Edinburgh Napier UNIVERSITY

CSN09101
Networked Services
Week 6 : Firewalls + Security

Module Leader: Dr Gordon Russell
Lecturers: G. Russell

Edinburgh Napier UNIVERSITY

This lecture

- Firewalls
- Stateful Firewall
- Discussions

Edinburgh Napier
UNIVERSITY

Firewalls

Edinburgh Napier UNIVERSITY

Firewalls

- Firewalls and the implementation of Management Policy plus proactive security methods
- Management Policy can include
  - Network Services allowed to run, and under what conditions
  - Client access to external resources
  - Quality of service
  - Security and maintaining availability

Edinburgh Napier UNIVERSITY

Corporate Firewalls

- Cisco PIX
- Cisco router ACLs
- Linux router iptables

- PIX syntax is strange, yet PIX solutions are popular!
- ACLs are weak for policy implementations
- iptables is powerful but uncommon.

Edinburgh Napier UNIVERSITY

Linux Firewalls

- Security issues which Linux firewalls can deal with:
  - Denial of service
  - Differences between external and internal users
  - Hiding local-only services
  - Traffic management
  - Virus and hacking protection
  - Implementing management policy
- Rules are needed in terms of packets arriving, leaving, and passing through.

Edinburgh Napier UNIVERSITY

iptables

- Since kernel 2.4, the standard interface for firewall configuration is iptables.
- It implements its rules using many “tables”
  - Filter – handles standard “firewall” things
  - NAT – rewriting of source/destination IPs
  - Mangle – specialised hacking of packet info
  - RAW – low-level modifications to packets
- Most firewalls only need to be involved with the filter table

Edinburgh Napier UNIVERSITY

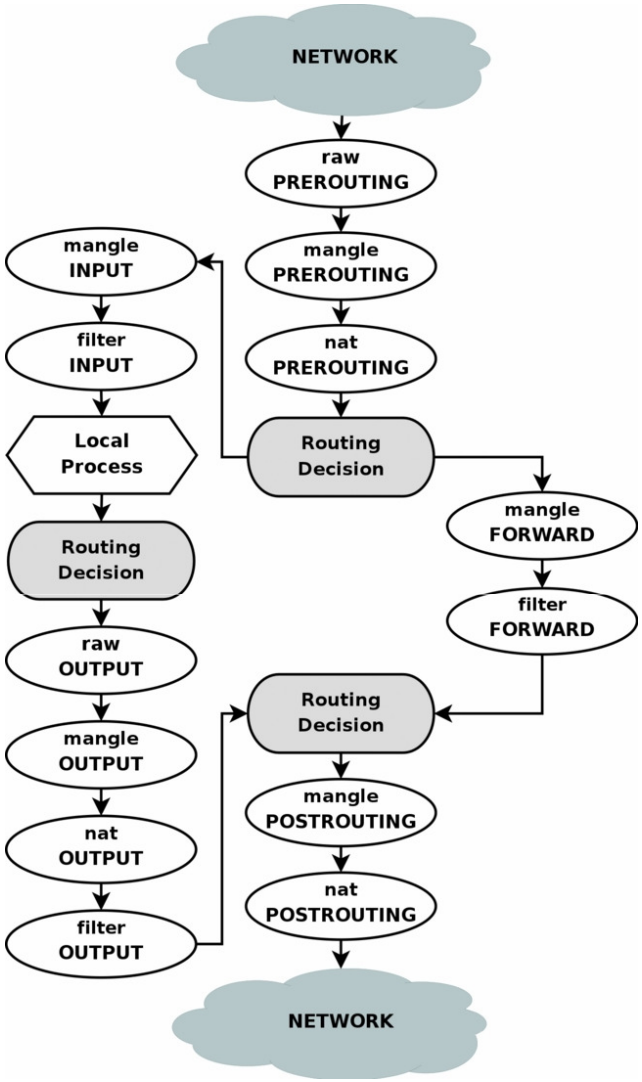
Chains

- Within each table is a number of chains.
- Think of each table as containing different types of rules you might want to use (like “filter” rules).
- Think of chains as defining WHEN a packet will have those rules applied to them.
- Chains are done in a particular order.
- Some packets only go to some chains and not others (depending on how the packet was made).

