

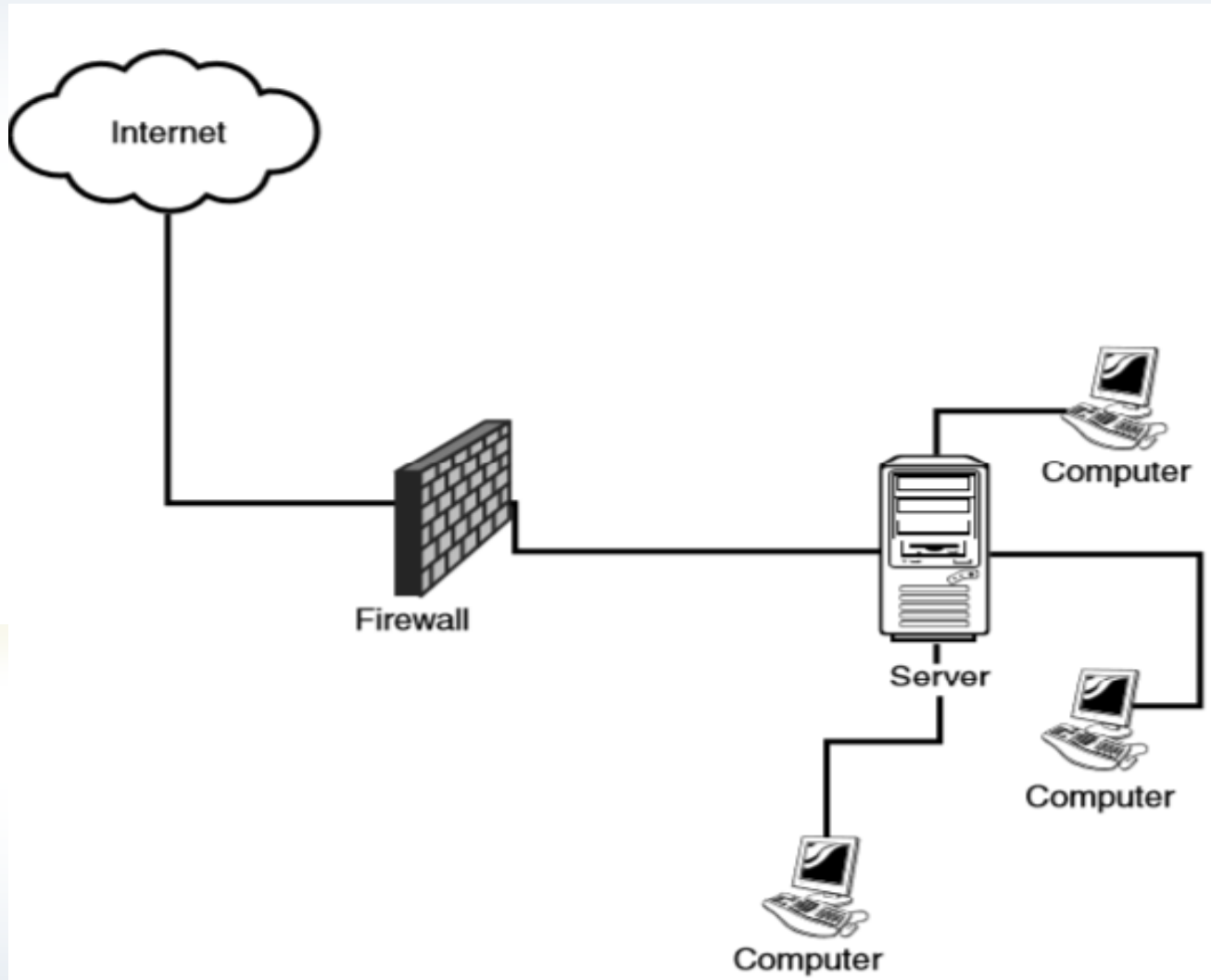
COURSE: SECURITY+ SY0-401

MODULE 1: NETWORK SECURITY

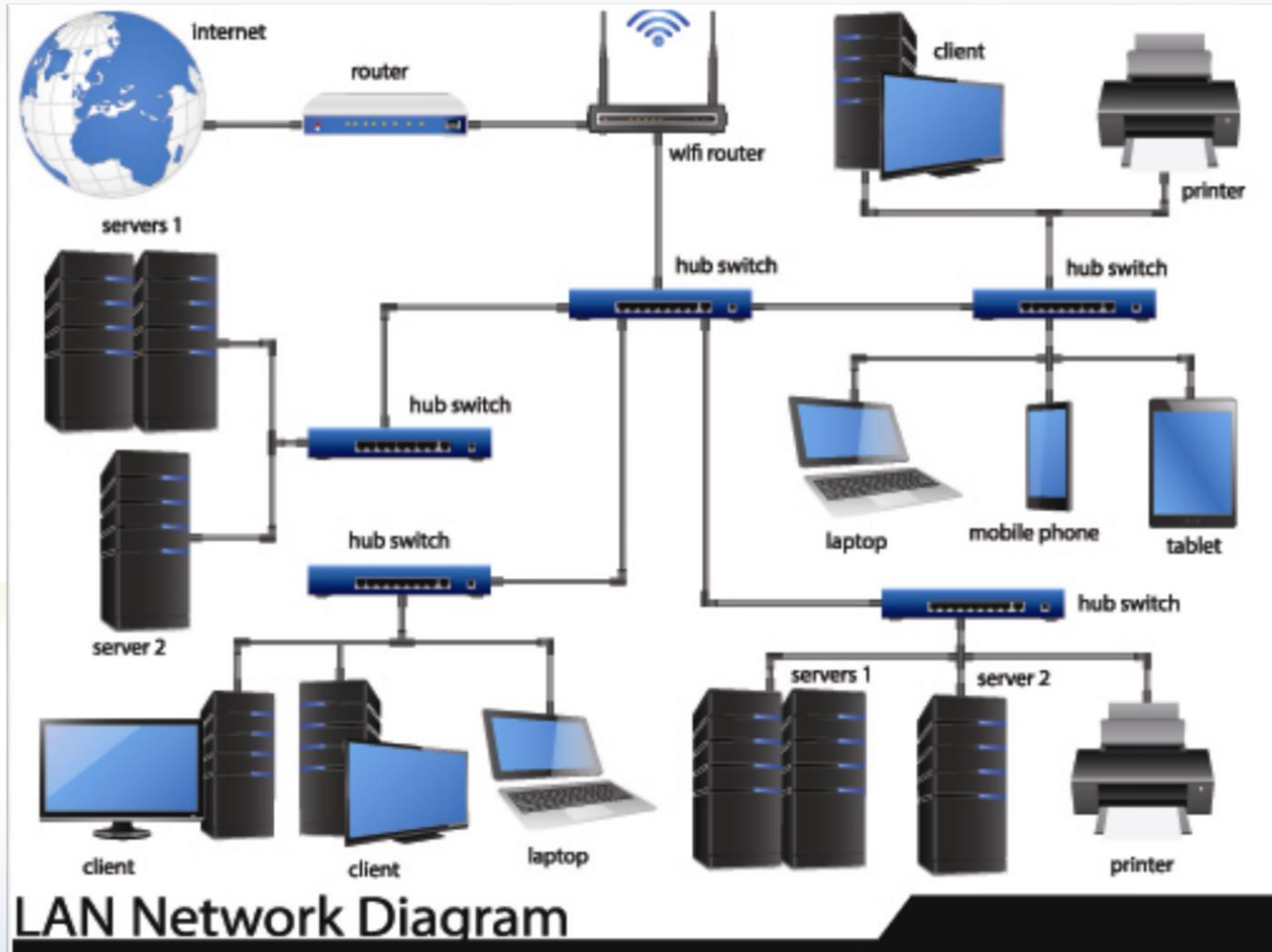
Part A

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

Firewalls



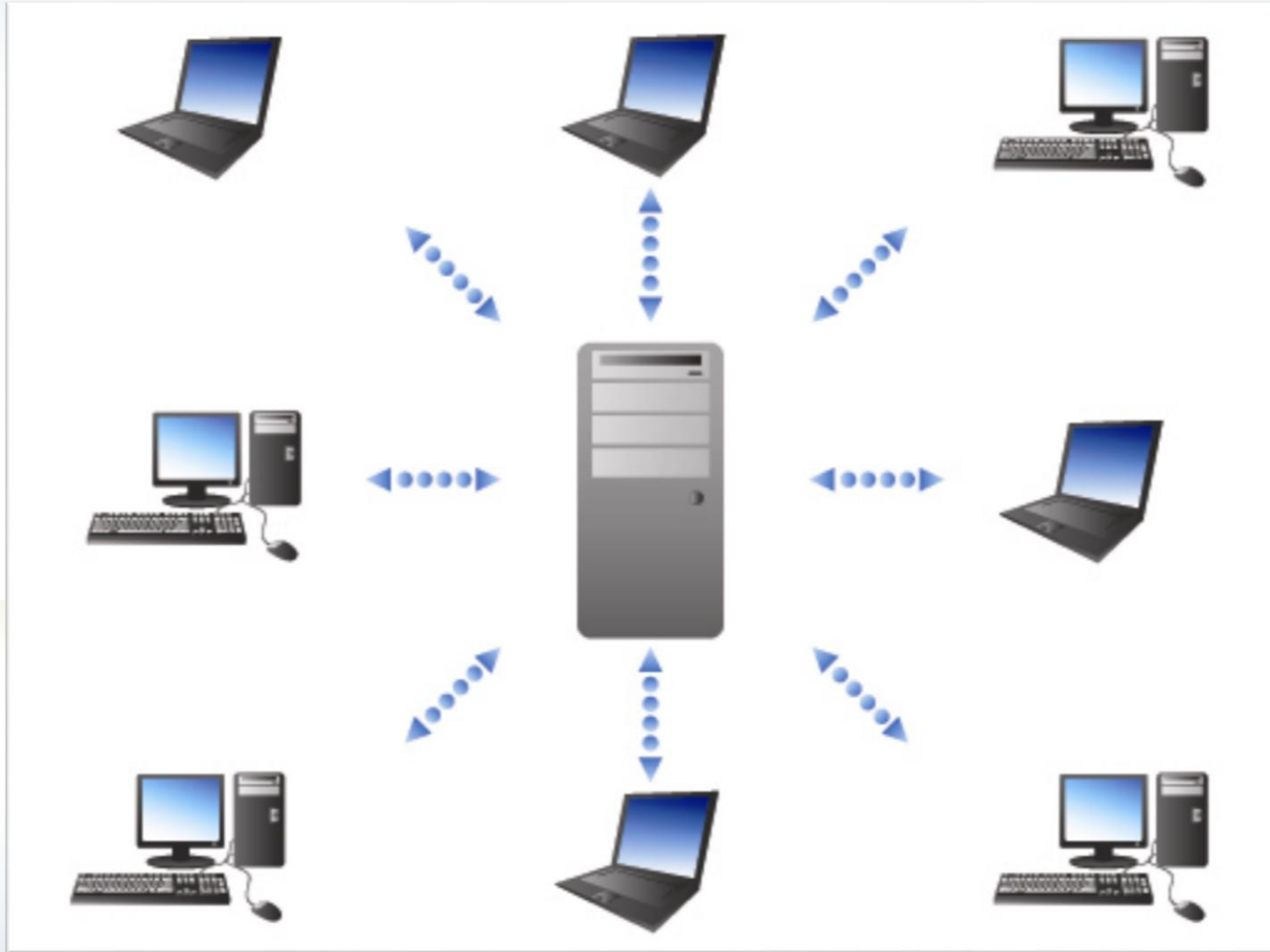
Routers and Switches



Load Balancers



Proxies and Web Security Gateways

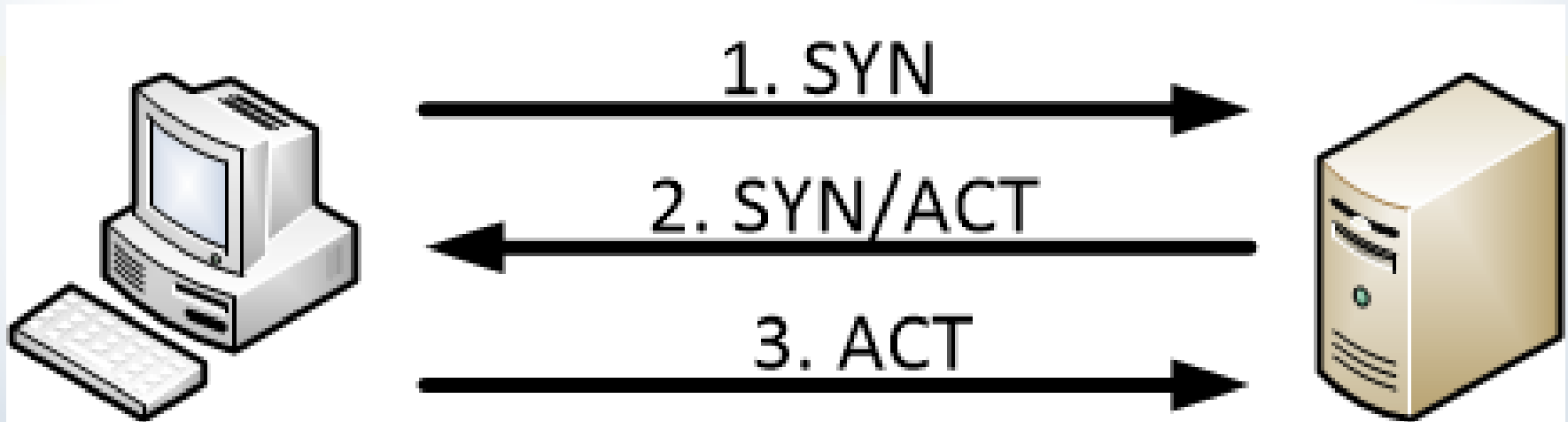


VPN Concentrators

