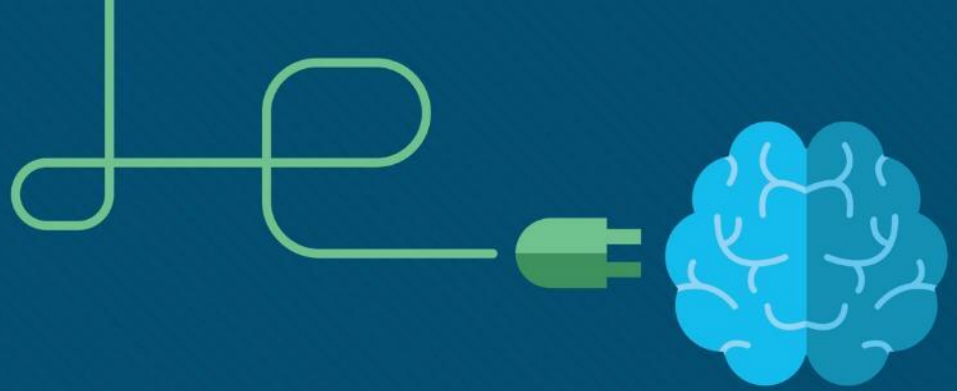


Security Monitoring

Technologies and Protocols

- Explain how security technologies affect security monitoring.
  - Explain the behavior of common network protocols in the context of security monitoring.
  - Explain how security technologies affect the ability to monitor common network protocols.

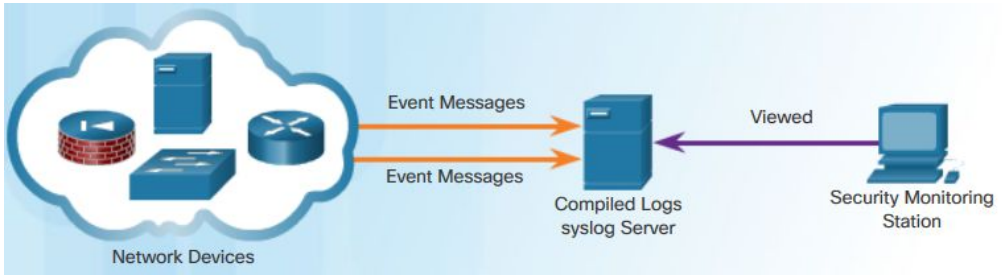
Log Files

- Explain the types of log files used in security monitoring.
  - Describe the types of data used in security monitoring.
  - Describe the elements of an end device log file.
  - Describe the elements of a network device log file.

11.1 Technologies and Protocols

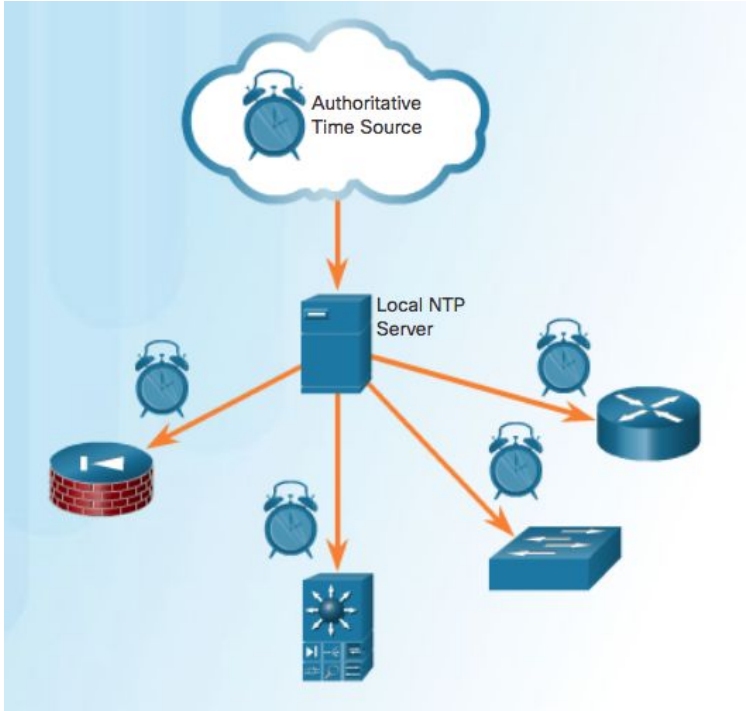
Syslog and NTP

- 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).



NTP

- Syslog messages are usually timestamped using the Network Time Protocol (NTP).
- NTP operates on UDP port 123.
- Timestamps are essential for detection of an exploit.
- Threat actors may attempt to attack NTP to corrupt time information used to correlate logged network events.
- Threat actors use NTP systems to direct DDoS attacks.



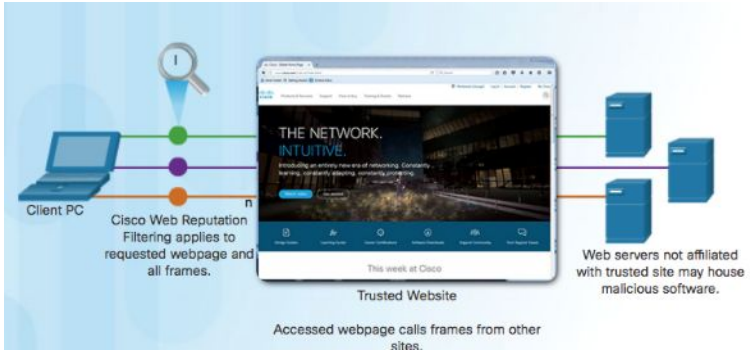
DNS

- DNS is used by many types of malware.
- Attackers encapsulate different network protocols within DNS to evade security devices.
- Some 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.
- 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.

HTTP and HTTPS

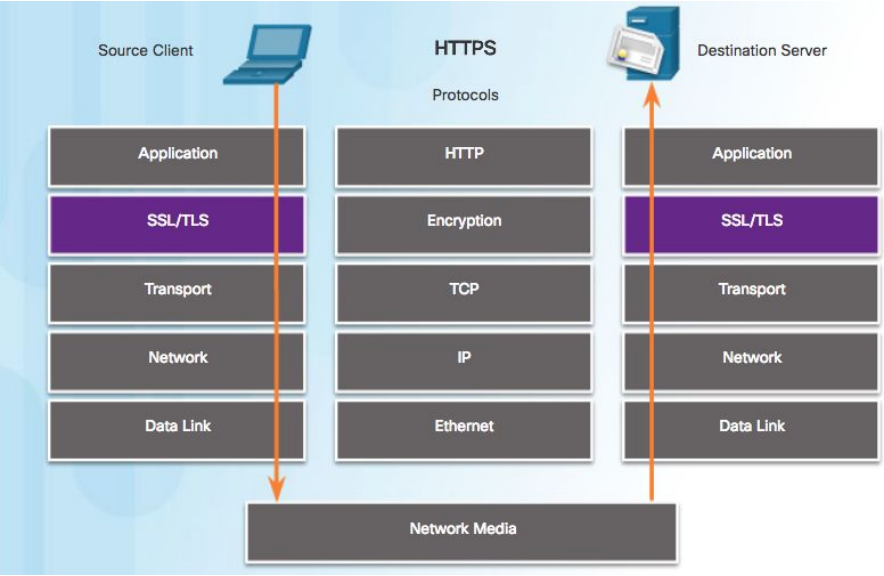
- All information carried in HTTP is transmitted in plaintext from the source computer to the destination on the Internet.
- HTTP does not protect data from alteration or interception.
- Web-based threats consist of malware scripts that have been planted on webservers that direct browsers to infected servers by loading iframes.
  - 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.

