
Introduction to Firewall and Firewall Configuration

Course: CS6315 Mobile Systems Security
Lecturer: Simon Foley

William Fitzgerald

Cork Constraint Computation Centre,
Department of Computer Science,
University College Cork,
Ireland.

Web: www.williamfitzgerald.net

Email: wfitzgerald@4c.ucc.ie

February, 2010

OSI Network Layer Stack

- ▷ Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

OSI model	TCP/IP model	Common Packet Attributes Filtered
Application	Application	Application Protocol Pattern Matching
Presentation		
Session	TCP/UDP	TCP & UDP protocol, TCP & UDP ports, TCP Flags
Transport		
Network	IP, ICMP	source & destination IP, ICMP Type
Data Link	Data link	source MAC address
Physical	Physical	

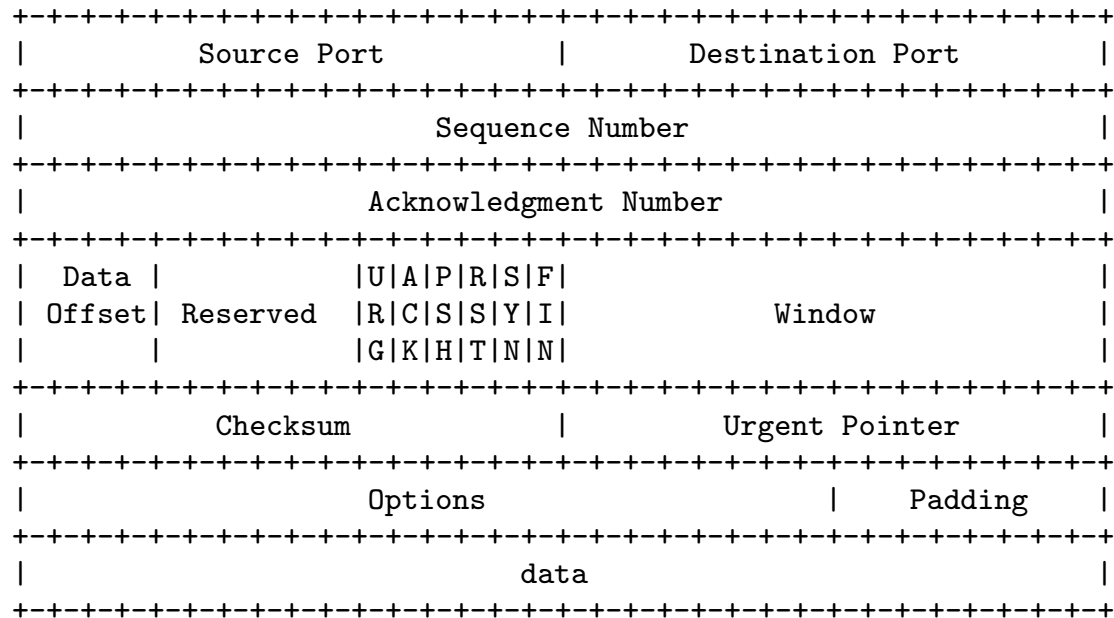
RFC791: IPv4 Protocol Header

- ▷ Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

```
+++++
|Version|  IHL  |Type of Service|          Total Length          |
+++++
|          Identification          |Flags|          Fragment Offset          |
+++++
| Time to Live |   Protocol   |          Header Checksum          |
+++++
|          Source Address          |
+++++
|          Destination Address          |
+++++
|          Options          |          Padding          |
+++++
```

RFC793: TCP Protocol Header

- ▷ Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary



RFC793: TCP Handshaking

- ▷ Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Connection setup (3-way Handshake):

1. Initiator sends SYN
2. Recipient sends SYN/ACK
3. Initiator sends ACK

Connection Tear-down (4-way Handshake):

1. Initiator sends FIN/ACK
2. Recipient sends ACK
3. Recipient sends FIN/ACK
4. Initiator sends ACK

Note: A TCP connection is full duplex (that is, data can flow independently in each direction), therefore each direction must be terminated independently.

Firewall Definition

- Prerequisite
 - ▷ The Firewall
 - Firewall Configuration
 - Packet-Filter Firewall
 - Stateful Firewall
 - Application-Layer Firewall
 - Proxy
 - Summary

One of the earliest definitions of a firewall [Cheswick] is *“a collection of components placed between two networks that collectively have the following properties:*

- 1. All traffic from inside to outside, and vice-versa, must pass through the firewall.*
- 2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.*
- 3. The firewall itself is immune to penetration.”*

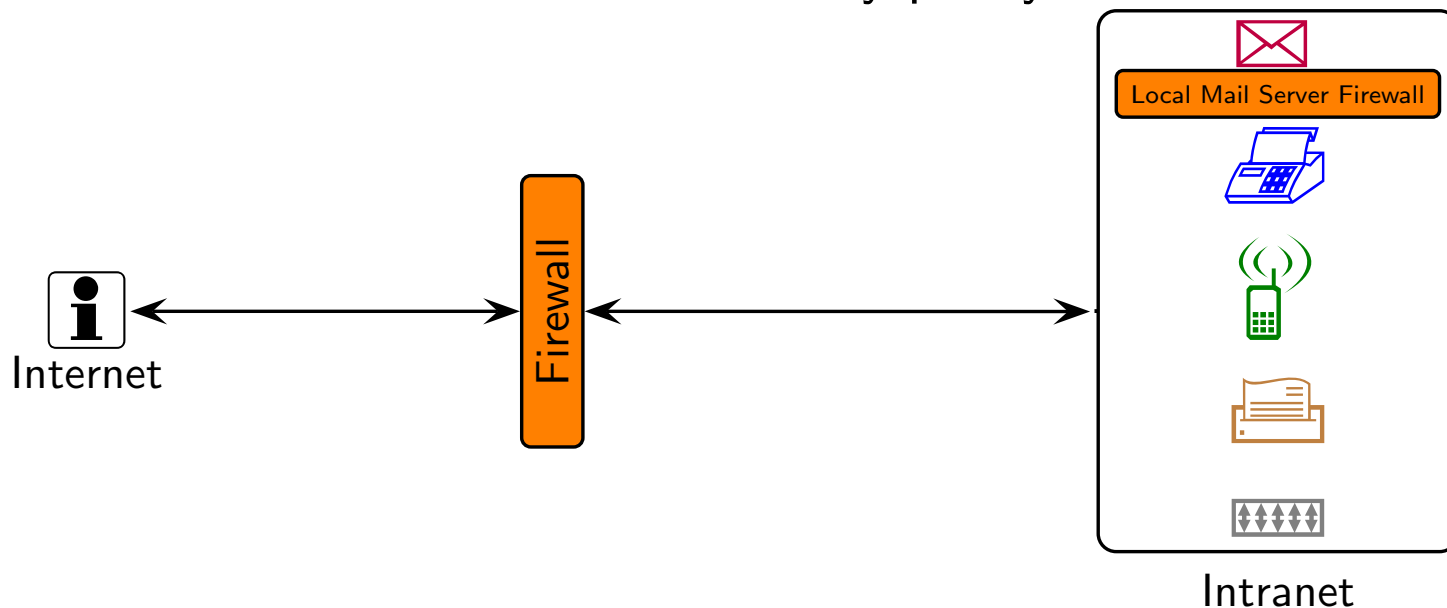
[Cheswick] William R. Cheswick and Steven M. Bellovin: *Firewall and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, April 1994.

Firewall Definition

- Prerequisite
- ▷ The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Refining properties *1* and *2* in the definition provided by [Cheswick], we provide the following definition:

A *firewall* is a security system that controls traffic flow to and from network resources which are hosted by a local firewall system or hosted by a network of systems behind a network-wide firewall in accordance with a security policy.



Definition: Security Policy

Prerequisite
The Firewall
 Firewall
 ▷ Configuration
 Packet-Filter
 Firewall
 Stateful Firewall
 Application-Layer
 Firewall
 Proxy
 Summary

A *Security Policy* is a high-level policy document that defines a “*set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources*” [RFC2828].

- Purpose of a *security policy* is to ensure that the high-level security requirements are upheld.
- However, it is not intended to prescribe specific firewall rules.
- The *security policy* is further refined into a *network security policy*.

Example: Security Policy

Prerequisite
The Firewall
 Firewall
 ▷ Configuration
 Packet-Filter
 Firewall
 Stateful Firewall
 Application-Layer
 Firewall
 Proxy
 Summary

Example fragment of a Payment Card Industry Data Security Standard (PCI-DSS) *security policy* recommendation.

Objective: Build and Maintain a Secure Network			
Requirement ID		Requirement	
req-1		Install and maintain a firewall configuration to protect cardholder data.	
	req-1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	
		req-1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.

