Protecting the Network – Intrusion Detection and Prevention Systems

INFO-6078 – Managing Enterprise Networks

FANSHAWE

Protecting the Network

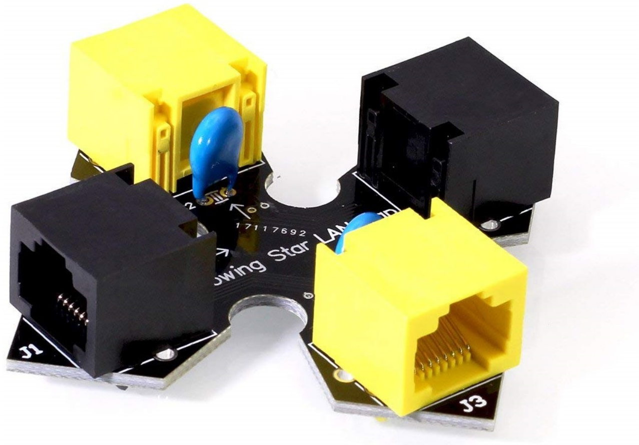
- A computer virus contains code that can infect a system and cause alteration, corruption, or destruction of the system and / or its data
- A computer worm is a piece of self-replicating malware that can spread across the network without human intervention and may conceal a hidden payload such as a cryptolocker designed to encrypt the contents of a systems storage
- A zero-day attack in the form of a worm can infect hosts all across the world in a matter of minutes or hours
- In addition to the threats caused by malware, employee hacking activities can compromise the network from within

Protecting the Network

- An employee connecting remotely through a VPN may circumvent some security boundaries
- Current trends of bring your own device (BYOD) means employees may bring already compromised devices and connect them to the corporate network
- To combat these and other threats, administrators must take a defense-in-depth approach to network security
- Components of this defense must include both intrusion detection systems (IDS) and intrusion prevention systems (IPS) as layers of the overall approach

Intrusion Detection System (IDS)

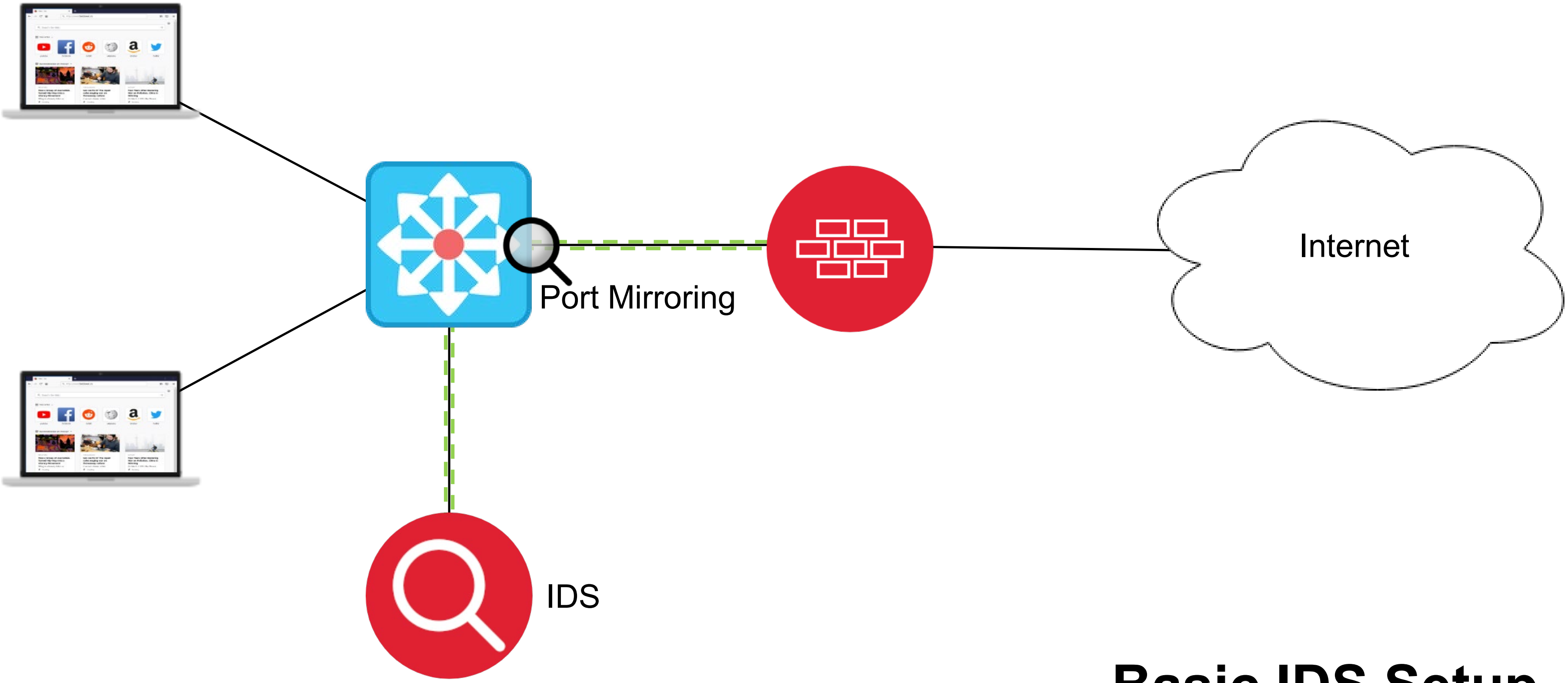
- IDS provides real-time monitoring and logging of network activity
- An IDS sensor is placed so it receives a copy of network traffic for analysis
- The network traffic can be copied as the result of using a network terminal access point (TAP), or by duplicating network traffic on a device such as a switch



