



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7028

Data Security and Compliance

Week 8: Protection Mechanisms and Physical Security

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Explain the various approaches to firewall implementation.
- Describe virtual private networks (VPNs) and discuss the technology that enables them.
- Identify and describe the categories and models of Intrusion Detection and Prevention Systems (IDPS).
- Describe the detection approaches used in modern IDPS.
- Define and explain honeypots, honeynets, and padded cell systems.

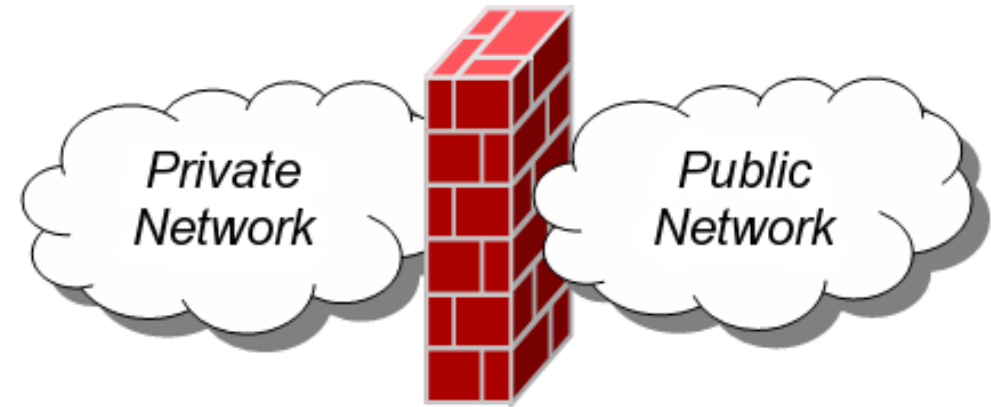
Key Concepts

We look at:

- Firewalls
- Firewall Types
- Firewall policies
- VPNs
- VPN Types
- IPS and IDS
- Honeypots, Honeynets and padded cell systems

Firewalls

- A **firewall** is an integrated collection of security measures designed to prevent unauthorised electronic access to a networked computer system.
- A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another.



Firewalls Processing Modes

- Packet filtering by data packet header information.
- Application-layer proxy by higher layer protocols and can include cache services.
- MAC layer firewalls by MAC address.
- Hybrids by a combination of the above.

Firewall Types

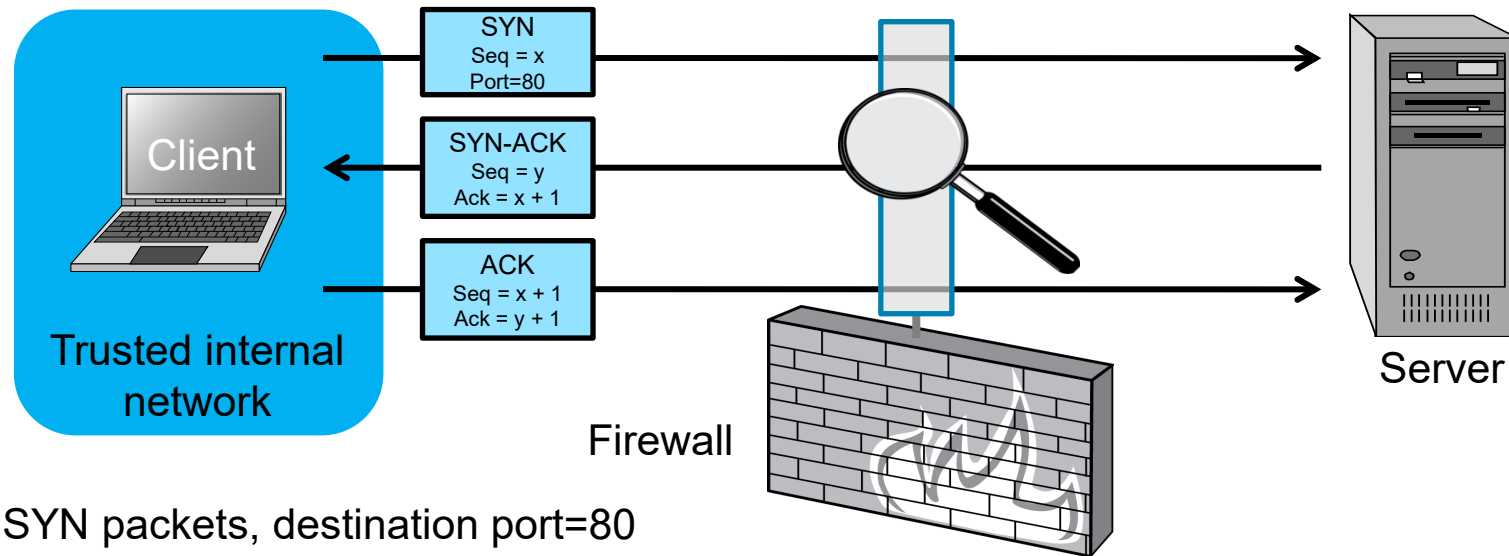
- **packet filters (stateless)**
 - If a packet matches the packet filter's set of rules, the packet filter will drop or accept it
- **"stateful" filters**
 - it maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection, or is an invalid packet.
- **application layer**
 - It works like a proxy it can “understand” certain applications and protocols.
 - It may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, vulnerabilities, ...)

