Cisco IPS Intelligent Detection Technology

Internet connectivity is both a business requirement and a business risk. Today's Internet is an increasingly hostile environment. Without effective and up-to-date protection, businesses can be exposed to a wide variety of attacks, from targeted espionage to data theft to denial of service. Cisco IPS **intelligent** detection technology is a core component of Cisco's intrusion prevention system (IPS) solution portfolio, providing continuously updated, proven protection to keep your business safe.

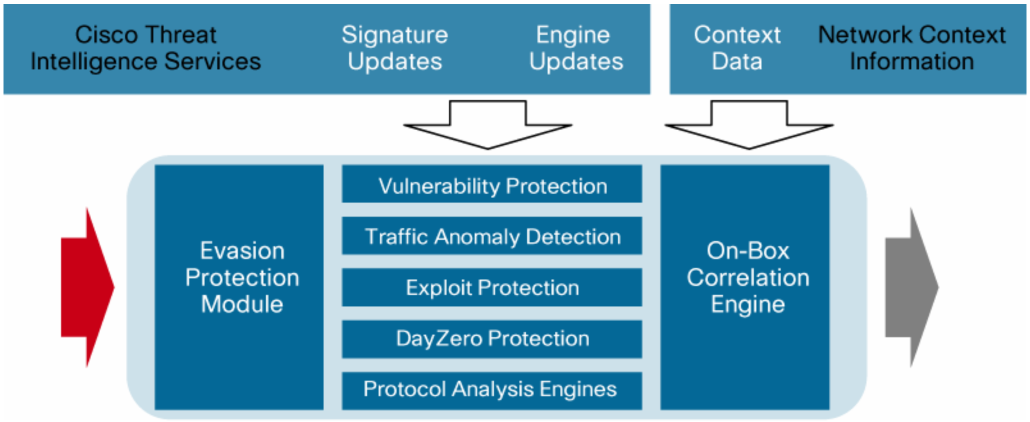
Product Overview

Cisco's uniquely effective intelligent detection technology provides unsurpassed detection capabilities for Cisco intrusion prevention solutions. Using information gathered by Cisco's global security intelligence organization and enabled by industry-leading technology and patented innovations, Cisco intrusion prevention solutions adapt in real time to detect and block intrusions ranging from never-before-seen worms to the most sophisticated and subtle criminal attacks. Innovations include the flexible, multilayer evasion protection module, vulnerability-focused signatures, dynamically updated protocol analysis engines, and on-box correlation capabilities that provide protection you can trust. For complete business application protection, Cisco's IPS Application Protection Packages provide focused and comprehensive detection capabilities for specific business applications such as Cisco Unified CallManager.

Superior Detection of Network Intrusions and Attacks

The intelligent detection capabilities in Cisco threat analysis and mitigation engines are based on 15 years of innovation, providing deep protection from known and unknown attacks such as fast-moving worms that overwhelm networks in minutes; stealthy botnets that proliferate global spam, phishing and distributed denial of service (DDoS) threats; targeted intrusions; day-zero attacks; and opportunistic attacks using automated exploit tools that easily slice through traditional network protections. Figure 1 shows components of the Cisco IPS Intelligent Detection architecture.

Figure 1. Cisco IPS Intelligent Detection Architecture


Cisco Threat Intelligence Services
Signature Updates
Engine Updates
Context Data
Network Context Information
Evasion Protection Module
Vulnerability Protection
Traffic Anomaly Detection
Exploit Protection
DayZero Protection
Protocol Analysis Engines
On-Box Correlation Engine

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- **Flexible evasion protection module** blocks hundreds of sophisticated evasions and attacks that attempt to exploit complexities in network and application protocols, including attacks designed to slip past hardware-accelerated IPS implementations.
- **Vulnerability-based protection approach** and sophisticated protocol engines provide tested protection against tens of thousands of known exploits and hundreds of thousands of potential unknown exploit variants with only a few thousand signatures.
- **Traffic anomaly detection** capabilities provide early warnings of changes in network behavior that can indicate worm activity, a DoS attack, reconnaissance, or other intrusions.
- **Day-zero protections** are central to the Cisco IPS architecture. These include vulnerability-focused signatures to provide protection from day-zero exploits, and protocol anomaly detectors that provide protection from undiscovered vulnerabilities. This day-zero technology protected Cisco IPS customers from exploits for the Microsoft Windows animated cursor vulnerability two years prior to the discovery of that specific vulnerability, and from the 2007 ICMP multicast vulnerability a full five years prior to discovery. And these capabilities provide protection without creating additional risk for the security community, a risk inherent in the controversial practice of providing IPS signatures for specific undisclosed vulnerabilities.
- **Protocol analysis engines** provide a framework for sophisticated inspection and analysis capabilities that, unlike hardware-based engines, can be dynamically updated to reflect changes and enhancements to network protocols as easily as a signature update. Cisco's universal engine technology takes this a step further, enabling deep, stateful analysis of virtually any network protocol. This enables the Cisco IPS team to rapidly create effective vulnerability-based signatures for new exploits and vulnerabilities, regardless of the underlying protocol.
- **On-box local event correlation technology** not only enables detection, but actually blocks multi-event attacks and malware in real time, complementing security incident management software such as the Cisco Security Monitoring, Analysis, and Reporting System (Cisco Security MARS) that correlate events across multiple devices. For example, Cisco's VNC Authentication Bypass sequence analyzes three distinct events and can take action to block access when the final attack event is detected, protecting the server from compromise.

