COURSE: SECURITY+ SY0-401

MODULE 1: NETWORK SECURITY

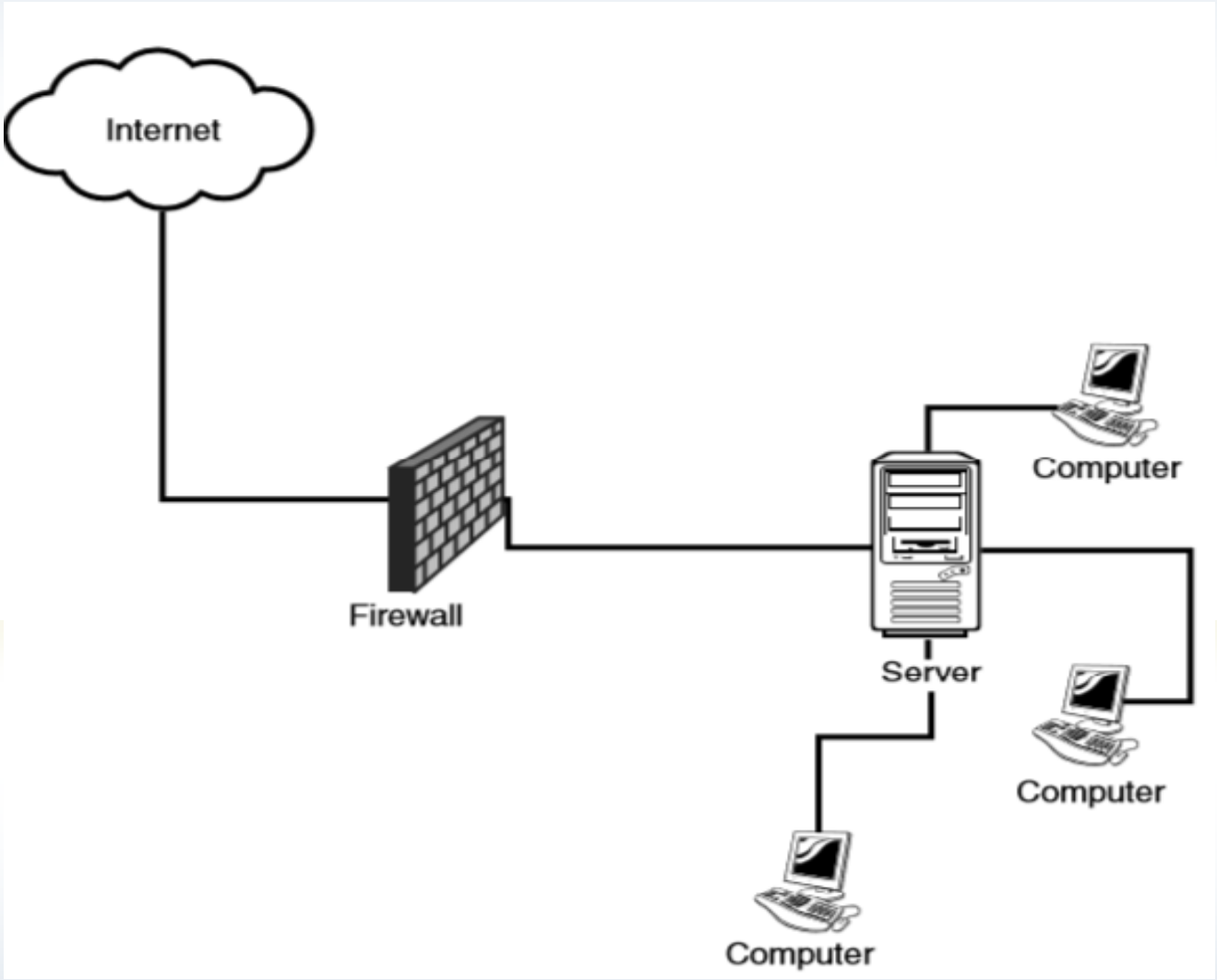
Part A

Overview

- Implement security configuration parameters on network devices and other technologies
- Given a scenario, use secure network administration principles

