GLOSSARY

Numerals

3DES Triple Data Encryption Standard. A stronger version of DES, which is the default encryption method for SSH version 1.5. Used when establishing an SSH session with the sensor. It can be used when the sensor is managing a device.

802.x A set of IEEE standards for the definition of LAN protocols.

A

AAA authentication, authorization, and accounting. Pronounced "triple a." The primary and recommended method for access control in Cisco devices.

ACE Access Control Entry. An entry in the ACL that describes what action should be taken for a specified address or protocol. The sensor adds/removes ACE to block hosts.

ACK acknowledgement. Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message).

ACL Access Control List. A list of ACEs that control the flow of data through a router. There are two ACLs per router interface for inbound data and outbound data. Only one ACL per direction can be active at a time. ACLs are identified by number or by name. ACLs can be standard, enhanced, or extended. You can configure the sensor to manage ACLs.

action The response of the sensor to an event. An action only happens if the event is not filtered. Examples include TCP reset, block host, block connection, IP logging, and capturing the alert trigger packet.

active ACL The ACL created and maintained by ARC and applied to the router block interfaces.

adaptive security appliance Combines firewall, VPN concentrator, and intrusion prevention software functionality into one software image. You can configure the adaptive security appliance in single mode or multi-mode.

AIC engine Application Inspection and Control engine. Provides deep analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications that try to tunnel over specified ports, such as instant messaging, and tunneling applications, such as gotomypc. It can also inspect FTP traffic and control the commands being issued.

AIM-IPS Advanced Integration Module. A type of IPS network module installed in Cisco routers.

AIP-SSC-5 Advanced Inspection and Prevention Security Services Card. The IPS plug-in module in the Cisco ASA 5505 series adaptive security appliance. AIP-SSC-5 uses IPS services to stop malicious traffic, including worms and network viruses, before they can affect your network. See also adaptive security appliance.

AIP-SSM	Advanced Inspection and Prevention Security Services Module. The IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance. AIP-SSM is an IPS services module that monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When AIP-SSM detects unauthorized activity, it can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the device manager. See also adaptive security appliance.
Alarm Channel	The IPS software module that processes all signature events generated by the inspectors. Its primary function is to generate alerts for each event it receives.
alert	Specifically, an IPS event type; it is written to the Event Store as an evidsAlert. In general, an alert is an IPS message that indicates a network exploit in progress or a potential security problem occurrence. Also known as an alarm.
Analysis Engine	The IPS software module that handles sensor configuration. It maps the interfaces and also the signature and Alarm Channel policy to the configured interfaces. It performs packet analysis and alert detection. The Analysis Engine functionality is provided by the SensorApp process.
anomaly detection	AD. The sensor component that creates a baseline of normal network traffic and then uses this baseline to detect worm-infected hosts.
API	Application Programming Interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. Computer application programs run a set of standard software interrupts, calls, and data formats to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create links that an application needs to communicate with the operating system or with the network.
application	Any program (process) designed to run in the Cisco IPS environment.
application image	Full IPS image stored on a permanent storage device used for operating the sensor.
application instance	A specific application running on a specific piece of hardware in the IPS environment. An application instance is addressable by its name and the IP address of its host computer.
application partition	The bootable disk or compact-flash partition that contains the IPS software image.
ARC	Attack Response Controller. Formerly known as Network Access Controller (NAC). A component of the IPS. A software module that provides block and unblock functionality where applicable.
architecture	The overall structure of a computer or communication system. The architecture influences the capabilities and limitations of the system.
ARP	Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.
attack relevance rating	ARR. A weight associated with the relevancy of the targeted OS. The attack relevance rating is a derived value (relevant, unknown, or not relevant), which is determined at alert time. The relevant OSes are configured per signature.
ASDM	Adaptive Security Device Manager. A web-based application that lets you configure and manage your ASA.

