ACS-2821-001
Information Security in Business

Telecommunications, Network, and Internet Security

ACS-2821-001 – Slides Used In The Course

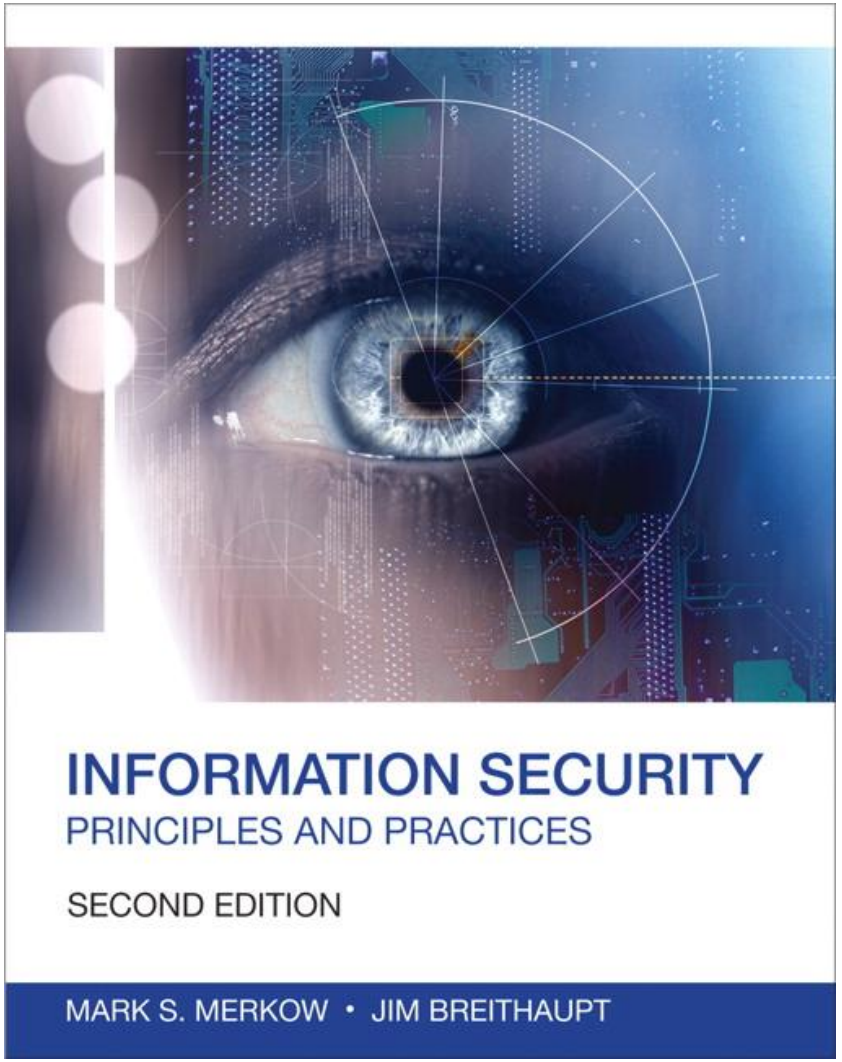
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Classify the International Standards Organization/Open Systems Interconnection (ISO/OSI) layers and characteristics
- Summarize the fundamentals of communications and network security and their vulnerabilities
- Analyze the Transmission Control Protocol/Internet Protocol (TCP/IP)
- Distinguish among wide area networks (WANs), local area networks (LANs), and the Internet, intranets, and extranets
- Outline the roles of packet-filtering routers, firewalls, and intrusion detection/prevention technology in network perimeter security
- Classify the various configurations and architectures for firewalls
- Illustrate the elements of IP security (IPsec) and how virtual private networks implement IPsec

Overview

- Information security practitioners must be aware of the risk of computer security incidents from the Internet and the steps they can take to secure public and private sites

Network and Telecommunications Security

Telecommunications, network, and Internet security is one of the largest domains in the Common Body of Knowledge (CISSP)

- Topics include
  - OSI model
  - TCP/IP protocol
  - Security services
  - Network types
  - Network security devices
  - VPNs

Network Security in Context

- **Confidentiality**
  - Touches upon the topics of network authentication and data encryption
- **Integrity**
  - Protects data from unauthorized or accidental modification through the use of firewalls, cryptography, and intrusion detection tools
- **Availability**
  - Involves sound disaster recovery planning procedures based on an accepted business continuity plan

Open Systems Interconnection (OSI) Reference Model

- A model for network communications developed by OSI in the early 1980s
- Consists of seven layers
  - Each layer has a different function and different protocols operate at each layer
  - Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, Physical Layer
  - To help remember the name of the different layers:
    - From Bottom to Up
      - ***P**lease **D**o **N**ot **T**hrow **S**alami **P**izza **A**way*
    - From top to bottom
      - ***A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing*

The seven layers are as follows:

- Application layer
  - Provides application services, such as file transfer and resource allocation
  - Emails, discussion groups, and the world wide web reside at this layer
- Presentation Layer
  - Performs data formatting such as encryption, decryption and data translation
- Session Layer
  - Establishes and manages connections between computers

