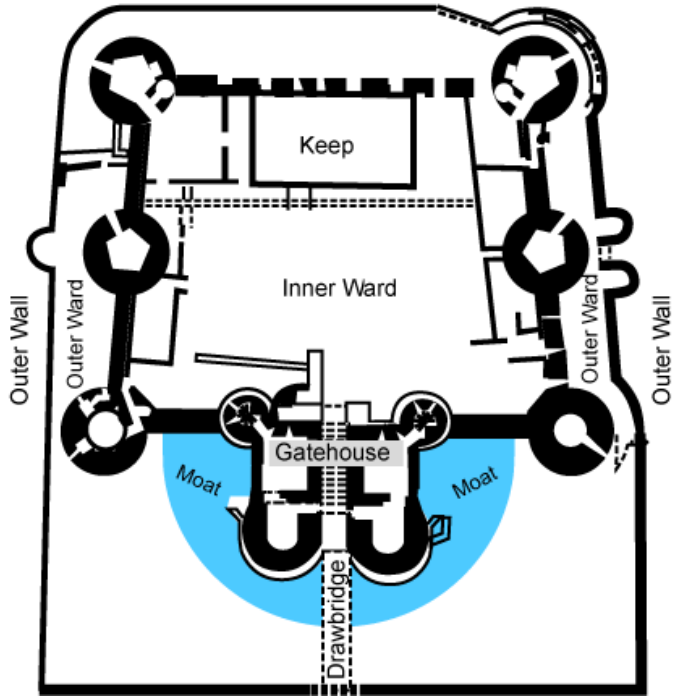
03- Network Security Technologies

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me

Defense-in-Depth Strategy

- Defense in depth can be considered a building block of other security design principles. This guideline calls for applying a layered approach to security, and it is aimed at providing redundant controls at multiple levels to mitigate risk.
- This same strategy was used in medieval castles to provide multiple layers of defense to resist lengthy sieges.

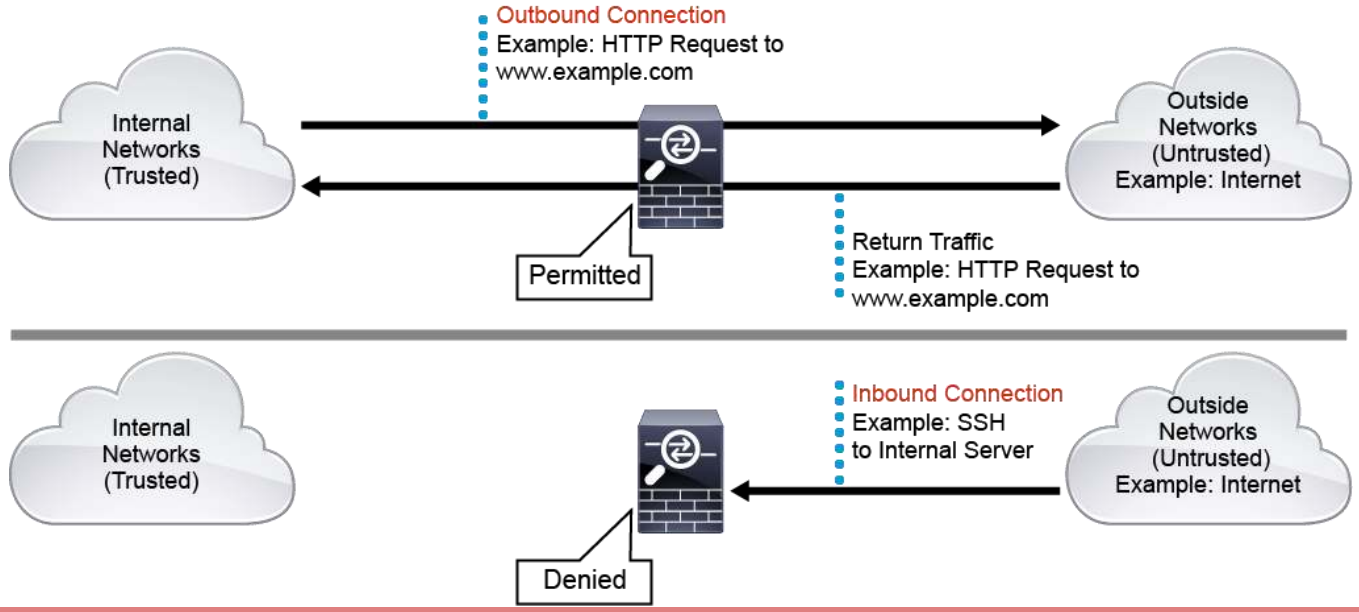


Defense-in-Depth Strategy (cont.)

- **Defense in depth is a philosophy that provides layered security to a system by using multiple security mechanisms and generally follows these principles:**
  - Security mechanisms should back each other up and provide diversity and redundancy of protection.
  - Security mechanisms should not depend on each other, so that their security does not depend on other factors that are outside their control.
  - Using defense in depth, you can eliminate single points of failure and augment weak links in the system to provide stronger protection with multiple layers.

Stateful Firewall Overview

- A Firewall is a network security device that monitors the incoming and outgoing network traffic and decides whether to allow or block the traffic based on a defined set of security rules.
- Firewalls have been a first line of defense in network security for many years.