Packet-Filtering Firewalls

- Packet-filtering firewalls examine the header information of data packets.
- Most often based on the combination of the following:
 - 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.

Stateless Firewalls

- A stateless firewall doesn't maintain any remembered context (or "state") with respect to the packets it is processing. Instead, it treats each packet attempting to travel through it in isolation without considering packets that it has processed previously.



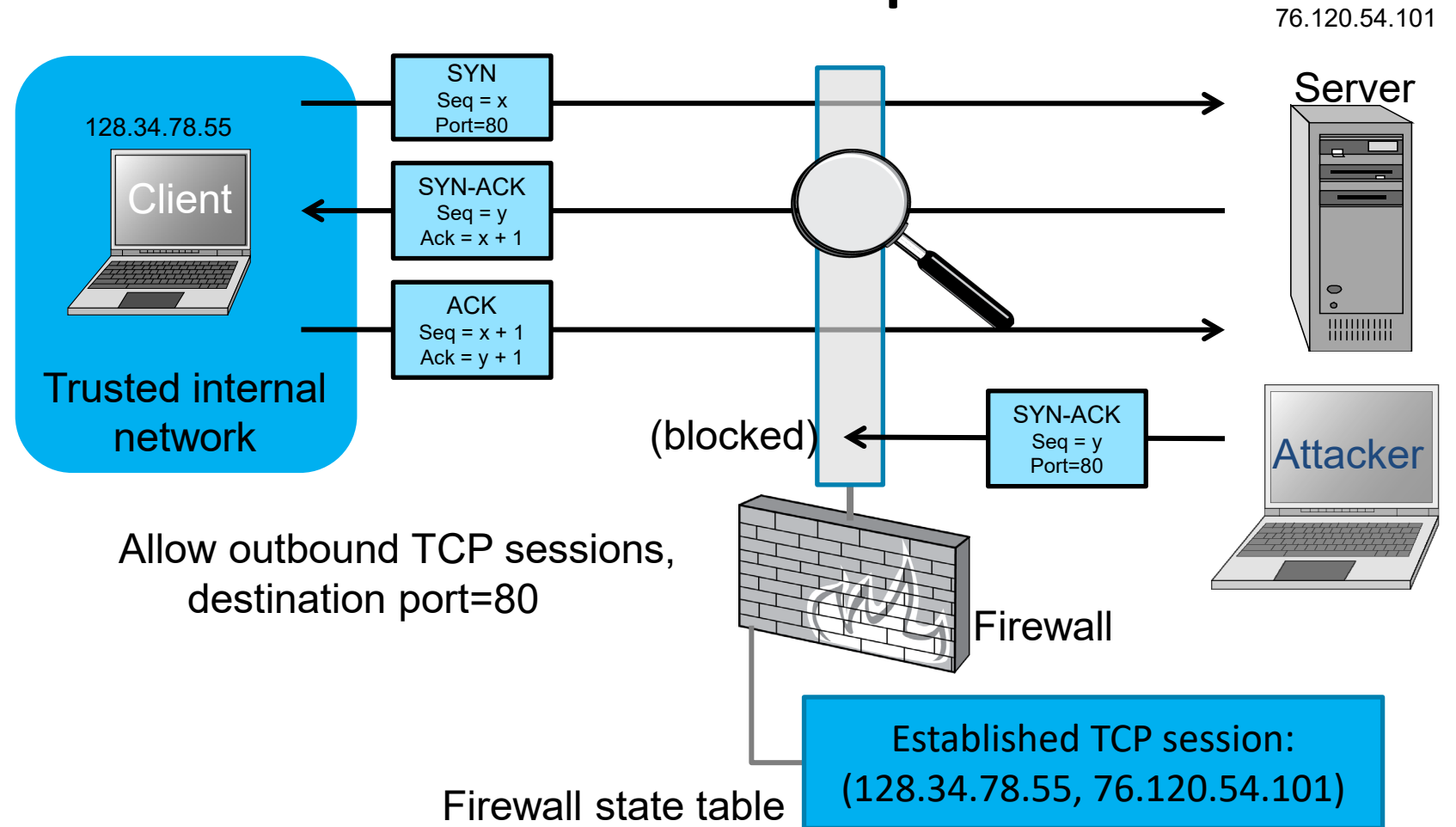
Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

Statefull Firewalls (SPI)

