Firewalls

Chapter 3

Network & Security

Gildas Avoine

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

IUF

SUMMARY OF CHAPTER 3

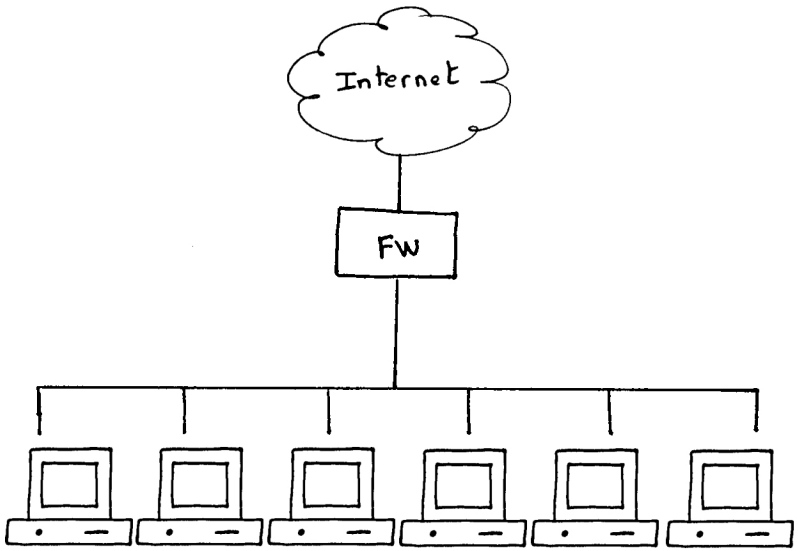
- Introduction
- Basic Principles
- Features
- Architectures
- Rules Organization
- Conclusion and References

INTRODUCTION

- Introduction
- Basic Principles
- Features
- Architectures
- Rules Organization
- Conclusion and References

Firewalls for Dummies

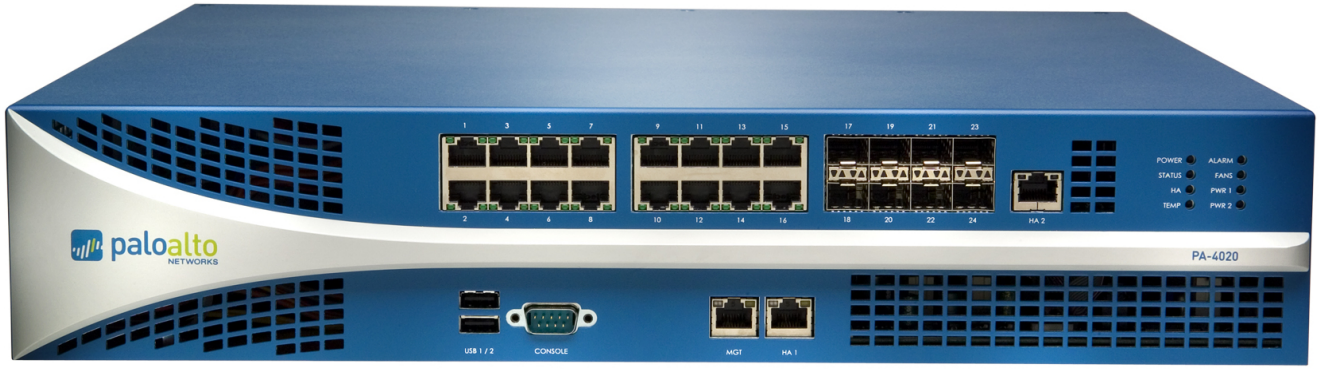
- An original firewall prevents the propagation of a fire.
- Network firewalls must prevent the propagation of an attack, while allowing desired traffic.



- A firewall can be made of one or several components.
- Firewalls can be software or hardware.

Types of Firewalls

- Software.
  - Standard workstation with firewall software: Checkpoint, IPcop, IPtables (nftables).
- Hardware.
  - Specialized black box (that also contains software): Cisco PIX, Juniper, WatchGuard, SonicWall.



Software vs Hardware

- Software firewalls inherit all vulnerabilities of the OS on which they run.
- Software firewall architectures are well known, it is easier to exploit its vulnerabilities (eg. Buffer overflow).
- Software firewalls often have better performance: they benefit of rapid advances and low prices in PC hardware.

BASIC PRINCIPLES

- Introduction
- Basic Principles
- Features
- Architectures
- Rules Organization
- Conclusion and References

The Seven Principles

- Least privileges.
- Defense in depth.
- Choke point.
- Weakest link.
- Deny by default.
- User participation.
- Simplicity.

Principle: Least Privileges

- Every element of a system (user, software) must only have the minimal rights necessary to carry out its task.
- Examples:
  - Regular users must not be administrators.
  - Administrators must also use regular user accounts.
  - A Web server runs under a non-privileged account (Unix: nobody; Windows: IUSR).

