

Network Security

Chapter 10

Firewalls

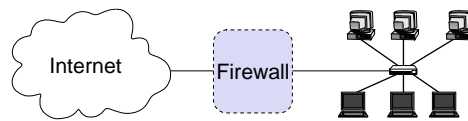
Arno Wacker
IngWiss / Distributed Systems
University Duisburg-Essen

Introduction to Network Firewalls (1)

- A network firewall can be compared to a moat of a medieval castle
 - It restricts people to **entering** at one carefully controlled point
 - It prevents attackers from getting close to other defenses
 - It restricts people to **leaving** at one carefully controlled point
- Physical realization
 - A special server with two networking cards
 - A special router

Introduction to Network Firewalls (2)

- A firewall connects two networks
 - Your corporate LAN
 - The evil internet



Introduction to Network Firewalls (3)

- What firewalls can do
 - A firewall is a **focus** for security decisions
 - A firewall can enforce a **security policy**
i.e. access control
 - A firewall can **log** Internet activity efficiently
 - A firewall can **limit exposure** to security problems in one part of a network

Introduction to Network Firewalls (4)

- What firewalls can not do
 - A firewall can't protect against **malicious insiders**
 - A firewall can't protect against connections that don't go through it
 - If, for example, there is a modem pool behind a firewall that provides PPP service to access a subnetwork, the firewall can not provide any protection against malicious traffic from dial-in users
 - A firewall can't protect against completely **new threats**
 - A firewall can't fully protect against **viruses**
 - A firewall can't set itself up correctly

Two Fundamental Approaches Regarding Firewall Policy (1)

- Default deny strategy
 - *“Everything that is not explicitly permitted is denied”*
 - Examine required services
 - Consider the security implications of these services and how the services can be safely provided
 - Allow only those services that can be safely provided and for which there is a legitimate need
 - Deny any other service

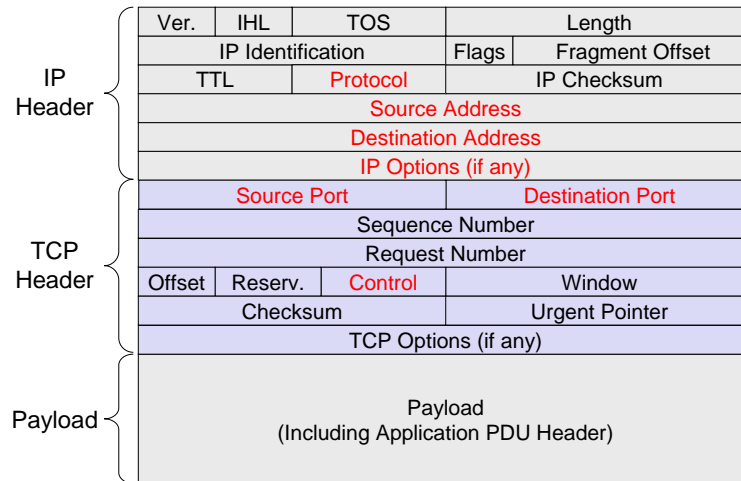
Two Fundamental Approaches Regarding Firewall Policy (2)

- Default permit strategy
 - *“Everything that is not explicitly forbidden is denied”*
 - Permit every service that is not considered dangerous
 - Example
 - Network file system (NFS) and X-Windows is not permitted across the firewall
 - Incoming telnet connections are only allowed to one specific host

What Internet Services are to be Considered?

- Electronic mail (SMTP)
- File exchange: (FTP), network file system (NFS)
- Remote terminal access: telnet, rlogin, ssh
- Usenet news: network news transfer protocol (NNTP)
- World wide web: hypertext transfer protocol (HTTP)
- Information about people: finger
- Messenger
- Name services: domain name service (DNS)
- Network management: simple network management protocol (SNMP)
- Time service: network time protocol (NTP)
- Window systems: X-Windows
- Printing systems: line printing protocols (LPR/LPD)

Recall: An IP Packet Carrying a TCP Segment



Protocol Fields Important for Firewalls (1)

- Data-Link Layer
 - Not of major interest to a firewall
 - Tells us about the network layer protocol
 - IP
 - Appletalk
 - IPX (Novell), etc.
 - MAC Addresses
 - E.g. Ethernet MAC Address

