Spolehlivá ochrana

Bezpečnostní brány

S rostoucí nebezpečností internetu se síťová bezpečnost stává jednou z klíčových otázek při řešení síťové infrastruktury. Pro vyřešení a zvýšení bezpečnosti PLANET nabízí řešení jak účinně chránit počítačové sítě.

Řešení zahrnují základní brány, brány s rozšířenými funkcemi včetně VPN, brány s automatickou detekcí napadení (IDP), anti-virové brány, anti-spam brány, brány s filtrací obsahu.

Bezpečnostní brány nejenom chrání sítě, ale rovněž poskytují další funkce, které zjednodušují administraci a poskytují přidanou hodnotu. Typicky jde o schopnost automatického zálohování připojení, detailní záznamy o komunikaci, statistické funkce, integrované VPN prostřednictvím Web SSL přístupu.

■ Úplné řešení

PLANET nabízí ve svých zařízeních řešení síťové bezpečnosti pro velké i malé sítě. Řeší otázku bezpečnosti od malých routerů pro širokopásmové připojení po velké a komplexní zařízení. Zařízení jsou vybavena kvalitními firewally. Navíc však přidávají řadu dalších funkcí:

■ Řízení přenosového pásma

PLANET do svých bran zabudoval kompletní management řízení přenosového pásma, které dovoluje omezovat nebo priorizovat účastníky nebo typy síťové komunikace.

■ Automatické zálohování připojení

Jednotky jsou schopny poskytovat současné připojení na více různých poskytovatelů internetu. To přináší výrazné zvýšení robustnosti a spolehlivosti.

■ Snadné vytváření VPN

Vytvoření bezpečně šifrovaného připojení do firmy zvládne s produkty PLANET i laik. Zavedením funkce SSL VPN je vytvoření propojení záležitostí vteřin, samozřejmě znáte-li své přístupové heslo...

■ Ochrana před viry

Brány chrání sítě před viry v přicházející elektronické poště. Zprávy, které přes ně procházejí jsou kontrolovány na přítomnost virů a je s nimi naloženo dle přání správce.

■ Redukce nevyžádané pošty

Rovněž mají brány zabudovánu ochranu proti obtěžující a nevyžádané elektronické poště. Brány automaticky kontrolují obsah, zprávy a jsou schopny rozpoznat i se naučit rozpoznat, které zprávy jsou pro uživatele obtěžující. Rovněž dle jeho přání tyto zprávy vyřazují nebo archivují.

■ Automatická detekce napadení

Bezpečnostní brány jsou schopny na základě signatur známých útoků rozpoznávat napadení sítě. Jakmile detekují napadení, zjistí jeho zdroj a pokud jim to uživatel dovolil, tak jej i zablokují.

■ Filtrace obsahu

Díky filtraci obsahu má správce sítě možnost vyblokovat nežádoucí typy komunikací. Typicky se jedná o možnost blokace služeb pro Internet Messaging nebo nelegální stahování softwaru a videa prostřednictvím P2P výměnných sítí.

■ Minimální nároky na obsluhu

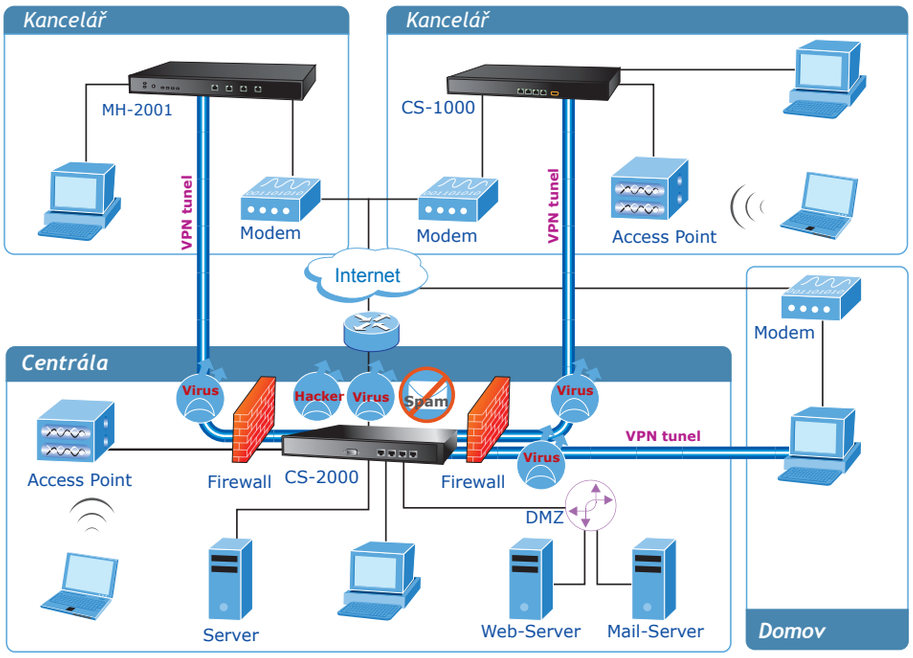
Zařízení jsou vybavena web managementem a poskytují grafický přehled v prováděných činnostech. Není nutný speciální trénink obsluhy.

