# CISCO SELF-DEFENDING NETWORKS
# INTEGRATED SOLUTIONS TO IDENTIFY, PREVENT AND ADAPT TO SECURITY THREATS

## CISCO SECURITY PRODUCTS

**Cisco Dedicated Security Appliances**
Cisco Dedicated Security Appliances deliver advanced security, are easy to deploy and manage, integrate into the network, and offer investment protection.

The Cisco PIX Security Appliance supports high-speed, application-aware firewall protection. Cisco intrusion prevention sensors offer high-speed, threat identification, analysis, and prevention. Cisco VPN 3000 Series Concentrators support secure communications through IPSec and SSL. Cisco Clean Access appliances offer turnkey policy-based Network Admission Control (NAC).

**Cisco Integrated Security Solutions**
Cisco Catalyst 6500, 4500, 3750, and 2950 series switches integrate firewall, IPSec VPN, and intrusion prevention to protect wired and wireless networks.

Optimized for the secure, wire-speed delivery of data, voice, and video, the Cisco 1800, 2800, and 3800 series of integrated service routers embed firewall protection, VPN, and IPS services for easier deployment and reduced operating costs.

**Cisco Dedicated Security Applications**
Cisco Security Agent provides behavior-based protection for servers and PCs and combines intrusion prevention, distributed firewall protection, spyware and malicious mobile code protection, endpoint inventory, NAC, and policy control of application use.

Cisco Secure Access Control Server (ACS) offers access management to ease networkwide authentication and authorization.

CiscoWorks VPN/Security Management Solution and CiscoWorks Security Information Management Solution offer centralized, scalable provisioning, monitoring, and reporting of security services.

## CISCO SELF-DEFENDING OVERVIEW

A Cisco Self-Defending Network provides a proactive defense against the primary security threats an organization will face, including worm and virus outbreaks, information theft, and denial of service (DoS) attacks. This poster details how integrated, system-level solutions from Cisco provide cost-effective protection against these and other critical threats for desktops, servers, applications, and networked resources.

### OUTBREAK PREVENTION

Virus and worm outbreak prevention requires a coordinated effort between traditional solutions and the network.

NAC and CCA combine network intelligence with endpoint security to prevent infection by helping to ensure that all devices comply with corporate security policy or are quarantined for remediation.

Firewall, VPN, intrusion prevention, and antivirus functions are embedded into network and security devices, allowing for the broadest distribution of security solutions. Network services, such as quality of service (QoS), network-based application recognition (NBAR), Weighted Fair Queuing (WFQ), and AutoSecure, also protect the flow of data during an outbreak.

Centralized management provides a topographical view of the network, identifies anomalous behavior and attack vectors, and allows for single-click attack mitigation.

www.cisco.com/go/outbreak

### THEFT OF INFORMATION

Protect against information theft from both external and internal sources using your existing investment in computing, network, and security platforms.

Components needed to prevent information theft include:

- VPN technologies that securely transport applications and information across untrusted networks
- Firewalls and intrusion detection functions that provide perimeter protection against unauthorized ingress and egress
- Access control servers that provide identity management for authentication, authorization, and accounting (AAA)
- NAC and Cisco Security Agent to help ensure that devices meet virus protection and device behavior criteria before network admission is granted

www.cisco.com/go/theft

### DISTRIBUTED DENIAL OF SERVICE

DoS attacks are among the most costly types of attacks for business continuity capabilities. The Cisco Traffic Anomaly Detector detects DDoS attack traffic and alerts the Cisco Traffic Anomaly Guard to take action. The Cisco Traffic Anomaly Guard diverts all traffic to the targeted system, filters out the malicious traffic, and forwards the legitimate traffic, enabling companies to continue business as usual. Cisco IOS® Software enables a router or switch to identify an attack and protect itself.

www.cisco.com/go/selfdefend

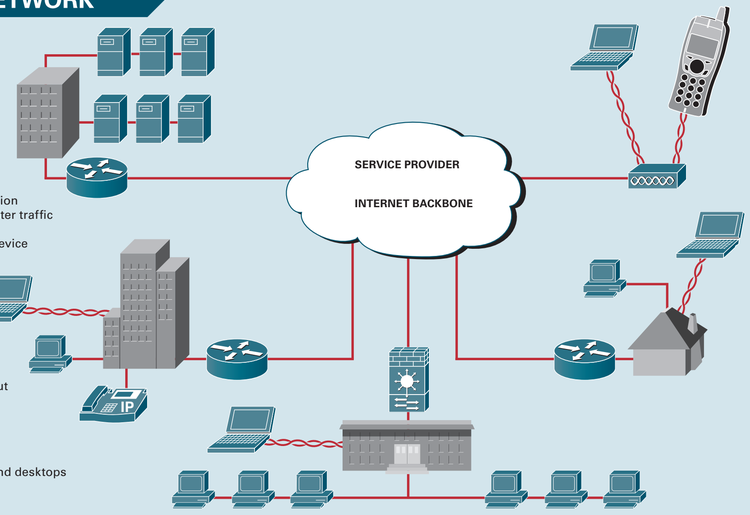
**THE CISCO SELF-DEFENDING NETWORK STRATEGY CONSISTS OF THREE SYSTEMS, EACH WITH A SPECIFIC PURPOSE.**