Protocol Fields Important for Firewalls (2)

- Network Layer (i.e. IP)
 - Source address
 - Destination address
 - Transport Protocol type: TCP, UDP, ...
 - IP Options
 - E.g. Source routing
 - The sender explicitly specifies the route an IP packet will take
 - As this is often used for attacks most firewalls discard these packets
 - In general, IP options are rarely used

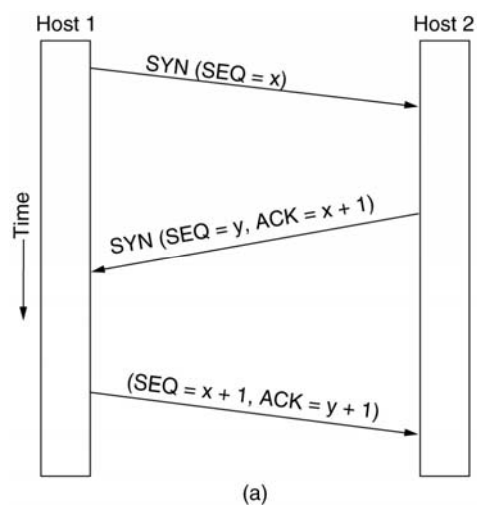
Protocol Fields Important for Firewalls (3)

- Transport Layer (i.e. TCP, UDP)
 - Source Port, Destination Port
 - Useful because of well-known port numbers
 - Allows (with a limited degree of confidence) for identifying the application protocol
 - Control
 - ACK: Helps to identify connection requests
 - SYN: Helps to identify connection confirmations
 - RST: It can be used to shut peers up without returning helpful error messages

Recall: Well known ports

- Well known ports
 - FTP 21
 - Telnet 23
 - SMTP 25
 - HTTP 80
 - Kerberos 88
 - POP3 110
 - IMAP 143
 - HTTPS 443
- Example: WWW
`http://www.heise.de = http://www.heise.de:80`

Recall: TCP Connection Establishment



Protocol Fields Important for Firewalls (4)

- Application Protocol
 - In some cases a firewall might even need to peek into application protocol header fields
 - HTTP
 - SMTP
 - FTP, ...
 - Idea: Check well-formedness of messages
 - Prevents attacks based on malformed messages
 - However, why should the implementation of the firewall be better than the real service?

Firewall Terminology (1)

- Firewall
 - A component or a set of components that restricts access between a protected network and the Internet or between other sets of networks
- Packet Filtering
 - The action a device takes to selectively control the flow of data to and from a network
 - Packet filtering is an important technique to implement access control on the subnetwork-level for packet oriented networks, e.g. the Internet
 - A synonym for packet filtering is screening

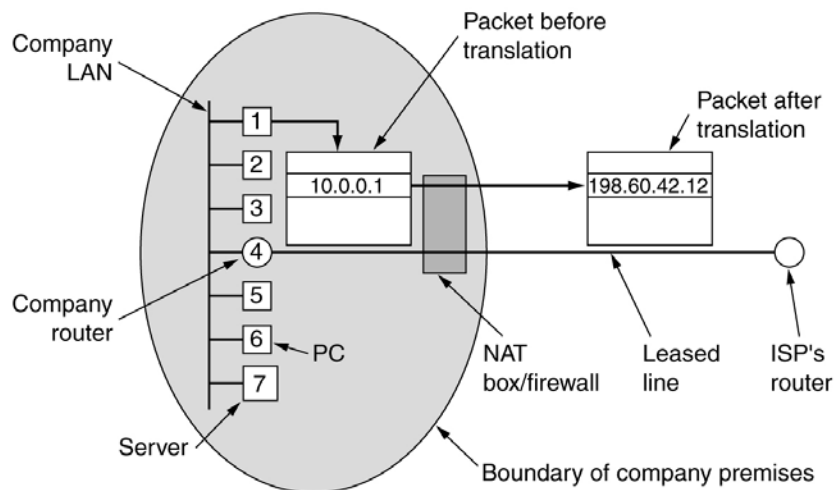
Firewall Terminology (2)

