Security Glossary

Additional Resources

These terms have been reviewed and approved by the Security Glossary Board.

To add a new term or update an existing term, see how to Submit a Term to the Security Glossary.

Question, comment, or suggestion? Email us your feedback!

- Cisco Technical Content Style Guide
- Customer-Facing Names for Firepower Appliances
- Security Glossary Wiki - Cisco Employee Communities

#

3DES (Triple Data Encryption Standard)

Products	Any
Definition	A stronger version of DES, which is the default encryption method for SSH version 1.5. Used when establishing an SSH session with the appliance. 3DES is a protocol that can be used to encrypt data in a VPN tunnel between two devices.
Usage	Docs—Expand on first use: 'Triple DES' GUI—Do not expand.

A

ABR (Area Border Router)

Products	ASA, Firepower
Definition	In OSPF, a router with interfaces in multiple areas.
Usage	Docs—Expand on first use. GUI—Do not expand.

access control

Products	ASA, CDO, Firepower
Definition	A policy-based feature that allows you to inspect, log, and direct network traffic. Also considered a security concept that concerns those firewall services and policies and rules that allow or deny network traffic to flow between internal and external networks.
Usage	Do not leave out 'control,' that is, Firepower has access control policies and access control rules, not access policies or access rules. Do not use NGIPS as a synonym for access control.

access policy

Products	WSA
Definition	Access policies block, allow, or redirect inbound HTTP, FTP, and decrypted HTTPS traffic. Access policies also manage inbound encrypted HTTPS traffic if the HTTPS proxy is disabled.
Usage	Example: "It is possible for an access policy to define policy membership by a predefined URL category and for the access policy to perform an action on the same URL category."

ACE (access control entry)

Products	ASA

Definition

An ACE evaluates network traffic using one or more characteristics, including source and destination IP address, IP protocol, ports, EtherType, and other parameters, depending on the type of ACL. By default, traffic that is not explicitly permitted is denied.

The ASA stores ACEs like this and each entry is also considered an access control entry. Consider the ACE `permit ip Foo Bar` where these are the object groups:

```
object-group Foo
192.168.10.1
192.168.10.2
object-group Bar
10.10.20.1
10.10.20.2
```

ASA stores the ACE like this:

```
permit ip 192.168.10.1 10.20.1.1
permit ip 192.168.10.1 10.20.1.2
permit ip 192.168.10.2 10.20.1.1
permit ip 192.168.20.2 10.20.1.2
```

Note The running config shows: `access-list permit_foo_bar extended permit ip object Foo object Bar`

So, this example doesn’t imply that 4 individual entries are entered into the running config, they're just stored on the ASA that way.

Usage

Docs—Expand on first use.

ACL (access control list)

Products

ASA

Definition

One or more access control entries (ACEs) that identify traffic flows by one or more characteristics, including source and destination IP address, IP protocol, ports, EtherType, and other parameters, depending on the type of ACL.

ACLs are named or numbered.

ASA has these types of ACLs:

- extended ACL
- standard ACL
- webtype ACL
- EtherType ACL

ACS server

Products

Any

Definition	The Cisco Secure Access Control System (ACS) server is a RADIUS security server that is the centralized control point for managing network users, network administrators, and network infrastructure resources. This product has reached its end-of-life. Migration path is to the Cisco Identity Services Engine (ISE).
Usage	Docs—Expand on first use.

action (rule action)

Products	Firepower
Definition	A component of a rule that determines how the system handles traffic that matches the rule.
Usage	Both 'action' and 'rule action' are acceptable, depending on context. You can use the name of the action to describe a rule, for example, 'block rule' or 'allow rule.'

actionable intelligence

Products	Threat Grid
Definition	The prioritization, remediation, and attribution of risk from malware that allows you to clean up, prioritize, remediate, and prevent threats more effectively in the future.
Usage	Example: "The analysis report provides detailed, actionable intelligence used by malware analysts and security teams to identify and prioritize potential threats."

active host

Products	Stealthwatch
Definition	A host that is known to the Stealthwatch Flow Collector and that has transmitted a data packet in the last 5 minutes. Contrast with 'inactive host.'

actor

Products	ATS, Stealthwatch
Definition	See 'threat actor.'

Advanced Persistent Threat

Products	Cognitive, Stealthwatch

Definition	Attack against a network during which an unauthorized person gains access and remains undetected for an extended period of time. The purpose of the attack is to illicitly obtain data, such as financial or competitive information, rather than to cause damage to the network.
Usage	Docs—Expand on first use. Thereafter, can be shortened to APT.

affected

Products	Cognitive
Definition	A term used to describe an asset or host when it has been touched by a finding, ranging from anomalous observed data to a threat or malware.
Usage	Do not use if redundant or implied in context. For example, on a page showing what anomalous data was observed on which assets in the network, avoid using 'affected asset' if 'asset' is sufficient.

alarm

Products	Stealthwatch Enterprise
Definition	A notification of unusual network activity or event that meets or exceeds a defined set of criteria that can indicate unacceptable behavior on your network.
Usage	Use as a noun.

alarm category

Products	Stealthwatch Enterprise
Definition	A “bucket” toward which a defined list of security events contributes. When network activity meets or exceeds a defined set of criteria specified, it triggers an alarm. Contains only host alarms. Alarm categories contain only host alarms. A host alarm is a security event that has triggered an alarm.

alert

Products	Any
Definition	A type of alarm to prepare for action, or to warn of an approaching threat. To be on the alert is to be on the lookout for danger and ready to act. See also 'alarm.'

allow (rule action)

Products	Firepower

Definition

A rule action that allows matching traffic to continue to the next stage of analysis or handling.

Note that an allow rule does not necessarily allow traffic to continue directly to its destination. For example, traffic that is allowed by a Firepower access control rule is still subject to network discovery, identity requirements, intrusion inspection, malware inspection, and rate limiting (QoS).

Contrast 'allow' with the 'trust' and 'fastpath' actions, which bypass more inspection.

Usage

Examples: allow rule, allow action, allow rule action

allow/allowed list

Products

Any

Definition

A list of senders, domains, or applications that are allowed or permitted access.

For example:

- In the SMA, the list specifies senders and domains that are never treated as spam.
- In the ESA, the list specifies known good senders that are not subjected to anti-spam scanning or rate limiting by the $TRUSTED mail flow policy.
- In Umbrella, this is a type of destination list with approved DNS addresses.

Contrast with 'block list' and 'blocked list.'

Usage

Synonyms: safelist, whitelist (do not use)

Standardize use around 'allow list' (to mean a list that allows).

In cases where it makes more sense, it's okay to use 'allowed list' (to mean a list of allowed items).

AMP (Advanced Malware Protection)

Products

AMP

Definition

Protective technology that monitors files, processes, memory, and network connections to detect and block known and unknown threats based on a variety of engines.

analysis engine

Products

Any

Definition

A process that takes information from sensors and processes it. Subtypes include:

- detection engine—consumes information (such as events, telemetry, and intelligence) and produces alerts
- enforcement engine—controls which activity on a network or an endpoint can take place (may also be known as enforcement agent or controller)
- enrichment engine—takes events and alerts and combines them with other data to annotate and aggregate them to support actions (such as triage and response)
- intelligence engine—extracts threat intelligence (in forms such as judgments and indicators) from a flow of information
- statistics engine—summarizes and generates telemetry from a flow of events and alerts
- triage engine—takes events and alerts, and escalates them into incidents, or otherwise helps to classify and filter them for presentation

Usage

Do not abbreviate intelligence as intel.

If the customer does not need to distinguish between multiple engines in order to choose one, you can refer to it as 'the engine' or 'the system' for simplicity.

analyze (rule action)

Products

Firepower

Definition

A rule action that allows matching traffic to continue to the next stage of analysis or handling.

Firepower prefilter policies use the analyze action instead of the allow action.

Usage

Examples: analyze rule, analyze action, analyze rule action

ancestor policy

Products

Firepower

Definition

A policy that has one or more descendant policies of the same type. These descendant policies inherit settings from the ancestor policy.

See also 'parent policy.'

anomalous observed data

Products

Cognitive

Definition	Information or event that was observed or happened in the network, that deviates from the baseline of normal network behavior monitored and established by the Cognitive system. Contrast with 'sighting,' which implies recognition.

anomaly

Products	Any
Definition	A deviation from what's normal or expected. For instance, in Cognitive Intelligence, an anomaly is any unusual activity, trend, or event found by real-time monitoring or offline analysis of network property or entity behaviors.

AnyConnect local policy

Products	AnyConnect
Definition	Determines when AnyConnect software and profile updates can occur, as well as when to exclude certificate stores, enable FIPS mode, restrict caching, and so on.

APCF (Application Profile Customization Framework)

Products	ASA
Definition	Lets a security appliance handle nonstandard applications so that they render correctly over a WebVPN connection.
Usage	Docs—Expand on first use.

app

Products	Cloudlock, Umbrella
Definition	A computer program generally accessed using web browsers in desktop operating systems, and natively on mobile devices. Apps are often associated with cloud services, and frequently offer limited and/or targeted functionality. Apps may not be versioned, particularly when they represent the user interface for a cloud-based service. Contrast with 'application.'
Usage	Can be used collectively, as in "...create a policy to block all social media apps in your environment." When referring to a specific app, use its trade name alone where possible ("...log in using Facebook", not "...log in using the Facebook app").

appliance

Products	Any

Definition	A device designed to perform a task such as protect computer networks from unwanted traffic.
Usage	Use the term 'device' instead. Avoid using 'appliance' and 'security appliance' as they are legacy terms. 'Appliance' is the hardware version of the ASA, and 'device' is the virtual version. Use 'appliance' or 'security appliance' if you need to specifically refer to the product name. For example, Cisco Adaptive Security Appliance.

application

Products	Cloudlock, Umbrella
Definition	A computer program that runs natively in a desktop operating system. Applications are generally versioned. Contrast with 'app.'
Usage	When referring to a specific application, use its trade name alone where possible ("...open the file using Microsoft Excel", not "...open the file using the Excel application"). Do not use 'application program.'

archive hour

Products	Stealthwatch
Definition	User-defined time when each Stealthwatch Flow Collector in the domain resets itself. Acceptable values are 0 to 23, where 0 is midnight local time. At the defined time, the Flow Collector resets all index counts to zero, saves the log and web files it has gathered during the preceding 24 hours, and then begins a new day (24 hours) of data collection. Defined on the Domain page of the Domain Properties dialog.

artifact

Products	AMP, Threat Grid
Definition	A file or other object generated by a submitted sample during analysis. An artifact may be any type of file, such a Word document, a graphic (.png, .jpg, etc.), or a downloaded executable. An artifact may be a file-like object, such as an image of a process running in memory. An artifact may be a SHA256, or an IP address or domain implicated in a compromise.
Usage	Example: "Artifacts are listed in the sample analysis report."

ASA (Adaptive Security Appliance)

Products	ASA
Definition	Combines firewall, VPN concentrator, and intrusion prevention into one software image. Operates in single mode and multimode.

Usage	Docs—Use 'adaptive security appliance' on first reference when referring to the hardware. Thereafter, use 'security appliance' or 'appliance.' Use ASA when referring to ASA models, for example: ASA 5508.

ASA FirePOWER

Products	Firepower
Definition	The short name for ASA with FirePOWER Services.
Usage	Docs—Use 'Cisco ASA with FirePOWER Services' for the first use. Then, you can say 'an ASA FirePOWER device' or just 'ASA FirePOWER.' Do not use 'onbox' or 'Elektra.'

ASA with FirePOWER Services

Products	Firepower
Definition	An ASA device running an ASA FirePOWER module (NGIPS).
Usage	Do not use 'onbox' or 'Elektra.'

ASDM (Adaptive Security Device Manager)

Products	ASA, Firepower
Definition	An application for managing and configuring a single ASA.
Usage	Docs—Expand on first use.

asset

Products	Cognitive
Definition	A component of the network environment, such as hardware, software, and information, that enables and supports the communication of data. In business terminology, something the business can put value on and hence evaluate the risk of a finding.

authenticate

Products	Any
Definition	Validate that a user, device, or software process is who or what they say they are based on credentials, such as password, digital certificate, biometrics, or some combination.

authorized network

Products

Threat Grid

Definition

A network that has been authorized for organization members (including devices) to access the Threat Grid Panacea server. Defined in the Authorized Networks field on the Organization page.

autostate

Products

ASA

Definition

In normal autostate mode, the Layer 3 interfaces remain up if at least 1 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.

AVC (Application Visibility and Control)

Products

Firepower

Usage

Docs—Expand on first use.

GUI—Always spell out, unless it's in a part of the GUI that's all about AVC, such as when a page title already clearly identifies the context as Application Visibility and Control, then you can abbreviate as needed.

B

backhaul

Products

Umbrella

Definition

Refers to the idea that traffic is not directed immediately to its ultimate destination (for example, facebook.com), but is first routed through a nonoptimal hop- like NGFW running at the central datacenter, or the idea that all traffic from a remote office goes through the central office before heading out to the internet.

Often referred to when VPN traffic gets routed through the central node before letting it back out to the ultimate destination on the public internet.

Usage

Use as a verb.

backplane

Products

Hardware

Definition

The physical connection between an interface processor or card and the data buses and the power distribution buses inside a chassis.

Usage

Do not use to describe the back of the chassis.

base policy

Products

Firepower

Definition

If you're configuring policy inheritance or policy layers, the base policy is the lowest-level policy in the stack. Other policies of the same type inherit rules and settings from the base policy.

behavioral indicator

Products

Threat Grid

Definition

Key traits and behaviors that have been identified as indicators of malicious activity. Behavioral indicators include threat severity levels, HTTP traffic, DNS traffic, TCP/IP network sessions, processes, artifacts, registry activities, and more.

Usage

Do not abbreviate. Always spell out.

Do not use 'behavior' or the British spelling (behavioural).

Can be used interchangeably with IOC (indicators of compromise).

BIOS (Basic Input/Output System)

Products

Hardware

Definition

The program that starts the sensor and communicates between the devices in the appliance and the system.

Usage

Do not expand.

blacklist

Usage

Do not use. Instead, standardize use around 'block list' (to mean a list that blocks).

In cases where it makes more sense, it's okay to use 'blocked list' (to mean a list of blocked items).

block (rule action)

Products

Firepower

Definition

A rule action that blocks matching traffic without further inspection of any kind.

Usage

Examples: block rule, block action, block rule action

You can use 'block rule' as a bucket for block rules and block with reset rules, when the 'reset' part is irrelevant.

block/blocked list

Products

Any

Definition

A list of senders, domains, or applications that are blocked or restricted from access.

For example, in the ESA, the list specifies known bad senders that get rejected by the $BLOCKED mail flow policy.

Contrast with 'allow list' and 'allowed list.'

Usage

Synonyms: blocklist, blacklist (do not use)

Standardize use around 'block list' (to mean a list that blocks).

In cases where it makes more sense, it's okay to use 'blocked list' (to mean a list of blocked items).

block page bypass code

Products

Umbrella

Definition

A code that can be given to certain individuals (or a group of individuals) to allow them to go to some or all blocked websites until the code expires.

Usage

Can be shortened to 'bypass code.'

block page bypass user

Products

Umbrella

Definition

A special user account that gives the rights to certain individuals (or a group of individuals) to go to blocked sites while still being part of the enforcement given to the larger policy group they belong to. For users of the Umbrella dashboard, it is a similar—but distinctly different—concept to Grant Permissions to a User in the Umbrella dashboard.

block with reset (rule action)

Products

Firepower

Definition

A rule action that blocks matching traffic without further inspection of any kind, and resets the connection.

