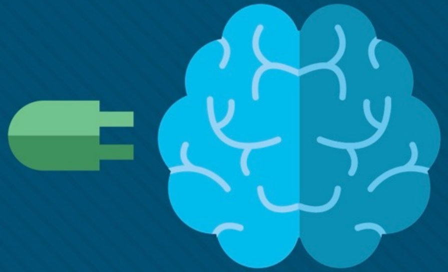


Chapter 9: Security Monitoring

Information Security

Dr. Ayman Aljarbouh

9.1 Technologies and Protocols

Module Objectives

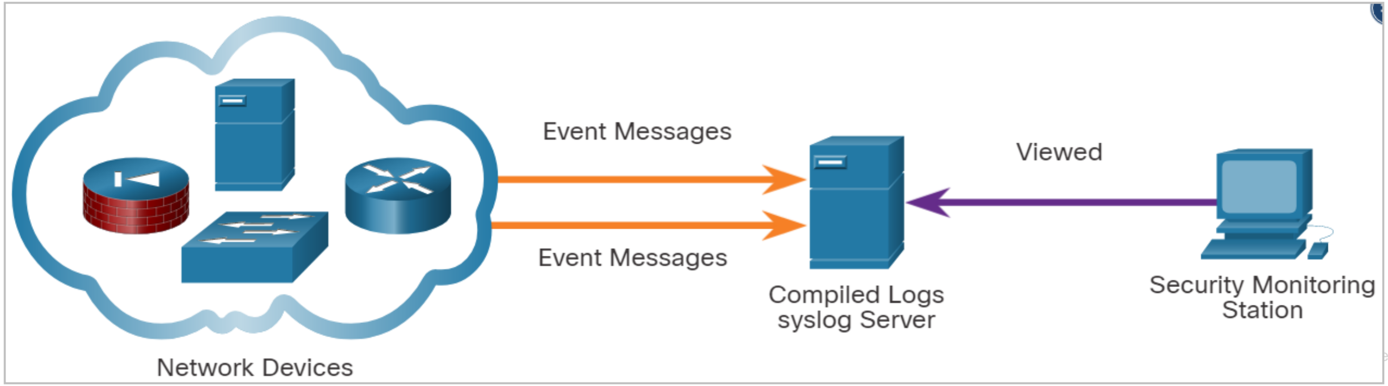
Module Title: Technologies and Protocols

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.

Syslog and NTP

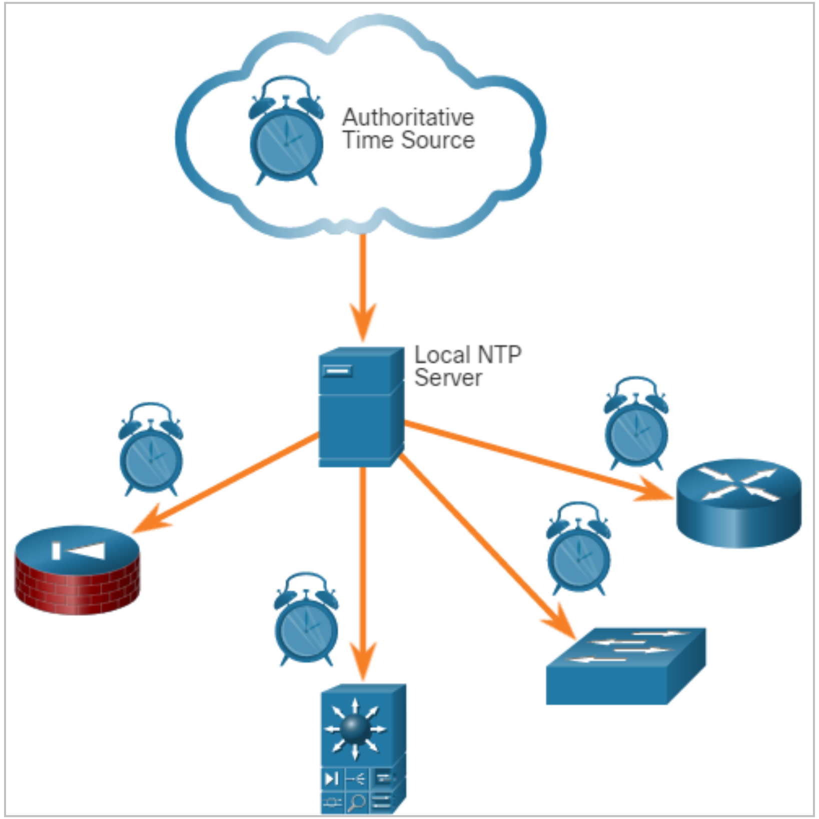
- Syslog and Network Time Protocol (NTP) essential to work of cybersecurity analyst
  - Syslog is used for logging event messages from network devices and endpoints.
  - Syslog servers typically listen on UDP port 514.
  - Syslog servers may be a target for threat actors.
  - Hackers may block the transfer of data, tamper with log data, or tamper with software that creates and transmits log messages.
  - Enhancements provided by syslog-ng (next generation).