Edinburgh Napier UNIVERSITY

Chain Names

- Some chain names you might see are
  - PREROUTING
  - INPUT
  - OUTPUT
  - FORWARD
  - POSTROUTING

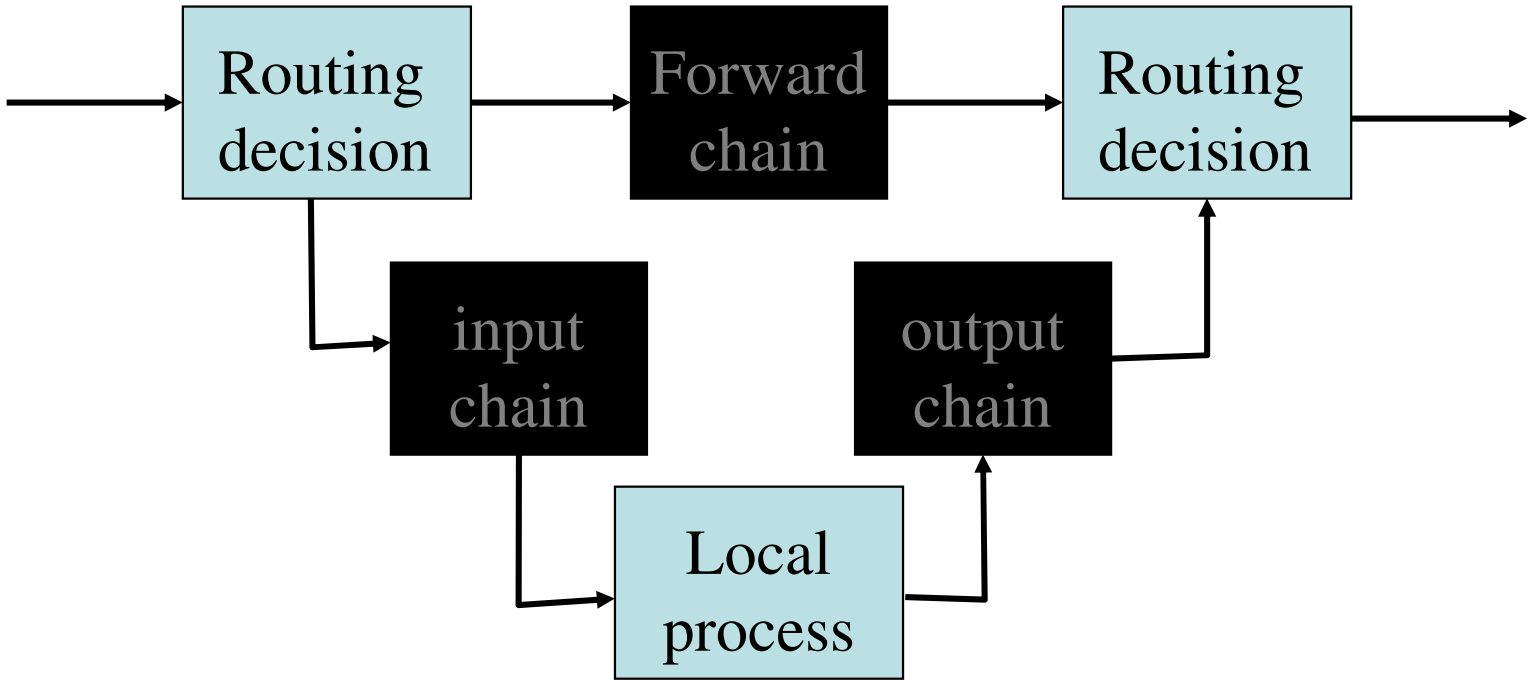


- Summary of the tables and chains a packet will traverse in iptables.

