Audio Real (port 7070): Real Networks Streaming
- TFTP (Trivial File Transfer Protocol, port 69): client-server file transfer
- VDOlive (port 7000): streaming

Example (1/5)



access-list 121 deny ip any any

ACL 121 applied to all the packets entering through the s0 interface

ACL 123 applied to all the packets leaving through the e0 interface

I want to access to http://www.google.com

```
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

Example (2/5)

- 1. The user types www.google.fr
  - The station emits a request for DNS name resolution to obtain the URL IP address
- 2. The DNS request packet (a UDP datagram) arrives on the router Ethernet internal interface
  - It is compared with the list “123” (filtering)
  - It is transmitted if authorized or removed
- 3. The authorized packet is controlled by the CBAC (Context-Based Access Control => contextual access control)
  - Inspection
  - Consignment of information in the table of states
    - source IP Address and port number
    - destination IP Address, port number and protocol
- 4. Creation of a temporary instruction `permit` on list 121
  - Authorization of the responding traffic by the destination host (DNS server)
  - Temporary instruction placed in front of the static instructions in the ACL

Example (3/5)

- 5. The DNS request packet (UDP 53 port) is transmitted to the DNS server
  - Response of the DNS server
  - ACL dynamic input kept during 5 seconds
- 6. Arrival of the DNS response packet
  - Comparison with the ACL n. 121
  - Authorized since it belongs to an established session
- 7. Inspection of the DNS response packet
  - Conservation of information until expiration of the timer (timer for the keeping of UDP sessions)
- 8. Arrival of the DNS response to the user PC and initiation by the PC of an HTTP session with google
  - HTTP is based on TCP, therefore the first packet comprises the SYN (synchronization) bit; this bit is activated to start the three-times negotiation process of TCP

Example (4/5)

- 9. HTTP packet is authorized
  - list 123 is authorizing HTTP port n. 80
- 10. Inspection of the output packet and consignment of information in the table of states
  - Source IP address and port
  - Destination IP address, port and protocol
- 11. Creation of a temporary instruction `permit` on list 121
  - Authorization of the traffic in response by the destination host (HTTP server)
  - Temporary instruction placed in front of the static instructions of the ACL
  - Maintenance of the entry during 30 seconds (time to receive a SYN-ACK packet, synchronization-acknowledgement from the Web server)
- 12. Reception of the packet coming from the Web server
  - Authorized by list 121 (because it belongs to an established session)

Example (5/5)

- 13. Inspection of the packet coming from the Web server
  - Elimination of the packet if there are specific violations of protocols
- In the case of HTTP and other protocols requiring several sessions
  - Continual update of the table of states
  - Continual update of the ACL
- Times of removal of temporary entries in the ACL
  - ICMP and UDP, with expiration of a timer (configurable duration)
  - TCP, five seconds after the exchange of FIN packets

Application firewalls

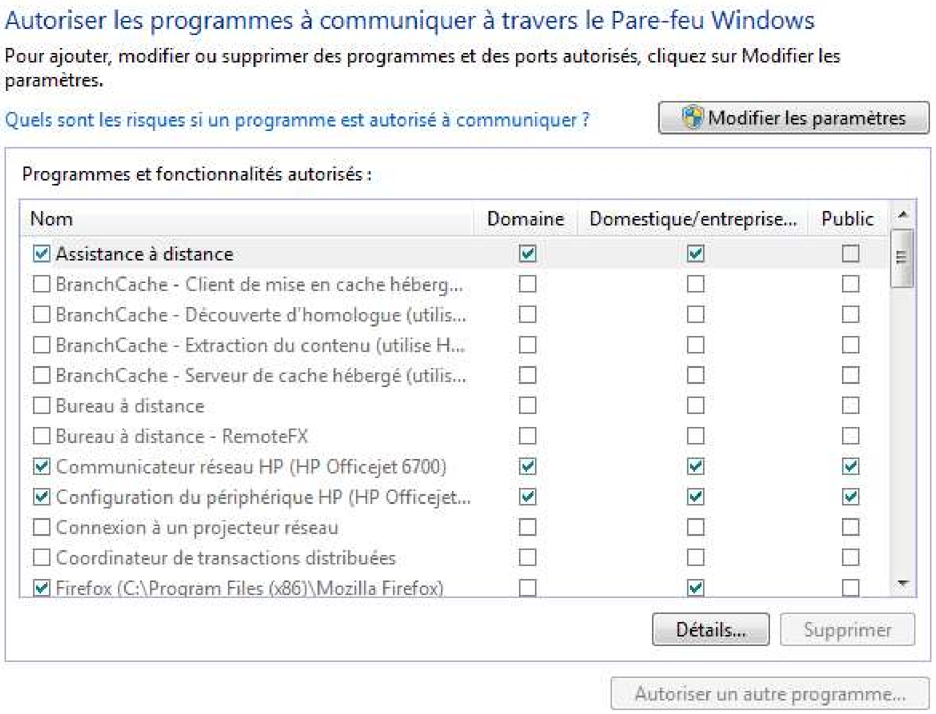
- Last generation of firewall
- Complete conformity of a packet to the expected protocol
- Ex : HTTP protocol only on the TCP port 80
- Need large calculation resources
- Problematics of some protocols not respecting strictly the layer-OSI model (some IP or TCP infos are managed at the application level)

Identifying firewalls

- Identification of connections crossing through the IP filter.
- Filtering rules per user and not only per IP or MAC addresses
- Possibility to monitor the network activity per user
- Dynamic rules based on a user authentication (ex Kerberos), the identity of her/his computer and the level of security (presence of an antivirus, of particular patches)

Personal firewalls

- Important element in a strategy of in-depth security
- Personal firewall
  - May be integrated to the OS (Windows, Mac…)
  - Ex of a configuration panel



Autoriser les programmes à communiquer à travers le Pare-feu Windows

Pour ajouter, modifier ou supprimer des programmes et des ports autorisés, cliquez sur Modifier les paramètres.

