



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



CYBS 7357 Network Security

Introduction to Unit 1

Lecture 2

Welcome to Unit 1 Lecture 2 of Network Security

Lecture 2 Topics

In this lecture, we will be discussing:

- Network definitions
- Different network topologies
- Network devices and their functions
- Network protocols and their functions

2

In this lecture we will be laying the groundwork for your understanding of networks and network security. We'll start with the basics and progress through the next dozen weeks with deeper and more complex topics.

Lecture 2 Learning Objectives

- At the conclusion of this Lecture, the student will be able to:
 - Define a network
 - Identify different network topologies
 - Describe network devices and their functions
 - Explain network protocols

3

Welcome to Unit 1 Lecture 2 of Network security.

In this lecture we will be laying the groundwork for your understanding of networks and network security. We'll start with the basics and progress through the next dozen weeks with deeper and more complex topics.

Welcome to Network Security Lecture 2

- **Define a network**
- Understand different network topologies
- Introduction to network nodes (devices)
- Introduction to network protocols

4

So what exactly is a network. For this course, we will consider a network a group of nodes (devices) connected by communications paths. In the IT world, there are several different topologies we should be familiar with and we will look at several.

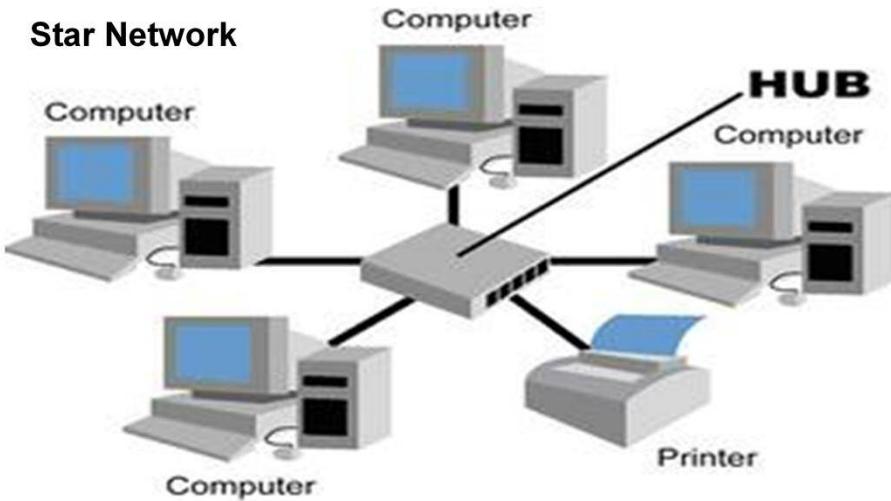
Welcome to Network Security Lecture 2

- **Define a network**
- Understand different network topologies
- Introduction to network nodes (devices)
- Introduction to network protocols

5

So what exactly is a network. For this course, we will consider a network a group of nodes (devices) connected by communications paths. In the IT world, there are several different topologies we should be familiar with and we will look at several.

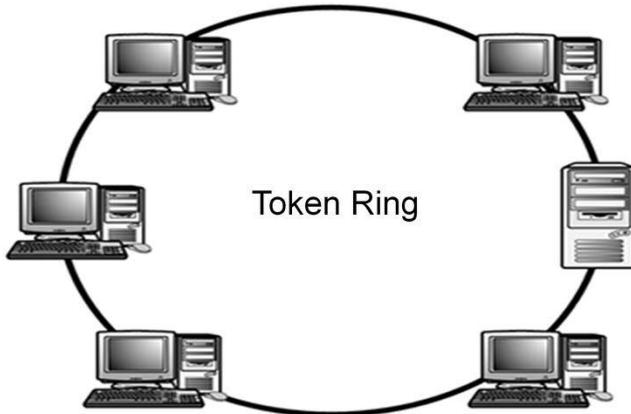
Network Topographies - Star



6

Throughout the history of information technology, there have been a number of topologies used. The network above shows a star network. In this network each node or workstation is connected to a central hub. A hub is a network device that is seldom used today. It served to connect devices but did not prevent issues such as packet collisions and packet storms. As we will see soon, hubs have been replaced with switches.

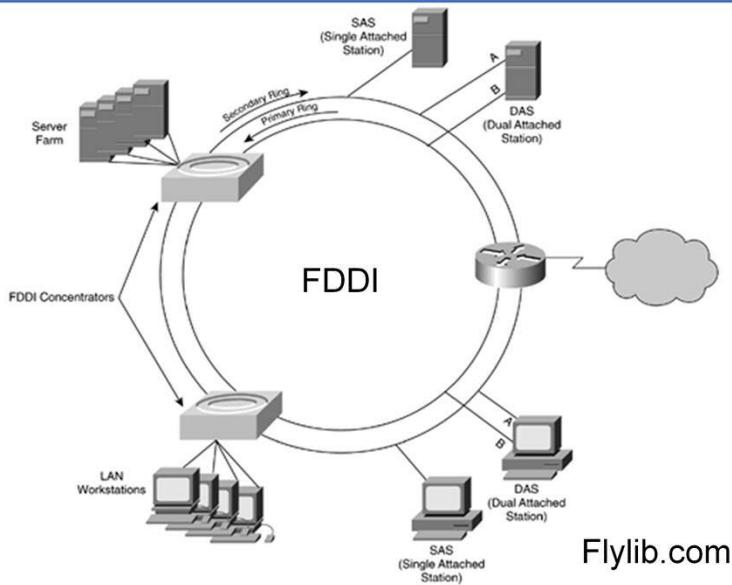
Network Topographies - Ring



7

The ring network, also called a token ring network was introduced by IBM in the mid 1980's. It solved some of the packet contention and flooding issues found in other topologies by passing a token around the ring. When a computer was in possession of the token it was their turn to communicate. When done, the token was passed to the next computer on the ring. If there was no need to communicate, the token continued to the next and so on.

Network Topographies - FDDI

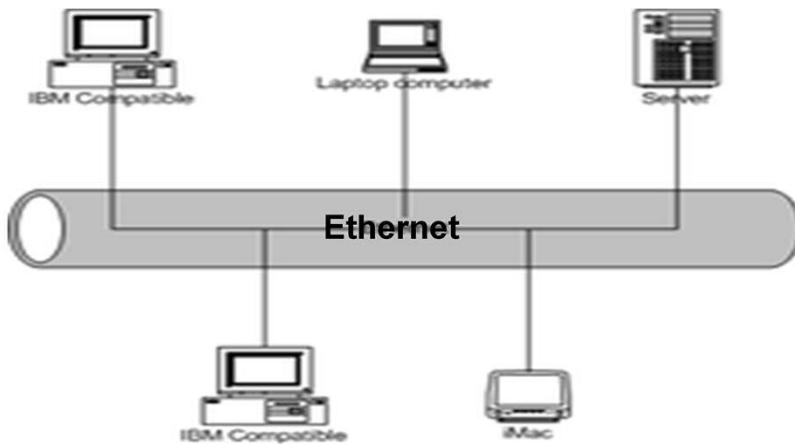


Flylib.com

8

Fiber Distributed Data Interface or FDDI is a dual counter directional ring network similar to the token ring network. The two rings pass token in opposite directions at 100 Mbps. One ring is the primary ring providing service during normal operations. When a device on the network fails and can no longer pass the token, the token is returned along the secondary path. This provides better fault tolerance than the IBM token ring as well as improvements in speed.

Network Topographies - Buss



9

The Ethernet network has been around since the early 1970s and was a contemporary of the token ring network. In fact, it was some of the issues presented by Ethernet that prompted the development and promotion of the token ring. As shown above, Ethernet communicates over a shared wire. That common communications channel has changed over time, originally being coax, then twisted pair and now fiber and more advanced twisted pair. Of course that is a simplified view, but not that far off. Nodes are attached to a common buss and may communicate with any other node on that buss by sending a packet with that nodes address.

There are a number of problems that can and do arise from this topology, nevertheless it has become the most accepted network topology in use today. Issues include contention (nodes fighting for the limited resource), collisions and more. These have been largely resolved through the years. One resolution was the use of Carrier Sense Multiple Access with Collision Detection or CSMA/CD. More on this later.

We will be spending the majority of our course looking at Ethernet and the devices and protocols that make it the most widely used network today.

Network Security Lecture 2

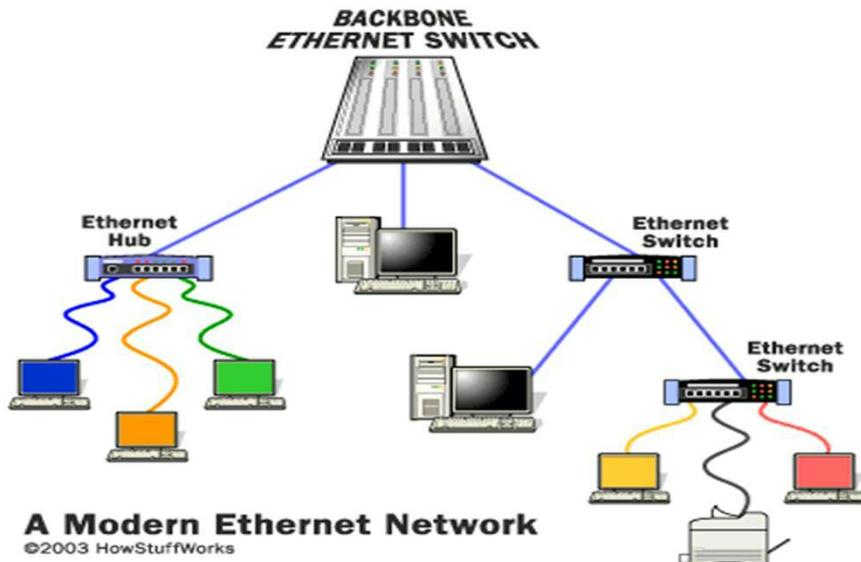
- Objectives:

- Define a network
- **Understand network topologies**
- Introduction to network nodes (devices)
- Introduction to network protocols

10

From looking at the previous slide, you may not recognize the Ethernet of today. Let's take a look at a more modern configuration.

Network Topographies - Ethernet



11

Here, the Ethernet backbone has been replaced with an Ethernet backbone switch. Nodes connect to the backbone either directly or through other network devices. Here we see both an Ethernet hub and an Ethernet Switch connected to the backbone. Each network device provides functionality to address specific issues present in the Ethernet network. As we progress through the course, each device will be discussed in detail along with the function they serve.

Welcome to Network Security Lecture 2

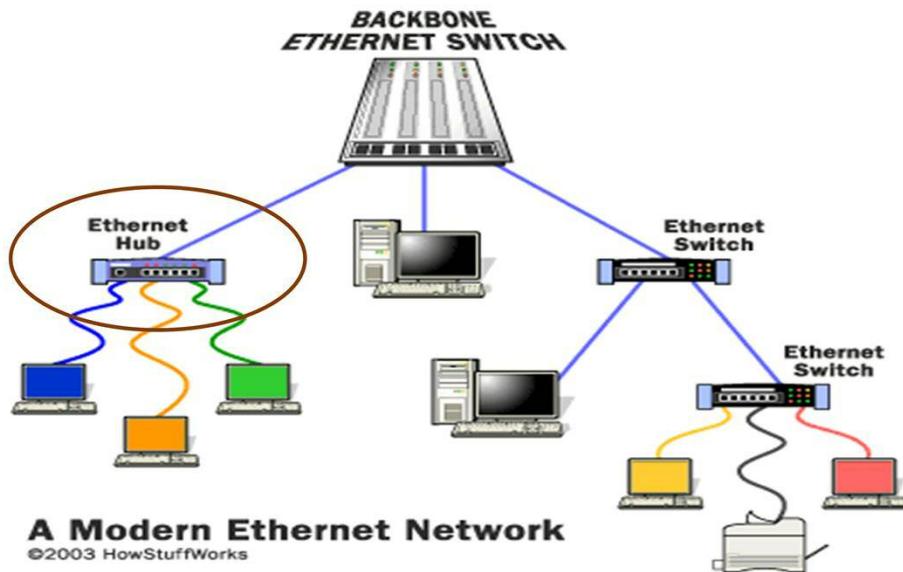
- Objectives:

- Define a network
- Understand different network topologies
- Introduction to network nodes (devices)
- Introduction to network protocols

12

Now that we've looked at a few of the network topologies, let's become more familiar with nodes and some network devices.

Network Nodes

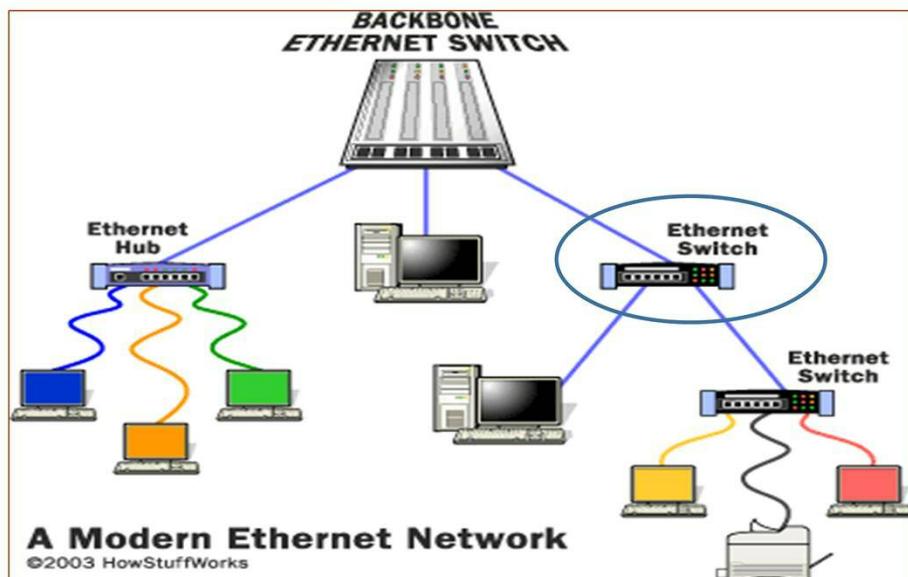


13

We'll go back to this diagram for a moment. I've circled an Ethernet hub. Hubs are seldom used today and have been replaced with switches. Hubs were used to consolidate and connect nodes serving as the backbone or Ethernet cable.

Hubs don't provide the ability to control communications between connected devices and thus suffer from issues such as contention and broadcast storms. Any data presented to the hub is in effect presented to all the devices connected to the hub.

Network Nodes (Continued)



14

Ethernet switches have become very inexpensive and as mentioned have replaced hubs. Switches come in a variety of types allowing different levels of control and management. Some switches provide functions similar to hubs, but can reduce or eliminate contention and storm issues by transferring packets only to the node or node which are intended recipients. Other switches allow creation of virtual LANs and have sophisticated remote management capabilities.

As shown here, most switches can be cascaded or connected to expand the number of ports nodes can connect to. Another advantage of switches is their ability to reconstitute an Ethernet signal effectively extending the distance Ethernet can be used.

Most switches function at layer 2, the data link layer of the OSI model, however some newer switches can perform functions at layer three, the network layer which is usually associated with routers. We will be looking a bit closer at the OSI model in lecture three of this unit.

Introduction to Network Protocols

- Objectives:

- Define a network
- Understand different network topologies
- Introduction to network nodes (devices)
- Introduction to network protocols

15

At this point, I'd like to start introducing some of the networking protocols that are widely used in todays Ethernet networks.

Protocols are structured methods used to initiate, conduct and shutdown communications over a medium. There are many protocols associated with different networks. While we will look briefly at some, we will spend a significant amount of time examining the Transmission Control Protocol (TCP) and the Internet Protocol (IP) starting in the next lecture in this unit.

Protocols are typically developed in suites that are combined using a layering technique to meet specific circumstances. Some protocols are general in design while others have a specific purpose.

Introduction to Network Protocols

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)
- Hypertext Transfer Protocol (HTTP)
- Post Office Protocol (POP)
- File Transfer Protocol (FTP)
- Internet Message Access Protocol (IMAP)

16

I've already mentioned that TCP and IP frequently work together. Here are several other protocols that work in concert with the Internet Protocol. Most of these should look pretty familiar to you. For example, almost everyone should recognize the Hypertext Transfer Protocol. This protocol is invoked whenever we type it into the address line of our web browser.

Other popular or at least well known protocols are File Transfer Protocol (FTP) and the Post Office Protocol (POP) used by many mail clients.

We'll look at these and many others as we progress through this course starting with TCP and IP in the next lecture.

End of Lecture 2



of Lecture 2

17

This ends Lecture 2. In Lecture 3 we will be taking a deeper dive into the TCP/IP protocol.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Introduction to Unit 1

Lecture 3

Network Security Lecture 3 Objectives

- Objectives:

- Review the TCP/IP Protocol Suites
- Identify how applications use TCP/IP
- Examine tools used to troubleshoot and study protocol behavior

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

2

Welcome to Unit 1 Lecture 3 of Network security.

In this lecture we will be diving into TCP/IP a suite of some of the most popular networking protocols in use today.

We will be looking at the structure and operation of TCP/IP and how these protocols interact with applications.

We will also examine some of the tools used to troubleshoot and study protocol behavior as they are used.

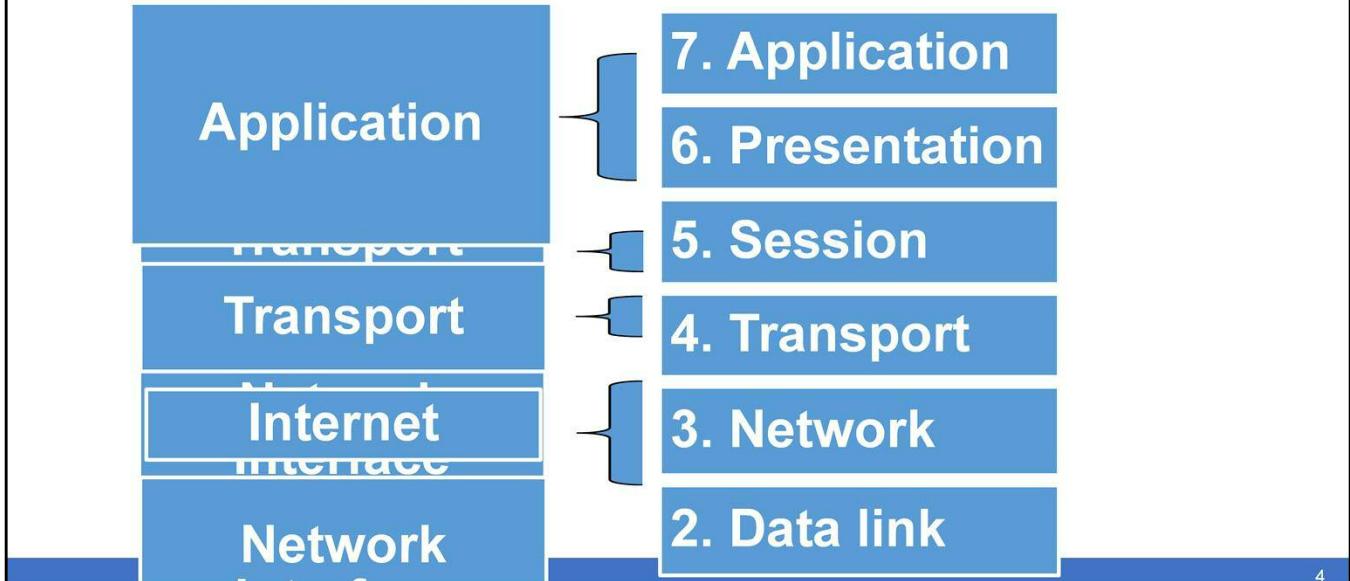
Network Security Lecture 3 Key Concepts

- Key Concepts covered in this lecture:
 - Essential TCP/IP characteristics
 - The OSI Model
 - Differentiating clear-text from cipher-text
 - IP networking protocol behavior
 - Network management tools
 - TCP/IP protocol analysis

3

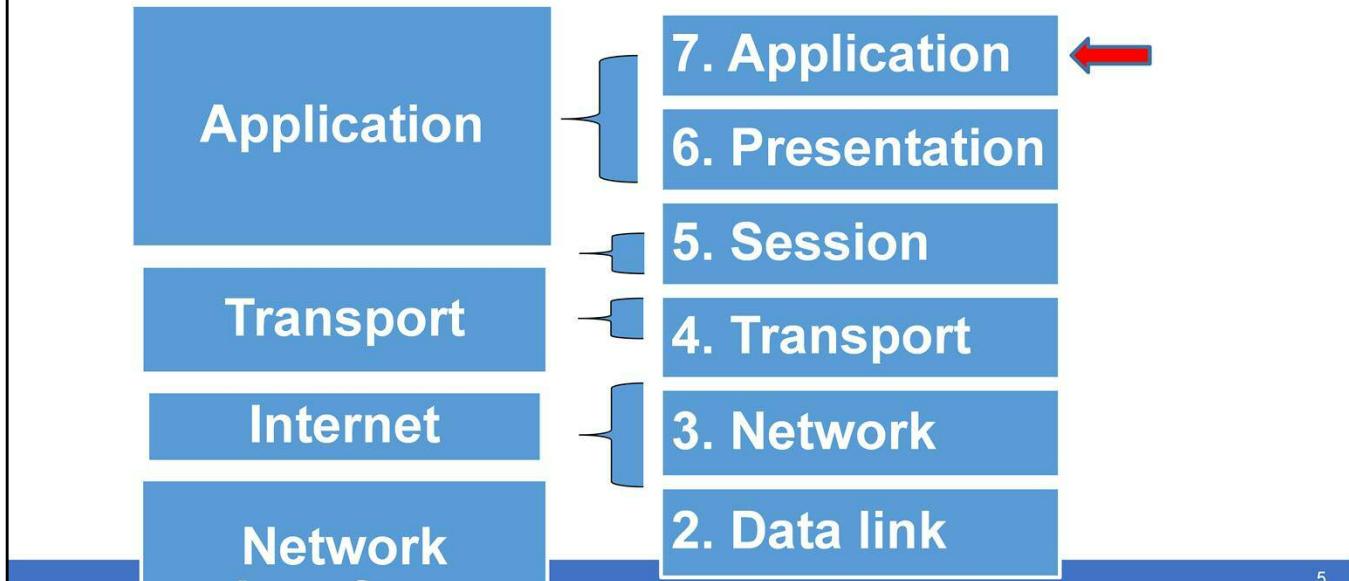
We will be learning several key concepts in this lecture including the characteristics of the TCP & IP protocols, the OSI model and how protocols relate, how to differentiate clear text from cypher text used by these protocols, and how these protocols function on the network. In addition, we will look at couple of the commonly used tools used to investigate the behavior of these (and other) protocols.

TCP/IP Networking and OSI Reference Models



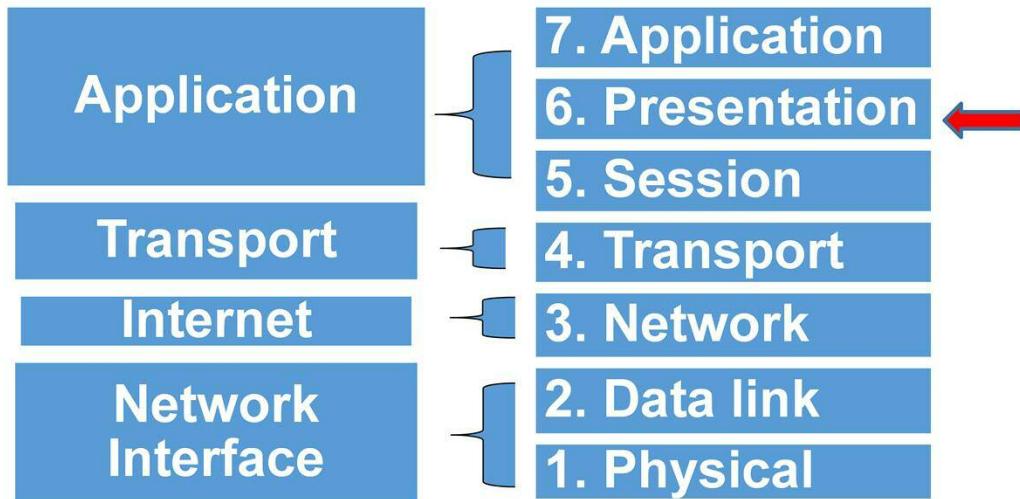
For those of you who are familiar with the seven layer OSI model, this slide depicts how the TCP/IP model corresponds to layers in the OSI model. The TCP/IP protocol stack layers are presented on the left and the corresponding OSI layers are on the right. Let's look briefly at each layer of the OSI model.

TCP/IP Networking and OSI Reference Models



Layer 7 is the Application layer — This layer enables communications with the host software, including the operating system. The application layer is the interface between host software and the network protocol stack. The sub-protocols of this layer support specific applications or types of data.

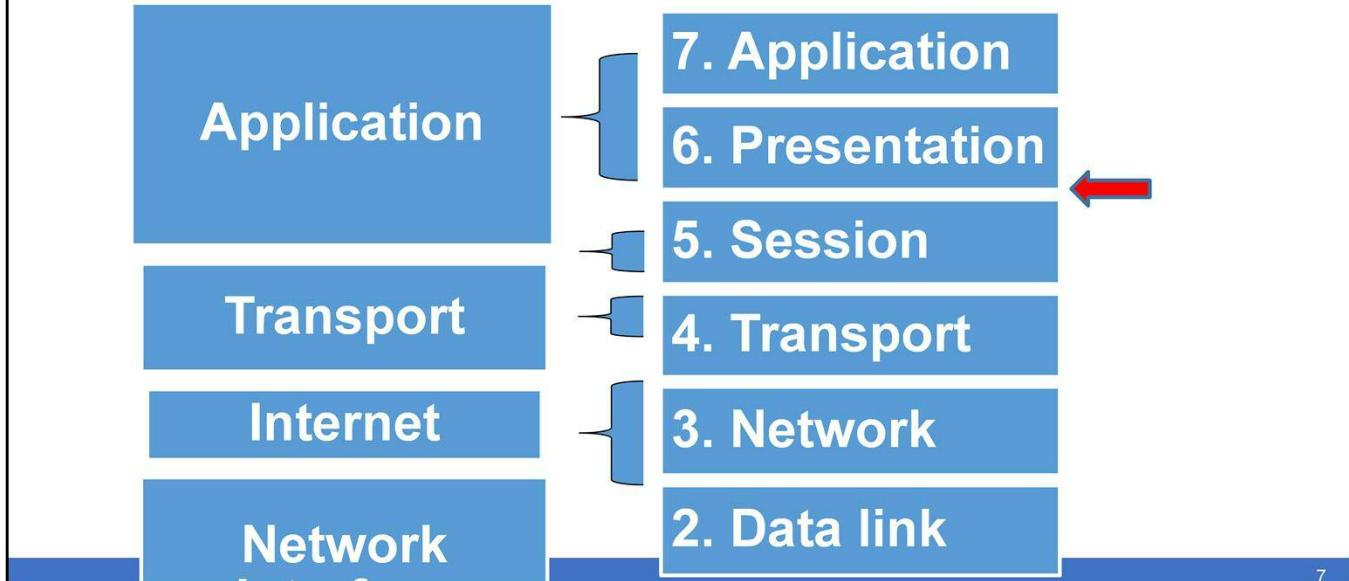
TCP/IP Networking and OSI Reference Models



6

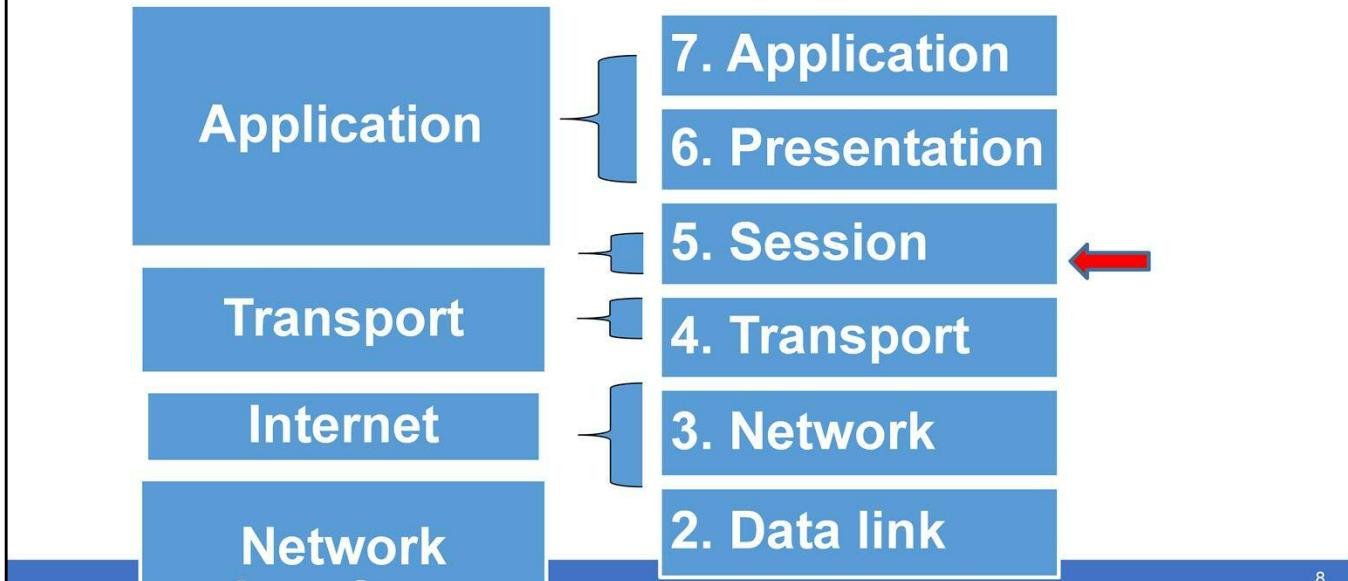
Layer 6 is the Presentation layer - This layer translates the data received from the host software into a format acceptable to the network. This layer also performs this task in reverse for data going from the network to the host software.

TCP/IP Networking and OSI Reference Models



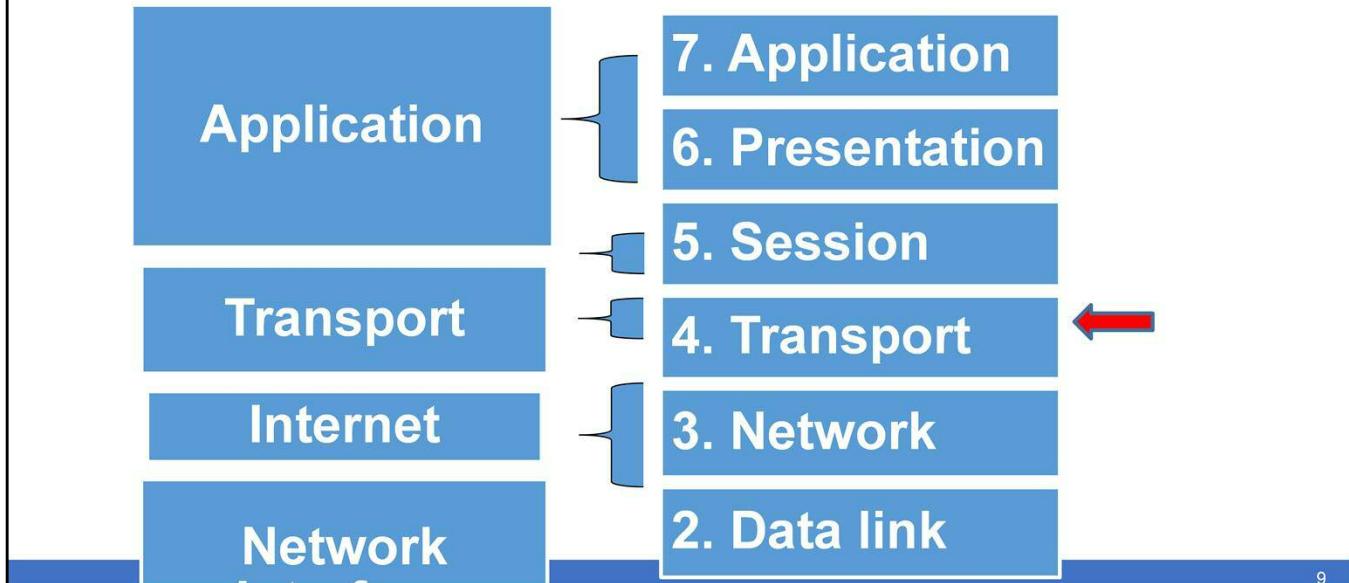
Layer 5 is the Session layer — This layer manages the communication channel, known as a session, between the endpoints of the network communication. A single transport layer connection between two systems can support multiple, simultaneous sessions.

TCP/IP Networking and OSI Reference Models



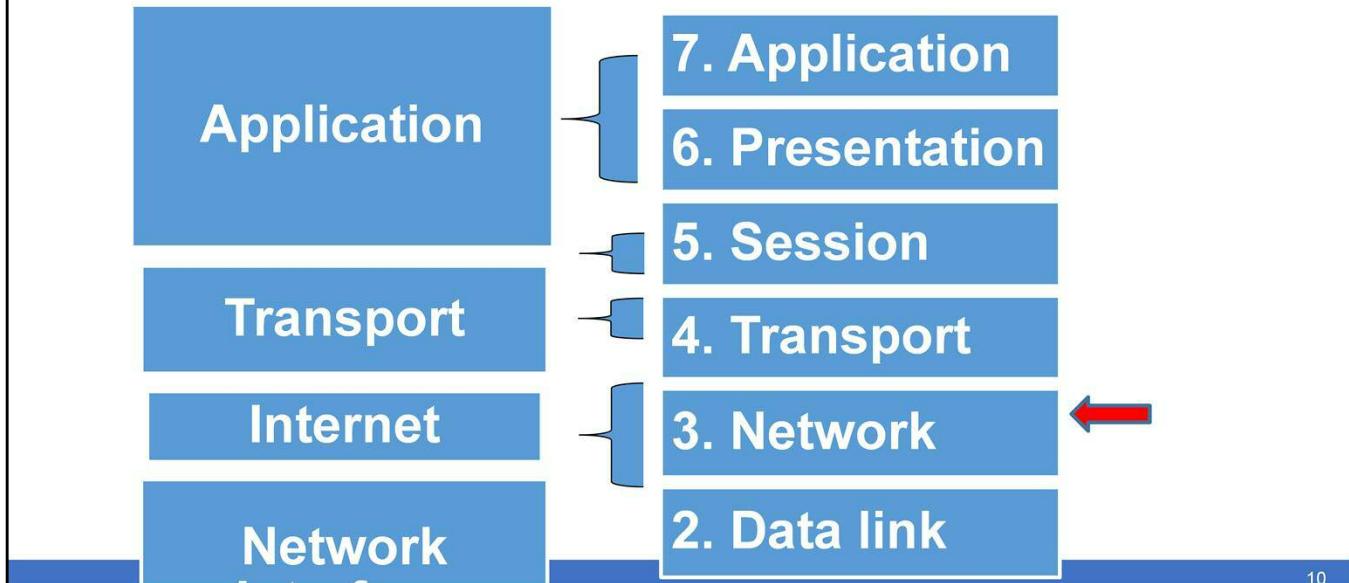
The Transport layer (layer 4) — formats and handles data transportation. This transportation is independent of and transparent to the application.

TCP/IP Networking and OSI Reference Models



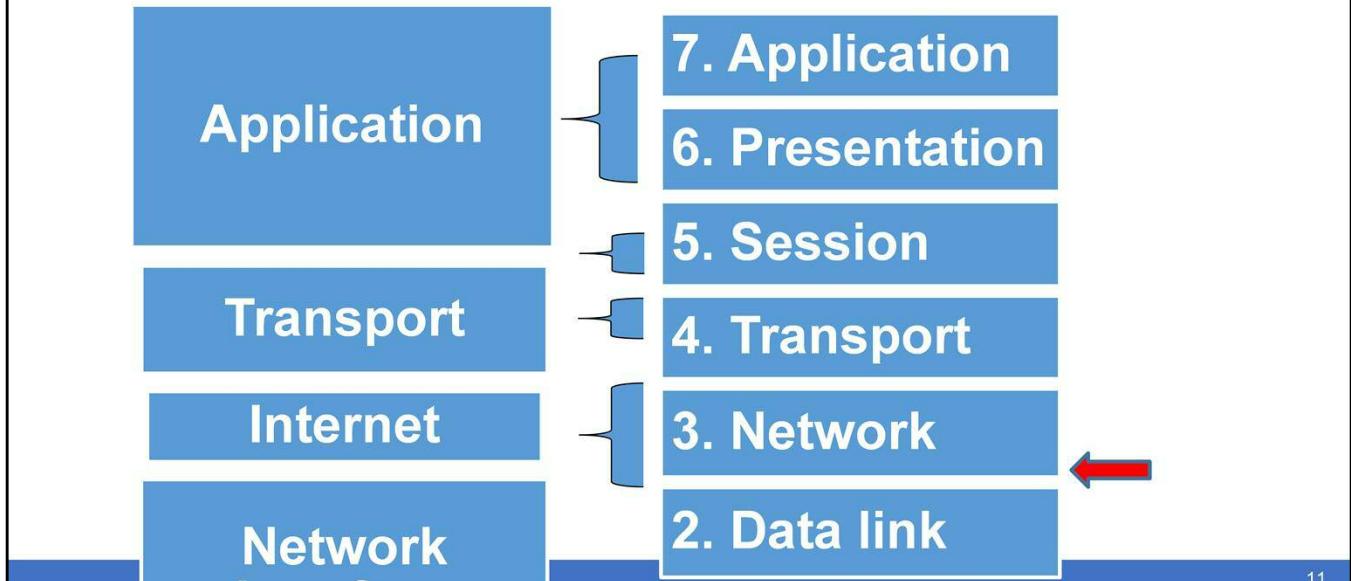
The Network layer (layer 3) — handles logical addressing (IP addresses) and routing traffic. This is where you would generally find the functions of a router however some switches are being built with some of these routing capabilities as well.

TCP/IP Networking and OSI Reference Models



The Data link layer (layer 2) manages physical addressing (MAC addresses) and supports the network topology or topologies, such as Ethernet. This is normally where switches are placed in the OSI model.

TCP/IP Networking and OSI Reference Models



The Physical layer (layer 1) — converts data into transmitted bits over the physical network medium. This is where the physical cable is attached. This is typically the network interface card or NIC. NICs are designed for specific network topographies and have sockets for those types of networks.

TCP/IP Protocol Suite

Application

- Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Hypertext Transfer Protocol (HTTP), Tele-network (Telnet), File Transfer Protocol (FTP)

Transport

- Transmission Control Protocol (TCP), User Datagram Protocol (UDP)

Internet

- Internet Protocol (IP), IPSec, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Internet Group Management Protocol IGMP

Network Interface

- Serial Line Internet Protocol (SLIP), Point to Point Protocol (PPP)

The four layer architecture of the TCP/IP protocols depicted here also shows a number of other protocols and where they rest on this stack. The application layer supports higher level operations found in the FTP, HTTP, DNS and DHCP protocols. FTP and HTTP have already been introduced. The Domain Name System or DNS and the Dynamic Host Configuration Protocol (DHCP) will be discussed in later lectures.

The transport layer is the home of the Transmission Control Protocol (TCP) and the User Datagram protocol (UDP).

The Internet layer hosts the Internet Protocol (IP) as well as the Address resolution protocol (ARP), IP Security protocol and the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). These will be discussed in later lectures.

The last layer is the Network Interface where the Serial Line Internet Protocol (SLIP) and the Point to Point Protocol (PPP) reside. These protocols are associated with Ethernet. Other protocols may be used to support other network topologies such as token ring.

The Structure of a Packet

Source port		Destination port			
Sequence number					
Acknowledgement number					
Data offset	Reserved	Flags	Window		
Checksum		Urgent pointer			
Options + padding					
Data (variable)					

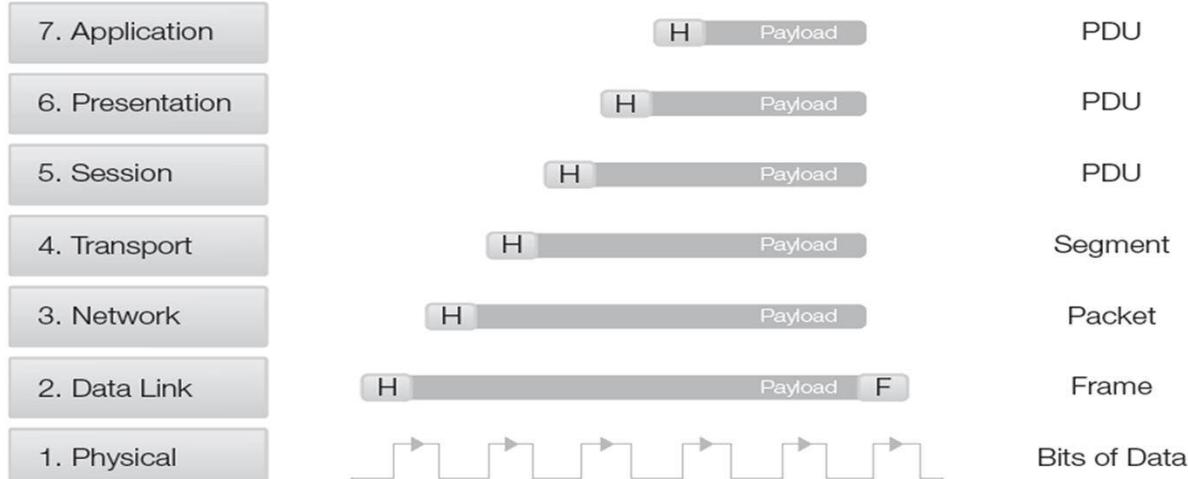
A primary data construct for communications on Ethernet is the packet. The packet is transferred within a frame. The frame has a seven byte preamble and a four byte Frame Check Sequence which is normally managed by the hardware (the NIC) connecting the Ethernet physical pathway. Most host based traffic investigation software such as Wireshark cannot see these frame components as they are either added or removed by the network interface. The Ethernet packet has defined fields to make the transport and management of packets efficient. As you go through the course and the labs, you will gain knowledge of the meaning and use of each of the fields that make up the packet.

Here I would call attention to just a few of the available fields starting with the source and destination ports at the top of the packet. Source and destination ports are established when a communications session is established and should be the same throughout the session. The source port is the MAC address of the sender while the Destination is the MAC address of the intended receiver. Each is six bytes long.

The sequence number is another critical component. Packets may take different routes to reach their destination and can be affected by delays along the way. The sequence number allows reconstruction of the message by the recipient as well as allowing the identification of missing packets.

The checksum is used for error detection. Lastly for now, the data field is what contains the actual information being transferred. The size of this field is variable with a minimum of 42-46 bytes and a maximum of 1500 bytes.

A Packet Moves Through the Protocol Stack



Let's go back to the OSI model and look at this from a little different perspective.

As data moves from a software application for transmission over the network, it traverses the layers of the protocol stack from top to bottom. As each layer receives data from the layer above it, that data becomes the payload with a layer specific header.

At the Data link layer, where Ethernet resides, the data receives a footer, as well. This process is known as encapsulation. The inverse, known as **de-encapsulation**, occurs when a network communication is received. As this process takes place, the data set being manipulated receives unique names, depending on the layer it traverses.