Intrusion Detection System (IDS)

- IDS analyses traffic based on pre-defined, rule-based signatures
- IDS is a passive technology and cannot block threats from penetrating the network; however, IDS can inform the network team of suspicious activity by providing alerts to detected events
- One benefit of using IDS is that network traffic does not suffer any latency, as only a copy of network traffic is analyzed

Intrusion Detection System (IDS)

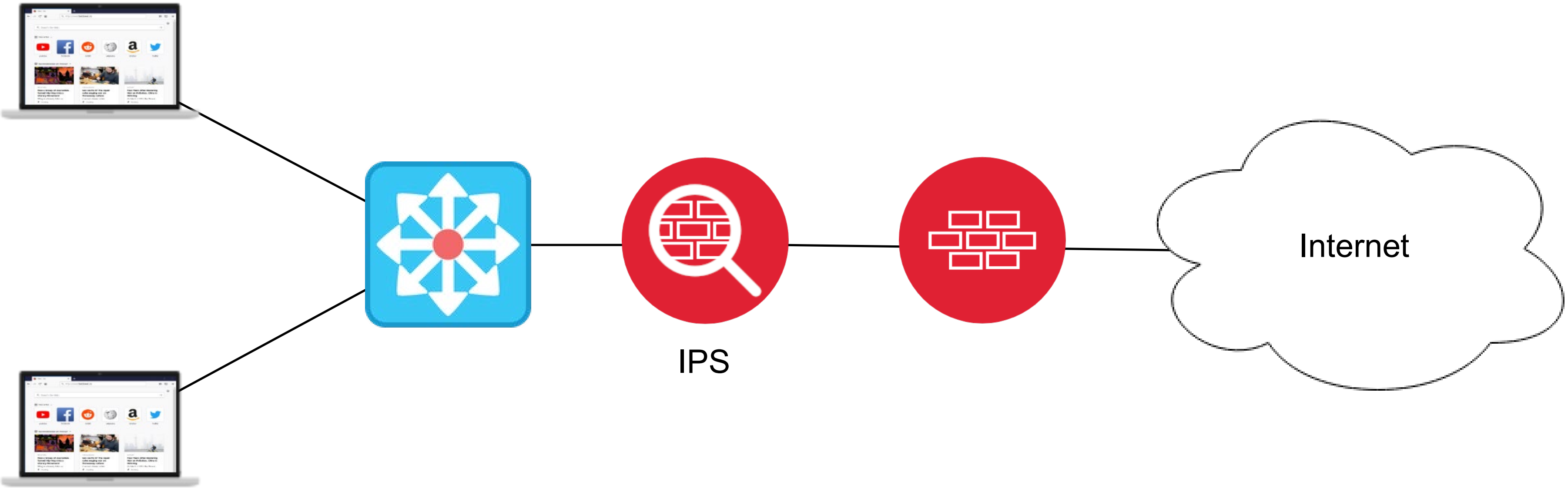


Basic IDS Setup

Intrusion Prevention System (IPS)

