WHITE PAPER

Beginner's Guide to IDS, IPS and UTM – What's the Difference?

There is often a lingering and general confusion over the acronyms IDS and IPS, and how they are like or unlike UTM software modules. Everyone likes primers and simple descriptive definitions; so let's take a look at IDS, IPS and UTM through that lens.

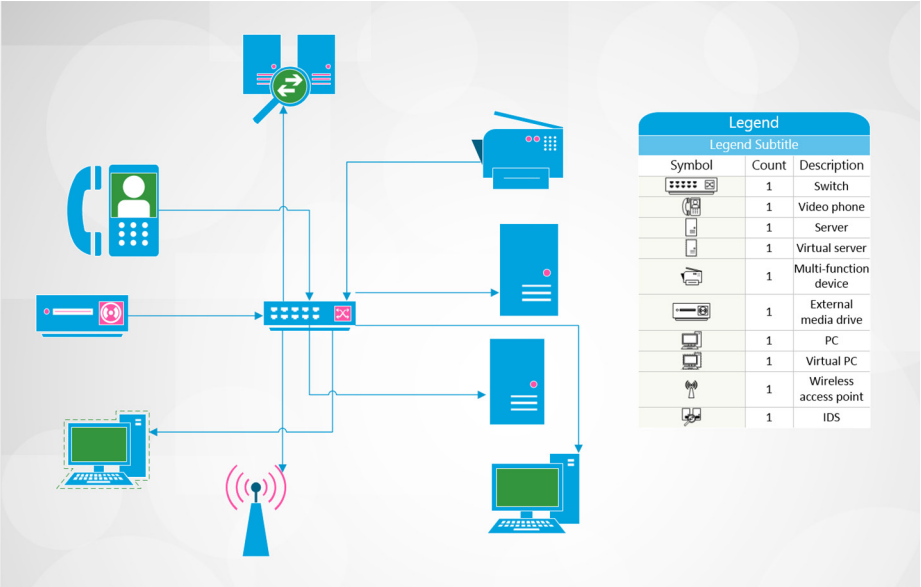
IDS

An Intrusion Detection Sensor (IDS) is a tool that most obviously detects things, but what things? Ultimately it could be anything, but thankfully most vendors include a large array of 'signatures' and or methods for detecting stuff. What do I want to detect? For each network this answer will vary, though generally it is looking for unusual traffic. What's unusual? In the simplest terms, it's traffic you don't want on your network, whether that is policy/misuse (IM, games, etc.) or the latest malware.

Just as they say in real estate: it's location, location, location. Not the location in the rack, but the segment of your network the IDS will monitor. Monitoring traffic at the ingress/egress point will show you what comes and goes (after the firewall policy approves of course), but may not allow you to see remote offices connecting to core components.

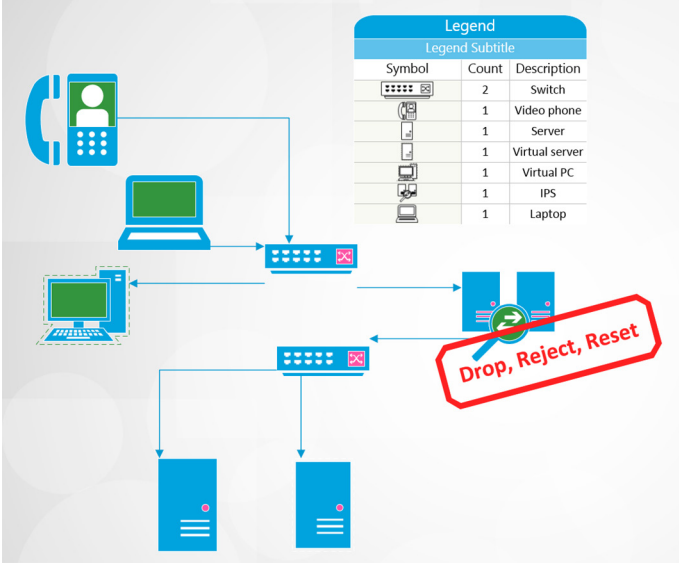
One thing you don't want to do is inspect traffic on the public side of the firewall. Monitoring all of the traffic on an internal switch, like your LAN or a DMZ, will allow the IDS to monitor user activity or key servers, but it won't see things happening on other parts of the network. Unless you have unlimited resources, you may not be able to monitor everything on the network, so a key decision will be which traffic matters the most and which segment provides the best vantage point.

IDS can passively monitor more than one segment and can monitor traffic that an IPS or UTM would never see, such as the traffic staying entirely within a LAN or DMZ. An IDS, therefore, could alert on a desktop machine attacking other desktop machines on the LAN, something the IPS or UTM would miss due to being inline.



IPS

An IPS (Intrusion Prevention Sensor) is an IDS in most regards, save for the fact it can take action inline on current traffic. This sounds amazing right? ...well almost. IPS and UTM, by their nature, must be inline and therefore can only see traffic entering and leaving an area. A huge concern is that an IPS can prevent business legitimate or revenue-generating traffic from occurring (an IPS, remember, can alter traffic flow). IPS actions include drop, reset, shun or custom-scripted actions and all of this occurs immediately upon signature match. This potentially negative action makes the person responsible for security now responsible for loss in revenue should the IPS drop legitimate traffic. In my experience, IPS devices make great tools as long as you also leverage the key components that differentiate the IPS.