The encapsulation process of adding headers (and a footer at the Data link layer) enables data exchange between layers on different systems. This is known as peer-to-peer communications. The content of a header includes information to be processed by the corresponding layer on the receiving end of a network link. The content of the headers are the greatest concern and focus of a firewall. **Application proxy** firewalls and stateful inspection firewalls can also examine the headers and the payload content of layers 5–7.

Functions of a Protocol Analyzer

- **Why analyze data packets?**
 - Detect network problems, such as bottlenecks
 - Detect network intrusions
 - Check for vulnerabilities
 - Gather network statistics
- **What does a protocol analyzer do?**
 - Captures and decodes data packets traveling on a network
 - Allows you to read and analyze them

Now that we have a little background on Ethernet packets, let's look at a couple of the tools frequently used when troubleshooting packets on networks. We use protocol analyzers to aid in evaluating the efficiency of our networks as well as a troubleshooting tool. There are a number of issues that can develop on networks which would not be visible without these aids. Listed here are just a few of the uses.

As indicated, protocol analyzers work by capturing packets traversing the networks and presenting them in a form which allow the network engineer to perform analysis. We will be doing this in some of the labs throughout this course.

NetWitness Investigator

- Threat analysis software
 - Protocol Analyzer
- Captures raw packets from wired and wireless interfaces
- Analyzes real-time data throughout the seven layers

One of the tools we will use is NetWitness Investigator. This is a free tool provided by RSA and will be used in a number of the labs. It's important to note that the tool allows some analysis through all seven layers of the OSI model.

NetWitness Investigator (cont.)

- Filters by Media Access Control (MAC) address, IP address, user, and more
- Supports Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6)
- Gets daily threat intelligence data from the SANS Internet Storm Center
- Freely available

The tool has a good deal of flexibility in how you can sort and present the collected data. In addition, it supports both the older IP version 4 as well as the newer IP Version 6.

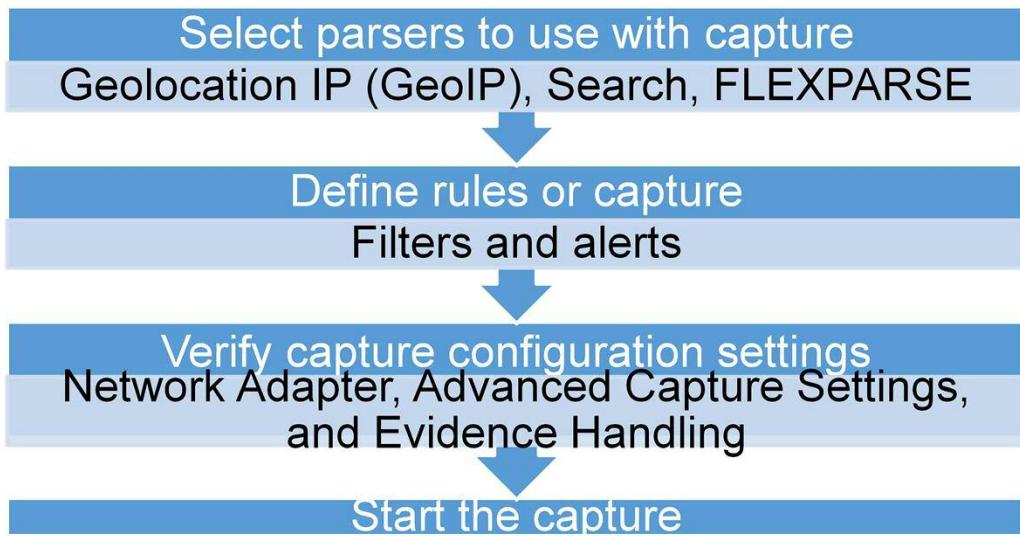
A significant advantage of this tool is its ability to obtain threat intelligence from the SANS Internet Storm Center which allows better analysis of malware and other threat behaviors on the network.

Wireshark

- Network protocol analyzer
- Captures Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and other packets
- Analyzes real-time and saved data
- Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and others
- Supports IPv4 and IPv6
- Allows Voice over IP (VoIP) analysis

Another widely used tool and one we will also be using in the labs is Wireshark. Wireshark is also freely available and performs similar functions to the NetWitness Investigator tool. Each program has strengths and weaknesses which has created supporters and opponents for each. It's important that you become somewhat familiar with both programs so you can develop your own opinions. Both these tools are used frequently in network security, partly because they are free, but more importantly because they are effective.

Packet Capture Using NetWitness Investigator



These are the general steps you will use to start capturing data using the NetWitness Investigator tool. Each lab will step you through the setup process so you can configure the software for the specific environment and data you will need to collect.

Trace Analysis Using NetWitness Investigator

Navigation

Select a collection.

Click Navigation.

Select a report.

Select a group of sessions.

Search for specific content.

Search

Open a collection.

Click the Content Search icon.

Search on keyword or regular expression.

Once you have collected data, which is known as a trace, you can begin the analysis. Again, each lab will step you through the entire process so you can become familiar with the basic functions of this tool. Like many software packages, NetWitness has a great many features which can take years to fully understand and utilize fully. In this course you will learn the basics, but you can plan on learning more as you grow in your careers and make more use of these tools.

TCP/IP Transaction Sessions

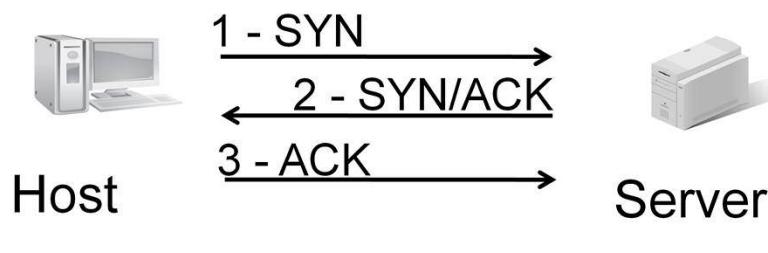
- **Connection-oriented**
 - Sender
 - Breaks data into packets
 - Attaches packet numbers
 - Receiver
 - Acknowledges receipt; lost packets are resent
 - Reassembles packets in correct order

TCP/IP sessions are connection oriented. From a practical standpoint, that means that a session is established that allows communications between established points. With a connection oriented session, messages (or files) are broken into small data units and packaged into packets which specify the senders MAC address as well as the receivers MAC address. Packets are numbered allowing identification of missing packets as well as the ability to re-assemble packet data in the correct sequence.

If you remember back a couple of slides, we saw that there was another protocol in the Transport layer of the TCP/IP protocol stack. That was the User Datagram Protocol. UDP differs from TCP in that it is not connection oriented. Packets are addressed to the intended receiver or receivers without any required acknowledgement and without the session requirements of TCP. UDP is order-less, so any ordering would have to be performed at the application layer. The greatest advantage of UDP is its speed. Without the overhead of TCP it is able to send more packets faster. The down side is that the packet ordering must be managed external to the protocol and packet loss must be accepted when it occurs.

Delivery is not guaranteed. Think in terms of a letter. You address it, put a stamp on it and hope it gets to your destination. That is UDP. If you want to ensure it is received, then you need to send it certified with a return receipt required. More costly and time consuming, that is TCP.

TCP Three-Way Handshake



Synchronize (SYN)
Acknowledge (ACK)

The TCP protocol uses a three-way handshake to establish a session between two systems.

The first system sends a packet with the SYN flag set.

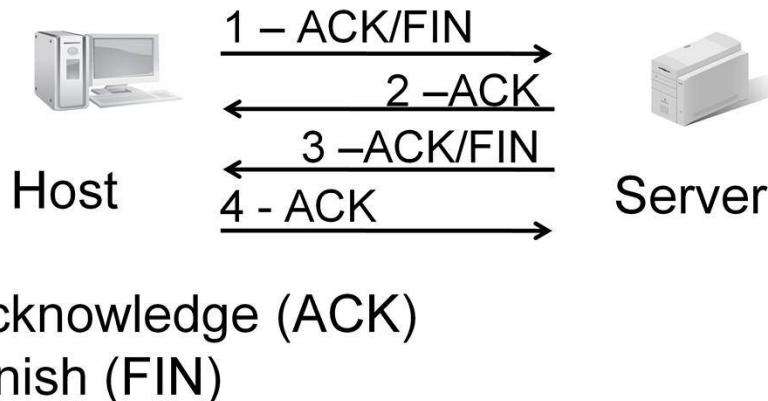
The second system responds with a packet that has the SYN and ACK flags set.

The first system responds with a packet with the ACK flag set.

The two systems have now started a session.

One type of the Denial of Service attack uses this handshake process to flood the server with SYN requests. The server generally will respond and wait for a preset amount of time for the final ACK from the host before timing out. As thousands of hosts flood the server with these requests, the server becomes overloaded waiting for responses and can stop communicating or even crash.

TCP Connection Termination



Because a TCP connection is two-way, it needs to be “torn down” in both directions.

The TCP connection termination process uses four packets.

The first system sends a TCP packet with the ACK and FIN flags set requesting termination.

The second system sends an ACK response.

The second system then sends a packet with ACK and FIN flags set.

The first system returns an ACK response.

This terminates the session at both ends.

End of Lecture 3



of Lecture 3

24

This ends Lecture 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Introduction to Unit 2

Lecture 1

Unit 2 Lecture 1 Topics

Topics:

- The primary and secondary tenants of security
- Fundamental concepts of network security
- The nature of Trust in network security
- Goals associated with network security
- The seven domains in a typical IT network
- The components of a security policy

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

2

Welcome to Unit 2 Lecture 1 of Network security.

In this lecture we will be exploring the tenants of security in general and how they are applied to networks. In addition, we will begin our exploration of network security concepts starting with the concept of Trust as it is applied to networks. We will look at the of the general goals of networks security. We will learn the seven domains of a typical network and study the formation and components of a security policy.

Unit 2 Lecture 1 Learning Objectives

At the conclusion of this lecture, the student will be able to:

- Describe the tenants of security in general
- Explain the fundamental concepts of network security
- Describe the nature of Trust in Network Security
- Identify the goals associated with network security
- Describe the seven domains in a typical IT network

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

3

Welcome to Unit 2 Lecture 1 of Network security.

In this lecture we will be exploring the tenants of security in general and how they are applied to networks. In addition, we

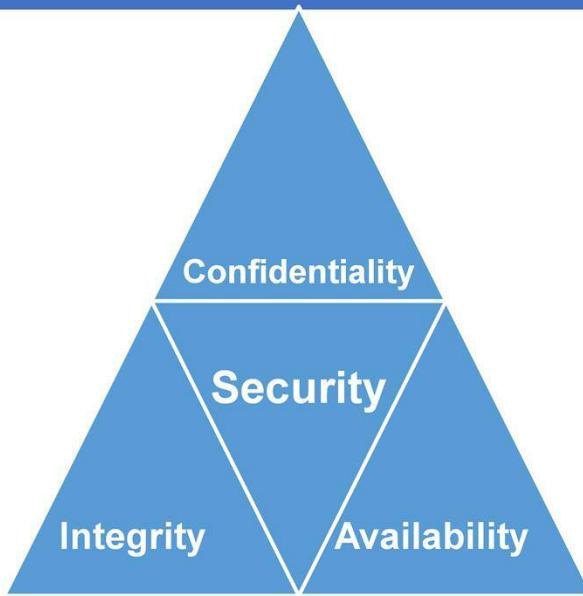
Key Concepts

- Confidentiality, integrity, and availability (CIA) mandates for network resource security
- Network security and its value to the enterprise
- Roles and responsibilities in network security
- Impact of network infrastructure design on security
- Features, uses, and benefits of network security countermeasures

During this lecture we will be reviewing a number of key concepts related to network security beginning with the security mandates. We will look at network security and the value network security brings to the organization. We will examine the roles and responsibilities commonly associated with network security.

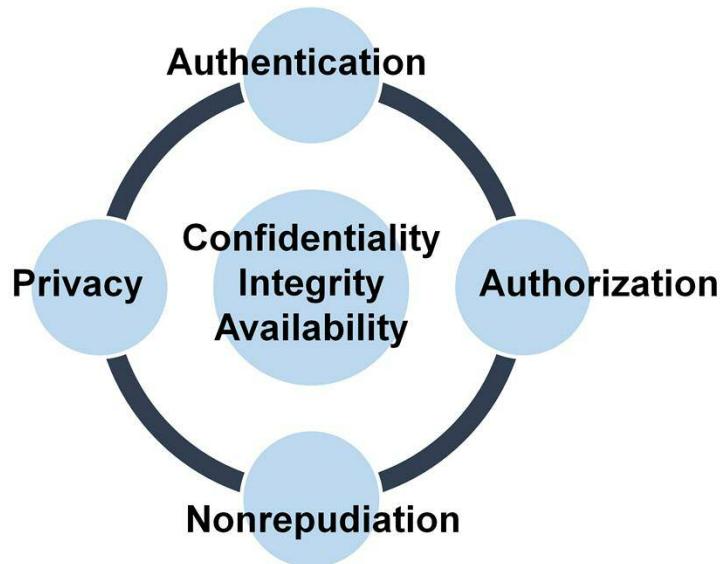
We will also begin to explore how network architecture impacts security and some of the controls and countermeasures that can be deployed.

Primary Goals of Information Security



We will start by looking at the three primary pillars or goals of security. They are confidentiality, integrity and availability. You will see and hear these throughout the course.

Secondary Goals of Information Security



Along with primary goals of confidentiality, integrity and availability, there are a number of secondary goals. Here we list authentication, authorization, nonrepudiation and privacy. Some would also add audit to this list as well.

The Need for Information Security

- **Risk**
- **Threat**
- **Vulnerability**

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

7

Three terms that you should become familiar with are Risk, Threats and Vulnerabilities. I'll start with vulnerabilities.

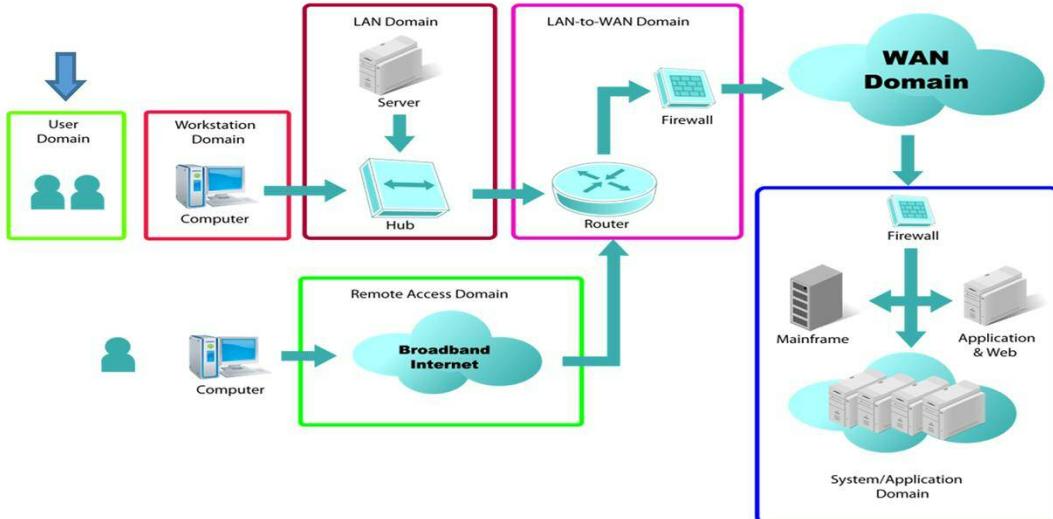
A Vulnerability: is a Weakness in a process or system that has the potential to adversely impact confidentiality, availability, or integrity

A Threat: is the possibility of an vulnerability being exploited

Risk: Is the likelihood that a threat will exploit a vulnerability and the impact that will have on an organization

We will be looking at these relationships in greater detail both in your text and in the lectures.

Seven Domains of a Typical IT Infrastructure

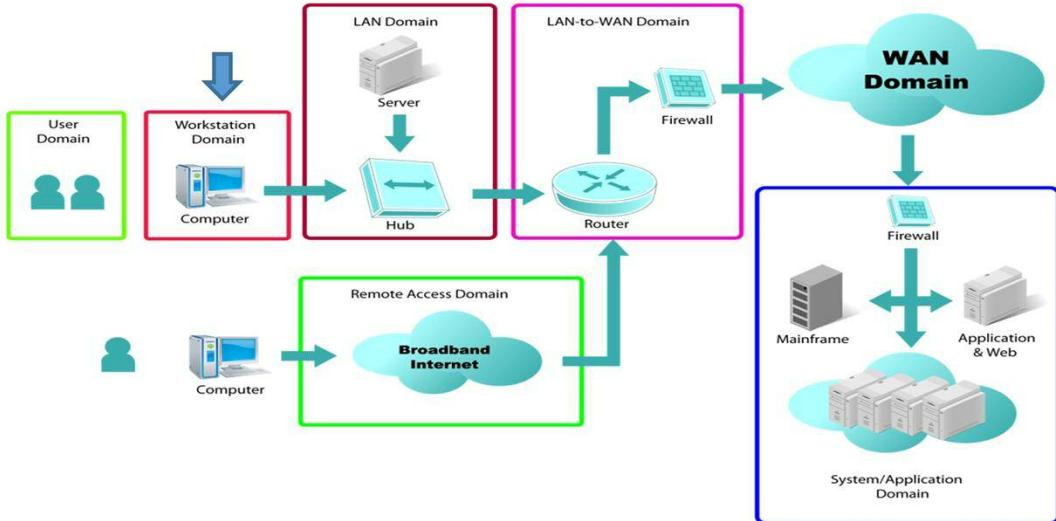


Let's start by looking at a typical IT infrastructure.

There are seven domains normally recognized in an IT infrastructure.

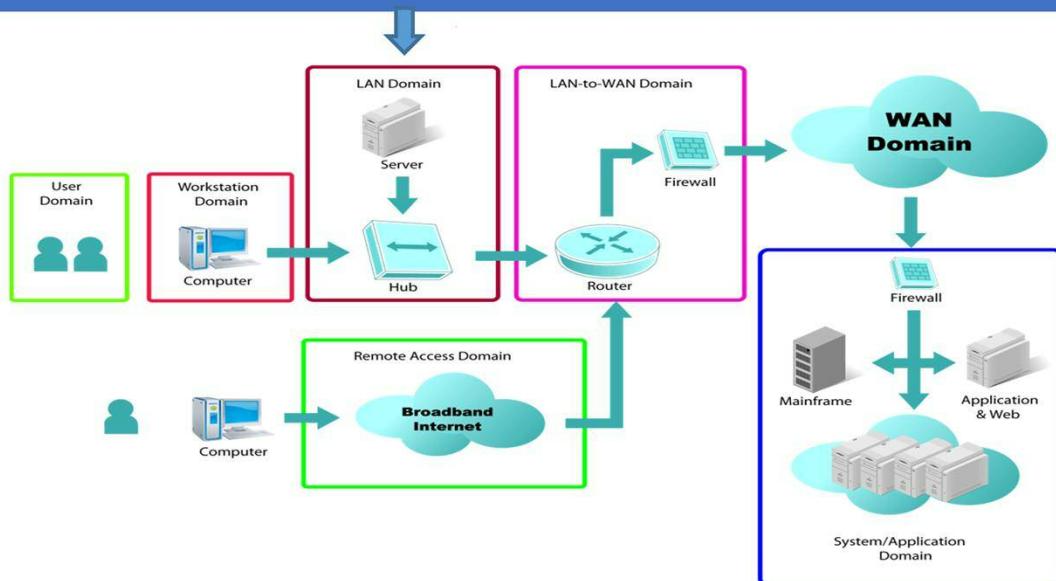
User Domain—This domain refers to actual users whether they are employees, consultants, contractors, or other third-party users. Any user who accesses and uses the organization's IT infrastructure must review and sign an acceptable use policy (AUP) prior to being granted access to the organization's IT resources and infrastructure.

Seven Domains of a Typical IT Infrastructure



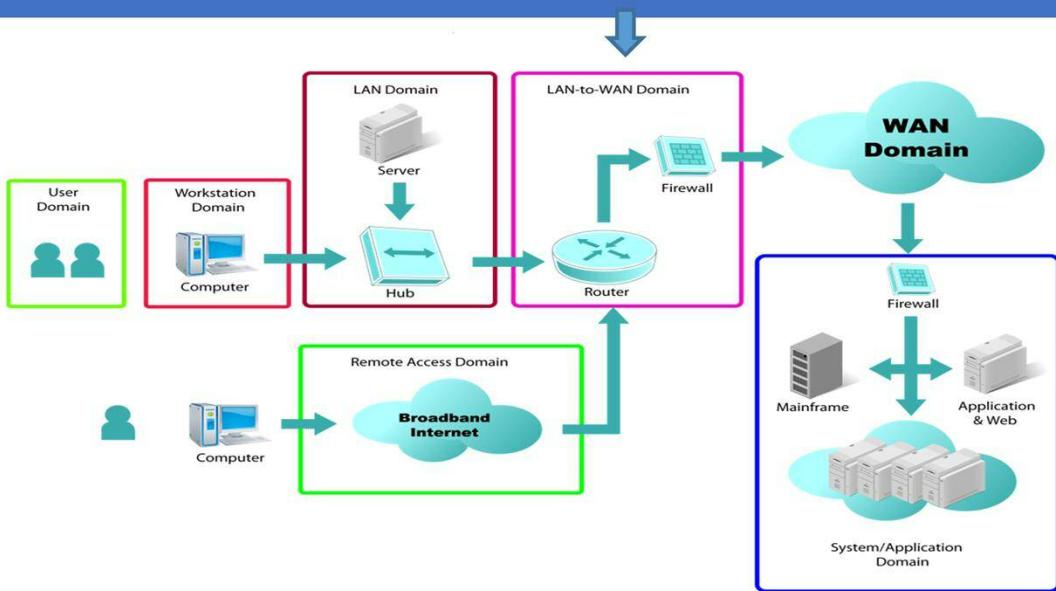
Workstation Domain—This domain refers to the end user's desktop devices such as a desktop computer, laptop, VoIP telephone, or other end-point device. Workstation devices typically require security countermeasures such as antivirus, antispyware, and vulnerability software patch management to maintain the integrity of the device.

Seven Domains of a Typical IT Infrastructure



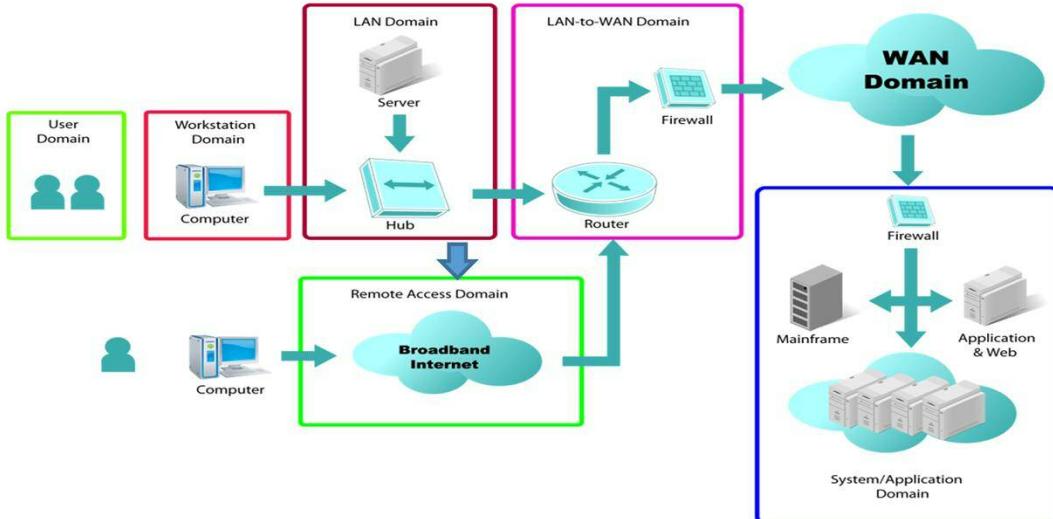
LAN Domain—This domain refers to the physical and logical local area network (LAN) technologies (i.e., 100 Mbps/1000 Mbps switched Ethernet, 802.11-family of wireless LAN technologies) used to support workstation connectivity to the organization's network infrastructure.

Seven Domains of a Typical IT Infrastructure



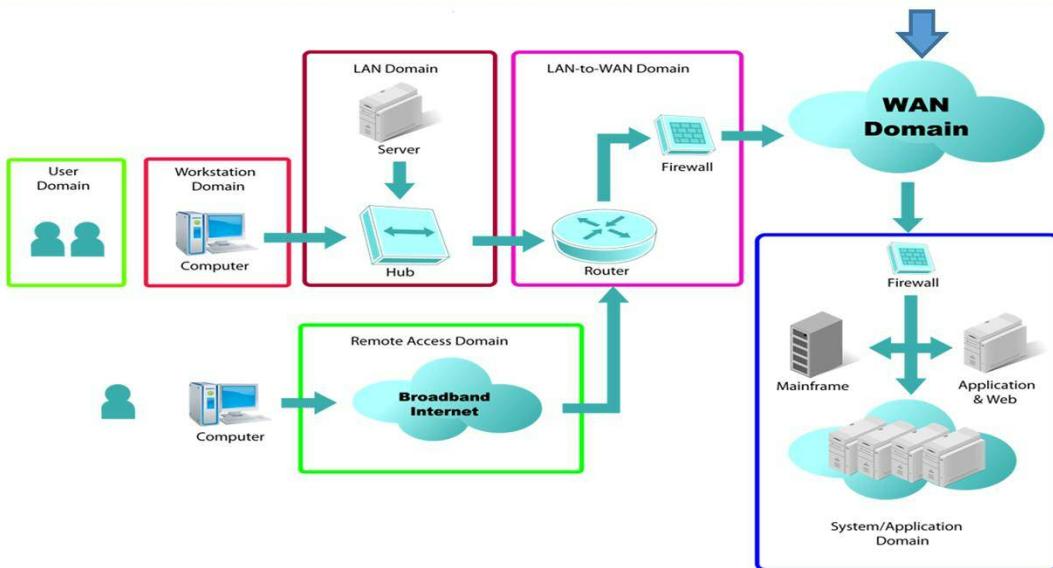
LAN-to-WAN Domain—This domain refers to the organization's internetworking and interconnectivity point between the LAN and the WAN network infrastructures. Routers, firewalls, demilitarized zones (DMZs), and intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are commonly used as security monitoring devices in this domain.

Seven Domains of a Typical IT Infrastructure



Remote Access Domain—This domain refers to the authorized and authenticated remote access procedures for users to remotely access the organization's IT infrastructure, systems, and data. Remote access solutions typically involve Secure Sockets Layer (SSL) 128-bit encrypted remote browser access or encrypted virtual private network (VPN) tunnels for secure remote communications.

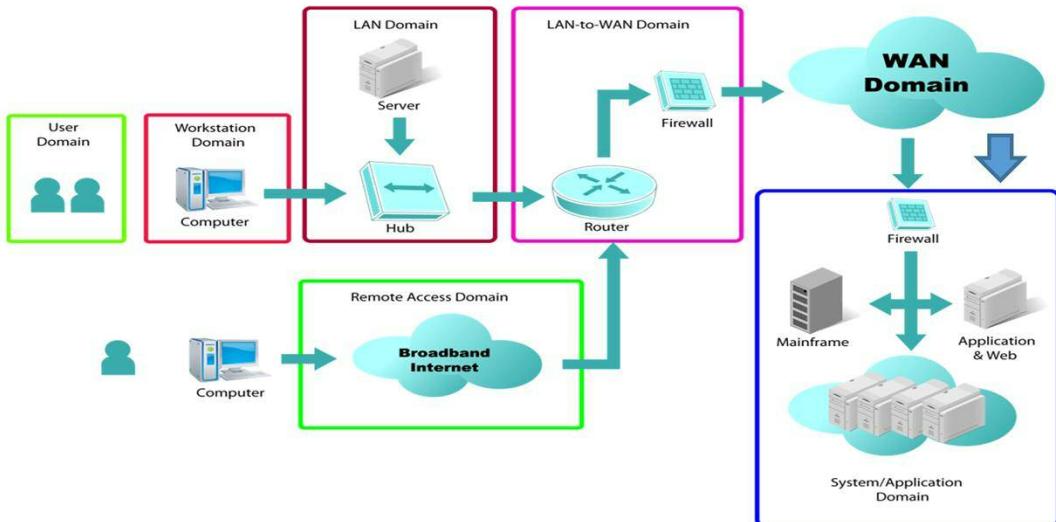
Seven Domains of a Typical IT Infrastructure



The Wide Area Network or WAN Domain

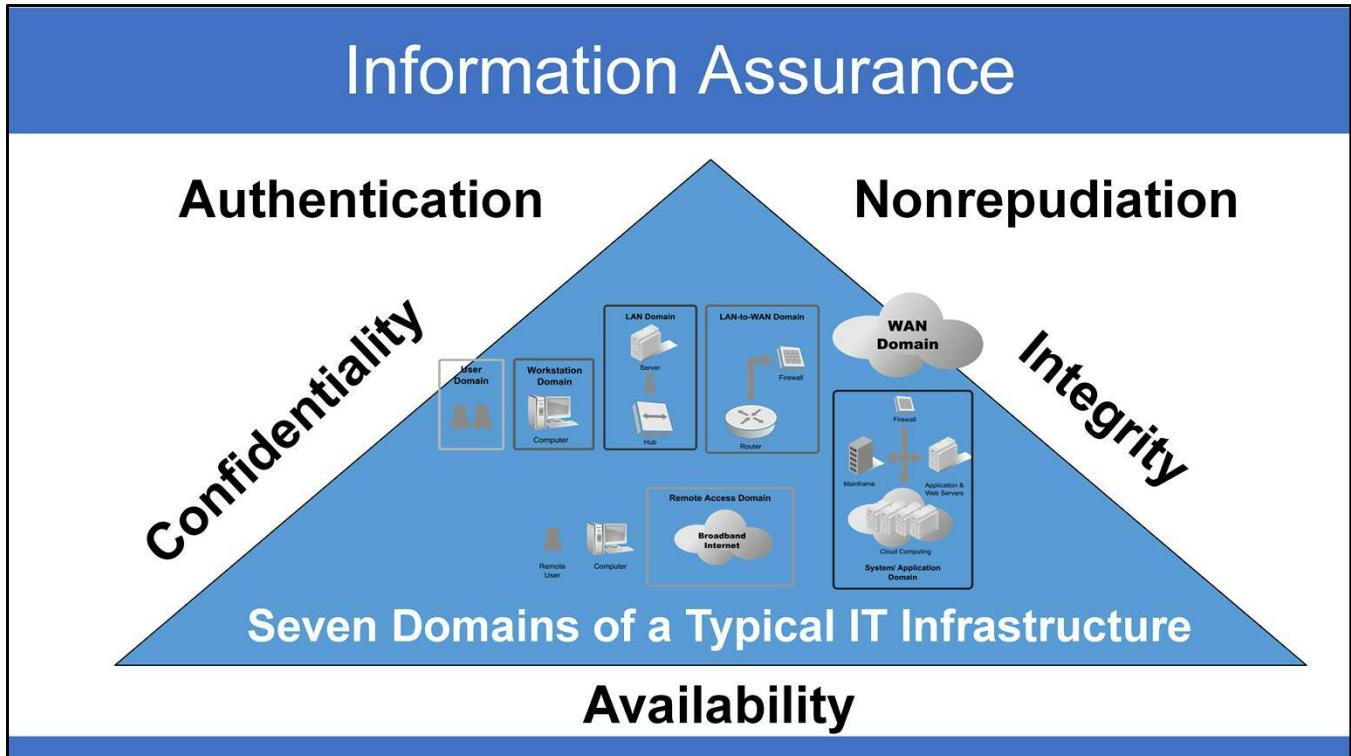
Organizations with remote locations require a WAN to interconnect them. Organizations typically outsource WAN connectivity from service providers for end-to-end connectivity and bandwidth. This is frequently done through common carriers such as the telephone companies, but can also include many third party providers. This domain typically includes routers, circuits, switches, firewalls, and equivalent gear at remote locations sometimes under a managed service offering by the service provider.

Seven Domains of a Typical IT Infrastructure



Finally, there is the System/Application Domain. This domain refers to the hardware, operating system software, database software, client/server applications, and data that is typically housed in the organization's data center and/or computer rooms.

The seven domains form the IT architecture that makes up most organizations. Of course this is an over simplification, however it will serve to illustrate the basic domains normally found.



The seven domains each provide or require one or more of the tenants or goals of security. Although Network security goals vary from organization to organization, they include a few common mandates:

- Ensure the confidentiality of resources
- Protect the integrity of data
- Maintain availability of the IT infrastructure
- Ensure the privacy of personally identifiable data
- Enforce access control
- Monitor the IT environment for violations of policy
- Support business tasks and the overall mission of the organization

Already you should be seeing some common threads in these mandates starting with confidentiality, integrity and availability. Some of the other goals include ensuring privacy, enforcing security policies and supporting business goals.

Security Policy

- Establish goals



In the previous slide we mentioned the monitoring of adherence to a security policy. Security policies are frequently used to establish and communicate security specific goals.

Security Policy

- Establish goals
- Address risk



Security policies are meant to address risk associated with the use and misuse of technology.

Security Policy

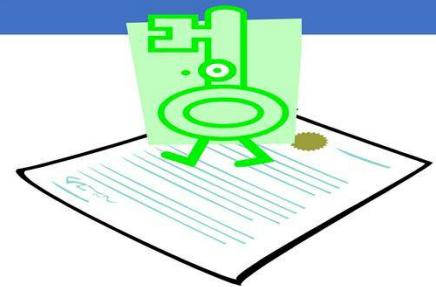
- Establish goals
- Address risk
- Provide roadmap for security



Security policies provide a general roadmap for security within the organization and emphasizes the management support behind that roadmap.

Security Policy

- Establish goals
- Address risk
- Provide roadmap for security
- Set expectations



Security policies are not the same as an acceptable use policy, however many of the requirements may be the same. For example both documents set levels of expectations and link behaviors to business objectives.

Security Policy

- Establish goals
- Address risk
- Provide roadmap for security
- Set expectations
- Link to business objectives



Security must be linked to business goals and objectives to be successful. The security policy illustrates how security supports the businesses goals.

Security Policy

- Establish goals
- Address risk
- Provide roadmap for security
- Set expectations
- Link to business objectives
- Map of laws and regulations



The security policy is a good place to indicate the regulatory and legal requirements that the organization may be subject to. In most cases, failing to provide a secure environment can lead to a failure to comply with required regulations or imposed standards which in turn can lead to significant fines and legal issues.

Security Policy

- Establish goals
- Address risk
- Provide roadmap for security
- Set expectations
- Link to business objectives
- Map of laws and regulations
- Supported by standards, procedures, and guidelines



Lastly, the security policy serves as the foundation document for standards, procedures and guidelines.

Briefly, Standards are the specifics of what devices and controls the organization chooses to use. Procedures are the step by step processes for establishing these in the organization. Guidelines are normally suggestions for best practices that may be applied. But are not mandatory within the organization.

Policy, Awareness, and Training

- Policy ~
 - sets expectations
- Awareness ~
 - promotes security
- Training ~
 - defines roles and responsibilities

Some of the other aspects of policies are that they are generally

Well-defined, but overarching in nature
Address business needs and security concerns
Sets expectations

They are meant to provide Awareness

Promote security
Keep security at the front of users' minds

They can serve as the initial Training to help

Individuals understand their roles and responsibilities
And to help Individuals understand security policy

End of Lecture 1



of Lecture 1

24

This ends Lecture 1 of Unit 2. We will continue with lecture 2 and begin our look at IT infrastructures.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Introduction to Unit 2

Lecture 2

Unit 2 Lecture 2 Topics

Topics:

- Networking terminology
- Typical network architectures
- Wired versus wireless networks
- VPNs
- Wireless benefits, issues, and concerns
- Mobile networking
- Security countermeasures

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

2

Welcome to Unit 2 Lecture 1 of Network security.

In this lecture we will be exploring the tenants of security in general and how they are applied to networks. In addition, we

Unit 2 Lecture 2 Learning Objectives

At the conclusion of this lecture, the student will be able to:

- Describe the impact of network infrastructure design on security
- Identify and characterize some common network architectures
- Discuss the pros and cons of wireless networks
- Identify the features, uses, and benefits of network security countermeasures

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

3

Welcome to Unit 2 Lecture 2 of Network security.

Examples of Network Infrastructures

- Workgroup
- SOHO
- Client/server

I'd like to start by looking at the characteristics of some of the more common classes of infrastructure starting with the workgroup.

Workgroups are normally small with limited uses. There is no central authority to manage security policies, so these are managed individually. Workgroups are often found in private or home networks where there are few if any restrictions on sharing resources.

The Small Office, Home Office SOHO is also relatively small but may have some level of central management. With the rapidly improving capabilities of network and computing equipment, the SOHO is becoming much more capable, but in general they are not very scalable. The use of centralized management allows some restriction on resource usage.

Client/Server environments are normally larger more complex network environments characterized by access controlled shared resources and formal centralized control of access and security policies. These are the types of networks found in most businesses of any significant size.

We will look at each of these in more detail in the coming slides.

Examples of Network Infrastructures

- LAN versus WAN
- Thin client and terminal services

It would be helpful at this point to address a few other terms associated with network infrastructures that aren't really considered infrastructures in and of themselves.

First, LAN or local area networks versus WAN or Wide area networks. Local area networks are normally confined to a single location such as a building, floor or department. Multiple LANs can be connected together to form a campus for example. The key is relatively close proximity.

Wide area networks connect local area networks across larger distances. WANs normally rely on the use of facilities provided by common carriers such as the phone companies to provide connectivity. WANs are often used to connect different business locations LANs.

Thin clients are computers that have little local storage – for example they would not normally have a hard disk and rely on servers or cloud services to provide the applications necessary to function.

Terminal services are typically displays connected to mainframe systems which provide all the computing and storage.

Examples of Network Infrastructures

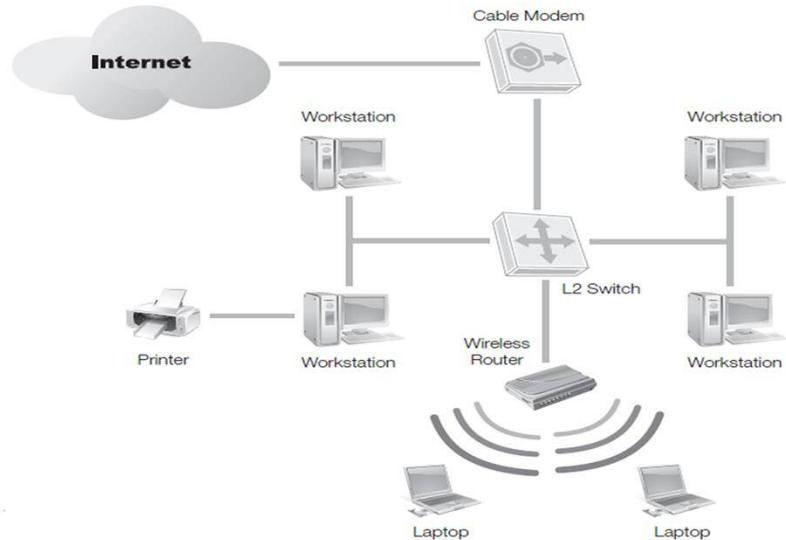
- Remote access and VPNs
- Boundary networks

A remote access link enables access to network resources on a geographically distant network. With remote access a user may perform the same functions remotely as they can as if connected to a local network.

A VPN or virtual private network is frequently used to establish a remote link. Will be looking at virtual private networks and how they can be used in this capacity as we go through this course.

A boundary network is a subnet or on the edge of a local area network. The boundary network can isolate certain activities such as programming a research from the internal environment or private lands. Another term for a boundary network is a demilitarized zone. These are formed between two firewalls which can contain resources that need to be accessed by both internal and external clients. We'll be looking at the deployment of DMZ's word demilitarized zones several times throughout this course.

A Typical Workgroup

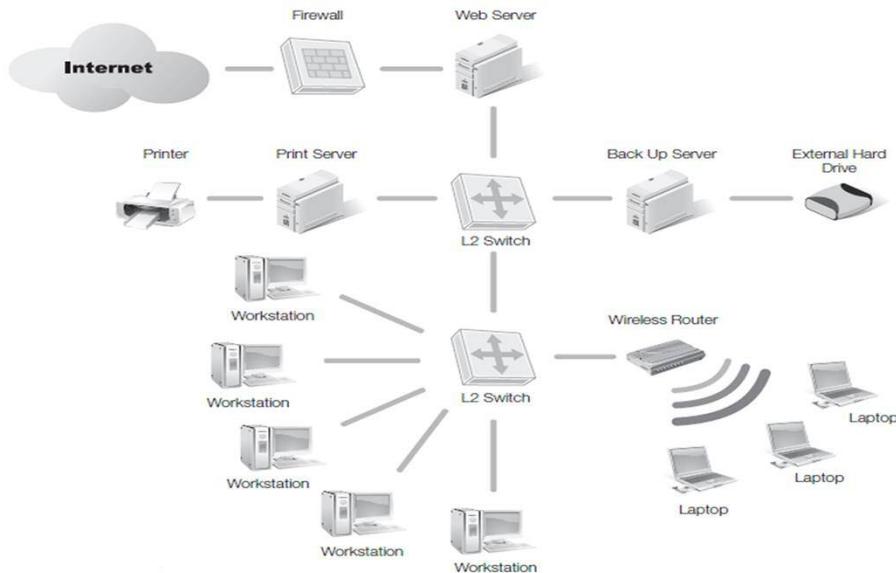


So I'd like to start by looking at a typical workgroup or small office home office. In this instance it's notable that a cable modem is used to connect the Internet through a switch to the devices contained in the network. While the cable modem may have some rudimentary firewall capabilities, it is not the traditional firewall. Consequently this configuration is subject to greater risk than a client/server environment. It's also notable that this configuration combines both wired and wireless capabilities. This is increasingly the case in our home and small office networks.

Workgroups tend to be Small with Limited uses and No central authority. The Security policy if any is managed individually.

The Small Office, Home Office may have Some level of central management. In general these environments are Not scalable and present other risks.

A Typical Client/Server Network



Looking at a typical client/server network, we see the network itself is isolated from the Internet using a firewall. A Web server sits on the trusted side of the firewall. That servers connected to a layer 2 switch which is cascaded to another layer 2 switch and the combination is used to form networks for the purpose of sharing resources.

In this particular instance, the lack of a second firewall between the Web server and the layer 2 switch creates some significant risk and exposure for this network architecture. This will become more apparent as we continue our study of network security.

Client/Server tend to be larger networks and are characterized by Shared resources, Complexity and Centralized control

A Typical VPN



In this diagram we depict the typical virtual private network connecting a remote client to a private LAN. In this case and is usually the case the VPN crosses the Internet.

Wired Networks

- Lack of external connectivity creates physical isolation
 - Can rely on physical controls to protect network
 - External threats must breach physical barrier
- If external connectivity is required
 - No control is the same as physical isolation but security must enable the business
 - Consider segmentation
 - Rigorous front door screening

Lack of external connectivity provides physical isolation

Can rely on physical controls to protect network

External threats must breach physical barrier

If external connectivity is required

No control is the same as physical isolation but security must enable the business

Consider segmentation

Rigorous front door screening

Filtering

Multiple firewalls

VPN for remote access

Connection to a wired network is limited to those directly attached to it. Physical isolation of a network require one to physically access a system connected to the network or otherwise attach to the network. However, the nature of networking is to connect networks to each other. External connectivity requires segmentation and filtering.

