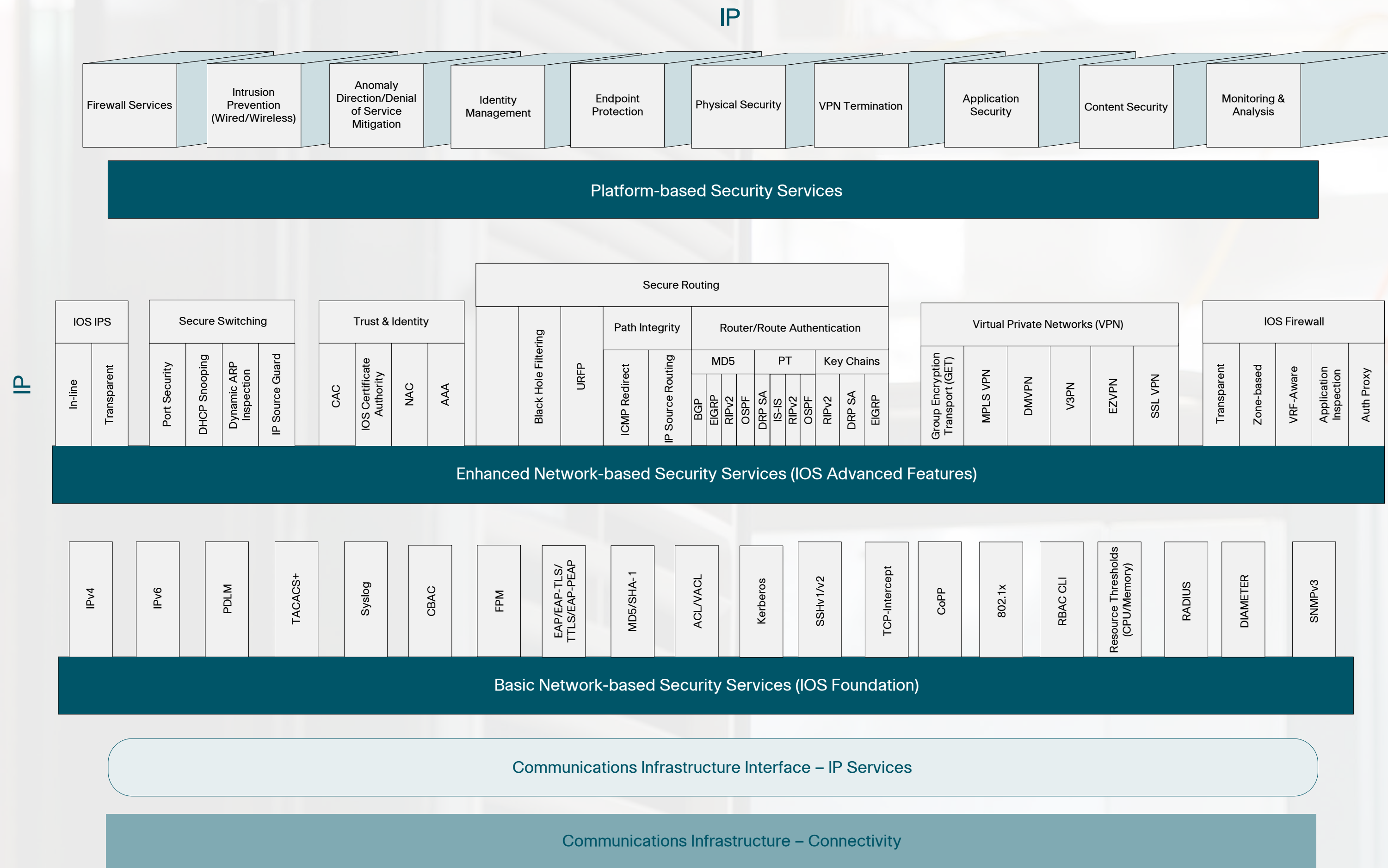


Cisco's Self-Defending Network Architecture Reference Model



IPV4 (Internet Protocol Version 4): The fourth iteration of the Internet Protocol (IP). It is the first version of the protocol to be widely deployed. IPv4 is the dominant network layer protocol on the Internet, and apart from IPv6, it is the only standard internetwork-layer protocol used on the Internet.

