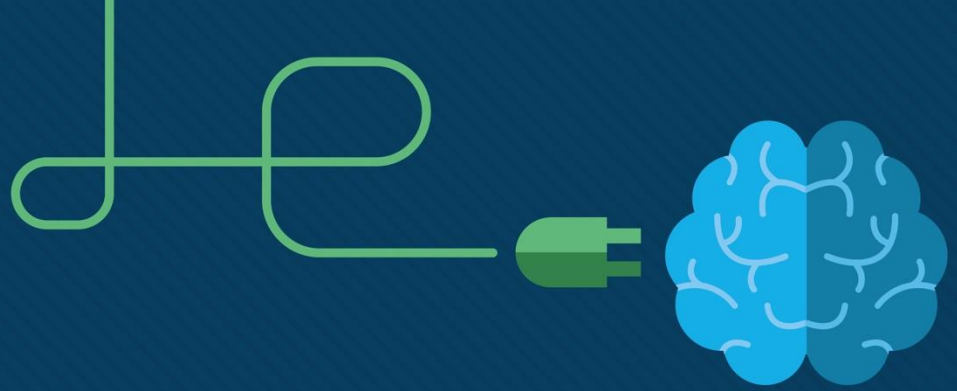


Module 15: Network Monitoring and Tools

CyberOps Associate v1.0

Module Objectives

Module Title: Network Monitoring and Tools

Module Objective: Explain network traffic monitoring.

Topic Title	Topic Objective
Introduction to Network Monitoring	Explain the importance of network monitoring.
Introduction to Network Monitoring Tools	Explain how network monitoring is conducted.

15.1 Introduction to Network Monitoring

Network Security Topology

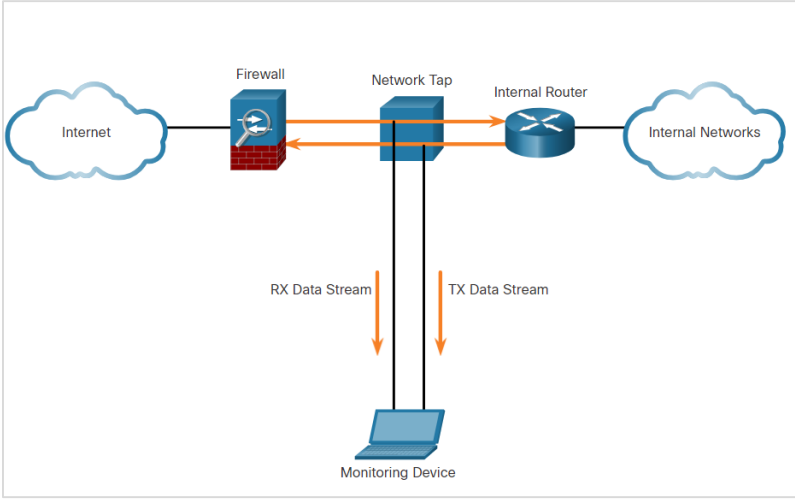
- To mitigate threats, all networks must be secured and protected.
- Network requires a security infrastructure consisting of firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and endpoint security software to protect.
- These methods and technologies are used to introduce automated monitoring, creating security alerts, or automatically blocking offensive devices.
- For large networks, an extra layer of protection is added.
- Devices such as firewalls and IPS operate based on pre-configured rules and monitor traffic and compare it against the configured rules. If there is a match, the traffic is handled according to the rule.
- An important part of the cybersecurity analyst is to review all alerts generated by network devices and determine the validity of the alerts.

Network Monitoring Methods

- The day-to-day operations of a network consists of traffic flow, bandwidth usage, and resource access. These patterns identify normal network behavior.
- To determine normal network behavior, network monitoring must be implemented.
- The tools such as IDS, packet analyzers, SNMP, NetFlow, and others are used for network monitoring .
- There are two common methods used to capture traffic and send it to network monitoring devices:
  - Network taps, sometimes known as Test Access Points (TAPs)
  - Traffic mirroring using Switch Port Analyzer (SPAN) or other port mirroring.

Network Taps

- A network tap is a passive splitting device implemented inline between a device of interest and the network.
- A tap forwards all traffic, including physical layer errors, to an analysis device while allowing the traffic to reach its intended destination.
- Here, the tap simultaneously sends both the transmit (TX) data stream from the internal router and the receive (RX) data stream to the internal router on separate, dedicated channels.
- This ensures that all data arrives at the monitoring device in real time.
- Taps are fail-safe, which means that the traffic between the firewall and internal router is not affected.