Usage

Examples: block with reset rule, block with reset action, block with reset rule action

You can use 'block rule' as a bucket for block rules and block with reset rules, when the 'reset' part is irrelevant.

botnet

Products

Any

Definition

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.

box

Usage

Do not use to refer to an appliance, chassis, or device.

BPDU (bridge protocol data unit)

Products

ASA, Firepower

Definition

Spanning tree protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.

Protocol data unit is the OSI term for packet.

Usage

Docs—Expand on first use.

GUI—Do not expand.

brownfield

Usage

Do not use. Instead, standardize use around 'existing deployment.'

See also 'greenfield.'

bypass mode

Products

Any

Definition

Mode that lets packets continue to flow through the appliance even if the appliance fails. Bypass mode is only applicable to inline-paired interfaces.

Usage

Do not abbreviate. Always spell out.

byte distribution

Products	ETA
Definition	Histogram giving the frequency of occurrence for each byte value, or range of values, in the first N bytes of application payload for a flow.

C

CA (certificate authority)

Products	Any
Definition	The certificate issuer used to create server certificates or user public key certificates. Server and user certificates provide an additional confirmation of a server or a user identity. A third-party entity that is responsible for issuing and revoking certificates. Each host with the public key of the CA can authenticate a host that has a certificate issued by the CA. The term CA also refers to software that provides CA services.
Usage	Synonym: certification authority Docs—Expand on first use.

CA certificate

Products	Any
Definition	Certificate for one CA issued by another CA.

CacheCheck

Products	Umbrella
Definition	Tool that allows internet users insight into what is happening in their DNS, empowering them to manually refresh DNS caches on their own. When a domain is failing and a website appears to be down, internet users can refresh the massive Umbrella caches and update them with the most current addresses for websites, in many cases enabling access automatically.
Usage	Use camel case: CacheCheck

CASB (Cloud Access Security Broker)

Products	CWS, WSA

Definition	Placed between cloud service providers and their consumers, a CASB enforces security policies as cloud-based resources are being accessed, thereby addressing cloud service risks, even when cloud services are beyond the enterprise perimeter and out of the organization's direct control.
Usage	Docs—Expand on first use.

CC (Common Criteria)

Products	Hardware, Software
Definition	An international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments.
Usage	Docs—Expand on first use.

Centralized Settings

Products	Umbrella
Definition	From Umbrella service provider consoles (MSP, MSSP, ISP, Multi-Org), these settings are applied to a customer’s Umbrella policy settings (default policy or all policies depending on settings). They can be applied concurrently to multiple customers, including new customers as they come on board.
Usage	Upper case when referring to console feature.

certificate

Products	Any
Definition	A signed cryptographic object that contains the identity of a user or device and the public key of the CA that issued the certificate. Certificates have an expiration date and may also be placed on a CRL if known to be compromised. Certificates also establish nonrepudiation for IKE negotiation, which means that you can prove to a third party that IKE negotiation was completed with a specific peer.
Usage	Do not abbreviate. Always spell out.

certificate authentication

Products	AnyConnect

Definition	The use of a digital certificate to identify users, appliances (that need to communicate with back-end services), desktops, laptops, and any mobile devices before granting access to a resource, network, application, and so on. The certificates are stored locally on the device. Unlike other solutions that only work for users (like biometrics or username/password), the same solution can be used for all endpoints.

certificate matching

Products	AnyConnect
Definition	Those certificates that match a specific set of keys established in the AnyConnect client profile with criteria such as key usage, extended key usage, and distinguished name.

CHAP (Challenge Handshake Authentication Protocol)

Products	ESA, SMA
Definition	An authentication protocol for communicating with the RADIUS server for configuring external authentication or two-factor authentication on the appliance.
Usage	Docs—Expand on first use.

chassis

Products	Any
Definition	A physical structure that houses the hardware components.
Usage	Use in procedures where components are added to or removed from the chassis. Also used in the name FXOS Firepower Chassis Manager.

child policy

Products	Firepower
Definition	A descendant policy that inherits rules and settings from its *immediate* ancestor, or *parent*, policy.
Usage	Use 'child' only if you're talking about a policy and its immediate ancestor policy. Otherwise, use 'descendant policy.' Do not use 'grandchild policy' or other such variations.

CIMC

Products	Threat Grid

Definition

Cisco Integrated Management Controller

Usage

Docs—Expand on first use.

GUI—Do not expand.

Cisco DNA (Digital Network Architecture)

Products

Any

Definition

Cisco’s enterprise architecture for intent-based networking across the campus, branch, WAN, and extended enterprise.

Cisco DNA is the core architecture that is the platform for software innovations and infrastructure.

The Cisco DNA architecture is delivered through:

- Cisco DNA Center: command and control for policy, automation, and analytics
- Cisco DNA Solutions: SD-Access, SD-WAN, and Assurance and Network Security
- Cisco DNA-ready physical and virtual infrastructure: switching, routing and wireless

Usage

Use camel case: Cisco DNA

When referring to Cisco DNA or Cisco DNA products and solutions, the complete term 'Cisco DNA' must be used.

'DNA' must be preceded by 'Cisco' in all content, diagrams, flow charts, presentations, keynotes, and so on.

Cisco IOS (Internetwork Operating System)

Products

Any

Definition

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.

Usage

Do not expand.

Cisco Threat Response

Products

Threat Response

Definition	An investigative tool that leverages AMP, Investigate, Talos, Threat Grid, and other Cisco and 3rd party products and services, to simplify and speed up common incident response tasks by automating and collating research and response functions across those multiple products and tools.
Usage	Do not abbreviate. Always spell out. Formerly known as Visibility.

Cisco TrustSec

Products	Solution including ASA
Definition	Provides access control that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the feature, enforcement devices use a combination of user attributes and endpoint attributes to make role-based and identity-based access control decisions. The availability and propagation of this information enables security across networks at the access, distribution, and core layers of the network. https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
Usage	Docs—Expand on first use: Cisco TrustSec. Thereafter, can be shortened to TrustSec. GUI—Use TrustSec. Do not abbreviate as CTS.

Cisco Umbrella

Products	Umbrella
Definition	Cloud-based security platform that uses the internet's infrastructure to block malicious destinations before a connection is ever established. Umbrella builds on a flexible, scalable cloud platform to continuously evolve ahead of the pace of threats, providing cloud-delivered network security for any device, anywhere, anytime.
Usage	Docs—Expand on first use. Can be shortened to Umbrella.

Cisco VRT

Products	Firepower
Definition	Cisco Vulnerability Research Team
Usage	Do not use. See 'Talos.'

claimed (CDO)

Products	CDO
Definition	Used in the context of CDO and serial number onboarding: A device is 'claimed' if its serial number has been onboarded to a CDO tenant.

class map

Products	ASA
Definition	Used for Modular Policy Framework; the class map, using an ACL or other criteria, matches traffic for a service policy.

client policy

Products	AnyConnect
Definition	Determines various options in the Network Access Manager, such as connection settings, media types, end user controls, and administrative status.

cluster (Cognitive)

Products	Cognitive
Definition	Incidents that have similar malware symptoms and correlated behaviors are grouped into a cluster.
Usage	May also be referred to as an 'incident group' or 'threat cluster.'

cluster (Threat Grid Appliance)

Products	Threat Grid Appliance
Definition	Two or more appliances joined together and saving data in a shared file system such that all nodes have the same data as the other nodes in the cluster. The main goal of clustering is to increase the capacity and scalability of a single system by joining several appliances together, and to support redundancy and recovery from failure.
Usage	Use as a noun or verb. For clustering, do not use 'master' and 'slave.' Instead, use 'control' and 'data.'

collection name

Products	ESA
Definition	The name of a collection of threat feeds that is hosted on the TAXII server. For example, 'guest.Abuse.ch.'

command-and-control callback

Products	Umbrella
Definition	Cisco Umbrella blocks the command-and-control callbacks made by the botnet to prevent compromised devices from communicating with the attackers' infrastructure.
Usage	Docs—Expand on first use. Thereafter, can be shortened to 'C&C callback.'

command-and-control server

Products	Cognitive
Definition	Server controlled by an attacker which is used to remotely send commands to a network of devices infected by malware or botnet.
Usage	Docs—Expand on first use. Thereafter, can be shortened to 'C&C server.'

compromised

Products	AMP for Endpoints
Definition	When a computer or device is in a hazardous or objectionable state as the result of one or more potentially related events, such as malware infection, credential theft, and so on.

computer

Products	Any
Definition	An outside computer, not the Cisco product.
Usage	When you want to use a more informal tone, or if there's limited space, use the term 'PC' to refer to only Windows-based computers. If the docs or GUI applies to both Windows-based and Mac computers or only Mac computers, use the term 'computer.'

concern index

Products	Stealthwatch
Definition	Primary means by which the system notifies you of suspicious activity. The Stealthwatch Flow Collector adds points to the concern index whenever it observes possible attacks on one or more hosts. The greater the concern index, the greater the level of concern over that behavior. When activity surpasses 100% of the index threshold set for a particular host, the Flow Collector generates a High Concern Index alarm against that host. See also 'alarm.'
Usage	Do not abbreviate. Always spell out.

connection failure policy

Products	AnyConnect
Definition	This policy blocks traffic if a connection to the Cisco Cloud Web Security proxy server cannot be established or allows traffic when it can.

connection profile

Products	AnyConnect
Definition	Determines how the user connects to the headend and to which tunnel group based on both its authentication and authorization configuration.

connect on demand

Products	AnyConnect
Definition	How Apple iOS checks other applications that start network connections, using the Domain Name System (DNS) and how match domain and host are defined.
Usage	Do not hyphenate.

console

Products	Any
Definition	A window in which the user interacts with an application or device using a command line interface.
Usage	Synonym: terminal window Related: console port

console (Umbrella)

Products	Umbrella
Definition	Web-based portion of the service provider products through which the user interacts with the software, configuring and monitoring the system. The parent org uses the console, child the dashboard.
Usage	Examples: MSP console, MSSP console, ISP console, Multi-Org console

console port

Products	Any

Definition	A physical interface on an appliance into which you plug an Ethernet or other cable so that you can administer a device, or an application on that device, using a console.

content category

Products	Umbrella
Definition	A grouping of websites with similarly themed content matching one of the types listed here: https://support.umbrella.com/hc/en-us/articles/231265768-Getting-Started-Category-Settings-and-Content-Category-Details
Usage	Sometimes referred to as just category.

content filter

Products	ESA
Definition	Used to process messages during the Per-Recipient Scanning phase of the work queue in the email pipeline. Content filters are evoked after Message filters and act on individual, splintered messages.

content matching classifier

Products	ESA
Definition	The detection component of the data loss prevention scanning engine. A classifier contains a number of rules for detecting sensitive data, along with context rules that search for supporting data. For example, a credit card classifier not only requires that the message contain a string that matches a credit card number, but that it also contains supporting information such as an expiration data, a credit card company name, or an address.

control subject

Products	Threat Grid
Definition	Internal convention for a virtual machine image used for sample analysis.
Usage	GUI—Do not use.

conversational bounce

Products	ESA
Definition	A bounce that occurs within the SMTP conversation. The two types of conversational bounces are hard bounces and soft bounces: • hard bounce—a message that is permanently undeliverable • soft bounce—a message that is temporarily undeliverable

coordinates

Products	Cognitive
Definition	An incident is located by coordinates that describe where and when the incident happened. With sufficient granularity, you can use the coordinates to locate the incident and correlate with other systems. Coordinates are composed of username, IP address, or MAC address coupled with a corresponding time span. For example, IP address 10.0.0.1 from Thursday to Friday. A single set of coordinates may refer to only one incident at a time.

C-Rank

Products	Umbrella
Definition	Algorithmic classifier derived from co-occurrence patterns among domains. Co-occurrence of domains means that a statistically significant number of clients have requested both domains consecutively in a short time frame.
Usage	Avoid. Instead, use 'integrations.' When possible, be specific: ESA integration, Meraki integration, AMP for Endpoints Private Cloud integration, and so on.

CRL (Certificate Revocation List)

Products	Umbrella
Definition	A digitally signed message that lists all of the current but revoked certificates listed by a given CA. This is analogous to a book of stolen charge card numbers that allow stores to reject bad credit cards. When certificates are revoked, they are added to a CRL. When you implement authentication using certificates, you can choose to use CRLs or not. Using CRLs lets you easily revoke certificates before they expire, but the CRL is generally only maintained by the CA or an RA. If you are using CRLs and the connection to the CA or RA is not available when authentication is requested, the authentication request fails.
Usage	Docs—Expand on first use.

CRUD (Create, Read, Update, and Delete)

Products	Any
Definition	This is a developer term used to describe the implementation of basic functionality. In computer programming, create, read, update, and delete are the four basic functions of persistent storage. Alternate words are sometimes used, such as retrieve instead of read, modify instead of update, and destroy instead of delete.

Usage	If possible, avoid using 'CRUD' in external, customer-facing documentation.

CSA integration

Products	Threat Grid
Definition	Other Cisco appliances and products, such as the ESA/WSA appliances, that connect with Threat Grid through the Cisco Sandbox API ("CSA API").
Usage	Avoid. Instead, use 'integrations.' When possible, be specific: ESA integration, Meraki integration, AMP for Endpoints Private Cloud integration, and so on.

CSM (Cisco Security Manager)

Products	CSM
Definition	The provisioning component of the Cisco Self-Defending Networks solution. CSM is fully integrated with CS-MARS.
Usage	Docs—Expand on first use.

CTIM (Cisco Threat Intelligence Model)

Products	Threat Response
Definition	Closely based on STIX, CTIM includes common data models used by Cisco Threat Intelligence services. Allows us to decompose the massive, comprehensive artifacts generated during malware sample analysis and extract the details most relevant to incident response into a data model specifically designed for rapid storage, retrieval, and enrichment.
Usage	Docs—Expand on first use.

CTIQBE (Computer Telephony Interface Quick Buffer Encoding)

Products	ASA
Definition	A protocol used in IP telephony between the Cisco CallManager and CTI TAPI and JTAPI applications. CTIQBE is used by the Cisco CallManager for call setup and voice traffic across the ASA.
Usage	If you need to explain this protocol, you can expand the acronym. Otherwise, this is like HTTP or RADIUS where it is not necessary to expand.

cut-through proxy

Products	ASA

Definition	Enables the ASA to provide faster traffic flow after user authentication. The cut-through proxy challenges a user initially at the application layer. After the ASA authenticates the user, it shifts the session flow and all traffic flows directly and quickly between the source and destination while maintaining session state information.
Usage	Always hyphenate cut-through. Cut-through is a compound modifier.

D

dashboard (Umbrella)

Products	Umbrella
Definition	Web-based portion of the Umbrella product through which the user interacts with the software to configure and monitor the system. In *SP, dashboard is what child org sees. Do not use dashboard for service provider consoles.

data collection policy

Products	AnyConnect
Definition	Determines what type of data (VPN, trusted, or untrusted) to send and whether the data (type, fields, or network state of the interface) is anonymized or not in NVM. The policy associates this data with a network type or connectivity scenario.

