Intrusion Prevention for the Cisco ASA 5500-X Series

As users and data leave the corporate boundary and the network access layer becomes more porous, traditional signature technology alone will not suffice. Only Cisco® intrusion prevention (IPS) technology, backed by Cisco Security Intelligence Operations (SIO), identifies and mitigates attackers and attacks up to Layer 7 with market-leading, context-aware threat prevention that augments your firewall and VPN deployment.

The Cisco ASA 5500-X Series IPS Solution scales from the Cisco Borderless Network Architecture to data center architectures, with integrated form factors ranging from 1 Gbps to 10 Gbps. Strong default efficacy allows you to install a device and secure your network immediately. Achieve full visibility across your network with Cisco Security Manager to mitigate risk and meet compliance - all while reducing your expenses.

Figure 1. Cisco ASA with IPS Product Family

Mitigate Risks

Manage risks with a broad and deep set of inspection capabilities:

- Defend against zero-day attacks with over 40 engines and 6500 stateful, vulnerability-based signatures that protect against tens of thousands of current exploits - and countless more to come.
- Inspect a wide variety of protocols to ensure RFC conformance and prevent hacks.
- Identify the source of and block denial of service (DoS), distributed denial of service (DDoS), SYN flood, and encrypted attacks with Cisco Global Correlation.
- Use patented anti-evasion technology to defend and monitor against worms, viruses, Trojans, reconnaissance attacks, spyware, botnets, phishing, peer to peer attacks, and malware, as well as numerous evasion techniques.
- Guard Cisco infrastructure with specific protections for Unified Communications, WLAN, routing, and switching.
- Utilize identity-based firewall to provide granular and powerful policy definition.

Ensure Compliance

- U.S. Sarbanes-Oxley Act (SOX)
- U.S. Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI DSS)
- NERC Critical Infrastructure Protection (CIP)
- Health Insurance Portability and Accountability Act (HIPAA)
- U.S. Federal Information Security Management Act (FISMA)

Seamless Network Integration

A critical component of the SecureX framework, Cisco IPS technology seamlessly integrates into the Cisco ASA firewall and network architecture. Whether defending the data center, core, or edge, Cisco IPS provides threat protection up to Layer 7. To reduce capital expenditures, the Cisco IPS solution is built upon a common software architecture and custom hardware platforms that enable deployment anywhere in the Cisco network, including routing, switching, and firewall platforms. A consistent policy and operations framework helps bring the system together to meet compliance demands and manage risk at a lower operational cost.

Unparalleled Global Correlation

As advanced persistent threats (APTs), botnets, and other blended threats evolve, signature-based content inspection alone becomes insufficient for threat identification and mitigation. With 10 years of reputation technology heritage, Cisco IPS with Global Correlation is the only IPS to identify and mitigate attackers - not just signature-based attacks. With Cisco IPS Global Correlation backed by Cisco SIO, Cisco IPS gains visibility into hundreds of additional security parameters, millions of rules, and 8 TB of threat telemetry per day from market-leading email, web, firewall, and IPS devices.

Network-Ready Capabilities

To meet the needs of the most demanding networks, Cisco IPS directly integrates into the firewall to deliver multigigabit performance, low latency, and high availability features. With dedicated hardware, the Cisco ASA 5500 Series with IPS delivers performance from 150 Mbps to 10 Gbps to meet the rigors of a broad range of applications and network use. Flexible and highly available deployment options include active-active and active-standby configurations, fail-open and fail-closed modes, IDS and IPS modes, redundant power supplies, and load-balancing capabilities, as well as the ability to inspect encapsulated traffic, including GRE, MPLS, 802.1q, IPv4 in IPv4, IPv4 in IPv6, and Q-in-Q double VLAN.

Proven Threat Prevention

With more than US$100 million invested in security research, 500 threat analysts, and terabytes of threat data fed into Cisco SensorBase™ every day, Cisco IPS backed by Cisco SIO brings confidence to customer networks. This is why Cisco IPS is the most widely deployed commercial IPS technology in the world. Independent testing agencies, such as NSS, also recommend Cisco IPS.

Complete Control and Real-Time Visibility

Cisco provides management solutions for a few Cisco IPS devices or hundreds. Cisco IPS Manager Express (Figure 2) is an all-in-one IPS management and reporting application for up to 10 devices. Cisco Security Manager is an enterprise-class security management application with thousands of real-world deployments. Both solutions support Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IPS 4200 Series Sensor Appliances, Cisco Integrated Services Routers (ISRs), and Cisco Intrusion Detection Services Modules (IDSMs).