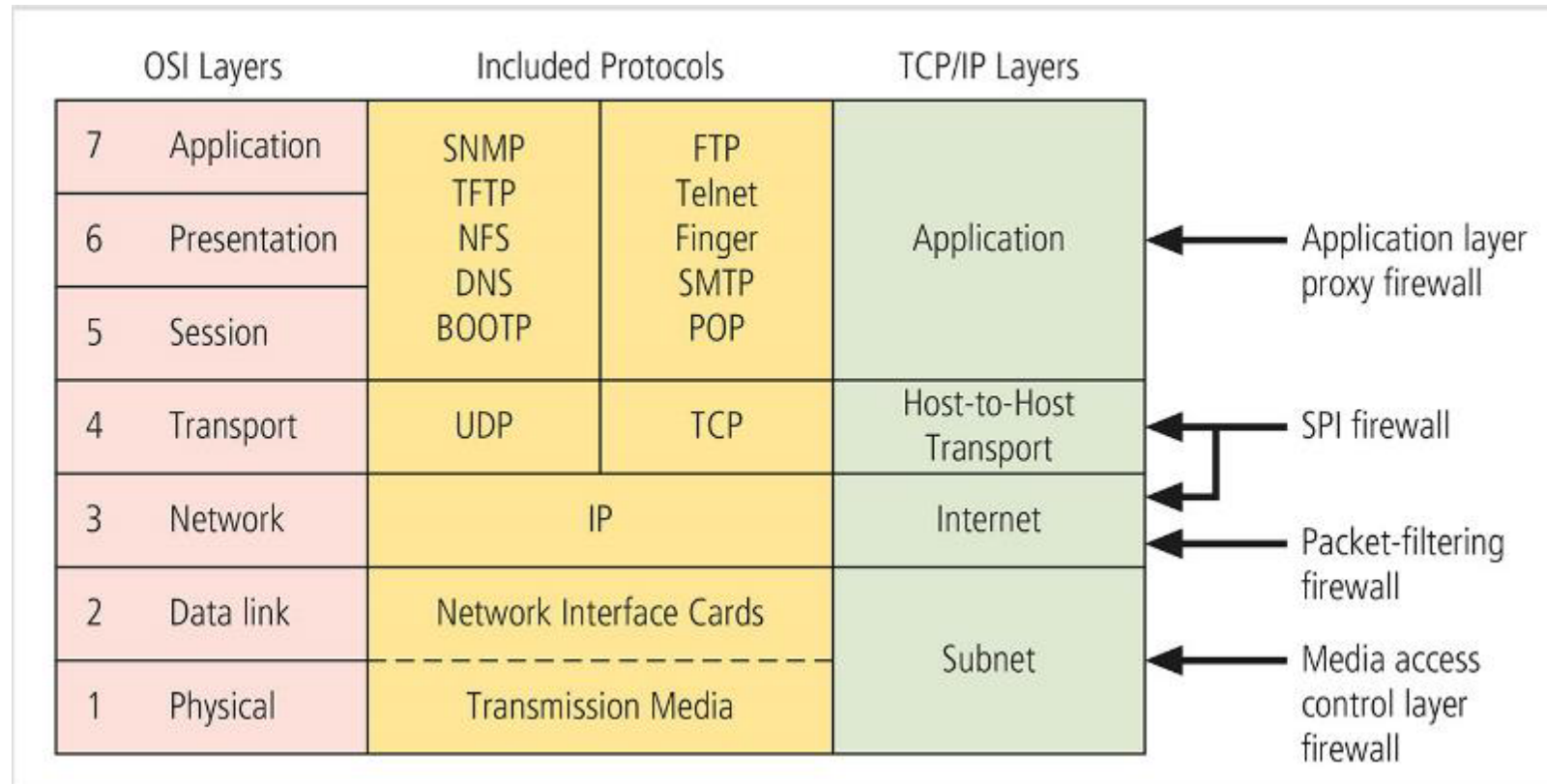
- **Stateful firewalls** can tell when packets are part of legitimate sessions originating within a trusted network.
- Stateful firewalls maintain tables containing information on each active connection, including the IP addresses, ports, and sequence numbers of packets.
- Using these tables, stateful firewalls can allow only inbound TCP packets that are in response to a connection initiated from within the internal network.

Statefull Firewall Example

Allow only
requested TCP
connections



Firewall Types and Protocol Levels



Hybrid Firewalls

- Combine elements of other types of firewalls, that is, elements of packet filtering and proxy services, or of packet filtering and circuit gateways.
- Alternately, may consist of two separate firewall devices, each a separate firewall system, but connected to work in tandem.
- Enables an organization to make security improvement without completely replacing existing firewalls.
- Include the Next Generation Firewall (NGFW) and Unified Threat Management (UTM) devices.

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: Single Bastion Hosts, Screened Host and Screened Subnet (with demilitarized zone (DMZ)).

