

Network Security - Week 7

João Soares

DCC/FCUP

2023

Responding to DoS Attacks

- Identify type of attack
 - Capture and analyze packets - Intrusion Detection Systems
 - Design filters to block attack traffic upstream - Firewalls
 - Identify and correct system/application bugs

Responding to DoS Attacks

- Identify type of attack
 - Capture and analyze packets - Intrusion Detection Systems
 - Design filters to block attack traffic upstream - Firewalls
 - Identify and correct system/application bugs
- Have ISP trace packet flow back to source
 - Often difficult and time consuming
 - Necessary when planning legal action

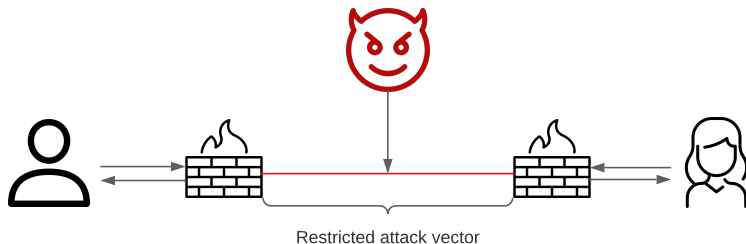
Responding to DoS Attacks

- Identify type of attack
 - Capture and analyze packets - Intrusion Detection Systems
 - Design filters to block attack traffic upstream - Firewalls
 - Identify and correct system/application bugs
- Have ISP trace packet flow back to source
 - Often difficult and time consuming
 - Necessary when planning legal action
- Implement contingency plan
 - Switch to alternate backup servers
 - Commission fresh servers at a new site with new addresses

Responding to DoS Attacks

- Identify type of attack
 - Capture and analyze packets - Intrusion Detection Systems
 - Design filters to block attack traffic upstream - Firewalls
 - Identify and correct system/application bugs
- Have ISP trace packet flow back to source
 - Often difficult and time consuming
 - Necessary when planning legal action
- Implement contingency plan
 - Switch to alternate backup servers
 - Commission fresh servers at a new site with new addresses
- Update incident response plan
 - Analyze the attack and response for future handling

Firewalls



- Firewall decides what to let in to internal network and/or to let out
- Access control for the network
- At a multitude of granularity levels

Managing what comes in and goes out

A firewall is like a **secretary**

- To meet with an executive:
 - 1 Contact the secretary
 - 2 Secretary will assess if the meeting is important
 - 3 Many requests are filtered according to relevance metrics

A firewall is like a **secretary**

- To meet with an executive:
 - 1 Contact the secretary
 - 2 Secretary will assess if the meeting is important
 - 3 Many requests are filtered according to relevance metrics
- If you want to meet the chair of CS department...
 - Secretary will do some filtering
- If you want to meet the President
 - Secretary will do a lot of filtering

Criteria under which “meetings can be scheduled”

- Filtering done according to an access policy
- Types of traffic
- Address ranges and protocols
- Applications and content types

Criteria under which “meetings can be scheduled”

- Filtering done according to an access policy
 - Types of traffic
 - Address ranges and protocols
 - Applications and content types
-
- Specification of which traffic types the org needs to support
 - Then refined to detail the filter elements, implemented with an appropriate firewall topology
 - Bad configuration **can lead to loss of communication**

Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several internet functions that are not security related (e.g. NAT)
- Can serve the platform for IPSec (tunnel mode)

Capabilities and Limits

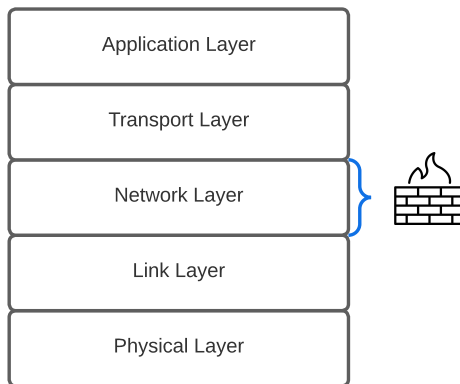
Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several internet functions that are not security related (e.g. NAT)
- Can serve the platform for IPSec (tunnel mode)

Limitations

- Cannot protect against attacks bypassing the firewall
- May not protect fully against internal threats
- Laptop, PDA, or portable storage device may be infected outside corporate network, and then used internally
- Improperly secured wireless LAN can be accessed outside the organization

Packet Filter- High-level view



- Operates at the network layer
- Observes IP packets and assesses their importance
- Why can this be incompatible with IPsec?