ASN.1	Abstract Syntax Notation 1. Standard for data presentation.
aspect version	Version information associated with a group of IDIOM default configuration settings. For example, Cisco Systems publishes the standard set of attack signatures as a collection of default settings with the S aspect. The S-aspect version number is displayed after the S in the signature update package file name. Other aspects include the Virus signature definitions in the V-aspect and IDIOM signing keys in the key-aspect.
attack severity rating	ASR. A weight associated with the severity of a successful exploit of the vulnerability. The attack severity rating is derived from the alert severity parameter (informational, low, medium, or high) of the signature. The attack severity rating is configured per signature and indicates how dangerous the event detected is.
atomic attack	Represents exploits contained within a single packet. For example, the "ping of death" attack is a single, abnormally large ICMP packet.
Atomic engine	There are two ATOMIC engines: ATOMIC.IP inspects IP protocol packets and associated Layer-4 transport protocols, and ATOMIC.ARP inspects Layer-2 ARP protocol.
attack	An assault on system security that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt (especially in the sense of method or technique) to evade security services and violate the security policy of a system.
authentication	Process of verifying that a user has permission to use the system, usually by means of a password key or certificate.
AuthenticationApp	A component of the IPS. It verifies that users have the correct permissions to perform CLI, IDM, IME, or RDEP actions.
autostate	In normal autostate mode, the Layer 3 interfaces remain up if at least one port in the VLAN remains up. If you have appliances, such as load balancers or firewall servers that are connected to the ports in the VLAN, you can configure these ports to be excluded from the autostate feature to make sure that the forwarding SVI does not go down if these ports become inactive.
AV	Anti-Virus.

B

backplane	The physical connection between an interface processor or card and the data buses and the power distribution buses inside a chassis.
base version	A software release that must be installed before a follow-up release, such as a service pack or signature update, can be installed. Major and minor updates are base version releases.
benign trigger	A situation in which a signature is fired correctly, but the source of the traffic is nonmalicious.
BIOS	Basic Input/Output System. The program that starts the sensor and communicates between the devices in the sensor and the system.
block	The ability of the sensor to direct a network device to deny entry to all packets from a specified network host or network.

block interface	The interface on the network device that the sensor manages.
BO	BackOrifice. The original Windows back door Trojan that ran over UDP only.
BO2K	BackOrifice 2000. A Windows back door Trojan that runs over TCP and UDP.
bootloader	A small set of system software that runs when the system first powers up. It loads the operating system (from the disk, network, external compact flash, or external USB flash), which loads and runs the IPS application. For AIM-IPS, it boots the module from the network and assists in software installation and upgrades, disaster recovery, and other operations when the module cannot access its software.
Botnets	A collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software. The term Botnet is used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed through worms, Trojan horses, or back doors, under a common command-and-control infrastructure.
Bpdu	Bridge Protocol Data Unit. Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.
bypass mode	Mode that lets packets continue to flow through the sensor even if the sensor fails. Bypass mode is only applicable to inline-paired interfaces.

C

CA	certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. Sensors use self-signed certificates.
CA certificate	Certificate for one CA issued by another CA.
CEF	Cisco Express Forwarding. CEF is advanced, Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.
certificate	Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.
cidDump	A script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.
CIDEE	Cisco Intrusion Detection Event Exchange. Specifies the extensions to SDEE that are used by Cisco IPS systems. The CIDEE standard specifies all possible extensions that may be supported by Cisco IPS systems.
CIDS header	The header that is attached to each packet in the IPS system. It contains packet classification, packet length, checksum results, timestamp, and the receive interface.
cipher key	The secret binary data used to convert between clear text and cipher text. When the same cipher key is used for both encryption and decryption, it is called symmetric. When it is used for either encryption or decryption (but not both), it is called asymmetric.

Cisco IOS	Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks while supporting a wide variety of protocols, media, services, and platforms.
CLI	command-line interface. A shell provided with the sensor used for configuring and controlling the sensor applications.
command and control interface	The interface on the sensor that communicates with the IPS manager and other network devices. This interface has an assigned IP address.
community	In SNMP, a logical group of managed devices and NMSs in the same administrative domain.
composite attack	Spans multiple packets in a single session. Examples include most conversation attacks such as FTP, Telnet, and most Regex-based attacks.
connection block	ARC blocks traffic from a given source IP address to a given destination IP address and destination port.
console	A terminal or laptop computer used to monitor and control the sensor.
console port	An RJ45 or DB9 serial port on the sensor that is used to connect to a console device.
control interface	When ARC opens a Telnet or SSH session with a network device, it uses one of the routing interfaces of the device as the remote IP address. This is the control interface.
control transaction	An IPS message containing a command addressed to a specific application instance. Example control transactions include *start*, *stop*, *getConfig*.
cookie	A piece of information sent by a web server to a web browser that the browser is expected to save and send back to the web server whenever the browser makes additional requests of the web server.
CSA MC	Cisco Security Agent Management Center. CSA MC receives host posture information from the CSA agents it manages. It also maintains a watch list of IP addresses that it has determined should be quarantined from the network.
CSM	Cisco Security Manager, the provisioning component of the Cisco Self-Defending Networks solution. CS-Manager is fully integrated with CS-MARS.
CS-Manager	See CSM.
CS-MARS	Cisco Security Monitoring, Analysis and Reporting System. The monitoring component of the Cisco Self-Defending Networks solution. CS-MARS is fully integrated with CS-Manager
CVE	Common Vulnerabilities and Exposures. A list of standardized names for vulnerabilities and other information security exposures maintained at http://cve.mitre.org/.

