

Security Configuration Parameters

Christopher Rees

<https://www.linkedin.com/in/cdrees>

@cdrees



pluralsight 
hardcore dev and IT training

Domain 1.0 - Security Configuration Parameters

- What we'll cover in this course

- Firewalls
- Routers
- Switches
- Load Balancers
- Proxies
- Web Security Gateways



Domain 1.0 - Security Configuration Parameters

- **Topics covered (continued)**
 - NIDS and NIPS
 - Network Intrusion Detection Systems
 - Network Intrusion Prevention Systems
 - Protocol Analyzers
 - Spam Filters
 - UTM Security Appliances
 - URL Filters
 - Content Inspection
 - Malware Inspection
 - Web Application Firewall vs. Network Firewall

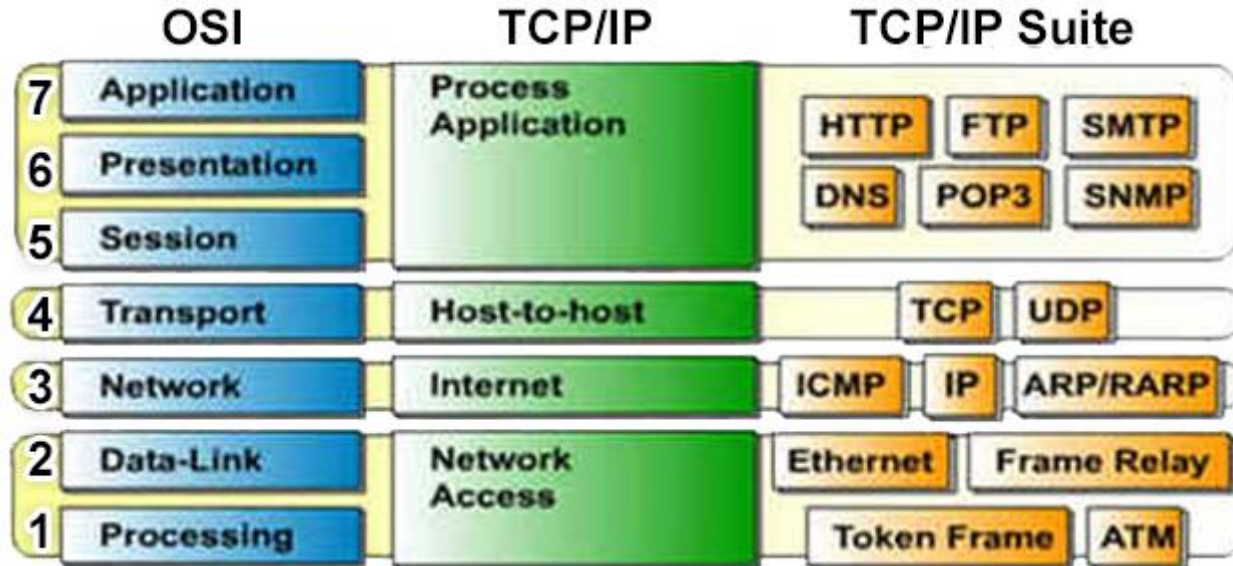


Before We Begin...

- **Why the Need for a Secure Network?**
 - Hackers
 - Identity and Data Theft
 - Espionage
 - Destruction of revenue / reputation / consumer confidence
- **Pre-requisite Knowledge**
 - TCP/IP Protocol Suite
 - OSI Model and Relevance
 - Review Network+ Course for more information

TCP/IP and OSI Models

- Reference models designed to illustrate and standardize communication protocols, methods and devices



