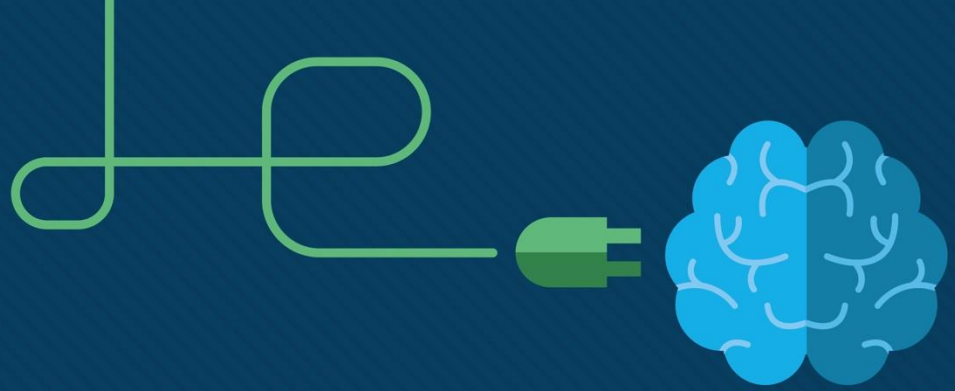
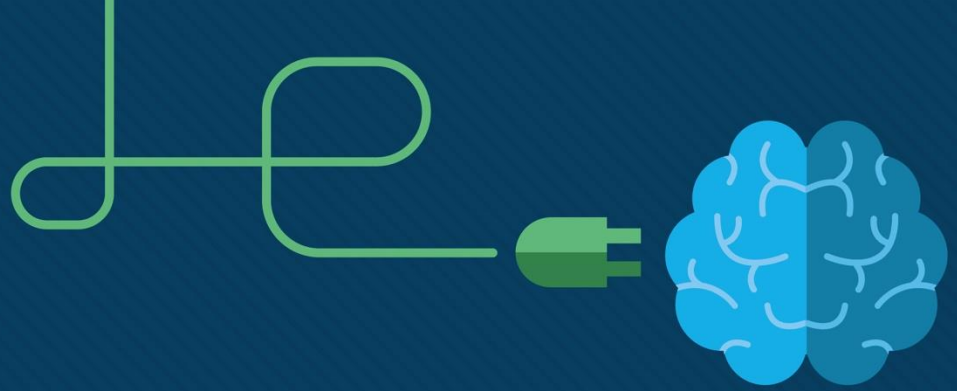


Module 24: Technologies and Protocols

Instructor Materials

CyberOps Associate v1.0



Module 24: Technologies and Protocols

CyberOps Associate v1.0

Module Objectives

Module Title: Technologies and Protocols

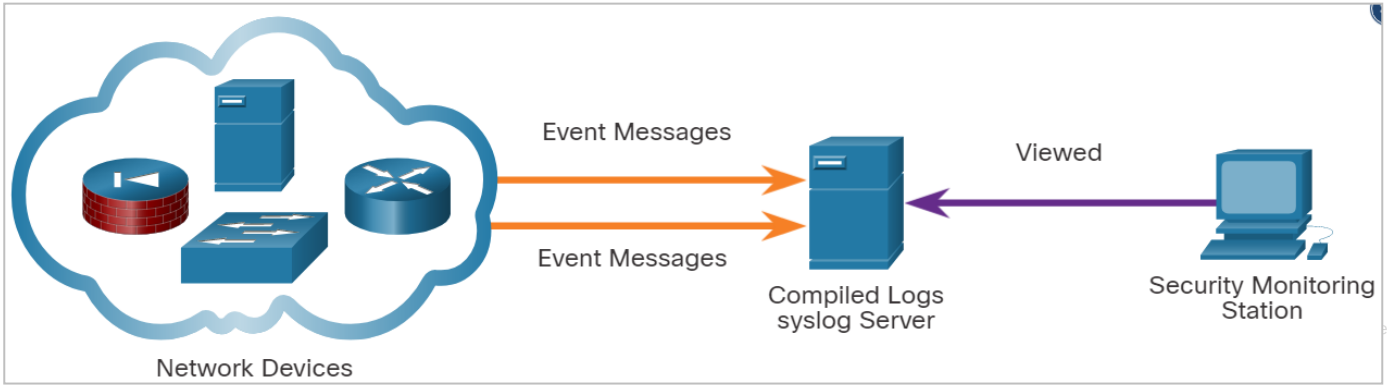
Module Objective: Explain how security technologies affect security monitoring.

Topic	Topic Objective
Monitoring Common Protocols	Explain the behavior of common network protocols in the context of security monitoring.
Security Technologies	Explain how security technologies affect the ability to monitor common network protocols.

24.1 Monitoring Common Protocols

Syslog and NTP

- Syslog and Network Time Protocol (NTP) are essential to the work of the cybersecurity analyst.
- The syslog standard is used for logging event messages from network devices and endpoints.
- The standard allows for a system-neutral means of transmitting, storing, and analyzing messages.
- Many types of devices from many different vendors can use syslog to send log entries to central servers that run a syslog daemon. This centralization of log collection helps to make security monitoring practical. Servers that run syslog typically listen on UDP port 514.