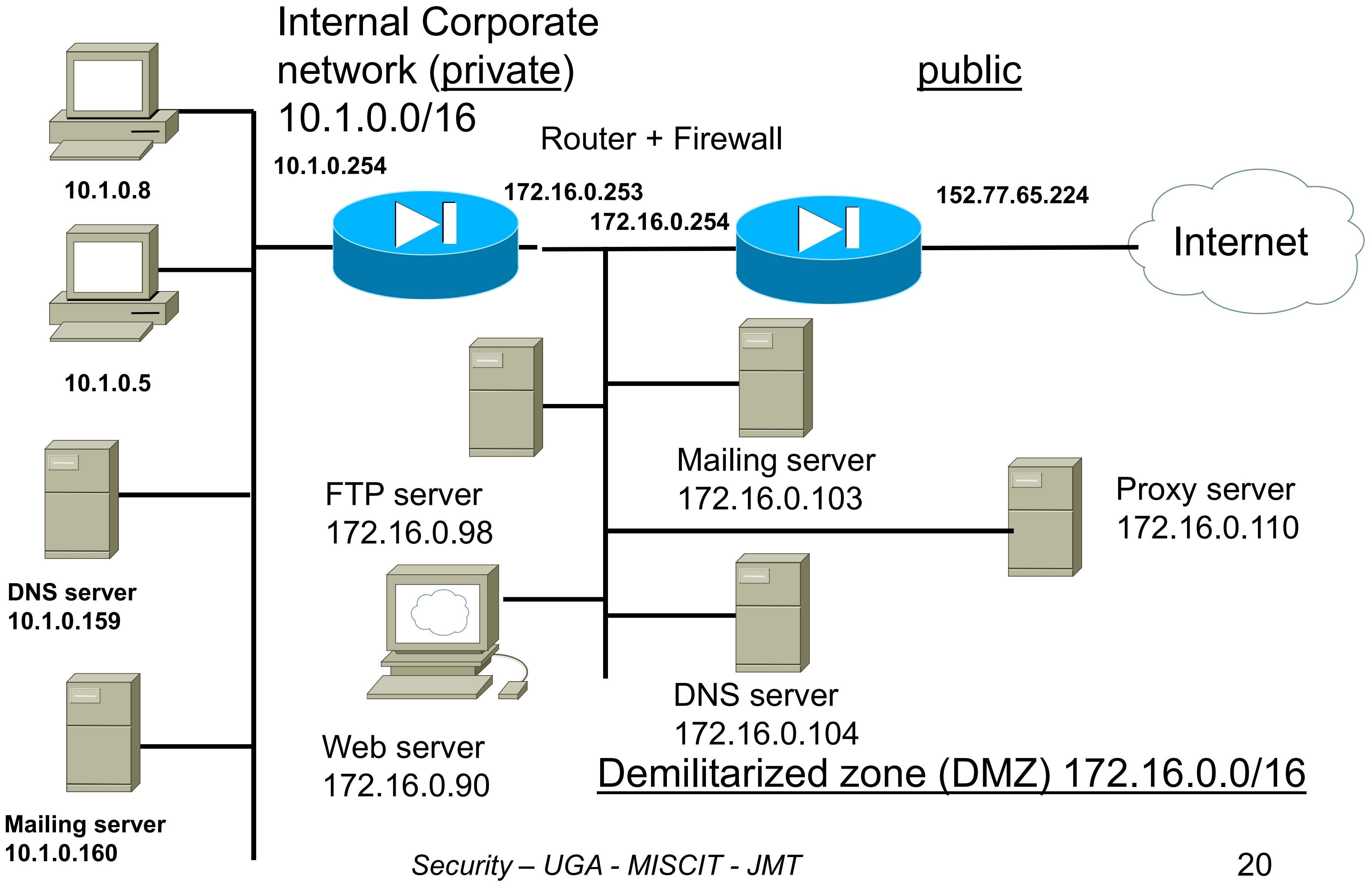
Quels sont les risques si un programme est autorisé à communiquer ?

Programmes et fonctionnalités autorisés :

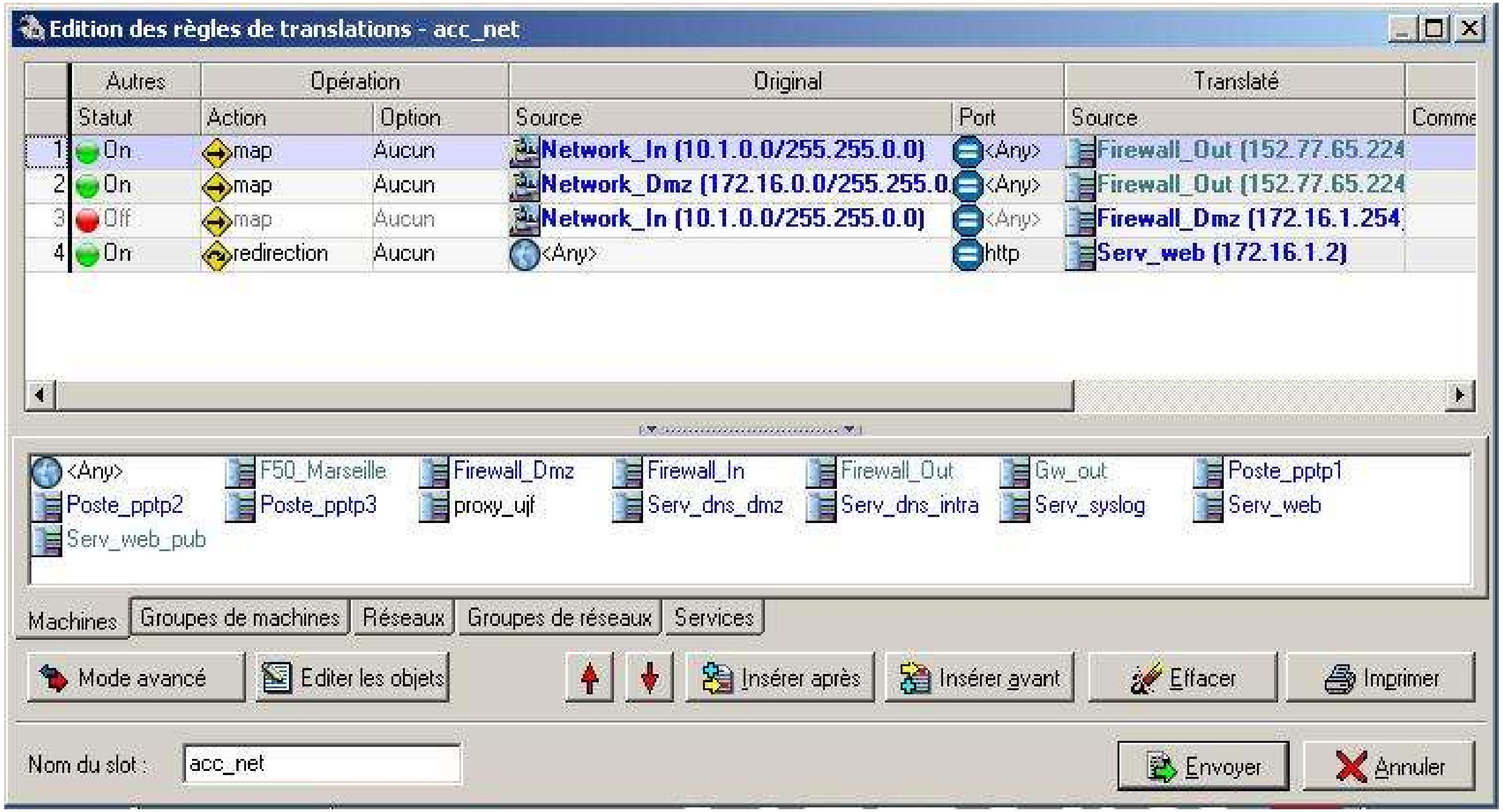
Nom	Domaine	Domestique/entreprise...	Public
☑ Assistance à distance	☑	☑	□
□ BranchCache - Client de mise en cache héberg...	□	□	□
□ BranchCache - Découverte d'homologue (utilis...	□	□	□
□ BranchCache - Extraction du contenu (utilise H...	□	□	□
□ BranchCache - Serveur de cache hébergé (utilis...	□	□	□
□ Bureau à distance	□	□	□
□ Bureau à distance - RemoteFX	□	□	□
☑ Communicateur réseau HP (HP Officejet 6700)	☑	☑	☑
☑ Configuration du périphérique HP (HP Officejet...	☑	☑	☑
□ Connexion à un projecteur réseau	□	□	□
□ Coordinateur de transactions distribuées	□	□	□
☑ Firefox (C:\Program Files (x86)\Mozilla Firefox)	□	☑	□

Type of firewalls

A network with a firewall/router…



Translation (Netsacq)

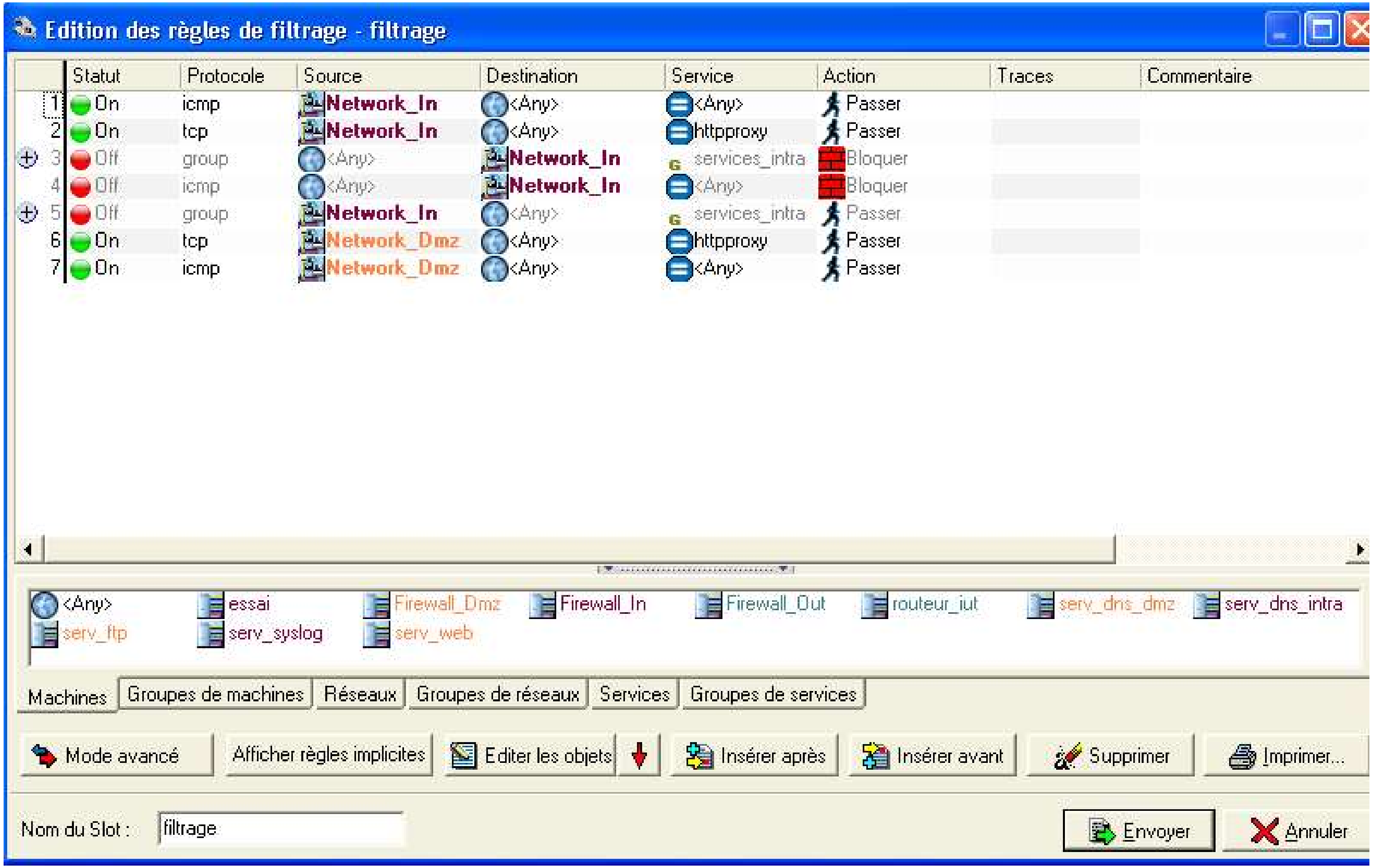


Edition des règles de translations - acc_net

	Autres	Opération		Original		Translaté	
	Statut	Action	Option	Source	Port	Source	Comme
1	On	map	Aucun	Network_In (10.1.0.0/255.255.0.0)	<Any>	Firewall_Out (152.77.65.224	
2	On	map	Aucun	Network_Dmz (172.16.0.0/255.255.0.0	<Any>	Firewall_Out (152.77.65.224	
3	Off	map	Aucun	Network_In (10.1.0.0/255.255.0.0)	<Any>	Firewall_Dmz (172.16.1.254	
4	On	redirection	Aucun	<Any>	http	Serv_web (172.16.1.2)	

Nom du slot : acc_net

Filtering rules (Netascq)



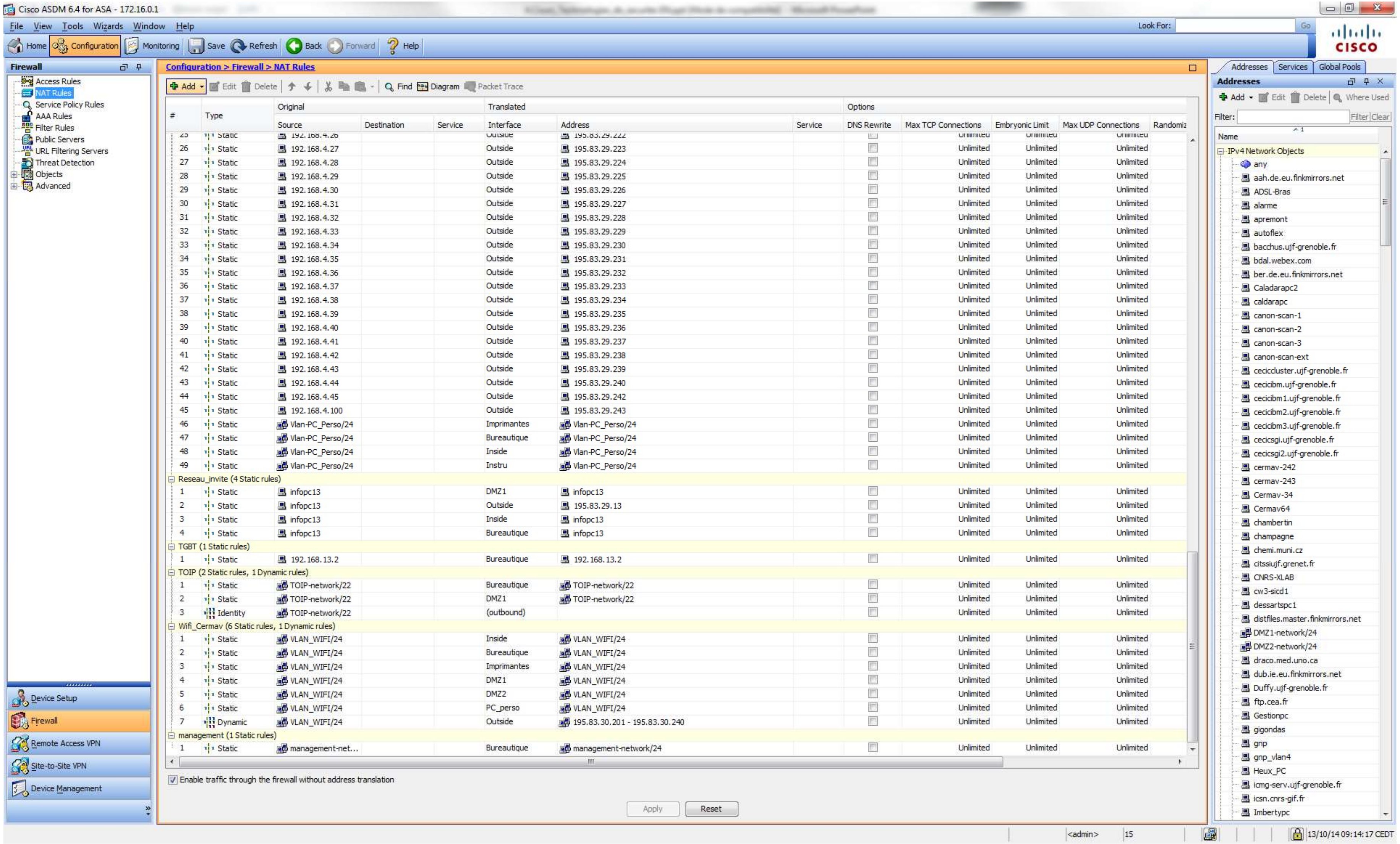
Edition des règles de filtrage - filtrage

	Statut	Protocole	Source	Destination	Service	Action	Traces	Commentaire
1	On	icmp	Network_In	<Any>	<Any>	Passer		
2	On	tcp	Network_In	<Any>	httpproxy	Passer		
⊕ 3	Off	group	<Any>	Network_In	services_intra	Bloquer		
4	Off	icmp	<Any>	Network_In	<Any>	Bloquer		
⊕ 5	Off	group	Network_In	<Any>	services_intra	Passer		
6	On	tcp	Network_Dmz	<Any>	httpproxy	Passer		
7	On	icmp	Network_Dmz	<Any>	<Any>	Passer		

<Any> essai Firewall_Dmz Firewall_In Firewall_Out routeur_iut serv_dns_dmz serv_dns_intra
serv_ftp serv_syslog serv_web

Nom du Slot : filtrage

Translation (Cisco ASA)



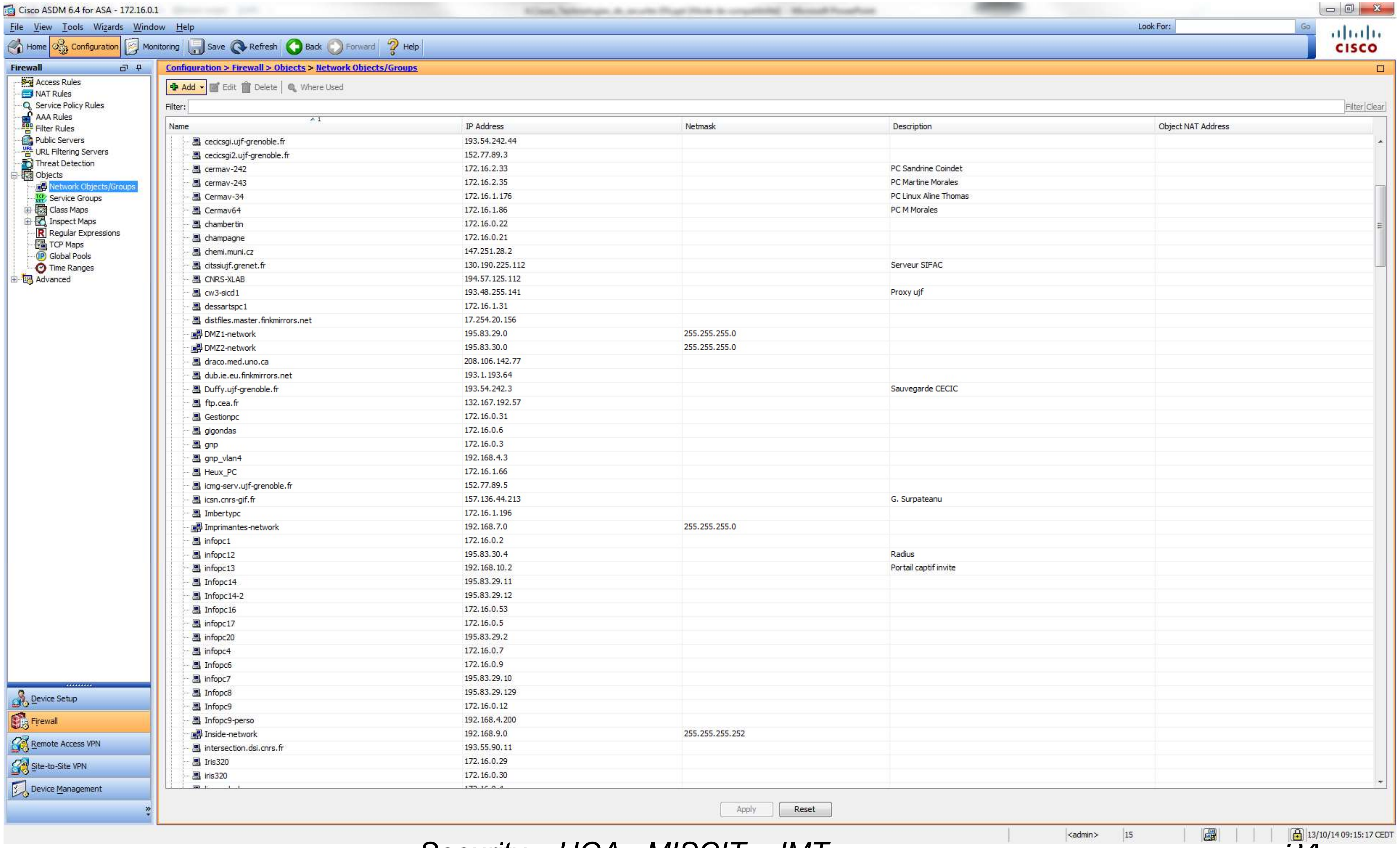
#	Type	Original			Translated			Options				
		Source	Destination	Service	Interface	Address	Service	DNS Rewrite	Max TCP Connections	Embryonic Limit	Max UDP Connections	Randomiz