Implementing a TAP in a Sample Network

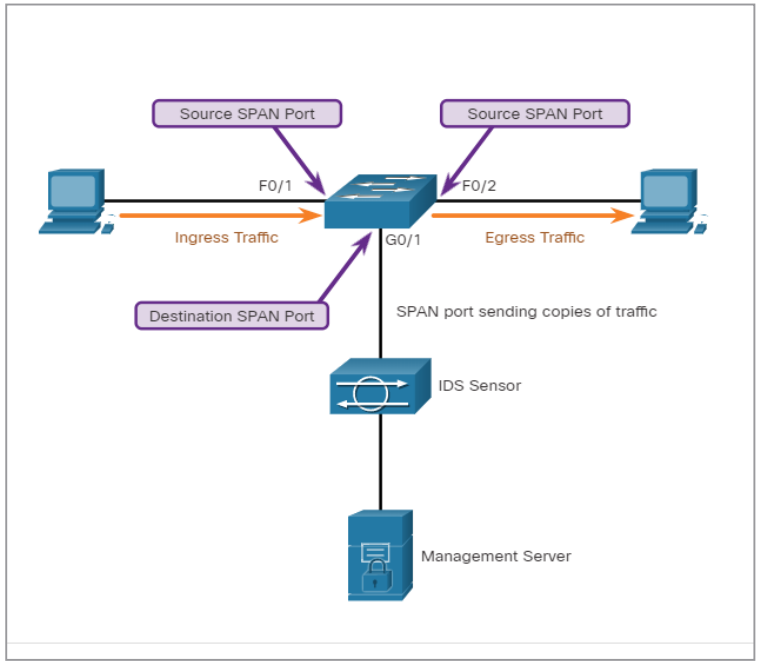
Traffic Mirroring and SPAN

- Capturing data for network monitoring requires all traffic to be captured.
- Special techniques such as port mirroring must be employed to bypass network segmentation imposed by network switches.
- Port mirroring enables the switch to copy frames that are received on one or more ports to a Switch Port Analyzer (SPAN) port that is connected to an analysis device.
- The table identifies and describes the SPAN terms.

SPAN Term	Description
Ingress traffic	Traffic that enters the switch
Egress traffic	Traffic that leaves the switch.
Source (SPAN) port	Source ports are monitored as traffic entering them is replicated (mirrored) to the destination ports.
Destination (SPAN) port	A port that mirrors source ports. Destination SPAN ports often connect to analysis devices such as a packet analyzer or an IDS.

Traffic Mirroring and SPAN (Contd.)

- The association between source ports and a destination port is called a SPAN session.
- In a single session, one or multiple ports can be monitored.
- In few Cisco switches, session traffic can be copied to more than one destination port.
- A source VLAN can be specified in which all ports in the source VLAN become sources of SPAN traffic.
- **Note**: A variation of SPAN called Remote SPAN (RSPAN) enables a network administrator to use the flexibility of VLANs to monitor traffic on remote switches.

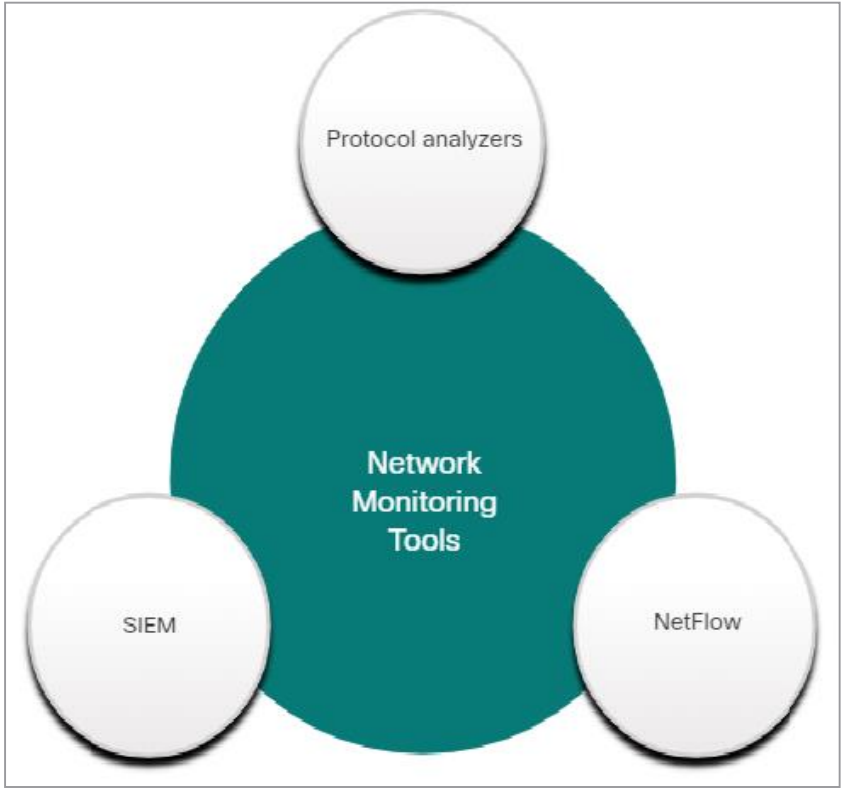


Switch interconnecting two hosts and mirroring traffic to an IDS and Network Management Server

