

Distributed Intrusion Prevention System

Patented Technology Automatically Senses and Responds to Threats in Real-Time

Extending IPS Protection to Every Edge Access Port

Traditional IPS and firewalls fall short of providing effective threat containment and can expose the enterprise to unacceptable levels of risk. As the majority of threats now originate from inside the organization rather than outside, security needs to be everywhere, rather than just at select perimeter locations. Network access layer threats can come from malicious employees; however, the more likely scenario is compromised end systems accidentally infected with malware. In either case, the best practice response to a threat must include containing or removing the source of the attack. An IPS can stop an attack from reaching its target but it leaves the source of the attack connected to the network, free to attempt another attack against another target. Firewalls offer threat containment for attacks originating from the Internet but offer no help for the 80% of all threats that originate from the network access edge.

“Assume an attacker has penetrated a network and corrupted some hosts. The ideal response gathers evidence of the attacker’s activity, removes the attacker’s access to the network, undoes the damage, and reconfigures the network to resist the attacker’s penetration technique.”

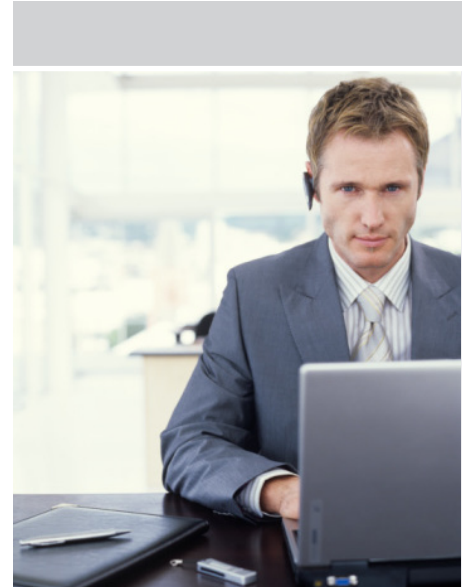
NIST Interim Report (IR) – 6416

In order to meet the National Institute of Science and Technology (NIST) recommendation, the IPS must detect the attack, mitigate or stop the attack and, most importantly, it must contain or remove the source of the threat. The simplest and most effective way to do this is to remove the source of the attack’s access to the network and to reconfigure the network to prevent future access. Traditional solutions fail to provide these critical location, containment, and removal capabilities.

Enterasys® patented Distributed Intrusion Prevention System is the industry’s first comprehensive IPS solution to cost-effectively address real-world operational requirements. It provides the highest level of protection by:

- Identifying a threat or security event
- Mitigating the attack by dropping the attack packet
- Reporting the details of the attack
- Locating the exact physical source of the attack
- Containing the threat by removing the source from the network

Threat containment is accomplished through the use of enforceable security policies, quarantine policies, or port level controls in multi-vendor networks. After isolating the threat to its source, the Distributed Intrusion Prevention System provides the option of several different pre-defined actions to contain the threat. Port-level control (on/off), specific quarantine policy rules (VLAN/ACL), time-based policy enforcement, bandwidth restriction, and notification are examples of actions that can be taken against the threat. By enforcing security policy at both the point of detection (intrusion prevention) and at the attacker’s ingress port (threat containment), the enterprise is protected from the current threat and from future threats by the malicious or accidental attacker.



Benefits

Patented technology uniquely protects from internal and external threats

- Detects and stops the attack
- Removes the source of the attack
- Seamlessly protects LAN and WLAN

Stronger security at lower cost

- Automated system and fewer required devices saves OPEX
- Superior 3rd party interoperability saves CAPEX