Open Systems Interconnection (OSI) Reference Model

- Transport Layer
  - Manages the transfer of data
  - TCP and UDP are two protocols operating at this layer
- Network Layer
  - Manages addressing and routing the packets
  - IP operates at this layer
- Data Link Layer
  - Handles data transfer across the network medium
- Physical Layer
  - Transmits the actual bits across the physical medium

OSI Reference Model and TCP/IP

- TCP/IP is a collection of protocols developed in the 1970s to build the ARPANET (Today's Internet)
- TCP/IP provides universal connectivity across the Internet offering reliable delivery
- It has four or five (depend on which book you are reading) layers as oppose to the seven in the OSI Reference Model
- Application Layer, Transport Layer, Internet Layer (Network Layer), Network Access Layer (Data Link Layer and Physical layer)
- Primary applications using TCP/IP
  - File Transfer Protocol (FTP)
  - Remote login (Telnet)
  - Electronic mail or Simple Mail Transfer Protocol (SMTP)

The four layers are as follows:

- Application layer
  - Provides applications with standardized data exchange
  - For example - Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP)
- Transport Layer
  - Is responsible for maintaining end-to-end communications across the network
  - Example – Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

- Internet Layer (or Network Layer)
  - Deals with packets and connects independent networks to transport the packets across network boundaries.Establishes and manages connections between computers
  - Example - Internet Protocol (IP) and the Internet Control Message Protocol (ICMP)
- Network Access Layer (or Physical Layer)
  - This layer sometime are split into two layers - the Data Link Layer and the Physical Layer
  - Here we will treat them as one layer
  - The network component that interconnects nodes or hosts in the network
  - Example – Address Resolution Protocol (ARP), Ethernet

OSI Reference Model and TCP/IP

OSI Layer	TCP/IP Layer		TCP/IP Protocol Examples
Application	Application		NFS, NIS +, RIP, SNMP, SMTP, HTTP, HTTPS, DNS, DHCP, ftp, telnet …
Presentation			
Session			
Transport	Transport (Host-to host)		TCP, UDP
Network	Internet (Network)		IP, IPsec, ICMP, IGMP
Data Link	Network Access	Data Link	PPP, IEEE 802.2, ARP
Physical		Physical	Ethernet (IEEE 802.3) Token Ring, RS-232

TCP/IP Stack – Wireshark Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	3.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	3.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A gaia.cs.umass.edu
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PE
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

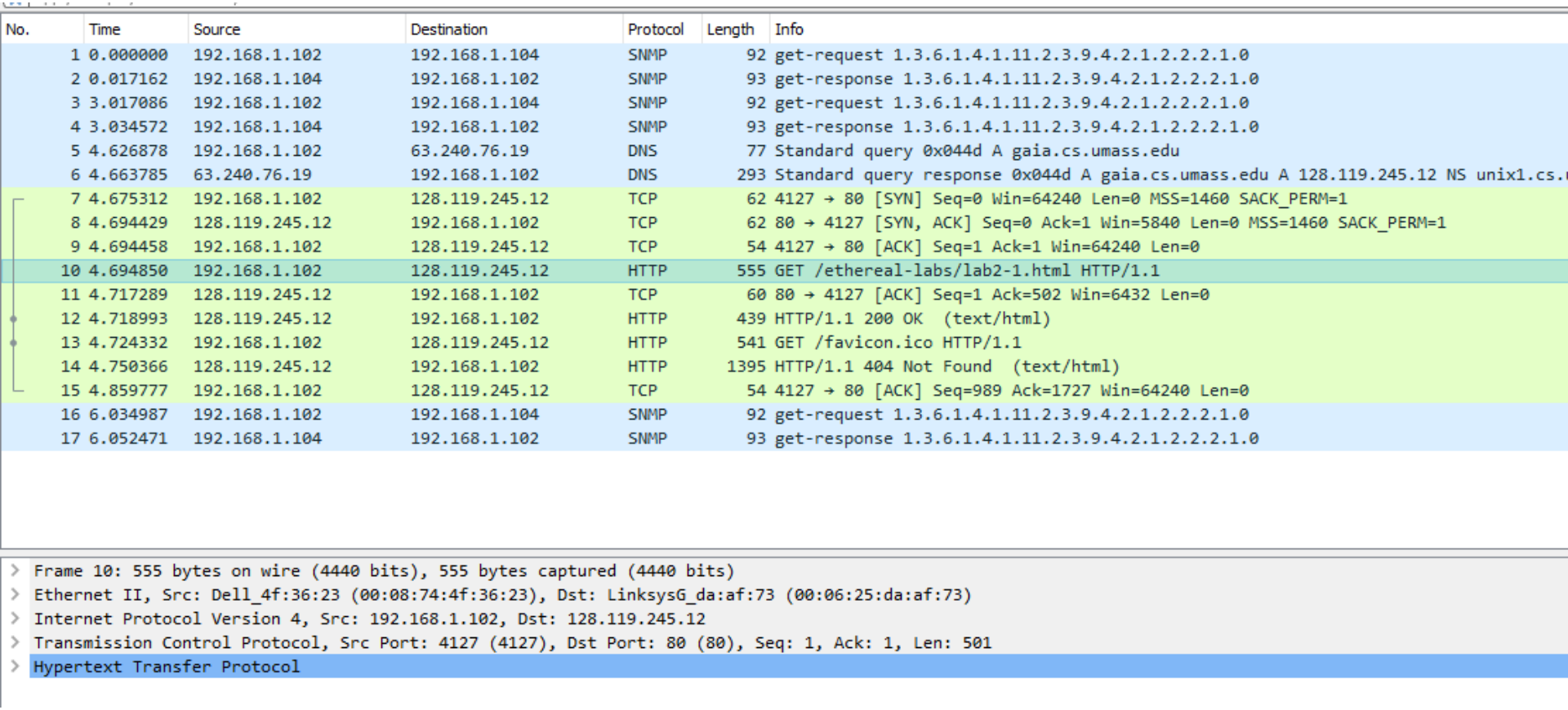
```
> Frame 5: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 63.240.76.19
> User Datagram Protocol, Src Port: 1026 (1026), Dst Port: 53 (53)
> Domain Name System (query)
```