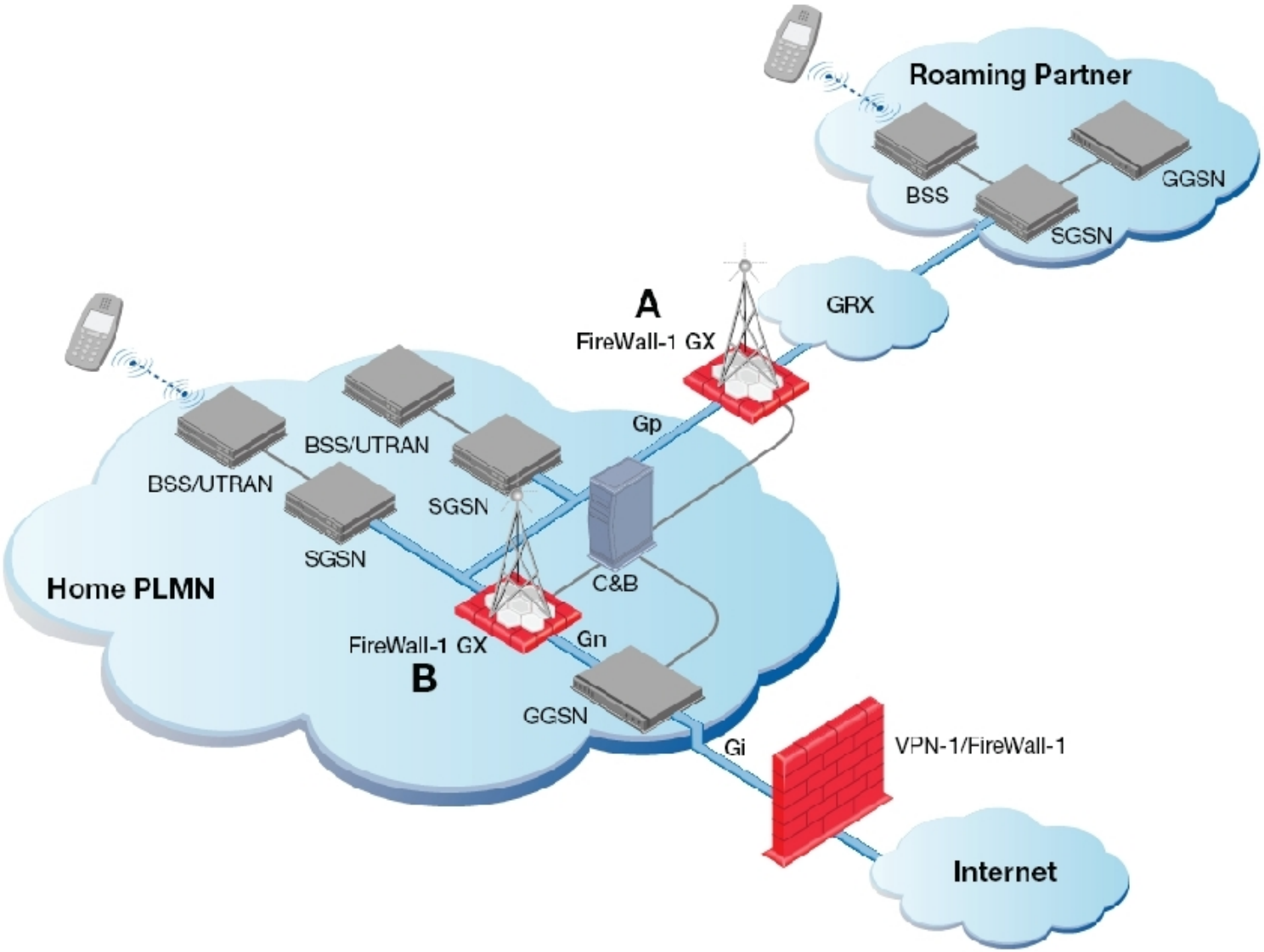
Principle: Defense in Depth

- Several security measures are better than a single one.
- Example:
  - Anti-virus software on mail servers and on desktops.
  - We also secure (configuration, patches) machines that are protected by a firewall.
  - Even if FTP connections are blocked by the firewall, workstations should not run FTP servers.

Principle: Choke Point

- It is easier to control security if all data has to go through a single point.
- Users should not be allowed to use clandestine access points (eg. modems, smartphones,...) to their machines.
- Interconnections with other companies must go through the firewall.

Principle: Choke Point



Principle: Weakest Link

- The firewall is only as secure as its weakest link.
- That is useless to spend money to protect a part of the FW if other parts are not protected.
- Example:
  - Useless to install expensive anti-virus software for HTTP traffic if you do not also install one for SMTP traffic

Principle: Deny by Default

- It is better to prohibit all that is not explicitly authorized than to authorize all that is not explicitly prohibited.
- We can never know in advance all the threats to which we will be exposed.
- If we make an error, it is better to prohibit something useful than enabling an attack.

Principle: User Participation

- A protection system is efficient only if all users support it (Thucydide).
- The goal of a firewall is to authorize all that is useful and at the same time avoid dangers.
- A system that is too restrictive pushes users to be creative.
- We must understand the user's needs and make sure that reasons for restrictions are well understood by them.

Principle: Simplicity

- Most security problems originate from human error.
- In a simple system:
  - The risk of error is smaller.
  - It is easier to verify its correct functioning.
  - Especially in evolving networks.
  - Especially with several administrators.

FEATURES

- Introduction
- Basic Principles
- Features
- Architectures
- Rules Organization
- Conclusion and References

Firewall Features

- Filtering.
- Network Address Translation.
- Content Analysis.
- Authentication.
- Remote Network Access.

Filtering

- Filtering helps limiting traffic to useful services. Can be based on multiple criteria:
  - IP addresses source or destination.
  - Protocols (TCP, UDP, ICMP, ...) and ports.
  - Flags and options (syn, ack, ICMP message type, ...)
- Filtering of source addresses prevents IP spoofing.
- Filtering of flags allows defining the direction in which connections can be established.

Filtering Rules (Organization)

- Filtering rules are specified in a list.
- FW runs through the list until it finds a rule that applies.
- FW executes the action specified by the rule and moves on to the next packet.
- We create a last rule that prohibits all that has not been authorized.

Filtering Rules: A Simple Example

	Src	Port	Dst	Port	Prot	Action
1	any	any	128.3.3.1	25	tcp	allow
2	128.3.3.1	25	any	any	tcp	allow
3	128.3.3.1	any	any	25	tcp	allow
4	any	25	128.3.3.1	any	tcp	allow
5	any	any	any	any	any	deny

- Problem: all ports of the server are accessible as long as the hacker chooses port 25 as source port.

Filtering Rules: Corrected Example

- Specification of the `ack` flag prevents the sending of `syn` packets and hence the establishment of connections.

	Src	Port	Dst	Port	Prot	Flag	Action
1	any	any	128.3.3.1	25	tcp	ACK=*	allow
2	128.3.3.1	25	any	any	tcp	ACK=1	allow
3	128.3.3.1	any	any	25	tcp	ACK=*	allow
4	any	25	128.3.3.1	any	tcp	ACK=1	allow
5	any	any	any	any	any	ACK=*	deny

- Problem: the attacker can still send un-solicited `ack` packets (scanning, denial of service).

Stateless vs Stateful

- Without memory (stateless)
  - Does not remember already-seen packets.
- With memory (stateful)
  - Keeps a trace of packets that pass by.
  - Reconstructs each connection's state, or even certain protocols.

Stateful Firewalls: Filtering

- For each connection, the FW knows what the next packet should look like: flags, sequence numbers.
- Stateful FW knows the established connections and can automatically authorize returning traffic.
- FW can eliminate packets that do not fit in.

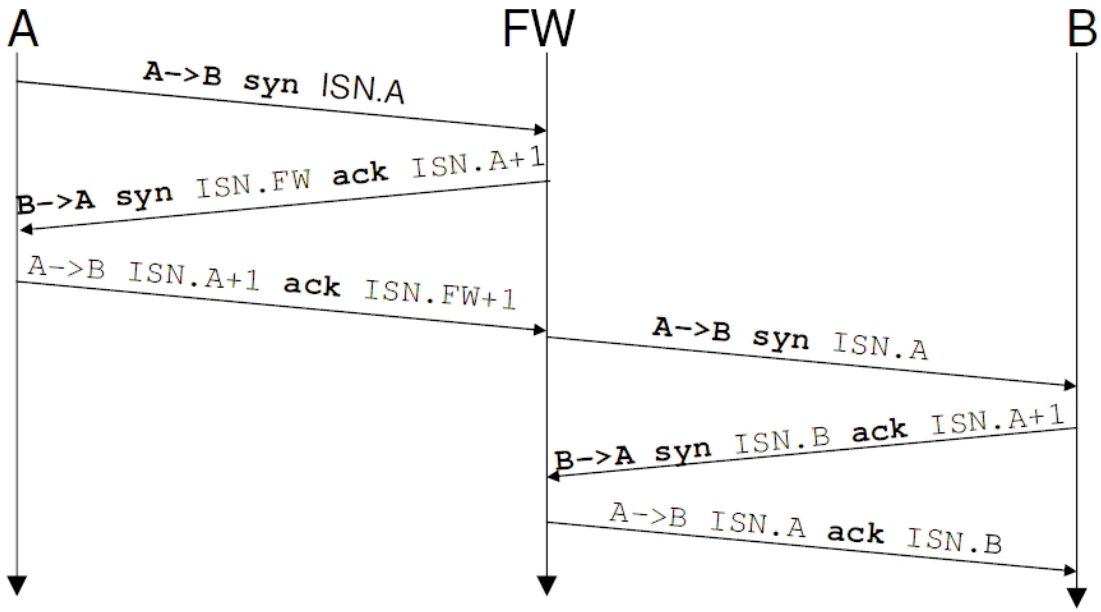
	Src	Port	Dst	Port	Prot	Action
1	any	any	128.3.3.1	25	tcp	allow
3	128.3.3.1	any	any	25	tcp	allow
5	any	any	any	any	any	deny

- Simpler to configure, hence less errors.
- May suffer from denial of service attacks.

Stateful Firewalls: Protection Against Syn-Flooding

- Simple.
  - FW keeps track of all attempts to open a connection.
  - If it judges that a connection stays half-open for too long, it sends a `rst` packet to the server.
- Advanced.
  - FW delays `syn` packets and generates a `syn-ack` packet in place of the server.
  - Only when it receives an `ack` packet does it send the original `syn` packet to the server.

Stateful Firewalls: Protection Against Syn-Flooding



- FW must generate an ISN in place of the server.
- FW spends the rest of the connection adjusting seq. numbers.