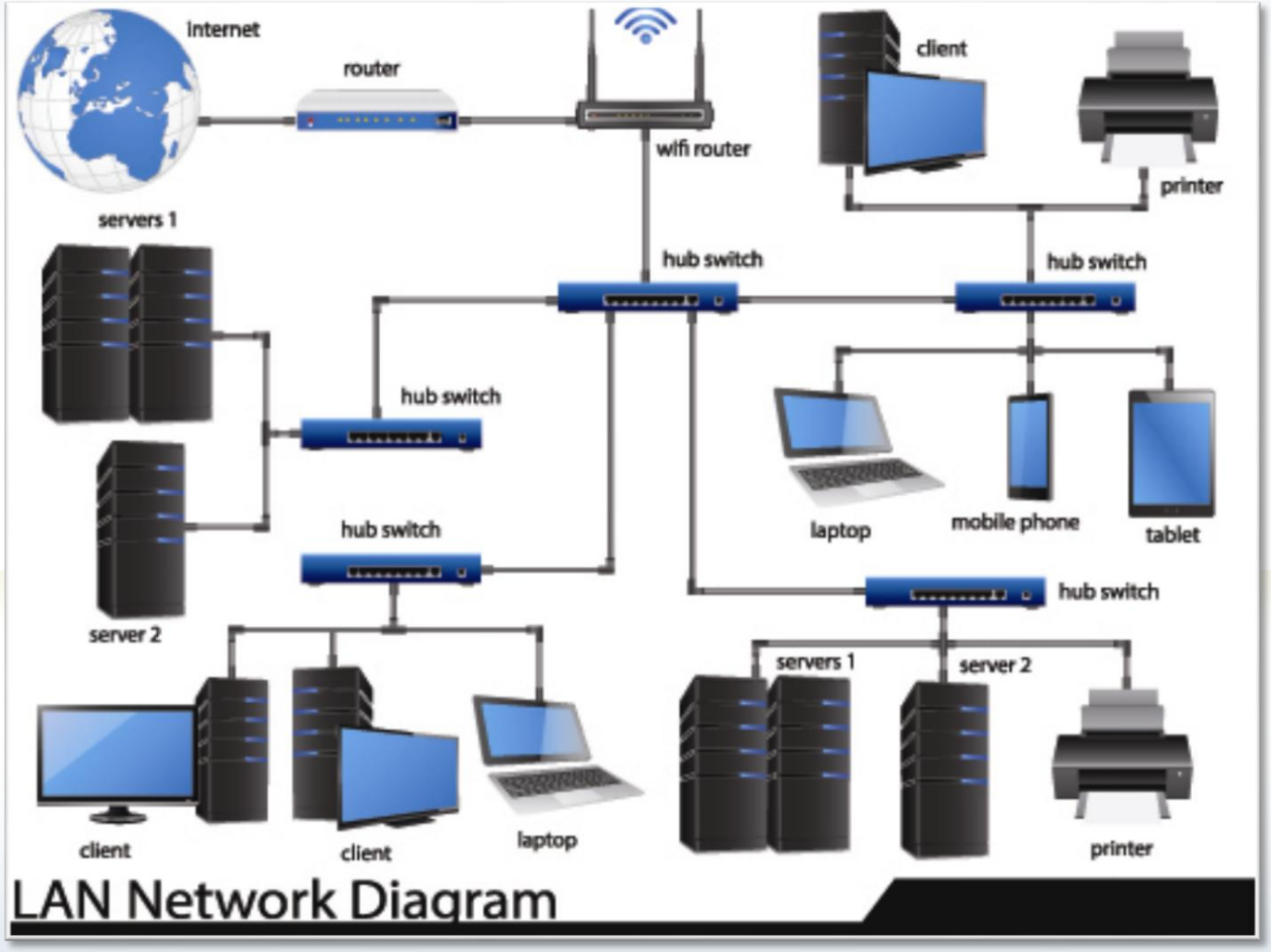
Roles of Network Devices

Firewalls



Roles of Network Devices

Routers and Switches

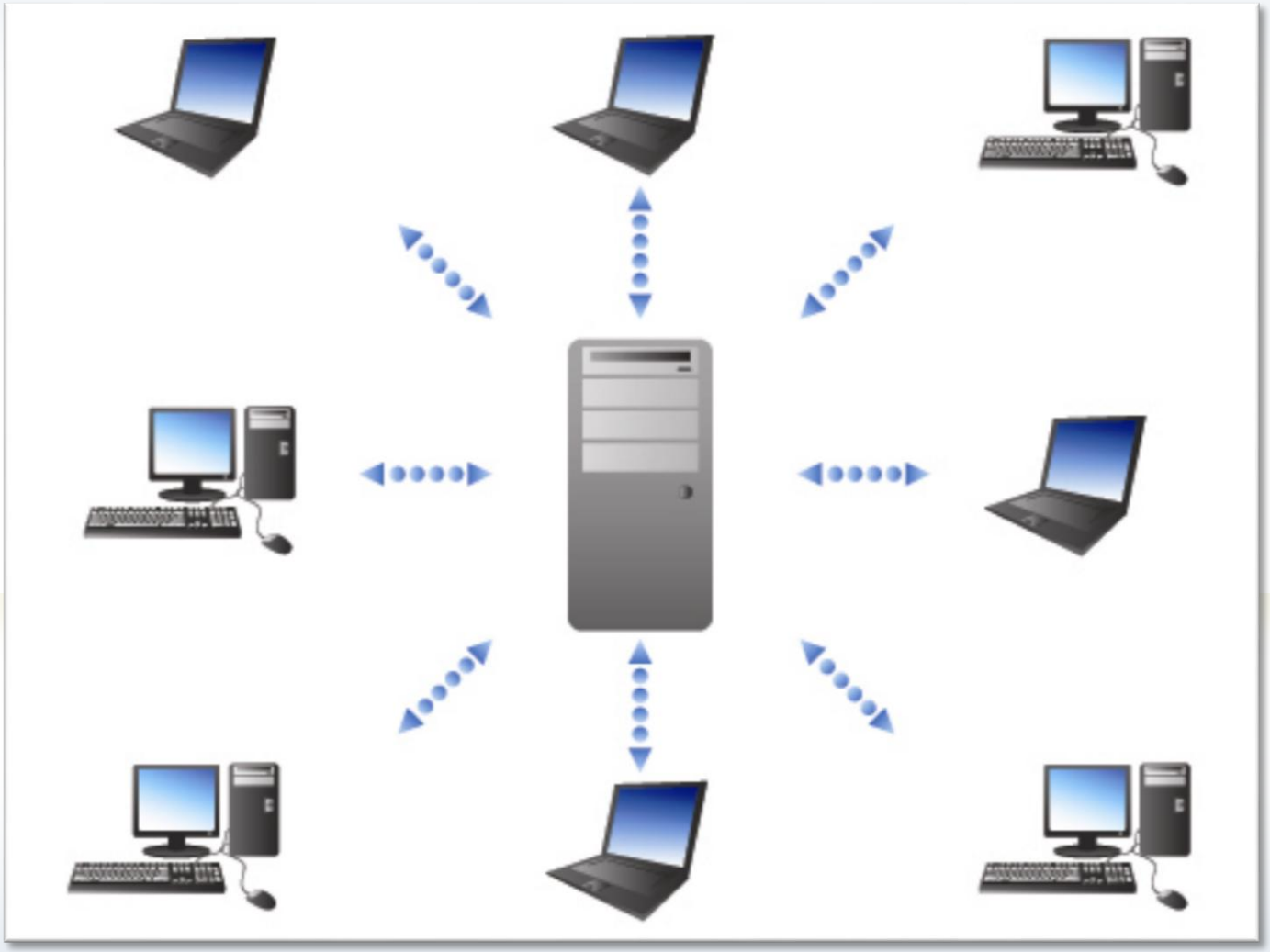


Roles of Network Devices

Load Balancers

