Advanced Security and Forensic Computing

Dr Bill Buchanan,
Reader,
School of Computing.

>Unit 2: Network Security Elements
Unit 2: Network Security Elements

OSI and Internet models

OSI

Application
Presentation
Session
Transport
Network
Data Link
Physical

Internet

Application
Transport
Internet

Firewall
Proxy
NAT
VPN/DMZ
IPSEC
Trans
Applic

© WJ Buchanan. ASFC (2)
Our First Security Model

Accesses are made through the proxy

Screening firewall. Filters packets, based on source/destination IP addresses and TCP ports

PIX firewall. Defines security rules.

NAT device. Maps private to public addresses.

Private IP addresses

Proxy

DMZ
Unit 2: Network Security Elements

Firewalls

Screening Firewalls and Proxies:

**Proxy** - isolates local network from untrusted networks (AKA: Application gateway)

**Screening firewall**: Filters for source and destination TCP ports

**Screen firewall**: Filters for source and destination IP addresses

Internet model:
- Application
- Transport
- Internet

Firewall
Proxy
NAT
VPN/DMZ
IPSEC
Trans
Applic
Screening Firewalls and Proxies:

**Proxy** - isolates local network from untrusted networks (AKA: Application gateway)

**Screening firewall:**

*Advantages:*
- Simple.
- Low costs

*Disadvantages:*
- Complexity of rules.
- Cost of managing firewall.
- Lack of user-authentication.
Screening Firewalls
A port on a router can be setup with **ACLs** to filter traffic based on the network address or the source or destination port number.

For example the firewall may block FTP traffic going out of the network.
- **Source IP address.** The address that the data packet was sent from.
- **Destination IP address.** The address that the data packet is destined for.
- **Source TCP port.** The port that the data segment originated from. Typical ports which could be blocked are FTP (port 21), TELNET (port 23), and WWW (port 80).
- **Destination TCP port.** The port that the data segment is destined for.
- **Protocol type.** This filters for UDP or TCP traffic.
Router# access-list access-list-value {permit | deny} source source-mask

Router# access-list 1 deny 156.1.1.10 0.0.0.0

Router# access-list 1 deny 156.1.1.0 0.0.0.255

Router# access-list 1 deny 156.1.1.0 0.0.0.255
Router# access-list 1 permit ip any any

Router (config)# interface Ethernet0
Router (config-if)# ip address 156.1.1.130 255.255.255.0
Router (config-if)# ip access-group 1 in

**Standard ACLs**

filter on the source IP address
Standard ACLs

Traffic from any address rather than 156.1.1.0 can pass

Router# access-list 1 deny 156.1.1.0 0.0.0.255
Router# access-list 1 permit ip any any

Router (config)# interface Ethernet0
Router (config-if)# ip address 156.1.1.130 255.255.255.0
Router (config-if)# ip access-group 1 in

Match this part
Ignore this part
Standard ACLs are applied as near to the destination as possible, so that they do not affect any other traffic.
Unit 2: Network Security Elements

Extended ACLs

Router# access-list access-list-value {permit | deny} {test-conditions}

Router(config)# access-list 100 deny ip host 156.1.1.134 156.70.1.1 0.0.0.0
Router(config)# access-list 100 permit ip any any

Router(config)# access-list 100 deny ip 156.1.1.0 0.0.0.255 156.70.1.0 0.0.0.255
Router(config)# access-list 100 permit ip any any

Router(config)# access-list 100 deny ip 156.1.1.0 0.0.0.254 host 156.70.1.1
Router(config)# access-list 100 permit ip any any

Router(config)# interface Ethernet0
Router(config-if)# ip address 156.1.1.130 255.255.255.192
Router(config-if)# ip access-group 100 in
Extended ACLs

**Firewall**

| E1 | 156.1.1.2 | E0 | 156.1.1.130 |

Firewall configuration:

- `Router(config)#access-list 100 deny ip host 156.1.1.2 70.1.2.0 0.0.0.255`
- `Router(config)#access-list 100 permit ip any any`

Denies traffic from 156.1.1.2 to the 70.1.2.0 network

- `Router(config)#access-list 100 deny ip 156.1.1.0 0.0.0.255 70.1.2.0 0.0.0.255`
- `Router(config)#access-list 100 permit ip any any`

Denies traffic from any host on 156.1.1.0 to the 70.1.2.0 network
Example of an Extended ACL