IPV6 (Internet Protocol Version 6): A network layer protocol for packet-switched internetworks. It is designated as the successor of IPv4, the current version of the Internet Protocol, for general use on the Internet. The main improvement brought by IPv6 is a much larger address space that allows greater flexibility in assigning addresses. IPv6 is able to support 2¹²⁸ (about 3.4x10³⁸) addresses, or approximately 5x10²⁸ addresses for each of the roughly 6.5 billion people alive today. It was not the intention of IPv6 designers, however, to give permanent unique addresses to every individual and every computer. Rather, the extended address length eliminates the need to use network address translation to avoid address exhaustion, and also simplifies aspects of address assignment and renumbering when changing providers.

PDLM (Packet Description Language Modules): Allows introduction of new application support for Network Based Application Recognition (NBAR). PDLMs contain the rules used by NBAR to recognize an application and can usually be loaded without the need for a Cisco IOS Software upgrade or router reboot. NBAR, an important component of the Cisco Content Networking architecture, is a new classification engine in Cisco IOS* Software that can recognize a wide variety of applications (including Web-based applications and client/server) that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR currently works with quality-of-service (QoS) features to help ensure that the network bandwidth is best used to fulfill business objectives.

TACACS+ (Terminal Access Controller Access-Control System Plus): A protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

SYSLOG: A standard of forwarding log messages in an IP network. SYSLOG is typically used for computer system management and security auditing. While it has a number of shortcomings, SYSLOG is supported by a wide variety of devices and receivers across multiple platforms. Because of this, SYSLOG can be used to integrate log data from many different types of systems into a central repository.

CBAC (Context-based Access Control): Intelligently filters TCP and UDP packets based on application-layer protocol session information and can be used for intranets, extranets and internets. CBAC can be configured to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network needing protection. (In other words, CBAC

can inspect traffic for sessions that originate from the external network.) However, while this example discusses inspecting traffic for sessions that originate from the external network, CBAC can inspect traffic for sessions that originate from either side of the firewall. Without CBAC, traffic filtering is limited to access list implementations that examine packets at the network layer, or at most, the transport layer. However, CBAC examines not only network layer and transport layer information but also examines the application-layer protocol information (such as FTP connection information) to learn about the state of the TCP or UDP session. This allows support of protocols that involve multiple channels created as a result of negotiations in the control channel. Most of the multimedia protocols as well as some other protocols (such as FTP, RPC, and SQL "Net) involve multiple channels. CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions (sessions that originated from within the protected internal network).

FPM (Flexible Packet Matching): Cisco FPM uses flexible and granular Layer 2-7 pattern matching deep within the packet header or payload to provide a rapid first line of defense against network threats and notable worms and viruses. Cisco FPM complements the Cisco IOS Intrusion Prevention System by supporting custom filters that can be defined and deployed more rapidly, before IPS signatures or antivirus patterns are updated. It gives network security administrators powerful tools with which to identify misrouted traffic and immediately drop or log it for audit purposes.