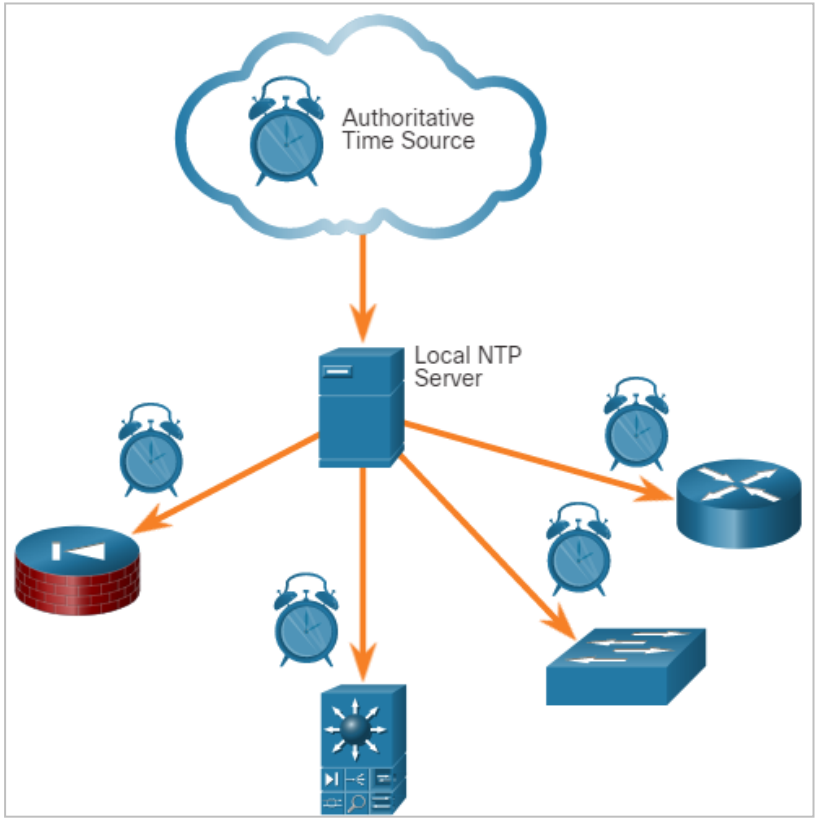


Syslog and NTP (Contd.)

- As syslog is so important to security monitoring, syslog servers may be a target for threat actors.
- Some exploits, such as those involving data exfiltration, can take a long time to complete due to the very slow ways in which data is secretly stolen from the network.
- Some attackers may try to hide the fact that exfiltration is occurring. They attack the syslog servers that contain the information that could lead to detection of the exploit.
- Hackers may attempt to block the transfer of data from syslog clients to servers, tamper with or destroy log data, or tamper with the software that creates and transmits log messages.
- The next generation (ng) syslog implementation, known as syslog-ng, offers enhancements that can help prevent some of the exploits that target syslog.

NTP

- Syslog messages are usually timestamped. As the messages come from many devices, so it is important that the devices share a consistent timeclock. This can be achieved by using Network Time Protocol (NTP).
- NTP uses a hierarchy of authoritative time sources to share time information between devices on the network. NTP operates on UDP port 123.
- Threat actors may attempt to attack the NTP infrastructure in order to corrupt time information used to correlate logged network events.
- Threat actors have been known to use NTP systems to direct DDoS attacks through vulnerabilities in client or server software. These attacks can disrupt network availability.



DNS

- DNS is now used by many types of malware. Some varieties of malware use DNS to communicate with command-and-control (CnC) servers and to exfiltrate data in traffic disguised as normal DNS queries.
- Malware could encode stolen data as the subdomain portion of a DNS lookup for a domain where the nameserver is under control of an attacker.
- A DNS lookup for ‘long-string-of-exfiltrated-data.example.com’ would be forwarded to the nameserver of example.com, which would record ‘long-string-of-exfiltrated-data’ and reply back to the malware with a coded response. This use of the DNS subdomain is shown in the figure. The exfiltrated data is the encoded text shown in the box. The threat actor collects the encoded data, decodes and combines it, and now has access to an entire data file.

DNS (Contd.)