Cisco IPS Manager Express offers:

- Provisioning, monitoring, and troubleshooting
- Drag-and-drop dashboard gadgets, which provide easy customization and personalized views that remember your settings to minimize setup time
- A flexible reporting tool for generating custom and compliance reports in seconds

Cisco Security Manager 4.x offers:

- Flexible processes to provision new and updated signatures incrementally, create IPS policies for those signatures, and then share the policies across devices
- Integrated tuning and troubleshooting tools including IPS event-to-policy linkages and cross-launching capabilities
- Enhanced reporting and event management support for Cisco's latest IPS features, including Global Correlation
- Role-based access control and workflow, which help ensure error-free deployments and process compliance

Figure 2. Cisco IPS Manager Express

Table 1. Cisco ASA 5500-X Series IPS Solution Specifications

Feature	Cisco ASA 5512-X IPS	Cisco ASA 5515-X IPS	Cisco ASA 5525-X IPS	Cisco ASA 5545-X IPS	Cisco ASA 5555-X IPS	Cisco ASA 5585-10 IPS	Cisco ASA 5585-20 IPS	Cisco ASA 5585-40 IPS	Cisco ASA 5585-60 IPS
IPS									
Maximum IPS Throughput; Media-Rich* (Mbps)	250	400	600	900	1300	2000 with IPS-SSP-10	3000 with IPS-SSP-20	5000 with IPS-SSP-40	10,000 with IPS-SSP-60
Maximum IPS Throughput; Transactional* (Mbps)	150	250	400	600	850	1150 with IPS-SSP-10	1500 with IPS-SSP-20	3000 with IPS SSP-40	5000 with IPS-SSP-60
Threat Protection	25,000+ threats	25,000+ threats	25,000+ threats	25,000+ threats	25,000+ threats	25,000+ threats	25,000+ threats	25,000+ threats	25,000+ threats
Zero-Day Protection with Anomaly Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Global Correlation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Custom Signature Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High Availability	Active/Active and Active/ Standby**	Active/Active and Active/ Standby	Active/Active and Active/ Standby	Active/Active and Active/ Standby	Active/Active and Active/ Standby	Active/Active and Active/ Standby	Active/Active and Active/ Standby	Active/Active and Active/ Standby	Active/Active and Active/ Standby
Redundant Power Supplies	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Firewall									
Maximum Firewall Throughput Large Packet (Mbps)	1000	1500	2000	3000	4000	5000	10,000	20,000	40,000
Maximum Firewall Connections	100,000	250,000	500,000	750,000	1,000,000	2,000,000	3,000,000	4,000,000	8,000,000
Ports									
Gigabit Ethernet (Copper)	6	6	8	8	8	16	16	12	12
10 Gigabit Ethernet	0	0	0	0	0	4	4	8	8

* Transactional is 440-byte HTTP traffic with high connections/second and one transaction per connection seen in e-commerce transactions and instant messaging. Media-rich is 765-byte HTTP traffic with low connections/second and multiple transactions per connection, which is seen on the most popular websites. Every deployment scenario is different, and IPS performance will vary based on live traffic profiles. Users should test with as much live traffic as possible to assess your network's individual characteristics.

** With Security plus license.

Table 2. Cisco ASA 5500-X IPS SSP Specifications

Feature	Cisco ASA 5512-X IPS	Cisco ASA 5515-X IPS	Cisco ASA 5525-X IPS	Cisco ASA 5545-X IPS	Cisco ASA 5555-X IPS	Cisco IPS SSP-10	Cisco IPS SSP-20	Cisco IPS SSP-40	Cisco IPS SSP-60
Technical Specifications									
Management and Monitoring Interface	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**	**1 Ethernet 10/100/1000 port**
Memory	**4 GB**	**8 GB**	**8 GB**	**12 GB**	**16 GB**	**6 GB**	**12 GB**	**24 GB**	**48 GB**
Minimum Flash	**4 GB**	**8 GB**	**8 GB**	**8 GB**	**8 GB**	**2 GB**	**2 GB**	**2 GB**	**2 GB**

Ordering Information

To place an order, visit the Cisco Ordering homepage. See Table 3 for ordering information.