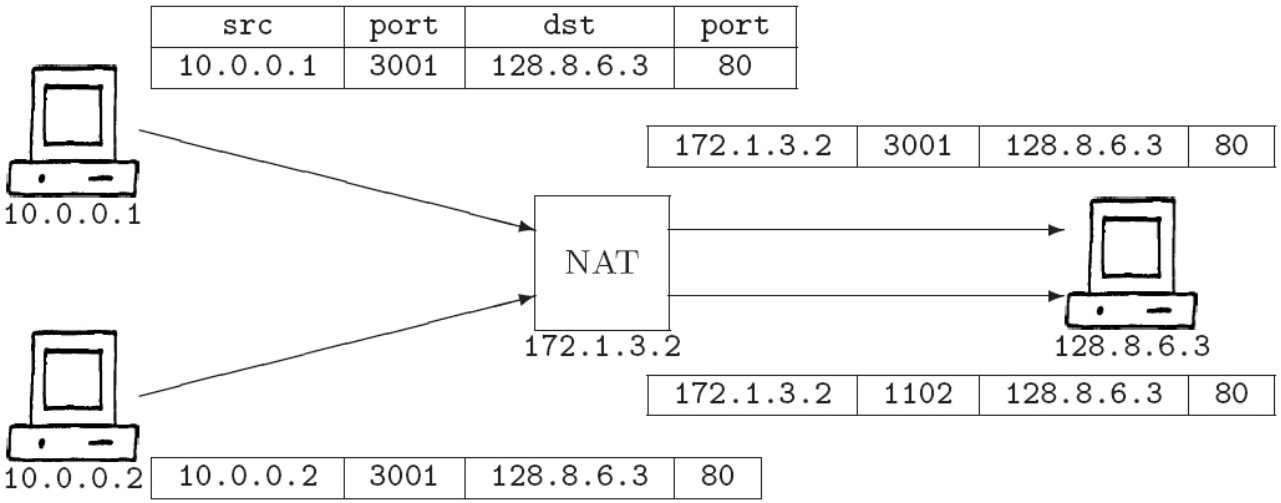
NAT: Network Address Translation

- Public IP addresses are rare.
- Instead of reserving 256 addresses for 100 workstations, we can hide those 100 workstations behind a single address.
- With regards to this, the IETF has reserved three address ranges:
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255

NAT: Basic Principle

- Use private addresses in the internal network and one/several public addresses to communicate with the Internet.
- When a packet leaves the internal network, we replace its source address by a public address.
- When a packet arrives from the Internet, we replace its public destination by a private address.
- We use a translation table to store the relations between internal and external addresses.
- Dynamic NAT does not allow establishing incoming connections.

NAT: Example of Dynamic

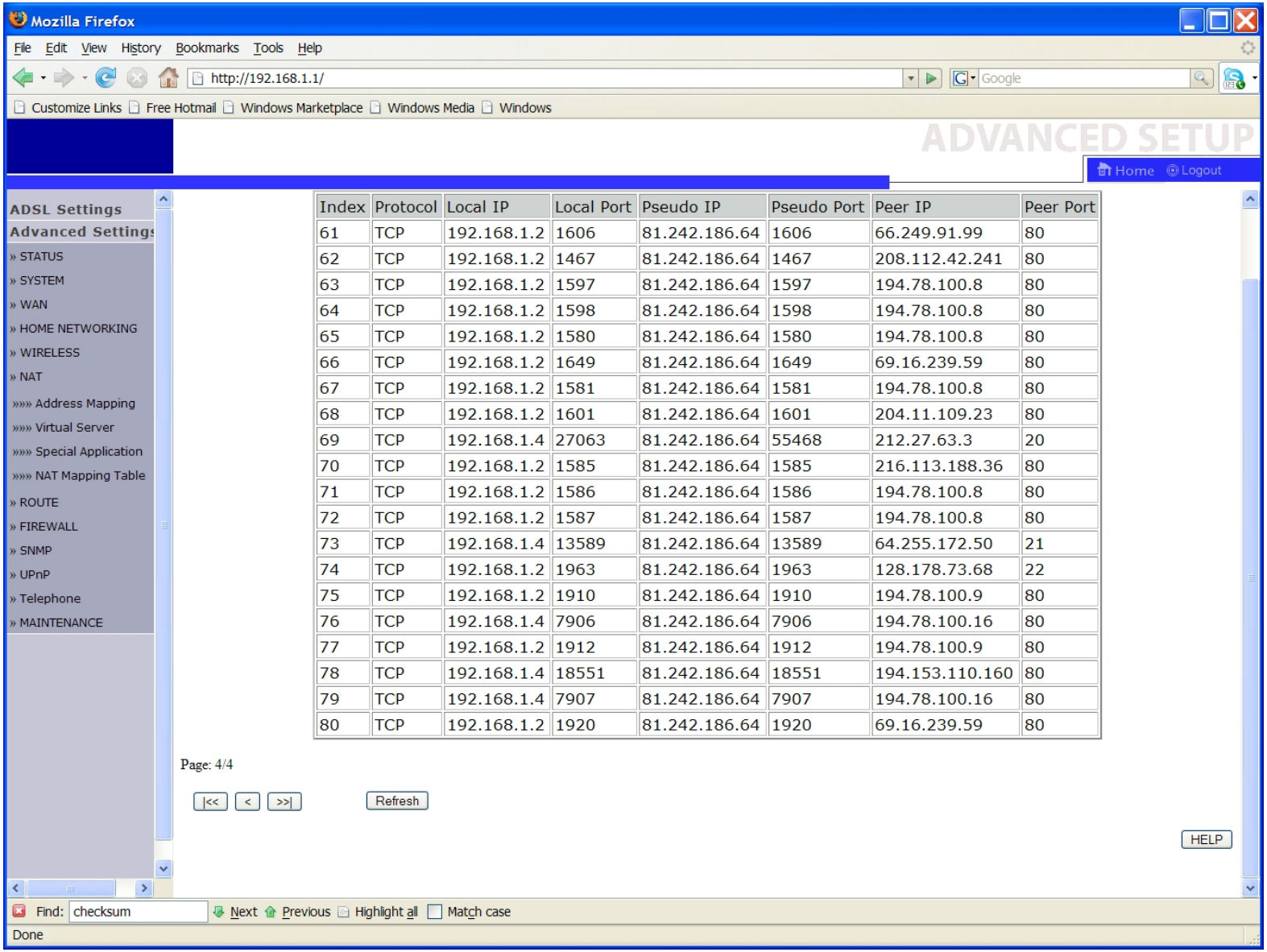


internal				external			
src	port	dst	port	src	port	dst	port
10.0.0.1	3001	128.8.6.3	80	172.1.3.2	3001	128.8.6.3	80
10.0.0.2	3001	128.8.6.3	80	172.1.3.2	1102	128.8.6.3	80

NAT: Properties of Dynamic NAT

- When two connections are differentiated only by their internal address we have a collision.
- Source port can be changed (Port and Address Translation).
- A pool of public addresses can be used.
- Dynamic NAT does not allow establishing incoming connections.
  - Peer to peer (eg. eMule).

