

# Cisco Network Security



Intelligent and adaptive computer networks not only protect against the malicious attacks that are crippling corporate America, they allow your company to maintain high network availability for legitimate purposes while attack countermeasures are in progress.

Through our mastery of Cisco's Self-Defending Network Initiative, VLSystems designs networks with a comprehensive, multilayered approach that ensures security and helps administrators overcome such challenges as:

## About VLSystems

VLSystems, founded in Irvine, Calif. in 1978, is a Cisco Advanced Security Specialized partner and a Microsoft Gold Certified partner specializing in secure information solutions involving Cisco LAN/WAN, data center and security, Microsoft advanced infrastructure, SharePoint Portal Server, workflow and collaboration, and managed services.

To arrange a private consultation, contact us at (949) 660-8855 or (800) 542-5050.

- **Structured threats targeting your organization**
- **Unstructured threats aimed at any Internet-connected entity**
- **Increased attack sophistication and remediation costs**
- **Poor attack and fault identification, prioritization and response caused by security information overload**
- **Meeting compliance and audit requirements**
- **Insufficient security staff, budget and knowledge**

## The Cisco Self-Defending Network

A Cisco Self-Defending Network has the knowledge to identify, prevent and adapt to threats, using functionality built into every security element. These adaptive defenses must:

- **Be highly available**
- **Operate unobtrusively**
- **Isolate the attack source**
- **Quickly respond to zero-day attacks**

In addition to providing appliances that meet specific security needs, Cisco integrates security capabilities directly into network devices to take advantage of existing infrastructure with minimal disruption to your operations.

## Cisco Multilayered Security Approach

### **Adaptive Threat Defense (ATD)**

Part of the Cisco Self-Defending Network security strategy, ATD dynamically addresses threats at multiple layers, enabling tighter control of network traffic, endpoints, users and applications.

### **Anomaly Detection and Mitigation**

Cisco Traffic Anomaly Detectors detect the presence of a potential DDoS attack, divert traffic destined for the targeted device, and identify and block malicious traffic in real time, without affecting the flow of legitimate transactions.



### **Compliance Validation**

Cisco Clean Access [Network Admission Control (NAC)] profiles and authenticates incoming traffic and validates host compliance, thereby minimizing damage from viruses and worms.

### **Endpoint Security**

Cisco Security Agent (CSA) includes policy-based administrator tools to monitor and control network activity. This includes measures to prevent malicious code installation such as malware and spyware, as well as helping to control digital information leakage.

### **Firewall**

Cisco PIX/ASA Security Appliance delivers robust traffic filtering and application policy enforcement, multivector attack protection, and secure connectivity services in easy-to-deploy solutions.

### **Identity Management**

Cisco Secure Access Control Server (ACS) provides a centralized identity networking solution across all RADIUS-compliant devices, controlling who can log in to the network, user privileges and administrator controls.

### **Integrated Router/Switch Security**

Cisco network products integrate security features, including Cisco IOS Firewall, VPN and Intrusion Prevention System (IPS) services across Cisco's router portfolio, providing robust and adaptable security solutions that defend against DDoS attacks and other threats.

### **Multifunction Security**

An Adaptive Security Appliance (ASA) is a high-performance, multifunction security appliance family delivering converged firewall, IPS, network antivirus and VPN services. As a key component of the Cisco Self-Defending Network, it provides protective threat mitigation that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity.

### **Network Intrusion Prevention**

The Cisco Intrusion Prevention System (IPS) delivers a new generation of highly accurate and intelligent in-line prevention services complemented by antivirus, antispymware and worm-mitigation capabilities for improved threat defense across multiple form factors, including appliances, switch-integrated modules and Cisco IOS Software-based solutions.

### **Security Management**

A Security Monitoring, Analysis and Response System (MARS) consolidates the management of network security by means of a threat-mitigation appliance and its management software. MARS monitors and manages the multilayered security devices as well as the network devices in order to provide protection and correlated security events and attack countermeasures. These include intruder details, viruses, zero-day attacks, Trojan horses, worms and spyware.

### **Virtual Private Networks**

Cisco Encryption Technology provides network data encryption at the IP packet level, offering a robust, standards-based security solution for secure VPNs. The Cisco VPN 3000 Series offers both IP Security and Secure Sockets Layer-based VPN connectivity with a secure desktop on a single platform. Conventional VPN client is also supported in this solution.

## **Services**

VLSystems can develop a customized long-term information security plan to meet your organization's unique requirements. We'll describe vulnerabilities in your current infrastructure, recommend corrective actions to create a detailed plan of attack, and design, install and maintain your Cisco Self-Defending Network.