Roles of Network Devices

Proxies and Web Security Gateways



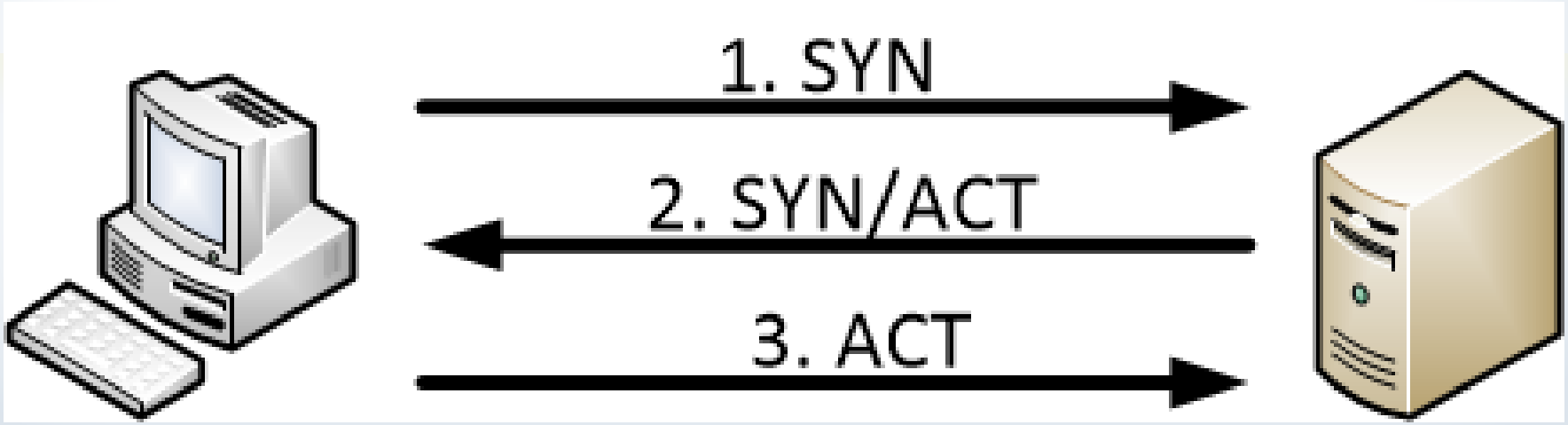
Roles of Network Devices

VPN Concentrators

Roles of Network Devices

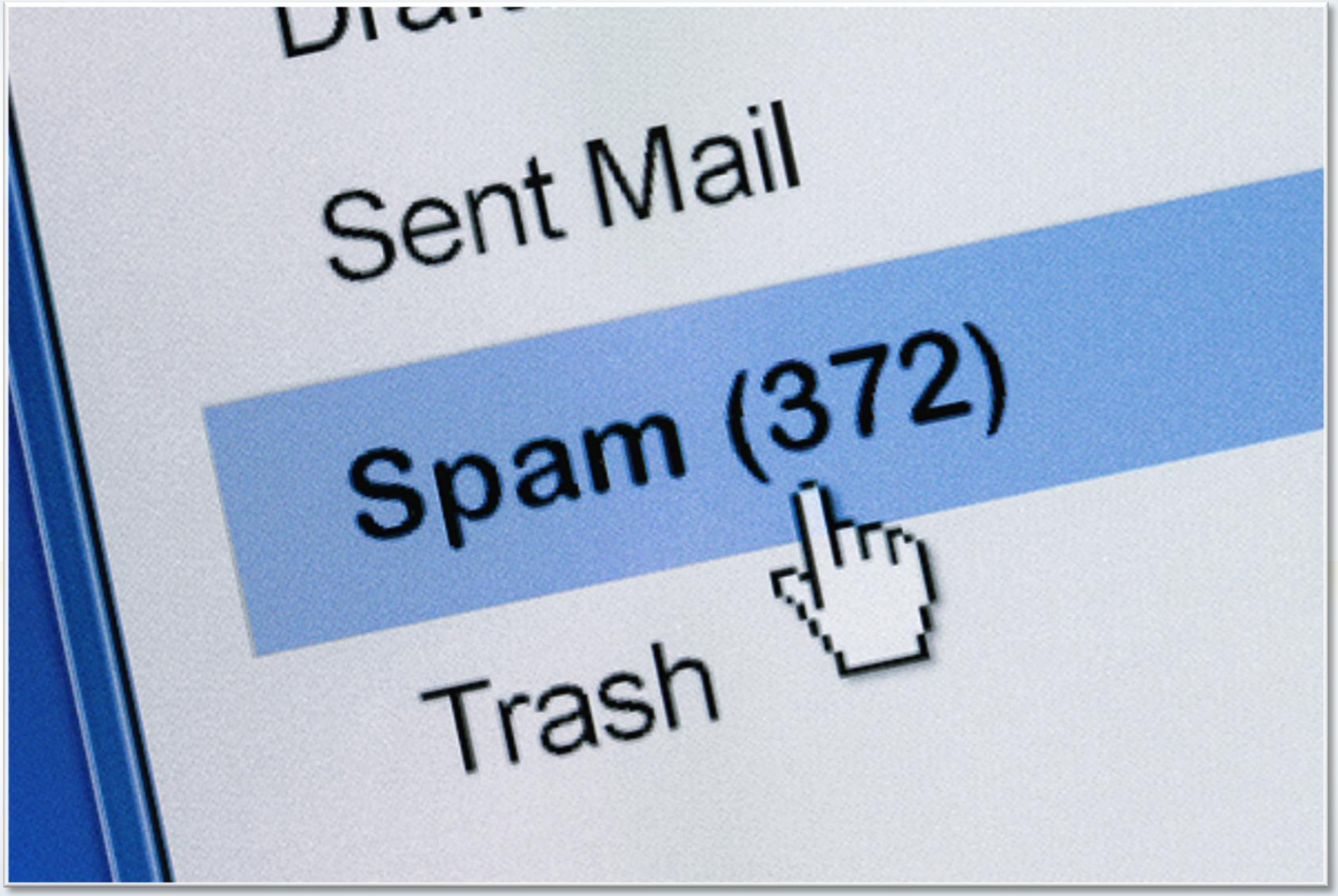
NIDS and NIPS