DCE (data circuit-terminating equipment)

Products	Any
Definition	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.
Usage	Do not expand.

decrypt (rule action)

Products	Firepower
Definition	A rule action that decrypts encrypted traffic and passes it to the next phase of analysis. There are two kinds of decrypt actions: • decrypt known key • decrypt re-sign

Usage

Examples: decrypt rule, decrypt action, decrypt rule action, decrypt known key rule, decrypt re-sign rule

decryption policy

Products

WSA

Definition

Decryption policies determine whether HTTPS transactions should be decrypted, dropped, or passed through.

Usage

Example: "If a decryption policy is configured to block servers with a low Web reputation score, then any request to a server with a low reputation score is dropped without considering the URL category actions."

default action

Products

Firepower

Definition

In a policy, the action the system uses when network traffic does not match any of that policy's rules or other settings.

delayed bounce

Products

ESA

Definition

A bounce that occurs within the SMTP conversation. The recipient host accepts the message for delivery, only to bounce it at a later time.

DES (data encryption standard)

Products

Any

Definition

Published in 1977 by the National Bureau of Standards and is a secret key encryption scheme based on the Lucifer algorithm from IBM. Cisco uses DES in classic crypto (40-bit and 56-bit key lengths), IPsec crypto (56-bit key), and 3DES (triple DES), which performs encryption three times using a 56-bit key. 3DES is more secure than DES but requires more processing for encryption and decryption.

See also 'AES' and 'ESP.'

Usage

Docs—Expand on first use.

descendant policy

Products

Firepower

Definition

A policy that inherits rules and settings from another policy of the same type.

See also 'child policy.'

Usage	Spell with an A: 'descendant.' Do *not* use an E: 'descendent.' See http://grammarist.com/usage/descendant-descendent/.

destination

Products	Any
Definition	Where the traffic is destined to arrive. A target network, host, port, domain, URL, or IP address for which a request is being made.
Usage	Do not abbreviate. Always spell out. For example, 'www.domain.com' is one type of destination.

destination list

Products	Umbrella
Definition	A list of destinations (for example, domain name, URL, or IP address) that is used to manage—block or allow—customer or organization access to specific internet destinations.
Usage	Use as a noun.

device

Products	Any
Definition	Generic term that may refer to a Cisco security product after you've officially introduced it. May also refer to a device connected to the Cisco security product to communicate with the network, such as a firewall, router, switch, or computer. Can be a physical hardware or virtual device.
Usage	Can use specific term with device. Examples: network device, managed device, mobile device

device (Threat Grid)

Products	Threat Grid
Definition	User. Each device is treated as a user record.

device user

Products	Threat Grid
Definition	Licensing authority for device entitlements.

Usage	GUI—Capitalize: Device User. Docs—Do not capitalize: device user.

digital certificate

Usage	See 'certificate.'

directional policy

Products	Stealthwatch Enterprise
Definition	A set of rules that offers additional control through the policy feature. It is a solution to either of the following scenarios when you are investigating a security event: • The behavior you discovered is of concern in general, but not for the current situation. • The behavior you discovered is of concern, but in only a few specific situations.

disposition

Products	Threat Response
Definition	Calculated from an analysis engine about the intent or nature of an observable: whether it's malicious, suspicious, unknown, common, clean, and so on.
Usage	The role of a disposition is different. It's more of an actionable statement, as opposed to a measure of threat. Here's a translation mapping between disposition in Threat Response and threat level in Talos:

Malicious	Untrusted
Suspicious	Questionable
Unknown	Neutral
Common	Favorable
Clean	Trusted
No judgement objected returned	Unknown

DLP (data loss prevention) incident

Products	ESA, Cloudlock
Definition	A data loss prevention incident occurs when a DLP policy detects one or more DLP violations that merit attention in an outgoing message.

Usage	Docs—Expand on first use.

DLP (data loss prevention) policy

Products	ESA, Cloudlock
Definition	A set of conditions used to determine whether content contains sensitive data and the actions that can be taken on the content that contains such data.
Usage	Docs—Expand on first use.

DLP (data loss prevention) violation

Products	ESA, Cloudlock
Definition	An instance of data being found in a message that violates your organization’s DLP rules.
Usage	Docs—Expand on first use. In Cloudlock, this is called a policy violation. The policy is a DLP policy, but Cloudlock does not use this specific terminology.

DNSCrypt

Products	Umbrella
Definition	Cisco Umbrella approach to securing the critical 'last mile' of DNS traffic and resolving an entire class of serious security concerns with the DNS protocol.
Usage	Use camel case: DNSCrypt

DNS-O-Matic

Products	Umbrella
Definition	A free service from Cisco Umbrella that gives you an easy way to distribute your dynamic IP changes to multiple services with a single update.

DoDIN APL (Department of Defense Information Network Approved Products List)

Products	Software
Definition	The DoDIN APL is the single approving authority for all Military Departments (MILDEPs) and DoD agencies in the acquisition of communications equipment that is to be connected to the Defense Information Systems Network (DISN) as defined by the Unified Capabilities Requirements (UCR).

Usage	Docs—Expand on first use. The DoD has changed the name of the list it uses for the procurement of IT products to be used over the DoD network infrastructures. Therefore, use DoDIN APL instead of Unified Capabilities Approved Products List (UC APL).

domain

Products	Any
Definition	An identification string that refers to one or more IP addresses. Registered in the Domain Name System (DNS) and used to provide recognizable names to numerically addressed resources on the internet. A domain is the name of a website.

do not decrypt (rule action)

Products	Firepower
Definition	A rule action that passes encrypted traffic to the next phase of analysis, without decrypting it.
Usage	Examples: do not decrypt rule, do not decrypt action, do not decrypt rule action

DoS (denial-of-service), DDoS (distributed denial-of-service)

Products	Any
Definition	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 disrupting access and denying service to the system to legitimate users.
Usage	Docs—Do not expand unless context requires it.

drive

Products	Hardware
Definition	Generic term to refer to a drive when it is not necessary to point out what specific drive it is.
Usage	Use as the generic term.

drop (rule action)

Products	Firepower

Definition	Block.
Usage	Avoid, except in legacy products and documentation.

drop and generate events

Products	Firepower
Definition	An intrusion rule action that drops (blocks) matching packets, and logs an intrusion event. You cannot block without logging. Contrast with the generate events action, which logs an intrusion event without dropping matching packets. An intrusion rule with a drop and generate events action is like an access control rule with a block action and logging enabled.
Usage	Avoid, except in legacy products and documentation.

DTP (Dynamic Trunking Protocol)

Products	Any
Definition	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.
Usage	Docs—Expand on first use.

dynamic analysis

Products	Threat Grid, Firepower
Definition	Sample analysis includes processes that capture any actions that are performed by the file. This is the dynamic analysis of the sample submission. For example, making a change to the registry, creating other files, launching executables, communicating with a remote IP address, generating other artifacts, and so on. Dynamic analysis also includes emulating user behavior with playbooks. These are canned sets of user behaviors, such as clicking the OK button in a dialog, which may be selected during sample submission. Many user actions will trigger malware. The results of running a playbook is part of the dynamic analysis.

dynamic NAT

Products	Any

Definition	Translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool typically includes fewer addresses than the real group. When a host you want to translate accesses the destination network, the ASA assigns the host an IP address from the mapped pool. The translation is added only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out.
Usage	Do not abbreviate 'dynamic NAT.'

dynamic PAT

Products	Any
Definition	Translates multiple real addresses to a single mapped IP address by translating the real address and source port to the mapped address and a unique port. Lets multiple outbound sessions appear to originate from a single IP address. With PAT enabled, the appliance dynamically chooses a unique port number from the PAT IP address for each outbound translation slot (xlate). This feature is valuable when an ISP cannot allocate enough unique IP addresses for your outbound connections. The global pool addresses always come first, before a PAT address is used.
Usage	Do not abbreviate 'dynamic PAT.'

E

egress

Products	Any
Definition	The action of traffic going out.
Usage	Verb: the packet egresses immediately Adjective: egress interface, egress security zone

EIGRP (Enhanced Interior Gateway Routing Protocol)

Products	Any
Definition	This is a Cisco-proprietary protocol. The ASA does not support EIGRP.
Usage	Docs—Expand on first use. GUI—Do not expand.

Email Security Manager

Products	ESA
Definition	A single, comprehensive dashboard to manage all email security services and applications on IronPort appliances. Email Security Manager lets you manage outbreak filters, anti-spam, anti-virus, and email content policies on a per recipient or per sender basis through distinct inbound and outbound policies.
Usage	Do not abbreviate. Always spell out.

EMBLEM (Enterprise Management BaseLine Embedded Manageability)

Products	Any
Definition	A syslog format designed to be consistent with the Cisco IOS system log format and is more compatible with CiscoWorks management applications.
Usage	Docs—Expand on first use. GUI—Do not expand.

encounter

Products	Threat Response
Definition	Detection of an observable outside of my environment (off network). See also 'sighting.'

endpoint

Products	Any
Definition	A computing device used to connect to and communicate on a network.
Usage	Examples: desktops, laptops, smartphones, tablets, servers, workstations

endpoint (Threat Grid)

Products	Threat Grid
Definition	API endpoints are URIs representing server resources that can be used by client applications.

Endpoint Concentrator

Products	Stealthwatch Enterprise
Definition	An appliance that analyzes high-value endpoint contextual data collected by the AnyConnect NVM.

Usage

Features do not require the branded portion of the name; they'll only be used within the Cisco Stealthwatch context.

endpoint isolation

Products

AMP

Definition

Process of isolating a compromised endpoint by blocking all network traffic to and from the endpoint. This prevents command-and-control communication, exfiltration of sensitive information, and further spread of malware. Can allow certain IP addresses to access the endpoint to perform forensics and cleaning of threats.

Synonym: node isolation

enrichment

Products

Threat Grid, Threat Response

Definition

Annotating or collecting events with threat intelligence, correlated events, and security context. For example, in Threat Grid, the process of using the database to build up context around an observation or a piece of suspicious information, such as a behavioral indicator. By searching the database for related indicators, and following those relationships to other information, you can enrich the information with the context necessary to generate the actionable intelligence to address the problem.

entitlement

Products

Threat Grid

Definition

A Threat Grid product or service that has been purchased and is covered in the license agreement. For example, access to Threat Grid Cloud portal and APIs. Entitlements are listed on the Organization Details page.

Use the following to describe times and dates related to entitlements:

- entitlement start—the date the entitlement goes into effect
- entitlement stop—the last day of the entitlement subscription period
- entitlement lapse—time from the entitlement stop date to the end of the entitlement grace period
- entitlement grace period—five days after the entitlement stop date
- entitlement terminated—end of the entitlement grace period

entity

Products

Stealthwatch Cloud

Definition	Host or endpoint on the network, whether in the cloud or on the local network.

entity modeling

Products	Stealthwatch Cloud
Definition	Analysis of the behavior for every entity on the network or in the public cloud to determine abnormal, suspicious, and malicious activity.

envelope recipient

Products	ESA
Definition	The recipient of an email message as defined in the RCPT TO: SMTP command. Also, sometimes referred to as the 'Recipient To' or 'Envelope To' address.

envelope sender

Products	ESA
Definition	The sender of an email message as defined in the MAIL FROM: SMTP command. Also, sometimes referred to as the 'Mail From' or 'Envelope From' address.

EPM (Ethernet Port Module)

Products	Hardware
Usage	Do not use. Instead, use 'network module.'

ESD (electrostatic discharge)

Products	Hardware
Definition	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.
Usage	Do not expand.

ETF (External Threat Feed) source

Products	ESA
Definition	Used to download information about a collection of threats that is available on a TAXII server.
Usage	Docs—Expand on first use.

EtherType ACL

Products	ASA
Definition	An ACL that applies to non-IP layer-2 traffic on bridge group member interfaces only. You can use these rules to permit or drop traffic based on the EtherType value in the layer 2 packet. With EtherType ACLs, you can control the flow of non-IP traffic across the device.
Usage	Use camel case: EtherType

event

Products	Any
Definition	A change of state or observed activity that has occurred on the network or endpoint which has a security significance for the management of the network. Not necessarily suspicious, a cause for alarm, or a security threat.

exception expression

Products	Cloudlock
Definition	Pattern allowed by a DLP policy.

exclusions

Products	AMP
Definition	A type of list that specifies an application, process, directory, and so on that should be ignored (not scanned) by the endpoint Connector.

exploit

Products	Cognitive, Umbrella
Definition	Attack on a computer system that takes advantage of a particular vulnerability that the system offers to intruders.

exploit kit

Products	Cognitive, Umbrella
Definition	Server-based toolkit used to automate attacks by targeting client-side vulnerabilities in browsers and other software. For example, the Blackhole exploit kit is the most prevalent web threat (as of 2012). Its purpose is to deliver a malicious payload to a victim's computer. It incorporates tracking mechanisms, so that intruders maintaining the kit can obtain information about the victims.

Usage

Depending on context, can be abbreviated as EK.

extended ACL

Products

Any

Definition

A group of ACEs with the same ACL ID or name. This is more obvious in ASDM where ACLs are named and the ACEs that comprise them are nested under the name. These ACLs are used for access rules to permit and deny traffic through the device, and for traffic matching by many features, including service policies, AAA rules, WCCP, Botnet Traffic Filter, and VPN group and DAP policies. Extended ACLs are also used to determine the traffic to which other services will be provided.

Types of extended access rules:

- extended access rules (Layer 3+ traffic) assigned to interfaces
- extended access rules (Layer 3+ traffic) assigned to Bridge Virtual Interfaces (BVI routed mode)
- extended access rules assigned globally
- management access rules (Layer 3+ traffic)
- EtherType rules (Layer 2 traffic) assigned to interfaces (bridge group member interfaces only)

Usage

Always use 'extended ACL.' Do not expand to 'extended access control list.'

An extended ACL is not specifically identified as such in the interface but it is obvious from the creation of the ACE.

external event

Products

Stealthwatch

Definition

Data received from technologies other than flow export technologies and associated with behavior-based, flow-driven events.

F

fail closed

Products

Any

Definition

The state of a device or software where traffic is blocked when traffic handling is busy or down.

For example, an AnyConnect fail closed policy disables network connectivity when the VPN is unreachable.

Contrast with 'fail open.'

Usage

Noun: fail closed

Adjective: fail-closed

fail open

Products

Any

Definition

The state of a device or software where traffic continues flowing when traffic handling is busy or down.

For example, you can configure Firepower to allow traffic to pass without intrusion inspection when the inspection engine is down.

For example, an AnyConnect fail open policy permits network connectivity when the VPN is unreachable.

Contrast with 'fail closed.'

Usage

Noun: fail open

Adjective: fail-open

Synonym: failsafe

This is not the same as 'fail-to-wire' or 'hardware bypass.'

failover

Products

ASA

Definition

Failover lets you configure two ASAs so that one takes over operation if the other one fails. The ASA supports two failover configurations, Active/Active failover and Active/Standby failover. Each failover configuration has its own method for determining and performing failover.

With Active/Active failover, both units can pass network traffic. This lets you configure load balancing on your network. Active/Active failover is only available on units running in multiple context mode.

With Active/Standby failover, only one unit passes traffic while the other unit waits in a standby state. Active/Standby failover is available on units running in either single or multiple context mode.

For an ASA, high availability is a condition achieved when two ASAs are configured in an Active/Standby or Active/Active failover mode.