Packet Filter - Criteria

Packet filtering depends on:

- Source IP address
- Destination IP address
- Source Port
- Destination Port
- Flag bits (SYN, ACK, etc.)
- Egress or ingress

Packet filtering depends on:

- Source IP address
- Destination IP address
 - Allows for excluding problematic sources (blacklist/whitelist)
- Source Port
- Destination Port
- Flag bits (SYN, ACK, etc.)
- Egress or ingress

Packet filtering depends on:

- Source IP address
- Destination IP address
 - Allows for excluding problematic sources (blacklist/whitelist)
- Source Port
- Destination Port
 - Easy to profile and avoid attacks on problematic services
- Flag bits (SYN, ACK, etc.)
- Egress or ingress

Packet Filter - Criteria

Packet filtering depends on:

- Source IP address
- Destination IP address
 - Allows for excluding problematic sources (blacklist/whitelist)
- Source Port
- Destination Port
 - Easy to profile and avoid attacks on problematic services
- Flag bits (SYN, ACK, etc.)
 - Remember how we can DoS on TLS?
- Egress or ingress

Packet Filter - Strengths x Weaknesses

Advantages

- Speed
- Simplicity
- Transparent to users

Packet Filter - Strengths x Weaknesses

Advantages

- Speed
- Simplicity
- Transparent to users

Disadvantages

- No concept of state
- Vulnerable to attacks on TCP/IP bugs
- Cannot see TCP connections
- Unknowing of application data and context

Packet Filter - Configuration

Configured via Access Control Lists (ACLs)

Action	Source IP	Dest IP	Source Port	Dest Port	Protocol	Flag Bits
Allow	Inside	Outside	Any	80	HTTP	Any
Allow	Outside	Inside	80	>1023	HTTP	ACK
Deny	All	All	All	All	All	All

- Traffic is restricted to web browsing:
- Accept all outgoing HTTP traffic to port 80
- Accept all incoming HTTP ACK replies
- Reject everything else

Issues

- Cannot prevent attack on application bugs
- Limited logging functionality
- Advanced user authentication not supported
- Improper configuration can lead to breaches

Issues

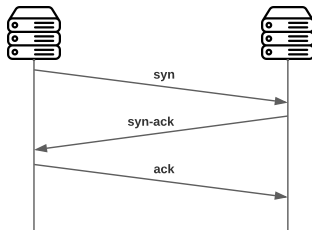
- Cannot prevent attack on application bugs
- Limited logging functionality
- Advanced user authentication not supported
- Improper configuration can lead to breaches

Attacks

- IP address spoofing
- Source route attacks
- Tiny fragment attacks

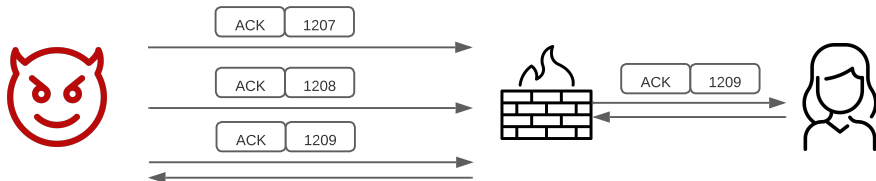
Packet filter exploits - Port scanning via TCP

Recall TCP (again)



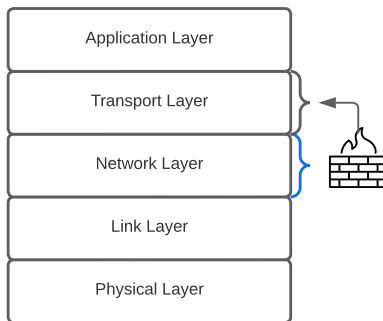
- ❶ A client sends a SYN (synchronize) message
- ❷ The server replies with a SYN-ACK message
- ❸ The client concludes with a ACK (acknowledge) message
 - What if we sent an unrelated ACK message?
 - Mismatched sequence numbers
 - The server replies with RST (TCP reset)
 - I think you are confused, buddy. Try again

Packet filter exploits - Port scanning via TCP



- Attacker gets to know 1029 is operational
- Handshake was unsuccessful, but that was never the point
- Firewall knows TCP traffic is allowed...
- ... but lacks *context* to know if it makes sense