25	Static	192.168.4.26			Outside	195.83.29.222		☐	Unlimited	Unlimited	Unlimited	
26	Static	192.168.4.27			Outside	195.83.29.223		☐	Unlimited	Unlimited	Unlimited	
27	Static	192.168.4.28			Outside	195.83.29.224		☐	Unlimited	Unlimited	Unlimited	
28	Static	192.168.4.29			Outside	195.83.29.225		☐	Unlimited	Unlimited	Unlimited	
29	Static	192.168.4.30			Outside	195.83.29.226		☐	Unlimited	Unlimited	Unlimited	
30	Static	192.168.4.31			Outside	195.83.29.227		☐	Unlimited	Unlimited	Unlimited	
31	Static	192.168.4.32			Outside	195.83.29.228		☐	Unlimited	Unlimited	Unlimited	
32	Static	192.168.4.33			Outside	195.83.29.229		☐	Unlimited	Unlimited	Unlimited	
33	Static	192.168.4.34			Outside	195.83.29.230		☐	Unlimited	Unlimited	Unlimited	
34	Static	192.168.4.35			Outside	195.83.29.231		☐	Unlimited	Unlimited	Unlimited	
35	Static	192.168.4.36			Outside	195.83.29.232		☐	Unlimited	Unlimited	Unlimited	
36	Static	192.168.4.37			Outside	195.83.29.233		☐	Unlimited	Unlimited	Unlimited	
37	Static	192.168.4.38			Outside	195.83.29.234		☐	Unlimited	Unlimited	Unlimited	
38	Static	192.168.4.39			Outside	195.83.29.235		☐	Unlimited	Unlimited	Unlimited	
39	Static	192.168.4.40			Outside	195.83.29.236		☐	Unlimited	Unlimited	Unlimited	
40	Static	192.168.4.41			Outside	195.83.29.237		☐	Unlimited	Unlimited	Unlimited	
41	Static	192.168.4.42			Outside	195.83.29.238		☐	Unlimited	Unlimited	Unlimited	
42	Static	192.168.4.43			Outside	195.83.29.239		☐	Unlimited	Unlimited	Unlimited	
43	Static	192.168.4.44			Outside	195.83.29.240		☐	Unlimited	Unlimited	Unlimited	
44	Static	192.168.4.45			Outside	195.83.29.242		☐	Unlimited	Unlimited	Unlimited	
45	Static	192.168.4.100			Outside	195.83.29.243		☐	Unlimited	Unlimited	Unlimited	
46	Static	Vlan-PC_Perso/24			Imprimantes	Vlan-PC_Perso/24		☐	Unlimited	Unlimited	Unlimited	
47	Static	Vlan-PC_Perso/24			Bureautique	Vlan-PC_Perso/24		☐	Unlimited	Unlimited	Unlimited	
48	Static	Vlan-PC_Perso/24			Inside	Vlan-PC_Perso/24		☐	Unlimited	Unlimited	Unlimited	
49	Static	Vlan-PC_Perso/24			Instru	Vlan-PC_Perso/24		☐	Unlimited	Unlimited	Unlimited	
⊟ Reseau_invite (4 Static rules)												
1	Static	infopc13			DMZ1	infopc13		☐	Unlimited	Unlimited	Unlimited	
2	Static	infopc13			Outside	195.83.29.13		☐	Unlimited	Unlimited	Unlimited	
3	Static	infopc13			Inside	infopc13		☐	Unlimited	Unlimited	Unlimited	
4	Static	infopc13			Bureautique	infopc13		☐	Unlimited	Unlimited	Unlimited	