Usage

Noun, adjective: failover

Verb: fail over

failsafe

Products

ASA, Hardware

Definition

A characteristic of an inline set that lets packets bypass processing and continue through the device if internal traffic buffers are full.

Usage

Synonym: fail open

This is not the same as 'fail-to-wire' or 'hardware bypass.'

fail-to-wire

Products

Firepower

Definition

A physical layer bypass that allows paired interfaces to go into bypass mode so that the hardware forwards packets between these port pairs without software intervention. Provides network connectivity when there are software or hardware failures.

Usage

Do not abbreviate. Always spell out.

Synonym: hardware bypass

This is not the same as 'fail open' or 'failsafe.'

FamilyShield

Products

Umbrella

Definition

A special service offered by Cisco Umbrella that is distinct from our standard packages. Meant for home users who want to keep their children from seeing inappropriate images on their computers, FamilyShield always blocks domains categorized in our system as Tasteless, Proxy/Anonymizer, Sexuality, or Pornography.

Usage

Use camel case: FamilyShield

fastpath

Products

Firepower

Definition

Exempt traffic from all further inspection and control, most often used in the context of prefiltering.

Usage

Capitalize according to style guidelines, except when referring to the prefilter or tunnel rule action, which is always capitalized: the 'Fastpath action.'

8000 Series fastpath rules are device-specific rules that are not related to prefiltering. Always refer to these as '8000 Series fastpath rules' to disambiguate.

feed

Products

Any

Definition

Curated security-related information such as behavioral indicators, malware signatures, security policies and so on, that are often delivered by security service providers on a subscription basis, to enhance the security posture of an application or device. The goal of these feeds is to give customers the most up-to-date security information possible.

Fetch Stats

Products

Umbrella

Definition

Tool to enable administrators to download the Top Domains log data that has been collected for a network. Useful when downloading data ranges that are greater than 200 records, which is the file-size limit for an online download from the Umbrella Stats page.

field

Products

REST API

Definition

A single piece of information within an object model.

file-sharing index

Products

Stealthwatch

Definition

Tracks atypical file transfers, which could indicate peer-to-peer activity, that could place an organization at risk. Once the file-sharing activity for a particular host causes its file-sharing index points to surpass 100% of its threshold, the Stealthwatch Flow Collector generates a High File-Sharing Index alarm.

See also 'alarm.'

Usage

Do not abbreviate. Always spell out.

FIPS (Federal Information Processing Standards)

Products

Hardware, WSA

Definition

Federal Information Processing Standards (FIPS) specify requirements for cryptographic modules that are used by all government agencies to protect sensitive but unclassified information.

For hardware, it refers to the opacity shield with tamper-resistant labels covering the front panel of the chassis.

Usage

Docs—Expand on first use.

Flow Collector

Products

Stealthwatch Enterprise

Definition	A physical or virtual device that aggregates and normalizes NetFlow and application data collected from up to 4000 exporters (such as Cisco routers and switches) per Flow Collector.
Usage	Features do not require the branded portion of the name; they'll only be used within the Cisco Stealthwatch context.

Flow Sensor

Products	Stealthwatch Enterprise
Definition	A physical or virtual device that provides an overlay solution for generating NetFlow data for older Cisco network infrastructures not capable of natively producing unsampled NetFlow data at line rates, for third-party components that do not support unsampled NetFlow, and for other environments where additional security context is required.
Usage	Features do not require the branded portion of the name; they'll only be used within the Cisco Stealthwatch context.

FMT (Firepower Migration Tool)

Products	NGFW
Definition	A tool to migrate ASA firewall configurations to Firepower Threat Defense (FTD).
Usage	Use the term abbreviation in collateral such as presentations and best practice guides. For example, "The Cisco FMT helps you migrate your firewall to FTD."

FPS (flows per second)

Products	Security Online Visibility Assessment, Stealthwatch Cloud, Stealthwatch Enterprise
Definition	Number of NetFlow packets detected per second. Used for licensing.
Usage	GUI—Do not expand. Docs—Do not expand unless context requires it.

FQDN (fully qualified domain name)

Products	Any

Definition	A domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone. Always written in this format: [host name].[domain].[tld]. For example, a mail server on the example.com domain may use the FQDN mail.example.com.
Usage	GUI—Do not expand. Docs—Do not expand unless context requires it.

G

Gb (Gigabit)

Products	Any
Usage	Do not expand.

GB (Gigabyte)

Products	Any
Usage	Do not expand.

geodiversity and geodistance scores

Products	Umbrella
Definition	Algorithmic classifier that looks at where DNS requests originate, and how far away the requests are from the IP address' geolocation. The classifier then compares the geographic distribution of DNS requests with the predicted one for the top-level domain (for example, RU, CN, COM).

global

Products	Any
Definition	Setting that applies to everything.
Usage	Not to be confused with 'Global domain.'

global configuration mode

Products	ASA

Definition	Lets you change the ASA configuration. All user EXEC, privileged EXEC, and global configuration commands are available in this mode.

Global domain

Products	Firepower
Definition	In a multidomain deployment, the top-level domain. If you do not configure multitenancy, all devices, configurations, and events belong to the Global domain. Administrators in the Global domain can manage the entire Firepower System deployment.

globally meshed VPNs

Products	Umbrella
Definition	A community of VPN-enabled gateways located at various points throughout the world. Each VPN can communicate with every other member of the community through a VPN tunnel.

global network (Umbrella)

Products	Umbrella
Definition	The Cisco Umbrella global network is comprised of geographically distributed data centers serving 50 million active users daily in more than 160 countries, and delivering the industry’s best uptime. Combined with Umbrella network security services, it provides the ultimate coverage, efficacy, and performance. Umbrella's infrastructure that handles more than 2 percent of the world’s daily internet requests with proven 100 percent uptime. It enforces security policies with no added latency, and in minutes covers any device worldwide, for Umbrella.

global network resolver

Products	Umbrella
Definition	Network of servers managed by Cisco Umbrella that are used to resolve DNS queries.

greenfield

Usage	Do not use. Instead, standardize use around 'new deployment.' See also 'brownfield.'

group policy

Products	AnyConnect, ASA, Firepower

Definition	A collection of attributes and their values that define behaviors of a remote access VPN connection. Attributes in the group policy are stored internally on the ASA, or externally on a AAA server. Group policies are associated with connection profiles (tunnel groups) and local user accounts. Based on the system's configuration, a group policy is determined and assigned to remote access clients upon the establishment of a VPN connection.

guardrail

Products	Threat Grid
Definition	Trusted signing authority that is included on allowed lists.
Usage	Do not use in interface or documentation. This is an internal-use-only term.

H

hardware bypass

Products	ASA, FMC, FxOS
Definition	Ensures that traffic continues to flow between an interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures.
Usage	Noun: hardware bypass Adjective: hardware-bypass Synonym: fail-to-wire This is not the same as 'fail open' or 'failsafe.' Standardize terminology around 'hardware bypass.'

hardware-bypass card

Products	Hardware
Definition	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. The hardware bypass passes traffic at the network interface; it does not pass it to the system.
Usage	This is not the same as 'fail open.'

HAT (Host Access Table)

Products	ESA

Definition	Maintains a set of rules that controls incoming connections from remote hosts for a listener. Every listener has its own HAT. HATs are defined for public and private listeners, and contain mail flow policies and sender groups.
Usage	Docs—Expand on first use. Example: "The settings configured in the listener, including its Host Access Table and Recipient Access Table, affect how the listener communicates with an SMTP server during the SMTP conversation."

HDD (hard disk drive)

Products	Hardware
Usage	Do not expand.

high availability

Products	ASA, Firepower
Definition	A pair of devices configured for failover to provide redundancy. Common configurations to achieve high availability are active/standby and active/active.
Usage	Lower case. Do not abbreviate as 'HA' in interfaces or documentation. In this context, do not use 'master' and 'slave.' Instead, use 'primary' and 'secondary.'

host

Products	Any
Definition	A device that is connected to a network and has an IP address.

host alarm

Products	Stealthwatch Enterprise
Definition	A security event that has triggered an alarm for an endpoint Stealthwatch is monitoring.
Usage	Use singular or plural in the GUI.

host identity

Products	Firepower

Definition	Contextual information about a host gathered by network discovery. Can contain attributes such as basic topology data, device type, operating system, and applications installed on the host.

hostname

Products	Any
Definition	A label used to identify a host on a network.

hotfix

Products	Any
Definition	A minor update to a security device that addresses a particular, urgent problem that cannot wait for the next release. Hotfixes are applied to “hot" (in use) devices. As much as possible, a hotfix should not interrupt normal operations.
Usage	Use as a noun.

hot plug

Products	Hardware
Definition	Lets you add components that expand the system but would not cause interruption to the system.
Usage	Two words. Verb: hot plug Noun: hot plugging Adjective: hot-pluggable

hot swap

Products	Hardware
Definition	Lets you add, replace, or remove components without interrupting the system power, entering console commands, or causing other software or interfaces to shut down.
Usage	Two words. Verb: hot swap Noun: hot swapping Adjective: hot-swappable

I

identity

Products	Any
Definition	A set of attributes, maintained by an authoritative identity source (such as Microsoft Active Directory or LDAP server) that describes a user. Examples of attributes include username, password, group associations, and so on.
Usage	Do not abbreviate. Always spell out.

identity (Umbrella)

Products	Umbrella
Definition	An entity you create in Umbrella that you can apply policy to and report on. An identity can be an entire network, or as granular as an individual user or device.
Usage	Do not abbreviate. Always spell out.

identity firewall

Products	ASA
Definition	Provides granular access control based on users’ identities rather than through source IP addresses. This concept, along with detailed implementations, is documented in the ASA configuration guide. **Note** Firepower does not identify 'identity firewall' as a feature or a kind of firewall. Customers simply implement security policies based on identity.

identity NAT

Products	Any
Definition	A real address is statically translated to itself, essentially bypassing NAT. You might want to configure NAT this way when you want to translate a large group of addresses, but then want to exempt a smaller subset of addresses.
Usage	Do not abbreviate 'identity NAT.'

identity policy

Products	ASA, Firepower
Definition	An identity policy associates traffic on your network with an authoritative identity source and a realm. You can configure access rules and security policies based on identity attributes rather than through source IP addresses. After configuring one or more identity policies, you can associate one with an access control policy and deploy the access control policy to a managed device.
Usage	Do not abbreviate. Always spell out.

identity type

Products	Umbrella
Definition	A category in which an identity is included. For example, networks, network devices, and roaming computers are identity types. Identities are grouped by type in order to design and apply policies consistently.
Usage	Do not abbreviate. Always spell out.

inactive host

Products	Stealthwatch
Definition	A host that is known to the Stealthwatch Flow Collector but has not transmitted a data packet in the last 5 minutes. Contrast with 'active host.'

inbound rule

Products	ASA
Definition	Inbound access rules apply to traffic as it enters an interface. Global and management access rules are always inbound.

incident

Products	AMP, Cognitive, CWS

Definition	An event, use, or behavior that does not conform to an established standard, and that is considered a possible security threat. Can be comprised of multiple events. For example, a malicious PDF file exploits an Acrobat vulnerability to execute a PE file, which in turn downloads malware, which is then detected and quarantined. Each of those events – exploit, download, detection, quarantine – makes up the single incident.
Usage	Use modifiers to describe different types, such as retrospective incident, incident response, low-risk incident, and high-risk incident.

indeterminate

Products	Threat Grid
Definition	A verdict that indicates the subject's risk cannot be determined.

index point

Products	Stealthwatch Enterprise
Definition	A value that represents an observed use of behavior that matches a defined set of criteria. When the accumulated index points meet or exceed a designated threshold, Stealthwatch triggers the applicable alarm.

indicator

Products	Any
Definition	A trait, behavior, pattern, or set of conditions that indicates the presence of malicious activity or the possibility of a compromise as observed in the field. Not all indicators are behavioral. See 'behavioral indicator.' Additionally, in Threat Response, an indicator can be a collection of judgements or a pattern specification that a sensor uses to characterize events or observed activity.
Usage	Can be used interchangeably with indicators of compromise (IOC).

infected

Products	Cognitive
Definition	A term used to describe an asset or host when you know it is affected by a threat or malware and needs remediation.
Usage	Do not use if redundant or implied in context. For example, on a page showing what malware was found on which hosts in the network, avoid using 'infected host' if 'host' is sufficient.

inline

Products	Any
Definition	A configuration where devices can affect network traffic flow. Contrast with passive, where you can analyze and respond to, but not affect, the flow of traffic.
Usage	Adjective: inline deployment, inline interface, inline mode

innocuous

Products	Threat Grid
Definition	A verdict that indicates the subject is listed in the National Software Reference Library (NSRL) database, a repository of known software.

inside

Products	ASA, Firepower, Hardware
Definition	The first interface, usually port 1, that connects your internal "trusted" network protected by the appliance.

inspect (rule action)

Products	Firepower
Definition	A rule action used when any inspection properties are applied to the match criteria. Within an access control policy, access control rules provide a granular method of handling network traffic across multiple managed devices. Each rule also has an action, which determines whether you monitor, trust, block, or allow matching traffic. When you allow traffic, you can specify that the system first inspect it with intrusion or file policies to block any exploits, malware, or prohibited files before they reach your assets or exit your network.
Usage	Examples: inspect rule, inspect action, inspect rule action

intelligence source

Products	Threat Response
Definition	An engine, website, or group of people that produces indicators and related data around malware, attack patterns, weaknesses, campaigns, actors, and targets.
Usage	Do not abbreviate intelligence as intel.

Intelligent Proxy

Products	Umbrella
Definition	When your computer makes a DNS query for a site that sometimes hosts bad content, the Intelligent Proxy kicks in to protect you. Instead of returning the correct address of the website, the DNS server returns the address of the Intelligent Proxy, where Umbrella security software can take a deeper look at the site and protect you as needed.
Usage	Do not abbreviate. Always spell out.

interactive block (rule action)

Products	Firepower
Definition	A rule action that allows users to load an initially blocked website after reading a warning.

interface

Products	Any
Definition	The connection between a particular network and an appliance.
Usage	Use as a noun.

interface PAT (Port Address Translation)

Products	ASA, Firepower
Definition	The use of PAT where the PAT IP address is also the IP address of the outside interface.
Usage	Docs—Expand on first use. Do not abbreviate 'interface PAT.'

intrusion alert

Products	Firepower
Definition	An IPS alert was an alert generated by the Sourcefire Intrusion Prevention System (IPS).
Usage	Use 'intrusion alert' instead of 'IPS alert.'

intrusion event

Products	Firepower
Definition	An event logged when network traffic hits an intrusion rule.

Usage	Use 'intrusion event' instead of 'IPS event.'

intrusion set

Products	Stealthwatch
Definition	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An intrusion set may capture multiple campaigns or other activities that are all tied together by shared attributes indicating a common known or unknown threat actor.

Investigate (Umbrella)

Products	Umbrella
Definition	A Cisco Umbrella threat intelligence product.
Usage	Docs—Expand on first use. Investigate by Cisco Umbrella. Thereafter, can be shortened to Investigate. Always capitalize.

IP (Internet Protocol)

Products	Any
Definition	Used to communicate across any set of interconnected networks. Well suited for LAN and WAN communications.
Usage	Do not expand.

IP address

Products	Any
Definition	An Internet Protocol address.
Usage	Do not shorten to 'IP.' Refers to both IPv4 and IPv6 addresses.