Stateful Firewall Overview (cont.)

- **By default**, a stateful firewall such as the Cisco Adaptive Security Appliance (ASA) or Cisco Firepower NGFW will **permit** and **inspect** the traffic that is **initiated** from the **internal** trusted networks and is destined **to** the **outside** untrusted networks.
- The stateful firewall will also automatically permit the corresponding return traffic from the outside networks back to the internal networks. But
- Any traffic that is **initiated** from the **outside** networks and is destined to the **internal** networks is **denied by default**.
- Traffic from the outside however can be permitted as required and must be specifically allowed.

Stateful Firewall Overview (cont.)

- A **Stateless Packet Filter**, such as an access control list (ACL), accesses on a packet-by-packet basis.
- A **Stateful Firewall** allows or blocks traffic based on the connection state, port, and protocol.
- **Stateful firewalls** inspect all activity from the opening of a connection until the connection is closed.
- Data that is associated with each connection is stored in the firewall connection's state table.

Stateful Firewall Overview (cont.)

- Stateful packet filters maintain a state table to keep track of all active sessions that are crossing the firewall, such as a Cisco ASA security appliance or Cisco Firepower NGFW.
- A state table, which is an internal data structure of a stateful packet filter, tracks all OSI Layer 4 sessions and inspects all packets that are passing through the device.
- Based on its memory of previous packets in a session, a stateful packet filter can anticipate what kind of traffic should arrive from communicating hosts in the near future.

Stateful Firewall Overview (cont.)

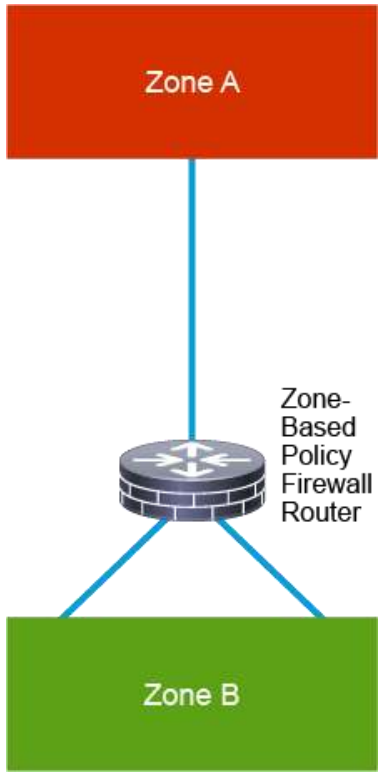
- Advanced stateful firewalls, such as the **Cisco ASA**, also offer features such as network address translations (NAT), identity-based access controls, applications layer inspections, VPN capabilities, and botnet traffic filtering.

Cisco IOS Zone-Based Policy Firewall Overview

- The Zone-Based Policy Firewall is a Cisco IOS Software feature that allows a router to act as a powerful and flexible stateful firewall between zones that correspond to security domains that are created through network separation.
- The router that is configured with Zone-Based Policy Firewall features can act either as a standalone firewall system or as an element of a more complex firewall system.
- Zone-Based Policy Firewall access control policies then control access between two or more zones that are configured on the router, using a flexible configuration language that allows you to specify simple or complex access policies in a manageable manner.

Cisco IOS Zone-Based Policy Firewall Overview (cont.)

- Router interfaces are assigned to security zones, and firewall inspection policy is applied to traffic moving between the zones.



Security Intelligence Overview

- Security Intelligence, threat intelligence, cyber threat intelligence, or "intel" for short is an important tool in preventing cyber attacks.
- Good security intelligence is one of first lines of defense against cyber attacks.
- For example, security intelligence feeds can be used to immediately block connections based on the latest reputation intelligence, removing the need for a more resource-intensive, in-depth packet analysis.
- To make gathering and maintaining security intelligence easier, several cloud-based services are available that can provide up-to-date threat intelligence.

Security Intelligence Overview (cont.)

- Many security intelligence services provide automatic updates that include dynamic lists of known Command and Control (CnC) servers, dangerous Uniform Resource Identifiers (URIs), or lists of known malicious hosts.
- Organizations can leverage these security intelligence feeds to prevent security incidents.
- Security intelligence feeds are extremely helpful, especially for organizations with no computer security incident response team, or an under-resourced security or Information Technology (IT) operations group.
- The use of security intelligence is a typical feature available in today's next-generation firewalls, and it works by blocking traffic to or from IP addresses that have a known bad reputation.

Security Intelligence Overview (cont.)