Definition: Network Security Policy

Prerequisite
The Firewall
 Firewall
 ▷ Configuration
 Packet-Filter
 Firewall
 Stateful Firewall
 Application-Layer
 Firewall
 Proxy
Summary

A Network Security Policy describes an organisation's network security concerns when providing access internally and externally to its network resources.

Example: Network Security Policy

Prerequisite
The Firewall
Firewall
▷ Configuration
Packet-Filter
Firewall
Stateful Firewall
Application-Layer
Firewall
Proxy
Summary

Example *network security policy* derived from the *security policy*:

Policy ID	Description
nsp-1	Permit Internet access to Web server on ports HTTP and HTTPS.
nsp-2	Permit business partners access to Extranet partner server over port VPN.
nsp-3	Permit Intranet users access to external Web servers on ports HTTP and HTTPS.
nsp-4	Permit Intranet users access to file server on port FTP only.
nsp-5	Permit firewall administration from Intranet on port SSH by administrator team.
nsp-6	Deny Skype communication.
nsp-7	Deny known Remote Access Trojans making outward connections.
nsp-8	Log and Deny all other Internet to Intranet access.

Definition: Firewall Configuration

Prerequisite
The Firewall
 Firewall
 ▷ Configuration
 Packet-Filter
 Firewall
 Stateful Firewall
 Application-Layer
 Firewall
 Proxy
 Summary

A *firewall configuration* implements a network security policy and is defined by a sequence of firewall rules against which all packets traversing the firewall are filtered.

Example: Firewall Configuration

- Prerequisite
- The Firewall
 - Firewall
 - ▷ Configuration
 - Packet-Filter
 - Firewall
 - Stateful Firewall
 - Application-Layer
 - Firewall
 - Proxy
 - Summary

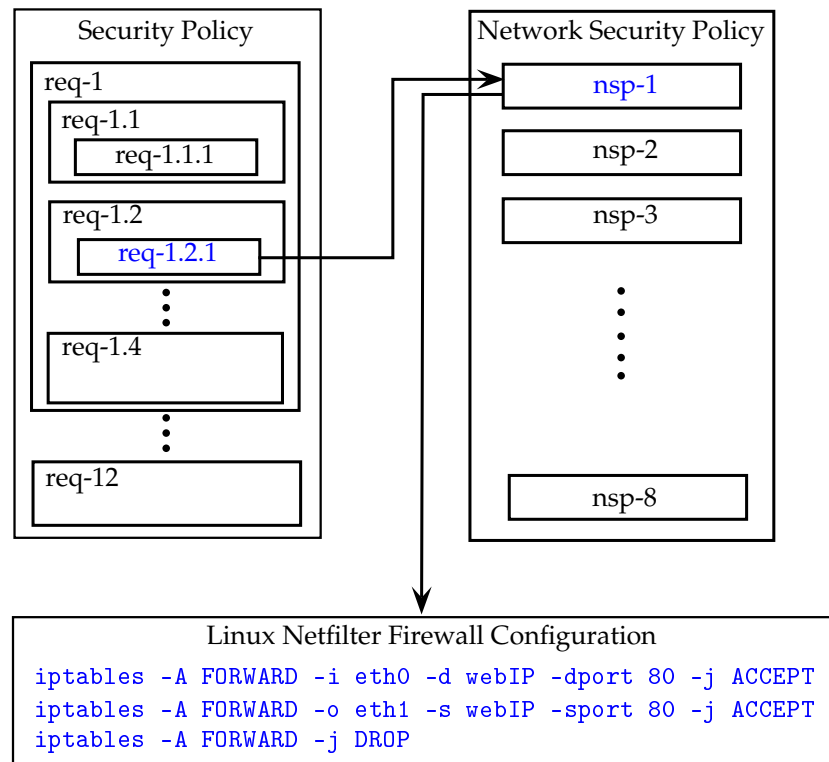
Linux Netfilter Firewall Configuration

```
iptables -A FORWARD -i eth0 -d webIP -dport 80 -j ACCEPT
iptables -A FORWARD -o eth1 -s webIP -sport 80 -j ACCEPT
iptables -A FORWARD -j DROP
```

Example: Firewall Configuration

- Prerequisite
- The Firewall
- Firewall
 - ▷ Configuration
- Packet-Filter Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

A *firewall configuration* derived from the *network security policy*.



Firewall Rules

- Prerequisite
- The Firewall
 - Firewall
 - ▷ Configuration
 - Packet-Filter Firewall
 - Stateful Firewall
 - Application-Layer Firewall
 - Proxy
 - Summary

Each firewall rule takes the form of a series of conditions on packet fields that must be met in order for that rule to be applicable, with a consequent action for the matching packet.

Column Name	Description	OSI Layer Filtered
<i>Index</i>	Rule position in firewall configuration.	-
<i>Dir</i>	Packet direction: inbound or outbound.	-
<i>Iface</i>	Network interface on which a packet was received.	Physical
<i>Mac</i>	Source MAC address.	Data Link
<i>Src IP</i>	Source IP address.	Network
<i>Dst IP</i>	Destination IP address.	Network
<i>ICMP-Type</i>	ICMP Type.	Network
<i>ICMP-Code</i>	ICMP Code.	Network
<i>Proto</i>	Protocol.	Transport
<i>Src Port</i>	Source port.	Transport
<i>Dst Port</i>	Destination port.	Transport
<i>Flag</i>	TCP Flags	Transport
<i>L7-filter</i>	Packet payload pattern match. Specific to Netfilter	Application
<i>Action</i>	Action to perform on the packet: allow, deny and log	-

Index	Dir	Iface	Proto	Src IP	Dst IP	Src Port	Dst Port	L7-filter	Action
1	out	eth1	udp	192.168.1.*	*.*.*.*	33033	*	skypeout	Deny

Default Firewall Configuration Policy

- Prerequisite
- The Firewall
- Firewall
 - ▷ Configuration
- Packet-Filter Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Rules are tested in the order in which they appear in the table.

Once a packet has been successfully matched against a rule, no further rule tests are carried out for that packet.

If the packet fails to be matched against any of the rules, then the firewall imposes a default policy/rule which can be either:

- Default Deny: everything is denied except that which is explicitly permitted.
- Default Allow: everything is permitted except that which is explicitly denied.

Packet-Filter Firewall

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

A *packet-filter* is a firewall that makes decisions about whether or not to permit a packet based only on information found at the data-link, network or transport layers.

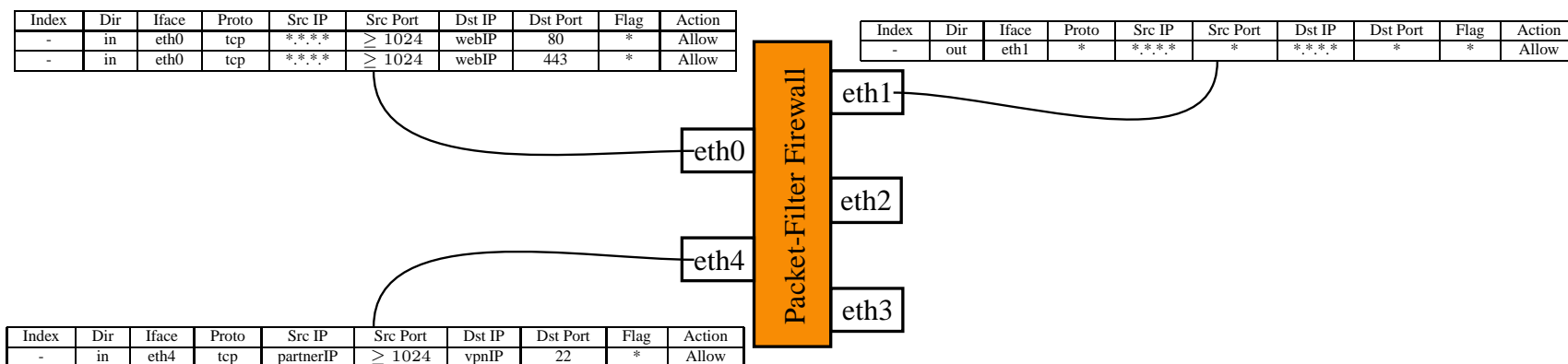
OSI model	TCP/IP model	Common Packet Attributes Filtered
Application	Application	Application Protocol Pattern Matching
Presentation		
Session	TCP/UDP	TCP & UDP protocol, TCP & UDP ports, TCP Flags
Transport		
Network	IP, ICMP	source & destination IP, ICMP Type
Data Link	Data link	source MAC address
Physical	Physical	

Packet-Filter Firewall

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter Firewall
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Modern packet-filters have the ability to specify firewall rules based on which physical network interface a packet is received or is destined to be transmitted from.

