Firewalls

Richard Rey - Mickaël Chapin

ESIEA

octobre 2015

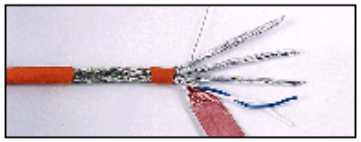
Plan

Plan

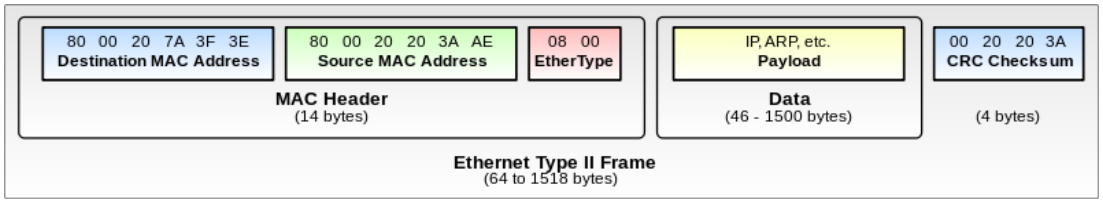
Networking basics

A network is a collection of interconnected objects. It allows you to move items between each of these objects :

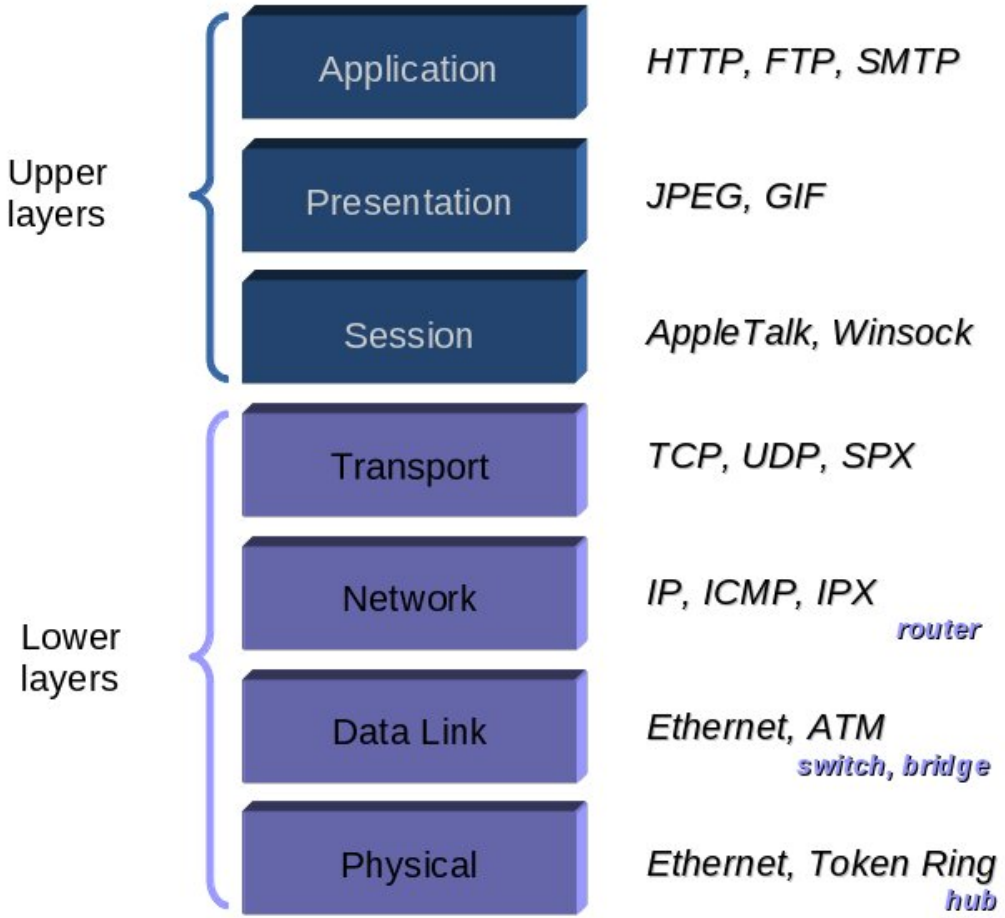
- using a medium: the transmission channel,
- using common rules : protocols.




Ethernet


80 00 20 7A 3F 3E
Destination MAC Address
80 00 20 20 3A AE
Source MAC Address
08 00
EtherType
MAC Header
(14 bytes)
IP, ARP, etc.
Payload
Data
(46 - 1500 bytes)
00 20 20 3A
CRC Checksum
(4 bytes)
Ethernet Type II Frame
(64 to 1518 bytes)

OSI model


Upper layers
Application
HTTP, FTP, SMTP
Presentation
JPEG, GIF
Session
AppleTalk, Winsock
Lower layers
Transport
TCP, UDP, SPX
Network
IP, ICMP, IPX
router
Data Link
Ethernet, ATM
switch, bridge
Physical
Ethernet, Token Ring
hub

Active network equipment

- Hub : Full or half duplex ?

Active network equipment

- Hub : Full or half duplex ?
- switch : Is there any collisions ? full or half duplex ?

Active network equipment

- Hub : Full or half duplex ?
- switch : Is there any collisions ? full or half duplex ?
- Auto-negotiation : What is the standard ?

Active network equipment

- Hub : Full or half duplex ?
- switch : Is there any collisions ? full or half duplex ?
- Auto-negotiation : What is the standard ?
- Broadcast and Multicast IP: What differences for Ethernet ?

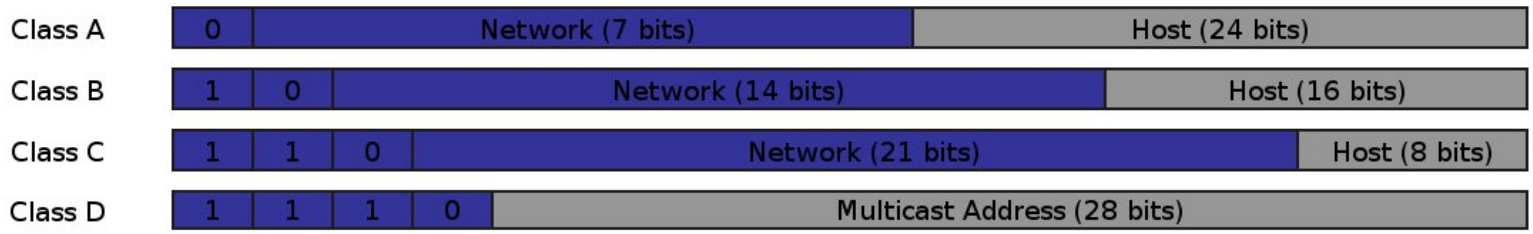
Active network equipment

- Hub : One medium = CSMA/CD = Half duplex.
- switch : Suppression of collisions = Full duplex .
- Auto-negotiation : No autoneg on the links between servers and network equipments.
- IP Multicast = Ethernet broadcast

Exercise

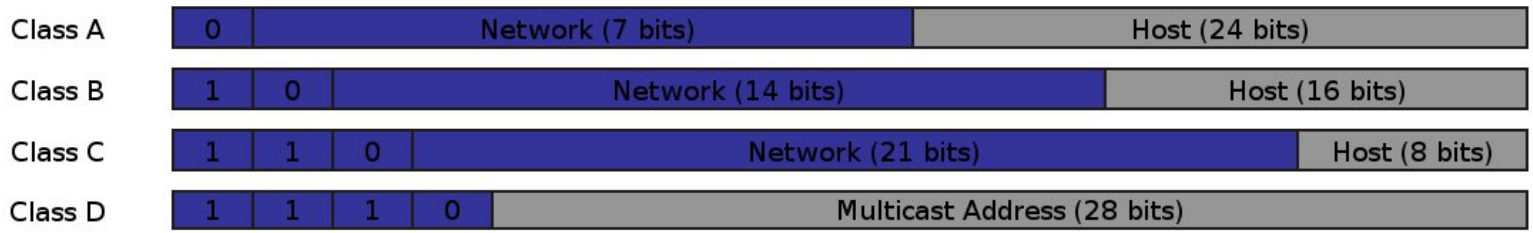
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	decimal value
128	64	32	16	8	4	2	1	
1	1	1	1	1	1	1	1	...
0	0	0	0	1	1	1	1	...
1	1	1	1	0	0	0	0	...
1	1	1	1	1	1	0	0	...

Classes of IP addresses



Three classes of private IP addresses (non-routable on the Internet)

Classes of IP addresses



Three classes of private IP addresses (non-routable on the Internet)

Class A: 10.0.0.0 to 10.255.255.255 (/8)
Class B: 172.16.0.0 to 172.31.255.255 (/12)
Class C: 192.168.0.0 to 192.168.255.255 (/16)

Classes of IP addresses

Class	Bits	Mask	CIDR default
A	0	255.0.0.0	/8
B	10	255.255.0.0	/16
C	110	255.255.255.0	/24
D	1110	Undefined	/4
E	11110	Undefined	/4
Loopback	01111111	255.0.0.0	/8

The network mask

Associated with an IP address, it is actually an IP address with network bits set to 1.

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

It serves two purposes for a workstation:

The network mask

Associated with an IP address, it is actually an IP address with network bits set to 1.

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

It serves two purposes for a workstation:

- Knowing the network to which it belongs.
- Check if the destination computer is on the same network.

Network membership

first computer

Address	192.168.182.10
Mask	255.255.255.0

Network membership

first computer

Address	192.168.182.10
Mask	255.255.255.0
Network	192.168.182.0

Network membership

first computer

Address	192.168.182.10
Mask	255.255.255.0
Network	192.168.182.0

second computer

Address	192.168.182.5
Mask	255.255.255.0

Network membership

first computer

Address	192.168.182.10
Mask	255.255.255.0
Network	192.168.182.0

second computer

Address	192.168.182.5
Mask	255.255.255.0
Network	192.168.182.0

Network membership

first computer

Address	192.168.182.10
Mask	255.255.255.0
Network	192.168.182.0

Network membership

first computer

Address	192.168.182.10
Mask	255.255.255.0
Network	192.168.182.0

third computer

Address	192.168.182.5
Mask	255.255.240.0

Network membership

first computer

Address	192.168.182.10
Mask	255.255.255.0
Network	192.168.182.0

third computer

Address	192.168.182.5
Mask	255.255.240.0
Network	192.168.176.0

Network membership

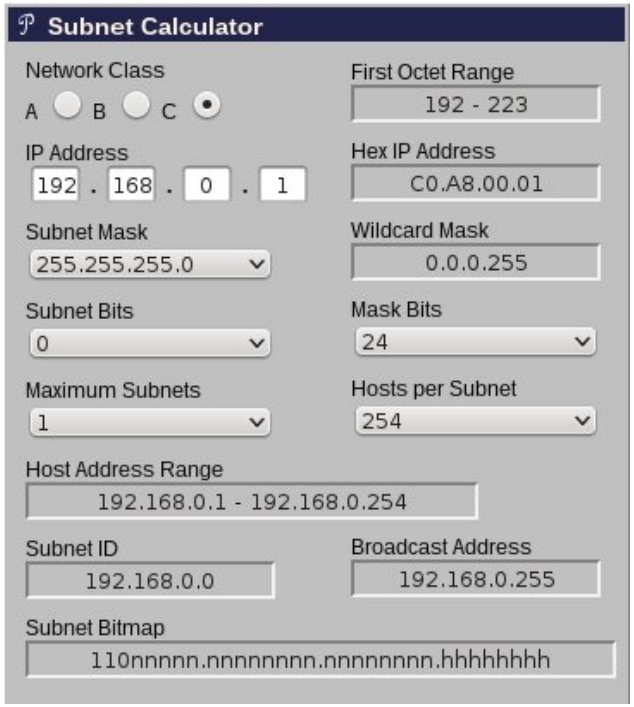
first computer

Address	192.168.182.10
Mask	255.255.255.0
Network	192.168.182.0

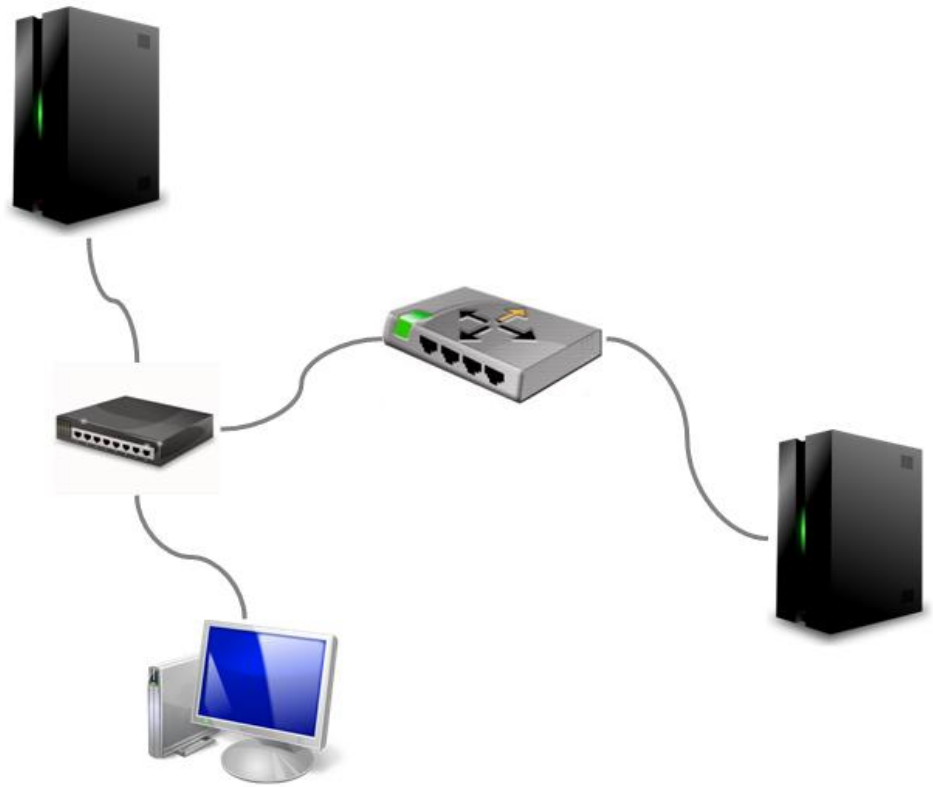
third computer

Address	192.168.182.5
Mask	255.255.240.0
Network	192.168.176.0

Network membership



In practice



IPV4 evolutions

Subnetting [RFC 950] 1985
Cutting method of the network. A subnet is a logically visible subdivision of an IP network.