Firewalls

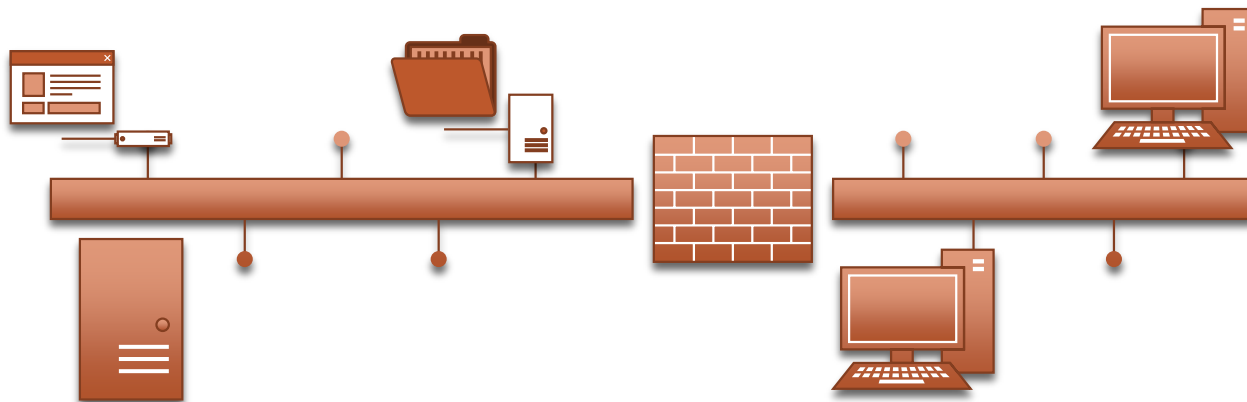
- **What's the purpose?**

- To isolate one network from another
- Can be hardware or software based
 - Standalone devices or integrated into other equipment (i.e. routers or switches)



Firewalls

- **Typically used to block or limit outside traffic from entering a network**
 - Corporate
 - Home
- **Can be placed internally to segment one area from another**
 - PCI Secure zone
 - Accounting & Finance
 - R&D



Important!

Hardware vs. Software

Firewalls can be Hardware or Software based
Standalone devices or integrated into other
devices like routers or switches

Hardware contains Software/Firmware
Even standalone devices contain software
and firmware

Types of Firewalls

- **Packet Filtering**

- Allow or Block traffic based on Port (i.e. HTTP on port 80 or FTP or port 21)
- No intelligence but easy to set up

- **Proxy Firewall**

- Dual-homed firewall
- Segments internal users from outside world
 - Masks IP address using NAT (Network Address Translation)
- Cache requests to improve perceived speed

Types of Firewalls

- **Stateful Packet Inspection Firewalls**

- Examines packet and keeps packet table of every communication channel
- SPI tracks the entire conversation
 - Only packets from known active connections are allowed
- Better than simple packet filtering, which only looks at current packet
- Possible to attack by overloading the State Table

History Lesson: Check Point Software introduced stateful inspection in the use of its FireWall-1 in 1994

Web Application Firewall

- **Web Application Firewall**

- Operates at the Application Layer of the OSI model (Layer 7)
- Designed with granular rules specifically to analyze traffic to web servers and prevent typical attacks
 - SQL Injection attacks
 - XSS (Cross-site-scripting)
 - Forged HTTP requests

- **Well known WAF vendors**

- Cisco
- Citrix
- Barracuda
- F5
- eEye

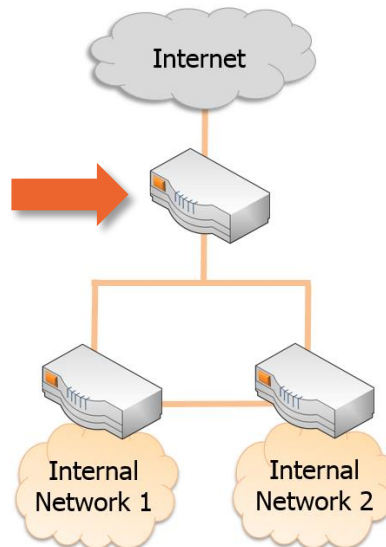
Firewall Examples



Routers

- **Routers connect different networks together and “route” traffic between them**
 - Have two or more network connections which have valid IP addresses on each network
 - Decide whether to keep traffic local or route to remote network based on source and destination address
- **Can Provide Firewall Functionality**