HTTP iFrame Injection Exploit



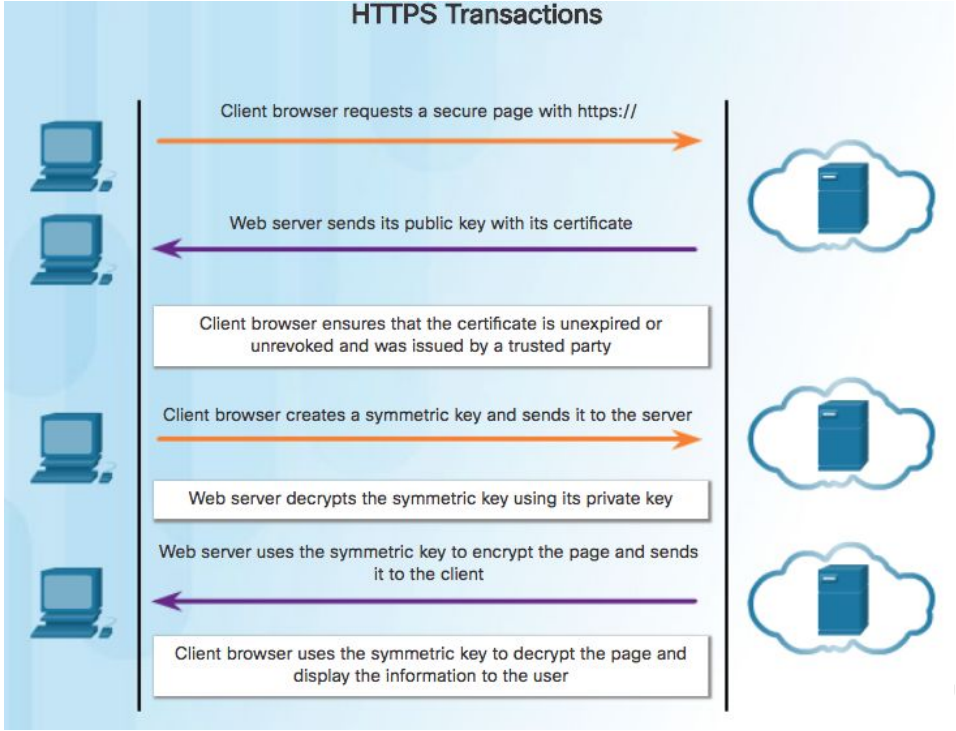
HTTP and HTTPS (Cont.)

- HTTPS adds a layer of encryption to the HTTP protocol by using secure socket layer (SSL).
  - SSL makes the HTTP data unreadable as it leaves the source computer until it reaches the server.



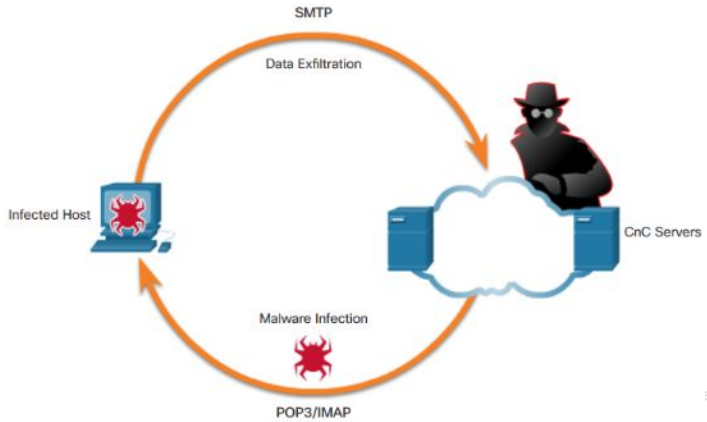
HTTP and HTTPS (Cont.)

- Encrypted HTTPS traffic complicates network security monitoring.
- HTTPS adds complexity to packet captures.



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.
  - SMTP sends data from a host to a mail server and between mail servers and is not always monitored.
  - IMAP and POP3 are used to download email messages from a mail server to the host computer and can be responsible for bringing malware to the host.
  - Security monitoring can identify when a malware attachment entered the network and which host it first infected.

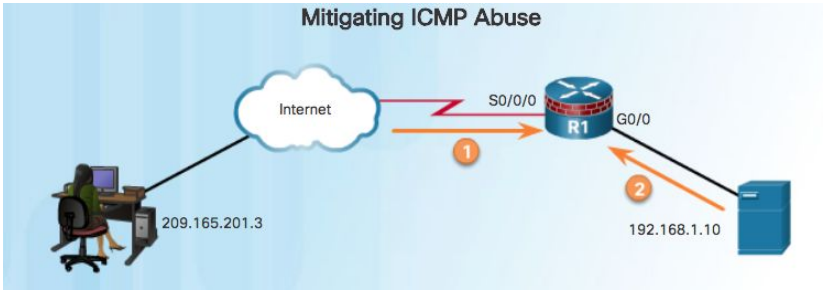


ICMP

- ICMP can be used to craft a number of types of exploits.
  - Can be used to identify hosts on a network, the structure of a network, and determine the operating systems at use on the network.
  - Can also be used as a vehicle for various types of DoS attacks.
  - ICMP can also be used for data exfiltration through ICMP traffic from inside the network.
    - ICMP tunneling - Malware uses crafted ICMP packets to transfer files from infected hosts to threat actors.

ACLs

- ACLs may provide a false sense of security.
  - Attackers can determine which IP addresses, protocols, and ports are allowed by Access Control Lists (ACLs), by port scanning, penetration testing, or through other forms of reconnaissance.
  - Attackers can craft packets that use spoofed source IP addresses or applications can establish connections on arbitrary ports.