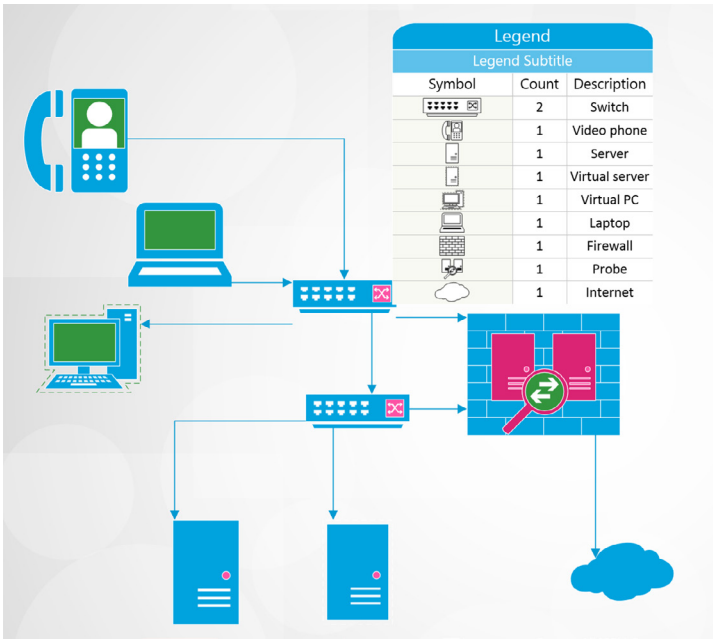


Make sure your IPS devices are capable of “failing open”; this means if any part of the application fails or even the chassis fails (power loss anyone?) the unit continues to pass traffic. No one wants a brick impeding the flow of data.

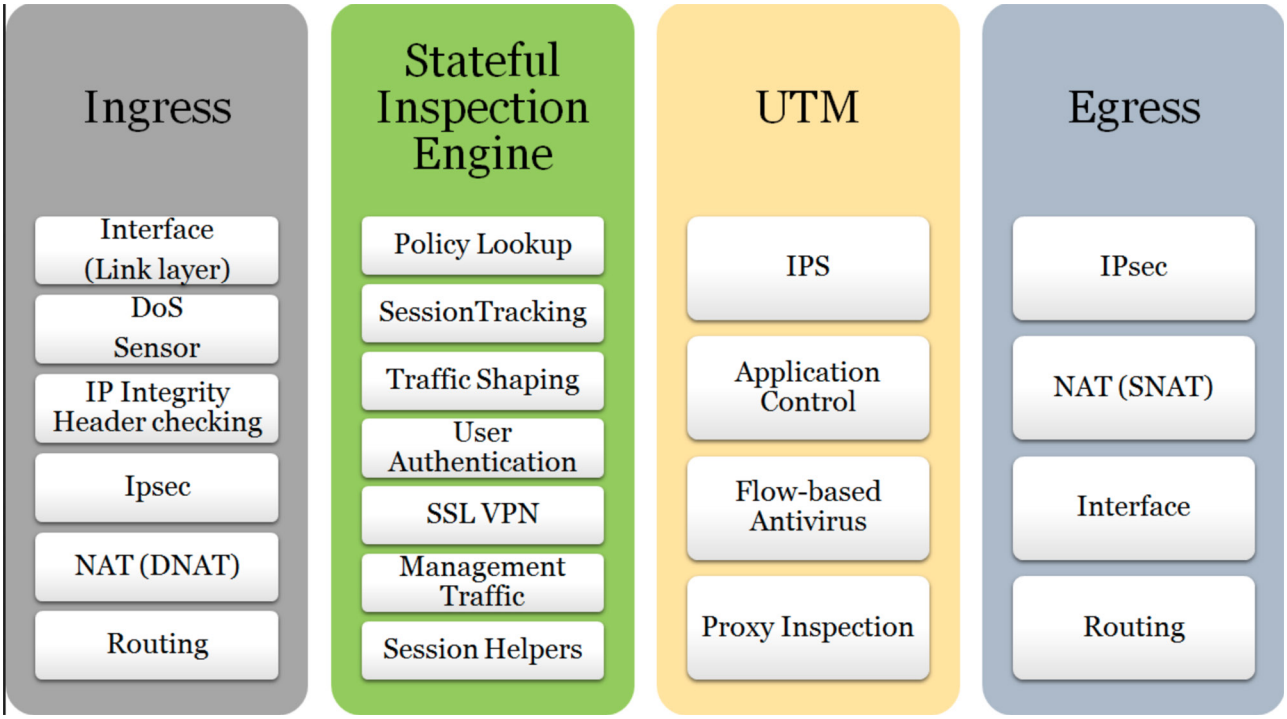
Also realize that only a small portion of the signatures that fire should actually be allowed to take action on traffic. To help reduce false positive rates, one should have very well defined home net or protected ranges allowing direction oriented signatures to be more effective. You will also need to spend quite a bit of time reviewing alarm and event output to ensure the signatures allowed to take action are working as intended. You can expect to spend more time up front and more time at each signature update looking at which signatures the vendor has chosen to take action and considering how that can impact your traffic. This often works best in settings where firewalls are not very favorably looked upon between “open” network segments.