Stateful Packet Filter



- Adds state to the packet filter
- Operates at the transport layer
- Remembers TCP connections (e.g. flag bits)
- Can even remember UDP packets (e.g. DNS requests)

Connection State Table - Example

Source Address	Source port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established

Stateful Packet Filter

Advantages

- Can do everything a packet filter can
- Keeps track on ongoing connections
- Relies on protocol logic to detect misbehaviors
 - Avoids TCP ACK scan

Stateful Packet Filter

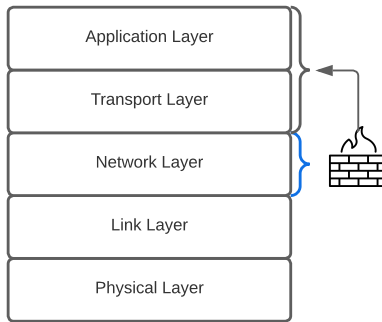
Advantages

- Can do everything a packet filter can
- Keeps track on ongoing connections
- Relies on protocol logic to detect misbehaviors
 - Avoids TCP ACK scan

Disadvantages

- Cannot see application data
 - Lacks internal application logic
 - Thus cannot accurately detect deviations from *expected behavior*
- Slower than packet filtering

Application Proxy



- A *proxy* is something that acts on your behalf
- Application proxy looks at incoming application data
- Verifies that data is safe before allowing passage

Application Proxy

a.k.a. Application-Level Gateway

Additional security layer

- For every supported application protocol
 - SMTP, POP3, HTTP, SSH, ...
 - Create a new packet before sending to the lower layers
 - Validation done at the data granularity
 - Spoofing packet implies convincing proxy to accept

Application Proxy

a.k.a. Application-Level Gateway

Additional security layer

- For every supported application protocol
 - SMTP, POP3, HTTP, SSH, ...
 - Create a new packet before sending to the lower layers
 - Validation done at the data granularity
 - Spoofing packet implies convincing proxy to accept
- Large amount of processing per connection
- Can enforce application-specific policies
- Highly configurable

Advantages

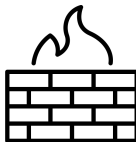
- Complete view of connections and application data
 - Can capture nuanced behavior
 - E.g. disable specific features, or specify execution criteria
- Filter bad data at application layer
 - Prevents software-level errors and vulnerability exploitation
 - E.g. macros allowing for SQL injection or buffer overflow

Advantages

- Complete view of connections and application data
 - Can capture nuanced behavior
 - E.g. disable specific features, or specify execution criteria
- Filter bad data at application layer
 - Prevents software-level errors and vulnerability exploitation
 - E.g. macros allowing for SQL injection or buffer overflow

Disadvantages

- Performance takes a toll – yet another security layer
- Each application must have the associated proxy code



Permissive

Allow by default; block some

- Easy to make mistakes
- Mistakes can lead to security breaches
- Exploits can be covert, i.e. not obvious that they are occurring

Restrictive

Block by default; allow some

- Much more secure
- Mistakes can lead to availability problems
- Exploits depend on the security requirements and specifications

A few examples

Permissive

Allow by default; block some

- IRC (messaging)
- Telnet
- SNMP (routing)
- Echo

Restrictive

Block by default; allow some

- HTTP
- POP3
- SMTP (mail)
- SSH

Rule Order

- A firewall policy is a collection of rules
- Packets can contain several headers (IPSec)
- Systems can be quite heterogeneous

- A firewall policy is a collection of rules
- Packets can contain several headers (IPSec)
- Systems can be quite heterogeneous

When setting a policy, you have to know in which order rules (and headers) are analysed and evaluated.

- Two main options for ordering rules:
 - Apply the *first matching entry* in the list of rules
 - Apply the *entry with the best match* for the packet

A Typical Firewall Ruleset

- **Allow** from internal network to Internet
 - HTTP, FTP, HTTPS, SSH, DNS
- **Allow** reply packets
- **Allow** from anywhere to Mail server
 - TCP port 25 (SMTP) only
- **Allow** from Mail server to Internet
 - SMTP, DNS
- **Allow** from inside to Mail server
 - SMTP, POP3
- **Block** everything else

Packet Filter Rules

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	CARLOS	*	We don't trust these people
allow	{our hosts}	25	*	*	Connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	Connection to their SMTP port

Rule Set D

action	ourhost	port	theirhost	port	flags	comment
allow	{our hosts}	*	*	25		Our packets to their SMTP port
allow	*	25	*	*	ACK	Their replies

Rule Set E

action	ourhost	port	theirhost	port	flags	comment
allow	{our hosts}	*	*	*		Our outgoing calls
allow	*	25	*	*	ACK	Replies to our calls
allow	*	*	*	>1024		Traffic to a specific domain

Firewall Location

- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?