1. Rules on R1 for ICMP traffic from the Internet

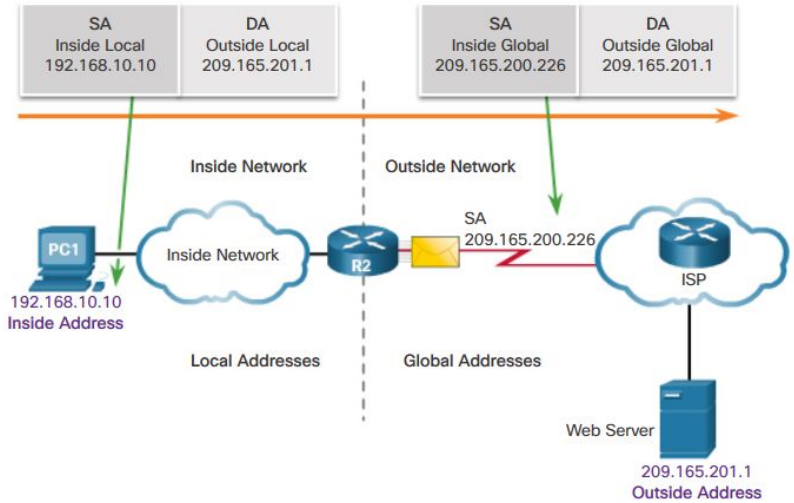
```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

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
```

NAT and PAT

- NAT and PAT can complicate security monitoring.
  - Multiple IP addresses are mapped to one or more public addresses that are visible on the Internet.
  - Hides the individual IP addresses that are inside the network.

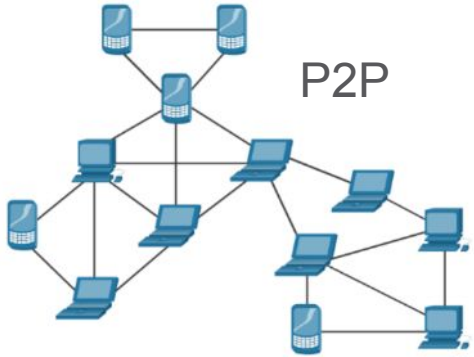


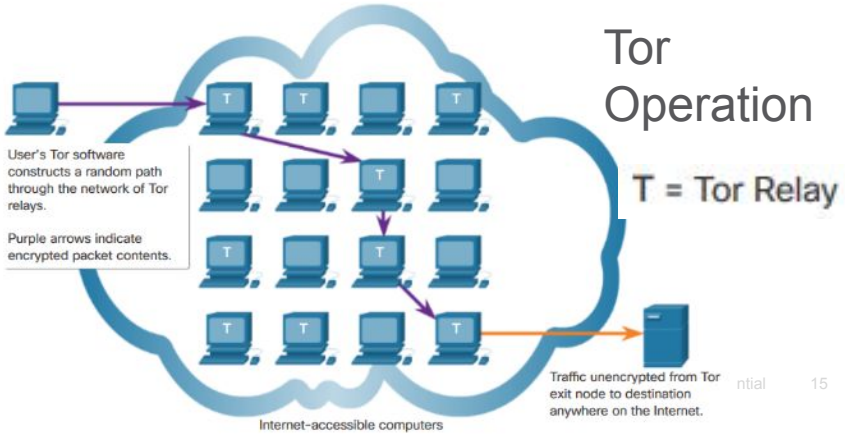
Encryption, Encapsulation, and Tunneling

- Encryption
  - Makes traffic contents unreadable by cybersecurity analysts.
  - Part of Virtual Private Network (VPN) and HTTPS.
- 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

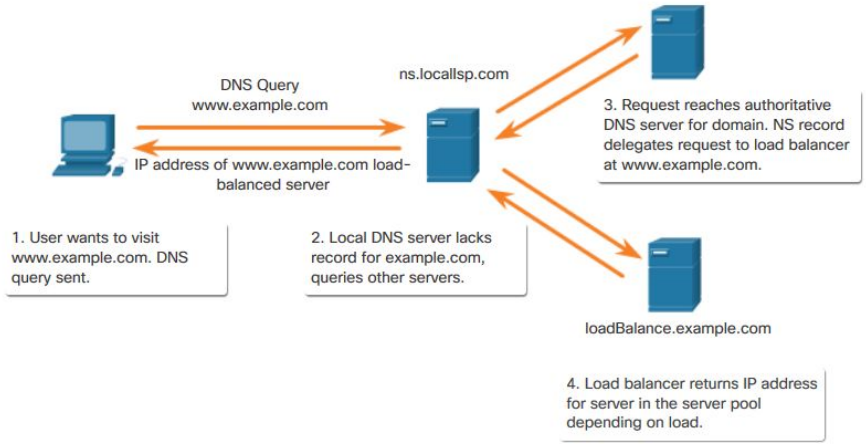
- Peer-to-Peer network activity
  - Can circumvent firewall protections and is a common vector for the spread of malware.
    - Three types of Peer-to-Peer applications exist: file sharing, processor sharing, and IM
    - File-sharing P2P applications should not be allowed on corporate networks.
- Tor is a software platform and network of Peer-to-Peer hosts that function as Internet routers on the Tor network.
  - Allows users to browse the Internet anonymously using a special browser.
  - Can be used to hide identity of threat actors and used by criminal organizations.





Load Balancing

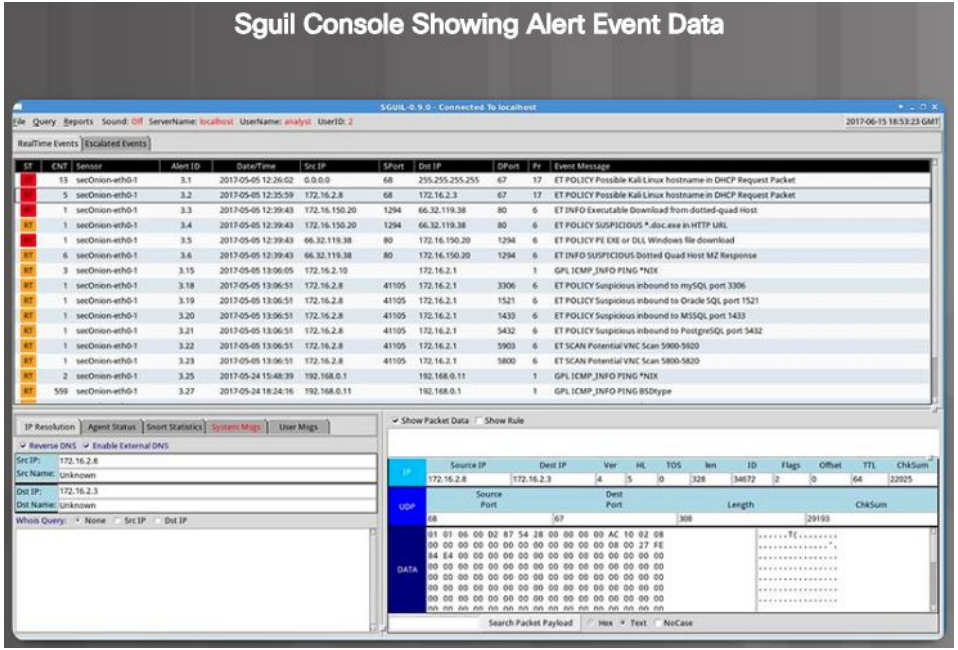
- Load balancing is the distribution of traffic between devices or network paths to prevent overwhelming network resources.
  - Some load balancing approaches use DNS to send traffic to resources that have the same domain name but multiple IP addresses.
  - This can result in a single Internet transaction being represented by multiple IP addresses on the incoming packets.
  - This may cause suspicious features to appear in packet captures.