TCP/IP Stack – Wireshark Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	3.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	3.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A gaia.cs.umass.edu
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 NS unix
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

```
> Frame 6: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 63.240.76.19, Dst: 192.168.1.102
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 1026 (1026)
> Domain Name System (response)
```

TCP/IP Stack – Wireshark Capture



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	3.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	3.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A gaia.cs.umass.edu
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 NS unix1.cs.
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

```
> Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4127 (4127), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 501
> Hypertext Transfer Protocol
```

TCP/IP Stack – Wireshark Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.2.1.0
3	3.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	3.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A gaia.cs.umass.edu
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 NS unix1.cs.uma
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.2.1.0

```
> Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 4127 (4127), Seq: 1, Ack: 502, Len: 385
> Hypertext Transfer Protocol
v Line-based text data: text/html
    <html>\n
    Congratulations.  You've downloaded the file lab2-1.html!\n
    </html>\n
```

TCP/IP Stack – Wireshark Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
2	0.017162	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
3	3.017086	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
4	3.034572	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
5	4.626878	192.168.1.102	63.240.76.19	DNS	77	Standard query 0x044d A gaia.cs.umass.edu
6	4.663785	63.240.76.19	192.168.1.102	DNS	293	Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 NS u
7	4.675312	192.168.1.102	128.119.245.12	TCP	62	4127 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	4.694429	128.119.245.12	192.168.1.102	TCP	62	80 → 4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	4.694458	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
11	4.717289	128.119.245.12	192.168.1.102	TCP	60	80 → 4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)
15	4.859777	192.168.1.102	128.119.245.12	TCP	54	4127 → 80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
16	6.034987	192.168.1.102	192.168.1.104	SNMP	92	get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
17	6.052471	192.168.1.104	192.168.1.102	SNMP	93	get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

```
> Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 4127 (4127), Seq: 1, Ack: 502, Len: 385
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
    ETag: "1bfed-49-79d5bf00"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 73\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.024143000 seconds]
    [Request in frame: 10]
    [Next request in frame: 13]
```

OSI Model and Security

- Security Services
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Logging and monitoring
- Security Mechanisms
  - Encipherment
  - Digital signature
  - Access control
  - Data integrity
  - Authentication
  - Traffic padding
  - Routing protocol
  - Notarization

