KENNESAW STATE UNIVERSITY

Module 9:

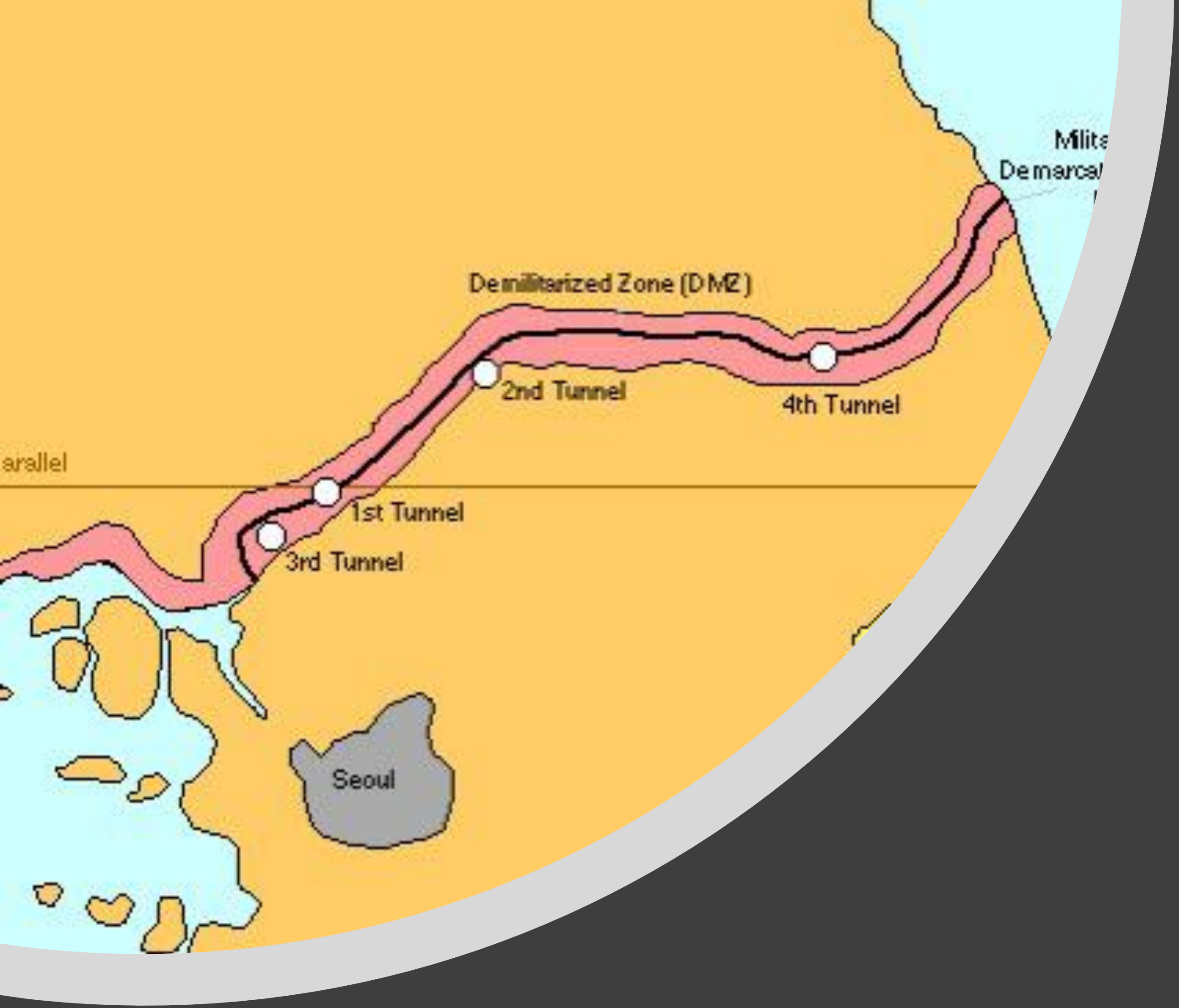
Defense Mechanism for physical IT Systems - Design Secure DMZ, secure firewall, IDS.

Dr. Maria Valero

Agenda

- Defense Mechanism for Physical IT Sytems
    - DMZ
    - Firewall
    - IDS/IPS
- DMZ
- Firewall
- IDS/IPS
- Relationship of all this concepts with IoT Devices

DMZ



DMZ (1)

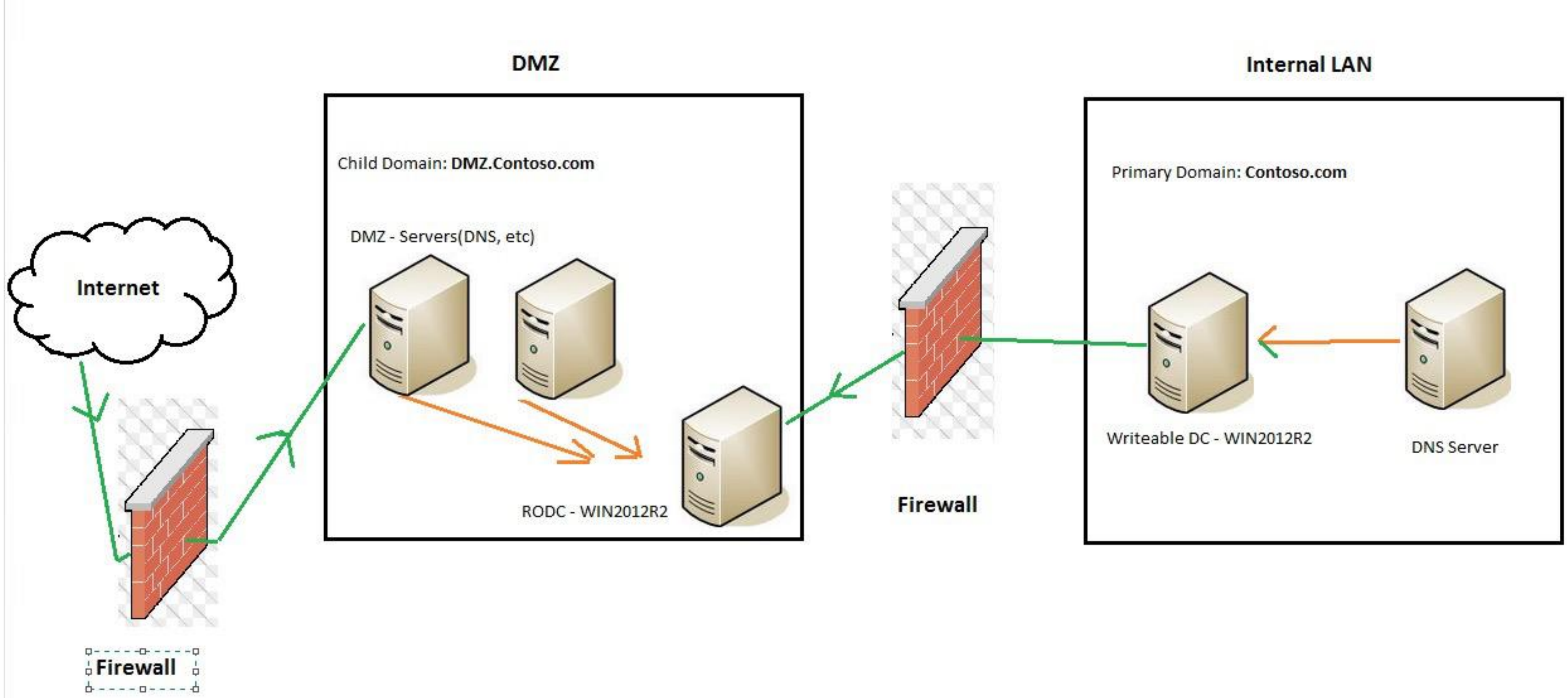
- It means De-Militarized Zone
  - A DMZ is a buffer zone between two adversaries
  - Free of military forces
  - Intended to provide warning of attack