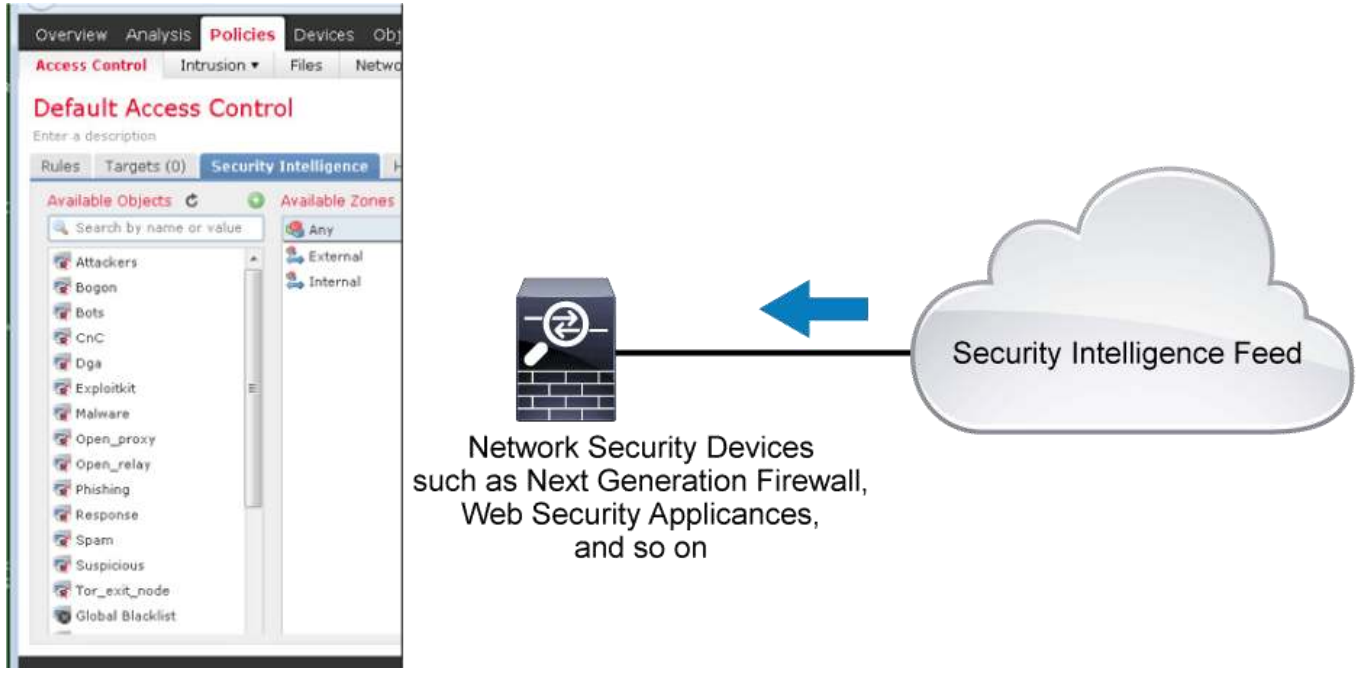
- This traffic filtering takes place before any other policy-based inspection, analysis, or traffic handling.
- Because the security intelligence feed is regularly updated, using it ensures that the system has up-to-date information to filter network traffic with.
- Malicious IP addresses that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and apply new policies.

Security Intelligence Overview (cont.)

- Cisco Talos Intelligence Group is one of the threat intelligence leaders in the market.
- Talos Intelligence Group is composed of leading threat researchers that create threat intelligence for Cisco products to protect customers from both known and emerging threats.
- The result is a security intelligence cloud producing "big intelligence" and reputation analysis tracking threats across networks, endpoints, mobile devices, virtual systems, web, and email providing a holistic understanding of threats, their root causes, and scopes of outbreaks.

Security Intelligence Overview (cont.)

- The figure shows an example of the Cisco FirePower Management Center GUI access control policy rule configuration where security intelligence can be used to drop specific malicious traffic before it is further analyzed by the access control rule.



Security Intelligence Overview (cont.)

- The security intelligence feed tracks known attackers, bogus IP addresses, and so on then categorizes them accordingly.
- Here, the security intelligence categorizes the blacklisted IP addresses as malware and attackers.

Security Intelligence Overview (cont.)

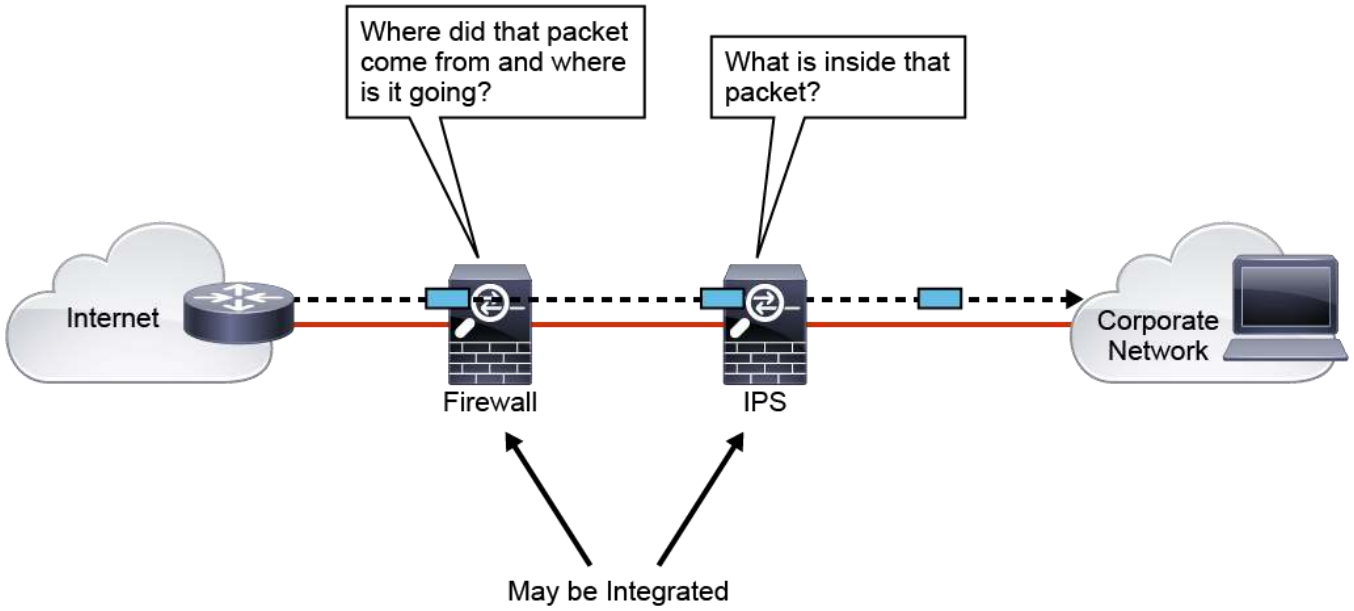
- In the previous figure, when the connections were initiated from the internal network IP addresses to the blacklisted IP address (123.151.149.222), The security intelligence feature immediately blocks the connections without the need for deeper analysis of the packet.
- It also categorizes the connection to the 123.151.149.222 IP address as malware.
- Overall, the data that are generated from Cisco FirePower Management Center provides important information to help you narrow down the threat and take protective action.