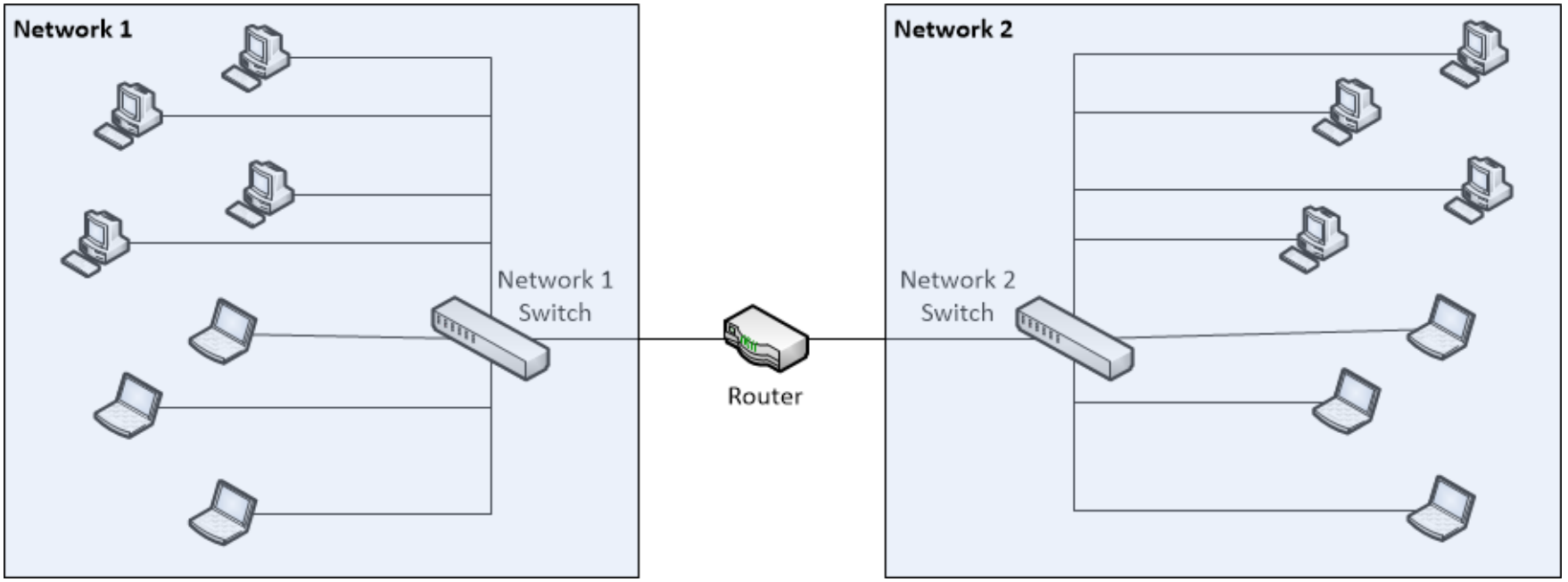
Network Types

- Local Area Network
  - A network configuration designed for a limited space or geographic area such as a series of offices in the same building
  - Two common types of LANs are the campus area network (CAN) and the metropolitan area network (MAN)
- Wide Area Network
  - A group of smaller LANs connected logically or physically
  - WANs can combine other subnetworks such as intranets, extranets, and virtual private networks (VPNs) to provide enhanced network capabilities

Network Types

- Internet
  - The Internet is an interconnection of different-sized networks (LANs) around the world
- Intranet
  - An intranet is a local or wide area network based on TCP/IP but with firewalls that limit the network's access to the Internet
  - An intranet is more secure than the Internet because it has a restricted user community and local control
- Extranet
  - An extranet is an intranet that allows select users outside of the firewalls to access the site

- Router
  - A network traffic management device that, unbeknown to the user, sits between subnetworks (LANs) and routes traffic intended for or leaving the network segments to which it's attached



Firewalls

- Firewalls typically run monitoring software to detect and thwart external attacks on the site and protect the internal corporate network
- Firewalls are an essential device for network security
- Many of the architectures needed for security rely on one or more firewalls within an intelligent design

Firewalls

- Packet Filtering Firewall
  - Packet Filter
    - A simple and effective form of protection that matches all packets against a series of rules
  - There are two types of packet filtering firewall
    - Basic Packet Filtering
      - Allows communication originating from one side of the communication path or the other
      - Identifies and controls traffic by examining the source, destination, port number, and protocol types
    - Stateful Inspection Packet Filtering
      - A more complex packet-filtering technology that keeps track of the state of the current connection to help assure that only desired traffic passes through

Firewalls

- Benefits of Packet-Filtering Firewall
  - Little or no cost to implement because packet filtering is a feature of standard routers
  - Little impact on router performance
  - Generally transparent to users and applications

Firewalls

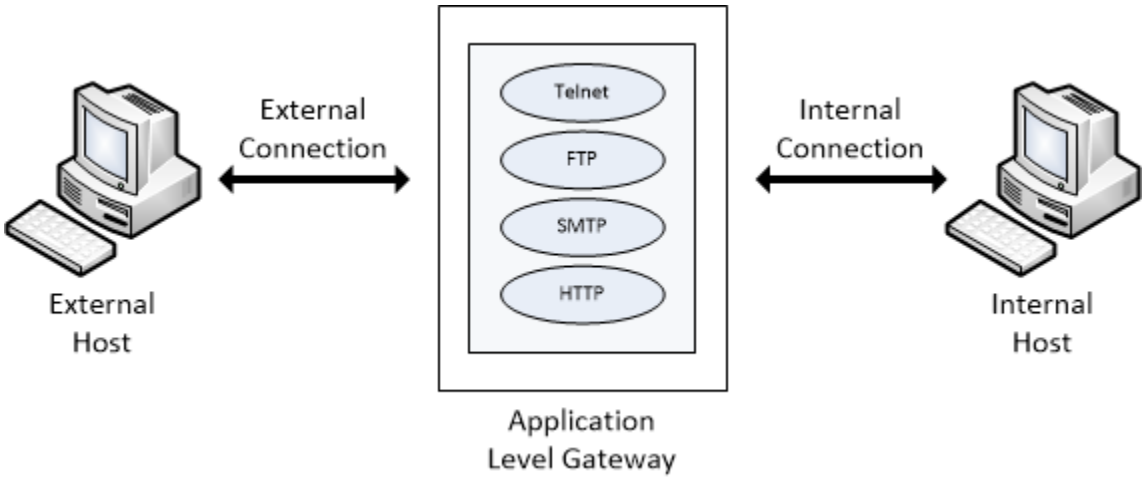
- Limitations of Packet-Filtering Firewall
  - Defining packet filters can be a complex task
  - The filtering rule set can become complicated, increasing in difficulty to manage and comprehend
  - There are few testing facilities to verify the correctness of the filtering rules
  - The packet throughput of a router decreases as the number of filters increase
  - It is not capable of understanding the context/data of a particular service

Firewalls

- Application-Level Gateway Firewall/Firewall/Proxy
  - Allows the network administrator to implement stricter security policies than packet-filtering routers can manage
  - Requires special-purpose code (a proxy service) for each desired application
  - The proxy code can be configured to support only acceptable features of an application
  - Users are permitted access to the proxy services but may not log in to the application-level gateway itself

