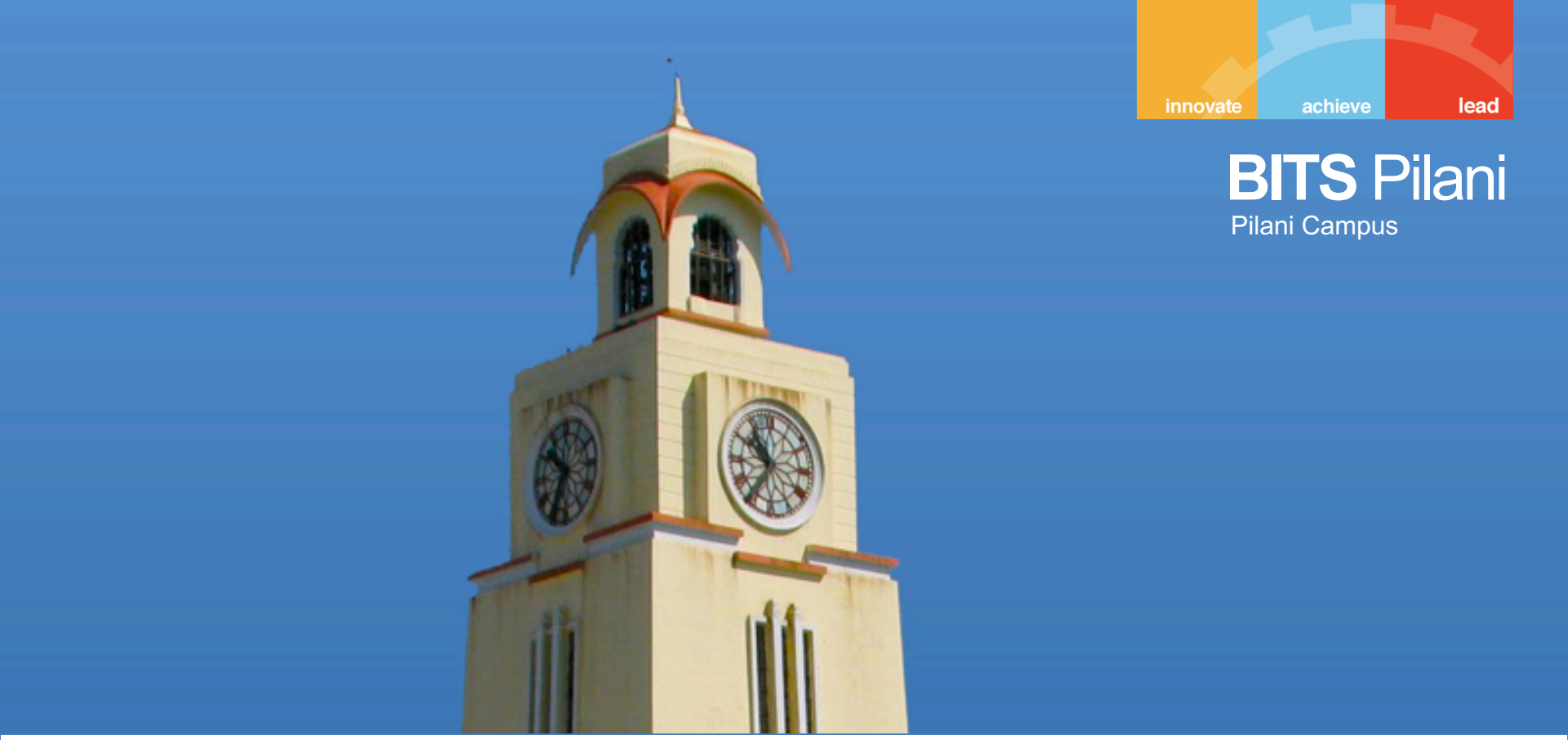
BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP



innovate achieve lead

BITS Pilani
Pilani Campus

SSZG681: Cyber Security
Lecture No: 06

Strategic Defenses

Agenda

- Intrusion Evasion Techniques
- Intrusion Detection Systems (IDS)
  - Overview and types of IDS
  - Methods used by IDS
  - IDS benefits
  - IDS strengths and limitations
  - IDS products
- Intrusion Prevention Systems (IPS)
  - Overview and working of IPS
  - Methods used by IPS
  - Preventive actions by IPS
  - IPS products
  - IDS v/s IPS
  - Firewall v/s IDS v/s IPS