DMZ (2)

- DMZ
  - Computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network
  - Network construct that provides secure segregation of networks that host services for users, visitors, or partners

- DMZ use has become a necessary method of providing a multilayered, defense-in-depth approach to security

DMZ Example


DMZ
Internal LAN
Child Domain: **DMZ.Contoso.com**
Primary Domain: **Contoso.com**
Internet
DMZ - Servers(DNS, etc)
RODC - WIN2012R2
Writeable DC - WIN2012R2
DNS Server
Firewall
Firewall

DMZ Architecture

- Inside-Versus-Outside Architecture
  - Routers act as initial line of defense
- Three-Legged Firewall Architecture
  - Firewall routes traffic to DMZ or internal network
- Weak-Screened Subnet Architecture
  - Router acts as perimeter device
- Strong-Screened Subnet Architecture
  - Both the DMZ and the internal networks are protected by a well-functioning firewall

DMZ Specific Operating System Design

- Precautions for DMZ Setup
  - Designer should consider other possible access to and from the DMZ
- Security Analysis for the DMZ
  - After the DMZ network segment design is finalized and the systems are placed where they need to be, the security requirements of such systems should be taken into account
- ISA Server Support to DMZ Configuration
  - ISA firewall network needs to be created for the wireless DMZ segment
  - ISA firewall networks are defined depending on per-network interfaces

DMZ Router Security Best Practices

- Checklist for ensuring router security:
    - Authenticate routing updates on dynamic routing protocols
    - Use ACLs to protect network resources and prevent address spoofing
    - Secure the management interfaces
    - Lock down the router services
    - Disable interface-related services
    - Disable unneeded services
    - Keep up to date on software bug fixes and vulnerabilities

DMZ Switch Security Best Practices

- Checklist to follow to ensure switch security:
  - Secure the management interfaces
  - Lock down switch services
  - Disable unneeded services
  - Use VLANs to logically segment a switch
  - Use port security to secure the input to an interface by limiting and identifying the MAC addresses of hosts that are allowed to access the port
  - Keep up to date on software bug fixes and vulnerabilities, and upgrade if necessary

Firewall

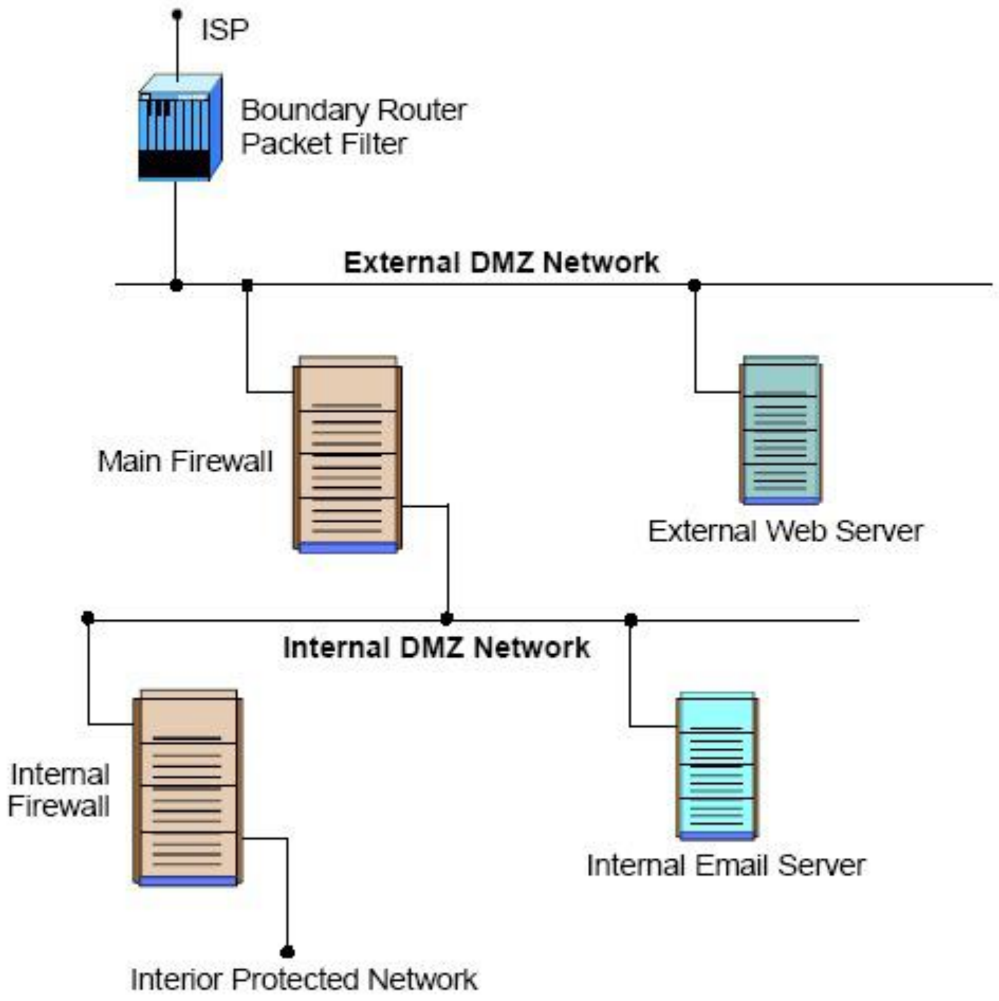
Firewalls (1)

- Firewalls control the flow of network traffic
- Firewalls have applicability in networks where there is no internet connectivity
- Firewalls operate on number of layers
- Can also act as VPN gateways
- Active content filtering technologies

Firewall Environments

- There are different types of environments where a firewall can be implemented.
- Simple environment can be a packet filter firewall
- Complex environments can be several firewalls and proxies