Log Files

Alert Data

- Alert Data consists of messages generated by IPSs or IDSs in response to traffic that violates a rule or matches the signature of a known exploit.
- A network IDS (NIDS), such as Snort, comes configured with rules for known exploits.
- Alerts are generated by Snort and are made readable and searchable by applications such as Sguil, which are part of the Security Onion suite of NSM tools.

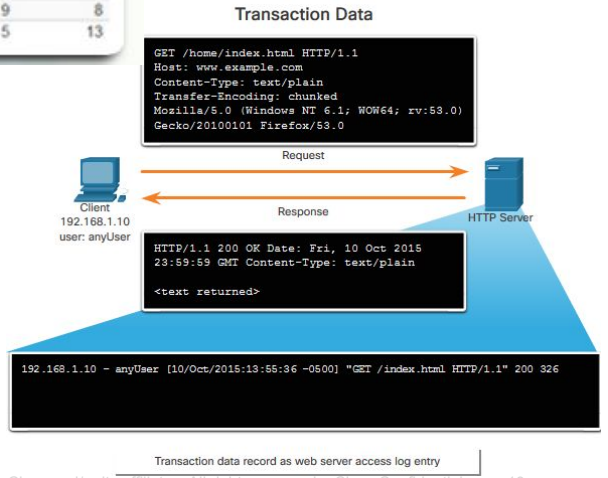


Session and Transaction Data

- Session Data is a record of a conversation between two network endpoints.
  - Includes a session ID, the amount of data transferred by source and destination, and information related to the duration of the session.
  - Bro is a network security monitoring tool.

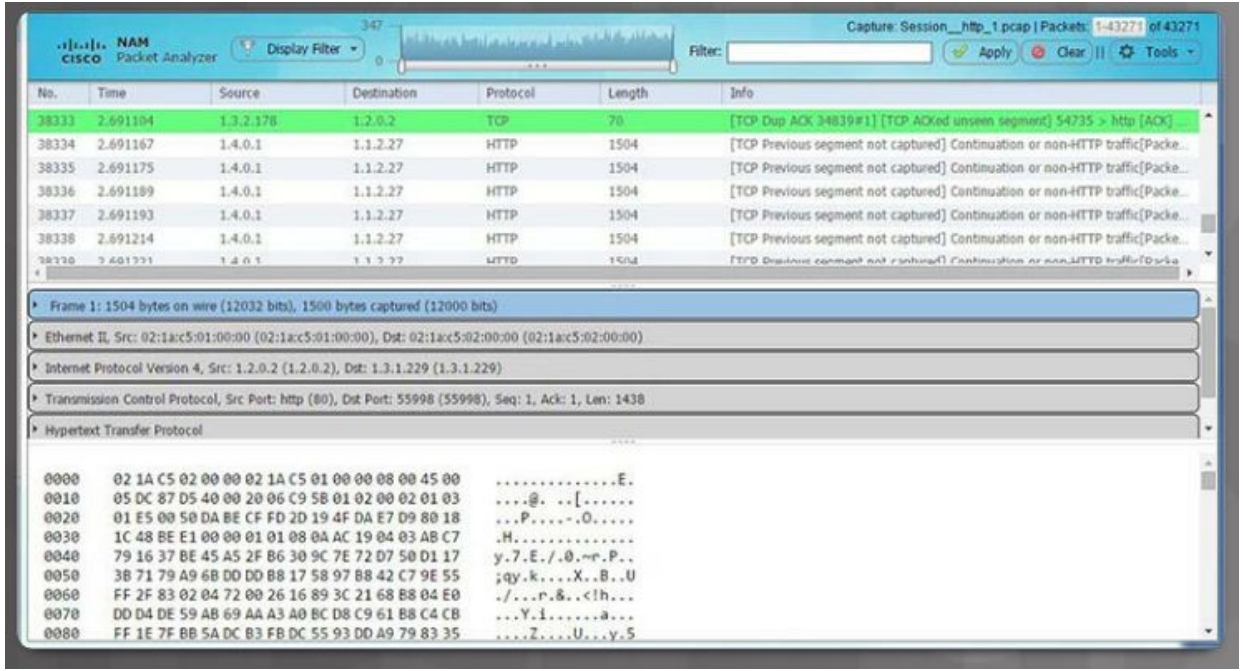
ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	orig_pkts	resp_pkts
1320279567	CEv1Z54N5gT3PwJLog	192.168.2.76	52034	174.129.249.33	80	tcp	http	0.082899	389	1495	5	4
1320279567	CI6Ueb3SkSJHwASNN4	192.168.2.76	52035	184.72.234.3	80	tcp	http	2.56194	905	731	9	8
1320279567	CaTMSv1Sb8HtFunqjj	192.168.2.76	52033	184.72.234.3	80	tcp	http	3.345539	1856	1445	15	13

- Transaction data consists of the messages that are exchanged during network sessions.
  - Can be viewed in packet capture transcripts.