EAP (Extensible Authentication Protocol): A universal authentication framework frequently used in wireless networks and Point-to-Point connections. It is defined by RFC 3748. EAP is an authentication framework, not a specific authentication mechanism. The EAP provides some common functions and a negotiation of the desired authentication mechanism. **EAP-TLS (EAP Transport Layer Security):** EAP-TLS is the original standard wireless LAN EAP authentication protocol. EAP-TLS is considered one of the most secure EAP standards available and is universally supported by all manufacturers of wireless LAN hardware and software, including Microsoft. The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security trade-off. A compromised password is not enough to break into EAP-TLS enabled systems because the hacker still needs the client-side certificate. When the client-side certificates are housed in smartcards, this offers the most security available because there is no way to steal a certificate's private key from a smartcard without stealing the smartcard itself. **EAP-TTLS (EAP-Tunneled Transport Layer Security):** Extends TSL protocol and is widely supported across platforms, and offers very good security. The client does not need to be authenticated via a CA-signed PKI certificate to the server, but only the server to the client. This greatly simplifies the setup procedure as a certificate does not need to be installed on

every client. After the server is securely authenticated to the client via its CA certificate, the server can then use the established secure connection ("tunnel") to authenticate the client. It can use an existing and widely deployed authentication protocol and infrastructure, incorporating legacy password mechanisms and authentication databases, while the secure tunnel provides protection from eavesdropping and man-in-the-middle attack. **EAP-PEAP:** A joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication.

IOS IPS (Intrusion Prevention System): Inline, deep-packet inspection-based feature that helps enable Cisco IOS Software to effectively mitigate a wide range of network attacks. As a core facet of the Self-Defending Network, Cisco IOS IPS helps enable the network to defend itself with the intelligence to accurately classify, identify, and stop or block malicious or damaging traffic in real time. While it is common practice to defend against attacks by inspecting traffic at the data centers and campus locations, distributing the defense to stop malicious traffic close to its entry point at the edge or remote premises is also critical.

Secure Routing: Capabilities that ensure continuous service delivery by protecting the router's data, control and management planes. **Route Filtering:** Protects networks from excessive conditions and limits route prefixes for enhanced stability. **Black Hole Filtering:** A technique that uses routing protocol updates to manipulate routing tables to drop undesirable traffic before it enters a protected network. **URPF (Unicast Reverse Path Forwarding):** Helps limit the malicious traffic on an enterprise network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode. **Router/Route Authentication:** A mechanism used to authenticate neighbors and provide a secure routing domain.

Firewall Services: Cisco's multiple integrated firewall solutions. Based on modular, scalable platforms, each firewall is designed to secure varying network environments. These firewalls can be independently deployed to secure specific areas of the network infrastructure, or they can be combined for a layered, defense in depth approach.

Intrusion Prevention: The first integrated wired and wireless security solution in the industry. The Cisco Unified IDS/IPS takes a comprehensive approach to security - wireless and wired, edge and data center.

VPN Termination: Provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. The solution engine helps to ensure enforcement of assigned policies.

Endpoint Protection: Cisco Security Agent (CSA) provides robust and granular host protection profiles to provide an end to end defense in-depth approach. CSA also can correlate threats with Cisco's IPS products to quickly determine the risk that a network-borne exploit may pose to a certain host running CSA.

Anomaly Detection and DDoS Mitigation: Cisco's Anomaly Detection and Mitigation products are deployed off the critical path at strategic locations throughout an enterprise environment. These products preserve network availability and business continuity, detect the broadest range of DDoS attacks, differentiate between legitimate traffic and attack traffic in real time, block large botnet and zombie attacks, deliver multigigabit performance at line rate for detection and mitigation; and allow legitimate, mission-critical transactions to flow through.

Secure Switching/Port Security: You can use the port security feature to limit and identify MAC addresses for the stations allowed to access the port. This restricts input to an interface. **DHCP Snooping:** DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch. **Dynamic ARP Inspection:** Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. **IP Source Guard:** IP source guard is a security feature that filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings in order to restrict IP traffic on non-routed Layer 2 interfaces. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP address of its neighbor. IP source guard prevents IP/MAC spoofing.

