**IDS/IPS**

Innhold

[Purpose 1](#_Toc196732584)

[Intrusion Detection: Out of Band 2](#_Toc196732585)

[Intrusion Prevention: In Band 2](#_Toc196732586)

[Network-based Intrusion Detection (NIDS): 4](#_Toc196732587)

[Intrusion Detection system overview: 5](#_Toc196732588)

[Intrusion Prevention system overview: 6](#_Toc196732589)

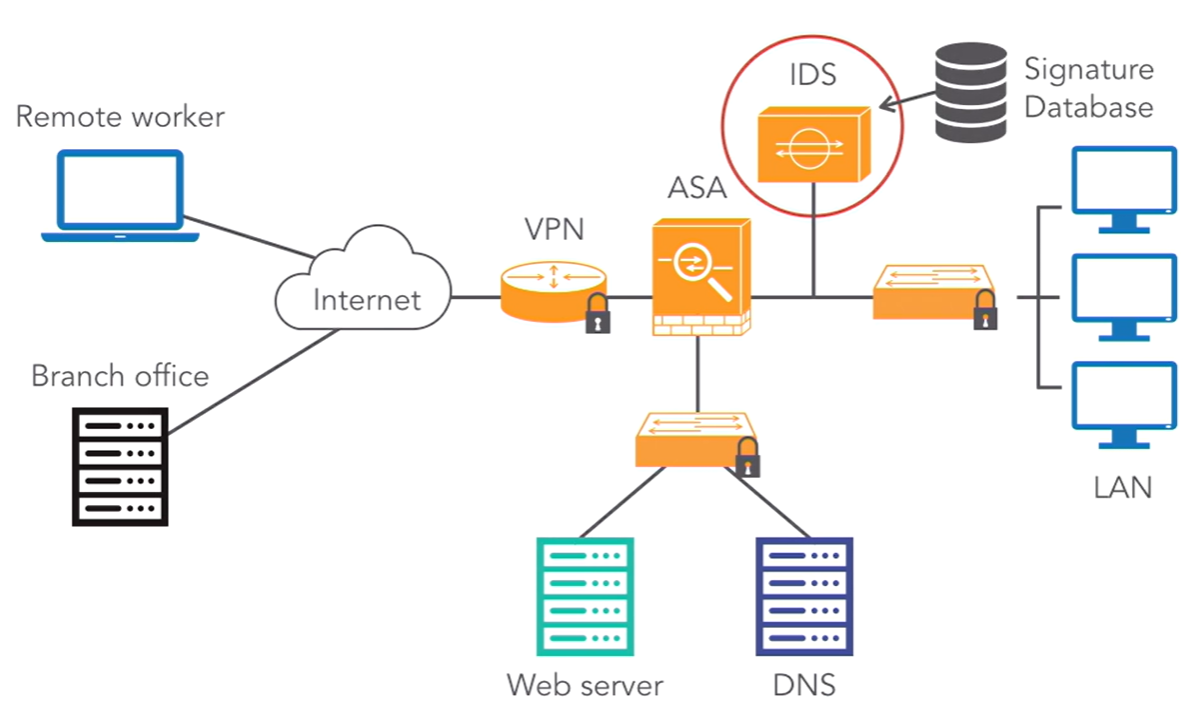
Purpose:

* **Increase security level of a network by enforcing policies on what is allowed and what is denied**
* **Can be Host-Based or Network-based**
* **Monitor for unusual or suspicious data or activities**
* **A stand-alone device or integrated within an Adaptive Security Appliance (ASA) or router**
* **Detect evidence of data exfiltration, virus, worms, trojans and bot activity, SQL Injection, cross-site scripting and denial of service**
* **Inspect ingress and egress traffic**
* **Uses signature and heuristic-based analysis**

(Which means that it looks for commands and instructions not normally present in a normal application)

