CompTIA Security+ Guide to Network Security Fundamentals, Sixth Edition

Chapter 7

Administering a Secure Network

Objectives

7.1 List and describe the functions of secure network protocols

7.2 Explain the placement of security devices and technologies

7.3 Tell how security data can be analyzed

7.4 Explain how to manage and secure network platforms

Secure Network Protocols (1 of 4)

- Protocols
  - Rules for communication
  - Essential for proper communication between network devices
- Transmission Control Protocol/Internet Protocol (TCP/IP)
  - Most common protocol suite used for local area networks and the Internet
  - Comprises several protocols that all function together

Secure Network Protocols (2 of 4)

- IP
  - Protocol that functions primarily at Open Systems Interconnection (OSI) Network Layer (Layer 3)
  - Provides network addressing and routing
- TCP
  - Transport Layer (Layer 4) protocol
  - Establishes connections and ensures reliable data transport between devices
- TCP/IP uses a four layer architecture
  - Network Interface, Internet, Transport, Application

Secure Network Protocols (3 of 4)

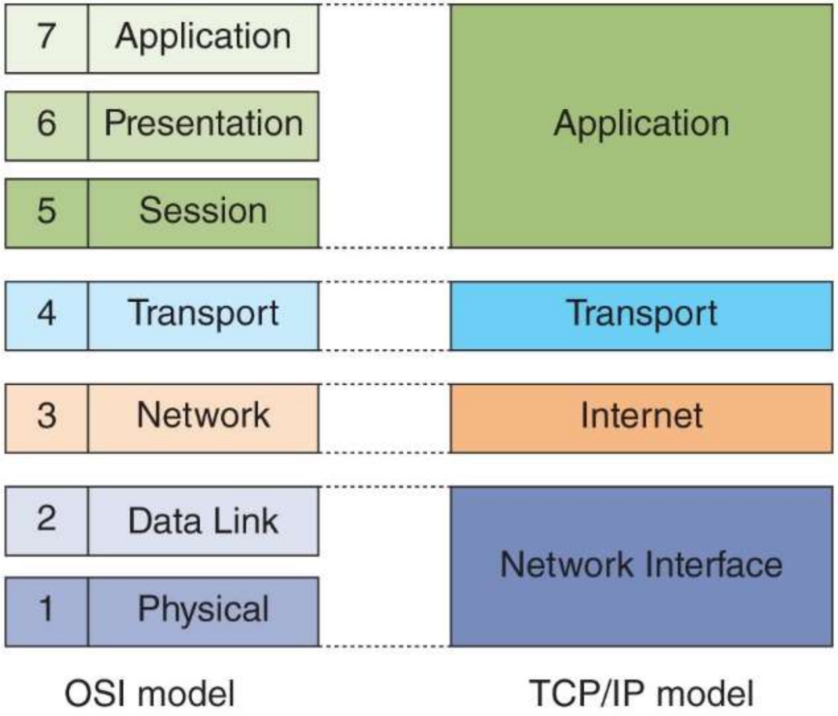


Figure 7-1 OSI model vs. TCP/IP model

Secure Network Protocols (4 of 4)

- Several basic TCP/IP Protocols that relate to security:
  - Simple Network Management Protocol (SNMP)
  - Domain Name System (DNS)
  - File Transfer Protocol
- There are also email protocols that are not natively secure
  - Steps can be taken to protect email correspondence

Simple Network Management Protocol (SNMP) (1 of 2)

- Used to manage network equipment and is supported by most network equipment manufacturers
- Allows administrators to remotely monitor, manage, and configure network devices
- Functions by exchanging management information between network devices
- Each SNMP-managed device has an agent or a service
    - Listens for and executes commands

Simple Network Management Protocol (SNMP) (2 of 2)

- Agents are password protected
  - Password is known as a **community string**
- Security vulnerabilities were present in SMNP versions 1 and 2
  - Version 3 uses usernames and passwords along with encryption to address vulnerabilities

Domain Name System (DNS) (1 of 3)

- DNS
  - A TCP/IP protocol that maps IP addresses to their symbolic name
- The DNS database is organized as a hierarchy
  - Database consists of the name of a site and a corresponding IP number
- The database is distributed to many different servers on the Internet
  - To prevent bottlenecking and to ensure efficiency

Domain Name System (DNS) (2 of 3)