Single Bastion Hosts

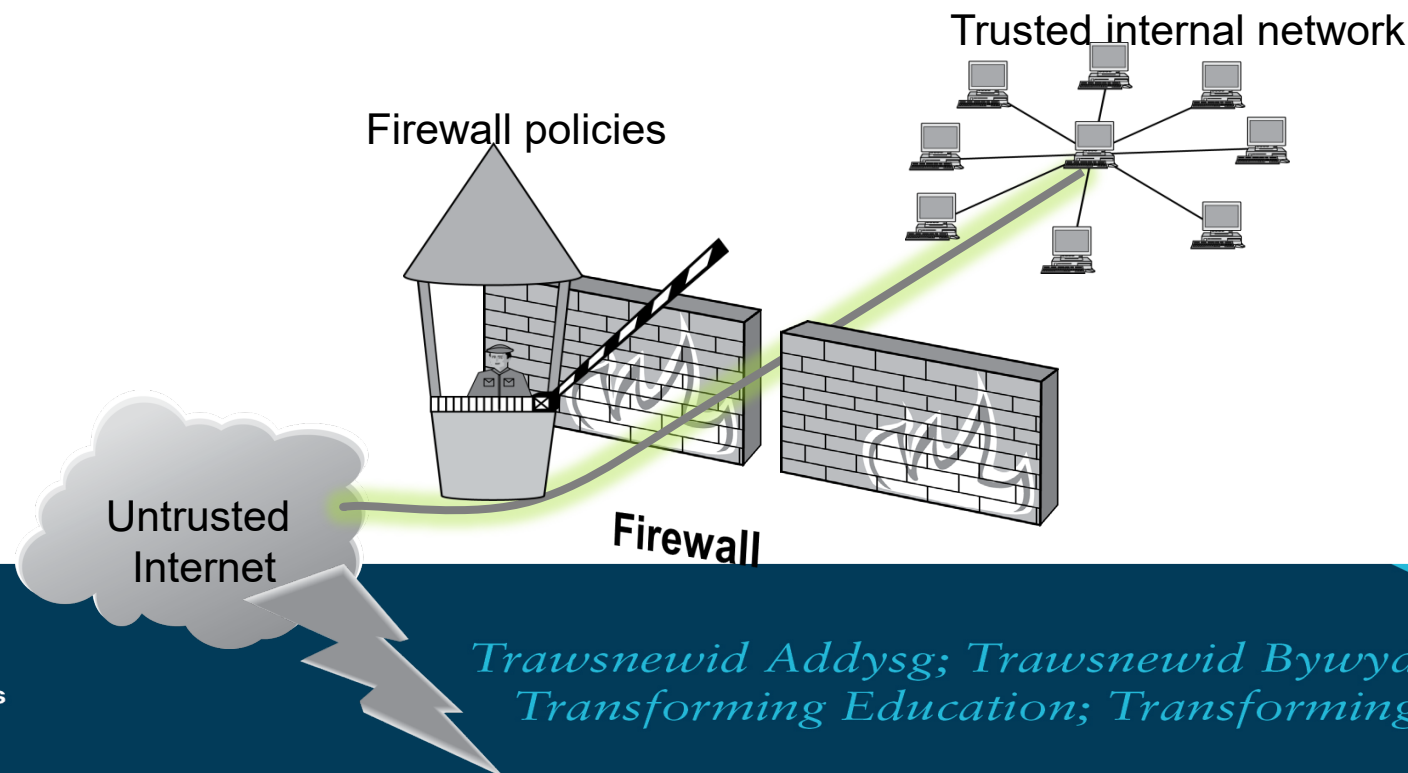
- Commonly referred to as sacrificial host as it stands as sole defender on the network perimeter.
- Usually implemented as a dual-homed host, which contains two network interface cards (NICs), one connected to external network, one connected to internal network.
- Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers.

Best Practices for Firewalls

- All traffic from the trusted network is allowed out.
- Firewall device is never directly accessed from the public network.
- Simple Mail Transport Protocol (SMTP) data are allowed to pass through firewall but must go to SMTP server.
- Internet Control Message Protocol (ICMP) data are denied.
- Telnet access to internal servers should be blocked from the public network.
- When Web services are offered outside the firewall, HTTP traffic should be blocked from reaching internal networks using a DMZ or proxy access.
- All data not verifiably authentic should be denied.

Firewall Policies

- To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called **firewall policies**.