Firewall to block unwanted traffic and connect internal network to the Internet



Routers

- **Configured as Static or Dynamic**
 - Static routes must be programmed manually
 - Dynamic routes are learned as routers communicate with each other

- **Common Routing Protocols**
 - RIP (Routing Information Protocol)
 - OSPF (Open Shortest Path First)
 - EIGRP (Enhanced Interior Gateway Routing Protocol)
 - BGP (Border Gateway Protocol)



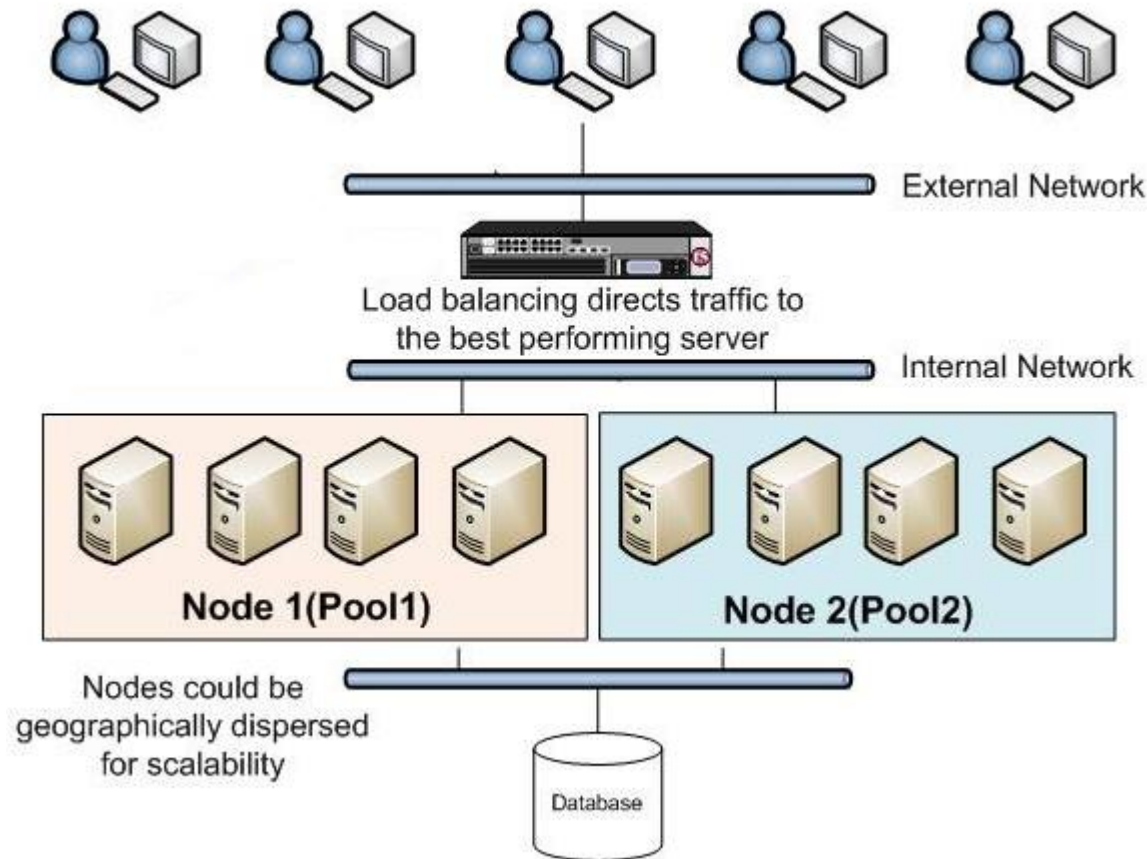
Switches

- **Multiport connectivity devices that improve network efficiency**
 - Maintain tables of MAC addresses and only send communication out the necessary port
 - Used on internal networks and don't provide routing functionality
 - Exceptions are layer 3 switches which can provide routing functionality internally



Load Balancers

- **Load Balancers dynamically balance the load between devices**
 - Typically servers but could be other devices as well
 - Could be hardware or software based