Extended ACLs are applied as near to the source as possible, as they are more targeted.

```
interface Ethernet0
   ip address 156.1.1.130 255.255.255.0
   ip access-group 100 in

access-list 100 deny ip 156.1.1.0 0.0.0.255 140.5.6.7 0.0.0.255
access-list 100 permit ip any any
```
An extended ACLs can also filter for TCP/UDP traffic, such as:

```
Router(config)#access-list access-list-value { permit | deny } {tcp | udp | igrp} source source-mask destination destination-mask {eq | neq | lt | gt} port
```

```
access-list 101 deny tcp 156.1.1.0 0.0.0.255 eq any host 156.70.1.1 eq telnet
access-list 101 permit ip any any
```

No Telnet Access to 156.70.1.1
A **closed** firewall, permits some things, and denies everything else.

An **open** firewall, denies some things, and permits everything else.
To block Napster traffic destined for port 8888:

```
(config)# access-list 100 deny tcp 192.5.5.0 0.0.0.255 any eq 8888 log
(config)# access-list 100 deny udp 192.5.5.0 0.0.0.255 any eq 8888 log
(config)# interface e0
(config-if)# ip access-group 100 in
```

or Kazaa (on port 1214):

```
(config)# access-list 101 deny tcp 192.5.5.0 0.0.0.255 any eq 1214 log
(config)# access-list 101 deny udp 192.5.5.0 0.0.0.255 any eq 1214 log
(config)# interface e0
(config-if)# ip access-group 101 in
```

Gnutella can be blocked with ports 6346 and 6347, while ICQ is blocked with 5190.
NAT
PAT (Port address translation) – Maps many addresses to one global address.

Network address translation
Network address translation

Src: 192.168.10.12:4444
Dest: 11.22.33.44:80

Outgoing data

Src: 168.10.34.21:5555
Dest: 11.22.33.44:80

Outgoing data

Src: 11.22.33.44:80
Dest: 192.168.10.12:4444

Incoming data

Src: 11.22.33.44:80
Dest: 168.10.34.21:5555

Incoming data

NAT router remembers the source and destination IP address and ports.
Unit 2: Network Security Elements

Incoming data

Outgoing data

Network address translation

<table>
<thead>
<tr>
<th>IP:port (inside)</th>
<th>IP:port (outside)</th>
<th>Ipdest:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.12:4444</td>
<td>168.10.34.21:5555</td>
<td>11.122.33.44:80</td>
</tr>
<tr>
<td>192.168.10.12:4445</td>
<td>168.10.34.21:5556</td>
<td>11.122.33.44:80</td>
</tr>
<tr>
<td>192.168.10.12:4446</td>
<td>168.10.34.21:5557</td>
<td>11.122.33.44:80</td>
</tr>
<tr>
<td>192.168.10.20:1234</td>
<td>168.10.34.21:5558</td>
<td>11.122.33.44:80</td>
</tr>
</tbody>
</table>

New connects in the table

© WJ Buchanan. ASFC (21)
Network address translation

Nat:
- Hides the network addresses of the network.
- Bars direct contact with a host.
- Increased range of address.
- Allow easy creation of subnetworks.

Src: 192.168.10.12:4444
Dest: 11.22.33.44:80
Outgoing data

Src: 168.10.34.21:5555
Dest: 11.22.33.44:80
Outgoing data

Src: 11.22.33.44:80
Dest: 192.168.10.12:4444
Incoming data

Src: 11.22.33.44:80
Dest: 168.10.34.21:5555
Incoming data
**Static translation.**
Each public IP address translates to a private one through a static table. Good for security/logging/traceability. Bad, as it does not hide the internal network.

**IP Masquerading (Dynamic Translation).**
A single public IP address is used for the whole network. The table is thus dynamic.

**Load Balancing Translation.**
With this, a request is made to a resource, such as to a WWW server, the NAT device then looks at the current loading of the systems, and forwards the request to the one which is most lightly used...
Unit 2: Network Security Elements

NAT - Load balancing

NAT device selects the least used resource

Private address

Public address

Server pool

a1.b1.c1.d1
Or
a1.b1.c1.d1
Or...
an.bn.cn.dn

w.x.y.z

Firewall

Proxy

NAT

VPN/DMZ

IPSEC

Trans

Applic
NAT is good as we are isolated from the external public network, where our hosts make the **initiate** connections.

... but what happens if we use applications which create connections in the reverse direction, such as with FTP and IRC?

