Chapter 3
Exploring Network Technologies and Tools

CompTIA Security+ objectives covered in this chapter:

1.2 Compare and contrast types of attacks.

- Application/service attacks (ARP poisoning, DNS poisoning)

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- Firewall (ACL, Application-based vs. network-based, Stateful vs. stateless, Implicit deny), Router (ACLs, Antispoofing), Switch (Port security, Layer 2 vs. Layer 3, Loop prevention, Flood guard), Proxy (Forward and reverse proxy, Transparent, Application/multipurpose), Mail gateway (Spam filter, DLP, Encryption), Bridge, Media gateway

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Command line tools (nslookup/dig)

2.3 Given a scenario, troubleshoot common security issues.

- Misconfigured devices (Firewall, Content filter)

2.4 Given a scenario, analyze and interpret output from security technologies.

- Host-based firewall, UTM, Web application firewall

2.6 Given a scenario, implement secure protocols.

- Protocols (DNSSEC, SSH, SRTP, FTPS, SFTP, SNMPv3, SSL/TLS, HTTPS, Secure POP/IMAP)
- Use cases (Voice and video, Time synchronization, Email and web, File transfer, Directory services, Remote access, Domain name resolution, Routing and switching, Network address allocation, Subscription services)

3.2 Given a scenario, implement secure network architecture concepts.

- Zones/topologies (DMZ, Extranet, Intranet, NAT), Segregation/segmentation/isolation (Physical, Logical (VLAN), Air gaps), Security device/technology placement (Filters, Proxies, Firewalls, Load balancers, DDoS mitigator, Aggregation switches)

1.3 Given a scenario, implement secure systems design.

- Operating systems (Disabling unnecessary ports and services)

**

CompTIA expects prospective CompTIA Security+ exam takers to have at least two years of networking experience. However, even with that amount of experience, there are often gaps in an information technology (IT) professional's or security professional's knowledge. For example, you may have spent a lot of time troubleshooting connectivity but rarely manipulated access control lists (ACLs) on a router or modified firewall rules. This chapter reviews some basic networking concepts, devices, and network topologies used within secure networks. When appropriate, it digs into these topics a little deeper with a focus on security.

Reviewing Basic Networking Concepts

Before you can tackle any of the relevant security issues on a network, you'll need a basic understanding of networking. As a reminder, CompTIA expects you to have a minimum of two years of experience in IT administration. Further, CompTIA recommends obtaining the Network+ certification before taking the Security+ exam. Although the Network+ certification isn't required, the knowledge goes a long way in helping you pass the networking portion of the Security+ exam.

This section includes a very brief review of many of the different protocols and networking concepts that are relevant to security. If any of these concepts are completely unfamiliar to you, you might need to pick up a networking book to review them.

This section also mentions some of the common attacks used against the protocols, or that the protocols help protect against. The following bullets introduce some of these attacks and Chapter 7, "Protecting Against Advanced

Attacks," covers these attacks in more depth:

- **Sniffing attack.** Attackers often use a protocol analyzer to capture data sent over a network. After capturing the data, attackers can easily read the data within the protocol analyzer when it has been sent in cleartext. Chapter 8, "Using Risk Management Tools," covers protocol analyzers in more depth.
- **DoS and DDoS.** A denial-of-service (***DoS***) attack is a service attack from a single source that attempts to disrupt the services provided by another system. A distributed DoS (***DDoS***) attack includes multiple computers attacking a single target.
- **Poisoning attack.** Many protocols store data in cache for temporary access. Poisoning attacks attempt to corrupt the cache with different data.

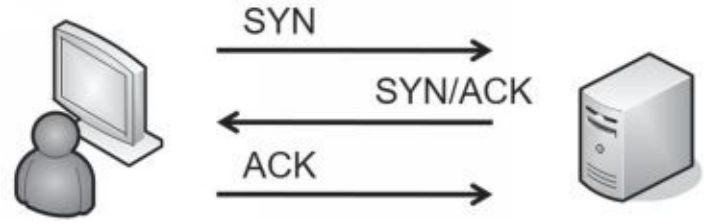
Basic Networking Protocols

Networking protocols provide the rules needed for computers to communicate with each other on a network. Some of the Transmission Control Protocol/Internet Protocol (TCP/ IP) protocols, such as TCP and IP, provide basic connectivity. Other protocols, such as Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP), support specific types of traffic. This section includes information on common protocols that you'll need to understand for the CompTIA Security+ exam.

TCP/IP isn't a single protocol, but a full suite of protocols. Obviously, there isn't room in this book to teach the details of all the TCP/IP protocols. Instead, the purpose of this section is to remind you of some of the commonly used protocols. Additionally, many of these protocols meet specific use cases and this section describes these protocols within the context of use cases.

CompTIA has historically placed a lot of emphasis on well-known ports used by protocols. For example, the default port for HTTP is 80 and CompTIA Security+ test takers needed to know that. The current objectives have deemphasized the importance of ports. However, you still need to know them when implementing access control lists (ACLs) in routers and stateless firewalls, and when disabling unnecessary ports and services. With that in mind, I've included the well- known ports for many of the protocols in this chapter.

The following list describes some basic networking protocols:

- 

TCP. Transmission Control Protocol (TCP) provides connection-oriented traffic (guaranteed delivery). TCP uses a three-way handshake and Figure 3.1 shows the TCP handshake process. To start a TCP session, the client sends a SYN (synchronize) packet. The server responds with a SYN/ACK (synchronize/acknowledge) packet, and the client completes the third part of the handshake with an ACK packet to establish the connection.

Figure 3.1: TCP handshake process

- **UDP.** User Datagram Protocol (UDP) provides connectionless sessions (without a three- way handshake). While TCP traffic provides guaranteed delivery, UDP makes a best effort to deliver traffic without using extra traffic to ensure delivery. ICMP traffic such as the ping command and audio/video streaming use UDP. Many network-based denial- of-service (DoS) attacks use UDP. TCP/IP traffic is either connection-oriented TCP traffic or connectionless UDP.
- **IP.** The Internet Protocol (IP) identifies hosts in a TCP/IP network and delivers traffic from one host to another using IP addresses. IPv4 uses 32-bit addresses represented in dotted decimal format, such as 192.168.1.100. IPv6 uses 128-bit addresses using hexadecimal code, such as FE80:0000:0000:0000:20D4:3FF7:003F:DE62.
- **ICMP.** Internet Control Message Protocol (ICMP) is used for testing basic connectivity and includes tools such as ping, pathping, and tracert. As an example, ping can check for basic connectivity between two systems, as discussed in Chapter 1, “Mastering Security Basics.” Many DoS attacks use ICMP. Because of how often ICMP is used in attacks, it has become common to block ICMP at firewalls and routers, which disables a ping response. Blocking ICMP prevents attackers from discovering devices in a network. For example, a scan can send a ping to every IP address in a subnet. The devices that reply verify that they are on and have an IP address.

- **ARP.** Address Resolution Protocol (ARP) resolves IPv4 addresses to media access control (***MAC***) addresses. MACs are also called physical addresses, or hardware addresses. TCP/ IP uses the IP address to get a packet to a destination network, but once it arrives on the destination network, it uses the MAC address to get it to the correct host. In other words, ARP is required once the packet reaches the destination subnet. ***ARP poisoning*** attacks

use ARP packets to give clients false hardware address updates and attackers use it to redirect or interrupt network traffic.

- **NDP.** Neighbor Discovery Protocol (NDP) performs several functions on IPv6. For example, it performs functions similar to IPv4's ARP. It also performs autoconfiguration of device IPv6 addresses and discovers other IPv6 devices on the network such as the address of the default gateway.

Implementing Protocols for Use Cases

Networks don't automatically support all the available protocols. Instead, IT professionals identify a need based on an organizational goal and enable the best protocol to meet that need. Chapter 1 discusses use cases. As a reminder, a ***use case*** typically describes an organizational goal. Many protocols mentioned in the CompTIA Security+ objectives support specific use cases and are discussed in this section.

Voice and Video Use Case

It's common for an organization to transport voice and video over a network and some protocols work better with voice and video than others. As mentioned previously, UDP is commonly used instead of TCP as the underlying protocol with voice and video streaming.

The Real-time Transport Protocol (RTP) delivers audio and video over IP networks. This includes Voice over Internet Protocol (VoIP) communications, streaming media, video teleconferencing applications, and devices using web-based push-to-talk features. However, organizations often want to secure these transmissions. The Secure Real-time Transport Protocol (***SRTP***) provides encryption, message authentication, and integrity for RTP.

SRTP helps protect the confidentiality of data from these attacks while also ensuring the integrity of the data transmissions. This provides protection against replay attacks. In a replay attack, an attacker captures data sent between two entities, modifies it, and then attempts to impersonate one of the parties by replaying the data. SRTP can be used for both unicast transmissions (such as one person calling another) and multicast

transmissions where one person sends traffic to multiple recipients.

File Transfer Use Case

Data-in-transit is any traffic sent over a network. When data is sent in cleartext, attackers can use a protocol analyzer to capture and read it. You can protect the confidentiality of Personally Identifiable Information (PII) and any other sensitive data-in-transit by encrypting it. Note that you can also encrypt data-at-rest, which is data stored on any type of medium. Chapter 10, "Understanding Cryptography and PKI," covers several specific encryption algorithms in more depth.

Some common use cases related to transferring files are transmit data over the network, ensure confidentiality when transmitting data over a network, and ensure administrators connect to servers using secure connections. The following list identifies basic protocols used to transfer data over a network:

- **FTP.** File Transfer Protocol (FTP) uploads and downloads large files to and from an FTP server. By default, FTP transmits data in cleartext, making it easy for an attacker to capture and read FTP data with a protocol analyzer. FTP active mode uses TCP port 21 for control signals and TCP port 20 for data. FTP passive mode (also known as PASV) uses TCP port 21 for control signals, but it uses a random TCP port for data. If FTP traffic is going through a firewall, this random port is often blocked, so it is best to disable PASV in FTP clients.
- **TFTP.** Trivial File Transfer Protocol (TFTP) uses UDP port 69 and is used to transfer smaller amounts of data, such as when communicating with network devices. Many attacks have used TFTP, but it is not an essential protocol on most networks. Because of this, administrators commonly disable it.

The following list identifies several encryption protocols used to encrypt data-in-transit.

They can be used for various use cases related to secure file transfer:

- **SSH.** Secure Shell (***SSH***) encrypts traffic in transit and can be used to encrypt other protocols such as FTP. Linux administrators often used Telnet when remotely administering systems, but this is not recommended because Telnet sends traffic over the network in cleartext. Instead, administrators commonly use SSH to remotely

administer systems. Secure Copy (SCP) is based on SSH and is used to copy encrypted files over a network. SSH can also encrypt TCP Wrappers, a type of access control list used on Linux systems to filter traffic. When SSH encrypts traffic, it uses TCP port 22.

- **SSL.** The Secure Sockets Layer (***SSL***) protocol was the primary method used to secure HTTP traffic as Hypertext Transfer Protocol Secure (HTTPS). SSL can also encrypt other types of traffic, such as SMTP and Lightweight Directory Access Protocol (LDAP). However, it has been compromised and is not recommended for use.
- **TLS.** The Transport Layer Security (***TLS***) protocol is the designated replacement for SSL and should be used instead of SSL. Additionally, many protocols that support TLS use ***STARTTLS***. STARTTLS looks like an acronym, but it isn't. Instead, it is a command used to upgrade an unencrypted connection to an encrypted connection on the same port.
- **IPsec.** Internet Protocol security (***IPsec***) is used to encrypt IP traffic. It is native to IPv6 but also works with IPv4. IPsec encapsulates and encrypts IP packet payloads and uses Tunnel mode to protect virtual private network (VPN) traffic. IPsec includes two main components: Authentication Header (AH) identified by protocol ID number 51 and Encapsulating Security Payload (ESP) identified by protocol ID number 50. It uses the Internet Key Exchange (IKE) over UDP port 500 to create a security association for the VPN. Chapter 4, "Securing Your Network," covers IPsec in more depth.
- **SFTP.** Secure File Transfer Protocol (***SFTP***) is a secure implementation of FTP. It is an extension of Secure Shell (SSH) using SSH to transmit the files in an encrypted format. SFTP transmits data using TCP port 22.
- **FTPS.** File Transfer Protocol Secure (***FTPS***) is an extension of FTP and uses TLS to encrypt FTP traffic. Some implementations of FTPS use TCP ports 989 and 990. However, TLS can also encrypt the traffic over the ports used by FTP (20 and 21). Notice that the difference between SFTP and FTPS is that SFTP uses SSH and FTPS uses TLS.

Remember this

Secure Shell (SSH) encrypts traffic over TCP port 22. Transport Layer Security (TLS) is a replacement for SSL and is used

to encrypt many different protocols. Secure FTP (SFTP) uses SSH to encrypt traffic. FTP Secure (FTPS) uses TLS to encrypt traffic.

SSL Versus TLS (Sidebar)

SSL has been compromised and is not recommended for use. In September 2014, a team at Google discovered a serious vulnerability with SSL that they nicknamed the POODLE attack. Poodle is short for Padding Oracle on Downgraded Legacy Encryption. The SSL protocol is not maintained or patched, so this vulnerability remains.