Monitoring Common Protocols

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.



Monitoring Common Protocols

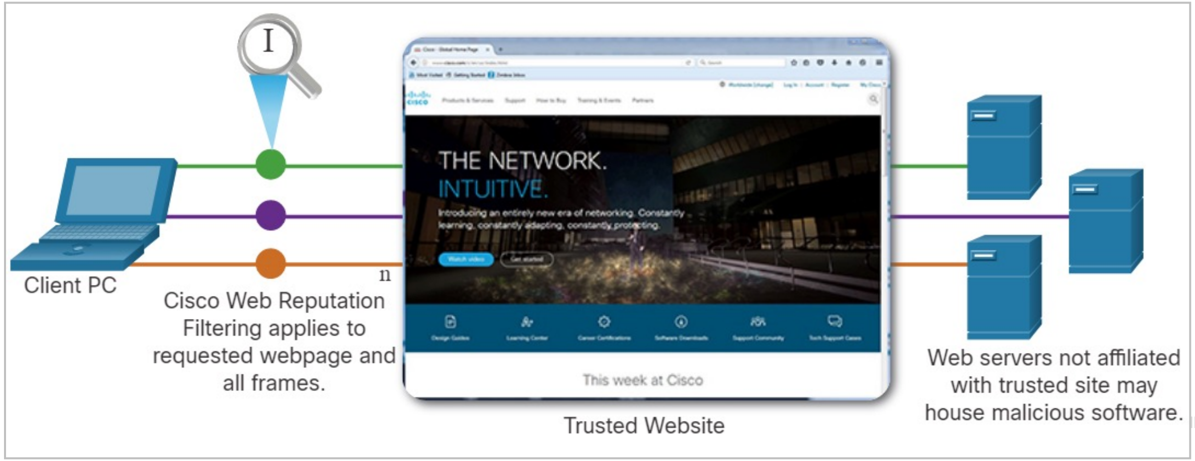
HTTP and HTTPS

- 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.

Monitoring Common Protocols

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.

