

Data Security and Privacy

Chapter 7:

Security and Backup Technologies:

Firewalls, VPNs, Intrusion Detection and Prevention Systems, and Other Security Tools, Backup technologies.

Introduction

- Technical controls are essential in enforcing policy for many IT functions not under direct human control.
- When properly implemented, **technical control solutions** improve an organization's ability to balance the objectives of making information readily available and preserving information's confidentiality and integrity.

1-Firewalls

- Prevent specific types of information from moving between an **untrusted network** (the Internet) and a **trusted network** (organization's internal network)
- May be:
 - **Separate computer** system
 - **Software service** running on existing router or server
 - **Separate network containing** supporting devices

Firewalls Processing Modes

- Five processing modes by which firewalls can be categorized:
 - Packet filtering
 - Application gateways
 - MAC layer firewalls
 - Hybrids

Packet-Filtering Firewalls

- Packet-filtering firewalls examine the **header information of data packets**.
- Most often based on the combination of:
 - **IP source** and **destination address**
 - Direction (**inbound or outbound**)
 - **Transmission Control Protocol** (TCP) or User Datagram Protocol (UDP) source and destination port requests
- Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through device.

Source address	Destination address	Service (e.g., HTTP, SMTP, FTP)	Action (allow or deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Table 6-2 Sample Firewall Rule and Format

Firewall Architectures

- Firewall devices can be configured in several network connection architectures.
- Best configuration depends on three factors:
 - Objectives of the network
 - Organization's ability to develop and implement architectures
 - Budget available for function
- Four common architectural implementations of firewalls:
 - **packet-filtering routers**, dual-homed firewalls, screened host firewalls, screened subnet firewalls

Firewall Architectures (cont'd)

- Packet-filtering routers
 - Most organizations with Internet connection have a router at the boundary between internal networks and external service provider.
 - Many of these routers can be configured to reject packets that the organization does not allow into its network.
 - Drawbacks include a lack of auditing and strong authentication.

Configuring and Managing Firewalls

- The organization must provide for the initial configuration and ongoing management of firewall(s).
- Each firewall device must have its own set of configuration rules regulating its actions.
- Firewall policy configuration is usually complex and difficult.
- Configuring firewall policies is both an art and a science .
- When security rules conflict with the performance of business, security often loses.

Configuring and Managing Firewalls (cont'd)

- All traffic from the **trusted network** is **allowed out**.
- Firewall device is **never directly accessed** from public network.
- Simple Mail Transport Protocol (SMTP) data are allowed to pass through firewall.
- Telnet access to internal servers should be **blocked**.
- All data **not verifiably authentic** should be **denied**.
- **Firewall rules**
 - Firewalls operate by **examining** data packets and **performing comparison** with predetermined **logical rules**.
 - The logic is based on a set of guidelines most commonly referred to as **firewall rules**, rule base, or firewall logic.
 - Most firewalls use packet header information to determine whether specific packet should be allowed or denied.