Virtual Private Networks (VPN): A communications network that is logically separated from other networks. This logical network may or may not use encryption as an additional layer of separation. **GET (Group Encryption Transport):** A WAN security technology that defines a new category of VPN, one that does not use tunnels. Group Encrypted Transport VPN eliminates the need to compromise between network intelligence and data privacy. This model introduces the concept of "trusted" group member routers using a common security methodology that is independent of any point-to-point relationship. By eliminating point-to-point tunnels, Cisco Group Encrypted Transport VPNs can scale higher while accommodating multicast applications and instantaneous branch-to-branch transactions. **MPLS VPN (Multiprotocol Label Switching VPN):** Cisco IOS Multiprotocol Label Switching (MPLS) enables next-generation intelligent networks to deliver a wide variety of services over a single infrastructure. This economical solution can be integrated seamlessly over any existing infrastructure, such as IP, Frame Relay, ATM, or Ethernet. MPLS Layer 3 VPNs enable value-added services like QoS and Traffic Engineering, allowing network convergence that encompasses voice, video and data. **DMVPN (Dynamic Multipoint VPN):**

Enables zero-touch deployment of IPsec networks. DMVPN spoke-to-spoke functionality enables the secure exchange of data between locations without traversing the head office. This improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization. **V3PN:** Voice and video enabled VPN (V3PN) solutions integrate cost-effective, secure connectivity provided by site-to-site IPsec VPNs with the AVVID architecture for delivering converged voice, video, and data IP networks. Integrating these two network solutions delivers cost-effective, flexible wide-area connectivity, while providing a network infrastructure that enables the latest converged network applications (such as IP Telephony and Video). **EZVPN (Easy VPN):** Simplifies virtual private network (VPN) deployment for remote offices and users. Based on the Cisco Unified Client Framework, the Cisco Easy VPN solution centralizes VPN management across all Cisco VPN devices, thus reducing the management complexity of VPN deployments. Cisco EZ VPN helps enable an integration of VPN remote devices—such as Cisco routers, Cisco PIX Security Appliances, the Cisco VPN 3002 Hardware Client, or the Cisco VPN Client—within a single deployment and with a consistent policy and key management method, simplifying remote site administration.

Trust & Identity: CAC (Common Access Card): Support for DoD Common Access Card. **IOS Certificate Authority:** Public Key Infrastructure (PKI) offers a scalable method of securing networks, reducing management overhead, and simplifying the deployment of network infrastructures by deploying Cisco IOS Security protocols, including Cisco IOS IPsec, Secure Shell (SSH), and Secure Socket Layer (SSL). Cisco IOS Software can also use PKI for authorization via access lists and authentication resources. **NAC (Network Admission Control):** Allows only compliant and trusted endpoint devices, such as PCs, servers, and PDAs onto the network, restricting the access of noncompliant devices, and thereby limiting the potential damage from emerging security threats and risks. Cisco NAC gives organizations a powerful, roles-based method of preventing unauthorized access and improving network resiliency. **AAA (Authentication, Authorization, Accounting):** A term for a framework that intelligently controls access to computer resources, enforces policies, audits usage and provides the information necessary to bill for services. These combined processes are considered important for effective network management and security.

IOS Firewall: Cisco IOS Firewall offers a threat defense foundation to deploy secure access policies at all network interfaces: perimeter, remote-site connectivity, extranet access, and edge connections. Application inspection and control builds on the existing stateful inspection infrastructure to offer comprehensive protection for industry-standard services, as well as a framework to configure custom protocol support to meet business requirements. Improvements to Cisco IOS Software's Zone-Based Policy Firewall provide innovative control capabilities for Instant Messaging and Peer-to-Peer applications, granular application-level control for HTTP traffic, and firewall policy bandwidth-Firewall Services.

Identity Management: Cisco Secure Access Control Server (ACS) is an important component of the Cisco Network Admission Control (NAC) that provides a centralized identity networking solution across all Cisco devices and security management applications. It acts as a policy decision point in NAC deployments. It extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework, thereby allowing greater flexibility and mobility, increased security, and user productivity gains.