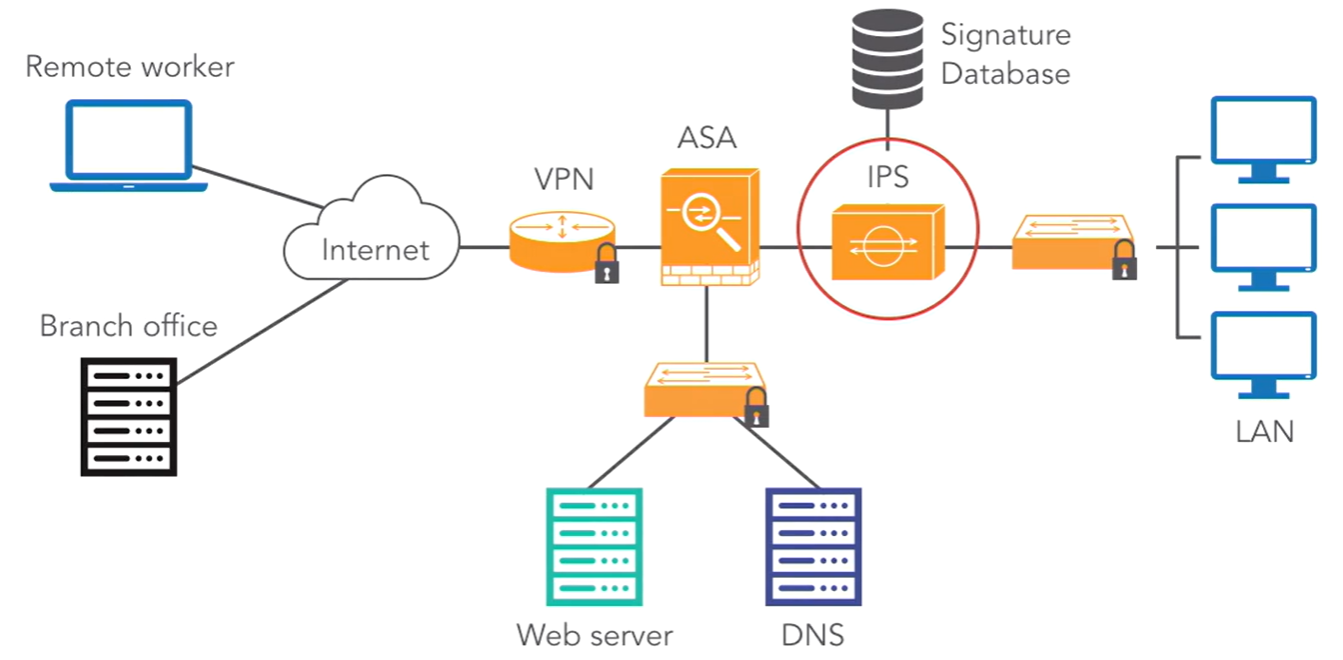
# Intrusion Detection: Out of Band

* Sits out of band in promiscuous mode
* Passively monitors network traffic
* Traffic is mirrored to the intrusion detection system so it can be checked against the signature database
* If the traffic is malicious, it will detect and provide log information about the activity and report the attack
* Does not negatively affect the traffic flow
* Is more vulnerable to evasion techniques



# Intrusion Prevention: In Band

* Builds on Intrusion detection technology
* Sits in Band
* Actively monitors network traffic
* Can detect and block attacks by dropping the suspect traffic
* It can negatively affect the network traffic if not configured properly