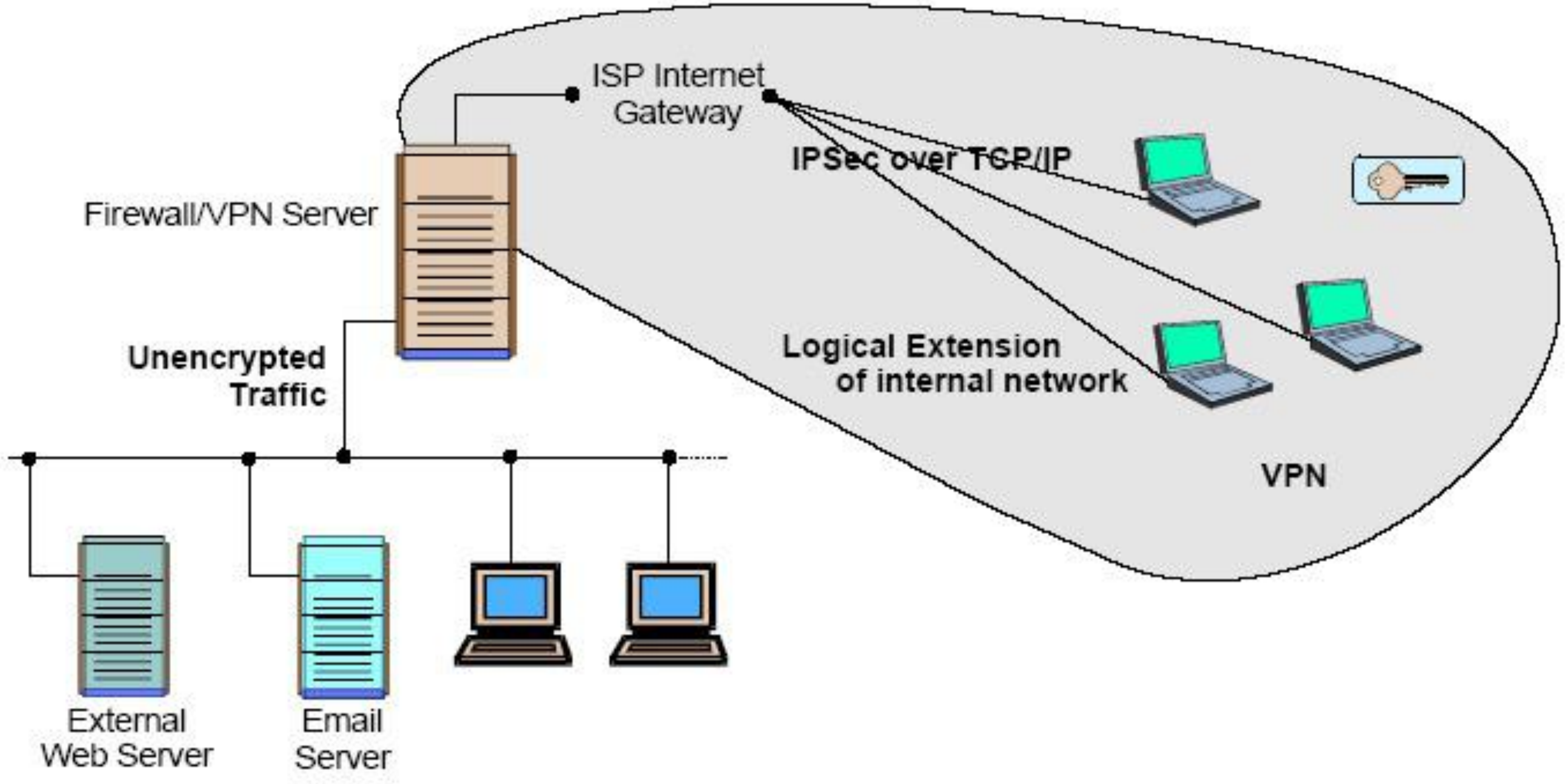
DMZ depends on Firewalls



VPN (1)

- VPN is used to provide secure network links across networks
- VPN is constructed on top of existing network media and protocols
- On protocol level IPsec is the first choice
- Other protocols are PPTP, L2TP

VPN (2)


ISP Internet Gateway
IPSec over TCP/IP
Firewall/VPN Server
Unencrypted Traffic
Logical Extension of internal network
VPN
External Web Server
Email Server

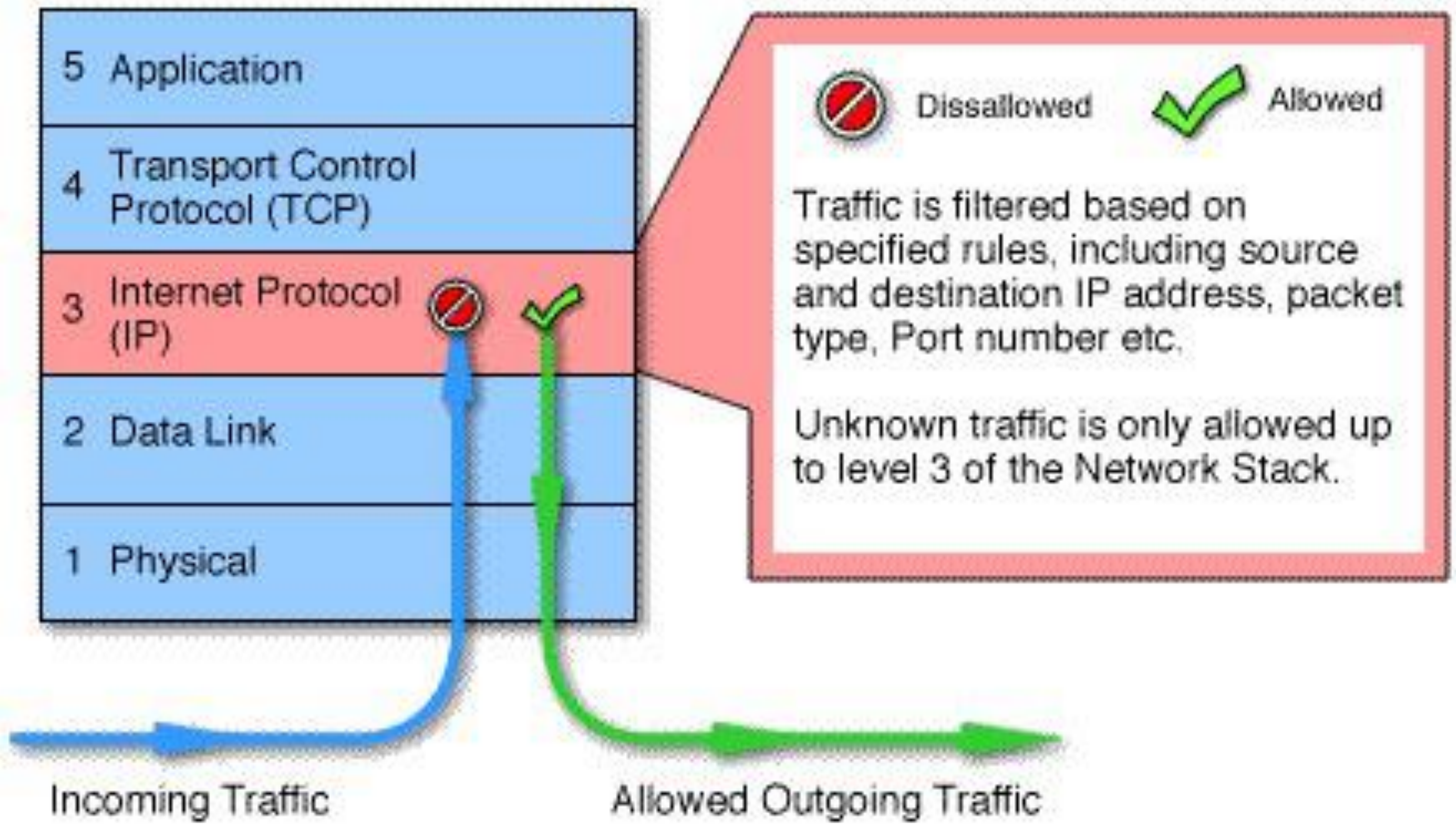
Types of Firewalls

- Firewalls fall into four broad categories
  - Packet filters
  - Circuit level
  - Application level
  - Stateful multilayer

Firewall - Packet Filters (1)

- Work at the network level of the OSI model
- Each packet is compared to a set of criteria before it is forwarded
- Packet filtering firewalls is low cost and low impact on network performance

Firewall - Packet Filters (2)