2-Content Filters

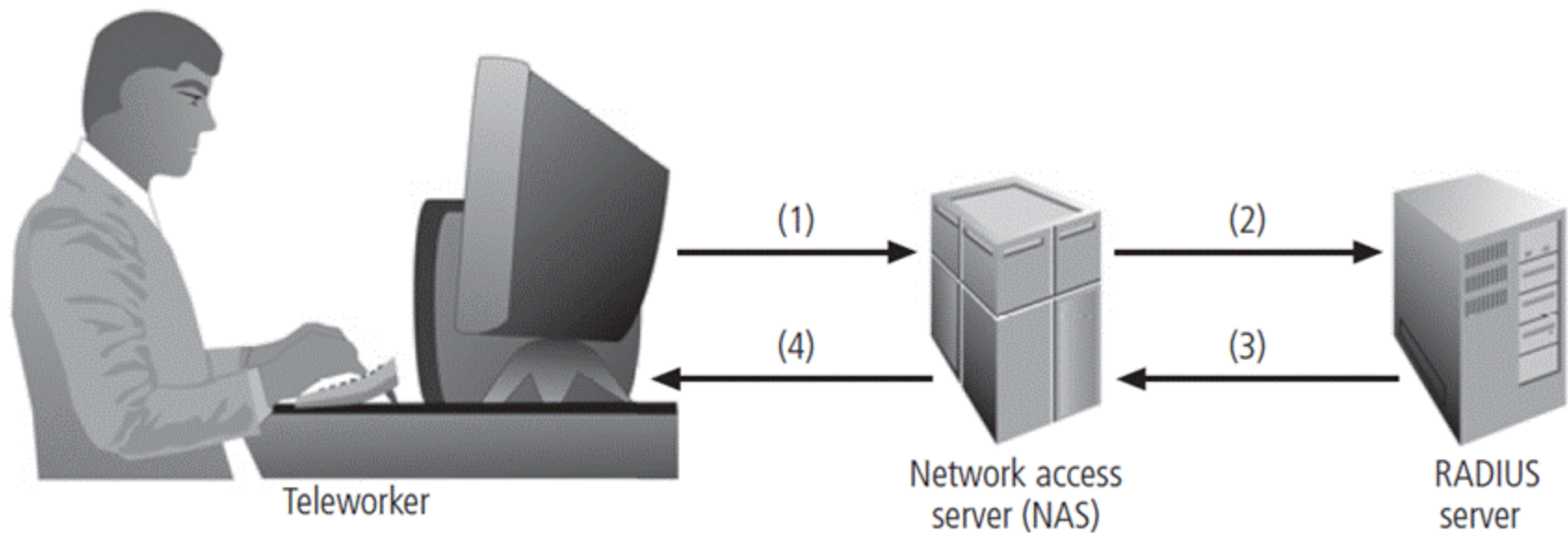
- Software filter—not a firewall—that allows administrators to restrict content access from within a network
- Essentially a set of scripts or programs restricting user access to certain networking protocols/Internet locations
- Primary purpose to restrict internal access to external material
- Most common content filters restrict users **from accessing non-business Web sites or deny incoming spam.**

3-Protecting Remote Connections

- Installing Internetwork connections requires leased lines or other data channels; these connections are usually secured under the requirements of a formal service agreement.
- When individuals seek to connect to an organization's network, a more flexible option must be provided.
- Options such as virtual private networks (VPNs) have become more popular due to the spread of Internet.

Remote Access

- Unsecured, dial-up connection points represent a substantial exposure to attack.
- Attacker can use a device called a **war dialer** to locate the connection points.
- War dialer: automatic phone-dialing program that dials every number in a configured range and records number if modem picks up
- Some technologies (RADIUS systems; TACACS; CHAP password systems) have improved the authentication process.



1. Remote worker dials NAS and submits username and password
2. NAS passes username and password to RADIUS server
3. RADIUS server approves or rejects request and provides access authorization
4. NAS provides access to authorized remote worker

Figure 6-20 RADIUS configuration

Virtual Private Networks (VPNs)

- **Private and secure** network connection between systems; uses data communication capability of unsecured and public network
- **Securely extends** organization's internal network connections to remote locations
- VPN must accomplish:
 - **Encapsulation** of incoming and outgoing data
 - **Encryption** of incoming and outgoing data
 - **Authentication** of remote computer and perhaps remote user as well
- In most common implementation, it allows the user to turn Internet into a private network.

Virtual Private Networks (VPNs) (cont'd)

- **Tunnel mode**

- Establishes two perimeter tunnel servers to **encrypt all traffic** that will traverse **unsecured network**
- Entire client package encrypted from one tunneling server to another
- Primary benefit to this model is that an **intercepted packet** reveals nothing about the true destination system.