⊟ TGBT (1 Static rules)												
1	Static	192.168.13.2			Bureautique	192.168.13.2		☐	Unlimited	Unlimited	Unlimited	
⊟ TOIP (2 Static rules, 1 Dynamic rules)												
1	Static	TOIP-network/22			Bureautique	TOIP-network/22		☐	Unlimited	Unlimited	Unlimited	
2	Static	TOIP-network/22			DMZ1	TOIP-network/22		☐	Unlimited	Unlimited	Unlimited	
3	Identity	TOIP-network/22			(outbound)			☐	Unlimited	Unlimited	Unlimited	
⊟ Wifi_Cermav (6 Static rules, 1 Dynamic rules)												
1	Static	VLAN_WIFI/24			Inside	VLAN_WIFI/24		☐	Unlimited	Unlimited	Unlimited	
2	Static	VLAN_WIFI/24			Bureautique	VLAN_WIFI/24		☐	Unlimited	Unlimited	Unlimited	
3	Static	VLAN_WIFI/24			Imprimantes	VLAN_WIFI/24		☐	Unlimited	Unlimited	Unlimited	
4	Static	VLAN_WIFI/24			DMZ1	VLAN_WIFI/24		☐	Unlimited	Unlimited	Unlimited	
5	Static	VLAN_WIFI/24			DMZ2	VLAN_WIFI/24		☐	Unlimited	Unlimited	Unlimited	
6	Static	VLAN_WIFI/24			PC_perso	VLAN_WIFI/24		☐	Unlimited	Unlimited	Unlimited	
7	Dynamic	VLAN_WIFI/24			Outside	195.83.30.201 - 195.83.30.240		☐	Unlimited	Unlimited	Unlimited	
⊟ management (1 Static rules)												
1	Static	management-net...			Bureautique	management-network/24		☐	Unlimited	Unlimited	Unlimited	

☑ Enable traffic through the firewall without address translation

Name

⊟ IPv4 Network Objects
- any
- aah.de.eu.finkmirrors.net
- ADSL-Bras
- alarme
- apremont
- autoflex
- bacchus.ujf-grenoble.fr
- bdal.webex.com
- ber.de.eu.finkmirrors.net
- Caladarapc2
- caldarapc
- canon-scan-1
- canon-scan-2
- canon-scan-3
- canon-scan-ext
- ceciccluster.ujf-grenoble.fr
- cecicibm.ujf-grenoble.fr
- cecicibm1.ujf-grenoble.fr
- cecicibm2.ujf-grenoble.fr
- cecicibm3.ujf-grenoble.fr
- cecicsgi.ujf-grenoble.fr
- cecicsgi2.ujf-grenoble.fr
- cermav-242
- cermav-243
- Cermav-34
- Cermav64
- chambertin
- champagne
- chemi.muni.cz
- citssiujf.grenet.fr
- CNRS-XLAB
- cw3-sicd1
- dessartspc1
- distfiles.master.finkmirrors.net
- DMZ1-network/24
- DMZ2-network/24
- draco.med.uno.ca
- dub.ie.eu.finkmirrors.net
- Duffy.ujf-grenoble.fr
- ftp.cea.fr
- Gestionpc
- gigondas
- gnp
- gnp_vlan4
- Heux_PC
- icmg-serv.ujf-grenoble.fr
- icsn.cnrs-gif.fr
- Imbertypc

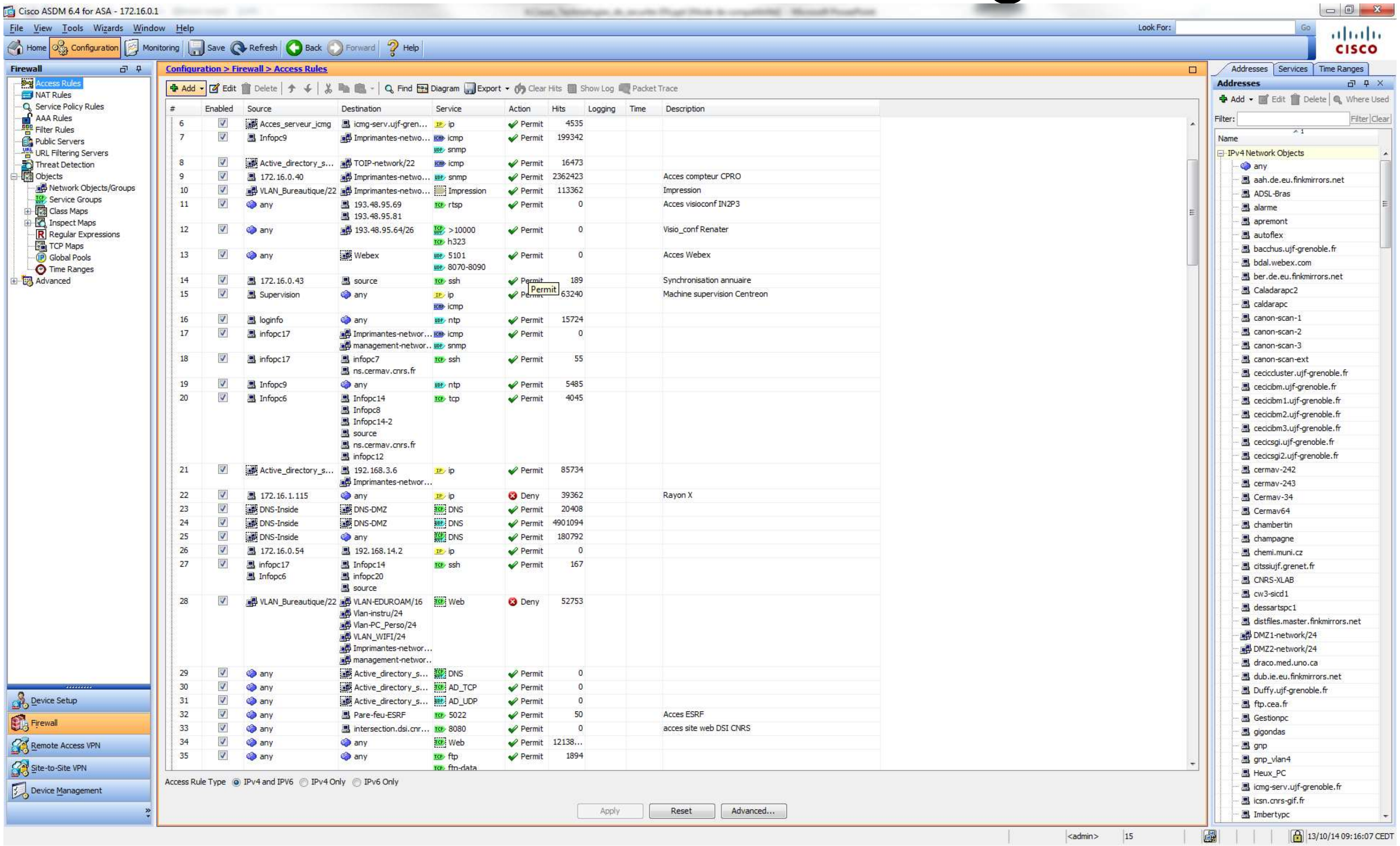
Cisco ASA Firewall
Definition of the machines/hosts



Configuration > Firewall > Objects > Network Objects/Groups