Intrusion Evasion Techniques

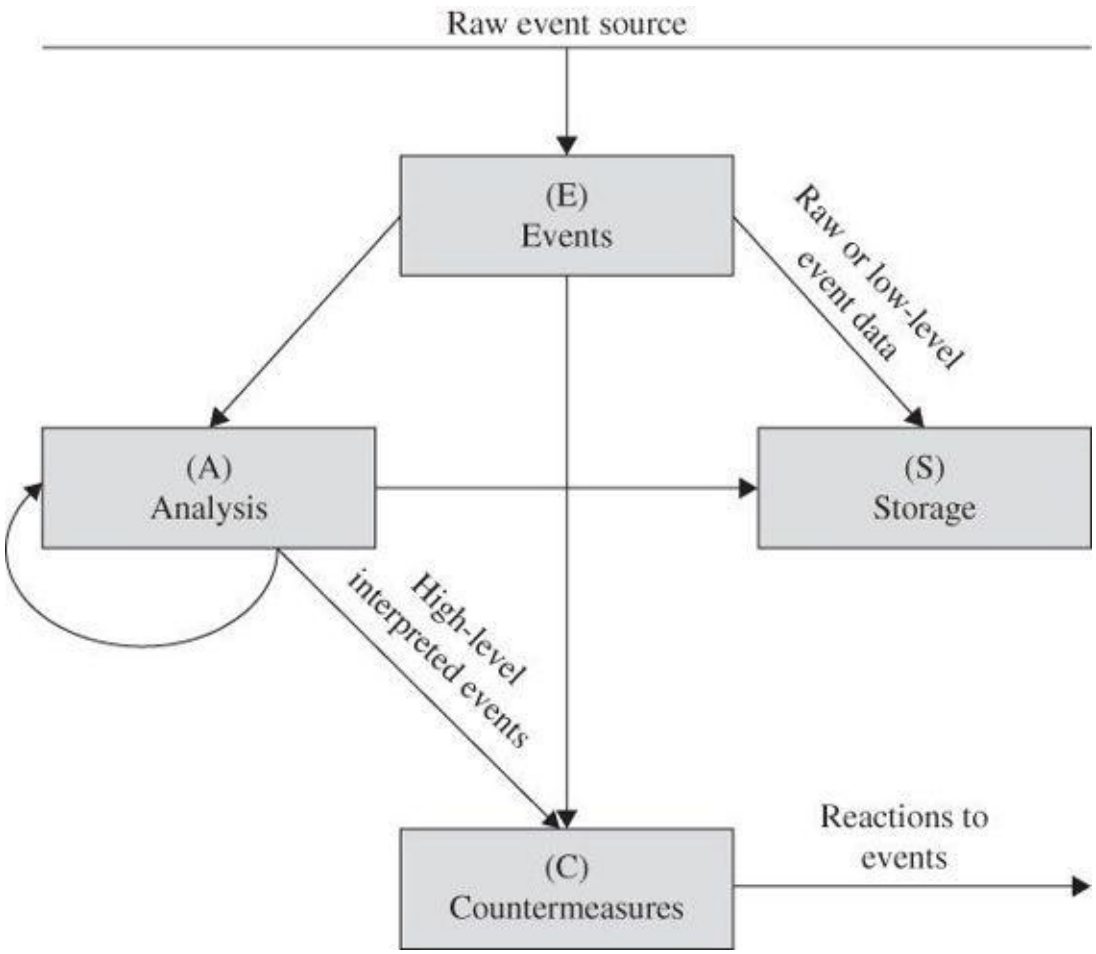
- **Fragmentation:** Sending fragmented packets allows an attacker to stay under the radar, bypassing the detection system's ability to detect the attack signature.
- **Avoiding defaults:** A port utilized by a protocol does not always provide an indication to the protocol that's being transported. If an attacker had reconfigured it to use a different port, the IDS may not be able to detect the presence of a trojan.
- **Coordinated, low-bandwidth attacks:** coordinating a scan among numerous attackers, or even allocating various ports or hosts to different attackers. This makes it difficult for the IDS to correlate the captured packets and deduce that a network scan is in progress.
- **Address spoofing/proxying:** attackers can obscure the source of the attack by using poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server, it makes it very difficult to detect.
- **Pattern change evasion:** IDS rely on pattern matching to detect attacks. By making slight adjust to the attack architecture, detection can be avoided.

Intrusion Detection System (IDS)

What is an IDS?

- Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered
- IDS is like a smoke detector that raises alarm if specific events occur
- IDS response may be:
  - **Manual:** raise alarm for someone to take action
  - **Automate:** get into protection mode to isolate the intruder (IPS)

How does IDS Work?



- Raw inputs from sensors
- Data storage of raw inputs
- Analysis of events
- Intrusion identification
- Countermeasure plan
- Response to events

What are IDS Functions?

- Monitor the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyberattacks
- Help administrators to tune, organize and understand relevant operating system audit trails and other logs that are often otherwise difficult to track or parse
- Assess integrity of critical system files for vulnerabilities and misconfiguration
- Provide a user-friendly interface so non-expert staff members can assist with managing system security
- Build and maintain an extensive attack signature database against which information from the system can be matched
- Recognize and report when data files have been altered

What are IDS Functions?...

- Manage audit trails and highlighting user violation of policy or normal activity
- Correct system configuration errors
- Install and operate traps to record information about intruders
- Generate an alarm and notify when security has been breached
- React to intruders by blocking them or blocking the server

Goals for IDS

An IDS should be simple, fast and accurate

- Filter on packet headers
- Filter on packet contents
- Filter in real time (on-line) mode
- Maintain connection state
- Use complex, multipacket signatures
- Use minimal number of signatures with maximum effect
- Hide it's presence
- Use optimal sliding-time window size to match signatures

IDS Types

- **Host based:** Runs on a single host to protect that particular host
- **Network based:** A separate device attached to a network to monitor traffic thru that network

Host Based IDS (HIDS)

- Examines events on a computer in a network rather than the traffic that passes around the system.
- Mainly operates by looking at data in admin files including log and config files on the computer that it protects.
- HIDS will back up the config files so system can restore settings, should a malevolent virus loosen the security of the system by changing the setup of the computer.
- Another key element that it guards is a root access on Unix-like platforms or registry alterations on Windows systems. **A HIDS won't be able to block these changes, but it would be able to raise alert if any such access occurs**.
- HIDS must be installed on each host it is expected to monitor for effective monitoring of overall network.
- This ensures that config changes on any of the host are not overlooked.
- A **distributed HIDS system needs to include a centralized control module**.

