CSC411: Advanced Networks

Firewalls and VPNs

Note: **This class lecture will be recorded!**
If you do not consent to this recording, please do not ask questions via your video, audio or public chat; send your question to the instructor using the private chat.

Dr. Lisa Frye, Instructor
frye@kutztown.edu
Kutztown University

Intro

- Look at 328 and 512 notes for some introduction here

Firewall Questions

- What are the advantages and disadvantages of a hardware firewall?

- What are the advantages and disadvantages of a software firewall?

Firewalls

- Purpose
  - Restrict people to enter at a carefully controlled point
  - Prevent attackers from getting close to your other defenses
  - Restrict people to leave at a carefully controlled point
- Design goals
  - All traffic from inside to outside and vice versa must travel through the firewall
  - Only authorized traffic can pas through the firewall
  - The firewall must be immune to penetration

Firewall Access Control

- Service control
- Direction control
- User control
- Behavior control

Firewall Management Cycle

- Draft a written security policy
- Design the firewall to implement the security policy
- Implement the firewall design by installing selected hardware or software
- Test the firewall
- Review new threats, requirements for additional security, and updates to adopted systems and software.

Stateless Packet Filter

- Rule Base
- Forward or Discard

- Advantages
- Disadvantages

Example Firewall Rules

Table 9-1 Stateless packet-filtering rules

Rule	Source IP	Source Port	Destination IP	Destination Port	Action
1	Any	Any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	Any	Any	Any	Deny
3	Any	Any	192.168.120.1	Any	Deny
4	192.168.120.0	Any	Any	Any	Any
5	Any	Any	192.168.120.2	25	Allow
6	Any	Any	192.168.120.3	80	Allow
7	Any	Any	Any	Any	Deny

Stateful Packet Filters

Table 9-2 State table example

Source IP	Source Port	Destination IP	Destination Port	Connection State
192.168.120.101	1037	209.233.19.22	80	Established
192.168.120.104	1022	165.66.28.22	80	Established
192.168.120.107	1010	65.66.122.101	25	Established
192.168.120.102	1035	213.136.87.88	79	Established
223.56.78.11	1899	192.168.120.101	80	Established
206.121.55.8	3558	192.168.120.101	80	Established
224.209.122.1	1079	192.168.120.105	80	Established

Firewall Rules

- Allow all, deny specific
- Deny all, allow specific

- Processed in order
- Keep simple and short

Establishing Effective Rules

- Based on Security Policy
  - Firewall Policy
- Simple and short
- Restrict access to internal network
- Control Internet services