Table 3. Ordering Information

Product Name	Part Number
Cisco ASA 5505 Adaptive Security Appliance	
Cisco ASA 5505 50-User Adaptive Security Appliance with AIP-SSC-5 (chassis, software, 8 Fast Ethernet interfaces,10 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license)	ASA5505-50-AIP5-K9
Cisco ASA 5505 Unlimited-User Adaptive Security Appliance with Security Plus License and AIP-SSC-5 (chassis, software, 8 Fast Ethernet interfaces, 25 IPsec VPN peers, 2 SSL VPN peers, DMZ support, stateless Active/Standby high availability, 3DES/AES license	ASA5505-U-AIP5P-K9
Cisco ASA 5512-X Adaptive Security Appliance IPS Edition	
Cisco ASA 5512-X Adaptive Security Appliance with IPS SSP (chassis, software, 250 VPN peers, 2 SSL VPN Peers, 6 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet management interface, DES)	ASA5512-IPS-K8
Cisco ASA 5512-X Adaptive Security Appliance with IPS SSP (chassis, software, 250 VPN peers, 2 SSL VPN Peers, 6 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet interface, 3DES/AES)	ASA5512-IPS-K9
Cisco ASA 5515-X Adaptive Security Appliance IPS Edition	
Cisco ASA 5515-X Adaptive Security Appliance with IPS SSP (chassis, software, 250 VPN peers, 2 SSL VPN Peers, 6 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet management interface, Active/Active, 2 contexts, DES)	ASA5515-IPS-K8
Cisco ASA 5515-X Adaptive Security Appliance with IPS SSP (chassis, software, 250 VPN peers, 2 SSL VPN Peers, 6 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet interface, Active/Active, 2 contexts, 3DES/AES)	ASA5515-IPS-K9
Cisco ASA 5525-X Adaptive Security Appliance IPS Edition	
Cisco ASA 5525-X Adaptive Security Appliance with IPS SSP (chassis, software, 750 VPN peers, 2 SSL VPN Peers, 8 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet management interface, Active/Active, 2 contexts, DES)	ASA5525-IPS-K8
Cisco ASA 5525-X Adaptive Security Appliance with IPS SSP (chassis, software, 750 VPN peers, 2 SSL VPN Peers, 8 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet interface, Active/Active, 2 contexts, 3DES/AES)	ASA5525-IPS-K9
Cisco ASA 5545-X Adaptive Security Appliance IPS Edition	
Cisco ASA 5545-X Adaptive Security Appliance with IPS SSP (chassis, software, 2500 VPN peers, 2 SSL VPN Peers, 8 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet management interface, Active/Active, 2 contexts, DES)	ASA5545-IPS-K8
Cisco ASA 5545-X Adaptive Security Appliance with IPS SSP (chassis, software, 2500 VPN peers, 2 SSL VPN Peers, 8 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet interface, Active/Active, 2 contexts, 3DES/AES)	ASA5545-IPS-K9
Cisco ASA 5555-X Adaptive Security Appliance IPS Edition	
Cisco ASA 5555-X Adaptive Security Appliance with IPS SSP (chassis, software, 5000 VPN peers, 2 SSL VPN Peers, 8 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet management interface, Active/Active, 2 contexts, DES)	ASA5555-IPS-K8
Cisco ASA 5555-X Adaptive Security Appliance with IPS SSP (chassis, software, 5000 VPN peers, 2 SSL VPN Peers, 8 CU Gigabit Ethernet interfaces, 1 CU Gigabit Ethernet interface, Active/Active, 2 contexts, 3DES/AES)	ASA5555-IPS-K9