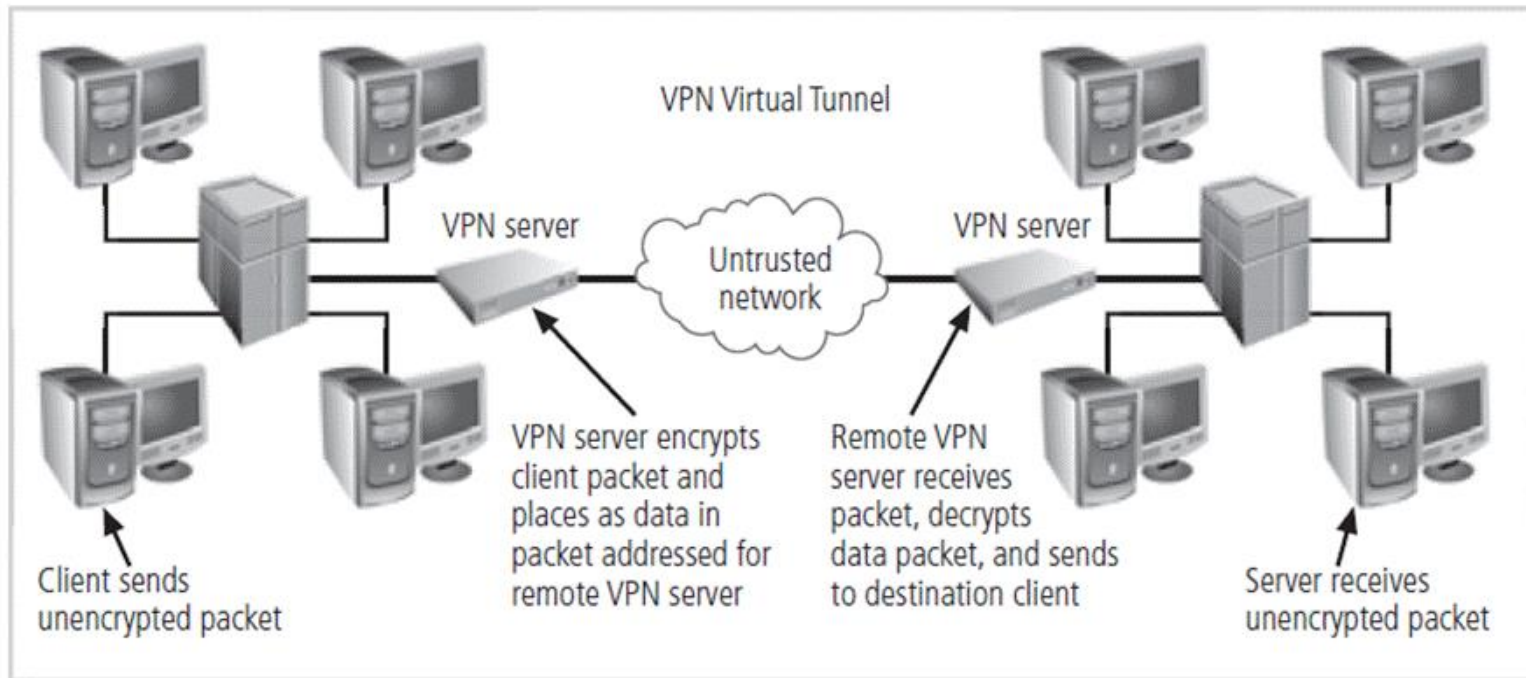


Figure 6-24 Tunnel mode VPN

4-Intrusion Detection and Prevention Systems

- An intrusion occurs when an attacker **attempts to gain entry into or disrupt the normal operations** of an organization's information systems.
- **Intrusion prevention** consists of **activities that deter** an intrusion.
- **Intrusion detection** consists of **procedures and systems** that **identify** system intrusions.
- Intrusion **reaction** encompasses actions an organization undertakes when intrusion event is detected.

Intrusion Detection and Prevention Systems (cont'd)

- Intrusion correction activities: **complete restoration** of operations to a normal state and seek to identify source and method of intrusion
- Intrusion detection systems **detect a violation** of its configuration and activate alarm.
- Many IDPSs enable administrators to configure systems to **notify them directly of trouble via e-mail or pagers.**
- Systems can also be configured to notify an external security service organization of a “break-in.”

Why Use an IDPS?