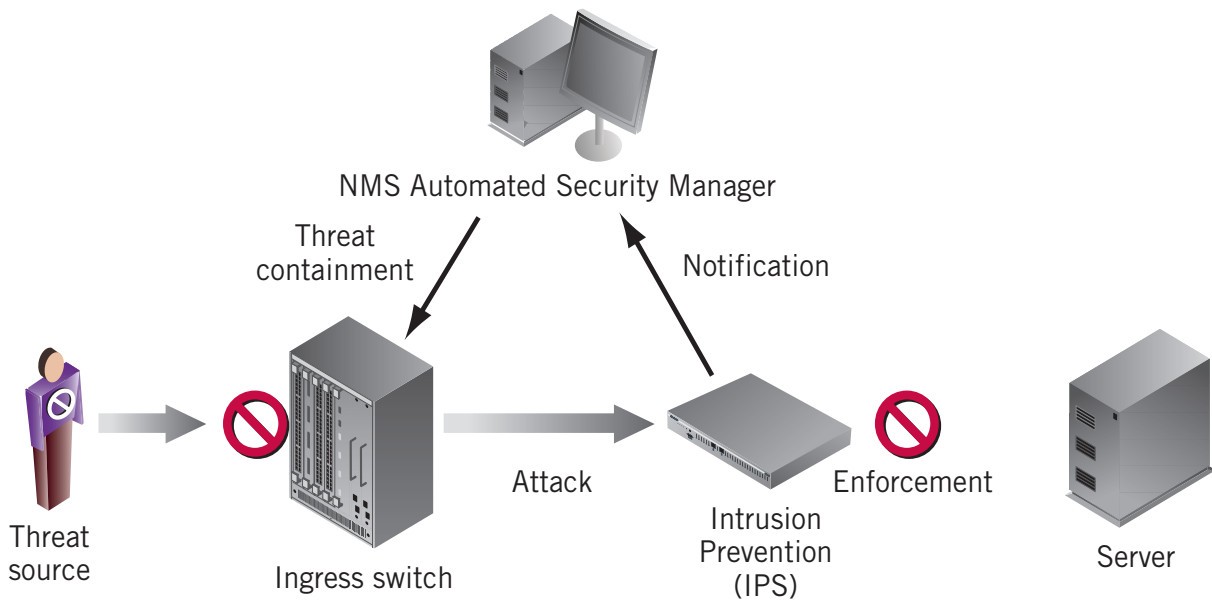
Minimizes damage to critical assets

- Faster response means less damage to critical assets
- Threat containment minimizes asset down time

Enables IT staff to respond to threats in real-time

- Provides staff with suggested action
- Enables “lights out” automated response

**There is nothing more important
than our customers.**



In the above diagram, Enterasys IPS detects the attack and enforces the security policy by dropping the attack packet. The IPS then notifies Enterasys NMS Automated Security Manager of the attack. Based on its configured rules, NMS Automated Security Manager locates the ingress (source) port of the attack and triggers an action to contain the threat. Depending on the capabilities of the ingress switch the action can range from triggering a policy (for Enterasys policy enabled switches), assigning packets to a quarantine VLAN (for RFC 3580 compliant switches) or turning off the port (for MIB II compliant switches).

The protection of the Enterasys Distributed Intrusion Prevention System can be further strengthened by incorporating other Enterasys Advanced Security Applications into the solution. Enterasys Security Information & Event Manager (SIEM) provides additional visibility for any abnormal network behavior. Enterasys NAC integration enables blacklisting of user/MAC addresses.

Because the Enterasys Distributed Intrusion Prevention System is fully automated, the time it takes to identify an event, drop the threat packet, isolate the source, and take action is significantly reduced over current manual and segmented processes. When dealing with fast-propagating threats to the enterprise like malware, time is of the essence. It is imperative to react quickly and effectively in mitigating a threat to prevent critical business processes from being impacted, ensure continuity of operations and reduce overall risk to the business.

Deploying the Enterasys Distributed Intrusion Prevention System reduces the exposure of IT resources to internal and external threats due to targeted business disruptions, opportunistic predators, or accidental malware infections. The Enterasys Distributed Intrusion Prevention System effectively leverages existing multi-vendor network infrastructure investments. The embedded security features proactively address security exposures, and the Distributed Intrusion Prevention System complements already deployed security appliances without requiring reconfigurations or disruption to networked users.

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2010 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

