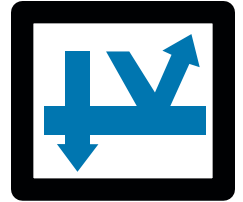




## Intrusion Prevention



### Features at a glance:

- Inbound and Outbound Scanning
- Automated Adjustment for False Positives
- Real-Time Logging and Reporting
- Automatic Classification of New IPS Rules
- Granular Control of Rules and Actions
- Automatic Tuning with Initial Configuration
- Wide Array of Protected Applications
- Dynamic Blocking of Attacks
- Automatically Updated Signature Database
- Zero-Day Updates
- Passive Monitoring Option
- Preview Changes to Rule Sets
- Detailed Threat Information
- Email Alerts

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★☆
<b>OVERALL RATING</b>	<b>★★★★★</b>



### Intrusion Prevention Service (IPS)

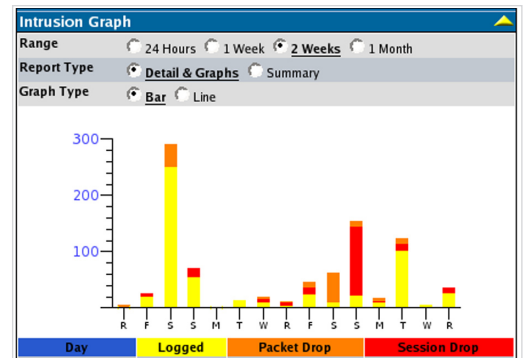
Automatically detect and block malicious network intrusions, Worms and Trojans that occur at the network and application layers. In addition, policy controls allow administrators to block Instant Messaging (IM) and Peer-to-Peer (P2P) applications. Intrusion Prevention blocks attacks in real-time, logs the attack for reporting or regulation requirements and notifies the administrator by email if further action is required. Signature updates are automatically downloaded to ensure protection from the latest threats. Intrusion Prevention is critical for IT managers trying to provide complete network and application protection.

### Key Features

Protect the network from a wide array of application level attacks targeting services such as web, FTP, email, IM/P2P and database/storage. IPS uses deep packet inspection to scan network traffic for worms, Trojans and application vulnerabilities such as browser vulnerabilities, buffer overflows, site cross-scripting, back-door exploits and SQL injection. IPS can detect active attacks in real-time and block them before they can do damage on the network.

Intrusion Prevention also monitors outbound traffic to identify and block backdoor exploits and infected computers. Policy controls are created to block access to Instant Messaging and Peer-to-Peer applications that create security risks, lower productivity, and waste bandwidth.

Logging and reporting allows the administrator to view information by the threat, severity, source or destination address and port, or network protocol. Statistical graphs and top threat views give administrators a quick view of items that need attention. Email alerts notify administrators for high priority threats.



Graphical statistics and reports.

Action Profile	Action	Move
High Priority Attacks	Log + Drop Connection	↓
Possible Breach	Log + Drop Connection	↑ ↓
Attempted Intrusion	Log + Drop Connection	↑ ↓
Attempted Denial of Service	Log + Drop Connection	↑ ↓
Policy: Peer To Peer Traffic	Log + Drop Connection	↑ ↓
Policy: Instant Messenger Traffic	Log + Drop Connection	↑ ↓
Unusual Traffic	Log + Drop Packet	↑ ↓
Reconnaissance	Log + Drop Packet	↑
Disabled Rules	Ignore	—

Action Profiles automatically classify new threats for real-time protection.

**The Intrusion Prevention SoftPak makes it easy for IT managers to enforce policies regarding the use of Instant Messaging and Peer-to-Peer applications.**

### Administration Features

Simple first-time configuration and automatic thresholds for false positives give IT managers a secure network environment without the high overhead associated with many IDS/IPS systems. Quick tuning through the web based administration tool allows administrators to protect their network in just a few minutes. eSoft's Threat Prevention Team classifies each new rule so that when it is deployed to your eSoft appliance it can automatically be associated with a profile and assigned appropriate actions.

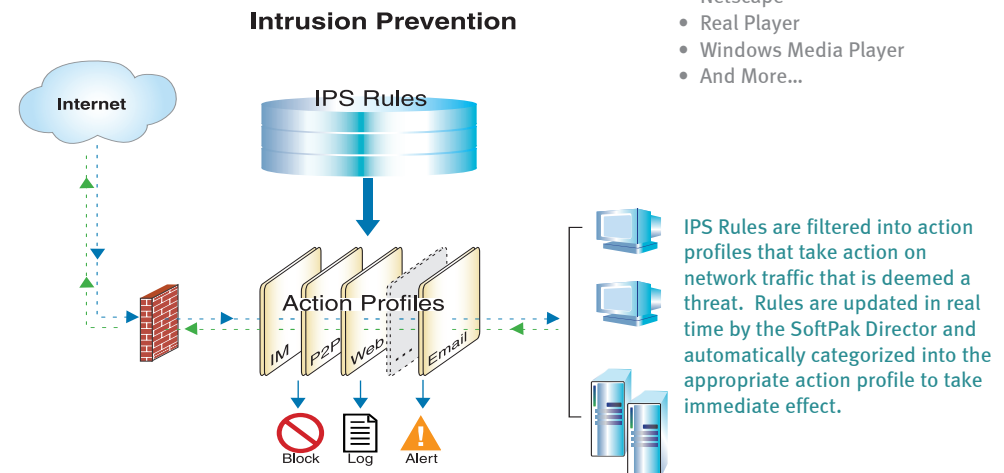
Custom rule configurations and action profiles may be set at a granular level, making it ideal for even complex network environments. Several criteria are applied to every Action Profile so that administrators can fine tune rules and actions that will be used to analyze traffic and automatically take action on threats.

#### Blocked Threats

- Intrusion Attempts
- IM and Peer-to-Peer Policy Violations
- Worms
- Trojans
- Backdoor Exploits
- Buffer Overflows
- SQL Injection
- Denial of Service (DoS) Attacks

#### Protected Applications

- Microsoft IIS
- Apache
- MS Exchange
- Sendmail
- Chat/IM
- Peer-to-Peer (P2P)
- Internet Explorer
- Firefox
- Netscape
- Real Player
- Windows Media Player
- And More...



### Part Numbers

Intrusion Prevention	1-Year Subscriptions
InstaGate 404	IG404-IPS-1
InstaGate 604	IG604-IPS-1
InstaGate 806	IG806-IPS-1
ThreatWall 250	TW250-IPS-1
ThreatWall 450	TW450-IPS-1
ThreatWall 650	TW650-IPS-1

### Features and Specifications

	InstaGate	ThreatWall
Inbound / Outbound Scanning	✓	✓
Proactive Blocking of Threats	✓	✓
Zero-day Updates	✓	✓
Large Signature Database	✓	✓
Simple First-time Configuration	✓	✓
Broad OS & App Support	✓	✓
Block IM & P2P Applications	✓	✓
Passive Monitoring	✓	✓
Automatic Rule Classification	✓	✓
Threat Research & Analysis Tools	✓	✓
Low False Positives	✓	✓
Preview the Result of Changes	✓	✓
Real-time Reporting & Logs	✓	✓
Email Notifications	✓	✓