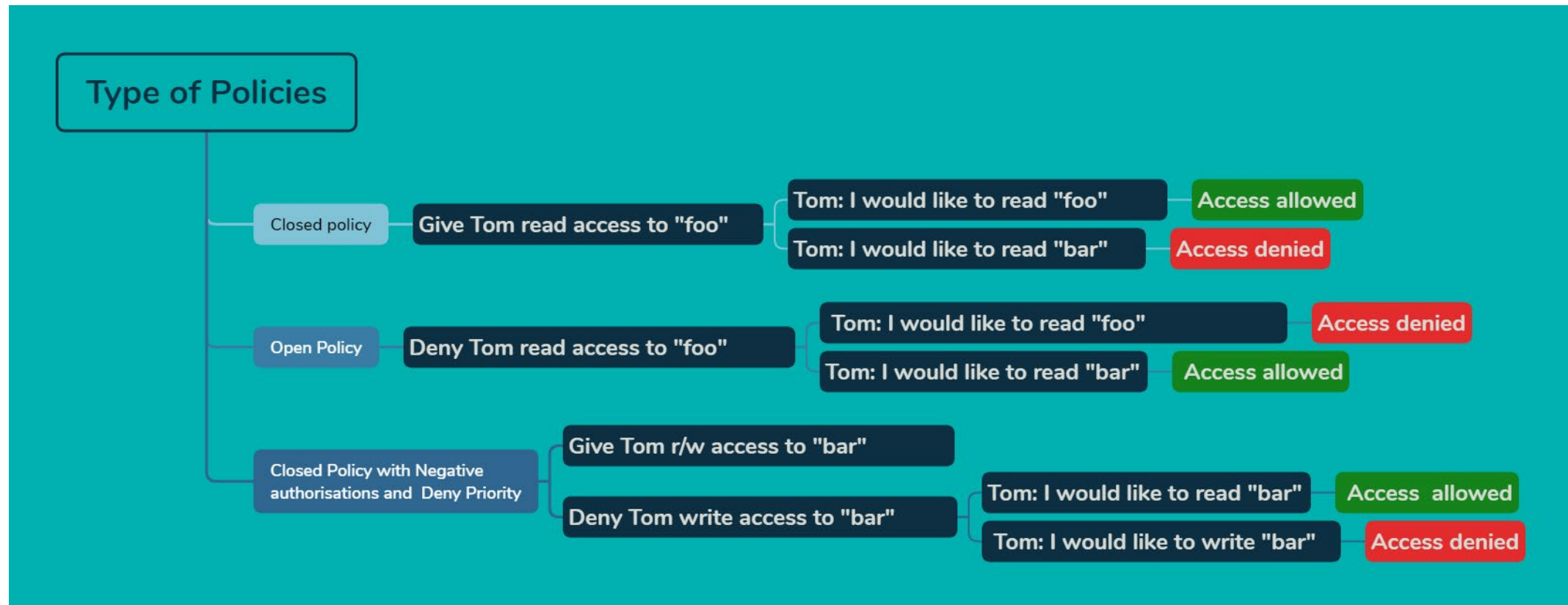
Policy Actions

- Packets flowing through a firewall can have one of three outcomes:
 - **Accepted:** permitted through the firewall
 - **Dropped:** not allowed through with no indication of failure
 - **Rejected:** not allowed through, accompanied by an attempt to inform the source that the packet was rejected
- Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:
 - TCP or UDP
 - the source and destination IP addresses
 - the source and destination ports
 - the application-level payload of the packet (e.g., whether it contains a virus).

Blacklists and White Lists

- There are two fundamental approaches to creating firewall policies (or rulesets) to effectively minimize vulnerability to the outside world while maintaining the desired functionality for the machines in the trusted internal network (or individual computer).
- **Blacklist Approach**
 - Allows all traffic except what is explicitly blocked.
 - More flexible but less secure, as it assumes all threats can be identified.
- **Whitelist Approach**
 - Blocks all traffic unless explicitly allowed.
 - More secure but requires careful rule management..