Aplikace

❖ Instituce, úřady, školy

Síťová bezpečnost je ve státních institucích na prvním místě. PLANET MH-2001 jsou speciálně navržena pro toto prostředí. Zabraňují, aby sítě byly napadány poštovními viry a zaneřáděny neužitečným spamem.

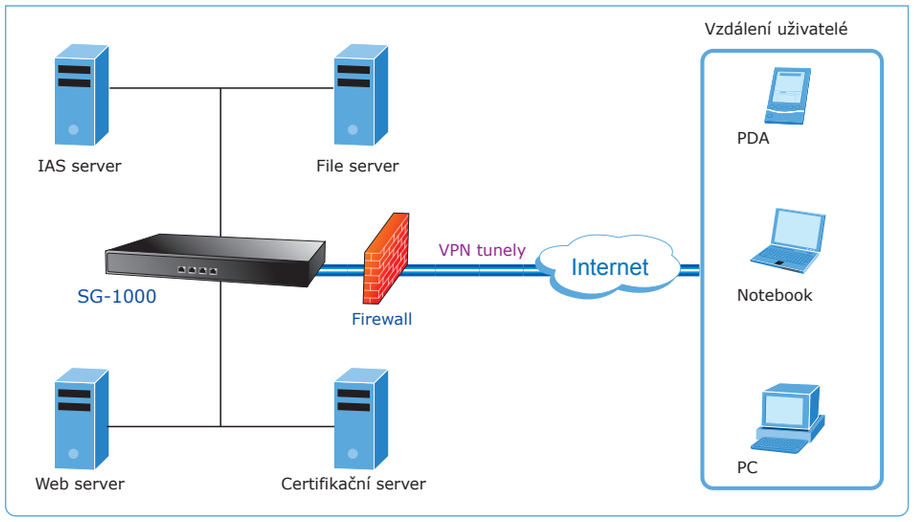
Navíc díky detekci napadení (Intrusion Detection System), uživatelské autorizaci spojení a filtraci obsahu vytvářejí automaticky velmi bezpečné síťové prostředí. Jednotky CS-2000 poskytují také řešení pro VPN pomocí IPSec, SSL VPN a PPTP VPN.



❖ VPN přístupy do podniku

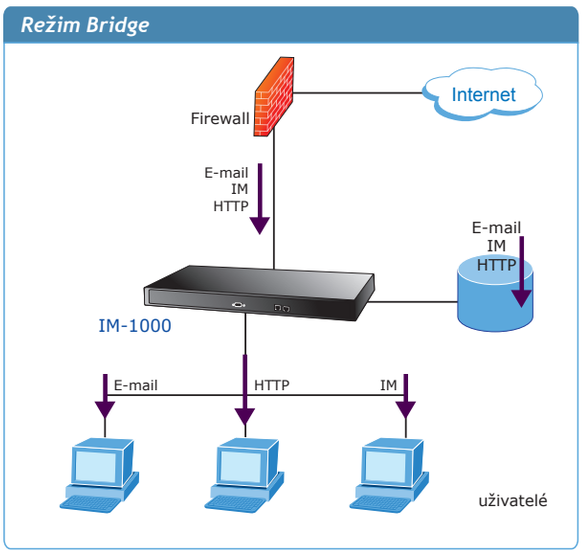
Jednotky řady SG-1000 poskytují bezproblémové vytváření VPN přístupů. Speciálně navržené vytváření VPN pomocí SSL umožňuje vytvoření připojení pro vzdálené uživatele během vteřin s minimálními znalostmi a potřebovat budou jen internetový prohlížeč.

