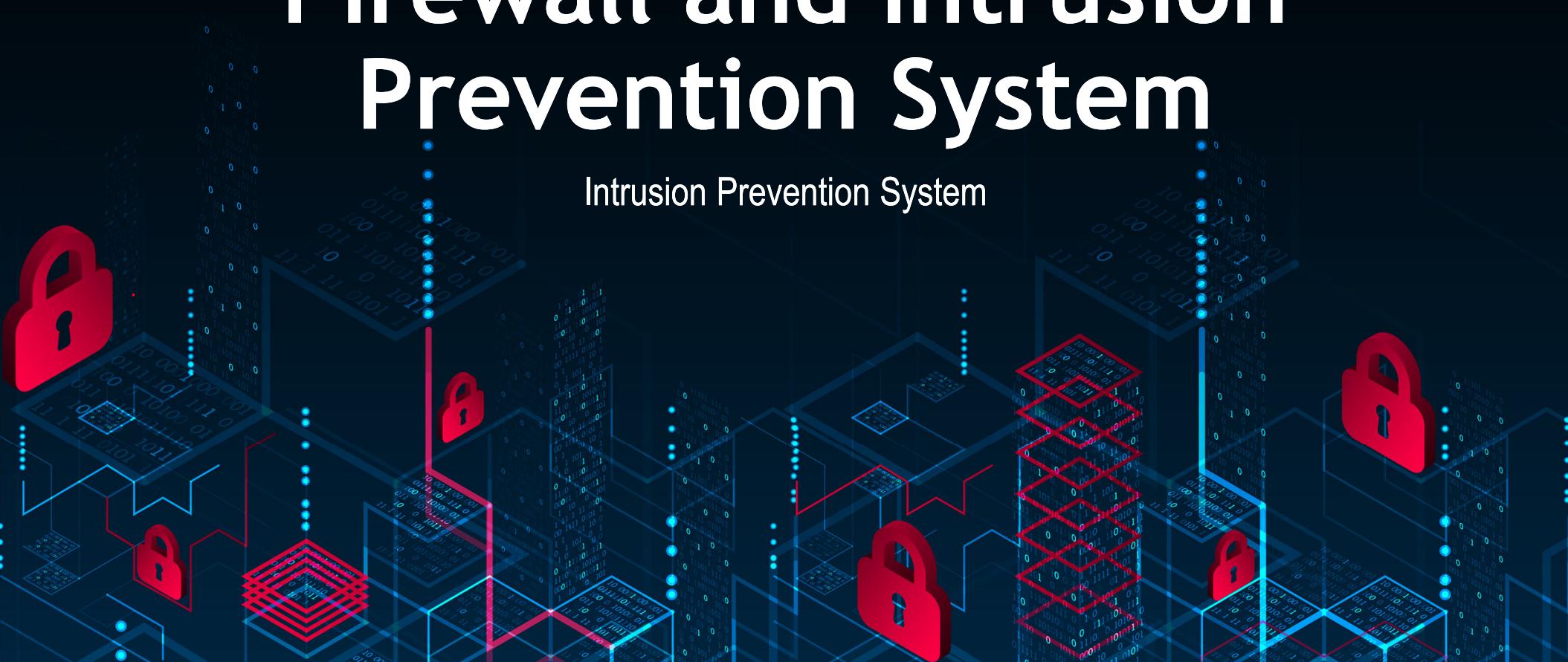


Firewall and Intrusion Prevention System

Intrusion Prevention System



Video Summary

- Intrusion Prevention System
- Host-Based IPS (HIPS)
- Network-Based IPS (NIPS)
- Digital Immune System
- Snort Inline

Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature detection to identify known malicious behavior can block traffic as a firewall does