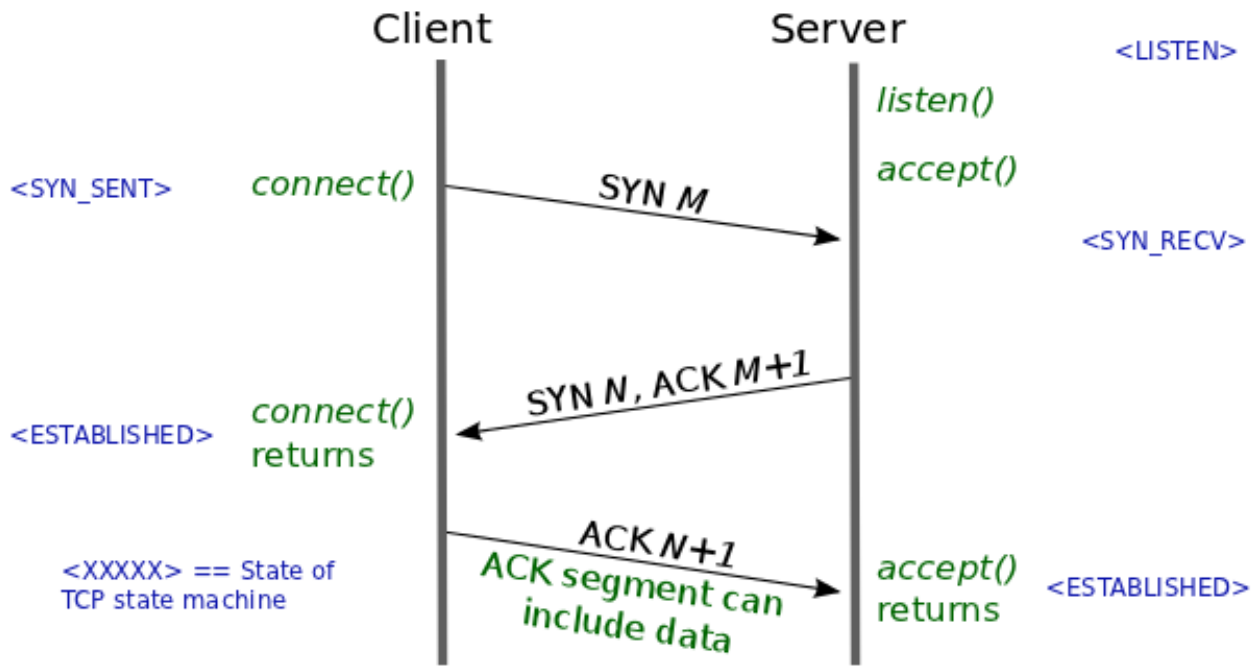
CIDR [RFC 1519] 1993
Classless Inter-Domain Routing is based on variable-length subnet masking (VLSM), which allows a network to be divided into variously sized subnets, providing the opportunity to size a network more appropriately for local needs.

IPV4 evolutions

NAT [RFC 1631] 1994

The process of modifying IP address information in IPv4 headers while in transit across a traffic routing device.

3 way handshake



Assigned ports

Well-known ports :

ftp-data 20/tcp File Transfer [Default Data]
ftp 21/tcp File Transfer [Control]
ssh 22/tcp SSH Remote Login Protocol
...

DNS

```
$ORIGIN domain.com
server1 IN A 10.0.1.5
server2 IN A 10.0.1.6
ftp IN CNAME server1
www IN CNAME server1
smtp IN CNAME server2
IN MX 10 smtp.domain.com.
```

```
$ORIGIN 1.0.10.in -addr.arpa
5 IN PTR server1.domain.com.
6 IN PTR server2.domain.com.
```

Exercises

TCP/IP exercises

Setting up computers

Exercises

Network traffic analysis

Wireshark Documentation
Wireshark Captures

Plan

A **firewall** is an element or set of elements placed between two networks and having the following characteristics :

- all network flows pass through,
- only flows allowed by local policy can pass,
- the system itself is attack-resistant.

Firewall in OSI model

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent. Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY Can be used on all layers		Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed). Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports). Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control. Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address). Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end). Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

A **"Bastion"** generally hosts a single application, for example a proxy server, and all other services are removed to reduce the threat to the computer.
It is hardened because it usually involves access from untrusted networks or computers...
A bastion host may include :

A **"Bastion"** generally hosts a single application, for example a proxy server, and all other services are removed to reduce the threat to the computer.
It is hardened because it usually involves access from untrusted networks or computers...
A bastion host may include :

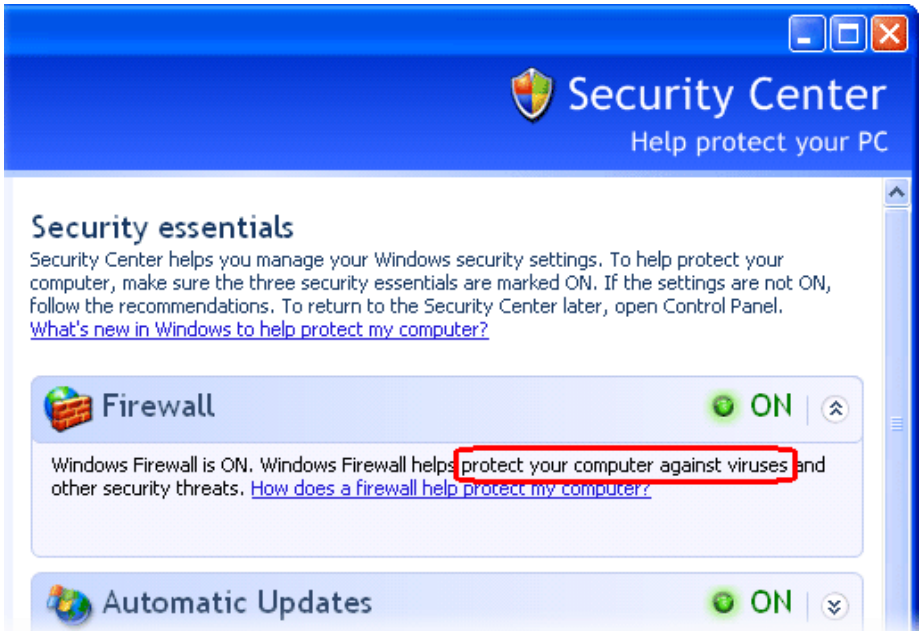
- one or more firewalls,
- Web servers, FTP, DNS, mail relay ...
- ... even sacrificial goat.

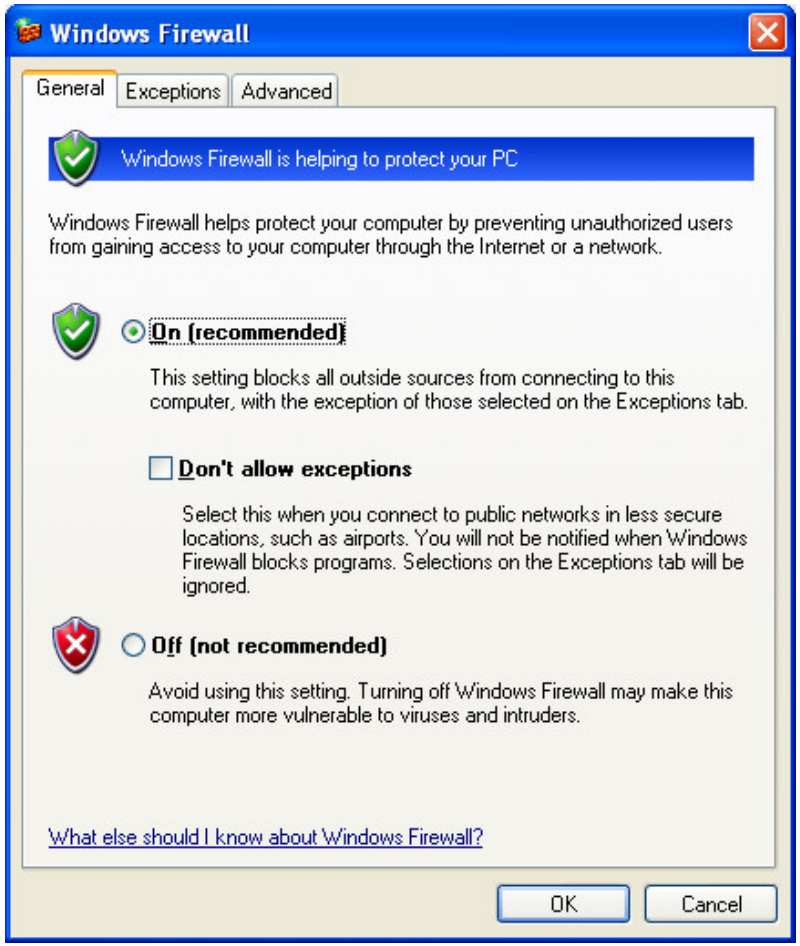
Principles

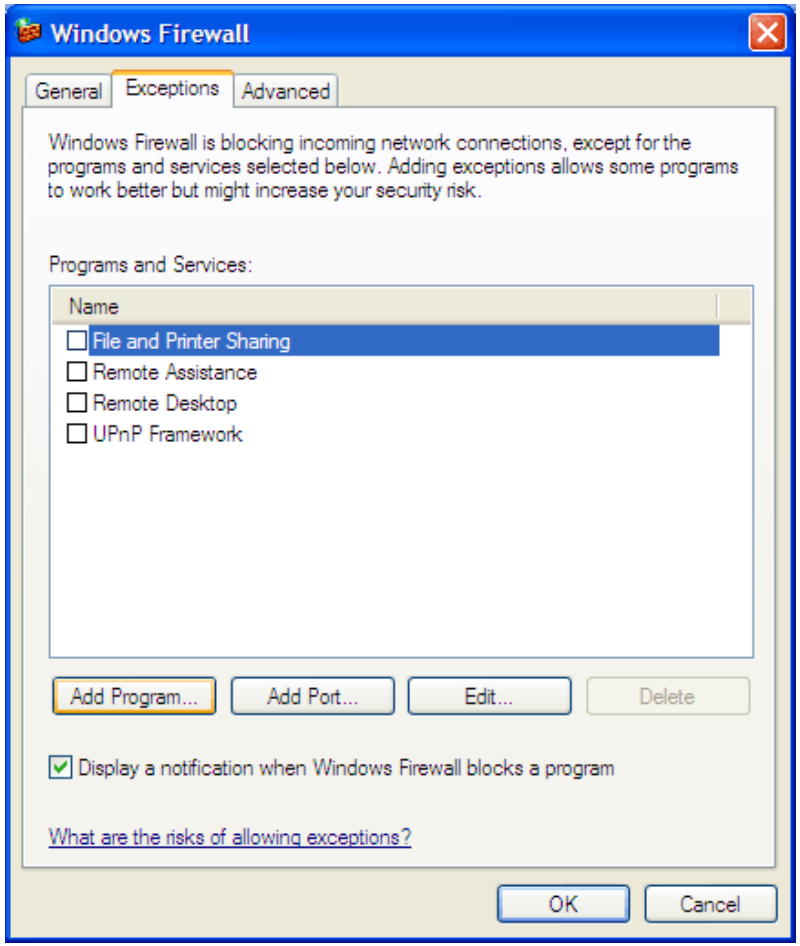
- Least privilege
- Defense in depth
- Choke point
- Weakest link
- Fail-safe stance
- Universal participation
- Diversity of defense
- KISS

