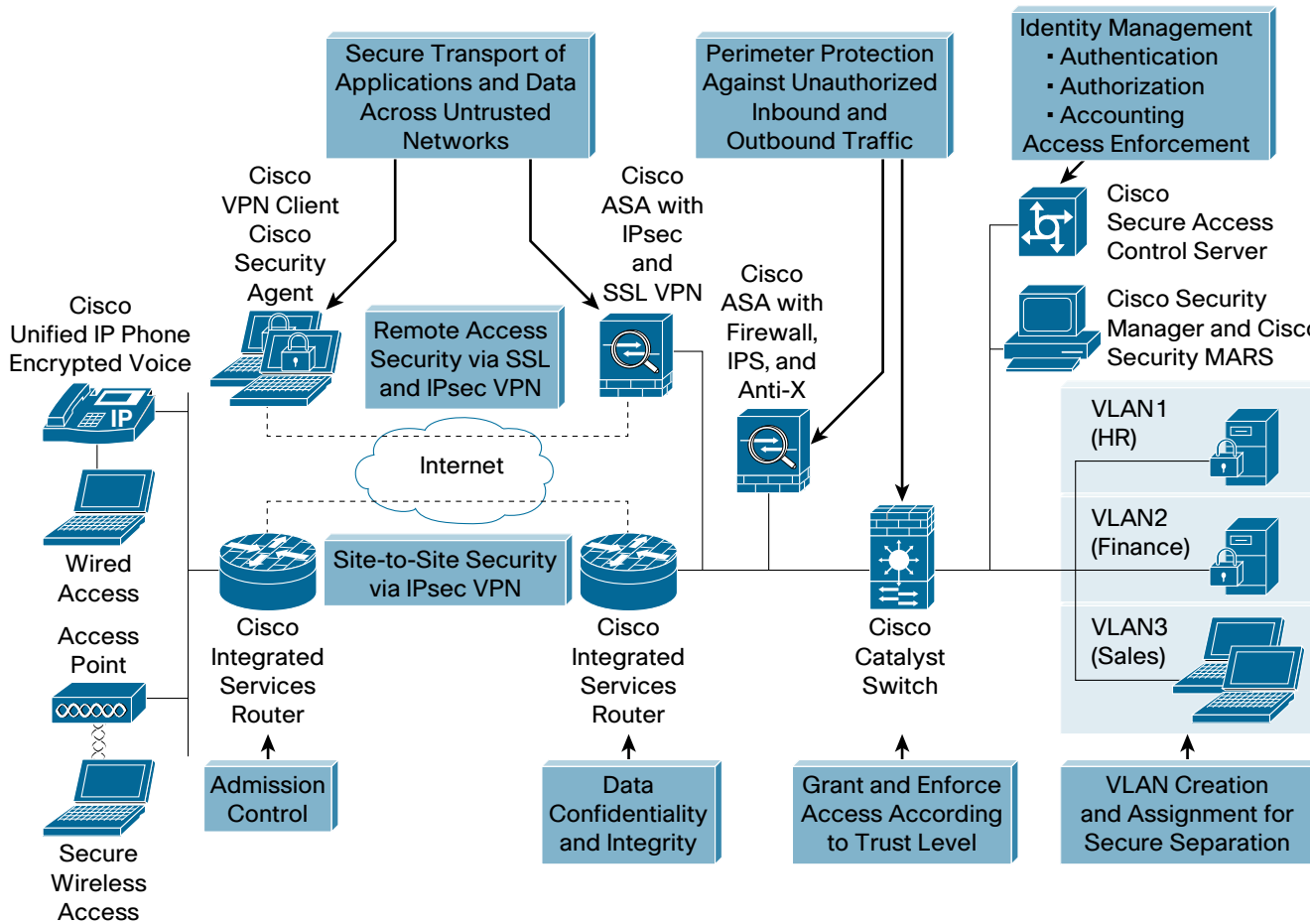


Cisco Network Security Blueprint: MidMarket Business—At-A-Glance



Cisco Self-Defending Network

Effective network security is a business imperative. To comprehensively protect the business network from being compromised, security features must be integrated into every element of the network and must work together as a system to ensure business continuity. This reference blueprint for integrated network security offers a network architecture solution to protect against theft of information, virus outbreak prevention, and application abuse.

Business Benefits

With integrated security solutions from Cisco Systems®, you can better protect your business network against the most serious security attacks while increasing greater control through effective management. Having an effective and manageable network provides increased control over costs associated with deploying and maintaining a secure network. Cisco® integrated security solutions are modular, allowing organizations to add components or capacity as business needs dictate. Operations staff have better insight into the users on their networks—where they are and what information they are trying to access—helping them devote more time to making their networked organizations efficient and productive.

A Cisco Self-Defending Network:

- Reduces risk and protects against known and unknown threats
- Improves productivity through business continuity
- Grows and adapts with emerging security requirements
- Offers increased control through effective management

Solution Components

Integrated network elements function collectively to securely meet your business objectives.

Products and Technologies	Description
Cisco Self-Defending Network	The Cisco Self-Defending Network offers a complete, modular approach to business network security. For security systems to react to threats in time, security features must be integrated into every aspect of the network, from desktops through the LAN and across the WAN. Only Cisco offers this solution.
Network Admission Control (NAC)	NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, limiting damage from viruses, worms, and spyware. The NAC industry initiative is led by Cisco.
Cisco ASA 5500 Series Adaptive Security Appliances	The Cisco ASA 5500 Series is a high-performance, multifunction security appliance family that delivers converged firewall, intrusion prevention system (IPS), network antivirus, and VPN services. It provides proactive threat mitigation to stop attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity—all in a single platform.
Cisco Integrated Services Routers	These routers provide modular, built-in VPN hardware encryption, Cisco IOS® Software-based VPN firewall, and inline IPS capabilities.
Cisco Secure Access Control Server (ACS)	Cisco Secure ACS provides a RADIUS authentication, authorization, and accounting (AAA) access control framework that manages user trust and identity for wired and wireless networks.
Cisco Catalyst® Switches	Cisco Catalyst switches deliver secure, converged services, including the Cisco Firewall Services Module (FWSM).
Cisco NAC Appliance (formerly Cisco Clean Access)	Extending NAC offerings, the Cisco NAC Appliance helps organizations intelligently provide trusted access to “clean” endpoints, thereby increasing the availability and integrity of customer networks and critical business applications.
Cisco Security Agent	Cisco Security Agent identifies and prevents malicious behavior, eliminating known and unknown (“day-zero”) security risks and helping reduce operational costs.
Cisco Security Manager	Cisco Security Manager is suitable for managing small networks consisting of a handful of devices or thousands of devices. Scalability is achieved through intelligent policy-based management techniques that can simplify administration.
Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS)	Cisco Security MARS efficiently aggregates and reduces massive amounts of network and security data from network devices and security countermeasures. By gaining network intelligence, Cisco Security MARS effectively identifies network and application threats through sophisticated event correlation and threat validation.

For More Information

For more information about the Cisco Self-Defending Network, how to protect your organization from virus outbreaks, and how to take advantage of special program offers, visit: <http://www.cisco.com/go/midsizedsecurity>.