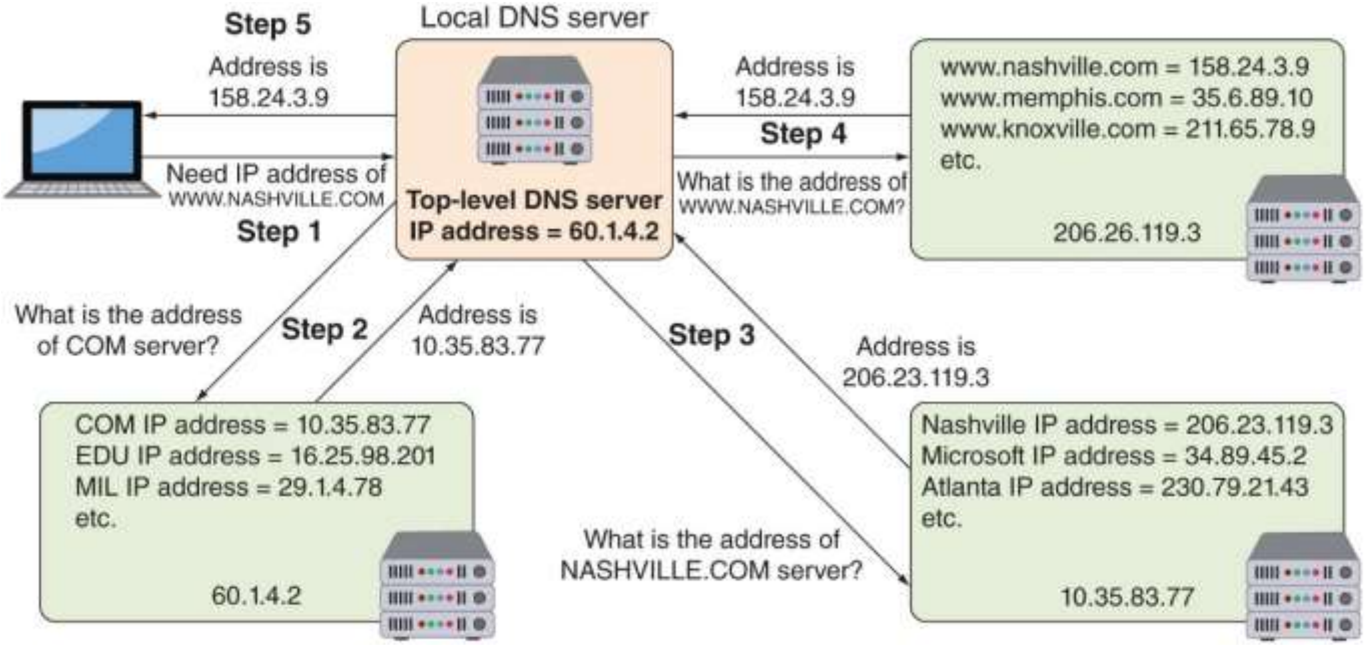

Local DNS server
Step 5
Address is 158.24.3.9
Need IP address of WWW.NASHVILLE.COM
Step 1
Top-level DNS server
IP address = 60.1.4.2
Address is 158.24.3.9
Step 4
What is the address of WWW.NASHVILLE.COM?
www.nashville.com = 158.24.3.9
www.memphis.com = 35.6.89.10
www.knoxville.com = 211.65.78.9
etc.
206.26.119.3
What is the address of COM server?
Step 2
Address is 10.35.83.77
Step 3
Address is 206.23.119.3
COM IP address = 10.35.83.77
EDU IP address = 16.25.98.201
MIL IP address = 29.1.4.78
etc.
60.1.4.2
What is the address of NASHVILLE.COM server?
Nashville IP address = 206.23.119.3
Microsoft IP address = 34.89.45.2
Atlanta IP address = 230.79.21.43
etc.
10.35.83.77

Figure 7-2 DNS lookup

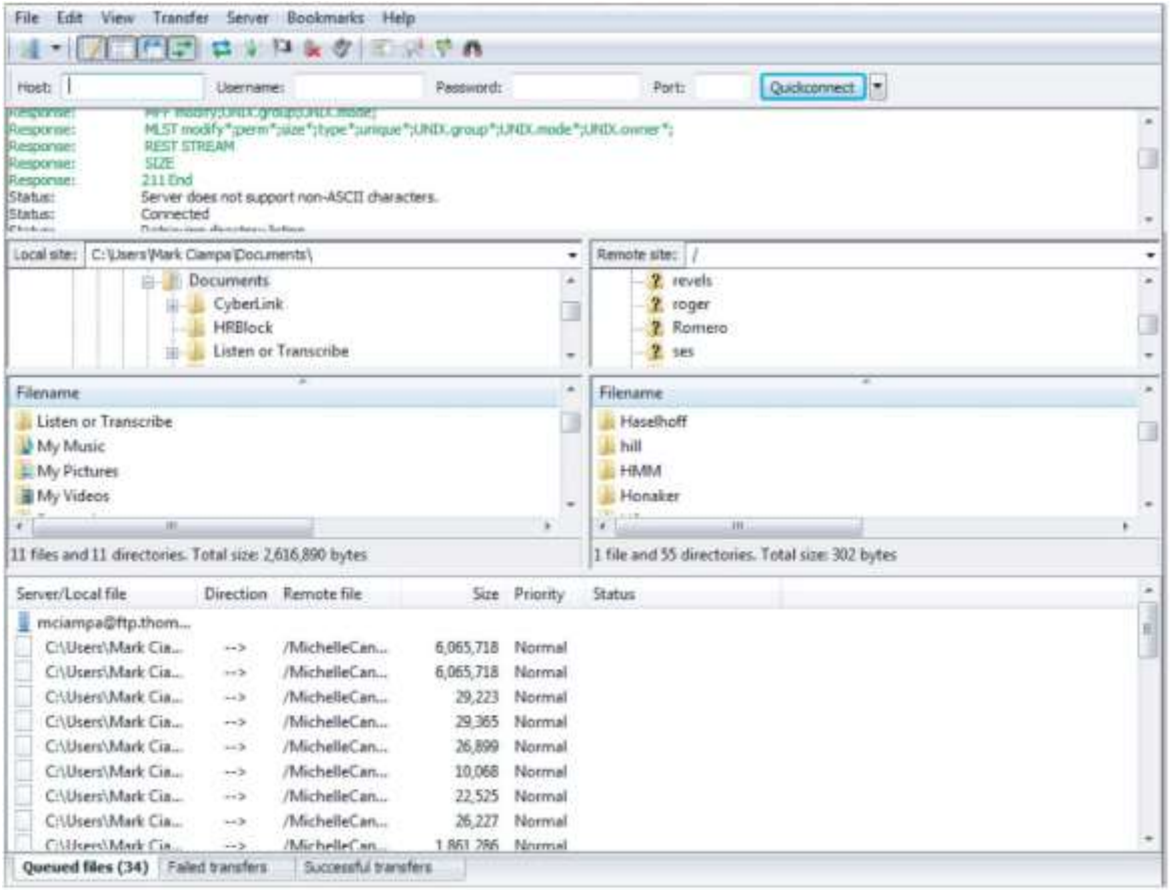
Domain Name System (DNS) (3 of 3)