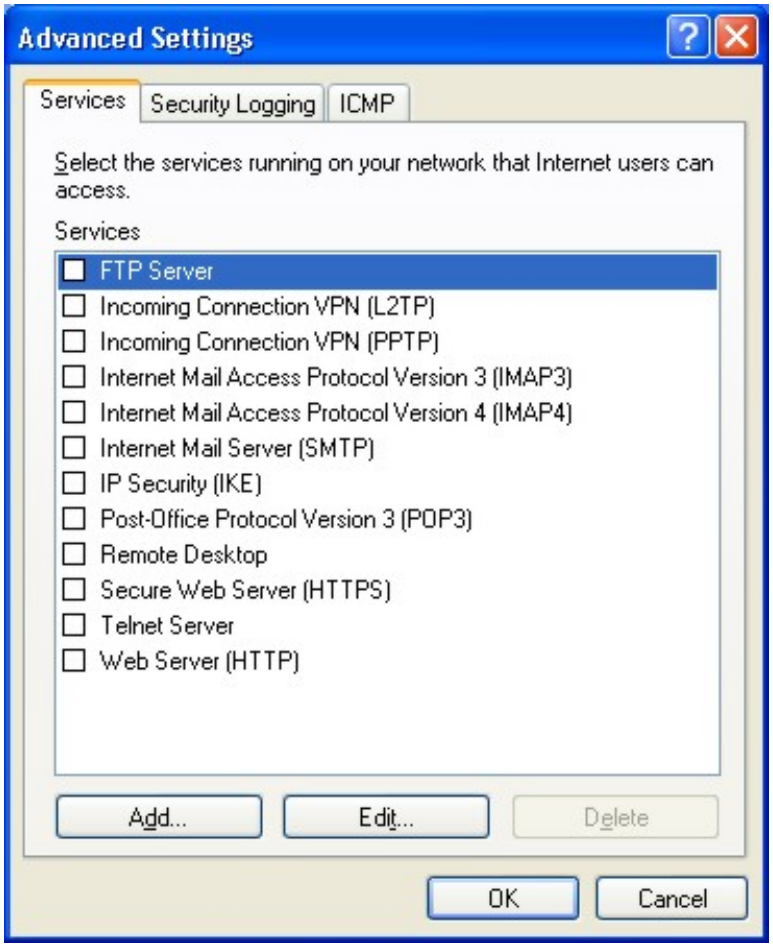
Personal Firewalls

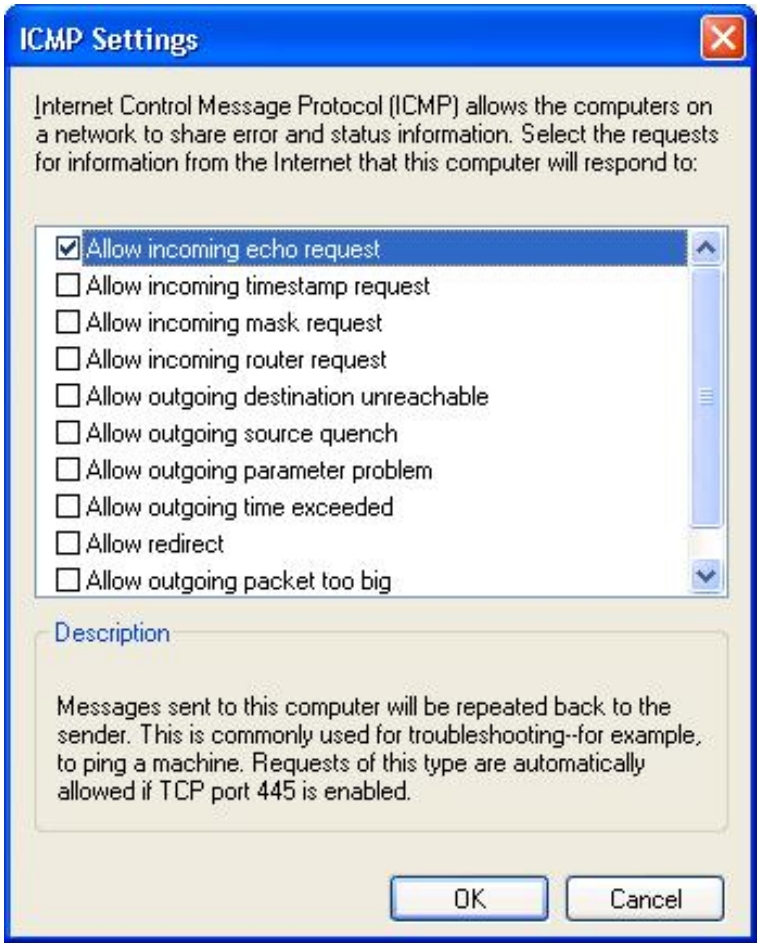
The weakest link ?


Security Center
Help protect your PC
Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?
Firewall
ON
Windows Firewall is ON. Windows Firewall helps protect your computer against viruses and other security threats. How does a firewall help protect my computer?
Automatic Updates
ON


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is helping to protect your PC
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
What else should I know about Windows Firewall?
OK
Cancel


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.
Programs and Services:
Name
File and Printer Sharing
Remote Assistance
Remote Desktop
UPnP Framework
Add Program...
Add Port...
Edit...
Delete
Display a notification when Windows Firewall blocks a program
What are the risks of allowing exceptions?
OK
Cancel


Advanced Settings
Services
Security Logging
ICMP
Select the services running on your network that Internet users can access.
Services
FTP Server
Incoming Connection VPN (L2TP)
Incoming Connection VPN (PPTP)
Internet Mail Access Protocol Version 3 (IMAP3)
Internet Mail Access Protocol Version 4 (IMAP4)
Internet Mail Server (SMTP)
IP Security (IKE)
Post-Office Protocol Version 3 (POP3)
Remote Desktop
Secure Web Server (HTTPS)
Telnet Server
Web Server (HTTP)
Add...
Edit...
Delete
OK
Cancel


ICMP Settings
Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:
Allow incoming echo request
Allow incoming timestamp request
Allow incoming mask request
Allow incoming router request
Allow outgoing destination unreachable
Allow outgoing source quench
Allow outgoing parameter problem
Allow outgoing time exceeded
Allow redirect
Allow outgoing packet too big
Description
Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting--for example, to ping a machine. Requests of this type are automatically allowed if TCP port 445 is enabled.
OK
Cancel

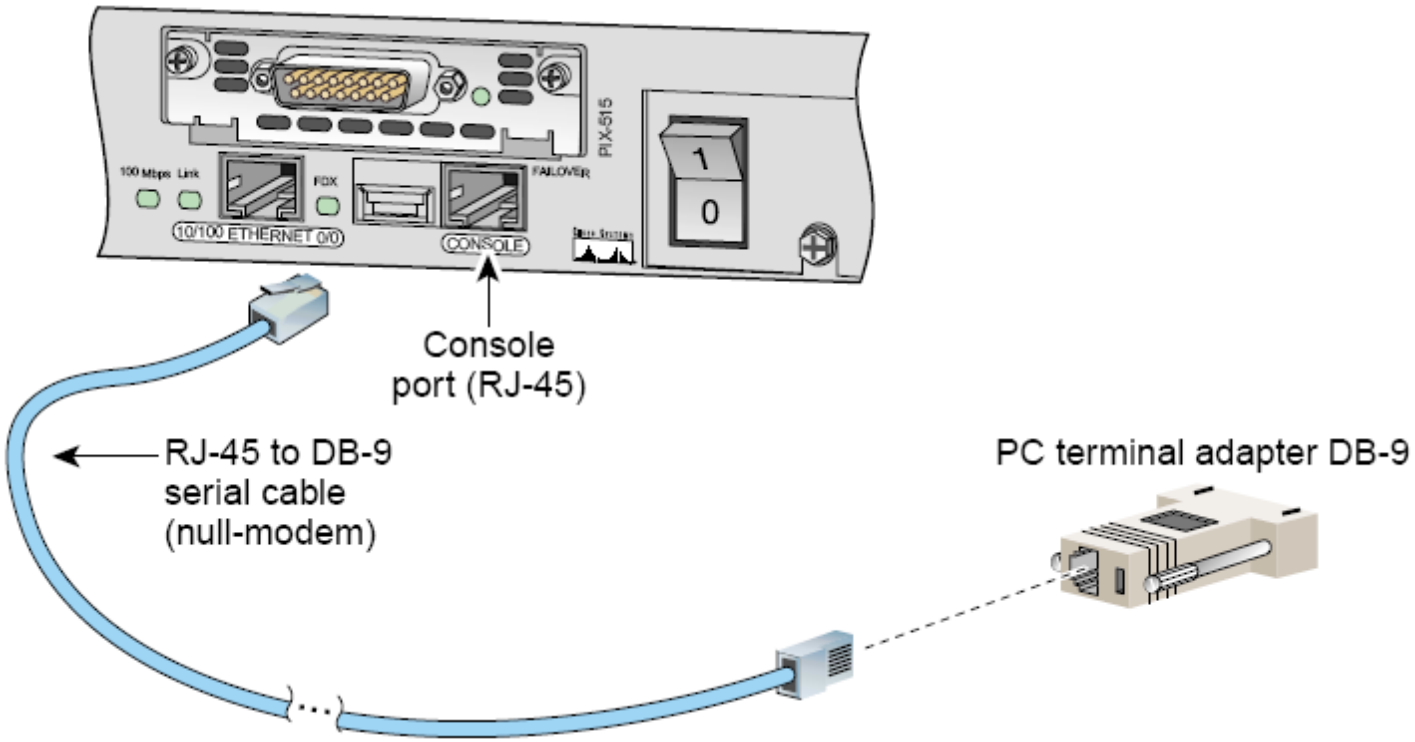
Conventional Firewalls

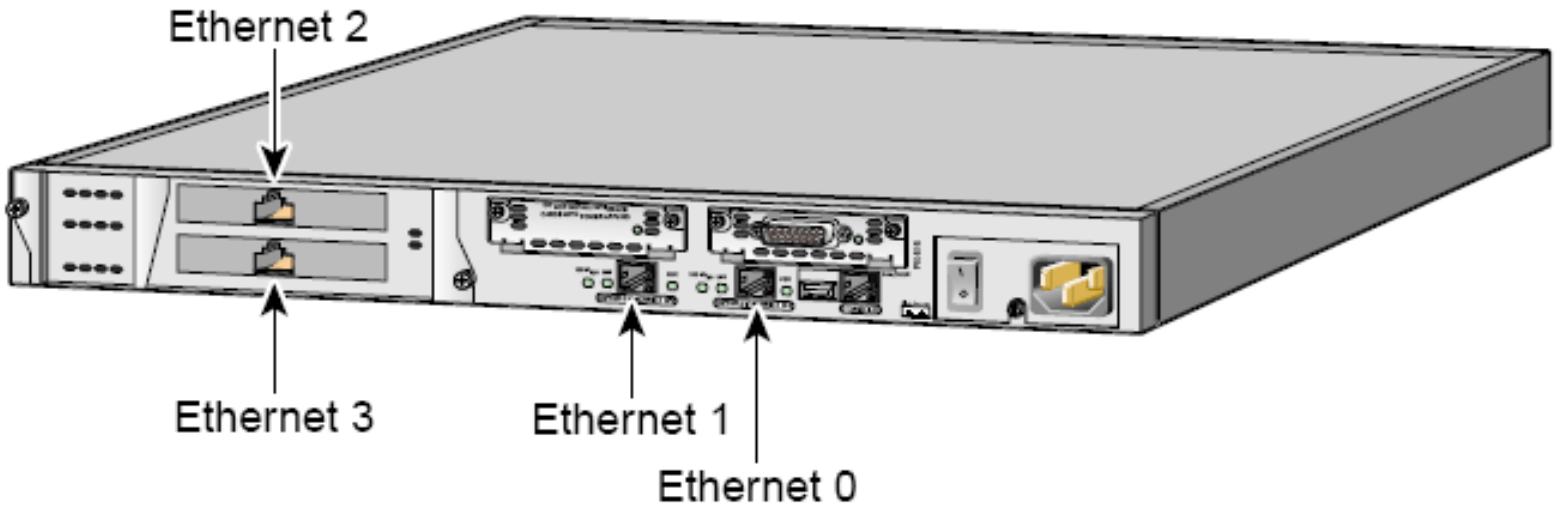

ARKOON
ARKOON

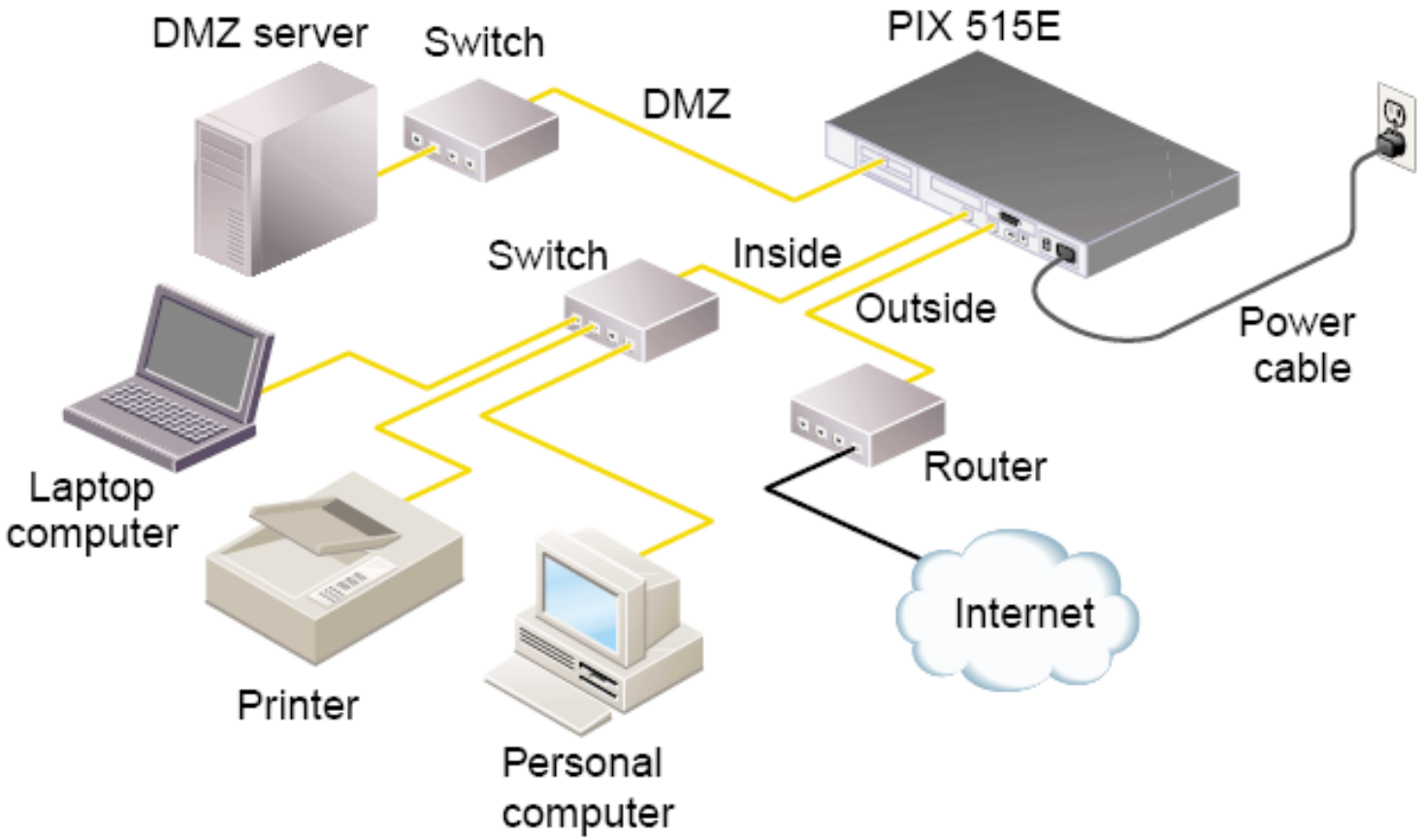

NETASQ F25

Key Features	Benefit
Enterprise-Class Security	
True security appliance	• Uses a proprietary, hardened operating system that eliminates security risks associated with general purpose operating systems • Cisco quality and no moving parts provide a highly reliable security platform
Stateful inspection firewall	• Provides perimeter network security to prevent unauthorized network access • Uses state-of-the-art Cisco ASA for robust stateful inspection firewall services • Provides flexible access-control capabilities for over 100 predefined applications, services and protocols, with the ability to define custom applications and services • Includes numerous application-aware inspection engines that secure advanced networking protocols such as H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), and more • Includes content filtering for Java and ActiveX applets
Easy VPN Server	• Provides remote access VPN concentrator services for a wide variety of Cisco software or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions upon connection, ensuring the latest corporate security policies are enforced • Extends VPN reach into environments using Network Address Translation (NAT) or Port Address Translation (PAT), via support of Internet Engineering Task Force (IETF) UDP-based draft standard for NAT traversal