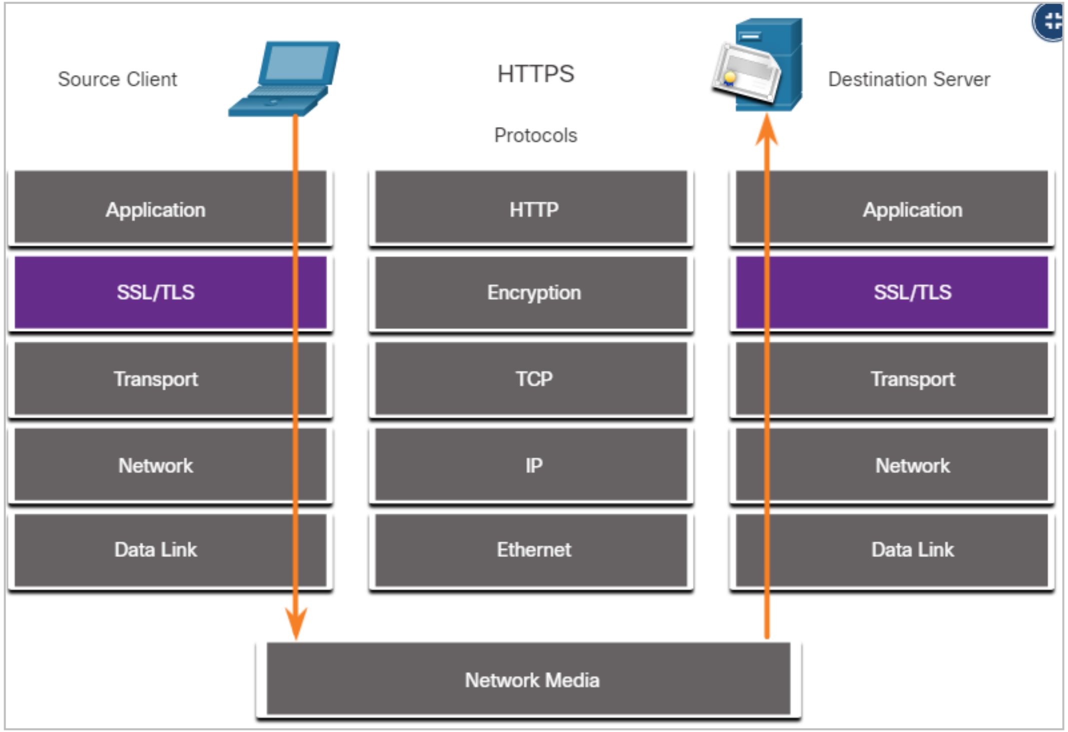

Client PC
Cisco Web Reputation Filtering applies to requested webpage and all frames.
THE NETWORK.
INTUITIVE.
Introducing an entirely new era of networking. Constantly learning, constantly adapting, constantly protecting.
This week at Cisco
Trusted Website
Web servers not affiliated with trusted site may house malicious software.

Monitoring Common Protocols

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.

HTTPS Protocol Diagram



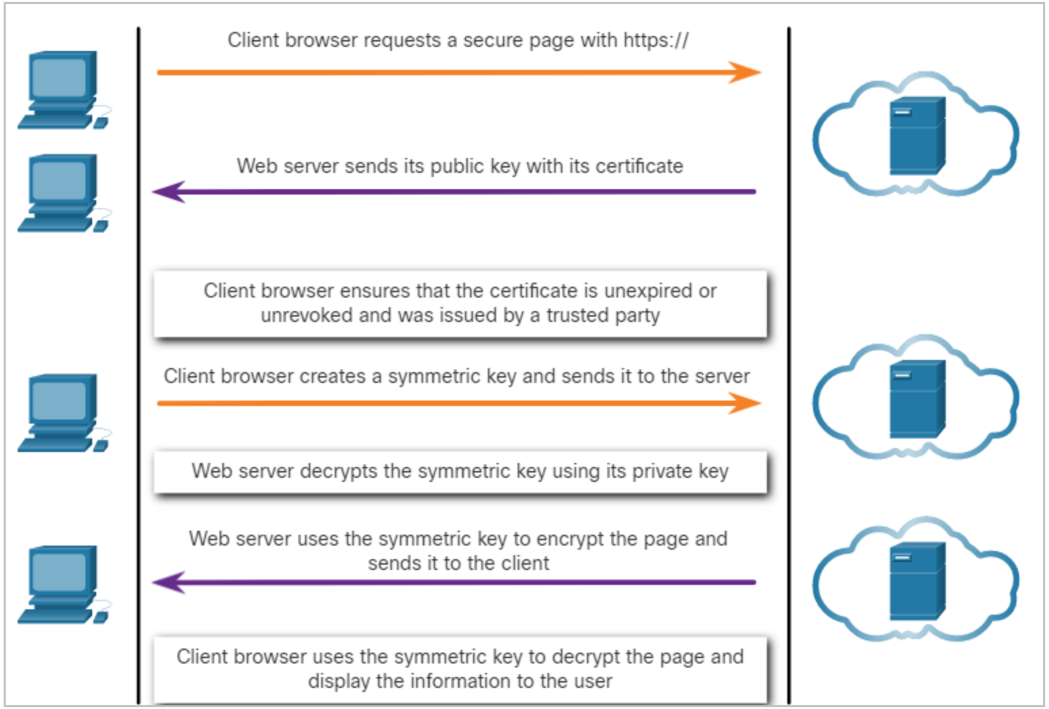
Source Client	HTTPS Protocols	Destination Server
Application	HTTP	Application
SSL/TLS	Encryption	SSL/TLS
Transport	TCP	Transport
Network	IP	Network
Data Link	Ethernet	Data Link

Network Media

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.