Name	IP Address	Netmask	Description	Object NAT Address
cecicsgi.ujf-grenoble.fr	193.54.242.44			
cecicsgi2.ujf-grenoble.fr	152.77.89.3			
cermav-242	172.16.2.33		PC Sandrine Coindet	
cermav-243	172.16.2.35		PC Martine Morales	
Cermav-34	172.16.1.176		PC Linux Aline Thomas	
Cermav64	172.16.1.86		PC M Morales	
chambertin	172.16.0.22			
champagne	172.16.0.21			
chemi.muni.cz	147.251.28.2			
citssiujf.grenet.fr	130.190.225.112		Serveur SIFAC	
CNRS-XLAB	194.57.125.112			
cw3-sicd1	193.48.255.141		Proxy ujf	
dessartspc1	172.16.1.31			
distfiles.master.finkmirrors.net	17.254.20.156			
DMZ1-network	195.83.29.0	255.255.255.0		
DMZ2-network	195.83.30.0	255.255.255.0		
draco.med.uno.ca	208.106.142.77			
dub.ie.eu.finkmirrors.net	193.1.193.64			
Duffy.ujf-grenoble.fr	193.54.242.3		Sauvegarde CECIC	
ftp.cea.fr	132.167.192.57			
Gestionpc	172.16.0.31			
gigondas	172.16.0.6			
gnp	172.16.0.3			
gnp_vlan4	192.168.4.3			
Heux_PC	172.16.1.66			
icmg-serv.ujf-grenoble.fr	152.77.89.5			
icsn.cnrs-gif.fr	157.136.44.213		G. Surpateanu	
Imbertypc	172.16.1.196			
Imprimantes-network	192.168.7.0	255.255.255.0		
infopc1	172.16.0.2			
infopc12	195.83.30.4		Radius	
infopc13	192.168.10.2		Portail captif invite	
Infopc14	195.83.29.11			
Infopc14-2	195.83.29.12			
Infopc16	172.16.0.53			
infopc17	172.16.0.5			
infopc20	195.83.29.2			
infopc4	172.16.0.7			
Infopc6	172.16.0.9			
infopc7	195.83.29.10			
Infopc8	195.83.29.129			
Infopc9	172.16.0.12			
Infopc9-perso	192.168.4.200			
Inside-network	192.168.9.0	255.255.255.252		
intersection.dsi.cnrs.fr	193.55.90.11			
Iris320	172.16.0.29			
iris320	172.16.0.30			

Cisco ASA Filtering rules



#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
6	☑	Acces_serveur_icmg	icmg-serv.ujf-gren...	ip	✓ Permit	4535			
7	☑	Infopc9	Imprimantes-netwo...	icmp snmp	✓ Permit	199342			
8	☑	Active_directory_s...	TOIP-network/22	icmp	✓ Permit	16473			
9	☑	172.16.0.40	Imprimantes-netwo...	snmp	✓ Permit	2362423			Acces compteur CPRO
10	☑	VLAN_Bureautique/22	Imprimantes-netwo...	Impression	✓ Permit	113362			Impression
11	☑	any	193.48.95.69 193.48.95.81	rtsp	✓ Permit	0			Acces visioconf IN2P3
12	☑	any	193.48.95.64/26	>10000 h323	✓ Permit	0			Visio_conf Renater
13	☑	any	Webex	5101 8070-8090	✓ Permit	0			Acces Webex
14	☑	172.16.0.43	source	ssh	✓ Permit	189			Synchronisation annuaire