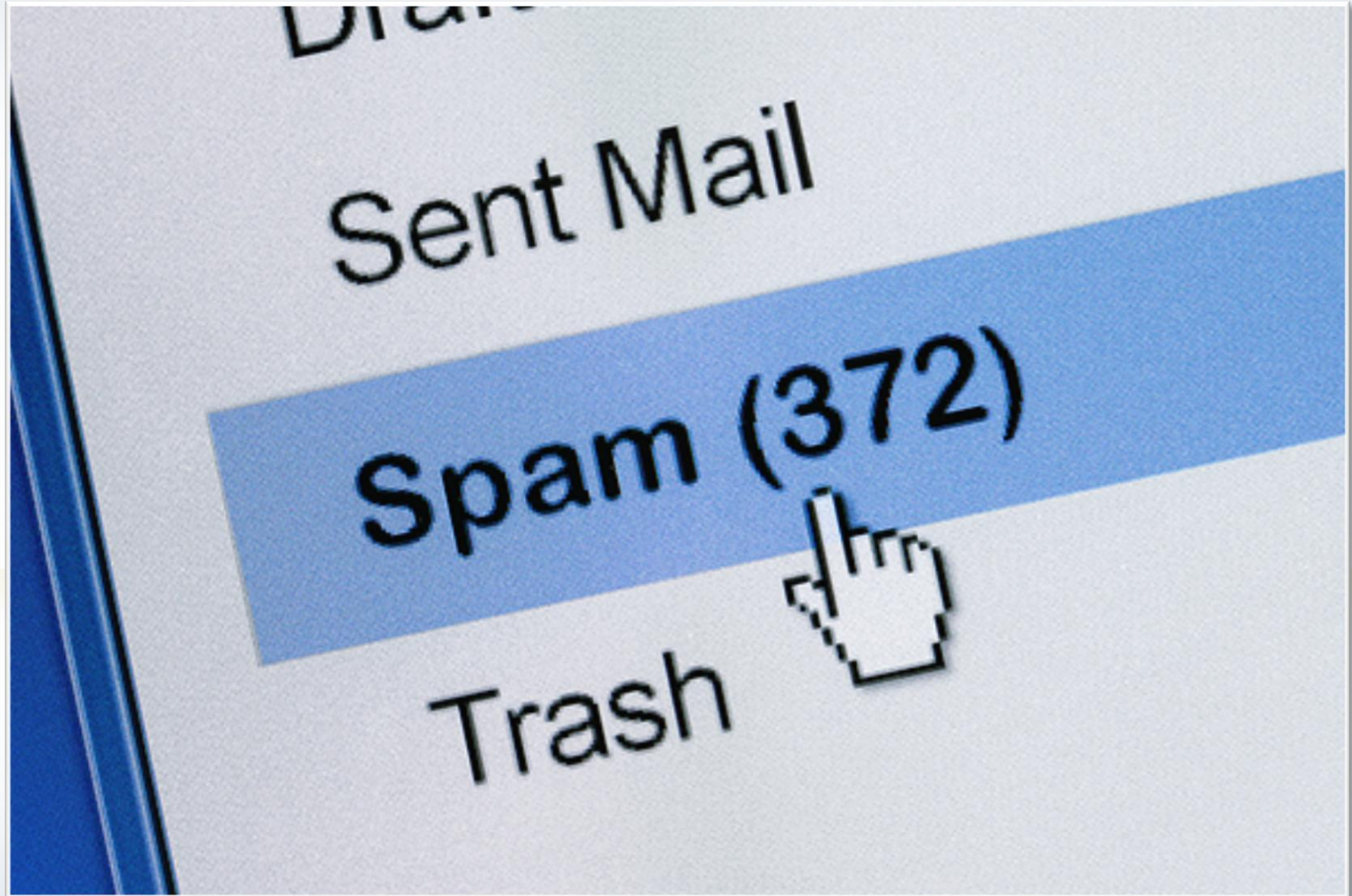


NIDS and NIPS

- Behavior based
- Signature based
- Anomaly based
- Heuristic



SPAM Filter

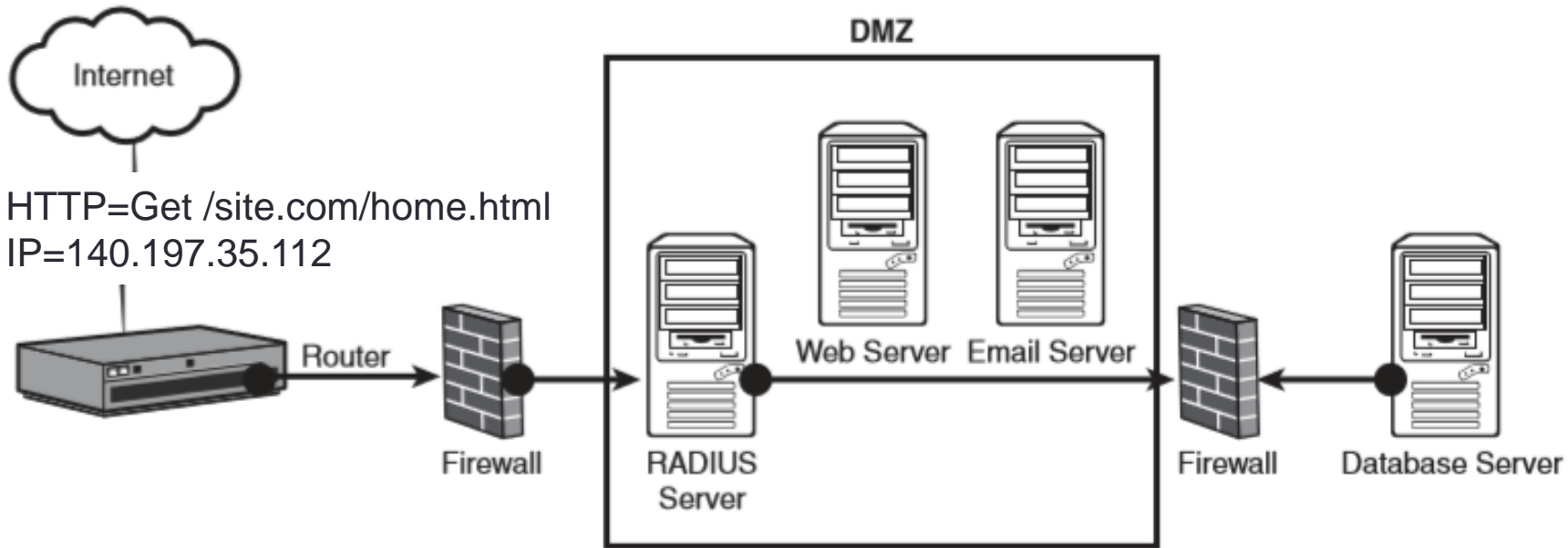


UTM Security Appliances

- URL filter
- Content inspection
-
- Malware inspection

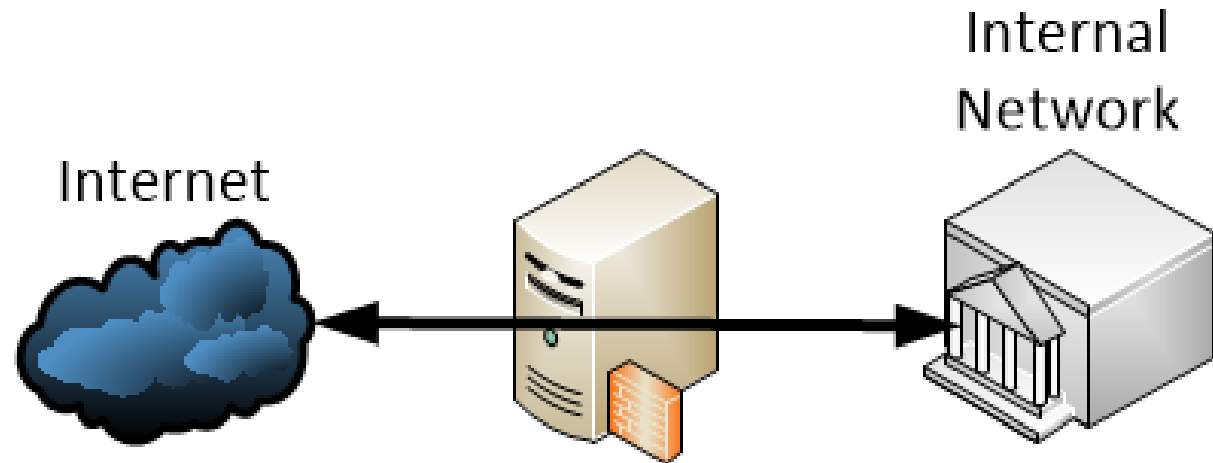


Web Application Firewall vs. Network Firewall



Application Aware Devices

- Firewalls
- IPS
- IDS
- Proxy



