










# Chapter 1 - Key Terms

 Term	 Page	 Description
<u>network firewalls</u>	585	A firewall that provides key features used for perimeter security. The primary task of a network firewall is to deny or permit traffic that attempts to enter or leave the network based on explicit preconfigured policies and rules. Firewalls are often deployed in several other parts of the network to provide network segmentation within the corporate infrastructure and also in data centers.
<u>Access Control Lists (ACLs)</u>	577	A set of predetermined rules against which stateful and traditional firewalls can analyze packets and judge them. They inspect the following elements within a packet: <i>source address</i> , <i>destination address</i> , <i>source port</i> , <i>destination port</i> , and <i>protocol</i> . ACLs are typically configured in firewalls, but they also can be configured in network infrastructure devices such as routers, switches, wireless LAN controllers (WLCs), and others.
<u>Network Address Translation (NAT)</u>	585	A method often used by firewalls; however, other devices such as routers and wireless access points provide support for NAT. By using NAT, the firewall hides the internal private addresses from the unprotected network and exposes only its own address or public range. This enables a network professional to use any IP address space as the internal network.
<u>Data Loss Prevention (DLP)</u>	580	A software or cloud solution for making sure that corporate users do not send sensitive or critical information outside the corporate network.
<u>Advanced Malware Protection (AMP)</u>	577	A Cisco solution for detecting and mitigating malware in the corporate network.
<u>Intrusion Prevention System (IPS)</u>	583	A network security appliance or software technology that inspects network traffic to detect and prevent security threats and exploits.

 Term	 Page	 Description
<u>Netflow</u>	584	Cisco technology that provides comprehensive visibility into all network traffic that traverses a Cisco-supported device. NetFlow is used as a network security tool because its reporting capabilities provide nonrepudiation, anomaly detection, and investigative capabilities. As network traffic traverses a NetFlow-enabled device, the device collects traffic
<u>Security Information and Event Manager (SIEM)</u>	587	A specialized device or software for security event management. It typically includes logs collection, normalization, aggregation and correlation capabilities, and built-in reporting.
<u>Security Orchestration, Automation, and Response (SOAR)</u>	587	A system that provides automation and security orchestration capabilities for the security operations center (SOC).
<u>Common Vulnerabilities &amp; Exposures (CVE)</u>	579	A dictionary of vulnerabilities and exposures in products and systems maintained by MITRE. A CVE-ID is the industry standard method to identify vulnerabilities.
<u>Common Vulnerability Scoring System (CVSS)</u>	579	An industry standard used to convey information about the severity of vulnerabilities.
<u>Common Weakness Enumeration (CWE)</u>	580	A specification developed and maintained by MITRE to identify the root cause (weaknesses) of security vulnerabilities. You can obtain the list of CWEs from <a href="https://cwe.mitre.org">cwe.mitre.org</a> .
<u>Common Weakness Scoring System (CWSS)</u>	580	A specification developed and maintained by MITRE to provide a way to prioritize software weaknesses that can introduce security vulnerabilities. You can obtain the list of CWSS from <a href="https://cwe.mitre.org/cwss">cwe.mitre.org/cwss</a> .

 Term	 Page	 Description
<u>Structured Threat Information Expression (STIX)</u>	588	A standard used to create and share cyber threat intelligence information in a machine-readable format.
<u>Trusted Automated Exchange of Indicator Information (TAXII)</u>	588	A standard that provides a transport mechanism (data exchange) of cyber threat intelligence information in STIX format. In other words, TAXII servers can be used to author and exchange STIX documents among participants.
<u>Cyber Observable eXpression (CybOX)</u>	580	A standard to document cyber threat intelligence observables in a machine-readable format. The OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) decided to merge the CybOX and the Structured Threat Information Expression (STIX) specifications into one standard. CybOX objects are now called STIX Cyber Observables. You can find additional information about the migration of CybOX to STIX at <a href="https://oasis-open.github.io/cti-documentation/stix/compare.html">https://oasis-open.github.io/cti-documentation/stix/compare.html</a> .
<u>Indicator of Compromise (IoC)</u>	583	One aspect of threat intelligence is knowledge about an existing or emerging threat to assets, including networks and systems.
<u>Script Kiddies</u>	587	People who use existing “scripts” or tools to hack into computers and networks; however, they lack the expertise to write their own scripts.