Network Based IDS (NIDS)

- NIDS examines the traffic on the network. A typical **NIDS** includes a packet sniffer in order to gather network traffic for analysis.
- The analysis engine of a NIDS is rule-based which supports addition, deletion and modification of rules.
- With many NIDS, the provider of the system, or the user community make rules available which can be imported into system for implementation.
- **There is no need to dump all of the traffic into files or run the whole lot through a dashboard** because it wouldn't be able to analyze all of that data.
- Rules that drive analysis in a NIDS also create selective data capture. For example, if there is a rule for a type of worrisome HTTP traffic, NIDS should only pick up and store HTTP packets that display those characteristics.
- Typically, a NIDS is installed on a dedicated piece of hardware. A NIDS requires a sensor module to pick up traffic, so it should be possible to load it onto a LAN analyzer, or may choose to allocate a computer to run the task.

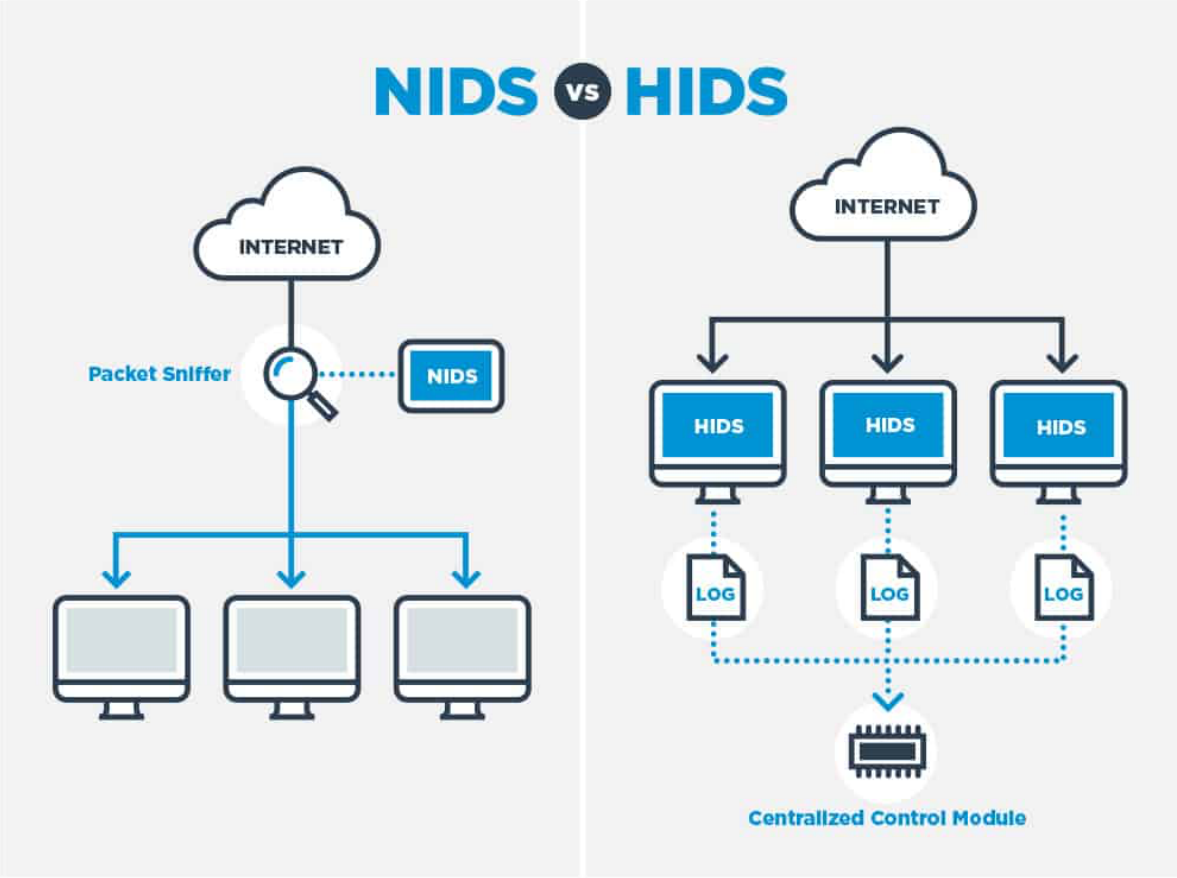
Front-End IDS

- Placed at entry point of a network
- Monitors traffic coming to network
- Can analyze the traffic and initiate action against suspicious traffic
- Visible to outside world and is exposed to attack
- Can not monitor internal traffic

Internal IDS

- Monitors activity within network
- Can spot suspicious activities from within network
- If an attacker sends a normal packet to a compromised machine and asks it to launch DOS attack, this implementation will be able to spot it
- Well protected from outside attack
- Can learn the typical behavior of internal users and spot any sudden change in their behavior