Product Name	Part Number
Cisco ASA 5585-X Adaptive Security Appliances	
Cisco ASA 5585-X Adaptive Security Appliance with IPS SSP-10 (IPS SSP-10 bundle includes 8 Gigabit Ethernet interfaces, 2 Gigabit Ethernet management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, DES license)	ASA5585-S10P10-K8
Cisco ASA 5585-X Firewall Edition SSP-10 (IPS SSP-10 bundle includes 8 Gigabit Ethernet interfaces, 2 Gigabit Ethernet management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license)	ASA5585-S10P10-K9
Cisco ASA 5585-X Firewall Edition SSP-10 (IPS SSP-10 bundle includes 8 Gigabit Ethernet interfaces, 2 10 Gigabit Ethernet SFP+ interfaces, 2 Gigabit Ethernet management interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, dual AC power, 3DES/AES license)	ASA5585-S10P10XK9
Cisco ASA 5585-X Firewall Edition SSP-20 (IPS SSP-20 bundle includes 8 Gigabit Ethernet interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, DES license)	ASA5585-S20P20-K8
Cisco ASA 5585-X Firewall Edition SSP-20 (IPS SSP-20 bundle includes 8 Gigabit Ethernet interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license)	ASA5585-S20P20-K9
Cisco ASA 5585-X Firewall Edition SSP-20 (IPS SSP-20 bundle includes 8 Gigabit Ethernet interfaces, 2 10 Gigabit Ethernet SFP+ interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, dual AC power, 3DES/AES license)	ASA5585-S20P20XK9
Cisco ASA 5585-X Firewall Edition SSP-40 (IPS SSP-40 bundle includes 6 Gigabit Ethernet interfaces, 4 10 Gigabit Ethernet SFP+ interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, dual AC power, DES license)	ASA5585-S40P40-K8
Cisco ASA 5585-X Firewall Edition SSP-40 (IPS SSP-40 bundle includes 6 Gigabit Ethernet interfaces, 4 10 Gigabit Ethernet SFP+ interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, dual AC power, 3DES/AES license)	ASA5585-S40P40-K9
Cisco ASA 5585-X Firewall Edition SSP-60 (IPS SSP-60 bundle includes 6 Gigabit Ethernet interfaces, 4 10 Gigabit Ethernet SFP+ interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, dual AC power, 3DES/AES license)	ASA5585-S60P60-K8
Cisco ASA 5585-X Firewall Edition SSP-60 (IPS SSP-60 bundle includes 6 Gigabit Ethernet interfaces, 4 10 Gigabit Ethernet SFP+ interfaces, 2 Gigabit Ethernet management interfaces, 10,000 IPsec VPN peers, 2 SSL VPN peers, dual AC power, 3DES/AES license)	ASA5585-S60P60-K9
Security Services Modules	
Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Card 5 (AIP-SSC-5)	ASA-SSC-AIP-5-K9=
Security Services Processor Software License	
Cisco ASA 5512-X IPS Security Services Processor Software License Spare (eDelivery)	L-ASA5512-IPS-SSP=
Cisco ASA 5515-X IPS Security Services Processor Software License Spare (eDelivery)	L-ASA5515-IPS-SSP=
Cisco ASA 5525-X IPS Security Services Processor Software License Spare (eDelivery)	L-ASA5525-IPS-SSP=
Cisco ASA 5545-X IPS Security Services Processor Software License Spare (eDelivery)	L-ASA5545-IPS-SSP=
Cisco ASA 5555-X IPS Security Services Processor Software License Spare (eDelivery)	L-ASA5555-IPS-SSP=
Security Services Processors	
Cisco ASA 5585-X IPS Security Services Processor 10 with 8 GE	ASA-SSP-IPS10
Cisco ASA 5585-X IPS Security Services Processor 20 (SSP-20) with 8 GE	ASA-SSP-IPS20
Cisco ASA 5585-X IPS Security Services Processor 40 (SSP-40) with 6 GE, 4 SFP+	ASA-SSP-IPS40
Cisco ASA 5585-X IPS Security Services Processor-60 (SSP-60) with 6 GE, 4 SFP+	ASA-SSP-IPS60

Service and Support

Cisco offers a wide range of service programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services for security, visit http://www.cisco.com/go/services/security.

Cisco Services for IPS

Cisco Services for IPS is an integral part of the Cisco ASA 5500-X Series IPS Solution and enables operators to receive time-critical signature file updates and alerts. Part of the Cisco Technical Support Services portfolio, Cisco Services for IPS allows your Cisco ASA 5500-X Series 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:

- Signature file updates and alerts
- Registered access to Cisco.com for online tools and technical assistance
- Access to the Cisco Technical Assistance Center
- Cisco IPS software updates
- Advance replacement of failed hardware

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

Export Considerations

The Cisco ASA 5500-X Series IPS Solution and Cisco AIP SSMs are subject to export controls. For guidance, refer to the export compliance website at http://www.cisco.com/wwl/export/crypto/. For specific export questions, contact export@cisco.com.

Additional Information

For more information about the Cisco ASA 5500-X Series IPS Solution, visit http://www.cisco.com/go/asaips.

For more information about Cisco IPS solutions, visit http://www.cisco.com/go/ips.

For more information about Cisco ASA 5500-X Series, visit http://www.cisco.com/go/asa.

For information about Cisco IDS and IPS sensors and software versions that have reached end-of-sale status, visit http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_eol_notices_list.html.

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

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

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.

Printed in USA C78-459036-08 10/12