Cyberoam NG Series UTM Firewall

Nejvýkonnější UTM firewall v SMB/SOHO segmentu

Snadná dostupnost vysokorychlostního internetu a zařízení pro vysokorychlostní sítě dnes umožňují i malým podnikům dovolit si výkonnou IT infrastrukturu. Jediným slabým článkem řetězu byla vždy bezpečnostní zařízení. Zapomeňme však na to, co bylo, přichází budoucnost v podobě Next Generation UTM Firewallů firmy Cyberoam!

Otevřete dveře budoucnosti

Společnost Cyberoam uvádí na trh své UTM firewally nové generace, s jejichž pomocí můžete konečně využít potenciál své sítě a internetového připojení. Všechny modely NG Series Vám totiž nabízí propustnost od 1Gbps. Díky zcela novému hardwaru s vícejádrovými procesory a novým operačním systémem CyberoamOS, který je optimalizován pro vysoký výkon nových appliancí, získáte nejrychlejší zařízení v kategorii SMB/SOHO/ROBO produktů. Nově můžete využívat SSL VPN spojení na všech New Generation Series appliancích, a to již od nejnižšího modelu. High Avalibility mód a Web Application Firewall jsou nyní dostupné na všech modelech kromě CR15iNG/15wiNG.

Klíčové přínosy

- ⇒ **Nejrychlejší UTM firewall ve své třídě.**
- ⇒ Ekonomické a zároveň vysoce funkční řešení pro komplexní zabezpečení perimetru sítě.
- ⇒ Definice politik dle identity uživatelů a aplikací (IM, P2P, Skype, hry, Facebook, ...)
- ⇒ Certifikace Common Criteria EAL4+.
- ⇒ Kontrola HTTPS.
- ⇒ Podpora připojení více ISP.
- ⇒ SSL VPN.
- ⇒ Podpora 3G modemů.
- ⇒ Podpora Wi-Fi.
- ⇒ Zapojení jako gateway / bridge umožňuje zachovat / využít stávající infrastrukturu.
- ⇒ Vestavěný nástroj pro analýzu provozu v reálném čase.
- ⇒ Reporty zdarma přímo na zařízení (dle identity, ...)
- ⇒ Jednoduché licencování.
- ⇒ Dostupný také ve formě virtuální appliance

K dispozici centrální management

Ideální řešení bezpečnosti pro malé a střední společnosti

Cyberoam poskytuje komplexní a vysoce spolehlivé zabezpečení vstupu do vnitřní sítě organizace za zlomek obvyklých nákladů. Chrání komerční firmy i veřejné instituce proti hrozbám zevnitř i vně sítí, jako jsou spam, spyware, phishing, pharming, viry, červi, trojani, DoS útoky, VoIP útoky, krádeže dat přes IM a další. Další výhodu pak představuje **dostupnost řešení v podobě virtuální appliance** s jednoduchým licencováním per CPU core.

Víte, co kdo dělá ve Vaší síti?

Integrujte jednoduše Cyberoam s MS AD, s jinou adresářovou strukturou nebo si vytvořte vlastní přímo na zařízení. Politiky, jako např. jaké aplikace může uživatel spouštět (IM apod.), jaký obsah využívat, kdy se může připojit vzdáleně, jakou šířkou pásma smí do internetu nebo jaký objem dat může stáhnout či uploadovat, uplatníte na uživatele, ať je kdekoliv. Pokud nechcete využít propojení s identitou uživatelů, poskytuje Cyberoam stejné funkce jako standardní firewally.

COMGUARD security & networking
COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

Cyberoam
A SOPHOS Company

NG Future-ready

Model	15iNG / 15wiNG	25iNG / 25wiNG	35iNG / 35wiNG	50iNG	100iNG	200iNG/XP	300iNG/XP
Typ hardwaru	malý box	malý box	malý box	střední box	střední box	střední box	střední box
1GbE cooper porty	3	4	6	8	8	10/6	10/6
Flexi Ports for XP appliances 1 GbE Cooper/1 GbE SPF/10 GbE SPF	-	-	-	-	-	8/8/4	8/8/4
USB porty / HW bypass segmenty	2/-	2/-	2/-	2 / 2	2 / 2	2 / 2	2 / 2
Konfig. Internal/DMZ/WAN porty	ano	ano	ano	ano	ano	ano	ano
Propustnost UDP/TCP (**Gbps**)	1 / 0,75	1,5 / 1	2,3 / 2	3,25 / 3	4,5 / 3,5	10 / 8	12 / 9,5
Propustnost IPS/UTM (Mbps)	**140 / 80**	**200 / 110**	**350 / 210**	**750 / 550**	**1 200 / 750**	**2 000 /1 200**	**2 400/1 500**
IPSec/SSL VPN propustnost (Mbps)	110 / 50	210 / 75	250 / 100	400 / 300	450 / 400	800 / 450	1 200 / 500
Současná/nová spojení za ses. (tis.)	60 / 3,5	150 / 5	350 / 11	1 000 / 30	1 250/ 45	1 500 / 70	2 000/ 85
Anti-Virus/WAF propustnost (Mbps)	180 / -NA-	300 / 100	525 / 150	1 000 / 450	1 400 / 700	2 200/1000	2 600/1250