15.2 Introduction to Network Monitoring Tools

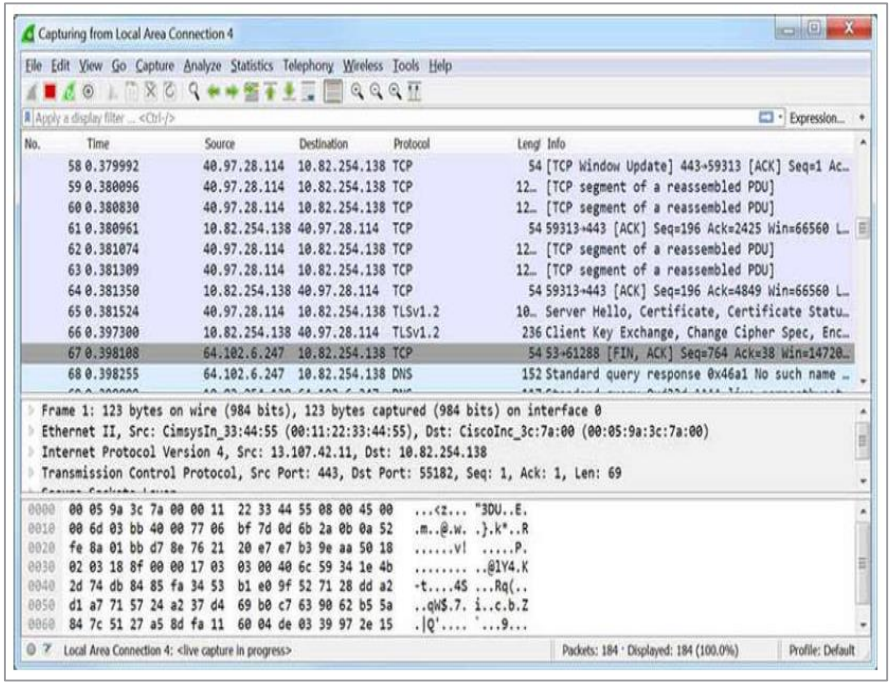
Network Security Monitoring Tools

- Common tools that are used for network security monitoring include:
  - Network protocol analyzers such as Wireshark and Tcpdump
  - NetFlow
  - Security Information and Event Management Systems (SIEM)
- It is common for security analysts to rely on log files and Simple Network Management Protocol (SNMP) for network behavior discovery.



Network Protocol Analyzers

- Network protocol analyzers (or ‘packet sniffer’ applications) are programs used to capture traffic.
- Protocol analyzers display what is happening on the network through a graphical user interface.
- Network protocol analyzers are not only used for security analysis but also used for network troubleshooting, software and protocol development, and education.
- As shown in the figure, Wireshark is used in Windows, Linux, and Mac OS environments. It is a very useful tool for learning network protocol communications.



Network Protocol Analyzers (Contd.)