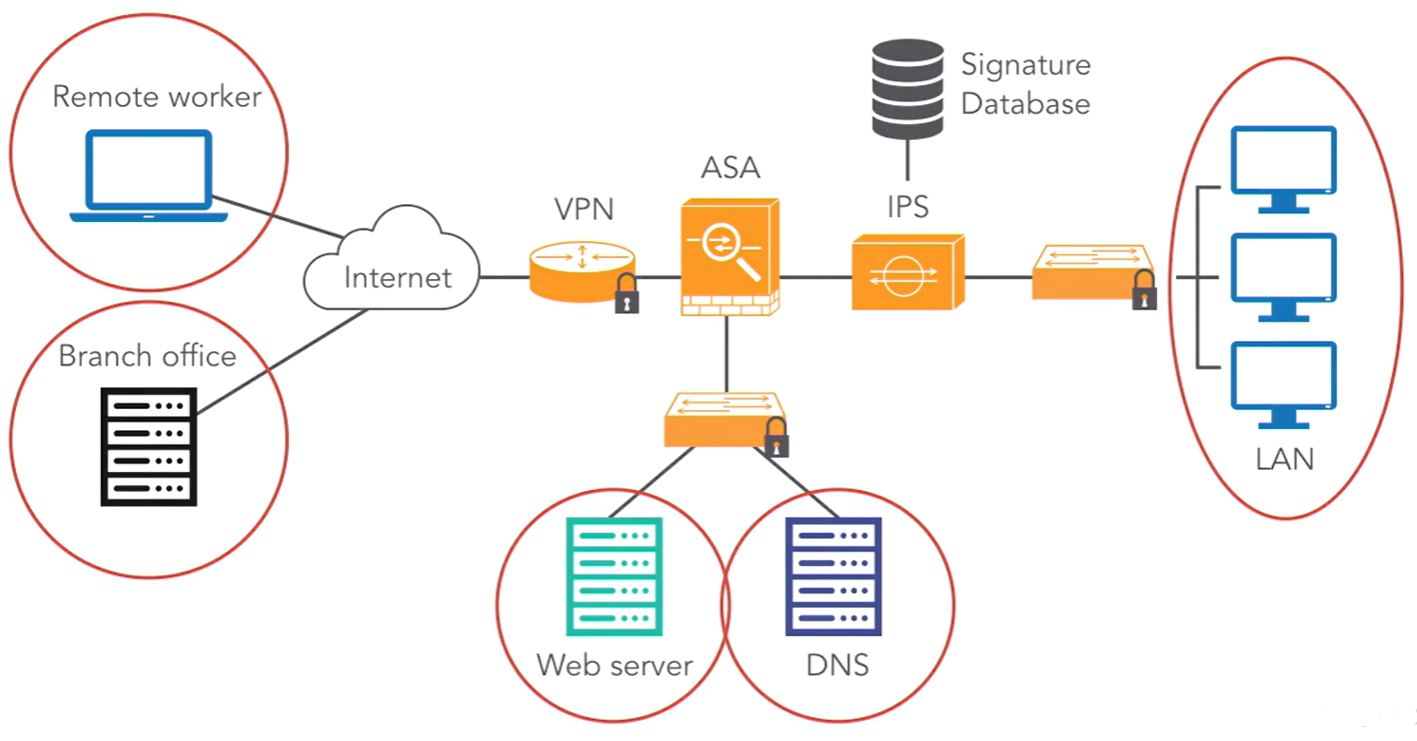


# Host-based Intrusion Detection:

* Monitors a single host or endpoint

(servers, workstations and mobile devices)

* Can be fine-tuned to for example user role or specific workflow
* Operating system specific, which means that they work independently to monitor events on a host for suspicious activity
* Encrypted traffic will be decrypted
* The IDS can examine the contents



# Network-based Intrusion Detection (NIDS):

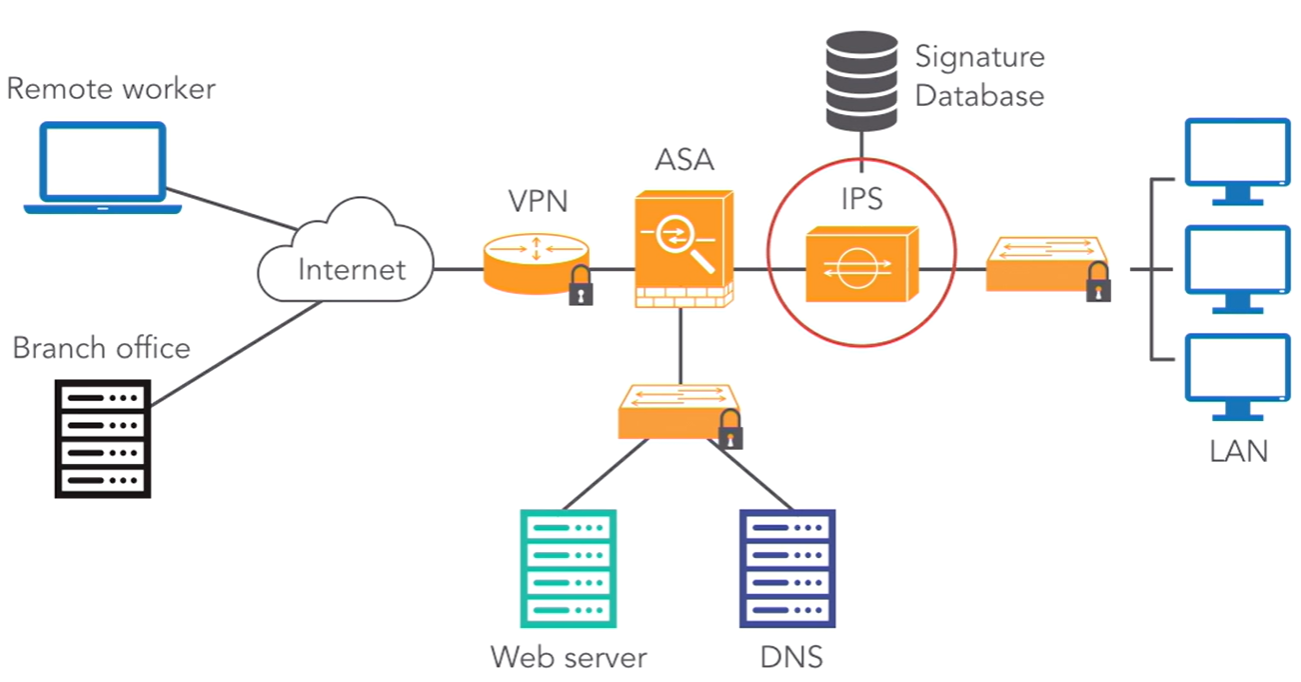
* Monitors the entire network
* Sensors are deployed at the network edge to monitor ingress and egress traffic
* Block network level attacks
* Operating system independent
* Should consist of:

- Sensors or agents

- State tables

- Signature databases

* Can not monitor encrypted traffic such as SSH, TLS or TLS which may allow malicious activity to go undetected
* CPU intensive
* NIC that’s able to communicate on the network to keep up with the traffic
* Memory intensive



# Intrusion Detection system overview:

* Sniffs a packet from the network
* The Preprocessor looks at the packet header

(decides whether to analyze it further, maintained in the state table)

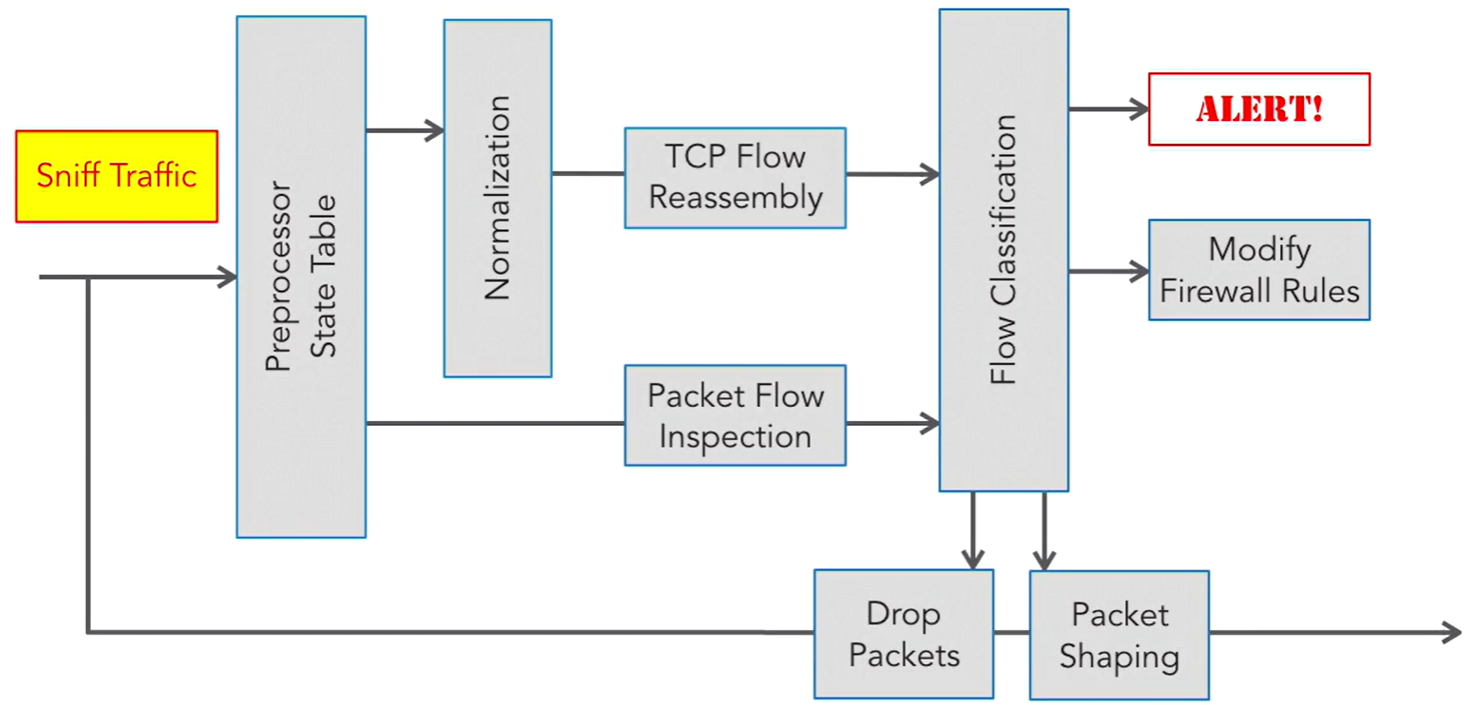
* Moves on to normalization for a careful examination of normal TCP/IP behavior
* Moves onto TCP flow reassembly, at the same time packet flow inspection examines the payload and compares it against the detection signature engine
* Moves then onto flow classification, here appropriate action is taken, for example:

- Alert

- Modify firewall rules

- Packet Shaping

- Drop the packet



# Intrusion Prevention system overview:

* Access to view the entire network
* Correlation of events for predictive analysis

(using previous data to predict future outcomes)

* Centralized management system with encrypted communications
* Detect policy violation and identify misconfigured or vulnerable devices on the network
* Detection engine with a range of signatures

(Automatic signature database updates?)