15	☑	Supervision	any	ip icmp	✓ Permit	63240			Machine supervision Centreon
16	☑	loginfo	any	ntp	✓ Permit	15724			
17	☑	infopc17	Imprimantes-networ... management-networ...	icmp snmp	✓ Permit	0			
18	☑	infopc17	infopc7 ns.cermav.cnrs.fr	ssh	✓ Permit	55			
19	☑	Infopc9	any	ntp	✓ Permit	5485			
20	☑	Infopc6	Infopc14 Infopc8 Infopc14-2 source ns.cermav.cnrs.fr infopc12	tcp	✓ Permit	4045			
21	☑	Active_directory_s...	192.168.3.6 Imprimantes-networ...	ip	✓ Permit	85734			
22	☑	172.16.1.115	any	ip	✗ Deny	39362			Rayon X
23	☑	DNS-Inside	DNS-DMZ	DNS	✓ Permit	20408			
24	☑	DNS-Inside	DNS-DMZ	DNS	✓ Permit	4901094			
25	☑	DNS-Inside	any	DNS	✓ Permit	180792			
26	☑	172.16.0.54	192.168.14.2	ip	✓ Permit	0			
27	☑	infopc17 Infopc6	Infopc14 infopc20 source	ssh	✓ Permit	167			
28	☑	VLAN_Bureautique/22	VLAN-EDUROAM/16 Vlan-instru/24 Vlan-PC_Perso/24 VLAN_WIFI/24 Imprimantes-networ... management-networ...	Web	✗ Deny	52753			
29	☑	any	Active_directory_s...	DNS	✓ Permit	0			
30	☑	any	Active_directory_s...	AD_TCP	✓ Permit	0			
31	☑	any	Active_directory_s...	AD_UDP	✓ Permit	0			
32	☑	any	Pare-feu-ESRF	5022	✓ Permit	50			Acces ESRF
33	☑	any	intersection.dsi.cnr...	8080	✓ Permit	0			acces site web DSI CNRS
34	☑	any	any	Web	✓ Permit	12138...			
35	☑	any	any	ftp ftp-data	✓ Permit	1894			

Access Rule Type ● IPv4 and IPV6 ○ IPv4 Only ○ IPv6 Only

Name
IPv4 Network Objects
any
aah.de.eu.finkmirrors.net
ADSL-Bras
alarme
apremont
autoflex
bacchus.ujf-grenoble.fr
bdal.webex.com
ber.de.eu.finkmirrors.net
Caladarapc2
caldarapc
canon-scan-1
canon-scan-2
canon-scan-3
canon-scan-ext
ceciccluster.ujf-grenoble.fr
cecicibm.ujf-grenoble.fr
cecicibm1.ujf-grenoble.fr
cecicibm2.ujf-grenoble.fr
cecicibm3.ujf-grenoble.fr
cecicsgi.ujf-grenoble.fr
cecicsgi2.ujf-grenoble.fr
cermav-242
cermav-243
Cermav-34
Cermav64
chambertin
champagne
chemi.muni.cz
citssiujf.grenet.fr
CNRS-XLAB
cw3-sicd1
dessartspc1
distfiles.master.finkmirrors.net
DMZ1-network/24
DMZ2-network/24
draco.med.uno.ca
dub.ie.eu.finkmirrors.net
Duffy.ujf-grenoble.fr
ftp.cea.fr
Gestionpc
gigondas
gnp
gnp_vlan4
Heux_PC
icmg-serv.ujf-grenoble.fr
icsn.cnrs-gif.fr
Imbertypc

Software firewall

- Suppression of every packets if they fit any conditions:
- 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

Place of the firewalls

- Where should we put the firewalls?
  - At the connection interface between internal network and outside (Internet)
