



CS – 1000 Multi-Homing Security Gateway

Phát minh ứng dụng mạng Internet ngày càng phát triển mạnh mẽ, đáp ứng nhu cầu giao dịch trao đổi thông tin ngày càng tăng. Nhưng vấn đề bảo mật cần được quan tâm khi giao dịch qua mạng Internet. Sản phẩm mới được PLANET đưa ra theo dòng Security Gateway là CS-1000, là thiết bị đặc biệt, sử dụng các thuật toán vết thông minh Heuristics Analysis để lọc bỏ các spam và virus mail, tự động cập nhật các nhận dạng spam, tích hợp sẵn sàng cơ chế diệt virus, worms và các dạng tấn công mạng theo nhiều dạng khác nhau từ mail.

Sản phẩm CS-1000 được cải tiến từ sản phẩm CS-500, kế thừa các tính năng cũ như Content Blocking khoá các địa chỉ URL, Scripts, IM/P2P, IPSec và PPTP VPN server, QoS, Authentication etc. Bên cạnh các chức năng trên, sự khác biệt đầu tiên là CS-1000 hỗ trợ 2 đường WAN cho phép cân bằng tải outbound và khả năng sẵn sàng cao đối với 2 nhà cung cấp khác nhau. Hơn nữa, chức năng liên kết VPN Trunk hỗ trợ tính chịu lỗi và cân bằng trên đường truyền VPN, cho phép đường truyền giảm độ trễ tới mức tối đa.

Chất lượng PLANET luôn đảm bảo CS-1000 hiệu năng firewall qua VPN là cao nhất. Hơn nữa, bên trong tích hợp cơ chế IDP và firewall đối với tận từng gói tin truyền thông chống tấn công mạng dưới mọi hình thức khi giao dịch qua Internet hay Intranet. Tất cả tập trung trong 1 thiết bị an ninh mạng đáp ứng các ứng dụng doanh nghiệp.

>>> Mô hình ứng dụng

Giải pháp cho trụ sở nhỏ và chi nhánh

Thiết bị CS-1000 cho phép lọc thư mail hai chiều (Incoming và Outgoing), dù bạn cài đặt mail server ở trong mạng LAN, DMZ hay ngoài Internet, người dùng trong mạng luôn được bảo vệ tốt bởi hệ thống an ninh CS-1000. Người dùng trong mạng hoàn toàn an tâm khi thiết bị hỗ trợ tương thích nhiều mô hình mạng.



- **Anti-Spam Filtering:** Bảo vệ an toàn mạng đa mức đa chức năng (Head Analysis, Text Analysis, Blacklist & Whitelist, Bayesian Filtering, Spam Fingerprint, kiểm tra tài khoản người gửi và địa chỉ IP address), và thuật toán tìm vết xử lý nhanh chóng loại bỏ tới 95% spam mail. Hỗ trợ các báo cáo và nhật ký theo nhu cầu người quản trị. Các hình thức kích hoạt chống spam mail gồm: Xoá, Phục hồi, hay chuyển gửi đi. Tích hợp sẵn hệ thống tự động cập nhật các nhận dạng spam mail liên tục
- **Anti-Virus Protection:** Tích hợp sẵn chức năng lọc virus, dò tìm các phần mềm có khả năng nguy hại từ email. Hệ thống lọc mail theo nội dung tương thích nhiều giao thức SMTP, POP3 theo thời gian thực hiệu quả cao. Hỗ trợ các hình thức báo cáo, cảnh báo theo nhu cầu người quản trị
- **VPN Connectivity:** Thiết bị an ninh mạng hỗ trợ kết nối VPN theo các giao thức PPTP theo mô hình server/client và bảo mật IPSec. Bảo mật mạng với xác thực SHA-1 / MD5, mã hoá DES, 3DES và AES đảm bảo giao thông trên mạng Internet công cộng
- **VPN Trunk:** Chức năng VPN trunk hỗ trợ cân bằng tải kết nối và chịu lỗi cao nâng cao chất lượng đường truyền.
- **Content Filtering:** An ninh mạng khoá một số kết nối dựa vào địa chỉ URLs, mã Scripts (Pop-up, Java Applet, cookies và Active X), P2P (eDonkey, Bit Torrent và WinMX), dịch vụ nhắn tin (MSN, Yahoo Messenger, ICQ, QQ, Skype) và Download. Khi phiên bản P2P hay dịch vụ nhắn tin cập nhật phiên bản mới, CS-1000 tự động cập nhật và xử lý theo cơ chế mới
- **IDP:** CS-1000 hỗ trợ 3 hình thức xác nhận theo cơ chế chống xâm nhập, người dùng có thể cấu hình ở chế độ "Anomaly", "Pre-defined" và "Custom" phù hợp với cấu hình mạng hiện tại
- **Chống Virus đối với HTTP, FTP, P2P, IM, NetBIOS:** Thiết bị CS-1000 không chỉ chống virus đối với mail, nó còn lọc virus theo các giao thức. Các dạng virus được cập nhật tự động thường xuyên
- **Policy-based Firewall:** Tích hợp cơ chế tường lửa chống nhiều dạng tấn công bao gồm SYN attack, ICMP flood, UDP flood, Ping of Death, etc. Điều khiển truy nhập cho phép một số người dùng truy cập WAN hay LAN theo thời gian cài đặt
- **QoS:** Các gói tin được phân loại dựa theo địa chỉ IP, mạng con hay cổng TCP/UDP và cơ chế ưu tiên băng thông theo 3 mức xác định
- **Authentication:** Cơ chế xác thực cho phép người dùng trên giao diện Web. Cơ sở dữ liệu người dùng được cấu hình trên các thiết bị mạng kết hợp đi kèm với RADIUS server
- **WAN Backup:** Thiết bị CS-1000 cung cấp các tính năng quan sát trạng thái đường link WAN đang hoạt động và đường links dự phòng. Các trạng thái có thể dựa theo bảng địa chỉ Internet
- **Multiple NAT:** Multiple NAT cho phép nhiều mạng con truy cập Internet thông qua 1 cổng giao tiếp duy nhất với nhiều địa chỉ WAN