- DNS is often the focus of attacks
  - DNS poisoning substitutes fraudulent IP address
    - Can be done in local host table or external DNS server
    - Can be thwarted by using Domain Name System Security Extensions (DNSSEC)
    - DNSSEC adds additional resource records and message header information which can be used to verify the requested data has not been altered in transmission
  - Attacker asks the valid DNS for a zone transfer
    - A zone transfer allows attacker access to network, hardware, and operating system information

File Transfer Protocol (FTP) (1 of 4)

- TCP/IP protocol used for transferring files
  - File transfer protocol (FTP) – an unsecure protocol used to connect to an FTP server
- Methods for using FTP on local host computer
  - **From a command prompt**
  - **Using a web browser**
  - **Using an FTP client**

File Transfer Protocol (FTP) (2 of 4)



```
Response:     MFF modify;UNIX.group;UNIX.mode;
Response:     MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*;
Response:     REST STREAM
Response:     SIZE
Response:     211 End
Status:       Server does not support non-ASCII characters.
Status:       Connected
Status:       Retrieving directory listing...
```

Local site: C:\Users\Mark Ciampa\Documents\

- Documents
  - CyberLink
  - HRBlock
  - Listen or Transcribe

Remote site: /

- revels
- roger
- Romero
- ses

Filename
Listen or Transcribe
My Music
My Pictures
My Videos

11 files and 11 directories. Total size: 2,616,890 bytes

Filename
Haselhoff
hill
HMM
Honaker

1 file and 55 directories. Total size: 302 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status
mciampa@ftp.thom...					
C:\Users\Mark Cia...	-->	/MichelleCan...	6,065,718	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	6,065,718	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	29,223	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	29,365	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	26,899	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	10,068	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	22,525	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	26,227	Normal	
C:\Users\Mark Cia...	-->	/MichelleCan...	1,861,286	Normal	

Figure 7-3 FTP client

Source: FileZilla

CENGAGE

File Transfer Protocol (FTP) (3 of 4)

- Using FTP behind a firewall can present challenges
  - FTP uses two ports
    - Port 21 is the FTP control part
    - Port 20 is the data port
  - FTP active mode
    - Client’s firewall may sometimes drop packets on Port 20 (the data channel connection)
  - FTP passive mode
    - The client sends a PASV command to the command channel and the server responds with the TCP port number to use to establish the data channel

File Transfer Protocol (FTP) (4 of 4)

- FTP vulnerabilities
  - Does not use encryption
  - Files transferred using FTP are vulnerable to man-in-the-middle attacks
- Secure transmission options over FTP
  - Secure sockets layer (FTPS) encrypts commands
    - Uses SSL or TLS to encrypt commands sent over the control port (port 21); data port may not be encrypted
  - Secure FTP (SFTP)
    - Uses only a single TCP port instead of two ports
    - All data and commands are encrypted

Secure Email Protocols

- Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - A protocol for securing email messages
- S/MIME has limitations:
  - Cannot be used when mail is accessed through a web browser instead of a dedicated email application
  - Because S/MIME encrypts the entire message, this makes it difficult for any third-party tools that inspect email for malware
    - Because it also would be encrypted
- Some enterprises and government agencies automate encrypting and decrypting email
  - Use a mail gateway appliance