Software Based Modules in UTM Devices

This brings us to software-based modules in Unified Threat Management (UTM) devices. Key items to point out about these devices happen to be drawbacks, though this does not reduce their efficacy. Obviously they can only be located where the UTM itself is located. Typically this is a junction point like your Internet gateway or an access control point between your LAN and DMZ. In this case a UTM would not be able to see all of the system-to-system traffic on the DMZ or LAN, rather only traffic coming and going from that segment.



In addition, UTMs are not purpose-built platforms, thus tending to have higher false positive rates (though this is getting better). In the case of high CPU or memory utilization, they will turn off software modules to preserve the primary function of the device, as a firewall. This is an important point related to not being a purpose-built platform and helps justify requests for dedicated devices. If all you have is a device like this, we say go for it! It is much better to have visibility in traffic coming and going from your network than to not have any IDS at all. Ask your vendor to validate that they logically inspect traffic after the firewall policy and make sure to notify yourself immediately should your device move in to conserve mode or consistently seeing high resource utilization.



So, in Summary, Comparing IDS, IPS and UTM

None of the three are “set it and forget it” devices. New malware and vectors for exploit and detection emerge daily. Regardless of your choice, you will have often recurring maintenance in signature event/alarm output and a need to update and manage your policies, especially in the case of IPS. Updates can be automatically applied in any of the devices discussed, but that does not absolve the need for human review. Set aside some time daily to check in on your device and consider turning off groups of signatures that have no role in your environment (think “policy based”) and tuning out other noise granularly.

Hopefully all the cautionary statements penned here don’t scare you off. Getting traffic inspection in your environment is a great way to get visibility into traffic on your network.

Ability by type	IDS	IPS	UTM Software module
Inspect	YES	YES	YES
Take Action (inline)	No	YES	Likely
Granular Tuning	YES	YES	Not Likely
Passively monitor multiple segments	YES	No	No

AlienVault Unified Security Management (USM): Accelerate Threat Detection with IDS plus a Complete Set of Security Controls

AlienVault USM delivers complete security visibility by integrating IDS with asset discovery, vulnerability assessment, SIEM and behavioral monitoring in one complete solution that can be up and running in under an hour.

The intrusion detection capabilities in AlienVault USM give you the ability to inspect traffic between devices, not just at the edge. You can also bring events from your existing IDS/IPS into AlienVault USM to benefit from the 1,800+ correlation directives developed and updated weekly by the AlienVault Labs threat research team.

Key Benefits of USM:

- **Reduced Noise:** Correlate IDS/IPS data with vulnerability and IP reputation data to reduce false positives
- **Full Threat Context:** See attack type, number of events, duration & source/destination IP addresses
- **Ticketing:** Create tickets from any alarm, delegate to users, or integrate with your ticketing system
- **Automatic Notifications:** Set up notifications via email or SMS

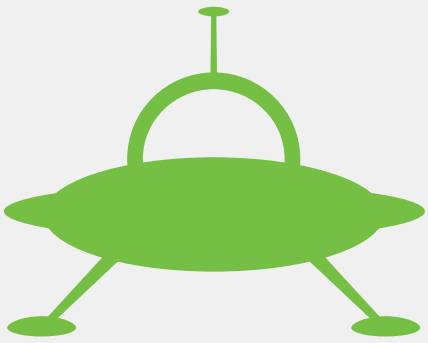
Next Steps:

- Learn more about IDS in AlienVault USM
- Download a free 30-day trial
- Watch a demo on-demand
- Play with USM in our product sandbox (no download required)

About the Author

Grant Leonard is a member of Castra Consulting, an AlienVault certified vendor and MSSP. The team at Castra Consulting regularly manages SIEM environments in global 24x7 scenarios. They pay close attention to the ever changing, dynamic world of the SIEM and devices by which the are fed. They build and manage SOC environments, convert NOC environments, and consistently allow companies to achieve full ROI with their security product suite.

Learn more about Castra Consulting



About AlienVault

AlienVault's mission is to enable organizations with limited resources to accelerate and simplify their ability to detect and respond to the growing landscape of cyber threats. Our Unified Security Management (USM) platform provides all of the essential security controls required for complete security visibility, and is designed to enable any IT or security practitioner to benefit from results on day one. Powered by threat intelligence from AlienVault Labs and the AlienVault Open Threat Exchange—the world's largest crowd-sourced threat intelligence network — AlienVault USM delivers a unified, simple and affordable solution for threat detection, incident response and compliance management. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, GGV Capital, Intel Capital, Sigma West, Adara Venture Partners, Top Tier Capital and Correlation Ventures. For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).