IPS Overview

- Intrusion sensors are systems that detect activity that can compromise the confidentiality, integrity, and availability of information resources, processing, or systems.
- To detect intrusions, various technologies have been developed.
- The first technology that was developed, intrusion detection system (IDS), had sensing capabilities but little capability to take action upon what it detected.
- An intrusion prevention system (IPS) builds upon previous IDS technology.
- An IPS has the ability to analyze traffic from the data link layer to the application layer.

IPS Overview (cont.)

- The figure shows a common IPS deployment, in which the firewall controls access between the corporate network and the Internet, based on source and destination IP addresses and ports, while the IPS controls access based on packet payload.



IPS Overview (cont.)

- An IPS also has other valuable capabilities, such as providing deeper insight into what is actually happening on your network.
- IPS technology is deployed in a sensor, which is variously described as one of the following:
  - An appliance that is specifically designed to provide dedicated IPS services. Cisco provides Cisco Firepower device, which offers many different capabilities, IPS being just one of them.
  - A module that is installed in another network device, such as an adaptive security appliance, a switch, or a router. Cisco provides Firepower services module that can be installed in Cisco ASA.

IPS Overview (cont.)

- IPS can identify, stop, and block attacks that would normally pass through a traditional firewall device.
- When traffic comes in through an interface on an IPS, if that traffic matches an IPS signature/rule, then that traffic can be dropped by the IPS.
- The essential difference between an IDS and an IPS is that an IPS can respond immediately, and prevent possible malicious traffic from passing.
- An IDS simply produces alerts when suspicious traffic is seen.
- An IDS is not responsible for mitigating the threat.

IPS Overview (cont.)

- Intrusion detection technology uses different strategies to detect and mitigate against attacks:

  - **Anomaly detection:** This type of technology generally learns patterns of normal network activity and, over time, produces a baseline profile for a given network.
  - **Rule-based detection:** Malicious activity detectors typically analyze live network traffic using a database of IPS rules (or also called IPS signatures) to determine whether suspicious activity is occurring.
  - **Reputation-based:** IPS security appliances can also make informed decisions on whether to permit or block the traffic based on reputations. Reputation-based filtering allows the IPS to block all traffic from known bad sources before any significant inspection is done.

IPS Overview (cont.)

- Cisco Firepower family of products use Snort, which is a free and open source network intrusion prevention system.
- An intrusion rule, also known as a Snort rule, is a specified set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities in your network.
- Custom rules can also be created, and added to the rule sets that ship with product.
- As the system analyzes network traffic, it compares packets against the conditions specified in each rule, and triggers the rule if the data packet meets all the conditions specified in the rule.

Next Generation Firewall Overview

- Today's threat-focused NGFW typically include additional features such as application visibility and control, advanced malware protection, URL filtering, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) decryption, and next-generation intrusion prevention systems.
- An example of a threat-focused NGFW is the **Cisco Firepower appliance**.

Next Generation Firewall Overview (cont.)

- **Some of the typical next generation requirements of a next-generation firewall.**

  - **Granular application visibility and control:** Example, allowing instant messaging (IM) but blocking file transfers over IM
  - **Intrusion prevention system**: Example, identify and potentially block malicious data that is carried in network sessions.
  - **Reputation-based filtering:** Example, automatic blocking to suspected bad web sites
  - **Enforce acceptable user policy:** Example, blocking employees from browsing to unacceptable web sites