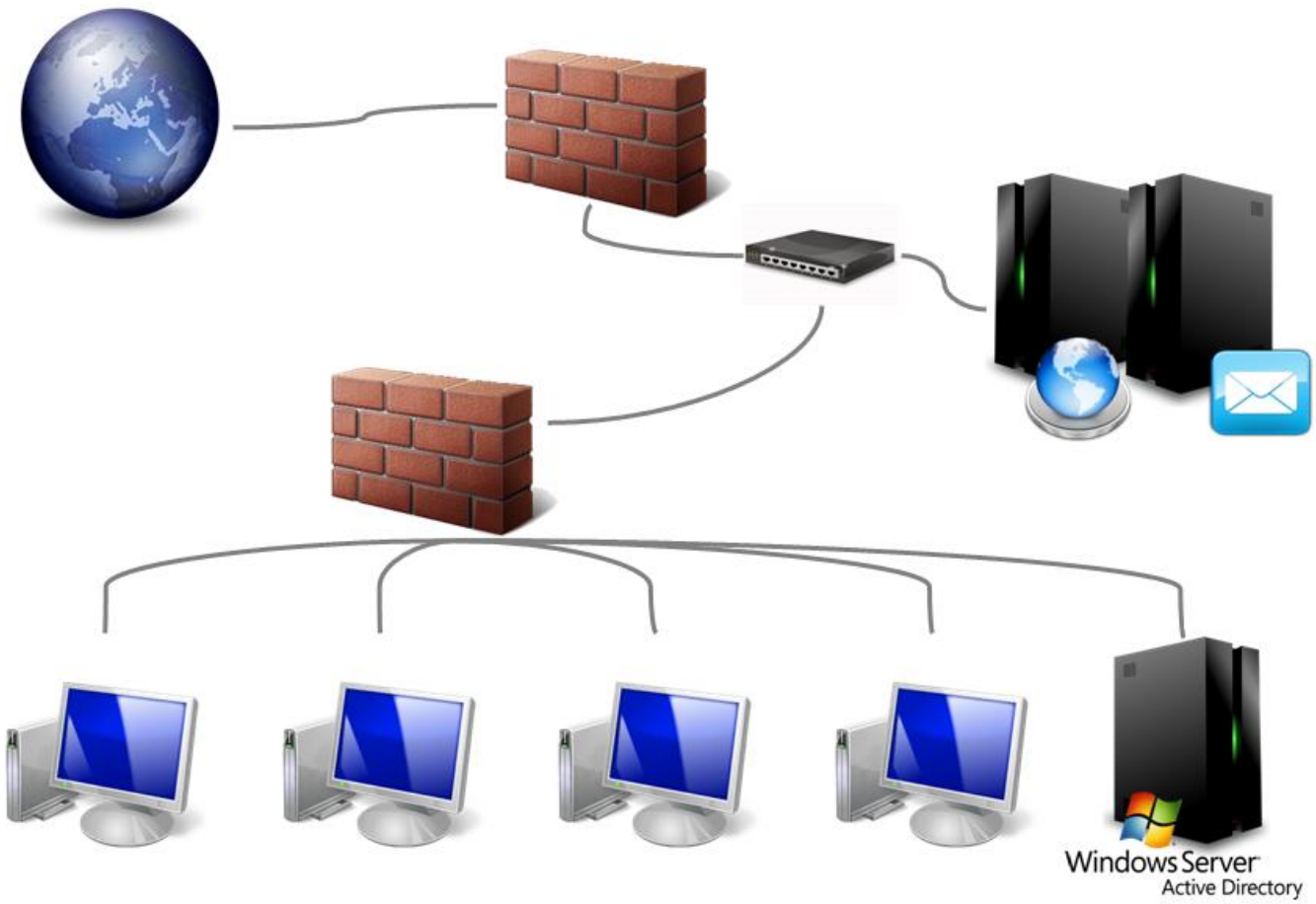
Key Features	Benefit
Site-to-site VPN	• Supports IKE and IPsec VPN standards • Ensures data privacy/integrity and strong authentication to remote networks and remote users over the Internet • Supports 56-bit DES, 168-bit 3DES, and up to 256-bit AES data encryption to ensure data privacy
Intrusion protection	• Provides protection from over 55 different types of popular network-based attacks ranging from malformed packet attacks to DoS attacks • Integrates with Cisco Network Intrusion Detection System (IDS) sensors for the ability to dynamically block/shun hostile network nodes via the firewall
AAA support	• Integrates with popular authentication, authorization, and accounting services via TACACS+ and RADIUS support • Provides tight integration with Cisco Secure Access Control Server (ACS)
X.509 certificate and CRL support	• Supports SCEP-based enrollment with leading X.509 solutions from Baltimore, Entrust, Microsoft, and VeriSign
Integration with leading third-party solutions	• Supports the broad range of Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Robust Network Services/Integration	
Virtual LAN (VLAN)-based virtual interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking • Supports multiple VLAN trunks per Cisco PIX Security Appliance • Supports up to 8 VLANs on Cisco PIX 515E Security Appliances
Open Shortest Path First (OSPF) dynamic routing	• Provides comprehensive OSPF dynamic routing services using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
DHCP server	• Provides DHCP Server services one or more interfaces for devices to obtain IP addresses dynamically • Includes extensions for support of Cisco IP Phones and Cisco SoftPhone IP telephony solutions
DHCP relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking, and maintenance of IP addresses
NAT/PAT support	• Provides rich dynamic/static NAT and PAT capabilities


PIX-515
100 Mbps Link
FDX
FAILOVER
10/100 ETHERNET 0/0
CONSOLE
1
0
Console
port (RJ-45)
RJ-45 to DB-9
serial cable
(null-modem)
PC terminal adapter DB-9

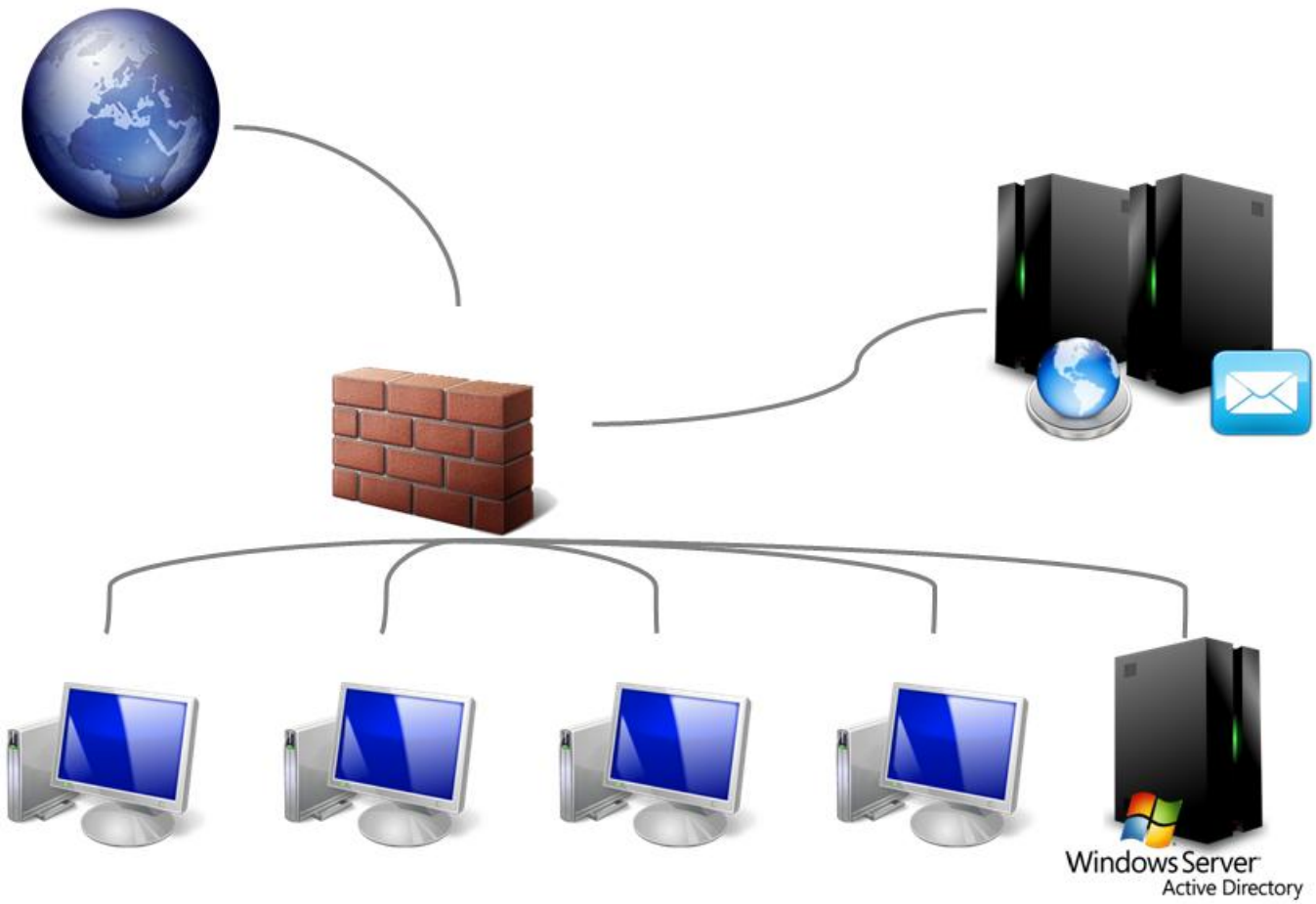

Ethernet 2
Ethernet 3
Ethernet 1
Ethernet 0


DMZ server
Switch
DMZ
PIX 515E
Switch
Inside
Outside
Power cable
Laptop computer
Router
Internet
Printer
Personal computer