Full Packet Capture

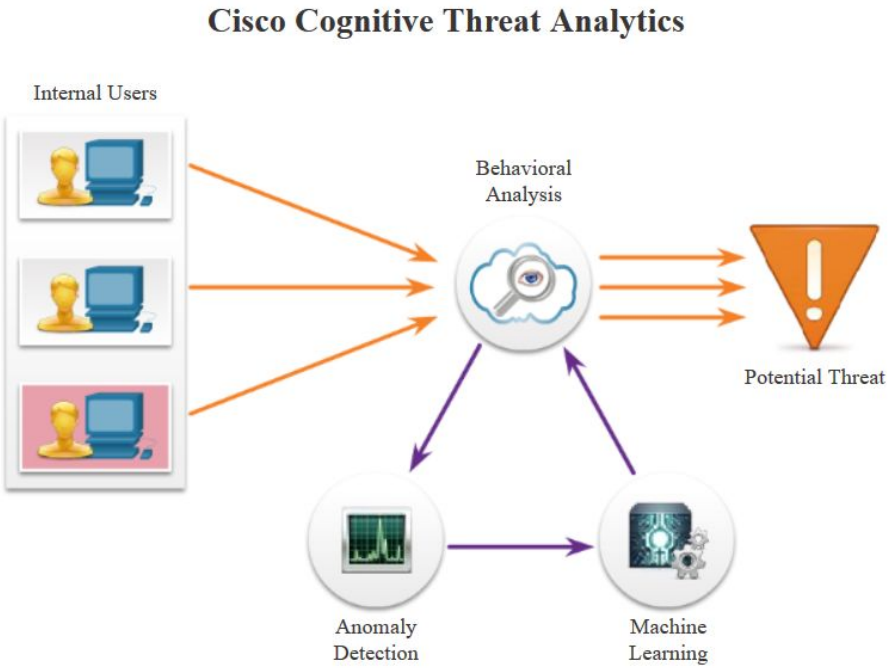
- Full Packet Capture contains the actual contents of the conversations themselves, including the text of email messages, the HTML in webpages, and the files that enter or leave the network.



Cisco Prime Network Analysis Module – Full Packet Capture

Statistical Data

- Statistical Data is about network traffic.
  - Created through the analysis of other forms of network data.
  - Allow conclusions to be made that describe or predict network behavior.
  - Normal network behavior can be compared to current traffic to detect anomalies.
- Cisco Cognitive Threat Analytics is a NSM tool.
  - Able to find malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside an organization's environment.



Host Logs

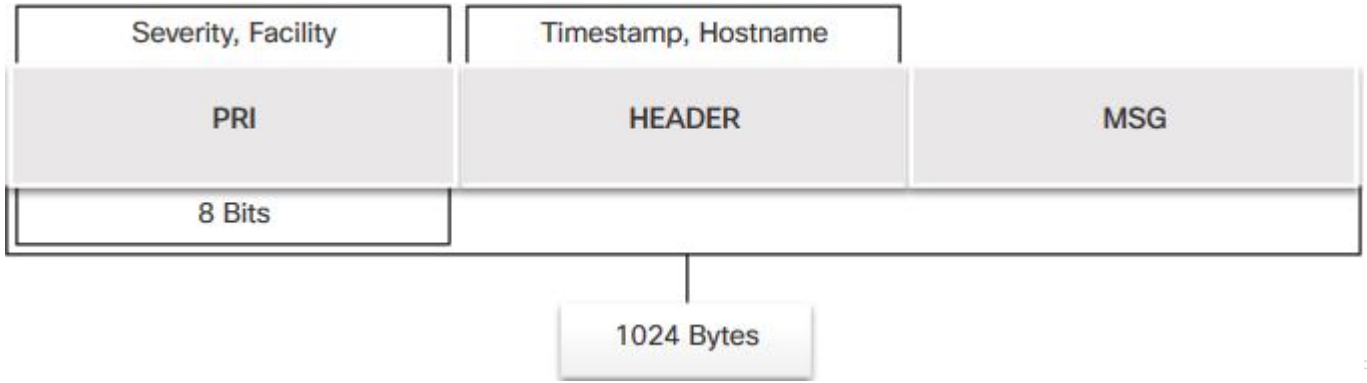
- Host-based intrusion protection (HIDS) runs on individual hosts.
  - HIDS not only detects intrusions, but in the form of host-based firewalls, can also prevent intrusion.
  - Creates logs and stores them on the host.
  - Microsoft Windows host logs are visible locally through Event Viewer.
  - Event Viewer keeps four types of logs: Application logs, System logs, Setup logs, and Security logs.

Event Type	Description
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event.
Information	An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.
Failure Audit	An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

Windows Host Log Event Types

Syslog

- Many types of network devices can be configured to log events to syslog servers.
  - Client/server protocol
  - Syslog messages have three parts: PRI (priority), HEADER, and MSG (message text).
    - PRI consists of two elements, the Facility and Severity of the message.
    - Facility consists of broad categories of sources that generated the message, such as the system, process, or application, directs message to appropriate log file.
    - Severity is a value from 0-7 that defines the severity of the message.



Syslog (Cont.)

Syslog Severity and Facility

Integer	Severity
0	**Emergency**: System is unusable
1	**Alert**: Action must be taken immediately
2	**Critical**: Critical conditions
3	**Error**: Error conditions
4	**Warning**: Warning conditions
5	**Notice**: Normal but significant condition
6	**Informational**: Informational messages

Integer	Facility
0	**kern**: Kernel messages
1	**user**: User-level messages
2	**mail**: Mail system
3	**daemon**: System daemons
4	**auth**: Security/authorization messages
5	**syslog**: Messages generated internally by Syslogd
6	**lpr**: Line printer subsystem
7	**news**: Network news subsystem
8	**uucp**: Unix-to-Unix copy subsystem
9	Clock daemon
10	**authpriv**: Security/authorization messages
11	**ftp**: FTP daemon
12	NTP subsystem
13	Log audit

Priority = (Facility X 8) + Severity

Server Logs

- Server Logs are an essential source of data for network security monitoring.
  - Email and web servers keep access and error logs.
  - DNS proxy server logs document all DNS queries and responses that occur on the network.
  - DNS proxy logs can identify hosts that visited dangerous websites and identify DNS data exfiltration and connections to malware CnC servers.

Web Server Logs

Apache Access Log

```
203.0.113.127 â€“ dsmith [10/Oct/2016:10:26:57 -0500]
"GET /logo_sm.gif HTTP/1.0â€œ 200
2254 ""http://www.example.com/links.html""
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0)
Gecko/20100101 Firefox/47.0"
```

IIS Access Log

```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3,
198.51.100.10, 80, GET, /home.htm, -, 200, 0, 15321,
159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0;
Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0), -,
http://www.example.com
```

Apache Webserver Access Logs

- Apache Webserver access logs record the requests for resources from clients to the server.
  - Two log formats
    - Common log format (CLF)
    - Combined log format, which is CLF with the addition of the referrer and user agent fields

Apache Access Log Format

```
203.0.113.127 - dsmith [10/Oct/2016:10:26:57 -0500] "GET /logo_sm.gif
HTTP/1.0" 200 2254 ""http://www.example.com/links.html""
"Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0"
```

Field	Name	Description	Example
1	Client IP address	IP address of requesting client	203.0.113.127
2	Client identity	Client userid, frequently omitted	-
3	User ID	User name of authenticated user, if any	dsmith
4	Timestamp	Date and time of request	[10/Oct/2016:10:26:57 -0500]
5	Request	Request method and requested resource	GET /logo_sm.gif HTTP/1.0“
6	Status Code	HTTP status code	200
7	Size of Response	Bytes returned to client	2254
8	Referrer	Location, if any, from which the client reached the resource	http://www.example.com/links.html
9	User Agent	Browser used by client	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0

IIS Access Logs

- Microsoft IIS creates access logs that can be viewed from the server with Event Viewer.