Example of Dynamic NAT

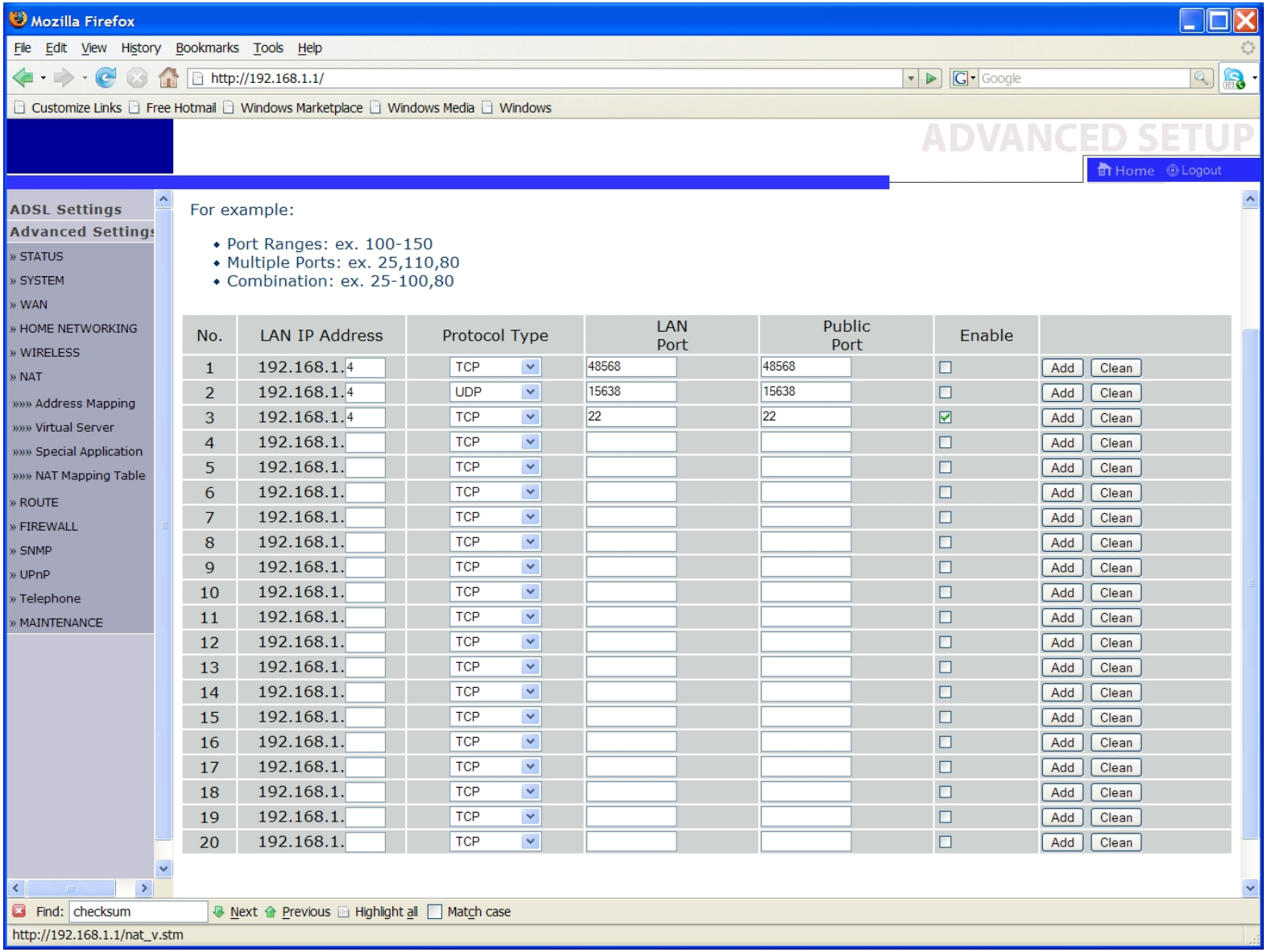


Index	Protocol	Local IP	Local Port	Pseudo IP	Pseudo Port	Peer IP	Peer Port
61	TCP	192.168.1.2	1606	81.242.186.64	1606	66.249.91.99	80
62	TCP	192.168.1.2	1467	81.242.186.64	1467	208.112.42.241	80
63	TCP	192.168.1.2	1597	81.242.186.64	1597	194.78.100.8	80
64	TCP	192.168.1.2	1598	81.242.186.64	1598	194.78.100.8	80
65	TCP	192.168.1.2	1580	81.242.186.64	1580	194.78.100.8	80
66	TCP	192.168.1.2	1649	81.242.186.64	1649	69.16.239.59	80
67	TCP	192.168.1.2	1581	81.242.186.64	1581	194.78.100.8	80
68	TCP	192.168.1.2	1601	81.242.186.64	1601	204.11.109.23	80
69	TCP	192.168.1.4	27063	81.242.186.64	55468	212.27.63.3	20
70	TCP	192.168.1.2	1585	81.242.186.64	1585	216.113.188.36	80
71	TCP	192.168.1.2	1586	81.242.186.64	1586	194.78.100.8	80
72	TCP	192.168.1.2	1587	81.242.186.64	1587	194.78.100.8	80
73	TCP	192.168.1.4	13589	81.242.186.64	13589	64.255.172.50	21
74	TCP	192.168.1.2	1963	81.242.186.64	1963	128.178.73.68	22
75	TCP	192.168.1.2	1910	81.242.186.64	1910	194.78.100.9	80
76	TCP	192.168.1.4	7906	81.242.186.64	7906	194.78.100.16	80
77	TCP	192.168.1.2	1912	81.242.186.64	1912	194.78.100.9	80
78	TCP	192.168.1.4	18551	81.242.186.64	18551	194.153.110.160	80
79	TCP	192.168.1.4	7907	81.242.186.64	7907	194.78.100.16	80
80	TCP	192.168.1.2	1920	81.242.186.64	1920	69.16.239.59	80

NAT: Static

- To allow incoming connections, we have to define certain static entries in the translation table.
- Typically we create one entry per protocol (SMTP, HTTP,...).
- Different ports from the same external address can lead to different internal addresses.

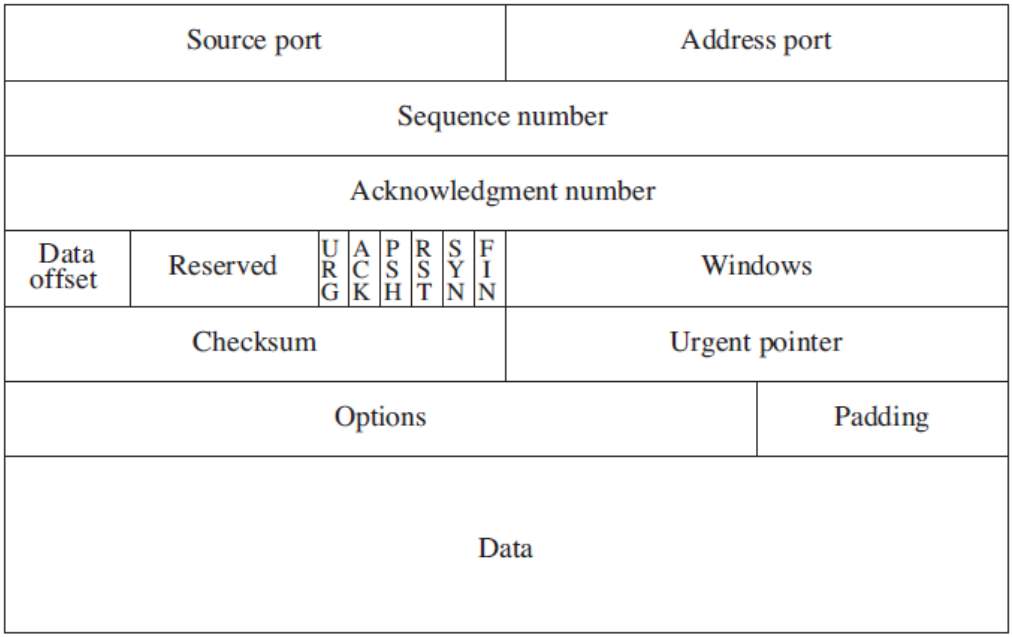
Example of Static NAT



NAT: Issues and Limitations

- TCP and UDP checksums.
- Some protocols do not support packet modifications, eg. IPSec.
- Some protocols exchange their IP addresses.
  - With NAT, that is the private address that will be provided.
  - The protocol can manage that problem itself.
  - If FW knows the protocol, it can "patch" packets to replace the private address by public addresses.
  - Examples: FTP, RealAudio, Quake3, X windows, H.323