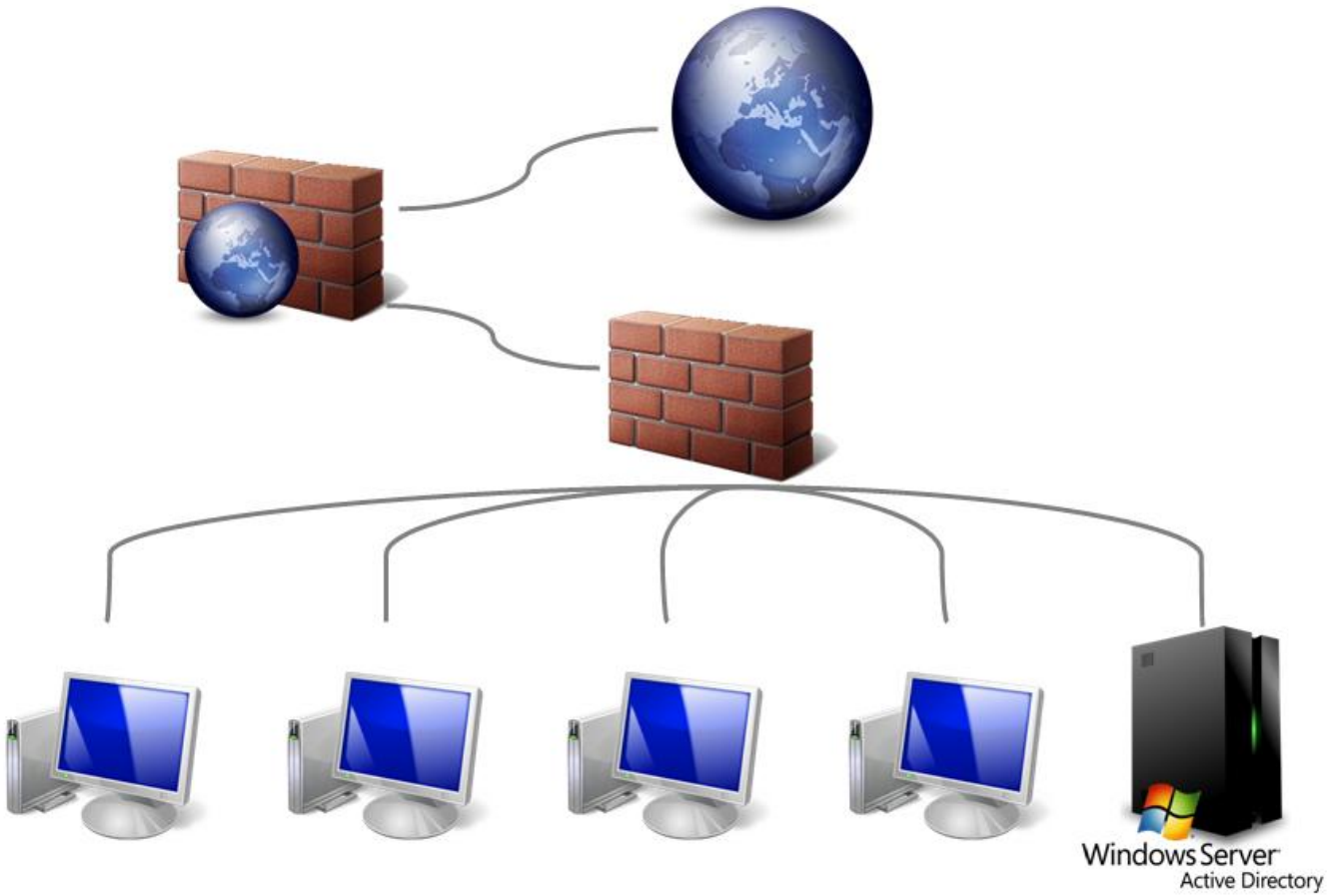
DMZ



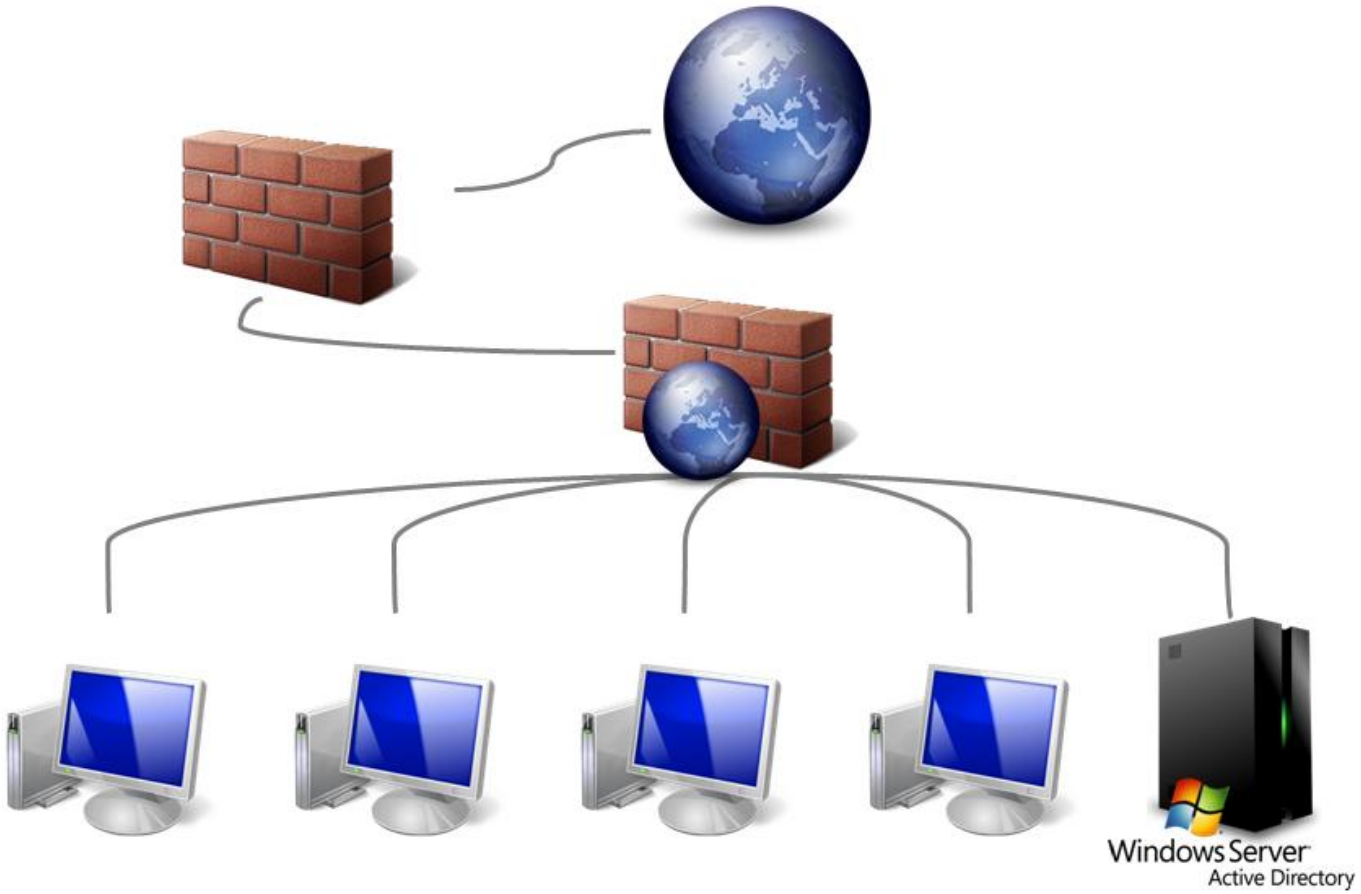
Three-Interface Firewall



The bastion host is ouside the firewall



The bastion host is behind the firewall



Security policy

Your security policy needs to meets your requirements for:

- Affordability (How much money does it cost ?)
- Functionality (Can you still use your computers ?)
- Cultural Compatibility (Conflict with people that interact ?)
- Legality

Security policy

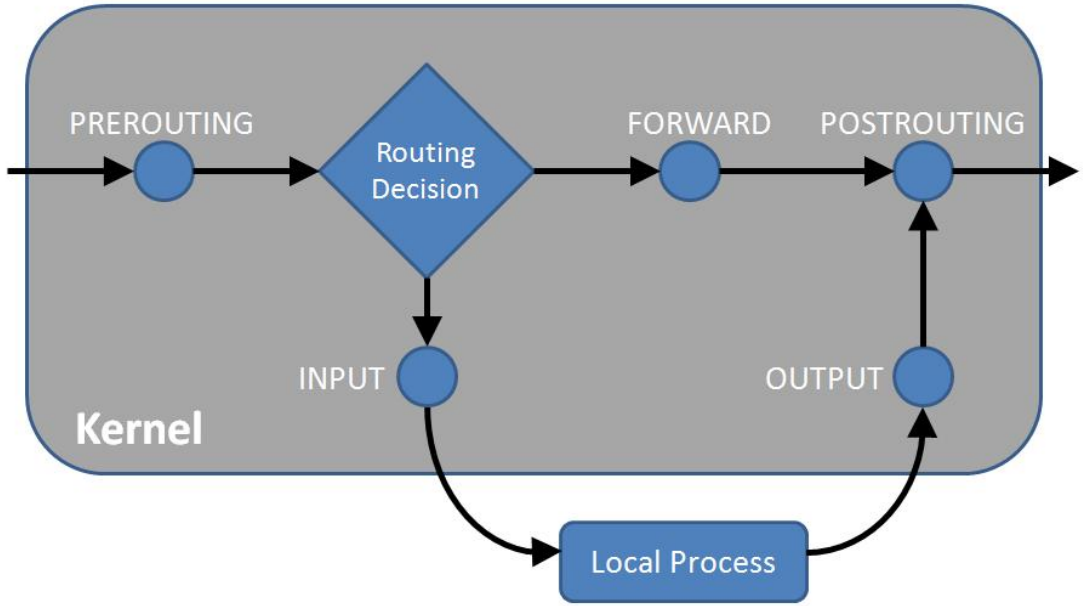
Allow mail exchanges, allow surfing while operating control over the inputs and outputs of the LAN.

Action	Flow	Src.	Dst.
authorize issuance	email	internal	DMZ
authorize receipt	email	DMZ	internal
allow web	internal	Navigation	DMZ
authorize issuance	email	DMZ	External
authorize receipt	email	external	DMZ
allow	web browsing	DMZ	External
deny	any flow	internal	external
reject	all	external	internal flow
reject	all external	flow	DMZ

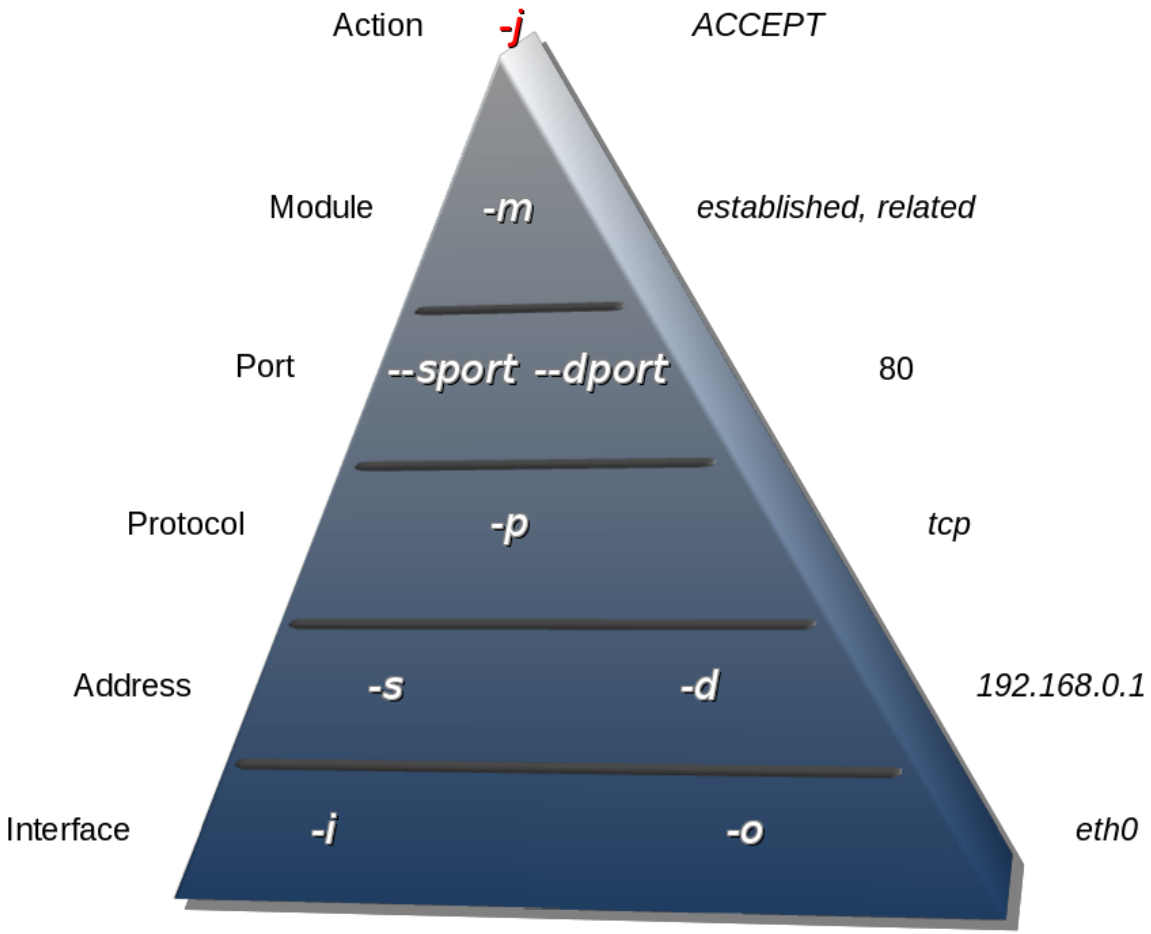
technical Declination

Action	Src. Address.	Dest. Address	Src. Port	Dest. Port	If.
ACCEPT	192.168.0.0/24	192.168.10.10		80	eth1
ACCEPT	192.168.10.10	192.168.0.0/24	80		eth2
ACCEPT	192.168.0.10	192.168.10.10		25	eth1
ACCEPT	192.168.10.10	192.168.0.10	25		eth2
ACCEPT	192.168.10.10	*		80	eth2
ACCEPT	*	192.168.10.10			
DENY	*	192.168.0.0/24			eth0
DENY	192.168.0.0/24	! 192.168.10.10			eth1