Using Secure Network Protocols

Application or technology	**Recommended secure protocol**
Voice and video	Secure Real-time Transport Protocol (SRTP)
Time synchronization	Network Time Protocol (NTP)
Email	Secure/Multipurpose Internet Mail Extensions (S/MIME)
Web browsing	Hypertext Transport Protocol Secure (HTTPS)
File transfer	Secure FTP (SFTP)
Remote access	Virtual Private Network (VPN)
Domain name resolution	DNS Security Extensions (DNSSEC)
Routing and switching	IP Security (IPsec)
Network address translation	IP Security (IPsec)
Subscription services	IP Security (IPsec)

Placement of Security Devices and Technologies (1 of 5)

- The protection that security devices provide can be easily negated if those devices are not properly located in the network architecture
- **SSL/TLS accelerator** – a separate hardware card that inserts into a web server that contains co-processors to handle SSL/TLS processing
  - a SSL/TLS hardware module can be installed as a "virtual SSL/TLS server" alongside the forward proxy server
- **Port mirrors** – allows the administrator to configure a switch to copy traffic that occurs on some or all ports to a designated port on the switch (see Figure 7-4)
- **Network tap (test access point)** – a device that can monitor traffic (see Figure 7-5)

Placement of Security Devices and Technologies (2 of 5)

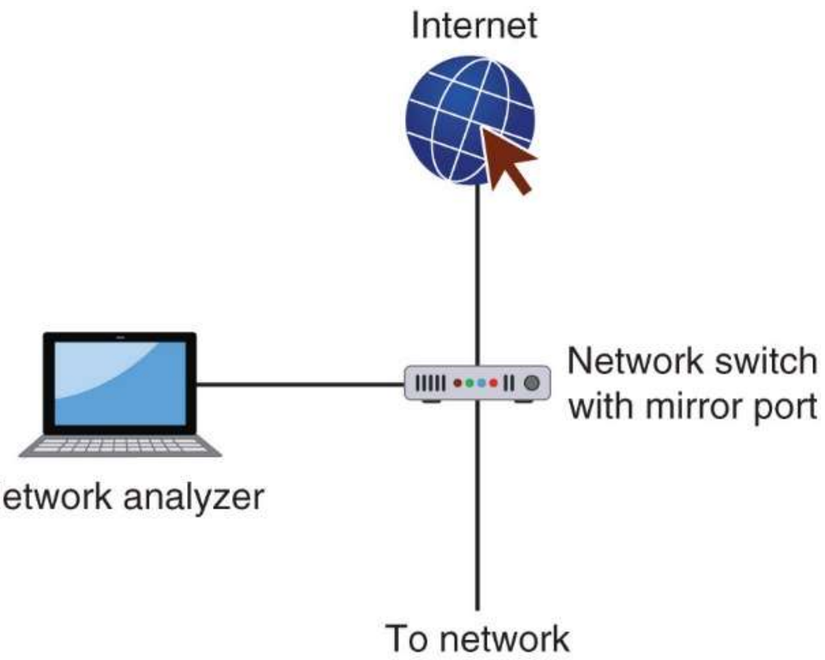


Figure 7-4 **Port mirroring**

Placement of Security Devices and Technologies (3 of 5)

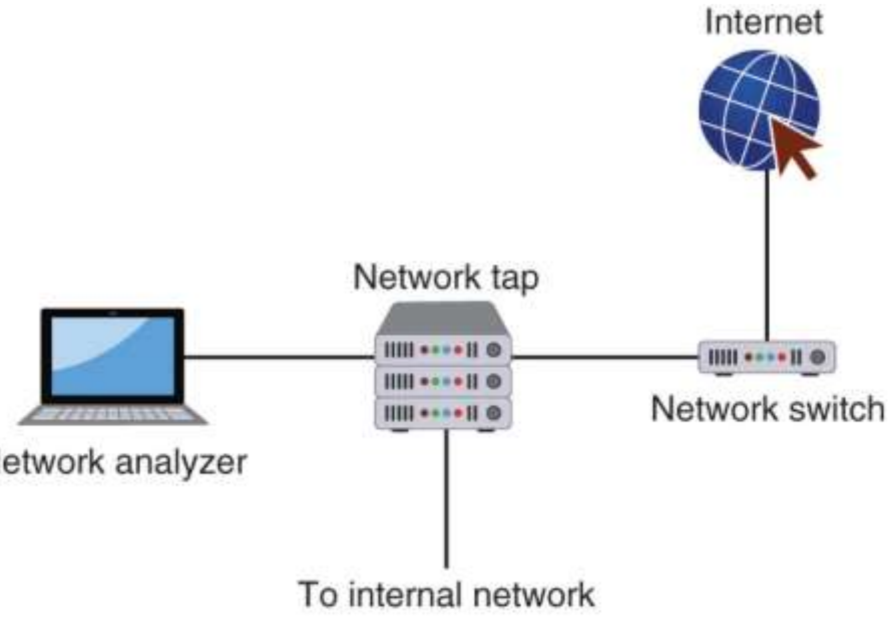


Figure 7-5 Network tap

Placement of Security Devices and Technologies (4 of 5)