Firewalls

- Application-Level Gateways/Firewall/Proxy
  - An application-level gateway is often referred to as a bastion host because it is a designated system that is specifically armored and protected against attacks
  - Application-level gateways allow information to flow between systems but do not allow the direct exchange of data



Firewalls

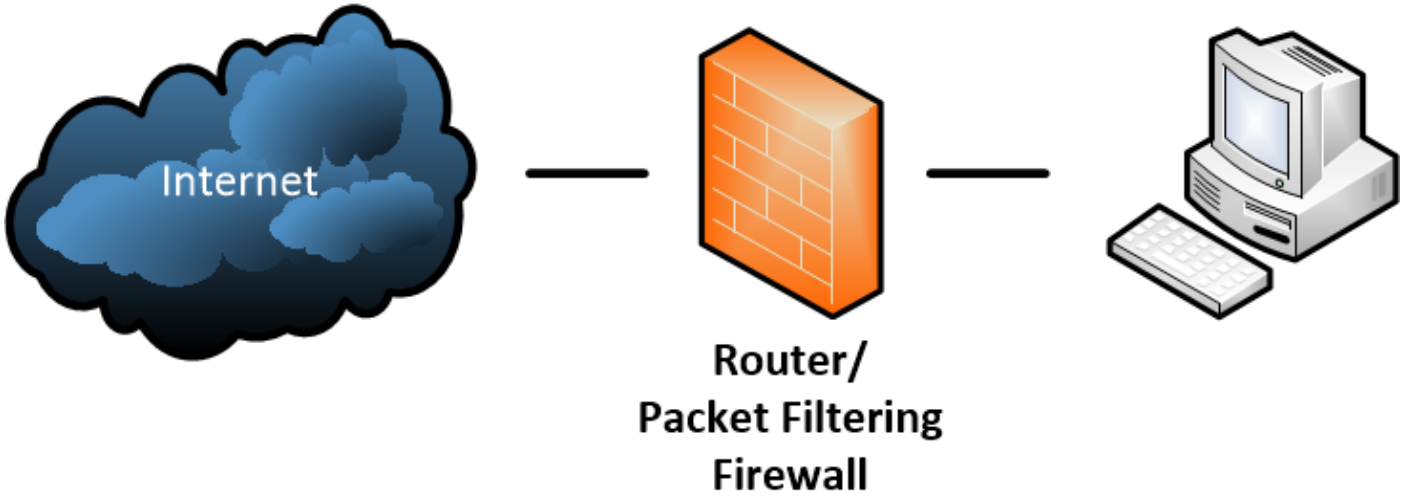
- Benefits of Application-Level Gateways
  - The network manager has complete control over each service and permitted services
  - It has the ability to support strong user authentication and provide detailed logging information
  - The filtering rules are much easier to configure and test
- Limitations of Application-Level Gateways
  - It requires either that users modify their behavior or that specialized software be installed on each system that accesses proxy services

Firewall Implementation Examples

- Packet-Filtering Router
  - Most common firewall type
  - Inexpensive and transparent to users
  - Inherent limitations of a packet-filtering router
- Screened Host Firewalls
  - Implements both network layer security (packet filtering) and application layer security (proxy services)
  - The intruder has to penetrate two systems to compromise security
  - Public information server can be placed on the segment shared by the packet-filtering router and the bastion host
  - Can be configured as a dual-homed host