- Intrusion detection:
 - Primary purpose to **identify and report** an intrusion
 - Can quickly contain attack and **prevent/mitigate** loss or damage
 - Detect and deal with preambles to attacks
- **Data collection** allows the organization to examine **what happened after an intrusion and why.**
- Serves **as a deterrent by increasing the fear of detection**
- Can help management with **quality assurance** and **continuous improvement**

Types of IDPSs

- IDPSs operate as **network-based** or **host-based** systems.
- Network-based IDPS is focused on protecting **network information assets**.
 - **Wireless IDPS:**
 - focuses on wireless networks
 - **Network behavior analysis IDPS:**
 - examines **traffic flow** on a network in an attempt to recognize **abnormal patterns**
 - **Ex:**(DoS) attacks, scanning, worms, unexpected application services, and policy violations.

Types of IDPSs (cont'd)

- Host-based IDPS (HIDPS)
 - Resides on a particular computer or server (host) and monitors activity only on that system
 - Benchmarks and monitors the status of key system files and detects when intruder creates, modifies, or deletes files

Types of IDPSs (cont'd)

- Disadvantages of HIDPSs
 - Pose more management issues
 - Does not detect multihost scanning, nor scanning of non-host network devices
 - Susceptible to some DoS attacks
 - Can use large amounts of disk space
 - Can inflict a performance overhead on its host systems

IDPS Detection Methods

- Anomaly-based detection (or behavior-based detection)
 - collects statistical summaries by observing traffic known to be normal.
 - When measured activity is outside baseline parameters or clipping level, IDPS **sends alert** to administrator.
 - IDPS can detect new types of attacks.
 - May generate many **false positives**:
 - A *false positive* is an error in which a test result incorrectly indicates the presence of a condition....

IDPS Detection Methods (cont'd)

- Log file monitors(similar to NIDPS)
 - Reviews log files generated by servers, network devices, and even other IDPSs for patterns and signatures
 - Patterns that signify attack may be much easier to identify when entire network and its systems are viewed as a whole
 - Requires considerable resources since it involves the collection, movement, storage, and analysis of large quantities of log data

IDPS Response Behavior

- IDPS response to external stimulation depends on the configuration and function.
- IDPS responses can be classified as active or passive.
 - **Active response**: collecting additional information about the intrusion, modifying the network environment, taking action against the intrusion.
 - **Passive response**: setting off alarms or notifications, collecting passive data through SNMP traps.
- Many IDPSs can generate routine reports and other detailed documents.

Strengths and Limitations of IDPSs

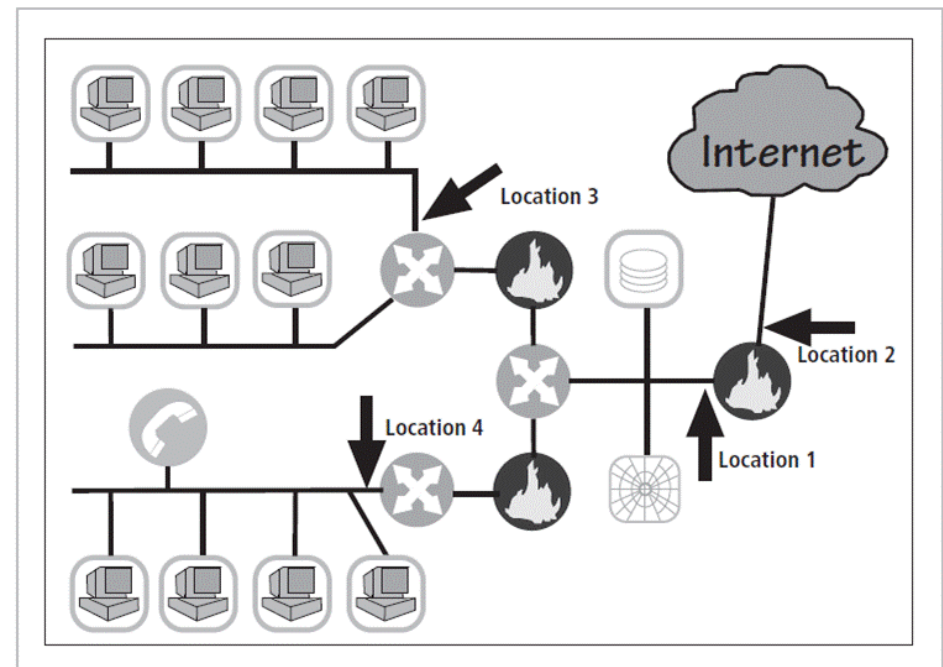
- IDPSs cannot perform the following functions:
 - Compensating for weak/missing security mechanisms in protection infrastructure.
 - Instantaneously detecting, reporting, responding to attack when there is heavy network or processing load.
 - Detecting new attacks or variants of existing attacks.
 - Effectively responding to attacks by sophisticated attackers.
 - Automatically investigating attacks without human intervention.