This is one of the reasons that the U. S. government and many other organizations prohibit the use of SSL to protect any sensitive data. For example, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations” specifically states that federal agencies should not use SSL.

TLS is the recommended replacement. While TLS can be used in almost any implementation that previously used SSL, the two aren’t the same protocol. Still, you will often see both SSL and TLS mentioned as if they are the same. Even the CompTIA objectives for the Security+ exam use “SSL/TLS” as if they are the same protocol.

The reason seems to be simply that people understand SSL. By lumping the topics together as SSL/TLS, many people understand the general purpose.

From a generic perspective, using the term SSL/TLS is effective at helping people understand the similarities. However, from a technical perspective, it’s important to realize that SSL is compromised and TLS should be used instead.

Email and Web Use Cases

Some common use cases related to email are send and receive email, send and receive secure email, and manage email folders. For the web, common use cases for internal employees are to provide access to the Internet and provide secure access to the Internet. Many organizations host web

servers and common use cases for these web servers are to provide access to web servers by external clients.

Many of these protocols support the use of STARTTLS. Instead of using one port to transmit data in cleartext and a second port to transmit data in ciphertext, the STARTTLS command allows the protocol to use the same port for both. Some common protocols used for email and the web include:

- **SMTP.** Simple Mail Transfer Protocol (SMTP) transfers email between clients and SMTP servers. SMTP uses TCP port 25. SMTP unofficially used port 465 with SSL and port 587 with TLS. However, it is now recommended that SMTP use STARTTLS to initialize a secure connection.
- **POP3 and Secure POP.** Post Office Protocol v3 (***POP3***) transfers emails from servers down to clients. POP3 uses TCP port 110. Secure POP3 encrypts the transmission with SSL or TLS and can use TCP port 995. However, STARTTLS is now recommended to create a secure connection on port 110.
- **IMAP4 and Secure IMAP.** Internet Message Access Protocol version 4 (***IMAP4***) is used to store email on an email server. IMAP4 allows a user to organize and manage email in folders on the server. As an example, Google Mail uses IMAP4. IMAP4 uses TCP port 143. IMAP4 with SSL or TLS can use TCP port 993, but STARTTLS is recommended using the same TCP port 143.
- **HTTP.** Hypertext Transfer Protocol (HTTP) transmits web traffic on the Internet and in intranets. Web servers use HTTP to transmit web pages to clients' web browsers. Hypertext Markup Language (HTML) is the common language used to display the web pages. HTTP uses TCP port 80.
- **HTTPS.** Hypertext Transfer Protocol Secure (***HTTPS***) encrypts web traffic to ensure it is secure while in transit. Web browsers commonly indicate that a secure session is using HTTPS by displaying a lock icon and by including HTTPS in the Uniform Resource Locator (URL) field. HTTPS is encrypted with either SSL or TLS and it uses TCP port 443.

Remember this

SMTP sends email on TCP port 25, POP3 receives email on port 110, and IMAP4 uses port 143. STARTTLS allows an

encrypted version of the protocol to use the same port as the unencrypted version. HTTP and HTTPS use ports 80 and 443 and transmit data over the Internet in unencrypted and encrypted formats, respectively.

Directory Services Use Case

Network operating systems commonly use a directory service to streamline management and implement security. A common use case is to provide secure access to the network. As an example, many organizations use Microsoft Active Directory Domain Services (AD DS). AD DS provides the means for administrators to create user objects for each authorized user and computer objects for each authorized computer. Administrators then use various methods within the directory service to enforce identification, authentication, and authorization methods.

Chapter 2, "Understanding Identity and Access Management," covers three relevant topics that help support this use case:

- **Kerberos.** Kerberos is the authentication protocol used in Windows domains and some Unix environments. It uses a Key Distribution Center (KDC) to issue timestamped tickets. Kerberos uses UDP port 88.
- **LDAP.** Lightweight Directory Access Protocol (***LDAP***) is the protocol used to communicate with directories such as AD DS. LDAP provides a clear syntax for object identification and management. LDAP uses TCP port 389. LDAP Secure (***LDAPS***) encrypts data with TLS using TCP port 636.
- **Group Policy.** Administrators use Group Policy Objects (***GPOs***) to configure settings. They can then apply these GPOs to users and computers within the domain.

Remote Access Use Cases

There are many situations where personnel need to access systems from remote locations. Some common use cases are remotely administer systems and remotely access desktops. For example, imagine a server room hosts hundreds of servers, including domain controllers for a Microsoft domain. If administrators need to create a user account or implement a change in a GPO, they would rarely go to the server room. Instead, they

access the server remotely and make the change from their desk computer.

Administrators often implement SSH (discussed in the "File Transfer Use Case" section) to meet a use case of supporting remote access. As an example, many Linux administrators use Netcat when connecting to remote systems for administration, and secure the Netcat transmissions with SSH. Chapter 8 covers Netcat in more depth, but you can check out the Chapter 3 labs for an introduction to Netcat.

Administrators and clients often use Remote Desktop Protocol (RDP) to connect to other systems from remote locations. Microsoft uses RDP in different solutions such as Remote Desktop Services and Remote Assistance. RDP uses either port TCP 3389 or UDP 3389, though TCP port 3389 is more common. A common reason why users are unable to connect to systems with RDP is that port 3389 is blocked on a host-based or network firewall. Another method of supporting remote access use cases is with a virtual private network (VPN). Chapter 4 discusses VPNs in more depth.

Remember this

Administrators connect to servers remotely using protocols such as Secure Shell (SSH) and the Remote Desktop Protocol (RDP). In some cases, administrators use virtual private networks to connect to remote systems.

Time Synchronization Use Case

There are many instances when systems need to be using the same time (or at least a time that is reasonably close). A common use case is to ensure systems have the accurate time. As an example, Kerberos requires all systems to be synchronized and be within five minutes of each other.

Within a Microsoft domain, one domain controller periodically uses the Windows Time service to locate a reliable Internet server running the Network Time Protocol (NTP). NTP is the most commonly used protocol for time synchronization, allowing systems to synchronize their time to within tens of milliseconds. Other domain controllers within the network periodically synchronize their time with the first domain controller. Last, all computers in the domain synchronize their time with one of these domain controllers. This process ensures all the computers have the accurate time.

The Simple NTP (SNTP) protocol can also be used for time synchronization. However, NTP uses complex algorithms and queries

multiple time servers to identify the most accurate time. SNTP does not use these algorithms, so it might not be as accurate as the result from NTP.

Network Address Allocation Use Case

Network address allocation refers to allocating IP addresses to hosts within your network. You can do so manually, but most networks use Dynamic Host Configuration Protocol (DHCP) to dynamically assign IP addresses to hosts. DHCP also assigns other TCP/IP information, such as subnet masks, default gateways, DNS server addresses, and much more. The following sections provide a review of some basic networking concepts.

IPv4

IPv4 uses 32-bit IP addresses expressed in dotted decimal format. For example, the IPv4 IP address of 192.168.1.5 is four decimals separated by periods or dots. You can also express the address in binary form with 32 bits.

All Internet IP addresses are public IP addresses, and internal networks use private IP addresses. Public IP addresses are tightly controlled. You can't just use any public IP address.

Instead, you must either purchase or rent it. Internet Service Providers (ISPs) purchase entire ranges of IP addresses and issue them to customers. If you access the Internet from home, you are very likely receiving a public IP address from an ISP.

Routers on the Internet include rules to drop any traffic that is coming from or going to a private IP address, so you cannot allocate private IP addresses on the Internet. RFC 1918 specifies the following private address ranges:

- **10.x.y.z.** 10.0.0.0 through 10.255.255.255
- **172.16.y.z–172.31.y.z.** 172.16.0.0 through 172.31.255.255
- **192.168.y.z.** 192.168.0.0 through 192.168.255.255

These are the only three IPv4 address ranges that you should allocate within a private network.

Remember this

Private networks should only have private IP addresses. These are formally defined in RFC 1918.

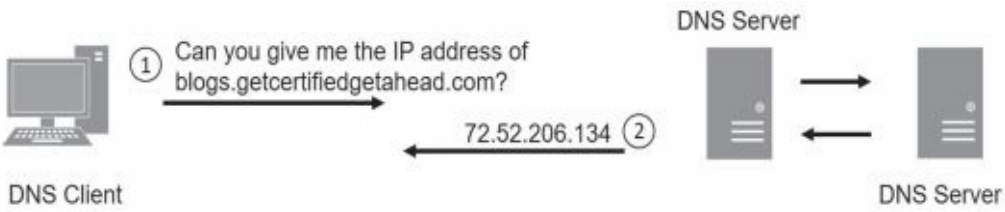
IPv6

Although the number of IP addresses at first seemed inexhaustible, the Internet Assigned Numbers Authority (IANA) assigned the last block of IPv4 addresses in February 2011. To prepare, the Internet Engineering Task Force (IETF) created IPv6, which provides a significantly larger address space than IPv4.

IPv6 uses 128-bit IP addresses expressed in hexadecimal format. For example, the IPv6 IP address of fe80:0000:0000:0000:02d4:3ff7:003f:de62 includes eight groups of four hexadecimal characters, separated by colons. Each hexadecimal character is composed of 4 bits.

Instead of private IP addresses, IPv6 uses unique local addresses. They are only allocated within private networks and not assigned to systems on the Internet. Unique local addresses start with the prefix of fc00.

Domain Name Resolution Use Case



The primary purpose of Domain Name System (***DNS***) is for domain name resolution. DNS resolves host names to IP addresses. Systems are constantly querying DNS, though it is usually transparent to users. Imagine that you want to visit *http://getcertifiedgetahead.com/.* You enter the URL into your web browser or click a link on a page and your system queries a DNS server for the site's IP address. Figure 3.2 shows what is occurring between your system and DNS. DNS uses UDP port 53 for these types of queries.

Figure 3.2: A basic DNS query

Sometimes, the DNS server you query knows the answer and just gives the response. Other times, it queries one or more other DNS servers to get the answer. When the DNS server queries other DNS servers, it puts the answer in its cache so that it doesn't have to do the same query again. Similarly, when clients receive answers from DNS servers, they store the answer in their cache so that they don't have to repeat the query.

DNS servers host data in zones, which you can think of as databases.

Zones include multiple records, such as the following:

- **A.** Also called a host record. This record holds the host name and IPv4 address and is the most commonly used record in a DNS server. A DNS client queries DNS with the name using a forward lookup request, and DNS responds with the IPv4 address from this record.
- **AAAA.** This record holds the host name and IPv6 address. It's similar to an A record except that it is for IPv6.
- **PTR.** Also called a pointer record. It is the opposite of an A record. Instead of a DNS client querying DNS with the name, the DNS client queries DNS with the IP address. When configured to do so, the DNS server responds with the name. PTR records are optional, so these reverse lookups do not always work.
- **MX.** Also called mail exchange or mail exchanger. An MX record identifies a mail server used for email. The MX record is linked to the A record or AAAA record of a mail server.
- **CNAME.** A canonical name, or alias, allows a single system to have multiple names associated with a single IP address. For example, a server named Server1 in the domain *getcertifiedgetahead.com* might have an alias of FileServer1 in the same domain.
- **SOA.** The start of authority (SOA) record includes information about the DNS zone and some of its settings. For example, it includes the TTL (Time to Live) settings for DNS records. DNS clients use the TTL setting to determine how long to cache DNS results. TTL times are in seconds and lower times cause clients to renew the records more often.

Most DNS servers on the Internet run Berkeley Internet Name Domain (BIND) software and run on Unix or Linux servers. Internal networks can use BIND, but in Microsoft networks, DNS servers commonly use the Microsoft DNS software.

Occasionally, DNS servers share information with each other in a process known as a zone transfer. In most cases, a zone transfer only includes a small number of updated records. However, some transfers include all the records in the zone. DNS servers use TCP port 53 for zone transfers. In contrast, name resolution queries use UDP port 53.

DNSSEC

One risk with DNS is ***DNS poisoning***, also known as DNS cache

poisoning. When successful, attackers modify the DNS cache with a bogus IP address. For example, imagine an attacker wants to send users to a malicious web site each time they want to go to *msn.com*. One way is to modify the A or AAAA record in the DNS cache for msn.com. Instead of sending users to the IP address used by msn.com, it will send users to the IP address of the malicious web site.

One of the primary methods of preventing DNS cache poisoning is with Domain Name System Security Extensions (***DNSSEC***). DNSSEC is a suite of extensions to DNS that provides validation for DNS responses. It adds a digital signature to each record that provides data integrity. If a DNS server receives a DNSSEC-enabled response with digitally signed records, the DNS server knows that the response is valid.

Remember this

DNS zones include records such as A records for IPv4 addresses and AAAA records for IPv6 addresses. DNS uses TCP port 53 for zone transfers and UDP port 53 for DNS client queries. Most Internet-based DNS servers run BIND software on Unix or Linux servers, and it's common to configure DNS servers to only use secure zone transfers. DNSSEC helps prevent DNS poisoning attacks. Nslookup and dig are two command-line tools used to test DNS. Microsoft systems include nslookup; Linux systems include dig.