Firewall Location

- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?
- Requires external access to receive mail from the Internet
 - Should be on the inside of the firewall

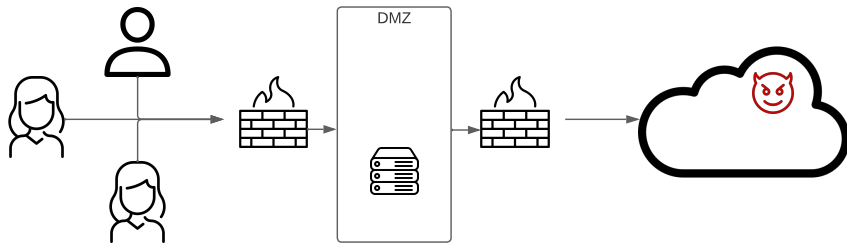
Firewall Location

- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?
- Requires external access to receive mail from the Internet
 - Should be on the inside of the firewall
- Requires internal access to receive mail from the internal network
 - Should be on the outside of the firewall

Firewall Location

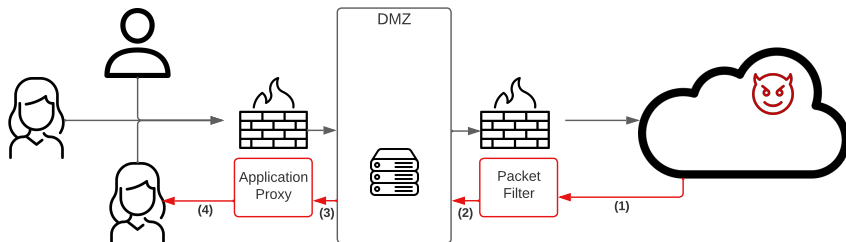
- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?
 - Requires external access to receive mail from the Internet
 - Should be on the inside of the firewall
 - Requires internal access to receive mail from the internal network
 - Should be on the outside of the firewall
- **R:** “perimeter network” (a.k.a. DMZ)

Demilitarized Zone (DMZ)



- Demilitarized Zone is used for servers that require (selective) access from both inside and outside the firewall
- Very unique position security-wisely

Defence in Depth



- If one layer is breached, there are more layers
- Carlos may breach one layer
 - But breaking other layers may require a different skillset
 - And it takes additional time to go from (1) to (4)
- Useful to detect an attack in progress

There are several option for locating firewalls

- I - Bastion host
- II - Host-based individual firewall
- III - Personal firewall

- Critical strongpoint in the network
- Host application/circuit-level gateways
- Common characteristics:
 - Runs secure O/S, only essential services
 - May require user auth to access proxy or host
 - Each proxy can restrict features, hosts accessed
 - Small, simple proxies, security-checked
 - Limited disk use, read-only code

II -Host-Based Firewalls

- Used to secure an *individual* host
- Available in/add-on for many O/Ss
- Filter packet flows
- Often used on server

II -Host-Based Firewalls

- Used to secure an *individual* host
- Available in/add-on for many O/Ss
- Filter packet flows
- Often used on server

Advantages

- Tailored filter rules for specific host needs
- Protection from both internal/external attacks
- Additional layer of protection to org firewall

III - Personal Firewalls

- Controls traffic flow to/from PC
- For both home and corporate usage
- Can be a software module on a PC
- Or in a DSL router/gateway

III - Personal Firewalls

- Controls traffic flow to/from PC
- For both home and corporate usage
- Can be a software module on a PC
- Or in a DSL router/gateway

Characteristics

- Typically much less complex than its counterparts
- Primary role to deny unauthorized access
- May also monitor outgoing traffic to detect/block malware activity

Scan open ports through firewall

- Attacker knows IP address of firewall
- An an IP address of one system inside firewall