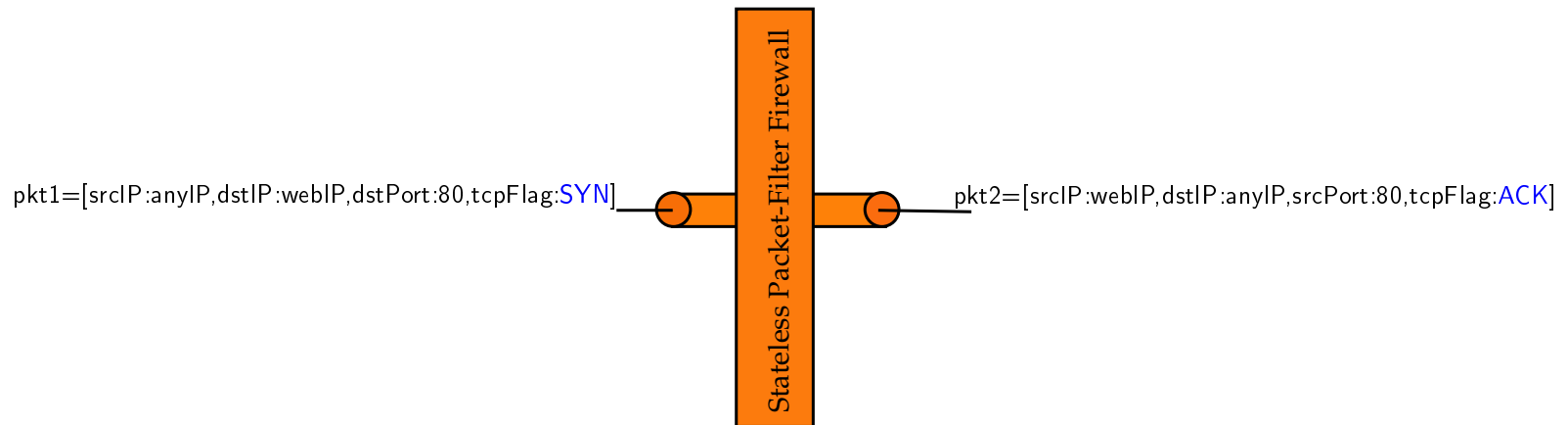
Firewalls typically have multiple inbound and outbound network interfaces.



Packet-Filter Firewall

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Packet-filters are stateless, meaning that each packet is examined in isolation of previously examined packets.



Packet-Filter does not take advantage of the semantic relationship between these two packets.

Example: Packet-Filter Configuration

Prerequisite
The Firewall
Firewall
Configuration
 Packet-Filter
 ▷ Firewall
Stateful Firewall
Application-Layer
Firewall
Proxy
Summary

Consider the following network security policy:

Policy ID	Description
nsp-1	Permit Internet access to Web server on ports HTTP and HTTPS.
nsp-2	Permit business partners access to Intranet partner server over port VPN.
nsp-3	Permit Intranet users access to external Web servers on ports HTTP and HTTPS.
nsp-4	Permit Intranet users access to file server on port FTP only.
nsp-5	Permit firewall administration from Intranet on port SSH by administrator team.
nsp-6	Deny Skype communication.
nsp-7	Deny known Remote Access Trojans making outward connections.
nsp-8	Log and Deny all other Internet to Intranet access.

Example: Packet-Filter Configuration

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Consider the following network security policy:

Policy ID	Description
nsp-1	Permit Internet access to Web server on ports HTTP and HTTPS.
nsp-2	Permit business partners access to Intranet partner server over port VPN.
nsp-3	Permit Intranet users access to external Web servers on ports HTTP and HTTPS.
nsp-4	Permit Intranet users access to file server on port FTP only.
nsp-5	Permit firewall administration from Intranet on port SSH by administrator team.
nsp-6	Deny Skype communication.
nsp-7	Deny known Remote Access Trojans making outward connections.
nsp-8	Log and Deny all other Internet to Intranet access.

The following firewall rule-set is an example implementation:

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	*	Allow
2	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	443	*	Allow
3	in	eth0	tcp	partnerIP	≥ 1024	vpnIP	22	*	Allow
4	in	eth0	tcp	*.*.*.*	80	lanIP	≥ 1024	ack	Allow
5	in	eth1	tcp	lanIP	≥ 1024	ftpIP	21	*	Allow
6	in	eth1	tcp	adminIP	≥ 1024	fwIP	22	*	Allow
7	in	eth0	udp	*.*.*.*	*	lanIP	23399	*	Deny
8	in	eth0	*	*.*.*.*	*	*.*.*.*	*	*	Log
9	in	eth0	*	*.*.*.*	*	*.*.*.*	*	*	Deny
10	out	eth0	tcp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny
11	out	eth0	udp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny
12	out	eth1	*	*.*.*.*	*	*.*.*.*	*	*	Allow

Example: Packet-Filter Configuration

Prerequisite
 The Firewall
 Firewall
 Configuration
 Packet-Filter
 ▷ Firewall
 Stateful Firewall
 Application-Layer
 Firewall
 Proxy
 Summary

Policy ID	Description
nsp-1	Permit Internet access to Web server on ports HTTP and HTTPS only.
nsp-2	Permit business partners access to Intranet partner server over port VPN.
nsp-3	Permit Intranet users access to external Web servers on ports HTTP and HTTPS.
nsp-4	Permit Intranet users access to file server on port FTP only.
nsp-5	Permit firewall administration from Intranet on port SSH by administrator team.
nsp-6	Deny Skype communication.
nsp-7	Deny known Remote Access Trojans making outward connections.
nsp-8	Log and Deny all other Internet to Intranet access.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	*	Allow
2	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	443	*	Allow
3	in	eth0	tcp	partnerIP	≥ 1024	vpnIP	22	*	Allow
4	in	eth0	tcp	*.*.*.*	80	lanIP	≥ 1024	ack	Allow
5	in	eth1	tcp	lanIP	≥ 1024	ftplIP	21	*	Allow
6	in	eth1	tcp	adminIP	≥ 1024	fwIP	22	*	Allow
7	in	eth0	udp	*.*.*.*	*	lanIP	23399	*	Deny
8	in	eth0	*	*.*.*.*	*	*.*.*.*	*	*	Log
9	in	eth0	*	*.*.*.*	*	*.*.*.*	*	*	Deny
10	out	eth0	tcp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny
11	out	eth0	udp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny
12	out	eth1	*	*.*.*.*	*	*.*.*.*	*	*	Allow

Example: Packet-Filter Configuration

Prerequisite
 The Firewall
 Firewall
 Configuration
 Packet-Filter
 ▷ Firewall
 Stateful Firewall
 Application-Layer
 Firewall
 Proxy
 Summary

Policy ID	Description
nsp-1	Permit Internet access to Web server on ports HTTP and HTTPS only.
nsp-2	Permit business partners access to Intranet partner server over port VPN.
nsp-3	Permit Intranet users access to external Web servers on ports HTTP and HTTPS.
nsp-4	Permit Intranet users access to file server on port FTP only.
nsp-5	Permit firewall administration from Intranet on port SSH by administrator team.
nsp-6	Deny Skype communication.
nsp-7	Deny known Remote Access Trojans making outward connections.
nsp-8	Log and Deny all other Internet to Intranet access.

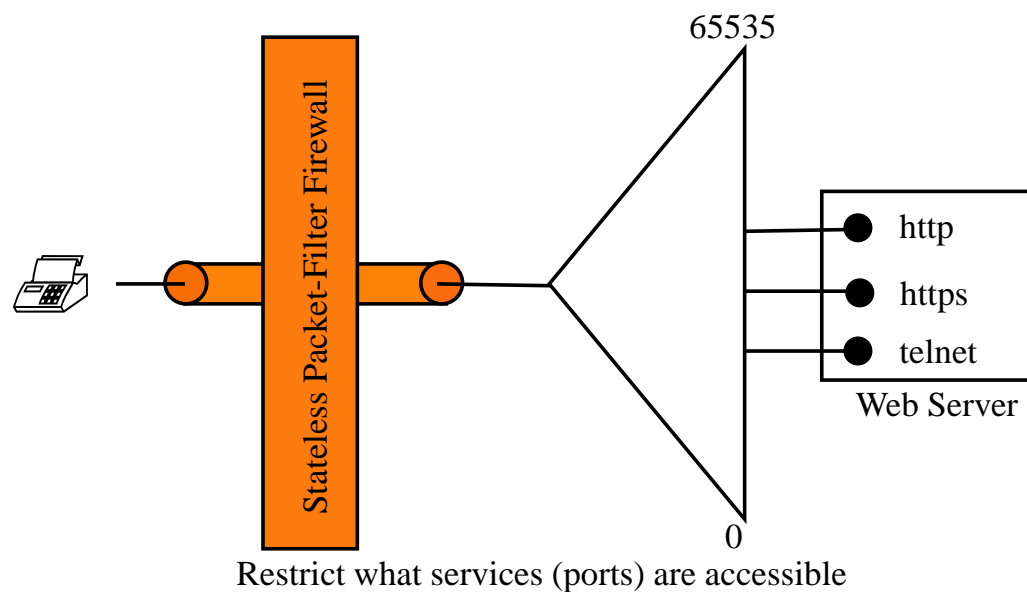
Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	*	Allow
2	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	443	*	Allow
3	in	eth0	tcp	partnerIP	≥ 1024	vpnIP	22	*	Allow
4	in	eth0	tcp	*.*.*.*	80	lanIP	≥ 1024	ack	Allow
5	in	eth1	tcp	lanIP	≥ 1024	ftplIP	21	*	Allow
6	in	eth1	tcp	adminIP	≥ 1024	fwIP	22	*	Allow
7	in	eth0	udp	*.*.*.*	*	lanIP	23399	*	Deny
8	in	eth0	*	*.*.*.*	*	*.*.*.*	*	*	Log
9	in	eth0	*	*.*.*.*	*	*.*.*.*	*	*	Deny
10	out	eth0	tcp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny
11	out	eth0	udp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny
12	out	eth1	*	*.*.*.*	*	*.*.*.*	*	*	Allow