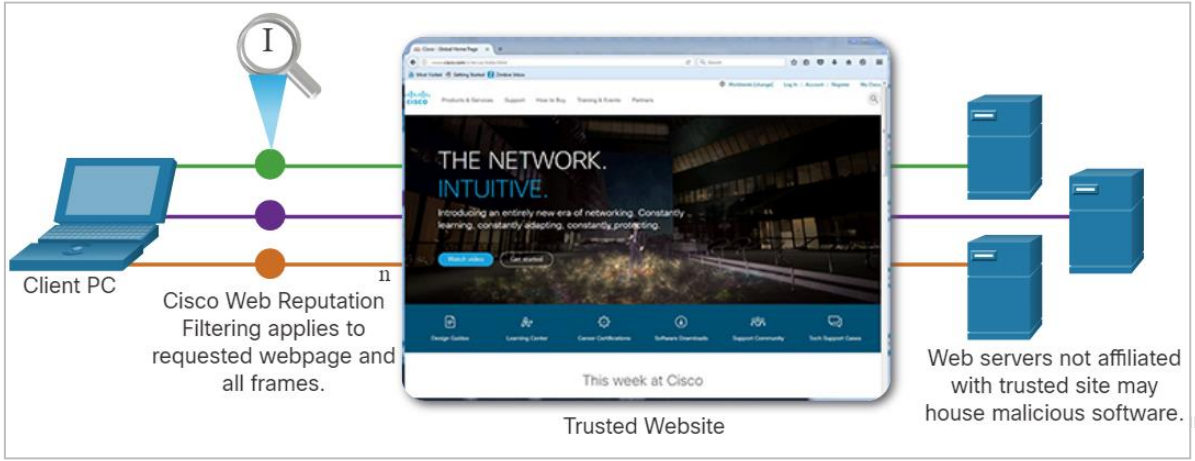
- It is likely that the subdomain part of such requests would be much longer than usual requests. Cyber analysts can use the distribution of the lengths of subdomains within DNS requests to construct a mathematical model that describes normality.
- They can then use this to compare their observations and identify an abuse of the DNS query process. For example, it would not be normal to see a host on the network sending a query to aW4gcGxhY2UgdG8gcHJvdGVjdC.example.com.
- DNS queries for randomly generated domain names, or extremely long random-appearing subdomains, should be considered suspicious, especially if their occurrence spikes dramatically on the network.
- DNS proxy logs can be analyzed to detect these conditions.
- Alternatively, services such as the Cisco Umbrella passive DNS service can be used to block requests to suspected CnC and exploit domains.

HTTP and HTTPS

- Hypertext Transfer Protocol (HTTP) is the backbone protocol of the World Wide Web.
- All information carried in HTTP is transmitted in plaintext from the source computer to the destination on the internet.
- HTTP does not protect data from alteration or interception by malicious parties, which is a serious threat to privacy, identity, and information security.
- All browsing activity should be considered to be at risk.

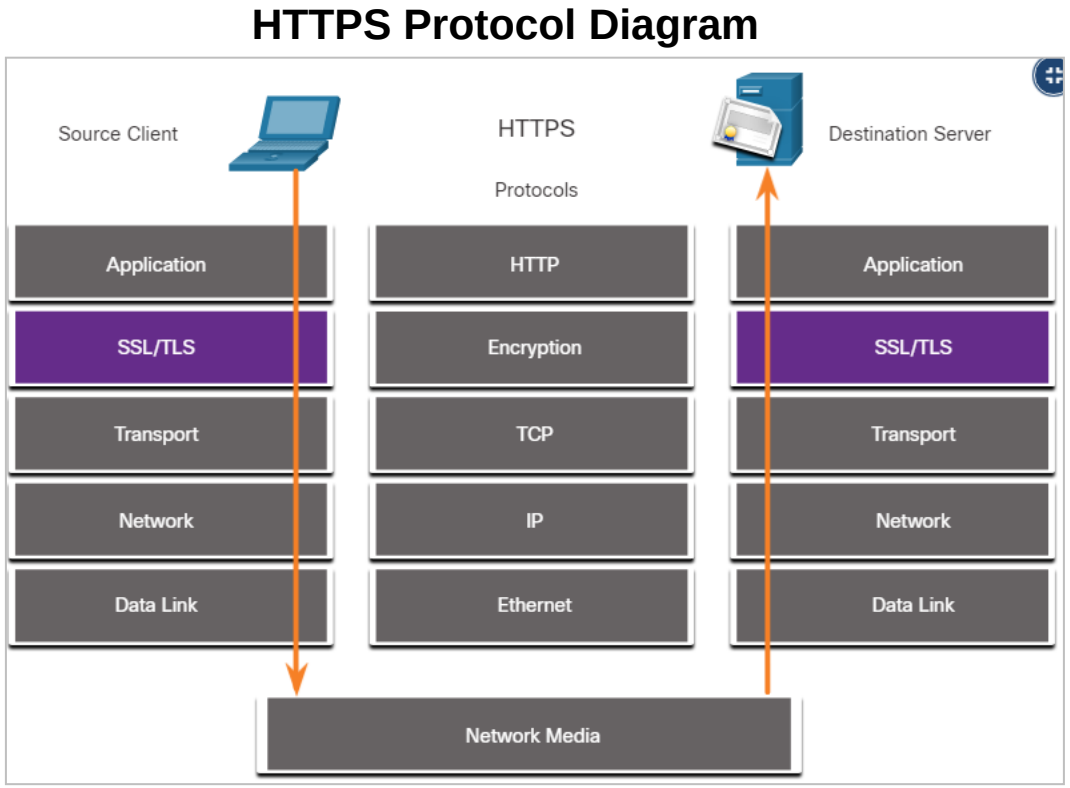
HTTP and HTTPS (Contd.)