D

darknets	A virtual private network where users connect only to people they trust. In its most general meaning, a darknet can be any type of closed, private group of people communicating, but the name is most often used specifically for file-sharing networks. Darknet can be used to refer collectively to all covert communication networks.

datagram   Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

DCE   data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.

DCOM   Distributed Component Object Model. Protocol that enables software components to communicate directly over a network. Developed by Microsoft and previously called Network OLE, DCOM is designed for use across multiple network transports, including such Internet protocols as HTTP.

DDoS   Distributed Denial of Service. An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

DES   Data Encryption Standard. A strong encryption method where the strength lies in a 56-bit key rather than an algorithm.

destination address   Address of a network device that is receiving data.

DIMM   Dual In-line Memory Modules.

DMZ   demilitarized zone. A separate network located in the neutral zone between a private (inside) network and a public (outside) network.

DNS   Domain Name System. An Internet-wide hostname to IP address mapping. DNS enables you to convert human-readable names into the IP addresses needed for network packets.

DoS   Denial of Service. An attack whose goal is just to disrupt the operation of a specific system or network.

DRAM   dynamic random-access memory. RAM that stores information in capacitors that must be refreshed periodically. Delays can occur because DRAMs are inaccessible to the processor when refreshing their contents. However, DRAMs are less complex and have greater capacity than SRAMs.

DTE   Data Terminal Equipment. Refers to the role of a device on an RS-232C connection. A DTE writes data to the transmit line and reads data from the receive line.

DTP   Dynamic Trunking Protocol. A Cisco proprietary protocol in the VLAN group used for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (ISL or 802.1q) to be used.

E

ECLB   Ether Channel Load Balancing. Lets a Catalyst switch split traffic flows over different physical paths.

egress   Traffic leaving the network.

encryption	Application of a specific algorithm to data to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.
engine	A component of the sensor designed to support many signatures in a certain category. Each engine has parameters that can be used to create signatures or tune existing signatures.
enterprise network	Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.
escaped expression	Used in regular expression. A character can be represented as its hexadecimal value, for example, \x61 equals 'a,' so \x61 is an escaped expression representing the character 'a.'
ESD	electrostatic discharge. Electrostatic discharge is the rapid movement of a charge from one object to another object, which produces several thousand volts of electrical charge that can cause severe damage to electronic components or entire circuit card assemblies.
event	An IPS message that contains an alert, a block request, a status message, or an error message.
Event Store	One of the components of the IPS. A fixed-size, indexed store (30 MB for all sensors, except the AIP SSC-5, which has 10 MB) used to store IPS events.
evIdsAlert	The XML entity written to the Event Store that represents an alert.

F

fail closed	Blocks traffic on the device after a hardware failure.
fail open	Lets traffic pass through the device after a hardware failure.
false negative	A signature is not fired when offending traffic is detected.
false positive	Normal traffic or a benign action causes a signature to fire.
Fast Ethernet	Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase 10 times that of the 10BaseT Ethernet specification while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification.
firewall	Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.
Flood engine	Detects ICMP and UDP floods directed at hosts and networks.
flooding	Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.
fragment	Piece of a larger packet that has been broken down to smaller units.
fragmentation	Process of breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP   File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

FTP server   File Transfer Protocol server. A server that uses the FTP protocol for transferring files between network nodes.

full duplex   Capability for simultaneous data transmission between a sending station and a receiving station.

FWSM   Firewall Security Module. A module that can be installed in a Catalyst 6500 series switch. It uses the **shun** command to block. You can configure the FWSM in either single mode or multi-mode.

G

GBIC   GigaBit Interface Converter. Often refers to a fiber optic transceiver that adapts optical cabling to fiber interfaces. Fiber-ready switches and NICs generally provide GBIC and/or SFP slots. For more information, refer to the *Catalyst Switch Cable, Connector, and AC Power Cord Guide.*

Gigabit Ethernet Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.

GMT   Greenwich Mean Time. Time zone at zero degrees longitude. Now called Coordinated Universal Time (UTC).

GRUB   Grand Unified Bootloader.

H

H.225.0   An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.

H.245   An ITU standard that governs H.245 endpoint control.

H.323   Allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.

half duplex   Capability for data transmission in only one direction at a time between a sending station and a receiving station. BSC is an example of a half-duplex protocol.

handshake   Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.

hardware bypass   A specialized interface card that pairs physical interfaces so that when a software error is detected, a bypass mechanism is engaged that directly connects the physical interfaces and allows traffic to flow through the pair. Hardware bypass passes traffic at the network interface, does not pass it to the IPS system.

host block   ARC blocks all traffic from a given IP address.