- **Bastion Host**
 - A computer that must be highly secured because it is more vulnerable to attacks than other hosts on a subnetwork
 - A bastion host in a firewall is usually the main point of contact for user processes of hosts of internal networks with processes of external hosts
- **Dual homed host**
 - A general purpose computer with at least two network interfaces

Firewall Terminology (3)

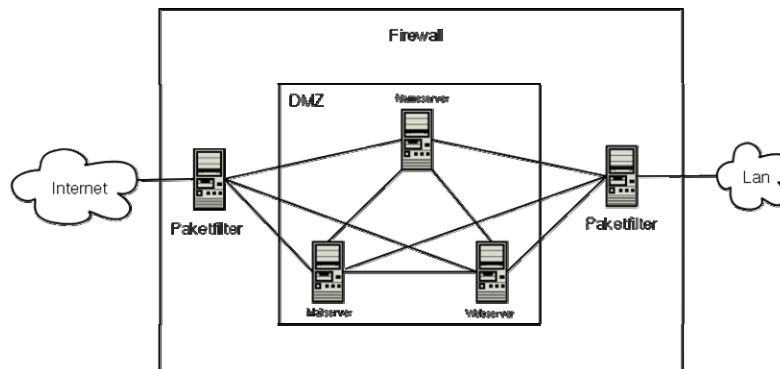
- **Proxy**
 - A program that deals with external servers on behalf of internal clients
 - Proxies relay approved client requests to real servers and also relay the servers answers back to the clients
 - A proxy understands the commands of an application protocol
- **Network Address Translation (NAT)**
 - A procedure by which a router changes data in packets to modify the network addresses
 - This allows to conceal the internal network addresses (even though NAT is not actually a security technique)

Recall: NAT – Network Address Translation

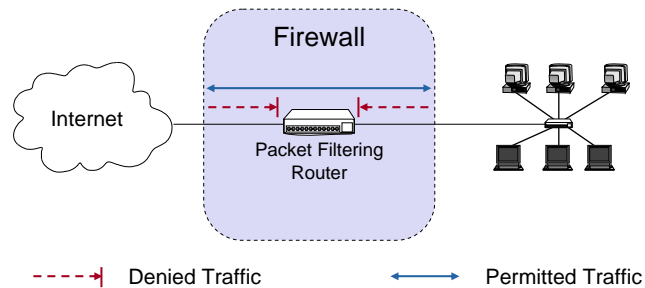


Firewall Terminology (4)

- De-Militarized Zone (DMZ)
 - A sub-network added between an external and an internal network

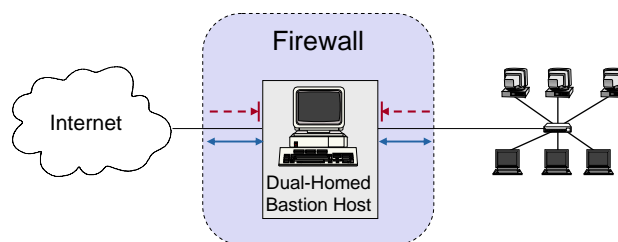


Packet Filtering Architecture



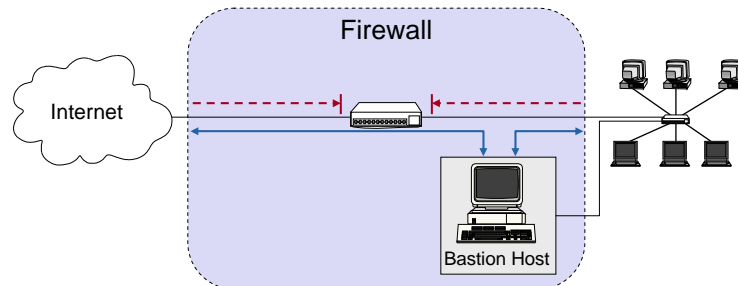
- The most simple architecture just consists of a packet filtering router or a Linux PC
 - Such a firewall PC is dual-homed