HTTPS Transactions



Client browser requests a secure page with https://

Web server sends its public key with its certificate

Client browser ensures that the certificate is unexpired or unrevoked and was issued by a trusted party

Client browser creates a symmetric key and sends it to the server

Web server decrypts the symmetric key using its private key

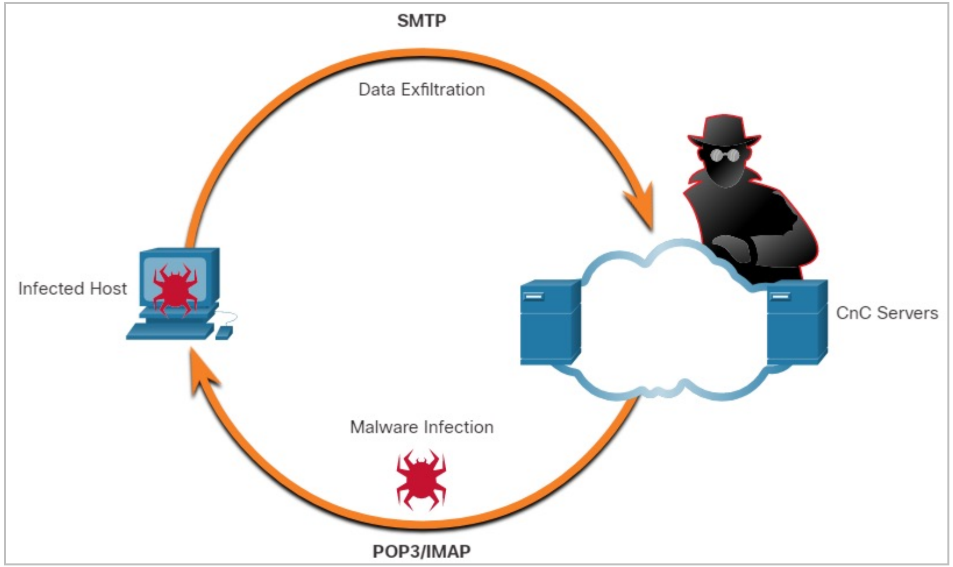
Web server uses the symmetric key to encrypt the page and sends it to the client

Client browser uses the symmetric key to decrypt the page and display the information to the user

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.

