TECHNICAL DATASHEET

.

SecureIT- NETWORK INTRUSION PREVENTION SYSTEM

Why SecureIT- Network Intrusion Prevention System?

Starting off, a network intrusion prevention system (NIPS) is a type of network security software that detects malicious activity on a network, reports information about said activity, and takes steps to block or stop the activity from occurring automatically.

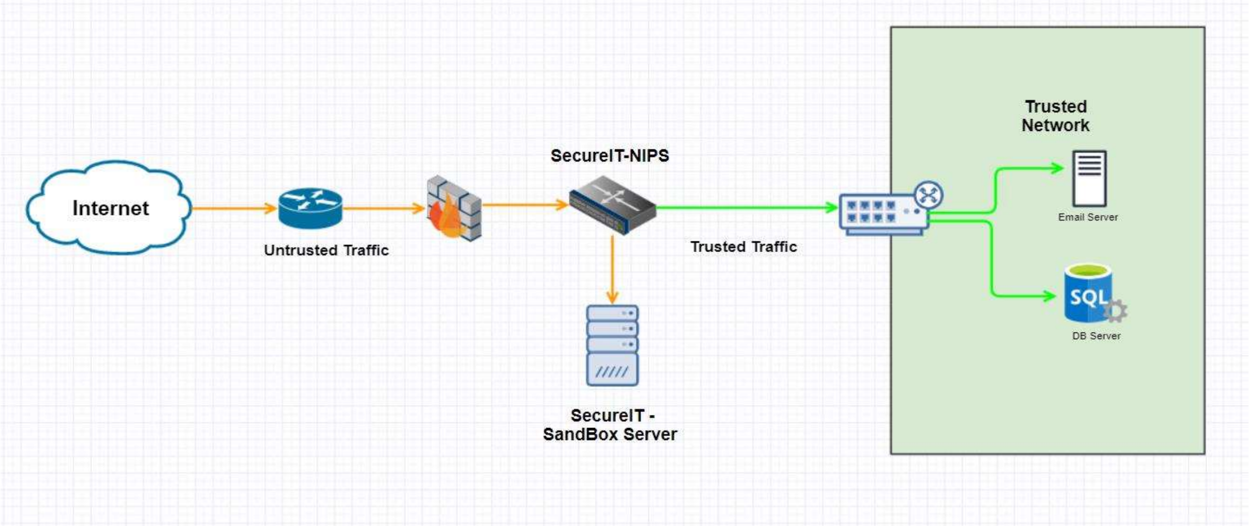
The NIPS lives within the network perimeter between the firewall and the router as a sort of checkpoint and enforcement point for network traffic passing through.

A network intrusion prevention systems use three types of intrusion detection:

- **Signature:** Detects attacks based on specific patterns, such as network traffic, number of bytes, and known previous attacks.
- **Anomaly:** Systems use machine learning to create a model of trustful activity and compare the current activity with it.
- **Policy:** Relies on predetermined network traffic baselines and activity outside of that baseline is seen as a potential threat to the network; requires a systems administrator to configure security policies manually.

Hardware for Network Intrusion Prevention System:-

How SecureIT Network Intrusion Prevention System works?



SecureIT- Network Intrusion Prevention System Features:

- Easy integration of a VA scanner to fine-tune the IPS (Supports OpenVAS , Nikto2,OWASP (ZAP) & Nexpose)
- Fallback option to bypass traffic events with the power on such as firmware corruption and memory errors.
- Integrates with TAP devices
- Intercepts and inspects SSL traffic for any malicious content without performance degradation.
- Protects & translates VLAN & inter-VLAN traffic.
- More than 15000 inbuilt signatures.
- Integrates with third party sandbox.
- Examines packets that are traveling through the network for known signs of intrusive activity.
- Asymmetric traffic environment with signatures/ filters protection
- Provides Security effectiveness report
- Latency <40 microseconds
- Bypass traffic in failover scenario
- Firmware and signature upgrade/reboot without requiring downtime.
- Machine learning
- Bypass traffic for IPS internal issues, i.e., memory hang, firmware crash, etc.
- Dashboard provides displays correlated data, such as the number of compromised hosts.
- Supports GTP inspection for GPRS/3G mobile.
- Supports SNMP v2, v3, and a private MIB
- Management for versioning, rollback, import and export (backup).
- Generates reports for all attacks, specific and top attacks, source, destination, misuse and abuse, and an advanced DDoS report for all attacks.
- Creates the reports in the following formats: PDF, HTML, CSV, XML, etc.
- Supports 80 GBPS real word throughput.

Benefits:

- Locally manage independently without any centralized management.
- This often eliminates the need to have a dedicated database or other means of providing long-term storage for IPS logs.
- Min.60 million legitimate concurrent Sessions/Concurrent connections scalable up to more.
- Provides Min. 300,000 new connections per second from day one which is scalable up to more.
- It gives security managers real-time security insight into their networks regardless of network growth.
- Easily configurable & maintains of hardware & virtual sensors