OVERVIEW

CISCO SELF-DEFENDING NETWORKS

SECURITY IS A BUSINESS IMPERATIVE

The vast interconnected information networks of today are essential to maintain pace with business change, and also provide an opportunity for businesses to evolve to higher levels of performance and results. With information theft, virus attacks, and application abuse on the rise, it is critical for organizations to secure their business network and protect valuable resources. Whether it is employees and trusted insiders stealing information or hackers attempting to penetrate external network defenses, organizations of all sizes must protect themselves against information theft, virus outbreaks, and application abuse that come from known and unknown threats as well as internal and external sources. Clearly, network security is a business imperative.

IMPLEMENTING NETWORK SECURITY PRECAUTIONS

To mitigate and prevent information theft, organizations must implement precautions such as establishing formal organizational security policies, enforcing access rights to authenticated users, and securing the transport of data and voice communications. Technical decision makers face a variety of concerns about network security—whether it is the theft of confidential data or a virus outbreak, bringing down critical business applications and crippling employee desktops, or application abuse, starving valuable business resources and bandwidth. Additionally, they must face other concerns such as internal access control, contingency plans on how to overcome attacks, and overall network performance. A security system must be fully integrated into all aspects of the network to proactively recognize potential suspicious activity, identify threats, react adaptively, and facilitate a coordinated response to attacks.

THE CISCO SELF-DEFENDING NETWORK

The Cisco® Self-Defending Network protects an organization by identifying, preventing, and adapting to threats from both internal and external sources. With this protection, companies are better able to take advantage of the intelligence in their network resources—thus improving business processes and cutting costs. The Cisco Self-Defending Network identifies, prevents, and adapts to threats from both internal and external sources.

Three Standard Characteristics of the Cisco Self-Defending Network

Integration Standard

Every element in the network acts as a point of defense, and all the elements work together to provide a secure and adaptive system. Routers, switches, appliances, and endpoints incorporate security functions, including firewalling, virtual private networking, trust and identity capabilities, and intrusion prevention systems (IPSs). In addition, this standard incorporates technologies inherent in the secure operation of network devices such as control plane policing and CPU/memory thresholding.

Collaborative Standard

Various components of the network work together to provide new means of protection, and security becomes a system involving cooperation between endpoints, network elements, and policy enforcement. Network Admission Control (NAC) is an example of this principle, whereby endpoints are admitted to the network based on their adherence to security policy and enforced by network devices such as routers and switches.

Adaptive Standard

Adaptive security allows for automatic deployment of innovative behavioral methods in order to recognize new types of threats as they arise. Mutual awareness can exist between security services and network intelligence, thus increasing security effectiveness and a more proactive response to new types of threats. This mutual awareness effectively mitigates security risks by broadening threat recognition capabilities and addressing threats at multiple layers of the network.

BENEFITS OF THE CISCO SELF-DEFENDING NETWORK

- Improves flexibility and simplicity in network protection
- Improves IT management and efficiency
- Provides the ability to recognize suspicious activity, identify threats, and respond to attacks in a coordinated way
- Protects against users with insecure or infected devices
- Improves network uptime by responding to known and unknown threats in real time
- Protects corporate assets and reputation
- Effectively enforces security polices companywide

Technologies and Products Associated with the Cisco Self-Defending Network

- Day zero protection with Cisco Security Agent
- Access control with NAC
- Secure connectivity with IP Security (IPSec) VPNs
- Adaptive security appliance with stateful firewall, VPN, IPS, and antivirus
- CiscoWorks Management Solution

CISCO IS THE INDUSTRY LEADER IN NETWORKING AND SECURITY SOLUTIONS

Cisco Systems® provides the most comprehensive range of integrated security solutions to protect organizations of all sizes from theft. With a systemic approach to business security based on the collaboration of networking and security technologies and services, the Cisco Self-Defending Network integrates security intelligence, protects corporate assets, and enhances the value of an organization's existing network infrastructure.

FOR MORE INFORMATION

For more information about protecting your organization from virus outbreaks and the Cisco Self-Defending Network strategy, visit: http://www.cisco.com/go/midsizedsecurity or http://www.cisco.com/go/selfdefend

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205353.M_ETMG_KL_8.05

Printed in the USA