- A common exploit of HTTP is called iFrame (inline frame) injection. In iFrame injection, a threat actor compromises a webserver and plants malicious code which creates an invisible iFrame on a commonly visited webpage.
- When the iFrame loads, malware is downloaded, frequently from a different URL than the webpage that contains the iFrame code.
- Network security services, such as Cisco Web Reputation filtering, can detect when a website attempts to send content from an untrusted website to the host, even when sent from an iFrame.



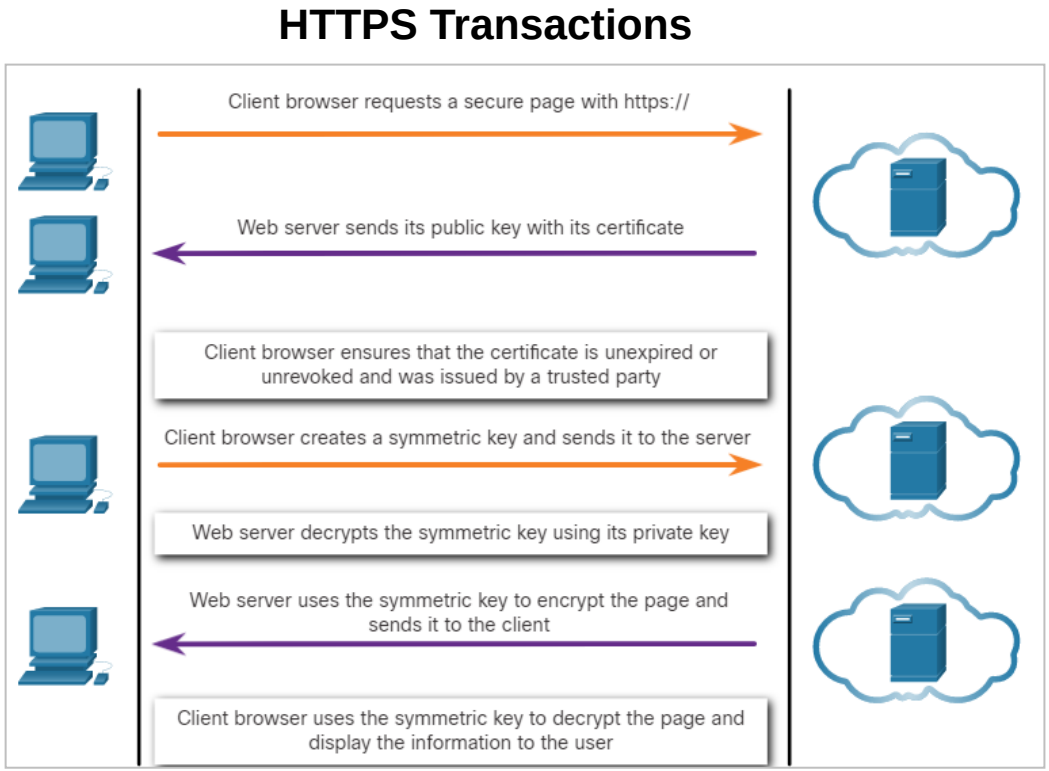
HTTP and HTTPS (Contd.)

- To address the alteration of confidential data, many organizations have adopted HTTPS or implemented HTTPS-only policies to protect visitors to their websites and services.
- HTTPS adds a layer of encryption to the HTTP protocol by using Secure Socket Layer (SSL), as shown in the figure.
- This makes the HTTP data unreadable as it leaves the source computer until it reaches the server.
- HTTPS is not a mechanism for web server security. It only secures HTTP protocol traffic while it is in transit.



HTTP and HTTPS (Contd.)

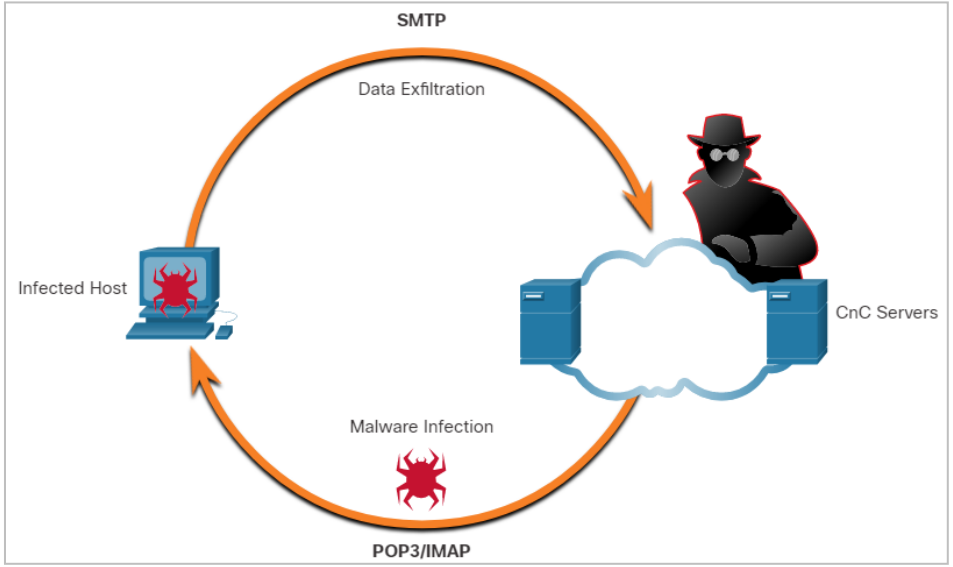
- Unfortunately, the encrypted HTTPS traffic complicates network security monitoring.
- Some security devices include SSL decryption and inspection; however, this can present processing and privacy issues.
- HTTPS adds complexity to packet captures due to the additional messaging involved in establishing the encrypted connection.
- This process is summarized in the figure and represents additional overhead on top of HTTP.