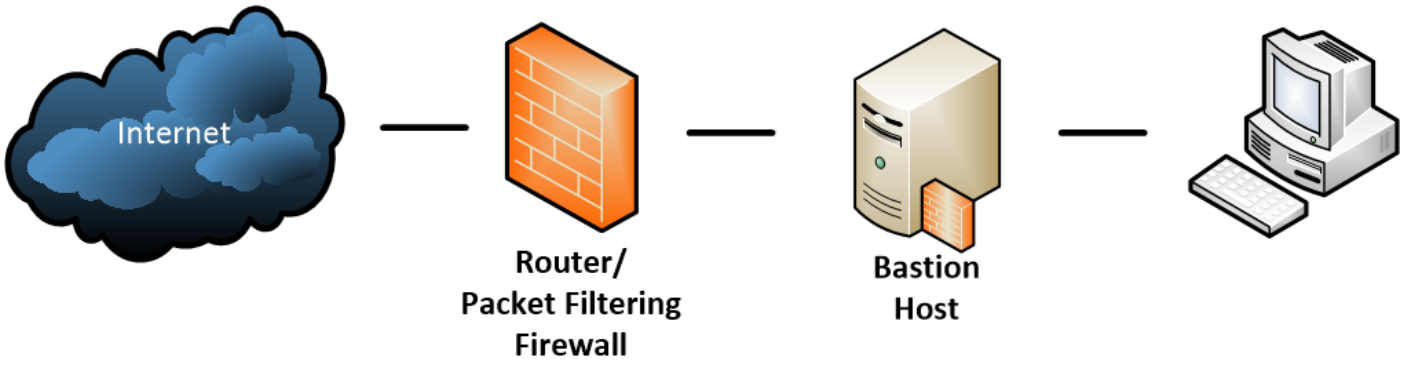
Firewall Implementation Examples

Packet Filtering Firewall



Firewall Implementation Examples

Screen Host Firewall



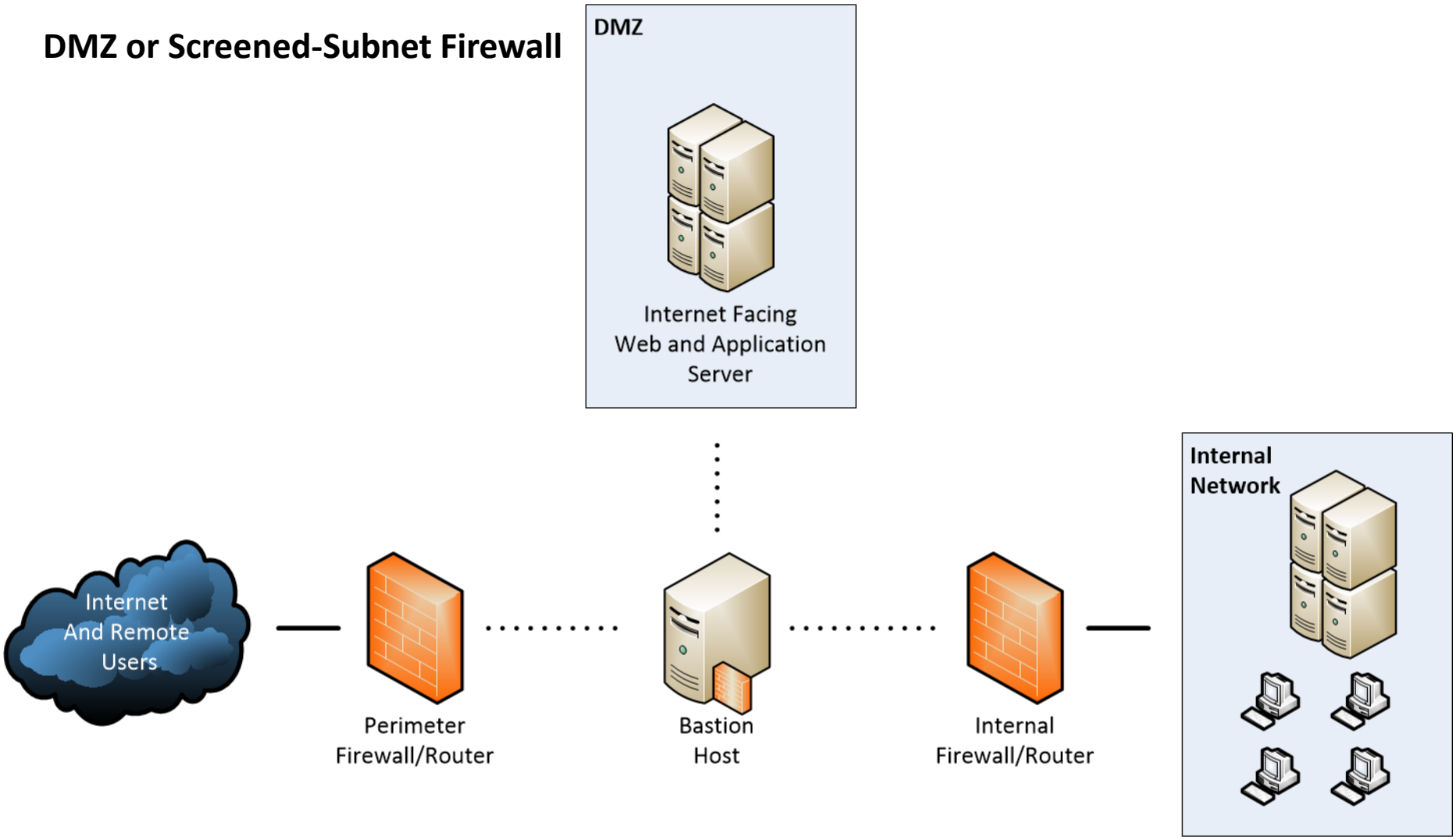
Firewall Implementation Examples

- DMZ or Screened-Subnet Firewall
  - Employs two packet filtering routers and a bastion host
  - The most secure configuration
  - Private network is invisible
  - Inside users must access the Internet via the proxy services
  - Can use Network Address Translation (NAT) for enhanced security
  - NAT is use to remap one IP address space into another by modifying network address information while they are transiting across a traffic routing device.

Firewall Implementation Examples

THE UNIVERSITY OF WINNIPEG

DMZ or Screened-Subnet Firewall



Intrusion Detection Systems (IDS)

- IDSs attempt to detect an intruder breaking into systems or an authorized user misusing system resources
- IDSs are needed to detect both types of intrusions
  - Break-in attempts from the outside
  - Knowledgeable insider attacks
- Two basic philosophical options
  - Prohibit everything that is not expressly permitted
  - Permit everything that is not expressly denied

Intrusion Detection Systems (IDS) -Two Classes

- Misuse intrusions (Signature Base)
  - Well-defined attacks on known weak points within a system
  - Can be detected by watching for certain actions being performed on certain objects
  - Can use pattern matching techniques on audit-trail information
- Anomaly intrusions
  - Observations of deviations from normal system usage patterns
  - Can be detected by building up a profile of the system in question and detecting significant deviations from the profile
  - Can use neural networks, machine learning classification techniques
  - Harder to detect