Source:
http://iptables-tutorial.frozentux.net/iptables-tutorial.html

Edinburgh Napier UNIVERSITY

FILTER TABLE CHAINS: INPUT, OUTPUT, FORWARD



Edinburgh Napier UNIVERSITY

FILTER TABLE

- In the filter table a packet will only go through 1 chain.
  - Packets created within the computer go through OUTPUT
  - Packets which need to be routed from one eth device to another eth device go through FORWARD.
  - Packets received by the computer for processing locally go through INPUT

Edinburgh Napier UNIVERSITY

A Chain

- Each chain is made up of 0 or more rules.
- A rule is a set of tests and an action.
- If the tests are all true then the action is performed.
- If a test is partially or completely false then the next rule is looked at instead.
- If all the rules are used up without an action taking place, then the chain POLICY is done instead (i.e. a default rule).

Edinburgh Napier UNIVERSITY

Tests

- Each rule has 0 or more tests.
- There are many tests possible, such as:
  - Is this TCP?
  - Is this from 10.0.0.5?
  - Is this from port 22?
  - Is this going to port 23?
  - Is this going to ip 50.0.0.1?
  - Am I receiving packets faster than 10 per second?
  - Which interface is it going out/in on?
- Remember you can combine these tests, e.g. TCP and from port 22.

Edinburgh Napier UNIVERSITY

Actions

- If all the tests are true then the action is carried out.
- Some actions are terminating, meaning that once they are done no more rules are looked at.
- A few actions are non-terminating. This is useful if you want to say print a message if the test is true, but continue on with the next rule anyway.

Edinburgh Napier UNIVERSITY

- Example actions are:
  - DROP – delete a packet immediately and terminate
  - ACCEPT – the packet is good and terminate
  - REJECT – delete the packet and terminate, but send back an ICMP message to the sender
  - LOG – print to syslog a message and move onto the next rule.

Edinburgh Napier UNIVERSITY

Some tests:

• Is this TCP ?	-p tcp
• Is this from 10.0.0.5?	-s 10.0.0.5
• Is this from port 22?	--sport 22
• Is this going to port 23?	--dport 23
• Is this going to ip 50.0.0.1?	-d 50.0.0.1
• Is this going out on eth0?	-o eth0
• Is this coming in from eth0?	-i eth0

Edinburgh Napier UNIVERSITY

Setting the policy

$ iptables –P INPUT ACCEPT

$ iptables –P OUTPUT ACCEPT

$ iptables –P FORWARD DROP

- This is a typical unsecured machine configuration. Typical machines only have 1 eth device, so don't forward. Otherwise, all packets are allowed.

Edinburgh Napier UNIVERSITY

Editing firewalls

- iptable does allow you to edit firewalls dynamically.
- However, this is very problematic and difficult.
- Instead, I recommend putting all your rules in a file and running that file to change the firewall.
- This allows you to use your favourite editor to write the firewall.
- At the start of the file, delete all current firewall rules in each table using “-F”.

Edinburgh Napier UNIVERSITY

```
$ touch firewall
$ chmod +x firewall
$ vi firewall
/sbin/iptables -F INPUT
/sbin/iptables -F OUTPUT
/sbin/iptables -F FORWARD

# Set the default policies for the chains
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -P FORWARD DROP
```

Edinburgh Napier UNIVERSITY

- To load these rules do

$ ./firewall

- However, don't do that yet. The default is DROP for INPUT. Without more rules you will be kicked out of the server never to return…
- This is bad if the server is 5 minutes walk away. But if it is 500miles away you are in trouble!
- This type of firewall is INGRESS ONLY. No rules for going out (OUTPUT/EGRESS). Kind of like the XP firewall…

Edinburgh Napier UNIVERSITY

Basic client machine

- Allow local machine to ssh and telnet out:

```
# Standard INGRESS FILTER RULES, then
iptables –t FILTER   –A INPUT –p tcp --sport 22 –j ACCEPT
iptables             –A INPUT –p tcp --sport 23 –j ACCEPT
```

