Module 3: Network Module 3 PT7

Network Layer - Layer 3 - Packets - Day 5

Vocabulary and Links

Access Control Lists - Sunny's Classroom
Stateful vs Stateless Firewall - AV Cyber Active
What is a firewall? - PowerCert
What is a firewall? - Sunny's Classroom
What is a Proxy Server - PowerCert
Proxy Server - Sunny's Classroom
Proxy vs Reverse Proxy Explained - PowerCert
Network Types... - PowerCert
7 LAN Topologies - Sunny's Classroom
Network Topology - PowerCert

Firewalls
ACL
Stateless vs Stateful
Unified Threat Management (UTM) - All in one application for firewalls, switch, router, load balancer, DNS Server
Next Generation Firewall (NGFW) - Upgraded version of UTM

Firewalls

Traffic filtering network security system.

- Monitors attempts to gain access
- Blocks unwanted traffic and unrecognized sources
- Port Filtering, MAC Filtering, IP Filtering, Content Filtering, Dynamic Filtering (Stateful Filtering) - All packets are examined as a stream. Depends on what packets have already been sent through.

Characteristics

- Can filter based on:
    - MACs, IP protocols, IP address, ports, domain name, apps/contents, key words, OR conversation/stream

Types

- Software-based vs hardware based, or both
- Network-based vs host-based

Access Control List (ACL) - tells the router(caveman firewall) to permit or deny traffic according to one or more filter parameters.

Stateless	Stateful
Just Packets	“Data Flow”
No History	“Conversation”
Fast	Resource Intensive

Stateful Firewall

Context: Maintains a record (state) of connections passing through it.

Packet Analysis: Analyzes the entire data flow and context of network packets.

Security: Provides greater security by considering packet context.

Resource Usage: More resource-intensive, may introduce latency.

Complexity: More complex configuration and setup.

Use Cases: Suitable for complex network setups and advanced threats.

Stateless Firewall

Context: Does not maintain any knowledge of past network connections

Packet Analysis: Evaluates each packet individually based on predefined rules.

Security: Offers basic packet filtering based on predefined rules.

Resource Usage: Lightweight and efficient, minimal impact on performance.

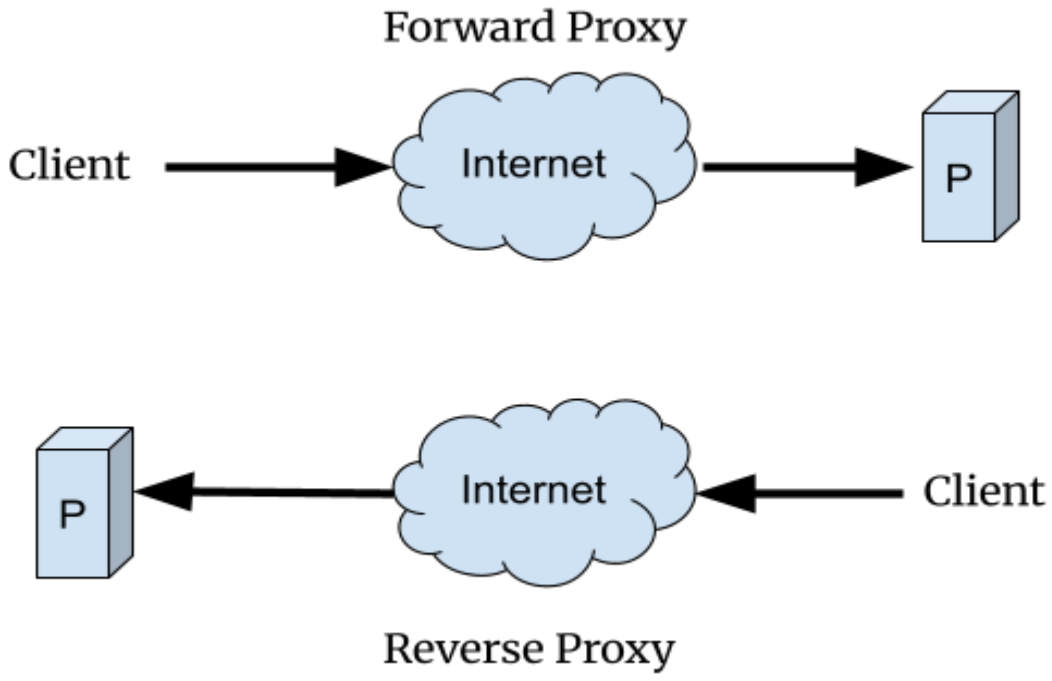
Complexity: Easier to configure and manage

Use Cases: Suitable for simple networks and basic packet filtering.

Firewall Selection and Placement

Unified Threat Management (UTM) - All in one application for firewalls, switches,
Next Generation Firewall (NGFW) - Filters on the different layers of the TCP/IP Model (Payload).
Proxy Server - A firewall of sorts that filters at the application layer. Proxy filters IP addresses, NAT doesn't filter.

- Controlling inbound and outbound traffic.
- Proxy servers can keep track of incoming traffic
- It can be setup to bypass firewalls
- "Middle-Man"
- "Agent of Client"
- Application F/W
- "WAF"
- "Cache"
- Forward proxy - acts as guardian for private network and the internet
- Reverse proxy - acts as a guardian for private servers against computers (clients)



Network Types

PAN - Personal Area Network
LAN - Local Area Network
WLAN - Wide Local Area Network
CAN - Campus Area Network

MAN - Metropolitan Area Network
SAN - Storage Area Network
WAN - Wide Area Network

Topology

Physical - Follow the cable
Logical - Follow the bits

1. Point-to-point
2. BUS
3. Ring
4. Star
5. Mesh

3 Tier Network Hierarchy

- Scaleable
    - The ability to provide growth
- Resilient
    - Tolerable faulty devices and keep working
- Management
    - How “easy” is it to monitor, change, troubleshoot, etc.

Top Level Core Layer

- Network “backbone”
- Forward traffic as fast as possible
- Layer 3 Switches

Middle Level Distribution/Aggregation Layer

- Fault tolerant links between access blocks and core
- Layer 3 switches

Low Level Access Layer

- Closest to users
- Workgroup switches