IPS alert

Usage	Legacy term. Going forward, do not use. Instead, use 'intrusion alert.'

IPS event

Usage	Legacy term. Going forward, do not use. Instead, use 'intrusion event.'

J

judgement

Products	Threat Response
Definition	A statement by a human or analysis engine that declares the perceived, calculated disposition of an observable: whether it's malicious, clean, suspicious, common, unknown, and so on. There can be many judgements. Judgements are the basis for returned verdicts. They're also the primary means by which users of Threat Response go from observables on their system, to the indicators and threat intelligence data in Threat Response. The judgement has more than just the disposition. It’s a record of which engine made the judgement, how long it is valid, why the judgement was made, and where more details can be seen.

K

kill chain

Products	Threat Response
Definition	A model of the progress of a security compromise. The dominant one being from Lockheed Martin, using it as a structure for modeling intrusion attacks on a network. The phases are: • recon • weaponization • delivery • exploitation • installation • command and control • actions

KVM (Kernel-based Virtual Machine)

Products	Hardware
Usage	Expand on first use to differentiate from other uses.

KVM (Keyboard, Video, and Mouse)

Products	Hardware

Usage	Expand on first use to differentiate from other uses.

L

last VPN local resource

Products	AnyConnect
Definition	When a VPN is unreachable, the client applies the last client firewall received from the ASA.

lexical feature scores

Products	Umbrella
Definition	Classifiers used to detect fast flux. Fast flux is a DNS technique that botnet command-and-control infrastructures use to hide behind a compromised system that acts like a proxy.

lina

Products	ASA, Firepower
Definition	A process on a Firepower Threat Defense device. It is closely associated with the ASA software and is frequently used by engineering as a reference to the ASA side of the bicameral FTD brain (the other side being Snort). Lina is closely associated with deploying and interpreting ASA configuration commands, which are used to configure ASA-based features such as routing.
Usage	GUI—Do not use. In most cases, you can use 'data plane' or 'the system, whichever is appropriate. Configuration commands that appear in the show running-config output are 'ASA configuration commands.' Commands that originally came from the ASA but now are exposed in the converged CLI are called 'Firepower Threat Defense commands.' In the documentation, you can use 'lina' if you are specifically discussing troubleshooting at the process level. Also, the first time you refer to the data plane in a book, you can say 'the data plane (sometimes called lina)...'

load balancer

Products	Hardware
Definition	A network device that distributes traffic to optimize performance and resource use. Using discovery, the system can identify load balancers.

local device manager

Products	ASA, Firepower, Stealthwatch
Definition	An application used to configure a device dedicated to performing a single function. It is "local" because it is installed on the same appliance as the device's software, or it is delivered with the device's software. A local device manager only manages the device it is installed on or delivered with. Firepower Device Manager and Stealthwatch Central Manager are examples of local device managers. The command line interface for a device is also considered a local device manager.
Usage	Do not use 'on-box manager' in place of 'local device manager.'

LOM (LAN on motherboard)

Products	Hardware
Usage	Expand on first use to differentiate from other uses.

LOM (Lights-Out Management)

Products	Hardware
Definition	The ability for an administrator to monitor and manage systems and their power by remote control.
Usage	Expand on first use to differentiate from other uses.

low-touch provisioning (CDO)

Products	CDO
Definition	Refers to the process of shipping an FTD from the factory to a customer site (typically a branch office). An employee at the site connects the FTD to their network, and the device contacts the Cisco Cloud. At that point, the device is onboarded to the CDO tenant if its serial number has already been claimed, or the FTD is parked in the Cisco cloud until it is claimed by a CDO tenant. The device is configured to receive its address by DHCP and the FTD’s default password has not been changed. The user interacting with the hardware is expected to have limited or no interaction with the device other than to plug it in and assess the status lights. See also 'claimed,' 'parked,' and 'serial number onboarding.'
Usage	At the beginning of a sentence: Low-touch provisioning In the middle of a sentence: low-touch provisioning As a field name or title: Low-Touch Provisioning After first use, can be shortened to LTP.

M

machine

Products	Any
Usage	Do not use to refer to an appliance, chassis, or device. Exceptions include 'machine-generated,' 'machine learning,' and 'virtual machine.'

mail flow policy

Products	ESA
Definition	A way of expressing a group of Host Access Table (HAT) parameters (an access rule, followed by rate limiting parameters and custom SMTP codes and responses) for a listener. Together, sender groups and mail flow policies are defined in a listener’s HAT. Your Cisco appliance ships with the predefined mail flow policies and sender groups for listeners.

malicious

Products	Any
Definition	Something that is known to be dangerous or harmful.

master

Usage	In some cases, used to describe the active unit when 2 units are operating in failover mode with each other. In this context, do not use 'master.' Instead, standardize terminology around 'active' or 'primary.' However, in ASA VPN load balancing, do not use 'master' (and 'backup'). Instead, use 'director' (and 'member').

MD5

Products	Any
Definition	Message-digest algorithm that's a hash function widely used to produce a 128-bit hash value.
Usage	Do not use md5, Md5, md-5, Md-5, or MD-5.

MDI

Products	Any

Definition	Media-dependent interface.
Usage	Docs—Expand on first use.

MDIX

Products	Any
Definition	Media-dependent interface crossover.
Usage	Docs—Expand on first use.

method

Products	REST API
Definition	Methods are the possible actions a user can perform on a REST API service. These include GET, PUT, POST, and DELETE.

MITRE ATT&CK

Products	Any
Definition	The MITRE Corporation is a non-profit organization, founded in 1958, that provides engineering and technical guidance on advanced technology problems like cybersecurity for a safer world. MITRE ATT&CK is a knowledge base of the methods that attackers use against enterprise systems, cloud apps, mobile devices, and industrial control systems. ATT&CK, which stands for Adversarial Tactics, Techniques, and Common Knowledge, can help you understand how cyber attackers think and work. See MITRE ATT&CK White Paper at Cisco.

model

Usage	Do not use generically. Instead, use when referring to the actual model number. For example, Firepower 2140 model.

module (hardware)

Products	Hardware
Definition	A removable component in a chassis, such as a network module or security module.

module (software)

Products	Software
Definition	A software module package that provides additional and complimentary functionality to the primary software on an appliance. A software module is installed separately and licensed separately from the primary function of the device. For example, the FirePOWER services module runs on an ASA and is installed and licensed separately from the ASA software.

monitor (rule action)

Products	Firepower
Definition	A rule action that ensures logging of matching connections without affecting traffic flow. Monitored traffic is matched against additional rules, if present, to determine how the traffic is handled.
Usage	Examples: monitor rule, monitor action, monitor rule action

MPF (Modular Policy Framework)

Products	ASA
Definition	This is a name given to a strategy which combines ASA objects to achieve an outcome. Combines an access control list (ACL), class map, policy map, and service policy to provide a consistent and flexible way to configure ASA features. The ACL is applied to a class map. The class map defines a traffic matching condition. The class map is associated with a policy map which defines enforcement. The policy map is associated with an interface using a service policy. MPFs can be used to direct traffic to IPS inspection, application inspection, and define Quality of Service requirements for an application.
Usage	Docs—Expand on first use. However, this is an antiquated and almost irrelevant ASA feature name. Do not use it in Firepower. Instead, describe a similar security approach using the actual terminology for the policies, rules, and objects used.

MSP (malware storage pack)

Products	Hardware
Definition	A secondary solid-state drive supplied by Cisco that you can install in certain devices to store captured files, which frees space on the device's primary hard drive for event and configuration storage.
Usage	Docs—Expand on first use.

MSP (Managed Service Provider)

Products	Umbrella
Definition	A third-party vendor that provides and manages internet services to a client.
Usage	Docs—Expand on first use.

MSSP (Managed Security Service Provider)

Products	Umbrella
Definition	A third-party vendor that provides and manages security services to a client.
Usage	Docs—Expand on first use.

MTA (Mail Transfer Agent)

Products	ESA
Definition	The program responsible for accepting, routing, and delivering email messages. Upon receiving a message from a Mail User Agent or another MTA, the MTA stores a message temporarily locally, analyses the recipients, and routes it to another MTA. It may edit and/or add to the message headers.
Usage	Docs—Expand on first use.

MUA (Mail User Agent)

Products	ESA
Definition	The program that lets the user compose and read email messages. The MUA provides the interface between the user and the Mail Transfer Agent. Outgoing mail is eventually handed over to an MTA for delivery.
Usage	Docs—Expand on first use.

multi-device manager

Products	ASA, Firepower

Definition	A client-based or cloud-based application used to configure a device. A multi-device manager is not installed on the appliance or delivered with the device's software. This kind of manager can manage a single device type or multiple device types. Adaptive Security Device Manager, Cisco Defense Orchestrator, Firepower Management Center, and Cisco Security Manager are examples of multi-device managers. See also 'remote device manager.'
Usage	Do not use 'off-box manager' in place of 'multi-device manager.'

multi-factor authentication (MFA)

Products	Any
Definition	Strengthens access security by requiring two or more different methods (also referred to as factors) to verify your identity. These factors can include something you know (username and password), something you are (fingerprint), or something you have (secondary trusted device like a smartphone app or token to approve authentication requests). Two-factor authentication (2FA) is a subset of MFA.
Usage	Docs—Expand on first use. Thereafter, can be shortened to MFA.

N

NAT (Network Address Translation)

Products	Any
Definition	Substituting an IP address in the header of a packet for another IP address so that the packet can be routed from one network to another. One of the main functions of NAT is to enable private IP networks to connect to the internet with a translated, public IP address.
Usage	Docs—Expand on first use. GUI—Use 'NAT.'

NEBS (Network Equipment Building System)

Products	Hardware, Software
Definition	Network Equipment Building System (NEBS) compliance refers to the conformance of a network product to the requirements of the NEBS standard. Compliance to this standard indicates that a network product or a telecommunications equipment performs at its optimum capacity.
Usage	Docs—Expand on first use.

NetFlow

Products	Stealthwatch Cloud, Stealthwatch Enterprise, Security Online Visibility Assessment, Firepower
Definition	An embedded instrumentation within Cisco IOS Software to characterize network operation. By analyzing the data provided by NetFlow, you can determine things such as the source and destination of traffic, class of service, and the causes of congestion.
Usage	Use camel case: NetFlow

network exit localization

Products	Threat Grid
Definition	Similar in concept to VPN, the Network Exit Localization setting makes any outgoing network traffic that is generated during the analysis to appear to exit from that location. Users may select a different location from the default while submitting samples for analysis, whether from the dropdown list on the Submit Sample modal, or by API.

NGFW (Next-Generation Firewall)

Products	ASA, Firepower
Definition	Means different things to different people. For example, some people consider an ASA with FirePOWER Services to be an NGFW. Other people consider only a Firepower Threat Defense (FTD) device to be an NGFW. The FTD device can be managed by command-line interface, Firepower Device Manager (FDM), Firepower Management Center (FMC), or Cisco Defense Orchestrator. Sometimes, FDM and FMC are confused with next-generation firewalls. These managers are not next-generation firewalls. They're user interfaces to manage traditional firewalls, next-generation firewalls, and even other device types. 'NGFW' is used extensively by Marketing and is the official product name in the Cisco.com product path.

Usage	Avoid using 'NGFW' whenever possible. Instead, use the specific product name. For example: *Firepower Threat Defense device* *ASA with FirePOWER Services module* Mentioning ONCE that your particular device is a next-generation firewall (NGFW) is acceptable if it helps the customer find that wording when they search for it. For a complete list of acceptable terms, see Customer-Facing Names for Firepower System Appliances. If you're spelling out 'NGFW,' spell out the whole term. Do not use 'Next-Gen' or other variants. Do not use as a synonym for access control.

NGIPS (Next-Generation Intrusion Prevention System)

Products	Firepower
Definition	Firepower software that runs on older/legacy Firepower devices (7000 series, 8000 Series, NGIPSv).
Usage	Docs—Expand on first use. Use as an adjective to modify a device or the software running on it: NGIPS device, NGIPS software. With the exception of NGIPSv, do not use as a noun. Do not use as a synonym for access control.

NLPRank

Products	Umbrella
Definition	Classifier that leverages natural language processing (NLP) techniques to detect cyber-squatting and targeted phishing domains.
Usage	Use camel case: NLPRank

node

Products	Any

Definition	A node is any device within a connected network of other devices that’s able to send, receive, and/or forward information. The computer is the most the common node and is often called the computer node or internet node. Modems, switches, hubs, bridges, servers, and printers are also nodes, as are other devices that connect over WiFi or Ethernet. Nodes within a computer network must have some form of identification, like an IP address, MAC address, or Data Link Control (DLC) address for it to be recognized by other network devices. A node without this information, or one that has been taken offline, no longer functions as a node.
Usage	For example, in Threat Grid Appliance, a node is a member of an appliance cluster.

NPU (network processor unit)

Products	Hardware
Usage	Expand on first use to differentiate from other uses.

NTP (Network Time Protocol)

Products	Any
Definition	Networking protocol for clock synchronization. For example, the ntpconfig command configures IronPort AsyncOS to use NTP to synchronize the system clock with other computers.
Usage	Docs—Expand on first use.

O

object

Products	REST API
Definition	An individual instance of a service.

object model

Products	REST API
Definition	The list of data which a service may contain.

observable

Products	Cognitive, Threat Grid, Threat Response

Definition	A single, atomic identifier, in the form of a discreet string, that can be recognized and communicated by sensors; such as IP address, domain, file hash, email, MAC address, file name, sensor-specific GUID, and web request. See also 'observation.' For example, the first thing that Threat Response does with an observable is determine its disposition, by aggregating what we know about that observable from the various enrichment modules we have configured. The disposition tells us whether the observable is clean, malicious, suspicious, unknown, and so on. Once we have a disposition for an observable, we begin to enrich it, gathering information about it from enrichment sources such as AMP and the Cisco Threat Intelligence API. Unknown observables are not enriched. See also 'disposition.'

observation

Products	Stealthwatch Cloud
Definition	A fact about your traffic, such as endpoints making connections they have not made before. Observations are not necessarily suspicious. See also 'observable.'

off-box manager

Usage	Do not use. Instead, see 'remote device manager' and 'multi-device manager.'

OIR (online insertion and removal)

Products	Hardware
Definition	Lets you add, replace, or remove components. OIR requires performing Cisco IOS commands before and after the OIR.
Usage	Docs—Expand on first use. Do not confuse with 'hot swap' or 'hot plug.'

on-box manager

Usage	Do not use. Instead, see 'local device manager.'

on premises

Products	Any
Definition	Software that runs on computers within an organization. Contrast with cloud software.

Usage	Can be abbreviated as 'on-prem.' Docs—Expand on first use. 'On premise' is incorrect. Do not leave off the 's.' Whether you include a hyphen depends on how 'on premises' is being used. If it’s being used as a compound adjective before a noun, we can hyphenate it as 'on-premises.' Otherwise, the hyphen is not needed.

OpenDNS

Products	Umbrella
Definition	The original company name of Cisco Umbrella. Still used for the public free offering of Umbrella.
Usage	Use 'Umbrella' instead of 'OpenDNS.'

OpenDNS Updater

Products	Umbrella
Definition	Software that ensures that Umbrella preferences are preserved whenever IP addresses change.

open relay

Products	ESA
Definition	An open relay (sometimes called an 'insecure relay' or a 'third-party relay') is an SMTP email server that allows unchecked third-party relay of email messages. By processing email that is neither for nor from a local user, an open relay makes it possible for unknown senders to route large volumes of email (typically spam) through your gateway.
Usage	Use in its singular form only.