Nslookup and Dig

Technicians use the ***nslookup*** command (short for name server lookup) to troubleshoot problems related to DNS. For example, you can use nslookup to verify that a DNS server can resolve specific host names or fully qualified domain names (FQDNs) to IP addresses. A fully qualified domain name includes the host name and the domain name.

The ***dig*** command-line tool has replaced the nslookup tool on Linux systems. It is sometimes referred to as domain information groper. You can use dig to query DNS servers to verify that the DNS server is reachable and to verify that a DNS server can resolve names to IP addresses. For example, these tools can verify that a DNS server has a host record that maps a host name to an IP address for a web server (or any host). Dig verifies DNS

functionality by querying DNS, verifying a record exists, and verifying that the DNS server responds.

Some versions of both commands support the @ symbol to identify a specific DNS server you want to query. This is useful if you want to pull all the records from a DNS zone. When doing this, you would use the any switch (indicating all records) or the axfr switch (short for all transfer). However, most DNS servers are configured to block these queries.

Check out the online resources for labs that show how to use these tools at *http://gcgapremium.com/501labs/.*

Subscription Services Use Case

Subscription services refer to a subscription-based business model. For example, instead of selling software applications to users, many vendors have moved to a subscription model where users pay over time.

As an example, years ago, it was common for people to purchase Microsoft Office for access to applications such as Microsoft Word, Microsoft Excel, Microsoft Outlook, and others. Today, organizations often pay monthly or annually for access to Office 365. This gives them the most current version of Microsoft Office products, along with additional features such as cloud storage.

The protocols used for subscription services use cases vary widely depending on the actual service. However, it's common for these to use HTTPS connections for security. Database servers maintain databases of customers, along with the products they're renting. The connections between web servers and database servers should be secure and might use HTTPS or TLS. When the subscription is nearing an end, systems send automated emails to customers using SMTP.

Understanding and Identifying Ports

Ports are logical numbers used by TCP/IP to identify what service or application should handle data received by a system. Both TCP and UDP use ports with a total of 65,536 TCP ports (0 to 65,535) and 65,536 UDP ports (0 to 65,535). Administrators open ports on firewalls and routers to allow the associated protocol into or out of a network. For example, HTTP uses port 80, and an administrator allows HTTP traffic by opening port 80.

Additionally, administrators disable unnecessary ports and services as part of a basic security practice. These ports and services are associated with specific protocols and if they are disabled, it blocks any attacks on these ports, services, and protocols.

The Internet Assigned Numbers Authority (IANA) maintains a list of official port assignments that you can view at *http://www.iana.org/assignments/port-numbers.* IANA divided the ports into three ranges, as follows:

- **Well-known ports: 0–1023.** IANA assigns port numbers to commonly used protocols in the well-known ports range.
- **Registered ports: 1024–49,151.** IANA registers these ports for companies as a convenience to the IT community. A single company may register a port for a proprietary use, or multiple companies may use the same port for a specific standard. As an example, Microsoft SQL Server uses port 1433 for database servers, Layer 2 Tunneling Protocol (L2TP) uses port 1701, and Point-to-Point Tunneling Protocol (PPTP) uses port 1723.
- **Dynamic and private ports: 49,152–65,535.** These ports are available for use by any application. Applications commonly use these ports to temporarily map an application to a port. These temporary port mappings are often called ephemeral ports, indicating that they are short lived.

Although virtually all the ports are subject to attack, most port attacks are against the well- known ports. Port scanners often simply check to see if a well-known port is open. For example, SMTP uses the well-known port 25, so if port 25 is open, the system is likely running SMTP.

Network administrators who regularly work with routers and firewalls can easily tell you which protocol is associated with which well-known port, such as 20, 21, 22, 23, 25, 80, or 443. The reason is that they use these ports to allow or block traffic.

For example, an administrator can close port 25 to block all SMTP traffic into a network. The router then ignores traffic on port 25 instead of forwarding it. Similarly, an administrator can close port 1433 to block database traffic to a Microsoft SQL server. On the other hand, the administrator can open port 25 to allow SMTP traffic.

Although ports are second nature to router and firewall administrators, they might not be so familiar to you. If you don’t work with the ports often,

you'll need to spend some extra time studying to ensure you're ready for the exam.

Combining the IP Address and the Port

At any moment, a computer could be receiving dozens of packets. Each of these packets includes a destination IP address and a destination port. TCP/IP uses the IP address to get the packet to the computer. The computer then uses the port number to get the packet to the correct service, protocol, or application that can process it.

For example, if the packet has a destination port of 80 (the well-known port for HTTP), the system passes the packet to the process handling HTTP. It wouldn't do much good to pass an SMTP email packet to the HTTP service or send an HTTP request packet to the SMTP service.

IP Address Used to Locate Hosts

Imagine that the IP address of *GetCertifiedGetAhead.com* is 72.52.206.134, and the address assigned to your computer from your ISP is 70.150.56.80. TCP/IP uses these IP addresses to get the packets from your computer to the web server and the web server's answer back to your computer.

There's a lot more that occurs under the hood with TCP/IP (such as DNS, NAT, and ARP), but the main point is that the server's IP address is used to get the requesting packet from your computer to the server. The server gets the response packets back to your computer using your IP address (or the IP address of your NAT server).

Server Ports

Different protocols are enabled and running on a server. These protocols have well-known or registered port numbers, such as port 22 for SSH, 25 for SMTP, 80 for HTTP, 443 for HTTPS, and so on. When the system receives traffic with a destination of port 80, the system knows to send it to the service handling HTTP.

Any web browser knows that the well-known port for HTTP is 80. Even though you don't see port 80 in the URL, it is implied as *http://GetCertifiedGetAhead.com**:80***. If you omit the port number, HTTP uses the well-known port number of 80 by default.

Popular web servers on the Internet include Apache and Internet Information Services (IIS). Apache is free and runs on Unix or Linux systems. Apache can also run on other platforms, such as Microsoft systems. IIS is included in Microsoft Server products. These web servers use port 80 for HTTP. When the server receives a packet with a destination port of 80, the server sends the packet to the web server application (Apache or IIS) that processes it and sends back a response.

Client Ports

TCP/IP works with the client operating system to maintain a table of client-side ports. This table associates port numbers with different applications that are expecting return traffic. Client-side ports start at port 49,152 and increment up to 65,535. If the system uses all the ports between 49,152 and 65,535 before being rebooted, it'll start over at 49,152.

When you use your web browser to request a page from a site, your system will record an unused client port number such as 49,152 in an internal table to handle the return traffic. When the web server returns the web page, it includes the client port as a destination port. When the client receives web page packets with a destination port of 49,152, it sends these packets to the web browser application. The browser processes the packets and displays the page.

Putting It All Together

The previous section described the different pieces, but it's useful to put this together into a single description. Imagine that you decide to visit the web site *http://GetCertifiedGetAhead.com* using your web browser so you type the URL into the browser, and the web page appears. Here are the details of what is happening. Figure 3.3 provides an overview of how this will look and the following text explains the process.

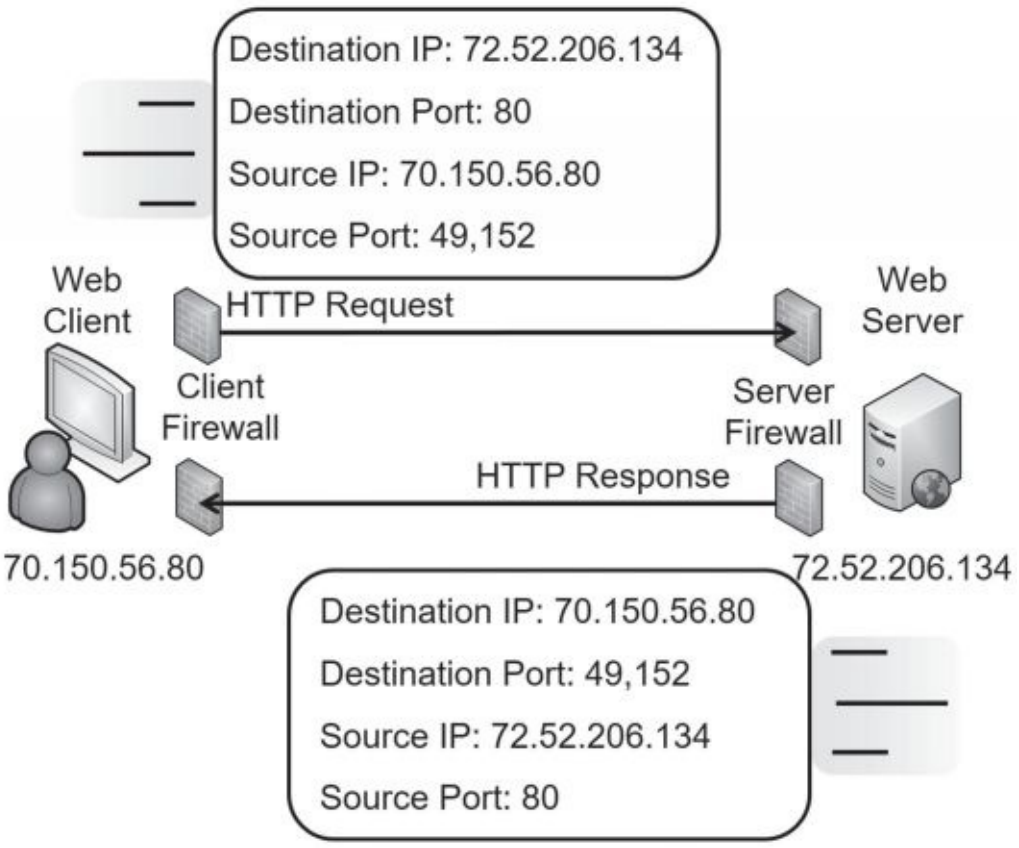


Figure 3.3: Using source and destination ports

Your computer creates a packet with source and destination IP addresses and source and destination ports. It queries a DNS server for the IP address of *GetCertifiedGetAhead.com* and learns that the IP address is 72.52.206.134. Additionally, your computer will use its IP address as the source IP address. For this example, imagine your computer's IP address is 70.150.56.80.

Because the web server is serving web pages using HTTP and the well-known port is used, the destination port is 80. Your computer will identify an unused port in the dynamic and private ports range (a port number between 49,152 and 65,535) and map that port to the web browser. For this example, imagine it assigns 49,152 to the web browser. It uses this as the source port.

At this point, the packet has both destination and source data as follows:

- Destination IP address: 72.52.206.134 (the web server)
- Destination port: 80
- Source IP address: 70.150.56.80 (your computer)

- Source port: 49,152

TCP/IP uses the IP address (72.52.206.134) to get the packet to the *GetCertifiedGetAhead* web server. When it reaches the web server, the server looks at the destination port (80) and determines that the packet needs to go to the web server program servicing HTTP. The web server creates the page and puts the data into one or more return packets. At this point, the source and destinations are swapped because the packet is coming from the server back to you:

Comparing Ports and Protocol Numbers (Sidebar)

Ports and protocol numbers are not the same thing, though they are often confused. Well-known ports identify many services or protocols, as discussed previously.

However, many protocols aren't identified by the port, but instead by the protocol numbers. For example, within IPsec, protocol number 50 indicates the packet is an Encapsulating Security Payload (ESP) packet, and protocol number 51 indicates it's an Authentication Header (AH) packet. Similarly, ICMP has a protocol number of 1, TCP is 6, and UDP is 17.

You can use a protocol number to block or allow traffic on routers and firewalls just as you can block or allow traffic based on the port. Note that it is not accurate to say that you can allow IPsec ESP traffic by opening port 50. IANA lists port 50 as a Remote Mail Checking Protocol. However, you can allow IPsec traffic by allowing traffic using protocol number 50. Protocol analyzers can capture and examine IP headers to determine the protocol number and the port, as well as read any unencrypted data. Note that you might see the protocol number listed as the protocol ID or a protocol identifier. Chapter 8 covers protocol analyzers in more depth.

- Destination IP address: 70.150.56.80 (your computer)
- Destination port: 49,152
- Source IP address: 72.52.206.134 (the web server)
- Source port: 80

Again, TCP/IP uses the IP address to get the packets to the destination, which is your computer at this point. Once the packets reach your system, it sees that port 49,152 is the destination port. Because your system mapped this port to your web browser, it sends the packets to the web browser, which displays the web page.

The Importance of Ports in Security

Routers, and the routing component of firewalls, filter packets based on IP addresses, ports, and some protocols such as ICMP or IPsec. Because many protocols use well-known ports, you can control protocol traffic by allowing or blocking traffic based on the port.

In the previous example, the client firewall must allow outgoing traffic on port 80. Firewalls automatically determine the client ports used for return traffic, and if they allow the outgoing traffic, they allow the return traffic. In other words, because the firewall allows the packet going to the web server on the destination port 80, it also allows the web page returning on the dynamic source port of 49,152.