Web Security Gateways

- **Proxy Server with advanced features**
 - Virus Scanning
 - Prevent connections to inappropriate sites such as P2P or file-sharing sites like Dropbox, Box.net, etc
 - Data Loss Prevention (DLP)
- **Can block things like ActiveX controls, Java applets, 3rd party cookies**
- **Enable granular access to websites**
 - Allow access to LinkedIn but not allow job searches
 - Allow access to Facebook but prohibit posting content or playing games

VPN and VPN Concentrators

- **Virtual Private Network (VPN)**

- Creates a private network across a public network
- Tunneling protocol such as:
 - L2TP (Layer 2 Tunneling Protocol)
 - PPTP (Point to Point Tunneling Protocol)
 - IPSec (IP Security)
- Security comes from tunneling protocol (i.e. PPTP) and encryption method (i.e. IPSec)

- **Many VPNs use two-factor authentication**

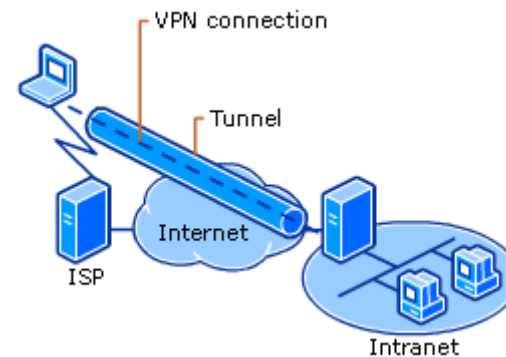
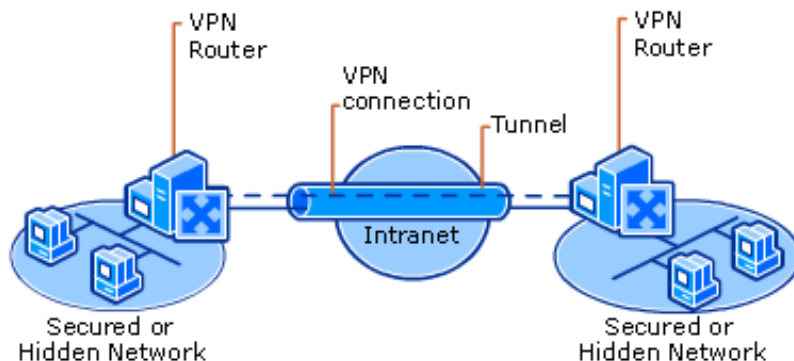
- RSA Hardware or Software Token



VPN

- Many companies provide VPN access to their remote employees
- Access corporate resources from offsite location
 - Access can be restricted to only certain parts of the corporate network

VPN between two corporate networks



VPN between remote user and office

Intrusion Detection and Prevention

- **NIDS and NIPS**
 - Network Intrusion Detection System (NIDS)
 - Network Intrusion Prevention System (NIPS)

- **Can be used to log, alert and/or take action when suspicious activity occurs on the network**
 - Active and Passive systems
 - Active systems can take action to prevent an attack or suspicious activity
 - Passive systems record activity for later analysis

IDS vs. IPS

- **IDS – Intrusion Detection System**

- Been around for quite awhile, fairly common and easier to set up. Logs alerts and events
- Allows for reactive response / research

- **IPS – Intrusion Prevention System**

- Newer platform over the last few years
- Enables prevention (such as blocking IP address, etc)
- False positives could block legitimate traffic

NIPS and NIDS Components

- **Alert**

- Message generated from the **analyzer** indicating an “interesting” event has occurred

- **Analyzer**

- Processes data collected from one or more **sensors** and looks for suspicious activity (deterministic or rule-based)

- **Data Source**

- Raw data being analyzed – log files, audit logs, system logs, network traffic, etc