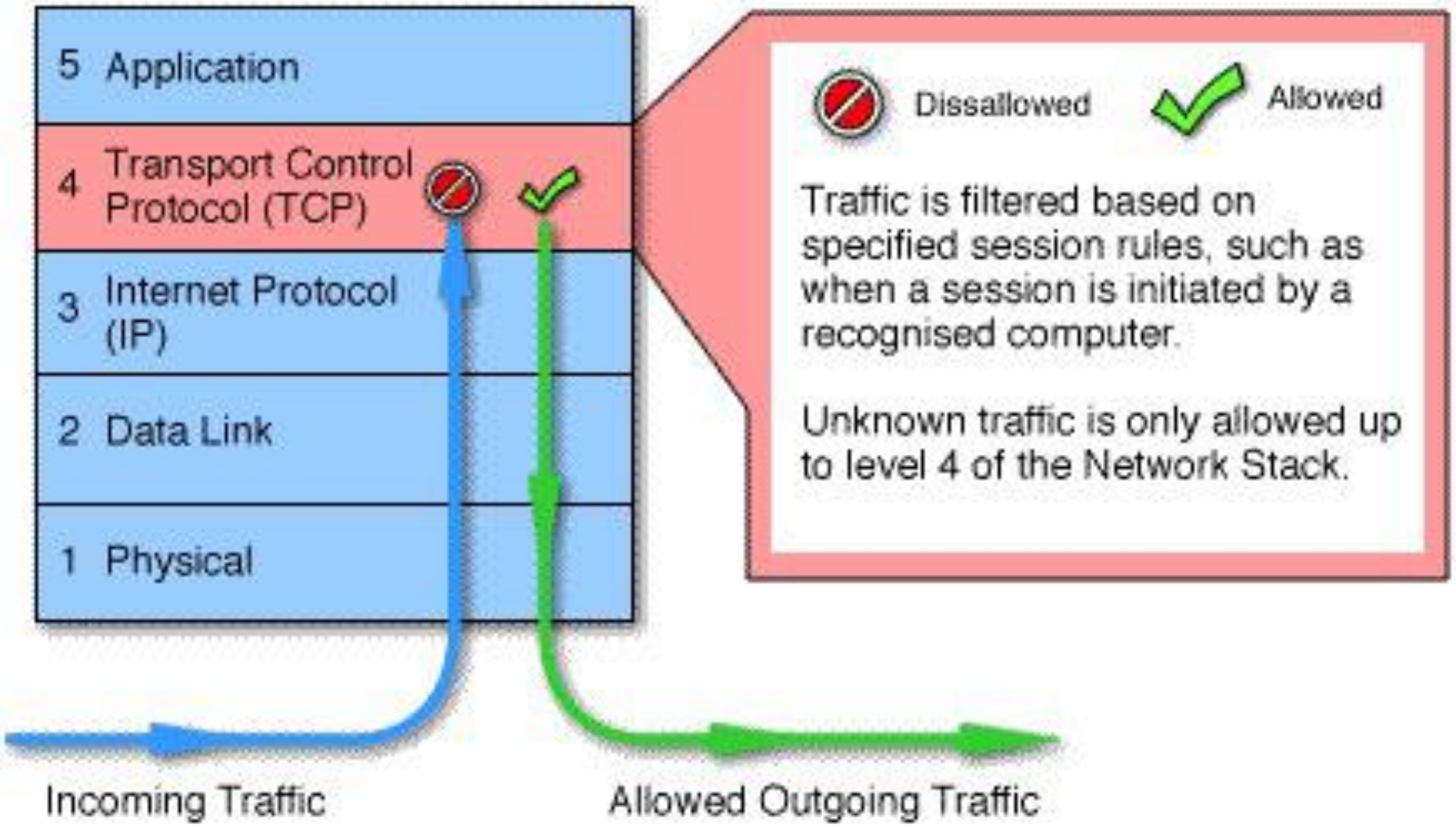
Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

Unknown traffic is only allowed up to level 3 of the Network Stack.

Firewall – Circuit Level(1)

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP
- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.

Firewall – Circuit Level(2)



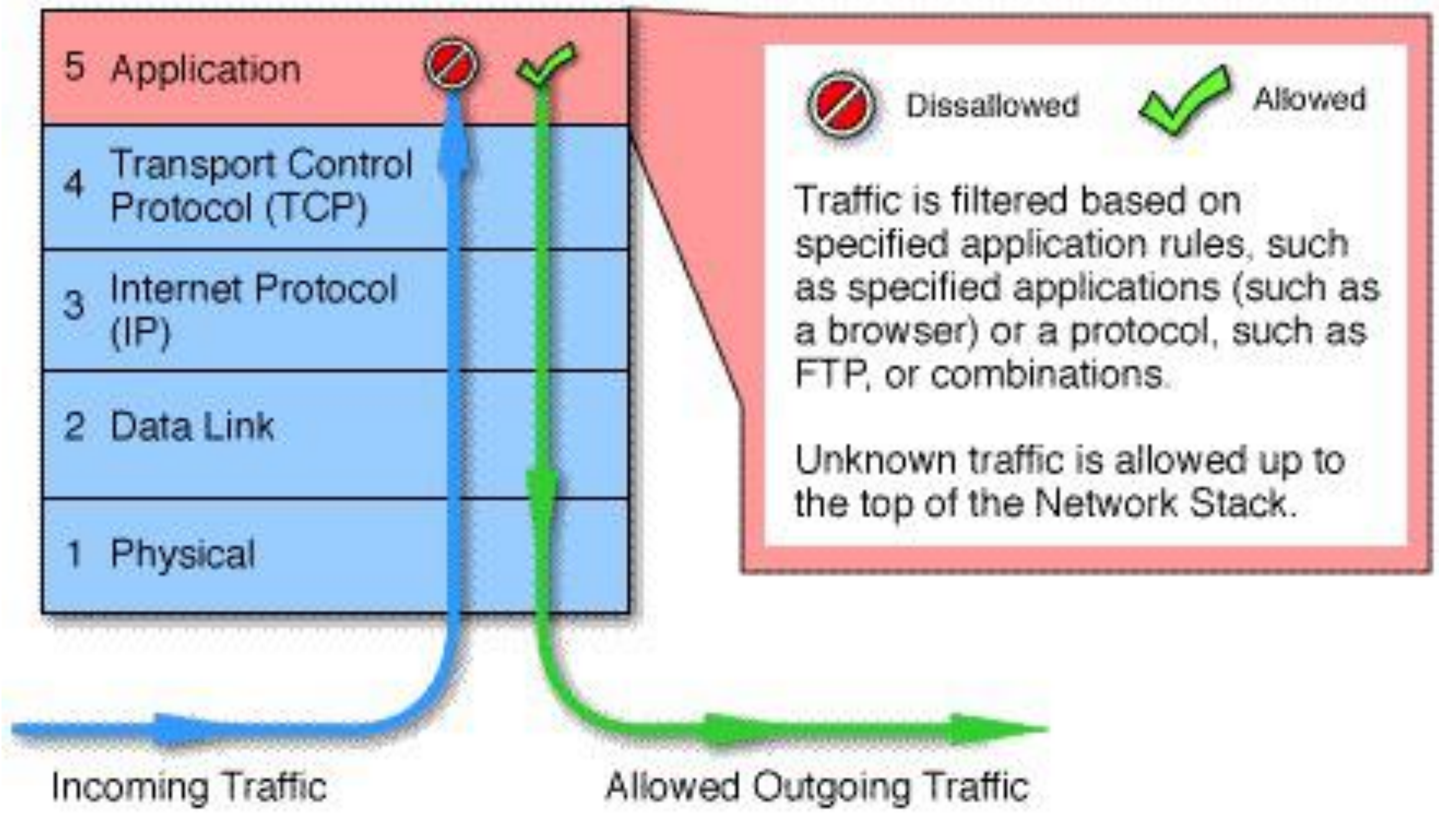
Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.