Note that the client firewall doesn't need to allow incoming traffic on port 80 for this to work. The web client isn't hosting a web server with HTTP, so the client firewall would block incoming traffic on port 80. However, the firewall that is filtering traffic to the web server needs to allow incoming traffic on port 80.

You can apply this same principle for any protocol and port. For example, if you want to allow SMTP traffic, you create a rule on the firewall to allow traffic on port 25. IT professionals modifying access control lists (ACLs) on routers and firewalls commonly refer to this as opening a port to allow traffic or closing a port to block traffic.

Understanding Basic Network Devices

Networks connect computing devices together so that users can share resources, such as data, printers, and other devices. Any device with an IP address is a host, but you'll often see them referred to as clients or nodes.

A common use case for a switch is to connect hosts together within a network. A common use case for a router is to connect multiple networks together to create larger and larger networks.

When discussing the different network devices, it's important to remember the primary methods IPv4 uses when addressing TCP/IP traffic:

- **Unicast.** One-to-one traffic. One host sends traffic to another host, using a destination IP address. The host with the destination IP address will process the packet. Most other hosts will see the packet, but because it isn't addressed to them, they will not process it.
- **Broadcast.** One-to-all traffic. One host sends traffic to all other hosts on the subnet, using a broadcast address such as 255.255.255.255. Every host that receives broadcast traffic will process it. Switches pass broadcast traffic between their ports, but routers do not pass broadcast traffic.

Switches

A ***switch*** can learn which computers are attached to each of its physical ports. It then uses this knowledge to create internal switched connections when two computers communicate with each other.

Consider Figure 3.4. When the switch turns on, it starts out without any knowledge other than knowing it has four physical ports. Imagine that the first traffic is the beginning of a TCP/IP conversation between Lisa's computer and Homer's computer.

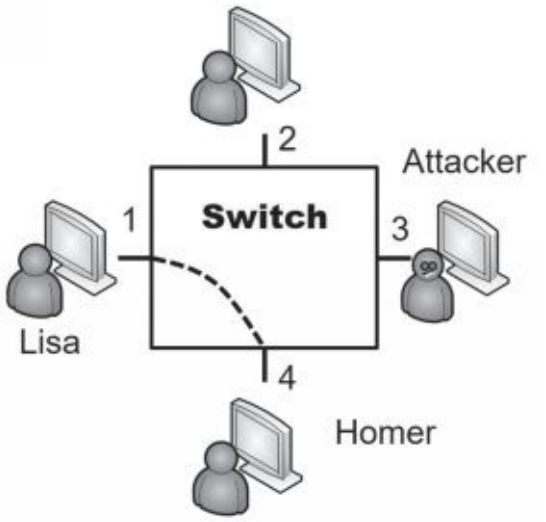


Figure 3.4: Switch

When Lisa's computer sends the first packet, it includes the MAC address of the destination computer. However, because the switch doesn't know which port Homer's computer is connected to, it forwards this first packet to all the ports on the switch.

Included in that first packet is the MAC address of Lisa's computer. The switch logs this information into an internal table. It then directs any future traffic addressed to Lisa's MAC address to port 1, and port 1 only.

When Homer's computer receives the packet, it responds. Embedded in this return packet is the MAC address of Homer's computer. The switch captures Homer's MAC address and logs it with port 4 in the internal table. From here on, any unicast traffic between Lisa's and Homer's computers is internally switched between only ports 1 and 4. Switches will internally switch unicast traffic. However, they pass broadcast traffic to all ports.

Security Benefit of a Switch

Most of the previous discussion is basic networking, but what you really need to know is why it's relevant in security. If an attacker installed a protocol analyzer on a computer attached to another port (such as port 3 in Figure 3.4), the protocol analyzer would not capture unicast traffic going through the switch to other ports. If Lisa and Homer are exchanging data on ports 1 and 4, none of the traffic reaches port 3. The protocol analyzer can't capture traffic that doesn't reach the port.

In contrast, if the computers were connected with a simple hub, the

attacker could capture it because unicast traffic goes to all ports on a hub. This is the main security reason why organizations replace hubs with switches. The switch reduces the risk of an attacker capturing data with a protocol analyzer. Of course, switches also increase the efficiency of a network.

Port Security

Port security limits the computers that can connect to physical ports on a switch. At the most basic level, administrators disable unused ports. For example, individual RJ-45 wall jacks in an office lead to specific physical ports on a switch. If the wall jack is not being used, administrators can disable the switch port. This prevents someone from plugging in a laptop or other computer into the wall jack and connecting to the network.

MAC address filtering is another example of port security. In a simple implementation, the switch remembers the first one or two MAC addresses that connect to a port. It then blocks access to systems using any other MAC addresses. You can also manually configure each port to accept traffic only from a specific MAC address. This limits each port's connectivity to a specific device using this MAC address. This can be very labor intensive, but it provides a higher level of security.

Remember this

Port security includes disabling unused ports and limiting the number of MAC addresses per port. A more advanced implementation is to restrict each physical port to only a single specific MAC address.

Physical Security of a Switch

Many switches have a console port that administrators can use to monitor all traffic. Unlike the normal ports that only see traffic specifically addressed to the port, the monitoring port will see all traffic in or out of the switch. This includes any unicast traffic the switch is internally switching between two regular ports. The monitoring port is useful for legitimate troubleshooting, but if the switch isn't protected with physical security, it can also be useful to an attacker.

Physical security protects a switch by keeping it in a secure area such

as in a locked wiring closet. Physical security ensures that attackers don't have physical access to the switch and other network devices.

Loop Prevention

In some situations, a network can develop a switching loop or bridge loop problem. The effect is similar to a broadcast storm and it can effectively disable a switch. For example, if a user connects two ports of a switch together with a cable, it creates a switching loop where the switch continuously sends and resends unicast transmissions through the switch. In addition to disabling the switch, it also degrades performance of the overall network.

This is trivial for many network administrators, because most current switches have Spanning Tree Protocol (***STP***) or the newer Rapid STP (***RSTP***) installed and enabled for ***loop prevention***. However, if these protocols are disabled, the switch is susceptible to loop problems. The simple solution is to ensure that switches include loop protection such as STP or RSTP.

Spanning Tree Protocol also protects the network against potential attackers. For example, imagine an attacker visits a conference room and has access to RJ-45 wall jacks. If loop protection isn't enabled, he can connect two jacks together with a cable, slowing network performance down to a crawl.

Remember this

Loop protection such as STP or RSTP is necessary to protect against switching loop problems, such as those caused when two ports of a switch are connected together.

Flood Attacks and Flood Guards

A MAC flood attack attempts to overload a switch with different MAC addresses associated with each physical port. You typically have only one device connected to any physical port. During normal operation, the switch's internal table stores the MAC address associated with this device and maps it to the port. In a MAC flood attack, an attacker sends a large amount of traffic with spoofed MAC addresses to the same port.

At some point in a MAC flood attack, the switch runs out of memory to

store all the MAC addresses and enters a fail-open state. Instead of working as a switch, it begins operating as a simple hub. Traffic sent to any port of the switch is now sent to all other switch ports. At this point, the attacker can connect a protocol analyzer to any port and collect all the traffic sent through the switch.

Many switches include a ***flood guard*** to protect against MAC flood attacks. When enabled, the switch will limit the amount of memory used to store MAC addresses for each port. For example, the switch might limit the number of entries for any port to 132 entries. This is much more than you need for normal operation. If the switch detects an attempt to store more than 132 entries, it raises an alert.

The flood guard typically sends a Simple Network Management Protocol (SNMP) trap or error message in response to the alert. Additionally, it can either disable the port or restrict updates for the port. By disabling the port, it effectively blocks all traffic through the port until an administrator intervenes. If it restricts updates, the switch will use currently logged entries for the port, but ignore attempts to update it. All other ports will continue to operate normally.

Another flood guard supported by some switches is a setting for the maximum number of MACs supported by a port. Most ports will typically have this set to 1 to support only a single MAC address. However, consider a virtual machine (VM) running within a physical host. If the VM is set to bridged, it can access the network using the physical host's NIC, but with the MAC address of the VM. In this scenario, the Maximum MAC setting should be set to 2.

Comparing Ports and Ports (Sidebar)

Note that a physical port used by a network device, such as a switch or a router, is completely different from the logical ports discussed previously. You plug a cable into a physical port. A logical port is a number embedded in a packet and identifies services and protocols.

This is like minute (60 seconds) and minute (tiny), or like the old joke about the meaning of *secure*. The Secretary of Defense directed members of different services to "secure that building." Navy personnel turned off the lights and locked the doors. The Army

occupied the building and ensured no one could enter. The Marines attacked it, captured it, and set up defenses to hold it. The Air Force secured a two-year lease with an option to buy.

Routers

A ***router*** connects multiple network segments together into a single network and routes traffic between the segments. As an example, the Internet is effectively a single network hosting billions of computers. Routers route the traffic from segment to segment.

Because routers don't pass broadcasts, they effectively reduce traffic on any single segment. Segments separated by routers are sometimes referred to as broadcast domains. If a network has too many computers on a single segment, broadcasts can result in excessive collisions and reduce network performance. Moving computers to a different segment separated by a router can significantly improve overall performance. Similarly, subnetting networks creates separate broadcast domains.

Cisco routers are popular, but many other brands exist. Most routers are physical devices, and physical routers are the most efficient. However, it's also possible to add routing software to computers with more than one NIC. For example, Windows Server products can function as routers by adding additional services to the server.

Routers and ACLs

Access control lists (***ACLs***) are rules implemented on a router (and on firewalls) to identify what traffic is allowed and what traffic is denied. Rules within an ACL provide rule-based management for the router and control inbound and outbound traffic.

Router ACLs provide basic packet filtering. They filter packets based on IP addresses, ports, and some protocols, such as ICMP or IPsec, based on the protocol identifiers:

- **IP addresses and networks.** You can add a rule in the ACL to block access from any single computer based on the IP address. If you want to block traffic from one subnet to another, you can use a rule to block traffic using the subnet IDs. For example, the Sales department may be in the 192.168.1.0/24 network and the Accounting department

may be in the 192.168.5.0/24 network. You can ensure traffic from these two departments stays separate with an ACL on a router.

- **Ports.** You can filter traffic based on logical ports. For example, if you want to block HTTP traffic, you can create a rule to block traffic on port 80. Note that you can choose to block incoming traffic, outgoing traffic, or both. In other words, it's possible to allow outgoing HTTP traffic while blocking incoming HTTP traffic.
- **Protocol numbers.** Many protocols are identified by their protocol numbers. For example, ICMP uses a protocol number of 1 and many DoS attacks use ICMP. You can block all ICMP traffic (and the attacks that use it) by blocking traffic using this protocol number. Many automated intrusion prevention systems (IPSs) dynamically block ICMP traffic in response to attacks. Similarly, you can restrict traffic to only packets encrypted with IPsec ESP using a rule that allows traffic using protocol number 50, but blocks all other traffic. PPTP uses protocol number 47 and can be allowed by allowing traffic using protocol ID 47.

Implicit Deny

Implicit deny is an important concept to understand, especially in the context of ACLs. It indicates that all traffic that isn't explicitly allowed is implicitly denied. For example, imagine you configure a router to allow Hypertext Transfer Protocol (HTTP) to a web server. The router now has an explicit rule defined to allow this traffic to the server. If you don't define any other rules, the implicit deny rule blocks all other traffic. Firewalls (discussed later in this chapter) also use an implicit deny rule.

The implicit deny rule is the last rule in an ACL. Some devices automatically apply the implicit deny rule as the last rule. Other devices require an administrator to place the rule at the end of the ACL manually. Syntax of an implicit deny rule varies on different systems, but it might be something like DENY ANY ANY, or DENY ALL ALL, where both ANY and ALL refer to any type of traffic.

Antispoofing

Attackers often use spoofing to impersonate or masquerade as someone or something else. In the context of routers, an attacker will spoof the source

IP address by replacing the actual source IP address with a different one. This is often done to hide the actual source of the packet. You can implement ***antispoofing*** on a router by modifying the access list to allow or block IP addresses. As an example, private IP addresses (listed earlier in this chapter) should only be used in private networks. Any traffic coming from the Internet using a private IP address as the source IP address is obviously an attempt to spoof the source IP address. The following three rules would be implemented on a router (though the syntax may be different on various routers for antispoofing):

- deny ip 10.0.0.0 0.255.255.255 any
- deny ip 172.16.0.0 0.15.255.255 any
- deny ip 192.168.0.0 0.0.255.255 any

Notice that the subnet mask portion of these rules is shown a little differently, but this is common syntax for many router rules. For example, 10.0.0.0 0.255.255.255 covers all the IP addresses in the range of 10.0.0.0 through 10.255.255.255.

Remember this

Routers and stateless firewalls (or packet-filtering firewalls) perform basic filtering with an access control list (ACL). ACLs identify what traffic is allowed and what traffic is blocked. An ACL can control traffic based on networks, subnets, IP addresses, ports, and some protocols. Implicit deny blocks all access that has not been explicitly granted. Routers and firewalls use implicit deny as the last rule in the access control list. Antispoofing methods block traffic using ACL rules.