HTTP	Hypertext Transfer Protocol. The stateless request/response media transfer protocol used in the IPS architecture for remote data exchange.
HTTPS	An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

I

ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.
ICMP flood	Denial of Service attack that sends a host more ICMP echo request ("ping") packets than the protocol implementation can handle.
IDAPI	Intrusion Detection Application Programming Interface. Provides a simple interface between IPS architecture applications. IDAPI reads and writes event data and provides a mechanism for control transactions.
IDCONF	Intrusion Detection Configuration. A data format standard that defines operational messages that are used to configure intrusion detection and prevention systems.
IDENT	Ident protocol, specified in RFC 1413, is an Internet protocol that helps identify the user of a particular TCP connection.
IDIOM	Intrusion Detection Interchange and Operations Messages. A data format standard that defines the event messages that are reported by intrusion detection systems and the operational messages that are used to configure and control intrusion detection systems.
IDM	IPS Device Manager. A web-based application that lets you configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through Internet Explorer or Firefox web browsers.
IDMEF	Intrusion Detection Message Exchange Format. The IETF Intrusion Detection Working Group draft standard.
IDSM-2	Intrusion Detection System Module. A switching module that performs intrusion detection in the Catalyst 6500 series switch.
IDS MC	Management Center for IDS Sensors. A web-based IDS manager that can manage configurations for up to 300 sensors.
IME	IPS Manager Express. A network management application that provides system health monitoring, events monitoring, reporting, and configuration for up to five sensors.
inline mode	All packets entering or leaving the network must pass through the sensor.
inline interface	A pair of physical interfaces configured so that the sensor forwards all traffic received on one interface out to the other interface in the pair.
intrusion detection system	IDS. A security service that monitors and analyzes system events to find and provide real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

IP address   32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

IPS   Intrusion Prevention System. A system that alerts the user to the presence of an intrusion on the network through network traffic analysis techniques.

IPS data or message   Describes the messages transferred over the command and control interface between IPS applications.

iplog   A log of the binary packets to and from a designated address. Iplogs are created when the log Event Action is selected for a signature. Iplogs are stored in a libpcap format, which can be read by WireShark and TCPDUMP.

IP spoofing   IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPSec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.

IPv6   IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

ISL   Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

J

Java Web Start   Java Web Start provides a platform-independent, secure, and robust deployment technology. It enables developers to deploy full-featured applications to you by making the applications available on a standard web server. With any web browser, you can launch the applications and be confident you always have the most-recent version.

JNLP   Java Network Launching Protocol. Defined in an XML file format specifying how Java Web Start applications are launched. JNLP consists of a set of rules defining how exactly the launching mechanism should be implemented.

K

KB   Knowledge Base. The sets of thresholds learned by anomaly detection and used for worm virus detection.

knowledge base   See KB.

L

LACP Link Aggregation Control Protocol. LACP aids in the automatic creation of EtherChannel links by exchanging LACP packets between LAN ports. This protocol is defined in IEEE 802.3ad.

LAN Local Area Network. Refers to the Layer 2 network domain local to a given host. Packets exchanged between two hosts on the same LAN do not require Layer 3 routing.

Logger A component of the IPS. Writes all the log messages of the application to the log file and the error messages of the application to the Event Store.

logging Gathers actions that have occurred in a log file. Logging of security information is performed on two levels: logging of events (such as IPS commands, errors, and alerts), and logging of individual IP session information.

LOKI Remote access, back door Trojan, ICMP tunneling software. When the computer is infected, the malicious code creates an ICMP tunnel that can be used to send small payload ICMP replies

M

MainApp The main application in the IPS. The first application to start on the sensor after the operating system has booted.

maintenance partition The bootable disk partition on IDSM-2, from which an IPS image can be installed on the application partition. No IPS capability is available while the IDSM-2 is booted into the maintenance partition.

maintenance partition image The bootable software image installed on the maintenance partition on an IDSM-2. You can install the maintenance partition image only while booted into the application partition.

major update A base version that contains major new functionality or a major architectural change in the product.

Malware Malicious software that is installed on an unknowing host.

manufacturing image Full IPS system image used by manufacturing to image sensors.

master blocking sensor A remote sensor that controls one or more devices. Blocking forwarding sensors send blocking requests to the master blocking sensor and the master blocking sensor executes the blocking requests.

MD5 Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Meta engine Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.

MIB   Management Information Base. Database of network management information that is used and
                     maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can
                     be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management
                     system. MIB objects are organized in a tree structure that includes public (standard) and private
                     (proprietary) branches.