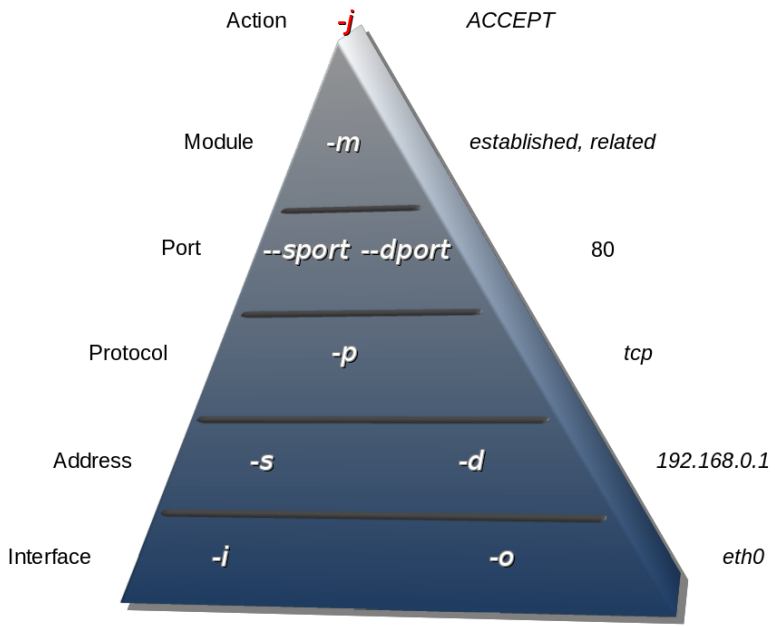
The filter table



Rules matching

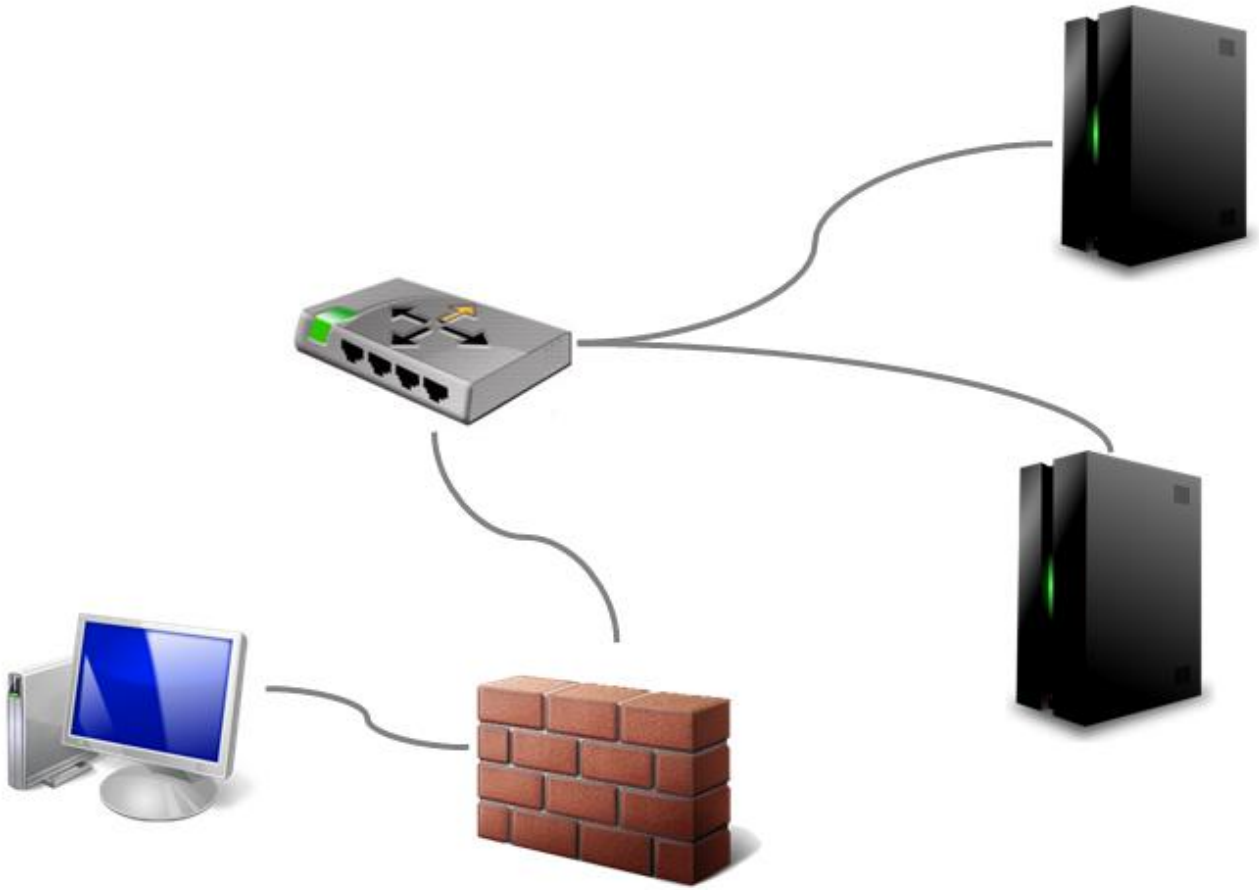


Rules matching



iptables -A FORWARD -i eth1 -o eth0 -s 192.168.0.4 -p tcp - dport 80 -j ACCEPT

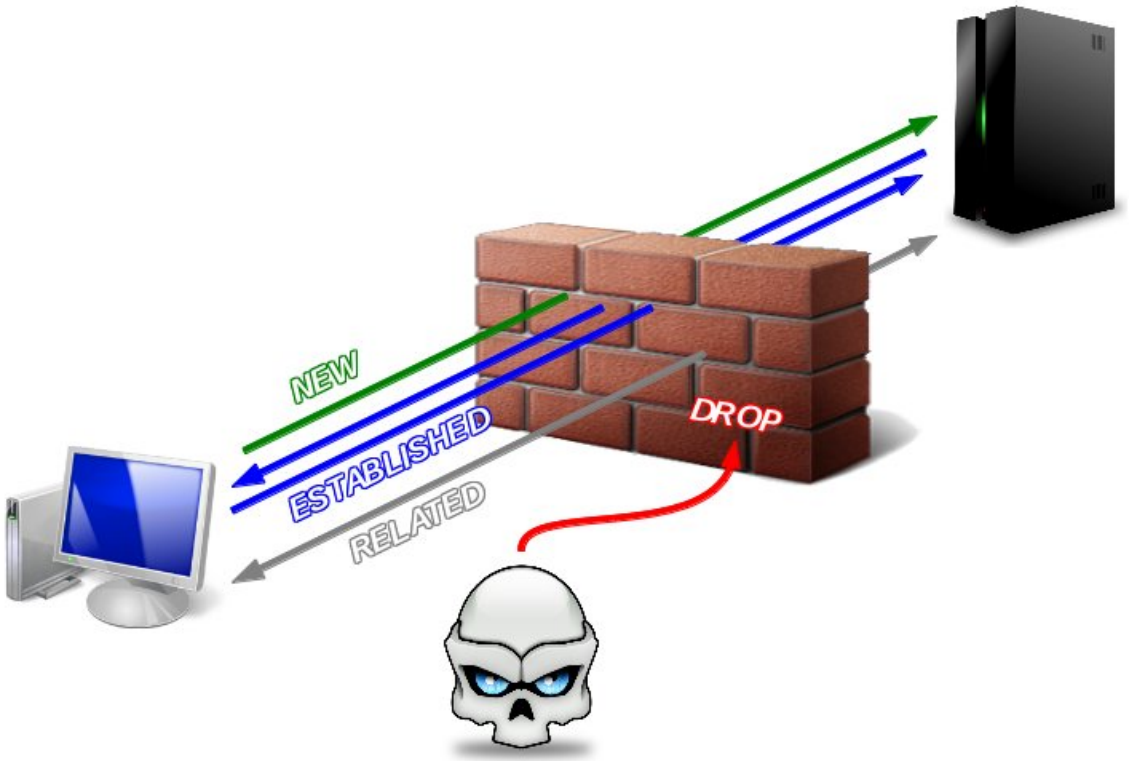
Exercises



Exercises

filter

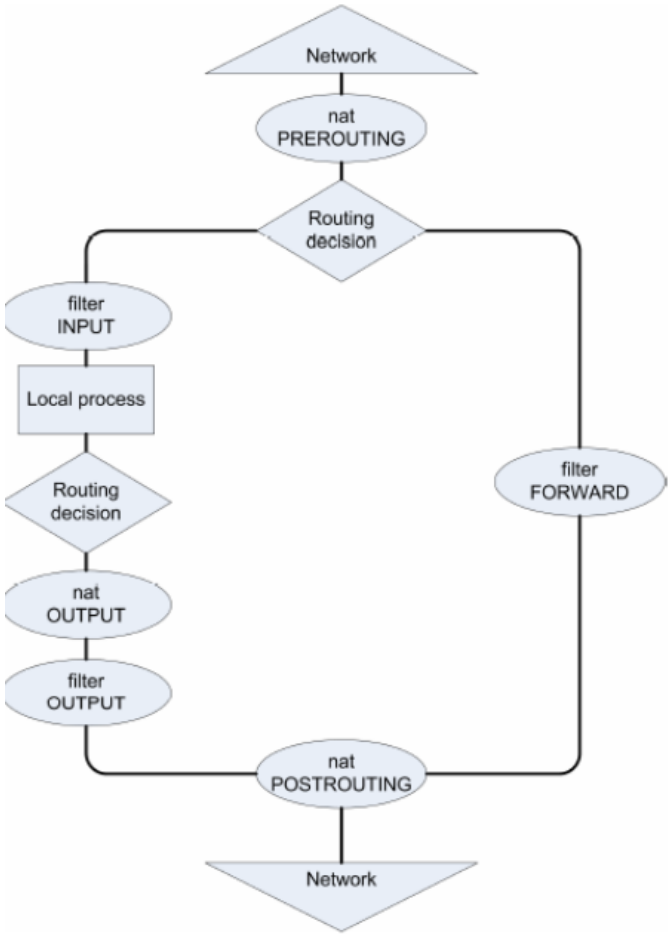
Connection tracking



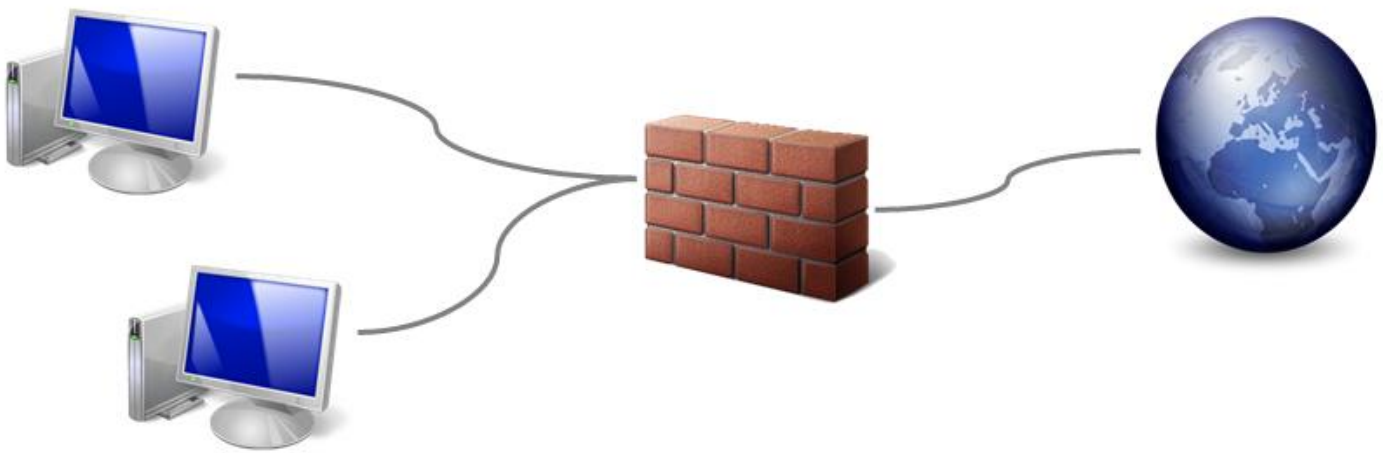
Exercises

TD connection tracking

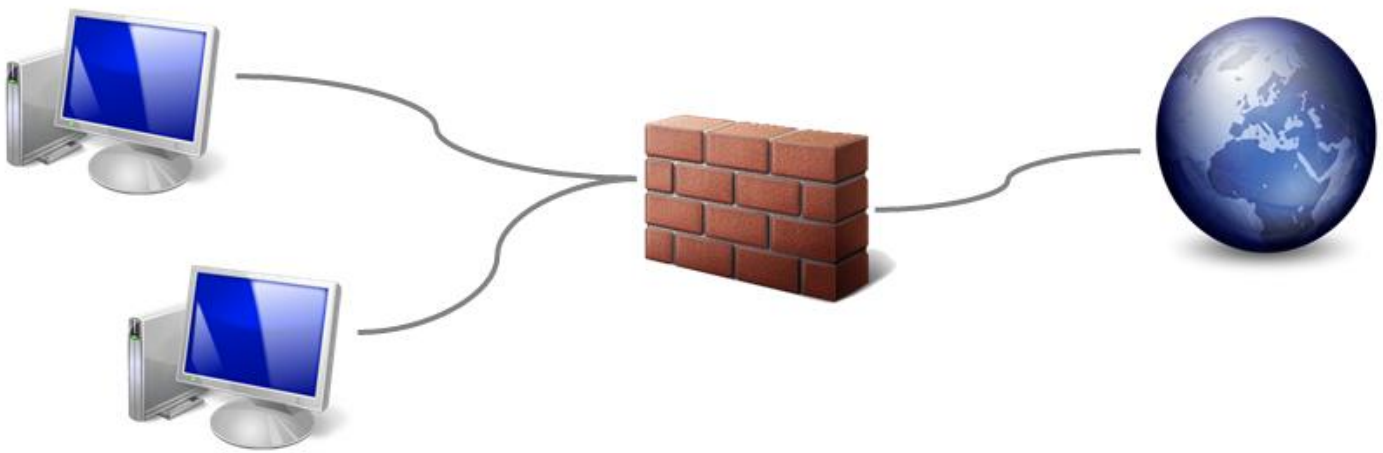
NAT and filter tables



SNAT

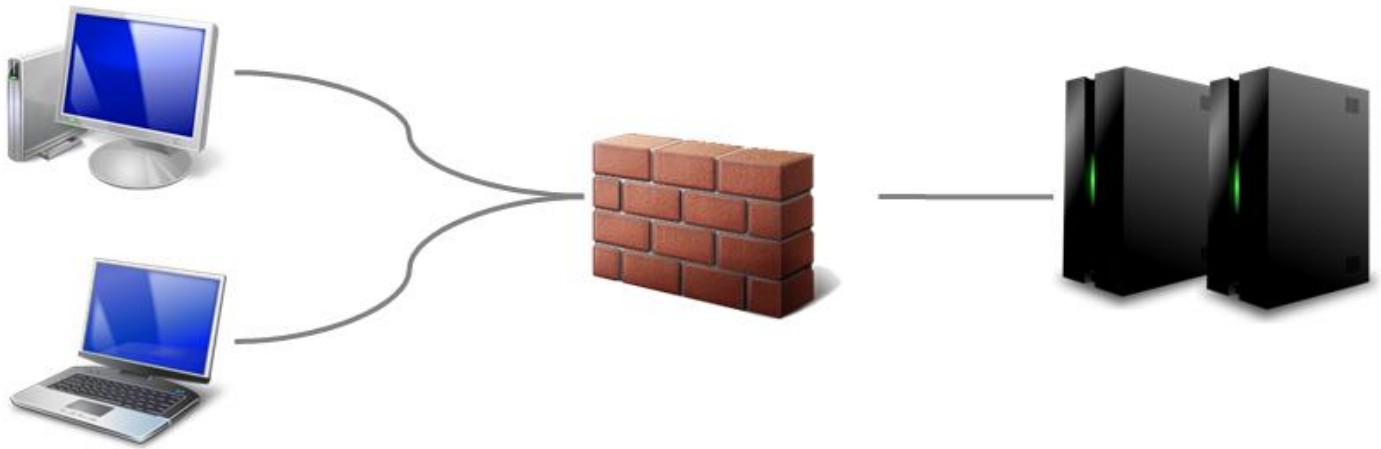


SNAT

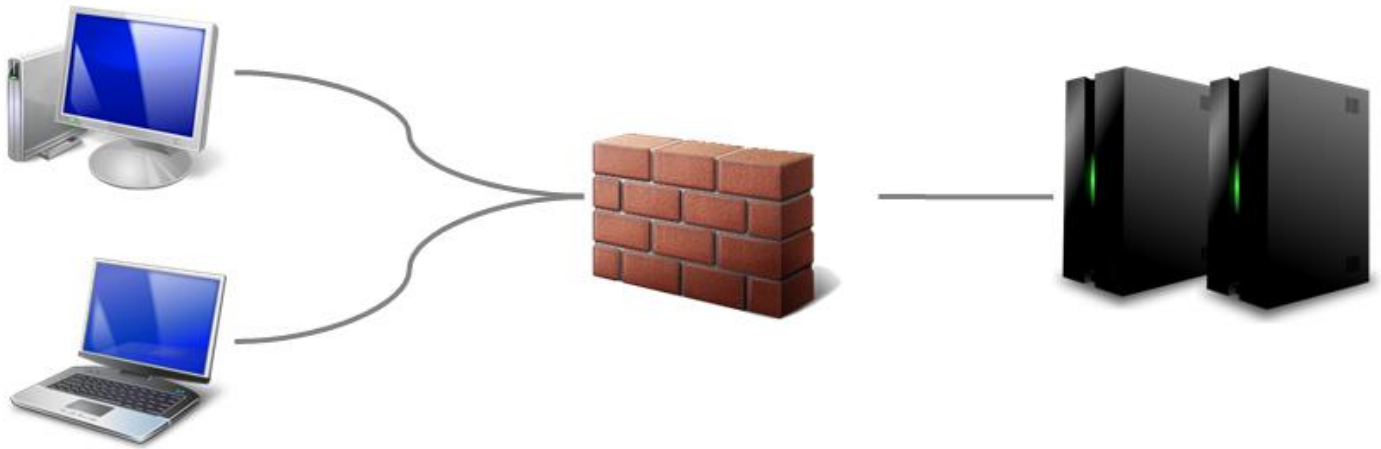


Before				After			