- Similar to IDS, IPS analyzes network traffic for threats; however, with IPS, the analysis occurs inline and traffic identified as suspicious is dropped at the IPS
- IPS can identify suspicious traffic patterns from layer 2 to 7 of the OSI model
- One benefit of IPS is that systems can rapidly respond to newly discovered threats, and protect the network against infection
- As traffic must be inspected before passing through the IPS, the network will experience some latency

Intrusion Prevention System (IPS)



Basic IPS Setup

IPS Architecture – Host-Based

- A host-based intrusion prevention system (HIPS) is software that is installed on a host system
- The HIPS monitors actions taken on the system and protects the operating system (OS) against malicious actions such as:
  - System file modifications
  - Installation of malicious applications
  - Modifications to the state of antivirus software
  - Users browsing dangerous websites
- Modern security suites often include HIDS as a component of overall protection

IPS Architecture – Network-Based

- Network-based IPS come in a variety of forms, including:
  - A dedicated network sensor
  - As a component of a network router
  - As a component of a security appliance
- Network-based sensors may be deployed at multiple locations in the network such as:
  - Behind a firewall at the network edge
  - Protecting network boundaries between a datacenter and host devices, or between a datacenter and a demilitarized zone (DMZ)

Host-Based vs Network-Based IPS

- Network-based IPS offers an attractive solution as it provides a single platform to protect all network hosts; reducing administrative overhead and deployment costs
- A disadvantage of network-based IPS is a lack of visibility when network traffic is encrypted
- Modern malware frequently makes use of encryption technologies such as Tor
- In July of 2019, Godlua the first malware that took advantage of DNS over HTTPS (DoH) to obscure its DNS traffic
- Host-based IPS solution are not affected by network encryption

IPS Components – Signatures

- IPS is comprised of a number of components working together to protect the system
- Signatures generally describe the distinctive characteristics or patterns present in malicious traffic that uniquely identify that type of attack
- IPS detection engines builds attack signatures by parsing the rules of a signature file
- By updating the signature file, administrators can protect the network from emerging network threats

IPS Components – Signatures

IPS signatures are represented in the following categories:

- **Atomic Signatures**
  - An atomic signature describes a single packet or event than can be used to identify suspicious traffic
  - Atomic signatures do not require the IPS to maintain state
- **Stateful Signatures**
  - Stateful signatures identify patterns spread across multiple packets to identify an attack
  - Stateful signatures require the IPS to maintain state

IPS Components – State

- State refers to the requirement of an IPS to monitor multiple packets to determine the context of a traffic pattern
- State can also reference the monitoring of TCP communications for connection establishment, teardown and validation of sequence and acknowledgement numbers
- Stateful signatures require an IPS to remember several packets for a period of time called the event horizon
- The event horizon defines the maximum amount of time needed to identify a suspicious traffic pattern
- The event horizon varies with each individual signature

IPS Components – Alerts

- The ultimate goal of any IDPS system is to inform the administrators that an attack is taking place
- The response an IDPS takes when it detects a suspicious pattern based on a signature is to generate an alert
- In addition the IDPS system will generate a log event that may contain the relevant traffic in pcap format
- Additionally, an IPS system can drop the packet in question and block future traffic from the attacking host

IPS Components – Alerts

- Receiving alerts from an IDPS does not always mean that the network is under attack
- A false positive occurs when an IDPS labels legitimate traffic as suspicious and generates an alert
- It is important to follow up with false positive alerts, and to tune the IDPS not to treat future events as suspicious
- A false negative occurs when an IDPS fails to identify malicious traffic and generate an alert
- If an IDPS does not detect a recognized attack, the network is at risk

IPS Components – Detection Mechanisms

- Rule-based pattern detection is the most popular method an IDPS can use to generate an alert
- To trigger a detection, the IDPS must be programmed with the attack signature
- Anomaly-based detection is the opposite of rule-based detection, instead of programming the sensor with signatures of malicious traffic, normal traffic patterns are defined, and any other activity triggers a response
- With anomaly-based detection, a training period usually occurs to define what is considered “normal” traffic for the network