Benefits of Wireless Networking

- Can be inexpensive to deploy
 - No need to run wires
 - Quick connectivity for multiple users
- Convenience
- Mobility
- Ubiquity
 - All laptops now come equipped with wireless

Wireless Concerns

- Introduces new attack surface
 - Require additional design considerations to mitigate attack
- Data is transmitted over the air and accessible
 - Use of encryption technology
 - Consider implementing segmented wireless networks
 - Require VPN authentication for wireless access
- Network can be directly accessed from a distance
 - Shielding

Introduces new attack surface

Require additional design considerations to mitigate attack

 MAC filtering

 Hidden SSID

 Authentication

Data is transmitted over the air and accessible

 Use of encryption technology

 Consider implementing segmented wireless networks

 Require VPN authentication for wireless access

Network can be directly accessed from a distance

 Shielding

Consider Business Requirements

- Availability of the network and its components
 - Redundancy
 - High availability
 - Single point of failure
 - Denial of service
- Sensitivity of the data
 - Encryption
 - Access control

Availability of the network and its components

Redundancy

High availability

 Active/Active

 Active/Passive

 Hot Standby

 Cold Standby

Single point of failure

Denial of service

Sensitivity of the data

Encryption

Access control

Internet Exposure

- Remote access
 - Will a VPN work?
 - Is direct internet access required?

Availability of the network and its components

Redundancy

High availability

 Active/Active

 Active/Passive

 Hot Standby

 Cold Standby

Single point of failure

Denial of service

Sensitivity of the data

 Encryption

 Access control

A system that needs to be accessed remotely can add additional concerns. Accessing a system over a VPN connection will ensure that the system maintains much of the security associated with the corporate network. If a system requires a direct connection to the internet for external users or customers one may need to consider additional firewalls, the creation of a DMZ, or additional SSL encryption.

Mobile Networking

- Allows user to be completely mobile
- Requires considerations for central management
- Potential for device to be lost

Security Countermeasures

Common Countermeasures	Uses	Benefits	Limitations
Firewalls	<ul style="list-style-type: none"> ▪ Filter traffic ▪ Segmentation 	<ul style="list-style-type: none"> ▪ Hardware ▪ Software ▪ First defense ▪ Keep noise out 	<ul style="list-style-type: none"> ▪ Perimeter defense ▪ Not content oriented ▪ Limited to yes or no
Virtual Private Network (VPN)	<ul style="list-style-type: none"> ▪ Remote access ▪ Encrypted tunnel 	<ul style="list-style-type: none"> ▪ Private tunnel ▪ Extends Cover 	<ul style="list-style-type: none"> ▪ Man-in-the-middle ▪ Not traffic oriented
Intrusion Detection/Prevention System	<ul style="list-style-type: none"> ▪ Monitor traffic ▪ May block attacks ▪ Host or Network 	<ul style="list-style-type: none"> ▪ Notification ▪ Prevention 	<ul style="list-style-type: none"> ▪ Relies on signatures ▪ False positives

Security Countermeasures (Continued)

Common Countermeasures	Uses	Benefits	Limitations
Data Loss Prevention	<ul style="list-style-type: none"> ▪ Monitor data loss ▪ Block data loss 	<ul style="list-style-type: none"> ▪ Sensitive Config ▪ Breach Notification 	<ul style="list-style-type: none"> ▪ Signature reliant ▪ False positives ▪ Circumventable
Security Incident and Event Management	<ul style="list-style-type: none"> ▪ Aggregate sec logs ▪ Correlate sec logs 	<ul style="list-style-type: none"> ▪ Monitor and review ▪ Generate alerts 	<ul style="list-style-type: none"> ▪ False positives ▪ Data heavy ▪ Limit to log info

Security Countermeasures (Continued)

Common Countermeasures	Uses	Benefits	Limitations
Continuous Control Monitoring	<ul style="list-style-type: none"> ▪ Checks config ▪ Standard compliant ▪ Real time monitor 	<ul style="list-style-type: none"> ▪ Automate monitors ▪ Self correction 	<ul style="list-style-type: none"> ▪ Emerging tech ▪ Policy dependent
Vulnerability Assessment	<ul style="list-style-type: none"> ▪ Tests systems 	<ul style="list-style-type: none"> ▪ Proactive address ▪ Centralize tracking 	<ul style="list-style-type: none"> ▪ Limited to known ▪ Create noise

Trust – Computers and Networks

- The confidence that other users will act in accordance with your organization's security rules
- The belief that others are trustworthy
- Third-party trust systems
 - Example: Digital certificates that a public certificate authority issues

Network Security Components Used to Mitigate Threats

- Hosts and nodes
- Firewalls
- VPNs
- Proxy servers
- Network address translation

Network Security Components Used to Mitigate Threats

- Routers, switches, bridges
- The Domain Name System (DNS)
- Directory services
- Intrusion Detection Systems and Intrusion Prevention Systems

General Terms

- Confidentiality
- Integrity
- Availability
- Trust
- Privacy
- Authentication
- Authorization
- Nonrepudiation

Networking Terminology

- Network
- Firewall
- Router
- Virtual Private Network
- IPSec
- Demilitarized Zone
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)

End of Lecture 2



of Lecture 2

24

This ends Lecture 1 of Unit 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Introduction to Unit 3

Lecture 1

Unit 3 Lecture Topics

Topics:

- Malware and application vulnerabilities
- Risk assessment for network infrastructure
- Wired and wireless network infrastructure risks, threats, and vulnerabilities
- Common network hacking tools: applications, exploits, and attacks
- Social engineering practices and their impact on network security efforts

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

2

Welcome to Unit 3 of Network security.

In this unit we're going to be discussing malware and application vulnerabilities. We'll be looking at the process of risk assessment for network infrastructures and will be examining wired and wireless network infrastructure risks, threats, and vulnerabilities. We'll be looking at common network hacking tools and will be examining social engineering practices.

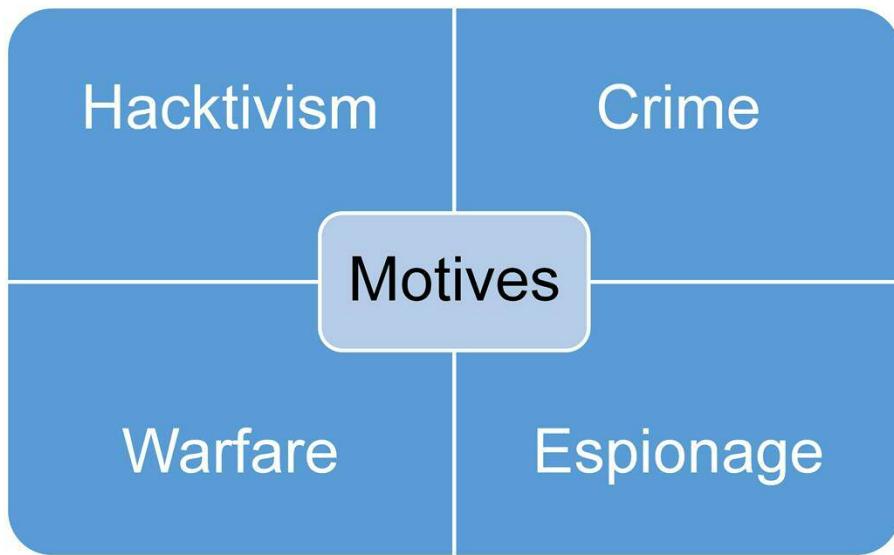
Learning Objectives

At the end of this unit, the student will be able to:

- Describe hacker motivations
- Describe the nature of Risk in networks
- Describe the different classes of exploits
- Explain how hackers operate
- Recognize the impact that malicious exploits and attacks have on network security

Our learning objectives for this unit are to describe hacker motivations, describe the different classes of exploits, explain how operators perform their tasks. We'll also learn to recognize the impact of malicious exploits and attacks have on network security.

Hacker Motivation



Let's start by looking at hacker motivation.

It's commonly accepted today that hacker motivations have changed over the last decade or two. What was once a benign exploration of networks their devices and their weaknesses evolved into a much more malicious venture. While there are certainly individuals that continue the tradition of exploring network flaws and weaknesses to gain status among their group of friends, most hackers today have more serious motives.

In general motivations can be broken into four different groups.

- Hacktivism is the process of using computers and networks to make political statements and express political and social views. So long as hacktivists do not cross legal boundaries their activities can be considered a form of free speech. This however is a fine line and one that is easy to cross.
- Crime is a general category that covers a number of hacking activities. The primary motivation here is financial gain. Criminal activities are currently dominated by well organized and well funded criminal organizations many of whom are based outside of the jurisdictions that might seek to control their activities.
- Espionage is conducted at a corporate and state level. Corporations and businesses seek to gain competitive advantage by stealing the intellectual property of others rather than investing the time and effort and money that it takes to develop that intellectual property on their own.

- Lastly there is warfare. As our society and world has become more interlinked with the proliferation of the Internet in distributed computing, it has become increasingly apparent that nation states have the capability of inflicting significant damage to critical infrastructure in times of war.

Favorite Hacker Targets

- Easy assets – those that pay off quickly
 - Monetary gain
 - Control of networks
- Unique targets
 - Challenging

Amateur hackers, and I'll use that term for hackers are not associated with a criminal organization, look for relatively easy targets. Typically these are ones that can create quick money. Gaining control of networks and large numbers of computers creates the opportunity for ongoing income by selling time on these botnets.

Occasionally they'll go after unique targets just because of the challenge of doing so.

Some of the techniques used by hackers to achieve their goals include:

Social engineering where users are attacked using psychological techniques such as

persuasion or impersonation in order to gain access to facilities or computing resources

Phishing, a form of broadcast email (aka spam) where users are tricked into giving away information such as login/passwords via fraudulent e-mail

Trojan horses & Spyware where users are tricked into installing malware on their systems

We'll look at each of these in more depth later in this course.

Favorite Hacker Targets

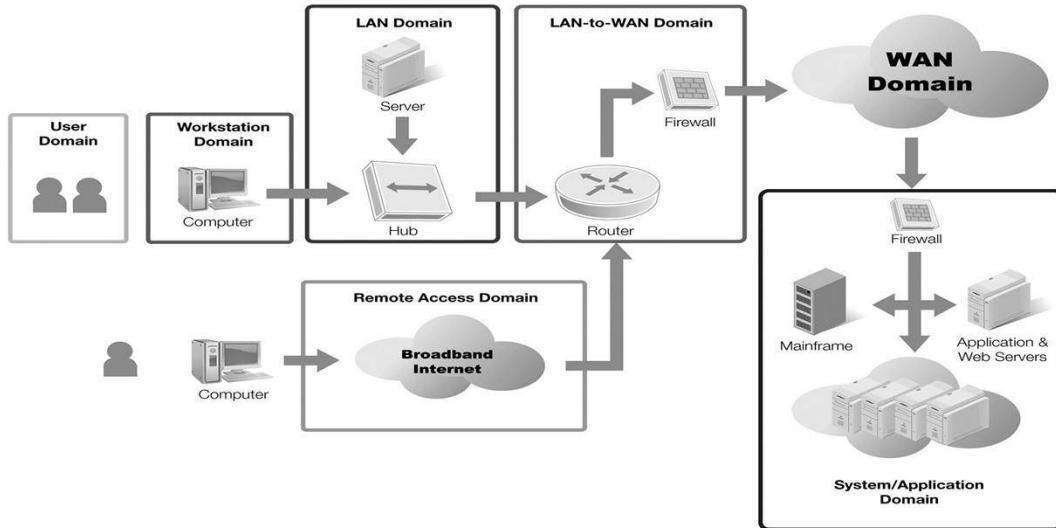
- Easy assets – those that pay off quickly
 - Monetary gain
 - Control of networks
- Unique targets
 - Challenging

Other techniques used to gain access to networks and systems by hackers include identifying and taking advantage of **Vulnerabilities**.

These may include taking advantage of Weak security procedures or Weak physical security. These types of attacks center around the user domain.

Many of the attacks at the user level use social engineering techniques. These will be explored in more depth later in this lecture.

Seven Domains of a Typical IT Infrastructure



I'd like to go back to the seven domains of the IT infrastructure and look at the types of vulnerabilities and threats which can be applied to each of them. We'll start with the user domain.

User Domain



Any individual associated with the organization, including users, employees, managers, contractors, or consultants, even if they don't have logins.

- Threats
- Vulnerabilities
- Risks

Threats in the user domain include

Social engineering, Phishing, and Trojan horses & Spyware. More generally, phishing would include spear phishing, whaling and other email social engineering techniques. Trojan horses and spyware would include any malware directed toward or facilitated by users.

Vulnerabilities in the user domain center around weak procedures and weak physical security.

Examples:

- A social engineer calls up IT pretending to be a user and gets a password reset, thereby gaining access to a user's account.
- A social engineer impersonates maintenance staff or a repair person and installs keylogging devices on computers.

Risks that can be realized when users are exploited include:

Unauthorized access to facilities, Compromised user accounts, and Unauthorized access to data.

The risk of damage from user-based attacks is high. For example, a successful social engineering attack in which an account is compromised allows the attacker to bypass security controls.

Workstation Domain



Workstations, stand-alone systems, home computers

- Threats
- Vulnerabilities
- Risks

Threats associated with the workstation domain include

- Malware (e.g., viruses, worms, Trojans, spyware, etc.) is a significant threat in this domain.
- Port scanning can be used to find unsecured ports on a workstation, which gives the attacker insight into what type of attack may be successful
- Malicious Web sites use attack techniques such as cross-site scripting to gain access to secure Web transactions

Often, workstations are not secured as well as servers and home computers are not secured as well as business computers. Common vulnerabilities include:

- Operating systems may not be patched at all, or may be deficient in patches, particularly systems that are not often connected to the network such as laptops.
- Operating systems may be patched, but users and IT staff may forget to patch applications or may choose not to because it is time consuming and perceived as low risk.
- At home or in organizations where password policies are not centrally administered, systems may have weak passwords or even no passwords.
- Unless specifically prohibited by security policy, the average user is likely to be using an account with administrative privileges, which means that any exploit taking place under the user's account is doing so with elevated privileges.

-Unless enterprise-level, managed antimalware software is used, there is a chance that malware definitions are not up to date, that scans are not conducted frequently, or that certain functionality has been disabled. For systems that are not connected to the network 24x7, definitions may be significantly out of date.

- Workstations may not be protected by firewalls (hardware or software). Home computers may be attached directly to the internet via cable modem.

Risks

Compromised systems can be used to attack others, Data exposure, loss, or change, Loss of availability

The risk depends on the environment. A compromised home computer may not affect the home user at all; however, while that user sleeps his computer may be conducting denial of service attacks on corporate networks. Alternatively, that same home user could have his bank account login credentials compromised and find that all his money has been transferred to a numbered account in the Cayman Islands. A compromised corporate workstation can lead to loss of confidential or proprietary data such as customer financial information, trade secrets, or payroll information. That compromised system may also be used as a stepping stone to other systems within the network.

LAN Domain



Hosts on private LANs

- Threats
- Vulnerabilities
- Risks

Threats

The specific threat depends upon the organization and its assets. Generally speaking, however, threats are electronic, natural or human.

-Electronic or logical threats include malware, malicious code, botnets, and software bugs

-Physical threats include hardware failure, natural disasters, and accidental or purposeful damage to equipment

-Human threats include disgruntled employees, poorly trained employees, hackers

Vulnerabilities

Like threats, vulnerabilities are specific to the organization and its resources. For example, different operating systems have different vulnerabilities. Generally, vulnerabilities are caused by weak security procedures, weak security controls, and weak perimeter controls.

Risks

Compromise of one host may result in compromise of the enterprise, Data exposure, loss, or change, or even Disruption of business

The risk depends on the environment, the organization's business, the type of assets it has, etc. Basic risks, such as data loss, change, or theft and disruption of business, apply to all organizations. Additionally, it should be stressed that compromise of one host on a network may result in compromise of the enterprise.

LAN-to-WAN Domain



Routers, firewalls, other devices at the LAN/WAN connection point

- Threats
- Vulnerabilities
- Risks

Threats

-Port scanning: Sequential port scans can be conducted from the public Internet side, revealing details of configuration that may allow an attacker to better profile additional services.

-DoS/DDoS: Because it is a gateway, it is a constrained point with limited bandwidth and the act of filtering increases latency per connection. It is easily saturated.

-Directed attack: The WAN connection is exposed to the public Internet and so is directly accessible.

Vulnerabilities include: Weak perimeter security, Remote access to routers and gateways, Weak or default firewall passwords

Incorrect configuration

Misconfiguration – due to complexities in rules sets, if careful planning is not performed in advance misconfigurations can result.

Risks

If an attacker gains control of the firewall, they can easily disrupt gateway functions and create network instability.

This can lead to Unfiltered malicious traffic, Loss of availability, Disruption of business

Remote Access Domain



Organization resources via remote access through dial-up, wireless, or standard broadband Internet connection

- Threats
- Vulnerabilities
- Risks

Threats

Malware on the remote client

War driving/Netstumbling

Rogue hotspots: If a VPN is not used, remote clients using rogue hotspots risk having their session captured.

Rogue wireless access points and ad hoc wireless within the organization can provide an attack vector into the network.

Vulnerabilities

Unencrypted wireless access points

Local cache of data on remote client

Weak security controls on remote client

Risks

Any service designed to give someone remote access can be exploited remotely

Compromise of a remote system could result in organizational compromise, bypassing network controls

Many remote access systems create encrypted sessions that do not allow direct inspection of packet contents, for example remote desktop protocol [RDP].

Mobile connectivity happens in the open – broadcast traffic is omnidirectional and can be intercepted anonymously

WAN Domain



WAN infrastructure elements, such as routers, switches, and firewalls

- Threats
- Vulnerabilities
- Risks

Threats

Eavesdropping – Unencrypted traffic can be intercepted.

Availability – The organization does not control the WAN.

Anonymity – Attackers are anonymous when coming in from the WAN because they can spoof their origins or distribute their attacks (e.g., botnets).

Interception/Proxy attacks – Because data moves through a public network, interception along the route of transit allows numerous attacks such as man-in-the-middle.

Vulnerabilities

Dependence on DNS – DNS poisoning or DNS spoofing can compromise traffic intended for hosts and services located in the LAN. Lack of Endpoint Validation – It is possible to construct a TCP/IP packet spoofing its origin, thus concealing backtracking efforts

Countries of convenience – Attackers may conduct their activities using systems located in countries with laws conducive to obscuring originating traffic or without law enforcement support.

Risks

A successful attack on the root DNS servers could cripple name resolution Internet-wide.

Clear-text traffic can be intercepted, rerouted or changed

Compromise of WAN infrastructure elements is undetectable by the organization.

WAN routing involves wide geographic areas and may pass traffic through unknown geopolitical areas.

Without knowing where it's going, natural disasters, power failures, and other wide area-

effecting issues could compromise availability. Laws involving data exposure may be different in other geopolitical areas.

System/Application Domain



Servers, applications, databases, data

- Threats
- Vulnerabilities
- Risks

Targets: Databases are attractive targets because they contain a large amount of information.

System Application domain Threats include: Cross-site scripting (XSS), Buffer overflows, SQL Injection, and Dos/DDos

System Application domain Vulnerabilities include: Use of default passwords, Weak security controls, Non-patched operating systems/applications Cached credentials, and Insecure coding practices

Risks would include: Use of unencrypted protocols can allow compromise of data in transit, Lack of code review can introduce instability, Data exposure, change or loss, DoS attacks against one service can also prevent function of other services on the same host

Port Scanning

Mechanics	Uses
<ul style="list-style-type: none">▪ TCP or UDP packets are sent to ports on a system▪ Scanning performed on single IP address or IP address range▪ Open ports can verify:▪ Indicators of open ports▪ Noticeable and detectable	<ul style="list-style-type: none">▪ Useful to both hackers and security professionals▪ Hackers▪ Security Professionals

Before we move on to the next lecture on Malware, I'd like to introduce port scanning. Port scanning is a technique used by security professionals and hackers. Security professionals conduct periodic scans as part of vulnerability scanning as well as to determine what systems and applications may be present on networks.

Vulnerability scanning will be discussed in more detail in Unit 4.

From a practical standpoint, TCP or UDP packets are sent to ports on a system either on single IP addresses or a range of IP addresses looking for open (responding) ports.

Discovered or Open ports can verify:

- Presence of a system on the network – when the system responds
- Particular services that are running on systems

Open ports are indicated

- TCP: Full TCP three-way handshake established
- UDP: Lack of response may indicate open port since closed ports usually generate errors

Noticeable and detectable

Port scanning is useful to both hackers and security professionals. For Hackers, Port scanning can: Determine existence of hosts and Determine existence of protocols and services

Security Professionals can use port scanning to Determine the existence of rogue hosts and servers – that is unauthorized installations of equipment on the network

Port scanning is a normal Part of a vulnerability scan

Summary

- What are hackers after
- Threats, Vulnerabilities & Risk in the seven domains
- Wired and wireless network infrastructure risks, threats, and vulnerabilities
- Port Scanning

In this lecture, we have taken a brief look at what hackers motives are and what they are after

We have examined the vulnerabilities, threats, and risks associated with the seven domains of the IT environment

We have begun the process of comparing and contrasting wired versus wireless networks
And lastly, we started our discussion of port scanning.

End of Lecture 1



of Lecture 1

17

This ends Lecture 1 of Unit 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 3

Lecture 2

Malware ~ Malicious Code

Distribution Methods

- Software downloads
- E-mail
- Malicious web sites
- File transfer
- Flaws in software

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

Malware, Also known as malicious code is Distributed through a number of different channels. These may include distribution by:

Software downloads, E-mail, Malicious Web sites, or File transfers. Flaws or vulnerabilities in software may also allow the introduction of malware.

Malware can cause a number of problems including: Data loss, exposure, or change; Poor system performance; Pop-up ads,
Or it's possible that the System becomes a "bot" or "zombie" in control of the attacker

Malware ~ Malicious Code

Effects of Malware

- Data loss, exposure, or change
- Poor system performance
- Pop-up ads
- System becomes a “bot” or “zombie”

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

Malware can cause a number of problems including: Data loss, data exposure, or change, Poor system performance or proliferation of Pop-up ads.

In some cases, the infected system can become a “bot” or “zombie” under the control of the attacker.

A current and very dangerous trend is the introduction of ransomware which encrypts your data and demands payment for the decryption keys.

In effect, system and data confidentiality, integrity and accessibility may be impacted by malware.

Common Types of Malware

- Viruses and Worms
- Trojan Horses
- Keystroke Loggers (“keyloggers”)
- Spyware and Adware
- Rootkits
- Logic Bombs
- Trapdoors and Backdoors
- URL Injectors and Browser Redirectors

These are some of the more common types of malware that can affect your systems. We will look at each group in more detail in the coming slides.

Malware: Viruses and Worms

- **Viruses**

- Infect boot sectors or files, such as executables, drivers, and system objects
 - Need user interaction to spread

- **Worms**

- Infect systems
 - Don't need user interaction to spread
 - Can be carriers for other types of malicious code

- Viruses have been around since the beginning of the computer age. The first one was created in 1949 long before the creation of the personal computer. A virus can Infect boot sectors or files, such as executables, drivers, and system objects.

- Viruses Need user interaction to spread. This means the user has to execute the file either directly or as part of the execution of another program for it to become active. Most viruses Spread file to file upon opening and may spread to other systems through e-mail or network shares. Originally, a virus was considered a success if it was able to spread very quickly over a wide geographic area. A virus can consume all the resources in a system through their replication and transit. Today, a virus can be much more malicious burrowing deep within your systems where they can wait until they are executed after which they can collect sensitive data to pass on to their makers. Viruses may also erase or damage data on your systems.

- Worms also Infect systems, but Don't need user interaction to spread. They can Scan systems for flaws and Exploit those flaws to infect yours or other systems. Worms Can be carriers for other types of malicious code.

Malware: Trojan Horses

- Delivery method for a malicious payload
- Usually appear to be a benign program, such as a game or utility
- Installed by users without knowledge of malicious payload
- Allows remote access to attackers

A Trojan horse is a piece of software that masquerades as something it is not. For example, the program may appear to be a handy on-screen calculator but may actually conceal a keylogger capturing all your keystrokes to be transmitted to a waiting hacker. Frequently trojans have a phone home function that allows the information they collect to be returned to the programs maker or some other site designated by the creator of the malware. The program may also open a channel or back door for the malware maker to enter your computer.

Malware: Keystroke Loggers

- Also called “keyloggers”
- Software-based keyloggers can be installed via worms or Trojan horses
- Record keystrokes and transmit them to the attacker
- Hardware-based keyloggers

- Keystroke loggers also called “keyloggers” are pieces of software that can be installed via worms or Trojan horses.
- They are designed to Record keystrokes and transmit them to the attacker via E-mail, FTP or Instant message.
- The attacker hopes to collect user names and passwords to other potential targets like your bank account. With this information, they can use your credentials to empty your accounts.
- Hardware-based keyloggers are relatively unobtrusive devices that are placed Inline with keyboard cable or In the keyboard itself. These can provide the same functionality as software keyloggers or they can work ‘offline’ collecting key strokes until removed by the attacker for data recovery.

Malware: Spyware and Adware

- Spyware
- Adware
- May be bundled together
- May be embedded in other programs
- May masquerade as antimalware product

Spyware

Monitors and records user activities, like keylogging software
Transmits information back to originating author

Adware

Similar to spyware
Delivers advertising through pop-ups, e-mail, or browser redirection
May be bundled together
May be embedded in other programs
They have also been known to masquerade as antimalware products
Some examples would include:

BonziBuddy
Gator/Gain Ad Server adware
Antivirus 2008

Malware: Rootkits

- Codes that position themselves between the operating system kernel and hardware
- Allows attacker to gain root/administrative access to system
- Uses of rootkits

Rootkits are one of the more dangerous forms of malware. Rootkits are Codes that position themselves between the operating system kernel and hardware.

This allows an attacker to gain root/administrative access to the entire system bypassing the normal security controls.

Rootkits can be used to:

- Take control of a system
- Hide data files
- Hide other malware or hacker tools

Malware: Logic Bombs

- Malicious code that lies dormant until triggered
- Triggering events
 - Time and date
 - Program launch
 - Keyword
 - Accessing a URL

Logic bombs lay dormant until they are triggered by some event. The event may be a time or date, entering a keyword, launching a program or other specific event that is programmed into the bomb. Another variant of the logic bomb requires a specific input periodically to prevent it from running. This type is sometime used to ‘cover one’s tracks’ or do damage by deleting files if an employee thinks they may be fired. If they are dismissed and removed from the job immediately, the software will, without the correct intervention, do what it is designed to do authomatically.

Malware: Backdoors and Trapdoors

- Synonyms for the same type of malware
- Bypass normal authentication or security controls
- Benefits to the attacker
- Examples of backdoors and trapdoors

Backdoors and trapdoors are Synonyms for the same type of malware
They are designed to bypass normal authentication or security controls and
May allow attacker to:

- Gain remote access to the system
- Alter files and system settings
- Install hidden software
- Gain control of the system
- Turn the system into a bot
- Use the system to send spam

Some Examples from the past:

- Back Orifice – Early Microsoft Windows program designed for remote access and administration but also had malicious properties
- Mydoom virus – Installs a back door on the infected computer

Malware: URL Injectors and Browser Redirection

- Also called browser hijacking
- Replace URLs with alternative addresses
- Redirect browser to target Web sites
- May also change browser home page
- May prevent access to anti-malware Web sites
- May inject entries into HOSTS file
- Other malware may contain URL injector code

URL injectors and browser redirection malware are designed to send your browser to target websites of the attackers choosing. This may be to a site that will download malware to the unsuspecting user or mimic a site such as their bank to steal credentials. Less malicious redirections may be used to collect click through points which can be redeemed for cash by the hacker.

The hosts file is a local legacy file that maps URLs to their IP addresses like the DNS system.

Advanced Persistent Threat

- Highly targeted
- Targeting intelligence often gleaned from other types of attacks
 - Phishing
 - Social engineering
- Occurrence has increased dramatically but represents a small percentage of attacks

One term that has recently taken the media by storm is Advanced Persistent Threat. These threats are typically state sponsored low and slow attacks designed to go undetected for long periods of time. Malware hides quietly with periodic intermittent reporting back to the command and control center. Information is quietly collected, concealed – usually using custom encryption, and transferred out in very small quantities on an irregular and intermittent schedule. This prevents detection by most IDS/IPS systems as well as other detective controls.

Targets for advanced persistent threats are often the victims of phishing attacks or social engineering. These techniques are frequently successful at introducing malware in an environment.

These attacks often require extensive planning and frequently use malware specifically designed for the environment it will be used in. This greatly decreases the probability of it being discovered by any existing anti-malware programs, most of which look for known signatures.

Impact of Malware on Organizations

- Melissa Virus caused \$80 million in damages in North America
- SQL Slammer Virus
- Code Red

Melissa virus caused \$80 million in damages in North America
SQL Slammer virus

\$1 billion in damages
Bank of America ATMs unavailable
Continental Airlines flights delayed or canceled

Code Red
300,000+ computers infected
Denial of service
Cisco DSL routers stopped forwarding traffic

Sources:

Sophos http://www.sophos.com/pressoffice/news/articles/1999/12/va_melissa.html
CNET <http://news.cnet.com/2009-1001-983540.html>
CNET <http://news.cnet.com/2100-1001-270314.html&tag=txt>

Application Vulnerabilities

- Buffer overflow
- SQL Injection
- Cross-site scripting (XSS)
- Cached credentials

While not technically malware, application vulnerabilities do present an opening to attackers which may facilitate the introduction of malware into systems. Application vulnerabilities may allow execution of arbitrary code or provide an attacker the ability to take control of the system by crashing the application. Typical application vulnerabilities include:

Buffer overflow

- Injection of more data than a memory buffer can hold
- May result in arbitrary code execution

SQL Injection

- Inserts code via un-sanitized data input on Web sites
- Allows access to back-end databases

Cross-site scripting (XSS)

- Attackers insert client-side script into Web pages
- Allows malicious scripts to be run in the user's context

Cached credentials

- Credentials stored on local machine, for example browser cache
- Can be discovered by and reused by an attacker

Mitigating Application Vulnerabilities

- In-House Coding
- Operating systems or applications
- Vulnerability scanning
- Open Web Application Security Project (OWASP) for Web application security

Mitigating vulnerabilities starts with the coding process. For in-house coding, the organization should implement secure coding practices. Including security in the software development life cycle provides a different insight into future potential problems. Also, perform testing and quality control. There are some excellent code testing applications to help identify common software coding errors and suggest fixes for them. Code testing application come in two varieties, static and dynamic. Static testers go through code line by line looking for errors. Dynamic testing actually runs the code and provides various inputs looking for flaws in the code.

For operating systems or applications, the organization must keep abreast of vulnerabilities. This can be done by monitoring the manufacturers web sites. In addition, there are several other sites that post vulnerabilities such as the National Vulnerability Database (www.nvd.nist.gov), the US-CERT Vulnerability Notes Database (www.kb.cert.org/vuls/), and the SecurityFocus (www.securityfocus.com/vulnerabilities) web site.

Of course information is only as good as the organizations ability to apply patches and updates in a timely manner.

Periodic vulnerability scanning should be performed this is critical for organizations that have compliance requirements.

Programmers should be aware of and utilize the Open Web Application Security Project (OWASP) for Web application security Web sites. These contain excellent information about secure coding practices that can help

avoid costly and dangerous errors in coding.

End of Lecture 2



of Lecture 2

17

This ends Lecture 2 of Unit 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Introduction to Unit 3

Lecture 3

What is Risk?

- Risk has several meanings
 - Danger
 - Consequences
 - Likelihood or probability
- Definition of risk in formal risk assessment

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

Risk has several meanings. Some of the common interpretations of risk are:

Danger

Consequences

Likelihood or probability

In a formal risk assessment we

define risk as A measurement based on the relationship between likelihood and impact.

More specifically, risk is the probability of a impact to an organization as the result of a successful threat exploiting a vulnerability.

Risk Assessment Methodology

- Identification
- Analysis
- Determine risk for each threat-vulnerability pair
- Prioritize mitigation efforts

We can define risks through a number of different methodologies, but most follow steps similar to these:

The first step is Identification. We need to:

Identify assets so we know what we are protecting.

We need to Identify potential threats that exist against those assets.

Next we need to Identify vulnerabilities that exist within those assets.

Finally, we need to Identify existing security controls.

During the Analysis phase, we

Identify threat-vulnerability pairs by matching threats with vulnerabilities to create exploit scenarios.

Analyze the effectiveness of existing controls.

Determine impact of a successful exploitation. This means predicting what will happen to our asset and organization.

Determine likelihood of a successful exploitation. This is often the most difficult task to accomplish. The lack of sufficient actuarial data often forces us to guess.

After identification and analysis, we can build a matrix of threats and vulnerabilities and Determine risk for each threat-vulnerability pair using a risk matrix.

This allow us to Use the results to prioritize mitigation efforts.

Measuring Risk

- Risk = Impact x Likelihood
 - Impact: The consequence of a successful exploitation of a vulnerability
 - Likelihood: How probable is it that an impact will occur?
- Risk can be measured

Risk = Impact x Likelihood

Impact: The consequence of a successful exploitation of a vulnerability can be Financial, damage to a companies Reputation or issues with Compliance

Likelihood: How likely is it that an impact will occur?

Risk can be measured. There are two common approaches to measuring risk:

Qualitatively: Low, Moderate, High

Quantitatively: Numerical value

IT risk assessment is usually qualitative **because it is difficult to obtain quantitative values.**

As an example of quantitative versus qualitative, Insurance companies use actuarial data in order to quantitatively determine risk for the purpose of setting rates. If one lives in an area prone to natural disaster, homeowner's insurance rates will be higher than for one who does not. If one lives in a high crime area or has a make/model of car that is popular to steal, then auto insurance rates are higher than if one lives in a low crime area and has a vehicle unattractive to thieves. Insurance companies have access to actuarial data that allow them to put a number to likelihood and the impact is the financial loss of the property.

IT does not have the same type of actuarial data and it is difficult to put a dollar value on many of the impacts that can be caused by a successful security incident. Impact is often more than just financial loss – it can involve reputation, employee morale, customer

satisfaction, or regulatory issues. It may also depend on the industry, the type of data, and where in the world the data is stored, processed, and transmitted. There are other qualitative components, such as what is important to management, that cannot be addressed in a quantitative risk assessment.

Risk Matrix				
		Likelihood		
		Low	Medium	High
Impact	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Critical

We can create a risk matrix using the likelihood and impact using qualitative measures. This is what one would look like

Hacking

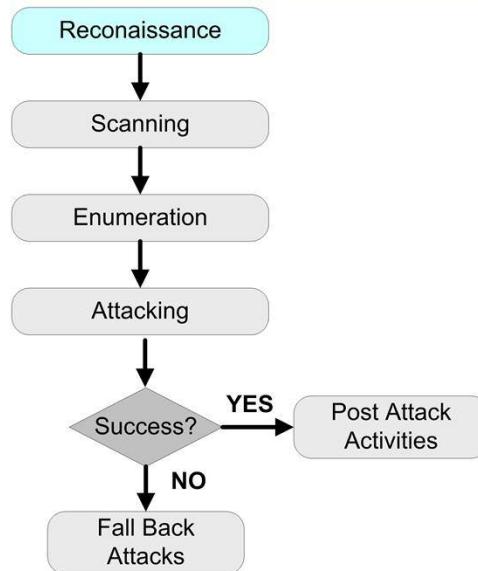


Slide 6

Let's switch gears for a bit and look at hacking. Hackers are not necessarily the highest risk producers in any particular environment, but they tend to get the greatest attention. Perhaps that is because of the media or perhaps of a deep seated paranoia of unknown and unseen malicious actors bent on stealing our hard earned assets. In any case, hackers are a real threat and must be addressed in proportion to the realistic potential damage they can produce.

Hackers operate by following a well known set of procedures which we will look at next.

The Hacking Process: Reconnaissance



Hackers begin with reconnaissance. They are not typically indiscriminating in their targets. Their motivations cause them to gravitate to certain types of companies or organizations that can satisfy their needs. Those hacker seeking financial gain may look for targets that handle large volumes of credit cards. Hackers seeking intellectual property look for businesses that create or store the type of IP they are looking for. Regardless of the motive, the process normally begins with reconnaissance.

The Hacking Process: Reconnaissance

Examples of information sources:

- Web research
- Search engines
- Background checks
- Newspaper searches
- Press releases
- Job openings
- Social networking
- Public records
- Eavesdropping
- Physical surveillance

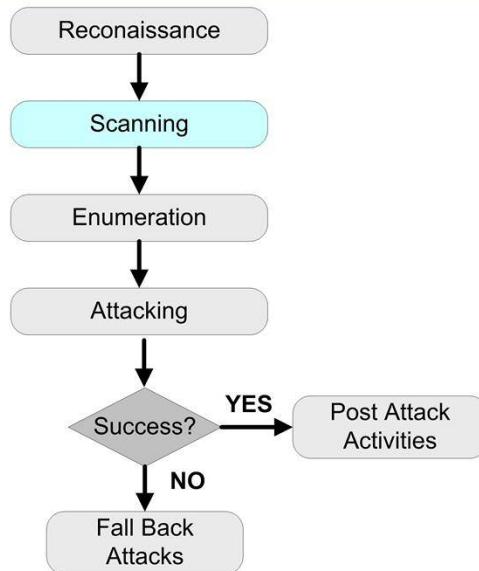
Slide 8

Here are some of the typical sources that can be used in reconnaissance. This is by no means comprehensive. Motivated hackers will use multiple sources of 'intel' to build as complete a picture of their target as possible.

Hackers normally begin with the easiest and safest types of reconnaissance. These would include web research, using search engines, newspapers, public releases, public records and job openings. These are all sources that are openly available and might be accessed by anyone interested in working for or investing in the company. Normally these sources will yield enough information to lay out a good plan of attack.

If sufficient information is not collected through public methods or more detailed and specific information is needed, the hacker can use background checks, social networking, eavesdropping and physical surveillance. These pose a bit more risk for the hacker so the motivation would need to be there to do these.

The Hacking Process: Scanning



Once a hacker has identified some potential targets, the next step is scanning. Scanning looks for exposed IP addresses and the ports that are open. Open ports can help identify what protocols, services and applications that may be running on the systems being scanned. The ports and protocols along with any other information such as versions numbers that can be captured are collected for further analysis.

The Hacking Process: Scanning

Examples of scanning terms:

- War dialing
- War driving
- Netstumbling
- Ping sweeps
- Port scanning

Slide 10

Here are some examples of scanning terms. War dialing is virtually obsolete. It was used when modems were used to provide remote access to and from computer systems. War dialing programs were provided a range of telephone numbers which were automatically called. If the called number responded with a modems tone, then that number was flagged for later use.

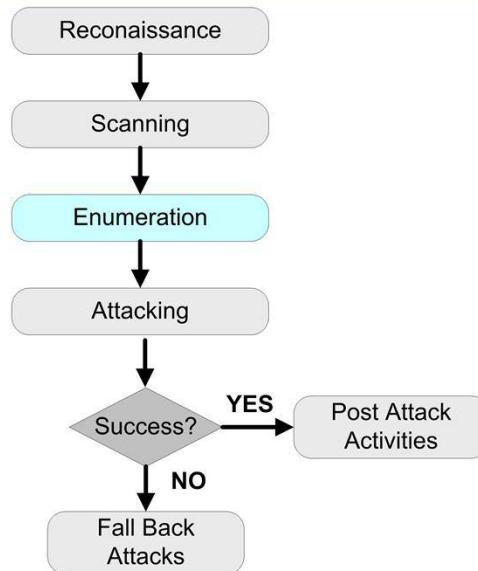
War driving uses a laptop and specialized software that collect information about wireless networks. These programs may provide GPS tags for identified wireless networks along with the SSID, frequency, manufacturer of the Access Point(s), any encryption that may be used and so forth. Some software packages can even attempt to crack weak encryption technology.

Netstumbling is another term for war driving that is derived from one of the more popular war driving utilities called Netstumbler.

Ping sweeps function much like war dialing for wired networks. The utility is provided a range of IP addresses to scan and simply sends out a ping package. Responding IP addresses are noted for later action.

Port scanning, scans specific IP addresses looking for open ports and protocols.

The Hacking Process: Enumeration

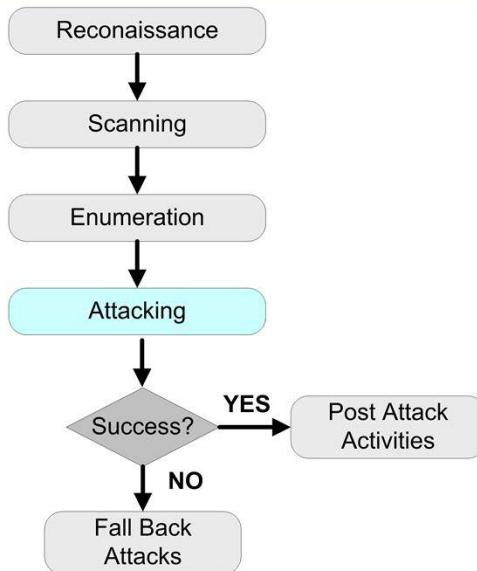


Enumeration is usually lumped in with scanning. This is where the results of the scans are collected and the information about the target details are produced. Typically the operating system(s) can be identified along with the protocols, services and potentially applications. Usually, versions can be determined through banner grabbing. Nmap, a free scanning tool is frequently used to gather this information. It should be noted that Nmap is a tool used for many legitimate purposes and is not considered a hacking tool.

A follow on to the enumeration process is identifying vulnerabilities present in the identified software that can be used in the next stage.

- Discover target details
- OS identification
 - Nmap
- Service identification
- Banner grabbing
- Identify vulnerabilities

The Hacking Process: Attacking

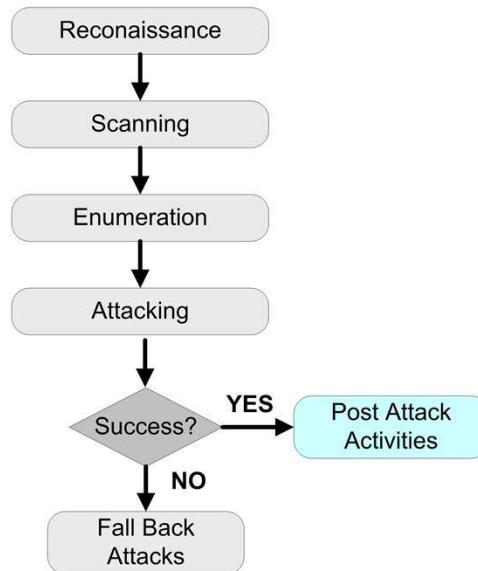


Attacking is the process of exploiting vulnerabilities. This can be done for a number of purposes, but one primary purpose is to gain unauthorized access to the network or systems. From this vantage point, additional surveillance can be done which can lead to privilege escalation, the installation of additional malware, back doors or other means to maintain a quiet presence. You should be aware that unauthorized access or attempted access to networks and/or computer devices is a criminal act and should not be attempted without explicit written permission from the network owner.