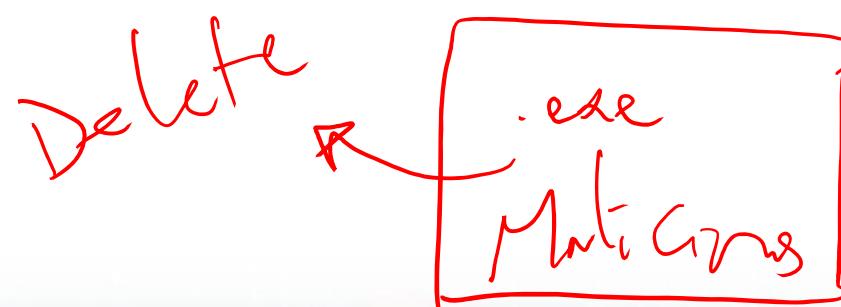
Host-Based IPS (HIPS)

- Can make use of either signature or anomaly detection techniques to identify attacks
 - Signature: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
 - Anomaly: IPS is looking for behavior patterns that indicate malware
- Examples of the types of malicious behavior addressed by a HIPS include:
 - Modification of system resources
 - Privilege-escalation exploits
 - Buffer-overflow exploits
 - Access to e-mail contact list



HIPS

- A set of general purpose tools may be used for a desktop or server system
- Some packages are designed to protect specific types of servers, such as Web servers and database servers
 - In this case the HIPS looks for particular application attacks
- Can use a sandbox approach
 - Sandboxes are especially suited to mobile code such as Java applets and scripting languages
 - HIPS quarantines such code in an isolated system area then runs the code and monitors its behavior



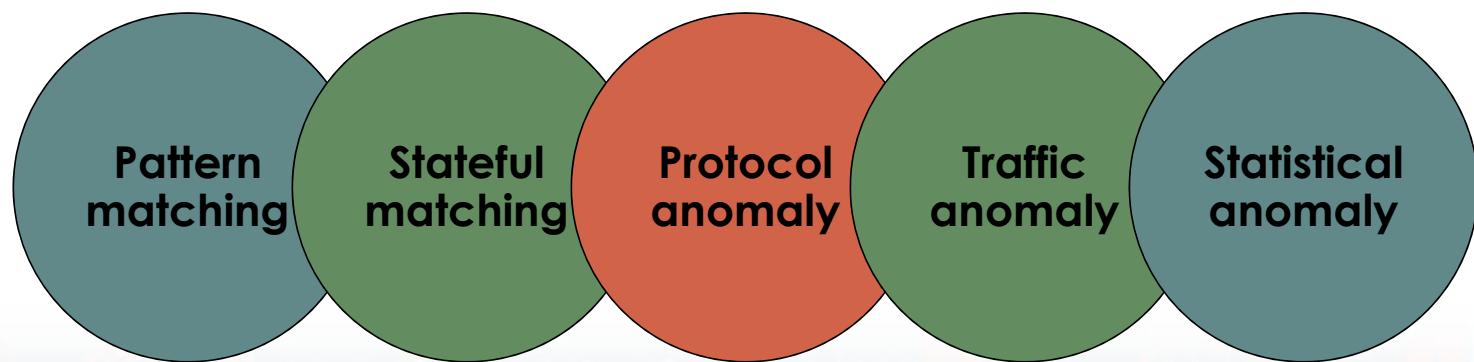
The Role of HIPS

- Many industry observers see the enterprise endpoint, including desktop and laptop systems, as now the main target for hackers and criminals
 - Thus security vendors are focusing more on developing endpoint security products
- Approach is an effort to provide an integrated, single-product suite of functions
 - Advantages of the integrated HIPS approach are that the various tools work closely together, threat prevention is more comprehensive, and management is easier



Network-Based IPS (NIPS)

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections
- Makes use of signature detection and anomaly detection
- May provide flow data protection
- Methods used to identify malicious packets:



Digital Immune System

- Comprehensive defense against malicious behavior caused by malware
- Developed by IBM and refined by Symantec
- Motivation for this development includes the rising threat of Internet-based malware, the increasing speed of its propagation provided by the Internet, and the need to acquire a global view of the situation
- Success depends on the ability of the malware analysis system to detect new and innovative malware strains