Focused and Rapid Protection Technology Updates

Cisco's Global Security Intelligence Team comprises security experts from around the world that work together internally and through partnerships with vulnerability research groups, vendors, critical industry response centers, and incident response teams globally to understand, document, and protect customers from network security threats to individuals, corporations, organizations, utilities, and government organizations.

Cisco's Global Security Intelligence Team works around the clock to quickly discover and analyze new threats and vulnerabilities before they become widespread and dangerous. Cisco IPS customers rely on the continuous, rapid development, testing, and deployment of detection and proactive protection technologies created by the Cisco IPS Signature Team to provide up-to-the-minute protection for their vital business assets. And to ensure the effectiveness of those protections, the IPS Signature Team continuously tests existing and new protections against a constantly growing library of more than 25,000 exploits. Cisco's real-world testing partners ensure that new protections target only those vulnerabilities and exploits for which they are designed.

Table 1 lists the Cisco IPS Signature Team's average signature release times.

Table 1. Average Signature Release Times

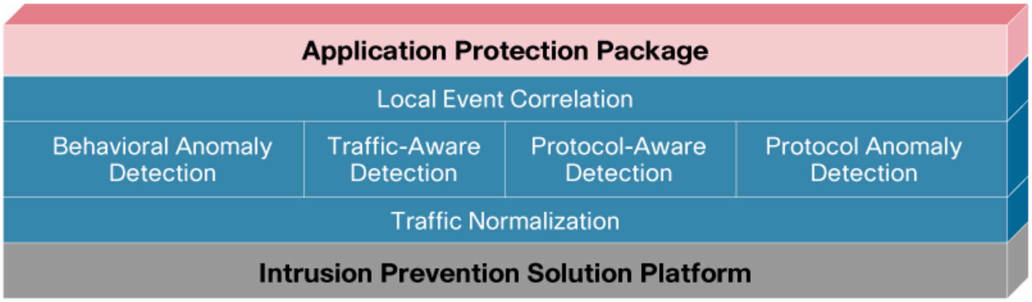
Feature	Description
3 Hours	Average response time to provide protection updates for Microsoft Windows Patch Tuesday vulnerabilities
8 Hours	Average response time to provide protection updates for critical vulnerabilities
24 Hours	Average response time to provide protection updates for urgent vulnerabilities

Cisco offers industry-leading average response times for signature update releases. But for high-priority scheduled or critical security events such as Microsoft Patch Tuesday, a critical vulnerability release, or a new, fast-moving worm, the entire Cisco security intelligence community mobilizes to provide up-to-the-minute information and updates that customers need to quickly and effectively contain and mitigate threats. In addition to IPS signature updates, Cisco Global Security Intelligence issues IntelliShield Applied Mitigation documents that give detailed mitigation information using Cisco products, and IntelliShield alerts that provide extensive detail on new vulnerabilities. The Cisco Security Center Event Response Website acts as the command center for new security events within hours of the occurrence.

Comprehensive Application Protection Packages

Your security solution is not just a product; it is a set of well-defined policies, well-understood processes, a well-trained team of people, and a broad, integrated set of products. This is a core principle of the Cisco Self-Defending Network. And like the Cisco Self-Defending Network, your business applications include hardware platforms, operating systems, applications, protocols, internal and external policies, access methods and more. Figure 2 illustrates the protection components of an Application Protection Package.

Figure 2. Cisco IPS Application Protection Package


Application Protection Package
Local Event Correlation
Behavioral Anomaly Detection
Traffic-Aware Detection
Protocol-Aware Detection
Protocol Anomaly Detection
Traffic Normalization
Intrusion Prevention Solution Platform

IPS Application Protection Packages help secure your business applications. The Cisco Secure Unified CallManager IPS Protection Package provides complete end-to-end protection, with protection for hard and soft phones, Cisco Unified CallManager applications, voice gateways, voice protocols, and underlying operating systems. When combined with Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Security Agent's host-based intrusion prevention, Cisco provides the most complete call manager protection available anywhere.

Table 2 lists some of the features of Cisco IPS intelligent detection technology.