Orbital, Orbital Advanced Search

Products	AMP, Threat Grid, Threat Response
Definition	Near real-time endpoint search and forensic snapshot service. Uses osquery.io schema for SQL queries. Currently a beta service installed by AMP for Endpoints Windows Connector.
Usage	The official name for this service being offered with AMP is Cisco Orbital. Thereafter, can be shortened to Orbital, but do not use OAS. The AMP Console may still refer to it as Orbital Advanced Search, but this should be updated in the future.

organization (Threat Grid)

Products

Threat Grid

Definition

An entity created within Threat Grid that is used to group users according to how the privacy and visibility rules are to be applied. Only users within the same organization can see samples that have been designated as private. A Threat Grid organization on the cloud can only be created by Threat Grid staff. Organizations can only be created on a Threat Grid appliance by an admin user.

Usage

Threat Grid-specific use of 'organization.'

organization, org (Umbrella)

Products

Umbrella

Definition

Generally, a term used in conjunction with service provider console. An organization is the term used to describe a customer.

Usage

Can be organization or org.

Most commonly used with 'Multi-Org console' instead of 'customer.'

outbound rule

Products

ASA

Definition

Outbound rules apply to traffic as it exits an interface. An outbound ACL is useful, for example, if you want to allow only certain hosts on the inside networks to access a web server on the outside network. Rather than creating multiple inbound ACLs to restrict access, you can create a single outbound ACL that allows only the specified hosts. The outbound ACL prevents any other hosts from reaching the outside network.

This term does not refer to a higher security to lower security interface, commonly known as outbound.

This term does not apply to Firepower firewalls: All access control rules in Firepower are modeled as global rules in the data plane. Global rules are always inbound.

Outbreak Filters

Products

ESA

Definition

IronPort’s Outbreak Filters feature provides an additional layer of protection from viruses. The Outbreak Filters feature quarantines suspicious email messages, holding the messages until an updated virus IDE is available, or until they are deemed not a threat.

Usage

Use the plural form only.

outside

Products	ASA, Firepower, Hardware
Definition	The first interface, usually port 0, that connects to other "untrusted" networks outside the appliance.

P

PAN (Policy Administration Node)

Products	ISE
Definition	See PAP (Policy Administration Point). Policy administration node is the Cisco term for this function.
Usage	Docs—Expand on first use. Lower case.

PAP (Password Authentication Protocol)

Products	ESA, SMA
Definition	An authentication protocol for communicating with the RADIUS server for configuring external authentication or two-factor authentication on the appliance.
Usage	Docs—Expand on first use. Lower case.

PAP (Policy Administration Point)

Products	ASA, Cisco TrustSec
Definition	Defines and inserts policies into the authorization system. Also acts as an identity repository by providing Cisco TrustSec tag-to-user identity mapping and Cisco TrustSec tag-to-server resource mapping. Policy administration point is the industry standard term for this function. In the Cisco TrustSec solution, the Cisco Identity Services Engine (ISE) acts as the PAP. However, ISE diverged from industry standard terms: they call their PAP a policy administration node (PAN).
Usage	Docs—Expand on first use. Lower case.

parameter

Products	REST API

Definition	A variable added to a REST API request which provides information for executing the method on the service. This can be as simple as the UUID of the specific resource being deleted or include the entire model when creating an object.

parked (CDO)

Products	CDO
Definition	Used in the context of CDO and serial number onboarding: A device is 'parked' if it has connected to the Cisco Cloud and its serial number has not been claimed by a CDO tenant.

Partner console

Products	Umbrella
Definition	Console used to create and start trials of Cisco Umbrella.
Usage	Cisco Umbrella for Partners console, never PPoV.

passive interface

Products	ASA, Firepower, Hardware
Definition	A sensing interface configured to analyze traffic in a passive deployment.

pass through

Products	WSA
Definition	Allow encrypted traffic to pass without decryption or further checks.
Usage	Avoid, except in legacy products and documentation. See also 'allow,' 'trust,' and 'do not decrypt.'

PAT (Port Address Translation)

Products	Any

Definition	PAT translates multiple real addresses to a single mapped IP address by translating the real address and source port to the mapped address and a unique port. If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used. Each connection requires a separate translation because the source port differs for each connection. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.
Usage	Docs—Expand on first use. GUI—Use 'PAT.'

patch

Products	Any
Definition	A minor upgrade that includes a limited range of fixes.
Usage	Use as a noun or verb.

PBR (policy-based routing)

Products	ASA
Definition	Traditional routing is destination-based, meaning packets are routed based on destination IP address. However, it's difficult to change the routing of specific traffic in a destination-based routing system. With PBR, you can define routing based on criteria other than destination network. PBR lets you route traffic based on source address, source port, destination address, destination port, protocol, or a combination of these. PBR is defined by access lists and route maps. PBR is available in routed mode only.
Usage	Docs—Expand on first use.

peer

Products	Any
Definition	Devices that communicate with each other without having to go through a server, such as sharing files over a peer-to-peer network.
Usage	Do not abbreviate. Always spell out. Such as peer-to-peer or point-to-point. Do not use 'P2P.'

phantom host

Products	Stealthwatch

Definition	A host that was previously unknown to the Stealthwatch Flow Collector and that was sent a data packet, but did not respond within 10 seconds. A large number of phantom hosts can be an indication of network scanning.

PhishTank

Products	Umbrella
Definition	The first and most successful collaborative clearinghouse for data and information about phishing on the internet. PhishTank is based on the idea that security researchers, exploited brands, technology developers, academic institutions and internet users are stronger together in fighting phishing than they are on their own.
Usage	Use camel case: PhishTank

PID (product identifier)

Products	Hardware
Definition	The orderable product identifier that is 1 of the 3 parts of the UDI. The UDI is part of the PEP policy.
Usage	Docs—Expand on first use. Lower case.

platform

Products	Hardware
Definition	Refers to a series of hardware models.
Usage	Do not use generically. For example, to refer to all of the Kentons or Queen's Park.

playbook

Products	Threat Grid
Usage	See 'user emulation playbook.'

policy

Products	Any
Definition	A mechanism for grouping and applying rules or settings. For more information, see the Policy archetype.

Usage	Unless context is absolutely clear, use the full name of the policy: access control policy, intrusion policy, NAT policy, and so on. Do not capitalize or abbreviate the name of the policy, except as a page title, field label, or other GUI element where you are required to capitalize the name. For example, it is 'access control policy,' not 'Access Control Policy' or 'AC Policy.'

policy (Stealthwatch Enterprise)

Products	Stealthwatch Enterprise
Definition	A set of rules that you can apply to entities within your network that monitors and can alert on behavior.

policy (Umbrella)

Products	Umbrella
Definition	Access to content rules and controls that determine how an Identity is protected by Umbrella. Created through the Policy wizard.

polling interval

Products	ESA
Definition	Defines the frequency of fetching threat feeds from a TAXII server.

polling path

Products	ESA
Definition	The part of the URL that identifies the polling service in the TAXII server. For example, '/taxii-data.'

popularity and page rank scores

Products	Umbrella
Definition	A ranking score based on the number of distinct origin IP addresses that have visited a domain name. This is a Bayesian average, similar to reputation scores.

POST (Power-On Self Test)

Products	Hardware
Definition	Set of hardware diagnostics that runs on a hardware device when that device is powered on.

Usage	Do not expand.

PPoV (Partner Proof of Value)

Products	Umbrella
Definition	Partner Proof of Value and Partner console.
Usage	Do not abbreviate. Always spell out. Do not use PPoV acronym.

preshared key

Products	Any
Definition	Provides a method of IKE authentication that is suitable for networks with a limited, static number of IPsec peers. This method is limited in scalability because the preshared key must be configured for each pair of IPsec peers. When a new IPsec peer is added to the network, the preshared key must be configured for every IPsec peer with which it communicates. Using certificates and CAs provides a more scalable method of IKE authentication.
Usage	Use 'PSK' only in field labels or other GUI elements where space is an issue, and in documentation describing those GUI elements. Otherwise, spell out 'preshared key.'

private

Products	Threat Grid
Definition	A privacy setting that controls access to sample analysis results. Samples designated as private are only available to members of the same organization as the submitting user or integration. Users who belong to a different organization than the submitting user have no access to the the analysis results.

private key

Products	Any
Definition	A cryptographic key known only to the owner of the paired public key certificate. The public key and private key are used for Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption and decryption.

privleged EXEC mode

Products	ASA
Definition	Privileged EXEC mode lets you change current settings. Any user EXEC mode command works in privileged EXEC mode.

promiscuous mode

Products	ASA
Definition	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.

provision (FTD)

Products

CDO, FTD

Definition

Strictly speaking there are two sets of actions that occur at the beginning of the FTD setup:

- provisioning
    - accept EULA
    - create new password
- system initialization
    - configure management IP address (IP type, DHCP/static)
    - set FQDN
    - set DNS servers
    - choose to manage the device locally (with FDM)

However, to the user, all of this is initial provisioning. This definition is useful to differentiate a claiming error and a provisioning error in CDO.

PUA (Potentially Unwanted Application)

Products	Cognitive, WSA
Definition	An application that is not malicious but may be considered to be unsuitable and undesirable for the business network.
Usage	Docs—Expand on first use.

public

Products	Threat Grid
Definition	A privacy setting that controls access to sample analysis results. Samples designated as public are available to all other users, regardless of which organization they belong to. (The one exception to this rule is for public samples submitted by integrations: integrations from a different organization will only have partial access to the analysis results.)

public key

Products	Any
Definition	A public key is one of a pair of keys that is generated by devices involved in public key infrastructure (PKI). Data encrypted with a public key can only be decrypted using the associated private key. When a private key is used to produce a digital signature, the receiver can use the public key of the sender to verify that the message was signed by the sender. These characteristics of key pairs provide a scalable and secure method of authentication over an insecure media, such as the internet.

pxGrid (Cisco Platform Exchange Grid)

Products	WSA
Definition	Enables collaboration between components of the network infrastructure, including security-monitoring and network-detection systems, identity and access management platforms, and so on. These components can use pxGrid to exchange information through a publish/subscribe method.

Q

R

RAID (Redundant Array of Independent Disks)

Products	Hardware
Usage	Do not expand.

RAT (Recipient Access Table)

Products	ESA
Definition	Defines which recipients are accepted by a public listener. Specifies the address (which may be a partial address or hostname) and whether to accept or reject it. Optionally, you can include the SMTP response to the RCPT TO command for that recipient. The RAT typically contains your local domains.
Usage	Docs—Expand on first use.

rate limit (Threat Grid)

Products	Threat Grid

Definition	A setting that controls the number of samples that may be submitted to Threat Grid for analysis by API within a particular timeframe. The sample rate limit is set in the Threat Grid license entitlements and maintained at the organization level. Additional rate limits within the organization can be further specified for greater control, including limits set on individual users and devices. A rate limit is set as [[N,minutes]], where N is the number of samples and minutes is the timeframe. For example, [[100,1440]] is 100 samples within 1440 minutes (24 hours). Multiple limits may be set for additional control. For example, [[100,1440],[50, 720]]. The rate limit timeframe begins when the first sample is submitted for analysis. Rate limits use a turnstile model: once the rate limit is reached for the timeframe specified, no more samples may be submitted until the timeframe has expired. Each sample expires one at a time. As each sample reaches the timeframe limit, it is cleared from the rate limit, and another sample may be submitted. Note that the rate limit order does not matter: the more restrictive limit is applied first.
Usage	Do not hyphenate. Usually referred to in the plural: rate limits And as a verb in the gerund form: rate limiting

RCM (Resource Conservation Mode)

Products	SMA
Definition	When an SMA becomes overloaded, it enters into the Resource Conservation Mode (RCM), and sends a critical system alert. This is designed to protect the appliance and allow it to process any backlog of messages.
Usage	Docs—Expand on first use.

regular expression

Products	Any
Definition	A sequence of characters that defines a search pattern.
Usage	Use 'regex' only in field labels or other GUI elements where space is an issue, and in documentation describing those GUI elements. Otherwise, spell out 'regular expression.'

remote device manager

Products	ASA, Firepower

Definition	A client-based or cloud-based application used to configure a device. A remote device manager is not installed on the appliance or delivered with the device's software. Adaptive Security Device Manager, Cisco Defense Orchestrator, Firepower Management Center, Cisco Security Manager, and a Meraki dashboard are examples of remote device managers. See also 'multi-device manager.'
Usage	Do not use 'off-box manager' in place of 'remote device manager.'

report

Products	Any
Definition	Mechanism used to track all activities within an organization over time.

reputation filter

Products	ESA
Definition	A way of filtering suspicious senders based on their reputation. The SenderBase Reputation Service provides an accurate, flexible way for you to reject or throttle suspected spam based on the connecting IP address of the remote host.

response action

Products	Cloudlock

Definition

An effect automatically triggered when a security incident is generated by a policy in which the response action is stored.

- Box: Quarantine User Files—Response action specific to the Box platform that places files that violate a policy in a quarantine state (as defined by Box).
- Delay Next—Response action that adds a delay between a set of response actions in a workflow. A use case can be delaying a response action that restricts sharing or changes file ownership to give the current document owner an opportunity to correct the policy violation.
- Incident Status Update—Response action that updates the status of an incident (for example, from New to Resolved) when previous response actions have automatically mitigated the policy violation.
- Send Admin Notification—Response action that sends an email to designated administrators informing them of a security incident generated by a DLP policy scanning content stored in a customer's cloud platform.
- Send User Notification—Response action that sends an email to the user account(s) owning files containing content that triggered a security incident generated by a DLP policy scanning content stored in a customer's cloud platform.

Usage

The term is the label of a control in the UI selected by an admin user.

revert

Products

Any

Definition

Return to a previous state. In most cases, this action is a willful initiation and not the outcome of a failed process.

Usage

Contrast with 'rollback.'

RMA (return material authorization)

Products

Hardware

Definition

The Cisco program for returning faulty hardware and obtaining a replacement.

Usage

Docs—Expand on first use.

'RMA' can also be used as a verb.

roaming client

Products

Umbrella

Definition	Umbrella product that when installed lets you work off-network and yet still remain protected by Umbrella

roaming computer

Products	Umbrella
Definition	A computer onto which the Umbrella roaming client is installed.

role (Stealthwatch Cloud)

Products	Stealthwatch Cloud
Definition	Assigned to entities, representing one task or set of tasks for what an endpoint does. More than 1 can be assigned to a given endpoint, as they are not exclusive or 1:1 relationship.

rollback

Products	Any
Definition	Restore (device, setup, system, database, and so on) to a previously defined state. In most cases, this action is for returning to a stable state as a fallback mechanism due to a failed process. For instance, in Firepower, a software upgrade rollback is the process of restoring a device to its previous software version.
Usage	Noun, adjective: rollback Verb: roll back Contrast with 'revert.'

routed firewall mode

Products	ASA
Definition	In routed firewall mode, the ASA is counted as a router hop in the network. It performs NAT between connected networks and can use OSPF or RIP.

routed interface

Products	ASA
Definition	An interface that routes traffic in a Layer 3 deployment. You can set up physical routed interfaces for handling untagged VLAN traffic, and logical routed interfaces for handling traffic with designated VLAN tags. You can also add static Address Resolution Protocol (ARP) entries to routed interfaces.

routing policy

Products	WSA
Definition	Directs web traffic through upstream proxies or directs it to destination servers. You might want to redirect traffic through upstream proxies to preserve your existing network design, to off-load processing from the WSA, or to leverage additional functionality provided by 3rd-party proxy systems. If multiple upstream proxies are available, the WSA can use load balancing techniques to distribute data to them.
Usage	Can be used in the singular and plural forms: routing policy, routing policies.