IP Src	Port Src	IP Dst	Port Dst	IP Src	Port Src	IP Dst	Port Dst
.101	1025	SRV	80	PUB	1025	SRV	80
.102	1026	SRV	80	PUB	1026	SRV	80

DNAT



DNAT



Before				After			
IP Src	Port Src	IP Dst	Port Dst	IP Src	Port Src	IP Dst	Port Dst
.101	1025	PUB	80	.101	1025	PRIV	80
.102	1026	PUB	80	.102	1026	PRIV	80

Exercises

Address Translation

References

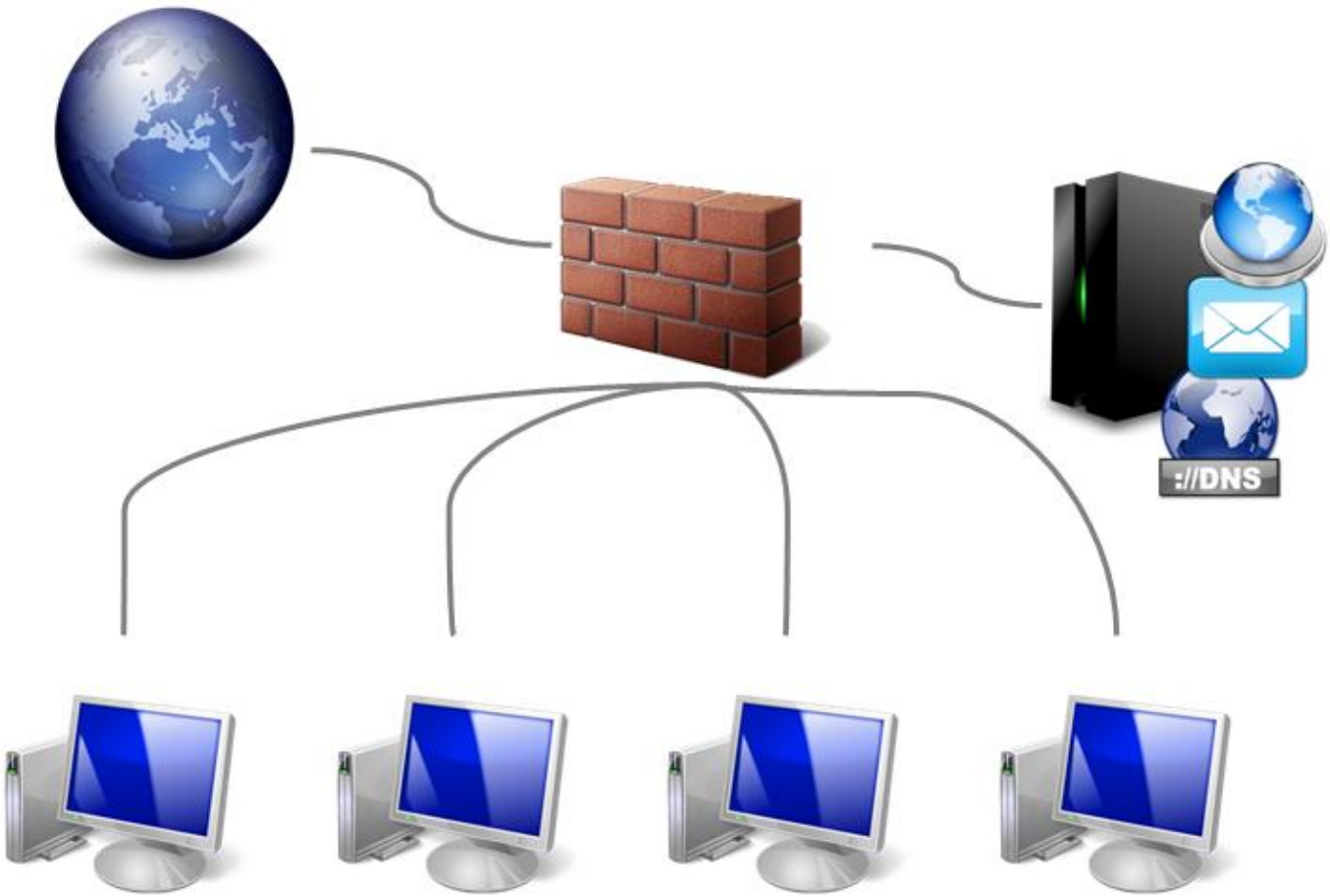
www.netfilter.org
Building Firewalls (O'Reilly)
Linux Firewalls (no starch press)

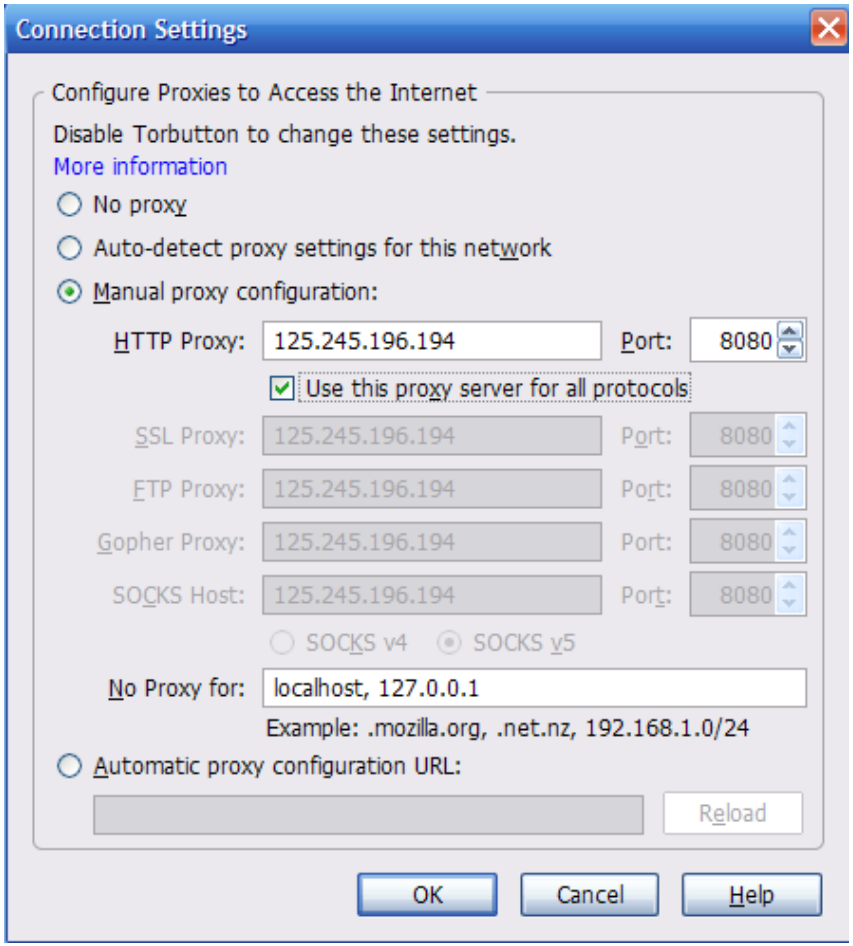
Plan

Proxy functions

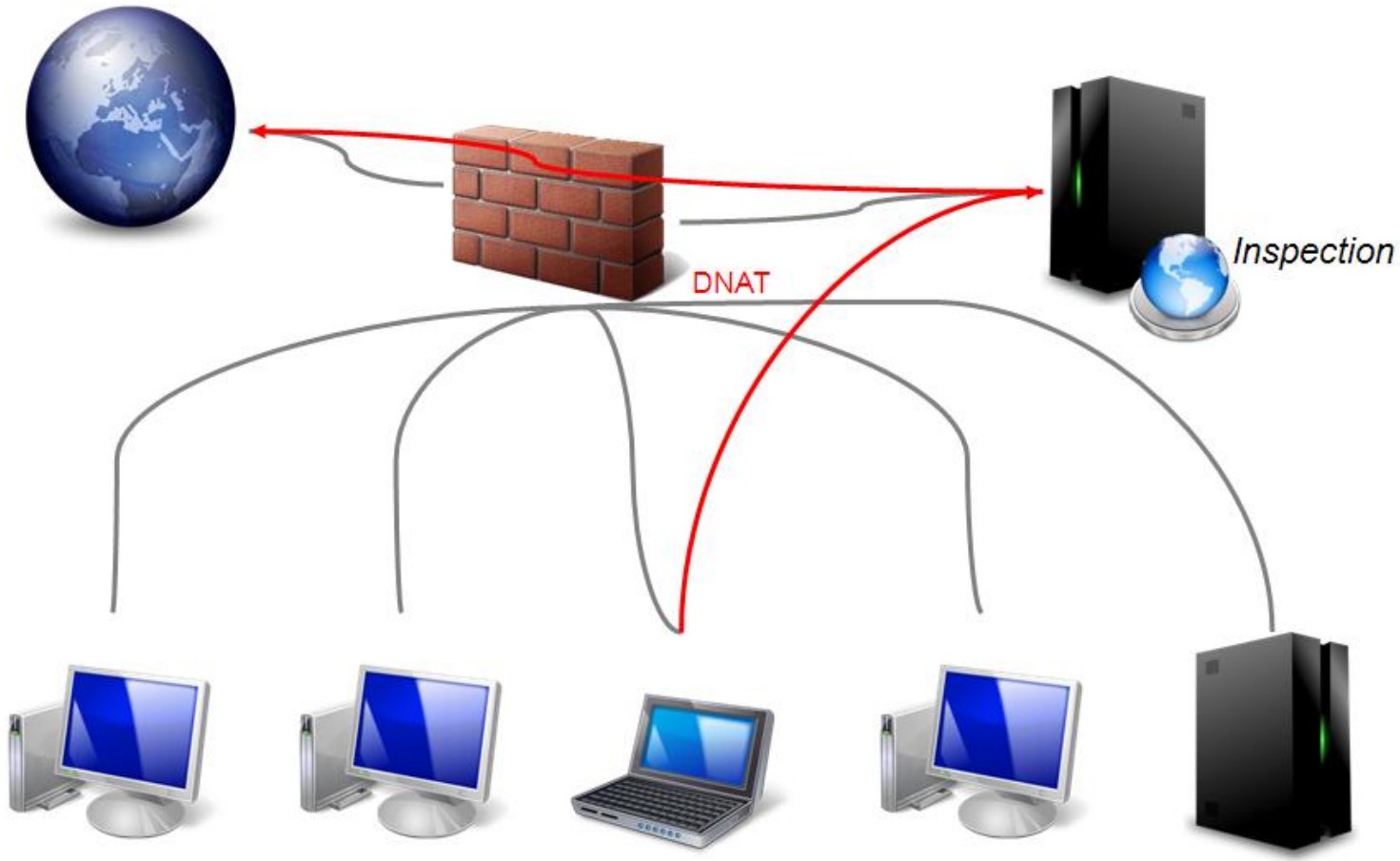
- Accelerate
- Verify compliance
- Anonymize
- Filter