  - Between various portions of internal networks (large companies)
  - On each machine

Firewalls limitations

- Cannot prevent users or attackers using modems to reach inside the network
- Cannot prevent a misuse of the passwords (non respect of the passwords strategy by the users)
- Concentration of the traffic in only one point = bottleneck = source of fatal breakdown

Criteria for the good choice of a firewall

- Nature, type of applications (FTP, email, SNMP, Audio, Video)
- Distribution and Load Balancing (QoS)
- type of filtering (network level, application level)
- Records, logs, for audit purpose
- Tools, aids for administration
- Ability to support an encrypted tunnel (VPN)
- tools for monitoring, alarms, active audit
- Vulnerabilities: Intrusion => configuration changes, access, modification or erasure of traces of logging, viral infection
- Rating: cf Common Criteria organization (www.commoncriteriaportal.org)

Guiding principles for the configuration of a firewall

- Less privilege: do not grant the users with a higher level of rights that they need; to prohibit for example the peer-to-peer protocol within a company
- Default Prohibition: To prohibit everything by default: everything which is authorized should be explicitely authorized
- In-depth defense: to use the protection means at all the possible levels, for example by analyzing and filtering everything which can be analyzed at the level of the firewall. This principle prevents letting enter the network undesirable communications, even if another method of control is used more in-depth in the network
- Bottleneck: all the communications incoming and outgoing of the network must pass through the firewall. Other paths are strictly forbidden, such as for example unauthorized modems or access points
- Simplicity: the firewall filtering rules must be the simplest and most comprehensible as possible in order to avoid any error on behalf of the administrator or his successors (every rule should be documented and traceable)
- Participation of the users: the users must be involved in the firewall definition. They must indeed express their needs and receive in exchange the reasons and the objectives of the installation of such a device; the constraints related with the firewall will be accepted thus better.