All contents are Copyright © 1992–2008 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Table 2. Cisco IPS Intelligent Detection Technology Features

Feature	Description
Detection Technologies	• Protocol anomaly detection • Statistical anomaly detection • Application anomaly detection • Statistical analysis • Evasion protection • Vulnerability-based signature detection (>97%) • Exploit-based signature detection (<3%) • Session normalization and evasion detection • On-box event correlation
Day-zero Protection	• Unknown exploit variant protection • Unknown exploit protection • Unknown vulnerability protection (H.323, SIP, SNMP, HTTP, FTP) • Day-zero worm protection
Tunneling Protocol Detection Support	GRE, IP-in-IP, MPLS, and IPv6.
Statistical Analysis-Based DoS Attack Protection	Fully automated DDoS and DoS anomaly recognition and mitigation options with automatic threshold configuration.
On-Box Correlation	Cisco IPSs correlate multiple events across time and protocols.
Evasion Protection	Evasion protection module stops attacks that use evasion techniques specially designed to circumvent IPS protection. The module supports RPC fragmentation handling and UTF-encoding transformations.
Vulnerability-Focused Protection	Cisco IPSs use a combination of vulnerability- and exploit-based signatures to provide superior protection when compared to systems that are solely exploit-based. Cisco IPSs protect against single attacks with many signatures, as well as detecting protocol anomalies.
Exploit-Focused Protection	Cisco IPSs include signatures for specific exploits, such as select high-severity file-based, Trojan, spyware, and virus attacks.
Advanced Statistical Analysis Methods	Sophisticated anomaly engine identifies normal traffic thresholds and takes action when those thresholds are exceeded.
Custom Signature Definition	Built-in custom signature wizard includes the ability to add, copy, and modify existing signatures.
Wide Variety of Network Protocols	Supported network protocols include IP, TCP, UDP, ICMP, NetBIOS/SMB, MPLS, ARP, 801.1q, IPv6 encapsulated IPv4, IGMP), IP-in-IP, and GRE. Cisco IPS Sensor Software Version 5.1 also inspects protocols to protect SCADA networks; Version 6.0 includes high-fidelity Microsoft SMB signatures and signatures to support database TNS clients and servers.
Wide Variety of Application Protocols	Application inspection control of HTTP, port 80 misuse/application tunneling, FTP, mime type filtering. DHCP, DNS, FTP, file sharing (peer-to-peer, Finger, HTTP, HTTPS, IMAP, Ident, LPR,NNTP, NTP, POP, R-Services, RPC, MSRPC, SMTP, SNMP, SOCKS, SQL, SSH, Telnet TFTP, H.323, H.225, WINS, MSSQL, IRC, LDAP, SMB, TNS, and anomaly-based day-zero scanning worm protection.
Protocol-Decode Support	Protocol decode-based signatures decode various elements in the same manner as the client or server in the conversation would. When the elements of the protocol are identified, the IPS applies rules defined by the RFCs to look for violations.
True "stateful" Inspection Technology	Supports full TCP/IP and application protocol state, spanning multiple packets in flows. Full flow normalization for proper packet ordering.
Full de-Obfuscation Support	Supports UTF-8 decoding, Microsoft's custom Unicode %Uxxxx encoding, double encoding, un-encoded octets mixed with encoded octets in a UTF-8 sequence, ambiguous bits, Microsoft Base 36, alternate code pages, and multiple directory delimiters.
Full Stream Reassembly	The evasion protection module performs full stream reassembly and is designed to handle all known evasion techniques. The module includes fragment reassembly, TTL handling, and TCP session validation.
SYN Attack Protection	Provides SYN detection and protection for both targets and IPS devices.
Detects and Blocks All Types Of Port Scans	Includes full connect, SYN stealth, FIN stealth, and UDP scans.

Cisco Services for IPS

Cisco Services for IPS enables operators to receive time-critical signature file updates and alerts. As part of Cisco's Technical Support Services portfolio, Cisco Services for IPS offers a comprehensive security service that allows your Cisco IPS solution to stay current on the latest threats so that malicious or damaging traffic is accurately identified, classified, and stopped. Cisco Services for IPS features include:

- Frequent signature and detection engine updates and alerts
- Access to Cisco IntelliShield Search Access feature for IPS signatures
- Registered access to Cisco.com for online tools and technical assistance
- Access to Cisco Technical Assistance Center (TAC)
- Cisco IPS Sensor Software updates
- Advance replacement of failed hardware

For more information about Cisco Services for IPS, please visit http://www.cisco.com/en/US/products/ps6076/serv_home.html.

For More Information

For more information about Cisco IPS solutions, visit:

- http://www.cisco.com/go/ips

For more information about Cisco Security Manager, Cisco Security MARS, and Cisco IPS Manager Express, visit:

- http://www.cisco.com/go/csmanager
- http://www.cisco.com/go/mars
- http://www.cisco.com/go/ime

To experience Cisco Security Center, visit:

- http://www.cisco.com/security

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Printed in USA C78-459520-00 03/08