- **Sensors, collectors, and filters** – should be placed where the stream of data is largest
  - Sensors – monitor traffic for network intrusion detection and prevention devices
  - Collectors – gather traffic for SIEM devices
  - Filters – block traffic for Internet content filters

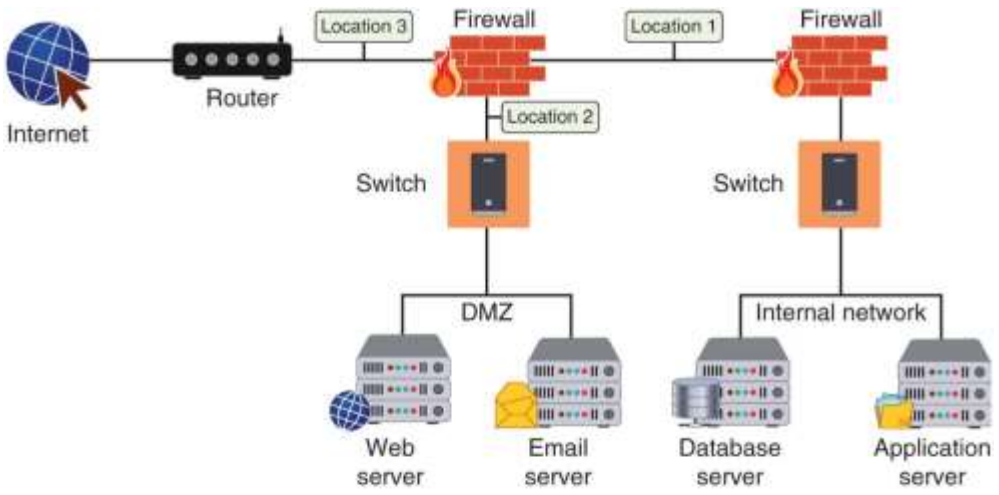


Figure 7-6 Sensor/collector/filter locations

Placement of Security Devices and Technologies (5 of 5)

- **Aggregation switch** – used to combine multiple network connections into a single link
  - Should be located between routers and servers where they can detect and stop attacks directed at a server or application
- **Correlation engine** – aggregates and correlates content from different sources to uncover an attack
  - Should be in the protected internal network using data collected from the logs of different hardware devices
- **DDoS mitigator** – a hardware device that identifies and blocks real-time distributed denial of service (DDoS) attacks
  - Should be in the network where they can monitor the largest stream of data

Analyzing Security Data (1 of 2)

- Security logs
  - Can reveal types of attacks that are being directed at the network and if attacks were successful
- Access logs
  - Provide details regarding requests for specific files
- Audit logs
  - Used to record which user performed an action
- Event logs
  - Document any unsuccessful events and the most significant successful events

Analyzing Security Data (2 of 2)

- A routine review of logs helps to identify:
  - Security incidents
  - Policy violations
  - Fraudulent activity
  - Operational problems
- Logs can be useful for:
  - Performing auditing analysis
  - Supporting the organization’s internal investigations
  - Identifying operational trends and long-term problems
- Logs can provide documentation that the organization is complying with laws and regulatory requirements

Data from Security Devices

- Almost every hardware device designed for security can generate logs
- Firewall log items to be examined
  - IP addresses rejected and dropped
  - Probes to ports that have no application services on them
  - Source-routed packets
  - Suspicious outbound connections
  - Unsuccessful logins

Data from Security Software

- Security software can produce important data that can be analyzed
- Data Execution Prevention (DEP)
  - A Microsoft Windows feature that prevents attackers from using buffer overflow to execute malware
- DEP events and those from similar software can be logged along with the level of severity
- File integrity check (FIC)
  - A service that can monitor any changes made to computer files, such as OS files
  - These changes can compromise security and indicate a security breach has occurred