- Frames captured by Wireshark are saved in a PCAP file that contains information regarding the frame, interface, packet length, time stamps, and all binary files sent across the network.
- Wireshark can open files containing captured traffic from other software such as the **tcpdump** utility.
- The example in the command output displays a sample **tcpdump** capture of **ping** packets.

```
[root@secOps analyst]# tcpdump -i hl-eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on hl-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:42:19.841549 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 5, length 64
10:42:19.841570 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 5, length 64
10:42:19.854287 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 6, length 64
10:42:19.854304 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 6, length 64
10:42:19.867446 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 7, length 64
10:42:19.867468 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 7, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

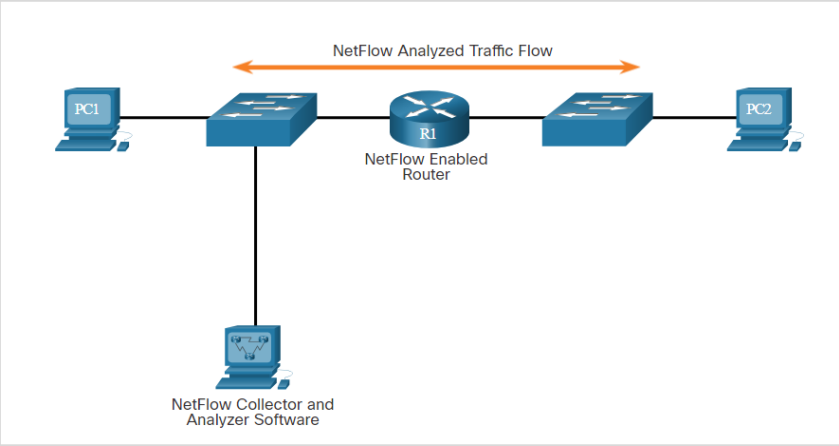
- **Note**: **windump** is a Microsoft Windows variant of **tcpdump**. **tshark** is a Wireshark command line tool that is similar to **tcpdump**.

NetFlow

- NetFlow is a Cisco IOS technology that provides 24x7 statistics on packets that flow through a Cisco router or multilayer switch.
- NetFlow is the standard for collecting IP operational data in IP networks.
- NetFlow can be used for network and security monitoring, network planning, and traffic analysis. It provides a complete audit trail of basic information about every IP flow forwarded on a device.
- Although NetFlow stores flow information in a local cache on the device, it should always be configured to forward data to a NetFlow collector which stores the NetFlow data.

NetFlow (Contd.)

- NetFlow can monitor application connection by tracking byte and packet counts for that individual application flow.
- It pushes the statistics over to an external server called a NetFlow collector.
- Cisco Stealthwatch collects NetFlow statistics to perform advanced functions including:
  - **Flow stitching -** It groups individual entries into flows.
  - **Flow deduplication** - It filters duplicate incoming entries from multiple NetFlow clients.
  - **NAT stitching** - It simplifies flows with NAT entries.



PC1 connected to PC2 using HTTPS

SIEM and SOAR

SIEM

- Security Information Event Management (SIEM) is a technology used in enterprise organizations to provide real time reporting and long-term analysis of security events.
- SIEM systems include the following essential functions:
  - **Forensic analysis** – The ability to search logs and event records from sources and provide complete information for forensic analysis.
  - **Correlation** – Examines logs and events from different systems or applications, speeding detection of and reaction to security threats.
  - **Aggregation** - Reduces the volume of event data by consolidating duplicate event records.
  - **Reporting** - Presents the correlated and aggregated event data in real-time monitoring and long-term summaries.

SIEM and SOAR (Contd.)

- SIEM provides details on the source of suspicious activity:
  - User information such as username, authentication status, location.
  - Device information such as manufacturer, model, OS version, MAC address, network connection method, and location.
  - Posture information such as compliance of the device with the security policy and updated antivirus files and OS patches.

SOAR

- Security Orchestration, Automation, and Response (SOAR) enhances SIEM.
- SOAR helps security teams investigate security incidents and add enhanced data gathering and a number of functionalities that aid in security incident response.

SIEM and SOAR (Contd.)

- SOAR solutions:
  - Provides case management tools that allow cybersecurity personnel to research and investigate incidents, frequently by integrating threat intelligence into the network security platform.
  - Use artificial intelligence to detect incidents that aid in incident analysis and response.
  - Automate complex incident response procedures and investigations, which are potentially labor intensive tasks performed by Security Operations Center (SOC) staff by executing run books.
  - Offers dashboards and reports to document incident response to improve SOC key performance indicators and can enhance network security for organizations.
- SOAR helps analysts respond to the threat.

SIEM Systems

- An open source product called Security Onion includes the ELK suite for SIEM functionality.
- ELK is an acronym for three products from Elastic:
  - **Elasticsearch** - Document oriented full text search engine.
  - **Logstash** - Pipeline processing system that connects ‘inputs’ to ‘outputs’ with optional ‘filters’ in between.
  - **Kibana** - Browser based analytics and search dashboard for Elasticsearch.
- **Note**: SolarWinds Security Event Manager and Splunk Enterprise Security are two popular proprietary SIEM systems used by SOCs.

Packet Tracer - Logging Network Activity

In this Packet tracer, you will do the following:

- Intercept credentials using a sniffer device, while observing an FTP session. An exchange of Syslog messages will also be intercepted by a sniffer device.

15.3 Network Monitoring and Tools Summary

What Did I Learn in this Module?

- To mitigate threats, all networks should be secured and protected using a defense-in-depth approach.
- This requires a security infrastructure that consists of firewalls, IDS, IPS, and endpoint security software.
- A cybersecurity analyst needs to review all alerts that are generated by network devices and validate them.
- Tools such as IDS, packet analyzers, SNMP, NetFlow, and others are used to determine normal network behavior.
- Two common methods that are used to capture traffic and send it to network monitoring devices are network taps and traffic mirroring using Switch Port Analyzer (SPAN) or other port mirroring.

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

- Common tools that are used for network security monitoring include network protocol analyzers (Wireshark and Tcpdump), NetFlow, and SIEM.
- Network protocol analyzers are programs that are used to capture traffic.
- Netflow is a Cisco IOS feature that provides 24x7 statistics on packets that flow through a Cisco router or multilayer switch. It can be used for network and security monitoring, network planning, and traffic analysis.
- SIEM is a technology that is used to provide real time reporting and long-term analysis of security events.


CISCO