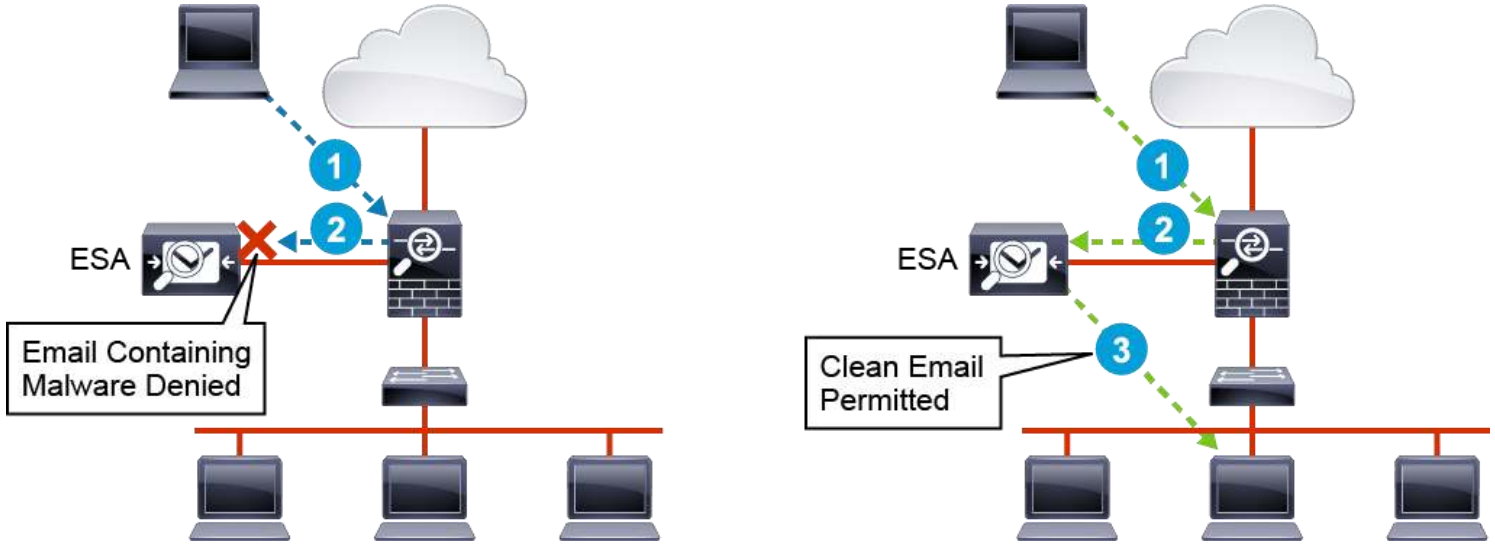
Next Generation Firewall Overview (cont.)

- **Some of the typical next generation requirements of a next-generation firewall (cont.)**

  - **SSL/TLS traffic decryption:** Example, decrypting Facebook traffic so it can be inspected and controlled
  - **User- or user group-based policies:** Example, allowing only the engineering employees to access the development servers
  - **Real-time contextual awareness:** Example, automatic passive network, hosts, operating systems, applications, and users discoveries
  - **Intelligent security automation:** Example, automatic correlation of different events data and impact assessment

Email Content Security Overview

- Due to the growing number of email-related threats, and the need to prevent sensitive information from leaking out of the company via email, email security is now a business imperative.
- Cisco Email Security Appliance (ESA) is an Email content security system provide fine-grained email security controls.



Email Content Security Overview (cont.)

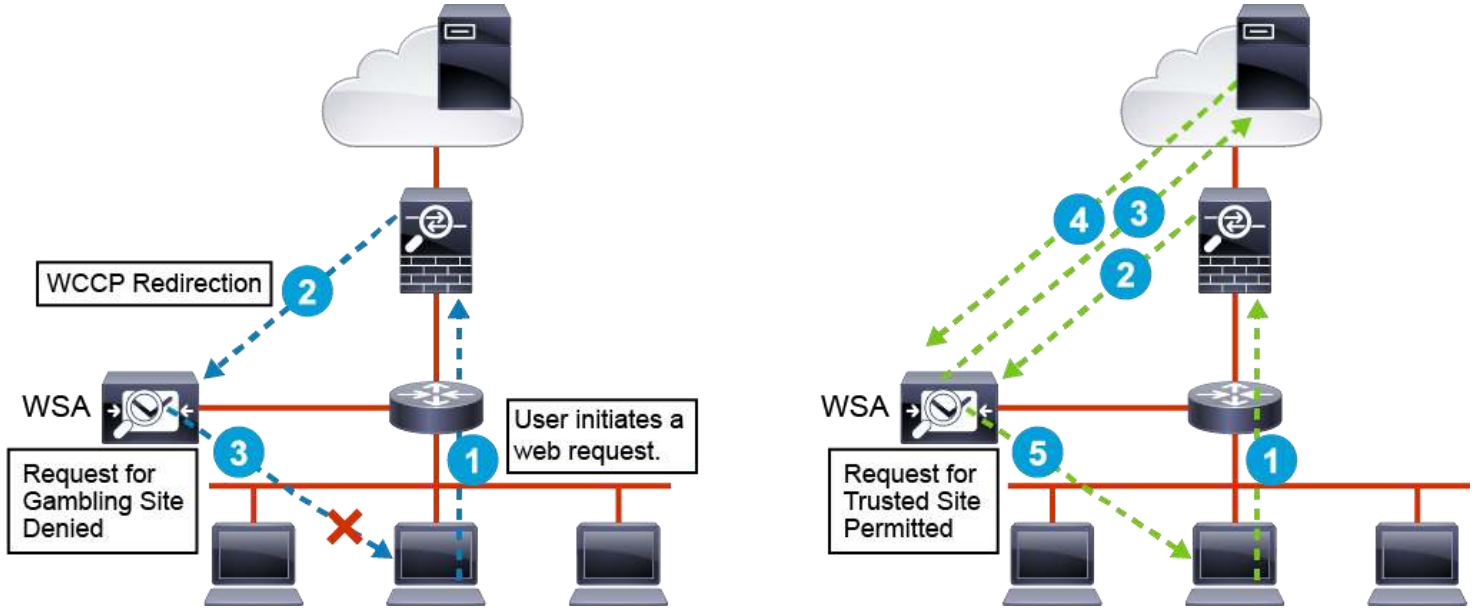
- **These security devices are a type of firewall and threat monitoring appliance for SMTP traffic that offer the following features:**
  - Block new email-based blended attacks
  - Control or encrypt sensitive outbound email
  - Provide email authentication
  - Provide a rapid spam capture rate with few false positives
  - Use reputation-based filtering to stop a large percent of spam before it enters the network
  - Perform traditional antivirus checks