IIS Access Log Format

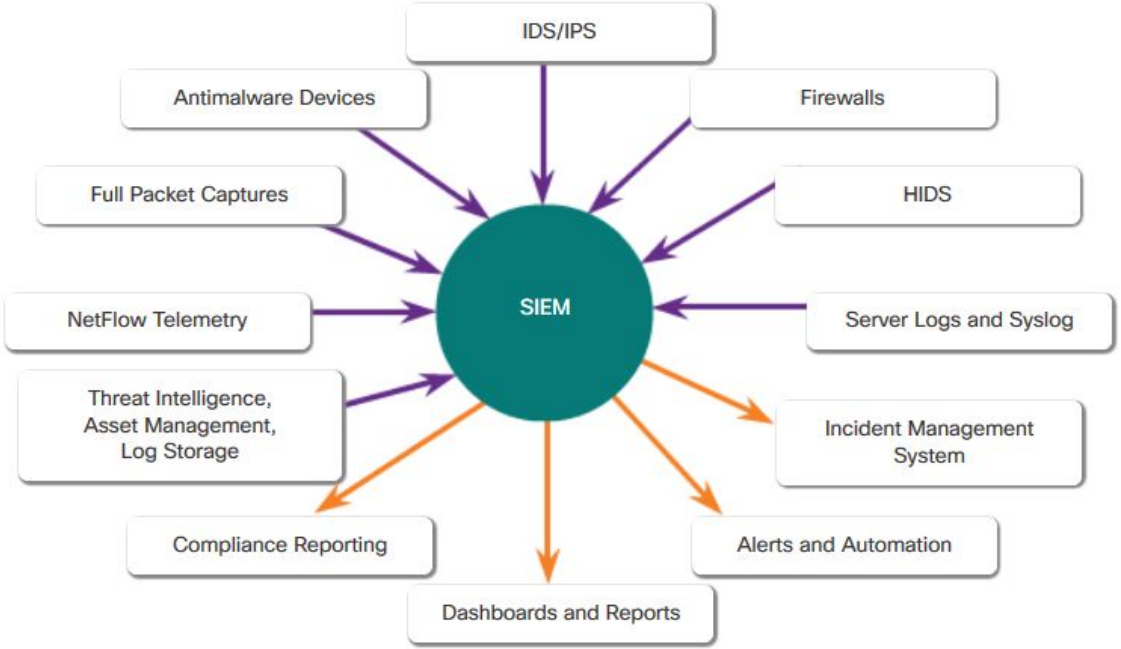
```
6/14/2016, 16:22:43, 203.0.113.24, -, W3SVC2, WEB3, 198.51.100.10, 80, GET,
/home.htm, -, 200, 0, 15321, 159, 15, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0;
Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0), -, http://www.example.com
```

Item	Field	Explanation	Example
Date	date	date on which the activity occurred	6/14/2016
Time	time	UTC time, at which the activity occurred	16:22:22
Client IP Address	c-ip	IP address of the client that made the request	203.0.113.24
User Name	cs-username	authenticated user name	-
Service Name and Instance Number	s-sitename	Internet service name and instance number	W3SVC2
Server Name	s-computername	name of the server that generated the log entry	WEB3
Server IP Address	s-ip	IP address of the server	198.51.100.10
Server Port	s-port	server port for the service	80
Method	cs-method	requested action (HTTP method)	GET
URI Stem	cs-uri-stem	target of the action	/home.htm
URI Query	cs-uri-query	the query the client was trying to perform	-
HTTP Status	sc-status	HTTP status code	200
Win32 Status	sc-win32-status	Windows status code	0
Bytes Sent	sc-bytes	bytes that the server sent	15321
Bytes Received	cs-bytes	bytes that the server received	159
Time Taken	time-taken	length of time that the action took, in milliseconds	15
Protocol Version	cs-version	the protocol version	HTTP/1.1
User Agent	cs(User-Agent)	browser type that the client used	Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0)
Cookie	cs(Cookie)	The content of the cookie sent or received, if any	-
Referrer	cs(Referrer)	site that provided a link	http://www.example.com

SIEM and Log Collection

- Security Information and Event Management (SIEM) technology
  - Provides real-time reporting and long-term analysis of security events.
  - Uses the following functions: Log collection, Normalization, Correlation, Aggregation, Reporting, Compliance
  - A popular SIEM is Splunk.