Example: Port-Based Attack Reduction

Prerequisite
The Firewall
Firewall
Configuration
 Packet-Filter
 ▷ Firewall
Stateful Firewall
Application-Layer
Firewall
Proxy
Summary

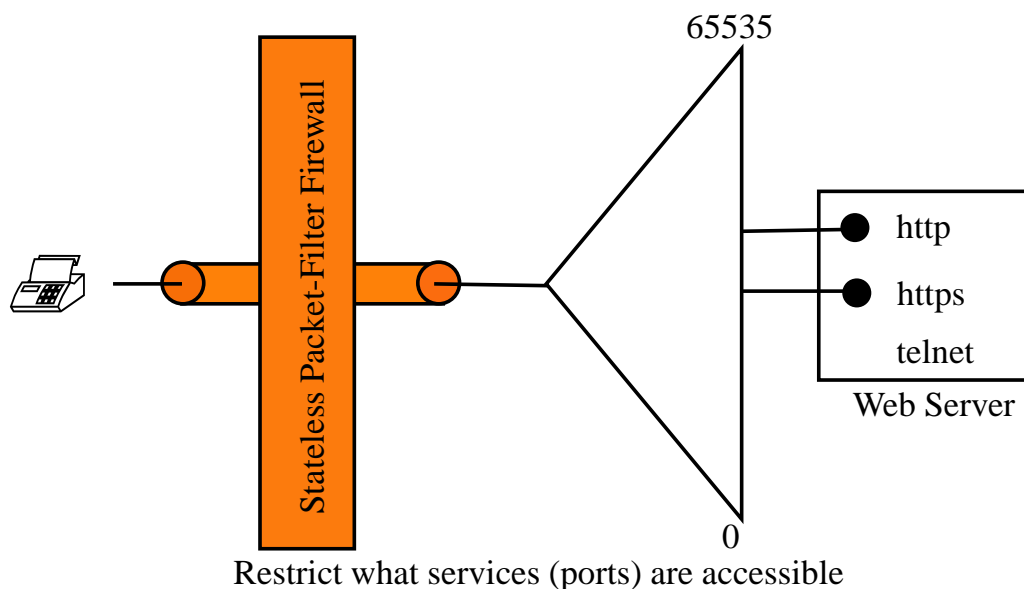
An attack surface is the number of Internet accessible network resources (in terms of IP addresses and ports) that are available for a potential attacker to exploit.

- A Web server may have a number of open ports, for example telnet, that are not intended for Internet access.



Example: Port-Based Attack Reduction

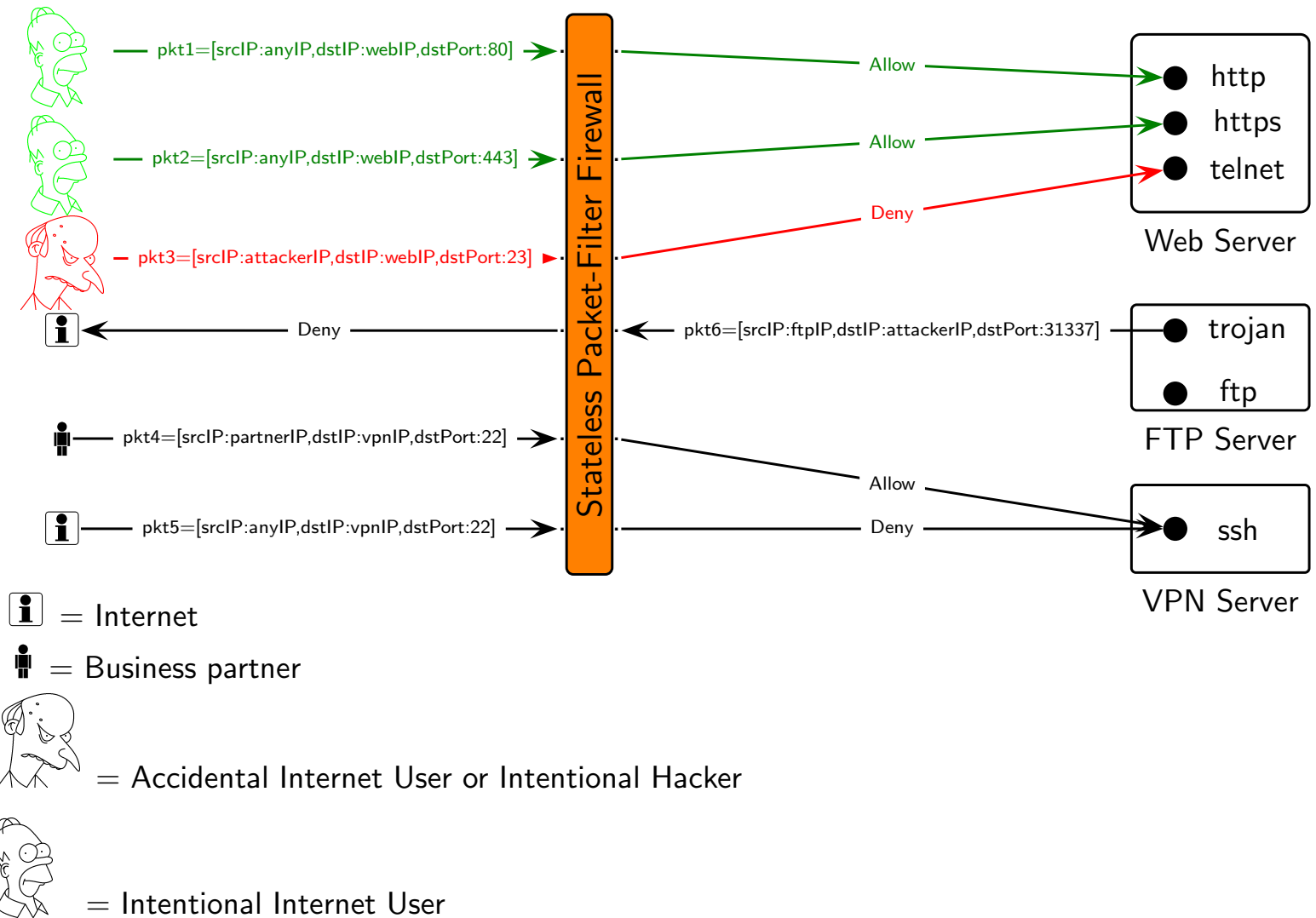
- Configuring a packet-filter firewall to permit intended Web server traffic destined for ports 80 and 443, will reduce the attack surface from a possible 65535 ports to just 2 ports.



Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	*	Allow
2	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	443	*	Allow

Example: Port-Based Attack Reduction

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary



Example: Client Access Restriction

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Recall the network security goal:

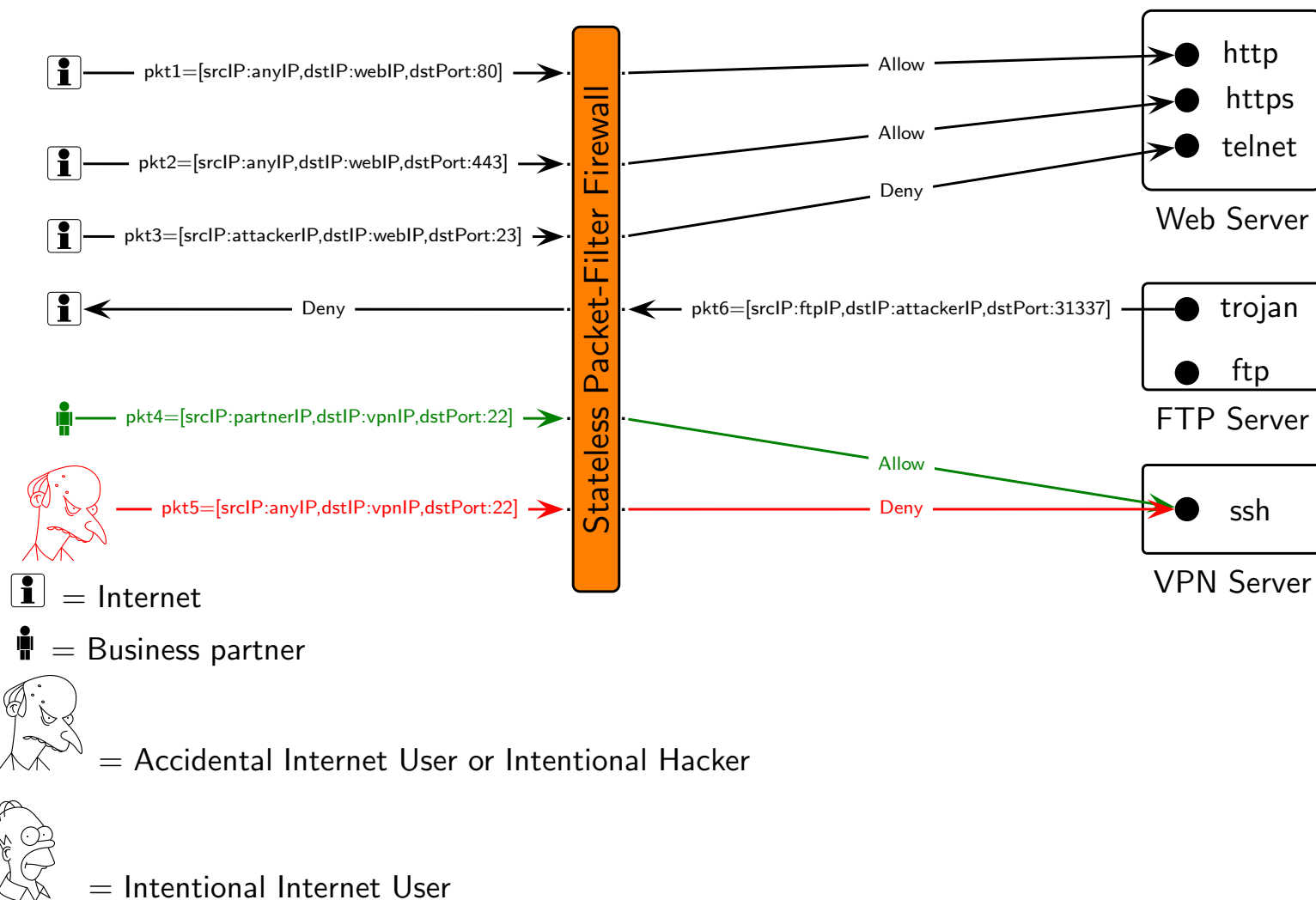
Policy ID	Description
nsp-2	Permit business partners access to Intranet partner server over port VPN only.

Configured with the following firewall rule:

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
3	in	eth0	tcp	partnerIP	≥ 1024	vpnIP	22	*	Allow

Example: Client Access Restriction

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary



Example: Malware Control

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Control of Malware can be applied to both inbound traffic (for example, IRC channels which are often used to control zombie networks) and to outbound traffic, normally considered trusted.

- Well known Remote Access Trojans (*RAT's*) such as Back-Orifice, can be blocked in terms of protocol and ports from indiscriminately making outbound connections to an external command control.

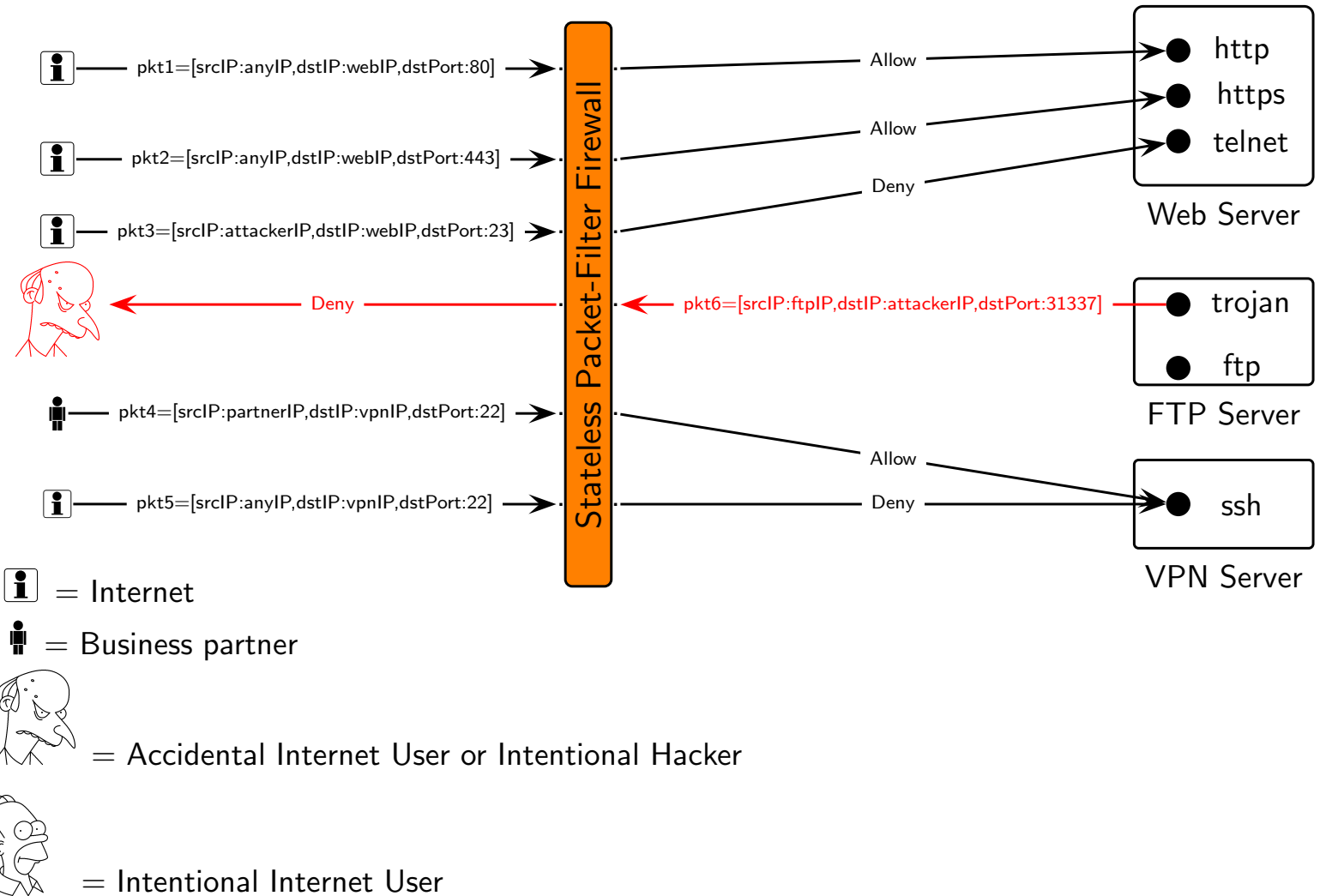
Recall rules 10 & 11:

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
10	out	eth1	tcp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny
11	out	eth1	udp	lanIP	≥ 1024	*.*.*.*	31337	*	Deny

Remember, traffic is bidirectional. Mitigating the outgoing traffic will prevent an established communication channel being constructed.

Example: Malware Control

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary



Example: Malware Control

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
 - Stateful Firewall
 - Application-Layer Firewall
 - Proxy
 - Summary

It is considered best-practice to avoid once-off firefighting rules and to adopt a default deny rule on outbound traffic.

As a consequence, one must explicitly define a set of outbound rules to complete the bi-directional communication requirements of previously permitted inbound traffic.

- Rules Rule 10, Rule 11 and Rule 12 are replaced with rules that explicitly state what (trusted) traffic is permitted outbound.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
-	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	*	Allow
-	out	eth1	tcp	webIP	443	*.*.*.*	≥ 1024	*	Allow
-	out	eth1	tcp	vpnIP	22	partnerIP	≥ 1024	*	Allow
-	out	eth1	tcp	lanIP	≥ 1024	*.*.*.*	80	*	Allow
-	out	eth1	tcp	ftplIP	21	lanIP	≥ 1024	*	Allow
-	out	eth1	tcp	fwIP	22	adminIP	≥ 1024	*	Allow
-	out	eth1	*	*.*.*.*	*	*.*.*.*	*	*	Deny

Example: Direction-Oriented Filtering

- Prerequisite
- The Firewall
- Firewall Configuration
 - Packet-Filter
 - ▷ Firewall
- Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Packets claiming to be sourced from the internal network inbound but arriving on an external network interface are considered to be spoofed and such packets should not be permitted by the firewall [RFC3330, RFC1918].