Email Content Security Overview (cont.)

- Cisco ESA can be either physical or virtual appliance.
- However, Cisco also offers Cloud Email Security (CES), which provides comprehensive cloud-based security and controls for the unique challenges of corporate email, including email content, email attachments, and embedded URL's.
- Cisco CES can recognize and protect against inbound and outbound email threats. With data loss prevention (DLP) extensions, Cisco CES can protect against sensitive data leaving the organization. Cisco CES also supports simple to use email encryption to protect the outgoing emails.

Web Content Security Overview

- Web content security systems act as a web proxy for the HTTP and the HTTPS traffic, and work with other network components such as firewalls, routers, or switches, to monitor and control web content requests from within the organization and defend the web infrastructure from various types of attacks.



Web Content Security Overview (cont.)

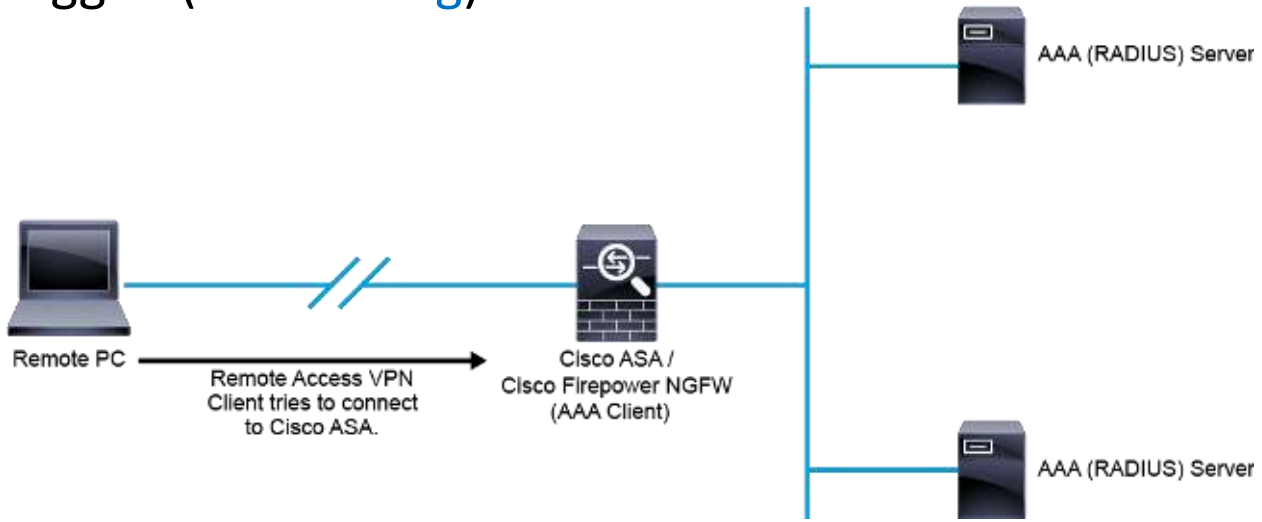
- **In addition to helping to secure and control web traffic, web content security systems can also provide the following forms of protection:**
  - Advanced malware protection
  - Web reputation filters
  - Application visibility and control
  - SSL/TLS decryption
  - Insightful reporting
  - Secure mobility

Authentication, Authorization, and Accounting Overview

- **AAA is an architectural framework for consistently configuring a set of three independent modular security functions:**
  - Authentication → Provides the method of identifying users, including login and password dialog. Authentication identifies a user before allowing the user access to the network
  - Authorization → Defines what an individual or groups of identities are allowed to do once authenticated
  - Accounting → Keeps track of what individual identities have done.

Authentication, Authorization, and Accounting Overview (cont.)

- **For example,** When remote user connecting from outside, the user is challenged for credentials to log on to the VPN (Authentication)
- Depending on the user's department, the user may be allowed or denied access to certain resources via the VPN (Authorization)
- Details of the session, such as dates and times, remote IP address, and systems that are accessed may be logged (Accounting)



Authentication, Authorization, and Accounting Overview (cont.)