NIDS v/s HIDS



- A NIDS gives a lot more monitoring power than a HIDS as it can intercept attacks as they happen, whereas a HIDS only notices anything wrong once a file or a setting on a device has already changed
- NIDS is usually installed on a stand-alone piece of equipment and doesn't drag down the server processors
- The activity of HIDS is not as aggressive as that of NIDS and can be fulfilled by a lightweight daemon on the computer with very small load on host CPU
- Neither NIDS nor HIDS generate extra network traffic

IDS Methods

- **Signature based:**
  - Monitor all the packets traversing the network
  - Compares traffic against a database of signatures or attributes of known malicious threats,
  - Works similar to antivirus software
- **Anomaly based:**
  - Monitor network traffic and compare it against an established baseline,
  - Determines what is considered normal for the network with respect to bandwidth, protocols, ports and other devices.
  - Also known as Heuristic based IDS

Signature Based IDS

- Monitors for known patterns of malicious behavior
  - Port scan i.e. same sender trying to communicate with multiple ports at same time
  - Abnormal packet sizes i.e. ICMP packet size of 65535 will crash the protocol stack
- Use statistical analysis to identify malicious behavior
- Works well with ping, echo-chargen type of DDOS attacks
- Attacker may change signature of attack
  - Conversion to upper/lowercase
  - Conversion to symbols/ASCII character set
  - Induction of spurious packet in between
  - Change of signature
- Attacks with new signatures can’t be detected

Anomaly Based IDS

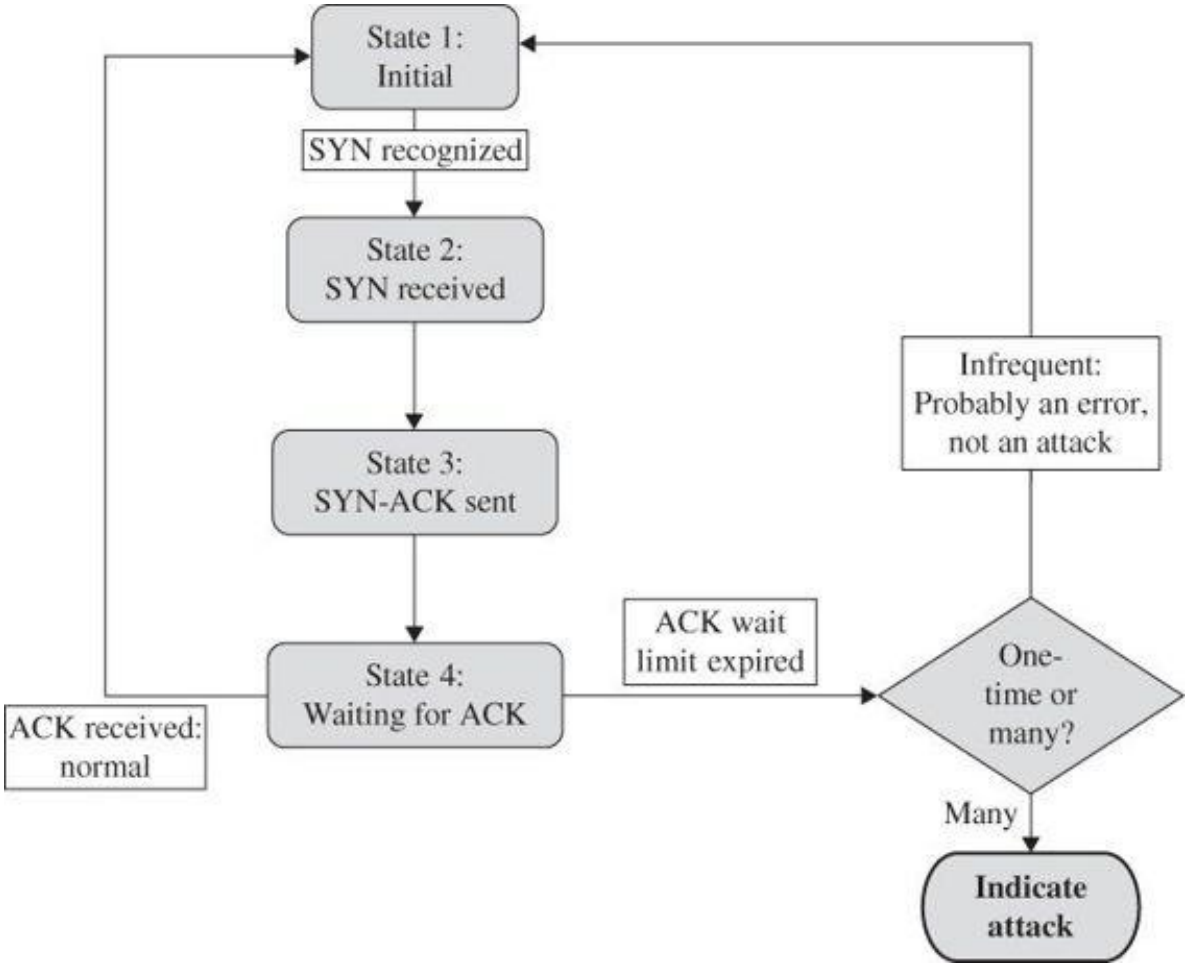
innovate achieve lead

- Monitors abnormal behavior:
  - One user normally performs email reading, word processing and file backup activities
  - If suddenly he starts executing administrator functions then it's suspicious – someone else might be using his account
- Monitors the system 'dirtiness' factor and raises alarm when it crosses a threshold.
- Activities classified as good/benign, suspicious, unknown
- Evaluates combined impact of asset of events
  - Ana tries to connect to Amit's machine, Amit's machine denies access (unusual)
  - Ana tries to connect to Abhay's machine, gets an open port and connects (more unusual)
  - Ana obtains listing of folder from Abhay's machine (suspicious)
  - Ana copies files from Abhay's machine (attack – raise alarm)
- Inference engine makes the decision to categorize actions and raise alarm