Deployment and Implementation of an IDPS

- An IDPS can be implemented via one of three basic control strategies:
 - Centralized:
 - All IDPS control functions are implemented and managed in a central location.
 - Fully distributed:
 - All control functions are applied at the physical location of each IDPS component.
 - Partially distributed:
 - Combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks.

Deployment and Implementation of an IDPS (cont'd)

- Deploying network-based IDPSs
 - NIST recommends four locations for NIDPS sensors
 - Location 1: Behind each external firewall, in the network DMZ
 - Location 2: Outside an external firewall
 - Location 3: On major network backbones
 - Location 4: On critical subnets



Deployment and Implementation of an IDPS (cont'd)

- Deploying host-based IDPSs
 - Deployment begins with implementing most critical systems first.
 - Installation continues until either all systems are installed or the organization reaches planned degree of coverage it will accept.

5-Scanning and Analysis Tools

- **Scanning tools** typically are used to collect information that an attacker needs to launch a successful attack.
- **Attack protocol** is a logical sequence of steps or processes used by an attacker to launch an attack against a target system or network.
- **Footprinting**: process of collecting publicly available information about a potential target
- **Fingerprinting**: reveals useful information about the internal structure and nature of the target system or network to be attacked.
- These tools are **valuable to the network defender** since they can quickly pinpoint the parts of the systems or network that need a **prompt repair to close vulnerabilities**.

6-Port Scanners

- Tools used by both attackers and defenders to identify/fingerprint computers active on a network and other useful information
- Can either perform generic scans or those for specific types of computers, protocols, or resources
- The more specific the scanner is, the more useful its information is to attackers and defenders.

7-Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator/attacker in analyzing them.
- Administrators who feel wary of using the same tools that attackers use should remember:
 - User intent dictates how gathered information will be used.
 - To defend a computer or network well, administrators must understand ways it can be attacked.
- A tool that can help close an open or poorly configured firewall will help the network defender minimize risk from attack.

8-Operating System Detection Tools

- Ability to detect a target computer's operating system (OS) is very valuable to an attacker.
 - Once OS is known, the attacker can easily determine the vulnerabilities to which it is susceptible.
- Many tools use networking protocols to determine a remote computer's OS.

9-Vulnerability Scanners

- **Active vulnerability scanners** examine networks for highly detailed information and initiate traffic to determine security holes.
- **Passive vulnerability scanners** listen in on network and identify the vulnerable versions of both server and client software.
- **Passive vulnerability scanners** have the ability to find **client-side vulnerabilities** typically not found in active scanners.

10-Packet Sniffers

- Network tool that captures **copies of packets** from network and analyzes them
- Can provide network administrator with **valuable information** for diagnosing and resolving networking issues
- In the wrong hands, a sniffer can be used to **eavesdrop** on network traffic.
- To use packet sniffers legally, an administrator must be on a network that the organization owns, be under direct authorization of owners of the network, and have knowledge and consent of the content's creators.

11-Wireless Security Tools

- An organization that spends its time securing a wired network while ignoring wireless networks is exposing itself to a **security breach**.
- Security professionals must assess the risk of wireless networks.
- A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and **assess the level of privacy or confidentiality afforded on the wireless network**.

12-Backup

- **There are three main types of backup:**
- **Full backup.**
 - refers to the process of **copying everything** that is considered important and that must not be lost.
- **Incremental backup.**
 - making copies of the files by taking into account the changes made in them since the previous backup. it saves time and space.
 - **do not try to employ this type of backup strategy using manual means**
- **Differential backup.**
 - has the same basic structure as an incremental backup—it involves making copies **only of new files or of files that underwent some kind of change.**
 - all the files created since the **original full backup** will always be copied again.