- AAA data must be stored somewhere, The simplest implementation is to use the **local database** on individual network devices.
- While simple, using the local AAA database does not scale well.
- Username and password definitions as well as authorization specifications must be configured and maintained on all network devices.
- Imagine password management where passwords must be updated independently on hundreds or thousands of devices.
- Another shortcoming of local AAA is that it does not support accounting, AAA accounting data can build up very quickly and network devices simply do not have enough persistent storage to support local AAA accounting.

Authentication, Authorization, and Accounting Overview (cont.)

- In all but the smallest deployments, **Centralized AAA** is preferred over local AAA.
- With centralized AAA, configuration and maintenance of AAA policy is more manageable.
- User identities are defined and managed centrally and made available to all devices in the network.
- Similarly, authorization policy can be defined centrally and made available to all devices in the network.
- If an authorization policy is changed in the centralized system, the change is inherited by all devices.
- Centralized AAA also facilitates accounting. The accounting records from all devices are sent to centralized repositories.

Authentication, Authorization, and Accounting Overview (cont.)

AAA Protocols

- AAA protocols are protocols that allow individual network devices to communicate with the centralized AAA resources.
- Generally, an individual network device is considered an AAA client and the systems that they communicate with are considered AAA servers.
- There are two AAA protocols that are commonly implemented in today's IP-based networks.
- They are RADIUS and TACACS+

Authentication, Authorization, and Accounting Overview (cont.)

AAA Servers

- AAA servers facilitate centralized resources for authentication databases, authorization policy configurations, and accounting records.
- Cisco offers Cisco Identity Services Engine (ISE) as AAA server for the enterprise market.
- Cisco ISE can consult several user repositories for user authentication, including Active Directory, LDAP, RADIUS and Rivest, Shamir, and Adleman (RSA) token servers.

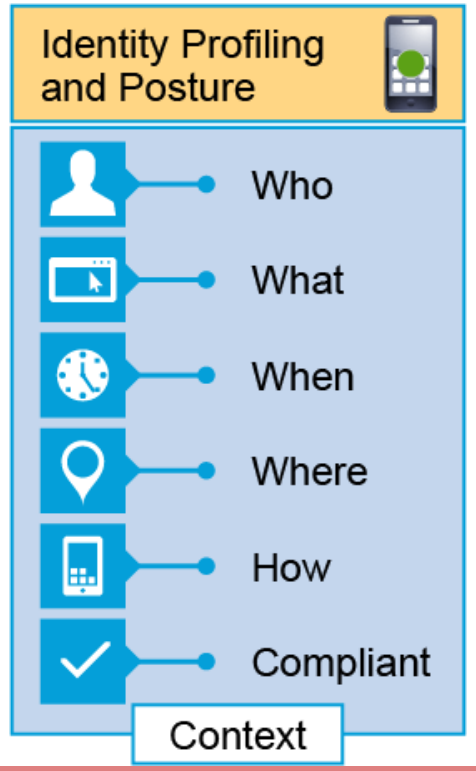
Authentication, Authorization, and Accounting Overview (cont.)

AAA Servers (cont.)

- Cisco ISE is a robust AAA server offering both TACACS+ and RADIUS services in one system.
- With ISE, an organization can centralize both user network access policies and network device administrative access policies in one server.
- Cisco ISE supports also features such as profiling, posture assessment, and centralized web authentication.

Identity and Access Management Overview

- The IAM solution allows security analysts to see and control users and devices connecting to the corporate network from a central location.



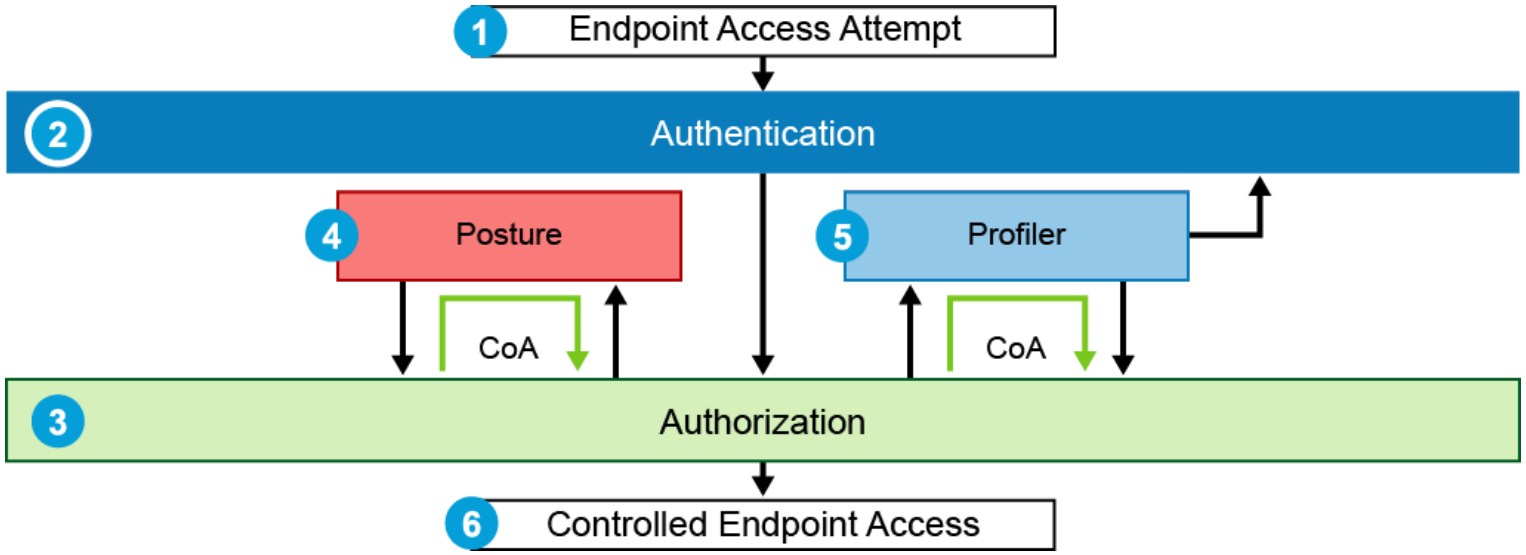
Identity and Access Management Overview (cont.)