The attacker forges packets to reflect the source IP addresses that are associated with internal systems so that a firewall (not configured with direction-oriented filter controls) interprets these packets as having originated within the internal network.

- No way to authenticate IPv4 packets.
- This type of attack typically forms part of a Denial of Service Attack (DoS) on an internal network.

Stateful Firewall

- Prerequisite
- The Firewall
- Firewall
- Configuration
- Packet-Filter
- Firewall
- ▷ Stateful Firewall
- Application-Layer
- Firewall
- Proxy
- Summary

A *stateful firewall* filters like the packet-filter,

OSI model	TCP/IP model	Common Packet Attributes Filtered
Application	Application	Application Protocol Pattern Matching
Presentation		
Session	TCPTCP/UDP	TCP & UDP protocol, TCP & UDP ports, TCP Flags
Transport		
Network	IP, ICMP	source & destination IP, ICMP Type
Data Link	Data link	source MAC address
Physical	Physical	

Stateful Firewall

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

A *stateful firewall* filters like the packet-filter, but also tracks the state of previous network packets.

- State information might include protocol, IP addresses, ports, TCP flags, sequence and acknowledge numbers.
- State information is recorded when a TCP connection or UDP exchange is initiated.
- Subsequent packets are examined not only based on stateless rule but also on the context of the ongoing connection.

State Table Entry	Description
Example TCP Packet State Information at Network and Transport Layer	
<i>Protocol</i>	Transport layer protocol name and number.
<i>Time</i>	Time remaining before state information is removed.
<i>TCP State</i>	State of TCP connection (TCP only).
<i>IP Addresses</i>	Source and destination IP addresses.
<i>Ports</i>	Source and destination ports.
<i>Expected</i>	Expected source and destination IP addresses and ports reversed.
<i>Connection State</i>	Connection-tracking state of the connection.
tcp 6 90 ESTABLISHED src=192.168.1.10 dst=192.168.2.3 sport=1060 dport=22 src=192.168.2.3 dst=192.168.1.10 sport=22 dport=1060 ASSURED	

Stateful Firewall

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

While UDP [rfc768] and ICMP [rfc792] are stateless protocols, their connections can be tracked, albeit in a limited fashion.

- For example, a UDP header does not contain flags or sequence numbers and, therefore, the only state information recorded is the protocol, IP addresses and ports.

Some stateful firewalls, for example Netfilter, can examine limited application layer data for some well known protocols like FTP in order to track related connections accross ports.

Example: Simplifying Stateless Complexity

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Stateless Packet-filters can examine packet headers for TCP flags settings.

In practice, TCP flag filtering tends to focus only on SYN and ACK flags.

- Consider permitting HTTP traffic to a Web server while filtering based on TCP flags.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	syn	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	syn, ack	Allow

However, in reality its much more complicated than that ...

Example: Simplifying Stateless Complexity

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Need to consider specifying additional rules involved in completing the TCP 3-way-handshake.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	syn	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	syn, ack	Allow
3	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow

Example: Simplifying Stateless Complexity

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Need to consider additional rules for ongoing bi-directional communications.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	syn	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	syn, ack	Allow
3	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
4	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
5	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	ack	Allow

Example: Simplifying Stateless Complexity

Prerequisite
The Firewall
Firewall
Configuration
Packet-Filter
Firewall
▷ Stateful Firewall
Application-Layer
Firewall
Proxy
Summary

Need to consider additional rules to permit either side of the connection to terminate.

- Client can initiate the closure (Rule 6).

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	syn	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	syn, ack	Allow
3	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
4	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
5	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	ack	Allow
6	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin,ack	Allow
7	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin,ack	Allow
8	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin,ack	Allow
9	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin	Allow

Previously defined Rules 5 and 6 are also activated.

Example: Simplifying Stateless Complexity

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Need to consider additional rules to permit either side of the connection to terminate.

- The Web server itself can initiate the closure (Rule 8).

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	syn	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	syn, ack	Allow
3	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
4	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
5	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	ack	Allow
6	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin,ack	Allow
7	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin	Allow
8	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin,ack	Allow
9	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin,ack	Allow

Example: Simplifying Stateless Complexity

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Need to consider additional rules to permit either side of the connection to terminate.

- Rules 10 and 11 allow either side to reset the connection.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	syn	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	syn, ack	Allow
3	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
4	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
5	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	ack	Allow
6	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin,ack	Allow
7	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin,ack	Allow
8	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin,ack,ack	Allow
9	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin,ack	Allow
10	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	rst	Allow
11	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	rst	Allow

Example: Simplifying Stateless Complexity

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

A stateful firewall manages this complexity seamlessly.

The following stateless rules can be replaced stateful rules.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	Flag	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	syn	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	syn, ack	Allow
3	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
4	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	ack	Allow
5	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	ack	Allow
6	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin,ack	Allow
7	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin	Allow
8	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	fin,ack	Allow
9	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	fin	Allow
10	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	rst	Allow
11	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	rst	Allow

Note there are some redundant rules in the above rule-set, a subject of the next lecture.

Example: Simplifying Stateless Complexity

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

A stateful firewall manages this complexity seamlessly.

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	State	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	New,Est	Allow
2	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	Est	Allow

Example: Stateful Port-based Attack Surface Reduction

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Recall, the packet-filter's example of port-based attack surface reduction where a the attack surface was reduced on the server-side.

Need to also consider client-side port-based attack surface reduction.

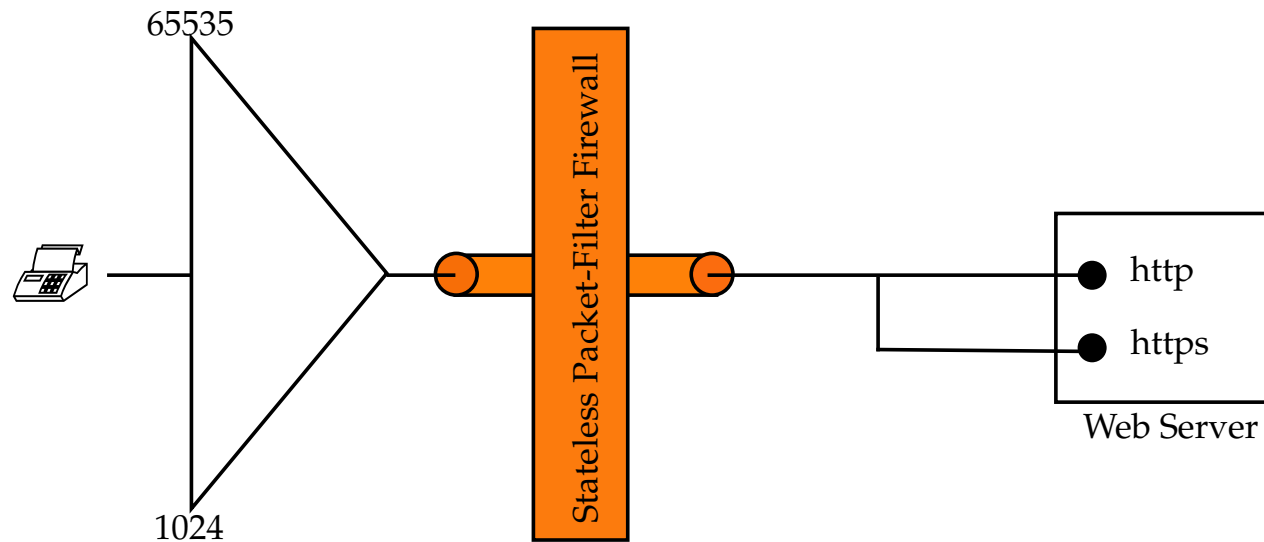
- Why?
- HTTP, for example, operates by creating a TCP connection in which the TCP port number for the Web server is 80 (privileged port defined by IANA) and the TCP port number for the client in the unprivileged port range (ports 1024 to 65535). Clients are dynamically assigned a port number from a range of 1024 to 65535.

Client side port assignment only exist during the lifetime of the TCP connection.