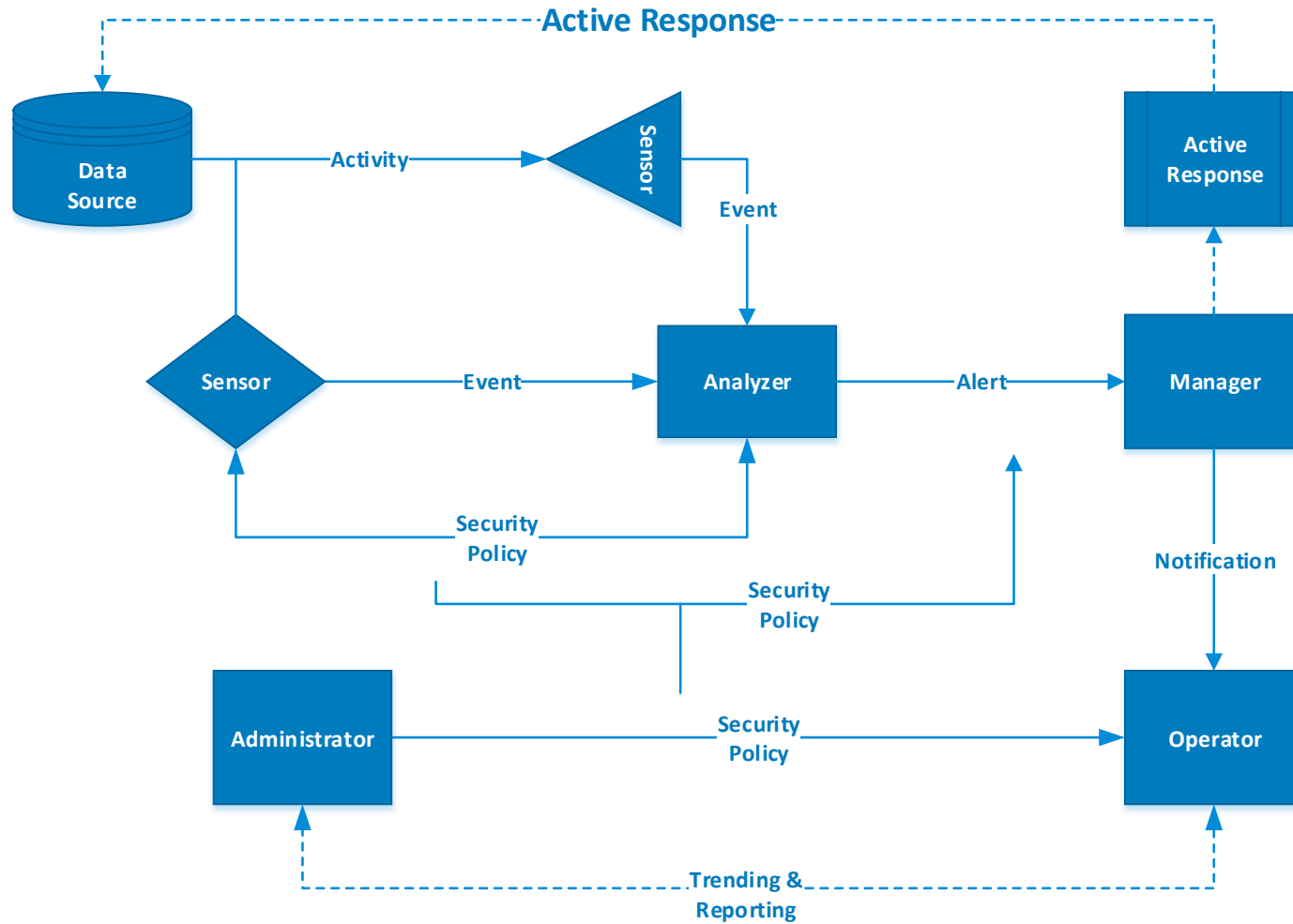
- **Event**

- Indication that suspicious activity may have occurred (can trigger an Alert or notification). If confirmed, **Event** becomes an “**Incident**”

NIPS and NIDS Components

- **Manager**
 - Intrusion Detection System (IDS) console – used to manage the system
- **Notification**
 - Process by which the operator is alerted to an Event or Incident
- **Operator**
 - User, Admin, etc., responsible for the IDS
- **Sensor**
 - Primary data collection point for the IDS
 - Device driver on a system or a separate physical device attached to the network to collect data

