Virtual private network

- Instead of a dedicated data link
- Packets securely sent over a shared network
- Internet VPN
  - Public internet
  - Security protocol encrypts packets
- Three scenarios
  - Host-to-host tunnel
  - Host-to-router tunnel
  - Router-to-router tunnel

VPN

- Packets tunnelled between routers
- Security parameters negotiated when the link is brought up

VPN

- Packets tunnelled between routers
- Security parameters negotiated when the link is brought up
Network Address Translation

- References
  - KR3 p 339
  - C4 chap 20
  - T4 p444

Network address translation

- To help with shortage of IPv4 addresses
- Set up a network using private addresses
- NAT router has one or more global IPv4 addresses
  - Traffic from inside the local network is relabelled with a global IP address
  - Traffic from outside is routed inside based on IP address and possibly port number

Basic NAT

- Outgoing packet:
  - Look up internal IP address → external IP address or assign new external IP address
  - Replace source address in packet with external
- Incoming packet:
  - Look up external IP address → internal IP destination address
  - Replace destination address in packet with internal IP address
- Address reuse: assignments expire
Basic NAT

- Outgoing packet:
  - Look up source (IP, port) → external port number or assign new external port number
  - Replace source address and port number
- Incoming packet:
  - Look up destination external port → (IP, port)
  - Replace destination address and port number in packet
- Port number reuse: assignments expire

PAT NAT

- Outgoing packet:
  - Look up source (IP, port) → external port number or assign new external port number
  - Replace source address and port number
- Incoming packet:
  - Look up destination external port → (IP, port)
  - Replace destination address and port number in packet
- Port number reuse: assignments expire

NAT: Port address translation

NAT: Basic and PAT

- Basic NAT
  - Limits number of computers
  - One IP per computer
  - Internal machine must contact outside to assign IP address
  - External machines can then initiate communication
- PAT NAT
  - Computers share a single IP
  - Internal machine must contact outside to assign port number
  - External machines cannot initiate communication
  - Well known ports can be permanently assigned to internal servers
**PAT NAT: Server setup**

- **Web server**
  - 192.168.0.11
  - 137.111.11.26:80 to 149.22.35.11:3582
  - 149.22.35.11 to 192.168.0.11:80
- **Web browser**
  - 192.168.0.32
  - 3582

**The Internet**

- 192.168.0.11:80 to 149.22.35.11:3582
- 137.111.11.26 to 192.168.0.11:80

**PAT NAT limitations**

- Only supports TCP and UDP – uses port number
- External machine can only contact forwarded ports
  - Internal origin
  - Well known port configured to internal server
  - Default "DMZ" host to receive unassigned ports
  - Can help ensure security

**PAT NAT limitations (cont)**

- Protocols that open additional ports may fail across PAT NAT
  - Port number is sent in a message on another port – the port number must be modified across the NAT box.
  - FTP client opens port but server cannot access it
    - Use FTP in passive mode
  - SIP → RTP
  - Games and P2P applications
- Firewalls have the same problem – they need to know which ports should be open
- Newer protocols must be designed for NAT

**DNS and NAT (CISCO)**

- DNS replies may be modified as they cross a NAT box
  - A user inside queries a DNS server outside for a machine that happens to be inside also

**Diagram:**

- User
- NAT
- DNS
- Query: ftp.cisco.com
- 209.165.201.10
-Reply: 10.1.0.17
- Reply: 209.165.210.10
- ftp.cisco.com
- 10.1.0.17
**Firewall references**
- C4 chap 32
- KR3 section 8.6

---

**Packet filtering**
- Packets are filtered by IP header and router interface
  - IP source
  - IP destination
  - Protocol
  - Source port
  - Destination port
- Block spoofed IP
- Block broadcast
- Block ICMP

Rules are checked in sequence: first matching rule is used

---

**Packet filtering**
- Filtering incoming packets also blocks outgoing connections
  - Reply packets come from outside
  - Destination port is not a well-known server
- Solution: bastion host acts as proxy for internal clients
- Alternative:
  - Stateful packet inspection tracks active connections and allows reply packets

---

**Bastion host**
- Acts as proxy for internal clients (e.g. web proxy)
- Provides services to external clients

Only admit: packets to bastion host (clients or services)
Only admit: packets from bastion host

Corporate network — Bastion host — Internet
Application gateway

- User connects to gateway, authorises, gateway connects externally.
  - telnet firewall.mysite.com
  - Login with user name and password
  - Now telnet to remote site and login there

Stateful packet inspection

- Maintains connection state
- Simplifies inspection of packets belonging to known connections
  - Does not need to apply firewall rules repeatedly
  - Allows detection of denial of service attacks
    - SYN flood, UDP flood, ICMP flood, etc
  - Allows intrusion detection
    - Port scanning