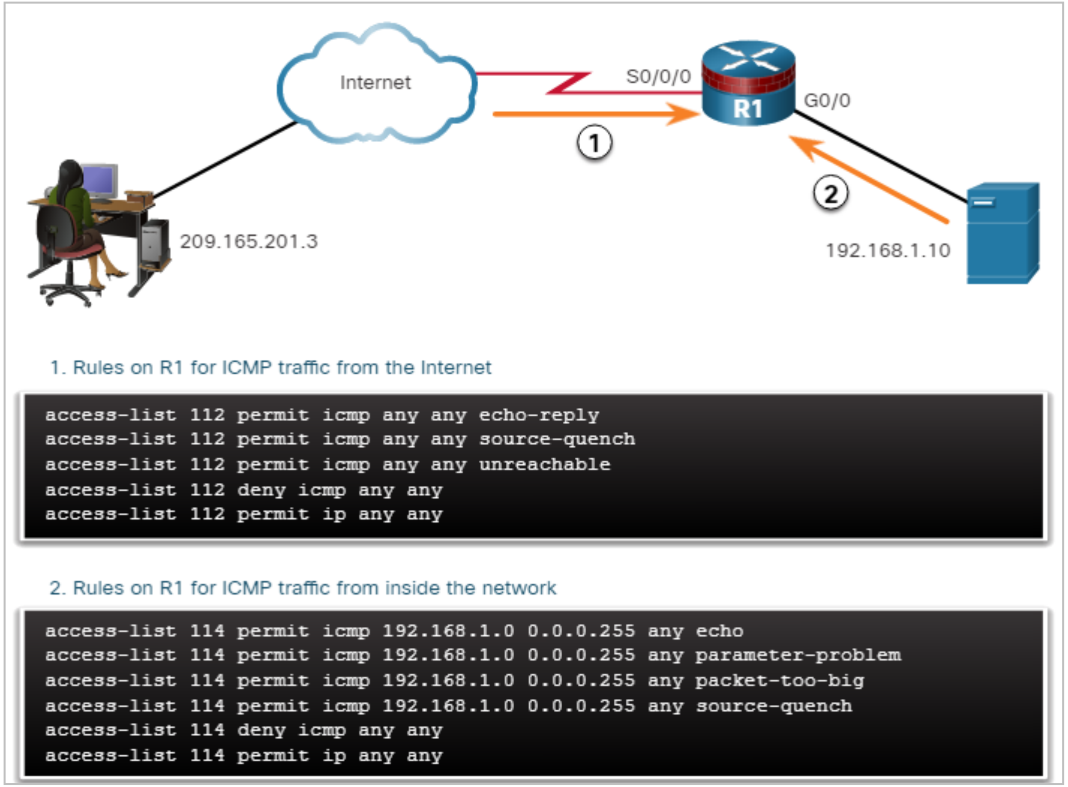
Email Protocol Threats



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
```

Security Technologies

ACLs (Contd.)

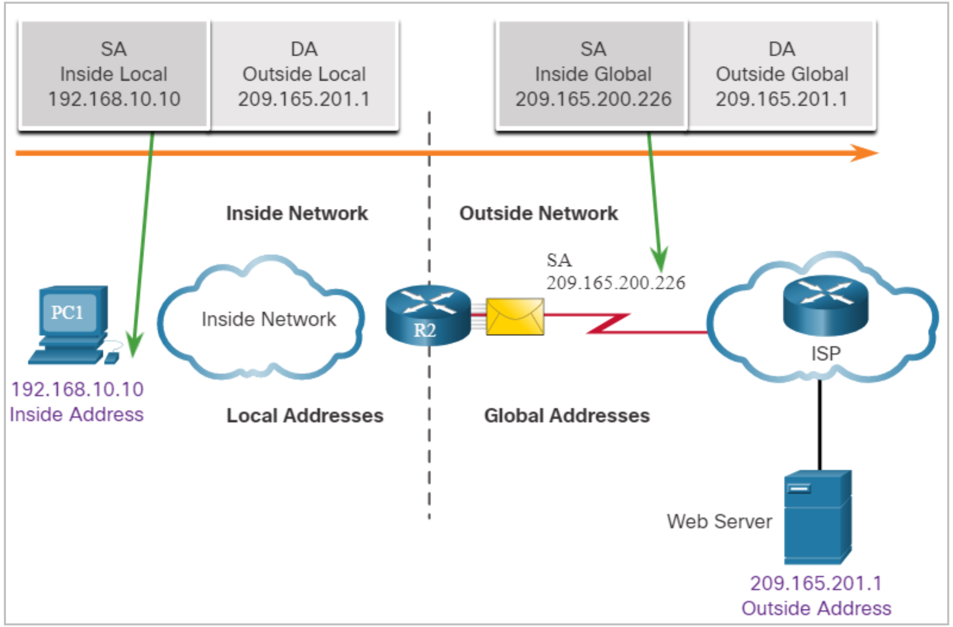
- Attackers can determine which IP addresses, protocols, and ports are allowed by ACLs. This can be done either by port scanning or penetration testing, or through other forms of reconnaissance.
- Attackers can craft packets that use spoofed source IP addresses.
- Applications can establish connections 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.

Security Technologies

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.

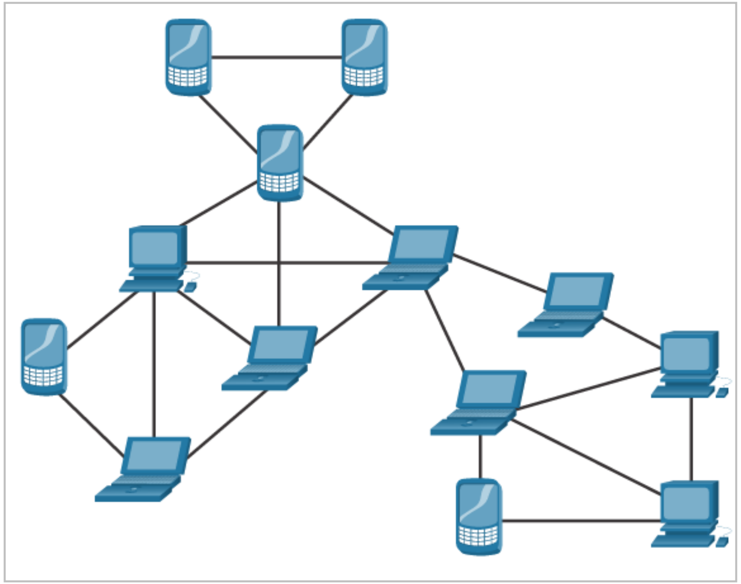
Network Address Translation



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.

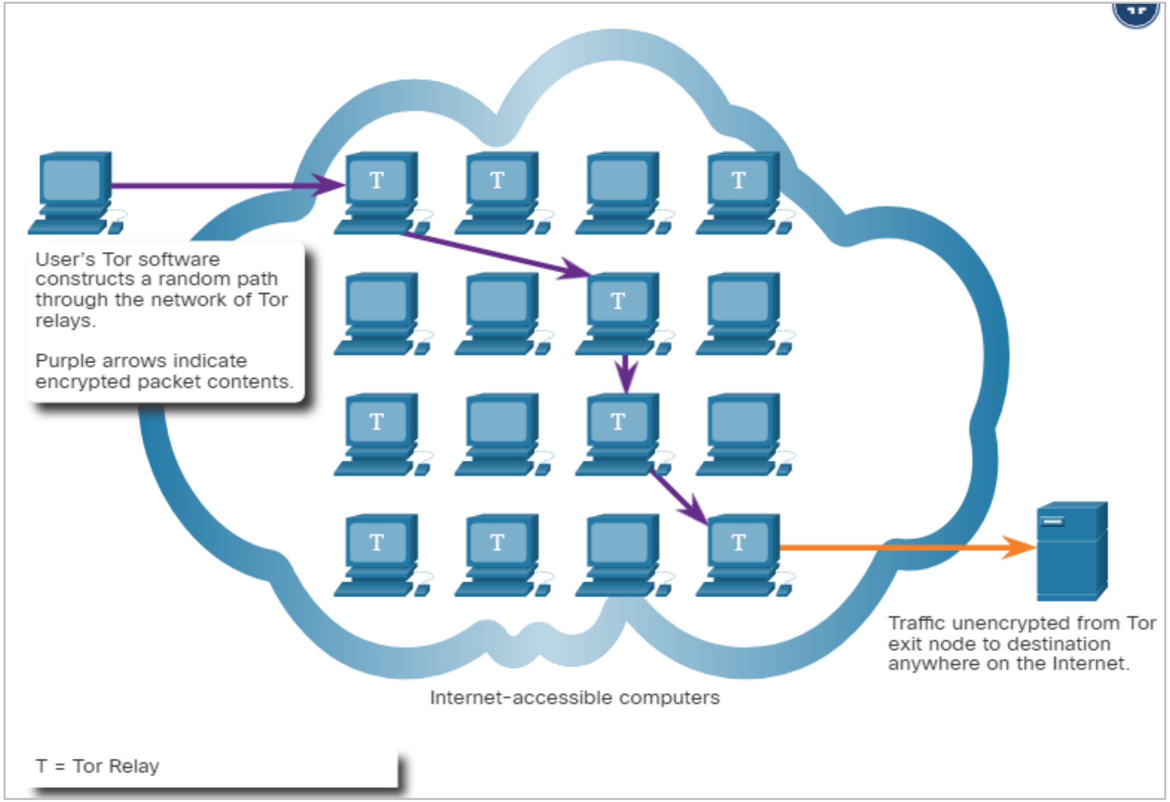
P2P



Security Technologies

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.


User's Tor software constructs a random path through the network of Tor relays.

Purple arrows indicate encrypted packet contents.

Traffic unencrypted from Tor exit node to destination anywhere on the Internet.

Internet-accessible computers

T = Tor Relay

Security Monitoring

New Terms and Commands

- Network Time Protocol (NTP)
- Command-and-control (CnC)
- Secure Socket Layer (SSL)
- Access Control Lists (ACLs)
- Advanced Malware Protection (AMP)

- Network Address Translation (NAT)
- Port Address Translation (PAT)
- Source Addresses (SA)
- Destination Addresses (DA)
- peer-to-peer (P2P)

Security Monitoring

Lab 32 - Logging from Multiple Sources

In this lab, you will do the following:

- Use Packet Tracer to compare network data generated by multiple sources including syslog, AAA, and NetFlow.