Funkce & vlastnosti

Firewall
- Firewall s „8. vrstvou" (uživatel – identita)
- Multizónová bezpečnost s různými pravidly pro každou zónu
- Přístupová pravidla založena na kombinaci uživatel/ zdroj&destinace/ MAC a IP adresa/ služba
- Akce zahrnují kontrolu dle politik pro IPS, webový a aplikační filtr, A-Virus, A-Spam a řízení šířky pásma
- Kontrola a rozpoznávání aplikací v pravidlech a jejich podrobné řízení (např. IM bez přenosu souborů)
- Rozvrhování času pro přístupy
- Source & Destination NAT dle politik
- H.323 NAT Traversal
- Podpora 802.1q VLAN
- Ochrana proti DoS&DDoS útokům
- MAC & IP-MAC filtrace a prevence spoofingu

Wi-Fi (CR15wiNG/25wiNG/35wiNG)
- Standardy: IEEE 802.11 a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, AES, PSK, 802.1x EAP)
- Anténa: Detachable 3x3 MIMO
- Přístupové body: do 8 bssid
- Vysílaný výkon (EIRP): 11n HT40 : +15dBm, 11b CCK: +15dBm, 11g OFDM:+15dBm
- Citlivost přijímače: -68dBm at 300Mbps, -70dBm at 54Mbps, -88dBm at 6Mbps
- Frekvenční rozsah: Europe (ETSI): 2.412GHz ~ 2.472GHz
- Počet volitelných kanálů (ETSI): 13
- Rychlost přenosu dat: 802.11n: up to 450Mbps, 802.11b: 1, 2, 5,5, 11Mbps, 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps

Wireless WAN
- Podpora 3G a Wimax přes USB port
- Primární / záložní WAN link

Anti-Virus&Spyware
- Integrovaný AV kontroluje HTTP/ HTTPS/ FTP/ SMTP/ POP3/ IMAP/ IM/ VPN tunely
- Kontrola SSL šifr. provozu dle politik
- Detekuje a odstraňuje viry, červi a trojany
- Ochrana proti Spywaru/Malwaru/Phishingu
- Automatické aktualizace databáze signatur
- Kontrolu lze přizpůsobit uživateli/skupině
- Karanténa na zařízení s možností uživatelského přístupu *
- Kontrola a doručování dle velikosti souboru
- Blokování dle typu souboru
- Vkládání „disclaimeru"/podpisu

Anti-Spam
- Filtrace příchozí/odchozí pošty **
- Integrován systém Commtouch s Recurrent Pattern Detection technologií,
- Filtrace dle hlavičky/velikosti/odesilatele/ příjemce,
- Real-time Blacklist, kontrola MIME hlavičky
- Karanténa na zařízení s možností uživatelského přístupu s oznamováním přes „Digest" *
- Označování předmětu zprávy
- Blacklist/Whitelist pro IP adresy
- Přesměrování spamu na jinou email adresu
- Filtr obrázkového spamu RPD technologií
- Antivirová ochrana v čase nula
- Filtrace spamu dle reputace IP adresy

IPS – prevence narušení
- Signatury: Default (4500+) / uživatelské
- IPS Politiky: kolektivní / uživatelské
- Vytváření politik pro jednotlivé uživatele
- Automatické aktualizace v reálném čase
- Detekce anomálií v provozu
- Prevence DDoS útoků

Webový filtr
- Vestavěná databáze web kategorií
- Blokuje URL, klíčová slova, typy souborů
- Kategorie: Default(82+) / uživatelské
- Podporované protokoly: HTTP, HTTPS
- Blokuje Malware/Phishing/Pharming URL
- Alokace a priorizace šířky pásma dle kategorií
- Nastavitelné upozornění pro každou kategorii
- Blokuje JavaApplety, Cookies, Active X
- Shoda s CIPA
- Prevence úniku dat přes HTTP/HTTPS upload
- Časová a objemová nastavení / kvóty pro uživatele

Aplikační filtr
- Vestavěná databáze aplikačních kategorií (např. hry, IM, P2P, Proxy, ...)
- Časová nastavení / rozvrhování pro uživatele
- Blokuje P2P aplikace (např. Skype) externí proxy a anonymizéry (např. Ultra Surf), aktivity typu „volání domů", zloděje hesel
- Důkladná kontrola a řízení 7. vrsty (aplikace) a „8. vrstvy" (uživatel - identity)