If the initial attack is unsuccessful, then additional attacks against identified vulnerabilities will be exploited until a foothold can be obtained.

Attackers may Exploit vulnerabilities in the network itself, nodes on the network or applications that operate on the network to gain access.

The Hacking Process: Post-Attack Activities

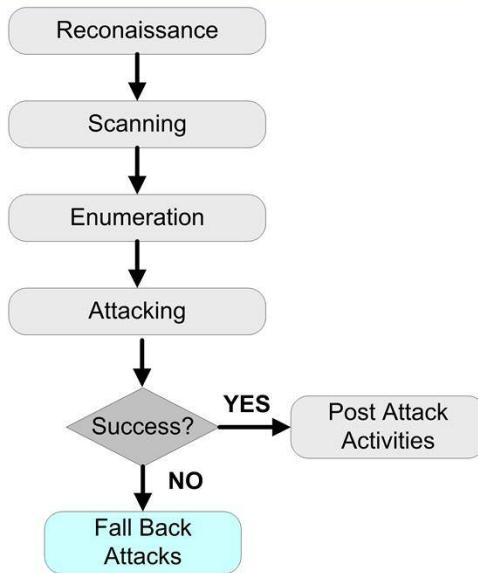


Again, if the Attack is successful, this is typically followed by attempts to Escalate privilege followed by

Installation of additional tools and creation of a back door to gain access at a later date and attempts to Accomplish their objective
(e.g., data theft)

Lastly, the hacker will try to Remove evidence of their intrusion. This usually means stopping logs on first entry, or erasing logs prior to leaving at which time logging would be turned on. It's important that the actions the hacker took are concealed.

The Hacking Process: Fall Back Attacks



If all direct Intrusion attacks fail, the attacker can Attempt non-intrusion attacks as shown on the next slide

The Hacking Process: Additional Types

Additional attacks:

- Denial of service (DoS)
- Eavesdropping
- Physical Breaking and entering
- Introducing Malware
- Session hijacking
- Man-in-the-middle attacks
- Web site attacks
- SQL injection
- Phishing
- Dumpster diving
- Social engineering

Slide 15

If a direct assault on the network infrastructure is unsuccessful, a motivated hacker won't stop there. There are a number of other attacks that can be employed. The end goal of the attack will dictate which of these techniques might be used. For example if theft is the goal, then a denial of service attack is not a good choice, however many of the others could lead to the desired access. For example, using a phishing campaign could lead to the introduction of malware in the network which could allow an opening for the attacker. If the prize is sufficient, then even breaking and entering can be employed.

Perhaps the most successful attack type is social engineering which we will look at next.

Social Engineering Basics

- “Hacking” people instead of systems
- Conducting research or reconnaissance to identify appropriate targets
- Communication methods
- Manipulating targets

Social engineering can be described as the “Hacking” people instead of systems. Social engineering can be used for Conducting research or reconnaissance to identify appropriate human targets such as Receptionists, IT staff, and Vulnerable employees as well as exploiting people to gain intelligence regarding the hackers target.

Receptionists are common targets because they have a great deal of knowledge about individual employees, events, and scheduling. They also tend to be highly social and helpful. Vulnerable employees include people with financial difficulties, emotional problems, or other issues that may make them susceptible to social engineering techniques.

Communication methods include:

In person, by Telephone, E-mail or through spoofed or purpose built Web sites

Goals include manipulating targets into:

Revealing information, including logon credentials, tricking them into Downloading malware

Reconfiguring systems, or Granting unauthorized physical access

Social Engineering Techniques

- Methods for conducting research
- Building relationships with targets then exploiting them
- Impersonating
- Reciprocity or a favor for a favor

Social engineers may use techniques similar to those used by hackers. As mentioned earlier, research can be done using Reconnaissance (watching), Public information, Social networking sites, Dumpster diving and Cold calling Just to name a few.

For significant targets, the social engineer may form relationships with targets to build trust then exploit them.

Impersonation is frequently used, with success gained by pretending to be: Authority figures, for example managers, executives, and police, maintenance technicians, Vendors or clients, other Employees or Tech support staff.

Reciprocity or a favor for a favor can be used as well.

Most People are raised to be trusting of authority and wanting to be helpful or pleasing in their interactions. Social engineers

Take advantage of this to achieve their goals.

As we go through the course, there will be other opportunities to explore pseudoscience of social engineering.

Summary

- Risk assessment for network infrastructure
- The hacking process
- Common network hacking tools: applications, exploits, and attacks
- Social engineering practices and their impact on network security efforts

In this lecture we have talked about Risk and what it is. We have looked at the hacking process and a few of the types of tools used to identify vulnerabilities and enumerate devices and software. Lastly we looked at social engineering.

End of Lecture 3



of Lecture 3

19

This ends Lecture 3 of Unit 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 4

Network Security Tools and Techniques

Lecture 1

Key Concepts

- Securing the LAN-to-WAN Domain
 - Internet ingress/egress point
- Mitigating risk with IDSs and IPSs
- Contrasting intrusion detection and intrusion prevention strategies

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this first lecture of Unit 4 we will begin looking at communications pathways and how we monitor and control the traffic on those pathways. We will also begin our examination of controlling our incoming and outgoing traffic which traverses our network boundaries. As we will see, the transition from trusted to untrusted environments and vice versa can be one of the most challenging areas to control, but also one of the most important.

We will be reviewing Intrusion detection and prevention strategies as a means of mitigating risk at the perimeter and within our networks.

Learning Objectives

By the end of this unit, the student will be able to:

- Identify some common network security tools
- discuss techniques for network protection
- Describe the difference between intrusion detection and intrusion prevention devices

By the end of this unit, the student will be able to identify and use some common network security tools. They will be able to discuss some of the techniques for protecting network perimeters including the deployment of intrusion detection and prevention devices.

Vulnerability Assessment Scanners

- Network Scanners
- Web Application Scanners

I'd like to start this lecture by looking at some of the tools used by both network and system administrators as well as hackers. For the moment, we will call these scanning applications. These fall into a couple of general classes:

Network or infrastructure scanners: General-purpose scanners that probe a network for a variety of widely known vulnerabilities.

and

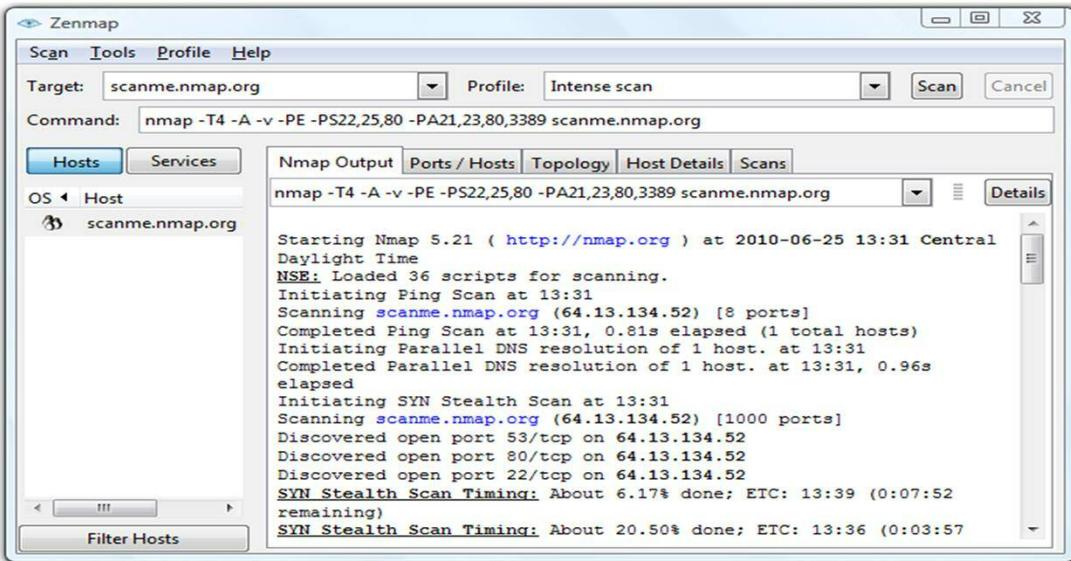
Web application scanners: Scan applications for known vulnerabilities. These scanning applications are not limited to web applications, but due to the high risk posed by these public facing applications, they are the most frequent targets.

Nmap and Zenmap

- Network mapper (Nmap) runs at command line
- Zenmap is the graphical user interface to Nmap
- Originally intended as a network mapping utility
- Port scanning and host detection features
 - Identify access points to a network
 - Identify holes in access controls
- Highly configurable
- Open source

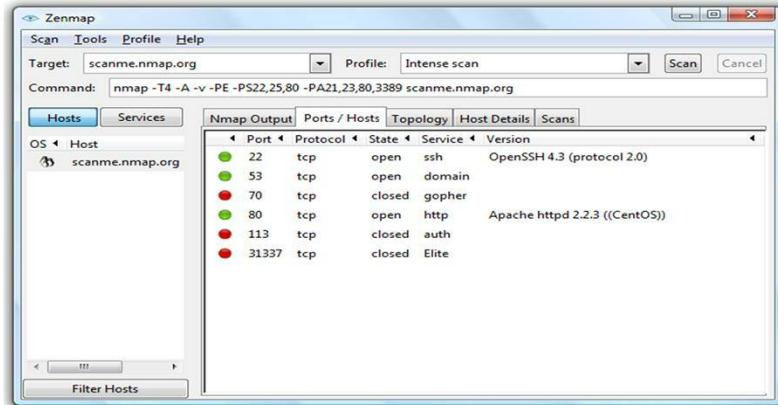
Nmap and the graphical user interface Zenmap are widely used free utilities used by network administrators and hackers alike. While this utility was originally intended to be a network mapping tool, its capabilities have grown over the years. Nmap is frequently used to identify active IP addresses, open ports and active services and protocols that are in use. Nmap has become a very powerful and flexible tool thanks in part to its continual development as an open source utility.

Zenmap: Nmap Output Tab



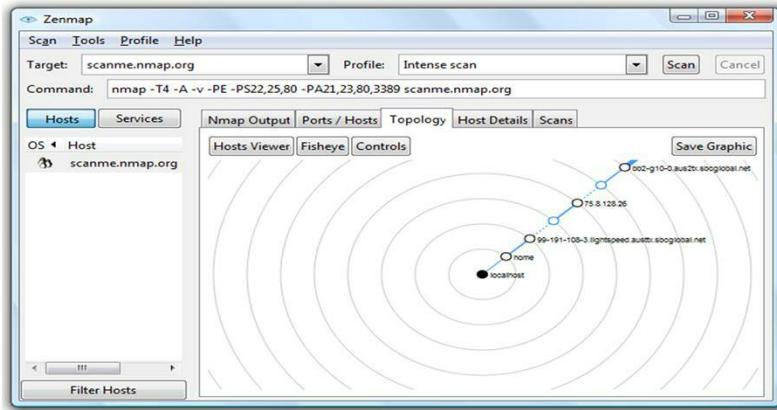
On this slide we can see an output report showing which hosts are on a network and which ports are open on those hosts. It also contains the common usage of those ports. Note the 'target' field. In this case, a URL was entered. Specific IP addresses or IP address ranges can also be used. These should be used with caution however. Scanning can be a precursor to an attack and may be considered a hostile act by companies. You should never scan IP addresses for which you do not have explicit written permission.

Zenmap Ports / Hosts Tab



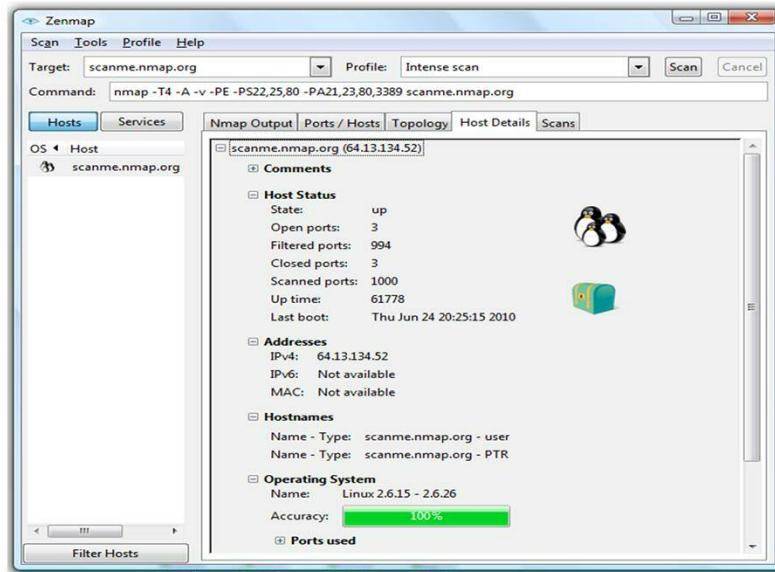
In this Zenmap view, we see the ports that were identified and their status of open or closed.

Zenmap Topology Tab



Another Zenmap view shows the topology, or what is connected to what. Notice there are other views available. As you have an opportunity to use this program, you should try the different options. You will find that some are more useful than others depending on the circumstance you are using the utility in.

Zenmap Host Details Tab



The host details tab is very informative. It provides a quick snapshot of the information you will find most useful as you continue your exploration of the target site. Of most interest will be the IP address, the open ports and the operating system with it's version.

Nessus

- Commercial security scanner developed by Tenable Network Security
- UNIX based
- Network-centric with Web-based consoles and a central server
- Offers a comprehensive set of tools
- Useful tool for larger networks
- Reports indicate which ports are open on which hosts and any security threats to those ports

Nessus is a commercial scanner developed by Tenable Network Security. Nessus is robust and offers a more extensive set of analysis tools than Nmap. Like most anti-virus tools, Nessus uses signatures to identify vulnerabilities based on identified versions of protocols and applications, especially operating systems that may be present on networks. Nessus can work on large networks, although the time required and the report sizes can grow to be unmanageable. Breaking scans up into IP address ranges associated with subnet is the most effective method of keeping the scanning time and reports manageable.

Retina

- Proprietary vulnerability scanner
- Deep-scan a network looking for known issues that have not been patched in existing applications
- Also scans for open ports
- Output report indicates network vulnerabilities and the state of the environment
- Easy-to-understand graphically intensive format

Retina is another commercial vulnerability scanner that is available for network administrators. Like Nmap, this application starts with scans for open ports and identifies applications on the network. Similar to Nessus, Retina scans the services, operating systems and protocols looking for missing patches and other potential vulnerabilities . Retina's strength is in it's reporting.

SAINT

- SAINT = System Administrator's Integrated Network Tool
- Commercial vulnerability assessment tool
- UNIX based
- Full suite of tools like Nessus
- Saint Corporation sells SAINT and other security tools

SAINT, another commercial product, combines a vulnerability scanner with a set of exploit tools. This allows penetration testers to validate vulnerabilities discovered by attempting to exploit them all within the same suite of tools. SAINT is a great concept, however like most multifunction applications, it does not excel at many of its functions. Consequently, most professional penetration testers use a variety of tools to perform their work.

Network Analysis

- Also referred to as “network forensic analysis”
- Analysis of network data to reconstruct network activity over a specific period of time
- Common uses
 - Detect vulnerabilities and threats
 - Reconstruct the sequence of events that took place during a network-based security incident
 - Discover the source of security policy violations or information assurance breaches

The term ‘Network Analysis’ has a number of meanings depending on the context it’s used in. For the purposes of this lecture, we’ll look at network analysis as a method of determining the events that have taken place within a specific time frame on the network. This may also be referred to as network forensic analysis.

Network analysis may also be used to troubleshoot or characterize the function of a network by mapping and measuring traffic flows against predicted results. This can be useful when looking for issues with throughput or quality of service issues. This aspect of network analysis will be examined later in the course.

For now we will be using network analysis as a means to detect vulnerabilities and threats, trace events that have occurred and investigate the source of security violations which may include breaches.

Network Analysis (Continued)

- Able to Reveal
 - Vulnerabilities
 - Services
 - Protocols
 - Applications

Network analysis can show us known Vulnerabilities which may be the result of services, open ports. By identifying services and open ports, we have the opportunity to determine whether they are required for environment and is not remove them. We can also identify potential vulnerabilities and apply patches to mitigate them. Unused services and protocols often provide an avenue for hackers to exploit. By proactively analyzing and monitoring our networks, a network administrator may be able to detect the activities of an attacker.

It should be no surprise that hackers will use the same tools we would use to perform these tasks. Let's look at what they can learn.

Network Analysis (Continued)

- Able to Reveal
 - Vulnerabilities
 - Probing (directed scanning)
 - Denial of service (DoS) attacks
 - User-to-root attacks
 - Remote-to-local attacks

Hackers frequently engage in the practice of Probing. Here an attacker scans a network to gather information in order to find known vulnerabilities. They may use tools such as Nmap, SAINT, or other vulnerability assessment tools. Again, the intent is to identify services, protocols, operating systems and applications that may be on a system along with the specific versions of each. This allows the attacker to determine if there are known vulnerabilities that may be exploited. Probing can be detected and defended against as we will see going forward.

Denial of service attacks or Distributed DoS attacks: Overwhelming a system with requests. These types of attacks are usually easy to detect, but are sometimes difficult to remediate.

Privilege escalation or User-to-root attacks are when an attacker uses an ordinary user account to access a system, and then exploits a vulnerability to get root privileges. Root privileges are always desired as they allow the installation and removal of software and system objects. Root privileges can also allow starting and stopping of logs so an attacker can hide their tracks.

Typically an attacker will use a Remote-to-local attack to gain access to the network. This is where the attacker does not have a user account but exploits a vulnerability to gain access.

Overview of Network Analysis Tools

- Packet Capture Tools
- Intrusion Detection Systems (IDSs)
- Data Collector

Let's take a look at some of the tools we can use for network analysis.

Packet capture tools -- allow you to record data that travels across your network and examine it in detail. Wireshark is an example of a packet capture tool.

Intrusion detection systems (IDSs) are used to monitor internal hosts or networks for suspicious traffic and alert administrators when such traffic is detected. Most IDS systems rely on a data collector appliance or software-based agent that records data on each network connection passing through the monitored device(s). These pass the collected information back to the IDS for analysis and actions if necessary.

Packet capture tools can limit the data captured to data with specific connection characteristics, such as to or from a specific system. Because packet capture tools generate a large volume of data in a short period of time, it's not feasible to keep packet capture data for an extended period.

Investigators can examine the records generated by an IDS to reconstruct a security incident.

Data collected through a data collector includes the source, destination, and volume of data.

Where to Capture Data on the Network

- Understanding the network's architecture
- Internal LAN usually generates too much traffic to analyze
- Main focus should be on inbound and outbound traffic
- Monitor/capture

To determine where to place packet capture probes on your network, you must first understand the network's architecture: where is the traffic of interest? Internal LANs usually generate far too much traffic to analyze so internal capture of traffic is usually confined to specific areas for short durations looking for specific events. Consequently, your main focus should be on inbound and outbound traffic; that is traffic entering or leaving your LAN. Typical locations to Monitor or capture traffic is at the External (demilitarized zone, or DMZ) network just inside the perimeter firewall.

Network Analysis Steps

- Create a baseline of the network
- Capture data at specific points on the network
- Analyze captured data, compare to baseline, review logs
- Uses of results of analysis

To be useful, analysis of traffic should begin with a baseline of the networks normal traffic patterns.

Capture data at specific points on the network to create a baseline which can then be used to Analyze future captured data. New captures can then be compared to baseline along with review logs to identify specific types of events of interest.

You can use results of analysis to:

Investigate and resolve issues, such as removing unnecessary services or closing open ports that present a vulnerability

Update baseline, if necessary

After an incident, build signatures into the IDS/IPS to prevent further losses

To build a baseline you can use Nmap/Zenmap to inventory network devices and see which services they run, as well as what OS and application versions are installed. This can be followed by using wireshark or similar tool for more in depth analysis and traffic profiling.

Once your baseline is established, periodic reviews and monitoring should become routine. Any changes should be investigated and resolved. Sometimes prohibited applications are discovered by a scan. These may include peer-to-peer (P2P) networking, instant messaging, Voice over IP, or social media file sharing.

When analyzing logs, analysis attempts to detect known attack patterns and deviations from normal behavior. As traffic captures can result in very large amounts of data, there is a need to reduce large volumes of audit data to small volumes of pertinent data.

End of Lecture 1



of Lecture 1

19

This ends Lecture 1 of Unit 4. We will continue to look at our perimeter defenses and tools in Lecture 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 4

Network Security Tools and Techniques

Lecture 2

Key Concepts

- Data Loss Protection devices & software
- Perimeter based tools
- Data protection strategies

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this lecture we will examine a number of key concepts associated with defending the perimeter of our networks.

Learning Objectives

By the end of this unit, the student will be able to:

- Identify some common network security tools
- discuss techniques for network protection

By the end of this unit, the student will be able to identify some common network security tools, especially those associated with perimeter defenses. In addition, the student will be able to discuss techniques used for protection of networks and data within the networks.

Data Loss/Data Leak Prevention Tools

- Detect and block sensitive data from exiting a network
- Enforce policies across file shares, databases, e-mail systems and on stored data
- Two basic types
 - Perimeter-based and client-based
 - Some products combine the types
- Cloud products are coming

Let's start our discussion by looking at a general class of tools associated with data loss prevention.

Most DLP products are designed to detect and block sensitive data from exiting a network. They can be used to enforce policies across file shares, databases, e-mail systems and on stored data. They come in two basic types:

Perimeter based: Stop leaks before they leave the local or wide area network

Client based or endpoint: Stop leaks at the client

Some products combine perimeter- and client-based protection. Cloud based DLP products are coming.

Companies often monitor e-mail for data leakage protection (DLP) and sensitive information. DLP monitoring may look for large files being e-mailed outside the organization. It can also scan e-mails for sensitive information such as account numbers and Social Security numbers. Some products on the market can tag sensitive documentation within the organization and prevent tagged documents from traversing specific points preventing the movement of sensitive data across unauthorized transit points.

Perimeter-Based Tools

- Commercial
 - GTB Inspector
 - Palisade PacketSure
 - Fidelis XPS
 - Code Green Content Inspector
- Open Source
 - OpenDLP

Here are some of the available perimeter based data loss protection tools currently on the market. It may be worth taking the time to visit the web sites for each of these to gain some insights on what they offer. I will warn you however that the information they provide is not necessarily objective. They will highlight the positives and disregard or omit any negatives in an effort to convince you that theirs is the best and only good solution.

From an open source – that is free perspective, OpenDLP is a widely accepted option. As with all DLP solutions, it is not without its strengths and weaknesses. It does require significant tuning to make it useful and lacks many of the fancy graphical user interfaces of the commercial products, but it does perform well once properly configured.

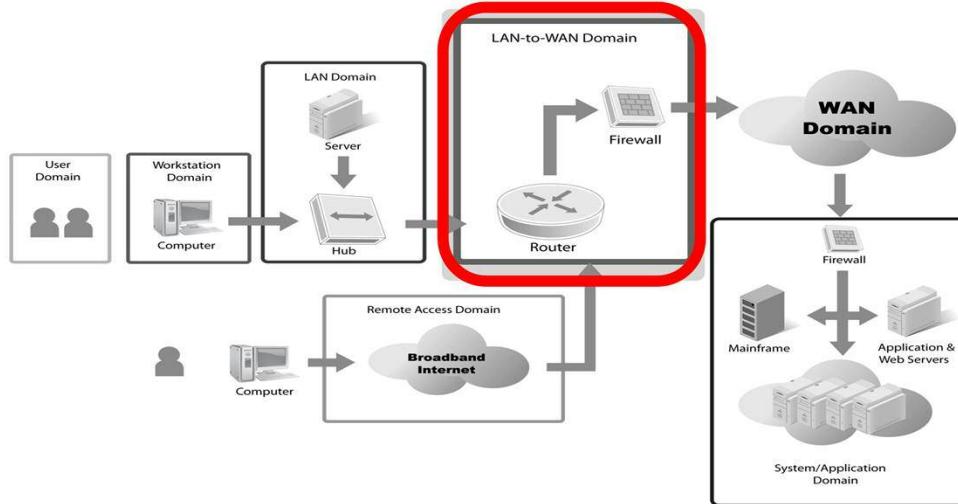
Client-Based or Endpoint Tools

- Sophos Endpoint Security and Data Protection software suite
- RSA DLP Endpoint

Client based, host or end point solutions include Sophos Endpoint security and data protection. Sophos is a widely used anti-virus/ anti-malware vendor. They have included this functionality in their suite of enterprise solutions.

RSA is another well known company with a wide variety of security related products . DLP is a relatively recent addition to their product line. Much more information is available at their web sites, but be aware, they are designed to sell you their products, so read their material with a skeptical eye.

The LAN-to-WAN Domain



Let's return to the LAN-to-WAN Domain which marks the boundary where the private network meets the public network. In this context, the public network is the Internet. We've been discussing the use of data loss prevention within the private network and at the perimeter of the network environment. What we are talking about is LAN-to-WAN domain from the seven domains discussed in earlier units. DLP is just one of the tools that can provide insights into the traffic within and traversing our network boundaries. We'll look at some additional tools and techniques now.

Many different types of attacks come from the Internet. The primary protection here is the use of one or more firewalls and boundary routers. Firewalls can examine traffic as it passes through and allow or block traffic based on rules. Other devices can assist in this process.

The Boundary Router

- Functions at the network perimeter in the DMZ
- Accepts traffic from the Internet
- Filters unapproved traffic and passes approved traffic to firewall
- Protects the internal network against IP address spoofing and directed IP broadcasts

One of these devices is the boundary router. A boundary router frequently is used on the untrusted or internet side of a demilitarized zone. It can act as an initial filter removing traffic not approved or intended for the enterprise. In this respect, the boundary router can behave like a firewall. Still, a firewall is normally positioned between the boundary router and the DMZ to further refine and restrict the incoming traffic.

Ingress Filtering

- Excludes or rejects all data packets that have an internal host address
- Drops non-routable IP addresses

Note:

***Non-routable IP addresses are specified in
RFC 1918 (Private Network Addresses)***

Ingress refers to Inbound traffic. Ingress filtering attempts to remove traffic that is obviously spoofed or otherwise incorrect. Examples shown here are packets with internal addresses and non-routable addresses. These should never come from outside the DMZ nor should they ever leave the DMZ.

Egress = Outbound traffic

Egress Filtering

- Stops packets from leaving the internal (company) network that have non-company addresses as their source address

Egress refers to Outbound traffic. Egress filtering is meant to protect internal addresses from being exposed to the untrusted network such as the internet. Depending on the configuration of the DMZ, traffic with internal addresses may be directed to approved assets in the DMZ or sent to a proxy server or other device for NATing. NATing is the process of substituting external addresses so session that transit the trusted environment do not expose internal devices. The NATted addresses are used while the session is active and removed once the session ends.

Intrusion Detection System (IDS)

- Monitors internal hosts or networks
- Seeks symptoms of compromise or intrusion
- Upon detection of an intruder, an IDS can:
 - Send commands or requests to the firewall to break a connection
 - Block an IP address
 - Block a port/protocol
- Some IPSs provide basic data loss/leak prevention capabilities

We mentioned that a firewall is a border sentry device. A controlled network border sentry device filters any traffic attempting to cross. However, not all traffic that needs monitoring crosses a network border guarded by a firewall. That's where an intrusion detection system comes

into play. An IDS or an IPS monitors internal hosts or networks watching for symptoms of compromise or intrusion. Effectively, an IDS is a form of burglar alarm that detects when an attack is occurring within the network.

Intrusion detection and prevention devices have evolved and in some cases they have merged into one. Initially an IDS was able to only detect events and provide alerts. They were not designed to be proactive. Intrusion prevention devices were. Both started as signature based analysis engines looking for matching parameters then taking an action based on that match.

Intrusion Prevention System (IPS)

- Monitors internal hosts or networks watching for symptoms of compromise or intrusion
- Detects attempts to attack or intrude before they are successful
- Upon detection of an intruder, an IPS can respond by preventing the success of the attempt

The IPS strives to detect the attempted attack or intrusion before it can be successful. Once detected, the IPS can respond preventing the success of the attempt, rather than waiting until after a successful breach to respond. This can be a real strength, but the first generation devices were prone to many false positives. Blocking desired traffic led many IPS devices to passive alert only modes allowing human decisions before a block could be enabled. Obviously this created risk and delay, but it was often preferred over losing legitimate traffic.

IDS vs. IPS

IDS	IPS
Detects and Acts	Prevents
Reacts to events that IPS misses	First layer of proactive defense

As these devices have advanced, they have adopted additional functionality including behavioral analysis. Rather than relying strictly on signatures which are frequently updated, the devices can be programmed to look for behavioral patterns and alert or block based on those. This is very similar to the way heuristic analysis works in modern anti-virus programs.

Host-Based vs. Network-Based IDSs/IPSs

- Host-based and Network-based IDSs/IPSs
 - Network-based IDSs/IPSs look for patterns in network traffic
 - Host-based IDSs/IPSs look for attack signatures in log files

IDS/IPS systems fall into two general categories. Host based and Network based. **Host-based intrusion detection system (HIDS):** Installed on individual systems. An HIDS is used in addition to antivirus software. The antivirus software detects and prevents malware attacks. An HIDS detects intrusion attacks on the system. Because an HIDS is installed on every system on a network rather than as a node on the network, it can't create an accurate network picture or coordinate events that occur across the network.

Network-based intrusion detection system (NIDS): Installed at various points on a network. An NIDS can detect and coordinate defenses against attacks that occur across a network.

Host-Based vs. Network-Based IDSs/IPSs

- **IDSs and IPSs**
 - IDSs and IPSs look for attack signatures—specific patterns that usually indicate malicious or suspicious intent
 - Can be anomaly-based or behavioral-based

As mentioned, IDS and IPS can use rule-based detection mechanisms similar to those of a firewall, but they can also employ detection mechanisms borrowed from anti-virus technology. For example, some IDS/IPS have a database of signatures or patterns of known malicious activity. This is known as signature-, database-, or knowledge-based detection. Any attack within the database can be detected in live activity by the IDS.

Another form of detection is anomaly based. Anomaly-based detection systems look for abnormalities. To do that, you have to first define “normal.” Normal can be defined by rules or filters that prescribe all of the valid packet constructions and header contents. Then, anything that fails to match the definition of normal is an anomaly. Since mistakes, errors, and poor network application programming can occur, an anomaly is not necessarily malicious or an intentional attack.

Yet another detection mechanism is behavioral based. Behavioral-based detection looks for differences from normal-based on a recording of real-world traffic that establishes a baseline. A normal baseline can be recorded over hours or days. Once recorded, it’s the yardstick to measure all future activities. Any future event not similar to behaviors in the baseline set represents a possible violation.

Summary

- Securing the LAN-to-WAN Domain ~
 - Internet ingress and egress point
- Mitigating risk with IDSs and IPSs
- Intrusion detection and intrusion prevention strategies
- Automated network scanning and vulnerability assessment tools
- Data protection strategies

So to summarize, in this lecture we had been looking at different methods of securing the LAN to WAN domain.

We've looked at Internet ingress and egress points

We've looked at using IDS is and IPS as risk mitigation tools.

We've looked at intrusion detection and prevention strategies and examined the way IDS and IPS devices function.

We've looked at automated network scanning and vulnerability assessment tools

And we have continued our discussion of data protection strategies

End of Lecture 2



of Lecture 2

17

This ends Lecture 2 of Unit 4.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 5

Network Security Tools and Techniques

Lecture 1

Key Concepts

- IP stateful firewalls
- Types, features, and functions of firewalls
- Software-based and hardware-based firewall solutions
- Filtering and port control strategies and functions
- Homed firewalls and placement

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this first lecture of Unit 5 we will begin looking more closely at firewalls. Firewalls are a class of device that frequently serves to protect our perimeters however there are several other critical functions that firewalls can perform. Indeed, there are several different types of firewalls, some with very specific applications in an IT environment. We will be examining the different types and functions of firewall as well as typical uses in different network scenarios.

Learning Objective

By the end of this unit, the student will be able to:

- Describe the fundamental functions performed by firewalls
- Explain single homed and multi-homed firewalls and their application
- Identify a bastion firewall and its function
- Describe stateful firewalls and their importance

Learning objectives for Unit 5 include students being able to:

describe the functions performed by firewalls.

Understand and explain the use and placement of single and multi-homed firewalls.

Identify the function of a bastion firewall and what make it different.

Describe what state is and how it is used by stateful firewalls

What Is a Firewall?

- A network traffic control device or service
- Enforces network security policy
- Protects the network against external attacks
- Establishes control over network traffic
- Prevents connections from unauthorized sources to protected network systems, services, and resources

Firewall Analogy

Bouncer at a night club with a guest list that defines specific names or types of individuals allowed in or specifically prohibited from the club

We'll begin our look at firewalls by answering the question What is a firewall?

Firewalls are either hardware or software appliances that serve to control network traffic. Firewalls are critical in enforcing security policies on our networks. They help to protect networks from external attacks and help to isolate and protect sensitive internal environments.

Looking at the analogy, we can imply that firewalls use rules to define what is allowed and what is to be stopped. Firewalls are the gatekeepers at the doors of our trusted networks.

Types of Firewalls

- Single-homed
- Multi-Homed
- Stateless
- Stateful
- Application gateway
- Application Proxy

There are several different types of firewalls and several ways in which firewall can be deployed. Some firewall appliances (either hardware or software) are designed to perform one type of service, while others are more flexible and may be configured to perform a variety of functions. This will become more apparent as we move through the unit and subsequent units.

Descriptions of Firewalls

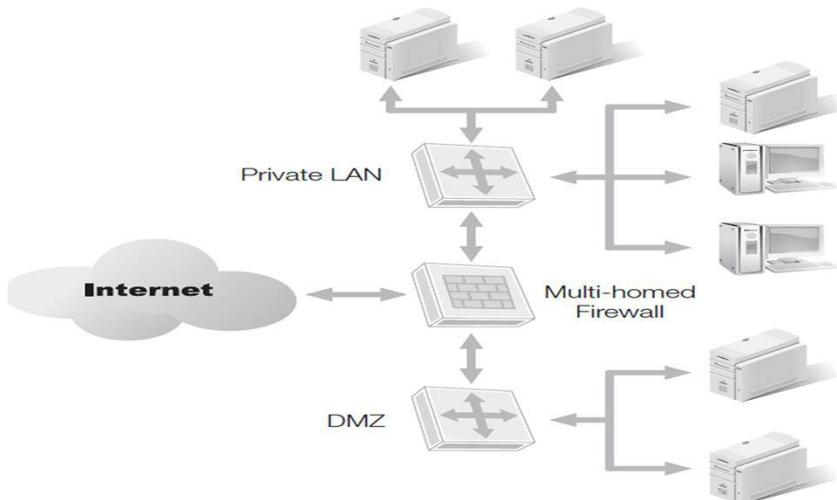
- May be for personal or commercial use
- Software or hardware based and virtual
- May use dynamic or static packet filtering

Firewalls are not just for enterprises. They can and should be used in both commercial and home settings. They are like the door to your environment allowing you to control who goes in and out.

As mentioned, firewalls can be implemented in hardware or software. They can be tangible devices in a server room rack or virtual appliances floating in the cloud.

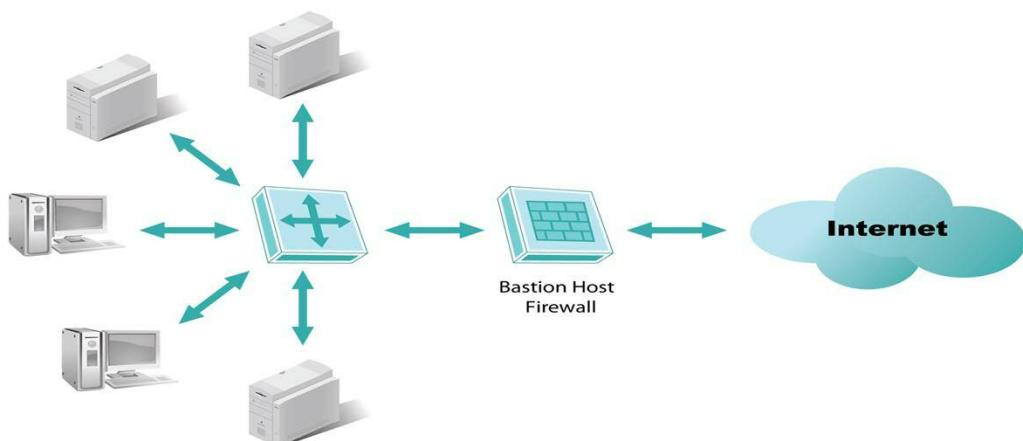
Firewalls can use dynamic and/or static packet filtering. This will be discussed later in the course.

A Firewall on a Network



In this diagram we see a multi-homed firewall. There are three legs, one to the internet, one to a router on a private LAN and one to a router on a demilitarized zone.

Bastion Host Firewall Implementation



Here we see a dual homed bastion host firewall. A dual homed firewall is used as a first line of defense and contains two network interface cards NICs. One is attached to the untrusted network – typically the internet while the other is connected to the trusted network. Bastion hosts are normally hardened in that they have all unnecessary functionality removed and are closely monitored to ensure they are up to date with the latest security patches. This is done to reduce the potential vulnerabilities that may be present in firewall to the absolute minimum.

Stateless Inspection

- Maintain no “state tables” for active connections
- Frames are treated individually rather than collectively
- Filtering decisions are based on static addresses and port numbers

Stateless firewalls maintain no “state tables” for active connections. They are unaware of session stream details for connection-oriented protocols such as TCP. Frames are treated individually rather than collectively consequently they cannot distinguish between packets in ongoing connections and rogue packets. Filtering decisions are based on static addresses and port numbers which are either Passed (allowed) or blocked (denied) based on well-known connection values.

Stateful Inspection

- Maintain records of active connections
- Pass (allow) and block (deny) decisions based on packets belonging to legitimate connection streams
- Looks for packets that do not belong to authorized sessions
- Advanced stateful firewalls track session endpoints
- Retain additional state details, such as acknowledgement numbers and sequence numbers
- Connectionless traffic is not “stateful” and therefore firewall state management does not apply

Stateful firewalls maintain records of active connections to determine whether or not packets are part of existing sessions.

Pass (allow) and block (deny) decisions are based on packets belonging to legitimate connection streams.

Once a session is established, the firewall looks for packets that do not belong to authorized sessions.

Advanced stateful firewalls track session endpoints and retain additional state details, such as acknowledgement numbers and sequence numbers.

Connectionless traffic is not “stateful” and therefore firewall state management does not apply.

Advantages of Stateful Filtering

- Keeping “state” observes network connections between points
- Provide efficient packet inspection
- Lack of “stateful record keeping” could result in breaking of legitimate connections

Keeping “state” observes network connections between points

Most session-oriented protocols use random source ports.

State tracking adjusts and adapts to real-time traffic conditions.

State tracking watches end-to-end traffic streams, session-oriented start-up and tear-down.

State tracking treats packets collectively (start to finish) rather than individually.

State tracking has high operational overhead, robust rule configurations

Stateful firewalls provide efficient packet inspection.

Existing connections are checked against state table.

Computationally-intensive firewall filter lookup are avoided

Lack of “stateful record keeping” could result in breaking of legitimate connections.

Arbitrary source ports to well-known service destinations get dropped.

Firewall Filtering Types and Strategies

- Ingress/egress filtering
- Packet filtering examines network protocol headers and parameters
- Content filtering focuses on network protocol payloads

Ingress/egress filtering

Monitoring and filtering directional inbound and outbound traffic

Packet filtering examines network protocol headers and parameters.

Static packet filtering (stateless) uses a fixed set of rules to filter network traffic.

Dynamic packet filtering (stateful) watches connection states to filter traffic.

Operates at the lowest OSI protocol layers

Content filtering focuses on network protocol payloads.

Intercepts and investigates packet content before it enters or leaves the network.

Concentrates on domain names, URLs, file names and extensions.

Administratively block unauthorized download resources and Web sites.

Operates at the higher OSI protocol layers

Firewall Filtering Types and Strategies

- Stateful multilayer inspection
- Stateful and stateless inspection
- Proxy servers respond to connection requests between clients and servers
- Network Address Translation (NAT)

Stateful multi-layer inspection

- Inspects packet headers and payloads
- Offers complete view of the entire seven-layer OSI protocol stack
- Examines setup, state, and teardown of connection-oriented protocols

Stateful and stateless inspection

- Tracking connection states to separate legitimate from questionable traffic
- Proxy servers respond to connection requests between clients and servers.
- Separates and isolates external and internal network endpoints
- Circuit proxy (circuit-level firewall) monitor TCP handshakes to track sessions.
- Application proxy filters by protocol content to enforce safe application behavior.

Network address translation (NAT)

- Separates and isolates external and internal network endpoints
- Maps several internal addresses to a common external address

Static and Dynamic Packet Filters

- Static filtering is constant and unchanging
- Dynamic filtering adapts to live traffic
 - Learns which ports are needed for a session
 - Blocks all others

Static filtering is constant and unchanging.

Connection values—address, port, and protocol—are known in advance.

Connections must use well-defined ports and protocols.

Sessions are not observed start-to-finish between endpoints.

Dynamic filtering adapts to live traffic by learning which ports are needed for a session and blocks all others.

Firewall monitors inbound connection requests.

Legitimate requests are tracked from start to finish.

When session ends, the firewall closes the ports.

Network Address Translation (NAT)

- NAT translates internal addresses to external addresses
- NAT creates one-to-many mappings to extend IP address class availability and share a common Internet connection among several “hidden” hosts
- NAT allows you to bypass individual IP assignments from an ISP
- NAT conceals internal machines from the external world

NAT translates internal addresses to external addresses.

NAT creates one-to-many mappings to extend IP address class availability and share a common Internet connection among several “hidden” hosts.

NAT allows you to bypass individual IP assignments from an ISP.

Create choke points through which all traffic must pass.

Reduce cost by using a single Internet IP among several internal computers.

Extend “full” IP address class ranges to smaller, separate network segments.

NAT conceals internal machines from the external world.

Keep private systems hidden from external access or view.

Let multiple internal connections appear to originate from one external system.

End of Lecture 1



of Lecture 1

16

This ends Lecture 1 of Unit 5. We will continue to look at firewalls in Lecture 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 5

Network Security Tools and Techniques

Lecture 2

Application Gateway Overview

- An application proxy, or application gateway, is like a packet filter but focuses more deeply on application protocol behaviors
- Acts as middleman between client and server
- Firewall and proxy combination achieves defense-in-depth strategy

Welcome to lecture 2. We've mentioned that there are multiple avenues that can be exploited to gain a foothold into the network. Because of their complexity and interaction with external clients, applications are a frequent target. To help mitigate these high risk applications, there are several hardware or software appliances that can be used. The distinctions between the functions provided by these products have become blurred over the last few years as they increase in capability.

Application gateways, application proxies and web application firewalls fall into this general category of device which I refer to as an application gateway from here on. All are designed to prevent attacks against the application and prevent exploitation. The devices may be hardware appliances, software or virtual appliances which sit between the client and the server application. Their job is to act as a middleman and mediate the traffic between the client and server ensuring that the client requests do not violate the security rules that have been established. The rules may be stop frequently exploited exploit attempts such as SQL injections, buffer overflows or other exploitable flaws applications are subject to.