Protocol Analyzers

Capturing from eth0 [Wireshark 1.8.5] (on kali)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
35	0.379876000	10.0.1.104	10.0.1.112	TCP	60	12523 > ssh [ACK] Seq=225 Ack=18149 Win=65535 Len=0
36	0.379888000	10.0.1.104	10.0.1.112	SSH	102	Encrypted request packet len=48
37	0.380065000	10.0.1.112	10.0.1.104	SSH	1514	Encrypted response packet len=1460
38	0.380211000	10.0.1.112	10.0.1.104	SSH	1514	Encrypted response packet len=1460
39	0.380347000	10.0.1.104	10.0.1.112	TCP	60	12523 > ssh [ACK] Seq=273 Ack=21069 Win=65535 Len=0
40	0.380435000	10.0.1.112	10.0.1.104	SSH	1514	Encrypted response packet len=1460
41	0.380616000	10.0.1.112	10.0.1.104	SSH	582	Encrypted response packet len=528
42	0.380829000	10.0.1.104	10.0.1.112	TCP	60	12523 > ssh [ACK] Seq=273 Ack=23057 Win=65535 Len=0
43	0.382029000	10.0.1.112	10.0.1.104	SSH	630	Encrypted response packet len=576
44	0.383775000	10.0.1.104	10.0.1.112	SSH	102	Encrypted request packet len=48
45	0.422705000	10.0.1.112	10.0.1.104	TCP	54	ssh > 12523 [ACK] Seq=23633 Ack=321 Win=330 Len=0

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0

- Ethernet II, Src: HewlettP_58:f9:63 (f0:92:1c:58:f9:63), Dst: Vmware_ea:2d:54 (00:0c:29:ea:2d:54)
- Internet Protocol Version 4, Src: 10.0.1.104 (10.0.1.104), Dst: 10.0.1.112 (10.0.1.112)
- Transmission Control Protocol, Src Port: 12523 (12523), Dst Port: ssh (22), Seq: 1, Ack: 1, Len: 48
- SSH Protocol

```
0000 00 0c 29 ea 2d 54 f0 92 1c 58 f9 63 08 00 45 00  ..)..-T.. .X.c...E.
0010 00 58 37 70 40 00 80 06 ac 58 0a 00 01 68 0a 00  .X7p@... .X...h..
0020 01 70 30 eb 00 16 f3 f1 eb c9 0a c3 69 64 50 18  .p0..... ....idP.
```