Bridge

A network ***bridge*** connects multiple networks together and can be used instead of a router in some situations. As discussed previously, a router directs network traffic based on the destination IP address and a switch directs traffic to specific ports based on the destination MAC address. Similarly, a bridge directs traffic based on the destination MAC address. Figure 3.5 shows all three devices in a simplified network diagram.

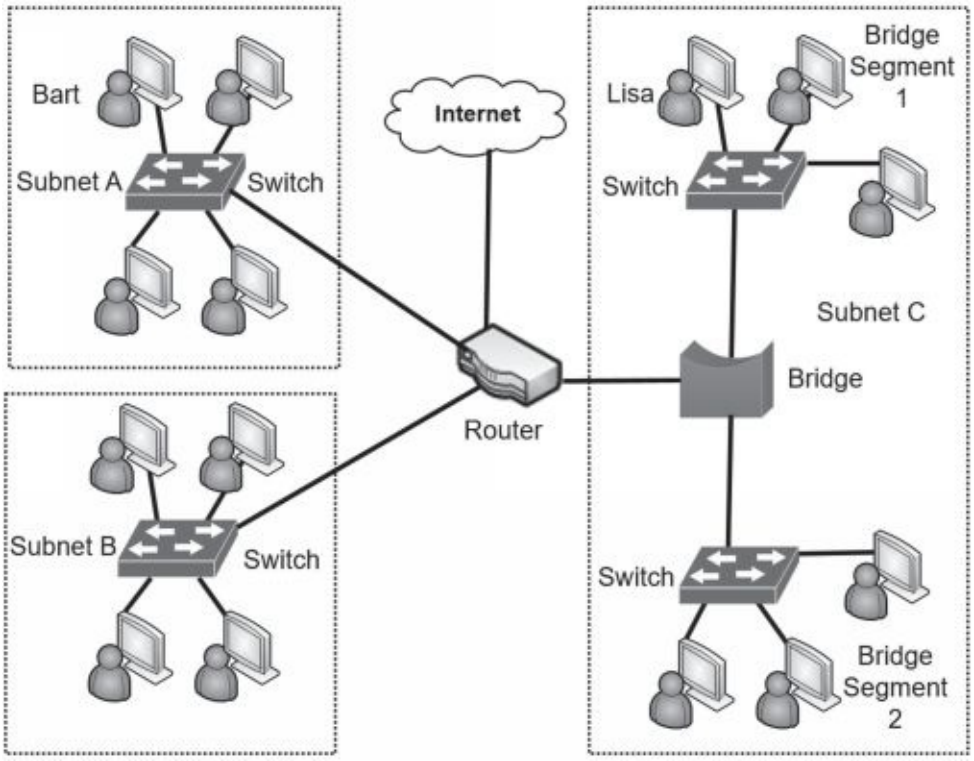


Figure 3.5: Network with a router, switches, and a bridge

Notice that there are three subnets (Subnet A, Subnet B, and Subnet C). The router directs traffic to each of these subnets. Subnet C has two segments separated by a bridge. The bridge sends traffic to the appropriate segment in Subnet C based on the MAC address.

A bridge typically learns MAC addresses in different bridge networks by analyzing traffic. This is similar to how a switch learns which MAC addresses are associated with each physical port. Imagine that Bart (in Subnet A) sends traffic to Lisa (in Subnet C). When the bridge receives the traffic, it doesn't know if Lisa's MAC address is in Bridge Segment 1 or Bridge Segment 2, so it sends the traffic to both bridge networks. When Lisa's computer replies, the bridge identifies her MAC address as being in Bridge Network 1 and stores this information in an internal table. When Bart sends other traffic to Lisa, the bridge forwards it to Bridge Segment 1 only.

A hardware bridge using this learning method is relatively easy to install. Connect the wires, turn it on, and it will begin learning.

Aggregation Switch

An ***aggregation switch*** connects multiple switches together in a network. Aggregate simply means that you are creating something larger from smaller elements. As an example, look back at Figure 3.5. If you replace the bridge with a switch, the switch is an aggregation switch.

Similarly, you can use an aggregation switch to connect Subnet A and Subnet B. The switches in Subnet A and Subnet B connect to the aggregation switch instead of connecting to the router. The aggregation switch connects to the router. This reduces the number of ports used in the router.

It's common to place an aggregation switch in the same location as you'd place routers. For example, large organizations locate network devices in the data center while smaller organizations locate them in a wiring closet. Both are secured using physical security.

Firewalls

A ***firewall*** filters incoming and outgoing traffic for a single host or between networks. In other words, a firewall can ensure only specific types of traffic are allowed into a network or host, and only specific types of traffic are allowed out of a network or host.

The purpose of a firewall in a network is similar to a firewall in a car. The firewall in a car is located between the engine and passenger compartment. If a fire starts in the engine compartment, the firewall provides a layer of protection for passengers in the passenger compartment. Similarly, a firewall in a network will try to keep the bad traffic (often in the form of attackers) out of the network.

Of course, an engine has a lot of moving parts that can do damage to people if they accidentally reach into it while it's running. The firewall in a car protects passengers from touching any of those moving parts. Similarly, a network can also block users from going to places that an administrator deems dangerous. For example, uneducated users could inadvertently download damaging files, but many firewalls can block potentially malicious downloads.

Firewalls start with a basic routing capability for packet filtering as described in the "Routers and ACLs" section, including the use of an implicit deny rule. More advanced firewalls go beyond simple packet filtering and include advanced content filtering.

Host-Based Firewalls

A host-based firewall monitors traffic going in and out of a single host, such as a server or a workstation. It monitors traffic passing through the NIC and can prevent intrusions into the computer via the NIC. Many operating systems include software-based firewalls used as host- based firewalls. For example, Microsoft has included a host-based firewall on operating systems since Windows XP. Additionally, many third-party host-based firewalls are available.

Figure 3.6 shows the host-based Windows Firewall on Windows 10. Notice that you can configure inbound rules to allow or restrict inbound traffic and outbound rules to allow or restrict outbound traffic. The connection security rules provide additional capabilities, such as configuring an IPsec connection in Tunnel or Transport mode to encrypt the traffic.

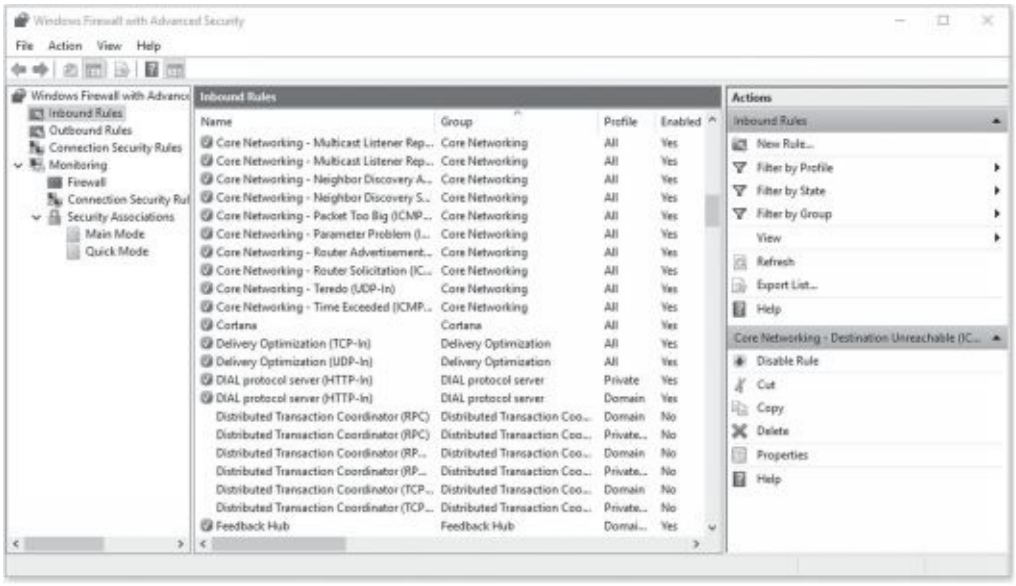


Figure 3.6: Windows Firewall with Advanced Security on Windows 10

Linux systems support iptables and many additions to iptables, such as ipv6tables, arptables, and so on. Generically, administrators commonly refer to these as xtables. You can configure rules within different tables. Combined, these rules work just like an ACL.

Personal firewalls provide valuable protection for systems against unwanted intrusions. Many organizations use personal firewalls on each system in addition to network firewalls as part of an overall defense-in-depth

strategy.

It's especially important to use personal firewalls when accessing the Internet in a public place. Free Wi-Fi Internet access is often available in public places, such as airports, hotels, and many fast-food establishments, such as Starbucks and McDonald's. However, connecting to a public Wi-Fi hot spot without the personal firewall enabled is risky, and never recommended.

Remember this

Host-based firewalls provide protection for individual hosts, such as servers or workstations. A host-based firewall provides intrusion protection for the host. Linux systems support xtables for firewall capabilities. Network-based firewalls are often dedicated servers or appliances and provide protection for the network.

Application-Based Versus Network-Based Firewalls

An application-based firewall is typically software running on a system. For example, host- based firewalls are commonly application-based. A network-based firewall is usually a dedicated system with additional software installed to monitor, filter, and log traffic. For example, Cisco makes a variety of different network-based firewalls. Many of them are dedicated servers with proprietary firewall software installed.

A network-based firewall would have two or more network interface cards (NICs) and all traffic passes through the firewall. The firewall controls traffic going in and out of a network. It does this by filtering traffic based on firewall rules and allows only authorized traffic to pass through it. Most organizations include at least one network-based firewall at the border, between their intranet (or internal network) and the Internet.

Stateless Firewall Rules

Stateless firewalls use rules implemented as ACLs to identify allowed and blocked traffic. This is similar to how a router uses rules. Firewalls use an implicit deny strategy to block all traffic that is not explicitly allowed. Although rules within ACLs look a little different depending on what hardware you're using, they generally take the following format:

Permission Protocol Source Destination Port

- **Permission.** You'll typically see this as PERMIT or ALLOW allowing the traffic. Most systems use DENY to block the traffic.
- **Protocol.** Typically, you'll see TCP or UDP here, especially when blocking specific TCP or UDP ports. If you want to block both TCP and UDP traffic using the same port, you can use IP instead. Using ICMP here blocks ICMP traffic, effectively blocking ping and some other diagnostics that use ICMP.
- **Source.** Traffic comes from a source IP address. You identify an IP address to allow or block traffic from a single computer, or from a range of IP addresses, such as from a single subnet. Wildcards such as any or all include all IP addresses.
- **Destination.** Traffic is addressed to a destination IP address. You identify an IP address to allow or block traffic to a single computer, or to a range of IP addresses, such as to an entire subnet. Wildcards such as any or all include all IP addresses.
- **Port or protocol.** Typically, you'll see the well-known port such as port 80 for HTTP. However, some devices support codes such as www for HTTP traffic. Some systems support the use of keywords such as eq for equal, lt for less than, and gt for greater than. For example, instead of just using port 80, it might indicate eq 80.

Some firewalls require you to include a subnet mask in the rule. For example, if you want to block all SMTP traffic to the 192.168.1.0/24 network, you would use an IP address of 192.168.1.0 and a subnet mask of 255.255.255.0. However, if you only wanted to allow SMTP traffic to a single computer with the IP address of 192.168.1.20/24, you would use an IP address of 192.168.1.20 and a subnet mask of 255.255.255.255.

Remember this

Firewalls use a deny any any, deny any, or a drop all statement at the end of the ACL to enforce an implicit deny strategy. The statement forces the firewall to block any traffic that wasn't previously allowed in the ACL. The implicit deny strategy provides a secure starting point for a firewall.

Stateful Versus Stateless

A stateful firewall inspects traffic and makes decisions based on the

context, or state, of the traffic. It keeps track of established sessions and inspects traffic based on its state within a session. It blocks traffic that isn't part of an established session. As an example, a TCP session starts with a three-way handshake. If a stateful firewall detects TCP traffic without a corresponding three-way handshake, it recognizes this as suspicious traffic and can block it.

A common security issue with stateless firewalls is misconfigured ACLs. For example, if the ACL doesn't include an implicit deny rule, it can allow almost all traffic into the network.

Web Application Firewall

A ***web application firewall (WAF)*** is a firewall specifically designed to protect a web application, which is commonly hosted on a web server. In other words, it's placed between a server hosting a web application and a client. It can be a stand-alone appliance, or software added to another device.

As an example, an organization may host an e-commerce web site to generate revenue. The web server will be placed within a demilitarized zone (DMZ) (discussed later in this chapter), but due to the data that the web server handles, it needs more protection. A successful attack may be able to take the web server down, and allow an attacker to access or manipulate data.

Note that you wouldn't use a WAF in place of a network-based firewall. Instead, it provides an added layer of protection for the web application in addition to a network-based firewall.

Remember this

A stateless firewall blocks traffic using an ACL. A stateful firewall blocks traffic based on the state of the packet within a session. Web application firewalls provide strong protection for web servers. They protect against several different types of attacks, with a focus on web application attacks and can include load-balancing features.

