

Intelligent Threat Management (ITM) vs. UTM



First there was the “UTM” appliance. Now there is the Intelligent Threat Management “ITM” appliance. What are they? How are they the same? How are they different?

- **What is a Unified Threat Management Appliance (UTM)?**

“The Unified Threat Management (UTM) Security appliance transforms single function appliances into a more flexible environment for deploying multiple security features on a single platform”

Charles Kolodgy, Research Director for Security Products at IDC

You might say that Unified Threat Management is the evolution of the traditional Firewall into a Swiss Army product that not only guards against intrusion but performs content filtering, spam filtering, intrusion detection and anti virus duties traditionally handled by multiple systems. Each technology is independent of one another, acting independently, protecting independently, no interaction of technologies, no coordination, static. Separated security technologies housed on one appliance/

- **What is a Intelligent Threat Management Appliance (ITM)?**

The ITM security appliance is the next generation UTM. The security technologies in the ITM appliance, i.e. firewall, anti-spam, anti-virus, etc. work not only independently but in concert, communicating. In addition the ITM appliance takes security to a whole new level of sophistication and effectiveness. The ITM appliance also analyzes the shared knowledge and makes predictive decisions. Why is this important? The ITM appliance is able to effectively combat complex threats, i.e. blended threats, denial of service and rootkits. No other product on the market can do this. To add another level of protection each Barrier1 ITM appliance is monitored 24 x 7 with updates twice an hour.

- **What makes the Barrier1 Intelligent Threat Management Appliance (ITM) so effective?**

The Advanced Analysis Reaction Engine (AARE) is a proprietary element of the Barrier1 ITM security appliance. The AARE leverages the feeds from each of the technologies integrated in the Barrier1 appliance logging them into a common database of our design. Proprietary analytics performed utilizing this common database allows the Barrier1 device to make very accurate decisions regarding network traffic regardless of protocol or threat vector.

In all cases all network traffic must transit both firewall rules and routing tables serially, after which the traffic is passed to the appropriate inspection technology. This architecture allows the Barrier1 device to introduce only .211 milliseconds of latency to the network traffic which is critical to newer “real time” applications such as VOIP.

This combination of speed, analysis and reaction regardless of protocol or threat vector is what sets the Barrier1 ITM appliance apart from the old UTM appliances on the market today.

Examples of how the AARE leverages the individual technologies are listed below:

As packets enter the Barrier1 environment they are first validated against the Intrusion Detection System which is based on Snort rules. If a packet fails any of the IDS rules the source IP is blocked for a predefined time period and pertinent data about the failed packet is logged into the AARE event database. The AARE queries past events that have occurred in a specific timeframe to determine if the source IP address has been logged with any other events, if so the event is upgraded to the next higher priority level and blocked for that predetermined time period.

Packets that successfully pass the IDS rules are passed to the firewall element, which is based on IPTables. The packets are tested and acted upon based upon the firewall rules, any packets that drop through the firewall rules with no action are considered firewall events and logged to the AARE event database. These events are initially considered priority 2 events and the source IP is blocked for a predetermined time period. The AARE queries past events that have occurred in a specific timeframe to determine if the source IP address has been logged with any other events, if so the event is upgraded to a priority 1 event and blocked for the priority 1 time period.

Packets that successfully pass the IDS rules and firewall rules are passed to the appropriate service (i.e. e-mail packets are passed to the e-mail queue, requested web pages are passed to the web proxy).

E-mail packets passed to the e-mail queue which authenticates the recipient against the local network directory services to validate that the e-mail recipient is a valid network user, if the recipient is not a valid network user the e-mail is bounced back to the sender. If the recipient is a valid network user the message is tested against known virus definitions. If the e-mail is infected it is quarantined and the event is logged in the AARE event database. If three infected messages are received from the same source IP within a one minute time period the source IP is flagged with a priority 3 event and blocked for a predetermined period of time. The AARE queries past events that have occurred in a specific timeframe to determine if the source IP address has been logged with any other events, if so the event is upgraded to the next higher level event and blocked for that predetermined period of time. Packets that pass the virus scan are passed to the anti-spam system and tested against the anti-spam rules and handled according to the anti-spam rules. If the packet passes the anti-virus and anti-spam rules it is then passed to the target mail server for delivery.

The AARE is engineered in a fashion that performs these activities with very high throughputs while introducing only 211 microseconds of latency in traffic flow. The higher level analytics built into the AARE enable the Barrier1 to correlate the disparate data captured by each of the technologies and leverage the events to holistically provide better protection to the customer's network.