Gateways may also prevent the application from responding to exploits by restricting the type of data that is permitted through from the server.

Application Gateway as a Packet Filter

- Static packet filters only inspect packet headers and segments
- Application proxy can fully inspect traffic up to the application payload
- Operates at any layer of the TCP/IP reference model

Application gateways can function as packet filters at multiple layers in the OSI stack. Static filters focus on headers and segments rejecting traffic that is malformed, duplicate or misdirected. Other gateways such as application proxies can look deeper into the packet and make decisions based on content as well as header and segment information. This can provide the greatest level of protection, but there is a cost in performance.

Application Gateway as a Middleman

- All application-specific communications are handled between client and server
- Maintains separate connections between client and server (“firewalling”)
- Not transparent: client is configured for proxy use, and therefore aware of it

The application gateway can manage all traffic between the client and the server and like a stateful firewall, it maintains separate connections for the session flows. This provides some isolation preventing direct access by the client which further reduces the possibility of malicious acts.

To function properly, the application and the application gateway must work together to prevent any side channels that would allow communications to bypass the gateway.

Application Gateway Defense-in-Depth

- Firewall and proxy combination achieves defense-in-depth strategy
 - Application proxies filter on content in the application layer payload
 - Network firewalls filter on lower-level protocol properties

By combining network firewalls with application gateways, we can achieve defense in depth. Network firewalls prevent intrusions through protocol examination while the application gateways can look deeper into the structure and content of the packets. This layered approach can significantly reduce the probability of attacks against applications.

Although application gateways can be deployed as standalone devices in hardware or software, cloud based implementations are becoming more available. It is likely that these cloud based services will become much more available and popular due to their ability to leverage the scalable processing power of cloud environments as well as draw on a much broader depth of experience to establish appropriate rules for evaluating packet traffic.

Network Circuit Proxy

- A circuit proxy or circuit-level firewall filters on connection-oriented startup
 - Observes initial setup of a circuit, session, or state
 - Once connected, a circuit is no longer filtered traffic

Circuit level firewalls or proxies are useful in providing some isolation between trusted and untrusted networks, however they do not filter traffic. These devices simply establish the connection and determine whether the connection is legitimate or not after which they cease observing traffic. This first generation firewall functionality is insufficient in most instances today.

Circuit Proxy Filtering Rules

- Circuit proxy filtering rules are similar to static packet filtering
 - Static values determine what circuits and connections are allowed
 - Filters can be set to default-deny or default-allow
 - Generally faster than application-layer firewalls due to fewer packet evaluations
 - Useful for connection-oriented protocols that perform TCP/IP handshakes

Filtering rules in circuit proxy appliances are similar to those in static packet filtering devices. Rather than operating on a packet level however, they operate on a circuit or connection level. Because they do not have so much traffic to analyze, they are generally much faster and require less resources than packet filters.

Software Firewalls

- Software firewalls are installed on host computers
- Built-in Windows Firewall or Linux packet filter
- Competes for shared resources on the host computer
- Static placement filters only connections made from/to the host
- Protect only one system on the network, unless forwarding IP traffic

Software firewalls or host based firewalls perform similar functions move firewall connection filtering to the endpoint or host. An example is the firewall built into the Microsoft operating system. This can be programmed to permit or deny access to and from specific applications on the host. Because the firewall is implemented in software on the host, it uses the same memory and CPU as other applications consequently it can be a performance issue when overused.

Another disadvantage is that these types of firewalls can normally protect only the host they reside on. This makes them unsuitable for larger environments where management would become very difficult.

Hardware Firewalls

- Hardware firewalls are installed on dedicated devices
- Firewall appliances and dedicated routers with firewall services

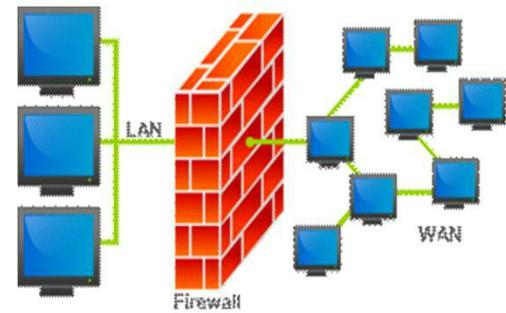


pfSense firewall images from Netgate.com

Hardware firewalls or firewall appliances are dedicated computing devices running a firewall application. The use of dedicated processing and memory allow efficient performance. They come in a variety of sizes and performance characteristics making them suitable for Small and Home offices like the top image to larger businesses and enterprises.

Hardware Firewalls

- Strategic placement throughout the network filters end-to-end connections
- Stand-alone unit can protect multiple systems on the network
- Optimized for network performance



Although firewalls are almost always found between an untrusted network such as the internet and trusted networks, they can also be used to control traffic and isolate segments of a LAN. This is very useful for preventing unauthorized access and meeting compliance requirements.

Virtualization has made deployment of firewalls in these environments relatively easy and more cost effective than deploying multiple hardware appliances.

Combination

- Achieve defense-in-depth by combining hardware and software firewalls
- Layered protection at the network and host levels by separate firewalls
- Especially practical for mobile employees that telecommute to work

Firewalls can be combined in numerous ways to provide layered defenses. Combining perimeter and host-based firewalls can improve security when computing devices such as laptops move between secured and unsecured environments.

Host-Based Firewalls

- Host-based firewalls protect only the local computer
- Filters traffic passing through the local system only
- Cannot filter traffic for other systems
- Host-based “personal” software firewalls
- Not optimized for firewall filtering

Let's revisit host-based firewalls for a moment. Recall that host-based firewalls only protect the host they reside on. They can be used to filter connection based traffic for the host but must use the resources of the host system they reside on. This resource contention can be problematic at times. These types of firewalls do not inspect packet contents and provide very limited protection.

Network-Based Firewalls

- Network-based firewalls span an entire network.
- Filters all traffic passing in and out of the network or network segment
- Can filter between other networks and systems

Network-based firewalls can provide protection for an entire network. They're designed to filter traffic passing both in and out of the network or network segment.

Network firewalls can provide enterprise class services especially when used on dedicated hardware.

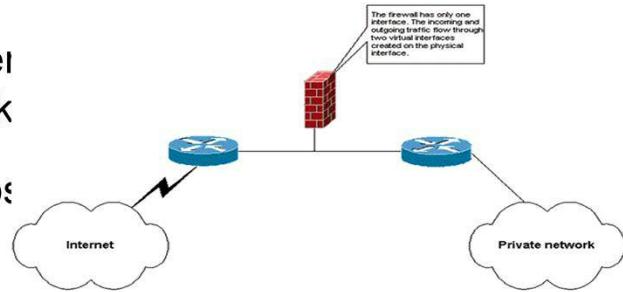
Network-Based Firewalls

- Commercial or corporate firewalls
- Optimized for network-wide firewall filtering
- Incorporate enterprise-grade network services
 - VPN
 - Enterprise-class encryption protocols
 - Enterprise-class security services

Commercial or corporate firewall is normally hardware-based. They are optimized for network wide filtering and incorporate new enterprise grade network services such as VPN encryption protocols and security services. We will be looking more closely at these throughout this course.

Single-Homed Firewalls

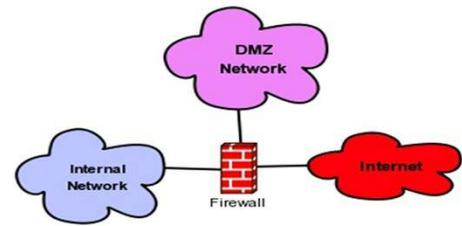
- Single-homed firewalls have only one network interface
- No physical isolation between internal and external network
- Ideal separation between host and network
- Cannot provide sentry services between network segments



Single home firewalls have only one network interface this means they provide no physical isolation between internal and external networks. Without separation capability they cannot provide sentry services between network segments.

Multi-Homed Firewalls

- Multi-homed means more than one network interface
- Dual or Triple homed
- Filter local traffic on an internal network interface
- Filter remote traffic on an external network interface
- Filter traffic between internal and external interfaces



Multi-Homed Firewalls

Create electronic isolations among segments, subnets, and networks

Ideal network separation with sentry services between networks

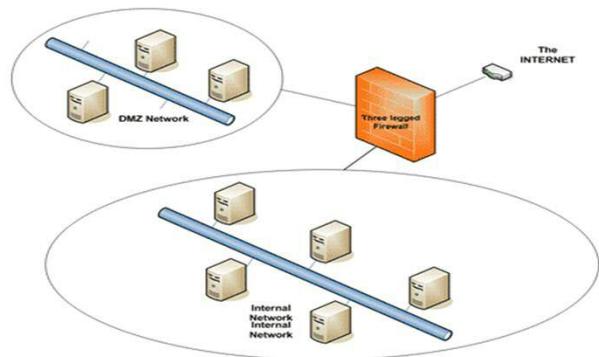


Image from <http://resources.infosecinstitute.com/itac-web-technology/#gref>

Multi-home firewalls have multiple network interface cards (NICs) forming isolation between the different legs. This is very useful to provide perimeter protection as well as creating multiple secure environments. Rules can be established to direct traffic from the internet to the DMZ and from the DMZ to and from the internal trusted network creating effective isolation.

Summary

In this unit we have discussed:

- The fundamental functions performed by firewalls
- The use of Application Gateways
- The difference between single-homed and multi-homed firewalls and their applications
- What a bastion firewall is and it's function
- What makes a firewall stateful why they are important

In this unit we have looked at a variety of firewalls and their functions.

We have discussed application gateways and application firewalls and how they fit in the security ecosystem.

We have examined the use and placement of single and multi-homed firewalls.

We were exposed to the function of a bastion firewall or host and what make it different.

We also discussed what state is and how it is used by stateful firewalls.

End of Lecture 2



of Lecture 2

19

This ends Lecture 2 of Unit 5.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 7

Firewall Design Strategies

Lecture 1

Welcome to Lecture 1 of Unit 7

Key Concepts

- Firewall limitations, weaknesses, and countermeasures
- Strategies for public Internet and private network separation
- Firewall rules for restricting and permitting data transit
- Use of protected demilitarized zones (DMZs)
- Security strategies and requirements for availability

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this first lecture of Unit 7 we will begin looking more closely at firewalls. We will be discussing the limitations and weaknesses of firewalls. We will look at the public and private network interface and protection strategies including the use of demilitarized zones, firewalls and other devices. We will begin looking at the rules that define how firewalls operate. And we will look at availability requirements and how firewalls may impact availability.

Learning Objectives

Learning Objectives

- Assess firewall design strategies
- Describe Firewall Rules
- Explain Access Control Strategies

By the end of this unit you will be able to assess simple firewall design strategies, describe the components and function of firewall rules and explain access control strategies.

Firewall Rules

- Sometimes called a filter or access control list (ACL)
- An instruction set that indicates how a firewall should take action on a particular type of network traffic

We'll begin this weeks lectures by looking at firewall rules. In previous lectures we have looked at the different firewall types and their functions, but how do we get them to perform those functions? Straight out of the box, a firewall looks neat, but doesn't do anything useful. To get it to perform in our environment we need to give it a set of rules to act on. These rules can be called filters and sometimes an access control list, but what they are is a list of instructions on what should be done with traffic that meets our specified criteria.

To be clear, what can be done with traffic usually comes down to a binary choice: will the traffic be allowed to pass or will it be denied and dropped. We will see how that works as we go through this unit.

Firewall Rules - General Guidelines

- Direction matters – validate source and target addresses
- **A deny-all catchall rule always goes at the bottom of the list**
- Denial exceptions go at the top of the list
- Rules pertaining to more common traffic belong closer to the top of the list
- Keep the number of rules to a minimum

Direction matters. Traffic from the outside and traffic from the inside of our networks can and should be handled differently. To do that we need to be sure to validate that the source and target addresses have been identified correctly.

As a best practice, when building our firewall rule sets, denial exceptions are normally placed at the top of our rule list along with our more common known and approved traffic. While it is easy and tempting to create relatively open rules, this is very dangerous and exactly what hackers hope for. All rules should be necessary and documented and all lists should end with an explicit ‘deny any any’ rule to ensure nothing that isn’t permitted explicitly is removed.

Keeping the number of rules to a minimum is another best practice as it greatly improves the management of the rule set. Also, all rules should have comments that describe why the traffic is being allowed or denied. This is a great time saver for whoever reviews the rule set later as they won’t have to guess why a particular rule was put in place.

Ports

- What ports should be allowed?
 - 443
 - 80
 - 25
 - Any required environmentally-specific application ports
- What ports should be blocked?
 - All others with a deny-all rule

Every environment is different and so too will be the permitted and denied ports.

This sample list allows the ports commonly used for HTTPS, HTTP and SMTP or the Simple Mail Transport Protocol. Should these ports always be permitted? No.

The ports used will depend on the applications that need to communicate through the firewall as well as where the firewall is deployed. For example, not all mail programs will use port 25 and even those that do will have other potential limitations. Having detailed knowledge of your environment is essential when establishing firewall rules.

Firewall Rule Example

The screenshot shows the SonicWall interface for managing access rules. The left sidebar includes options like System, Network, Wireless, WGS, Firewall, Access Rules (selected), Advanced, Services, VoIP, and Connections Monitor. The main area is titled "Firewall > Access Rules" and displays a table of "Access Rules". The columns are Priority, Source, Destination, Service, Action, Options, Enable, and Configure. There are 11 rules listed:

Priority	Source	Destination	Service	Action	Options	Enable	Configure
1	WLAN	192.168.168.168 (LAN)	HTTP Management	Allow		<input checked="" type="checkbox"/>	
2	LAN	192.168.168.168 (LAN)	HTTPS Management	Allow		<input checked="" type="checkbox"/>	
3	LAN	192.168.168.168 (LAN)	HTTP Management	Allow		<input checked="" type="checkbox"/>	
4	WLAN	192.168.168.168 (LAN)	HTTPS Management	Allow		<input checked="" type="checkbox"/>	
5	*	192.168.168.168 (LAN)	Key Exchange (IKE)	Allow			
6	192.168.168.168 (LAN)	*	Key Exchange (IKE)	Allow			
7	WLAN	WLAN	Any	Allow			
8	WLAN	WAN	Any	Allow		<input checked="" type="checkbox"/>	
9	WAN	WLAN	Any	Deny		<input checked="" type="checkbox"/>	
10	LAN	*	Any	Allow		<input checked="" type="checkbox"/>	
11	*	LAN	Any	Deny		<input checked="" type="checkbox"/>	

A red arrow points to the "Deny" action for rule 11.

As mentioned earlier, Direction matters, so be sure to validate that the source and target addresses have been identified correctly. Look for a moment at this screen shot of a set of Sonic Wall firewall rules. Note that each line has a source, destination, service and action. We can see that the Deny All rule is placed at the bottom of the list. Look closely at the rest of the rules though. Do you see anything that should be of concern?

One thing to note here is that this set of rules uses a combination of IP addresses and labels for their required fields. This type of shortcut is allowed in most firewalls, however it should be used with some caution.

Firewall Rule Components



We've looked at a few sample rules now and there should be some patterns that are developing. Almost all firewall rules have some common elements such as those shown in this slide. The base protocol is typically TCP or UDP. The allowable protocols should be based on what your environment needs and can manage.

The source address and port and the destination and port are always present, but as you may have noticed in the previous slide, wild cards can be used as well. Lastly is the action. What are you going to do when the rule is met?

Firewall Rule Structure

- Common structure

[Protocol]	[Source Address]	[Source Port]	[Target Address]	[Target Port]	[Action]
TCP	192.168.42.0/24	ANY	ANY	80	Allow

- Source address and port often set as ANY unless rule applies to specific system or port

Here again is the common structure of a firewall rule. All of the elements are here. Notice that the protocol is TCP and the source address is a range of RFP-1918 non-routable addresses. These would be internal addresses and the /24 indicates that up to 128 IP addresses may be in this range – less special purpose addresses. Sources may use any port and may go to any address, but only target port 80 (HTTP) on the destination address. This traffic is specifically allowed per the allow action.

Firewall Rule Example 2

[Protocol]	[Source Address]	[Source Port]	[Target Address]	[Target Port]	[Action]
TCP	ANY	ANY	192.168.42.0/24	>1023	Allow
TCP	192.168.42.1	ANY	ANY	ANY	Deny
TCP	ANY	ANY	192.168.42.1	ANY	Deny
TCP	192.168.42.0/24	ANY	ANY	ANY	Allow
TCP	ANY	ANY	192.168.42.55	25	Allow
TCP	ANY	ANY	192.168.42.98	80	Allow
TCP	ANY	ANY	ANY	ANY	Deny

Lets look at some additional examples from a little longer list.

The first line allows the TCP protocol coming from any address using any port to go to any of the 128 addresses in the 192.168.42.1 to 128 range, but only to ports greater than 1023.

Firewall Rule Example 2

[Protocol]	[Source Address]	[Source Port]	[Target Address]	[Target Port]	[Action]
TCP	ANY	ANY	192.168.42.0/24	>1023	Allow
TCP	192.168.42.1	ANY	ANY	ANY	Deny
TCP	ANY	ANY	192.168.42.1	ANY	Deny
TCP	192.168.42.0/24	ANY	ANY	ANY	Allow
TCP	ANY	ANY	192.168.42.55	25	Allow
TCP	ANY	ANY	192.168.42.98	80	Allow
TCP	ANY	ANY	ANY	ANY	Deny

The next two lines says that 192.168.42.1 can't communicate with any address on any port using TCP. The following line denies any source address using TCP on any port attempting to communicate with 192.168.42.1.

Think about why you would do this?

Firewall Rule Example 2

[Protocol]	[Source Address]	[Source Port]	[Target Address]	[Target Port]	[Action]
TCP	ANY	ANY	192.168.42.0/24	>1023	Allow
TCP	192.168.42.1	ANY	ANY	ANY	Deny
TCP	ANY	ANY	192.168.42.1	ANY	Deny
TCP	192.168.42.0/24	ANY	ANY	ANY	Allow
TCP	ANY	ANY	192.168.42.55	25	Allow
TCP	ANY	ANY	192.168.42.98	80	Allow
TCP	ANY	ANY	ANY	ANY	Deny

The following line allows any address in our internal address range of 128 addresses to use any port to communicate to any other address using any port. Does this mean that any of these addresses can now communicate with 192.168.42.1 address from the line above?

No. The rules are applied in order, top down with each request, so the denial of traffic to 192.168.42.1 will occur before the allowed traffic on the next line.

Firewall Rule Example 2

[Protocol]	[Source Address]	[Source Port]	[Target Address]	[Target Port]	[Action]
TCP	ANY	ANY	192.168.42.0/24	>1023	Allow
TCP	192.168.42.1	ANY	ANY	ANY	Deny
TCP	ANY	ANY	192.168.42.1	ANY	Deny
TCP	192.168.42.0/24	ANY	ANY	ANY	Allow
TCP	ANY	ANY	192.168.42.55	25	Allow
TCP	ANY	ANY	192.168.42.98	80	Allow
TCP	ANY	ANY	ANY	ANY	Deny

Think about the next two lines with target IP addresses ending in 55 and 98. Why are they needed? In the line above we've already allowed any traffic from our 192.168.42.xxx range to communicate to everything (except 192.168.42.1).

The port addresses provide the clue. Port 25 is the Simple Mail Transport Protocol and port 80 is HTTP. This implies a mail server and a web server are using these IP addresses.

These two rules allow access from addresses outside the 192.168.42 range to these services on these two servers.

Firewall Rule Example 2

[Protocol]	[Source Address]	[Source Port]	[Target Address]	[Target Port]	[Action]
TCP	ANY	ANY	192.168.42.0/24	>1023	Allow
TCP	192.168.42.1	ANY	ANY	ANY	Deny
TCP	ANY	ANY	192.168.42.1	ANY	Deny
TCP	192.168.42.0/24	ANY	ANY	ANY	Allow
TCP	ANY	ANY	192.168.42.55	25	Allow
TCP	ANY	ANY	192.168.42.98	80	Allow
TCP	ANY	ANY	ANY	ANY	Deny

The final line is the explicit deny all.

I say required because best practices as well as some regulatory requirements such as PCI require this rule. It is a safety mechanism to prevent any traffic that is not specifically identified to be blocked from passing the firewall and entering your systems.

Firewall Rule Example 2 (Cont.)

- Allow response to TCP connections to internal hosts
- Prevent the firewall (192.168.42.1) from directly connecting to anything
- Prevent external hosts from directly accessing the firewall
- Allow internal hosts to access external resources

So lets review this again, the first line allows **internal** TCP connections.

The second and third lines, in case you haven't already guessed, prevents anything from connecting directly to the firewalls IP address as well as preventing the firewall from connecting directly to anything.

The next line allows internal hosts access externally.

Firewall Rule Example 2 (Cont.)

- Allow external hosts to send e-mail inbound to the e-mail server at 192.168.42.55
- Allow external hosts to access an internal Web server at 192.168.42.98
- Apply a default-deny rule to all traffic not matching a previous exception

The next two rules allow external communications from outside the local network we have defined to connect to the mail and web servers. And lastly, we deny all other traffic on any port.

Ingress/Egress Filtering - Common Rules

- Access to insecure Internet Web sites (HTTP)
- Access to secure Internet Web sites
 - HTTP over SSL or TLS
- Access to other Internet Web site protocols
 - SQL and Java
- Inbound Internet e-mail
- Outbound Internet e-mail

Firewall rules are established to enforce the security policy of the organization and protect the organization and its information from disclosure, alteration and harm. The rules we establish depend on many factors which make standardizing on a set of common rules extremely difficult. There are some general considerations we can apply however. HTTP is not considered secure, especially if viewing or transferring sensitive data.

Rules can be used to ensure that SSL/TLS is required by restricting access to port 443 which is used by SSL/TLS on some websites. Likewise other, IP and port combinations can be used to limit traffic to specific servers performing specific purposes.

Ingress/Egress Filtering

- External entities initiating connection
- Inbound rules when an internal resource is specifically hosted for the purposes of being accessed by external entities
- Use a single IP address for a single host
- Correct subnet or range designation for a collection of hosts
- Specify the port when possible

Some additional thoughts on building your firewall rules:

- Don't allow external entities to initiate a connection unless you are running internal services, such as a Web or mail server. If that is the case, these servers should be placed in a demilitarized zone to prevent direct access from the untrusted internet to your trusted internal LAN.
- Inbound rules are needed only when an internal resource is specifically hosted for the purposes of being accessed by external entities, otherwise, incoming traffic should be blocked.
- Use a single IP address for a single host and the correct subnet or range designation for a collection of hosts
- Specify the port when possible, otherwise use a valid port range.

Ingress/Egress Comm. Commonly Blocked

- All ICMP traffic originating from the Internet
- Any traffic directed specifically to the firewall
- Any traffic to known closed ports
- Any traffic to known ports of known malware

Things that should be blocked in all circumstance are:

- All ICMP traffic originating from the Internet. ICMP or Internet Control Message Protocol can be used on your local area network as a management and troubleshooting protocol, but it should never originate outside your LAN.
- Any traffic directed specifically to the firewall. The firewall should not accept traffic. Should someone gain access to the firewall, than rules could be modified to allow any traffic an attacker might choose.
- Any traffic to known closed ports. The only purpose for traffic directed to closed ports is malicious. Block it.
- Any traffic to known ports of known malware. Yes indeed, there are malware programs that are known to use specific ports. These should be blocked too.

Ingress/Egress Comm. Commonly Blocked

- Inbound TCP 53 to block external DNS zone transfer requests
- Inbound UDP 53 to block external DNS user queries
- Any traffic from IP addresses on a blacklist
- Any traffic from internal IP addresses that are not assigned

Additional traffic that should normally be blocked are:

- Inbound TCP 53 to block external DNS zone transfer requests – DNS will be discussed in greater detail later in the course.
- Inbound UDP 53 to block external DNS user queries
- Any traffic from IP addresses on a blacklist
- Any traffic from internal IP addresses that are not assigned

End of Lecture 1



of Lecture 1

21

This ends Lecture 1 of Unit 5. We will continue to look at firewalls in Lecture 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 7

Firewall Design Strategies

Lecture 2

Welcome to Lecture 2 of Unit 7

Logging and Monitoring

- Why log?
 - Validation that firewall rules are configured properly
 - Historical tracking and trend analysis
 - Reactive tracking and tracing of attacks

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

We will begin this lecture by looking at logging and asking the question why should you log events?

First, what is a log? A log is a record of events or activities that have taken place and are associated with a device or application. Many devices, operating systems and applications produce logs. Administrators usually have some degree of control over what specific information is logged, but not always. It depends on the device or application. Occasionally the only choice is to turn logging on or turn it off. So what should you do?

Logs can and should be used for several purposes. Here we've listed just a few. Critical areas in your environment such as your firewall should always have logging turned on. The same is true of critical applications and operating systems supporting your applications.

Logging and Monitoring

- Why log?
 - Validation that firewall rules are configured properly
 - Historical tracking and trend analysis
 - Reactive tracking and tracing of attacks
 - Meet compliance requirements

A significant addition to this list would be to meet compliance requirements. The payment card industry and HIPAA both require logging of events associated with the environments containing and transporting or processing their relevant data. Logging is a detective control which as the name implies allows you to detect issues and intrusions. Of course to do that, logs need to be examined.

Logging and Monitoring

- What data should be logged?
 - All connection rejections
 - All traffic to successfully transverse through the firewall
 - Firewall configuration changes
 - Access to the firewall system

Let's focus on firewall logs for the time being. What should we be looking at?

This is the short list of important events to observe.

Starting at the top, why do we care about connections that were denied?

This is important because it will tell us who or what was trying to get though our firewalls but failed. We can't assume that all the refused traffic is malicious, so it also tells us about traffic that is being blocked that we may want. More likely though, it will give us an indication of the type and volume of traffic that we do want to block. This gives us a measurement of the interest in malicious actors wanting into our network. It also gives an indication of the effectiveness of our rules.

If traffic does get through, we want to know if it was traffic we specifically wanted. If it wasn't then we may need to adjust our rules.

Anytime firewall rules are changed, we should be aware of it whether we intended to make the change or not. Changes to firewall rules can be dangerous if not implemented correctly. A solid change control process with appropriate management oversight is needed to ensure that the firewall is not compromised.

That leads us to the last event. All access to the firewall should be logged. The firewall should not be accessed administratively that often and when it is, there needs to be a record of who accessed it and what was done.

Logging and Monitoring (cont.)

- Monitoring allows for alerting
- Alerting allows for prompt response
- **Review log files regularly!**

To be a good detective control. Logs need to be reviewed regularly. This can be done manually or through automated processes. Large volumes of logs can be generated in larger or high traffic environments which usually means manual review is not practical. Security Information & Event Management tools can help to automate the process of parsing volumes of logs and generating alerts based on specific activities.

Logging and Monitoring (cont.)

- Monitoring allows for alerting
- Alerting allows for prompt response
- **Review log files regularly!**
- **Keep logs for at least a year!**

Logs should be kept for at least a year. This is a requirement of the payment card industry to be in compliance, but it is also a best practice. On average, breaches are discovered about seven months after they occur. Often breaches are found when investigating something completely different. If the logs have been deleted, then there is little forensic evidence to trace back the events that led to the breach. So even if there is no compliance requirement to maintain logs, it is still very highly recommended.

IDS and IPS

- Benefits
 - Logical pairing of functionality
 - Reduction in administrative overhead of maintaining multiple devices
- Drawbacks
 - Potential performance implications
 - Wirespeed
 - Possible feature set limitations

We looked at IDS and IPS devices briefly in an earlier unit, but its time to revisit these important functions. Earlier we talked about IDS and IPS as separate devices with separate functions and they can be. We also discussed the merger of capabilities. Today it is common to find IDS and IPS functionality consolidated in a single device.

I'm bringing this up again here because IDS/IPS cards or blades are often available as add-ons for firewalls. This is a more cost effective way of adding this functionality in small to moderate environments. Of course when installed on perimeter firewalls, the IDS/IPS is limited to traffic traversing the firewall and cannot normally see traffic on the LAN. For closer inspection of LAN traffic, additional firewall/IDS/IPS combinations would be needed, or stand-alone IDS/IPSs.

Exploitable Programming Bugs

- Firewalls run software
- Bugs are result of human error in the software
- Once discovered, bugs are typically addressed and corrected in software patches

Firewalls can be dedicated appliances, software or virtual. Even dedicated appliances however run software to perform their tasks and like virtually all software, there can be flaws. Once discovered these flaws or bugs in the code are usually quickly corrected with a patch. But to do this, the firewall administrator needs to be on the lookout for new patches and take action as quickly as reasonably possible to avoid exposure. Awareness can be through getting on the software vendors mailing list or subscribing to services that track some or all your deployed products and inform you when new releases are available.

Periodic visits to the vendor site is OK, but it may create delays depending on the frequency of visits.

Buffer Overflow

- Memory-based attack
- Typically a result of poor programming
- Can result in code injection
- Used for systems crashing

While we are talking about software flaws, there are a few others that should be mentioned here. These are by no means the only types of vulnerabilities that software may be subject too, but it's a start.

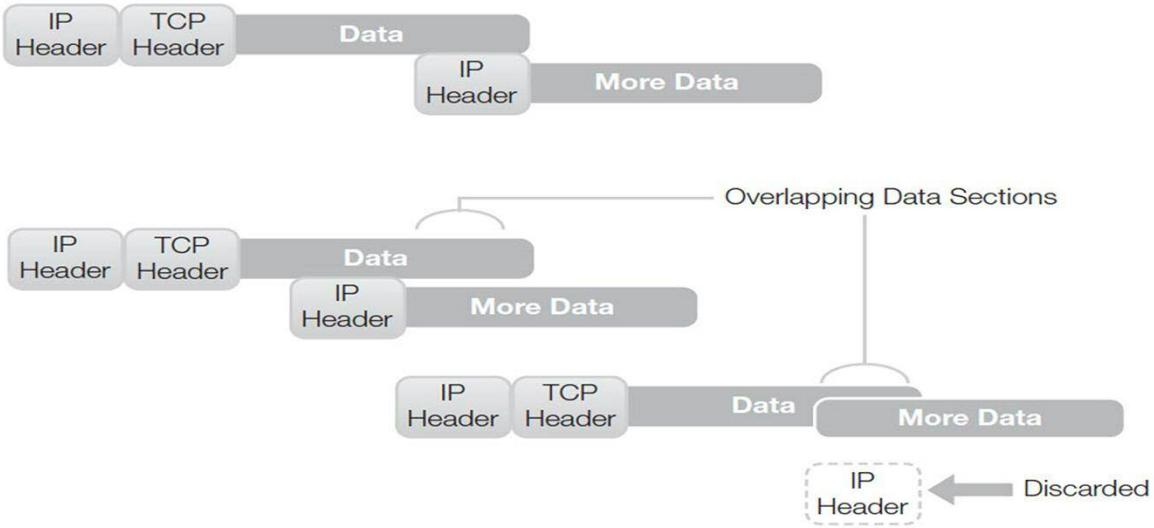
Buffer overflows are a typical software flaw that results from poor programming practices. When software is collecting information from say an address field in a web form, that information is placed in an area of memory called a buffer. Programmers can defines the size of the field and buffer to use. A poor program however may allow an excessive amount of information to be collected which exceeds the buffer size. The excess information will usually be placed in memory adjacent to the buffer which may overwrite the programs code causing the program to crash. If the attacked has sufficient knowledge of the software under attack, they may be able to place executable code outside the buffer and force it to run.

Fragmentation

- Overlapping
 - Full or partial overlapping datagrams
- Overrun
 - Excessively large datagrams
- Potential result in denial of service

Fragmentation has a number of different forms that may be used. IP datagrams can be intentionally manipulated so that when reassembling them they overlap causing a data fault which may cause the system to crash. In another variation, excessively large datagrams can cause buffer overflows that may also cause a system to crash. The net effect is a denial of service.

Fragmentation and Overlapping



This graphic shows how the fragmentation and overlapping flaws look at the packet level. More information is available in your text.

Internal Code Planting

- Requires access from inside the network environment
- Involves either a hacker or a user placing malicious code onto internal systems
- Assumes the firewall has lenient outbound traffic restrictions
- Results in internally initiated connections connecting to malicious internet presence

You will often hear that the weakest link in the security chain is the employee. Employees are subject to various influences and may intentionally or unwittingly aid a hacker in placing malicious code within your environment. Often the firewall engineer focuses too much on external traffic attempting to enter the environment while ignoring traffic coming from within.

It is very important therefore to know what your environment should look like normally and prevent unknown or suspicious traffic from leaving. This may be harder than it seems, but it is possible, and should be done with the same focus as protecting inbound traffic.

Denial of Service (DoS)

- Flooding attack that overwhelms systems
- Often causes system shut down or failure
- May manifest as performance problems

The firewall is one of the first lines of defense against denial of service attacks. DoS and distributed denial of service DDoS attacks attempt to flood systems with more requests than the system can manage. The results can range from poor performance to system failures. As system capacities have improved reducing the effectiveness of DoS attacks, the attacks too have evolved to incorporate very large numbers of compromised systems called zombies or bots to increase the traffic past manageable levels.

Gateway Bottlenecks

- Gateway or pass-through firewall can become a bottleneck during high-traffic periods
- DoS attack can consume all processing capabilities of the firewall

Using a gateway or pass-through firewall can be a target for a DoS or DDoS attack. A successful attack can consume all the firewalls capacity to manage traffic and cause it to fail. This effectively closes the door to the organization until the firewall can come back up.

Encrypted Transport

- Two main forms of communication encryption
 - tunnel mode
 - transport mode
- Tunnel mode encrypts the original payload and header
- Transport mode encrypts only the payload
- Firewall cannot filter encrypted data

A firewall is typically not the intended destination or direct communication partner of a communication, especially encrypted communications. Thus, any encrypted data cannot be filtered by a firewall.

There are two main forms of transaction or communication encryption: tunnel mode and transport mode. Tunnel mode encrypts the entire original payload and header, while transport mode only encrypts the payload. In tunnel mode, a temporary header goes with the encrypted packet to guide its path across the VPN tunnel. In transport mode, the original header remains in plain text.

Filtering on the transport mode header is a viable option, as this is the same filtering and the same header in the packet was not transport mode encrypted. Thus, any header-only filtering rules could still apply to transport mode-encrypted communications. However, any filtering that requires an examination of the payload will be unsuccessful.

Encrypted Transport (cont.)

- May choose to support or allow encryption of specific types over specific protocols or ports, but disallow and prevent encrypted communications elsewhere
- Firewall rules of encrypted traffic can range from full allowance to full denial
- May allow encryption over a specific port or only certain users

When building or designing firewall filtering rules, you must make a choice about how to handle encrypted content. Consider both the valid and invalid reasons for content encryption. The organization can choose to support or allow encryption of specific types over specific protocols or ports, but disallow and prevent encrypted communications elsewhere. Encryption for Web communications and e-mail exchanges are often acceptable, while other transactions with the Internet might not be encrypted.

When designing the firewall rules, the management of encrypted traffic can range from full allowance to full denial. Whether to allow encryption over a specific port but not another and whether to allow encryption all the time, for only certain users, or for no one are common issues your organization needs to address and plan for.

Example: Encrypt Web communications and e-mail, do not encrypt other Internet communications

Malware Scanning

- Benefits
 - Scanning for various malware: viruses, Trojans, spam, spyware, etc.
- Drawbacks:
 - Potential of negative impact on performance
 - Wire-speed performance
 - Memory and CPU implications
 - Requires regular maintenance and update
 - Feature set may not be comparable to other dedicated solutions or may not complement current mechanisms

Newer forms of packet inspecting firewalls can have the ability to scan traffic for malware as it transits from the untrusted to your trusted network. While this may be tempting as a first level intervention, it has serious drawbacks. Depending on your environment and the traffic volumes, there can be significant performance problems. The firewall must be designed with sufficient memory and processing capacity which raises costs. Also, just like other anti-malware solutions, updates are frequent for the software to be effective. This alone can be an issue placing your firewall in an unstable condition as new signatures are implemented.

In general, it's not a bad idea to take this approach, but it is not practical in most situations. Standalone anti-malware solutions are still a superior bet.

VPN Endpoint

- Benefits
 - Reduction in administrative overhead of maintaining multiple devices
- Drawbacks
 - Potential performance implications
 - Possible feature set limitations as compared to stand alone solutions

Lastly a firewall can serve as a VPN endpoint or terminus. This avoids the need for another piece of hardware and the associated maintenance and administrative overhead, but like the anti-malware solution, it creates issues. Again performance impacts can result. In addition, it's not likely that a firewall implementation will have the same feature rich environment that a standalone system would have. Again, this is a very environment specific judgement call. Infrequently used VPN services may make incorporating this into the firewall a cost effective solution.

End of Lecture 2



of Lecture 2

19

This ends Lecture 2 of Unit 7. We will continue in Lecture 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 7

Firewall Design Strategies

Lecture 3

Welcome to Lecture 3 of Unit 7

Reverse Proxy

- Reverse proxy allows access to internal Web site content from the public network
- Benefits
 - Enhanced security
 - Encryption
 - Reverse caching

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

Earlier in a previous unit we briefly introduced proxies. If you recall, proxies are middlemen between your trusted network and the outside world. They prevent direct connectivity and thus isolate your trusted devices from direct contact with the untrusted. Now we introduce the reverse proxy. The reverse proxy as the name suggests operates like a regular proxy but in the reverse direction mediating communications from the untrusted internet to specific areas in your trusted network. The reverse proxy offers the benefits of:

Enhanced security: No direct access to internal Web servers from the public network

Encryption: The proxy server can function as the encryption endpoint, allowing for packet inspection of traffic destined for the Web server

Reverse caching: Increased performance because Web pages are cached on the proxy server

Port Forwarding

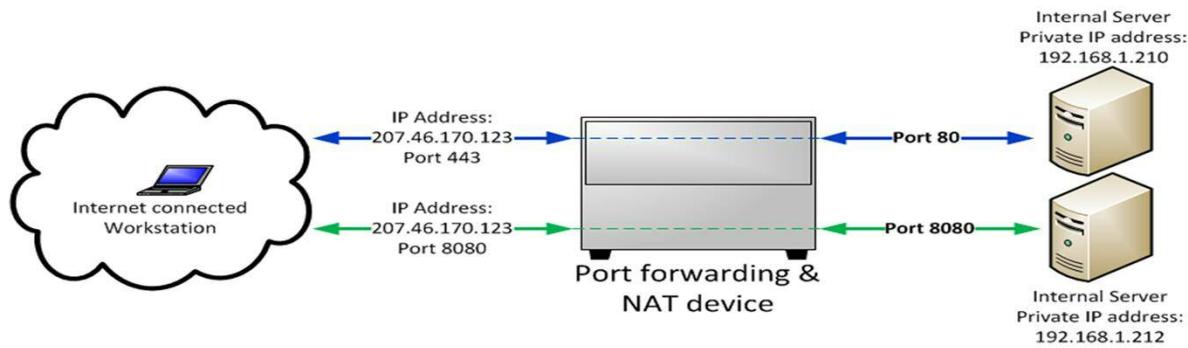
- Receipt of IP traffic based on IP/port number
- IP/port number forwards to another IP/port number
- Benefits
 - Ability to utilize a single public IP address
 - Maps to multiple other internal destinations
 - No direct connectivity to internal resources

Port forwarding is another access method that allows external connections to the external IP address with a specified port number. This IP and port number are mapped to a specific devices in the trusted network. This operates like Network Address Translation in reverse. The external party does not know the internal address associated with the shared external IP and port number combination.

This can have a number of benefits including making more efficient use of a single external IP address which can be mapped to multiple internal addresses. Also, the process removes direct connectivity to internal resources and protects their internal IP addresses from disclosure.

Combining Port Forwarding with NAT

Private IP addresses of the internal systems are masked from the public network



In this diagram we see the combination of NAT and port forwarding. By adding NAT to a port forwarding configuration, the private IP addresses of the internal systems are masked from the public network.

Bastion Hosts

- Simple single-layer architecture
- Reside outside of the firewall or in the demilitarized zone (DMZ)
- Typically serve as the first point of connection from the Internet
- Can be a software or hardware solution

All these connections need to be managed and the primary firewall is not always the best place to do it. One choice is to use a Bastion Host firewall also referred to as just a Bastion Host. These are specially hardened devices that reside outside the primary firewall or more frequently in the DMZ. The Bastion host is normally the first point of connection with the internet. Its job is to evaluate connections and prevent malicious ones from being established.

Bastion hosts may operate as a safety valve of sorts and cease allowing communications if it determines the connections are malicious or it cannot manage the volume of traffic.

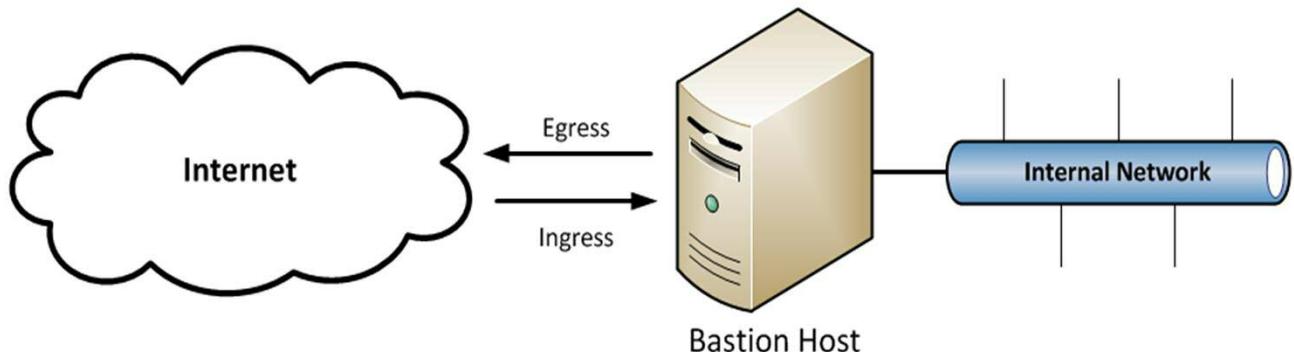
Categories of Bastion Hosts

- Proprietary OS
 - Built specifically to be bastion hosts
- General-Purpose OS
 - Serve as client or server Oss
 - Can be configured to serve as bastion hosts

Bastion hosts fall into a couple of categories. Those that are purpose built with a proprietary operating system and those that use a general purpose operating system. As the point is to have as bulletproof a system as possible, going the proprietary OS is probably the better choice but that choice will also be more expensive.

Bastion Host Placement

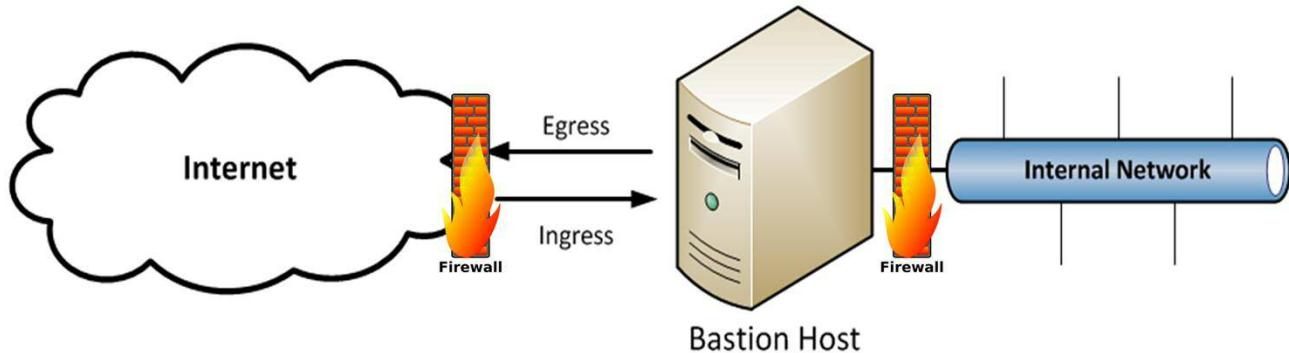
Ingress/egress architecture with a bastion host



Here we see a Bastion host firewall between the internet and the internal network.
This is not the best placement however.