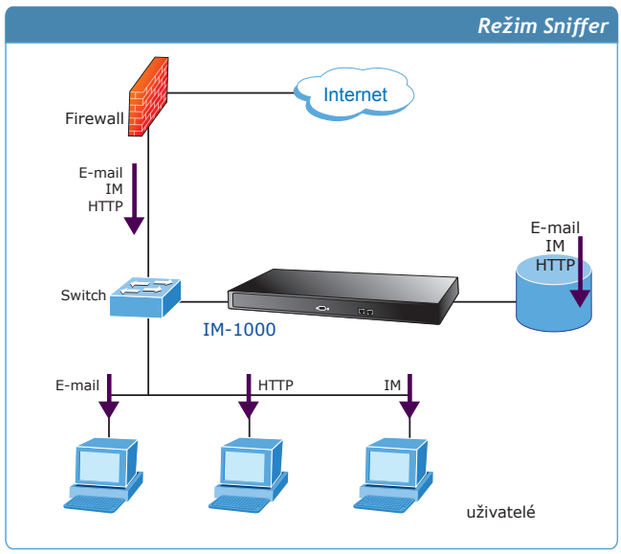
SG-1000 také nabídne funkce filtrace obsahu, blokování určených URL, skriptů, IM, P2P a nežádoucího stahování souborů. Má také implementován detektor anomálií sítě a je schopna odhalit zavirované stroje.



❖ Monitorování komunikace v podniku

Pro zvýšení produktivity práce bylo vyvinuto zařízení IM-1000, které trvale zaznamenává komunikaci prováděnou zaměstnanci v podniku. Avšak samotné hromadění dat by bylo k ničemu. IM-1000 je přehledně zpřístupňuje pro pozdější analýzu. Dává možnost nahlédnout jak do statistických přehledů tak i do konkrétních zpráv a komunikace uživatele. Monitoruje populární služby jako je poštovní komunikace SMTP/POP3, on-line komunikace jako MSN, ICQ, Yahoo Messenger. Monitoruje prohlížené web stránky (HTTP), stahované soubory přes FTP a terminálovou komunikaci TELNET. Tím zabraňuje zaměstnancům v aktivitách, které s jejich pracovní činností nesouvisí.