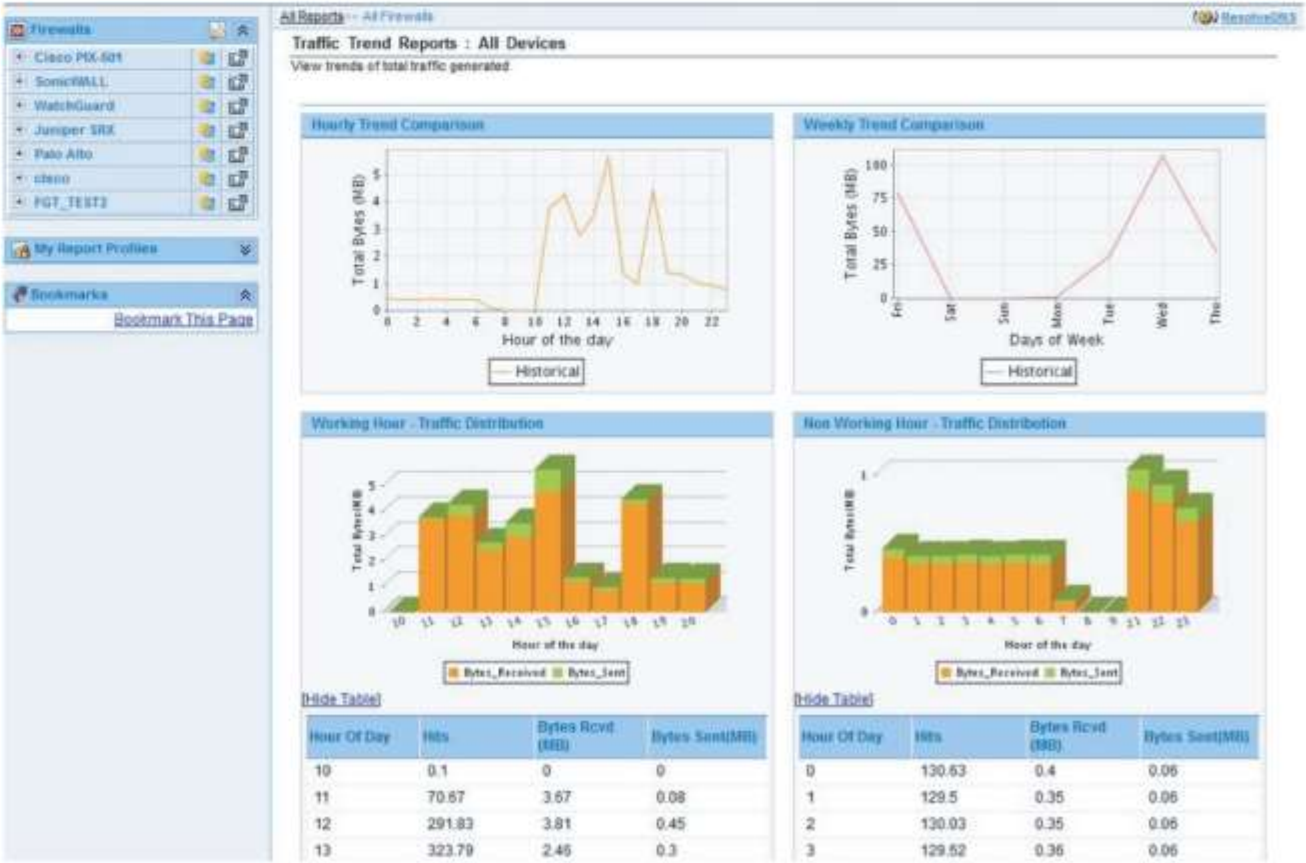
Data from Security Tools

Tool	Description	Explanation
Application Whitelisting	A whitelist is an inventory of applications and associated components that have been pre-approved and authorized to be active and present on the device	Application whitelisting technologies are designed to permit only known good activity and block everything else
Removable media control	Removable media control is a tool that can be used to restrict which removable media can be attached to a system	Removable media can introduce malware into a system and be used to steal valuable information
Advanced malware management	Often a third-party service, advanced malware management tools monitor a network for any unusual activity	Advanced malware management tools often use experience-based techniques such as heuristic monitoring to determine if a threat exists

Issues in Analyzing Security Data (1 of 2)

- There are issues with log management
  - Generating, transmitting, storing, analyzing, and disposing of computer security log data
- This is due to:
  - Multiple devices generating logs
  - Very large volume of data
  - Different log formats
- A solution:
  - Use a centralized device log analyzer

Issues in Analyzing Security Data (2 of 2)



Traffic Trend Reports : All Devices

View trends of total traffic generated

[Hide Table]

Hour Of Day	Hits	Bytes Rcvd (MB)	Bytes Sent(MB)
10	0.1	0	0
11	70.67	3.67	0.08
12	291.83	3.81	0.45
13	323.79	2.46	0.3

[Hide Table]

Hour Of Day	Hits	Bytes Rcvd (MB)	Bytes Sent(MB)
0	130.63	0.4	0.06
1	129.5	0.35	0.06
2	130.03	0.35	0.06
3	129.52	0.36	0.06

Figure 7-7 Centralized device log analyzer

Source: ManageEngine.com

Managing and Securing Network Platforms

- Some applications and platforms require special security considerations:
  - Virtualization
  - Cloud computing
  - Software defined networking

Virtualization (1 of 7)

- Virtualization
  - A means of managing and presenting computer resources without regard to physical layout or location
- Host virtualization
  - An entire operating system environment is simulated
  - Virtual machine - a simulated software-based emulation of a computer
  - The host system runs a hypervisor that manages the virtual operating systems and supports one or more guest systems

Virtualization (2 of 7)

- The VM monitor program is called a **hypervisor**
  - Manages the VM operating systems
- Two types of hypervisor:
  - Type I – runs directly on the computer's hardware instead of the underlying OS
  - Type II – run on the host OS, much like an application