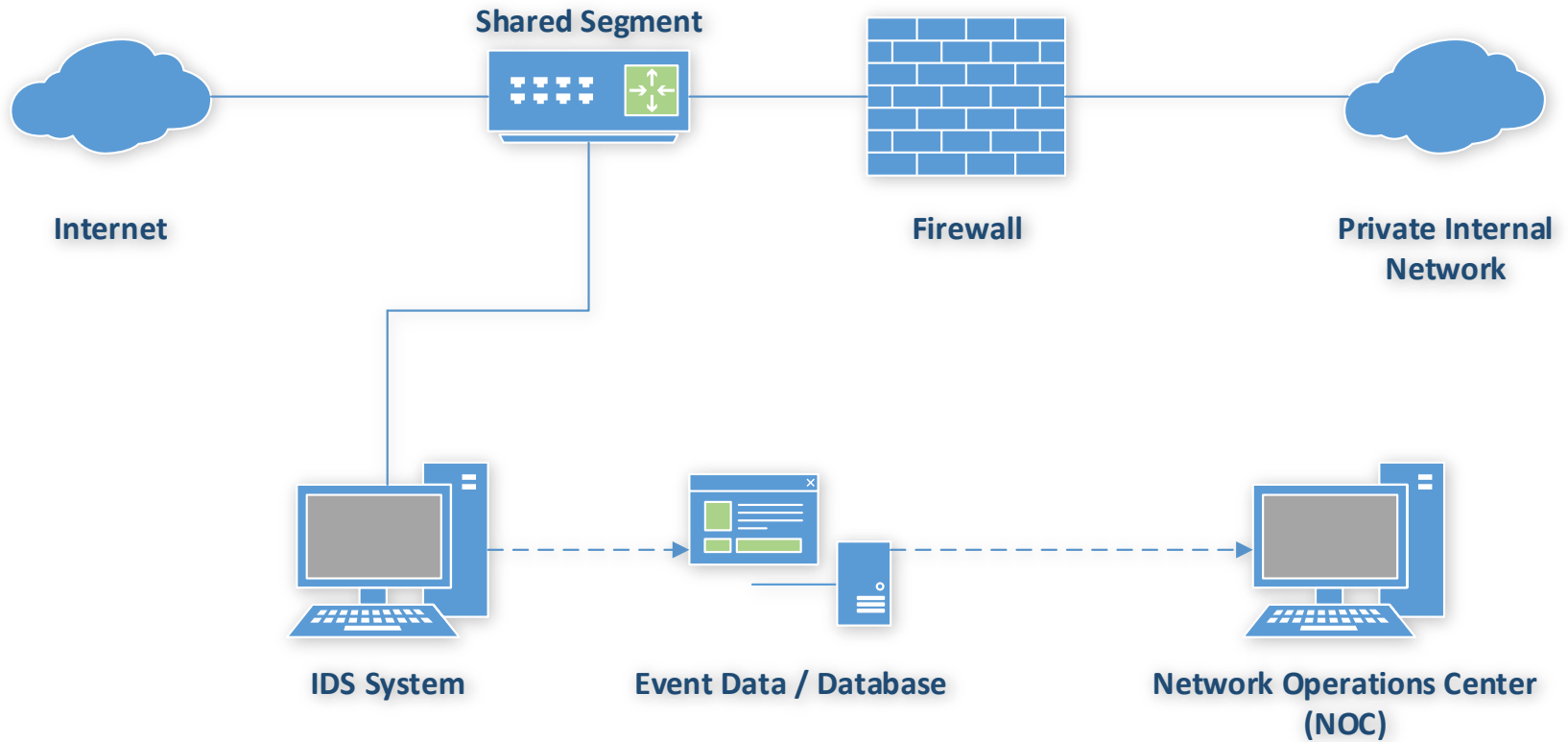
IDS Component Workflow



Four Approaches to IDS

- **Behavior Based Detection IDS**
 - Variations in behavior, increased traffic, policy violations, etc
- **Signature Based Detection IDS**
 - Uses attack signatures and audit trails
- **Anomaly Detection IDS**
 - Learns what is “normal” then looks for deviations from the baseline
- **Heuristic IDS**
 - Utilizes algorithms to analyze traffic as it passes through

