



# Security Services Integration with Cisco Catalyst 6500 and 7600 Series Services Modules

## At-A-Glance

### Secure, High-Performance, and Efficient Network Deployments

#### Security Services Integration

Cisco® Catalyst® 6500 Series switches and Cisco 7600 Series routers are designed for security and VPN aggregation, high performance, and scalability, enabling customers to build an integrated and efficient intelligent network.

Cisco Systems® provides a comprehensive suite of security services modules that can be added in a modular fashion to a customer's existing switching and routing infrastructure, allowing low total cost of ownership (TCO) while obtaining the highest performance and the most complete secured IP services.

#### Enhanced Security

- Multilayer (Layers 2–7) defense-in-depth
- Secured IP services integration

#### Highest Performance and Scalability

- Modular and hardware-accelerated
- Low-latency integration with network infrastructure

#### Service Virtualization

- Granular, customized control of policies, monitoring, and reporting
- Reduced TCO by using the same physical infrastructure
- Resource limiter that allocates resources per virtual context, helping to ensure high availability

#### Efficient Management

- Role-based remote access control
- Embedded single device managers (CiscoView Device Manager [CVDM], Cisco Adaptive Security Device Manager [ASDM], Cisco Router and Security Device Manager [SDM])
- Centralized multidevice manager (Cisco Security Manager)
- Real-time monitoring, analysis, and reporting (Cisco Security Monitoring, Analysis, and Response System [MARS]) with multiple devices and end-to-end network awareness
- Cisco Security Auditor, which detects policy violations and reports recommendations based upon compliance and best practices

**Table 1.** Cisco Catalyst 6500 Series and Cisco 7600 Series Security Services Components

Components	Description
<b>Switch-Integrated Security</b>	<ul style="list-style-type: none"> <li>• <b>Switch-Embedded Security:</b> Port security, private VLAN, VLAN access control lists (VACLs), DHCP Snooping, DHCP and ARP rate limiting, protocol filtering</li> <li>• <b>Hardware-Integrated Security:</b> CPU rate limiting</li> <li>• <b>Identity-Based Networking Services:</b> IBNS 802.1X, AAA</li> <li>• <b>Network Admission Control (NAC)</b></li> </ul>
<b>Firewall Services Module (FWSM)</b>	<ul style="list-style-type: none"> <li>• <b>High Performance:</b> 5 Gbps; 2.8M pps; 1M concurrent connections; 100,000 cps; 250 virtual firewalls; 80,000 ACLs; 1000 VLANs; 4 FWSMs per chassis</li> <li>• <b>Stateful-Inspection Firewall:</b> Tracks the state of all network communications and prevents unauthorized access</li> <li>• <b>Application and Protocol Inspection Engines:</b> Examine network flows at Layers 4–7, including protection for port 80 misuse, IM, P2P, VoIP, and multimedia</li> </ul>
<b>Intrusion Detection and Prevention Service Module (IDSM-2)</b>	<ul style="list-style-type: none"> <li>• <b>High Performance:</b> 500 Mbps per IDSM, multigigabit (up to 8 IDSMs per chassis) with Cisco EtherChannel® load balancing</li> <li>• <b>Thousands of Dynamic Signatures:</b> Integrates with Trend Micro Outbreak Prevention Service</li> <li>• <b>Multivector Threat Identification and Accurate Inline Prevention:</b> With risk rating and meta event correlation</li> </ul>
<b>IPSec VPN Shared Port Adapter (VPN SPA)</b>	<ul style="list-style-type: none"> <li>• <b>High Performance:</b> 2.5 Gbps of AES and 3DES IPSec, 8000 tunnels, 10 SPAs per chassis, 25 Gbps, 5M pps</li> <li>• <b>Next-Generation Encryption:</b> Includes all key sizes (128-, 192-, and 256-bit keys)</li> <li>• <b>Attractive Form-Factor:</b> Half-slot form factor reduces slot consumption and increases total performance per slot</li> </ul>
<b>SSL VPN Services Module (WEBVPN SM)</b>	<ul style="list-style-type: none"> <li>• <b>High Performance:</b> 8000 tunnels; 32,000 maximum connections; 300 Mbps throughput; 128 virtual contexts; 356 certificates; up to 4 WEBVPN SMs per chassis</li> <li>• <b>Clientless, Port Forwarding, and Full Tunnel Support</b></li> </ul>
<b>Traffic Anomaly Detection and Guard Services Modules (ADM, AGM)</b>	<ul style="list-style-type: none"> <li>• <b>High Performance:</b> One 1-Gbps interface; 1.5M concurrent connections; 150,000 dynamic filters; less than 1 ms latency or jitter</li> <li>• <b>Detects and Mitigates</b> the broadest range of distributed denial of service (DDoS) attacks</li> <li>• <b>Behavioral Anomaly Recognition:</b> Helps ensure accuracy to forward legitimate transactions</li> </ul>
<b>Network Analysis Module (NAM-1, NAM-2)</b>	<ul style="list-style-type: none"> <li>• <b>Visibility into network and application traffic</b></li> <li>• <b>Intelligent IP Services Monitoring:</b> Monitors application response times, QoS, and voice and video traffic</li> <li>• <b>Easy to Deploy and Use:</b> Includes an on-board Traffic Analyzer GUI for access to configuration templates and reports</li> </ul>

# Security Services Integration with Cisco Catalyst 6500 and 7600 Series Services Modules

## At-A-Glance

### Enterprise Services Deployments

- **Data center protection (FWSM, IDSM, NAM, ADM, AGM):** Protect confidential data and business-critical applications, and prevent security threats from both outside and inside the organization.
- **Internet edge attack prevention (FWSM, IDSM):** Identify and restrict access to unauthorized users, and prevent security threats from both outside and inside the organization.
- **Secure connectivity (VPN SPA, WEBVPN SM):** Provision and manage secure remote and site-to-site access, extend access to key applications, and protect endpoint devices.
- **Campus security (FWSM, IDSM, NAM):** Identify and restrict access to unauthorized users, and prevent security threats from both outside and inside the organization.

**Security Bundles:** Full system configurations are available with FWSM, IDSM, and VPN SPA.

World-class global support is provided by Cisco TAC and Advanced Services.

For more information:

<http://www.cisco.com/en/US/partner/products/hw/modules>