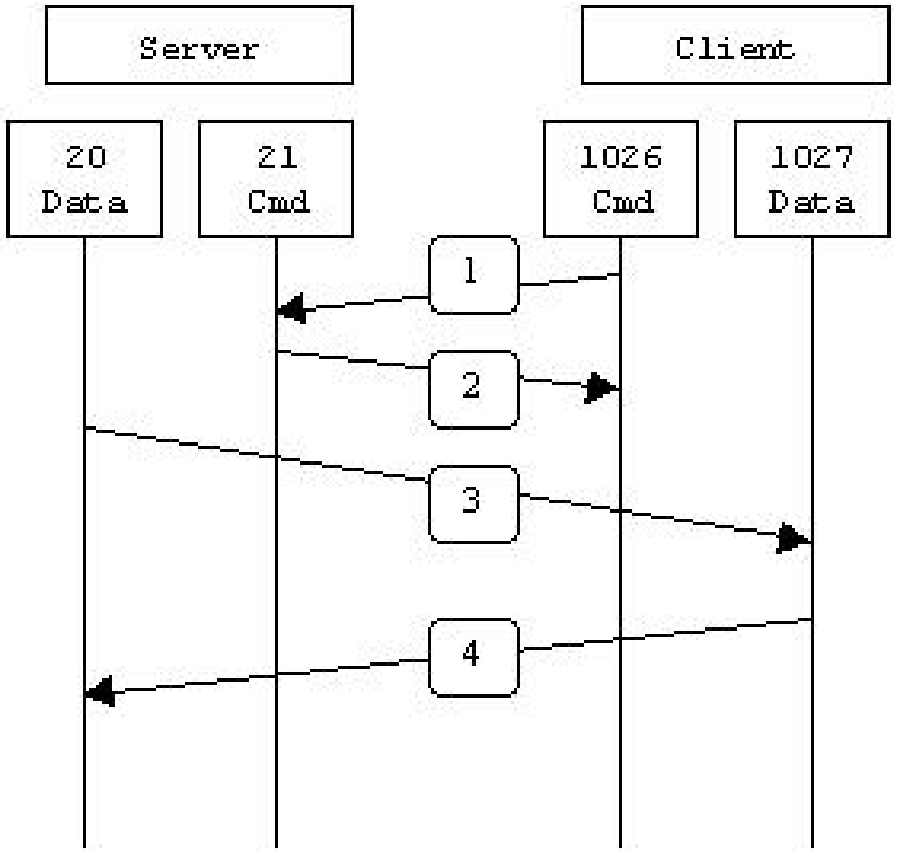
NAT Limitations: TCP Checksums



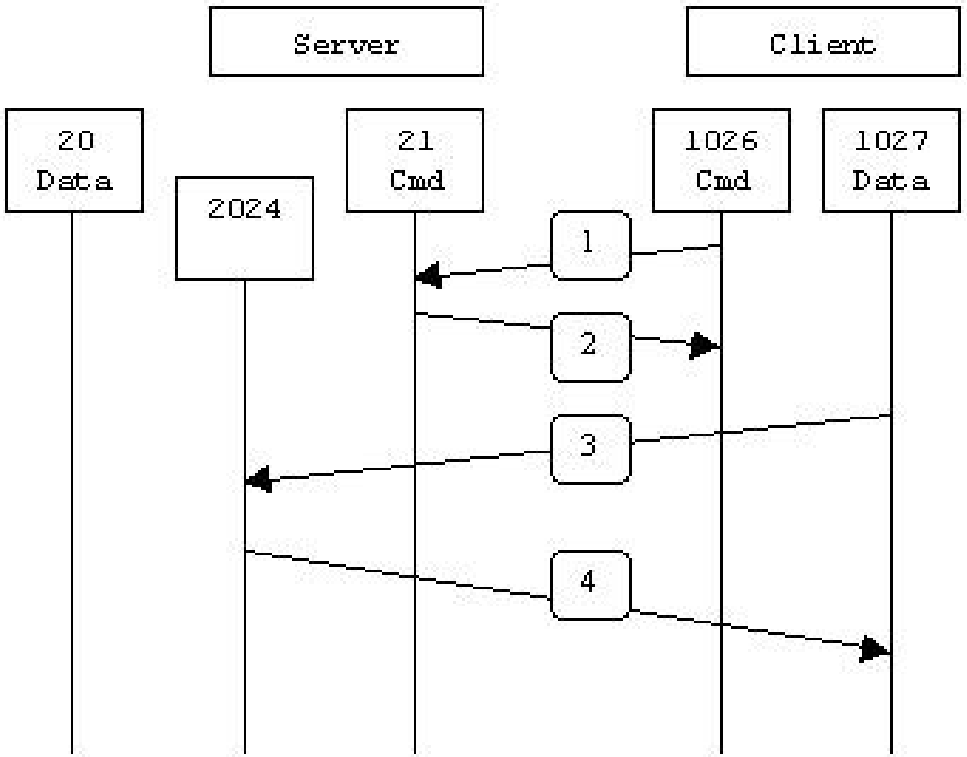
NAT Limitations: FTP

- FTP consists of 2 connections.
  - Control connection (port 21).
  - Data connection (port negotiated).
- Mode: Active vs Passive.
  - Active: Data connection initiated by server.
  - Passive: Data connection initiated by client.

FTP: Active Mode



FTP: Passive Mode



NAT: Advantages

- Less public addresses, limited costs.
- Easy to change access provider.
- Easy to re-organize the internal network.
- Automatic protection effect.
- Hides the internal network's structure.

NAT and IPv6

- RFC 3002: "There was clear consensus that any IPv4-based model relying on traditional stateless NAT technology is to be strongly discouraged. NAT has several inherent faults, including breaking the Internet peer-to-peer communication model, breaking end-to-end security, and stifling deployment of new services. In addition, the state and performance implications of supporting 10's to 100's million users is cost and technologically prohibitive."

- RFC 3002: "It was recommended that an effort be made to eliminate any requirement for NAT in an IPv6 Internet."

Content Analysis

- FW can analyze packets to verify their format and content.
  - Allows elimination of malformed packets (eg. ping of death).
  - Allows elimination of packets that do not correspond to the protocol's current state.
  - Allows elimination of packets with undesired content (eg. virus).
- FW can analyze an application protocol.
  - Allows prohibiting certain SMTP commands(`expn`, `vrfy`)

Authentication

- FW can require an authentication letting a connection through.
- Outbound: allows limiting Internet access only to privileged users.
- Inbound: allows authorizing access to internal resources for employees on that are traveling.
- Authentication can be done based on a local database or by interaction with a central database.

Remote Network Access

- The FW allows external users to access the LAN.
- The external user establishes an encrypted (tunnel) with FW.
- The user finds himself just as if he was inside the LAN.
- The connection can be done via Internet or modem.

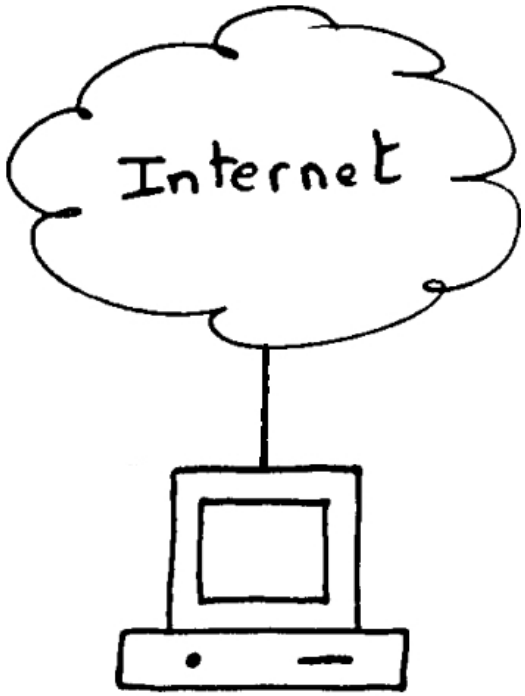
ARCHITECTURES

- Introduction
- Basic Principles
- Features
- Architectures
- Rules Organization
- Conclusion and References

Firewall Architectures

- Personal Firewall.
- NAT + filtering.
- FW with demilitarized zone.
- Sandwiched demilitarized zone.