Inference Engine Types

- State based
  - Monitors system going thru overall state change
  - Identify when a system has veered into unsafe state
- Model based
  - List of known bad activities
  - Each activity has a degree of bad
  - Action when an activity of certain bad degree occurs
  - Overall cumulative activities cross a certain degree of bad
- Misuse intrusion detection
  - Compare real activity with a known representation of normality
  - Ex: password file being access by utilities other than login, change password, create user etc

Stateful Protocol Analysis: SYN Flood Attack



Other IDS Technologies…

- **Protocol-based Intrusion Detection System (PIDS):** comprises of a system or agent that resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It tries to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol.
- **Application Protocol-based Intrusion Detection System (APIDS):** a system or agent that resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.
- **Hybrid Intrusion Detection System :** combination of two or more approaches of the intrusion detection system. In this, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. **Prelude** is an example of Hybrid IDS

Other IDS Technologies…

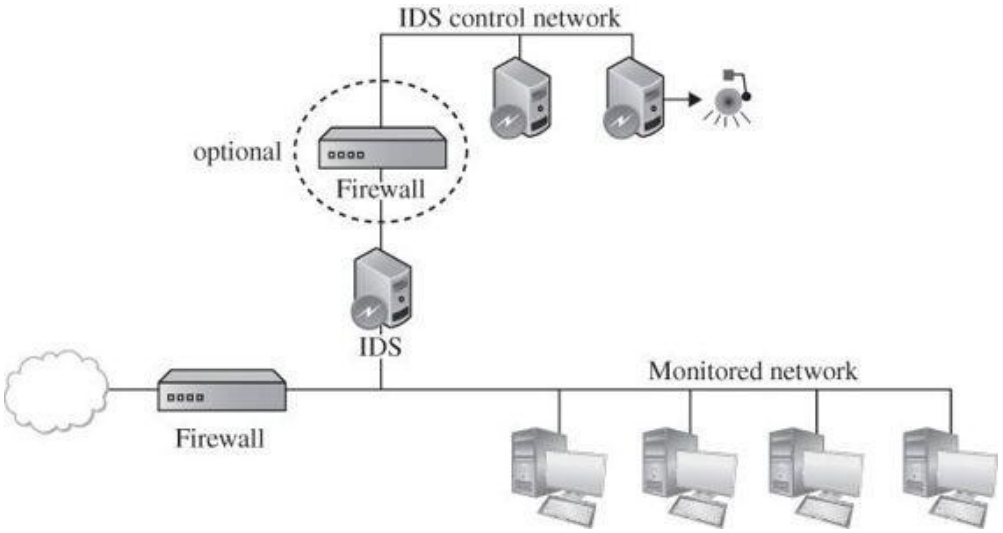
- **Code modification checkers:** compares the active version of source code with saved version (Tripwire)
- **Vulnerability scanners:** checks and report known vulnerabilities and flaws in a network (ISS Scanner, Nessus)

Accurate Situation Assessment

- Accuracy is important factor for IDS else administrators will have trust deficit
  - False Positive: Alarm raised where not real attack happened
  - False Negative: No alarm raised when a real attack happened

  - Sensitivity = both False Positive & False Negative should be minimized

Stealth Mode



- IDS runs in stealth mode to avoid attack (DDOS etc)
- IDS has two network interfaces:
- A. For the network being monitored – used only for inputs – this interface is not published – it's a wiretap
- B. for alerts a separate control network interface is configured

IDS Strengths and Limitations

- Strengths:
  - Can detect ever growing number of attacks
  - New signatures can be configured
  - Have become cheaper and easy to operate
  - Can operate in stealth mode to avoid attackers

- Limitations:
  - Requires strong defense else attacker can render an IDS ineffective
  - Attackers tend to gain insight into IDS working over a period of time
  - Poor sensitivity could limit accuracy
  - Someone needs to monitor IDS reports for actions

Benefits of IDS

- Ability to identify security incidents and help analyze the quantity and types of attacks
- Help organizations to change their security systems or implement more effective controls
- Identify bugs or problems with their network device configurations
- Use IDS data to assess future risks
- Help the enterprise attain required regulatory compliances by providing greater visibility across their networks
- Use IDS logs as part of the documentation to show regulators that they are meeting certain compliance requirements.
- Improve response to security incidents
- Inspect data within the network packets and identify the operating system services being used