Email Protocols

- Email protocols such as SMTP, POP3, and IMAP can be used by threat actors to spread malware, exfiltrate data, or provide channels to malware CnC servers, as shown in the figure.
- SMTP sends data from a host to a mail server and between mail servers.
- IMAP and POP3 are used to download email messages from a mail server to the host computer. They are the application protocols that are responsible for bringing malware to the host.
- Security monitoring can identify when a malware attachment entered the network and which host it first infected.

Email Protocol Threats



ICMP

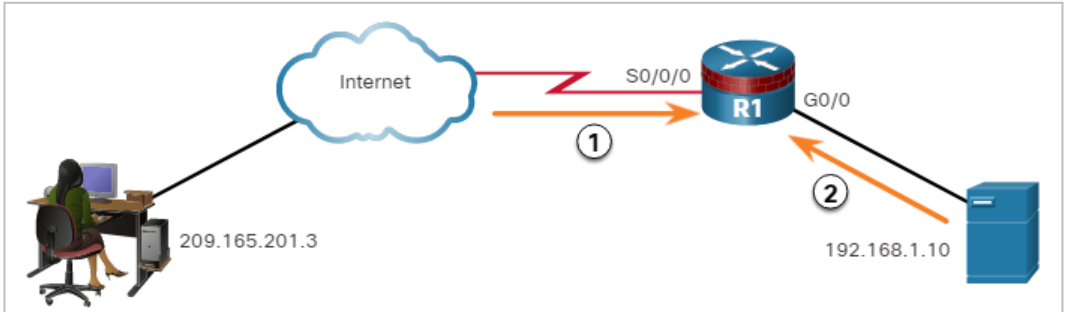
- ICMP can be used to identify hosts on a network, the structure of a network, and determine the operating systems at use on the network. It can also be used as a vehicle for various types of DoS attacks.
- ICMP can also be used for data exfiltration.
- Because of the concern that ICMP can be used to surveil or deny service from outside of the network, ICMP traffic from inside the network is sometimes overlooked.
- Some varieties of malware use crafted ICMP packets to transfer files from infected hosts to threat actors using this method, which is known as ICMP tunneling.

24.2 Security Technologies

ACLs

- Access Control Lists (ACLs) and packet filtering are technologies that contribute to an evolving set of network security protections.
- The figure shows the use of ACLs to permit only specific types of Internet Control Message Protocol (ICMP) traffic. The server at 192.168.1.10 is part of the inside network and is allowed to send ping requests to the outside host at 209.165.201.3.
- The outside host's return ICMP traffic is allowed if it is an ICMP reply or any ICMP unreachable message. All other ICMP traffic types are denied.

Mitigating ICMP Abuse



1. Rules on R1 for ICMP traffic from the Internet

```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

2. Rules on R1 for ICMP traffic from inside the network