Unknown traffic is only allowed up to level 4 of the Network Stack.

Firewall – Application Level(1)

- Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific
- Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through

Firewall – Application Level(2)



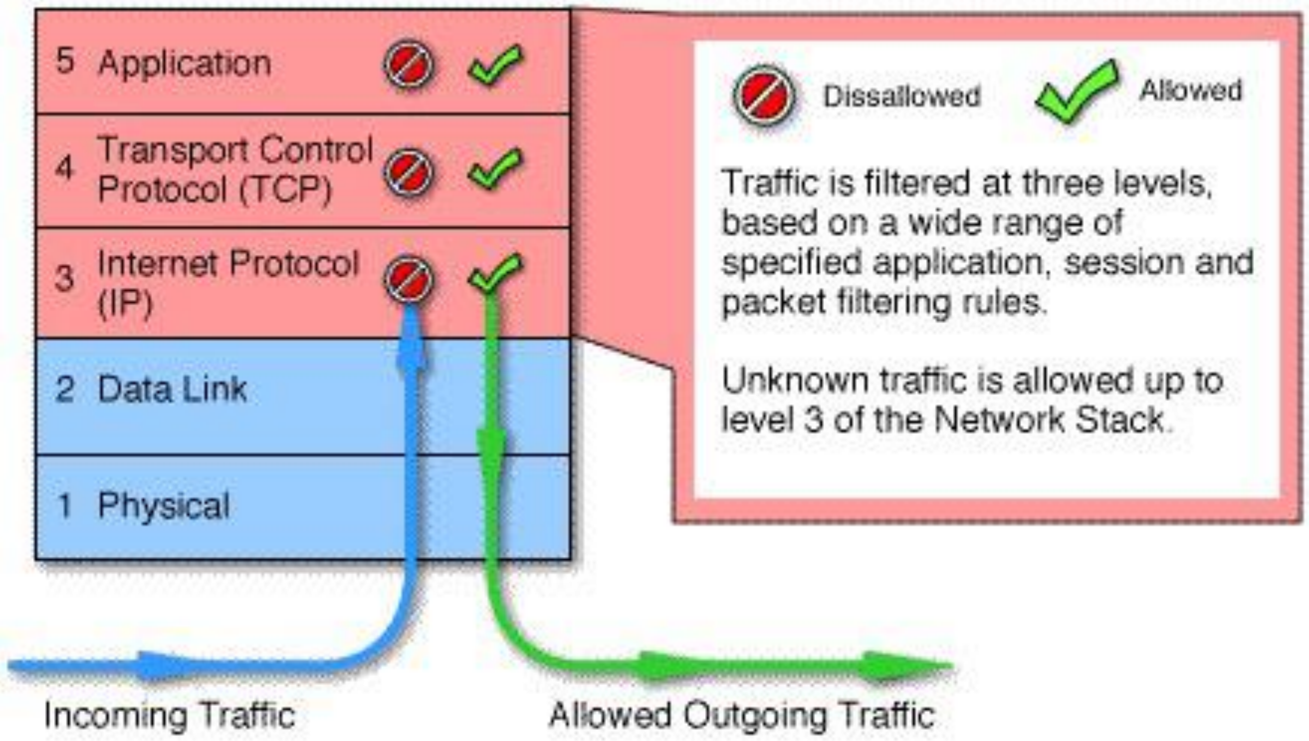
Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

Firewall – Stateful Multilayer (1)

- Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer

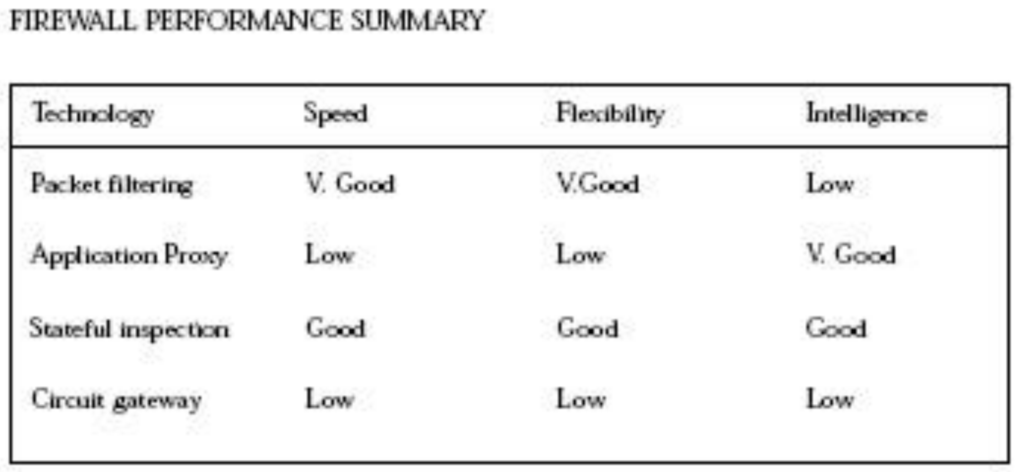
Firewall – Stateful Multilayer (2)



Traffic is filtered at three levels, based on a wide range of specified application, session and packet filtering rules.

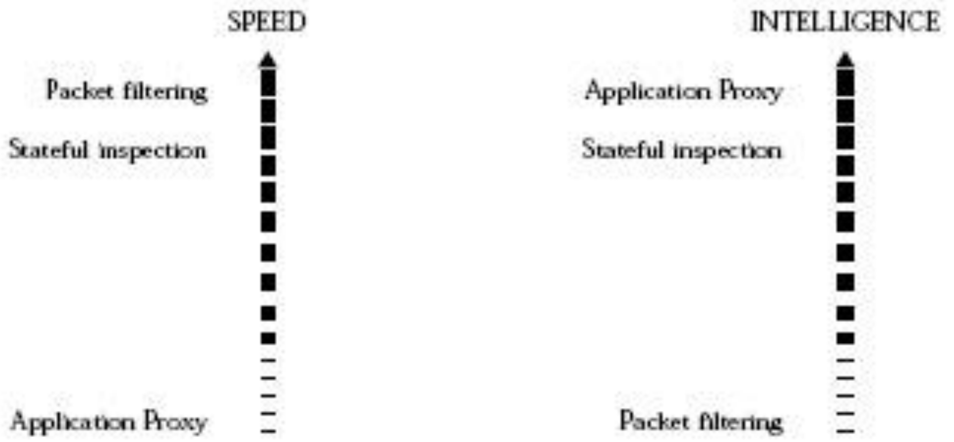
Unknown traffic is allowed up to level 3 of the Network Stack.