RU (rack unit)

Products	Hardware
Definition	A rack is measured in rack units. An RU is equal to 44 mm or 1.75 inches.
Usage	Do not expand.

rule

Products	Any
Definition	A configuration of conditions or criteria and the action taken as a result of meeting those criteria.
Usage	Use as a noun.

rule set

Products	Any
Definition	A way to group rules with a logical name to organize the rules.
Usage	Use as a noun.

rule preemption

Products	ASA, CDO, Firepower
Definition	Rule preemption occurs when a rule in a security policy will never match traffic because a rule earlier in the evaluation order matches the traffic first.

Usage	Use as a noun or verb, for example: • Proper rule order prevents rule preemption. • Rule 1 preempts Rule 2. Do not use these terms or their variants: • shadowed rule • redundant rule • superseded rule • masked rule • rule conflict

S

SAML (Security Assertion Markup Language)

Products	Any
Usage	GUI—Do not expand. Docs—Expand on first use.

sample

Products	Threat Grid
Definition	A sample is an example of possible malware. It may be a type of file, a URL, or even a file-like object, such as a process running in memory. Samples are submitted for malware analysis.

SAS (Serial Attached SCSI)

Products	Hardware
Usage	Do not expand.

SATA (Serial Advanced Technology Attachment)

Products	Hardware
Definition	Connects the host bus adapters to mass storage devices such as hard disk drives, optical drives, and SSDs.
Usage	Do not expand.

SBRS (SenderBase Reputation Score)

Products	ESA, SMA
Definition	A numeric value assigned to an IP address based on information received from the SenderBase Reputation Service.
Usage	Docs—Expand on first use.

SCEP (Simple Certificate Enrollment Protocol)

Products	Any
Definition	Protocol used for client enrollment and other PKI operations. An encrypted certificate issued by a certificate authority provides unalterable confirmation of the server identity. You can request a certificate from any certificate authority and upload that custom certificate to your appliance.
Usage	GUI—Do not expand. Docs—Do not expand unless context requires it.

SCSI (Small Computer System Interface)

Products	Hardware
Usage	Do not expand.

seat

Products	Umbrella
Definition	An internet-connected user who may have access to the service. Equivalent to a user of a service.

secret key

Products	Any
Definition	A key shared only between the sender and receiver.

SecureRank

Products	Umbrella

Definition	An algorithmic classifier based on graph theory that effectively finds domains guilty by association. It creates a large bipartite graph of the internet, and examines where known compromised systems are going, as well as other systems that are hitting malicious locations. Then this classifier finds other common locations that those systems are visiting and determines those locations that are malicious. This classifier ranks the security risks of all domain names by applying an iterative process similar to Google's PageRank algorithm.
Usage	Use camel case: SecureRank

security appliance

Usage	See 'appliance.'

security certifications compliance

Products	Hardware, Software
Definition	Compliance with security standards established by organizations such as the U.S. Department of Defense and other global certification organizations.

security context (ASA)

Products	ASA
Definition	You can partition a single ASA 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 context (Threat Response)

Products	Threat Response
Definition	Information about the assets, data policy, and customer environment. For example: • Where was the observable seen in the environment? • What value are the assets involved? • What's the policy regarding priority?

security event

Products	Stealthwatch Enterprise

Definition

The algorithm Stealthwatch uses that looks for specific behavior and can alert on that behavior on your network. It does this by directly generating a host alarm (if set to do so), or by assigning index points to alarm categories that can in turn trigger a host alarm.

A security event can indicate a security breach, a misconfigured device, malfunctioning server, or other source of networking issues. Every time that behavior is seen on your network, the number of index points increases.

security policy

Products

Any

Definition

A description of security requirements that define access to corporate assets. A security policy is implemented by creating things like rules and filters that evaluate traffic and allow or block access to resources. A security policy is not an object or a feature that is enabled or created.

There can be different kinds of security policies. For example, Firepower considers these types of policies security policies:

- access control
- identity policies
- intrusion policies
- security intelligence

In addition, the ASA considers these actions aspects of a security policy:

- applying application inspection
- applying HTTP/HTTPS/FTP filtering
- enabling threat detection
- protecting from IP fragments

Usage

Do not abbreviate. Always spell out.

sender group

Products

ESA

Definition

A list of senders gathered together for the purpose of handling email from those senders in the same way, such as applying a mail flow policy to a group of senders. In a sender group, the senders (identified by IP address, IP range, host/domain, SenderBase Reputation Service classification, SenderBase Reputation score range, or DNS List query response) are separated by commas in a listener’s Host Access Table (HAT).

sensing interface

Products

ASA, Firepower, Hardware

Definition

The interface on the appliance that monitors the chosen network segment. The sensing interface is in promiscuous mode; it has no IP address and is not visible on the monitored segment.

sensor

Products

Hardware

Definition

Analyzes network traffic by searching for signs of unauthorized activity.

Usage

Legacy term in security hardware for a physical device that analyzes network traffic.

Instead, use 'device' except for Stealthwatch, which uses 'Flow Sensor' as a branded term for legacy purposes.

sensor (Threat Response)

Products

Threat Response

Definition

A process or device which observes activity on a network or endpoint and generates events, alerts, or other data flows. Examples include a NetFlow-generating router or an AMP for Endpoints connector.

serial number onboarding

Products

CDO

Definition

Refers to the process of onboarding an FTD by using its serial number, which has already been installed and set up.

Could also be onboarding with a serial number. The goal is not to rigidly define this term but point out that this process is different from low-touch provisioning.

Usage

We're using this kind of terminology generically. Like, onboarding with username and password.

server certificate

Products

Any

Definition

An encrypted certificate issued by a certificate authority that provides unalterable confirmation of the server identity. You can request a certificate from any certificate authority and upload that custom certificate to your appliance.

service

Products	REST API
Definition	The object or function which can be manipulated using the REST API. These are presented to the user as a URL, sometimes with other options within the URL.
Usage	These are also called endpoints, resources, or objects. In the past these have been called objects, but going forward, we prefer 'service' to avoid ambiguity. Note that a service *is not* an API.

service policy

Products	ASA
Definition	A service policy consists of multiple actions or rules applied to an interface or applied globally. Use service policies to apply advanced services to the traffic you are allowing. Any traffic permitted by access rules can have service policies applied, and thus receive special processing, such as being redirected to a service module or having application inspection applied. Features configured with service policies: https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/firewall/asa-98-firewall-config/inspect-service-policy.html#ID-2094-0000007b
Usage	Do not abbreviate. Always spell out.

SFP transceiver (small form-factor pluggable)

Products	Hardware
Definition	A fiber optic transceiver that adapts optical cabling to fiber interfaces.
Usage	Docs—Expand on first use.

SHA-256

Products	Any
Definition	SHA-256 value or hash.
Usage	Do not use SHA256, Sha-256, Sha256, sha-256, or sha256.

shared secret

Products	Any

Definition	A piece of data known only to the parties involved in a secure communication. The shared secret can be a password, a passphrase, a big number, or an array of randomly chosen bytes.

sighting

Products	Threat Response
Definition	Detection of an observable within my environment (on network). For example, a data object encoding an event, alert, or observed behavior that is security-significant, and a limited set of information about the context of the observation. See also 'encounter.'

sinkhole

Products	Any
Definition	A server that gives out false DNS responses so that the domain requested cannot be reached. Often used to block botnets from connecting to their command-and-control servers.
Usage	Do not use 'blackhole.'

slave

Usage	Do not use. Instead, use 'backup,' 'secondary,' 'standby,' or 'subordinate,' contextually. For example, when 2 units are operating in failover mode with each other, instead of 'master' and 'slave,' use 'primary' and 'secondary.' However, in ASA VPN load balancing, do not use 'backup' (and 'master'). Instead, use 'member' (and 'director').

SmartCache

Products	Umbrella
Definition	Makes websites that are effectively down for others accessible only on Umbrella. SmartCache uses the intelligence of the Umbrella network at large, providing DNS service to tens of millions of people around the world, to locate the last known correct address for a website when its authoritative name server is offline or otherwise failing.
Usage	Use camel case: SmartCache

SN (serial number)

Products	Hardware
Definition	Part of the UDI. The SN is the serial number of your Cisco product.
Usage	Docs—Expand on first use.

Snort

Products	Firepower
Definition	Firepower's access control and intrusion inspection engine. Includes (but is not limited to) Security Intelligence, application control, URL filtering, user control, file control and device-side AMP for Networks, intrusion inspection, and SSL decryption/reencryption.
Usage	Do not use as a synonym for the Firepower software or operating system, especially in the GUI. Instead, use generic terms such as 'Firepower,' 'the system,' or 'inspection engine.' Use Snort only in the documentation in the following contexts: • describing Snort process restarts • commands that include the snort keyword • troubleshooting and interpreting CLI output or other system messages Capitalize unless you are talking about commands or system output. Do not use the registered trademark symbol.

SOCKS policy

Products	WSA
Definition	Allows or blocks SOCKS (Socket Secure) communication requests.
Usage	SOCKS (all caps) in docs and GUI.

software agent

Products	Any
Definition	For instance, in Cisco Tetration, a software agent is a small software application running on a host system. Its core functionality is to monitor and collect network flow information.

SOL (Serial Over LAN)

Products	Hardware

Definition	Mechanism that enables the input and output of the serial port of a managed system to be redirected over IP.
Usage	Expand on first use to differentiate from other uses.

spam quarantine

Products	SMA
Definition	Provides a safeguard mechanism for organizations that are concerned about false positives. Quarantines legitimate email messages that the SMA has deemed to be spam.

SPAN (Switched Port Analyzer)

Products	ASA
Definition	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.
Usage	Do not expand. Noun: SPAN Adjective: SPAN port

SPRank

Products	Umbrella
Definition	A detection model that uses mathematical concepts more commonly used to analyze sound waves in real time. Instead of sound waves, the model tracks patterns in network traffic, "listening" for categorized malicious patterns.
Usage	Use camel case: SPRank

SSD (Solid State Drive)

Products	Hardware
Usage	Do not expand.

SSL (Secure Sockets Layer) decryption

Products	Firepower

Definition

Some protocols, such as HTTPS, use Secure Sockets Layer (SSL) or its successor, Transport Layer Security (TLS), to encrypt traffic for secure transmissions. Undesirable traffic can be hidden within encrypted connections. Because the system cannot inspect encrypted connections, you must decrypt them if you want to apply access rules that consider higher-layer traffic characteristics to make access decisions.

SSL decryption can decrypt connections, inspect them to ensure that they do not contain threats or other undesirable traffic, and then re-encrypt them before allowing the connection to proceed. The decrypted traffic goes through your access control policy and matches rules based on inspected characteristics of the decrypted connection, not on the encrypted characteristics.

Usage

Docs—Expand on first use.

Because TLS and SSL are often used interchangeably, we use the expression TLS/SSL to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret TLS/SSL as referring to TLS only.

The exception is SSL policies. Because the FMC configuration option is **Policies > Access Control > SSL**, we use the term SSL policies, even though these policies are used to define rules for TLS and SSL traffic.

SSP (Security Services Processor)

Products

Hardware

Usage

Expand on first use to differentiate from other uses.

stack, stacked

Products

Hardware

Definition

A feature that lets you increase the amount of traffic inspected on a network segment by connecting 2 to 4 physical devices in a stacked configuration. When you establish a stacked configuration, you combine the resources of each stacked device into a single, shared configuration.

standard ACL (ASA)

Products

ASA

Definition

An ACL that identifies traffic by *destination* address only. There are few features that use them: route maps and VPN filters. Because VPN filters also allow extended access lists, limit standard ACL use to route maps.

Usage

Do not expand.

standard ACL (Cisco IOS)

Products	Cisco IOS
Definition	Filters traffic (performs access control) by *source* address only. Contrast with standard ACLs in ASA, which are primarily for matching traffic in features other than access control. When it comes to access control, IOS and ASA are fundamentally very different.
Usage	Do not expand.

static analysis

Products	Firepower, Threat Grid
Definition	The basic analysis of the sample submission as a file, including file type, metadata, its contents, attachments, and so on.

static NAT

Products	Any
Definition	Creates a fixed translation of a real address to a mapped address. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if an access rule exists that allows it).
Usage	Do not abbreviate 'static NAT.'

Stealthwatch Cloud Sensor

Products	Stealthwatch Cloud
Definition	The deployed software that connects to Stealthwatch Cloud and submits log and other data from your local network.
Usage	GUI—Do not use. Docs—Always use 'Stealthwatch Cloud Sensor.' Do not shorten ('sensor') or abbreviate ('SCS').

Stealthwatch Management Console

Products	Stealthwatch Enterprise

Definition	Aggregates, organizes, and presents analysis from up to 25 Flow Collectors, the Cisco Identity Services Engine, and other sources. This interface uses graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis. The capacity of the console determines the volume of telemetry data that can be analyzed and presented, as well as the number of Flow Collectors that are deployed. The console is available as a hardware or virtual machine.
Usage	Do not abbreviate. Always spell out.

STIX (Structured Threat Information eXpression)

Products	Cognitive, ESA
Definition	The industry standard, structured language to represent cyber threat information.
Usage	Docs—Expand on first use.

submission

Products	Threat Grid
Definition	A sample of suspected malware that has been submitted (uploaded) for analysis.

support mode

Products	Threat Grid
Definition	A live support session that gives Threat Grid appliance support engineers remote access to an appliance or account.

suspicious

Products	Threat Grid, Threat Response
Definition	A verdict that indicates the subject should be examined thoroughly because it contains logic that must be emulated, or there are anomalies that suggest some sort of obfuscation or malicious intent.

system

Products	Any
Definition	A set of things working together as parts of a mechanism or an interconnecting network; a complex whole.

Usage	Use 'system' to refer to the platform with its software installed. Do not use to refer to only the hardware such as legacy terms Firepower System, Sourcefire 3D System, and Stealthwatch System. While the use of the term 'system' is generic, its use helps to stop cluttering text with repetitive product names and avoid discussing the inner workings of our products unless the customer really needs the information. Use the term 'system' after being introduced with the proper names of the products it represents.

T

TAC (Cisco Technical Assistance Center)

Products	Any
Definition	There are 4 centers worldwide providing technical assistance to Cisco customers.
Usage	Do not say 'the TAC.'

TACACS+ (Terminal Access Controller Access Control System Plus)

Products	Any
Definition	Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.
Usage	Do not expand.

Talos (Cisco Talos Intelligence Group)

Products	Any
Definition	The Talos team protects customers' people, data, and infrastructure. Researchers, data scientists, and engineers collect information about existing and developing threats. They then deliver protection against attacks and malware. For more information, see https://talosintelligence.com/.

Usage

Docs—Expand on first use. Cisco Talos Intelligence Group.

Shorten the name in GUI messages and subsequent documentation mentions, such as Talos or Cisco Talos.