sport or dport

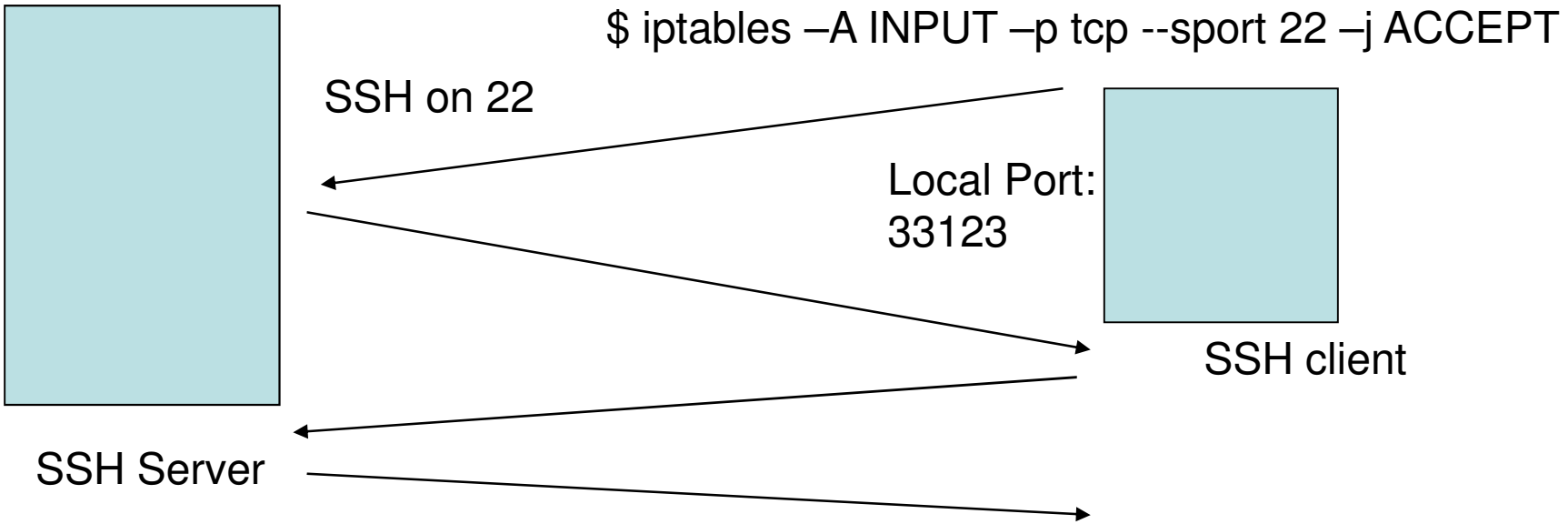
Edinburgh Napier UNIVERSITY

Server End

$ iptables –A INPUT –p tcp --dport 22 –j ACCEPT

Your End

$ iptables –A INPUT –p tcp --sport 22 –j ACCEPT



Edinburgh Napier UNIVERSITY

Basic client machine

- Allow local machine to ssh only to 10.0.0.1

```
# Standard INGRESS FILTER RULES, then
iptables –A INPUT –p tcp --sport ssh –s 10.0.0.1
                  –j ACCEPT
```

Edinburgh Napier UNIVERSITY

Add a rule to permit ping

- Anyone can ping this machine:

```
# Add to the end of the file
iptables –A INPUT –p icmp
                --icmp-type echo-request –j ACCEPT
```

Edinburgh Napier UNIVERSITY

Add a rule to permit safe ping

- Anyone can ping this machine, but I will only respond if the ping requests are slower than 2 per second:

```
# Add to the end of the file
iptables –A INPUT –p icmp
                --icmp-type echo-request
                -m limit --limit 2/second –j ACCEPT
```

- Would protect a system from a “ping of death”.

Edinburgh Napier UNIVERSITY

Monitor safe ping

- Anyone can ping this machine, but I will only respond if the ping requests are slower than 2 per second. Faster than that gets a logged message

```
# Add to the end of the file
iptables –A INPUT –p icmp
                --icmp-type echo-request
                -m limit --limit 2/second –j ACCEPT
iptables –A INPUT –p icmp
                --icmp-type echo-request –j LOG
```

Edinburgh Napier UNIVERSITY

Monitor Monitor safe ping

- Anyone can ping this machine, but I will only respond if the ping requests are slower than 2 per second. Faster than that gets a logged message, but don't log more than 10 per minute…

```
# Add to the end of the file
iptables –A INPUT –p icmp
                    --icmp-type echo-request
                    -m limit --limit 2/second –j ACCEPT
iptables –A INPUT –p icmp
                    --icmp-type echo-request
                    -m limit --limit 10/minute –j LOG
```