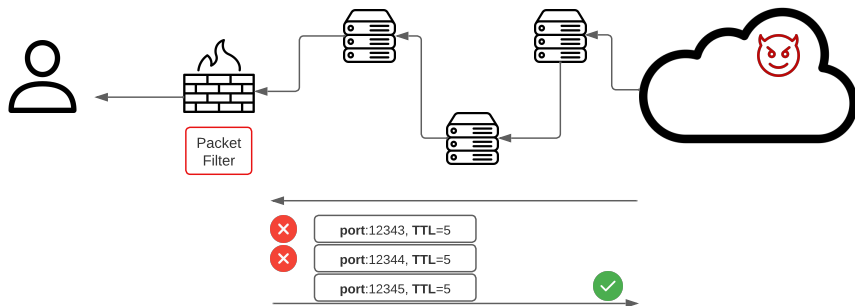
Scan open ports through firewall

- Attacker knows IP address of firewall
- An an IP address of one system inside firewall

Method (test port N):

- Set TTL to 1 more than the number of hops to firewall
- Set destination port to N
- If firewall allows data port N , get TIME EXCEEDED error message
- Otherwise, no reply
- More info here

Firewalk and Proxy Firewall



- Not feasible through an application proxy
- The application creates a new packet
- Which rewrites old TTL

IPTables: Firewalls in Linux

Terminology

Tables: Context of applying rules

- Filter: packet filtering/firewalling
- Nat: network address translation
- Mangle: modification of packets

IPTables: Firewalls in Linux

Terminology

Tables: Context of applying rules

- Filter: packet filtering/firewalling
- Nat: network address translation
- Mangle: modification of packets

Chains: Place/stage of packet processing

- Input: at system entrance (before being sent to apps)
- Output: at system exit (before being sent for routing)
- Forward: for systems operating as routers

IPTables: Firewalls in Linux

Terminology

Tables: Context of applying rules

- Filter: packet filtering/firewalling
- Nat: network address translation
- Mangle: modification of packets

Chains: Place/stage of packet processing

- Input: at system entrance (before being sent to apps)
- Output: at system exit (before being sent for routing)
- Forward: for systems operating as routers

Targets: Destination to give to packet

- Drop, Accept, Reject, Log, Return, Queue

Methodology

- Add rules to TABLES specifying the CHAINS there in.

Methodology

- Add rules to TABLES specifying the CHAINS there in.
- When a packet matches a rule, its TARGET is selected
 - TARGETS vary according to TABLES
 - Filter Table: DROP, ACCEPT
 - NAT Table: DNAT, SNAT, MASQUERADE, REDIRECT

Methodology

- Add rules to TABLES specifying the CHAINS there in.
- When a packet matches a rule, its TARGET is selected
 - TARGETS vary according to TABLES
 - Filter Table: DROP, ACCEPT
 - NAT Table: DNAT, SNAT, MASQUERADE, REDIRECT
- New CHAINS may be created by the user
- These can then be set as TARGETS of rules

IPTables: Filter Targets

Target	Purpose
DROP	Discard a packet without notification to source
ACCEPT	Accept packet
REJECT	Reject packet with notification to source
LOG	Log information about the packet
RETURN	Stops evaluation of rules in the current chain
QUEUE	Puts the packet in queue to be sent to an application

IPTables: Examples

Accept ICMP echo-request pks with source address 10.1.0.1

```
iptables -A INPUT -S 10.1.0.1 -p icmp --icmp-type  
echo-request -j ACCEPT
```

Accept at server exit TCP pks in interface eth1 with dest. port 22 and dest. address in network 10.5.0.0/24

```
iptables -A OUTPUT -d 10.5.0.0/24 -p tcp --dport 22  
-o eth1 -j ACCEPT
```

Set DROP policy to all packets that are not authorized by previous policies

```
iptables -P INPUT DROP
```

More examples here

Firewalls as the first line of defence

- Establish the criteria under which packets come in/go out
- Can be deployed in a variety of ways
 - Packet filter - network
 - Stateful packet filter - transport layer
 - Application proxy - application layer
- No clear-cut “best” practice.
- Depends on security requirements

Firewalls as the first line of defence

- Establish the criteria under which packets come in/go out
- Can be deployed in a variety of ways
 - Packet filter - network
 - Stateful packet filter - transport layer
 - Application proxy - application layer
- No clear-cut “best” practice.
- Depends on security requirements

Firewall deployment/configuration

- Firewall efforts can be done in multiple ways
 - Bastion hosts; Host-based firewalls; Personal firewalls
- Firewalking vulnerability
- IPTables to establish access rules

Network Security - Week 7

João Soares

DCC/FCUP

2023