MIME   Multipurpose Internet Mail Extension. Standard for transmitting nontext data (or data that cannot be
                     represented in plain ASCII code) in Internet mail, such as binary, foreign language text (such as
                     Russian or Chinese), audio, or video data. MIME is defined in RFC 2045.

minor update   A minor version that contains minor enhancements to the product line. Minor updates are incremental
                     to the major version, and are also base versions for service packs.

module   A removable card in a switch, router, or security appliance chassis. AIM-IPS, AIP-SSC-5, AIP-SSM,
                     IDSM-2, and NME-IPS are IPS modules.

**monitoring   See sensing interface.
interface**

MPF   Modular Policy Framework. A means of configuring security appliance features in a manner similar to
                     Cisco IOS software Modular QoS CLI.

MSFC, MSFC2   Multilayer Switch Feature Card. An optional card on a Catalyst 6000 supervisor engine that performs
                     L3 routing for the switch.

MSRPC   Microsoft Remote Procedure Call. MSRPC is the Microsoft implementation of the DCE RPC
                     mechanism. Microsoft added support for Unicode strings, implicit handles, inheritance of interfaces
                     (which are extensively used in DCOM), and complex calculations in the variable-length string and
                     structure paradigms already present in DCE/RPC.

MySDN   My Self-Defending Network. A part of the signature definition section of IDM and IME. It provides
                     detailed information about signatures

N

NAC   Network Access Controller. See ARC.

NAT   Native Address Translation. A network device can present an IP address to the outside networks that is
                     different from the actual IP address of a host.

NBD   Next Business Day. The arrival of replacement hardware according to Cisco service contracts.

Neighbor Discovery Protocol for IPv6. IPv6 nodes on the same link use Neighbor Discovery to discover each other's
                     presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability
                     information about the paths to active neighbors.

network device   A device that controls IP traffic on a network and can block an attacking host. An example of a network
                     device is a Cisco router or PIX Firewall.

never block address Hosts and networks you have identified that should never be blocked.

never shun address See never block address.

NIC	Network Interface Card. Board that provides network communication capabilities to and from a computer system.
NME-IPS	Network Module Enhanced. An IPS module that you can install in any network module slot in the Cisco 2800 and 3800 series integrated services routers.
NMS	network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.
node	A physical communicating element on the command and control network. For example, an appliance, an IDSM-2, or a router.
Normalizer engine	Configures how the IP and TCP normalizer functions and provides configuration for signature events related to the IP and TCP normalizer.
NOS	network operating system. Generic term used to refer to distributed file systems. Examples include LAN Manager, NetWare, NFS, and VINES.
NTP	Network Timing Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
NTP server	Network Timing Protocol server. A server that uses NTP. NTP is a protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
NVRAM	Non-Volatile Read/Write Memory. RAM that retains its contents when a unit is powered off.

O

OIR	online insertion and removal. Feature that permits you to add, replace, or remove cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown.
OPS	Outbreak Prevention Service.

P

packet	Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data. The terms datagram, frame, message, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.
PAgP	Port Aggregation Control Protocol. PAgP aids in the automatic creation of EtherChannel links by exchanging PAgP packets between LAN ports. It is a Cisco-proprietary protocol.
passive fingerprinting	Act of determining the OS or services available on a system from passive observation of network interactions.

passive OS fingerprinting	The sensor determines host operating systems by inspecting characteristics of the packets exchanged on the network.
PASV Port Spoof	An attempt to open connections through a firewall to a protected FTP server to a non-FTP port. This happens when the firewall incorrectly interprets an FTP 227 **passive** command by opening an unauthorized connection.
PAT	Port Address Translation. A more restricted translation scheme than NAT in which a single IP address and different ports are used to represent the hosts of a network.
patch release	Release that addresses defects identified in the update (minor, major, or service pack) binaries after a software release (service pack, minor, or major update) has been released.
PAWS	Protection Against Wrapped Sequence. Protection against wrapped sequence numbers in high performance TCP networks. See RFC 1323.
PCI	Peripheral Component Interface. The most common peripheral expansion bus used on Intel-based computers.
promiscuous delta	PD. A weight in the range of 0 to 30 configured per signature.
PDU	protocol data unit. OSI term for packet. See also BPDU and packet.
PEP	Cisco Product Evolution Program. PEP is the UDI information that consists of the PID, the VID, and the SN of your sensor. PEP provides hardware version and serial number visibility through electronic query, product labels, and shipping items.
PER	packed encoding rules. Instead of using a generic style of encoding that encodes all types in a uniform way, PER specializes the encoding based on the date type to generate much more compact representations.
PFC	Policy Feature Card. An optional card on a Catalyst 6000 supervisor engine that supports VACL packet filtering.
PID	Product Identifier. The orderable product identifier that is one of the three parts of the UDI. The UDI is part of the PEP policy.
ping	packet internet groper. Often used in IP networks to test the reachability of a network device. It works by sending ICMP echo request packets to the target host and listening for echo response replies.
PIX Firewall	Private Internet Exchange Firewall. A Cisco network security device that can be programmed to block/enable addresses and ports between networks.
PKI	Public Key Infrastructure. Authentication of HTTP clients using the clients X.509 certificates.
POST	Power-On Self Test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.
Post-ACL	Designates an ACL from which ARC should read the ACL entries, and where it places entries after all deny entries for the addresses being blocked.