Edinburgh Napier UNIVERSITY

Learning firewalls

- To learn firewalls safely most people play with INPUT and OUTPUT policy ACCEPT.
- All the examples rely on the last rule effectively DROPPING all packets.
- If you want to try default ACCEPT, then you have to invert all the rules…

```
# Set the default policies for the chains
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P OUTPUT ACCEPT
/sbin/iptables -P FORWARD DROP
```

Edinburgh Napier UNIVERSITY

Basic client machine

- Allow local machine to ssh and telnet out, but using INPUT policy of ACCEPT:

```
/sbin/iptables -P INPUT ACCEPT
#
iptables –A INPUT –p tcp --sport 22 –j ACCEPT
iptables –A INPUT –p tcp --sport 23 –j ACCEPT
iptables –A INPUT –p tcp –j DROP
```

Edinburgh Napier UNIVERSITY

Basic client machine

- Allow local machine to ssh only to 10.0.0.1, but using INPUT policy of ACCEPT:

```
iptables -P INPUT ACCEPT
#
iptables –A INPUT –p tcp --sport ssh ! –s 10.0.0.1
                          –j DROP
# Get to the end and the default in ACCEPT
```

Edinburgh Napier UNIVERSITY

Monitor Monitor safe ping

- Anyone can ping this machine, but I will only respond if the ping requests are slower than 2 per second. Faster than that gets a logged message, but don't log more than 10 per minute…
- using INPUT policy of ACCEPT

```
iptables -P INPUT ACCEPT
# Add to the end of the file
iptables –A INPUT –p icmp --icmp-type echo-request
        -m limit --limit 2/second –j ACCEPT
iptables –A INPUT –p icmp
        --icmp-type echo-request -m limit --limit 10/minute –j LOG
iptables –A INPUT –p icmp
        --icmp-type echo-request -m limit --limit 10/minute –j DROP
```

Edinburgh Napier UNIVERSITY

INPUT ACCEPT

- To be clear, a policy of ACCEPT is seriously silly…
- Good to learn on but wide open to attack.
- ACCEPT policy means you need rules to block. Anything you didn't think about is accepted.
- DROP policy means you need rules to allow. Anything you didn't think about is dropped.
- Security relies on a good policy, and that must be DROP.

Edinburgh Napier UNIVERSITY

DROP or REJECT

- DROP just blocks the packet.
- REJECT blocks and also sends an ICMP message to the sender saying it is blocked.
- DROP gives nothing away, and a hacker finds it difficult to get useful information about your network if packets are dropped.
- REJECT gives away information about your firewall ruleset.
- With DROP and IP, where packets are lossy, some protocols may retransmit a packet which you have dropped thinking it has been lost. This means dealing with the same packet again and again.
- A good rule: intranet traffic should be REJECT, internet traffic should be DROP.

Edinburgh Napier UNIVERSITY

subroutines

- Sometimes, complex rules in a single chain are difficult to manage.
- My server firewall has 200 rules…
- In the same way as programs benefit from subroutines, so do firewall rules.
- Subroutines are created with –N, deleted with –X, and can be reached with a target of “-j subroutinename” and returned with a target of “-j RETURN”.

Edinburgh Napier UNIVERSITY

Monitor Monitor safe ping subroutine

- Anyone can ping this machine, but I will only respond if the ping requests are slower than 2 per second. Faster than that gets a logged message, but don't log more than 10 per minute… Use a SUBROUTINE

iptables –X ECHO
iptables –N ECHO
Iptables –A ECHO -m limit --limit 2/second –j ACCEPT
iptables –A ECHO -m limit --limit 10/minute –j LOG
iptables –A ECHO –j DROP

iptables –A INPUT –p icmp --icmp-type echo-request –j ECHO

Edinburgh Napier UNIVERSITY

Extra tests

- There are many other simple tests.
- Use man iptables to find more
- For example:
  - Stop apache surfing the web:

    iptables –A OUTPUT state --state NEW -p tcp
    --sport 80 -m owner --uid-owner=apache -j DROP
  - Specify port ranges like:

    --sport 137:139
  - Specify ip masks like:

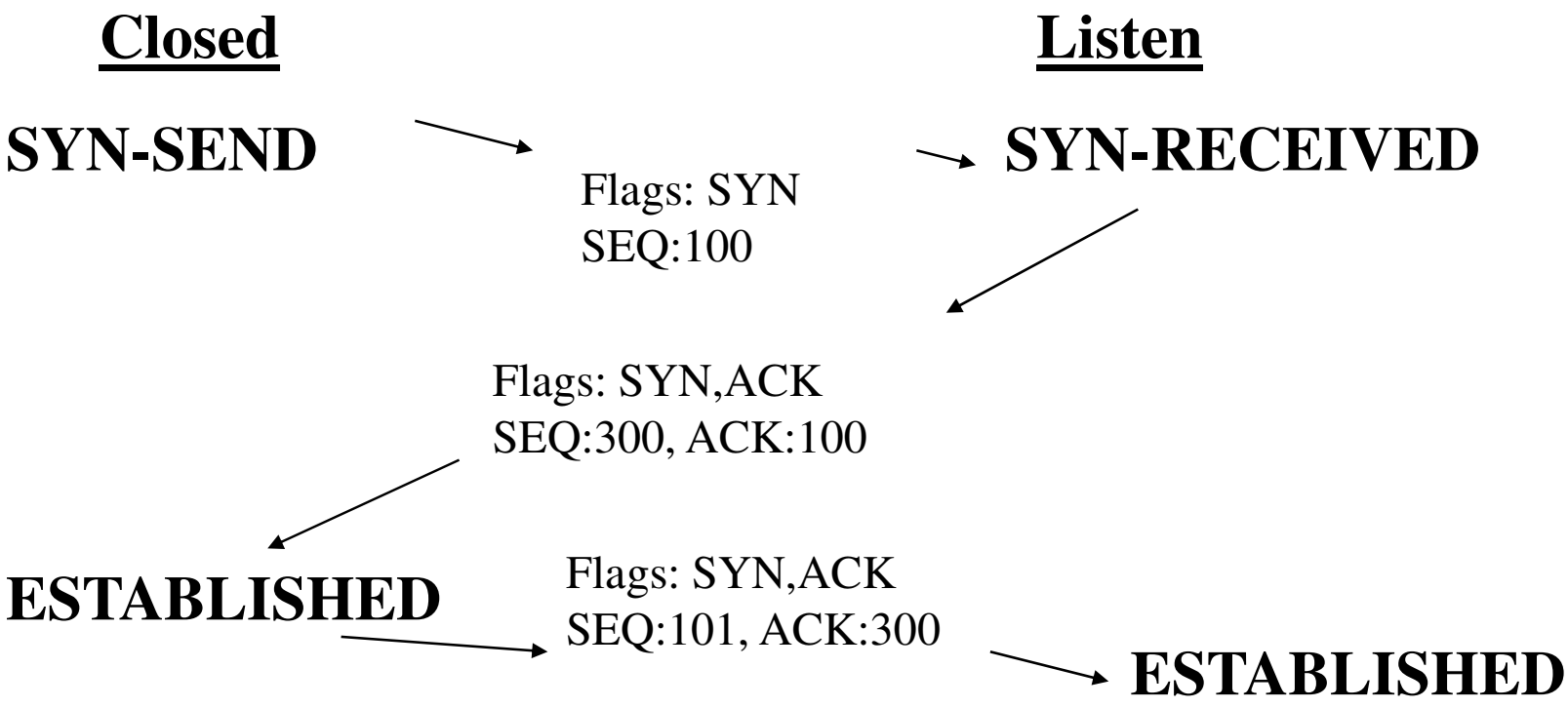
    -d 10.0.0.1/24

Edinburgh Napier
UNIVERSITY

Stateful Firewalls

Established: Stateful Firewall

- In TCP/IP, TCP goes through a number of states:



Edinburgh Napier UNIVERSITY

Stateful Rules

- You can add iptables rules to detect what state a packet is in.
- This is REALLY useful for FORWARD tables.
- It also, in general, makes your firewall rules more reliable and much smaller, even in INPUT and OUTPUT.