Intrusion Detection Systems (IDS)

- A Good Intrusion Detection System Must
  - Run continually without human supervision
  - Be fault-tolerant
  - Resist subversion
  - Impose minimal overhead on the attached network
  - Observe deviations from normal behavior
  - Be easily tailored to the network
  - Cope with changing system behavior

Intrusion Detection Systems (IDS)

- False Positives, False Negatives, and Subversion Attacks
  - A false positive occurs when the system classifies an action as anomalous when it is legitimate
  - A false negative occurs when an intrusive action has occurred but the system allows it to pass as nonintrusive behavior
  - A subversion error occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur

Intrusion Prevention Systems

- An extension of IDS
- Uses the same detection technic and method in an IDS system
- An active system that analyzes all traffic and can perform the following actions
  - Send an alarm to an administrator
  - Block the traffic
  - Reset the connection

Virtual Private Networks (VPNs)

- VPN is a network technology that makes it possible to establish private “tunnels” over the public Internet
- Three primary uses:
  - Employee connecting remotely to the corporate network
  - Extranet connection with business partners
  - Branch office networks
- Uses IP security (IPsec) for security
  - IPsec operates at both the network layer and session layer of the TCP/IP protocol stack

Virtual Private Networks (VPNs)

- IPsec
  - Performs both encryption and authentication to address the inherent lack of security on IP-based networks
  - Three characteristics
    - Sender authentication, message integrity, and data confidentiality
  - No modification to user applications
  - Can operate in two basic modes:
    - Transport mode
    - Tunnel mode

Virtual Private Networks (VPNs)

- IPsec has two security mechanisms:
  - Authentication Header (AH)
    - Modifies IP datagrams by adding an additional field that enables receivers to check the authenticity of the data within the datagram
  - Encapsulating Security Protocol (ESP)
    - Operates under the principle of encapsulation: Encrypted data is sandwiched between an ESP header and ESP trailer

Virtual Private Networks (VPNs)

- IPsec cont.
  - Security Association (SA)
    - AH and ESP require several parameters that both senders and receivers must agree on
    - SA is used to manage these parameters
    - SA is a secure “connection” between two end-points that applies a security policy and keys to protect information
    - SA is uniquely identified by the combination of three fields: IP destination address, security protocol identifier (AH or ESP), and security parameter index (SPI)
    - The protocol that negotiates security associations is called Internet Security Association and Key Management Protocol (ISAKMP)

- Used with IPsec
  - IPsec associates ISAKMP with Oakley Key Determination Protocol to form a new protocol called Internet key Exchange (IKE)
  - Oakley Key Determination Protocol
    - Used to exchange session keys on Internet hosts and routers
    - Can also derive new keys from old keys
    - Has three components

- Security Policies
  - The security policy database (SPD) is used for decision making on each packet of traffic
  - The database contains an ordered list of rules that define which IP packets within the network will be affected by the rule
  - The database enforces the scrutiny or transformation by the IPsec gateway server(s)

- IPSec Key Management
  - Manual key exchange (IETF RFC 1825): Using the manual exchange, a person manually configures each system with its own keys and those needed to communicate with other VPNs
  - Simple Key Interchange Protocol (SKIP): SKIP is based on the generation of a shared secret using Diffie-Hellman with already authenticated public key values
  - Internet Security Association and Key Management Protocol (ISAKMP)/Oakley: ISAKMP is needed to negotiate, establish, modify, and delete security associations and their corresponding data
- Applied VPNs
  - Many VPNs now use SSL for security and encryption
    - They require no end user software
    - Connections originate from the Internet accessible URL

Cloud Computing

Cloud computing must have these five essential characteristics:

- On-demand self-service
  - A consumer can provision any computing capabilities, like server time, network storage on a as needed automatically without human interaction from service provider.
- Broad network access
  - Access and capabilities are available over the network and accessed through standard mechanisms e.g., mobile phones, tablets, laptops, and workstations.
- Resource pooling.
  - Computing resources are pooled to serve multiple consumers using a multi-tenant model. Different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Cloud Computing

Cloud computing must have these five essential characteristics:

- Rapid elasticity.
  - Can be elastically provisioned and released and scale rapidly outward and inward commensurate with demand.
- Measured service
  - Automatically control and optimize resource use by leveraging a metering e.g., storage, processing, bandwidth, and active user accounts. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Cloud Computing

- Three main service type:
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- Four deployment model:
  - Private Cloud
  - Public Cloud
  - Community Cloud
  - Hybrid Cloud
- Examples of popular cloud services:
  - Drobox
  - Amazon
  - Salesforce

Cloud Computing – Service Types

- Software as a Service (SaaS)
  - Users access and use application software like email, databases, storage from the cloud provider
  - Cloud providers manage the infrastructure and platforms that run the applications
  - The user pay the cloud provider by either pay-per-use basis or using a subscription fee.