Do not use:

- TALOS
- Sourcefire Vulnerability Research Team
- Cisco Vulnerability Research Team
- Cisco Talos Security Intelligence and Research Group

Talos Threat Level

Products

Any

Definition

Talos reputation verdict scores are referred to with Talos Threat Levels in integration documentation and on TalosIntelligence.com. CTR and SSE-Eventing both use Talos Web Reputation, and all Talos consumers should align with the same terminology and score ranges for consistency across the Cisco security product portfolio.

Usage

Use these Talos Threat Levels when Talos Web Reputation verdicts are shown in a product or documentation. The reputation verdict scores should not be shown.

Talos Threat Level	Definition	Score Range
Untrusted	Displaying behavior that is exceptionally bad, malicious, or undesirable.	-10.0 through -6.0
Questionable	Displaying behavior that may indicate risk or could be undesirable.	-5.9 through -3.1
Neutral	Displaying neither positive nor negative behavior. However, has been evaluated.	-3.0 through 0.0
Favorable	Displaying behavior that indicates a level of safety.	+0.1 through +5.9
Trusted	Displaying behavior that indicates exceptional safety.	+6.0 through +10.0
Unknown	Not previously evaluated, or lacking features to assert a threat level verdict.	No score

target (Threat Response)

Products

Threat Response

Definition	Any device, user, identity, asset, or resource which is infected, compromised, or impacted by a threat. A target is identified by one or more observables. Targets are always part of a sighting.
Usage	Outside of Threat Response, 'target' can be used in its standard English definition.

target index

Products	Stealthwatch
Definition	Tracks hosts that appear to be victims of the suspicious behavior of other hosts. Every time a Stealthwatch Flow Collector sees that a host is the target of suspicious behavior, it adds points to the target index for that host. When the number of points exceeds 100% of the acceptable threshold for that host, the Flow Collector generates a High Target Index alarm, alerting you to the possibility that the host is under attack. See also 'alarm.'
Usage	Do not abbreviate. Always spell out.

TAXII (Trusted Automated eXchange of Indicator Information)

Products	Cognitive, ESA
Definition	Defines a set of specifications to exchange cyber threat information using services (TAXII servers) across different organizations or product lines.
Usage	Docs—Expand on first use.

threat actor

Products	ATS, Stealthwatch
Definition	Individuals, groups, or organizations believed to be operating with malicious intent. A threat actor is not an intrusion set, but may support or be affiliated with various intrusion sets, groups, or organizations over time.

threat hunting

Products	Any
Definition	The process of proactively and iteratively searching the network to detect and isolate advanced threats that may have evaded your existing security solutions. For more information, see https://www.threathunting.net/reading-list.
Usage	Threat hunting starts with a hypothesis. Do not use in reference to any activity that starts with a security alert or detection.

threat intelligence

Products	Any
Definition	What threat information becomes once it has been collected, analyzed, and evaluated in the context of its source and reliability.
Usage	Do not abbreviate intelligence as intel.

threat root cause

Products	AMP
Definition	The parent file or application that allowed a threat onto an endpoint. An example of a threat root cause is the vulnerable application that was exploited and allowed the threat to be downloaded and executed on the endpoint.

threat score

Products	Threat Grid
Definition	A measure of the amount of system weakening, obfuscation, persistence, modification, data exfiltration, and other behaviors discovered during sample analysis, that may be a threat to the host system's integrity. It is intended as an overall threat indicator--a triage metric--that can be used as a guide to the likelihood that a submission is malicious. 'Look at this first.' The threat score can range from 0 - 100. It is not an authoritative classification of good and bad software; for that we use allowed lists.

TLS (Transport Layer Security) decryption

Products	Firepower
Definition	By default, the Firepower system cannot inspect traffic encrypted with the Secure Socket Layer (SSL) protocol or its successor, the Transport Layer Security (TLS) protocol. TLS/SSL decryption and inspection enables you to either block encrypted traffic without inspecting it, or inspect encrypted or decrypted traffic with access control. The combination of inspecting encrypted traffic and analyzing encrypted session data allows greater awareness and control of the encrypted traffic in your network.
Usage	Docs—Expand on first use. Because TLS and SSL are often used interchangeably, we use the expression TLS/SSL to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret TLS/SSL as referring to TLS only. The exception is SSL policies. Because the FMC configuration option is **Policies** > **Access Control** > **SSL**, we use the term SSL policies, even though these policies are used to define rules for TLS and SSL traffic.

trajectory

Products	AMP, Firepower
Definition	The course of actions a threat takes on an endpoint or across a network. An example of a trajectory is when Threat A exploits a vulnerability, downloads files X, Y, and Z, executes files X, Y, and Z, and then copies itself to all network shares.

transparent firewall mode

Products	ASA
Definition	A mode in which the ASA is not a router hop. You can use transparent firewall mode to simplify your network configuration or to make the ASA invisible to attackers. You can also use transparent firewall mode to allow traffic through that would otherwise be blocked in routed firewall mode.

transparent inline mode

Products	ASA
Definition	An advanced inline set option that lets a device act as a bump in the wire and forward all the network traffic it sees regardless of its source and destination.

trust (rule action)

Products	Firepower
Definition	A rule action that allows matching traffic to pass without further *deep* inspection, while still being subject to limited further handling. For example, traffic that is trusted by a Firepower access control rule is still subject to identity requirements and rate limiting (QoS), but is not subject to network discovery, intrusion inspection, and malware inspection. Contrast 'trust' with the 'fastpath' action, which exempts matching traffic from *all* further inspection and control.
Usage	Examples: trust rule, trust action, trust rule action

trusted certificate

Products	Any
Definition	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

Products	Any
Definition	Public key upon which a user relies; especially a public key that can be used as the first public key in a certification path.

trusted server validation

Products	AnyConnect
Definition	The process of analyzing and validating a server's certificate chain sent in an authentication exchange, such as TLS. The client validates that the server's certificate was issued by a trusted CA and also validates the name of the server contained in the certificate (as compared to the DNS name used to connect), the certificate purpose, key usages, and dates of validity.

two-factor authentication (2FA)

Products	Any
Definition	Strengthens access security by requiring two different methods (also referred to as factors) to verify your identity. These factors can include something you know (username and password), something you are (fingerprint), or something you have (secondary trusted device like a smartphone app or token to approve authentication requests). Compare with two-step verification, which can use the same type of information delivered by different sources. For example, a password you know plus a code you're sent over SMS.
Usage	Docs—Expand on first use. Thereafter, can be shortened to 2FA.

two-step authentication

Products	Any
Definition	A method of confirming a user's claimed identity by utilizing something they know (password) and a second step other than something they have or something they are. An example of a second step is the user repeating back something that was sent to them through an out-of-band mechanism.
Usage	Synonym: two-step verification

two-step verification

Products	Umbrella

Definition	A method used to prove one’s identity by entering 2 different components, something one knows and something one possesses. Most often, two-step verification is a password plus a unique and randomly generated string of numbers sent to the user.
Usage	Synonym: two-step authentication

U

UDI (Unique Device Identifier)

Products	Hardware
Definition	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.
Usage	Docs—Expand on first use.

UDP Director

Products	Stealthwatch Enterprise
Definition	A physical or virtual device that allows NetFlow data to be sent transparently to multiple collection points, such as network management solutions.
Usage	Expand the full name on first use: Cisco Stealthwatch UDP Director. Thereafter, can be shortened to UDP Director.

Umbrella Threat Intelligence

Products	Umbrella
Definition	Automates detection of both known and emergent threats. Umbrella threat intelligence analyzes a cross section of the world’s internet activity to observe infrastructure being staged. It is a tool built by Cisco Umbrella security researchers that allows us to block sites that are going to host malware, bot networks, and phishing, before they actually become malicious. It is Umbrella technology that automates protection against both known and emergent threats before an attack is launched.
Usage	Do not abbreviate. Always spell out.

unit

Products	Any
Definition	A device that has been enabled for high availability.

Usage	Also used in clustering. Also used in Regulatory statements to refer to the hardware device. Examples: primary unit, secondary unit

update

Products	Any
Definition	A change that provides new information for use by a product, but that does not change functionality. For example, you can update rules, reputation data, vulnerabilities, geolocation information, and so on. Contrast with 'upgrade' and 'patch.'
Usage	Use as a noun or verb.

upgrade

Products	Any
Definition	A change that introduces new features and functionality, changes behavior, fixes bugs, or otherwise improves a product. Upgrades are usually associated with a change in version number. See also 'patch.' Contrast with 'update.'
Usage	Use as a noun or verb.

URL categories

Products	WSA
Definition	URL categories are predefined or custom categories of websites, such as News, Business, Social Media, and so on. These can be used to identify or apply actions to web requests.

USB (Universal Serial Bus)

Products	Hardware
Definition	USB Type A USB Type B USB Type C USB Mini B USB Micro B USB 3.0 Type B

Usage	Do not expand. Use as a noun or adjective. For example, USB Type A connector.

user emulation playbook

Products	Threat Grid
Definition	A predefined set of user actions that may be selected when submitting a sample, which is performed automatically during analysis as if a user were present and operating the keyboard and mouse, for example, mouse movements, clicking mouse buttons, entering data, or opening a browser. If the sample submission is looking for user actions that are defined in the selected playbook, then those requirements are fulfilled and the sample continues its execution.
Usage	Shorten to just 'playbook' after first use.

user EXEC mode

Products	ASA
Definition	User EXEC mode lets you see the ASA settings.

USGv6 (U.S. Government Compliance for IPv6)

Products	Software
Definition	The U.S. Government Compliance for IPv6 (USGv6) indicates that it is compliant to U.S. government profiles for products that implement IPv6.
Usage	Docs—Expand on first use.

V

verdict

Products	Threat Response
Definition	The most current, unexpired judgement with the highest priority for an observable. A verdict is chosen from among the unexpired judgements for a particular observable. The judgement with the highest priority becomes the active verdict. If there is more than one judgement with that priority, then they are prioritized as follows: a 'clean' disposition has priority over all others, 'malicious' is next, and so on down to 'unknown.'

VID (version identifier)

Products	Hardware

Definition	Part of the UDI.
Usage	Docs—Expand on first use.

virtual appliance

Products	Any
Definition	Created by the installation of a software appliance on a virtual machine. Packaged into an image file, a virtual appliance consists of a pre-configured operating system environment and an application. The purpose of a virtual appliance is to simplify delivery and operation of an application. Virtual appliances are a subset of the broader class of software appliances.
Usage	Depending on context, can be abbreviated as VA.

virtual device

Products	Any
Definition	While it exists only in software form, a virtual device can mimic a physical hardware device. In UNIX, a virtual device is a file that is treated as a device, although it is generated by the kernel without reference to hardware.
Usage	Do not abbreviate.

virtual machine

Products	Any
Definition	A virtual machine is an operating system or application that is installed on software, which imitates dedicated hardware. An emulation of a computer system, virtual machines are based on computer architectures and provide the functionality of a physical computer.
Usage	Depending on context, can be abbreviated as VM.

Visibility

Products	Visibility
Definition	An investigative tool that leverages AMP, Threat Grid, and other Cisco and 3rd party products and services, to simplify and speed up common incident response tasks by automating and collating research and response functions across those multiple products and tools.
Usage	Always capitalize. Changed to Cisco Threat Response.

visibility

Products	Threat Grid
Definition	The level of access a user has to the contents of a sample analysis report. It is based on the privacy setting of the sample, and the organization membership of the submitting user and the viewing user. Full visibility grants users full access to the sample and the analysis results. Users with no visibility have no access. Partial visibility grants access to reports that have been scrubbed of sensitive, identifying information.

VPC (Virtual Private Cloud)

Products	Stealthwatch Cloud
Definition	Similar to NetFlow, it allows the service to monitor AWS environments without the need for a software agent.
Usage	Docs—Do not expand unless context requires it. GUI—Do not expand.

VPN load balancing

Products	ASA
Definition	A mechanism for equitably distributing remote-access VPN traffic among the devices in a VPN load-balancing group. It's based on simple distribution of traffic without taking into account throughput or other factors. A VPN load-balancing group consists of two or more devices. One device is the director, and the other devices are member devices. Group devices do not need to be of the exact same type, or have identical software versions or configurations. All active devices in a VPN load-balancing group carry session loads. VPN load balancing directs traffic to the least-loaded device in the group, distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.
Usage	Do not use VPN load-balancing 'cluster.' Instead, use VPN load-balancing 'group.' Do not use 'master' and 'backup.' Instead, use 'director' and 'member.'

VPN local policy

Products	AnyConnect
Definition	Specifies security authorizations with update policy settings when AnyConnect is installed manually or deployed to a device using an enterprise software development system.

VSA (vendor-specific attribute)

Products	Any
Definition	An attribute in a RADIUS packet that is defined by a vendor rather than by RADIUS RFCs. The RADIUS protocol uses IANA-assigned vendor numbers to help identify VSAs. This lets different vendors have VSAs of the same number. The combination of a vendor number and a VSA number makes a VSA unique. For example, the cisco-av-pair VSA is attribute 1 in the set of VSAs related to vendor number 9. Each vendor can define up to 256 VSAs. A RADIUS packet contains any VSAs attribute 26, named Vendor-specific. VSAs are sometimes referred to as subattributes.
Usage	Docs—Expand on first use.

W

warn (policy action)

Products	WSA
Definition	In the WSA access policy, the warn action displays a notification to the end user, who may then choose to click through to continue.
Usage	Warnings, notes, and cautions are addressed in the Cisco Technical Content Style Guide.

WCCP (Web Cache Communication Protocol)

Products	ASA
Definition	Transparently redirects selected types of traffic to a group of web cache engines to optimize resource usage and lower response times.
Usage	Docs—Expand on first use.

WCCP (Web Cache Communication Protocol) service

Products	WSA
Definition	An appliance configuration that defines a service group to a WCCP v2 router. It includes information such as the service ID and ports used. Service groups allow a web proxy to establish connectivity with a WCCP router and to handle redirected traffic from the router.
Usage	Docs—Expand on first use.

WBRS (Web-Based Reputation Score)

Products	WSA
Definition	Web Reputation Filters assign a Web-Based Reputation Score (WBRS) to a URL to determine the likelihood that it contains URL-based malware. This granular score of -10 to +10 offers increased flexibility, since different security policies can be implemented based on different scoring ranges. The WSA uses WBRS to identify and stop malware attacks before they occur.
Usage	Docs—Expand on first use.

Web Reputation Filters

Products	WSA
Definition	Web Reputation Filters analyze web server behavior and assign a Web-Based Reputation Score to a URL to determine the likelihood that it contains URL-based malware.

webtype ACL

Products	ASA
Definition	An ACL used for filtering clientless SSL VPN traffic. These ACLs can deny access based on URLs or destination addresses.

whitelist

Usage	Do not use. Instead, standardize use around 'allow list' (to mean a list that allows). In cases where it makes more sense, it's okay to use 'allowed list' (to mean a list of allowed items).

X

XAUTH (extended authentication)

Products	Any
Definition	Provides the capability of authenticating a user within IKE using TACACS+ or RADIUS. Authenticates a user using RADIUS or any of the other supported user authentication protocols. The XAUTH username and password parameters are used when secure unit authentication is disabled and the server requests XAUTH credentials.
Usage	Docs—Expand on first use.

xlate

Products	ASA
Definition	Also referred to as a translation entry, an xlate represents the mapping of 1 IP address to another, or the mapping of 1 IP address and port pair to another.

Y

Z