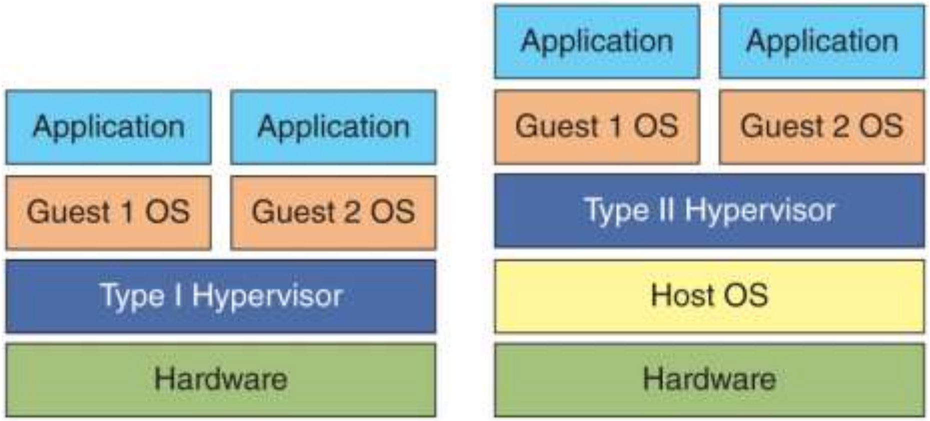


Figure 7-8 Type I and Type II hypervisors

Virtualization (3 of 7)

- Container or application cell
  - Holds only the necessary OS components that are needed for that specific application to run
  - Reduces the necessary hard drive storage space and RAM needed
  - Allows for containers to start more quickly because the OS does not have to be started

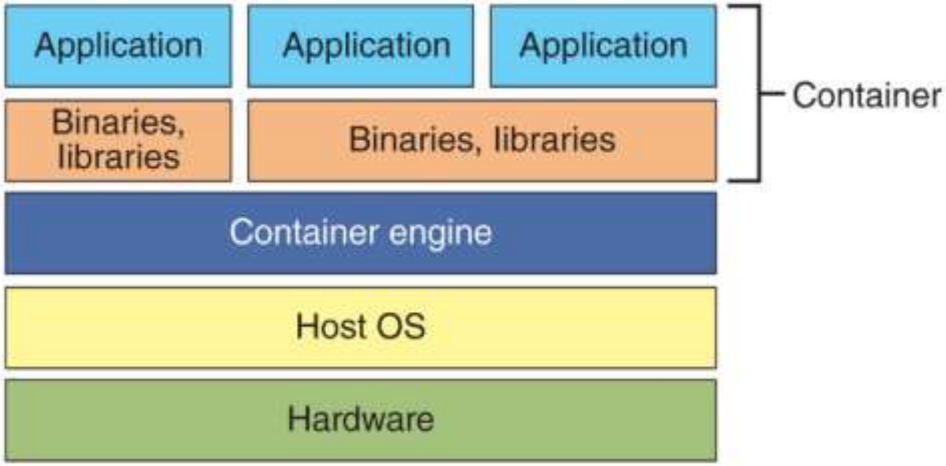


Figure 7-9 Containers

Virtualization (4 of 7)

- Virtual Desktop Infrastructure (VDI)
  - The process of running a user desktop inside a VM that resides on a server
  - Enables personalized desktops for each user to be available on any computer or device that can access the server
  - Allows centralized management of all virtual desktops
- Virtual Distributed Ethernet (VDE)
  - An Ethernet-compliant virtual network that can connect physical computers and/or virtual machines together

Virtualization (5 of 7)

- Virtualization advantages
  - New virtual server machines can be made available (host availability) and resources can easily be expanded or contracted as needed (host elasticity)
  - Can reduce costs
    - Fewer physical computers must be purchased and maintained
  - Can provided uninterrupted server access to users
    - Supports **live migration** which allows a virtual machine to be moved to a different physical computer with no impact to users

Virtualization (6 of 7)

- Security-related advantages of virtualization:
  - Test latest security updates by downloading on a virtual machine before installing on production computers
  - A **snapshot** of a particular state of a virtual machine can be saved for later use
  - Testing the existing security configuration **(security control testing)** can be performed using a simulated network environment
  - A suspicious program can be loaded into an isolated virtual machine and executed **(sandboxing)**
    - If malware, only the virtual machine will be impacted

Virtualization (7 of 7)

- Security concerns for virtualized environments:
  - Not all hypervisors have the necessary security controls to keep out attackers
  - Existing security tools were designed for single physical servers
  - VMs must be protected from both outside networks and other VMs on the same physical computer
  - VMs may be able to “escape” from the contained environment and directly interact with the host OS
    - Important to have **virtual machine escape protection**
  - **Virtual machine sprawl**
    - The widespread proliferation of VMs without proper oversight or management

Cloud Computing (1 of 3)

- **On-premises model**
  - Enterprises in the past purchased all the hardware and software necessary to run the organization
  - Resulted in spiraling costs
- **Hosted services**
  - Servers, storage, and the supporting networking infrastructure are shared by multiple enterprises over a remote network connection
- **Cloud computing**
  - A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources
  - It is a pay-per-use computing model
    - Customers pay for only the resources they need

Cloud Computing (2 of 3)