- Behavior based
- Signature based
- Anomaly based
- Heuristic



Roles of Network Devices

SPAM Filter



Roles of Network Devices

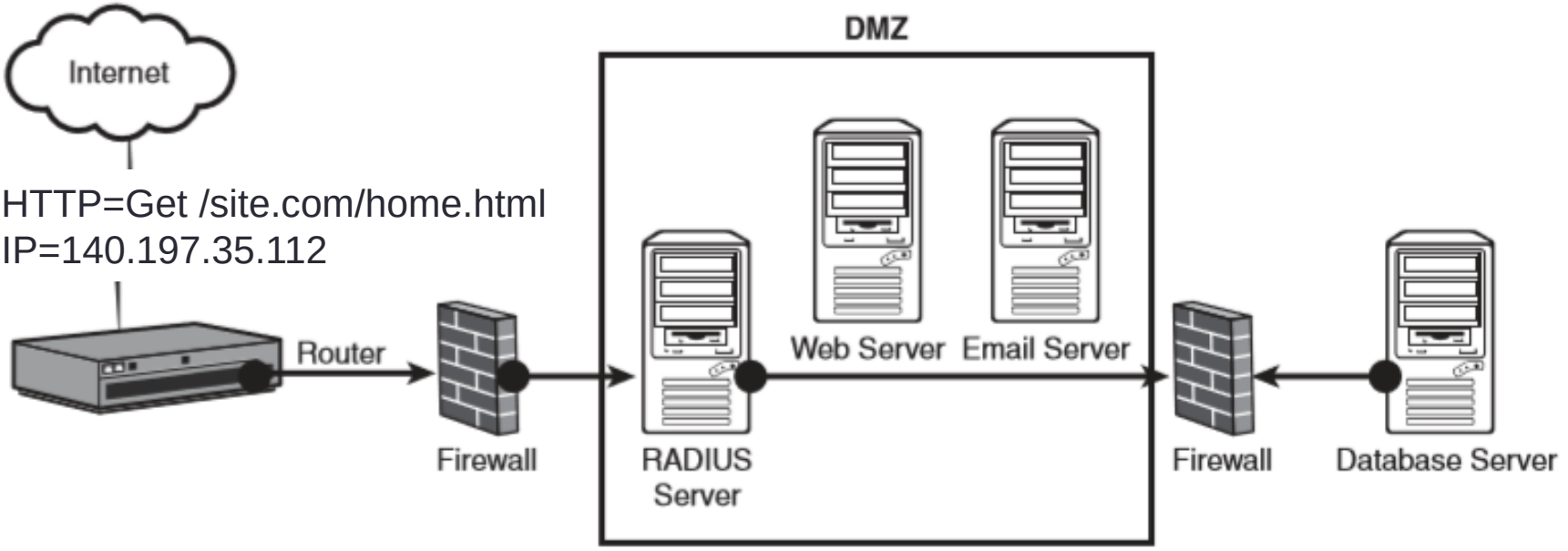
UTM Security Appliances

- URL filter