```
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 114 deny icmp any any
access-list 114 permit ip any any
```

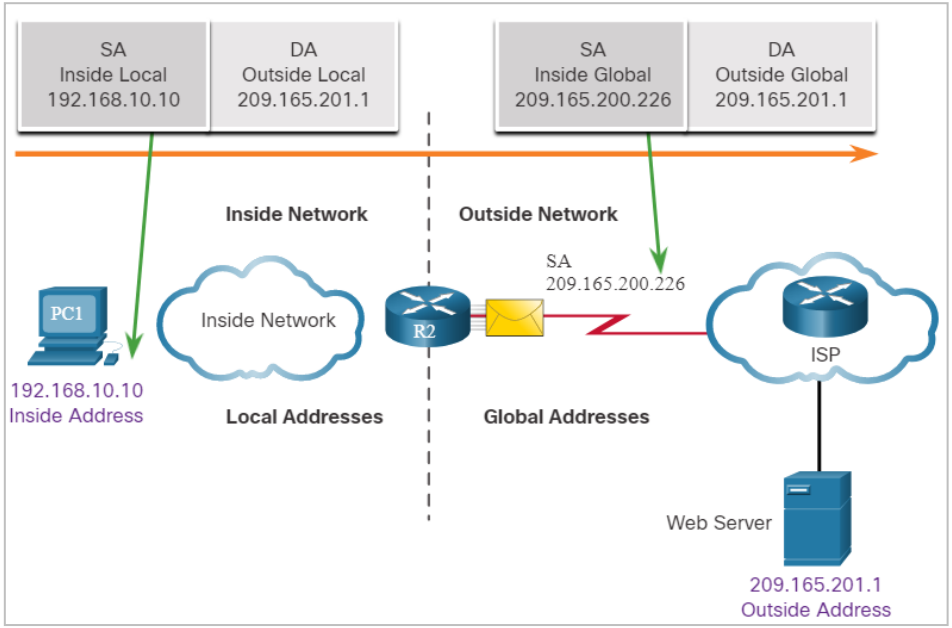
ACLs (Contd.)

- Attackers can determine which IP addresses, protocols, and ports are allowed by ACLs. This can be done either by port scanning or penetration testing, or through other forms of reconnaissance.
- Attackers can craft packets that use spoofed source IP addresses.
- Applications can establish connections on arbitrary ports. Other features of protocol traffic can also be manipulated, such as the established flag in TCP segments. Rules cannot be anticipated and configured for all emerging packet manipulation techniques.
- In order to detect and react to packet manipulation, more sophisticated behavior and context-based measures need to be taken.
- Cisco Next Generation firewalls, Advanced Malware Protection (AMP), and email and web content appliances are able to address the shortcomings of rule-based security measures.

NAT and PAT

- Network Address Translation (NAT) and Port Address Translation (PAT) can complicate security monitoring.
- The figure shows the relationship between internal and external addresses that are used as Source Addresses (SA) and Destination Addresses (DA).
- If PAT is in effect, it could be difficult to log the specific inside device that is requesting and receiving the traffic when it enters the network.
- This problem can be relevant with NetFlow data. NetFlow flows are unidirectional and are defined by the addresses and ports that they share.

Network Address Translation



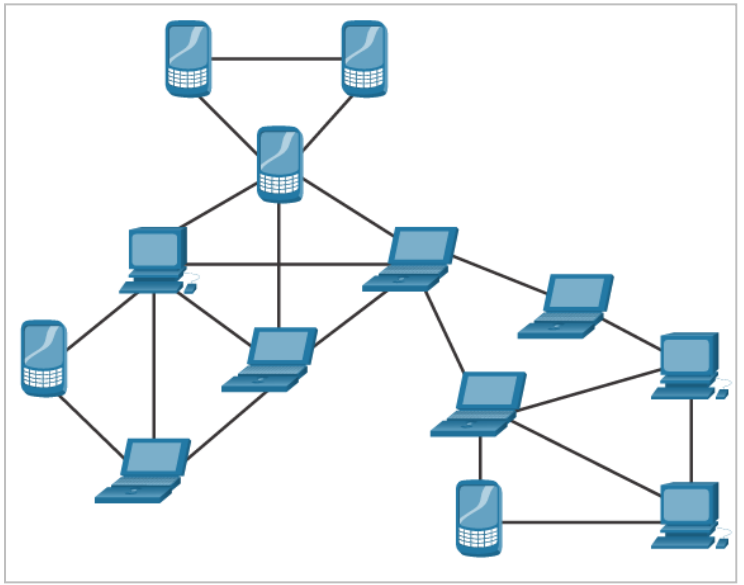
Encryption, Encapsulation, and Tunneling

- Encryption can present challenges to security monitoring by making packet details unreadable.
- Encryption is part of VPN technologies. In VPNs, IP is used to carry encrypted traffic.
- The encrypted traffic essentially establishes a virtual point-to-point connection between networks over public facilities.
- Encryption makes the traffic unreadable to any other devices but the VPN endpoints.
- A similar technology can be used to create a virtual point-to-point connection between an internal host and threat actor devices.
- Malware can establish an encrypted tunnel that rides on a common and trusted protocol, and use it to exfiltrate data from the network.

Peer-to-Peer Networking and Tor

- In peer-to-peer (P2P) networking, shown in the figure, hosts can operate in both client and server roles.
- The three types of P2P applications are file sharing, processor sharing, and instant messaging.
- In file sharing P2P, files on a participating machine are shared with members of the P2P network.
- Bitcoin is a P2P operation and BitTorrent is a P2P file sharing network.
- File-sharing P2P applications should not be allowed on corporate networks. P2P network activity can avoid firewall protections and is a common vector for the spread of malware.

P2P

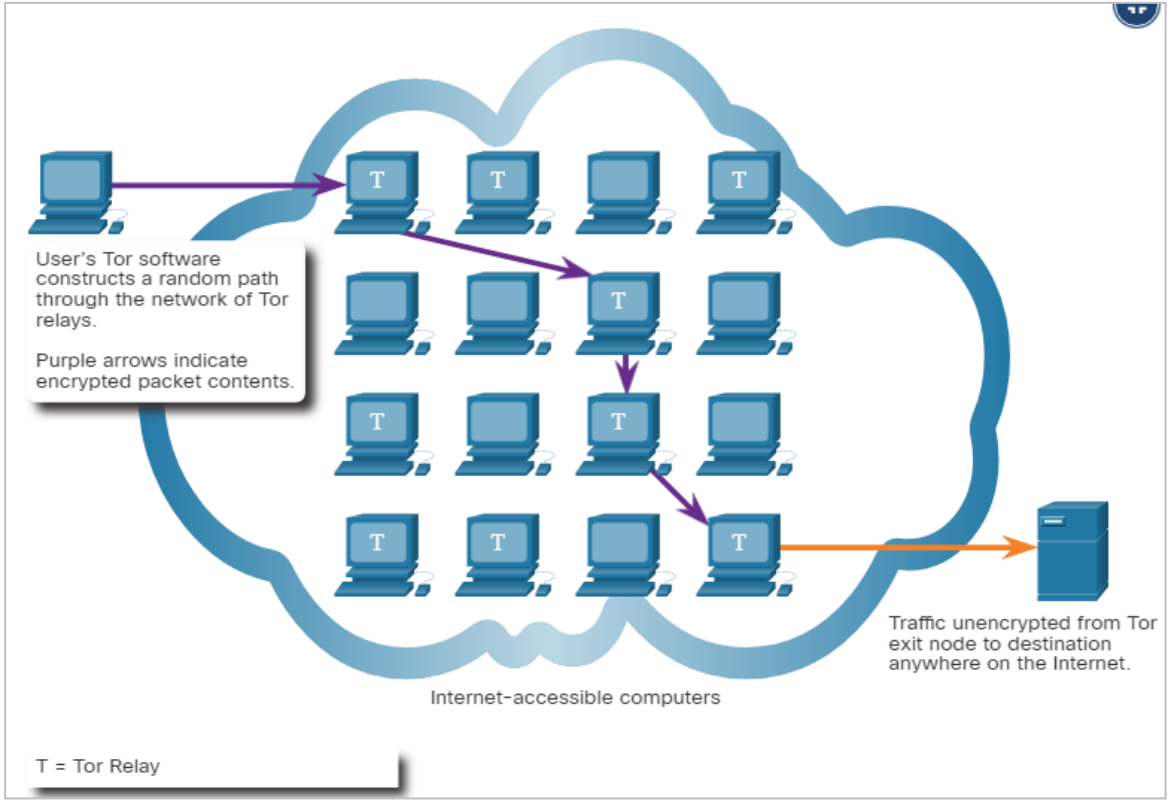


Peer-to-Peer Networking and Tor (Contd.)

- P2P is inherently dynamic. It can operate by connecting to numerous destination IP addresses, and it can also use dynamic port numbering.
