PART XIX

PRIVATE NETWORK INTERCONNECTION
(NAT AND VPN)
Definitions

- An internet is *private* to one group (sometimes called *isolated*) if none of the facilities or traffic is accessible to other groups
  - Typical implementation involves using leased lines to interconnect routers at various sites of the group
- The global Internet is *public* because facilities are shared among all subscribers
Hybrid Architecture

- Permits some traffic to go over private connections
- Allows contact with global Internet
Example Of Hybrid Architecture
The Cost Of Private And Public Networks

- Private network extremely expensive
- Public Internet access inexpensive
- Goal: combine safety of private network with low cost of global Internet
Question

How can an organization that uses the global Internet to connect its sites keep its data private?

• Answer: Virtual Private Network (VPN)
Virtual Private Network

- Connect all sites to global Internet
- Protect data as it passes from one site to another
  - Encryption
  - IP-in-IP tunneling
Illustration Of Encapsulation
Used With VPN
The Point

A Virtual Private Network sends data across the Internet, but encrypts intersite transmissions to guarantee privacy.
Example Of VPN Addressing And Routing

Site 1

128.10.1.0

128.10.2.0

Site 2

192.5.48.0

128.210.0.0

destination | next hop
---|---
128.10.1.0 | direct
128.10.2.0 | R2
192.5.48.0 | tunnel to R3
128.210.0.0 | tunnel to R3
default | ISP's router

Routing table in R1
Example VPN With Private Addresses

- Advantage: only one globally valid IP address needed per site
General Access With Private Addresses

- Question: how can a site provide multiple computers at the site access to Internet services without assigning each computer a globally-valid IP address?
- Two answers
  - Application gateway (one needed for each service)
  - Network Address Translation (NAT)
Network Address Translation (NAT)

- Extension to IP addressing
- IP-level access to the Internet through a single IP address
- Transparent to both ends
- Implementation
  - Typically software
  - Usually installed in IP router
  - Special-purpose hardware for highest speed
Network Address Translation (NAT) (continued)

- Pioneered in Unix program slirp
- Also known as
  - Masquerade (Linux)
  - Internet Connection Sharing (Microsoft)
- Inexpensive implementations available for home use
NAT Details

- **Organization**
  - Obtains one globally valid address per Internet connection
  - Assigns nonroutable addresses internally (net 10)
  - Runs NAT software in router connecting to Internet

- **NAT**
  - Replaces source address in outgoing datagram
  - Replaces destination address in incoming datagram
  - Also handles higher layer protocols (e.g., pseudo header for TCP or UDP)
NAT Translation Table

- NAT uses translation table
- Entry in table specifies local (private) endpoint and global destination.
- Typical paradigm
  - Entry in table created as side-effect of datagram leaving site
  - Entry in table used to reverse address mapping for incoming datagram
Example NAT Translation Table

<table>
<thead>
<tr>
<th>Private Address</th>
<th>Private Port</th>
<th>External Address</th>
<th>External Port</th>
<th>NAT Port</th>
<th>Protocol Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.5</td>
<td>21023</td>
<td>128.10.10.20</td>
<td>80</td>
<td>14003</td>
<td>tcp</td>
</tr>
<tr>
<td>10.0.0.1</td>
<td>388</td>
<td>128.10.10.20</td>
<td>80</td>
<td>14010</td>
<td>tcp</td>
</tr>
<tr>
<td>10.0.2.8</td>
<td>26600</td>
<td>207.200.75.200</td>
<td>21</td>
<td>14012</td>
<td>tcp</td>
</tr>
<tr>
<td>10.0.0.3</td>
<td>1274</td>
<td>128.210.1.5</td>
<td>80</td>
<td>14007</td>
<td>tcp</td>
</tr>
</tbody>
</table>

- Variant of NAT that uses protocol port numbers is known as *Network Address and Port Translation (NAPT)*
Use Of NAT By An ISP
Higher Layer Protocols And NAT

- NAT must
  - Change IP headers
  - Possibly change TCP or UDP source ports
  - Recompute TCP or UDP checksums
  - Translate ICMP messages
  - Translate port numbers in an FTP session
Applications And NAT

NAT affects ICMP, TCP, UDP, and other higher-layer protocols; except for a few standard applications like FTP, an application protocol that passes IP addresses or protocol port numbers as data will not operate correctly across NAT.
Summary

- Virtual Private Networks (VPNs) combine the advantages of low cost Internet connections with the safety of private networks
- VPNs use encryption and tunneling
- Network Address Translation allows a site to multiplex communication with multiple computers through a single, globally valid IP address.
- NAT uses a table to translate addresses in outgoing and incoming datagrams