.. we thus need some form of **backtracking** of connections in the NAT device.
Static NAT is poor for security, as it does not hide the network. This is because there is a one-to-one mapping.

Dynamic NAT is good for security, as it hides the network. Unfortunately it has two major weaknesses:

- **Backtracking** allows external parties to trace back a connection.
- If the NAT device becomes compromised the external party can redirect traffic.
PIX firewall
Unit 2: Network Security Elements

Perimeter router

E0 - outside

PIX

E1 - inside

trusted network

DMZ

untrusted network
Proxies
Screening Firewalls and Proxies:

**Proxy** - isolates local network from untrusted networks (AKA: Application gateway)

**Proxy:**

*Advantages:*
- User-oriented authentication.
- User-oriented logging.
- User-oriented accounting.

*Disadvantages:*
- Build specifically for each application (although the SOCKS protocol has been designed, which is an all-one proxy).
Blocking the Incoming Traffic to Hosts

```
hostname myRouter

interface Ethernet0
ip address 192.168.10.1 255.255.255.0
ip access-group 100 in

interface Ethernet1
ip address 169.10.11.1 255.255.0.0
ip access-group 101 in

access-list 100 permit ip 192.168.10.65 any
access-list 100 deny any any

access-list 101 permit ip any host 192.168.10.65
access-list 101 deny any any
end
```

Data can be send to the proxy

Access to proxy is allowed
Everything else is barred
Blocking Outgoing Traffic from Hosts

```
hostname myRouter
!
interface Ethernet0
ip address 192.168.10.1 255.255.255.0
ip access-group 100 in
!
interface Ethernet1
ip address 169.10.11.1 255.255.0.0
ip access-group 100 in
!
access-list 100 permit ip 192.168.10.65 any
access-list 100 deny any any
!
access-list 101 permit ip any host 192.168.10.65
access-list 101 deny any any
end
```
An Improvement - Application Level Firewall

Screened firewall only allows traffic to flow to and from the proxy

Screened firewall only allows traffic between the hosts and the proxy
Access made to WWW site on Port 80

HTTP goes out on TCP port 6588, to the proxy

Proxy setup
Unit 2: Network Security Elements

Proxy setup

Access made to WWW site on Port 80

192.168.10.65

HTTP (web browsers) (port 6588)
HTTPS (secure web browsers) (port 6588)
SOCKS4 (TCP proxying) (port 1080)
SOCKS4a (TCP proxying w/ DNS lookups) (port 1080)
SOCKS5 (only partial support, no UDP) (port 1080)
NNTP (usenet newsgroups) (port 119)
POP3 (receiving email) (port 110)
SMTP (sending email) (port 25)
FTP (file transfers) (port 21)
Unit 2: Network Security Elements

Filtering incoming ports

Only telnet, ftp, http and pop3 are allowed

```
hostname myRouter
!
interface Ethernet1
ip address 169.10.11.1 255.255.0.0
ip access-group 101 in
!
access-list 101 permit tcp any any eq telnet host 192.168.10.65
access-list 101 permit tcp any any eq ftp host 192.168.10.65
access-list 101 permit tcp any any eq http host 192.168.10.65
access-list 101 permit tcp any any eq pop3 host 192.168.10.65
access-list 101 deny any any
!
end
```
Filtering outgoing ports

Only telnet, ftp, http and pop3 are allowed out

```
hostname myRouter
!
interface Ethernet0
ip address 192.168.10.1 255.255.255.0
ip access-group 100 in
!
!
access-list 100 permit tcp host 192.168.10.65 any any eq telnet
access-list 100 permit tcp host 192.168.10.65 any any eq ftp
access-list 100 permit tcp host 192.168.10.65 any any eq http
access-list 100 permit tcp host 192.168.10.65 any any eq pop3
access-list 100 deny any any
!
end
```
Proxy logging

Unit 2: Network Security Elements

Access made to WWW site on Port 80

WWW server

192.168.10.65

Firewall
Proxy
NAT
VPN/DMZ
IPSEC
Trans
Applic

WWW server

Proxy logging

© WJ Buchanan. ASFC (38)
Proxy logging

The log will always show the address of the proxy.

Proxy allows:

- The hosts to be hidden from the outside.
- Private addresses can be used for the internal network.
- Logging of data packets.
- User-level authentication, where users may require a username and a password.
- Isolation of nodes inside the network, as they cannot be directly contacted.