Product	
Description	Multi-Homing Security Gateway
Model	CS-1000
Hardware	
Ethernet	LAN: 1 x 10/100 Base-TX RJ-45 WAN: 2 x 10/100 Base-TX RJ-45 DMZ: 1 x 10/100 Base-TX RJ-45
Power	100~250 VAC, 50~60 Hz, 0.6A
Operating Environment	Temperature: 0 ~ 60 DegreeC Relative Humidity: 5% ~ 95%
Dimension	237 x 440 x 43 mm
Regulatory	FCC, CE Mark
Software	
Management	Web
Network Connection	Transparent, NAT, Multi-NAT
Routing Mode	Static Route, RIPv2
Concurrent Sessions	110,000
New session / second	10,000
Email Capacity per Day	120,000
Firewall Throughput	100Mbps
3DES Throughput	17Mbps
Firewall	Policy-based Firewall rule with schedule, NAT/ NATP, SPI Firewall
VPN Tunnels	100/200
VPN Function	PPTP server and client, IPSec DES, 3DES and AES encrypting SHA-1 / MD5 authentication algorithm Remote access VPN (Client-to-Site) and Site to Site VPN VPN Trunk
Content Filtering	URL Blocking Blocks Popup, Java Applet, cookies and Active X P2P Application Blocking Instant Message Blocking Download Blocking
IDP	Anti-Virus for HTTP, FTP, P2P, IM, NetBIOS Automatic or manual update virus and signature database Anomaly: Syn Flood, UDP Flood, ICMP Flood and more Pre-defined: Backdoor, DDoS, DoS, Exploit, NetBIOS and Spyware Custom: User defined based on TCP, UDP, ICMP or IP protocol
Scanned Mail Settings	The allowed size of scanned mail : 10 ~ 512KBytes
Anti-Virus	Email attachment virus scanning by SMTP, POP3 Inbound scanning for internal and external Mail Server Action of infected mail: Delete, Deliver to the recipient, forward to an account Automatic or manual update virus database
Anti-Spam	Inbound scanning for external and internal Mail Server Support Spam Fingerprint, Bayesian filtering, checking sender account and IP to filter the spam mail Black list and white list support auto training system Action of spam mail : Delete, Deliver to the recipient, forward to an account
QoS	Policy-based bandwidth management Guarantee and maximum bandwidth with 3 priority levels Classify traffics based on IP, IP subnet, TCP/UDP port
User Authentication	Built-in user database with up to 200 entries Support local database, RADIUS and POP3 authentication
Logs	Log and alarm for event and traffic Log can be saved from web, sent by e-mail or sent to syslog server
Accounting Report	Record inbound and outbound traffic's utilization by Source IP, Destination IP and Service
Statistics	Traffic statistic for WAN interface and policies, Graphic display
Others	Dynamic DNS, NTP support, DHCP server, Virtual server