- Content inspection
-
- Malware inspection

Roles of Network Devices

Web Application Firewall vs. Network Firewall

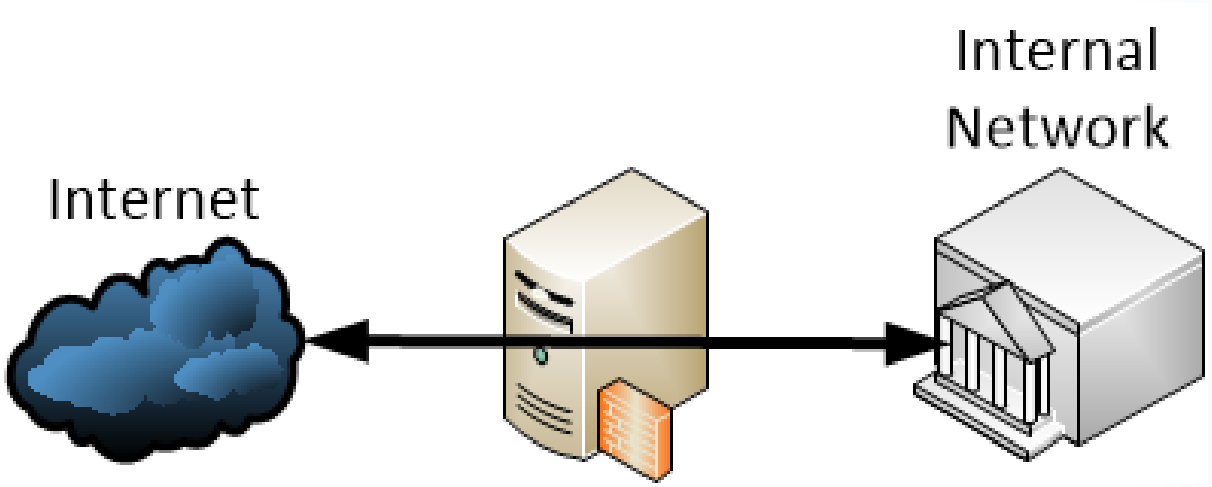
Layer 7: HTTP=Get /site.com/home.html
Layer 3: IP=140.197.35.112