Popular IDS Products

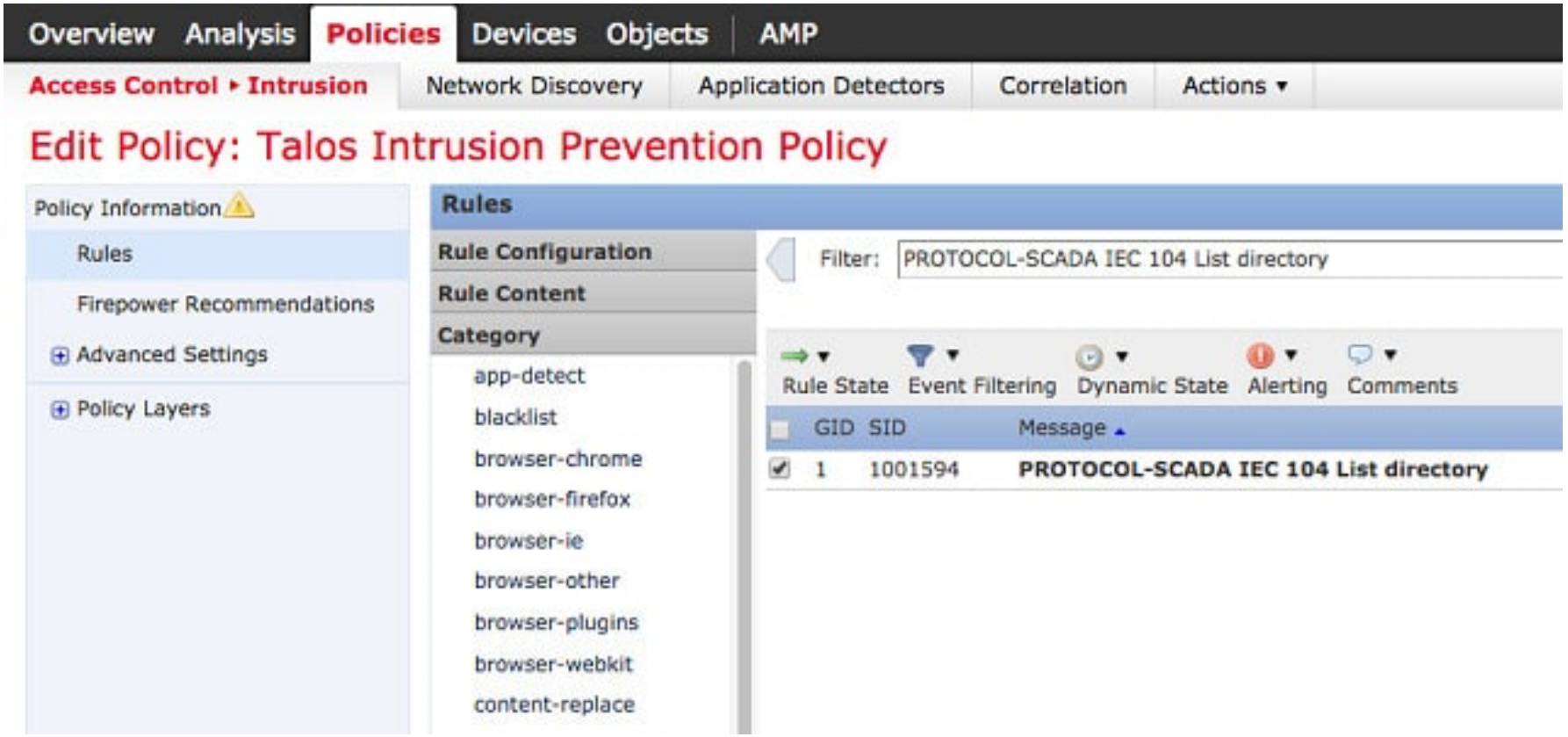
innovate achieve lead

- **SolarWinds Security Event Manager:** Combines both HIDS and NIDS functionality to give full Security Information and Event Management (SIEM) system
- **Snort:** Provided by Cisco Systems and free to use, a leading network-based intrusion detection system
- **OSSEC:** Excellent host-based intrusion detection system that is free to use
- **Suricata:** Network-based intrusion detection system that operates at the application layer for greater visibility
- **Bro:** Network monitor and network-based intrusion prevention system
- **Sagan:** Log analysis tool that can integrate reports generated on snort data, so it is a HIDS with a bit of NIDS
- **Security Onion:** Network monitoring and security tool made up from elements pulled in from other free tools
- **AIDE:** Advanced Intrusion Detection Environment is a HIDS for Unix, Linux, and MacOS
- **OpenWIPS-NG:** Wireless NIDS and intrusion prevention system from makers of Aircrack-NG
- **Samhain:** HIDS for Unix, Linux, and Mac OS
- **Fail2Ban:** Lightweight HIDS for Unix, Linux, and Mac OS

IDS Products Comparison

IDS	HIDS/NIDS	Unix	Linux	Windows	Mac OS
SolarWinds Security Event Manager	Both	No	No	Yes	No
Snort	NIDS	Yes	Yes	Yes	No
OSSEC	HIDS	Yes	Yes	Yes	Yes
Suricata	NIDS	Yes	Yes	Yes	Yes
Bro	NIDS	Yes	Yes	No	Yes
Sagan	Both	Yes	Yes	No	Yes
Security Onion	Both	No	Yes	No	No
AIDE	HIDS	Yes	Yes	No	Yes
Open WIPS-NG	NIDS	No	Yes	No	No
Samhain	HIDS	Yes	Yes	No	Yes
Fail2Ban	HIDS	Yes	Yes	No	Yes