Network Based IDS



Reacting to Alerts/Issues

- **Passive Response**

- Logging the issue for later analysis
- Notifying admin or kick off some type of workflow
- Shunning or ignoring the attack (i.e. attacker could be targeting a service that doesn't exist)

- **Active Response**

- Issues some type of action
 - Block ports
 - Reset connections
 - Configuration changes

- **Deception**

- Honey Pots

Intrusion Detection Systems

- Snort (www.snort.org)
 - Most popular IDS
 - Open source
 - Runs on various Linux distros and Windows
 - Real time monitoring / protocol analyzer / sniffer



SPAM Filters

- SPAM is a **MAJOR** issue that everyone is familiar with! 😞
 - 90% of all email is reported to be spam content
- SPAM filters use rules or heuristics to detect if email is bogus based on header, content or IP address / IP block
- SPAM filters can be located at the enterprise/company level as well as individual computers
 - SPAM Assassin
 - Postini (end of life 2013)
 - Barracuda
 - Microsoft, Symantec, Trend Micro, McAfee



UTM and URL Filters

- **Unified Threat Management (UTM)**
 - All-in-one security appliances
 - Contain Anti-Virus (AV), IDS, Content/URL Filtering, Malware Detection
 - Also referred to as **Next Gen Firewalls (NGFW)**

- **URL Filters**
 - Block websites based on URL or partial URL match
 - Included in some web browsers
 - Can detect / prevent **PHISHING**
 - Phishing filter has been replaced with Smart Screen Filter (IE)

Phishing Example

- Email that appears to be from a legitimate source, asking for your personal information or credentials
 - Usually don't contain your actual name (i.e. Dear Customer)
 - Hovering over the links reveal bogus URLs

From: "Apple Customer Service" <secure@appleid.co.uk>
Subject: Your Apple ID Requires Validation [#487334]
Date: July 8, 2014 at 7:42:43 PM EDT



Dear Customer,

We recently failed to validate your account information we hold on record for you, therefore we need to ask you to complete a brief validation process in order to verify your account.

[Click here to verify your account](#)

Failure to complete our validation process will result in a suspension of your Apple ID.

We take every step needed to automatically validate our users, unfortunately in this case we were unable to verify your details. The process will only take a couple of minutes and will allow us to maintain our high standard of account security.

Wondering why you got this email?

This email was sent automatically during routine security checks. We are not

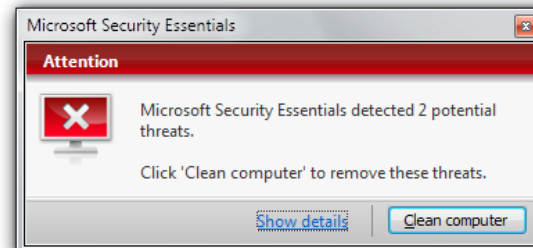
Content Inspection and Malware Detection

■ Content Inspection

- Content filtering available in some browsers that inspect the content and can block it; rather than looking at the URL (which might not be identified as malicious if it's a new threat)

■ Malware Detection

- Best defense is to **NOT GET INFECTED**
- Malware can be very difficult to disinfect
 - Often downloads other malicious programs once infected
- Malware detection software
 - Microsoft Security Essentials / Defender
 - Malwarebytes



Application Aware Devices

- **Device that can respond to traffic based on what is there**
 - Typically combines SNMP and Quality of Service (QoS)
 - Prioritizes traffic based on importance of content
- **Can be added to other devices**
 - Firewalls
 - IPS/IDS
 - Proxies, etc

Network Security Summary

- **Components**

- Firewalls, Routers, Switches
- Load Balancers and Proxies

- **Tools**

- IDS and IPS systems
- SPAM Filters
- Content Inspection / URL Filtering
- UTM Appliances