12-Backup Technologies

The most common techniques or technologies:

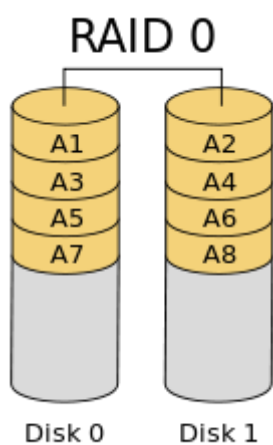
- Removable media.
- Redundancy.
- External hard drive.
- Hardware appliances.
- **Backup software.**
- **Cloud backup services.**

12-Backup Technologies(cont'd)

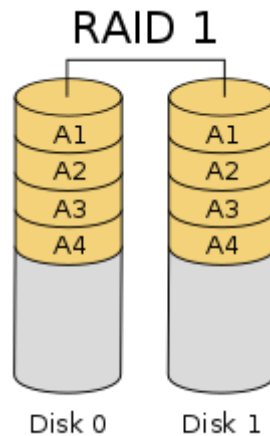
- Redundancy:
 - Data **redundancy** and **backups** are intended to **prevent data loss**, but the two technologies are quite different.
 - Data **redundancy** often takes the form of a synchronized copy of the organization's data. ...
 - **Backups**, are copies of data and other resources.

12-Backup Technologies(cont'd)

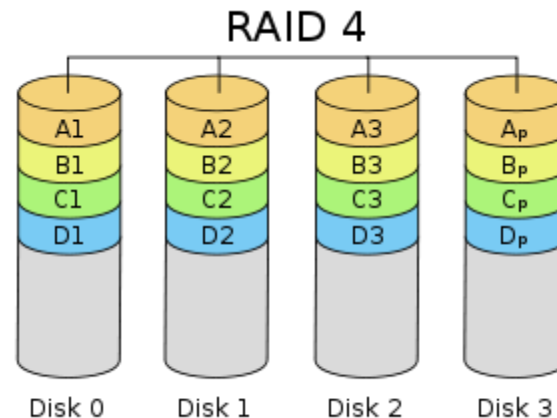
- **RAID**(Redundant Array of Independent Disks):
 - is a **data storage virtualization technology** that combines **multiple physical disk drive** components into one or more logical units for the purposes of **data redundancy**, **performance improvement**, or both



Disk stripping



Disk mirroring



Disk stripping + parity

12-Backup-Lifespan

Medium	Lifespan	Capacity
HD	5–10 years	From GB to TB
Floppy disk	3–5 years	Hundreds of KB to a few MB
CD/CD-ROM	25–50 years	80 minutes or 700 MB
MD (Mini Disc)	25–50 years	60 minutes or 340 MB
DVD	25–50 years	4.7 GB
SD card	10 years or more	A few MB to tens of GB
USB flash drive	10 years or more	A few MB to tens of GB
SSD	10 years or more	From GB to TB

12-Cloud Data Backup

- a service in which the **data** and applications on a business's servers are backed up and stored on a **remote server**.
- Customers typically back up and restore their **data** and apps **using a web browser or a service provider's control panel**.

Top best cloud storage services 2021:

- ✓ **iDrive**. Quality storage solution that also includes network drives.
- ✓ **pCloud**. Go-to provider for large files.
- ✓ **Mega**. Beefed up security offering.
- ✓ **OneDrive**. Windows-first option.
- ✓ **iCloud**. Apple's solution for iOS and macOS users.
- ✓ **Google Drive**.
- ✓ **Box**.
- ✓ **NextCloud**.

12-Backup Mistakes

Common 5 mistakes made while doing a backup:

1. Not doing a backup.
2. Saving the backup copies on the same hardware as the original files.
3. Not testing the backup.
4. Not running the backup regularly and sufficiently frequently.
5. Not labeling the backup files.

12-Backup Strategy

The 3-2-1 backup strategy states that you should keep:

1. At least **THREE** copies of your data;
2. Backed-up data on **TWO** different storage types;
3. At least **ONE** copy of the data **offsite**.