Bastion Host Placement

Ingress/egress architecture with a bastion host in the DMZ



A better option is to place the bastion host in the DMZ. Traffic from the internet terminates at the bastion host. If needed, the bastion host can forward requests to the trusted network. Likewise, the bastion host accepts communications from the trusted network and acts as a proxy forwarding the internet bound traffic outside.

What Should You Allow or Block?

- Perform complete inventory
- Include:
 - Protocol in use
 - Port(s) in use
 - Likely source and destination addresses

As we wrap up this unit, I'd like to return to the question of what to allow or block. I'll start by saying that the answer is not simple and depends greatly on the unique configuration of your environment. To begin to understand the answer to this question, you must first inventory everything in your environment. As part of that inventory you need to include what protocol or protocols are used, on what ports and if possible what the likely source and destination IP addresses would be.

What Should You Allow or Block?

TABLE 8-1 A partial list of communications occurring on a network.

TRANSPORT LAYER PROTOCOL	PORT	PROTOCOL	SOURCE	DESTINATION
TCP	8080	HTTP	Internal Clients	192.168.42.101 (Internal Web site)
TCP	8081	HTTPS	Internal Clients	192.168.42.101 (Internal Web site)
TCP	80	HTTP	Internal Clients	Numerous Internet Web sites
TCP	443	HTTPS	Internal Clients	Numerous Internet Web sites
TCP	110	POP	Internet Clients	192.168.42.115 (Internal e-mail server)
TCP	25	SMTP	Internet Clients	192.168.42.115 (Internal e-mail server)
TCP	25	SMTP	192.168.42.115	External e-mail server (ISP based)
TCP	22	SSH	Internal Clients	Numerous internal servers

Your inventory should end up looking something like this. You should notice that this is approaching the appearance of the access control rules in a firewall – and that is the point. As you refine and complete your inventory you will have the information you need to begin establishing a reasonable start at your firewall rules.

What to Block

- All Internet control message protocol (ICMP) traffic originating from the Internet
- Any traffic directed specifically to the firewall
- Any traffic to known closed ports
- Any traffic to known ports of known malware, such as 31337, used by Back Orifice

In lecture 1 we mentioned some of the common ports allowed along with the caveat that even they would depend on your specific environment. By completing the inventory of your environment, you should have a good idea of what traffic should be taking place into and out of your systems.

So what should you be blocking? In general there are some things that should never be allowed in. Any ICMP traffic from the internet should be block. This type of traffic is for use on your internal network and should never originate from outside.

Any attempts to connect directly to your firewall should be blocked.

Traffic to known closed ports should be blocked. There can be nothing good coming from this traffic.

Lastly, there are several known ports used by malware that should be blocked as a precaution.

What to Block (Cont.)

- Inbound Transmission Control Protocol (TCP) 53 to block external DNS zone transfer requests
- Inbound User Datagram Protocol (UDP) 53 to block external DNS user queries
- Any traffic from IP addresses on a blacklist
- Any traffic from internal IP addresses that are not assigned

Additional traffic to block are inbound TCP requests to port 53 as well as inbound UDP requests to port 53.

IP addresses that are blacklisted should be blocked. These IP addresses are available from Anti-virus vendors and other sources that track malicious activity on the internet.

Lastly, any traffic from internal addresses that are not known to be assigned should be blocked. This type of addressing may be an attempt by malware in your environment to find a way out of the firewall. In addition to blocking this traffic, you should also be investigating the source.

Summary

- Firewall limitations, weaknesses, and countermeasures
- Public Internet and private network separation
- Firewall rules for restricting and permitting data transit
- Use of protected demilitarized zones (DMZs)
- Security strategies and requirements for availability

To summarize, in this unit we have examined firewall limitations, weaknesses and countermeasures.

We have explored how firewalls and other techniques can provide separation between the internet and your trusted private networks. We have begun exploring the construction and purposes of firewall rules.

We've looked at the use of demilitarized zones and the use of bastion hosts. Lastly we have begun our discussion on security strategies with regard to availability and the impact on firewall selection and configuration.

End of Lecture 3



of Lecture 3

14

This ends Lecture 3 of Unit 7.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 8

VPN Fundamentals

Lecture 1

Welcome to Lecture 1 of Unit 8

Key Concepts

- Strategies for protection of remote network access using a virtual private network (VPN)
- Network architecture necessary for VPN implementation
- Types of VPN solutions and common protocols used for connectivity and data transport
- Planning and selection of VPN options for best value to the organization

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this first lecture of Unit 7 we will begin looking more closely at firewalls. We will be discussing the limitations and weaknesses of firewalls. We will look at the public and private network interface and protection strategies including the use of demilitarized zones, firewalls and other devices. We will begin looking at the rules that define how firewalls operate. And we will look at availability requirements and how firewalls may impact availability.

Learning Objectives

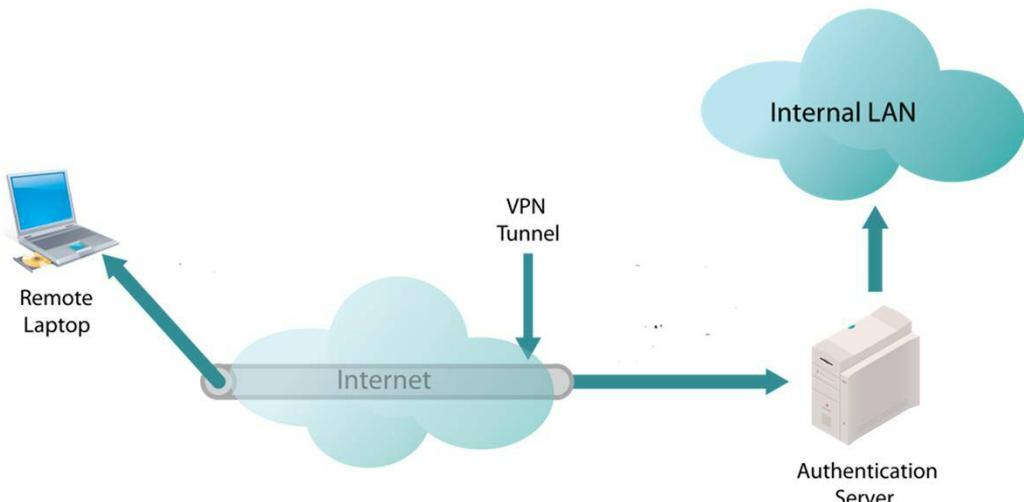
Learning Objective

- Describe the foundational concepts of VPNs
- Discuss the use cases for VPNs
- Explain the strengths and weaknesses of VPNS

Our learning objective for this Unit is to describe the foundational concepts of VPNs.

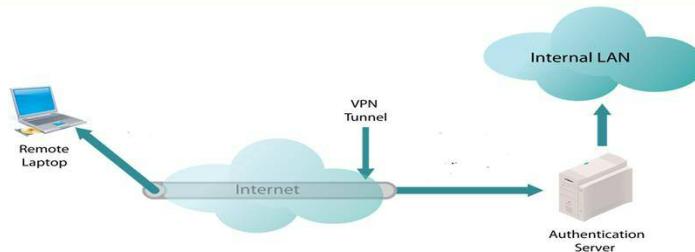
We will describe the use cases for VPNs and explain the strengths and weaknesses of VPN use.

Virtual Private Network (VPN)



This graphic depicts a VPN and one of the potential uses. Here a remote user is connecting to a private network through an internet tunnel.

What is a VPN?

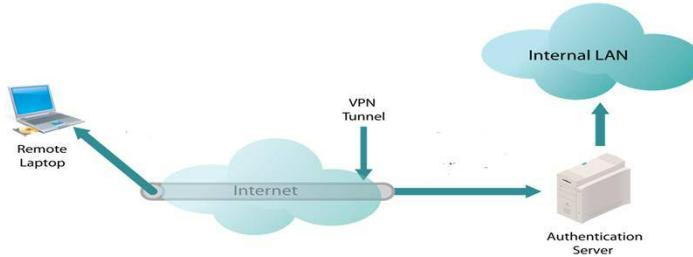


- Network that uses the Public Telecom Infrastructure (Internet) to provide remote access to secure private networks
- Allows organizations to privately transmit sensitive data remotely over public networks

So what exactly is a Virtual Private Network (VPN)?

In a nut shell, a VPN is a method of establishing a secure connection by a computer network that uses the public telecom infrastructure (i.e., Internet) to provide remote access to secure private networks. This allows organizations to privately transmit sensitive data remotely over public networks which are inherently insecure. A VPN secures communication between remotes hosts and private networks through tunneling, which protects sensitive information transiting the public network. We will be looking more closely at this process throughout this unit.

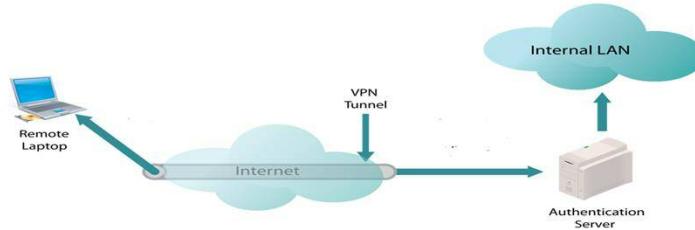
What is a VPN?



- Secures communication between separate private networks through tunneling
- Protects sensitive information transiting the public network

Tunneling refers to creating an encrypted channel between two points through the internet. It is the encryption that keeps the information private as it traverses the public network.

What is a VPN?



- Low-cost alternative to leased-line infrastructure
- Supports Internet remote access
- Provide remote access and remote control

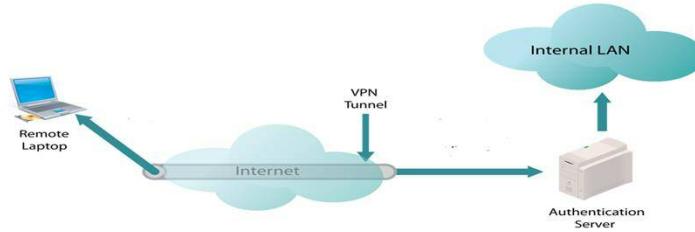
VPNs can be a low-cost alternative to leased-line infrastructure for delivering remote connectivity to offices and workers.

Leased lines create a direct and permanent path between two locations. This was the norm before the internet became widespread, fast, and stable.

Leased lines still provide wide area connectivity via reserved connection for private customer use, but the cost has limited this use to special purposes such as between financial entities. For consumers, the telco provides dedicated circuits that provide “last mile” access from user premises to ISP.

VPNs Support Internet remote access (i.e., remote office and telecommuter), LAN-to-LAN internetworking (i.e., home office and satellite offices), and controlled access within a network (i.e., mobile users and desktop users).

What is a VPN?



- Employs encryption and authentication for secure transmission
- Restrictions for mobile users that ensure a baseline level of conformity and security

Organizations can keep private information protected by encryption and remotely accessible to individuals or groups on an as-needed basis.

Unauthorized parties cannot eavesdrop, intercept, or otherwise capture private sessions between VPN client and server.

VPNs provide remote access and remote control, and employ encryption and authentication for secure transmission

VPN policies can impose restrictions for mobile users that ensure a baseline level of conformity and security. Use of VPNs can also allow businesses to enforce network policies that mandate client systems maintain up-to-date patches, signature files, and versions of anti-malware and anti-virus packages.

Enforce minimum and mandatory rules that dictate levels of user privilege, separate areas of access, ensure recommended cryptographic capabilities, etc.

VPN Deployment Models

- True, Trusted, Secure, and Hybrid Models
- Tailor VPN security to match organizational and data privacy needs
- Establish control
 - Components (software and hardware)
 - Conversations (endpoint connections)
 - Communications (network infrastructure)

The text defines a true VPN as one which is totally owned and controlled by the organization using the VPN. This is not a common occurrence however. Where that situation does exist, it would be termed a Trusted VPN. Another example of a trusted VPN is one which employs dedicated circuits provided by a common carrier or telephone company. This idea here is that the telco is trusted and the medium is not shared but dedicated to this application. This situation does rely on the trustworthiness of the telco and of course it does not come cheap. Dedicated circuits are very pricy.

A secure option requires the use of encryption and abandons the need for dedicated circuits and wholly owned systems. Instead, public networks are utilized. Encryption ensures privacy and authentication however eavesdropping may still be possible but won't be effective without being able to decrypt the channel. This is the most cost effective and most used of the different models.

The hybrid approach establishes a secure channel over trusted VPN connections. With the trusted VPN, the organization has knowledge and control of the pathway.

VPN Deployment Models

- Customers and providers may separately manage and maintain devices
- Customers may outsource different aspects of VPN ownership and operation to service providers
- Custom tailor ownership and operator responsibilities to budgetary needs

The different models we've looked at, but especially the secure and hybrid models, provide a number of options as to who controls and manages the devices used for and by the VPN connections. This can vary from single control to each party being responsible for their own to outsourcing the responsibility to a third party.

Which model will depend on a number of factors including your security requirements, your budget or perhaps your regulatory requirements.

Network Protocols

- Tunneling protocols package packets within packets for secure transport
- Transport protocols package payloads within packets
- Encapsulating protocols wrap around original passenger protocols
- Carrier protocols carry the packaged VPN packets

There are two modes of operation that can be used by VPNs, tunneling and transport. In Tunneling mode, each packet, including its header information is encrypted and encapsulated into another packet. The new packet contains its own IP header which allows it to be routed to the appropriate gateway. Tunneling mode allows NAT traversal which allows local area networks to be connected such that non-routable (RFC1918) addresses can be used within the encapsulated packet. When the encapsulated packet reaches the gateway and the encapsulation is removed and the packet is decrypted, it is as if the remaining packet originated from the new network.

Transport protocol does not encapsulate packets. Rather, it encrypts the data within the packet. The source and destination addresses are not protected as they are in tunneling mode. Neither can these packets provide NAT traversal. Only the information

VPNs Bridge Distant Connections

- Home and satellite offices
- May span separate cities, states, countries, geographic territories, and international borders
- Provide varying levels of granular network access to separate locations
- VPNs maintain confidentiality and integrity for users and data (C-I-A triad)

VPNs then can link Home and satellite offices that may span separate cities, states, countries, geographic territories, and international borders.

The allow the Sharing of private LAN and intranet resources globally.

They may be used by trusted third parties such as Suppliers and distributors so they may maintain a separate private network for product sales and purchasing or parts ordering.

Organizational headquarters and satellite offices may share common directory services, informational databases, supply chain resources, etc.

VPNs as Access Control

- VPNs can provide varying levels of granular network access to separate locations.
 - Client-server connections focus on user profile permissions and restrictions.
 - Multiple site-to-site connections apply user policies and network controls.
 - VPN clients are browser-based and executable formats.
 - VPN servers can integrate into routing devices and network appliances.

VPNs can provide varying levels of granular network access to separate locations depending on the type of service being provided.

For example, Client-server connections focus on user profile permissions and restrictions.

Multiple site-to-site connections can apply user policies and network controls.

From the user perspective, VPN clients are browser-based and executable formats.

From the network administrator view, VPN servers can integrate into routing devices and network appliances.

This requires careful planning in order to ensure the security that can be provided by VPNs is not compromised.

Drawbacks of VPNs

- Congestion, latency, fragmentation, and packet loss
- Difficulties with compliance and troubleshooting
- Encrypted traffic does not compress
- Lacks repeating patterns
- More bandwidth-intensive than clear-text transmission
- Connectivity requires high availability

There are two sides to all things and VPNs are no different. They have their drawbacks too. VPNs suffer from the same congestion, latency, fragmentation, and packet loss as any long-distance connection experiences.

VPN clients are more difficult to keep compliant and troubleshoot than on-site devices and systems.

Encrypted traffic does not compress because it lacks repeating patterns and is therefore more bandwidth-intensive than clear-text transmission.

VPN connectivity requires high availability for constant uptime and accessibility

VPN Vulnerabilities

- Denial of service attacks
- Missing patches
- Backdoor attacks
- Unpublished vulnerability in the code
- Weak client security
- Weak authentication
- Hair Pinning
- Credential sharing

VPNs are also subject to a number of vulnerabilities including most associated with software such as missing patches, backdoor attacks 0-day or unpublished vulnerabilities, weak client security and weak authentication. Although more of a human failing, human factors such as credential sharing can come into play as well.

Denial of service attacks are ever present and depend on the resources allocated to the VPN gateways.

Hairpinning or U-turning is a technique that can be implemented that returns the traffic out the same interface it was received in. There are some legitimate uses for this as will be described later, but it also presents an opportunity for exploitation.

VPNs Benefits

- Corporations can save on leased-line costs with VPN.
 - Eliminates need for long-distance leased-line connectivity
 - Reduces long-distance telecommunication charges
 - Can offload support costs (outsource) to network operators
- Scalable network arrangements are possible with VPN.
 - Branch offices can deploy readily available VPNs.
 - VPNs can scale from a few nearby offices to several campuses around the world.

Some of the potential benefits of VPNs include cost savings.

Corporations can save on leased-line costs with VPN. VPNs can eliminate the need for long-distance leased-line connectivity. This reduces long-distance telecommunication charges and it can offload support costs (outsource) to network operators.

Scalable network arrangements are possible with VPN. Branch offices can deploy readily available VPNs. VPNs can scale from a few nearby offices to several campuses around the world.

VPNs Security and Privacy Issues

- Cannot ensure quality of service (QoS) or complete security
- Links depend on availability, stability, and throughput of ISP connection
- Not ideal connection method for dial-up modems or low-bandwidth links
- Infected mobile users can potentially damage or disrupt the private network
- Confidential data can be copied outside the boundaries of internal controls

On the downside, VPNs cannot ensure quality of service (QoS) or complete security.

VPN links depend on availability, stability, and throughput of ISP connection. They are not an ideal connection method for dial-up modems or low-bandwidth links.

VPNs may allow infected mobile users to spread their infections which can potentially damage or disrupt the private network.

Also, confidential data can be copied outside the boundaries of internal controls. This can be mitigated using other control mechanisms such as Data Loss Prevention, but this adds to the cost of the implementation.

VPNs Are Not a Cure-all Solution

Upkeep, Updates, and Upgrades

- Safety and Security
- Software Fixes
- Software Patches
- Software Updates
- Hardware Upgrades

Client Compliance

- Roaming profiles
- Tamper with systems
- Bypass restrictions
- Careless users
- Defiant users

Inconsistent Security

- True VPN
- Trusted VPN
- Secure
- Hybrid VPN

In short, VPNs are not a cure-all solution. To be effective, VPNs require upkeep, updates, and upgrades just like any other network.

Clients must maintain baseline levels of safety and security.

Servers must maintain current fixes and patches for software.

Administrators must maintain software updates and hardware upgrades.

In addition, VPN clients are harder to keep compliant.

VPNs Are Not a Cure-all Solution

Upkeep, Updates, and Upgrades

- Safety and Security
- Software Fixes
- Software Patches
- Software Updates
- Hardware Upgrades

Client Compliance

- Roaming profiles
- Tamper with systems
- Bypass restrictions
- Careless users
- Defiant users

Inconsistent Security

- True VPN
- Trusted VPN
- Secure
- Hybrid VPN

Using VPNs make Roaming profiles more challenging to maintain than local user profiles.

Offline users can tamper with systems or bypass some restrictions.

Careless or defiant users may compromise systems and threaten the network.

VPNs Are Not a Cure-all Solution

Upkeep, Updates, and Upgrades

- Safety and Security
- Software Fixes
- Software Patches
- Software Updates
- Hardware Upgrades

Client Compliance

- Roaming profiles
- Tamper with systems
- Bypass restrictions
- Careless users
- Defiant users

Inconsistent Security

- True VPN
- Trusted VPN
- Secure
- Hybrid VPN

Varying VPN client-server setups provide inconsistent security provisions.

As a reminder, with a True VPN—a single organization owns all of the network infrastructure (ideal)

With the Trusted VPN, the organization controls communication pathway, but this doesn't prevent eavesdropping

The Secure VPN—uses public networks so the corporation does not control or ensure transmission path

Lastly, the Hybrid VPN provides secure VPN over a trusted VPN connection.

End of Lecture 1



of Lecture 1

21

This ends Lecture 1 of Unit 8. We will continue to look at VPNs in Lecture 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

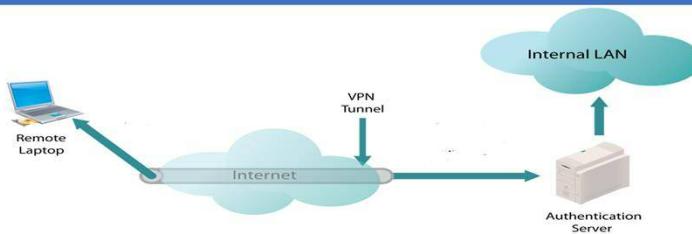
Unit 8

VPN Fundamentals

Lecture 2

Welcome to Lecture 2 of Unit 8

VPN Endpoints



- Host Computer Systems
- Edge Routers
- Corporate Firewalls
- Dedicated VPN Appliances

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In the previous lecture we have looked closely at the VPN in general and discussed the modes of operation. In this lecture, we will continue our exploration of VPNs by looking at endpoints. VPNs can originate and terminate the connection using a number of different devices. For example, endpoints can terminate at a host computer system, edge router, a corporate firewall, or dedicated VPN appliance.

The intent is to provide secure remote access, site-to-site connectivity (i.e., college campuses), host-to-host networking, and extranet (i.e., distributor to supplier), et cetera.

As a reminder, VPNs can operate in two modes of encryption “encapsulation” or tunnel mode which protects the entire packet from header to payload and Transport mode which protects only the packet payload. Which mode is used will influence the endpoint selection.

VPN Deployment ~ Edge Routers

- Transport VPN over public networks
- Insures that all traffic complies with firewall
- Ideal for customer and supplier or business partner access
- Best suited for controlled access into DMZ

One option for VPNs traversing public networks is to terminate at the edge router. This has the advantage of ensuring that the firewall rules are able to be applied. Recall that firewalls cannot normally inspect encrypted traffic, so this method decrypts the packets prior to them reaching the firewall. This makes this option ideal for external partners as it forces compliance with the organizations entrance policies as enforced by the firewall.

It also provides a good option for controlling access into the DMZ.

VPN Deployment ~ Corporate Firewall

- Pass LAN-to-LAN traffic
- Joined networks are treated as any other LAN route
- Users don't have to re-authenticate across segments
- No additional firewall filtering or restriction applies

VPNs can also be terminated at the corporate firewall. This configuration lends itself to LAN to LAN bridges. As we discussed earlier, traffic behaves as if it was on the same LAN. This means re-authentication is not necessary and no additional firewall rules need to be applied.

VPN Deployment ~ Appliances

- Dedicated network offload devices
- Specialized to handle VPN offloading from routers and host systems
- Can be placed outside corporate firewalls for traffic filtering
- Supplements existing corporate firewalls that do not support VPN services

Another approach is to use dedicated VPN appliances. The advantage here is that the appliances are designed to perform this task and use their own resources to do so. This frees up CPU and memory that might otherwise be consumed on routers or firewalls if they were the endpoints. Dedicated VPN appliances can be positioned outside the firewall to allow application of firewall rules before traffic is allowed to enter the trusted network.

VPN Architectures

- Remote access (host-to-site) supports single connections into the LAN
- LAN-to-LAN and WAN (site-to-site) supports LAN-to-LAN via Internet
- Client-server (host-to-host) supports direct connections via Internet

Continuing our look at VPN architectures, we note that remote access (host-to-site) supports single connections into the LAN. This is typically a software or client based VPN that supports private LAN access without edge routers, corp. firewalls, or appliances. This is commonly used by remote or traveling users to access corporate resources.

LAN-to-LAN and WAN (site-to-site) supports LAN-to-LAN via Internet requires endpoints. This combines site-to-site with remote access VPN capabilities and has the ability to scale to large groups of users and network endpoints.

Client-server (host-to-host) supports direct connections via Internet. This configuration provides additional security over shared public infrastructure and links mobile platforms to mission-critical systems and services.

VPN Architectures

- A corporation may control different aspects of the network
 - Provider network: uses a service provider infrastructure for VPN services
 - Customer network: customer-controlled network infrastructure for VPN
 - Customer site: physical location is the only control point
 - Provider device: not under customer control, operates as routing device

Depending on the architecture chosen, a corporation may directly control or assign different aspects of the network. Some term associated with this are:

Provider network: uses a service provider infrastructure for VPN services

Customer network: customer-controlled network infrastructure for VPN

Customer site: physical location is the only control point

Provider device: not under customer control, operates as routing device

VPN Architectures

- Authentication, Authorization, and Accounting (AAA) server deployment
- Different technologies for different needs
 - Desktop and server software for remote client connections
 - Dedicated firewalls, optimized routers, VPN servers, and VPN concentrators
 - Network Access Servers (NASs) for service providers
 - VPN network and policy management centers

Some other considerations when evaluating which VPN architecture to deploy are:

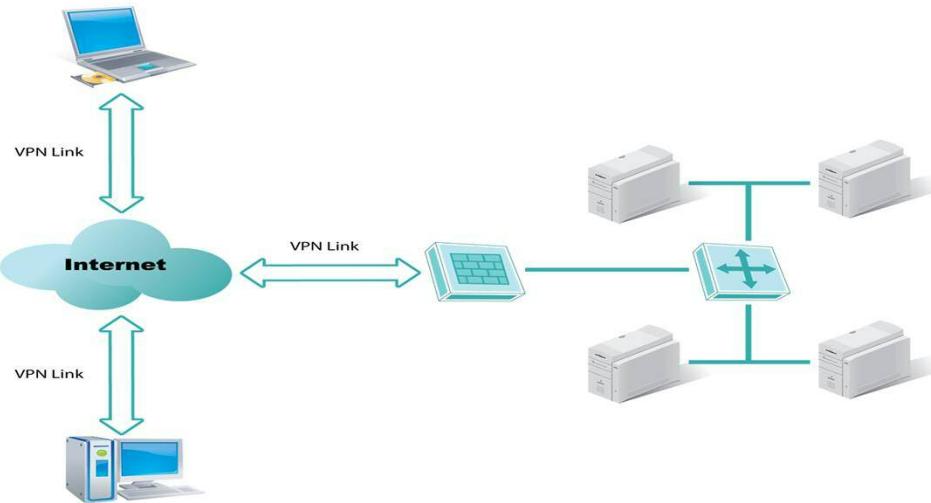
Authentication, Authorization, and Accounting (AAA) server deployment. This vital function tracks who you are (authentication), checks what you're authorized to do (authorization), and records what you've done (accounting). Who manages this and where these services are located can impact your choice of VPN architecture.

Setting up a VPN solution requires different technologies for different technological needs. Some things to consider are:

- Desktop and server software for remote client connections
- Dedicated firewalls, optimized routers, VPN servers, and VPN concentrators
- Network Access Servers (NASs) for service providers
- VPN network and policy management centers

As we continue our examination of VPN's these considerations will become more clear.

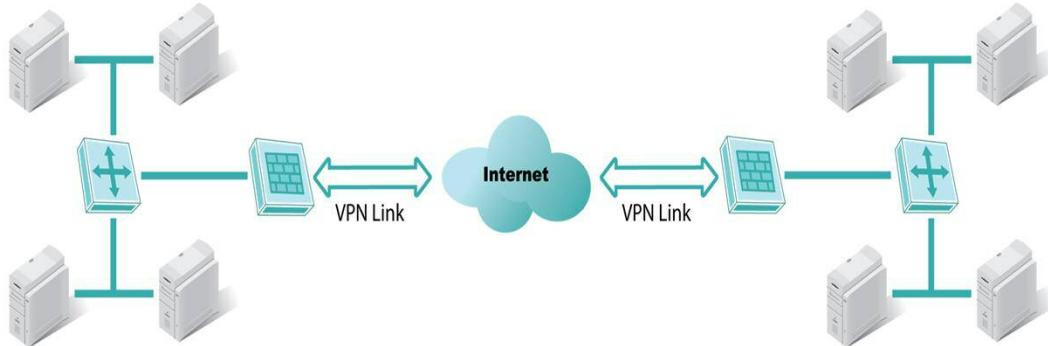
VPN to Connect a LAN with Remote Mobile Users



Let's take a moment to look at how some of the discussed architecture would look in typical implementations.

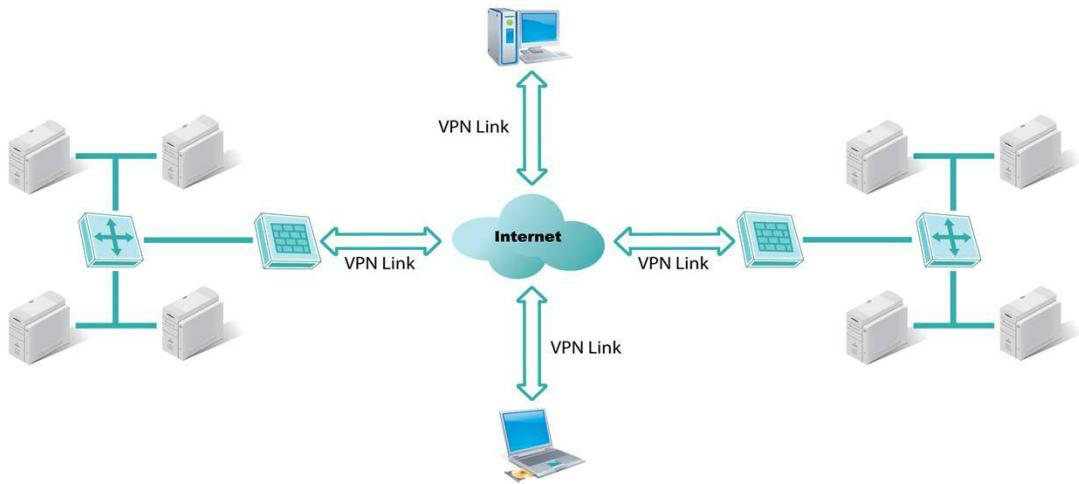
In this configuration, remote users are connecting through the internet to a private LAN. The firewall is serving as the endpoint.

VPN Used to Connect Multiple LANs



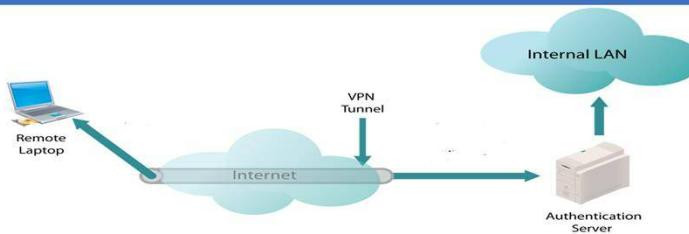
Here, a VPN is being used to bridge Local Area Networks. Corporate firewalls are shown as the endpoints.

VPN Connect Multiple LANs with Remote Mobile Users



This configuration adds remote users to the LAN to LAN VPN. What do you think could make this architecture more efficient?

VPN Encryption Modes



- Tunnel mode
 - Protects packet from header to payload
- Transport mode
 - Protects only the packet payload

We have mentioned that VPNs have two basic modes of operation. Tunnel mode and transport mode. We've also noted that endpoints can terminate at a host computer system, edge router, corp. firewall, or dedicated VPN appliance.

Let's take a closer look at these two modes.

VPN Tunnel

- Encapsulates an entire packet within another packet
- Encrypts payload and header (IP and UDP/TCP) to protect identities
- Carrier protocol used to transmit the VPN packets
- Encapsulating protocol packages the original data

VPN tunnels use encapsulation. This process encrypts the entire original packet including the header and payload. Encrypting the header protects both the destination and source addresses, but it makes the packet un-routable as it is. This original packet becomes the payload of a new packet that has a new header applied so it can make it to its destination.

VPN Tunnel

- Passenger protocol—original data payload or protocol being carried
- Encapsulates packets that are not routable through the Internet
- Routes non-routable address traffic over public infrastructure
- Ideal for gateway-to-gateway or network-to-network communication

The tunneling process requires three different protocols:

Passenger protocol The original data packet that's been encapsulated. Examples: IP, IPX, NetBEUI

Encapsulating protocol The protocol used to provide the new packet around the original data packet. Examples: IPSec, GRE, L2F, L2TP, PPTP

Carrier protocol The network protocol used to transport the final encapsulation

VPN Transport

- Encapsulates only the packet payload
- Cannot prevent some forms of observation (eavesdropping and alteration)
- Does not conceal endpoint identity
- Ideal for direct endpoint-to-endpoint or endpoint-to-gateway communication

Transport mode encapsulates only the payload of the packet. The header addressing information remains known which also allows the packet to be routed normally.

Cryptographic Protocols

- Ensure confidentiality and nonrepudiation
- Require encryption algorithms, protocols, and authentication methods
- Endpoints must support identical cryptographic protocols and methods

We keep mentioning encryption, but what is it really doing for us with regard to VPNs? First, there are multiple different cryptographic protocols that may be employed. Which specifics ones will depend on the architecture or intended use and the endpoints capabilities. Encryption is intended to provide confidentiality and non-repudiation. To do that encryption algorithms, protocols and authentication methods will be needed.

It's important to note that endpoints must support the same algorithms, protocols and authentication methods for the VPN to function.

VPN Authentication, Authorization, and Accountability

- Allow approved external entities to interconnect and interact with private network
- Use varying methods for authenticating users (passkeys, biometrics, etc.)
- Track and log user interactions to maintain user accountability

Authentication, Authorization and accountability, or the triple A of security is an essential process of validating users on a network. This is no different for users entering the network from a VPN however the exact process may be a bit different. Secure Authentication of remote users normally the use of a second factor, that is something beyond the known password and user ID. The second factor can be something the user has such as a token, passkey or certificate or something they are such as a biometric.

After authentication, the user is provided access to those resources they are authorized to use.

Activity, that is use of the assets the user has been authorized to use is tracked which provides accountability for the users actions.

VPN Supporting Services and Protocols

- Enterprise-class VPNs require enterprise-class security
- Authentication establishes levels of authorization and access
- Cryptographic transport protocols don't "play well" together

Enterprise-class VPNs require enterprise-class security. What does that mean? It means that Confidentiality is maintained by using strong cryptographic tunneling protocols which will avoid interception and sniffing. Strong authentication for non-repudiation and identity spoofing will be employed and secure cryptographic transport protocols will be used.

Authentication will be used to establish the appropriate levels of authorization and access using passwords, two-factor authentication, biometrics, and other forms.

Cryptographic transport protocols don't "play well" together, so care must be taken when selecting the different available protocols.

Internet Protocol Security (IPSec) VPNs use IPv4 and L2TP running over an IPSec layer.

Transport Layer Security (TLS/SSL) tunnels over IPv4 networks (i.e., Internet).

Platform-specific transport methods using proprietary protocol formats

This is one of the primary reasons that endpoints must have similar configurations and capabilities to make VPN work.

End of Lecture 2



of Lecture 2

19

This ends Lecture 2 of Unit 8. We will continue to look at VPNs in Lecture 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

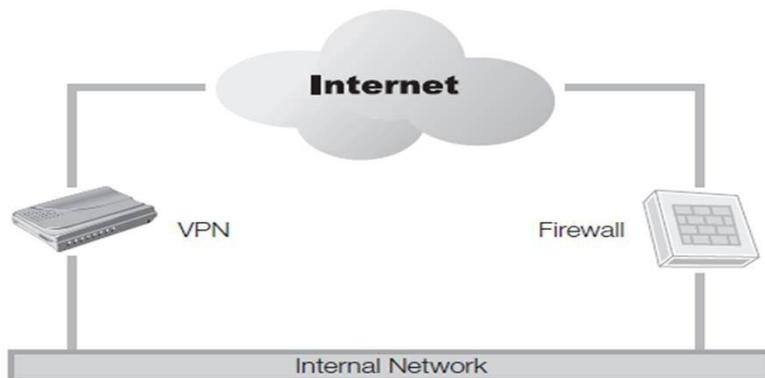
Unit 8

VPN Fundamentals

Lecture 3

Welcome to Lecture 3 of Unit 8

Types of VPN Implementations

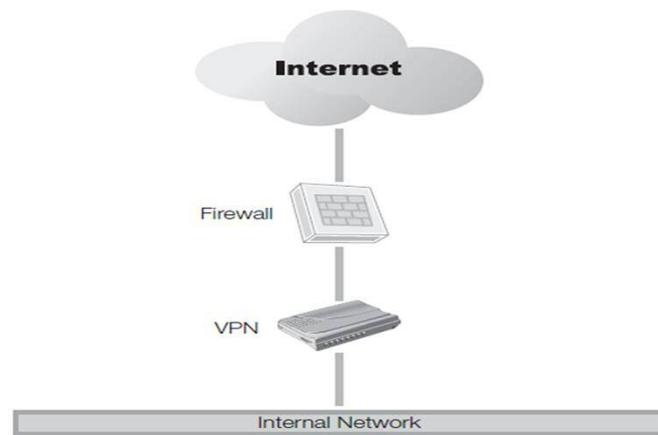


Bypass VPN

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In a bypass VPN configuration, the VPN acts as a gateway which bypasses the firewall. This typically requires the use of a dedicated VPN device. The advantage is that the firewall does not have to manage this traffic if in fact it is capable of doing so. The real disadvantage is that the traffic is not filtered by the firewall. Traffic coming through the VPN must be trusted.

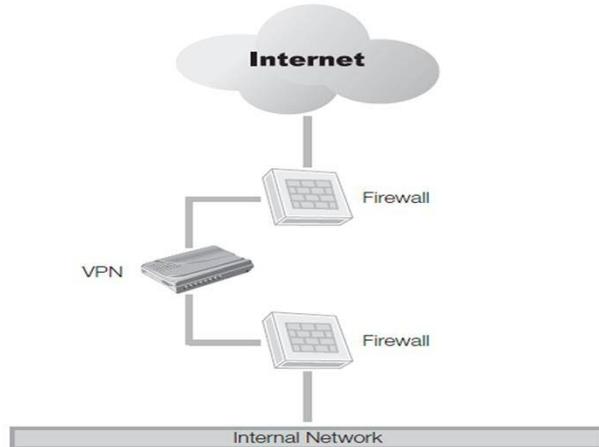
Types of VPN Implementations



Internally Connected VPN

An internally connected VPN passes traffic through the perimeter firewall. In most cases, the firewall is not able to inspect the traffic as it is encrypted. This may present a security risk that should be addressed through other mechanisms.

Types of VPN Implementations

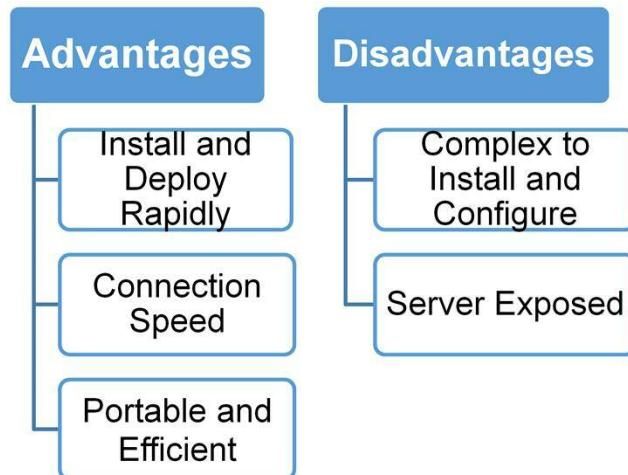


A VPN in a DMZ

Placing the VPN gateway in a DMZ is a good choice for access provided to trusted third party vendors. The decrypted traffic must traverse the second firewall which allows application of the rules before the traffic hits the trusted network.

Software-Based VPNs

Platform-independent SSL/TLS VPNs to connect systems



We mentioned earlier in this unit that VPNs may be appliance or hardware based or software based.

Software based implementations have the following advantages:

Browser-based VPN clients install and deploy rapidly.

Establish quick VPN connections using client-server software

Are lightweight, portable, cross-platform, and inexpensive

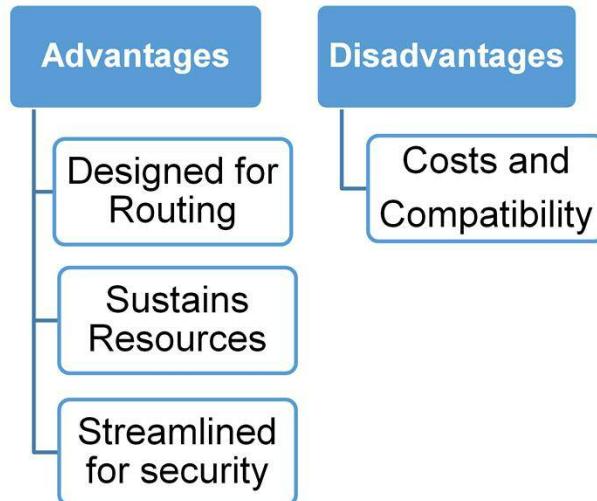
They also have the following Disadvantages:

Open source client software can be complex to install and configure.

The Server must be exposed to the public network to make connections.

Hardware-Based VPNs

Dedicated Resources and Optimized Processing



For hardware based VPNs, the Advantages are:

VPN appliances and supportive corporate firewalls are designed for routing.

Dedicated services never borrow from general processing resources.

Devices are streamlined for high-throughput secure network delivery.

The primary Disadvantage is that they are more expensive and exclusive to compatible VPN termination points. This can limit the availability to third parties.

Owned and Outsourced VPNs

- Own or operate telecommunications infrastructure and VPN endpoints
- Contract maintenance or management

As you consider your VPN implementation options, you should consider the extent to which you want to be involved with the ownership and operation of the VPN systems. There are a number of options here from full ownership of the end to end solution to completely outsourcing the solution. Which of the many options you select will depend on your risk appetite as well as your budget. As part of that decision making process, you may wish to consider outsourcing some portion of the maintenance and/or management of the system. Designing and maintaining contracts for this can also require ongoing effort that should be taken into account.

Developing a VPN Policy

- Restrict remote access to the organization's VPN solution.
- Prohibit split tunneling.
- Define classes of employee that can access the network by VPN.
- Define types of VPN connections to permit.

A VPN solution without a solid policy behind it is a liability that can become a serious security risk to your organization. It is vital to have a policy developed PRIOR to deciding on a solution and implementing it. Here are some of the things you should consider for inclusion in the policy.

Developing a VPN Policy

- Define authentication methods permitted.
- Prohibit sharing of VPN credentials.
- List configuration requirements for remote hosts, including current virus protection, anti-malware, host-based intrusion detection system (HIDS), and a personal firewall.

Not all the policy will reference technical requirements. Some of the softer issues to address are which authentication methods should be used. Prohibiting the sharing of credentials. And ensuring that the endpoints adhere to corporate policies including anti-virus/anti-malware, host based intrusion detection and a host based firewall for example.