Example: Stateful Port-based Attack Surface Reduction

Prerequisite
The Firewall
Firewall
Configuration
Packet-Filter
Firewall
▷ Stateful Firewall
Application-Layer
Firewall
Proxy
Summary

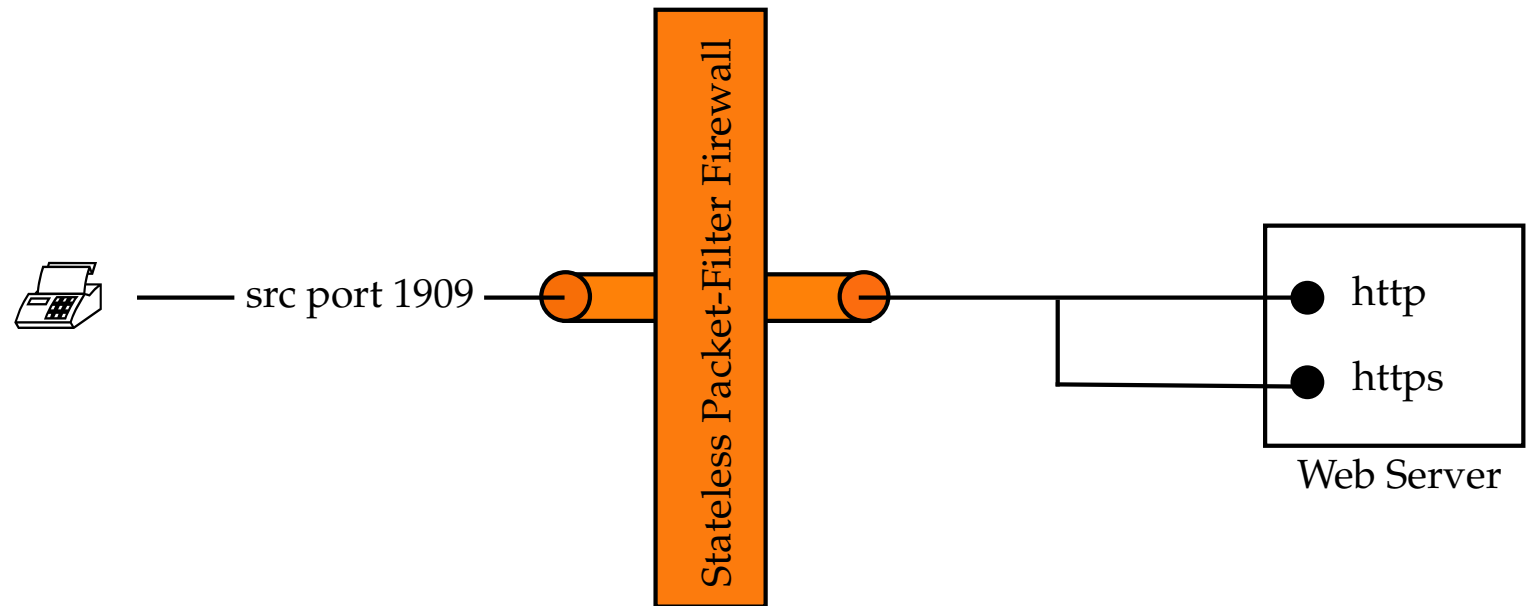
- The (stateless) packet-filter must statically open ports for the entire unprivileged port range.
- Totaling 64511 individual ports, resulting in unnecessary attack surface exposure.



Example: Stateful Port-based Attack Surface Reduction

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

A stateful firewall has state information that allows for dynamic port opening on demand, resulting in an attack surface applicable only to the actual client and server ports only.

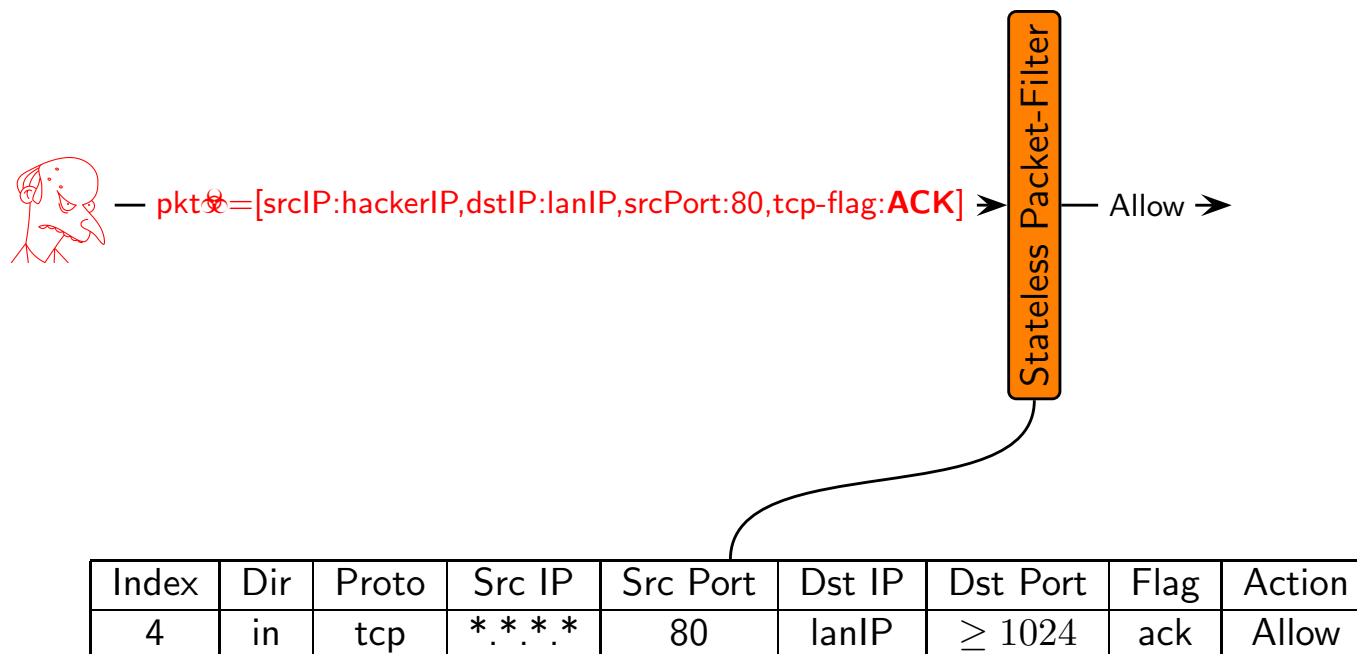


Example: Port Scan Reduction

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

In comparison to stateful firewalls, stateless packet-filters are more prone to port scanning attacks.

- The lack of authentication in typical network and transport layers means that TCP packet header fields can be forged to bypass stateless firewall rules.

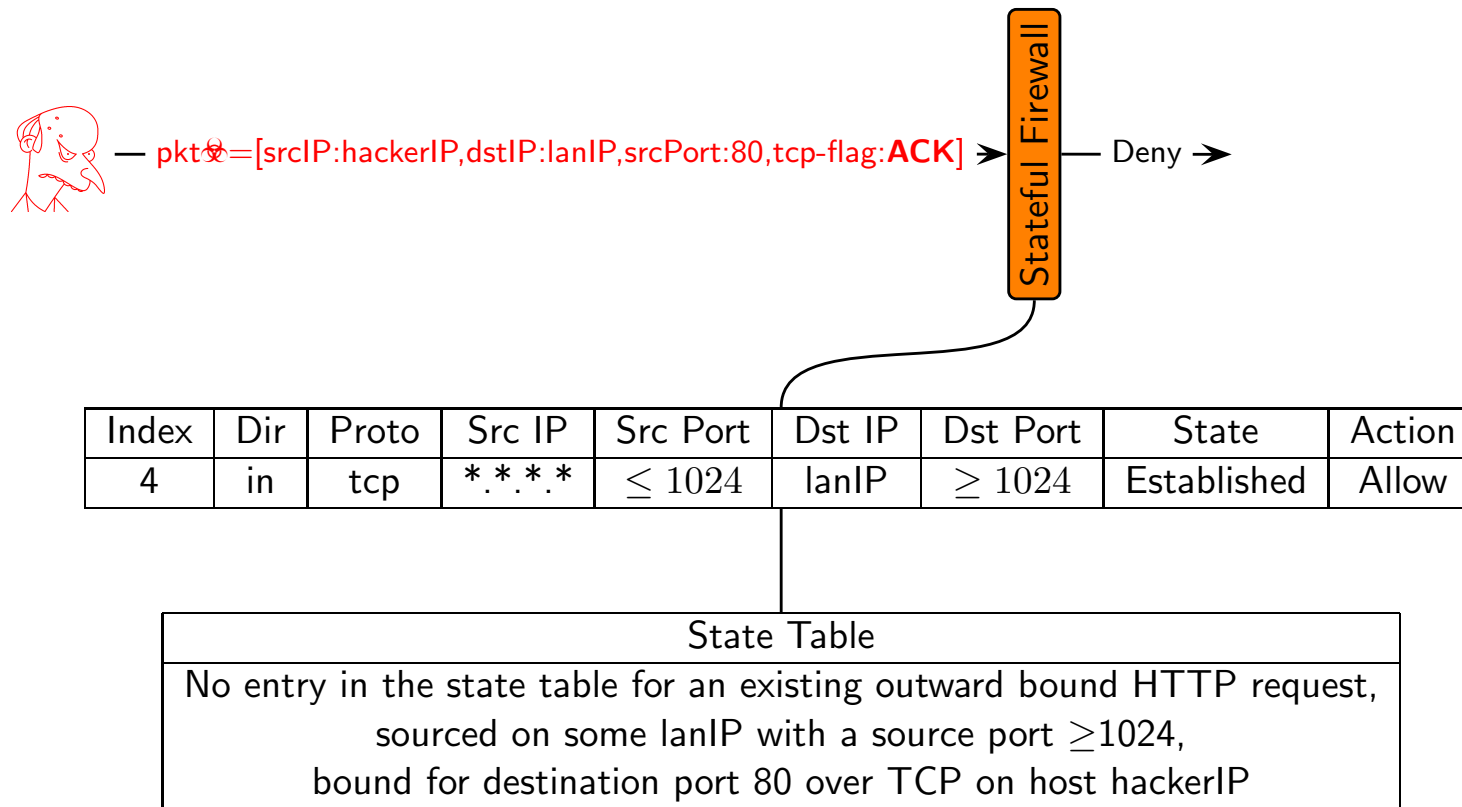


Example: Port Scan Reduction

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

Attacks of this nature against a stateful firewall will fail.