Cloud Computing – Service Types

- Platform as a Service (PaaS)
  - Create a development environment to application developers
  - Cloud provider provide develops toolkit and standards for development and channels for distribution and payment
  - Cloud providers deliver a computing platform, typically including operating system, programming-language execution environment, database, and web server

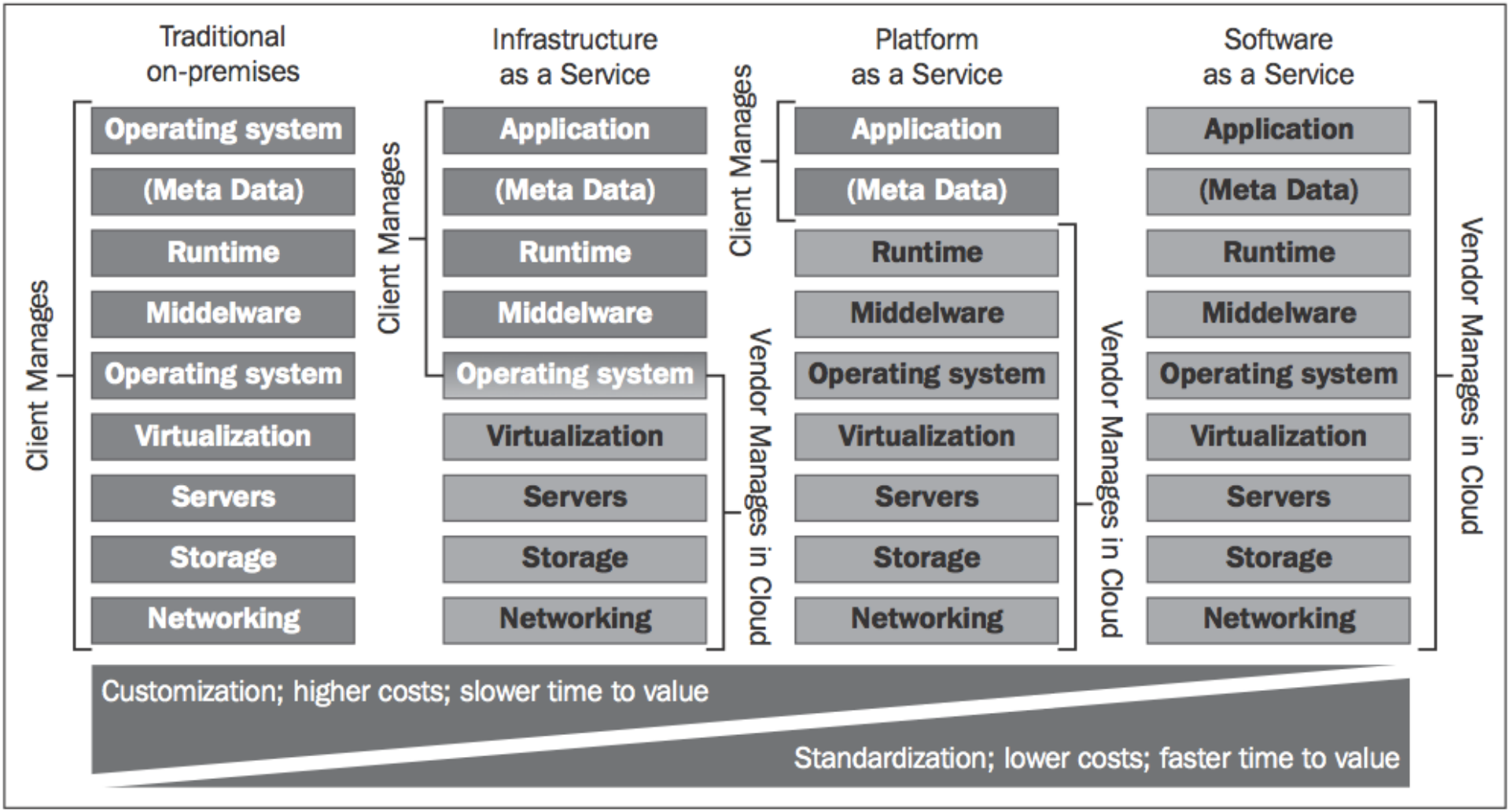
Cloud Computing – Service Types

- Infrastructure as a Service (IaaS)
  - Cloud provider supply on-demand resources from their large pools of equipment installed in data centers
  - They also often offer resources such as a virtual-machine disk-image library, raw block storage, file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles

Cloud Computing – Service Types

- Other services being offered and developed
  - iPaaS (Integration Platform as a Service)
  - dPaaS (Data Platform as a Service)
  - Mobile "backend" as a service (MBaaS)
  - Function as a service (FaaS)
  - Security as a Service (SECaaS)

Cloud Computing



Cloud Computing – Deployment Model

- Private Cloud
  - Operated solely for a single organization
  - Could be managed internally or by a third party
  - Hosted either internally or externally
- Public Cloud
  - Services are rendered over a network that is open for public use

Cloud Computing – Deployment Model

- Community Cloud
  - Shares infrastructure between several organizations that forms a specific community or with common concerns
  - Example - security, compliance, jurisdiction, etc.
- Hybrid Cloud
  - A composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models.

- The Telecommunications, Network, and Internet Security domain is one of the most important areas that security practitioners must understand well
- We can begin to mix and match the building blocks of network security tools and techniques to implement defense in depth in preserving confidentiality, integrity, and availability
- It is important to know how to find security information and how to decide which security architecture is most appropriate for a given situation

ACS-2821-001 – Questions?