* Ability to manually update the signature database
* Knowledge base for monitoring heuristic or anomaly-based activity
* Collect and log data for further analysis
* Summarize the events in the form of a report
* Keep tuning the system, keep up to date and harden against attacks
* Compatibility:

- Devices

- Network speeds

- Bandwidth requirements

# Detection and Signature Engines

**Atomic signature**

* a single packet
* activity or event

**Composite signature**

* also called a stateful signature
* sequence of events involving multiple packets
* Dispersed across multiple hosts during a period

**Signature Engine**

* A **parser** (reads the text-based descriptions for all signatures)
* An **inspector** (looks for malicious activity in the traffic stream

**Signature Engines**

* **Service** – inspect common application layer services

HTTP, MySQL, NTP, DNS

* **String** – search for regex strings in the traffic stream
* **Flood** – monitor for flood activity

Monitor for a host or network sending multiple packets to a single host or network as in a DOS attack

**Atomic Micro-Engines**

create simple single-packet signatures that triggers a warning if a matching signature is detected

**Atomic-IP**

Examines the headers of TCP, IP, UDP and ICMP packets

**Atomic-IP Advanced**

Includes advanced IP options such as IPv6 packets with fragment options header

**Fixed TCP, UDP, and ICMP**

Examine the fixed or immutable portion of the TCP, UDP and ICMP headers

**Atomic ARP**

Examines ARP packets for ARP spoofing attacks

**Sweep Engines**

Monitor for the various signatures related to sweeps and scans

Common scans:

**Ping Sweep** – A series of packets sent to identify live hosts

**Port Scan** – Identifies listening TCP and UDP ports on a system looking for services

**Anomaly or Profile-Based Detection**

Best practice against zero-day

* Monitor virus and malware behavior
* Detects new and previously unpublished attacks
* Requires careful initial configuration

**Learning mode**

* Builds a normal profile by monitoring network or host activity for at least 24 hours
* After the system learns the normal behavior, the signature triggers if activity occurs beyond a specified threshold

**#NOTE: The network must be free of attacks while establishing normal activity!**

**Detect mode**

* Anomaly detection monitors for anomalies
* Records gradual changes and builds a profile of normal system activity over time

**Inactive mode**

* Turn off anomaly detection

**Reputation-Based Detection**

Reputation-based IDS help prevent threats from malware and zero-day attacks by sharing collective knowledge

* Selections are made based on the reputation of the company or product
* Event correlation provides information to the IDS

- About IP addresses that may have a reputation associated with

malicious or risky websites

**Policy-Based Detection**

Administrators define suspicious behavior and then create a customized policy to monitor that activity.

* Policy-based IDS is like pattern-based detection
* Instead of defining a specific pattern, policy-based signatures can analyze a specific type of packet

**Rule Header:**

Et bilde som inneholder tekst, line, Font, skjermbilde

KI-generert innhold kan være feil.

**Signature Detection**

The signature database is the heart of the IDS. For the system to be most effective, the signature file must be updated regularly.

Monitors the network for a matching pattern by using predefined signatures.

Three distinctive attributes:

* Type
* Trigger
* Action

**Real-Time Threat Defense**

If the system can be obtained automatically, it’s best to set this option

**Blacklist Objects**

* Websites
* Hosts and usernames
* TCP/UDP ports
* ICMP types and codes
* Specific file extensions

**Whitelist Objects**

* Restricts access to only trusted objects

- MAC address filtering on a WAP (Wireless Access Point)

* Can be more time consuming and difficult
* Reduce the number of false positives that involve known benign traffic

# Types of alarms

**False positive –** occurs when processing benign traffic

**False negative –** occurs when processing attack traffic that the intrusion system is configured to detect

* Dangerous, as the system is not detecting known attacks

**True positive -**  is a response to known malicious traffic

**True negative** – normal traffic does not generate an alarm

You want **TRUE POSITIVE** alarms

Minimize false positives and false negatives

**Threat levels:**

* **High** – an immediate threat is extremely likely
* **Medium** – an immediate threat is likely
* **Low** – an immediate threat is not likely
* **Informational** – no immediate threat