Demonstration

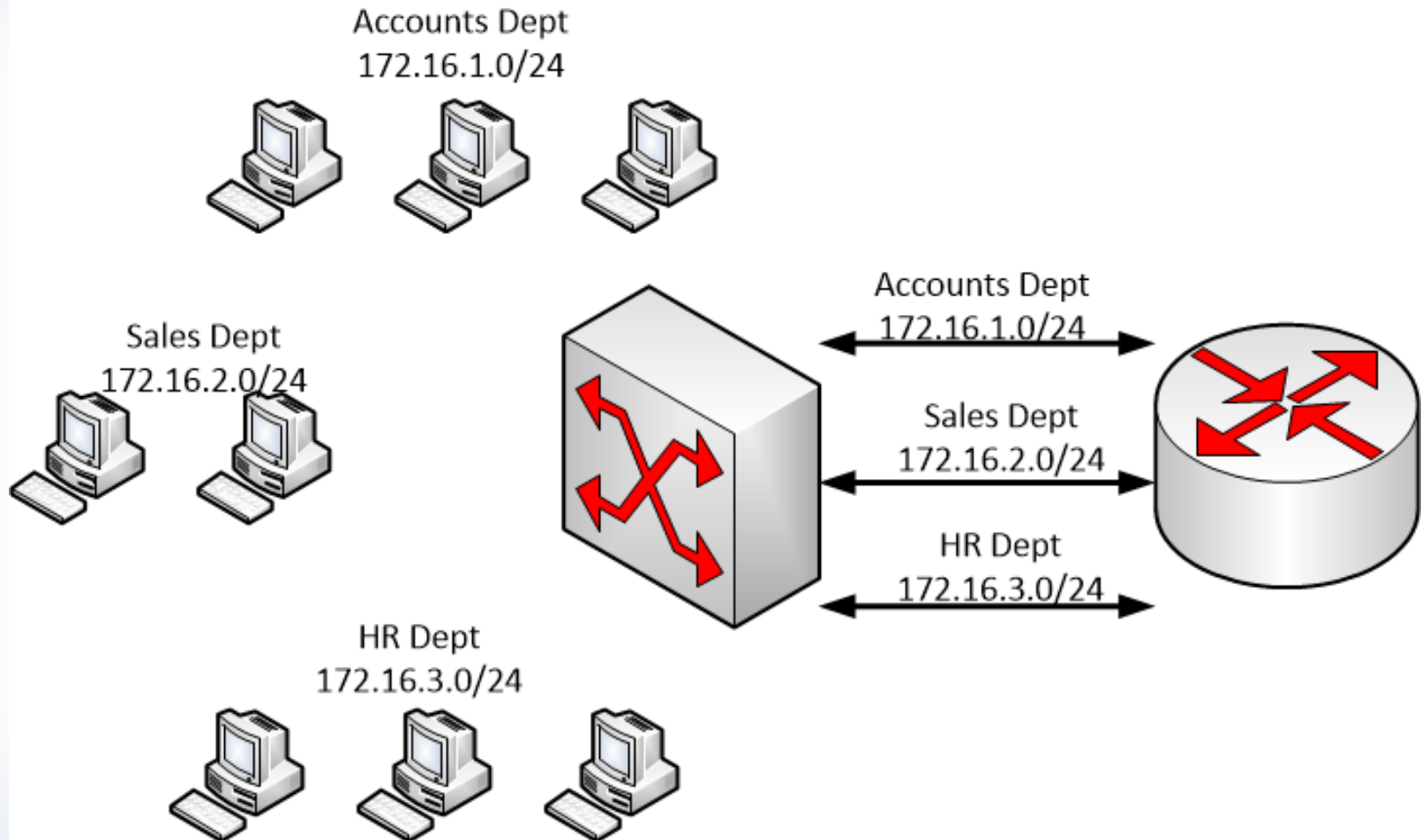
Wireshark

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

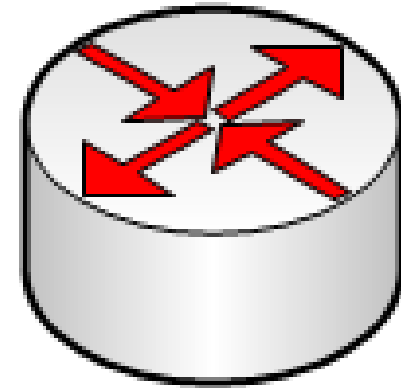
VLAN Management



Secure Router Configuration & Access Control Lists

```
RT1>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--
```