Proxy Cache

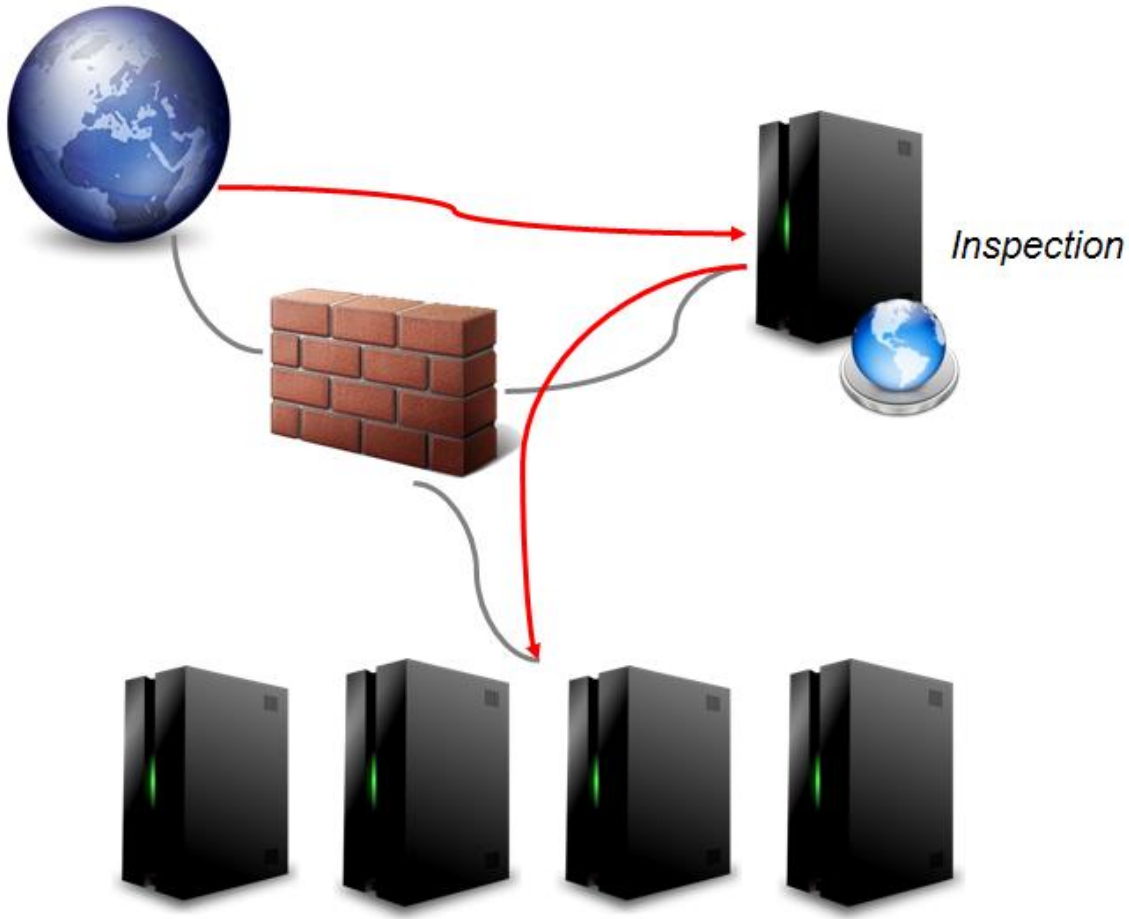



Connection Settings
Configure Proxies to Access the Internet
Disable Torbutton to change these settings.
More information
No proxy
Auto-detect proxy settings for this network
Manual proxy configuration:
HTTP Proxy: 125.245.196.194 Port: 8080
Use this proxy server for all protocols
SSL Proxy: 125.245.196.194 Port: 8080
FTP Proxy: 125.245.196.194 Port: 8080
Gopher Proxy: 125.245.196.194 Port: 8080
SOCKS Host: 125.245.196.194 Port: 8080
SOCKS v4 SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Automatic proxy configuration URL:
Reload
OK
Cancel
Help

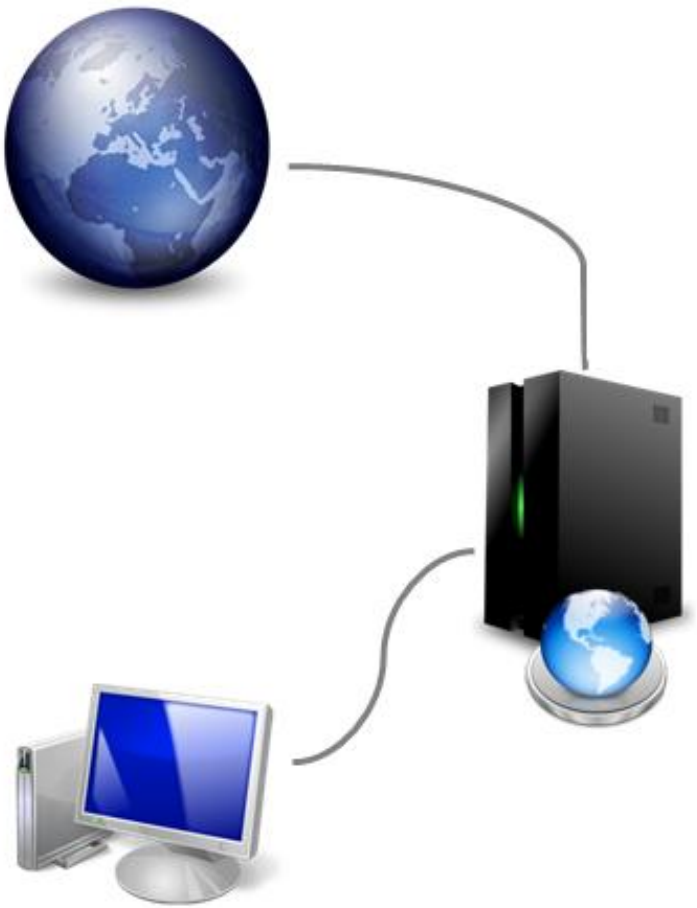
Transparent Proxy



Reverse Proxy



Exercises



Exercises

Proxy

Plan

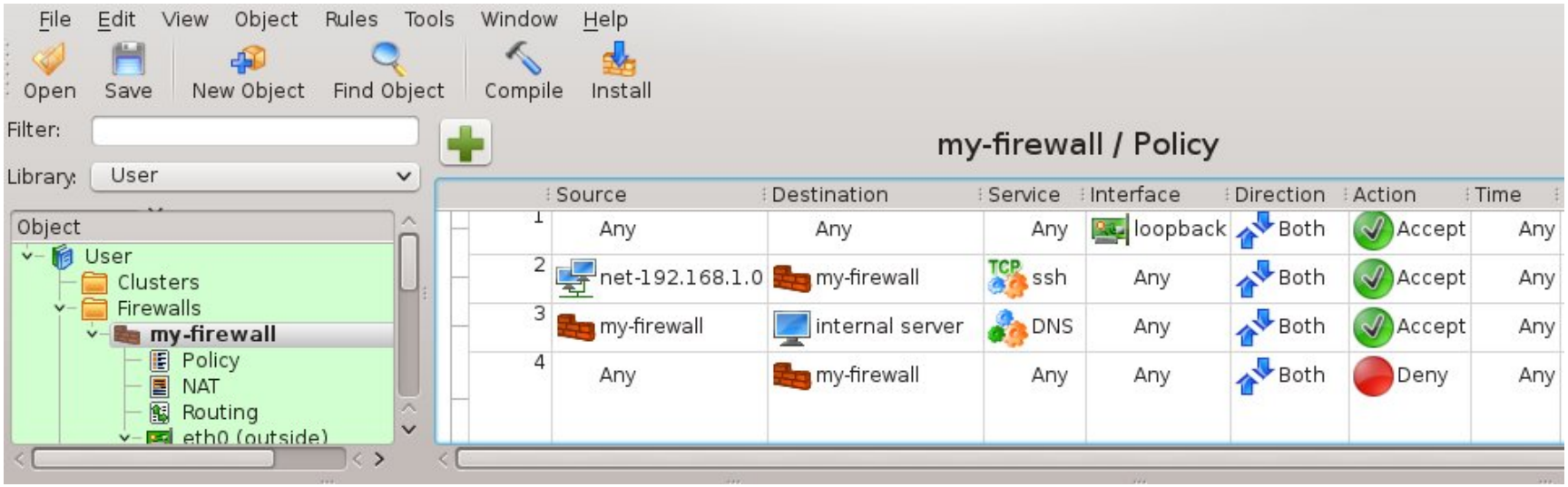
Exercises

Netfilter script reading

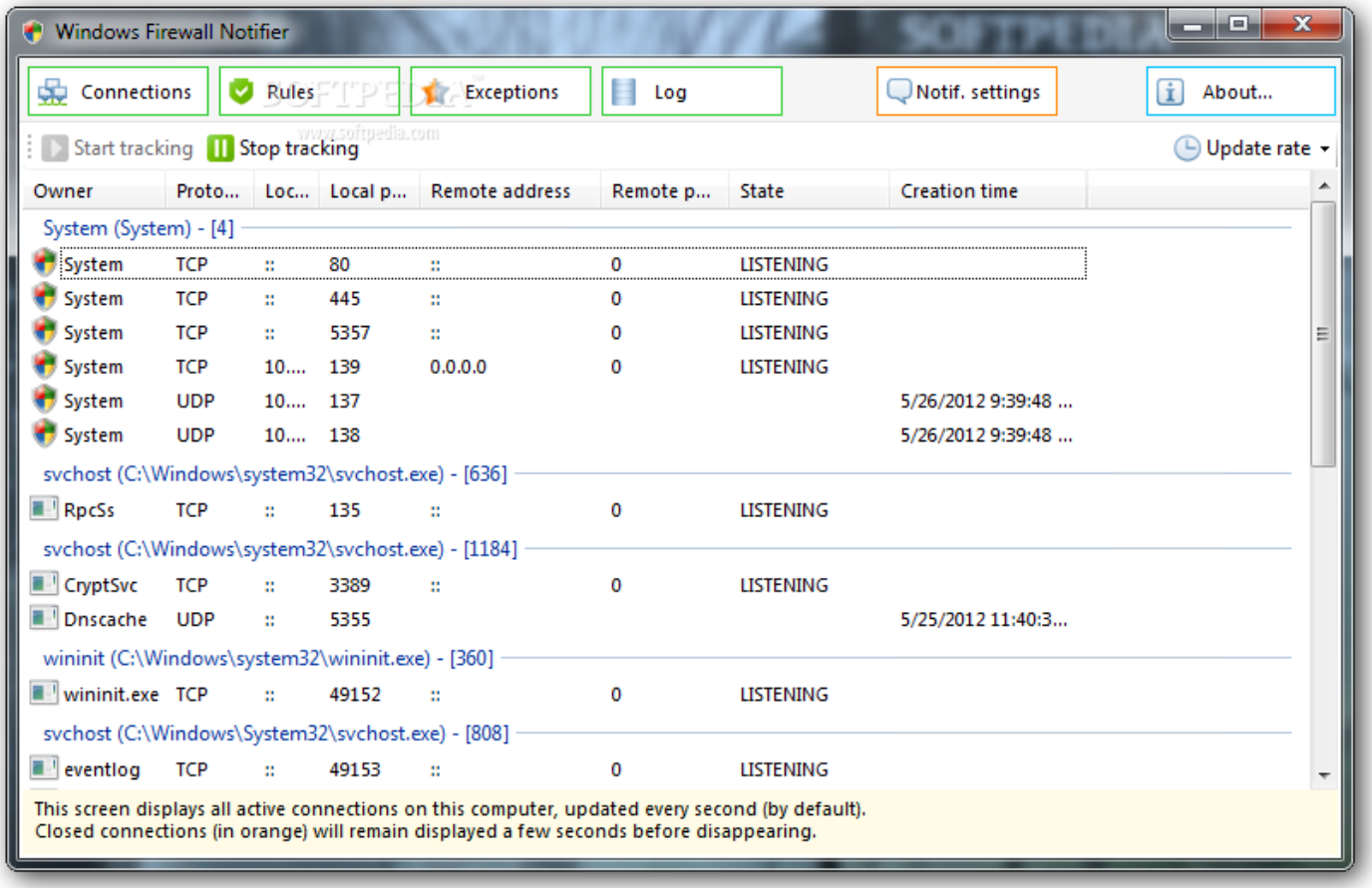
Exercises

Firewall logs

Overview


File Edit View Object Rules Tools Window Help
Open
Save
New Object
Find Object
Compile
Install
Filter:
Library: User
Object
User
Clusters
Firewalls
my-firewall
Policy
NAT
Routing
eth0 (outside)
my-firewall / Policy
Source
Destination
Service
Interface
Direction
Action
Time
1 Any Any Any loopback Both Accept Any
2 net-192.168.1.0 my-firewall ssh Any Both Accept Any
3 my-firewall internal server DNS Any Both Accept Any
4 Any my-firewall Any Any Both Deny Any

Overview


Windows Firewall Notifier
Connections
Rules
Exceptions
Log
Notif. settings
About...
Start tracking
Stop tracking
Update rate
Owner
Proto...
Loc...
Local p...
Remote address
Remote p...
State
Creation time
System (System) - [4]
System TCP :: 80 :: 0 LISTENING
System TCP :: 445 :: 0 LISTENING
System TCP :: 5357 :: 0 LISTENING
System TCP 10.... 139 0.0.0.0 0 LISTENING
System UDP 10.... 137 5/26/2012 9:39:48 ...
System UDP 10.... 138 5/26/2012 9:39:48 ...
svchost (C:\Windows\system32\svchost.exe) - [636]
RpcSs TCP :: 135 :: 0 LISTENING
svchost (C:\Windows\system32\svchost.exe) - [1184]
CryptSvc TCP :: 3389 :: 0 LISTENING
Dnscache UDP :: 5355 5/25/2012 11:40:3...
wininit (C:\Windows\system32\wininit.exe) - [360]
wininit.exe TCP :: 49152 :: 0 LISTENING
svchost (C:\Windows\System32\svchost.exe) - [808]
eventlog TCP :: 49153 :: 0 LISTENING
This screen displays all active connections on this computer, updated every second (by default).
Closed connections (in orange) will remain displayed a few seconds before disappearing.

Exercises

Firewall Builder

Plan

Case study of a firewall implementation