- A stateful firewall will consult both its rules and the current state table.



Example: Port Scan Reduction

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- ▷ Stateful Firewall
- Application-Layer Firewall
- Proxy
- Summary

While the construction of forged TCP packets that have the TCP ACK flag set will not open a connection to a system behind the firewall (stateless or stateful), it is a useful TCP ACK scan.

Using this type of network scan, it is possible to infer information about the rules within a firewall configuration.

- For example, if the firewall (or internal hosts) returns a TCP RST packet, the attacker can determine that an internal host exists; if not, it is assumed the port of the firewall is closed.

Application-Layer Firewall

- Prerequisite
- The Firewall
- Firewall
- Configuration
- Packet-Filter
- Firewall
- Stateful Firewall
 - Application-Layer
- ▷ Firewall
- Proxy
- Summary

An *application-layer firewall*, while it can examine both network and transport layer packet headers, can also examine a packets payload at the application layer.

It provides increased assurance of the validity of packet content and can make decisions based on. For example:

- Multimedia applications being tunneled over HTTP.
- Access requests to restricted web sites.
- Malicious content.
- Information disclosure, proprietary information filtered with keywords or regular expressions.

Example: Control Tunnel Bypass Attempts

Prerequisite
The Firewall
Firewall
Configuration
Packet-Filter
Firewall
Stateful Firewall
 Application-Layer
 ▷ Firewall
Proxy
Summary

From the point of view of the firewall, the term *tunneling* refers to the practice of encapsulating data from one protocol inside another protocol in order to evade the firewall.

- For example, a Skype client typically listens on TCP and UDP port 33033.
- However, should Skype fail to establish communication over that port, it has the ability to operate on ports required by HTTP (port 80) and HTTPS (port 443).
- Note, if Skype defaults to port 443 then a SSL scanner will be required to inspect the data.

Example: Control Tunnel Bypass Attempts

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
 - Application-Layer
 - ▷ Firewall
- Proxy
- Summary

The previously defined stateful firewall rule (rule 8) that is intended to mitigate the use of Skype is now ineffective.

Skype packets can traverse the stateful firewall unhindered exploiting the intended purpose of the HTTP rules (rules 4 & 13).

Index	Dir	Iface	Proto	Src IP	Src Port	Dst IP	Dst Port	State	Action
1	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	80	New,Est	Allow
2	in	eth0	tcp	*.*.*.*	≥ 1024	webIP	443	New,Est	Allow
3	in	eth0	tcp	partnerIP	≥ 1024	vpnIP	22	New,Est	Allow
4	in	eth0	tcp	*.*.*.*	80	lanIP	≥ 1024	Est	Allow
5	in	eth1	tcp	lanIP	≥ 1024	ftpIP	21	New	Allow
6	in	eth1	tcp	lanIP	≥ 1024	ftpIP	21	Est,Rel	Allow
7	in	eth1	tcp	adminIP	≥ 1024	fwIP	22	New,Est	Allow
8	in	eth0	udp	*.*.*.*	*	lanIP	33033	New	Deny
9	in	eth0	*	*.*.*.*	*	*.*.*.*	*	*	Log
10	out	eth1	tcp	webIP	80	*.*.*.*	≥ 1024	Est	Allow
11	out	eth1	tcp	webIP	443	*.*.*.*	≥ 1024	Est	Allow
12	out	eth1	tcp	vpnIP	22	partnerIP	≥ 1024	Est	Allow
13	out	eth1	tcp	lanIP	≥ 1024	*.*.*.*	80	New,Est	Allow
14	out	eth1	tcp	ftpIP	21	lanIP	≥ 1024	Est,Rel	Allow
15	out	eth1	tcp	fwIP	22	adminIP	≥ 1024	Est	Allow
16	*	*	*	*.*.*.*	*	*.*.*.*	*	*	Deny

Example: Control Tunnel Bypass Attempts

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
 - Application-Layer
- ▷ Firewall
- Proxy
- Summary

Having the ability to inspect the data at the application layer for Skype traffic is essential.

- An example of then many possible Skype signatures used in a *Skype-to-Skype* communication, is given as:

^..\x02.....

Example: Control Tunnel Bypass Attempts

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
 - Application-Layer Firewall
- Proxy
- Summary

Application-layer firewalls typically provide a pre-built database of known filter signatures.

- For example, **Skype-to-Skype** (UDP voice call between two or more skype clients) and **Skypeout** (UDP voice call from Skype client to POTS phone).

Index	Dir	Iface	Src IP	Dst IP	Proto	Src Port	Dst Port	L7-filter	Action
-	out	eth1	*.*.*.*	lanIP	udp	80	*	skypeout	Deny
-	out	eth1	*.*.*.*	lanIP	udp	80	*	skypotoskype	Deny

Example: Granular Malware Control

- Prerequisite
- The Firewall
- Firewall Configuration
- Packet-Filter Firewall
- Stateful Firewall
 - Application-Layer Firewall
- Proxy
- Summary

Application-layer firewalls can be used to filter some kinds of Malware.

For example, the Nimda worm made it possible for a Windows IIS Web server to be exploited by allowing a client with a specially formed request to break out of the Web server's document root and begin executing arbitrary programs on the Web server.

Index	Dir	Iface	Proto	Src IP	Dst IP	Src Port	Dst Port	L7-filter	Action
-	in	eth0	tcp	*.*.*.*	webSrvIP	*	80	nimda	Deny

Note, inspecting layer-7 for Malware payloads has a performance impact. More importantly, filter controls can often be subverted using packet fragmentation for example.

A *proxy* is a system that acts as an intermediary when forwarding packets on behalf of a client system requesting access to a network resource (server).

- A client system establishes a TCP/IP connection with the proxy system when it has a request that is to be forwarded to a server.
- The proxy in turn, contacts the remote server and establishes a secondary TCP/IP connection where the proxy then relays the ongoing communication between the client and server.
- To the client, it appears that there is a direct TCP/IP connection between itself and the server.
- Similarly, the server has no knowledge of the client and communicates with the proxy as if it were the client.

Proxy

- Prerequisite
- The Firewall
- Firewall
- Configuration
- Packet-Filter
- Firewall
- Stateful Firewall
- Application-Layer
- Firewall
- ▷ Proxy
- Summary

Each successful connection attempt actually results in the creation of two separate TCP connections, one between the client and the proxy system, and another between the proxy system and the destination server.

The proxy is transparent to the two end systems (client and server), and from their perspective they are directly connected to one another.

This provides an additional level of protection to the internal systems because external client systems can only communicate with the proxy and therefore internal IP addresses are not publicly known to the external Internet.

Application Proxy

Prerequisite
The Firewall
Firewall
Configuration
Packet-Filter
Firewall
Stateful Firewall
Application-Layer
Firewall
▷ Proxy
Summary

An *application proxy* is a proxy that has application-layer firewall capabilities.

Application proxies are systems that specialise in providing access control for a single application protocol, for example, HTTP, FTP or SMTP.

Circuit-level Proxy

Prerequisite
The Firewall
Firewall
Configuration
Packet-Filter
Firewall
Stateful Firewall
Application-Layer
Firewall
▷ Proxy
Summary

An *circuit-level proxy* is a proxy that has stateful firewall capabilities. Circuit-level proxies such as SOCKS are concerned only with IP addresses and port numbers.

Summary

Prerequisite
The Firewall
Firewall
Configuration
Packet-Filter
Firewall
Stateful Firewall
Application-Layer
Firewall
Proxy
▷ Summary

Provided an overview regarding the:

- Importance of firewalls in terms of network access control.
- Firewall classifications: advantages and disadvantages.
- Deep understanding of network protocols and firewall capabilities is required to configure firewall correctly.