Pre-ACL	Designates an ACL from which ARC should read the ACL entries, and where it places entries before any deny entries for the addresses being blocked.
promiscuous mode	A passive interface for monitoring packets of the network segment. The sensing interface does not have an IP address assigned to it and is therefore invisible to attackers.

p

Q

Q.931	ITU-T specification for signaling to establish, maintain, and clear ISDN network connections.
QoS	quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

R

rack mounting	Refers to mounting a sensor in an equipment rack.
RAM	random-access memory. Volatile memory that can be read and written by a microprocessor.
RAS	Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.
RBCP	Router Blade Control Protocol. RBCP is based on SCP, but modified specifically for the router application. It is designed to run over Ethernet interfaces and uses 802.2 SNAP encapsulation for messages.
RDEP2	Remote Data Exchange Protocol version 2. The published specification for remote data exchange over the command and control network using HTTP and TLS.
reassembly	The putting back together of an IP datagram at the destination after it has been fragmented either at the source or at an intermediate node.
recovery package	An IPS package file that includes the full application image and installer used for recovery on sensors.
repackage release	Used to address defects in the packaging or the installer.
Regex	See regular expression.
regular expression	A mechanism by which you can define how to search for a specified sequence of characters in a data stream or file. Regular expressions are a powerful and flexible notation almost like a mini-programming language that allow you to describe text. In the context of pattern matching, regular expressions allow a succinct description of any arbitrary pattern.
repackage release	A release that addresses defects in the packaging or the installer.
RMA	Return Materials Authorization. The Cisco program for returning faulty hardware and obtaining a replacement.

ROMMON   Read-Only-Memory Monitor. ROMMON lets you TFTP system images onto the sensor for recovery purposes.

round-trip time See RTT.

RPC   remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

risk rating   RR. A value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network. The risk of the attack accounts for the severity, fidelity, relevance, and asset value of the attack, but not any response or mitigation actions. This risk is higher when more damage could be inflicted on your network.

RSM   Router Switch Module. A router module that is installed in a Catalyst 5000 switch. It functions exactly like a standalone router.

RTP   Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

RTT   round-trip time. A measure of the time delay imposed by a network on a host from the sending of a packet until acknowledgement of the receipt.

RU   rack unit. A rack is measured in rack units. An RU is equal to 44 mm or 1.75 inches.

S

SCP   Switch Configuration Protocol. Cisco control protocol that runs directly over the Ethernet.

SCEP   Simple Certificate Enrollment Protocol. The Cisco Systems PKI communication protocol that leverages existing technology by using PKCS#7 and PKCS#10. SCEP is the evolution of the enrollment protocol.

SDEE   Security Device Event Exchange. A product-independent standard for communicating security device events. It is an enhancement to RDEP. It adds extensibility features that are needed for communicating events generated by various types of security devices.

Secure Shell Protocol   Protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

security context You can partition a single adaptive security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management.

Security Monitor Monitoring Center for Security. Provides event collection, viewing, and reporting capability for network devices. Used with the IDS MC.