Implementing a Secure Network

There are several elements of a secure network, including the implementation of different zones and topologies, segmenting and isolating some elements, and using various network devices. This section covers these

topics in more depth.

Zones and Topologies

Most networks have Internet connectivity, but it's rare to connect a network directly to the Internet. Instead, it's common to divide the network into different zones, using different topologies. Two terms that are relevant here are:

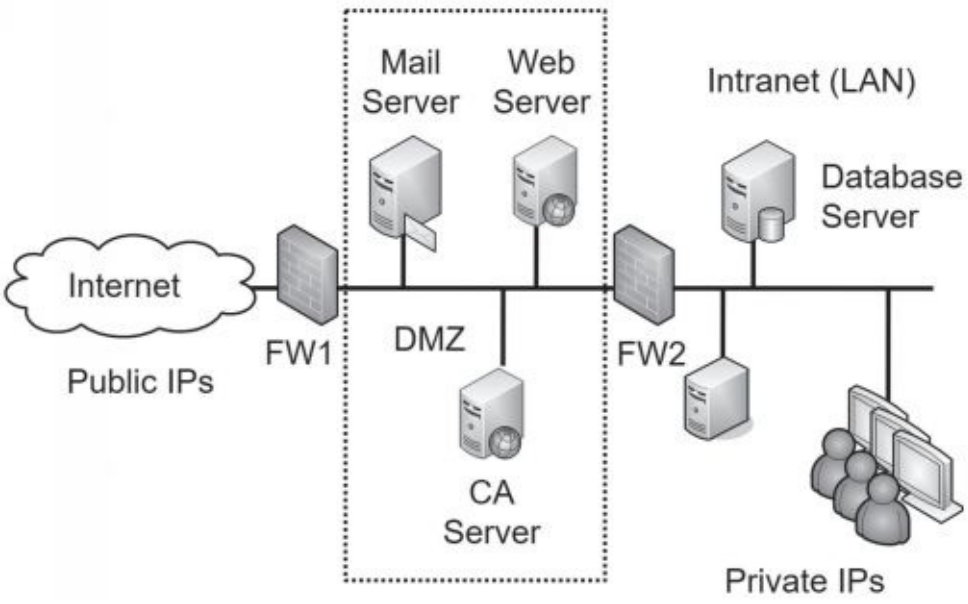
- **Intranet.** An ***intranet*** is an internal network. People use the intranet to communicate and share content with each other. While it's common for an intranet to include web servers, this isn't a requirement.
- **Extranet.** An ***extranet*** is part of a network that can be accessed by authorized entities from outside of the network. For example, it's common for organizations to provide access to authorized business partners, customers, vendors, or others.

The network perimeter provides a boundary between the intranet and the Internet.

Boundary protection includes multiple methods to protect the network perimeter.

DMZ

The demilitarized zone (***DMZ***) is a buffered zone between a private network and the Internet. Attackers seek out servers on the Internet, so any server placed directly on the Internet has the highest amount of risk. However, the DMZ provides a layer of protection for these Internet-facing servers, while also allowing clients to connect to them.



As an example, Figure 3.7 shows a common network configuration with a DMZ. The DMZ is the area between the two firewalls (FW1 and FW2) and hosts several Internet-facing servers. Many DMZs have two firewalls, creating a buffer zone between the Internet and the internal network, as shown in Figure 3.7, though other DMZ configurations are possible.

Figure 3.7: Network with DMZ

In this configuration, one firewall separates the DMZ from the Internet. The second firewall separates the DMZ from the internal network. Each firewall includes detailed rules designed to filter traffic and protect both the internal network and the public servers. One way of saying this is that the DMZ provides access to the services hosted in the DMZ, while segmenting access to the internal network.

For example, FW1 can have rules to allow traffic to the servers in the DMZ, but block unsolicited traffic to FW2. The mail server would send and receive email to other email servers on the Internet through port 25 of FW1, and also send and receive email to internal clients through port 25 on FW2. The web server hosts web pages to any Internet users through ports 80 and 443 on FW1, but FW2 blocks incoming traffic using these ports. The Certificate Authority (CA) server validates certificates for Internet clients by answering through FW1.

Notice in Figure 3.7 that the intranet includes a database server. The web server may use this to create web pages for an e-commerce site. It could

hold product data, customer data, and much more. FW2 allows traffic between the web server (and only the web server) and the database server on port 1433. FW2 would block all other Internet traffic to the database server.

It's also possible for the web server and the database server to be part of an extranet. For example, imagine that the web server hosts a site that business partners can use to place orders. The web server would first authenticate them before granting them full access. After users log on, the web site connects to the back-end database server, allowing them to browse the inventory

and place orders. Because this site is only for authorized business partners, it is an extranet.

The DMZ can host any Internet-facing server, not just those shown in the figure. Other examples include FTP servers used for uploading and downloading files and virtual private network (VPN) servers used for providing remote access.

Remember this

A DMZ is a buffer zone between the Internet and an internal network. It allows access to services while segmenting access to the internal network. In other words, Internet clients can access the services hosted on servers in the DMZ, but the DMZ provides a layer of protection for the intranet (internal network).

Understanding NAT and PAT

Network Address Translation (***NAT***) is a protocol that translates public IP addresses to private IP addresses and private addresses back to public. You'll often see NAT enabled on an Internet-facing firewall. A commonly used form of NAT is network address and port translation, commonly called Port Address Translation (PAT).

If you run a network at your home (such as a wireless network), the router that connects to the Internet is very likely running NAT. Some of the benefits of NAT include:

- **Public IP addresses don't need to be purchased for all clients.** A home or company network can include multiple computers that can access the Internet through one router running NAT. Larger companies requiring more bandwidth may use more than one public

IP address.

- **NAT hides internal computers from the Internet.** Computers with private IP addresses are isolated and hidden from the Internet. NAT provides a layer of protection to these private computers because they aren't as easy to attack and exploit from the Internet.

One of the drawbacks to NAT is that it is not compatible with IPsec. You can use IPsec to create VPN tunnels and use it with L2TP to encrypt VPN traffic. Although there are ways of getting around NAT's incompatibility with IPsec, if your design includes IPsec going through NAT, you'll need to look at it closely.

NAT can be either static NAT or dynamic NAT:

- **Static NAT.** Static NAT uses a single public IP address in a one-to-one mapping. It maps a private IP address with a single public IP address.
- **Dynamic NAT.** Dynamic NAT uses multiple public IP addresses in a one-to-many mapping. Dynamic NAT decides which public IP address to use based on load. For example, if several users are connected to the Internet on one public IP address, NAT maps the next request to a less-used public IP address.

Remember this

NAT translates public IP addresses to private IP addresses, and private IP addresses back to public. A common form of NAT is Port Address Translation. Dynamic NAT uses multiple public IP addresses while static NAT uses a single public IP address.

Network Separation

A common network security practice is to use different components to provide network separation. The CompTIA objectives list these as segregation, segmentation, and isolation. Segregation provides basic separation, segmentation refers to putting traffic on different segments, and isolation indicates the systems are completely separate. Chapter 1 covers virtualization concepts in depth and virtualization can be used to provide isolation. For example, some antivirus experts use virtual machines to analyze malware. This section covers physical security and logical security methods used for isolation.

Physical Isolation and Airgaps

Physical isolation ensures that a network isn't connected to any other network. As an example, consider supervisory control and data acquisition (SCADA) systems. These are typically industrial control systems within large facilities such as power plants or water treatment facilities. While SCADA systems operate within their own network, it's common to ensure that they are isolated from any other network.

This physical isolation significantly reduces risks to the SCADA system. If an attacker can't reach it from the Internet, it is much more difficult to attack it. However, if the system is connected to the internal network, it's possible for an attacker to gain access to internal computers, and then access any resource on the internal network.

An ***airgap*** is a metaphor for physical isolation, indicating that there is a gap of air between an isolated system and other systems. When considered literally, an air-gapped system is not connected to any other systems. As an example, many organizations use both classified (red) and unclassified (black) networks. Strict rules ensure that these two systems are not connected to each other. Some rules require that any cable from a red network must be physically separated from black network cables.

Logical Separation and Segmentation

As mentioned previously in this chapter, routers and firewalls provide a basic level of separation and segmentation. Routers segment traffic between networks using rules within ACLs. Administrators use subnetting to divide larger IP address ranges into smaller ranges. They then implement rules within ACLs to allow or block traffic. Firewalls separate network traffic using basic packet-filtering rules and can also use more sophisticated methods to block undesirable traffic.

It's also possible to segment traffic between logical groups of users or computers with a virtual local area network (VLAN). This provides logical separation.

Comparing a Layer 2 Versus Layer 3 Switch

A traditional switch operates on Layer 2 of the Open Systems Interconnection (OSI) model. As discussed previously, a traditional switch (a

Layer 2 switch) uses the destination MAC address within packets to determine the destination port. Additionally, a Layer 2 switch forwards broadcast traffic to all ports on the switch.

Routers operate on Layer 3 of the OSI model. They forward traffic based on the destination IP address within a packet, and they block broadcast traffic. A Layer 3 switch mimics the behavior of a router and allows network administrators to create virtual local area networks (VLANs). Because a Layer 3 switch forwards traffic based on the destination IP address instead of the MAC address, it is not susceptible to ARP-based attacks.

Isolating Traffic with a VLAN

A virtual local area network (***VLAN***) uses a switch to group several different computers into a virtual network. You can group the computers together based on departments, job function, or any other administrative need. This provides security because you're able to isolate the traffic between the computers in the VLAN.

Normally, a router would group different computers onto different subnets, based on physical locations. All the computers in a routed segment are typically located in the same physical location, such as on a specific floor or wing of a building.

However, a single Layer 3 switch can create multiple VLANs to separate the computers based on logical needs rather than physical location. Additionally, administrators can easily reconfigure the switch to add or subtract computers from any VLAN if the need arises.

For example, a group of users who normally work in separate departments may begin work on a project that requires them to be on the same subnet. You can configure a Layer 3 switch to logically group these workers together, even if the computers are physically located on different floors or different wings of the building. When the project is over, you can simply reconfigure the switch to return the network to its original configuration.

As another example, VoIP streaming traffic can consume quite a bit of bandwidth. One way to increase the availability and reliability of systems using this voice traffic is to put them on a dedicated VLAN. Other systems transferring traditional data traffic can be placed on a separate VLAN. This separates the voice and data traffic within the VLAN.

Similarly, you can use a single switch with multiple VLANs to separate user traffic. For example, if you want to separate the traffic between the HR

department and the IT department, you can use a single switch with two VLANs. The VLANs logically separate all the computers between the two different departments, even if the computers are located close to each other.

Remember this

Virtual local area networks (VLANs) separate or segment traffic on physical networks and you can create multiple VLANs with a single Layer 3 switch. A VLAN can logically group several different computers together, or logically separate computers, without regard to their physical location. VLANs are also used to separate traffic types, such as voice traffic on VLAN and data traffic on a separate VLAN.

Media Gateway

A media gateway is a device that converts data from the format used on one network to the format used on another network. As an example, a VoIP gateway converts telephony traffic between traditional phone lines and an IP-based network. This allows users to make and receive phone calls using VoIP equipment and the gateway can translate the traffic and transmit the calls over a traditional phone line.

Proxy Servers

Many networks use ***proxy*** servers (or forward proxy servers) to forward requests for services (such as HTTP or HTTPS) from clients. They can improve performance by caching content and some proxy servers can restrict users' access to inappropriate web sites by filtering content. A proxy server is located on the edge of the network bordering the Internet and the intranet, as shown in Figure 3.8.

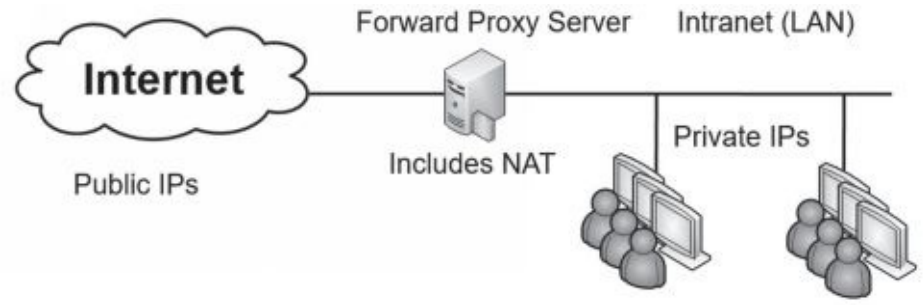


Figure 3.8: Proxy server

Administrators configure internal clients to use the proxy server for specific protocols. The proxy accepts their requests, retrieves the content from the Internet, and then returns the data to the client. Most proxy servers only act as a proxy for HTTP and HTTPS. However, proxy servers can also proxy other Internet protocols, such as FTP.

Caching Content for Performance

The proxy server increases the performance of Internet requests by caching each result received from the Internet. Any data that is in the proxy server's cache doesn't need to be retrieved from the Internet again to fulfill another client's request. In this context, *cache* simply means "temporary storage." Cache could be a dedicated area of RAM, or, in some situations, it could also be an area on a high-performance disk subsystem.