Application Security: Protecting the application while in transit can be accomplished in several different manners. Cisco offers application security for standard internet protocols (HTTP, SMTP, FTP, etc) as well as for XML, SQL and other common enterprise applications.

Physical Security: Leveraging the network as a convergence platform, Cisco can combine legacy physical security devices and newer IP enabled security devices to create a centralized common operating picture for an entire enterprise.

Content Security: Protection of critical data and application transactions can be provided by different content security technologies within Cisco's Self-Defending Network architecture.

Monitoring & Analysis: Whether it's a single device or an enterprise, monitoring and correlation of events is a critical component of the security lifecycle. Cisco provides various device managers and enterprise monitoring and analysis systems.

MD5/SHA-1 (Message Digest 5/ Secure Hash Algorithm): MD5: A cryptographic hash function with a 128-bit hash value. An MD5 hash is typically expressed as a 32-character hexadecimal number. MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function, MD4. **SHA-1:** five Secure Hash Algorithm (SHA) cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length. They are called "secure" when (in the words of the standard), "it is computationally infeasible to, find a message that corresponds to a given message digest, or find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest." SHA-1 is employed in several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It was considered to be the successor to MD5, an earlier, widely-used hash function.

ACL / VAACL (Access Control List / VLAN Access Control Lists): **ACL:** Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. The router examines each packet to determine whether to forward or drop the packet based on the criteria specified within the access lists. **VAACL:** Used for security packet filtering and redirecting traffic to specific physical switch ports. VAACLs are not defined by the direction of the traffic and enable a fine degree of granularity when specifying which traffic to capture.

Kerberos: A computer network authentication protocol which allows individuals communicating over an insecure network to prove their identity to one another in a secure manner. Its designers targeted primarily client-server model, it provides mutual authentication (both the user and the server verify each other's identity), Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party.

Extensions to Kerberos can provide for the use of public key cryptography during certain phases of the authentication protocol.

SSHv1 / v2 (Secure Shell version 1/ version 2): A network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary. SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding arbitrary TCP ports and X11 connections. It can transfer files using the associated SFTP or SCP protocols.

TCP Intercept: The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack. The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. The software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.

CoPP (Control Plane Policing): The Control Plane Policing feature allows users to configure a quality of service (CoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

RBAC CLI (Role Based Access Control Command Line Interface): Provides role-based access control (RBAC) for securing the management interface on the Cisco IOS routers and switches. With RBAC, authentication, authorization and accounting

features limit access to operations by assigning roles to users. Specific user/group roles may be defined in Cisco's Access Control Server (ACS). These roles are explicitly assigned commands that are either permitted or denied based on the authorization of a particular use or group.

Resource Thresholds (CPU/Memory): CPU and memory are critical resources that mitigate the potential availability impact of the networking device. SNMP MIBs currently enable a monitoring application to inquire as to the availability of a given resource. Due to the dynamic nature of these resources, scheduled polling of these variables often delays the action necessary to maximize network availability. Memory Thresholding Notification enables users to manage the amount of memory consumed by various resource groups. Users can specify the maximum amount of memory in bytes, or as a percentage of total processor resources. They receive notification when a resource group approaches its specified memory threshold.

RADIUS (Remote Access Dial-in User Service): An AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

DIAMETER: The Diameter Base Protocol is defined by RFC 3588, and defines the minimum requirements for an AAA protocol. Diameter applications can extend the base protocol by adding new commands and/or attributes. An application is not a program, but a protocol based on diameter. Diameter security is provided by IPSEC or TLS, both well-regarded protocols.

SNMPv3 (Simple Network Management Protocol version 3): SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMPv3 primarily adds security and remote configuration enhancements to SNMP. SNMPv3 provides important security features including message integrity to ensure that a packet has not been tampered with in transit, authentication to verify that the message is from a valid source, and encryption of packets to prevent snooping by an unauthorized source.

Cisco's Self-Defending Network Architecture Reference Model