SPI connection filtering rules

<table>
<thead>
<tr>
<th>Outbound Services</th>
<th>Action</th>
<th>LAN Users</th>
<th>WAN Users</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Service Name</td>
<td>Action</td>
<td>LAN Users</td>
<td>Log</td>
</tr>
<tr>
<td>1</td>
<td>rlogin</td>
<td>ALLOW always</td>
<td>Any</td>
<td>137.111.0.1 - 137.111.255.255</td>
</tr>
<tr>
<td>2</td>
<td>FTP</td>
<td>ALLOW always</td>
<td>Any</td>
<td>Always</td>
</tr>
<tr>
<td>3</td>
<td>HTTP</td>
<td>ALLOW always</td>
<td>Any</td>
<td>137.111.0.1 - 137.111.255.255</td>
</tr>
<tr>
<td>4</td>
<td>DNS</td>
<td>ALLOW always</td>
<td>Any</td>
<td>Always</td>
</tr>
<tr>
<td>5</td>
<td>SSH</td>
<td>ALLOW always</td>
<td>Any</td>
<td>21 - 21.161.32 - 211.32.254</td>
</tr>
<tr>
<td>6</td>
<td>SMTP</td>
<td>ALLOW always</td>
<td>Any</td>
<td>Always</td>
</tr>
<tr>
<td>7</td>
<td>SMB</td>
<td>ALLOW always</td>
<td>Any</td>
<td>Always</td>
</tr>
<tr>
<td>8</td>
<td>Airport</td>
<td>ALLOW always</td>
<td>Any</td>
<td>21 - 21.161.32 - 211.32.254</td>
</tr>
<tr>
<td>9</td>
<td>Port</td>
<td>ALLOW always</td>
<td>Any</td>
<td>21 - 21.161.32 - 211.32.254</td>
</tr>
<tr>
<td>10</td>
<td>POP3</td>
<td>ALLOW always</td>
<td>Any</td>
<td>21 - 21.161.32 - 211.32.254</td>
</tr>
<tr>
<td>11</td>
<td>POP2</td>
<td>ALLOW always</td>
<td>Any</td>
<td>Always</td>
</tr>
<tr>
<td>12</td>
<td>MSNP</td>
<td>ALLOW always</td>
<td>Any</td>
<td>192.168.1.1 - 192.168.1.254</td>
</tr>
<tr>
<td>13</td>
<td>Mail</td>
<td>ALLOW always</td>
<td>Any</td>
<td>10 - 10.168.1.0 - 10.255.255.254</td>
</tr>
<tr>
<td>14</td>
<td>PNTP</td>
<td>ALLOW always</td>
<td>Any</td>
<td>192.168.0.0 - 192.168.255.254</td>
</tr>
<tr>
<td>15</td>
<td>IIS</td>
<td>ALLOW always</td>
<td>Any</td>
<td>192.168.1.24</td>
</tr>
<tr>
<td>16</td>
<td>HTTP</td>
<td>ALLOW always</td>
<td>Any</td>
<td>Always</td>
</tr>
</tbody>
</table>

SPI connection filtering rules

<table>
<thead>
<tr>
<th>Inbound Services</th>
<th>Action</th>
<th>LAN Source IP address</th>
<th>WAN Policies</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Service Name</td>
<td>Action</td>
<td>LAN Source IP address</td>
<td>WAN Policies</td>
</tr>
<tr>
<td>1</td>
<td>IRC</td>
<td>ALLOW always</td>
<td>192.168.0.24</td>
<td>Always</td>
</tr>
<tr>
<td>2</td>
<td>watch</td>
<td>ALLOW by schedule</td>
<td>192.168.0.24</td>
<td>Always</td>
</tr>
<tr>
<td>3</td>
<td>HTTP</td>
<td>ALLOW always</td>
<td>192.168.0.24</td>
<td>Always</td>
</tr>
</tbody>
</table>

Options
- Default DMZ Server
- Respond to Ping on Internal (LAN) Port
- Enable VPN Pass-through (IPsec, PPTP, L2TP)
- Drop fragmented IP packets
- Block TCP flood
- Block UDP flood
- Block non-standard packets

Apply/ Cancel
DMZ

- External & internal hosts may access DMZ
- DMZ hosts may only access external hosts
- DMZ hosts via PAT
- Soho ‘DMZ’ not true DMZ - unprotected

(from Wikipedia)

Deep packet inspection

- Inspects packet contents not just headers
- Can recognise packets not conforming to higher-level protocol
  - E.g. non-HTTP on port 80
- Can recognise attacks within protocols
  - Merged IDS functionality
  - E.g. SMTP VRFY command
  - Drop connection before damage can happen

http://www.securityfocus.com/infocus/1716

Difficult protocols

- Involve additional connections
- May convey port numbers in an existing connection
- FTP
  - Passive mode
- SIP & RTP

SIP & RTP firewall problem

- Signaling messages negotiate parameters for media streams
- Signaling messages may travel on different path through network than media streams do
- SIP/RTCP firewall traversal problem

http://www.ikr.uni-stuttgart.de/Content/VFF_IKR_Workshop_2006/VoIP_Firewall_Signaling.pdf
SIP & RTP firewall problem

- Remove firewall?
- HTTP tunnel?
  - Insecure solutions
- SIP decoder in packet filter
  - Cannot handle path differences
- Application layer gateways
  - Media path forced to follow signalling path

SIP & RTP firewall problem

- Firewall control protocol messages
  - Open ‘pinhole’ for RTP
  - Who is in control?
  - Path-coupled: messages follow future path
    - RSVP
    - IETF NSIS (Next Steps in Signalling)
    - Problem: secure and efficient signalling message authorization
  - Path-decoupled
    - Current research: SIMCO protocol

SIP & RTP – firewall signalling

Multiple connections

- Firewalls on each external connection must implement the same access rules
  - Otherwise, the least restrictive rules can be used to gain access
Monitoring and logging

- Active – firewall notifies manager of event when it occurs
- Passive – firewall writes information to log – manager can review it
  - Periodic analysis to detect trends
  - Investigation of security events after they occur – what led up to them

VPN Risk

- VPN makes PC that is ‘outside’ part of ‘inside’
- Encrypted VPN packets cannot be inspected by firewall unless firewall is tunnel endpoint