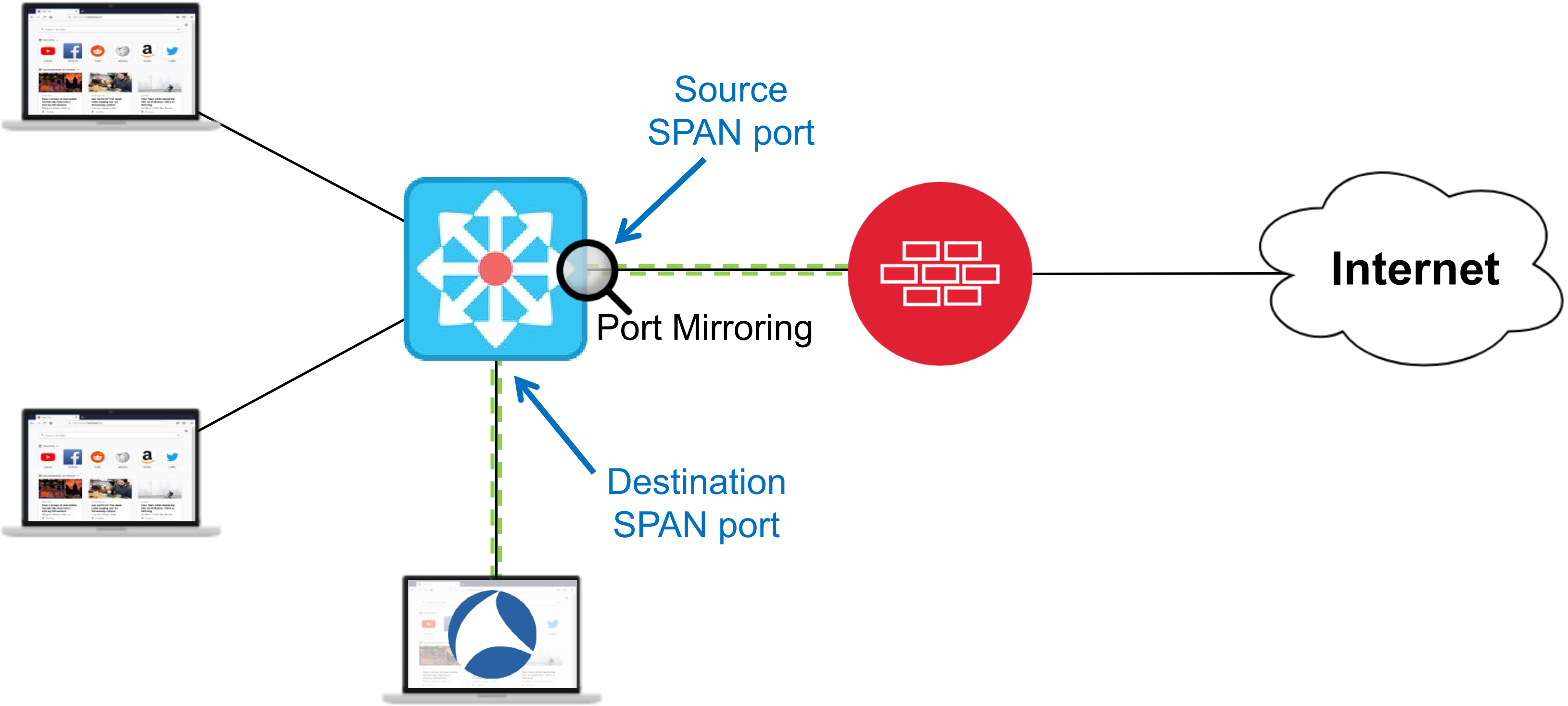
IPS Components – Detection Mechanisms

- One advantage of anomaly-based detection is that the network is more resilient to new attacks, as any significantly different activity is considered suspicious
- Despite the obvious benefits of anomaly-based detections, it is often overlooked as it can trigger a large number of alerts and potentially block legitimate traffic
- Defining “normal” traffic patterns is a difficult and complicated task’ additionally, network traffic patterns tend to change with time, which could lead to disruption in communications