Developing a VPN Policy (Cont.)

- Prohibit the use of non-company equipment or, if personal systems may connect to the VPN, define the minimum standards for those connections.
- Define required encryption levels for VPN connections.
- If you will be using your VPN for network-to-network connections, define approval process and criteria for establishing a network-to-network connection.

Many corporate environments will choose to prohibit the use of personal devices unless they can ensure those devices meet the security policy required by the corporation. Policies may require specific types and strength of encryption algorithms.

If network to network connections are to be implemented, then a robust approval process should be follow. This is due to the high risk exposure created when connecting two LANs together.

VPN Troubleshooting

- Identify the symptoms
- Determine the scope of the problem
- Look for changes
- Call the vendor
- Try the most likely solution
- Test it
- Check to see if you broke anything else
- Document, document, document

VPNs are not bullet-proof. They can and most likely will develop problems. To troubleshoot, you will need to be able to identify and describe the symptoms of the issue. You will need to determine the scope of the problem. Is it limited to one individual or a group? Does it affect every user?

Look for changes that have recently taken place. Is it possible that a change has affected the VPN system?

If you own the VPM system, you may need to call the vendor for help. Work with them to try likely solutions.

If the fix requires a patch or change in the configuration, be sure to test it to ensure you didn't break something else.

Lastly, document what happened and what you did to fix it. It may happen again!

Types of Virtualization

Desktop

- Separates PC desktop environment from physical desktop machine using a client/server model of computing
- Can complicate VPN troubleshooting

SSL VPN

- Separates physical and logical sides of VPN
- Greater flexibility, delegation of management, added security in multigroup environment

Before we get to the unit summary, let's touch on two types of virtualization used in VPNs.

Desktop virtualization uses a client/server model to separate the physical desktop machine from the logical desktop environment. While this provides good security when accessing the corporate VPN environment, it does create a complicated environment that can be difficult to troubleshoot.

Utilizing an SSL/TLS based VPN also provides some separation from the physical and logical sides, but has the benefit of added security in multi-group environments, greater flexibility and delegation of management.

Summary

- Strategies for protection of remote network access using a virtual private network (VPN)
- Network architecture necessary for VPN implementation
- Types of VPN solutions and common protocols used for connectivity and data transport
- Planning and selection of VPN options for best value to the organization

To summarize, in this unit we have taken a closer look at Virtual Private Networks. We have examined the use of VPN as a strategy for providing secure remote access. We have seen how VPNs can be used to bridge LANs. We have looked at multiple LAN architectures and operating modes and started developing the skills needed to define those solutions that would work best in different common environments. We have also looked at security and cost considerations in selecting the solutions that would best meet specific business needs.

End of Lecture 3



of Lecture 3

14

This ends Lecture 3 of Unit 8.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 9

Network Security

Implementation Strategies

Lecture 1

Welcome to Lecture 1 of Unit 9

Key Concepts

- Why layered security strategies help mitigate risks, threats, and vulnerabilities
- Layering security to provide enhanced security for enterprise network resources
- Practices for hardening systems and networks against an attack
- Security concerns for local, remote, and mobile hosts

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this first lecture of Unit 9 we will begin looking at security strategies. We will be discussing the different approaches to providing security for our networks and the devices that make up our networks.

We will discuss at best practices for hardening networks and network devices and endpoints.

We will explain the security concerns that exist for our local, remote and mobile hosts.

Learning Objective

- Describe network security implementation strategies.
- Explain the roles each strategy each can play within the security life cycle
- Describe the importance of endpoint protection

Our learning objectives for this unit are to describe some of the common network security implementation strategies and explain how those different strategies can impact the security life cycle.

Layered Security

Security Policy

Firewall

IDS/IPS

Vulnerability Assessments

Antivirus

Network

One of the best practices to achieve our security goals of confidentiality, integrity and accessibility, is to employ layered security. In this depiction, the layers consist of administrative and technical controls both detective and preventative. All are governed by the security policy, an administrative control. All controls in the layers under the security policy should implement or support some element of the security policy.

The firewall is normally our first line of defense in support of the policy. The rules we establish to restrict the flow of traffic should be a direct reflection of the security policy. The Intrusion detection and prevention system acts as both a detective and preventative control depending on how it is configured. The IDS/IPS inspects traffic that has passed the initial firewall rules.

Vulnerability assessments are another administrative control used to identify weaknesses in our network and systems which require resolution. Anti-virus and anti-malware typically provide host-based protection against malicious content that has made it into our network. It is the networks itself that is at the heart of our protection scheme.

Layered Security in Action

- Known Exploit Targets Your Web Server
 - Firewall—configured to allow Web traffic
 - IDS—detects the exploit
 - Vulnerability assessment—informs no action is needed because server is not vulnerable
- A Zero-Day Virus E-mailed to a User
 - Firewall—configured to allow E-mail
 - IDS—does not have signature for new virus
 - Antivirus—Heuristic engine identifies possible virus-like activity

Looking at this slide, we can trace the actions for a couple of common scenarios and how layered defenses might manage the situations.

First, is where an active attempt to attack a server on your network through a known exploit takes place. The traffic did not violate any firewall rules and was passed. The IDS detected the exploit and generated an alert. A review of the most recent vulnerability scan shows that the server under attack is not vulnerable so the attack will not be successful.

In the second scenario, a 0-day virus is emailed to someone on your network. The firewall is configured to allow mail traffic so the message goes through. The IDS doesn't have a matching signature, so the virus is not recognized and no alert is generated. The virus once executed on the host exhibits behavior similar to other viruses and the heuristics engine sees a potential threat and quarantines the code protecting the system from being exploited.

Concentric Castles

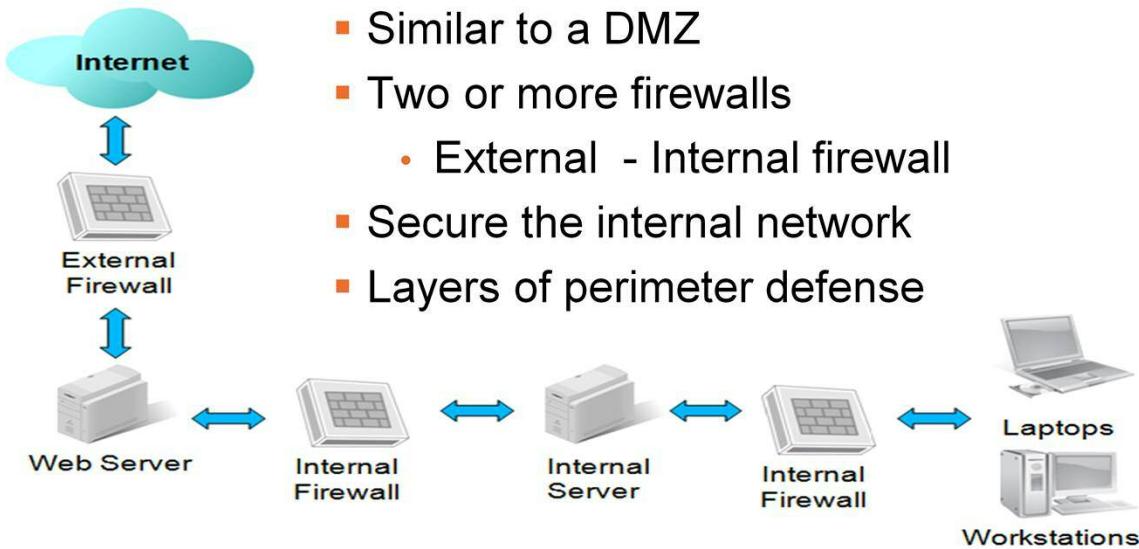
- Superior defense
- Two or more perimeter walls
 - Outer wall
 - Inner wall
- Collapsible defense
- Secure the keep
- Focus on perimeter security



Layered security as shown in the scenarios we just walked through is far superior to a single barrier type defense. The techniques developed of centuries of battles. Consider the castle. Originally, there was a single perimeter was designed protect the occupants and their goods. Advances in weaponry and tactics meant that any breach in the perimeter would likely be fatal.

Consequently a second perimeter was created. A wall within a wall. If the first wall was breached. Then the occupants could fall back to the second one and remount their defense of the keep. The focus here was on perimeter defense for at this time all attack was ground based. Good solid walls with well guarded limited access was the order of the day.

Network Security Application



In one respect, the two tiered castle system is like the Demilitarized zones we employ today. Instead of two walls, we use two or more firewalls, an External firewall and an Internal firewall are normally implemented. The intent is to secure the internal network by providing layers of perimeter defense. Additional firewalls can be added to cordon off sensitive areas and add additional layers of security and control.

Improving Concentric Castles

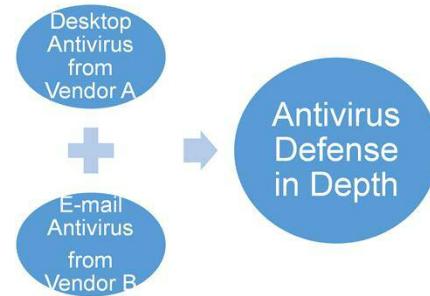
1. Relied upon walls as barriers to entry
 - Add additional barriers
 - Moats
2. Add additional defenses
 - Ranged defense
 - Archers
 - Vats of hot oil
 - Melee defense
 - Knights
 - Swordsmen



In our logical environments we can also add additional layers of defenses. At the network level we can add IDP/IPS, Data Loss Prevention (DLP) and security monitoring such as fire eye. On the end points we can install anti-virus and anti-malware programs, personal firewalls, as well as preventing modification of the endpoints my non-administrative personnel.

Building Upon Layered Security

- Layered only provides breadth
- Depth=overlapping countermeasures at each layer
- Can be from multiple vendors
 - If one is good two must be better
 - Different AV patterns=higher chance for detection



Layering defenses provide breadth of coverage, but ideally we want depth too. As an example, consider anti-virus software. From a support perspective, we prefer to stick with one vendor. In reality however, this presents a risk. Like a single walled castle, any breach of the vendors defenses opens our entire environment. A better approach is to use multiple vendors where possible. This increases the work factor needed by the attacker, slows them down and increases the potential for them to be discovered.

The Bigger Picture

Firewall

External Firewall from Vendor A

Internal Firewall from Vendor B

Antivirus

Server AV

Desktop AV

IDS/IPS

Network IDS

Host IPS

The same may be said for the hardware we deploy. Mixing it up makes it harder on the attacker. Our hope is that it will be difficult enough to either cause them to go elsewhere or stumble long enough that we can discover them. Of course having a diverse hardware environment increases the need to maintain them as well. Ensuring that patches are identified and applied will take a bit more effort, but the improvement in the overall security posture will make it worth while.

Public Addresses

- Finite number of addresses available
- Issued by Internet Assigned Numbers Authority (IANA)
- Controlled at the regional level by Regional Registry Entry
- Direct communication with the Internet
- Required for Internet-facing applications

The makers of the Ethernet addressing scheme did not anticipate just how quickly or how large the internet would grow nor did they anticipate how many devices would be connected. With a 32 bit address space, IPv4 only has **4,294,967,296** addresses. IPv4 is still the dominate protocol in use however due to the rapid exhaustion of IPv4 addresses IPv6 was developed and is ready to deploy. The problem is much of the equipment used to route and switch traffic today was built for IPv4 and cannot handle IPv6.

Regardless, the IANA assigns IP addresses and the addresses have become a scarce commodity. Almost all businesses with public facing (internet) presence require an IP address from the IANA or through a regional reseller.

Private Addresses

- Reserved IP space
 - Class A: 10.0.0.1 - 10.255.255.255
 - Class B: 172.16.0.0 - 172.31.255.255
 - Class C: 192.168.0.0 - 192.168.255.255
- Can be reused on internal networks
- Isolated from Internet
- Need to use network address translation (NAT) to communicate with Internet

When the IP address scheme was established, there were three ranges that were set aside for use inside organizations. These were defined in RFP1918. Routing equipment used to support the internet infrastructure does not route these addresses so they are called non-routable. In reality, they just won't move through the internet, but will just fine through your organizations routers.

Because there is a consistent need to communicate from within private LANs to and through the internet, a mechanism was needed to convert these un-routable addresses to ones that can traverse the internet. That process is called Network Address Translation or NAT. Natting, the process of translating is typically handled by the perimeter firewall. As an internal packet destined to an outside address is received, the firewall replaces the internal address with its external address and a port number as a unique identifier. It also creates a table so it can keep track of the session and return responses it receives back to the internal address. This allows efficient use of a single external IP address and protects and isolates the internal addressing scheme from external view.

Static Addressing

- Each system is configured with an address
- IP addresses managed at the device level
- Each system is guaranteed the same address
- Making changes can be cumbersome

Static addresses are assigned at the device level. Systems are manually configured with an IP address. A central authority does not exist. This is a time intensive manual process and is not used except in special circumstances. Changes can be time consuming and can create potential errors.

Dynamic Addressing

- Dynamic Host Control Protocol (DHCP)
- Requests IP address from centralized system
- Addresses leased for a set period of time
- Systems may acquire different addresses.
- Reservations for the same address can be made
- Addressing centrally controlled
- An attacker may be able to “borrow” an address

Dynamic addresses are assigned dynamically from a central system. DHCP is the process used to assign IP addresses dynamically. IP addresses are ‘leased’ based on how the administrator configures the DHCP server. Leases prevent churning of the address space and make for a more efficient routing environment. Depending on the configuration of the DHCP server, address spaces can be purposed in blocks to allow long term leases for equipment that doesn’t change often. Other block could be assigned to short term leases for a guest network for example where equipment changes frequently.

DHCP will be discussed in greater detail in our text and in later units.

End of Lecture 1



of Lecture 1

15

This ends Lecture 1 of Unit 9. We will continue in Lecture 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 9

Network Security

Implementation Strategies

Lecture 2

Welcome to Lecture 1 of Unit 9

Network Security

- Addressing
 - Private/Public
 - Static/Dynamic
- Topology
 - Ring, Bus, Star, Line, Tree, Full Mesh, Partial Mesh
- Protocols
- Communication
 - Outbound
 - Inbound
- Redundancy

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In the last lecture we covered addressing looking at private and public addresses. We also looked briefly at static and dynamic assignment of addresses. In earlier units we have examined some of the different topologies such as Rings, Star, Bus, Line Tree, and Meshes that have been used in the past along with some that continue to this day. We have also looked at a number of protocols and protocol families. We reviewed inbound and outbound communications and the Ingress and Egress rules that firewalls use to control them. We haven't spent much time on redundancy, but it's coming up.

All of these topics contribute to network security. In this second lecture of Unit 9, we will look at some additional topic needed to secure our networking environment.

Network Security: Key Components

- Primary objectives: confidentiality, integrity, availability
- Security policy
- Layered security + defense-in-depth
- Network design: protocols, topologies, addressing, and communication
- Equipment selection

Let's begin this lecture by a quick review.

Recall that the goal of security is to provide confidentiality, integrity and availability. At the highest level, it is the security policy that characterizes an organization's specific security requirements. We've seen that layered security and defense-in-depth provide our best chance of meeting our goals. We have also begun our investigation of topologies and how protocols are used to support our network designs.

As we have looked at the different types of equipment such as firewalls, and IDS/IPS devices we've seen that our choices can impact our security posture.

Network Security: Key Components

- System hardening
- Authentication, authorization, and accounting
- Encryption
- Redundancy
- Endpoint security

We have discussed the importance of system hardening, especially for bastions hosts. We have also noted that the triple A of security, authentication, authorization and accounting plays an important role in using VPNs as well as within our trusted networks.

Redundancy and endpoint security were touched on briefly and will be explored in greater detail as we go through the unit.

Physical Security

- Physical access bypasses many other controls.
- Critical devices should be stored in an isolated data center.
 - Multifactor physical authentication
 - Limit staff with access

With all the focus on data, communications and logical controls, it's easy to forget about physical security. This is often a grave error. Physical security can bypass almost all other security controls. A careless regard for physical security has resulted in some major headlines with millions or records lost or exposed. Frequently this is the result of the theft of laptops and other mobile devices, but other losses occur as well.

Devices that store our critical data should always be secured physically as well as logically. Data centers are of special concern because they contain large concentrations of assets as well as data. We should be very restrictive about who can gain access and under what circumstances. Just as we employ multifactor authentication for access to our sensitive data, multifactor authentication as well as logging of physical activities should be part of our security efforts.

Physical Security

- Fire suppression
- CCTV cameras where appropriate
- Compensating controls for mobile devices
 - Encryption
 - Anti-theft tracking software

Physical security involves much more than keeping the door locked. Failure to address environmental needs like fire suppression, Air conditioning, power conditioning and resilient communications channels can have even more disastrous effects than a data loss.

When working in the physical world of servers, routers and firewall, care should be taken to monitor even our trusted employees. Just as we log behaviors and access on our networks, we should employ video and other detective controls in our sensitive areas. This is important enough to be mandated by some of the compliance requirements many businesses must meet.

When working with mobile devices, encryption and anti-theft tracking software should be the norm, not the exception.

Administrative Controls

- Corporate objectives
- Policies
- Procedures
- Standards
- Guidelines
- Training
- Awareness

We've talked about a number of technical and logical controls, but I'd like to spend a little more time on administrative controls. Like physical controls, people tend to under estimate the importance of administrative controls. Administrative controls are the foundation that our technical and logical controls are built upon. They generally consist of the policies, procedures, standards and guidelines, but also include train, awareness, hiring and termination practices and more. Security policies should always support the corporate goals and objectives in order to be seen as facilitating those business goal rather than being an impediment.

Authentication

- Verification of identity
- Drivers license
- User name/password
 - Most common
 - Weakness of passwords
- Multifactor
 - Something you know (password/pin)
 - Something you have (security token/ATM card)
 - Something you are/do (biometrics/behavioral based)

One of the administrative controls that crosses the lines into the technical and logical is authentication. Authentication is the process of verification of identity. An example from our daily lives would be a drivers license. It is an official document that was issued by the State after you proved your identity with a birth certificate or other documents.

Our logical identity is usually confirmed with a User name and password. This traditional means of identity is weak on several fronts, but passwords tend to be the weakest point. Passwords we create tend to be easy to remember which usually translates to short, common words, names birthdates or other easily guessed strings of characters.

I'd like to introduce the concept of factors into the discussion on identity and authentication. Usernames and passwords fall into the category of 'Something you Know', but there are several other factors that can be used as well. These are:

Something you have (security token/ATM card)

Something you are/do (biometrics/behavioral based)

Combining more than one factor provides a much stronger indication of identity validation than a single factor even if that single factor is used multiple times. Three

user IDs and five different strong passwords is still a single factor and not considered strong at all. Multifactor identification or authentication is considered strong and should be used to access sensitive areas or any area remotely. An example is the use of a card key or HID device and a pin number. This is something you know, the pin number and something you have, the card key.

Authorization

- Concerned with what one has access to do
- Least privileges
 - Access to what one needs to complete job
- Typically occurs after authentication
- Example: purchasing beer
 - Clerk checks ID verifies picture match (authentication)
 - Checks DOB to see if > 21 (authorization)

Authorization is about privileges, in other words, who is allowed to do what. The normal best practice is to operate with the principle of least privilege. What that means is that a person has the privileges necessary to do their job, but nothing more. This is especially true with regard to access to sensitive information or access to sensitive devices. Most people don't need that type of access to do their jobs and consequently should be restricted from those environments.

Authorization normally takes place after authentication as privileges are associated with an identity. The example here is purchasing beer. To buy, the individual must show proof of their age, usually in the form of an ID such as a drivers license. The clerk checks the birthdate and if the individual is over the required age, then the sale is allowed.

Accounting

- Logging
 - All attempts failed and successful
 - Who, what, when
- Auditing
 - Checking for compliance to ensure appropriate access
- Monitoring
 - Looking for violations
 - Checking for unauthorized access

Accounting, the third A, may have multiple components. Logging is the process of recording access and events. For example, if a person accesses a database that contains sensitive data, a log entry would be created. That entry should show who (what ID) accessed what object, when (the exact time and date), what occurred (i.e. was something added, deleted or changed) and what was the outcome, (was it successful or did the attempt fail). Logs can of immense value after the fact and provide one of the primary sources of forensic evidence.

Auditing may have several facets. One of the uses of audit is to periodically evaluate and confirm that the access privileges assigned to individuals are still appropriate. This may be accomplished by having responsible managers review the access rights their employees have and adjust them accordingly. Several of the compliance and regulatory requirements have this as a required element.

Monitoring is more proactive or perhaps one should say more real time. Devices and agents placed strategically in the network can trigger alerts based on established rules that support the security policy. An example would be attempts to access objects or files to which the individual does not have authorization. Monitoring does not have to be focused on the employees or human element. Monitoring can also ensure that system maintain their integrity and do not make unexpected connections or changes.

Encryption

- Data at rest
 - File encryption
 - Database encryption
 - Disk encryption
- Data in transit
 - Ensures integrity, confidentiality, and privacy
 - Nonrepudiation
 - Encrypted tunnel: IPSec and SSL/TLS

Encryption is a major tool used to maintain Confidentiality and Integrity when data is at rest or in transit. Unlike other security areas there are no direct availability implications. Encryption can be used to secure data at rest using one of several different modes such as file encryption, which encrypts only specific files, Database encryption which may encrypt specific rows or columns or an entire database and disk encryption which encrypts the entire disk including all the files it contains. Encryption is frequently a compliance requirement to protect sensitive data such as Payment card data, health records, etc. To be effective encryption must be managed well. That means selecting an appropriate algorithm, key strength and method of managing keys.

Data in transit is also data which should be protected. Encryption can provide integrity, confidentiality and privacy. In some situations, encryption may also provide nonrepudiation. Typical examples of using encrypted transport are IP Security (IPSec) and Secure Socket Layer or Transport Layer Security (SSL/TLS).

Endpoint/Node Security

- A node is any device on the network; an endpoint does have an IP address
- Different types of nodes require different types of security
- Security of individual devices creates greater network security

In an earlier unit we defined a node as any device on the network. An endpoint is a device or node that has an IP address. Most endpoints can usually send and receive packets. Depending on the type of endpoint, there are different levels of security that should be applied. Applying security controls to endpoints is one of the layers in achieving defense in depth. An exploited endpoint on a network can affect the security of the entire network and all the devices that share it.

Endpoint/Node Security

- Roles involved in node security
 - End-Users: acceptable use, security awareness
 - System Admin: responsible for implementation
 - Network Admin: responsible for networking devices
 - Physical Security Staff: responsible for physical controls

There are a number of roles within the organization that participate in achieving node security. These include the end user, system administrators, network administrators, and those responsible for physical security. All must do their part, and do it successfully in order to achieve and maintain end point security.

Endpoint/Node Security Concerns

- **Clients**
 - Antivirus scanner
 - Firewall
 - Screen lockout
 - Physical lock
- **Server**
 - Redundancy
 - Strong authentication
 - Physical isolation

Some of the areas that should be addressed are based on the type of endpoints. Clients systems such as desktop or laptop computers for example should install and maintain anti-virus software and personal firewalls. They should employ a screen lockout that requires re-authentication to unlock and use the system. Physically attaching the system to the desk is also a good idea to keep them from ‘walking off’.

Servers may also have anti-virus and anti malware software installed as well as file integrity monitoring software. Redundancy should be employed for servers that perform critical functions where any interruption would significantly impact the business. Servers should also have strong authentication requirements to ensure only those authorized to access them may do so. Servers should also physically secured. This means placing them in a protected environment with strong physical controls and appropriate environmental controls.

Endpoint/Node Security Concerns

- Networking Devices (routers and switches)
 - Strong authentication
 - Accounting
 - Physical isolation

Like servers, networking devices should be protected logically with strong access controls using strong authentication. Logging and accounting is critical for these devices. Physical isolation is also very important to prevent tampering, theft or additions of rogue devices that could monitor traffic.

Summary

- Why layered security strategies help mitigate risks, threats, and vulnerabilities
- Layering security to provide enhanced security for enterprise network resources
- Practices for hardening systems and networks against an attack
- Security concerns for local, remote, and mobile hosts

So, in summary, we have discussed the importance of layered security to help mitigate the risks in our network environment. We have discussed the need to protect our network and end point devices with enhanced security to achieve defense in depth. We have also looked at some of the issues associated with local, remote and mobile hosts.

End of Lecture 2



of Lecture 2

17

This ends Lecture 2 of Unit 9.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 10

Firewall and VPN Implementation and Management

Lecture 1

Welcome to Lecture 1 of Unit 10

Key Concepts

- Best practices for management of enterprise and personal firewalls
- Security appliances that work with firewalls
- Best practices for management of VPN connectivity
- Risks in using remote access technologies in the context of an enterprise

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this unit we will be exploring best practices for implementing firewalls. We will take another look at different security appliances that work with firewalls . We will also look at best practices for the management of both firewalls and VPNs and how good management practices can reduce risks associated with remote access.

Learning Objective

Appraise the elements of firewall and VPN implementation and management

Firewall Management Best Practices

- Create a written firewall policy
- Evaluate potential and known threats
- Confirm that the existing firewall policy and setup is sufficient or correct based on known threats
- Maintain physical security control over all access to firewalls

Good security starts with well defined and written policies. Policies establish a documentation trail that everyone in the organization can read, consider, and follow. To have a good security policy, you must thoroughly understand your organization's infrastructure, its mission and goals, and the processes necessary to produce its products and services. With a well designed policy you can create a security plan that implements the policy.

Like the security policy, in order to have a great firewall, you will need to understand and organizations security policy, the technical environment and the goals and mission as well. The firewall policy should support the corporate goals and guide the implementation of the firewalls in the network. These implementations in turn should be documented in a procedures and guidelines.

To be successful, security policies and firewall policies need to be aware of and consider the threat environment to ensure they can address the known and predicted threats. Evaluating the changing threatscape along with system vulnerabilities needs to be an ongoing process that drives needed changes in the firewall documentation and implementation. And this includes physical threats as well. Firewalls require strong physical protection.

Firewall Management Best Practices

- Limit and filter Internet connectivity
- Filter systems attached to the network
- Don't forget internal firewall deployments
- Make sure its working

In all environments that connect to the internet, care must be taken to limit and filter internet traffic to only that which is required for your business. The firewall policy should stipulate that every border communication point should have a firewall.

The firewall policy should require that every host should have a local software firewall where feasible. Systems connected to the network are vulnerable to both malicious code (Trojans, viruses, worms, etc.) and malicious traffic (spam, phishing attacks, etc.) and should have adequate filters.

Internally, the policy should require every transition between subnets of different trust, risk, or purpose have a firewall.

Confirm, after evaluating potential and known threats, that the existing firewall policy and setup is sufficient or correct.

Firewall Management Best Practices

- Defense in depth—layer defenses along pathways of communication and transitions
- Use Internet Protocol Security (IPSec) to secure all *intranet* communications
- Harden internal and border firewalls
- Default Deny is better than Default Permit
- Monitor logs for signs of breach attempts

Practice Defense in depth. Layer defenses along pathways of communication and transaction points.

Don't forget your internal connections. Use IPSec to secure connections between networks and also remote users.

Harden all your systems. Remove unneeded services, protocols and daemons. Remove unnecessary software and keep up with your patching. Establish strong passwords. Close unneeded ports. And change all default settings where possible.

Use default deny rather than default permit. Always place your explicit denies at the top of your rules, followed by your explicit allows and ALWAYS end with an explicit deny any any.

Never assume everything is working as expected. Monitor your logs to see what is being blocked and what is getting through.

Firewall Management Best Practices

- Create an intrusion and incident response plan
- Create business continuity and disaster recovery plans
- Prioritize securing against the largest threats first
 - Probability, Frequency and Consequence
- Develop and periodically confirm your firewall checklist
- Periodically reassess your security assumptions against current evolving guidelines

A firewall policy is only one of many policies, procedures, standards and guidelines that need to be in place. As you monitor your logs or IDS/IPS devices, you may see an active attack. How will you respond? Your response should have been laid out in an incident response plan. Never wait until you must respond to an incident to develop a plan. Do it in advance. The same is true of a business continuity and disaster recovery plan. Plan in advance. Even a plan with poor predictions as to what can go wrong is better than no plan.

Prioritize your security efforts to protect against those threats that are most likely to occur and have the largest impact. There won't be enough resources to provide protection against every possible event, so you will need to pick your battles. Consider the probability or likelihood of an occurrence, the frequency of occurrences and the probable impact.

Periodically check your firewall implementation to ensure it continues to address the changing threat environment as well as the changes to your network. Also, periodically review and test your incident response and business continuity and disaster recovery plans at least annually.

Firewall Management Best Practices

- Perform internal compliance audits periodically
- Use an ethical hacking team to attempt penetration of the network

There are always new lessons to be learned
and new challenges to be met –
keep educating yourself!

Check your compliance requirements and make sure you are compliant before an auditor shows up. Speaking of audits, most compliance mandates require penetration testing to ensure your controls have been implemented properly and are providing the desired security. Periodically engaging an external company to perform penetration testing is a good way to evaluate your work and meet the necessary compliance requirements. Remember when negotiating penetration tests to include both external and internal tests as well as re-tests after any required remediation.

That's a lot of best practices to absorb and there are doubtless more. The security environment is ever changing. Adversaries are smart, motivated and often well financed. They have the time and resources to nibble away at our defenses. We must keep on top of changes to ensure we continue to provide the security to the networks and systems we are asked to protect.

To be successful in security you must constantly challenge yourself and never stop learning.

Security Measures in Addition to a Firewall

- Authentication
- Encryption
- Logging and auditing
- Network segmentation and traffic control
- Network access control
- Virtual private networks for remote access

Choosing a Firewall

- Speed, flexibility, and simplicity
- Real-time applications and bandwidth
- Strong authentication
- Detailed logging
- Customized unique/complicated filtering
- Major threats: internal vs. external

We've talked about the policy foundations of security and firewalls. We've noted that what and how we implement our solutions will depend on those foundations along with the threat environment we've identified. So how do we select the right firewall? Unfortunately that is not an easy answer. Every environment is different as is every implementation. We haven't even mentioned the cost constraints that may also be present. Here are some additional factors that should go into your consideration for selecting a firewall or firewalls.

Firewalls are designed to manage different traffic volumes and complexity. Large organizations with significant traffic volume will need higher capacity firewalls than a very small organization with limited traffic. Large organizations will likely have staff to manage more complex firewalls too. Smaller businesses will probably have limited staff managing multiple areas of the network making relatively easy to manage firewalls a plus.

The existence of real-time applications such ecommerce necessitate higher throughput and greater flexibility.

Strong authentication and detailed logging capabilities are important for all firewalls.

Large and diverse environments may require specialized, complex filtering rules. This may limit your firewall choices to higher end devices.

Lastly, your choice of firewall depends on it's placement in your environment with some consideration of the types of threats it will be expected to prevent. Will it be internal to your network isolating sensitive areas or will it be on the perimeter facing the internet. All of these considerations will narrow your choices.

Buying vs. Building

- Off-the-shelf solutions offer ease of setup
- Off-the-shelf solutions often work out of the box requiring only to be plugged in
- Custom builds can be less expensive and provide more desired features
- Custom builds are not good when there are time sensitivities because they require a lot of a IT personnel effort

The buy versus build question is not a frequent consideration. Building your own solution is certainly possible, but it is likely to create more issues than it solves. Off the shelf solutions are more likely to provide easy to maintain solutions with fewer vulnerabilities to track and resolve. It would normally require a unique set of circumstances to make a custom firewall worth pursuing.

Firewalking

- A method for testing the vulnerability of a firewall and mapping the routers of the network
- Also a method of disguising port scans that normally are easily detected and deterred
- TCP or UDP packets are sent one hop beyond the firewall—to a known target inside the defense of the firewall
- The Time to Live (TTL) is set to exactly one hop greater than the number needed to reach the firewall

Firewalking is a technique used to map routers and test firewall vulnerabilities. The technique can be used like port scanning, but has the benefit of disguising the effort so that it is less likely to be detected. The technique uses TCP or UDP packets that are sent one hop past the firewall to a known location. The packet has a Time To Live of exactly one hop plus the number of hops needed to reach the firewall.

Firewalking

- If the packet makes it to the target, the TTL decrements to zero and elicits a “TTL exceeded in transit” message and the packet is discarded
- Very useful in determining if the probe is successful
- Firewalking produces a list of the known packet constructions that bypass the firewall and get to the target in question
- From here the potential hacker can devise future attacks

IF the packet makes it to the target, the Time To Live reaches zero, the packet is discarded and a message is returned. By constructing different packets the attacker can characterize the types of packets that get through the firewall and can reach the target. This is useful information for future attacks.

Packet Inspection

- Filtering can apply to packet content inspection. An exploit can send benign looking payload in packets at first.
- Once communication is established malicious content can be added
- Packet inspection can be defeated by fragmentation and overlapping attacks

While packet inspection is an enhanced feature for most firewalls, it is not infallible. An attacker can start with benign packets to establish a session and later switch to more malicious payloads. Fragmentation and overlap attacks may also be used to bypass packet inspection.

Packet Inspection

- Fragmentation off-set values can produce an abnormal reconstruction
- Turn benign-seeming content into a malicious attack
- Overlapping can cause full or partial overwriting
- Deploy a dynamic filtering system that does a virtual reassembly to combat this

Fragmentation off-set values can produce an abnormal reconstruction turning benign seeming content into a malicious attack

Overlapping can cause full or partial overwriting of datagram components creating new datagrams out parts of previous datagrams

To combat this deploy a dynamic filtering system that does a virtual reassembly.
Once the packet is reassembled it may be analyzed to see if it is non-malicious and then passed on.

Tunneling

- Creation of quasi-VPN tunnels is a serious network security risk
- Two types of tunnel attacks
 - Inbound attacks
 - Outbound attacks
- Exploit can convert almost any protocol at any layer of the OSI model into an encapsulation or tunneling protocol

Creation of quasi-VPN tunnels is a serious network security risk. This technique creates an encrypted channel that communicates through a port or protocol that is not blocked by the firewall because it is used for legitimate purposes.

There are two types of tunnel attacks ~ inbound and outbound

Inbound attacks require a malicious server installed inside the perimeter of a firewall that permits inbound communication.

Outbound attacks require an external server with an internal client that initiates contact and a firewall that permits outbound communication.

Exploit can convert almost any protocol at any layer of the OSI model into an encapsulation or tunneling protocol.

Defenses Against Tunneling

- Strictly enforce deny-by-default for both inbound and outbound communications
- Clearly define in the acceptable use policy (AUP) what is not authorized and deemed a risk
- Use network and host IDS/IPS monitoring
- Deploy whitelist controls to prevent the installation of unapproved software
- Limit mobile code, such as ActiveX, Java, Flash, Silverlight, and JavaScript

To prevent most tunneling attacks, it is important to strictly enforce a deny by default rule. Acceptable communications should be established in a policy and implemented through firewall rules. Adding IDS and IPS functionality to the network can help to catch and mediate unexpected traffic.

Using whitelisting and/or limiting the end user ability to install unapproved software also helps reduce the likelihood of tunneling.

Lastly restricting mobile code such as ActiveX, JAVA, Flash, etc. can help limit the introduction of potentially malicious software from establishing tunnels.

End of Lecture 1



of Lecture 1

18

This ends Lecture 1 of Unit 10. We will continue in Lecture 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 10

Firewall and VPN Implementation and Management

Lecture 2

Welcome to Lecture 2 of Unit 10

Testing Firewall Security

Simulated
firewall tests

Virtual
firewall tests

Laboratory
tests

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

There are a number of different methods used to test the effectiveness of firewalls.

Outside of the penetration testing discussed earlier, most of the testing is done in simulated or lab environments. One of the methods used for firewalls and applications as well is fuzzing.

Fuzzing tools:

- Use a brute-force technique to craft packets and other forms of input directed toward the target
- These crafted packets stress a system to determine whether it will react improperly, fail, or reveal unknown vulnerabilities.
- Fuzzing can discover coding errors, buffer overflows, race conditions, remote exploit flaws, injection weaknesses, and so on
- Fuzzing can take a significant amount of time to discover anything interesting as it must create a very wide range of inputs and evaluate their affects.

Tools for Monitoring Firewalls

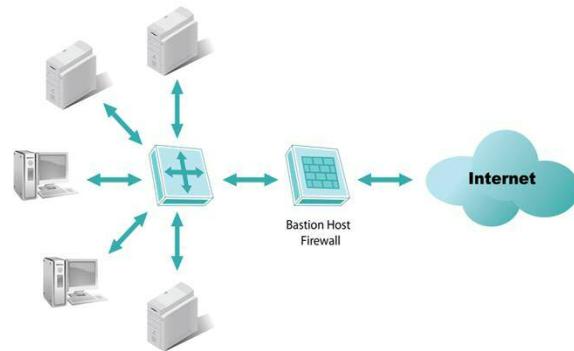
- Firewalls are incomplete security on their own
- Tools and software will be dictated by budget and threat evaluation—don't over buy or under buy
- The nature of exploits and attack methodologies can change quickly which limits the useful lifespan of any recommendation

As necessary as firewalls are to the protection of our perimeters, they are not enough. We've talked about layered defenses and defense in depth and firewalls are definitely an important element, but what else is needed to improve our security? Just like the selection of a particular firewall, the tools, software and devices will depend on the environment you wish to protect, the likely threats against that environment, any regulatory or compliance requirements that must be met and of course your budget.

It's important to choose your weapons wisely. Selecting flexible multiple use devices and tools can stretch your dollars, but it's important not to go too cheap as well. Going for the lowest cost possible will usually result in a product that lacks flexibility and growth capability. That means a short life span before it will need to be replaced with something better. Remember that the security environment is a constantly changing one. Flexible products are needed to accommodate that change as well as growth and changes in the business environment.

Tools for Monitoring Your Firewall

- Nmap (Zenmap)
- Netstat
- Tcpview
- Fport
- Snort



Still, there are a number of very useful tools that can be obtained for little or no money. Some examples are:

Nmap – a network mapper, port scanner, and OS fingerprinting tool. Can check the state of ports, identify targets, and probe services

Netstat – a simple command line tool to list the current open, listening, and connection sockets on a system

Tcpview – a GUI tool to list the current open, listening, and connection sockets on a system as well as the service/program related to each socket

Fport - a command line tool to list the current open, listening, and connection sockets on a system as well as the service/program related to each socket

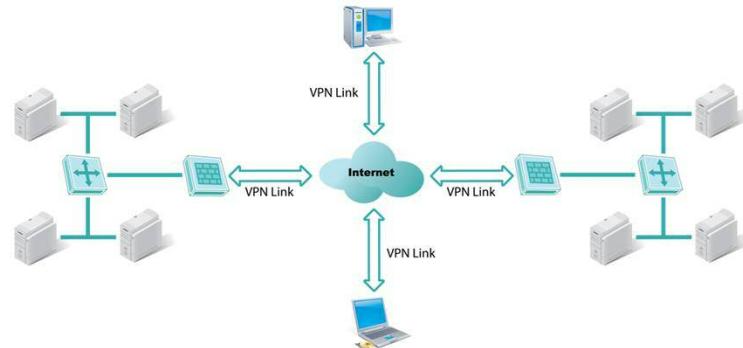
Snort – a open source rule-based IDS that can detect firewall breaches

Most of these are open source products. What that typically means is that there is no or very limited support or training. Some of these products have created cottage industries that fill that support and training gap at a cost of course. Some have also branched into free and pro paid versions that will

offer some level of support based on subscription fees. Always look at ALL of the potential costs associated with implementing free or open source software solutions.

Tools for Monitoring Your Firewall

- Nessus
- OpenVAS
- Wireshark
- Netcat
- Backtrack
- Syslog



Some additional software tools are listed here. Nessus is a widely used vulnerability scanning product that offers a limited free version and a professional paid version.

Wireshark is a free network packet sniffer you should be more familiar with now through this course.

Netcat is a tool used by both hackers and network administrators to check a firewall's effectiveness by creating covert channels which the firewall should detect and block. Cryptcat does the same but used encrypted channels.

Backtrack is a great collection of hacking tools which includes many of the open source tools used by administrators and hackers alike. It is available as a Linux distribution.

Syslog is a log collection and backup program that helps maintain backups of system logs.

Nessus – an open source vulnerability assessment engine that can scan for known vulnerabilities

Wireshark – a free packet capture/protocol analyzer/sniffer that can analyze packets/frames as they enter or leave a firewall

Netcat – a hacker tool that creates network communication links using UDP or TCP ports that support the transmission of standard

input and output. Commonly creates covert channels to control a target system remotely or bypass a firewall. Can test a firewall's ability to detect and block covert channels. Cryptcat offers similar capabilities using encryption

Backtrack – a Linux distribution that includes hundreds of security and hacking tools, including Nessus and Metasploit. Can perform attacks against or through a firewall for testing purposes

Syslog – a centralized logging service that hosts a duplicate copy of log files. Provides real-time backup of every log on every participating host

Basic Troubleshooting Tips

- Trouble involving network security demands a prompt resolution
- Be patient
- Know your firewall thoroughly
- Focus

Troubleshooting under the gun or during an actual incident requires a cool head and the ability to find prompt solutions. These two qualities are sometimes at odds. Here are some pointers that should help the situation:

Have patience – keeping your cool and taking your time will pay off by allowing you to find a solution quickly without making mistakes, overlooking essential details, or intensifying the problem further.

Know your firewall thoroughly – the more you already know about the firewall, hardware and software, the more you will know how it functions and can immediately use that knowledge to seeking out a solution.

Focus – seek to find a solution to the current most critical problem. Don't waste time fixing, repairing, upgrading, resetting, or configuring any other problem or aspect of the firewall system until you've resolved the primary problem. You can become distracted by minor details that "only take a second" to address; make a list of these smaller issues and come back to them later.

Basic Troubleshooting Tips

- Isolate the problem
- Simplify
- Try the quick-and-easy fixes first
- Avoid destructive or non-reversible solutions

Isolate the problem – whenever possible, isolate elements or components of the firewall system that are functioning correctly to narrow the range of suspects of potential problem sources.

Simplify – disable or disconnect software and hardware non-essential to the function of the firewall. This will reduce the complexity of the situation and may assist in discovering the cause.

Try the quick and easy fixes first – try the fast and easy stuff before the hard and complicated options. You might be lucky, but if not, undoing easily attempted failed solutions will be simpler than the more complex options.

Avoid destructive or non-reversible solutions until last – attempts to use an irreversible fix is a poor idea early in the troubleshooting process; only after reversible and/or safe solutions have failed should you attempt more drastic measures.

Basic Troubleshooting Tips

- Try the free options before the costly ones
- Let the problem guide and direct you
- Make fixes one at a time
- Test after each attempt
- Reverse or undo solution failures

Try the free options before the costly ones – always try to perform repairs and fixes in-house using tools and resources that you already own or can obtain for free. Hold off on purchasing new resources or hiring technical support until you've exhausted other options.

Let the problem guide and direct you – the more you understand how your firewall operates and what the problem is, the more the problem directs you toward the affected area or the source of the issue.

Make fixes one at a time – only try one fix or repair option at a time; attempting multiple fixes at once is more complex and might mask the successful resolution.

Test after each attempt – after each fix is made, test the repair to see if it was successful.

Reverse or undo solution failures – if a fix does not resolve the issue, undo it to return to the previous state. Leaving failed fixes in place may cause other problems or may intensify the main problem.

