

Product Name:

PAETEC's Intrusion Detection and Prevention System (IDPS).

Product Availability:

IDPS is available nationwide.

Product Requirements:

IDPS requires customers to subscribe to the PAETEC Network Firewall service and to have a hub and 60% of its locations on the PAETEC network.

CPE Requirements:

IDPS is an MPLS cloud-based security solution that does not require any additional CPE.

Intrusion Detection and Prevention System (IDPS) | In Brief

Product Description

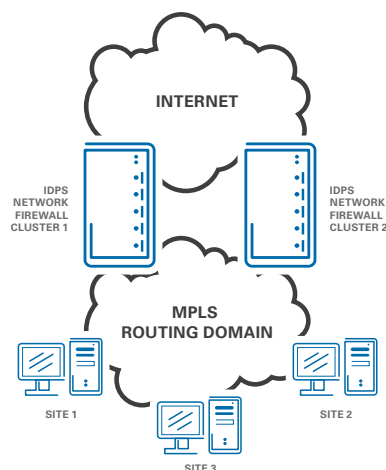
A firewall actively blocks and allows information to and from sources inside and outside a data network, but it does not detect new types of threats that could originate from an allowed source. A system must be in place that is smart enough to recognize malicious activity regardless of the source and stop it in its tracks. The Intrusion Detection and Prevention System (IDPS) identifies and prevents misuse of network resources by examining packets using sensors within the network infrastructure. By analyzing the content and correlating packet transmissions as individual events, the IDPS can identify malicious activity such as propagation of malware, port scans, software vulnerability exploitations, denial of service attacks, and other dangerous activities that normally go undetected by even the most advanced firewall systems.

PAETEC's IDPS consists of a set of quadruple-redundant, geographically diverse Intrusion Prevention Sensors (IPS) in line with PAETEC's Network Firewall located at each of PAETEC's eight major Internet peering points. A centralized, redundant event correlation engine retrieves information from the IPS, correlates the information, and alerts the PAETEC Security Operations Center, which actively monitors the IDPS service 24 x 7 x 365.

If a potentially negative event is detected, the IPS and the event correlation engine determine the threat level of the event based on customer-defined constraints, known intrusion signatures, and the ever-evolving event correlation database and act accordingly within a 99.9999% Service Level Agreement (SLA) guarding against false positives. The IDPS then opens an alarm ticket in the Security Operations Center, while simultaneously e-mailing the customer with the alarm details and an estimated time within which the Security Operations Center will contact the customer to begin remediation discussions.

Product Capabilities

PAETEC's IDPS acts as both an IPS and an Intrusion Detection System (IDS) to provide the most robust network protection available. Since IDPS resides within PAETEC's MPLS network, there is no need for on-site equipment installation or upgrades and the product protects all sites on the network, not just one.



Why an Intrusion Detection and Prevention System?

- Thwart attacks on your network
- Alert a network administrator of possible security events
- Help meet compliance regulations
- Enforce network security policies
- Limit non-business IM and video streaming
- Better understand network activity
- Learn what applications users have installed on the network
- Build trust with partners
- Save time and money

Application One

A large, regional bank, in business for almost 150 years, took advantage of the PAETEC Network Firewall to provide stateful firewall protection and geographically diverse and redundant Internet connectivity to all locations on their network. Furthermore, due to the tight constraints imposed on the banking industry from PCI DSS and Graham-Leach Bliley, the bank added PAETEC's industry-leading Intrusion Detection and Prevention System (IDPS) to provide the most secure network protection available.

With the combination of Network Firewall and IDPS, the bank has been able to easily meet the compliance standards imposed by PCI DSS and GLBA, implement a robust business continuity plan for its award-winning Web site, and gain peace of mind knowing that their network and resources are protected to the highest extent and monitored constantly by a dedicated group of PAETEC Security Engineers.

Application Two

As a result of tightening HIPAA standards, an award-winning healthcare provider in the Southeast, offering the very latest lasers, surgical, and diagnostic equipment, needed a business continuity plan with a close relationship to their network and information security strategy.

PAETEC Network Firewall with IDPS was not only able to provide a comprehensive business continuity and disaster recovery option, but was also able to easily exceed the stringent network security constraints required by HIPAA for compliance. HIPAA auditors are also able to continuously utilize the Security Operations Center as a resource in guaranteeing compliance while freeing up the eye care center's IT staff for day-to-day business operations.