Dual-Homed Bastion Host Architecture



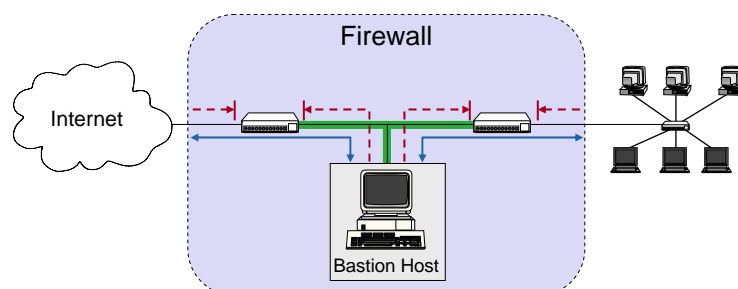
- The dual-homed host provides
 - Proxy services, e.g. for HTTP
 - Sometimes packet filtering
- Drawback
 - Can become a bottleneck

Screened Bastion Host Architecture



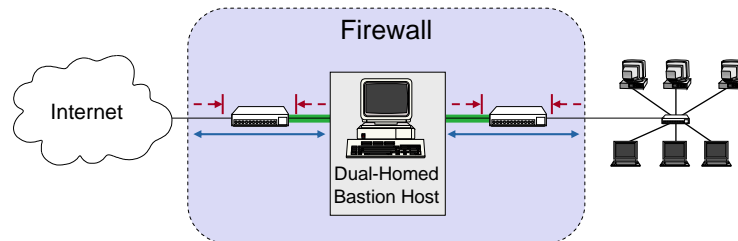
- The packet filter ...
 - allows traffic between screened host and the Internet
 - blocks traffic between internal hosts and the Internet
- The screened host provides proxy services

Screened Subnet Architecture



- A DMZ is created between two packet filters
- The inner packet filter helps against a compromised bastion host
 - For example, this avoids a compromised bastion host to sniff on internal traffic

Split Screened Subnet Architecture



- A dual-homed bastion host splits the DMZ in two distinct networks
 - The dual-homed bastion host provides finer control on the connections as his proxy services are able to interpret application protocols

An Example Packet Filtering Rule Set (1)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP		25		Permit
B	Outbound	Internal	External	TCP		>1023		Permit
C	Outbound	Internal	External	TCP		25		Permit
D	Inbound	External	Internal	TCP		>1023		Permit
E	Either	Any	Any	Any		Any		Deny

- This first rule set aims to specify, that incoming and outgoing email should be the only allowed traffic into and out of a protected network
- Email is relayed between two servers by transferring it to an SMTP-daemon on the target server (server port 25, client port > 1023)

An Example Packet Filtering Rule Set (2)

- For example, telnet is blocked now
 - Telnet servers listen on port 23
 - All allowed traffic must be either to port 25 or to a port number > 1023
- However, X11 is not blocked ☹️
 - An X11-server usually listens at port 6000, clients use port numbers > 1023
 - Thus, an incoming X11-request is not blocked (B), neither is any answer (D)
 - This is highly undesirable, as the X11-protocol offers many vulnerabilities to an attacker, like reading and manipulating the display and keystrokes

An Example Packet Filtering Rule Set (3)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP	>1023	25		Permit
B	Outbound	Internal	External	TCP	25	>1023		Permit
C	Outbound	Internal	External	TCP	>1023	25		Permit
D	Inbound	External	Internal	TCP	25	>1023		Permit
E	Either	Any	Any	Any	Any	Any		Deny

- Traffic is allowed only between
 - Port 25 external/internal
 - Port >1023 internal/external
- However, we do not yet distinguish between initiator and responder

An Example Packet Filtering Rule Set (4)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP	>1023	25	Any	Permit
B	Outbound	Internal	External	TCP	25	>1023	Yes	Permit
C	Outbound	Internal	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Internal	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

- As the ACK-bit is required to be set in rule B, it is not possible to open a new TCP connection in the outbound direction to ports >1023
 - Reason: TCP's connect-request is signaled with the ACK-bit not set

An Example Packet Filtering Rule Set (5)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Bastion	TCP	>1023	25	Any	Permit
B	Outbound	Bastion	External	TCP	25	>1023	Yes	Permit
C	Outbound	Bastion	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Bastion	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

- If the firewall comprises a bastion host, the packet filtering rules should further restrict traffic flow (→ screened host architecture)