Firewall in Action

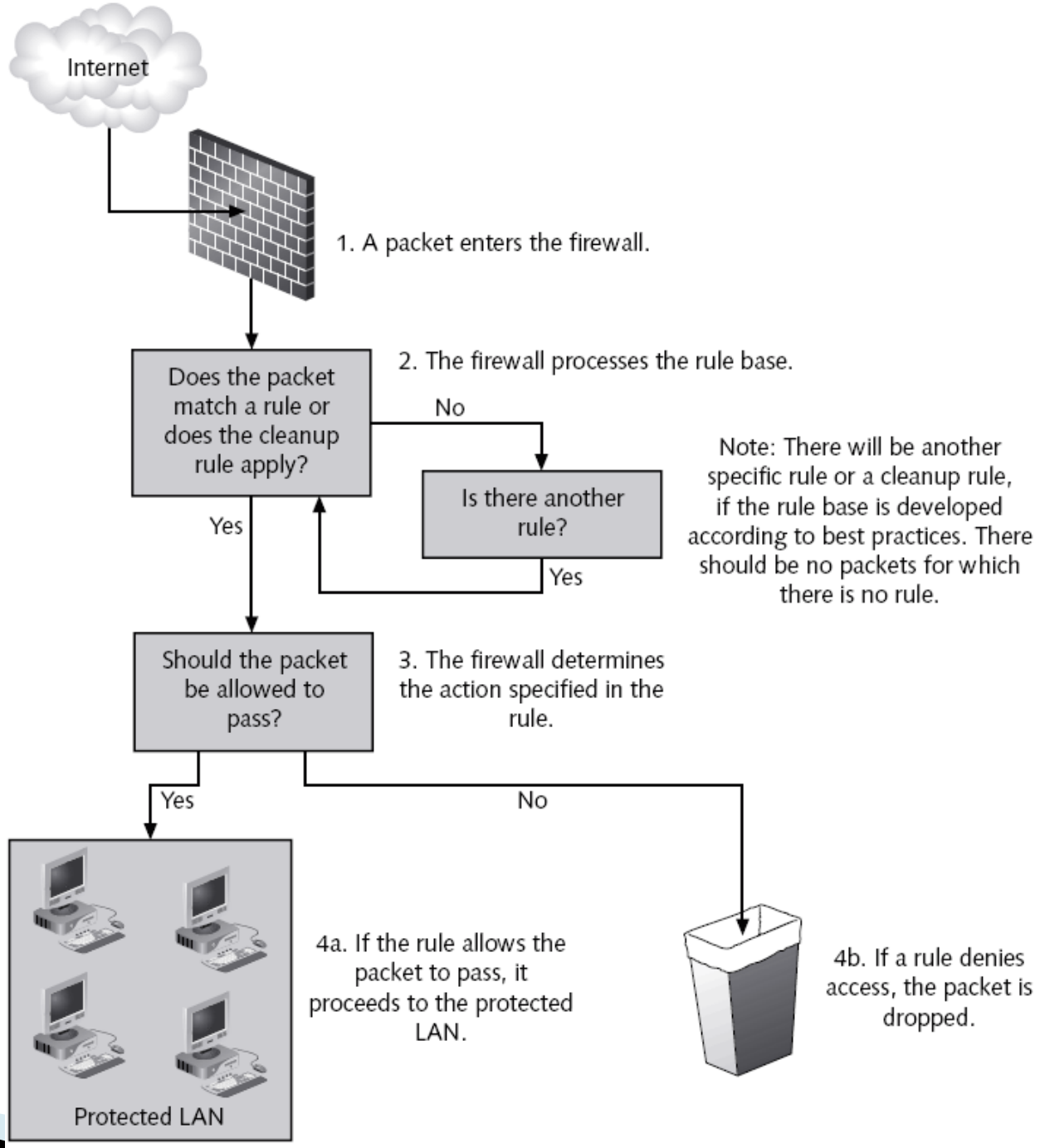

Figure 9-11 Firewalls process rules in order until a match is found

Example Rules

Table 9-11 A typical packet-filtering rule base

Rule	Source IP	Source Port	Destination IP	Destination	Action	What It Does
1	192.168.120.1	Any	Any	Any	Deny	Prevents the firewall itself from making any connections
2	Any	Any	192.168.120.1	Any	Deny	Prevents anyone from connecting to the firewall
3	192.168.120.0	Any	Any	Any	Allow	Allows internal users to access external computers
4	192.168.120.0	Any	192.168120.4	53	Allow	Enables internal users to connect to the DNS server

Table 9-11 A typical packet-filtering rule base (continued)

Rule	Source IP	Source Port	Destination IP	Destination	Action	What It Does
5	Any	Any	192.168.120.2	25	Allow	Allows external and internal users to access the e-mail server via SMTP port 25
6	192.168.120.0	Any	192.168.120.2	110	Allow	Enables internal users to connect to the e-mail server using POP3 port 110
7	Any	Any	192.168.120.3	80	Allow	Enables both external and internal users to connect to the Web server
8	Any	Any	Any	Any	Deny	Blocks all traffic not covered by previous rules

DMZ

- Perimeter network
- Public access servers

- What type of servers/services should be placed in DMZ?