- Processor sharing P2P networks donate processor cycles to distributed computational tasks.
- Cancer research, searching for extraterrestrials, and scientific research use donated processor cycles to distribute computational tasks.
- Instant messaging (IM) is also considered to be a P2P application.
- IM has legitimate value within organizations that have geographically distributed project teams.
- In this case, specialized IM applications are available, such as the Webex Teams platform, which are more secure than IM that uses public servers.

Peer-to-Peer Networking and Tor (Contd.)

- Tor is a software platform and network of P2P hosts that function as internet routers on the Tor network.
- The Tor network allows users to browse the internet anonymously. Users access the Tor network by using a special browser.
- When browsing begins, the browser constructs a layered end-to-end path across the Tor server network that is encrypted, as shown in the figure.



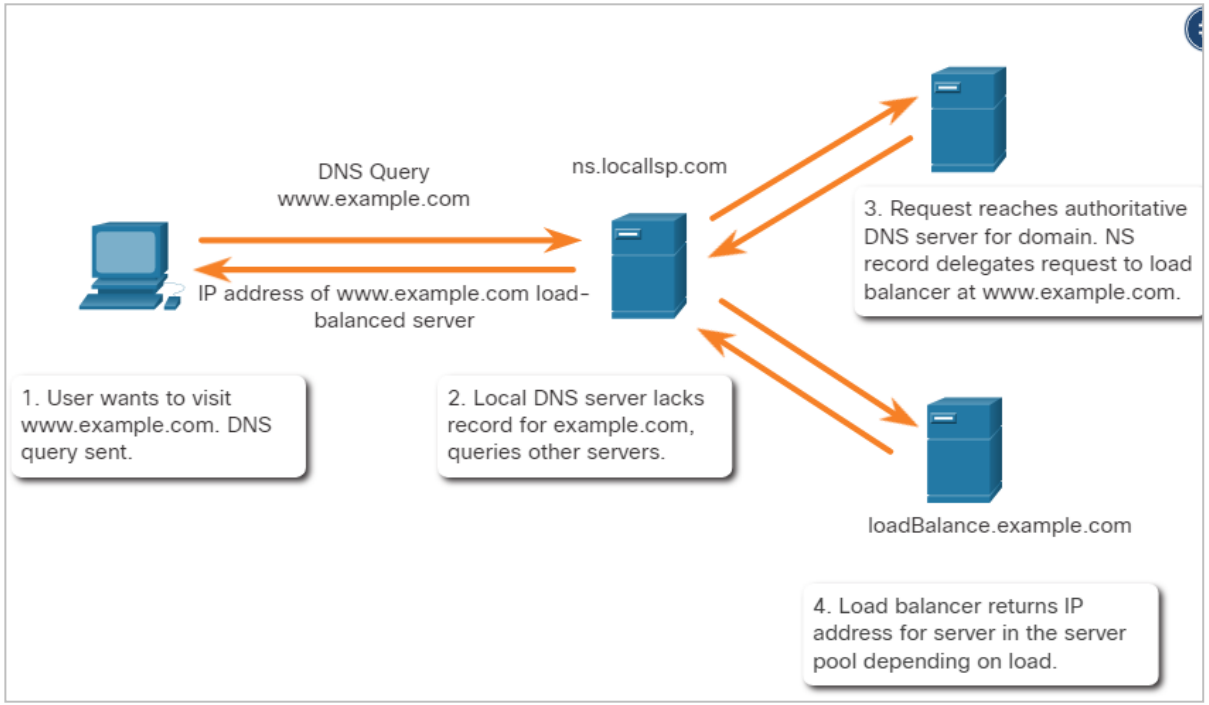
Peer-to-Peer Networking and Tor (Contd.)

- Each encrypted layer is "peeled away" like the layers of an onion as the traffic traverses a Tor relay. The layers contain encrypted next-hop information that can only be read by the router that needs to read the information.
- In this way, no single device knows the entire path to the destination, and routing information is readable only by the device that requires it.
- Finally, at the end of the Tor path, the traffic reaches its internet destination.
- When traffic is returned to the source, an encrypted layered path is again constructed.
- Tor presents a number of challenges to cybersecurity analysts.
- First, Tor is widely used by criminal organizations on the "dark net."
- Also, Tor has been used as a communications channel for malware CnC.
- As the destination IP address of Tor traffic is confused by encryption, with only the next-hop Tor node known, Tor traffic avoids blacklists that have been configured on security devices.

Load Balancing

- Load balancing involves the distribution of traffic between devices or network paths to prevent overwhelming network resources with too much traffic.
- If redundant resources exist, a load balancing algorithm or device will work to distribute traffic between those resources, as shown in the figure.
- One way this is done is through techniques that use DNS to send traffic to resources that have the same domain name but multiple IP addresses.

Load Balancing with DNS Delegation



Load Balancing (Contd.)

- In some cases, the distribution may be to servers that are distributed geographically. This results in single internet transaction which is represented by multiple IP addresses on the incoming packets. This may cause suspicious features to appear in packet captures.
- Also, some load balancing manager (LBM) devices use probes to test for the performance of different paths and the health of different devices.
- An LBM may send probes to the different servers that it is load balancing traffic to in order to detect that the servers are operating.
- This is done to avoid sending traffic to a resource that is not available.