SIEM Components

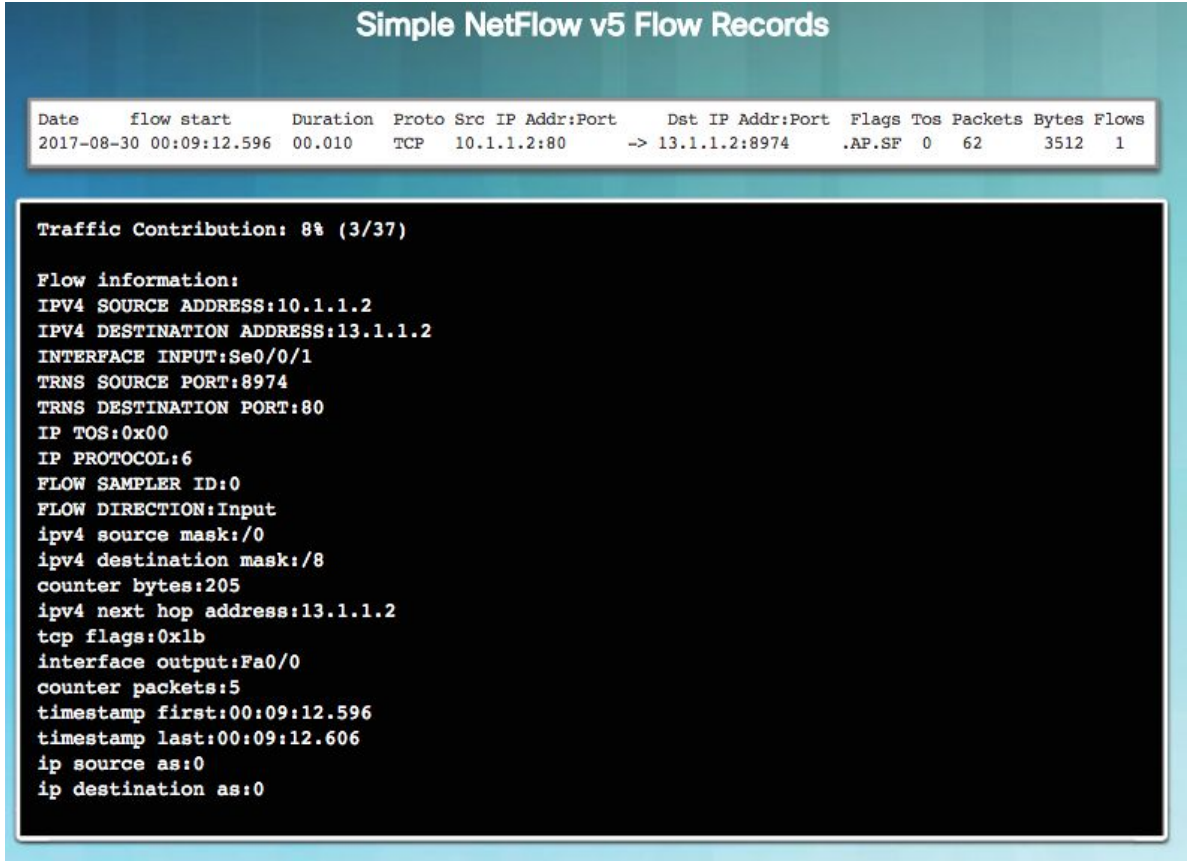


TCPdump

- Tcpdump command line tool is a popular packet analyzer.
  - Displays packet captures in real time, or writes packet captures to a file.
  - Captures detailed packet protocol and content data.
  - Wireshark is a GUI built on tcpdump functionality.

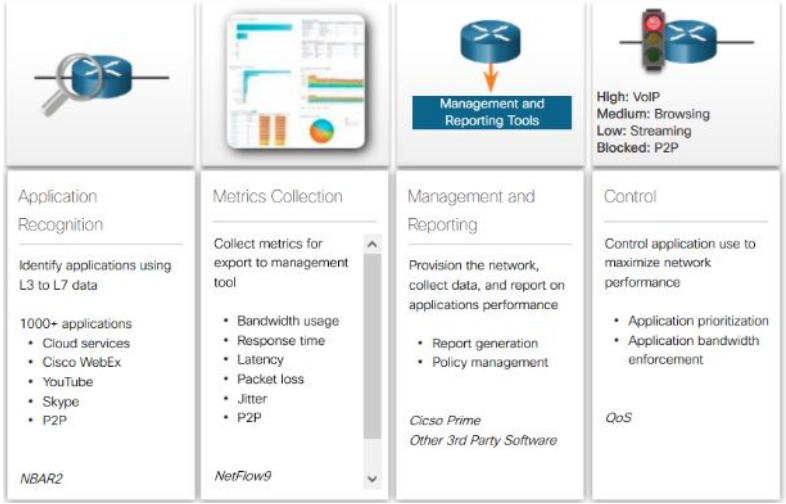
NetFlow

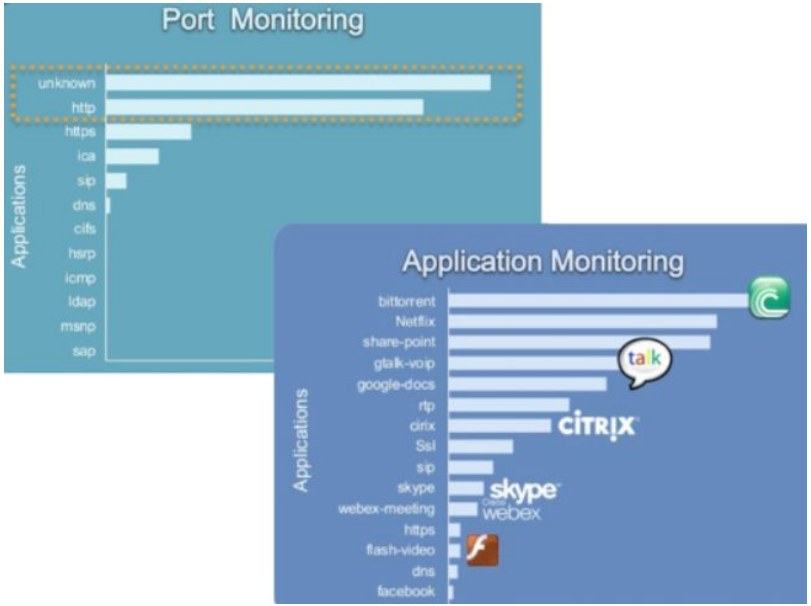
- NetFlow is a protocol used for network troubleshooting and session-based accounting.
  - Provides network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring.
  - Provides information about network users and applications, peak usage times, and traffic routing.
  - Collects metadata, or data about the flow, not the flow data itself.



Application Visibility and Control

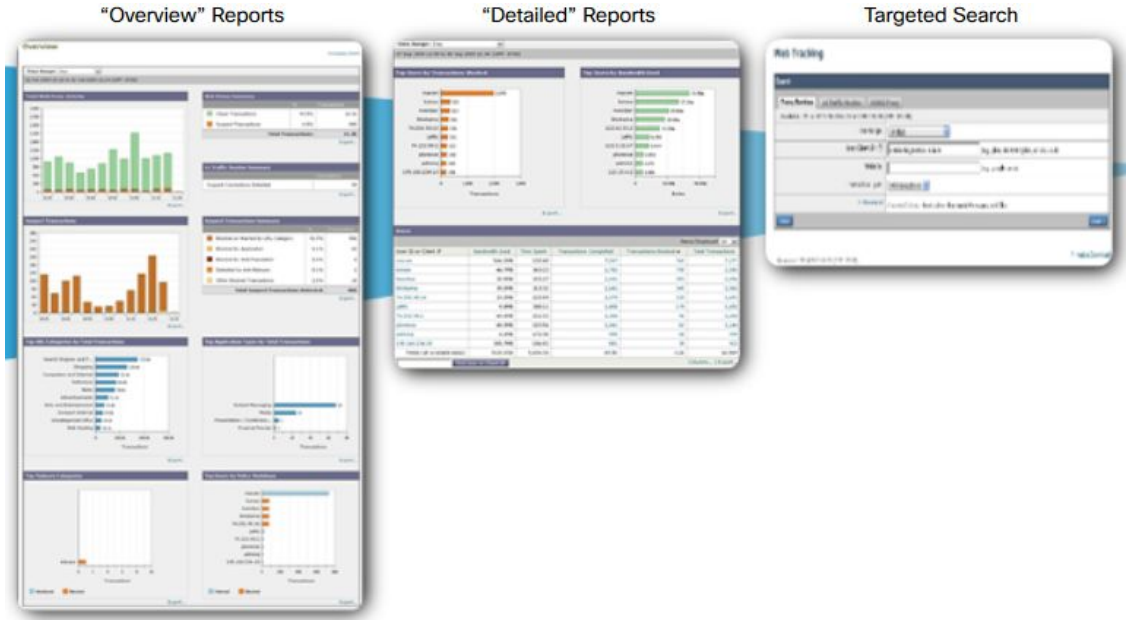
- Cisco Application Visibility and Control (AVC) system
  - Combines multiple technologies to recognize, analyze, and control over 1000 applications
  - Applications include voice and video, email, file sharing, gaming, peer-to-peer, and cloud-based applications.
  - More information than port monitoring alone.