Remote Users

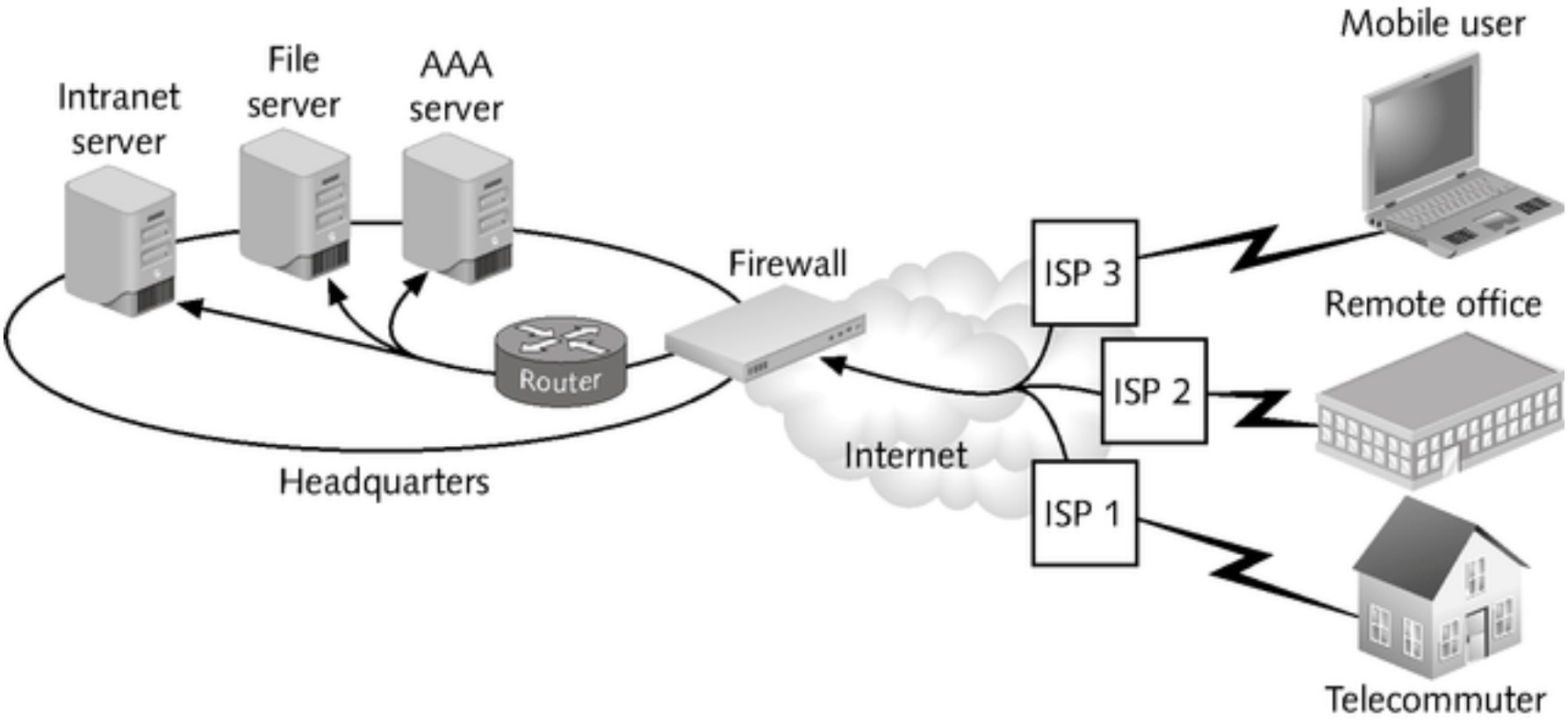

Figure 4-3 VPN diagram

Remote Access VPNs

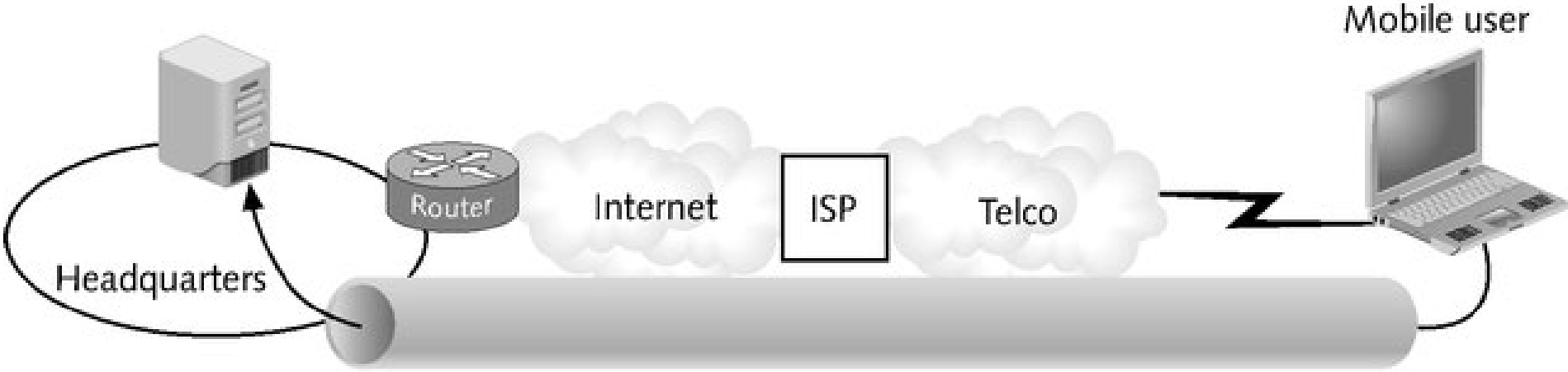

Figure 4-4 Client-side tunneling

VPN Objectives

- Isolate a distributed network from outsiders
- Protect the privacy and integrity of messages traversing untrusted networks
- Handle the whole range of Internet protocols currently in use
- Public Internet access is available and cost is very important

Essential Activities of VPNs

- IP encapsulation
- Data payload encryption
  - Transport
  - Tunnel
- Encrypted authentication

VPN Successful Operation

- Establishing a VPN Policy for users
- Packet filtering
- Test the VPN
- Audit the VPN operation