**Cisco Secure Connectivity Systems** use encryption and authentication capabilities to provide secure transport across untrusted networks. To protect data, voice, and video applications over wired and wireless media, Cisco offers IPSec, SSL, Secure Shell (SSH), and Multiprotocol Label Switching (MPLS)-based VPN technologies. Cisco wireless networks also support Wi-Fi Protected Access (WPA) and WPA2 for standards-based, interoperable WLAN security via the Cisco Wireless Security Suite. In addition, the extensive security capabilities integrated into Cisco wireless and IP telephony solutions help ensure the privacy of all IP communications.

**Cisco Threat Defense Systems** combine security solutions and intelligent networking technologies that identify and mitigate both known and unknown threats from inside and outside your organization. A threat defense system must include security that is integrated directly into routers, switches, and appliances, and must include solutions such as firewalls, network-based IPSs, DDoS attack protection, detection instrumentation, and traffic isolation techniques. Cisco Security Agent enables endpoint protection. The Cisco threat defense system provides comprehensive protection throughout the network—from the network data center, to the branch offices, and down to the endpoints. The Cisco Threat Defense System also integrates with the Cisco Structured Wireless-Aware Network (SWAN) wireless LAN Intrusion Detection System (IDS) to secure WLANs from malicious and unauthorized access—including rogue access points.

**Cisco Trust and Identity Systems** maintain the integrity of a network by making the network itself responsible for identification, authorization, and enforcement of security policy. Cisco trust and identity solutions include Cisco Secure ACS, AAA, identity-based network services (IBNSs), IEEE 802.1x, NAC, and Cisco Clean Access. These solutions are embedded in routers, switches, servers, and appliances, with selective components available for Cisco wireless LANs, to provide control of essential compliance activities, including user validation, verification of endpoint compliance with security policy, granting of tiered access rights, creation of quarantine and remediation zones for noncompliant devices, and the ability to dynamically block unauthorized access.

## SELF-DEFENDING NETWORK




**DATA CENTER SECURITY CHALLENGES**
- Protect confidential data
- Protect business critical applications
- Prevent security threats from outside and inside the organization

**DATA CENTER SECURITY SOLUTIONS**
- Software agents protect key servers and desktops
- Intrusion Prevention for Threat Protection
- Firewall appliances, switch modules filter traffic
- VPNs for secure communications
- Identity services manage authorized device and user access

**BRANCH SECURITY CHALLENGES**
- Protect business communications
- Prevent malicious traffic
- Adopting new network services without impacting performance
- Limited IT resources
- Provide secure WLAN connectivity

**BRANCH SECURITY SOLUTIONS**
- Software agents protect key servers and desktops
- Router embedded security services (Firewall, VPN, IPS)
- Router integrated VPN, IDS/IPS for high-performance secure connectivity and threat prevention
- Identity services manage authorized devices and user access
- Centralized management and analysis
- Cisco Wireless Security Suite and Cisco SWAN for end-to-end WLAN security

**CAMPUS SECURITY CHALLENGES**
- Identify and restrict access to authorized users
- Protect users (mobile and otherwise); isolate unauthorized or corrupt users
- Prevent security threats from outside and inside the organization
- Provide secure WLAN connectivity

**CAMPUS SECURITY SOLUTIONS**
- Software agents protect key servers and desktops
- Embedded security within switches (VLANs, DHCP Server Spoofing)
- Intrusion Prevention for Threat Protection
- Internal firewalls for critical area protection
- Identity servers for strong authentication
- Centralized management and analysis

**MOBILE WLAN SECURITY CHALLENGES**
- Wireless LANs for branch office, campus, and teleworker
- Ensure that only legitimate users access the network
- Protect data as it is transmitted across the WLAN
- Protect the network from active and passive WLAN attacks including rogue access points

**MOBILE WLAN SECURITY SOLUTIONS**
- Cisco Wireless Security Suite supporting WPA and WPA2
- WPA and WPA2 for 802.1X per-user authentication for secure access control and enterprise-class encryption for strong data privacy
- Cisco SWAN WLAN IDS to detect and mitigate unauthorized access points and network attacks

**TELEWORKER SECURITY CHALLENGES**
- Provisioning and managing 100s or 1000s
- Ensuring ease-of-use and supportability for non-technical remote employees
- Extending access to key applications
- Protecting endpoint devices

**TELEWORKER SECURITY SOLUTIONS**
- Software agents protect desktops
- Embedded security (Firewall, VPN, IPS) within low cost router
- Central site VPN gateways securely extend applications
- Easy VPN enables touchless provisioning
- Centralized management and analysis
- Secure WLAN connectivity with VPN






Part# 9563450412