Firewall – General Performance

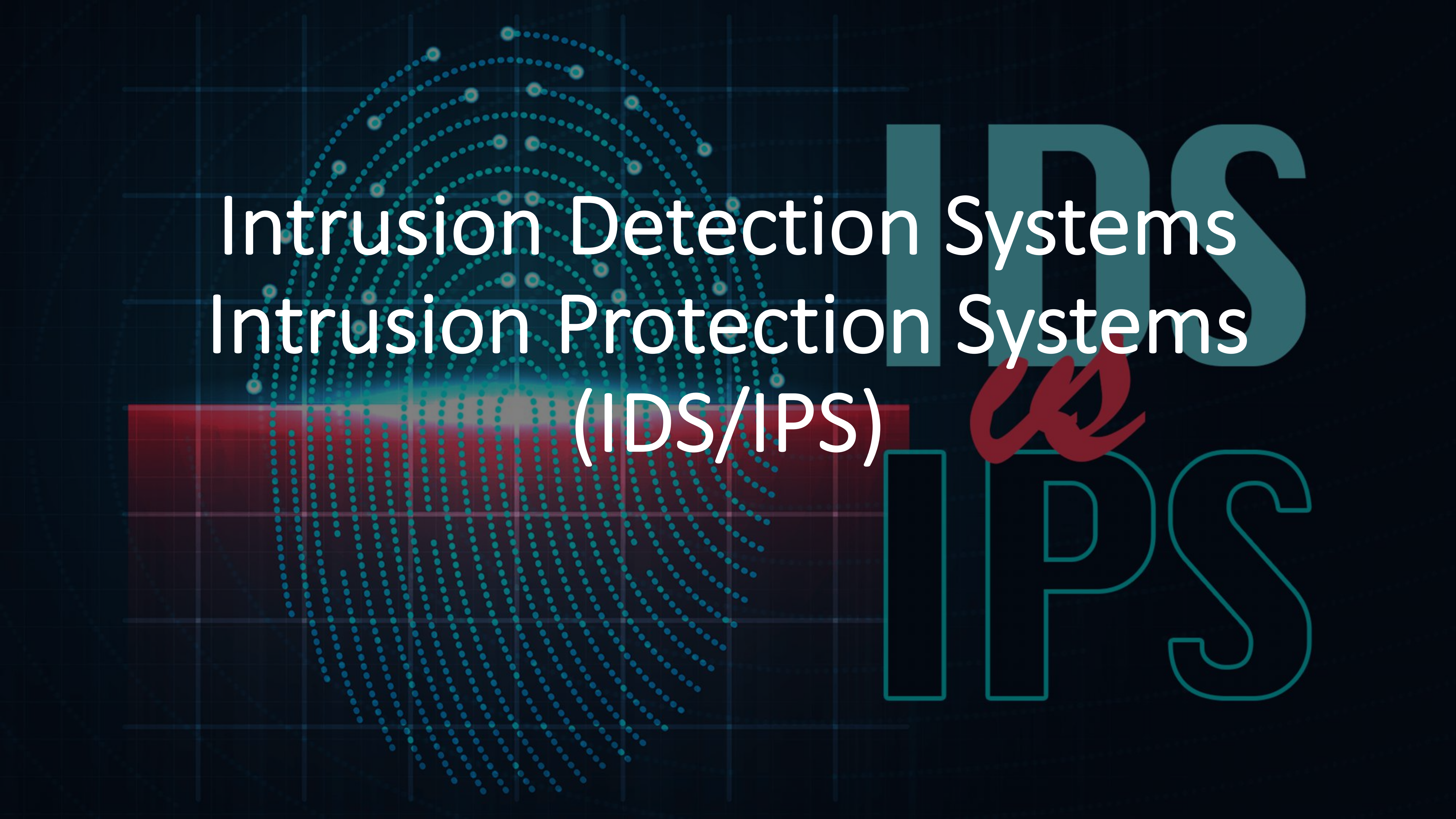


FIREWALL PERFORMANCE SUMMARY

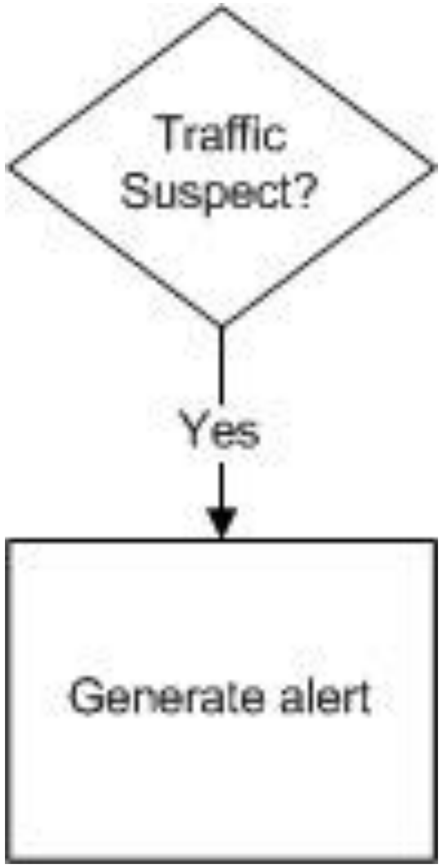
Technology	Speed	Flexibility	Intelligence
Packet filtering	V. Good	V.Good	Low
Application Proxy	Low	Low	V. Good
Stateful inspection	Good	Good	Good
Circuit gateway	Low	Low	Low

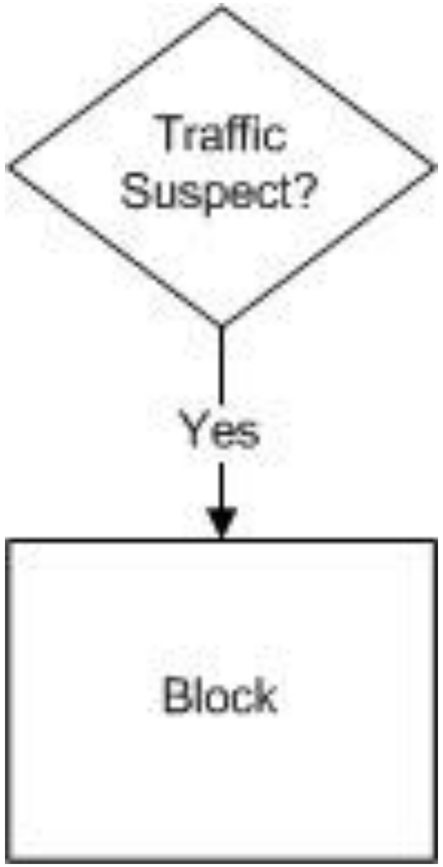


Intrusion Detection Systems
Intrusion Protection Systems
(IDS/IPS)