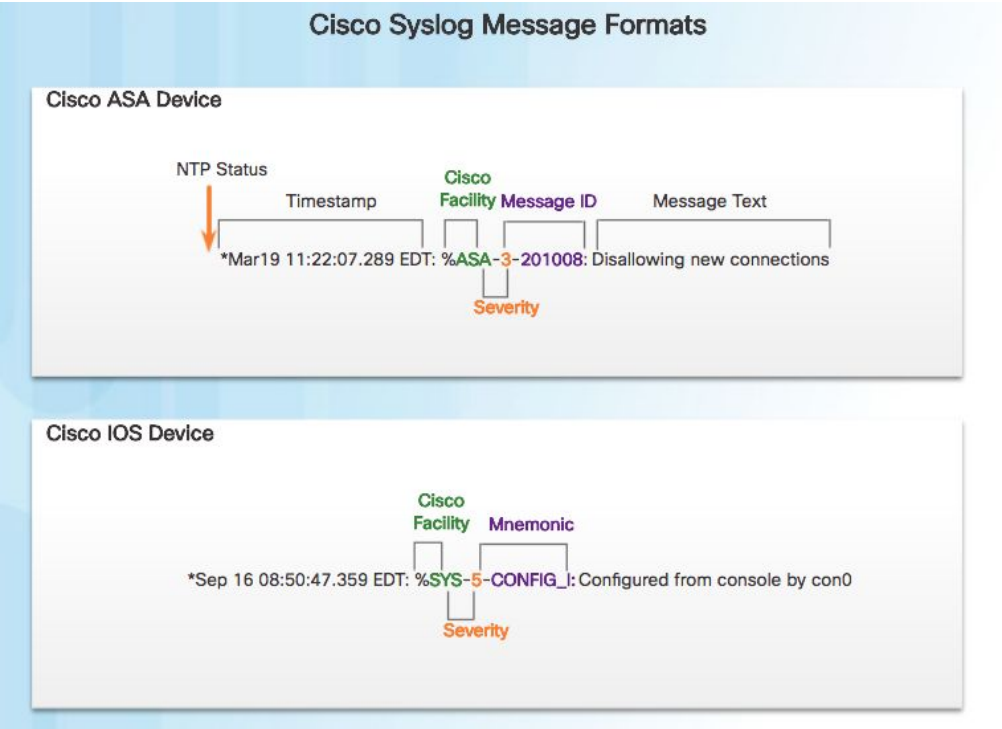
Content Filter Logs

- Devices that provide content filtering
  - Cisco Email Security Appliance (ESA)
  - Cisco Web Security Appliance (WSA)
- Provide a wide range of functionalities for security monitoring. Logging is available for many of these functionalities.



Logging from Cisco Devices

- Cisco devices can be configured to submit events and alerts to security management platforms using SNMP or syslog.



Proxy Logs

- Proxy servers contain valuable logs that are a primary source of data for network security monitoring.
  - Proxy servers make requests for resources and return them to the client.
  - Generate logs of all requests and responses.
  - Can be analyzed to determine which hosts are making the requests, whether the destinations are safe or potentially malicious, and to gain insights into the kind of resources that have been downloaded.
- Web proxies provide data that helps determine whether responses from the web were generated in response to legitimate requests or only appear to be responses.
- Open DNS offers a hosted DNS service that extends the capability of DNS to include security enhancements.
  - DNS super proxy
  - Apply real-time threat intelligence to managing DNS access and the security of DNS records

NextGen IPS

- Cisco NexGen IPS devices extend network security to the application layer and beyond.
  - Provide more functionality than previous generations of network security devices.
  - Include reporting dashboards with interactive features that allow quick reports on very specific information without the need for SIEM or other event correlators.
  - Use FirePOWER Services to consolidate multiple security layers into a single platform.
  - FirePOWER services include application visibility and control, reputation and category-based URL filtering, and Advanced Malware Protection (AMP).

NextGen IPS (Cont.)

- Common NGIPS events include:
  - Connection Event
  - Intrusion Event
  - Host or Endpoint Event
  - Network Discovery Event
  - Netflow Event

Summary

Summary

- In this lecture, you learned about the security technologies and log files used in security monitoring.
- Some of the common protocols that are monitored are: syslog, NTP, DNS, HTTP and HTTPS, SMTP, POP3, IMAP, and ICMP.
- Some commonly used technologies have an impact on security monitoring, including: ACLs, NAT and PAT, encryption, tunneling, peer-to-peer networks, TOR, and load balancing.
- There are different types of security data, including: alert data, session and transaction data, full packet captures, and statistical data.
- End devices create logs. Microsoft Windows host logs are visible locally through Event Viewer. Event Viewer keeps four types of logs:
  - **Application logs** – These contain events logged by various applications.
  - **System logs** – These include events regarding the operation of drivers, processes, and hardware.
  - **Setup logs** – These record information about the installation of software, including Windows updates.
  - **Security logs** – These record events related to security, such as logon attempts and operations related to file or object management and access.

Summary (Cont.)

- Syslog includes specifications for message formats, a client-server application structure, and network protocol.
- Network application servers such as email and web servers keep access and error logs.
- Apache webserver access logs record the requests for resources from clients to the server.
- Microsoft IIS creates access logs that can be viewed from the server with Event Viewer.
- SIEM combines the essential functions of security event management (SEM) and security information management (SIM) tools to provide a comprehensive view of the enterprise network.
- Tcpdump is a packet analyzer that displays packet captures in real time. Wireshark is a GUI built on tcpdump functionality.

Summary (Cont.)

- NetFlow provides network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring.
- The Cisco Application Visibility and Control (AVC) system combines multiple technologies to recognize, analyze, and control over 1000 network applications.
- Cisco ESA and WSA provide a wide range of functionalities for security monitoring, including logging.
- Cisco security devices can be configured to submit events and alerts to security management platforms using SNMP or syslog.
- Proxy servers generate logs of all requests and responses.
- NexGen IPS provide more functionality than previous generations of network security devices including content-based services.

New Terms and Commands

- Bro
- load balancing
- NextGen IPS
- Session data
- Squil
- Snort
- statistical data
- tcpdump
- Tor
- Transaction data