As an example, if Lisa retrieves a web page from *GetCertifiedGetAhead.com*, the proxy server would store the result in cache. If Homer later requests the same page, the proxy server retrieves the page from cache and sends it to Homer. This reduces the amount of Internet bandwidth used for web browsing because the page doesn't need to be retrieved again.

Transparent Proxy Versus Nontransparent Proxy

A transparent proxy will accept and forward requests without modifying them. It is the simplest to set up and use and it provides caching.

In contrast, a nontransparent proxy server can modify or filter requests. Organizations often use nontransparent proxy servers to restrict what users can access with the use of URL filters. A URL filter examines the requested URL and chooses to allow the request or deny the request.

Many third-party companies sell subscription lists for URL filtering.

These sites scour the Internet for web sites and categorize the sites based on what companies typically want to block. Categories may include anonymizers, pornography, gambling, web-based email, and warez sites. Anonymizers are sites that give the illusion of privacy on the Internet. Employees sometimes try to use anonymizers to bypass proxy servers, but a proxy server usually detects, blocks, and logs these attempts. Web-based email bypasses the security controls on internal email servers, so many organizations block them. Warez sites often host pirated software, movies, MP3 files, and hacking tools.

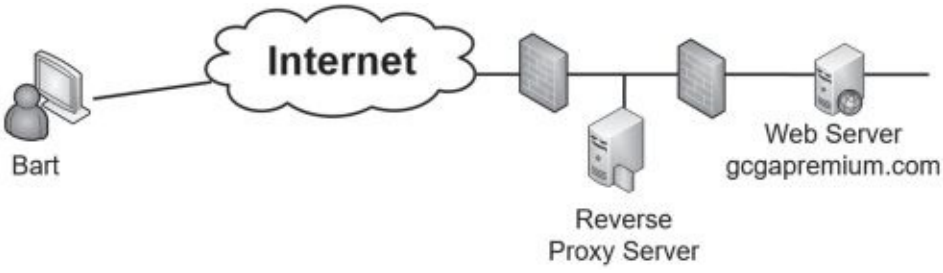
The subscription list can be loaded into the proxy server, and whenever a user attempts to access a site on the URL filter block list, the proxy blocks the request. Often, the proxy server presents users with a warning page when they try to access a restricted page. Many organizations use this page to remind users of a corporate acceptable usage policy, and some provide reminders that the proxy server is monitoring their online activity.

Proxy servers include logs that record each site visited by users. These logs can be helpful to identify frequently visited sites and to monitor user web browsing activities.

Remember this

A proxy server forwards requests for services from a client. It provides caching to improve performance and reduce Internet bandwidth usage. Transparent proxy servers use URL filters to restrict access to certain sites, and can log user activity.

Reverse Proxy



A reverse proxy accepts requests from the Internet, typically for a single web server. It appears to clients as a web server, but is forwarding the requests to the web server and serving the pages returned by the web server. Figure 3.9 shows how a reverse proxy server is configured to protect a web server. Note that this configuration allows the web server to be located in the private

network behind a second firewall.

Figure 3.9: Reverse proxy server

Imagine that Bart wants to access *http://gcgapremium.com.* He types the URL into his browser and it connects to the reverse proxy server. The reverse proxy server connects to the web server and retrieves the web page. It then sends the web page to Bart. A reverse proxy server caches the web pages just as a forward proxy server does, so it can improve the overall web site performance.

The reverse proxy server can be used for a single web server or a web farm of multiple servers. When used with a web farm, it can act as a ***load balancer***. You would place the load balancer in the DMZ to accept the requests and it then forwards the requests to different servers in the web farm using a load-balancing algorithm. Chapter 9, “Implementing Controls to Protect Assets,” covers load balancing in more depth.

Application Proxy

An application proxy is used for specific applications. It accepts requests, forwards the requests to the appropriate server, and then sends the response to the original requestor. A forward proxy used for HTTP is a basic application proxy. However, most application proxies are multipurpose proxy servers supporting multiple protocols such as HTTP and HTTPS.

As a more advanced example, imagine you buy a book from Amazon and Amazon ships it via United Parcel Service (UPS). Later, you check your account to see the status of the shipment. The Amazon web site sends a query to a UPS application proxy for the status. The UPS application proxy provides the status in a response. Internet applications exchange data this way using application programming interfaces (APIs). For example, UPS specifies the format of the request in an API. If the application proxy receives a properly formatted and valid request, it provides an answer.

Unified Threat Management

Unified threat management (***UTM***) is a single solution that combines multiple security controls. The overall goal of UTMs is to provide better security, while also simplifying management requirements. In many cases, a UTM device will reduce the workload of administrators without sacrificing security.

As IT-based threats first began appearing, security experts created various solutions to deal with each of them. When attackers began releasing malware to infect computers, vendors created antivirus software. Attackers started attacking networks, and in response, security experts developed and steadily improved firewalls. When organizations recognized a need to control what sites users can visit, organizations implemented proxies with URL filters.

Although these solutions are effective, they are also complex. Administrators often find it challenging to manage each of these solutions separately. Because of this, UTM security appliances have become quite popular.

UTM security appliances combine the features of multiple security solutions into a single appliance. For example, a UTM security appliance might include a firewall, antivirus protection, anti-spam protection, URL filtering, and content filtering.

In general, a computer appliance is a hardware device designed to provide a specific solution. For example, spam appliances scan all incoming email and strip off spam. The intent of the word *appliance* is to evoke a sense of simplicity. For example, you don't have to know the details of how a toaster works to make toast. Similarly, you don't have to know the details of how a computer appliance operates to use it.

UTM security appliances include multiple capabilities, including:

- **URL filtering.** URL filters within a UTM security appliance perform the same job as a proxy server. They block access to sites based on the URL. It's common to subscribe to a service and select categories to block access to groups of sites. Administrators can also configure URL filters manually to allow or block access to specific web sites. As an example, if an administrator realizes that users are routinely connecting to a peer-to- peer (P2P) file sharing site, the administrator can add the URL to the filter, and block access to that site.
- **Malware inspection.** Malware often comes into a network via spam, or malicious web pages. The malware inspection component of a UTM appliance screens incoming data for known malware and blocks it. Organizations often scan for malware at email servers and at individual systems as part of a layered security or defense-in-depth solution.
- **Content inspection.** Content inspection includes a combination of

different content filters. It monitors incoming data streams and attempts to block any malicious content. It can include a spam filter to inspect incoming email and reject spam. It can also block specific types of transmissions, such as streaming audio and video, and specific types of files such as Zip files.

- **DDoS mitigator.** A DDoS mitigator attempts to detect DDoS attacks and block them. This is similar to how intrusion prevention systems (IPSs) block attacks. Chapter 4 covers IPSs in more depth.

The output of the UTM varies depending on the device and what it sees. For example, if it detects malware, it will typically raise an alert and send it to administrators.

A common security issue with UTMs is a misconfigured content filter. For example, if the spam filter is misconfigured, it can block valid mail or allow too much spam into the network. Administrators adjust the sensitivity of the spam filter to meet the needs of the organization. For example, one organization might find it unacceptable to block emails from customers or potential customers. Administrators would adjust the sensitivity allowing more spam into the network to meet this need.

It's common to place UTM appliances at the network border, between the Internet and the intranet (or the private network). This allows it to intercept and analyze all traffic to and from the Internet. However, the placement is dependent on how the UTM appliance is being used. As an example, if it is being used as a proxy server, it can be placed within the DMZ. Administrators would configure the clients to use the UTM appliance for proxy servers ensuring that all relevant traffic goes through it.

Remember this

A unified threat management (UTM) appliance combines multiple security controls into a single appliance. They can inspect data streams and often include URL filtering, malware inspection, and contention inspection components. Many UTMs include a DDoS mitigator to block DDoS attacks.

Mail Gateways

A ***mail gateway*** is a server that examines all incoming and outgoing email and attempts to reduce risks associated with email. Many vendors sell

appliances that perform all the desired services of a mail gateway. Administrators locate it between the email server and the Internet and configure it for their purposes. All mail goes to the gateway before it goes to the email server. Additionally, many vendors include a mail gateway within a UTM appliance. The mail gateway is just another security feature within the UTM appliance.

Spam is unsolicited email and attackers commonly use spam to launch attacks. For example, spam can include malware as an attachment or it might include a link to a malicious web site. A spam filter within a mail gateway filters out spam from incoming email. By filtering out spam, it helps block attacks.

Mail gateways often include data loss prevention (***DLP***) capabilities. They examine outgoing email looking for confidential or sensitive information and block them. As an example, imagine an organization is working on a secret project with a codeword of "DOH." All documents associated with this project have the keyword within them. The mail gateway includes this keyword in its searches and when it detects the keyword within an email or an attachment, it blocks the email. Administrators have the choice of configuring the gateway to notify security personnel, the user who sent the email, or both when it blocks an email. Chapter 5, "Securing Hosts and Data," discusses DLP in more depth.

Many mail gateways also support encryption. They can encrypt all outgoing email to ensure confidentiality for the data-in-transit, or only encrypt certain data based on policies. For example, if an organization is working on a project with another organization, administrators can configure the gateway to encrypt all traffic sent to the other organization. The method of encryption varies from vendor to vendor. For example, some vendors use certificate-based encryption. Others use password-based encryption. Chapter 10 discusses encryption in more depth.

Summarizing Routing and Switching Use Cases

Several use cases were covered earlier in this chapter. While they could be covered independently, it was important to have a basic understanding of

routers and switches before connecting them with routing and switching use cases. This section summarizes some of the routing and switching topics.

The following bullets identify some use cases that you can implement with switches:

- **Prevent switching loops.** You do this by implementing STP or RSTP on switches.
- **Block flood attacks.** Flood guards block MAC flood attacks.
- **Prevent unauthorized users from connecting to unused ports.** Port security methods, such as disabling unused ports, prevent these unauthorized connections.
- **Provide increased segmentation of user computers.** VLANs provide increased segmentation. They are implemented on Layer 3 switches.

Simple Network Management Protocol version 3 (***SNMPv3***) monitors and manages network devices, such as routers or switches. This includes using SNMPv3 to modify the configuration of the devices or have network devices report status back to a central network management system. SNMPv3 agents installed on devices send information to an SNMP manager via notifications known as traps (sometimes called device traps).

The first version of SNMP had vulnerabilities, such as passing passwords across the network in cleartext. SNMPv2 and SNMPv3 are much more secure and they provide strong authentication mechanisms. SNMPv3 uses UDP port 161. It sends traps (error messages and notifications) on UDP port 162.

The following bullets identify some use cases that you can implement with routers:

- **Prevent IP address spoofing.** Antispoofing methods prevent IP address spoofing. These are implemented with rules in ACLs.
- **Provide secure management of routers.** SNMPv3 is used to securely manage network devices such as routers.

Remember this

Administrators use SNMPv3 to manage and monitor network devices and SNMP uses UDP ports 161 and 162. It includes strong authentication mechanisms and is more secure than earlier versions.

Chapter 3 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Reviewing Basic Networking Concepts

- A use case typically describes an organizational goal and administrators enable specific protocols to meet organizational goals.
- Protocols used for voice and video include Real-time Transport Protocol (RTP) and Secure Real-time Transport Protocol (SRTP). SRTP provides encryption, message authentication, and integrity for RTP.
- File Transfer Protocol (FTP) is commonly used to transfer files over networks, but FTP does not encrypt the transmission.
- Several encryption protocols encrypt data-in-transit to protect its confidentiality. They include File Transfer Protocol Secure (FTPS), Secure File Transfer Protocol (SFTP), Secure Shell (SSH), Secure Sockets Layer (SSL), and Transport Layer Security (TLS).
- SMTP sends email using TCP port 25. POP3 receives email using TCP port 110. IMAP4 uses TCP port 143. Secure POP uses TLS on port 995 (legacy) or with STARTTLS on port 110. Secure IMAP uses TLS on port 993 (legacy) or with STARTTLS on port 143.
- HTTP uses port 80 for web traffic. HTTPS encrypts HTTP traffic in transit and uses port 443.
- Directory services solutions implement Kerberos as the authentication protocol. They also use Lightweight Directory Access Protocol (LDAP) over TCP port 389 and LDAP Secure (LDAPS) over TCP port 636.
- Administrators commonly connect to remote systems using SSH instead of Telnet because SSH encrypts the connection. Administrators also use Remote Desktop Protocol (RDP) to connect to remote systems using TCP port 3389.
- The Network Time Protocol (NTP) provides time synchronization services.
- Domain Name System (DNS) provides domain name resolution.

DNS zones include A records for IPv4 addresses and AAAA records for IPv6 addresses. Zone data is updated with zone transfers and secure zone transfers help prevent unauthorized access to zone data. DNS uses TCP port 53 for zone transfers and UDP port 53 for DNS client queries.

- Domain Name System Security Extensions (DNSSEC) provides validation for DNS responses and helps prevent DNS poisoning attacks.
- Two command-line tools used to query DNS are nslookup and dig. Both support the axfr switch, allowing them to download all zone data from a DNS server, unless the DNS server blocks the attempt.