DMZ, demilitarized zone (concept of perimetric security)

Demilitarized zone (perimetric security) (DMZ)

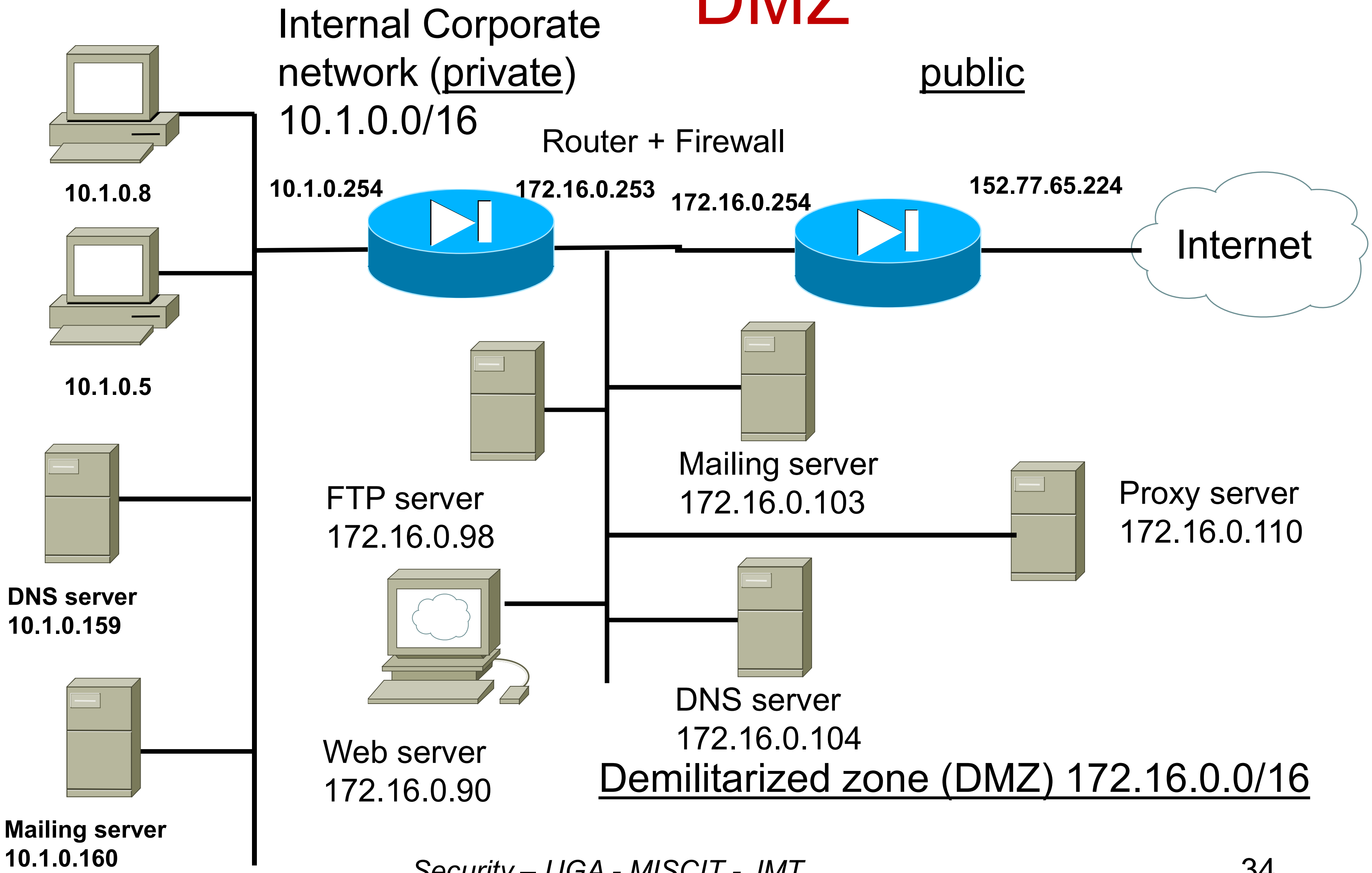
- Specific isolated zone of the internal network (between the public zone and the private zone)
  - Web server
  - Mailing server
  - FTP server
  - …
- This strategy allows the traffic coming from Internet to go in this zone, but not to penetrate elsewhere in the internal network
- Possibility of audit traffic exchanged with the DMZ
- Possibility of placing an intrusion detection system (IDS)

DMZ: its role

- To propose a zone
  - Receiving requests from outside
  - Does not allow direct communication from outside
  - Using its own addressing policy
- Access to the zone
  - Through the router from outside
  - Through the router + NAT from inside
- To realise a buffer zone
  - Can be corrupted
  - Does not reveal the presence of the local network

A network with a firewall/router…

DMZ



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)
- The machines from the DMZ should be able to reach any machine outside BUT NOT inside (for the mail)
- 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)
  - 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)
  - The proxy should be able to reach any http server (port 80) everywhere
- We should not forget the DNS aspects (port 53)

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

Protocol e	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

Some considerations about NAT

Network Address Translation

NAT function (network address translation)

- Internet Addresses (IPv4)
  - Theory, 2^{32} addresses (~4,3.10^{9} addresses)
  - Practical
    - Public addresses: ~3,2.10^{9}
    - Reserved addresses: test…
    - Private addresses: reserved for the internal networks (non accessible from outside)
      - 10.0.0.0 to 10.255.255.255 (prefix 10/8)
      - 172.16.0.0 to 172.31.255.255 (prefix 172.16/12)
      - 192.168.0.0 to 192.168.255.255 (prefix 192.168/16)
- NAT ensures the conversion between public and private addresses, between the internal network and the outside accesses
  - firewall,
  - sometimes a router or a computer

NAT

- Static NAT
  - Always the same public IP address to a given private IP address
  - Ex: Web server
- Dynamic NAT
  - Association of a random public address drawn from a group, to a private IP address
- PAT (Port Address translation)
  - Associate only one public address to several private addresses by using various ports
  - *Let's remember*: 65.535 TCP ports are supported by an IP address

Security with NAT

- More difficult for an attacker to:
  - Determine the topology of the network and the type of connectivity of the target company
  - Identify the number of systems which are running on the network
  - Identify the type of machines and their operating systems
  - Carry out attacks such as denial of service (Ex: SYN Flood, scan of ports, packets injection)

Disadvantages of NAT

- Bad management of UDP connections
  - Difficult estimation of how many time must the connection remain open
- Other protocols are badly managed
  - Kerberos, X Windows, rsh (remote shell), SIP (Session Initiation Protocol)
- Systems of ciphering and authentication
  - These systems are based on the integrity of the packets
  - However NAT modifies these packets
- Journalizing is complicated
  - Analyzing the correlation between journals requires to take into considerations the NAT
- Problem with the sharing of address with PAT
  - Authentication by a protected external resource (all the users sharing the same address are likely to be able to use this resource)

References

- 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 steps towards a secure network environment), 2006, SNAC