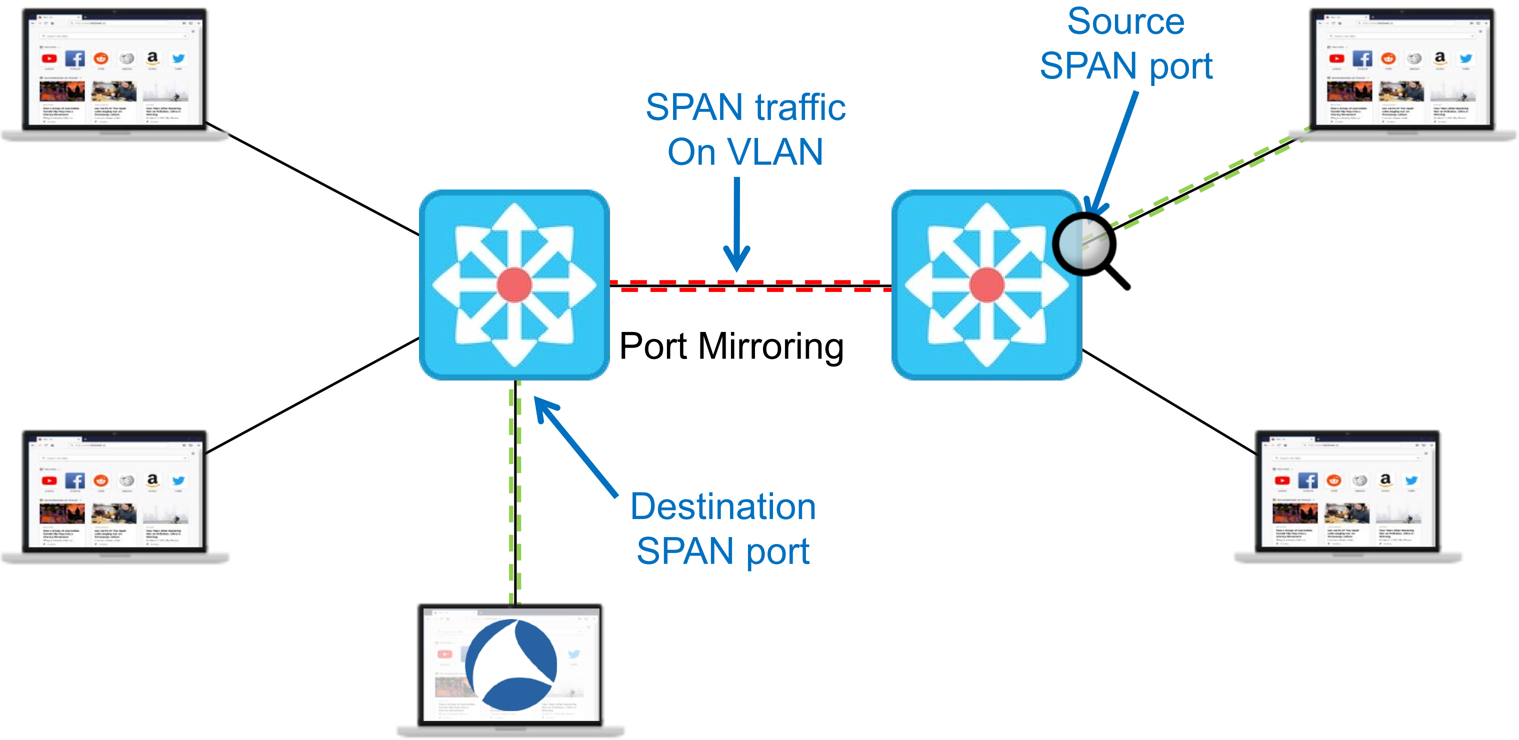
Port Mirroring

- Port mirroring allows a switch or similar device to duplicate traffic sent to or destined to one or more of its ports and send a copy of the traffic to another port
- Port mirroring can duplicate and monitor ingress, egress or both traffic directions
- Cisco uses the term switched port analyzer (SPAN) to reference mirroring traffic from a local switch, and remote switched port analyzer (RSPAN) for traffic traversing one or more additional switches

Switched Port Analyzer (SPAN)



Remote Switched Port Analyzer (RSPAN)


Source
SPAN port
SPAN traffic
On VLAN
Port Mirroring
Destination
SPAN port