



Product Overview

Intrusion Detection and Prevention System (IDPS)

Common Applications:

- Multi-location MPLS networks with Internet access and security needs
- Industry security compliance
- Visibility over network activity

Compliance Requirements:

- Industry standards such as PCI DSS and HIPAA require Intrusion Detection and Intrusion Prevention Systems
- Security Operations Center is equipped to consult with PAETEC customers to assist in compliance

What is an Intrusion Detection and Prevention System?

PAETEC's Intrusion Detection and Prevention System (IDPS) is a feature of the PAETEC Network Firewall product and consists of two key components:

An **intrusion detection system (ids)** inspects all inbound and outbound traffic and identifies suspicious patterns that may indicate a network or system attack. The system then notifies administrators of the suspicious activity and offers threat remediation suggestions.

intrusion prevention sensors (ips) rely on a preemptive approach to identify potential threats and respond to them swiftly. Like an IDS, IPS monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action.

By combining the monitoring and detecting components of IDS with the reactive, zero-hour components of IPS, PAETEC has been able to create one of the most robust intrusion protection services available. If a potentially negative event is detected, the IPS and 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 acts accordingly within a 99.9999% Service Level Agreement (SLA) guarding against false positives.

The IDPS then opens an alarm ticket in the 24 x 7 x 365 Security Operations Center, while simultaneously e-mailing the customer with the alarm details and an estimated time within which the Center will contact the customer to begin remediation discussions.

Key Facts:

- Requires PAETEC's Network Firewall
- Quadruple-redundant and both locally and geographically diverse
- Real-time monitoring and alarming with automated e-mail notifications
- 99.9999% protection against false positives
- Zero-hour protection
- Intrusion Detection System (IDS)
- Intrusion Prevention Sensors (IPS)
- Extensive reporting and logging information available through PAETEC Online
- Automated patching and updating

Product Features & Benefits:

As with Network Firewall, IDPS resides within PAETEC's MPLS network so there is no need for on-site equipment installation or upgrades and the product protects all sites on the network, not just one. All this helps relieve the burden of costly equipment purchases.

Simply sign up and enjoy the peace of mind that comes with proactively monitored, zero-hour, quadruple-redundant, geographically diverse security protection for your entire network.