Implementing Secure Converged Wide Area Networks (ISCW)

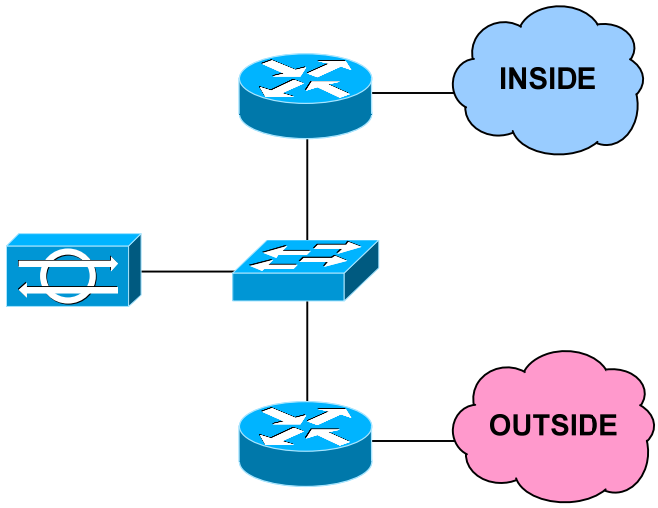
Cisco IOS IPS

http://www.INE.com

IDS Overview

- Intrusion Detection System
- Monitors traffic for malicious traffic
- Responds accordingly
  - Generate logs/alarms
  - Instruct managed device to block traffic
  - Reset TCP session
- Typically not in the traffic transit path
  - i.e. “promiscuous”
- Attack response time an issue

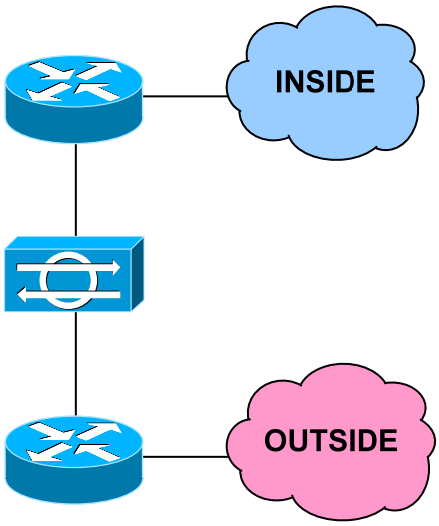
Typical IDS Design



IPS Overview

- Intrusion Prevention System
- Same as IDS, but directly in the transit path
  - i.e. “inline”
- Allows more sophisticated attack responses and faster response times

Typical IPS Design



Types of IDS/IPS

- Signature based
  - Checks traffic against known database of attacks
- Anomaly based
  - Discovers nominal network behavior and adapts to events outside the norm
- Policy based
  - Checks for events to breach preconfigured thresholds
  - e.g. TCP SYN attack

Types of IDS/IPS (cont.)

- Honeypots
  - Unprotected systems designed to collect attack patterns for further analysis
- Network based (NIPS)
  - IPS appliance in the network transit path
- Host based (HIPS)
  - IPS software on the end host

Cisco IPS Devices

- Hardware based
  - IPS 4200
  - Catalyst 6500
    - Intrusion Detection System Services Module (IDSM)
  - ASA 5500
    - Advanced Inspection and Prevention Security Services Module (AIP-SSM)
- Software based
  - IOS IPS

IOS IPS Overview

- Software based inline IPS solution
- Signature based
  - Includes built-in signatures
  - Downloadable Signature Definition Files (SDFs)

IOS IPS Event Actions

- Alarm
  - Syslog
  - Security Device Event Exchange (SDEE)
    - Uses HTTPS
- Drop
- Reset
- Block attacker inline
- Block connection inline

IOS IPS CLI Configuration

- Create IPS rule
- Apply rule to interface
- Retire all signatures
- Specify signature storage location in flash
  - Signature configuration not stored in NVRAM
- Install signatures public key
- Compile signatures
- Fail open or closed
- Signature tuning

IOS IPS Configuration Examples