Type of policies



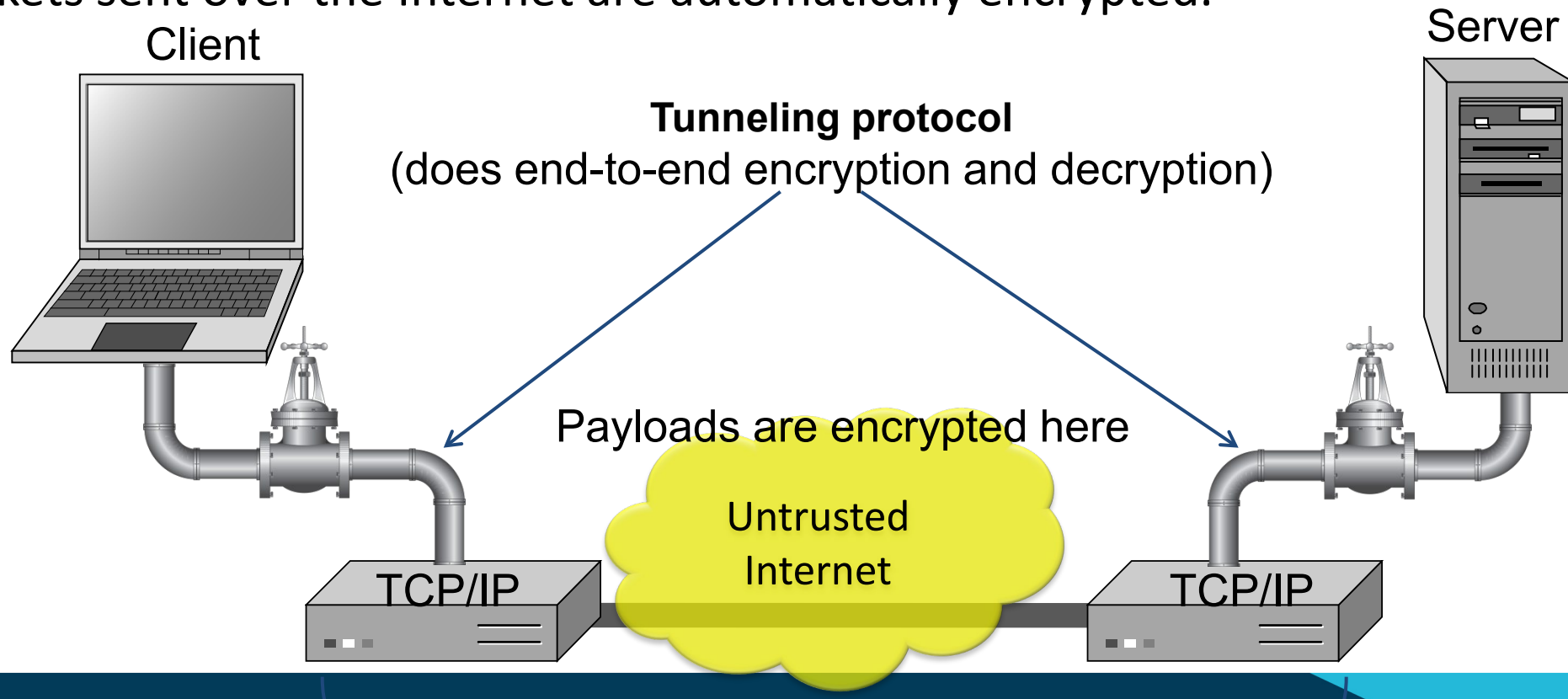
VPN

Tunnels

- The contents of TCP packets are not normally encrypted, so if someone is eavesdropping on a TCP connection, he can often see the complete contents of the payloads in this session.
- One way to prevent such eavesdropping without changing the software performing the communication is to use a **tunnelling protocol**.
- In such a protocol, the communication between a client and server is automatically encrypted, so that useful eavesdropping is infeasible.

Tunneling Prevents Eavesdropping

- Packets sent over the Internet are automatically encrypted.



IPSec

- IPSec defines a set of protocols to provide confidentiality and authenticity for IP packets
- Each protocol can operate in one of two modes, **transport mode** or **tunnel mode**.
 - In **transport mode**, additional IPsec header information is inserted before the data of the original packet, and only the payload of the packet is encrypted or authenticated.
 - In **tunnel mode**, a new packet is constructed with IPsec header information, and the entire original packet, including its header, is encapsulated as the payload of the new packet.

Virtual Private Networking (VPN)

- **Virtual private networking (VPN)** is a technology that allows private networks to be safely extended over long physical distances by making use of a public network, such as the Internet, as a means of transport.
- VPN provides guarantees of data confidentiality, integrity, and authentication, despite the use of an untrusted network for transmission.
- There are two primary types of VPNs, **remote access VPN** and **site-to-site VPN**.

Types of VPNs

- **Remote access** VPNs allow authorized clients to access a private network that is referred to as an **intranet**.
 - For example, an organization may wish to allow employees access to the company network remotely but make it appear as though they are local to their system and even the Internet itself.
 - To accomplish this, the organization sets up a VPN endpoint, known as a **network access server, or NAS**. Clients typically install VPN client software on their machines, which handle negotiating a connection to the NAS and facilitating communication.
- **Site-to-site** VPN solutions are designed to provide a secure bridge between two or more physically distant networks.
 - Before VPN, organizations wishing to safely bridge their private networks purchased expensive leased lines to directly connect their intranets with cabling.

INTRUSION DETECTION AND PREVENTION SYSTEMS

Intrusion Detection and Prevention Systems

- An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an organisation'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 organisation undertakes when intrusion event is detected

Intrusion Detection and Prevention Systems

- 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 organisation of a “break-in”.

Intrusion Detection Systems

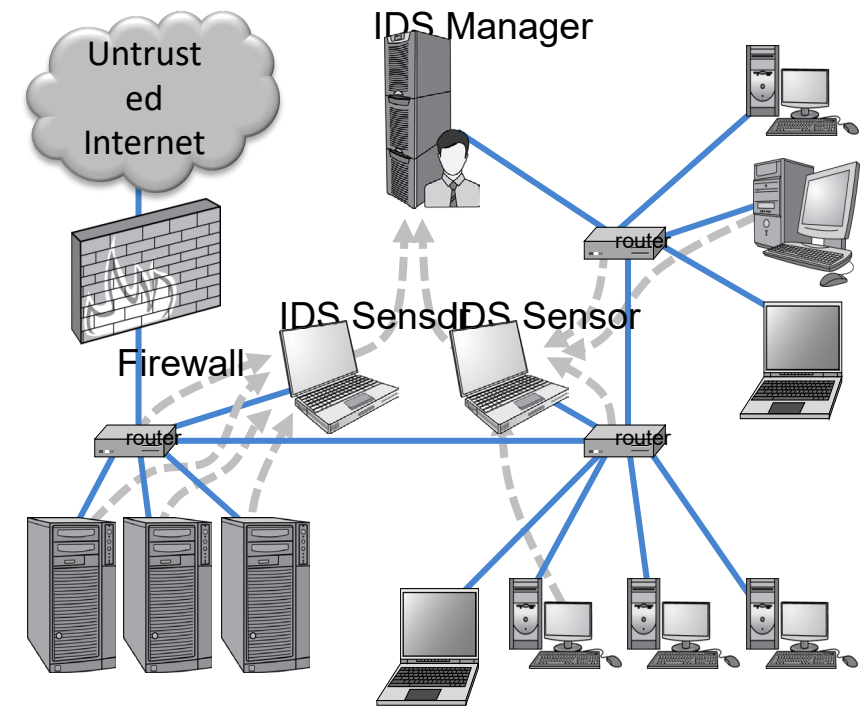
- **Intrusion**
 - Actions aimed at compromising the security of the target (confidentiality, integrity, availability of computing/networking resources)
- **Intrusion detection**
 - The identification through intrusion signatures and report of intrusion activities
- **Intrusion prevention**
 - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network