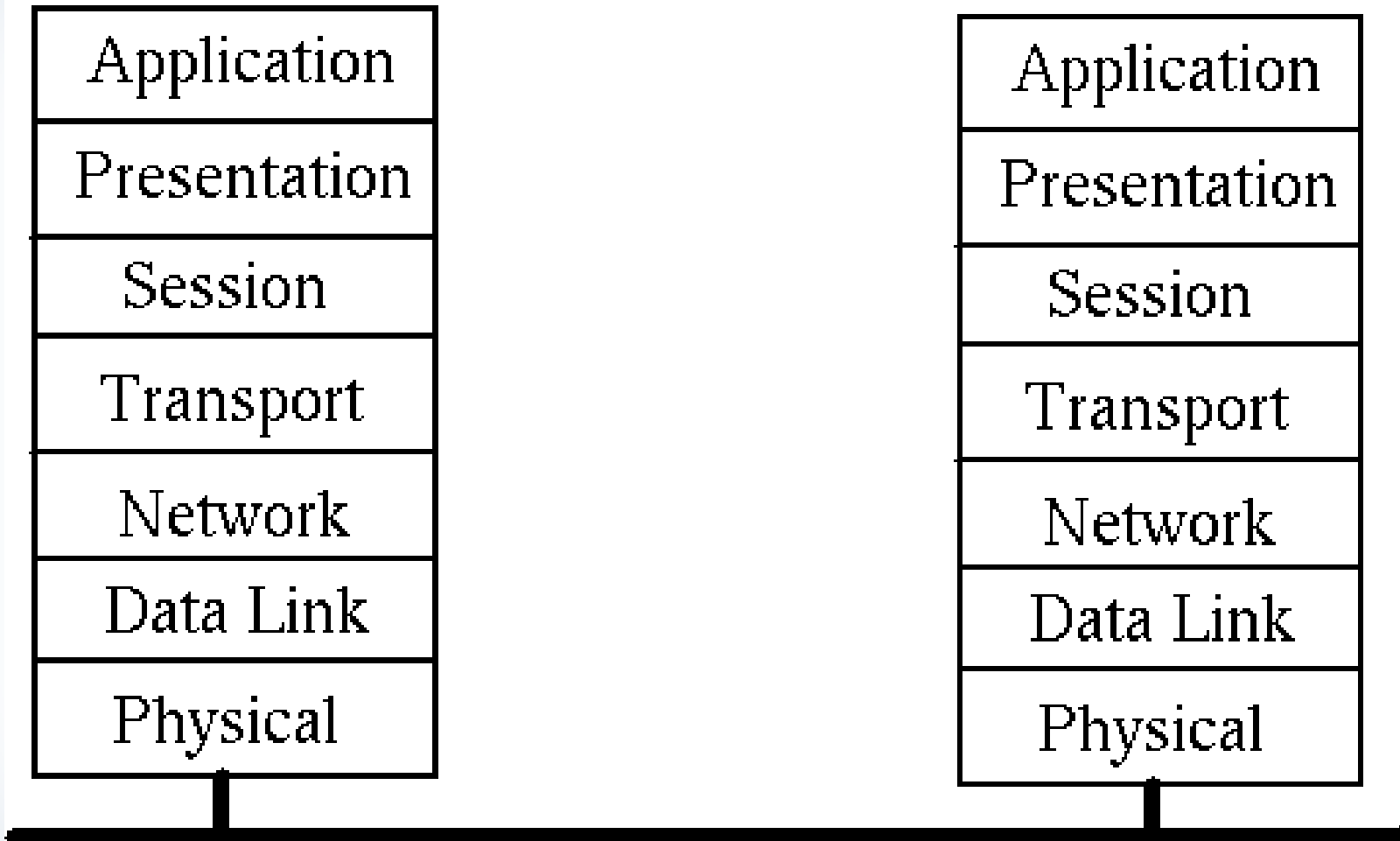


Port Security and 802.1x



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

OSI Model – Secure Networking





THANK YOU