Edinburgh Napier UNIVERSITY

Rules based on network state

- Packets can be in a number of different states:
  - NEW – a packet which starts a new connection
  - RELATED – new connection, but part of an old session
  - ESTABLISHED – connection already running
  - INVALID – something else (?)

> iptables –A INPUT –i eth+ -m state --state RELATED,ESTABLISHED –j ACCEPT

Edinburgh Napier UNIVERSITY

Basic Stateful FORWARDING

- You are running your firewall machine with 2 network cards, eth0 and eth1.
- Eth0 connects to the internet, Eth1 to the intranet.
- In this regard Eth1 is a gateway for your local network.

Edinburgh Napier UNIVERSITY

- Eth0 is 10.0.1.1/24, Eth1 is 10.0.2.254/24
- You have two servers in your intranet.
  - M1 is 10.0.2.1/24, running an ssh server
  - M2 is 10.0.2.2/24, running an http server
- GW Firewall FORWARD would be:

```
iptables -F FORWARD
iptables -P FORWARD DROP
iptables –A FORWARD –m state --state RELATED,ESTABLISHED –j
    ACCEPT
iptables –A FORWARD –p tcp –i eth0 --dport ssh –d 10.0.2.1 –j ACCEPT
iptables –A FORWARD –p tcp –i eth0 --dport http –d 10.0.2.2 –j ACCEPT
```

Edinburgh Napier UNIVERSITY

Egress filtering

- So far it is normal to see ACCEPT as the default policy for OUTPUT.
- However, this is not as secure as having a DROP policy.
- DROP as the policy in OUTPUT is called *egress filtering*.
- Although easy to completely mess up it is no harder than INPUT DROP policy.
- It limits OUTPUT packets to only those which you explicitly define.
- It could help reduce hacking attempts, and the spread of viruses.

Edinburgh Napier UNIVERSITY

Complete EGRESS Example

- Configure a non-routing server firewall which runs telnet and http servers. Users on the server can ssh out. Use EGRESS filtering.

```
/sbin/iptables -F INPUT
/sbin/iptables -F OUTPUT
/sbin/iptables -F FORWARD
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -P FORWARD DROP
```

Edinburgh Napier UNIVERSITY

```
iptables -A INPUT –m state --state RELATED,ESTABLISHED –j
    ACCEPT
iptables –A INPUT –m state --state NEW –p tcp --dport telnet –j ACCEPT
iptables –A INPUT –m state --state NEW –p tcp --dport http –j ACCEPT
iptables -A OUTPUT –m state --state RELATED,ESTABLISHED –j
    ACCEPT
iptables –A OUTPUT state --state NEW -p tcp --dport ssh -j ACCEPT
```

Edinburgh Napier UNIVERSITY

Other Firewall Ideas

- Block private IPs leaving the gateway for the internet:

iptables -A FORWARD -o eth0 -s 192.168.0.0/16 -j DROP

iptables -A FORWARD -o eth0 -s 172.16.0.0/12 -j DROP

iptables -A FORWARD -o eth0 -s 10.0.0.0/8 -j DROP

- Only the loopback device can have IPs 127.0.0.1/8
- Blocking packets with a source port of smtp cuts down on viruses if the machine has no email server.
- Block netbios (ports 136/137) leaving for the internet.

Edinburgh Napier UNIVERSITY

Discussion

- How would iptables firewall rules, combined with a Linux based router, compare with a custom firewall appliance, such as a Cisco ASA5500?

Edinburgh Napier UNIVERSITY

Discussion

- Here are some past exam questions you should now be able to answer:

Edinburgh Napier UNIVERSITY

Question 1

Show the iptables commands relevant in defining an egress filter allowing only related or established connections, as well as outgoing http, to be accepted and all other egress traffic to be rejected. You can assume egress only involves eth0.

Edinburgh Napier UNIVERSITY

Question 2

Consider the following iptable configuration:

```
iptables –P INPUT drop
iptables –A INPUT –m state --state
    RELATED,ESTABLISHED –j ACCEPT
iptables –A INPUT –p tcp --sport ssh –j
    ACCEPT
```

Would incoming ssh connection requests be blocked? Give an explanation for your answer.