- Types of clouds
  - Public cloud
  - Community cloud
  - Private cloud
  - Hybrid cloud
- Four service models in cloud computing:
  - **Software as a Service (SaaS)**
    - Vendor provides access to the vendor’s software applications running on a cloud infrastructure
  - **Platform as a Service (PaaS)**
    - Consumers install and run their own specialized applications on the cloud computing network
  - **Infrastructure as a Service (IaaS)**
    - Vendor allows customers to deploy and run their own software, including OSs and applications
  - **Security as a Service (SECaaS)**
    - All security services are delivered from the cloud to the enterprise

Cloud Computing (3 of 3)

- Cloud computing security challenges
  - Cloud provider must guarantee means to approve authorized users and deny imposters
  - Transmissions from the cloud must be protected
  - Customers' data must be isolated from other customers
  - The highest level of application availability and security must be maintained
- **Cloud access security broker (CASB)**
  - A set of software tools or services that resides between the enterprises' on-premises infrastructure and the cloud provider's infrastructure
  - Acts as a "gatekeeper"
  - Ensures that the security policies of the enterprise extend to its data in the cloud

Software Defined Network (SDN) (1 of 2)

- Software defined network (SDN)
  - Virtualizes parts of the physical network so that it can be more quickly and easily reconfigured
  - Accomplished by separating the **control plane** from the **data plane**

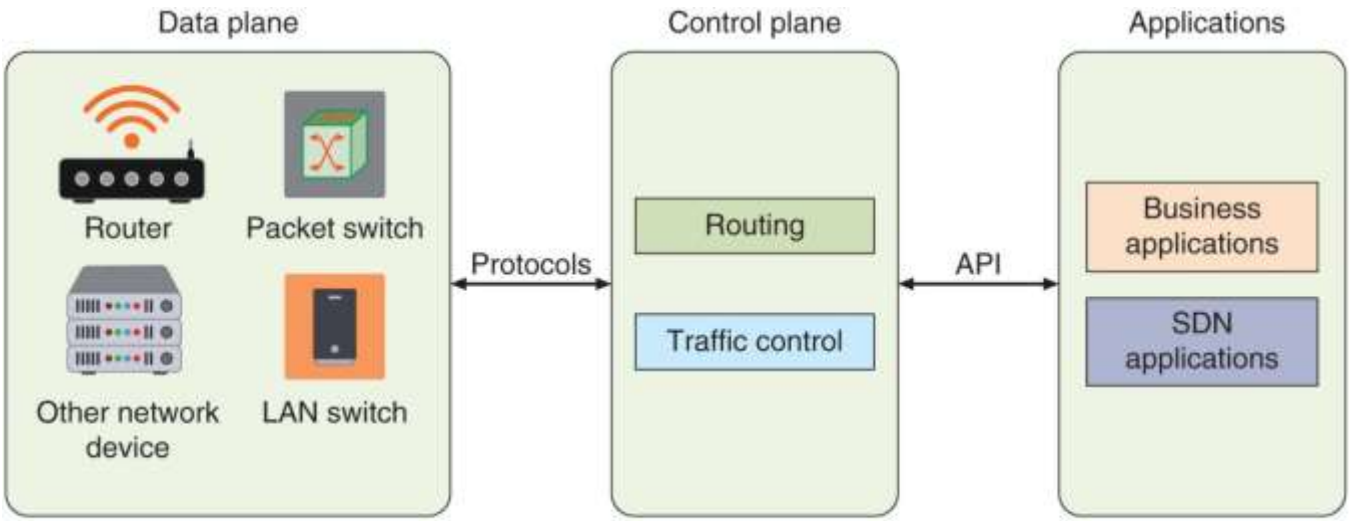


Figure 7-10 Software defined network

Software Defined Network (SDN) (2 of 2)

- If traffic needs to flow through the network
  - It receives permission from the SDN controller, which verifies the communication is permitted by the network policy of the enterprise
  - Once approved, the SDN controller computes a route for the flow to take
  - Adds an entry for that flow in each of the switches along the path
- SDN s can provide stronger protection
  - Simplifies extending VLAN beyond the perimeter of the building, which can help secure data
  - An SDN can ensure that all network traffic is routed through a firewall
  - Can help capture data for NIDS and NIPS

Chapter Summary (1 of 2)

- TCP/IP is the most common protocol for LANs and the Internet
- Protocols for transferring files
  - FTP and FTPS
- The correct placement of security devices is essential for protection
  - An SSL/TLS accelerator can be a separate hardware card or a separate SSL/TLS hardware module installed as a “virtual SSL server”
- Monitoring traffic on switches can be done in two ways:
  - A managed switch that supports port mirroring
  - Install a network tap (test access point)

Chapter Summary (2 of 2)

- A log is a record of events that occur
  - Security logs are particularly important because they can reveal the types of attacks that are being directed at the network
- A solution to log management is to use a centralized device log analyzer
- Some applications and platforms require special security considerations
  - Virtualization
  - Cloud computing
  - Software defined network (SDN)