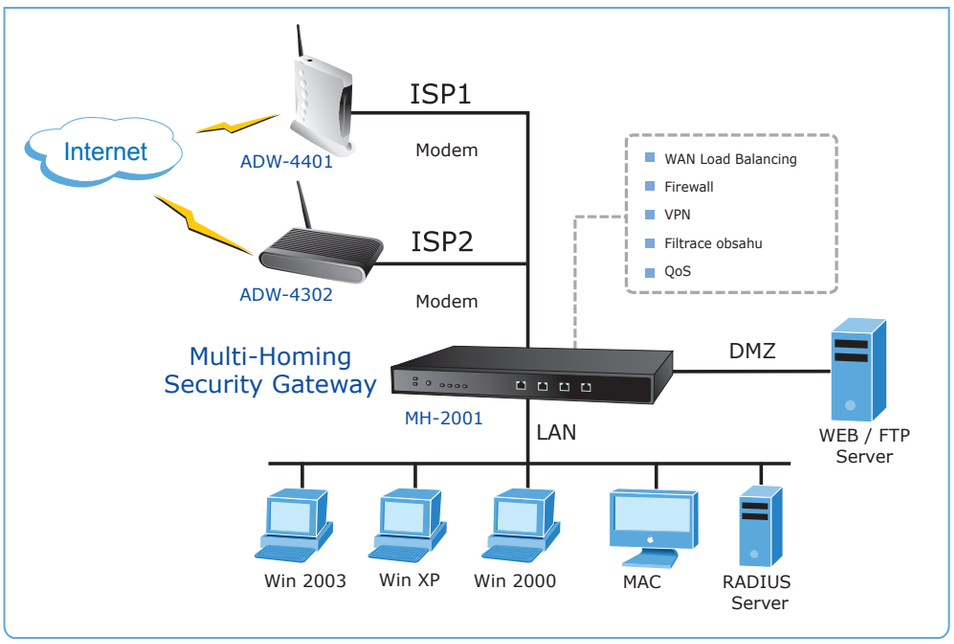




❖ Malé sítě

Řešení Multi-Homing Security Gateway MH-2001 integruje v jediném zařízení schopnost vícenásobného připojení k internetovým poskytovatelům, QoS a řízení pásma, vytváření VPN, autorizační funkci a firewall.

Je ideálním řešením pro malé sítě s požadavkem na nízkou cenu realizace vzdáleného přístupu k aplikacím a robustního internetového připojení.



Bezpečnostní brány

Multi-Homing Security Gateway

Řada	Model	MH-1000	MH-2001	MH-5001
	Foto			
	Rozměr	Stolní zařízení	Stolní zařízení	do 19" rozvaděče
Síťové rozhraní	Rozhraní	8 x LAN, 2 x WAN	1 x LAN, 2 x WAN, 1 x DMZ	2 x LAN, 2 x WAN, 1 x DMZ (definovatelné uživatelem, až 4x WAN)
	Max. počet spojení	10,000	45,000	300,000
Management	Management	Web	Web	Web, SNMP, HTTPS, Telnet
Bezpečnost	SPI Firewall	■	■	■
	DoS / DDoS prevence	■	■	■
	P2P, IM blokace	-	■	■
	Povoleni/zakázání stahování	-	■	Jen stahování
	Autorizace připojení Interní databáze	-	200 entries	200 entries
	RADIUS	-	■	■
	POP3 autorizace	-	■	■
	FTP filtr	-	-	■
	E-mail filtr	-	-	■
	Filtrace obsahu	■	■	■
VPN	VPN spojení	100	200	2,000
	IPSec VPN (DES, 3DES, AES)	■	■	■
	VPN Hub	-	-	■
	PPTP Server / Klient	■	■	■
Ostatní	Odchozí Load Balancing	■	■	■
	Příchozí Load Balancing	■	-	-
	Bandwidth management	■	■	■
	High Availability	-	-	■
	Transparentní spojení	-	■	■
	Více NAT podsítí	-	■	■
	Server Load Balancing	-	4 skupiny	4 skupiny

Broadband Router

Řada	Model	XRT-401D	XRT-401E	XRT-412	XRT-501	VRT-311S	VRT-401	VRT-401G
	Foto							
Síťové rozhraní	Rozhraní	1 x WAN, 4 x LAN	1 x WAN, 4 x LAN	1 x WAN, 4 x LAN, 2 x USB	1 x WAN, 4 x LAN (všechny porty Gigabitové)	1 x WAN, 3 x LAN, 1 x DMZ	1 x WAN, 4 x LAN, 1 x DMZ	1 x WAN, 4 x LAN, 1 x WiFi
	Bezdrátové rozhr.	-	-	-	-	-	-	IEEE 802.11 b/g
VPN	IPSec/PPTP	-	-	-	-	■	■	■
	IPSec VPN spojení	-	-	-	-	10	100	10
	Umožňuje VPN	■	■	■	■	■	■	■
Bezpečnost	SPI Firewall	■	■	■	■	■	■	■
	Filtrace obsahu	-	-	-	■	■	■	■
	ACL	■	■	■	■	■	■	■
	URL filtr	■	■	■	■	■	■	■
Ostatní	DMZ	■	■	■	■	■	■	■
	DDNS	■	■	■	■	■	■	■
	Virtual Server	■	■	■	■	■	■	■
	QoS	-	-	-	■	-	-	-
	LPR Printer Server	-	-	■	-	-	-	-