Intrusion Detection Systems

- **Intrusion:** Unauthorised access or disruption of an organisation's systems.
- **Prevention:** Measures taken to deter intrusions.
- **Detection:** Systems and procedures identifying intrusions.
- **Reaction:** Actions taken in response to an intrusion.
- **Correction:** Restoring normal operations and identifying the attack source.
- **IDPS Alerts:** Detect violations, trigger alarms, and notify administrators or external security services.

IDS Components

- The **IDS manager** compiles data from the IDS sensors to determine if an intrusion has occurred.
- This determination is based on a set of **site policies**, which are rules and conditions that define probable intrusions.
- If an IDS manager detects an intrusion, then it sounds an **alarm**.

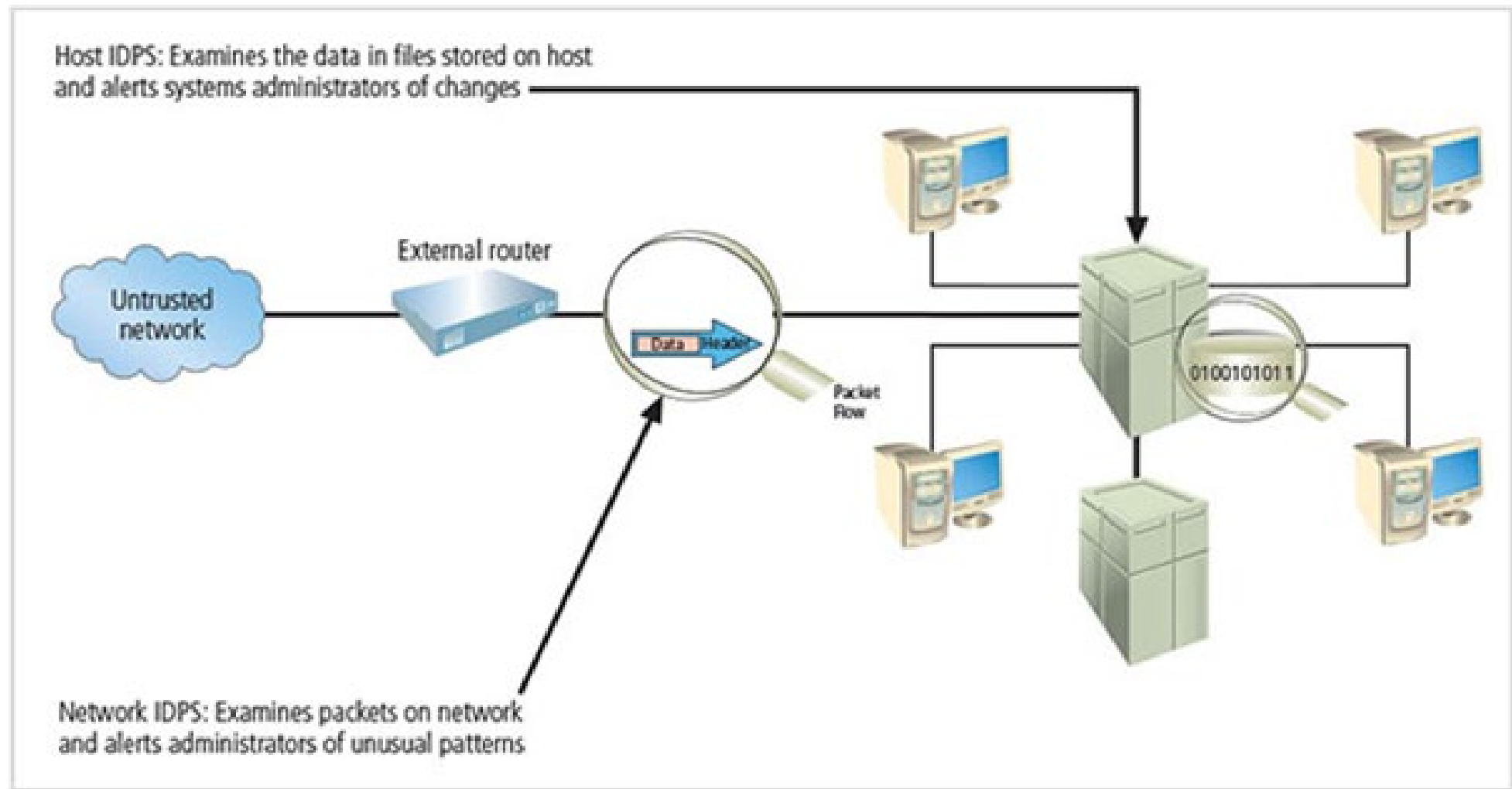


Why use an Intrusion Detection and Prevention system IDPS?