Understanding Basic Network Devices

- Switches are used for network connectivity and they map media access control (MAC) addresses to physical ports.
- Port security limits access to switch ports. It includes limiting the number of MAC addresses per port and disabling unused ports. You can also manually map each port to a specific MAC address or group of addresses.
- An aggregation switch connects multiple switches together in a network.
- Routers connect networks and direct traffic based on the destination IP address. Routers (and firewalls) use rules within access control lists (ACLs) to allow or block traffic.
- Implicit deny indicates that unless something is explicitly allowed, it is denied. It is the last rule in an ACL.Host-based firewalls (sometimes called application-based) filter traffic in and out of individual hosts. Some Linux systems use iptables or xtables for firewall capabilities.
- Network-based firewalls filter traffic in and out of a network. They are placed on the border of the network, such as between the Internet and an internal network.
- A stateless firewall controls traffic between networks using rules within an ACL. The ACL can block traffic based on ports, IP addresses, subnets, and some protocols. Stateful firewalls filter traffic based on the state of a packet within a session.
- A web application firewall (WAF) protects a web server against web application attacks. It is typically placed in the demilitarized zone

(DMZ) and will alert administrators of suspicious events.

Implementing a Secure Network

- A DMZ provides a layer of protection for servers that are accessible from the Internet.
- An intranet is an internal network. People use the intranet to communicate and share content with each other. An extranet is part of a network that can be accessed by authorized entities from outside of the network.
- NAT translates public IP addresses to private IP addresses, private back to public, and hides IP addresses on the internal network from users on the Internet.
- Networks use various methods to provide network segregation, segmentation, and isolation.
- An airgap is a metaphor for physical isolation, indicating a system or network is completely isolated from another system or network.
- Routers provide logical separation and segmentation using ACLs to control traffic.
- Forward proxy servers forward requests for services from a client. It can cache content and record users' Internet activity. A transparent proxy accepts and forwards requests without modifying them. A nontransparent proxy can modify or filter requests, such as filtering traffic based on destination URLs.
- Reverse proxy servers accept traffic from the Internet and forward it to one or more internal web servers. The reverse proxy server is placed in the DMZ and the web servers can be in the internal network.
- A unified threat management (UTM) security appliance includes multiple layers of protection, such as URL filters, content inspection, malware inspection, and a distributed denial-of-service (DDoS) mitigator. UTMs typically raise alerts and send them to administrators to interpret.
- Mail gateways are logically placed between an email server and the Internet. They examine and analyze all traffic and can block unsolicited email with a spam filter. Many include data loss prevention (DLP) and encryption capabilities.

Summarizing Routing and Switching Use Cases

- Loop protection protects against switching loop problems, such as when a user connects two switch ports together with a cable. Spanning Tree Protocols protect against switching loops.
- Flood guards prevent MAC flood attacks on switches.
- VLANs can logically separate computers or logically group computers regardless of their physical location. You create them with Layer 3 switches.
- Routers use rules within ACLs as an antispoofing method. Border firewalls block all traffic coming from private IP addresses.
- SNMPv3 is used to monitor and configure network devices and uses notification messages known as traps. It uses strong authentication mechanisms and is preferred over earlier versions. SNMP uses UDP ports 161 and 162.

Online References

- Remember, the online content includes some extras, such as labs, performance-based question examples, and more. Check it out at *http://gcgapremium.com/501-extras.*

Chapter 3 Practice Questions

1. Your organization's security policy requires that PII data-in-transit must be encrypted. Which of the following protocols would BEST meet this requirement?

   A. FTP
   B. SSH
   C. SMTP
   D. HTTP

2. Marge needs to collect network device configuration information and network statistics from devices on the network. She wants to protect the confidentiality of credentials used to connect to these devices. Which of the following protocols would BEST meet this need?

   A. SSH

B. FTPS
C. SNMPv3
D. TLS

3. Lisa is enabling NTP on some servers within the DMZ. Which of the following use cases is she MOST likely supporting with this action?

A. Support voice and video transmissions
B. Provide time synchronization
C. Enable email usage
D. Encrypt data-in-transit

4. Your organization wants to increase security for VoIP and video teleconferencing applications used within the network. Which of the following protocols will BEST support this goal?

A. SMTP
B. TLS
C. SFTP
D. SRTP

5. Management within your organization wants to ensure that switches are not susceptible to switching loop problems. Which of the following protocols is the BEST choice to meet this need?

A. Flood guard
B. SNMPv3
C. SRTP
D. RSTP

6. A network technician incorrectly wired the switch connections in your organization's network. It effectively disabled the switch as though it was a victim of a denial-of-service attack. Which of the following should be done to prevent this situation in the future?

A. Install an IDS.
B. Only use Layer 2 switches.
C. Install SNMPv3 on the switches.
D. Implement STP or RSTP.

7. Developers recently configured a new service on ServerA. ServerA is in a DMZ and accessed by internal users and via the Internet. Network administrators modified firewall rules to access the service. Testing shows the service works when accessed from internal systems. However, it does not work when accessed from the Internet. Which of the following is

MOST likely configured incorrectly?

A. The new service
B. An ACL
C. ServerA
D. The VLAN

8. You manage a Linux computer used for security within your network. You plan to use it to inspect and handle network-based traffic using iptables. Which of the following network devices can this replace?

A. Wireless access point
B. Firewall
C. Layer 2 switch
D. Bridge

9. You need to implement antispoofing on a border router. Which one of the following choices will BEST meet this goal?

A. Create rules to block all outgoing traffic from a private IP address.
B. Implement a flood guard on switches.
C. Add a web application firewall.
D. Create rules to block all incoming traffic from a private IP address.

10. An organization has recently had several attacks against servers within a DMZ. Security administrators discovered that many of these attacks are using TCP, but they did not start with a three-way handshake. Which of the following devices provides the BEST solution?

A. Stateless firewall
B. Stateful firewall
C. Network firewall
D. Application-based firewall

11. Which type of device would have the following entries used to define its operation? permit IP any any eq 80
permit IP any any eq
443 deny IP any any

A. Firewall
B. Layer 2 switch
C. Proxy server
D. Web server

12. Your organization hosts a web server and wants to increase its security. You need to separate all web-facing traffic from internal network traffic. Which of the following provides the BEST solution?

A. DMZ
B. VLAN
C. Firewall
D. WAF

13. Management at your organization wants to prevent employees from accessing social media sites using company-owned computers. Which of the following devices would you implement?

A. Transparent proxy
B. Reverse proxy
C. Nontransparent proxy
D. Caching proxy

14. You need to configure a UTM security appliance to restrict traffic going to social media sites. Which of the following are you MOST likely to configure?

A. Content inspection
B. Malware inspection
C. URL filter
D. DDoS mitigator

15. Your organization recently purchased a sophisticated security appliance that includes a DDoS mitigator. Where should you place this device?

A. Within the DMZ
B. At the border of the network, between the intranet and the DMZ
C. At the border of the network, between the private network and the Internet
D. In the internal network

Chapter 3 Practice Question Answers

1. **B.** You can use Secure Shell (SSH) to encrypt Personally Identifiable Information (PII) data when transmitting it over the network (data-in-transit). Secure File Transfer Protocol (SFTP) uses SSH to encrypt File

Transfer Protocol (FTP) traffic. FTP, Simple Mail Transfer Protocol (SMTP), and Hypertext Transfer Protocol (HTTP) transmit data in cleartext unless they are combined with an encryption protocol.

2. **C.** Simple Network Management Protocol version 3 (SNMPv3) is a secure protocol that can monitor and collect information from network devices. It includes strong authentication mechanisms to protect the confidentiality of credentials. None of the other protocols listed are used to monitor network devices. Secure Shell (SSH) provides a secure method of connecting to devices, but does not monitor them. File Transfer Protocol Secure (FTPS) is useful for encrypting large files in transit, using Transport Layer Security (TLS). TLS is commonly used to secure transmissions, but doesn't include methods to monitor devices.

3. **B.** The Network Time Protocol (NTP) provides time synchronization services, so enabling NTP on servers would meet this use case. The Real-time Transport Protocol (RTP) delivers audio and video over IP networks, and Secure RTP (SRTP) provides encryption, message authentication, and integrity for RTP. Protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol v3 (POP3), and Internet Message Access Protocol version 4 (IMAP4) are used for email. Encrypting data isn't relevant to time synchronization services provided by NTP.

4. **D.** The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication, and integrity for Voice over Internet Protocol(VoIP), video teleconferencing, and other streaming media applications. None of the other answers are directly related to VoIP or video teleconferencing. Simple Mail Transfer Protocol (SMTP) transfers email. The Transport Layer Security (TLS) protocol is used to encrypt data-in-transit, but isn't the best choice for streaming media. Secure File Transfer Protocol (SFTP) is a secure implementation of FTP to transfer files.

5. **D.** Rapid STP (RSTP) prevents switching loop problems and should be enabled on the switches to meet this need. A flood guard on a switch helps prevent a media access control (MAC) flood attack. Simple Network Management Protocol version 3 (SNMPv3) is used to manage and monitor network devices. The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication, and integrity for

video and voice data.

6. **D.** Spanning Tree Protocol (STP) and Rapid STP (RSTP) both prevent switching loop problems. It's rare for a wiring error to take down a switch. However, if two ports on a switch are connected to each other, it creates a switching loop and effectively disables the switch. An intrusion detection system (IDS) will not prevent a switching loop. Layer 2 switches are susceptible to this problem. Administrators use Simple Network Management Protocol version 3 (SNMPv3) to manage and monitor devices, but it doesn't prevent switching loops.

7. **B.** The most likely problem of the available choices is that an access control list (ACL) is configured incorrectly. The server is in a demilitarized zone (DMZ) and the most likely problem is an incorrectly configured ACL on the border firewall. The service is operating when accessed from internal clients, so it isn't likely that it is the problem. Also, the server works for internal systems indicating it is working correctly. There isn't any indication a virtual local area network (VLAN) is in use.

8. **B.** Iptables include settings used by the Linux Kernel firewall and can be used to replace a firewall. While it's possible to implement iptables on a wireless access point (assuming it is Linux-based), iptables still function as a firewall, not a wireless access point. A Layer 2 switch routes traffic based on the destination media access control (MAC) address, but iptables focus on IP addresses. A network bridge connects multiple networks together.

9. **D.** You would create rules to block all incoming traffic from private IP addresses. The border router is between the internal network and the Internet and any traffic coming from the Internet with a private IP address is a spoofed source IP address. All outgoing traffic will typically use a private IP address, so you shouldn't block this outgoing traffic. A flood guard on a switch protects against media access control (MAC) flood attacks and is unrelated to this question. A web application firewall protects a web application and is unrelated to antispoofing.

10. **B.** A stateful firewall filters traffic based on the state of the packet within a session. It would filter a packet that isn't part of a TCP three-way handshake. A stateless firewall filters traffic based on the IP address, port, or protocol ID. While it's appropriate to place a network firewall in

a demilitarized zone (DMZ), a network firewall could be either a stateless firewall or a stateful firewall. An application-based firewall is typically only protecting a host, not a network.

11. **A.** These are rules in an access control list (ACL) for a firewall. The first two rules indicate that traffic from any IP address, to any IP address, using ports 80 or 443 is permitted or allowed. The final rule is also known as an implicit deny rule and is placed last in the ACL. It ensures that all traffic that hasn't been previously allowed is denied. Layer 2 switches do not use ACLs. A proxy server would not use an ACL, although it would use ports 80 and 443 for Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS), respectively. A web server wouldn't use an ACL, although it would also use ports 80 and 443.

12. **A.** A demilitarized zone (DMZ) is a buffered zone between a private network and the Internet, and it will separate the web server's web-facing traffic from the internal network. You can use a virtual local area network (VLAN) to group computers together based on job function or some other administrative need, but it is created on switches in the internal network. A firewall does provide protection for the web server, but doesn't necessarily separate the web-facing traffic from the internal network. A web application firewall (WAF) protects a web server from incoming attacks, but it does not necessarily separate Internet and internal network traffic.

13. **C.** A nontransparent proxy includes the ability to filter traffic based on the URL and is the best choice. A transparent proxy doesn't modify or filter requests. A reverse proxy is used for incoming traffic to an internal firewall, not traffic going out of the network. Proxy servers are caching proxy servers, but won't block outgoing traffic.

14. **C.** You would most likely configure the Uniform Resource Locator (URL) filter on the unified threat management (UTM) security appliance. This would block access to the peer-to-peer sites based on their URL. Content inspection and malware inspection focus on inspecting the data as it passes through the UTM, but they do not block access to sites. A distributed denial-of-service (DDoS) mitigator will attempt to block incoming DDoS attack traffic.

15. **C.** A distributed denial-of-service (DDoS) mitigator attempts to block DDoS attacks and should be placed at the border of the network, between the private network and the Internet. If the network includes a demilitarized zone (DMZ), the appliance should be placed at the border of the DMZ and the Internet. Placing it in the DMZ or the internal network doesn’t ensure it will block incoming traffic.