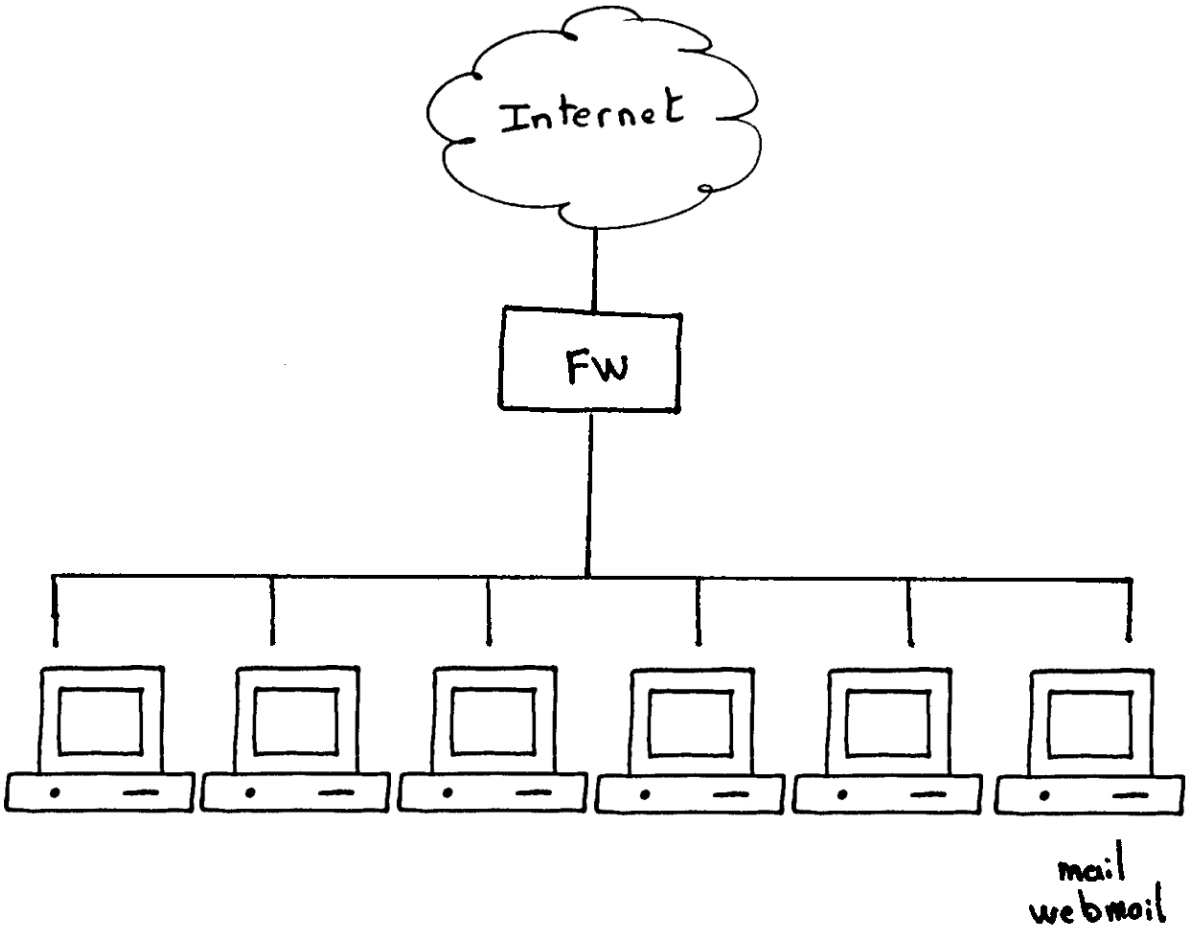
Personal Internet Access



Personal Internet Access

- The personal firewall initially prohibits all connections.
- At each alarm, the user can authorize the application to connect for that time only or for always.
- Allows blocking backdoors, spywares,...
- An ideal complement to an anti-virus for safe surfing.

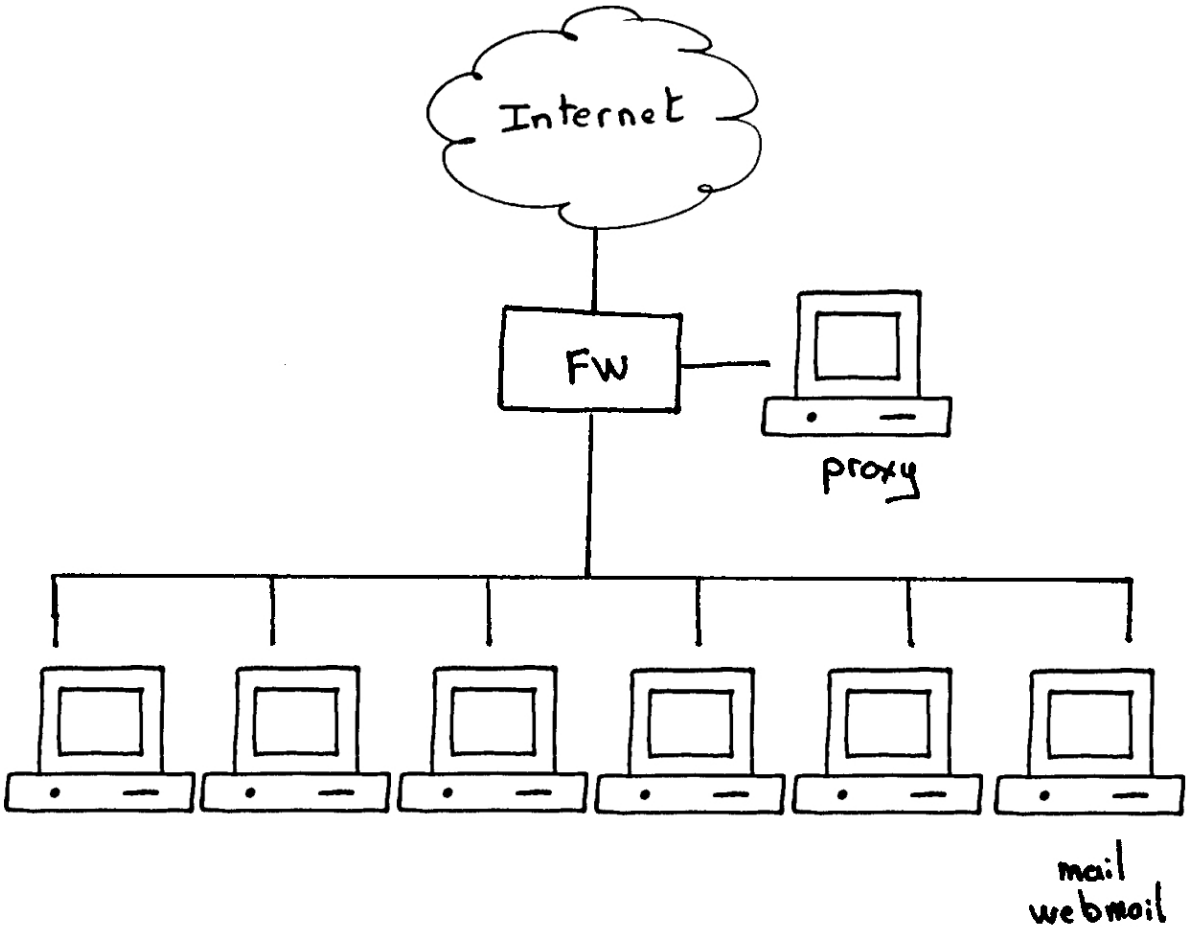
NAT + Filtering



NAT + Filtering

- Configuration.
  - Dynamic NAT for all internal machines.
  - Static NAT for all accessible servers.
  - Outbound filtering.
  - Inbound filtering.
- Limitations.
  - No analysis of contents (virus) from Internet.
  - Direct connections on internal servers (exploits, DoS).
- Application.
  - Low security.
  - No large public Web server.

