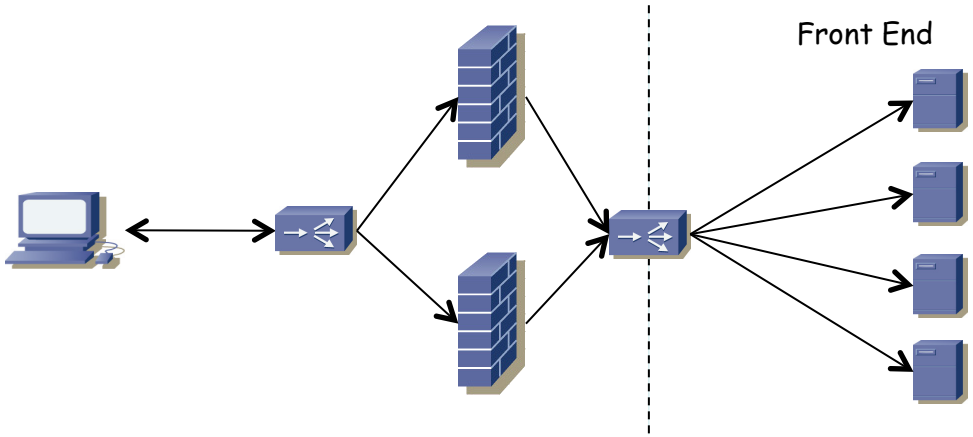
# Otros servicios

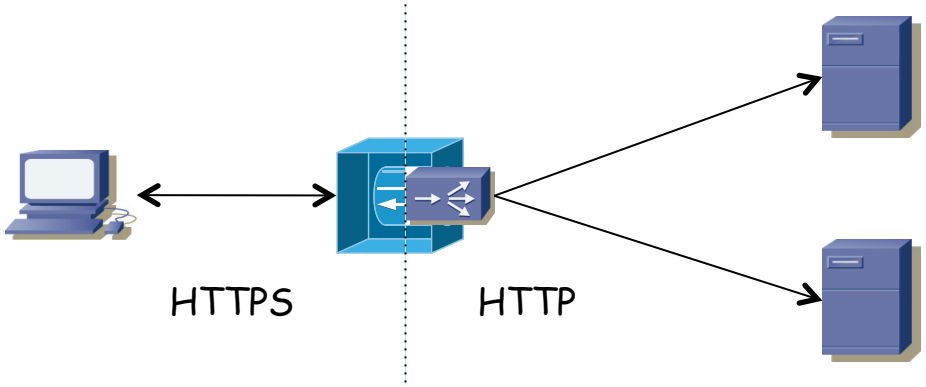
# Firewalls e IDS

- Seguridad, seguridad, seguridad
- Reglas de filtrado para permitir el acceso solo a las direcciones IP y puertos de los servicios
- Inspección de contenido
- Pueden estar antes o después del balanceador
- Si no vale con uno se pueden poner varios balanceados (aumenta la complejidad)
- Ese balanceador podría ser el mismo que hacia los servidores (varias direcciones IP virtuales o instancias virtuales)



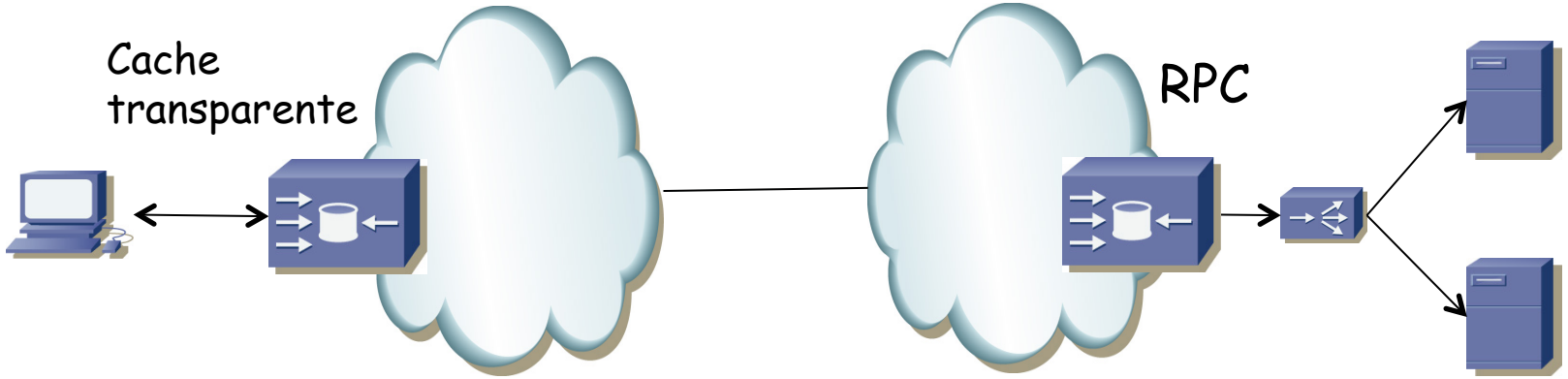
# SSL offloading

- Portales web seguros
- También otros servicios sobre un túnel SSL
- SSL tiene un coste computacional considerable
- Este equipo termina la sesión SSL con el usuario e inicia una conexión sin SSL con el servidor
- El equipo puede disponer de hardware especializado para SSL
- También podríamos poner varios y balancearlos
- Es común que el balanceador integre esta funcionalidad



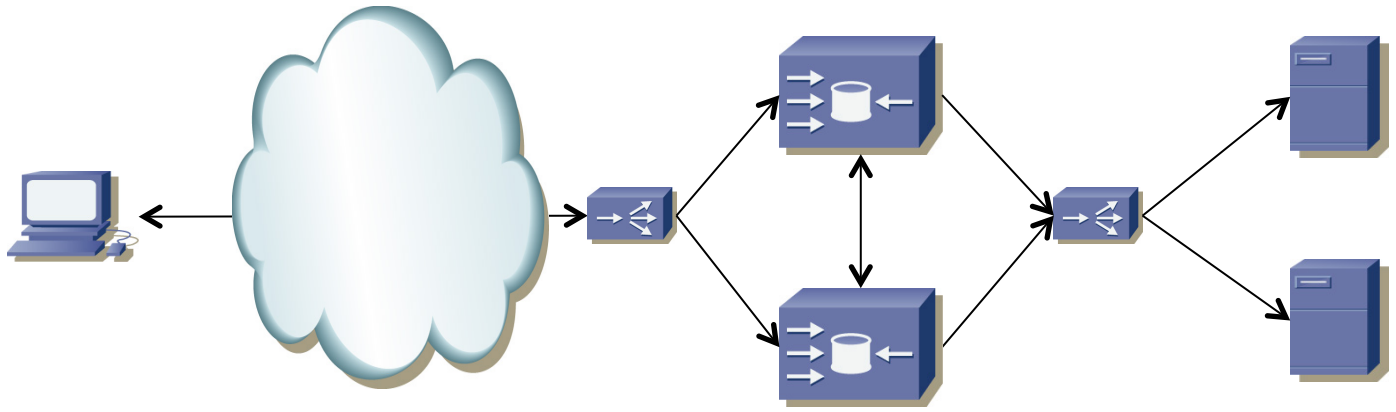
# Cache

- Puede ser cercana a los servidores, a los clientes o a ambos
- Cercanas al servidor
  - Se habla de "*reverse proxy cache*" (RPC)
  - Reduce carga sobre los servidores
- Cercanas al cliente
  - Se habla de "*transparent caching*"
  - Reducen carga sobre el enlace a Internet
  - Reducen tiempos de respuesta por cercanía (menor RTT)



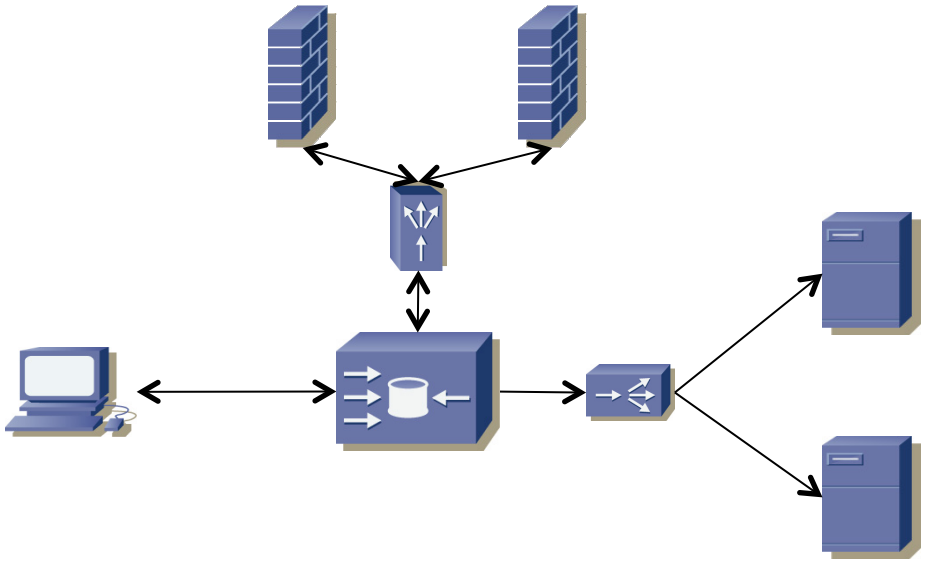
# Cache

- La cache podría implementarse con varias caches balanceadas
  - Aumenta la capacidad (CPU) de la cache
  - Busca maximizar el *cache hit ratio* y así reducir peticiones a servidores
  - Para ello el balanceador debería reenviar la petición a la cache con mayor probabilidad de contenerlo (en función del FQDN)
  - O las caches deben sincronizarse (*clustering*), pues si no acabarán haciendo peticiones repetidas



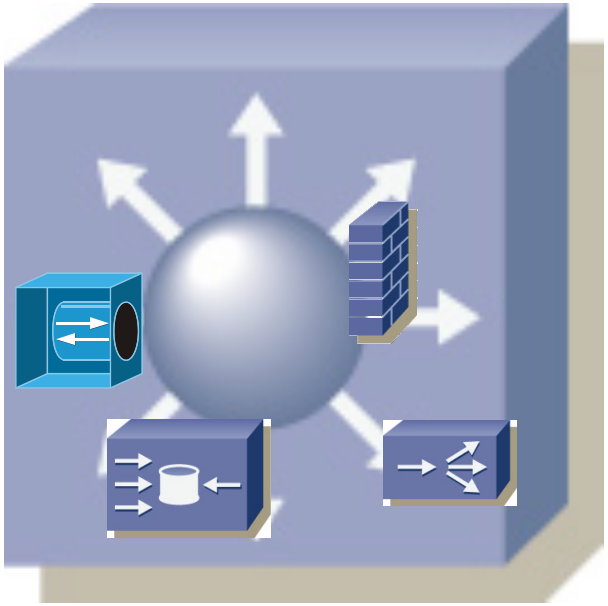
# Cache

- Puede redirigir parte de la petición a un antivirus o filtro de contenido
- Se encargaría de verificar que se puede hacer esa petición o que el documento obtenido no es peligroso
- Protocolos específicos para pasar la petición o respuesta: ICAP = *Internet Content Adaptation Protocol* (RFC 3507)
- O a varios con balanceo de carga
- El balanceador puede ser el mismo equipo



# Servicios y redundancia

- Todos estos servicios se pueden dar desde equipos independientes
- Si no queremos un punto único de fallo debemos tenerlos replicados
- Según el tipo de servicio deberán coordinarse entre ellos para mantener el estado ante un fallo
- Por ejemplo un NAT para conocer las sesiones de mapeo que estaban establecidas
- También pueden ser módulos en un conmutador



# Ejemplo: Cisco Catayst 6500-E

# Chasis

| | Catalyst 6503-E | Catalyst 6504-E | Catalyst 6506-E | Catalyst 6509-E | Catalyst 6513-E | Catalyst 6509-V-E |
|---|---|---|---|---|---|---|
| **Slots** | 3 | 4 | 6 | 9 | 13 | 9 vertical |
| **Max 10/100/1000 ports** | 97 | 145 | 241 | 385 | 529 | 385 |
| **Max 1 GE ports[1]** | 99 | 147 | 243 | 387 | 534 | 387 |
| **Max 10 GE ports[2]** | 34 | 50 | 82 | 130 | 180 | 130 |
| **Max 40 GE ports** | 8 | 12 | 20 | 32 | 44 | 32 |
| **Maximum forwarding performance (IPv4)** | 150 Mpps | 210 Mpps | 330 Mpps | 510 Mpps | 720 Mpps | 510 Mpps |
| **Height (RU)** | 4 | 5 | 11 | 14 | 19 | 21 |
| **Weight (chassis)** | 33 lbs (15 kg) | 40 lbs (17.8 kg) | 50 lbs (22.7 kg) | 60 lbs (27.3 kg) | 79.1 lbs (35.9 kg) | 121 lbs (54.9 kg ) |

[1] Assumes use of supervisor uplinks in single supervisor configuration

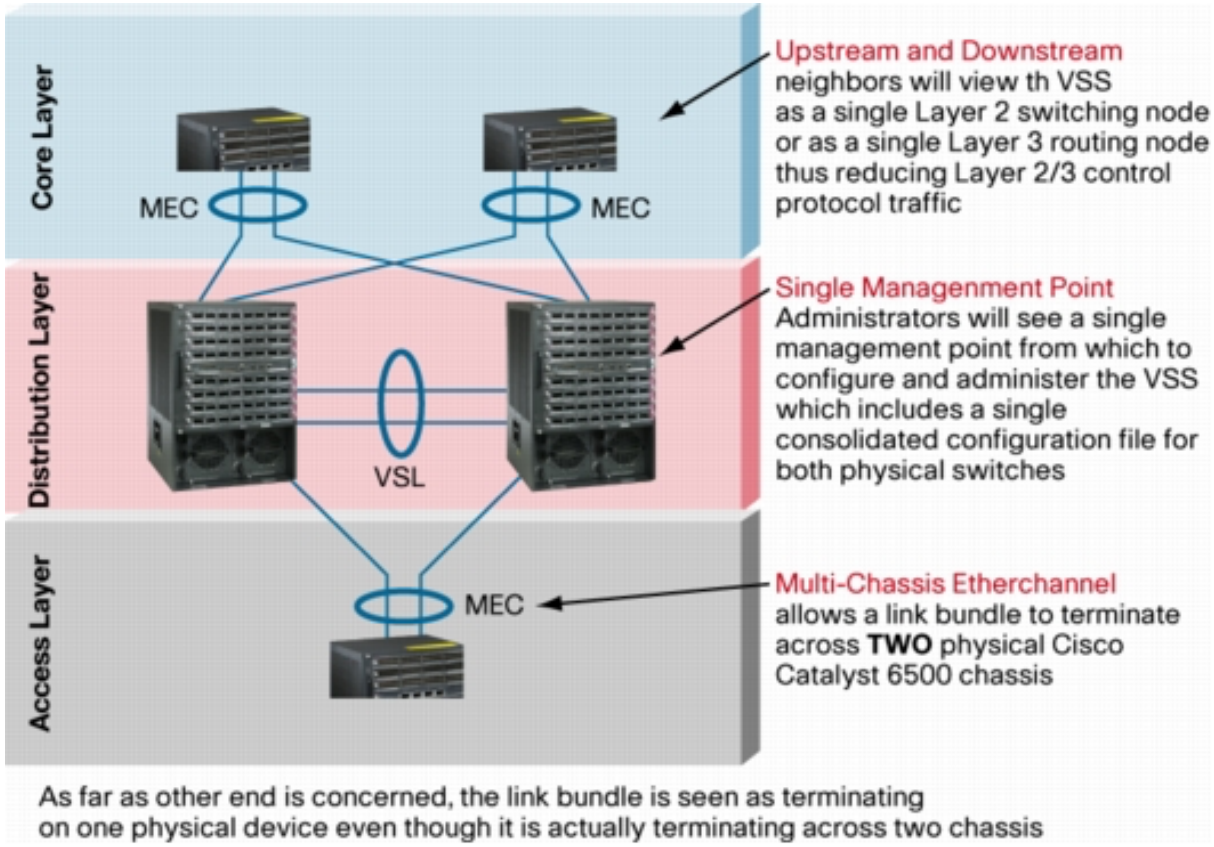
[2] Assumes use of supervisor uplinks in single supervisor configuration

# Supervisoras

**Catalyst Supervisor Engines**

| | 2T | 2T-XL | 720-10G | 720-10G-XL | 720-3B | 720-3BXL |
|---|---|---|---|---|---|---|
| **Switch fabric** | Integrated 2T | Integrated 2T | Integrated 720G | Integrated 720G | Integrated 720G | Integrated 720G |
| **Virtual Switching System (VSS)** | Yes | Yes | Yes | Yes | No | No |
| **Uplinks** | 3 x 1 GE (SFP)<br>2 x 10 GE (X2)<br>1 management (CMP) | | 2 x 1 GE (SFP)<br>2 x 10 GE (X2)<br>1 x 10/100/1000 RJ-45 | | 1 x 1 GE (SFP)<br>1 x 1 GE (SFP) or 10/100/1000 RJ-45 | |
| **Chassis** | E-Series only | E-Series only | 6503/6503-E<br>6504-E<br>6506/6506-E<br>6509/6509-E<br>6509-NEB-A<br>6509-V-E<br>6513/6513-E | 6503/6503-E<br>6504-E<br>6506/6506-E<br>6509/6509-E<br>6509-NEB-A<br>6509-V-E<br>6513/6513-E | 6503/6503-E<br>6504-E<br>6506/6506-E<br>6509/6509-E<br>6509-NEB<br>6509-NEB-A<br>6513/6513-E | 6503/6503-E<br>6504-E<br>6506/6506-E<br>6509/6509-E<br>6509-NEB<br>6509-NEB-A<br>6513/6513-E |

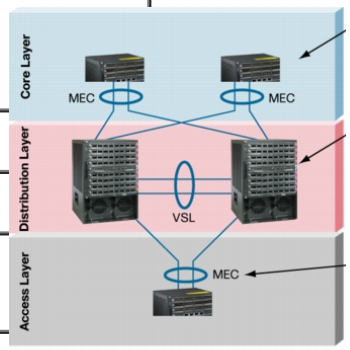
# *Virtual Switching System (VSS)*



# *Virtual Switching System (VSS)*

**Table 1.** Specifications of the Cisco Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet uplinks

| Feature | Cisco Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet uplinks (PFC 3C) | Cisco Virtual Switching Supervisor Engine 720 with 10 Gigabit Ethernet uplinks (PFC 3CXL) |
|---|---|---|
| Support for Cisco VSS 1440 | Yes | Yes |
| MAC entries | 96,000 | 96,000 |
| IP Routes | 256,000 (IPv4); 128,000 (IPv6) | 1,000,000 (IPv4); 500,000 (IPv6) |
| IPv4 Routing | • In hardware<br>• Up to 450 Mpps* | • In hardware<br>• Up to 450 Mpps* |
| IPv6 Routing | • In hardware<br>• Up to 225 Mpps* | • In hardware<br>• Up to 225 Mpps* |
| Layer 2 Bridging | • In hardware<br>• Up to 450 Mpps* | • In hardware<br>• Up to 450 Mpps* |
| NetFlow Entries | 128,000 | • 256,000 |
| MPLS | • MPLS in hardware to enable use of Layer 3 VPNs and EoMPLS tunneling.<br>• Up to 1024 virtual routing and forwarding instances (VRFs) with a total of up to 256,000 routes per system. | • MPLS in hardware to enable use of Layer 3 VPNs and EoMPLS tunneling.<br>• Up to 1024 VRFs with a total of up to 1,000,000 routes per system. |
| GRE | In hardware | In hardware |
| NAT | Hardware-assisted | Hardware-assisted |




* With Cisco Distributed Forwarding Card 3C (DFC3C)

100Mpps x 64 Bytes/paquete = 51.5 Gbps
100Mpps x 1518 Bytes/paquete = 1.21 Tbps

2014: Tabla de rutas BGP excede las 500k entradas

# Supervisor Engine 32

| Features | Benefits |
|---|---|
| Identity-based networking services with IEEE 802.1x:<br>• VLAN ID assignment<br>• Security ACL assignment<br>• QoS policy assignment<br>• Unidirectional controlled port for "wake-on-LAN" applications<br>• Authentication identity-to-port description mapping<br>• Domain Name System (DNS) resolution for RADIUS server configuration | Allows close control over which users can access the network and what privileges they are granted |
| Intrusion detection and spoofing protection mechanisms:<br>• DHCP snooping, dynamic ARP inspection, IP source guard-Cisco Catalyst 6500 Security Toolkit<br>• CPU rate limiting<br>• Control Plane Policing<br>• Port-based ACLs<br>• User-based rate limiting<br>• Hardware-based MAC learning<br>• Cisco Catalyst 6500 IDS module<br>• Broadcast and multicast suppression<br>• Port Security on Access, 802.1Q Trunks and 802.1Q Tunneling ports | Provides local containment of security threats and protects networks against security vulnerabilities, including malicious and inadvertent intrusion |
| **Hot-Swapping of Standby Supervisor Engines**<br>• Layer 2 rapid convergence protocol suite includes:<br>· IEEE 802.1s, multiple spanning trees<br>· IEEE 802.1w, rapid reconfiguration of spanning tree<br>· Per-VLAN rapid spanning tree (PVRST)<br>• Hardware redundancy with subsecond stateful failover and Layer 2 resiliency through 802.1x high availability<br>• Fault management:<br>· Fault detection and troubleshooting<br>· System health check<br>· Enhanced memory protection<br>· Proactive detection and prevention of network equipment failures using GOLD | Ensures business continuity through minimizing network downtime for mission-critical applications |
| Switched Port Analyzer (SPAN), Remote SPAN (RSPAN) | Enables remote troubleshooting from anywhere, reducing troubleshooting time and tool costs |
| Two USB 2.0 ports (hardware ready, software support post-first customer shipment [FCS]) | Enables direct access from laptops for network management, simplifies software downloading using USB memory devices, and enhances security by enabling USB keys on console port to limit access to authorized personnel |
| ACE counters | Identifies frequency that specific ACL entries are hit for ease of management |

# Supervisor Engine 32

| | |
|---|---|
| Cisco SmartPort macros, config rollback, and switch profiles | Simplifies operational complexity |
| SNMPv3, SSH Protocol Version 2, Secure Copy Protocol (SCP) | Provides secure management |
| Multicast capabilities:<br>• Hardware-based multicast<br>• Bidirectional Protocol Independent Multicast (PIM)<br>• Internet Group Management Protocol (IGMP) Querier<br>• Router-port Group Management Protocol (RGMP), Multiprotocol Border Gateway Protocol (MBGP)<br>• PIM SM, PIM SSM and PIM snooping<br>• IGMP version 3 | Enables efficient video broadcasting, e-learning, and information sharing |
| Integrated high-density uplinks-eight Gigabit Ethernet SFP-based ports or two 10-Gigabit Ethernet XENPAK-based ports | Increases uplink density and saves slots to deploy integrated service modules or higher-density chassis |
| Backward compatibility-supports all Cisco Catalyst 6500 classic and Cisco Express Forwarding 256-based modules and services modules; supported in all Cisco Catalyst 6500 Series and Cisco 7600 Series Router chassis | Allows deployment of new advanced services on existing equipment, prolonging the deployment lifetime of interface modules and providing greater return on investment |
| • Advanced QoS uses packet classification and marking and congestion avoidance based on Layer 2-4 header information<br>• User-based rate limiting enforces any of 64 policy rates, maintaining service-level agreements on a per-user basis independent of traffic type or IP address<br>• QoS scheduling rules with thresholds can be configured in the switch for multiple receive and transmit queues | Superior traffic management enables efficient handling of converged networks that carry a mix of mission-critical, time-sensitive, and bandwidth-intensive multimedia applications |
| • Hardware-enabled MPLS-Enables use of VPNs and Layer 2 tunneling while improving traffic engineering for QoS and adding multiprotocol support<br>• Hardware-enabled IPv6-Expands available IP addresses, enabling better address allocation and address aggregation and supporting greater end-to-end connectivity and services<br>• Hardware-enabled GRE tunnels for IP traffic<br>• NAT (hardware ready, software support post-FCS)-Translates addresses for inbound and outbound traffic in hardware, allowing clean separation between internal and external networks | Advanced Layer 2-4 forwarding enables service providers and enterprises to build feature-rich networks |

# Supervisor Engine 32

| Feature | Supervisor Engine 720 | Supervisor Engine 32 |
|---|---|---|
| **Uplinks** | Two Gigabit Ethernet ports-one gigabit interface converter (GBIC) based and one configurable to GBIC based or 10/100/1000 RJ-45 based | • Eight Gigabit Ethernet ports, SFP based + one 10/100/1000 RJ-45 port<br>OR<br>• Two 10 Gigabit Ethernet ports, XENPAK based + one 10/100/1000 RJ-45 port |
| **Uplink Queue Structure** | • Tx 1p2q2t<br>• Rx 1p1q4t<br>• 512 KB buffer per port | • Tx 1p3q8t<br>• Rx 2q8t<br>• 9.5 MB buffer per Gigabit Ethernet port<br>• 100 MB buffer per 10 Gigabit Ethernet port |
| **Uplink Port Scheduler** | WRR | DWRR or SRR |
| **USB Port** | No | Two USB 2.0 ports-one host port and one device port |
| **Self-Power Cycling** | No, power cycle line cards only | Yes, power cycle remotely through console port |
| **Backplane** | 720 Gbps integrated switch fabric module (SFM) | 32 Gbps shared bus |
| **Performance** | Up to 400 Mpps for Cisco Express Forwarding interface modules | Up to 15 Mpps IPv4 services |
| **Cisco Express Forwarding** | Yes | Yes, hardware-based forwarding with MSFC2A |
| **Distributed Cisco Express Forwarding** | Yes, with a DFC3 present | No |

| Feature | Supervisor Engine 720 | Supervisor Engine 32 |
|---|---|---|
| **SP NVRAM** | 2 MB (SP) | 2 MB (SP) |
| **SP Dynamic RAM (DRAM)** | 512 MB default, upgradeable to 1 GB on Supervisor Engine 720 and Supervisor Engine 720-3B; 1 GB default on Supervisor Engine 720-3BXL | 512 MB default, upgradeable to 1 GB |
| **SP Onboard Flash (BootFlash)** | 64 MB upgradeable to 512 MB, 1GB | 256 MB, through internal compact flash (referred to as bootdisk in command-line interface), upgradeable to 512 MB, 1 GB |
| **Removable Memory** | Compact flash type II-64, 128, and 256 MB; hardware capable to support 512 MB, 1 GB | Compact flash type II-64, 128, and 256 MB; hardware capable to support 512 MB, 1 GB; USB |
| **Chassis Supported** | All Cisco Catalyst 6500 Series chassis and Cisco 7600 Series chassis with fan tray 2 or E-Series fan tray and 2500W power supplies or above | All Cisco Catalyst 6500 Series chassis with fan tray 2 or E-Series fan tray and 2500W power supplies or above; Cisco 7604, Cisco 7606, Cisco 7609, and Cisco 7613 with high speed fan tray |
| **Minimum Software Support** | • Cisco Catalyst 6500 Series:<br>· CatOS 8.1(1)<br>· Cisco IOS ® Software 12.2(14)SX<br>• Cisco 7600 Series: Future | • Cisco Catalyst 6500 Series:<br>· CatOS 8.4(1)<br>· Cisco IOS 12.2(18)SXF<br>• Cisco 7600 Series: IOS 12.2.18SXF |
| **Slot Requirements** | Slots 1 and 2 in a 3-slot chassis, slots 5 and 6 in a 6- or 9-slot chassis, and slots 7 and 8 in a 13-slot chassis | Slots 1 and 2 in a 3-slot and 4 slot chassis, slots 5 and 6 in a 6- or 9-slot chassis, and slots 7 and 8 in a 13-slot chassis |

Tx 1pNqMt = 1 cola de prioridad estricta, N colas normales con M umbrales de WRED
Rx {1p}NqMt = {1 cola de prioridad estricta,} N colas normales con M umbrales de *drop-tail*

# Módulos 1GE

| | Catalyst 6800 Series | | | Catalyst 6700 Series | | |
|---|---|---|---|---|---|---|
| | 6848-SFP | 6848-TX | 6824-SFP | 6748-SFP | 6748-TX | 6724-SFP |
| **Ports** | 48 | 48 | 24 | 48 | 48 | 24 |
| **Optics** | SFP | None (RJ-45) | SFP | SFP | None (RJ-45) | SFP |
| **Onboard memory** | 1 GB | 1 GB | 1 GB | 256 MB, upgradable to 512 MB or 1 GB | 256 MB, upgradable to 512 MB or 1 GB | 256 MB, upgradable to 512 MB or 1 GB |
| **Forwarding engine** | DFC4A(XL) | DFC4A(XL) | DFC4A(XL) | CFC, optional DFC3B(XL) / DFC3C(XL)upgradable to DFC4A(XL) | CFC, optional DFC3B(XL) / DFC3C(XL)upgradable to DFC4A(XL) | CFC, optional DFC3B(XL) / DFC3C(XL)upgradable to DFC4A(XL) |
| **Supported with Sup 2T** | Yes | Yes | Yes | Requires CFC or DFC4A(XL) | Requires CFC or DFC4A(XL) | Requires CFC or DFC4A(XL) |
| **Supported with Sup 720 / Sup 720 10G** | No | No | No | Yes | Yes | Yes |

# Módulos 10GE

| | Catalyst 6900 Series | Catalyst 6800 Series | | Catalyst 6700 Series | | | |
|---|---|---|---|---|---|---|---|
| | 6908-10G | 6816-10G | 6816-10T | 6716-10G | 6716-10T | 6708-10G | 6704-10G |
| **Ports** | 8 | 16 | 16 | 16 | 16 | 8 | 4 |
| **Optics** | X2, OneX adapter, SFP+ | X2, OneX adapter, SFP+ | None (RJ-45) | X2, OneX adapter, SFP+ | None (RJ-45) | X2, OneX adapter, SFP+ | XENPAK |
| **Switch fabric connection** | 80 Gbps | 40 Gbps | 40 Gbps | 40 Gbps | 40 Gbps | 40 Gbps | 40 Gbps |
| **Over-subscription** | 1:1 | 4:1 (1:1 performance mode) | 4:1 (1:1 performance mode) | 4:1 (1:1 performance mode) | 4:1 (1:1 performance mode) | 2:1 (1:1 performance mode) | 1:1 |
| **Onboard memory** | 2 GB | 1 GB | 1 GB | 1 GB | 1 GB | 1 GB | 256 MB, upgradable to 512 MB or 1 GB |

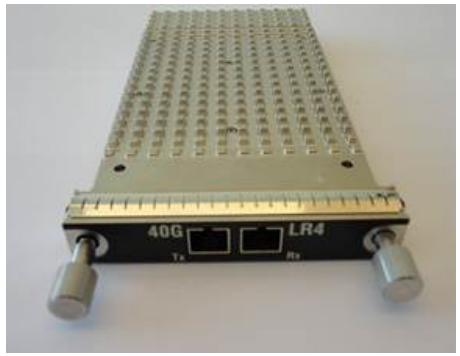
OneX Converter Module

10GBASE SFP+ Module

10GBASE X2 and Xenpak Modules

# Módulos 40GE

| | Catalyst 6900 Series | | |
|---|---|---|---|
| | 6904-40G | | |
| | 40 GE mode | 10 GE mode | Mixed mode |
| **Ports** | 4 x 40 GE | 16 x 10 GE | 2 x 40 GE<br>8 x 10 GE |
| **Optics** | CFP | FourX adapter, SFP+ | CFP, FourX Adapter, SFP+ |
| **Switch fabric connection** | 80 Gbps | 80 Gbps | 80 Gbps |
| **Over-subscription** | 2:1<br>(1:1 performance mode) | 2:1<br>(1:1 performance mode) | 2:1<br>(1:1 performance mode) |
| **Onboard memory** | 2 GB | 2 GB | 2 GB |
| **Forwarding engine** | DFC4E(XL) | DFC4E(XL) | DFC4E(XL) |
| **Supported with Sup 2T** | Yes | Yes | Yes |
| **Supported with other Sup** | No | No | No |

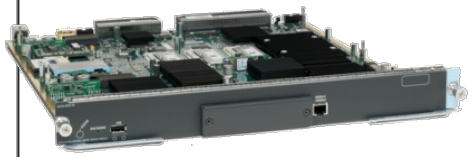



40GBASE-LR4 CFP Module

FourX converter Module con 4 puertos 10GBASE (SFP+)

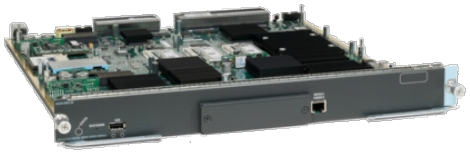
# Application Control Engine Module

| Features | Benefits |
|---|---|
| **Available** | |
| **Application switching** | The Cisco ACE Module represents the next generation of application switches, delivering tightly integrated, essential application service functions in a single powerful system. It provides load-balancing and content switching functions with granular traffic control based on customizable Layer 4 through 7 rules.<br>• Intelligent device load balancing: Cisco ACE provides support for Domain Name System (DNS), cache, transparent caches, firewalls, intrusion detection system (IDS), intrusion prevention system (IPS), VPNs, and SSL VPN.<br>• Generic protocol parsing (GPP): Cisco ACE has native understanding of the following protocols: HTTP, FTP, DNS, Internet Control Message Protocol (ICMP), Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), Extended RTSP, RADIUS, and Microsoft Remote Desktop Protocol (RDP).<br>• Cisco ACE's GPP feature enables you to configure application switching and persistence policies based on any information in traffic payload for custom and packaged applications without requiring any programming.<br>• The Cisco ACE performs payload parsing through hardware using a powerful regular-expression engine to obtain high performance, unlike other software-based solutions.<br>• HTTP header manipulation: Cisco ACE supports the capability to modify, insert, or delete HTTP headers in both client requests and server responses.<br>• Partial server farm failover: Cisco ACE provides the capability to determine which server farm (primary or backup) receives new traffic based on the number of available real servers (rservers.).<br>• TCP dump: Cisco ACE can capture real-time packet information for the network traffic that passes through the Cisco ACE Module, for enhanced troubleshooting.<br>• Source Network Address Translation (NAT) for virtual IP: Source NAT for virtual IP allows you to include a virtual IP address in the NAT pool for dynamic NAT and Port Address Translation (PAT), saving real-world IP addresses on the client-side network.<br>• Source NAT for server farm: Source NAT can back up to a server farm multiple hops away during the failure of a primary server farm, resulting in continuous application availability even during a primary server farm failure.<br>• Flexible network deployment: The Cisco ACE Module uses internal VLAN interfaces. VLANs can be assigned from the supervisor engine to the Cisco ACE. Corresponding VLAN interfaces then can be configured on the Cisco ACE as either routed or bridged. The Cisco ACE Module can be configured in the following modes:<br>• Routed mode: Cisco ACE can be configured to route the traffic when the client-side and server-side VLANs are on different subnets.<br>• Bridge mode: Cisco ACE can be configured to bridge traffic when the client-side and server-side VLANs are on the same subnets.<br>• Asymmetric server normalization (ASN): Cisco ACE can load balance an initial request from the client to a real server; however, the server directly responds to the client, bypassing Cisco ACE. |
| **Predictors** | Cisco ACE performs a series of checks and calculations to determine the server that can best service each client request depending on the load-balancing algorithm or predictor. Cisco ACE uses the following predictors to select the best server to satisfy a client request: adaptive response, least loaded, least bandwidth, least connections, round-robin, hash address, hash cookie, hash header, and hash URL. |



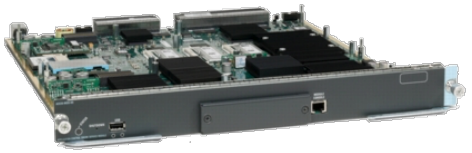
# Application Control Engine Module

| | |
|---|---|
| **Server health monitoring** | To instruct Cisco ACE to check the health of servers and server farms, you can configure health probes (sometimes referred to as keepalives). The following probes are supported: ICMP, TCP, UDP, ECHO {tcp \| udp}, Finger, HTTP, HTTPS, FTP, Telnet, DNS, Simple Mail Transfer Protocol (SMTP), Internet Mail Access Protocol (IMAP), Post Office Protocol (POP), RADIUS, scripted, Keepalive Appliance Protocol (KAL-AP), RTSP, SIP, HTTP return-code parsing, and Simple Network Management Protocol (SNMP) probes. |
| **Persistence and stickiness** | Cisco ACE provides stickiness that allows the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session. Cisco ACE supports the following sticky methods: source or destination IP address, cookie, HTTP header, and SSL session ID. |
| **Redundancy** | The Cisco ACE Module offers three types of high availability:<br>• Interchassis: A Cisco ACE Module in one Cisco Catalyst 6500 Series or Cisco 7600 Series device is protected by a Cisco ACE Module in a peer Cisco Catalyst 6500 Series or Cisco 7600 Series device.<br>• Intrachassis: A Cisco ACE Module in a Cisco Catalyst 6500 Series or Cisco 7600 Series device is protected by another Cisco ACE Module in the same Cisco Catalyst 6500 Series or Cisco 7600 Series device.<br>• Inter-virtual devices: A Cisco ACE Module supports high availability between virtual devices configured across two modules to allow specific devices to fail over without affecting the other devices and applications on a given module.<br>Cisco ACE integrated with the Cisco Global Site Selector (GSS) can provide a multiple-data center failover system. |
| **Fast** | |
| **User Datagram Protocol (UDP) booster** | Cisco ACE can boost performance of UDP-based applications such as DNS load balancing to millions of requests per second. |
| **UDP fast aging** | Cisco ACE can provide very high scalability in terms of number of clients serviced for applications requiring a single response per request. |



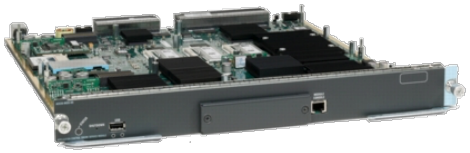
# Application Control Engine Module

| | |
|---|---|
| **SSL acceleration** | • The Cisco ACE solution integrates SSL acceleration technology, which offloads the encryption and decryption of SSL traffic from external devices (servers, appliances, etc.), thereby allowing the Cisco ACE to look more deeply into encrypted data and apply security and application switching policies. This enables the Cisco ACE to make more intelligent policy decisions and also helps ensure that your application-delivery platform complies with internal and external regulations.<br>• With reencryption capabilities, Cisco ACE's SSL acceleration feature helps ensure end-to-end encryption of sensitive data while providing the capability to apply intelligent policies.<br>• SSL features supported: SSL termination and initiation, SSL Version 3.0, Transport Layer Security (TLS) Version 1.0, back-end SSL, exportable Rivest, Shamir, and Adelman (RSA) cipher suites, session ID stickiness, SSL URL rewrite (HTTP header rewrite), session ID reuse, client authentication, HTTP header insert of client and server certificate fields and SSL session parameters, HTTP Redirect on client authentication failure, strong RSA cipher suites, and Advanced Encryption Standard (AES) cipher suites.<br>• SSL accelerated protocols: HTTPS, Secure IMAP (IMAPS), Secure Lightweight Directory Access Protocol (LDAPS), Secure Network News Transfer Protocol (NNTPS), Secure POP Version 3 (POP3S), and Secure Telnet (STELNET)<br>• SSL accelerated ciphers: rsa-with-rc4-128-md5, rsa-with-rc4-128-sha, rsa-with-des-cbc-sha, rsa-with-3des-ede-cbc-sha, rsa-export-with-rc4-40-md5, rsa-export-with-des40-cbc-sha, rsa-export1024-with-rc4-56-md5, sa-export1024-with-des-cbc-sha, rsa-export1024-with-rc4-56-sha rsa-with-aes-128-cbc-sha, and rsa-with-aes-256-cbc-sha<br>• Public key exchange algorithm: RSA 512-bit, 768-bit, 1024-bit, 1536-bit, and 2048-bit<br>• Digital certificates: All major digital certificates from certificate authorities, including the following: VeriSign, Entrust, Netscape iPlanet, Windows 2000 Certificate Server, Thawte, Equifax, and Genuity<br>• Sample SSL key and certificate pair |
| **TCP offloading** | TCP offloading directs traffic in the most efficient manner by analyzing and directing incoming traffic at the request level. TCP offloading breaks the dependency between application requests and the transport layer. It multiplexes and demultiplexes application-level requests onto persistent connections to back-end servers. It keeps client and server TCP connections alive independent of each other and reuses TCP connections, enabling granular application layer policy and offloading TCP processing from web servers, saving CPU cycles. |



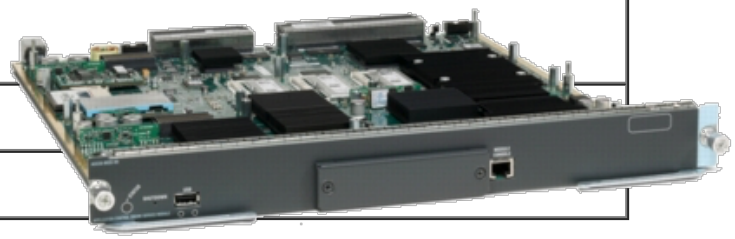
# Application Control Engine Module

| Features | Benefits |
|---|---|
| **Secure** | |
| **Data center security** | The Cisco ACE Module is designed to serve as a last line of defense for servers and applications in data centers. The data center security protects against protocol and denial-of-service (DoS) attacks and encrypts mission-critical content. The Cisco ACE data center security capabilities protect the data center and critical applications from malicious traffic with the following features:<br>• HTTP deep packet inspection: HTTP header, URL, and payload<br>• Bidirectional NAT and PAT<br>• Support for static, dynamic, and policy-based NAT and PAT.<br>• Access control lists (ACLs) to selectively allow traffic between ports<br>• TCP connection state tracking<br>• Virtual connection state for UDP<br>• Sequence number randomization<br>• TCP header validation<br>• TCP window-size checking<br>• Unicast Reverse Path Forwarding (URPF) checking at session establishment<br>• ACL object grouping<br>• TCP SYN cookies, providing distributed DoS (DDoS) protection.<br>• Rate limiting: Cisco ACE rate limiting capabilities can be applied to a set of real servers, virtual servers, or both. |
| **Application security** | Integrated hardware-accelerated protocol control offers efficient inspection and filtering of popular data center protocols such as HTTP, RTSP, DNS, FTP, ICMP, SIP, Skinny Client Control Protocol (SCCP), and LDAP. |



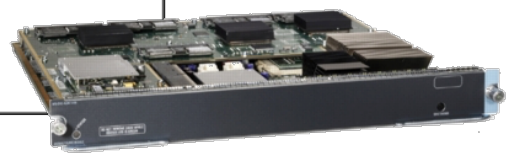
# Application Control Engine Module

| Feature | Maximum Performance and Configuration |
|---|---|
| **Global Parameters** | |
| **Throughput** | 16 Gbps*, 8 Gbps*, and 4 Gbps |
| **Syslogs per second** | 350,000 |
| **Global Configuration** | |
| **Total VLANs (client and server)** | 4000 |
| **Probes** | ICMP, TCP, UDP, Echo, Finger, DNS, Telnet, FTP, HTTP, HTTPS, SMTP, POP3, IMAP, RTSP, RADIUS, SIP, SNMP, KAL-AP, and TCL Scripts |
| **NAT entries** | 1 million |
| **Virtual partitions** | Up to 250*; 5 virtual partitions (devices) included in base price |
| **SSL Performance** | |
| **SSL throughput** | 3.3 Gbps |
| **SSL TPS** | 1000 TPS included in base price, and 5000, 10,000, or 15,000 TPS with licensing |
| **Application Switching Performance** | |
| **Maximum connections per second** | 325,000 complete transactions sustained rate |
| **Concurrent connections** | 4 million |
| **Sticky table entries** | 4 million |

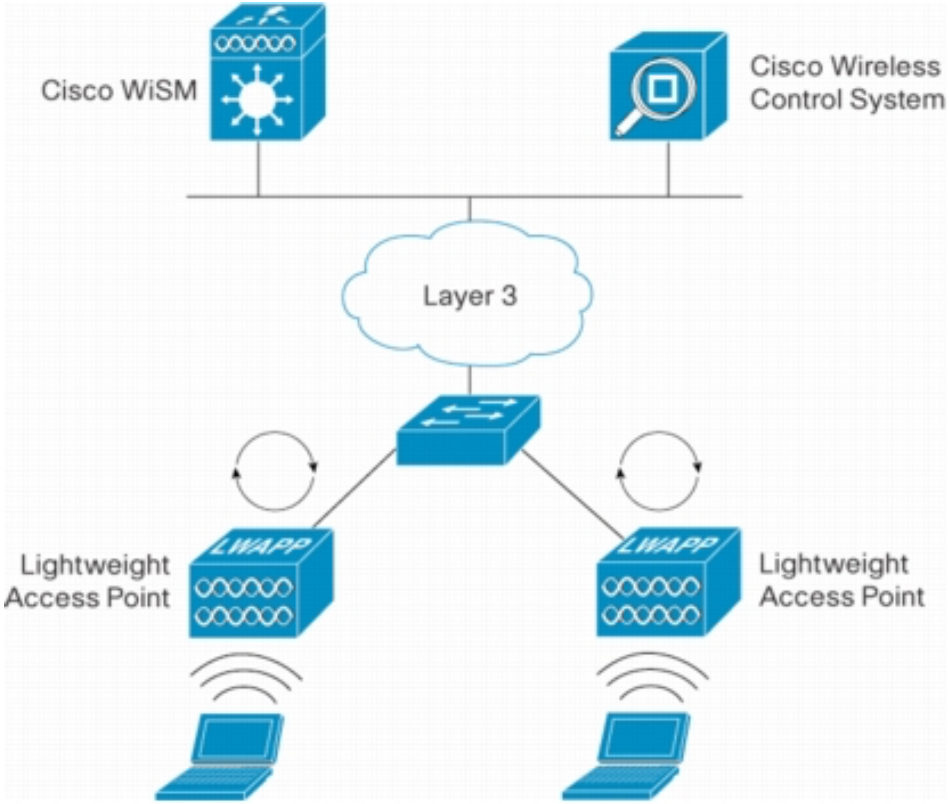


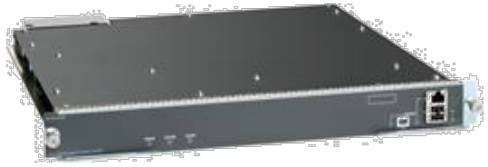
# Anomaly Guard Module

| Feature | Description |
|---|---|
| **Attack Protection** | • Spoofed and non-spoofed attacks<br>• TCP (syns, syn-acks, acks, fins, fragments) attacks<br>• User Datagram Protocol (UDP) attacks (random port floods, fragments)<br>• Internet Control Message Protocol (ICMP) attacks (unreachable, echo, fragments)<br>• Domain Name System (DNS) attacks<br>• Client attacks<br>• Inactive and total connections attacks<br>• HTTP Get Flood attacks<br>• Border Gateway Protocol (BGP) attacks<br>• Session Initiation Protocol (SIP) voice over IP (VoIP) attacks |
| **Continuous Learning and Protection** | • Can operate in continuous learning and protection mode (Release 5.0 and later)<br>• Simultaneously adjusts thresholds and protect from attacks<br>• Switches between learning and protection modes automatically<br>• Returns to learning mode after an attack is completed |
| **Traffic Analysis** | • Ability to capture and packets that are traversing the guard and save them as pcap files.<br>• The GUI allows extensive analysis of the captured packets.<br>• The user may limit capture to packets with a certain decision value only (forward, drop, reply).<br>• The user may filter the capture using a tcpdump expression. |
| **Signature Extraction-Deep Packet Inspection** | • Ability to find prominent patterns in the payload of captured packets<br>• Automated algorithm analyzes packet capture to extract a signature found only in malicious packets<br>• Content-based filter can be applied for extracted signature |
| **Content-Based Filter** | • Provides ability to look for patterns in the payload<br>• Can define multiple content-based filters<br>• Can be configured to either just count packets, or drop them |



# Wireless Services Module 2



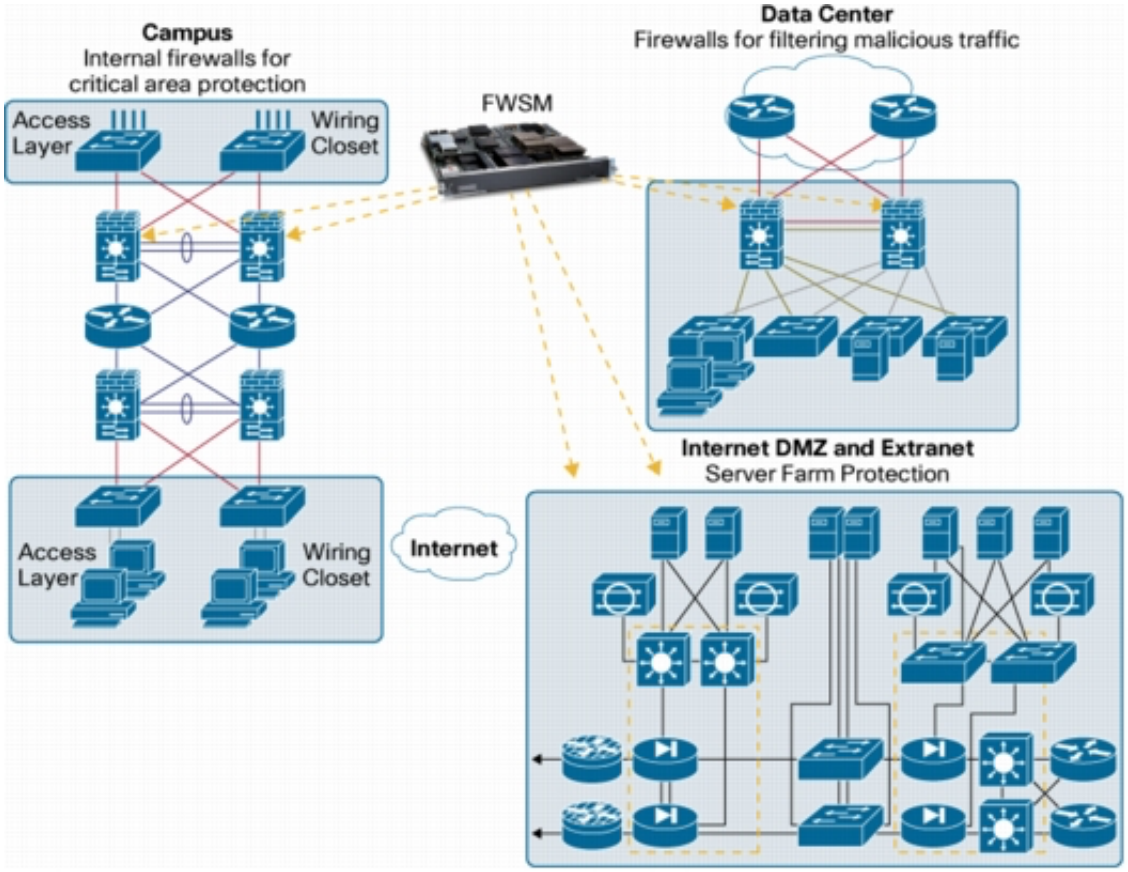



# Wireless Services Module 2

| Feature | Benefits |
|---|---|
| **Scalability** | • Supports 100, 300, 500 and 1000 access points for business-critical wireless services at locations of all sizes |
| **High Performance** | • Wired-network speed, nonblocking performance for 802.11n and optimized for 802.11ac networks |
| **RF Management** | • Provides both real-time and historical information about RF interference impacting network performance across controllers, through systemwide Cisco CleanAir technology integration |
| **High-Performance Video** | • Integrates Cisco VideoStream technology as part of the Cisco medianet framework to optimize the delivery of video applications across the WLAN |
| **End-to-End Voice** | • Supports Unified Communications for improved collaboration through messaging, presence, and conferencing<br>• Supports all Cisco Unified IP Phones for cost-effective, real-time voice services |
| **Comprehensive End-to-End Security** | • Offers control and provisioning of wireless access points (CAPWAP)-compliant Datagram Transport Layer Security (DTLS) encryption to help ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links |
| **Cisco OfficeExtend** | • Supports corporate wireless services for mobile and remote workers with secure wired tunnels to the Cisco Aironet 600, 1130, or 1140, 3500, 3600 Series Access Points<br>• Extends the corporate network to remote locations with minimal setup and maintenance requirements (zero-touch deployment)<br>• Improves productivity and collaboration at remote site locations<br>• Separate service set identifier (SSID) tunnels allow both corporate and personal Internet access<br>• Reduced carbon dioxide emissions from a decrease in commuting<br>• Higher employee job satisfaction from ability to work at home<br>• Improves business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather |
| **Cisco Enterprise Wireless Mesh** | • Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network<br>• Available on select Cisco Aironet access points, Cisco Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing |

CAPWAP = Control And Provisioning of Wireless Access Points (RFC 5415)

# Firewall Services Module



# Firewall Services Module

| | Capacities |
|---|---|
| **Performance** | • 5.5 Gbps throughput per service module<br>• Up to 4 FWSMs (20 Gbps) per Catalyst 6500 chassis with static VLAN or IOS Policy-based Routing<br>• 2.8 Mpps<br>• 1 million concurrent connections<br>• 100,000 connection setups and teardowns per second<br>• 256,000 concurrent NAT or PAT translations<br>• Jumbo Ethernet packets (8500 bytes) supported |
| **VLAN Interfaces** | • 1000 total per service module<br>• 256 VLANs per security context in routed mode<br>• 8 VLAN pairs per security context in transparent mode |
| **Access Lists** | • Up to 80,000 Access Control Entries in single context mode<br>• Note: the FWSM implements Layer 3 and 4 access control security checks in hardware with virtually no performance impact using non-upgradeable high-speed memory |
| **Virtual Firewalls (Security Contexts)** | • 20, 50, 100, 250 Virtual Firewall licenses<br>• 2 Virtual Firewalls and 1 administrative context are provided for testing purposes. |

# Firewall Services Module

| Features | Summary |
|---|---|
| **Scalable Architecture to Support Up to 20+ Gbps of Firewall Services within the Catalyst 6K Infrastructure** | • A variety of industry proven clustering techniques deliver a seamless method to scale firewall performance to 20 Gbps and beyond. |
| **Visibility into Encrypted Threats** | • Leveraging SSL decryption capabilities within the Catalyst 6K infrastructure, the FWSM has the ability to gain visibility into encrypted policy violations to which traditional firewalls have no visibility. |
| **Intelligent Network Services** | • Layer 2 Firewall (transparent mode) with NAT and PAT support<br>• Layer 2 Firewall (transparent mode) with NAT and PAT support<br>• Layer 3 Firewall (route and/or NAT mode)<br>• Mixed Layer 2 and Lyer 3 firewall per FWSM<br>• Dynamic/static NAT and PAT<br>• Policy-based NAT<br>• VRF-aware NAT<br>• Destination NAT for Multicast<br>• Static routing support in signle- and multiple security content mode<br>• Dynamic routing in single security context mode: Open Shortest Path First (OSPF). Routing Initiation Protocol (RIP) v1 and v2, PIM Sparse Mode v2 multicast routing, Internet Group Management Protocol (IGMP) v2.<br>• Dynamic routing in single and virtual security context mode using stub iBGP (Licensed feature)<br>• Transparent mode supports static routing only<br>• Private VLAN for L2 and L3 firewall enables firewall security policies between isolated ports.<br>• Asymmetric routing supporting without redundancy by using asymmetric routing groups<br>• IPv6 networking and management access using IPv6 HTTPS, Secure Shell Protocol (SSH) v1 and v2, and Telnet |

# Firewall Services Module

| | |
|---|---|
| **Core Stateful Firewall** | • NAT Translate bypass enhances scalability by not creating NAT translate entries when no NAT-control or NAT except is used<br>• Selective TCP State Bypass on a per flow basis<br>• Timeout on a per flow for TCP and non-TCP flows<br>• ACLs: Extended ACL for IP traffic, Ethertype ACL for non-IP traffic, standard ACL for OSPF route distribution, per-user Cisco Secure Access Control Server (ACS)-based ACLs, per-user ACL override, object fgrouping for ACLs, time-based ACLs<br>• Cisco Modular Policy Framework (MPF) with flow-based security policies<br>• Cut-through user authentication proxy with local database and external AAA server support: TCP, HTTP, FTP, HTTPS, and others<br>• URL filtering: Filter HTTP, HTTPS, and FTP requests by Websense Enterprise or HTTP filtering by N2H2 (now part of Secure Computing Corporation)<br>• Same security-level communication between VLANs (without NAT/static policies) and per-host maximum connection limit<br>• Protection from denial of service (DoS) attacks: DNS Guard, Flood Defender, Flood Guard, TCP Intercept with SYN cookies organization, Unicast Reverse Path Forwarding (uRPF), Mail Guard, FragGuard and Virtual Reassembly, Internet Control Message Protocol (ICMP) stateful inspection, User Datagram Protocol (UDP) rate control, TCP stream re-assembly and deobfuscation engine, TCP traffic normalization services for attack detection<br>• Address Resolution Protocol (ARP) inspection in transparent firewall mode<br>• DHCP server, DHCP relay to upstream router with per interface configuration |

# Firewall Services Module

| Features | Summary |
|---|---|
| **Service Virtualization (Multiple Security Context Mode)** | • Transparent<br>• Routed Mode<br>• NAT/PAT<br>• ACL<br>• Protocol Inspection<br>• SNMP<br>• Syslog<br>• DHCP<br>• Resource management controls resource usage per security context |
| **Inspection Engines** | • Application policy enforcement<br>• Protocol conformance checking<br>• Protocol state tracking<br>• Security checks<br>• NAT/PAT support<br>• Dynamic port allocation<br>• Core internet protocols: HTTP, FTP, Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP), DNS, Extended DNS (EDNS), ICMP, TCP, UDP<br>• Database/OS services: Internet Locator Services/Lightweight Directory Access Protocol (ISL/LDAP), Oracle/SQL*Net v1 and v2, NetBIOS over IP, NFS, Remote Shell Protocol (RSH), sUNrpc/nis+, XWindows (SDMCP), Registration Admission and Status (RAS) v2<br>• Multimedia/VoIP: H.323 v1–4, H.323 Gatekeeper Cluster GUP message support, Session Initiation Protocol (SIP), SCCP (Skinny), Skinny Video, GPRS Tunneling Protocol (GTP) v0 and v1 (3G Mobile Wireless), Media Gateway Control Protocol (MGCP) v0.1 and v1.0, Real-Time Streaming Protocol (RTSP), Telephony Application Programming Interface (TAPI) and Java TAPI (JTAPI) T.38 Fax over IP, Gatekeeper Routed Control Signaling (GKRCS), fragmented and segmented multimedia stream inspection<br>• Specific applications: Microsoft Windows Messenger, Microsoft NetMeeting, Real Player, Cisco IP phones, Cisco SoftPhone<br>• Security services: Point-to-Point Tuneling Protocol (PPTP) |
| **High Availability** | • Intrachassis and interchassis<br>• Active-Standby stateful failover<br>• Active-Active stateful failover support in multiple context mode<br>• Asymmetric routing support with Active-Active redundancy |
| **Application Inspection Control** | • Advanced HTTP inspection services: RFC compliance checking for protocol anomaly detection, HTTP command filtering, MIME type filtering content validation, Uniform Resource Identifier (URI) length enforcement, and more<br>• Tunneling application control: AOL Instant Messenger, Microsoft Messenger, Yahoo Messenger, peer-to-peer applications (such as KaZaA and Gnutella), and other applications (such as GoToMyPC) |