IDS vs IPS

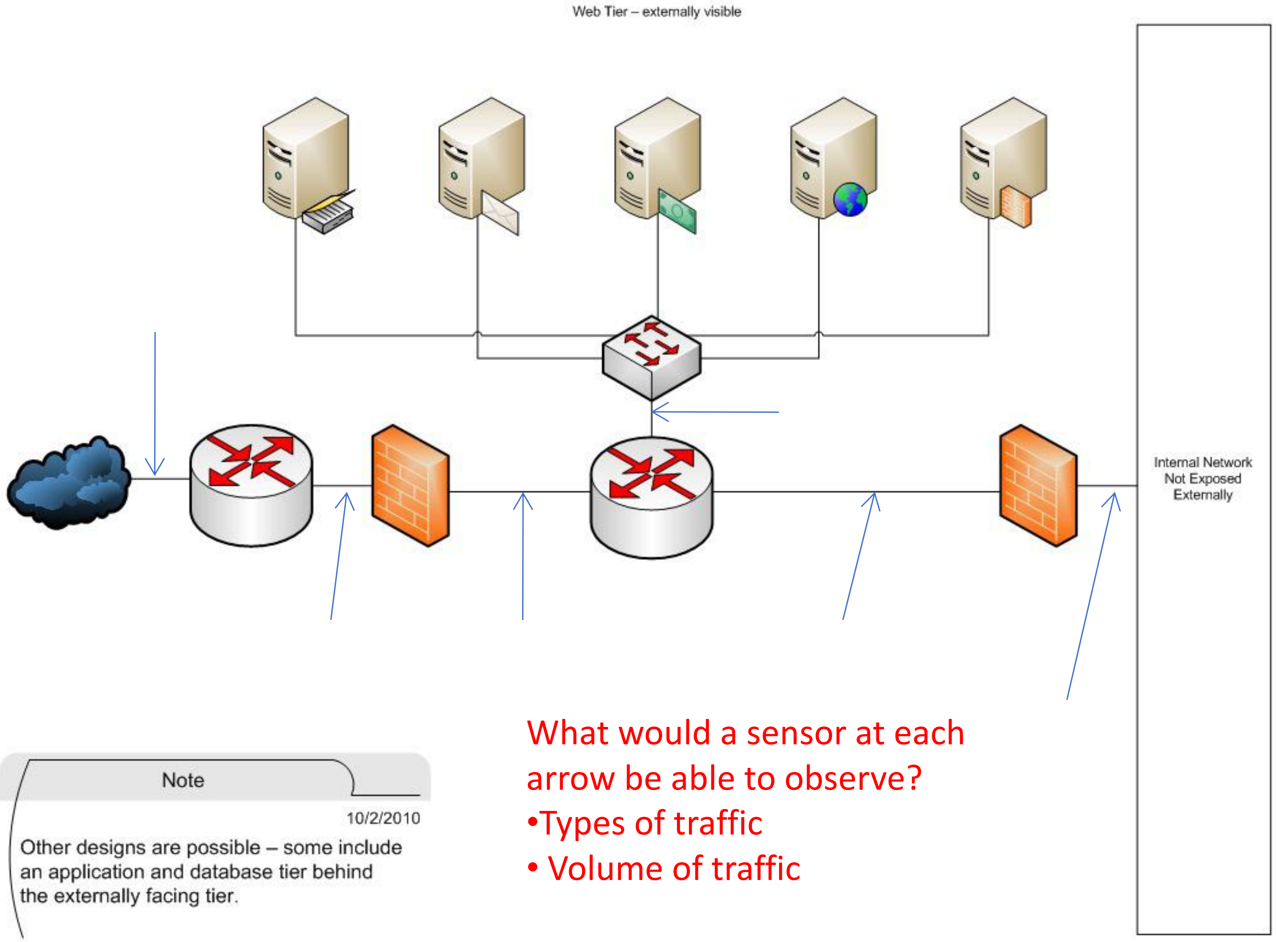

Traffic Suspect?
Yes
Generate alert


Traffic Suspect?
Yes
Block

Concept

- IDS/IPS can be a simple, monolithic system or a distributed set of sensors feeding a central analysis and correlation engine
- Critical to any design is placing the sensors so that they have appropriate visibility of the traffic to be monitored

Sensors Placement


Web Tier – externally visible
Internal Network Not Exposed Externally

Note

10/2/2010

Other designs are possible – some include an application and database tier behind the externally facing tier.

What would a sensor at each arrow be able to observe?

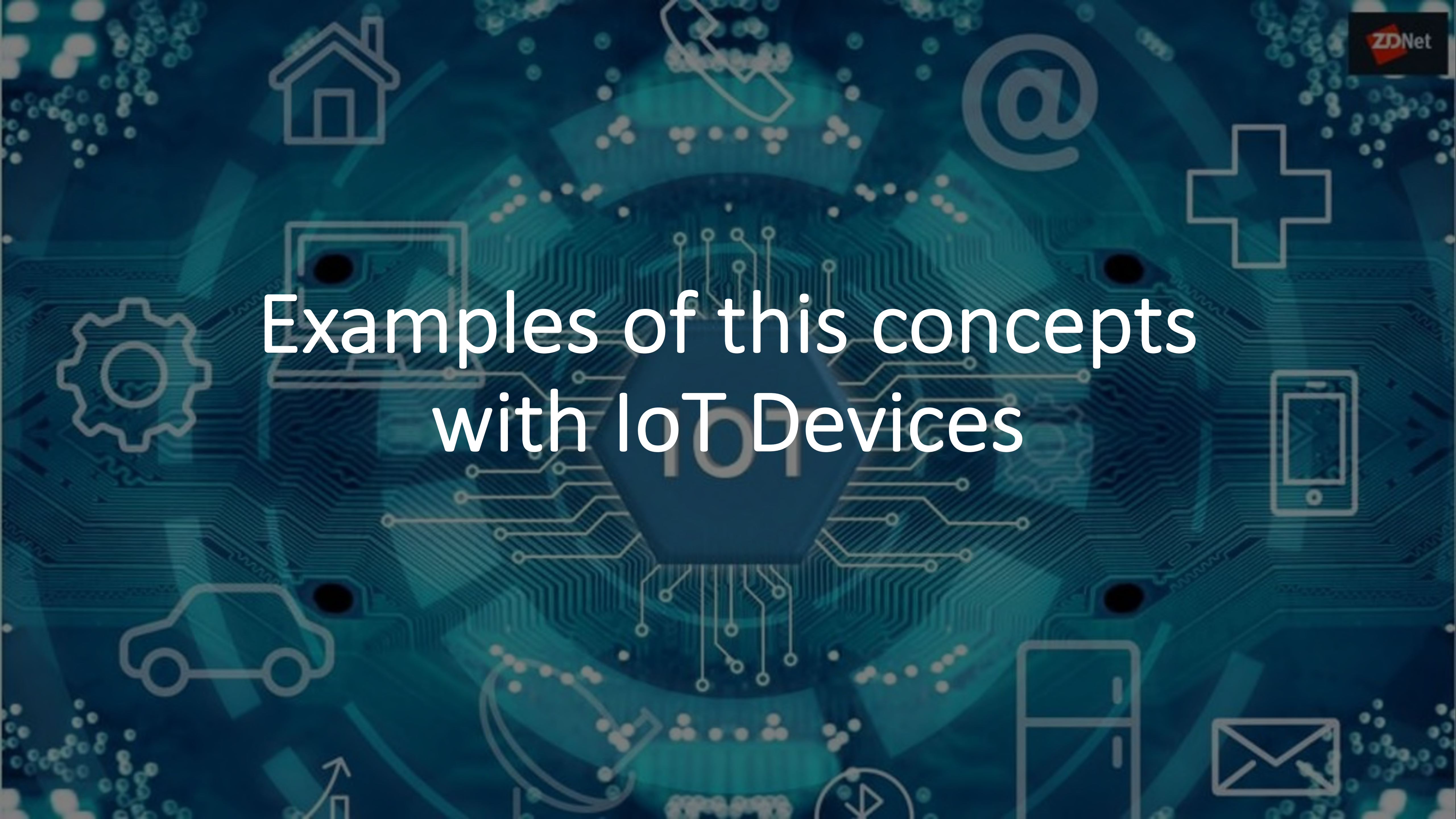
- Types of traffic
- Volume of traffic

Technologies

- Signature based (e.g., SNORT)
  - Pattern-matches traffic against known bad traffic
  - Weaknesses
    - Malicious traffic may morph
      - New XOR encoder
    - Traffic must be known before a signature can be written
- Anomaly based (e.g., BRO)
  - Compares traffic to “normal” baseline