Demilitarized Zone (Simple case)



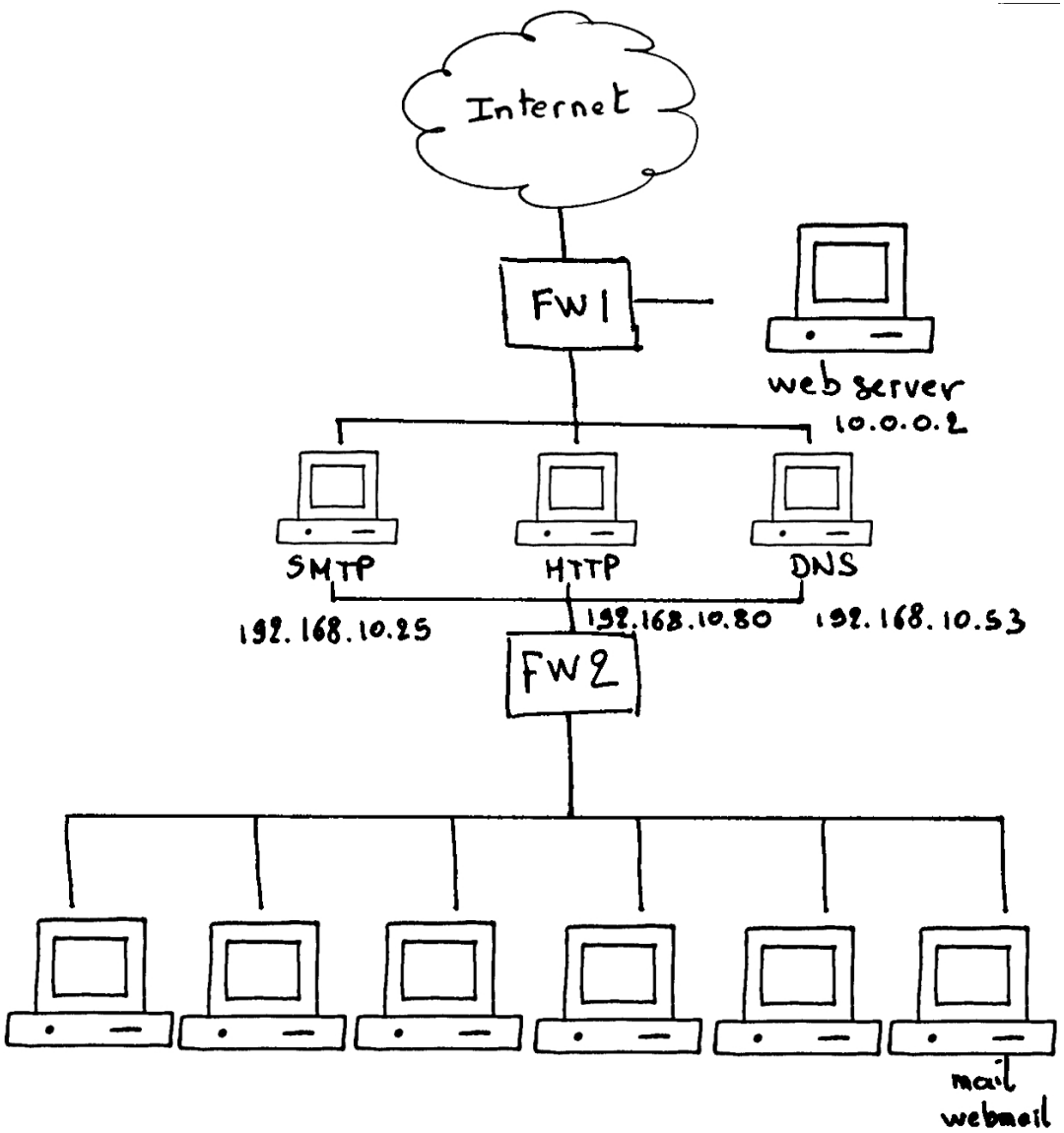
Demilitarized Zone (Simple case)

- The demilitarized zone (DMZ) is connected neither to the Internet, nor to the internal network.
- Configuration.
  - Internal machines can only connect to the proxy.
  - Only the proxy can connect to the Internet.
  - Outbound dynamic NAT.
  - Inbound static NAT toward the proxy.
  - Outbound filtering and inbound filtering.

Demilitarized Zone (Simple case)

- Limitations (of the example, not DMZ).
  - The firewall is a critical point.
  - All services pass through the same proxy, a vulnerability on a single service can give access to all traffic.
- Application.
  - Medium security needs.

Sandwiched DMZ



Sandwiched DMZ

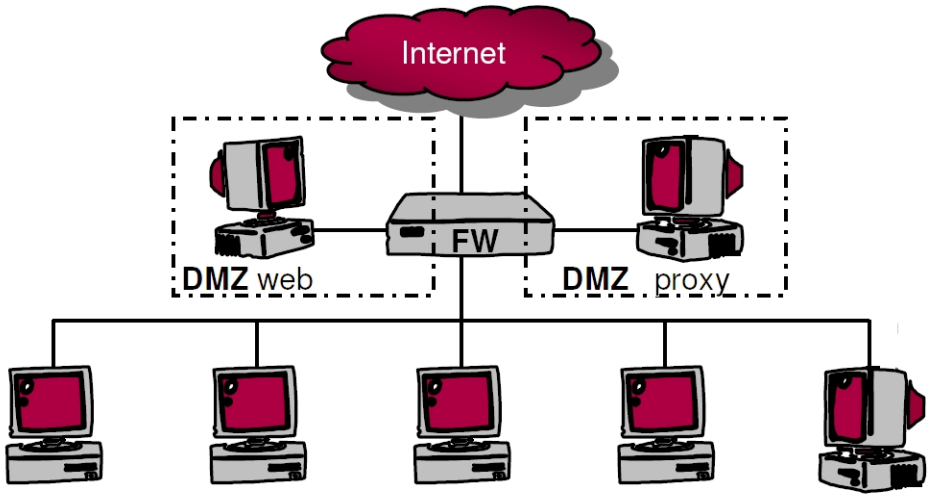
- Configuration.
  - Internal machines can only connect to the proxies (one protocol per proxy).
  - Only proxies can connect to the Internet.
  - No routing in proxies.
  - Outbound dynamic NAT, inbound static.
  - Outbound filtering and inbound filtering.
- Applications.
  - High security needs.

RULES ORGANIZATION

- Introduction
- Basic Principles
- Features
- Architectures
- Rules Organization
- Conclusion and References

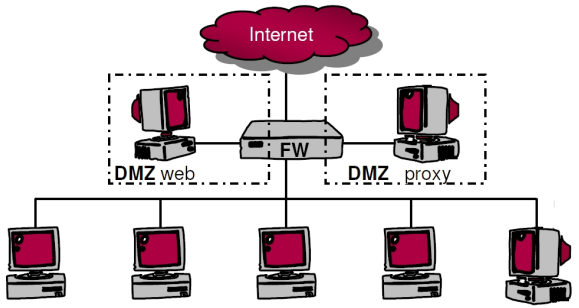
Organization of Filtering Rules: Example

- FW should allow external connections to go to DMZ_web.
- FW should allow internal connections to go to Internet, but though the DMZ_proxy only.



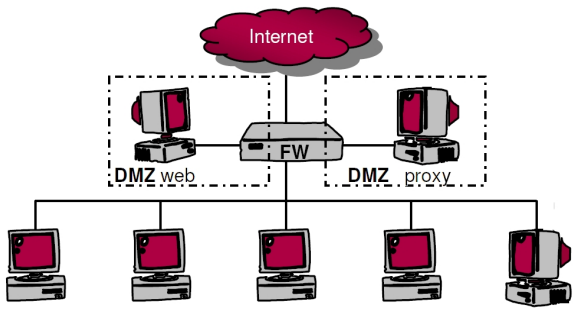
Organization: Example

	Src	Port	Dst	Port	Prot	Action
1	any	any	dmz_web	80	tcp	allow
2	internal	any	dmz_proxy	8080	tcp	allow
3	internal	any	any	any	any	denydeny
4	any	any	any	any	any	deny, log



Organization: Corrected Example

	Src	Port	Dst	Port	Prot	Action
1	internal	any	dmz_proxy	8080	tcp	allow
2	internal	any	any	any	any	denydeny
3	any	any	dmz_web	80	tcp	allow
4	any	any	any	any	any	deny, log



Organization: Method

- The order in which rules are specified is important.
- Rules must be organized systematically.
- We define a security level for each zone.
- We group rules by zones in descending order of security level.
- Each groups consists of four parts.
  - Explicit authorizations for inbound traffic.
  - General prohibition for inbound traffic.
  - Explicit authorizations for outbound traffic.
  - General prohibition for outbound traffic.

Organization: Example (4 zones)

Zone	Rule	Src	Port	Dst	Port	Prot	Action
Zone 1	1	bob	any	alice	23	tcp	allow
	2	any	any	zone_1	any	any	deny
	3	alice	any	bob	22	tcp	allow
	4	zone_1	any	any	any	any	deny
Zone 2	5	authorized traffic entering zone 2					allow
	6	other traffic entering zone 2					deny
	7	authorized traffic leaving zone 2					allow
	8	other traffic leaving zone 2					deny
Zone 3	9	authorized traffic entering zone 3					allow
	10	other traffic entering zone 3					deny
	11	authorized traffic leaving zone 3					allow
	12	other traffic leaving zone 3					deny
	13	any	any	any	any	any	deny, log

Organization: Properties

- For each zone, it is sufficient to declare the flow towards less secure zones.
- The flow towards more secure zones cannot be influenced anymore: "any" refers to lower levels.
- A rule that involved 2 zones appears in the block related to the most secure zone.
- The block related to the last zone is empty.
- The last rule (any-any) must not be required. By activating logs on that rule we may detect possible errors.

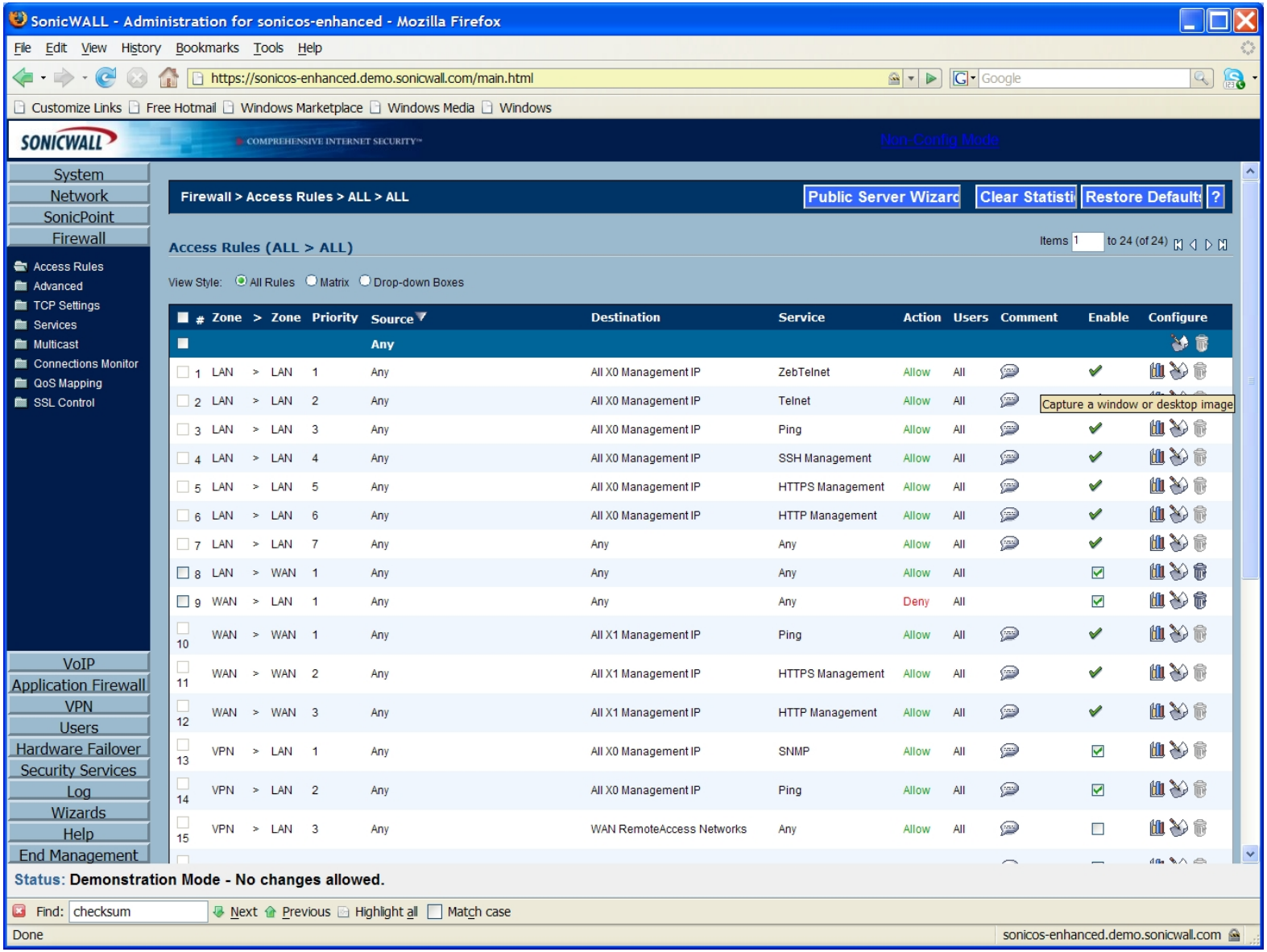
CONCLUSION AND REFERENCES

- Introduction
- Basic Principles
- Features
- Architectures
- Rules Organization
- Conclusion and References

Example: Checkpoint

69	Any	zone4 -wwwsrv	http https echo-request traceroute dest-unreach	accept
70	Any	zone4 -ftpsrv	ftp	accept
71	Any	zone4-subnet1 zone4-subnet2 zone4-subnet3	Any	reject
72	zone4-subnet1 zone4-subnet2	Any	icmp-services	accept
73	DNS primaire	Any	dns	accept
74	zone4-subnet1 zone4-subnet2 zone4-subnet3	Any	Any	reject

Example: Sonic Wall https://sonicwall.com



Conclusion

- FW is an unavoidable security equipment.
- FW must be adapted to the environment: a yound driver will feel better with a Honda Civic than a Lamborghini.
- FW does not protect well against:
  - Internal attacks.
  - Attacks due to mobile equipment (Laptop, USB key, ...).
  - Naivety of users.