- While an IDS primary purpose to identify and report an intrusion, an IDS with a prevention mechanism can quickly contain an attack and prevent/mitigate the loss or damage.
 - An IPDS Detect and deal with preambles to attacks
 - Data collection allows the organisation 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 behaviour analysis IDPS examines traffic flow on a network in an attempt to recognise abnormal patterns



© Cengage Learning 2015

Network-based IDPS (NIDPS)

- **Location:** Resides on a computer or appliance within a network segment, monitoring for attack indicators.
- **Packet Analysis:** Looks for attack patterns in network traffic.
- **Network Placement:** Installed to monitor traffic entering or exiting a specific network segment.
- **Attack Detection:** Compares activity against known attack signatures in the knowledge base.
- **TCP/IP Stack Implementation:**
 - Protocol Stack Verification: Detects invalid data packets.
 - Application Protocol Verification: Examines higher-level protocols for unexpected or improper packet behaviour.

Advantages of NIDPSs

- Good network design and placement of NIDPS can enable an organisation to monitor a large network with few devices
- NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
- NIDPS are not usually susceptible to direct attack and may not be detectable by attackers

Disadvantages of NIDPSs

- Can become overwhelmed by network volume and fail to recognise attacks
- Require access to all traffic to be monitored
- Cannot analyse encrypted packets
- Cannot reliably ascertain if an attack was successful or not
- Some forms of attacks are not easily discerned by NIDPS's, specifically those involving fragmented packets

Wireless NIDPS

- Monitors and analyses wireless network traffic
- Issues associated with it include physical security, sensor range, wired network connections, cost, access point and wireless switch locations,

Network behaviour analysis systems

- Identify problems related to the flow of traffic
- Types of events commonly detected include denial-of-service (DoS) attacks, scanning, worms, unexpected application services, and policy violations
- Offer intrusion prevention capabilities that are passive, inline, and both passive and inline

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
- Advantage over NIDPS: can access encrypted information traveling over network and make decisions about potential/actual attacks
- Most HIPDS's work on the principle of configuration and change management

Advantages of HIDPSs

- Can detect local events on host systems and detect attacks that may elude a network-based IDPS
- Functions on host system, where encrypted traffic will have been decrypted and is available for processing
- Not affected by use of switched network protocols
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

Disadvantages of HIDPSs

- Pose more management issues
- Vulnerable both to direct attacks and attacks against the host operating system
- 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

Signature-based detection

(or knowledge-based detection or misuse detection)

- Examines network traffic in search of patterns that match known signatures
- Widely used because many attacks have clear and distinct signatures
- Problem with this approach is that new attack patterns must continually be added to the IDPS's database of signatures
 - Slow methodical attack involving multiple events might escape detection

Anomaly-based detection (or behaviour-based detection)

- Anomaly-based detection collects statistical summaries by observing traffic known to be normal
- When measured activity is outside the baseline parameters or clipping level, IDPS sends an alert to the administrator
- IDPS can detect new types of attacks
 - Requires much more overhead and processing capacity than signature-based detection

IDS Data

- An Intrusion detection should record for each event the following:
 - **Subject:** Initiator of an action on a target.
 - **Object:** Targeted resource (e.g., file, command, device, network protocol).
 - **Action:** Operation performed by the subject on the object.
 - **Exception-Condition:** Errors or exceptions raised by the action.
 - **Resource Usage:** System resources consumed during the action.
 - **Time-Stamp:** Unique identifier marking when the action was initiated.

HONEYPOTS, HONEYNETS, AND PADDED CELL SYSTEMS

Honeypots and Honeynets

- Honeypots: Decoy systems designed to divert attackers from critical systems and gather information about their activities.
- Honeynets: A network segment with multiple interconnected honeypots.
- Honeypots are designed to:
 - Divert attackers from accessing important systems.
 - Collect data on the attacker's actions.
 - Encourage attackers to remain on the system long enough for administrators to document and potentially respond.

Padded cell system

- Padded cell system: protected honeypot that cannot be easily compromised
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS
- When the IDPS detects the attackers, padded cell system seamlessly transfers them to a special simulated environment where they can cause no harm—hence the name padded cell

References

- Slides are devised from the recommended books:
 - Whitman, M.E.,Mattord, H.J., Principles of Information Security . Cengage Learning 658.
 - Management of Information Security 6th Ed by Whitman & Herbert Chapter 8: Security Management Models



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk