AMS.NET
Technology Solution Provider

Cisco Security

Network security up until this point has been a scattered collection of appliances and software providing overlapping functionality creating a potential for missed threats or irrelevant and inconsistent information. AMS.NET and Cisco's security solutions and threat intelligence capabilities consolidate these functions to deliver fully integrated security, advanced malware protection and unified management for security before, during and after an attack.

Cisco Firepower- Single Vendor, Fully Integrated Next-Generation Firewall

The Cisco Firepower Next Generation Firewall (NGFW) is a fully integrated, threat-focused next-gen firewall with unified management. It includes Application Visibility and Control (AVC), optional Firepower next-gen IPS (NGIPS), Cisco Advance Malware Protection (AMP), and URL filtering. Cisco Firepower provides advanced threat protection before, during, and after attacks.

Most next-generation firewalls focus heavily on enabling application access control, but little on their threat defense capabilities. Cisco's Firepower Next Generation Firewall addresses attacks across the entire continuum. Cisco Firepower delivers not only granular application control but also security against the threats posed by sophisticated and evasive malware attacks. It is a fully integrated solution therefore reducing complexity and providing even more control and visibility. The Cisco Firepower single management interface delivers unified visibility from the network to the endpoint and stops more threats by superior visibility into your environment. Firepower NGFW enables comprehensive policy management that controls access, stops attacks, defends against malware and provides integrated tools to track, contain and recover from attacks that do get through.

This solution is performance and density optimized with support for 1/10/40 Gigabit Ethernet interfaces, up to 60 Gbps stateful firewall throughput, low latency, and 1 RU form factor. The Cisco Firepower Next Gen Firewall integrates with other Cisco networking and security solutions to further enhance security and visibility. Cisco Firepower delivers superior threat defense, at faster speeds, with a smaller footprint.

Cisco Firepower Highlights

- Consolidate security vendors with single vendor integrated solution
- Fully integrated advanced malware protection
- Performance and density optimized- 1/10/40 GB support
- Maximum firewall throughput
- Ability to track and contain malware infections
- Precise application visibility and control
- Next-generation Sourcefire IPS
- Reputation and category-based URL filtering
- Automatically correlates threat events
- Analyzes your networks weaknesses
- Integrates with a number of Cisco network security products

Celebrating More Than 25 Years

Learn More!
Go to www.ams.net/solutions
800-893-3660

Next Generation Firewall/URL Filtering Comparison

Feature	Cisco Firepower/ASA	Palo Alto Networks	iboss	Lightspeed Systems
Virtual Private Network (VPN)	✓	✓	–	–
Firewall Throughput	✓	✓	–	–
Application Visibility and Control (AVC)	✓	✓	✓	–
Intrusion Prevention System (IPS)	✓	✓	–	–
URL Filtering	✓	✓	✓	✓
Advanced Malware Protection (AMP)	✓	✓	–	–
High Availability	✓	✓	✓	✓
User Device Mobility Support/ Persistent Security Away from the Network	✓	✓	–	✓
Unified Management	✓	✓	–	–
Integrated Network & Security Solution	✓	–	–	–

Cisco Firepower Models

Features	4110	4120	4140	4150*	9300 with 1 SM-24 Module	9300 with 1 SM-36 Module	9300 with 3 SM-36 Modules
Maximum firewall throughput (ASA)	20 Gbps	40 Gbps	60 Gbps	-	75 Gbps	80 Gbps	225 Gbps
Maximum throughput FW + AVC (Firepower Threat Defense)	12 Gbps	20 Gbps	25 Gbps	-	25 Gbps	35 Gbps	100 Gbps
Maximum throughput: FW + AVC + NGIPS (Firepower Threat Defense)	10 Gbps	15 Gbps	20 Gbps	-	20 Gbps	30 Gbps	90 Gbps

*Cisco Firepower 4150 is scheduled for release in the first half of 2016; specifications to be announced.

Single vendor provides integrated and comprehensive Advanced Malware Protection (AMP) for all enforcement points in the extended network including endpoints, network appliances, secure content gateways, mobile devices and virtual environments.

AMS.NET
Technology Solution Provider

Cisco Advanced Malware Protection (AMP) for Endpoints- Protect Devices from Malware Attacks

Cisco's security solution provides protection throughout the extended network including endpoints whether connected to a protected network or roaming on the Internet. Cisco's Advanced Malware Protection (AMP) for Endpoints goes beyond point-in-time detection to provide the level of visibility and control you need to stop advanced threats missed by other security layers.

Supporting protection throughout the attack continuum, AMP for Endpoints performs analysis in real time, behavior over time and retrospectively. Cisco AMP for Endpoints increases security intelligence across all endpoints - PCs, Macs, Linux, mobile devices, and virtual systems. Utilizing threat intelligence, once an attack is detected, AMP provides immediate protection across the rest of the attack vectors. AMP can quickly detect, contain, and remediate malware before damage is done.

Cisco AMP for Endpoints Highlights

- Protects endpoints and networks from malware attacks
- Deep visibility and control
- Threat intelligence
- Continuous analysis
- Broad endpoint coverage

Cisco OpenDNS- Cloud-Delivered Network Security

As a part of Cisco's security solution, OpenDNS provides cloud-delivered network security services that protect any device, no matter where it's located. Security is delivered at the DNS layer, to keep malware from compromising your systems and to stop botnets, phishing and ransomware from exfiltrating your data.

OpenDNS complies with internal acceptable use policies or regulatory requirements with up to 60 content categories. Open DNS extends protection beyond the perimeter and to mobile devices. OpenDNS Roaming Client extends protection to devices that are not always connected to your network without sacrificing performance.

The cloud platform instantly displays activity from all locations to identify targeted attacks by comparing your activity over any port, protocol, or app to the rest of the word. Predictive intelligence tracks the worlds Internet activity to stay ahead of attacks. OpenDNS knows which DNS infrastructures and IP networks will distribute malware, control botnets or phish login credentials before their used for cyber-attacks. More than 80 million security events are blocked daily.

Cisco OpenDNS Highlights

- Cloud-delivered security
- Malware and breach protection
- Security visibility
- Leverage 60 content filters
- Secures mobile or remote users
- Location-based policies and customizable block lists and pages
- Predictive intelligence to protect against emerging threats

AMS.NET and Cisco's security solution provides security everywhere, across all the attack vectors such as web, cloud, email, data center and mobile. Integrated security products and threat intelligence deliver protection throughout the attack continuum- before, during and after attack.

AMS.NET
Technology Solution Provider