Roles of Network Devices

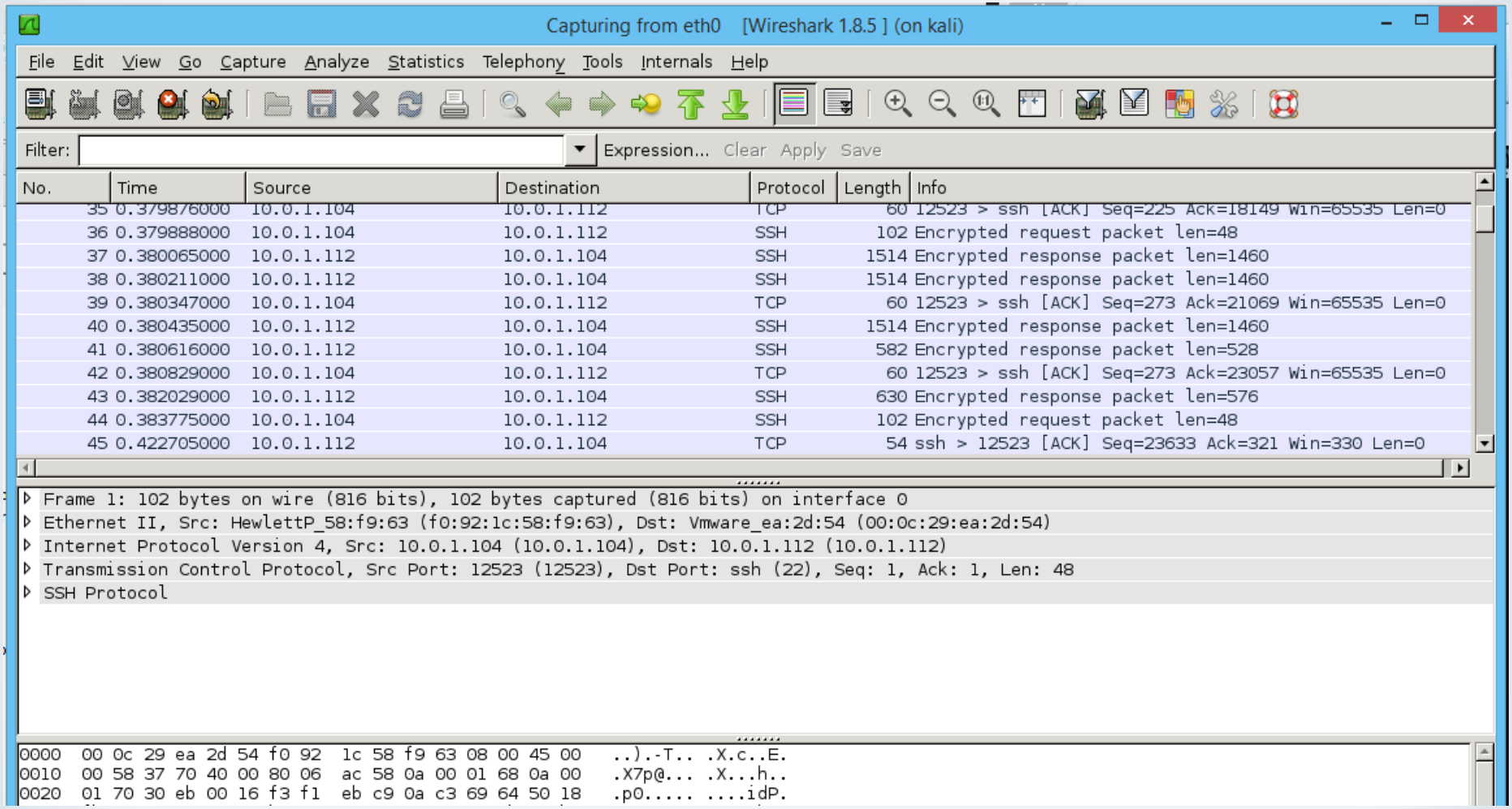
Application Aware Devices

- Firewalls
- IPS
- IDS
- Proxie



Roles of Network Devices

Protocol Analyzers



Demonstration

Wireshark

Secure Network Principles

HYBRID TECHNOLOGY TRAINING
PRINCE GEORGE'S COMMUNITY COLLEGE

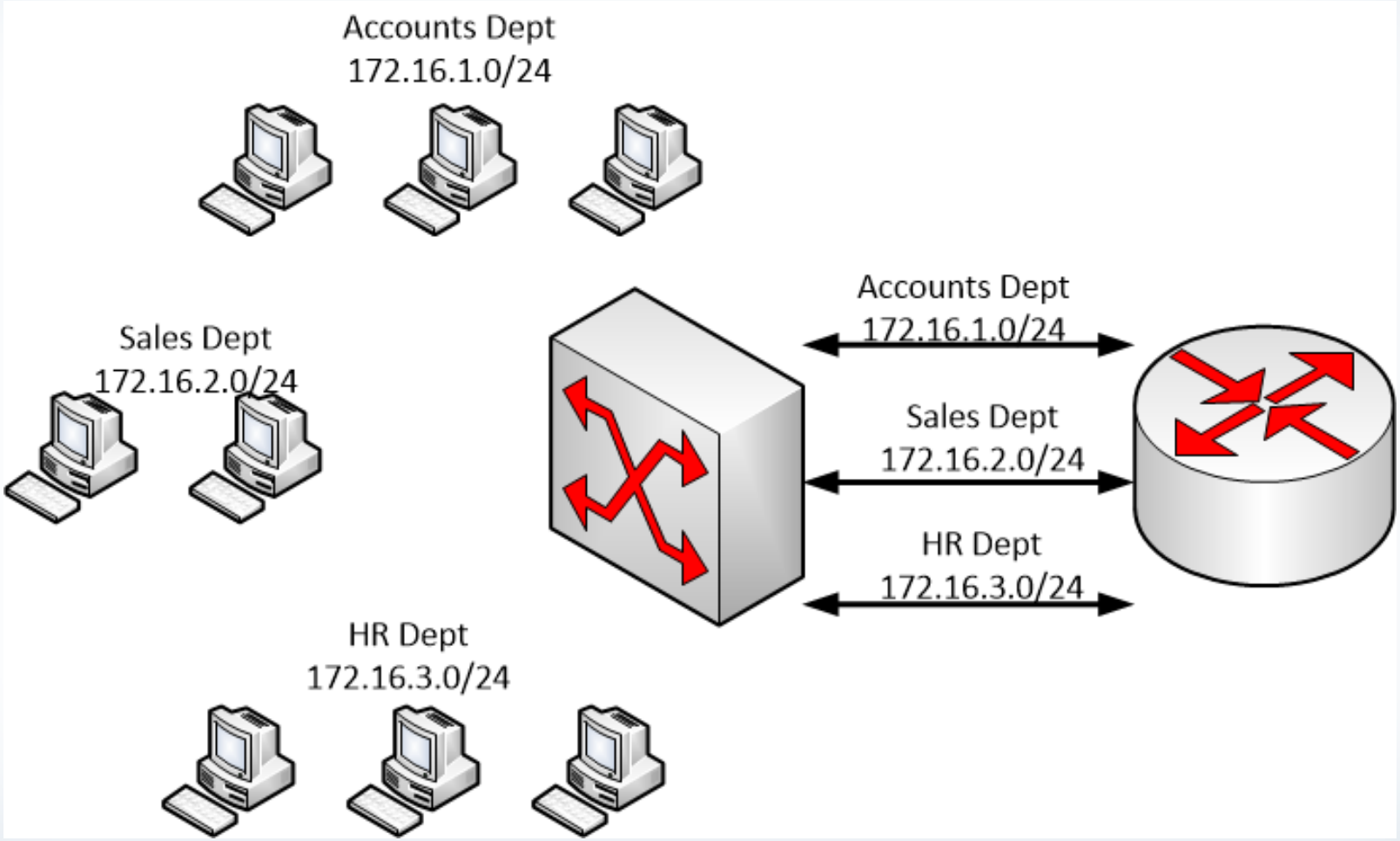
Rule-based Management & Firewall Rules

Add | Edit | Remove | Activate | Inactivate | Move

Status	Priority	From	To	Schedule	User	IPv4 Source	IPv4 Destination	Service	Access	Log
	1	any	any (Excluding ...	none	any	Max_IP	any	FTP	allow	log alert
	2	WAN	DMZ	none	any	any	any	IRC_TCP	allow	log alert
	3	WAN	DMZ	none	any	any	any	SSH_TCP	allow	log alert
	4	WAN	DMZ	none	any	any	any	HTTP	allow	log alert
	5	TUNNEL	any (Excluding ...	none	any	Public_IP_0	any	L2TP-UDP	allow	log
	6	WAN	any (Excluding ...	none	any	Public_IP_0	any	VPN_IPSEC	allow	log
	7	LAN1	any (Excluding ...	none	any	any	any	any	allow	no
	8	LAN2	any (Excluding ...	none	any	any	any	any	allow	no
	9	DMZ	WAN	none	any	any	any	any	allow	no
	10	IPSec_VPN	any (Excluding ...	none	any	any	any	any	allow	no
	11	SSL_VPN	any (Excluding ...	none	any	any	any	any	allow	no
	12	TUNNEL	any (Excluding ...	none	any	any	any	any	allow	no
	13	LAN1	ZyWALL	none	any	any	any	any	allow	no