Some of the main attributes available for use by IAM platforms for user- and device-related context include:

- **User:** User name, IP address, authentication status, location
- **User class:** Authorization group, guest, quarantined
- **Device:** Manufacturer, model, operating system, OS version, MAC address, IP address, network connection method (wired or wireless), location
- **Posture:** Posture refers to the compliance status of the endpoint device including antivirus is installed, antivirus at correct version, operating system patch level, and other device posture compliance status data.

Identity and Access Management Overview (cont.)

- The following diagram depicts the general flow of IAM policy decisions when an endpoint attempts to access the network.

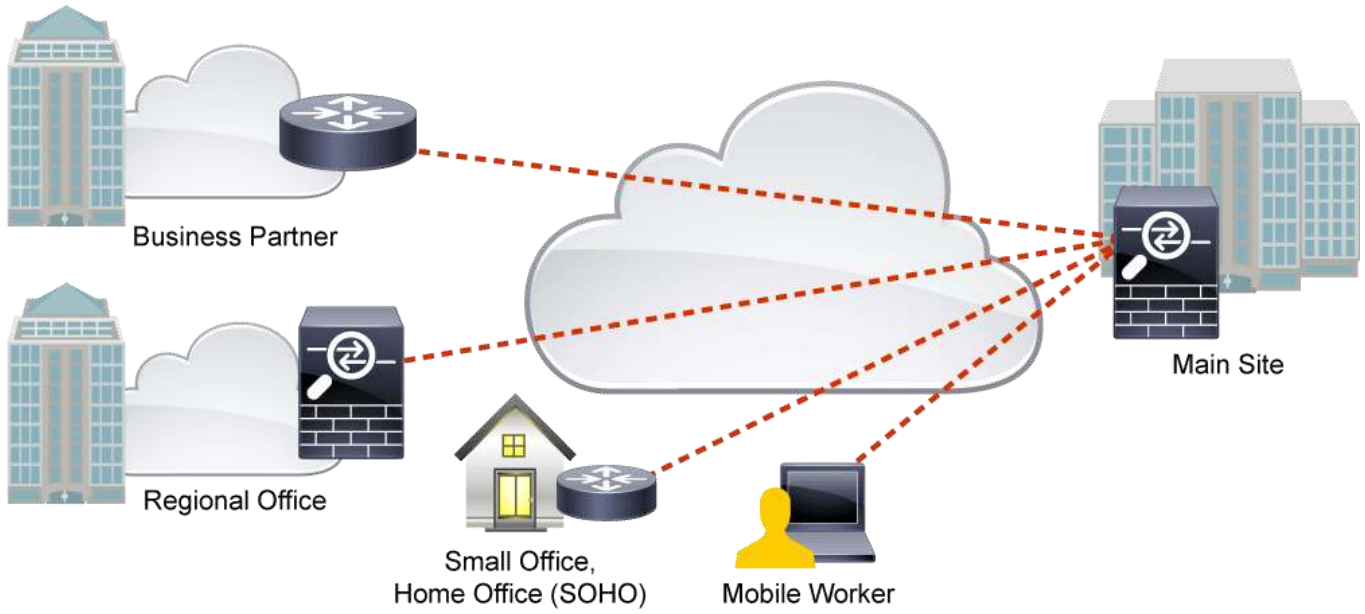


Identity and Access Management Overview (cont.)

- An example of an IAM solution is the Cisco ISE, which maintains contextual information about connection sessions – who, what, how, where, and when.
- Beyond Cisco ISE, many other Cisco and third-party platforms could benefit from this information. Also, Cisco ISE (and other platforms) might be able to benefit from other information gleaned from other platforms.
- Cisco Platform Exchange Grid (pxGrid) provides a secure communication framework to share context information with Cisco ISE Ecosystem partners and other Cisco platforms.

Virtual Private Network Technology Overview

- A VPN is a technology that secures communication across an untrusted network.



Virtual Private Network Technology Overview (cont.)

- A VPN is typically utilized to carry private traffic over a public or shared infrastructure, such as the Internet.
- The most common and effective VPN technology is applied at the network layer of the Open Systems Interconnection (OSI) model to encrypt traffic flow among specific users, applications, or IP subnet pairs.
- VPN at the network layer is transparent to the applications at higher OSI layers and is also independent of network topology.