sensing interface	The interface on the sensor that monitors the desired network segment. The sensing interface is in promiscuous mode; it has no IP address and is not visible on the monitored segment.
sensor	The sensor is the intrusion detection engine. It analyzes network traffic searching for signs of unauthorized activity.
SensorApp	A component of the IPS. Performs packet capture and analysis. SensorApp analyzes network traffic for malicious content. Packets flow through a pipeline of processors fed by a producer designed to collect packets from the network interfaces on the sensor. Sensorapp is the standalone executable that runs Analysis Engine.
Service engine	Deals with specific protocols, such as DNS, FTP, H255, HTTP, IDENT, MS RPC, MS SL. NTP, RPC, SMB, SNMP, and SSH.
service pack	Used for the release of defect fixes and for the support of new signature engines. Service packs contain all of the defect fixes since the last base version (minor or major) and any new defects fixes.
session command	Command used on routers and switches to provide either Telnet or console access to a module in the router or switch.
SFP	Small Form-factor Pluggable. Often refers to a fiber optic transceiver that adapts optical cabling to fiber interfaces. See GBIC for more information.
signature fidelity rating	SFR. A weight associated with how well a signature might perform in the absence of specific knowledge of the target. The signature fidelity rating is configured per signature and indicates how accurately the signature detects the event or condition it describes.
shun command	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection. It is used by ARC when blocking with a PIX Firewall.
signature	A signature distills network information and compares it against a rule set that indicates typical intrusion activity.
signature engine	A component of the sensor that supports many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values.
signature engine update	Executable file with its own versioning scheme that contains binary code to support new signature updates.
Signature Event Action Filter	Subtracts actions based on the signature event signature ID, addresses, and risk rating. The input to the Signature Event Action Filter is the signature event with actions possibly added by the Signature Event Action Override.
Signature Event Action Handler	Performs the requested actions. The output from the Signature Event Action Processor is the actions being performed and possibly an evIdsAlert written to the Event Store.
Signature Event Action Override	Adds actions based on the risk rating value. The Signature Event Action Override applies to all signatures that fall into the range of the configured risk rating threshold. Each Signature Event Action Override is independent and has a separate configuration value for each action type.
Signature Event Action Processor	Processes event actions. Event actions can be associated with an event risk rating threshold that must be surpassed for the actions to take place.

signature update   Executable file that contains a set of rules designed to recognize malicious network activities, such as worms, DDOS, viruses, and so forth. Signature updates are released independently, are dependent on a required signature engine version, and have their own versioning scheme.

SMB   Server Message Block. File-system protocol used in LAN manager and similar NOSs to package data and exchange information with other systems.

SMTP   Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SN   Serial Number. Part of the UDI. The SN is the serial number of your Cisco product.

SNAP   Subnetwork Access Protocol. Internet protocol that operates between a network entity in the subnetwork and a network entity in the end system. SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks. The SNAP entity in the end system makes use of the services of the subnetwork and performs three key functions: data transfer, connection management, and QoS selection.

sniffing interface   See sensing interface.

SNMP   Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP2   SNMP Version 2. Version 2 of the network management protocol. SNMP2 supports centralized and distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.

software bypass   Passes traffic through the IPS system without inspection.

source address   Address of a network device that is sending data.

SPAN   Switched Port Analyzer. Feature of the Catalyst 5000 switch that extends the monitoring abilities of existing network analyzers into a switched Ethernet environment. SPAN mirrors the traffic at one switched segment onto a predefined SPAN port. A network analyzer attached to the SPAN port can monitor traffic from any other Catalyst switched port.

spanning tree   Loop-free subset of a network topology.

SQL   Structured Query Language. International standard language for defining and accessing relational databases.

SRAM   Type of RAM that retains its contents for as long as power is supplied. SRAM does not require constant refreshing, like DRAM

SRP   Stream Reassembly Processor. Reorders TCP streams to ensure the arrival order of the packets at the various stream-based inspectors. It is also responsible for normalization of the TCP stream. The normalizer engine lets you enable or disable alert and deny actions.

SSH   Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.

SSL   Secure Socket Layer. Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

Stacheldraht   A DDoS tool that relies on the ICMP protocol.

State engine	Stateful searches of HTTP strings.
String engine	A signature engine that provides regular expression-based pattern inspection and alert functionality for multiple transport protocols, including TCP, UDP, and ICMP.
subsignature	A more granular representation of a general signature. It typically further defines a broad scope signature.
surface mounting	Refers to attaching rubber feet to the bottom of a sensor when it is installed on a flat surface. The rubber feet allow proper airflow around the sensor and they also absorb vibration so that the hard-disk drive is less impacted.
switch	Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data link layer of the OSI model.
SYN flood	Denial of Service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.
system image	The full IPS application and recovery image used for reimaging an entire sensor.

T

TAC	A Cisco Technical Assistance Center. There are four TACs worldwide.
TACACS+	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TCPDUMP	The TCPDUMP utility is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can use different options for viewing summary and detail information for each packet. For more information see http://www.tcpdump.org/.
TCP reset interface	The interface on IDSM-2 that can send TCP resets. On most sensors the TCP resets are sent out on the same sensing interface on which the packets are monitored, but on IDSM-2 the sensing interfaces cannot be used for sending TCP resets. On the IDSM-2 the TCP reset interface is designated as port 1 with Catalyst software, and is not visible to the user in Cisco IOS software. The TCP reset action is only appropriate as an action selection on those signatures that are associated with a TCP-based service.
Telnet	Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
terminal server	A router with multiple, low speed, asynchronous ports that are connected to other serial devices. Terminal servers can be used to remotely manage network equipment, including sensors.
TFN	Tribe Flood Network. A common type of DoS attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.
TFN2K	Tribe Flood Network 2000. A common type of DoS attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.