VPN Security Gateway

	Model	SG-500	SG-1000
Řada	Foto		
	Rozměr	Stolní	do 19" rozvaděče
Síťové rozhraní	Rozhraní	1 x LAN, 1 x WAN, 1 x DMZ	1 x LAN, 2 x WAN, 1 x DMZ
	Max. počet spojení	20,000	110,000
Bezpečnost	Firewall	■	■
	Autorizace připojení	■	■
	RADIUS	■	■
	Filtrace obsahu	■	■
	URL filtrace	■	■
	Upozornění na útok	■	■
	DoS, DDoS prevence	■	■
VPN	VPN tunelů	100/200	100/200
	VPN propustnost	10 Mbps	17 Mbps
	Šifrování	DES, 3DES, AES	DES, 3DES, AES
	IPSec autentifikace	SHA-1, MD5	SHA-1, MD5
	SSL VPN	■	■
	SSL VPN tunelů	5	50
Ostatní	WAN Load Balancing	-	Round-Robin, traffic, packet, session
	QoS	■	■
	Transparentní DMZ	■	■
	Statické routování	■	■
	NAT, PAT	■	■
	H/W Watch-Dog	■	■

Bandwidth Management Gateway

	Model	BM-525	BM-2101
Řada	Foto		
Síťové rozhraní	Rozhraní	1 x LAN, 1 x WAN, 1 x DMZ	1 xLAN, 2 x WAN, 1 x DMZ
	Max. počet spojení	20,000	241,000
Management	Pracovní režimy	NAT, Transparentní	NAT, Transparentní
	Management	Web	Web, SNMP
Šířka pásma	Řízení přensoového pásma	Garantované a maximální pásmo	Garantované a maximální pásmo
	Propustnost	Jen NAT: 25 Mbps Při NAT + logování + statistiky: 9 Mbps	100 Mbps
Bezpečnost	Pravidlový firewall	■	■
	URL filtr	■	■
	Virtuální Server/DMZ	■	■
	Detekce anomálií sítě	■	■
	Blokace P2P	■	■
	Blokace IM	■	■
	Blokace stahování souborů	■	■
	Vestavěná autorizační databáze	■	■
Ostatní	Server Load Balancing	4 IP adresy	4 IP adresy
	Statistiky WAN a jednotlivých politik řízení	■	■
	Zálohování statistik	-	■

Bezpečnostní brány

UTM Content Security Gateway

Řada	Model	CS-1000	CS-2000
	Foto		
Síťové rozhraní	Rozhraní	2 x WAN, 1 x LAN, 1 x DMZ	2 x WAN, 1 x LAN, 1 x DMZ (DMZ port může být nastaven jako WAN3)
	Max. počet spojení	110,000	582,000
	New Sessions / Second	10,000	20,000
Propustnost	Firewall	100 Mbps	100 Mbps
	VPN při 3DES	17 Mbps	30 Mbps
VPN	VPN tunelů	100/200	200/1000
	SSL VPN tunelů	-	200
Bezpečnost	IDP	■	■
	IDP hlášení a statistiky	-	■
	Email filtr	POP3, SMTP	POP3, SMTP
	Autorizace uživatelů	lokální databází, RADIUS, POP3	lokální databází, RADIUS, POP3, LDAP
	Anti-Virus	1 (Clam)	2 (Clam a Sophos)
	Akce Anti-viru	Smaž, Doruč a upozorni, Přesměruj	Smaž, Doruč a upozorni, Přesměruj, Ulož do karantény
	FTP/HTTP Anti-Virus	■	■
	Upozorňování Antiviru Emailem	■	■
	Akce Anti-Spamu	Smaž, Doruč a upozorni, Přesměruj	Smaž, Doruč a upozorni, Přesměruj, Ulož do karantény
	Zasílání Spam přehledů Emailem	-	■
	Spam a Ham trénování sytému	■	■
Ostatní	QoS, propustnost	50	100
	WAN Load Balancing	Odchozí	Odchozí / Příchozí
	Email účty	-	■
	High Availability	-	■
	Záznamy o událostech	■	■
	Podpora Syslog	■	■
	Statistické přehledy účtů uživatelů	■	■
	Statistické přehledy rozhraní	WAN a jednotlivá pravidla	WAN a jednotlivá pravidla