- These probes can appear to be suspicious traffic if the cybersecurity analyst is not aware that this traffic is part of the operation of the LBM.

24.3 Technologies and Protocols Summary

What Did I Learn in this Module?

- Syslog is used to send log entries to central servers that run a syslog daemon. This centralization of log collection helps to make security monitoring practical. As syslog is so important to security monitoring, syslog servers may be a target for threat actors.
- Syslog messages are usually timestamped. As the messages come from many devices, it is important that the devices share a consistent timeclock by using Network Time Protocol (NTP).
- Attackers encapsulate different network protocols within DNS to evade security devices.
- DNS is now used by many types of malware. Some varieties of malware use DNS to communicate with command-and-control (CnC) servers and to exfiltrate data in traffic disguised as normal DNS queries.
- An exploit of HTTP is called iFrame (inline frame) injection. To address the alteration or interception of confidential data , HTTPS should be adopted.
- HTTPS adds a layer of encryption to the HTTP protocol by using secure socket layer (SSL), making the HTTP data unreadable.

What Did I Learn in this Module? (Contd.)

- Email protocols such as SMTP, POP3, and IMAP can be used by threat actors to spread malware, exfiltrate data, or provide channels to malware CnC servers.
- ICMP can be used to identify hosts on a network, the structure of a network, and determine the operating systems at use on the network.
- It can also be used as a vehicle for various types of DoS attack and can also be used for data exfiltration.
- Attackers can determine which IP addresses, protocols, and ports are allowed by ACLs. This can be done either by port scanning or penetration testing, or through other forms of reconnaissance.
- Network Address Translation (NAT) and Port Address Translation (PAT) can complicate security monitoring.
- This problem can be especially relevant with NetFlow data which are unidirectional and are defined by the addresses and ports that they share.

What Did I Learn in this Module? (Contd.)

- Encryption can present challenges to security monitoring by making packet details unreadable. Encryption is part of VPN technologies.
- In peer-to-peer (P2P) networking, hosts can operate in both client and server roles.
- Three types of P2P applications exist: file sharing, processor sharing, and instant messaging.
- Tor is a software platform and network of P2P hosts that function as internet routers on the Tor network. This allows users to browse the internet anonymously.
- Load balancing involves the distribution of traffic between devices or network paths to prevent overwhelming network resources with too much traffic.
- This can be achieved through various techniques that use DNS to send traffic to resources that have the same domain name but multiple IP addresses.
- Some load balancing manager (LBM) devices use probes to test for the performance of different paths and the health of different devices.


CISCO