Problems with IDS/IPS

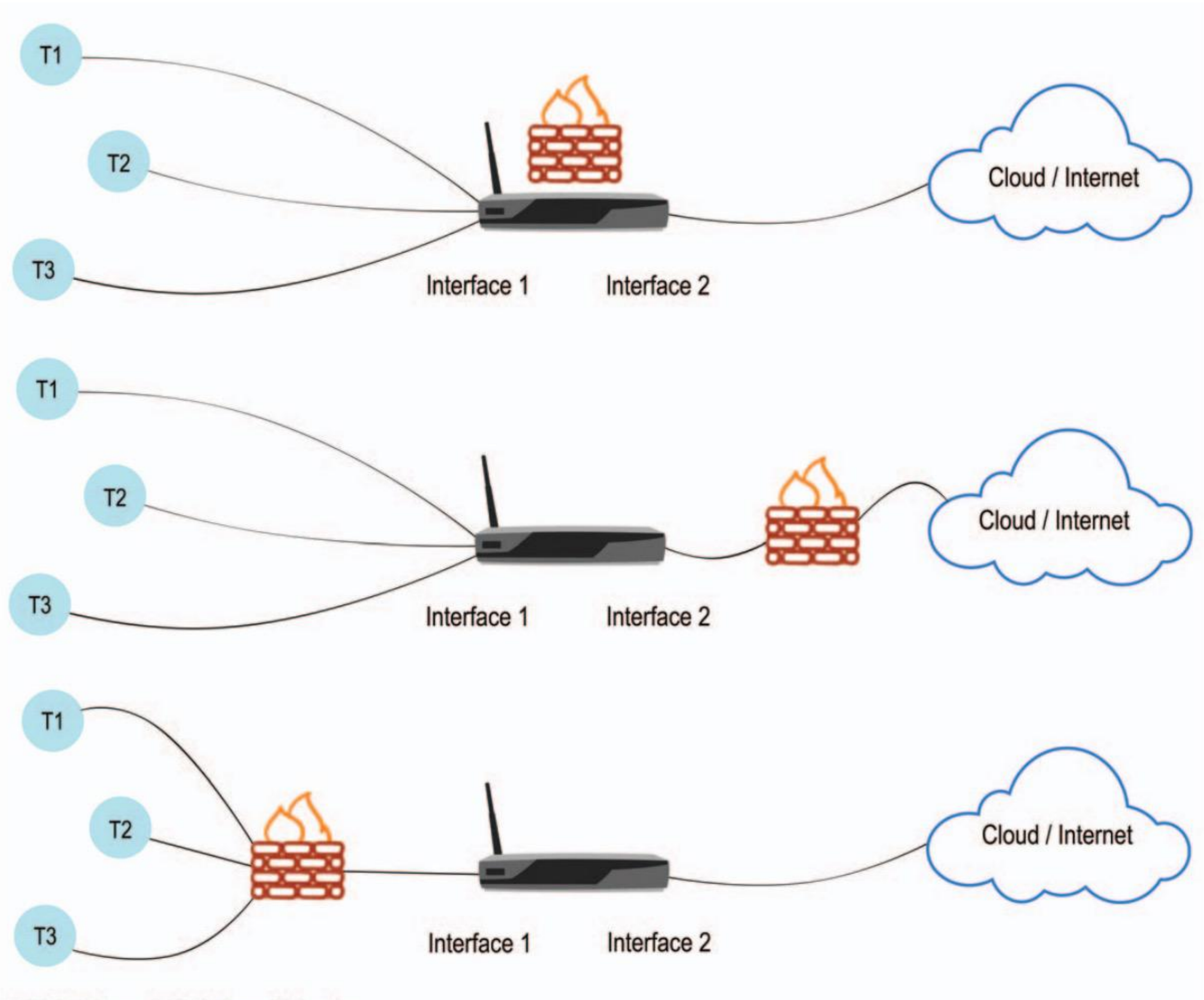
- False positives
  - Detecting malicious network traffic is difficult and for that reason rulesets tend toward the paranoid
  - This leads to the situation where normal traffic may be labeled as suspicious
    - telnet is a disallowed protocol within the DMZ
    - A hapless web server administrator uses telnet to connect to a server while troubleshooting a problem
- Triage, event correlation, etc are critical steps in any incident detection strategy



Examples of this concepts with IoT Devices

Firewalls for IoT

- Firewalls can help to isolate IoT devices to protect them to send private data to the Cloud or Internet



T1, T2, T3 are IoT devices (things)

IDS for IoT

- There are many research works on designing an effective IDS for IoT

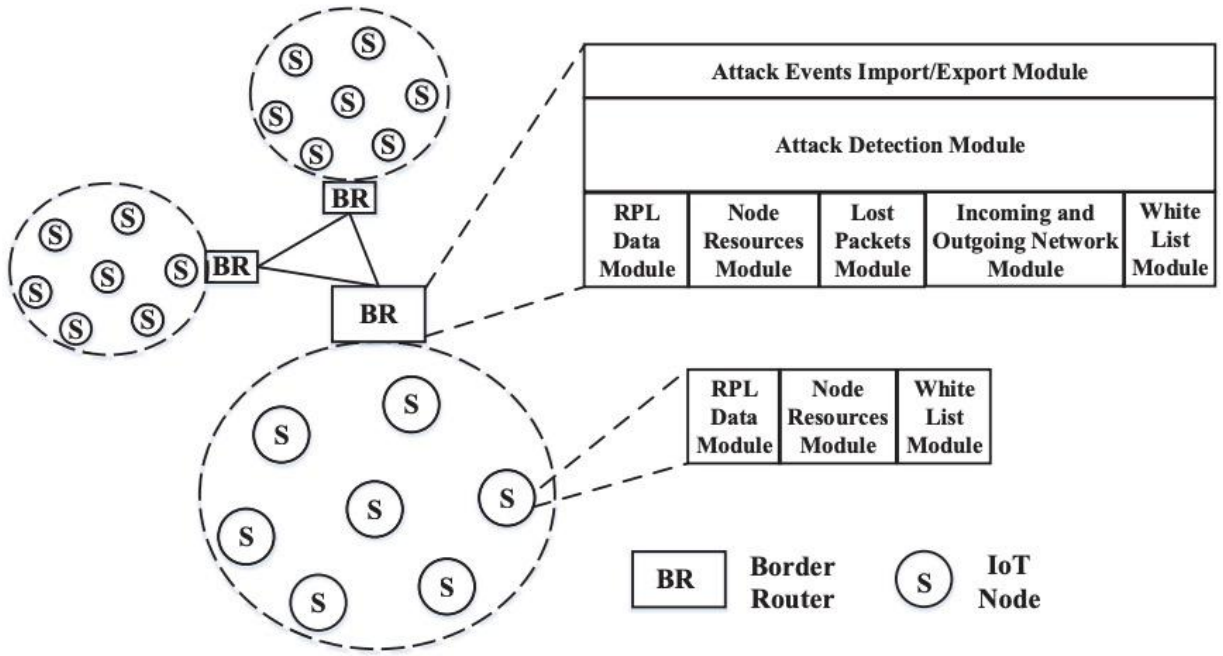


Figure 1. Proposed IDS Block Diagram.