Snort


Overview
Analysis
Policies
Devices
Objects
AMP
Access Control ▸ Intrusion
Network Discovery
Application Detectors
Correlation
Actions ▾
Edit Policy: Talos Intrusion Prevention Policy
Policy Information
Rules
Firepower Recommendations
Advanced Settings
Policy Layers
Rules
Rule Configuration
Rule Content
Category
app-detect
blacklist
browser-chrome
browser-firefox
browser-ie
browser-other
browser-plugins
browser-webkit
content-replace
Filter:
PROTOCOL-SCADA IEC 104 List directory
Rule State
Event Filtering
Dynamic State
Alerting
Comments
GID
SID
Message
1
1001594
PROTOCOL-SCADA IEC 104 List directory

Intrusion Prevention System (IPS)

What is an IPS?

- IPS is a network security application that monitors network or system activities for malicious activity
- IPS identifies malicious activity, collects information about this activity, reports it and attempts to block or stop it
- Intrusion Prevention System is also known as Intrusion Detection and Prevention System
- IPS is an IDS with in-built protective response capability

How Does an IPS Work?

- IPS performs real-time packet inspection, deeply inspecting every packet that travels across the network. If any malicious or suspicious packets are detected, the IPS will carry out one of the following actions:
  - Terminate the TCP session that has been exploited and block the offending source IP address or user account from accessing any application, target hosts or other network resources unethically.
  - Reprogram or reconfigure the firewall to prevent a similar attack occurring in the future.
  - Remove or replace any malicious content that remains on the network following an attack. This is done by repackaging payloads, removing header information and removing any infected attachments from file or email servers.

How Does IPS Work?...

- Signal an alert to other protection components
- Cut-off user access
- Reject traffic from identified sources
- Block all users to access a particular resource
- Call a human
  - High numbers of alarms generated may miss a human attention
  - Happened with Target in Nov/Dec 2013 where Russian hacker stole 40Mn credit card details

IPS Types

- **Network-based intrusion prevention system (NIPS):** Monitors the entire network for suspicious traffic by analyzing protocol activity.
- **Wireless intrusion prevention system (WIPS):** Monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
- **Network behavior analysis (NBA):** Examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
- **Host-based intrusion prevention system (HIPS):** Inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

IPS Detection Methods

- **Signature-based:** operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.
- **Statistical anomaly-based:** monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.
- **Stateful protocol analysis:** recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.
- **Policy-based:** requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an activity occurs that violates a security policy, an alert is triggered and sent to the system administrators.

Adaptive Behavior

IPS can be configured to initiate following actions

- Continue to monitor the network
- Block the attack by re-directing attack traffic to monitoring host, discarding the traffic or terminate session
- Re-configure the network by bringing other hosts on-line (increase capacity) or adjust load balancers
- Adjust performance to slow the attack i.e. drop some of the incoming traffic
- Deny access to particular network hosts or services
- Shut down whole network

Counter Attack

- Final option against an attack is counterattack
- Counterattack must be taken after good thought and caution
- Reasons for caution:
  - Apparent attacker may not be real attacker, taking action against wrong party could make matters worse
  - Counterattack may lead to rea-time battle of info-war
  - Legality may shift – taking offensive action may open one to legal geopardy
  - Provoking attacker may lead to escalation
- Example: Wikileaks battle in Dec, 2006

