



A sentinel on the system

Intrusion detection is important for any system, and is becoming increasingly so as cyber threats grow more sophisticated. Most intrusion detection devices are placed at the periphery of the network; Sentiariant from Extreme Networking sits at the centre of the system. Colin Campbell explains why this is a far more effective place to be

Business brief

There is hardly a need to make a business case for network security. Any business with an IT system – and that means just about every business – needs to make that system secure against attack. A firewall goes part way to protecting the system: it blocks obvious intrusions and unexpected traffic types; it controls access to the network, but does little to signal an attack or protect against attacks from the inside of the network.

“Threats can come just as easily by more surreptitious routes”

An intrusion detection system (IDS) goes further than this. Its purpose is to inspect all traffic that passes through it and to identify suspicious patterns that might indicate attack. It evaluates a suspected intrusion and then signals an alarm. Moreover, it watches for attacks that originate from anywhere within a system.

It is important to make this distinction between firewalls and intrusion detection systems, because threats are not only from the outside.

Threats can come just as easily by more surreptitious routes, from the inside, from within the office environment, via uploads from an MP3 player, or a mobile device. A homeworke’s PC or laptop can easily become infected with malware – this can happen by opening one infected email, or making a single visit to an innocent-looking but malicious website. If that infected laptop or phone is then connected to the office network, the whole business network becomes infected.

Anti-virus software can only defend against known malware, and does little to protect against new forms of attack. Anti-virus heuristics go some way towards stopping a small proportion of day zero attacks but in reality are often ineffective.

Unethical hackers are being recruited for the targeted theft of information either directly by organised crime or by unscrupulous competitors. Conventional network

security measures are having to become increasingly complex and expensive just to keep pace with the increased levels of risk.

Traditional IDS appliances have a number of limitations. They can become a network performance bottleneck (like a police road block). IDS appliances can only monitor traffic that actually travels through that point on the network and multiple probes or devices need to be deployed throughout the network.

Sentriant and CLEAR-Flow

Unlike traditional networking products whose security resources are proprietary and closed, Extreme Networks uses an open-networking approach. The Sentriant appliance is aimed at securing the inside of the network against rapidly propagating and unknown attacks. It will sit in any network to monitor network traffic, and differs from other intrusion detection devices in that it looks for all anomalous behaviour and not just for known signatures. It identifies unusual behaviour as a threat, and instructs the network to take remedial action.

The Sentriant appliance also takes this a step further: when used in conjunction with the Extreme Network Security Rules Engine, CLEAR-Flow, it monitors the network out-of-band. It talks to every device on the network without taking up any bandwidth on the network, so does not create bottlenecks. It therefore does not limit network performance, which is especially critical when the network is under attack. CLEAR-Flow gives the IDS appliance a 1000-mile view of the network without the need for multiple probes or devices.

When CLEAR-Flow detects suspicious traffic, it mirrors only the threatening traffic to Sentriant for a closer look. Based on the results, Sentriant directs the core switch to take specific action to mitigate the threat. This strategy enables the Sentriant appliance to provide detailed packet inspection for the entire network without affecting performance.

Sentriant can insert itself between one or more attackers and one or more target devices by redirecting communications streams from attackers to itself. It can then selectively pass or drop packets based on their threat potential, isolating infected computers while permitting all other communication to flow normally on a network.

In the mid-90s, Computer Associates came up with an analogy that likened a firewall to a door access system and an IDS appliance to a burglar alarm.



Sentriant can insert itself between one or more attackers and one or more target devices

“The complexity, unpredictability and increased level of security threats, combined with today’s multi-gigabit networks and high availability requirements, make securing a network both overwhelming and costly,” said Paul O’Kelly. “Customers would do well to draw on the experience of an integrator like Dynax when implementing a project of this nature.”

The Dynax contribution

Colin Campbell of Dynax is the man to contact when it comes to intrusion detection. As he says, “The edge of the network is very well defended. Now the biggest threat is coming from inside the network, and this is where Sentriant can help. We’ve chosen to go with a unique solution, rather than a more mainstream approach.”

Dynax can take Sentriant to a customer’s facilities and leave it in place for a month, to show them how many threats they have had, from inside and from outside.