Secure Network Principles

VLAN Management

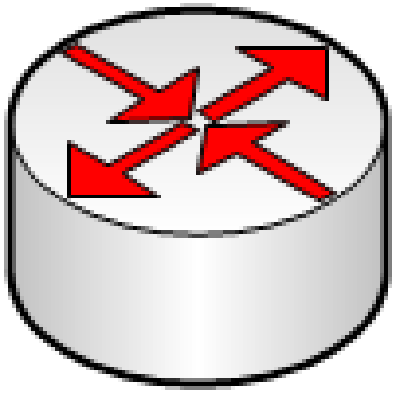


Secure Network Principles

Secure Router Configuration & Access Control Lists

```
R1#sh run
Building configuration...

Current configuration : 633 bytes
!
version 12.2
service password-encryption
!
hostname R1
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 --More--
```



Secure Network Principles

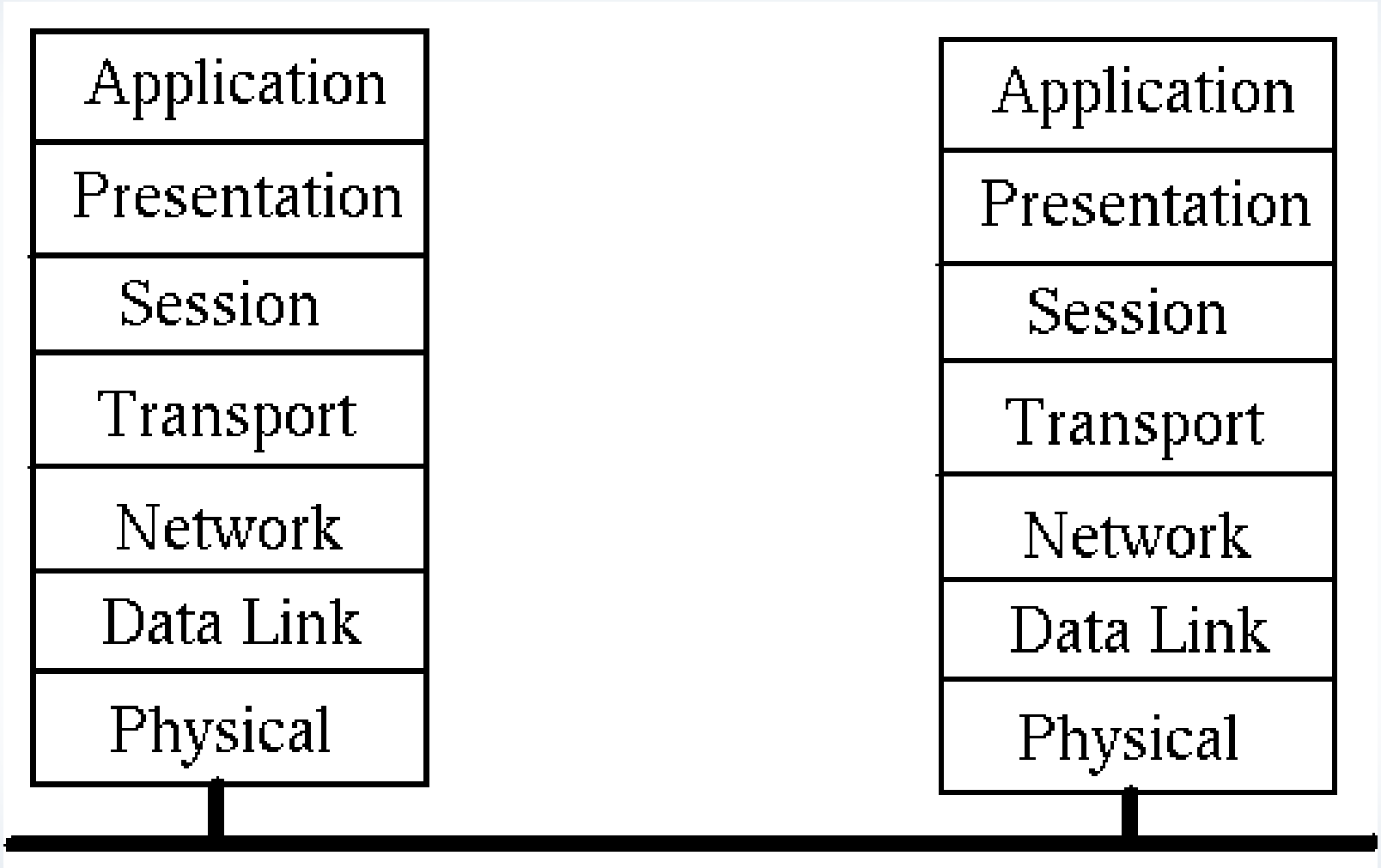
Port Security and 802.1x

Secure Network Principles

- Flood guards
- Loop protection
- Implicit deny
- Network separation
- Log analysis
- Unified Threat Management

Secure Network Principles

OSI Model – Secure Networking



THANK YOU