Popular IPS Products

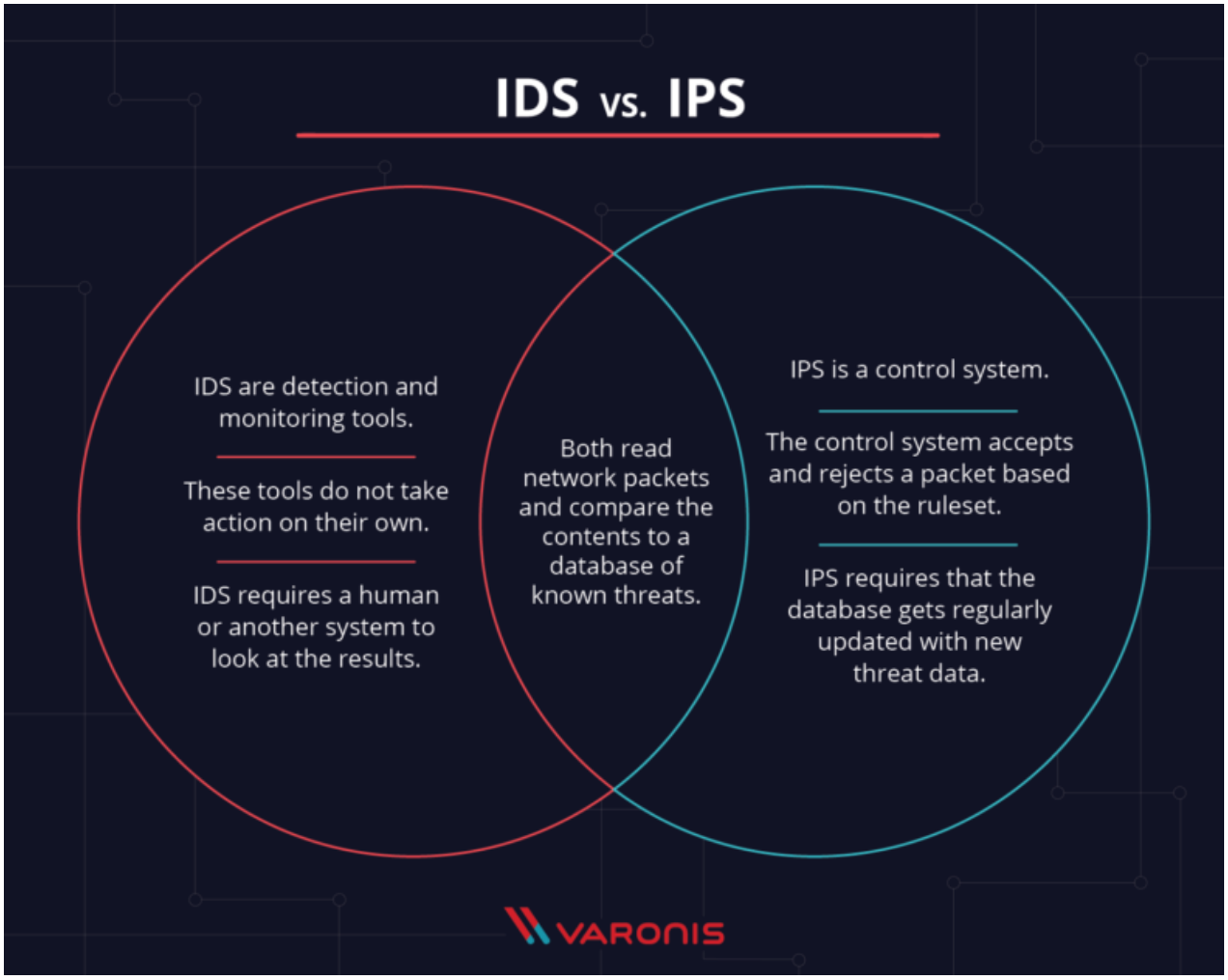
- McAfee NSP
- Trend Micro TippingPoint
- HillStone NIPS
- Darktrace Enterprise Immune System
- NSFocus NGIPS
- H3C SecBlade IPS
- Huawei NIP
- Entrust IoTrust Identity and Data Security
- Cisco FirePower NGIPS

Popular IPS Products…

innovate achieve lead

Vendor	Use Cases	Metrics	Intelligence
McAfee	NSP is deployed across all market segments in the data center, cloud, or hybrid enterprise environments	Aggregate Performance - 40 Gbps; Maximum number of connections ranges from 40,000 on the 100 Mbps appliance up to 32 million on the 40 Gbps appliance	Bot analysis, endpoint-enhanced application control, analysis of flow data, self-learning DoS profiles and an analytics feature to report potentially malicious hosts
Trend Micro	Large and very large enterprises	40 Gbps inspection throughput in a 1U form factor; can be stacked to deliver 120 Gbps in a 3U form factor. Network traffic inspection throughputs 250 Mbps to 120 Gbps	TippingPoint solutions provide rea l-time, threat prevention for vulnerabilities through Digital Vaccine threat intelligence
Hillstone	Government, finance, education, ISP and enterprises customers	Can identify more than 3,000 applications, including mobile and cloud applications. IPS throughput up to 14 Gbps	Advanced threat detection engine and abnormal behavior detection engine
Darktrace	Large enterprise sites across all verticals	The Darktrace vSensor extracts only relevant metadata, sending 1% of network traffic onto the master appliance	Machine learning
NSFocus	Fortune 500 companies, mobile providers, global financial institutions, SMEs and service providers	Up to 20 Gbps of application-layer data processing capacity	Virtual sandboxing appliance is capable of detecting, analyzing and mitigating known, zero-day, and advanced persistent threats
H3C	All market sizes	Millisecond response to threats	Defense and traffic pattern self-learning capabilities
Huawei	Large- and medium- size enterprises, as well as carrier-grade enterprises	NIP can identify more than 1,200 network applications	Protocol anomaly detection, traffic anomaly detection, and heuristic detection
Entrust	Energy, utility, chemical, automotive, telecom and manufacturing	More than 10 million identity and payment credentials daily	Data filtering, aggregation and integration with edge analytics
Cisco	From remote offices to large data centers	Appliances range from 50 Mbps to 60 Gbps of inspected IDPS throughput	URL-based security intelligence, AMP Threat Grid integration, security research team

IDS v/s IPS



- IPS are placed in-line and are able to actively prevent or block intrusions that are detected.
- IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
- IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

Firewalls v/s IDS v/s IPS

- Firewall is first line of perimeter defense. Best practices recommend that firewall be explicitly configured to DENY all incoming traffic and then you open up holes where necessary. You may need to open up port 80 to host websites or port 21 to host an FTP file server.
- Each of these holes may be necessary from one standpoint, but they also represent possible vectors for malicious traffic to enter network rather than being blocked by the firewall.
- That is where IDS would come in, the IDS will monitor the inbound and outbound traffic and identify suspicious or malicious traffic which may have somehow bypassed the firewall or it could possibly be originating from inside network as well.
- An IPS is essentially a firewall which combines network-level and application-level filtering with a reactive IDS to proactively protect the network.

Thank You