TFTP	Trivial File Transfer Protocol. Simplified version of FTP that lets files be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
three-way handshake	Process whereby two protocol entities synchronize during connection establishment.
threshold	A value, either upper- or lower-bound that defines the maximum/minimum allowable condition before an alarm is sent.
TLS	Transport Layer Security. The protocol used over stream transports to negotiate the identity of peers and establish encrypted communications.
TNS	Transparent Network Substrate. Provides database applications with a single common interface to all industry-standard network protocols. With TNS, database applications can connect to other database applications across networks with different protocols.
topology	Physical arrangement of network nodes and media within an enterprise networking structure.
TPKT	Transport Packet. RFC 1006-defined method of demarking messages in a packet. The protocol uses ISO transport services on top of TCP.
threat rating	TR. A value between 0 and 100 that represents a numerical decrease of the risk rating of an attack based on the response action that depicts the threat of an alert on the monitored network.
traceroute	Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393.
traffic analysis	Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.
Traffic ICMP engine	Analyzes traffic from nonstandard protocols, such as TFN2K, LOKI, and DDOS.
trap	Message sent by an SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.
Trojan engine	Analyzes traffic from nonstandard protocols, such as BO2K and TFN2K.
trunk	Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.
trusted certificate	Certificate upon which a certificate user relies as being valid without the need for validation testing; especially a public-key certificate that is used to provide the first public key in a certification path.
trusted key	Public key upon which a user relies; especially a public key that can be used as the first public key in a certification path.
tune	Adjusting signature parameters to modify an existing signature.
target value rating	TVR. A weight associated with the perceived value of the target. The target value rating is a user-configurable value (zero, low, medium, high, or mission critical) that identifies the importance of a network asset (through its IP address).

U

UDI Unique Device Identifier. Provides a unique identity for every Cisco product. The UDI is composed of the PID, VID, and SN. The UDI is stored in the Cisco IPS ID PROM.

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

unblock To direct a router to remove a previously applied block.

unvirtualized sensing interface An unvirtualized sensing interface has not been divided into subinterfaces and the entire interfaces can be associated with at most one virtual sensor.

UPS Uninterruptable Power Source.

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

V

VACL VLAN ACL. An ACL that filters all packets (both within a VLAN and between VLANs) that pass through a switch. Also known as security ACLs.

VID Version identifier. Part of the UDI.

VIP Versatile Interface Processor. Interface card used in Cisco 7000 and Cisco 7500 series routers. The VIP provides multilayer switching and runs Cisco IOS. The most recent version of the VIP is VIP2.

virtual sensor A logical grouping of sensing interfaces and the configuration policy for the signature engines and alarm filters to apply to them. In other words, multiple virtual sensors running on the same appliance, each configured with different signature behavior and traffic feeds.

virtualized sensing interface A virtualized interface has been divided into subinterfaces each of which consists of a group of VLANs. You can associate a virtual sensor with one or more subinterfaces so that different intrusion prevention policies can be assigned to those subinterfaces. You can virtualize both physical and inline interfaces.

virus Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—that is, inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

virus update A signature update specifically addressing viruses.

VLAN Virtual Local Area Network. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VTP VLAN Trunking Protocol. Cisco Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis.

VMS   CiscoWorks VPN/Security Management Solution. A suite of network security applications that combines web-based tools for configuring, monitoring, and troubleshooting enterprise VPN, firewalls, network intrusion detection systems and host-based intrusion prevention systems.

VoIP   Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

VPN   Virtual Private Network(ing). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

VTP   VLAN Trunking Protocol. A Cisco Layer 2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis.

vulnerability   One or more attributes of a computer or a network that permit a subject to initiate patterns of misuse on that computer or network.

W

WAN   wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

WHOIS   A TCP-based query/response protocol used for querying an official database to determine the owner of a domain name or an IP address.

Wireshark   Wireshark is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, see http://www.wireshark.org.

watch list rating   WLR. A weight associated with the CSA MC watch list in the range of 0 to 100 (CSA MC only uses the range 0 to 35).

worm   A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

X

X.509   Standard that defines information contained in a certificate.

XML   eXtensible Markup Language. Textual file format used for data interchange between heterogeneous hosts.

Z

zone   A set of destination IP addresses sorted into an internal, illegal, or external zone used by anomaly detection.