Basic Troubleshooting Tips

- Review change documentation
- Review previous troubleshooting logs
- Update the troubleshooting log
- Repeat the failure
- Perform a post-mortem review

Review change documentation – could a recent change be responsible for the unwanted activity? If so, try to undo the change to see if the problem stops.

Review previous troubleshooting logs – consider whether the current problem is the same as or similar to recent problems already in the log. Try repeating successful solutions.

Update the troubleshooting log – with every action attempted, whether successful or not. Record it into the troubleshooting log and use it as a journal. Think of something, then write it down and try the solution; write it down, then test for effectiveness; write it down, then repeat the failure fix; write it down, then repeat until resolved; write down the successful solution and make note of any other thoughts, ideas, or observations.

Repeat the failure – sometimes causing the failure to repeat can assist in identifying the cause. However, only do so when the repetition will not cause further harm or loss.

Perform post-mortem review – the most valuable result of a problem,

especially a resolved problem, is your ability to learn something from the event. Always review the entire troubleshooting response process. Look for ways to improve the response for future problems.

And of course, document all your actions, successful or not.

Documentation

- Good documentation and planning makes troubleshooting firewalls simpler
- Useful troubleshooting information
 - Complete hardware and software inventory (relative to firewalls)
 - Written and electronic copies of configuration settings
 - Firewall policy
 - Change documentation
 - Previous troubleshooting logs
 - Activity, error, and alert logs
 - Maintenance logs
 - Any information about the current problem

Having access to good documentation makes troubleshooting easier. Having for example the firewall configuration and list of changes can provide a starting point to seek the source of the problem. Don't stop at documenting the firewall. You should have a complete inventory of the devices and software in your environment along with model numbers, firmware versions and software versions.

Don't forget the logs. It's likely that the logs contain clues to what is happening as well as when it started and potentially why.

Again, document the occurrence and everything you try to fix it. Don't wait until the end because you will have forgotten many important facts.

Firewall Design and Implementation

- **Suitability:** Can the firewall implement the policy?
- **Flexibility:** Is it easily reconfigurable?
- **Training:** Is training required? What is the cost?
- **Need:** Make a list of traffic you want to allow, filter, or block (see organization's security policy).
- **Risk:** Make a separate list of all the risks in the network based on the traffic allowed.
- **Cost:** How much will everything cost?

Let's return to the design and implementation considerations for your firewall. These are examples only. Every organization's needs differ.

Remember that a firewall policy should be a reflection of the security policy which in turn supports the mission and goals of the organization. Understand what the firewall policy is and determine whether the firewall options you are considering are actually capable of implementing it.

Businesses change as does the threat environment. Is the firewall capable of being reconfigurable so it can accommodate these changes?

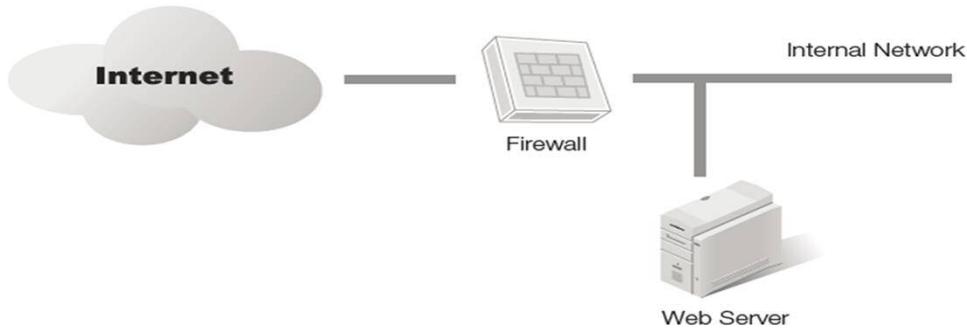
Will training be available and at what cost? On the job learning is probably not the best course for firewalls.

Know your current environment include the volume and types of traffic. Make sure the firewall can provide the filters you will need.

Know and itemize your networks risks. Look for a firewall that will address those risks and any risks you might anticipate.

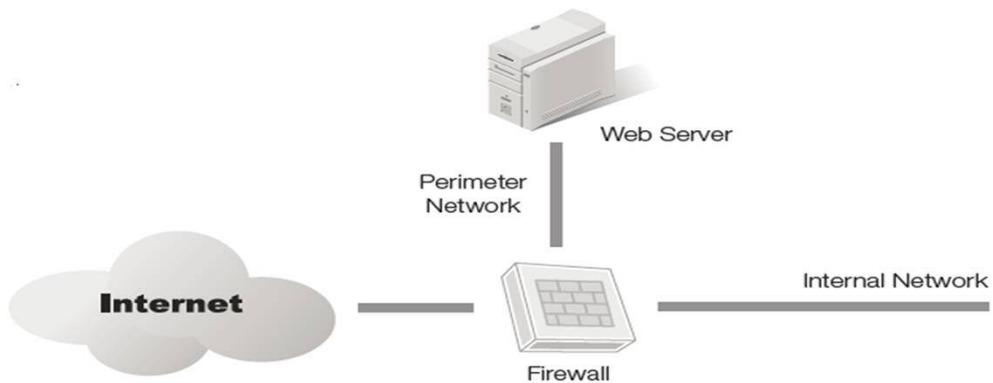
Of course, consider cost. Can you get everything you need for your available budget? What about the things you want?

Firewall Topology: Simple Solution



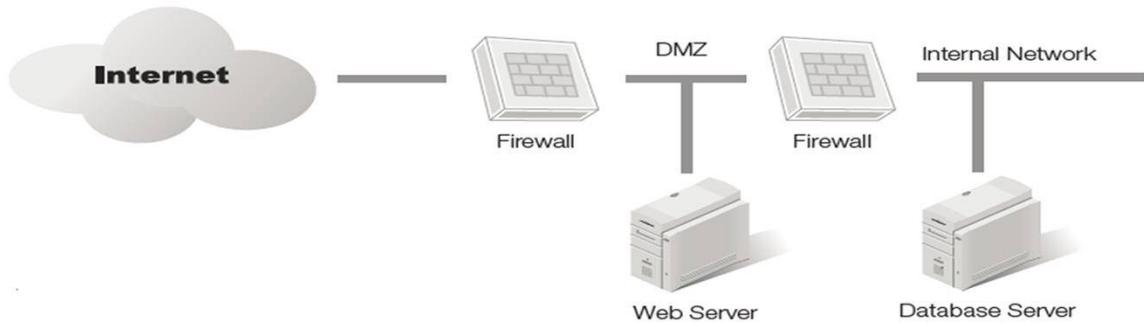
When evaluating firewalls, you should understand the topology they will be used in. Organizations differ widely in size and complexity and consequently require different solutions. This simple solution may be workable for environments that do not have sensitive data that requires additional protection. This type of design may be suitable for a small business with a static web server that provides very limited web pages to their clients.

Multi-homed Firewall for Perimeter



Using a multi-homed firewall allows more options for protecting your environment. This configuration reduces exposure to your trusted network and still provides for a web presence.

Firewall Topology: DMZ



By adding an additional firewall, you can establish a traditional demilitarized zone. This provides additional isolation and protection for your trusted internal network while being able to provide services and interaction with the internet. This type of architecture would be appropriate for some ecommerce implementations.

Appliance/Hardware Firewalls

- Dedicated hardware device specifically built and hardened to support firewall software
- Does not require additional hardware or software for deployment
- Needs network connections and a power connection
- Has dedicated hardware resources not shared with other services
- Can protect a single system or an entire network

Although it has been mentioned before, firewalls come in hardware, software and virtual forms. Each has its place. The advantage of hardware firewalls is its purposeful design and hardening. It has its own CPU and memory to improve throughput and capacity. It doesn't rely or compete with other systems. It is capable of protecting an entire network or a single system.

On the down side, they are generally more costly. They require power and a controlled environments. They should be afforded strong physical protection and need to be positioned to intercept all traffic.

Appliance/Hardware Firewall Examples

- Barracuda
- Cisco
- D-Link
- Fortinet
- Juniper Networks
- Linksys (owned by Cisco)
- NetGear
- SonicWALL
- WatchGuard
- ZyXEL

These are just some of the different brand names that produce firewalls. Many produce other products as well. All will have marketing literature available for download or viewing over the web.

Virtual Firewalls

- Includes:
 - Virtualized software firewalls provide filtering services for a standard physical network
 - Firewalls running between virtualized client and server operating systems
- Benefits: Rapid development, quick prototyping, isolation, traffic management, quick recoveries, testing

Lastly in this second lecture, I'd like to touch on virtual firewalls. A virtual firewall functions the same as its hardware or software equivalent. Rather than existing on dedicated hardware however, they normally exist on a dedicated server in the virtual environment. Virtual firewalls are easy and relatively inexpensive to deploy making them ideal for prototyping, isolation, traffic management and testing.

End of Lecture 2



of Lecture 2

18

This ends Lecture 2 of Unit 10. We will continue in Lecture 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 10

Firewall and VPN Implementation and Management

Lecture 3

Welcome to Lecture 3 of Unit 10. In this lecture we will return to our discussion of VPNs.

VPN Implementation Choices

- A VPN can be implemented as software on the host and gateway
- A VPN can be implemented as a hardware appliance
- Both have advantages and disadvantages
- Both offer cost savings and scalability

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

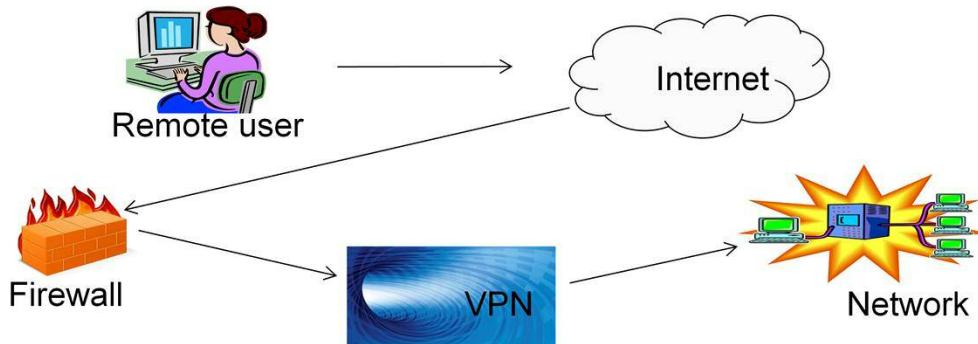
The problem remote users face is that their communications are open on the long journey from the laptop or home computer to the work environment. One solution is the leased line. This is expensive compared to all VPN options but has the advantage in that it would require a physical attack to compromise. The major disadvantage is that you can only have so many physical leased lines and installation of leased lines is extremely time consuming and expensive.

VPNs can be implemented in hardware or software. The advantages and disadvantages are similar to those we noted in firewalls. VPN appliances often are deployed in the corporate environment where they can manage multiple secure connections. The advantage with a hardware deployment is the dedicated CPU and memory, higher throughput and typically a richer feature set.

VPN Clients are normally software based as they are inexpensive and easy to deploy on end user devices.

VPN Appliance

- Some firewalls have virtual private networking built in
- Some stand-alone VPN appliances work as a firewall



Some firewalls have a VPN feature built into them and some VPN appliances have firewall capabilities.

Here we show a Remote User traversing the Internet to VPN through firewall to target Network.

Appliances come in all shapes and sizes. The larger the number of remote users the more likely the network will require a dedicated VPN. In the next slide we talk about the range of security risks we see in clients.

Operating System–Based VPNs

- No additional hardware needed
- Runs on top of or is part of server operating system
- Can use Windows Server Network Policy and Access Services role, configure as a VPN server
- Typical clients: Windows Vista, Windows 7/8, Linux, and UNIX
- Benefit: Can refer to remote servers by IP address rather than use NAT

Some operating systems have VPN clients built in. The advantage here is relatively low overhead, little or no cost, and sometimes the ability to use direct IP address rather than going through NAT.

VPN Protocols

Remote Access Protocol	Encryption Protocol
Point-to-Point Tunneling Protocol (PPTP)	Microsoft Point-to-Point Encryption (MPPE)
Layer 2 Tunneling Protocol (L2TP)	IPSec
Secure Sockets Layer (SSL)-based tunneling protocols	SSL
Internet Key Exchange v2—Internet Key Exchange v2 (IKEv2)	IPSec

Here are some examples of remote access protocols and the encryption protocols they use. Of these, the ones using IPSec would arguably be the best choices, but as always, the environment may dictate a different choice.

VPN Security Measures

- IPSec (originally for IPv6 but widely used on IPv4)
- SSL / Transport Layer Security
- Datagram Transport Layer Security (DTLS)
- Microsoft Point-to-Point Encryption
- Secure Socket Tunneling Protocol (SSTP)

VPN security relies heavily on encryption technologies, especially when crossing the internet. Here are a number of encryption technologies that can be used. As mentioned, IPSec remains a popular choice. Secure Socket Layer (SSL) has recently been shown to be exploitable as has the early versions of Transport Layer Security (TLS). Only TLS 1.2 is currently considered secure.

VPN Security Measures

- User initiated VPN tunnels use passwords, biometrics, two-factor authentication, and other cryptographic methods
- Gateway-to-gateway tunnels use certificates

Authenticating a VPN connection can use a variety of identifiers. Passwords and a second factor such as an RSA token are often used to establish identity.

Gateway to gateway connections typically use certificates.

Nature of VPN Threats and Attacks

- Home computers are often less secure than IT-maintained machines
- If a home computer is compromised, that attack can follow the VPN to the internal network
- A constant live connection such as always-on DSL gives hackers more opportunities to penetrate the corporate network via VPN
- A personal firewall on the home computer should be mandatory and will mitigate a lot of risk

A machine with a VPN on it needs security passwords, firewalls, and physical security. As a best practice, you should never allow others to use your VPN-enabled computer. Treat the machine the same way you would a dangerous weapon. You wouldn't leave it out of your sight or laying around carelessly. You want to control who has access to it. Corporate espionage can start with the home being burglarized so consider physical security recommendations.

Nature of VPN Threats and Attacks

- All home users should have intrusion detection.
- When possible, the IT team should set up the home system and not trust the user to get it right
- Make sure home users are all aware of the latest patches and make sure they get applied
- Traveling workers should be reminded not to leave computers in hotel rooms or cars—don't let a system with a VPN into the company network out of sight.

As you can no doubt tell, a remote machine with a VPN on it can present a considerable risk to the organization. It therefore requires special attention and additional protective measures. Ensuring the VPN client is properly installed and kept up to date with security patches is a must. Providing physical security is also a must. Traveling with VPN enabled computers represents the greatest risk.

Firewall and VPN Integration

- Firewalls control access to the network through a variety of means
- VPNs facilitate secure communication for hosts, not on the network
- VPNs allow the host to appear as if it were on the target network
- VPNs can work across the Internet or across a intranet

Earlier we noted that some firewalls have VPN integrated into their suite of functions. Their normal function is to control access and a VPN is access worthy of control. VPNs facilitate communications for remote hosts allowing them to appear as if they were on the target network. Although VPNs may operate across different communication channels, going across the internet is perhaps the most common.

VPN Hosts and Trust

Trust should vary depending on who is allowed in via the VPN

Least Risk

Employee on corporate laptop on managed network

Employee on home computer

Employee on airport internet (wireless or kiosk)

Authorized partner

Most Risk

Authorized customer

VPNs represent varying levels of risk depending on who is accessing what resources. With each level there is less control that IT has. The first level might be an employee on a hotel network (assuming a decent hotel). At home the employee should be following IT policy but also has potentially a family or a roommate and friends and neighbors who might have access. Also, there is the risk of physical breach. Policy may be sufficient in mitigating these risks if the employee is trustworthy.

Airport networks are improving every day and many are at the level of the managed network. The disadvantage is that the employee is out in the open and subject to surveillance. It is not always assured that wireless access points are secure and not spoofed.

Authorized partners and customers are more of a risk because there is no expectation of corporate policy controls. One has to assume they will act autonomously and may represent an increased risk.

VPN/Firewall Security and Performance

- Do not implement a VPN with no firewall—the two complement each other
- Make sure your operating system is IPSec compliant.
- For a wireless LAN, make sure you are secure.
 - Place wireless access point outside of the firewall
 - Place VPN inside the firewall
 - Optionally layer firewalls
- Be careful—VPNs produce a security overhead that may affect network Internet bandwidth.

Even if you are implementing a VPN that is capable of some firewall functions, you should never rely on those alone. Always utilize a firewall in conjunction with the VPN device. Make sure your VPN appliance is IPSec compliant. IPSec stands for Internet Protocol Security, and is a VPN-supporting technology included in Windows XP, Vista®, Windows 7, Windows Server 2008, and Windows Server 2008 R2. Used with compatible VPNs, IPSec guarantees the authenticity, integrity, and confidentiality of network traffic. Interoperability with a VPN may be an issue with Macintosh systems or some variants of UNIX or Linux. If you decided to buy a VPN, make sure it is compatible with your operating system.

Wireless presents its own set of security challenges. As a best practice, wireless should be placed outside the firewall so that firewall can control that traffic. VPNs are typically inside the firewall as the traffic is encrypted and the firewall – unless it is performing VPN services – cannot view the traffic.

As always, traffic should be monitored from a performance perspective. VPNs may impact the overall performance of your network.

Protect the VPN

- Firewall is the best protection
- Keep the VPN behind a firewall or
- Use a firewall/VPN appliance
- Rule of thumb

If your VPN is compromised

So is your firewall

And the network behind it

Protect your VPNs like they were back doors into the network. They are. Follow these important security considerations. Think like a hacker. What is easier to attack, a surface or a gap? Protect your gaps and harden your surfaces to keep the network safe.

Summary

- Best practices for management of enterprise and personal firewalls
- Security appliances that work together with firewalls or extend their functionality
- Best practices for management of VPN connectivity
- Risks to the enterprise presented by the use of remote access technologies

In this unit we have examined best practices for the management of enterprise and personal firewalls. We have looked at some of the security devices that supplement firewalls to add to our perimeter and internal security. We've listed the considerations that should be taken into account when selecting a firewall or implementation strategy.

We have also looked at best practices for VPNs. We've examined the pros and cons of different implementation options including hardware and software in integrated solutions in firewalls. We ended our discussion with a careful look at the security concerns presented by VPNs.

End of Lecture 3



of Lecture 3

15

This ends Lecture 3 of Unit 10. If you are interested in using Smoothwall for a firewall implementation you can continue to Lecture 4.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 11

Network Security Management

Lecture 1

Welcome to Lecture 1 of Unit 11

Key Concepts

- Best practices for network security management
- Strategies for integrating network security strategies with firewall defenses and VPN remote access
- Value of incident response planning, testing and practice

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this unit we will explore best practices for network security management. We will look at integrating our firewall and VPN defenses into the overall security strategy. We will also expand on the value of incident response planning, testing and practice.

Learning Objective

Learning Objectives

- Identify network security management best practices and strategies for responding when security measures fail

Our learning objective for this unit is the identification of security management best practices for when our security measures fail.

Best Practices: Strategy

■ Create written plans

- Security policy
- Incident response plan
- Business continuity plan (BCP)
- Disaster recovery plan (DRP)
- Security checklists

We have stated on several occasions that having written security plans that implement our written security policies is a necessity. These plans become the basis of our controls which do the work of protecting our environments. We've also emphasized that change is inevitable both in our business and in the threats and vulnerabilities we seek to mitigate. Despite our efforts there is always the possibility that a control will fail or an attack will be successful. Another potential is an environmental event that can impact our business. This could be a fire, flood, tornado, hurricane or other natural occurrence.

To manage these situations and keep the business running we need a plan. Actually we need several plans. We should already have our security plan which supports our business goals and objectives, We need an incident response plan that provides instructions on how we deal with those events that impact our security on a frequent basis. Incidents if left unresolved can escalate into major issues that could halt our business.

A business continuity plan is designed to keep the business operating despite a major interruption. The goal here is to lessen the impact of serious events and allow the business and its employees to continue to work and generate revenue.

A disaster recovery plan manages longer term business interruptions. It lays out the

steps needed to get the business back up and running in the most efficient way possible after a disaster.

Security checklists can provide a convenient way to ensure that each element of your security implementation is checked either before or after an event.

Best Practices: Strategy

- **Perform regular maintenance**
 - Back up regularly and test restores frequently
 - Monitor and review collected log files frequently
 - Constantly identify the weakest architectural link

Part of ensuring a well operating network is performing regular maintenance. Just as a vehicle or home needs constant or at least consistent attention, so does your security environment. Ensuring that you have sufficient capacity and that your nodes are operating efficiently takes frequent if not continuous attention. Providing redundancy for critical systems with automatic fail over or load balancing is often used to maintain uptime for those critical systems.

Backing up your critical system configurations is just as important as backing up your critical data. Both should be done on a regular basis. Backups should be regularly tested too. Although it can be time consuming, periodic verification that backups can be restored is essential to avoiding an incident becoming a disaster.

Logs should be collected and reviewed frequently. Some compliance requirements demand daily review of logs.

Network, systems and security administrators should constantly be looking for and propping up the weak points in their domains. Continual improvement is a best practice that pays well in the long haul.

Best Practices: Strategy (cont.)

- Perform diligent testing of new systems before deploying in production
- Implement the principle of least privilege
- Deploy layered defenses

Introducing new devices and software into your secure environment injects new risk. One way to reduce that risk is by building new devices to a proven standard which incorporates hardening and thorough testing prior to installation. Just as employees should be subject to the principle of least privilege, so should software and devices. They should be built to perform their defined tasks well, but have unnecessary and undesired functionality removed.

As a best practice, deploy defenses in layers and with depth. Don't rely on a bulletproof perimeter, there is no such thing. Place controls throughout your networks including on your endpoints.

Best Practices: Devices

- Maintain physical security over users and equipment
- Install and maintain virus and malware protection at all layers in the environment
- Harden both internal and perimeter devices
- Develop and follow a patch management strategy
- Enforce hard drive or file encryption

Don't forget physical security. Great logical security is undone if someone can gain physical access to the systems or devices.

Anti-virus and anti-malware is still an essential part of your security arsenal. But it must be kept up to date and kept active. Prevent your users from being able to turn it off and ensure updates are frequently applied. Look for products that use heuristics as well as signatures and enable periodic system scans.

Harden all your devices, not just those on your perimeter. Don't make it easy for an attacker that gets through the first wall.

Keep up to date with your patching. Patches frequently address found vulnerabilities and many of those can be publically known. That means unpatched system are targets. Prioritize your patching to ensure that security and critical patches are applied promptly. Most compliance requirements specify 30 days to get your critical patches installed.

Use encryption. Hard drive, file or database encryption can save you if there is a breach. Ensure that your critical data is protected at rest and in transit using strong encryption and good key management.

Best Practices: Connectivity

- Restrict Internet connections to required activity
- Limit remote access to required connectivity
- Encrypt all internal network traffic
- Require multifactor authentication
- Use default-deny over default-permit as possible

Restrict connections into your networks to those that are truly required. An open door is an invitation for trouble.

Remote access has many benefits, but it also raises security concerns. Control your remote access channels and keep them to a manageable level. Monitor access and require strong authentication including two factor.

Even though internal traffic is trusted, encrypt it when possible. This keeps it from being easily sniffed to collect authentication credentials or other critical information.

Multifactor is always better than single factor authentication, and no repeating single factors multiple times does not improve security.

Default deny should always be preferred over default permit. Don't leave doors open.

So many best practices, it's hard to remember them all. But they do form patterns that are easier to remember. Look for them. Also, remember that every environment is different. Not all best practices work in every situation. Use those that do.

Network Security Assessments

Q: What is a network security assessment?

Let's change gears a bit and look at security assessments. What is a security assessment?

Network Security Assessments

Q: What is a network security assessment?

A: The process of judging, testing, and evaluating a deployed security solution

Security assessments are how we judge the effectiveness of our controls. We believe we have implemented all those best practices, in fact we would swear to it, but the only way to really have confidence is to validate through an assessment process.

Assessments are frequently mandated through regulations or other compliance requirements such as Sarbanes Oxley, HIPAA and PCI. These seek to ensure that the controls we implement do in fact provide the intended protection. Is it 100%? No, but an independent assessment is more likely to identify flaws than internal reviews.

User Training

Q: What is user training?

What about training?

User Training

Q: What is user training?

A: Educational information presented through various mechanisms that clearly defines security policies, their boundaries and imposed limitations

Another aspect of security that is mandated by many regulations is user training. Great security can be easily undone by unintentional actions. Training is the key to improving the effectiveness of our security programs.

User Training

Q: What is user training?

A: Educational information presented through various mechanisms that clearly defines security policies, their boundaries and imposed limitations

Q: Why is user training important?

Is it really that important?

User Training

Q: What is user training?

A: Educational information presented through various mechanisms that clearly defines security policies, their boundaries and imposed limitations

Q: Why is user training important?

A: Training drives user accountability, understanding, and acceptance of obligatory security policies

Yes. Not only is training necessary to meet many regulatory requirements, it is by far the least expensive method of improving the effectiveness of your security program. Training informs people of their obligations and drives accountability. Training gives individuals the tools to identify and respond appropriately to potential security events.

User Training

Q: What is user training?

A: Educational information presented through various mechanisms that clearly defines security policies, their boundaries and imposed limitations

Q: Why is user training important?

A: Training drives user accountability, understanding, and acceptance of obligatory security policies

It is imperative that regular renewal of security awareness training occurs

Training is not a one shot event. To be effective, training must be done periodically and should involve multiple different modes. Annual training is an opportunity to review and refresh users understanding and acceptance of acceptable use policies as well as other obligations required by the organization.

Security Awareness

- Defines, informs, explains, and teaches users the principles and importance of security
- Every user in an organization has a part to play in upholding company security
- Awareness and education may be tailored to job specific or role specific content
- Policies and procedures are driven by people
 - Without mechanisms to aid users in secure network use, much of the work put into implementing best practices for network security may become degraded

Security awareness defines, informs, explains, and teaches users the principles of security and why they are important.

Every user in an organization has a part to play in upholding company security.

Awareness and education may be tailored to job specific or role specific content.

Training is an inexpensive mechanism that can be used to aid users in secure network use. Untrained or poorly trained individuals can undo great security unintentionally through error or ignorance. Training is one tool to avoid that possibility.

End of Lecture 1



of Lecture 1

17

This ends Lecture 1 of Unit 11. We will continue in Lecture 2.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 11

Network Security Management

Lecture 2

Welcome to Lecture 2 of Unit 11

Network Monitoring Tools (Open Source)

- Nagios – network management and monitoring
- SmokePing –monitors network latency
 - Can visualize the entire network
- GroundWork – highly scalable network management and monitoring
- Ganglia – geared toward clusters and grids
- Cacti
- Ntop

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this lecture we will be discussing the monitoring, identification and response to potential events in our networks. There are many tools available to the network administrator for monitoring their network. I've listed a number of open source tools here. There are many more and all have strengths and weaknesses. Their advantage is they are free or close to free. They can give you an opportunity to identify the types of information and features you need to monitor your specific environments.

Network Monitoring Tools (Commercial)

- WhatsUp Gold
 - Proactive monitoring and management tool
- Iris
 - Network traffic monitoring and analysis tool

After trying free and open source tools, you may find that they don't provide the full range of features you want. Here are a couple of commercial tools that offer more robust capabilities, at a cost of course. These are just two of many. You will need to research others based on the environment and traffic you are concerned about.

Security Information and Event Monitoring (SIEM)

- A SIEM is a tool that allows for automation of log and event centralization and analysis
- Functions of a SIEM
 - Log centralization
 - Log management
 - Log monitoring
- Purposes of a SIEM
 - Incident detection
 - Incident response and alerting

As mentioned multiple times, monitoring and logging of network and security events is essential and often a compliance requirement. Larger environment can generate massive amounts of logs making manual review impossible. Enter the Security Information and Event Monitoring system. SIEMs collect, protect, and analyze logs from many sources in a centralized repository. SIEMs can parse large amounts of logs and correlate events to identify patterns that could indicate attacks. They are especially useful for identifying the low and slow attacks that often are missed by manual review. SIEMs can generate alerts when suspicious events are identified.

While many SIEMs have fair functionality out of the box, they require time on the network to develop baselines of traffic and event patterns. They also require programming of rules specific to the environments they operating in. This can create some support and maintenance overhead, but it is usually much less than what is needed for manual review of logs.

Commonly Available SIEM Tools

- enVision
- Qradar
- Eventia
- Security Manager
- nDepth

Here is a short list of SIEMs. There are many more in the marketplace and more are being introduced on a regular basis.

Incident Response

Preparation

Detection

Containment

Eradication

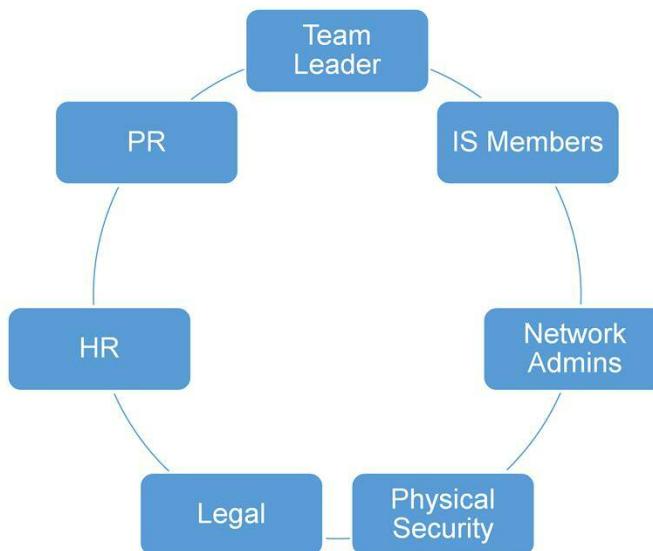
Recovery

Follow-up

So what happens when your SIEM detects an event and issues an alert?

It depends. If the first responders determine that the alert is valid and an impact is eminent, they may invoke the incident response plan. This assumes there is a plan – that is the preparation box above. The SIEM was used for the Detection. Now it's up to the incident response team to contain the event, eradicate or mediate it, recover any damage to systems or data and follow-up.

Incident Response Team (IRT)



Incident response typically requires a flexible team of individuals or roles and vary depending on the type and scale of the incident. The team can be made up of the:

- Team leader
- Information security members
- Network administrators
- Physical security personnel
- Legal
- Human resources (HR)
- Communications/public relations (PR)

Again, the actual members will depend on the specific incident. The incident response plan should identify the players, provide guidance on who needs to be involved under different circumstances and provide contact information

The Future State of Network Security Strategies

- Threats
- Firewall capabilities

Threats

Ten years ago, major of malicious threats were waged against operating systems. Today, the focus is on applications and mainly browsers. We now see a lot of hacking, targeted attacks against companies, viruses that target credit card numbers, bank account information and Social Security numbers, DoS and DDoS attacks, and root kits that turn hosts into zombies.

In the future, you will see more resilient networks that mitigate the risk of traffic-based attacks, more secure operating systems and applications to resist malware, and intrusion prevention systems that will respond instantly to attacks, choking them off before they can damage your infrastructure. Of course attackers will up their game as well providing new challenges to be overcome. Its truly an arms race that has no end in sight.

Firewall Capabilities

Firewalls have been adding capabilities since they were first introduced. Early firewalls contained some limited filtering and NAT capabilities, and not much else. Today's firewalls offer a wide range of capabilities and specialties, which continue to grow rapidly. Deep packet inspection and operation over all layers of the OSI model will become the norm, especially in the higher end devices.

The Future State of Network Security Strategies

- Encryption
- Authentication
- Metrics

Encryption

Encryption is a standard that is constantly evolving. We have gone from DES, a 56-bit algorithm, to 3DES, an effective 168-bit algorithm, to AES, which supports a 256-bit algorithm. Changes in technology, especially advances in quantum computing threaten to make even AES obsolete sooner than expected. Still, encryption is one of our best tools for protecting data at rest and in motion.

Encryption's popularity has been growing as concerns with respect to protecting data at rest, in transit, and while archived. The key to keep in mind as you look into encryption solutions is ensuring they support AES or an equivalent algorithm, and be sure that you encrypt your data everywhere it is vulnerable.

Authentication

Another area where you can expect to see dramatic changes in future capabilities is in authentication, especially with respect to identity and access management.

One trend is moving away from passwords to tokens, smart cards, and biometric authentication as a replacement or supplement to existing user ID and password solutions.

Identity and account management solutions provide automation, full account life cycle management, and associated auditing. However, the solutions are complex to install and maintain and can be expensive.

Metrics

The Trend has been moving toward increased use of metrics and this is expected to continue. There are now a number of standards available for establishing and generating metrics. The most popular is ITIL, the Information Technology Infrastructure Library, which is a set of concepts you can use to formalize your security management practice and the associated reporting.

The Future State of Network Security Strategies

- Industry focus
- Cloud security
- Mobile device security

Industry Focus

What is the industry focused on securing? Initially, information security was about keeping the bad guys out of your network.

The Focus has begun shifting from network to host: patch management, hardening operating systems, and installing host-based firewalls will become increasingly important.

Attackers have shifted to attacking applications on our hosts, so we focused on integrating security into the software development life cycle, penetration testing, and firewall and proxy server deployment.

Next shift in focus for information security is on data. Industry heading towards a data-centric security model, a significant paradigm shift from previous models. A data-centric model will force companies to focus on classifying and applying values to their data.

Securing the Cloud

You have to trust the vendor providing your cloud. This requires a shift in focus from deploying security technologies to ensuring your vendors are contractually obligated to keep your data secure. You also need to be able to evaluate vendors to determine how trustworthy they are, and if you have the available resources, you should be auditing the vendor(s) to ensure they continue to keep your data secure.

Securing Mobile Devices

There are already virus protection, mobile device management, and encryption applications available for mobile devices. The challenge you'll typically see in both current and future implementations is that these types of devices are frequently overlooked or discounted when security risks are being documented. Be sure to keep these on your list of risks – there is an alarming amount of storage and processing capacity on these devices, which makes it easy for an employee to put confidential information on them without thinking twice about it.

The Future State of Network Security Strategies

- IPv6 support

IPv6 Support

IPv6 includes a native information security framework based on IP Security (IPsec) which provides for both data and control packets. This means that what you currently do with a traditional VPN you will be able to do natively with any IPv6 device. At a high level that means you can run your IPsec VPN without requiring a client, but the implications are significantly more profound than just that.

In a fully IPv6 environment, any connection can be configured to utilize an IPsec connection. This means that any connection from a user to an application, host-to-host, or even peer-to-peer connection will be authenticated and encrypted as it passed across the network. That's the good news.

On the other side of the coin, Ipv6 has been slow to be adopted. IPv4 is very well established and is supported by all current equipment. Ensuring the IPv6 is available widely will depend on replacing a considerable amount of equipment throughout the infrastructure of the Internet as well as in businesses. The investment in new equipment will have to be phased in over time as older equipment is replaced. The net affect is that we won't be seeing wide adoption of IPv6 for some years to come.

Integration of Firewalls and VPNs

- **Functions**
 - Enhanced threat management
 - Authentication
 - Encryption

Integration of VPNs into firewalls is a trend that is likely to continue. At least with appliance based firewalls. By terminating the VPN connection at the firewall, the firewall has the opportunity to decrypt and inspect the traffic.

Summary

- Best practices for network security management
- Strategies for integrating network security strategies with firewall defenses and VPN remote access
- Value of incident response planning, testing and practice

To summarize, in this unit we have looked at quite a few best practices for firewalls and VPN. We have also examined some of the potential pitfalls with remote access using VPNs. We discussed strategies for maintaining security in different implementations. We expanded our discussion of the importance of monitoring and alerting on events and emphasized the need for an Incident Response plan. We also noted the importance of periodic testing and updating or Incident Response plans as well as business continuity and disaster recovery plans.

End of Lecture 2



of Lecture 2

14

This ends Lecture 2 of Unit 11. We will continue in Lecture 3.



UNIVERSITY OF DALLAS

Satish & Yasmin Gupta
College of Business



Network Security

Unit 11

Network Security Management

Lecture 3

Welcome to Lecture 3 of Unit 11

Network Security Management

Fail-Secure, Fail-Open, and Fail-Close States

- Fail-secure state: Reverts to a condition where little or no harm is likely to happen
 - Depending on situation, fail-secure state could be fail-open or fail-close
- Fail-open state: To revert to a state of being open, available, or unlocked
- Fail-close state: To revert to a state of being closed, unavailable, or locked

Slides in this deck contain material from the Jones and Bartlett ISSA series and are used with permission

In this lecture we will be covering a few more topics in Network Security Management as well as reviewing some important topics from earlier units.

Let's start with some definitions. When devices or systems fail, they may adopt one of several conditions. These are listed on this slide. It may be more clear to use a physical example to make the distinction. Consider a door to your business. During working hours you have employees and visitors coming and going on a regular basis. The door they use has a magnetic lock. Should the power go out during business hours you would want the door to fail open to allow people to enter and leave as usual. After hours when the business is empty would be different. During a power outage you would want the door to remain locked to prevent unauthorized entry and theft. This would be a fail-closed situation.

Being safety conscious, you want to make sure that the cleaning people that work in the evening when the business is normally closed wouldn't be trapped in the event of a fire, so you install an emergency break bar that allows the door to be opened from the inside in the event of a power failure. If no one is inside, the door remains locked.

Physical Security



Starting with a physical security example leads us to some additional physical considerations for the protection of our networks and systems. All of these may seem obvious and hopefully all have been implemented in your workplace. If not, they should be considered bearing in mind the level of sensitivity of the data and system you operate.

First there should be no direct access either physically or logically to your trusted network. Just as we use a firewall to block unwanted traffic, we use door, balusters, gates, guards and other mechanisms to prevent unauthorized physical access.

When access is granted monitoring is still the norm. We monitor activity into, within and out of our trusted networks. We should also monitor physical movements of personnel at sensitive areas including entrances and exits.

Other detective controls we should consider are using card key entry, alarms, motion detectors, cameras, etc.

Backup and Recovery



Online

Offsite

Onsite

Backup and recovery are essential elements of business continuity. There are typically three widely used approaches to store and maintain these backups. Online has become very popular as the prices have dropped. Those still using tape will benefit from offsite storage. Vendors such as Iron Mountain have made a great business out of securing other businesses materials in secure offsite locations.

Onsite is still widely used although there are some obvious risks involved with this approach. The lower cost of disk storage has made virtual copies much more feasible.

Network Security Management Tools

- Written security policy
- Complete inventory of hardware and software
- Physical cabling layout and device location map
- Logical organization, addressing, and subnetting map
- Complete configuration documentation for every device
- Change documentation and log

We have already emphasized the importance and need for security policies. Did we remember that physical security is a component of that?

Another component, and one that is mandated by some compliance requirements as well as best practices is maintaining an inventory. An inventory is a good way to start evaluating your network, tracking potential vulnerabilities and meeting compliance requirements.

Knowing where devices are physically located and how they are connected is another huge plus. This is especially true when troubleshooting your network.

The same is true from a logical perspective. Maintaining accurate drawings which include device addresses is another shortcut for troubleshooting as well as meeting compliance requirements.

Maintaining records of device configurations can be done manually or managed automatically using software applications. Going the automated route has distinct advantages even though there is a cost involved. For larger organizations, automated configuration management is the way to go.

Tracking changes to your environment is another necessity. Having a robust change management program provides for management review and other benefits.

Network Security Management Tools (cont.)

- Backup and restoration procedures
- Business continuity and disaster recovery strategy
- Troubleshooting guidelines
- Hardware and software documentation
- Personal knowledge and skill
- Access to online resources

Some of the other tools in the network security management tool kit include procedures for backups and restoration. Business continuity and disaster recovery strategies along with their documented plans are an important part of every business's security management program.

Troubleshooting guidelines are not often thought of, but these can be incorporated into the incident response plan.

Maintaining hardware and software documentation is also a best practice. Being able to lay your hands on product and software documentation in an emergency can often shorten the time needed to troubleshoot and resolve issues.

Don't underestimate your employees knowledge and skills. They people that work on systems on a daily basis have intimate knowledge that should be called upon when needed.

Access to online materials and knowledge bases is another great benefit. Searching for similar issues may yield quicker options to try or even direct solutions from those who have had the same issue.

Physical Security Checklist

- Check window and door locks
- Check external walls
- Inspect access points to raised floor areas and drop ceilings
- Ensure that cabinets or containers are locked
- Verify that security cameras are pointed in the correct direction

Checklists can be applied to physical security as well as other security domains. These are a few of the common checkpoints. More are on the following slide.

Physical Security Checklist (cont.)

- Verify that all light bulbs are of the correct type and are functioning
- Check motion detectors
- Test alarm systems
- Interview security guards and confirming compliance with procedures

As promised, here are some additional items to put on your physical security check list. There are many more. Can you think of them?

Logical Security Checklist

- Check authentication, authorization, and access control
- Audit systems
- Verify firewalls and other filters
- Check proxies and other communication management solutions
- Verify encryption, including key management
- Update antivirus software and scanners
- Back up and store archival information securely

Here is another example of a logical checklist. Again, this is the tip of the iceberg. How many more can you think of?

Tools for Network Security

Commercial Off-the-Shelf (COTS) Software

- Combines hardware and software into an appliance
- Companies rely on solutions they can support
- Commercialization of open source solutions

Open Source Applications and Tools

- Affordable way to build your information security skill set
- Same tools many attackers use; allows you to develop parallel expertise

Obtaining and using appropriate tools for network security is another job of the security engineer or administrator. Tools typically fall into a couple of categories, commercial tools and open source or free tools. Of course there are also tools built in house, but you should ask yourself why recreate the wheel if a suitable tool already exists?

We have already discussed many options for both open source and commercial tools and those were only a few. A quick internet search will yield dozens if not hundreds of free, low cost and commercial tools to help solve your security management problems.

Wireless Ubiquity



Wireless deployed as a LAN technology

Public and home office wireless

Mobile wireless

Before we close this lecture, there are a couple more topic that should be mentioned. The first is wireless. Wireless can and is being deployed as a LAN technology. Wireless is widely used in both home and business environments. Wireless is becoming ubiquitous especially in mobile situations. It's a great feature to be connected wherever you are to all the home work and entertainment resources you desire. But wireless is far from secure. The issues surrounding wireless insecurity could be a course in itself, so there isn't time here to explore it in any detail. Just be aware that wireless requires special attention to ensure the risks associated with it are not excessive.

Emerging Network Security Technologies

- Data leakage prevention (DLP)—New government regulations will drive implementation in health care; HIPAA, HITECH, and PCI have specific data protection requirements
- Biometrics—Being included in ATMs, laptops, and computer networks
- Virtualization security—Antivirus, vulnerability management, data leakage prevention, and IDS/IPS being developed to run virtually

I'd like to close with a short list of emerging technologies that will be coming to a retail outlet close to you. Data loss protection is not a new technology, however it is one that is evolving. There are a number of compliance mandates that can be met using DLP which will continue to drive its evolution.

Biometrics are also not new. They are as old as people themselves. The new twists using technology are still maturing and there has yet to be a foolproof biometric system produced. Nevertheless, biometrics has great promise to be the identification mechanism of the future. We're just not sure when the future will get here!

The last bit is on virtualization. Many of the security processes and applications we rely on today are reaching our virtual environments. One of the major drivers is the rapid adoption of cloud computing and cloud resources. Stay tuned. Many believe our future is in the clouds.

End of Lecture 3



of Lecture 3

13

This ends Lecture 3 of Unit 11.