Web Application Firewall
- Positive Protection model
- Unikátní technologie „Intuitive Website Flow Detector"
- Ochrana před SQL injekcemi/ XSS/ Session Hijacking/ manipulacemi s URL a cookies
- Podpora http 0.9/1.0/1.1
- Podpora 5-200 back-end serverů
- Detailní logování a reporting

Instant Messaging (IM)
- Podpora Yahoo a Win Live Messenger
- Antivirová kontrola / obsahový filtr
- Povolení/blokace pro: přihlášení/ přenos souborů/ webové kamery/ 1 na 1 nebo skupinový chat
- Logování IM aktivit
- Archivace přenášených souborů
- Nastavitelná upozornění

VPN brána
- IPSec, L2TP, PPTP,
- Šifrování - 3DES, DES, AES, Twofish, Blowfish, Serpent
- Hash algoritmus - MD5, SHA-1
- Autentizace: Preshared Key, certifikáty
- IPSec NAT Traversal
- Detekce mrtvých připojení a podpora PFS
- Diffie Hellman skupiny - 1,2,5,14,15,16
- Podpora externích certifikačních autorit
- Export nastavení VPN připojení mob. klienta
- Podpora doménových jmen pro tunely a koncové body
- Redundance VPN připojení
- Podpora překrývání sítí
- Podpora „Hub & Spoke VPN"

SSL VPN *
- Tunelování TCP & UDP,
- Autentizace: AD, LDAP, RADIUS, Cyberoam
- Víceúrov. autentizace klienta: certifikát, jméno a heslo
- Politiky dle uživatelů či skupin
- Přístup do sítě: „Split and Full tunelling"
- Přístup přes webový prohlížeč (portál) – bezklientský přístup
- Tenký klient pro SSL VPN
- Podrobná kontrola přístupu ke zdrojům v síti
- Administrativní kontroly: Session timeout, detekce mrtvých spojení, upravitelný portál
- Přístup k aplikacím založený na TCP – HTTP, HTTPS, RDP, TELNET, SSH

IPSec VPN klient ***
- Vyhovuje IPSec, kompatibilní se všemi hlavními IPSec VPN branami
- Podpora Windows 2000, XP 32/64-bit, 2003 32-bit, 2008 32/64-bit, Vista 32/64-bit, 7 RC1 32/64-bit, 8 RC1 32/64-bit
- Import konfigurace spojení

Networking
- Podpora připojení / distribuce datového toku přes více ISP
- Failover: automatický Failover/Failback, Multi-WAN failover, 3GModem failover
- Load balancing založený na WRR
- Přidělování IP adres: statické, PPPoE, L2TP, PPTP & DDNS Client, Proxy ARP, DHCP Server, DHCP relay
- Směrování (routing) dle aplikace/uživatele
- Podpora pro nasazení jako HTTP Proxy
- Podpora „Parent Proxy" s FQDN
- Dynamické směrování: RIP v1&v2/OSPF/ BGP/Multicast Forwarding
- Podpora IPv6 (Gold Logo)

Řízení šířky pásma
- Management dle identit, aplikací, nebo kategorií
- Garance minima/sdílení nevyužitého pásma
- Průzkum provozu dle aplikací/identity *

Reportování i pro více WAN připojení

Autentizace uživatele
- Lokální databáze / Integrace s Active Directory
- Automatický Windows Single sign-on
- Integrace s externí LDAP/RADIUS databází
- Podpora tenkého klienta: MS Windows Server 2003 Terminal Services, Citrix XenApp
- Podpora RSA SecureID
- Externí autentizace pro uživatele a administrátory
- Vazba na uživatele/MAC adresu
- Podpora různých autentizačních serverů

Administrace systému
- Konfigurace skrze webového průvodce
- Admin. role, více admin. a uživ. úrovní
- Upgrady & změny via Web UI (HTTPS)
- Web 2.0 shodné UI (HTTPS) s možností upravovat barvy
- Příkazová řádka (Serial, SSH, Telnet)
- SNMP (v1, v2c, v3)
- Cyberoam Central Console (volitelné)
- Podpora NTP serveru

Logování / Monitorování
- Monitor.v reálném čase i historii s grafickým výstupem
- Upozorňování mailem na reporty, útoky
- Podpora Syslogu
- Prohlížeč logů: IPS, Web Filter, A-Virus, A-Spam, Autentizace, System, admin události

Reportování na zařízení ****
- Integrován webový reportovací nástroj – Cyberoam iView
- 1000+ reportů s možností „rozpadu"
- 45+ reportů pro deklaraci shody se standardy
- Historické i real-time reporty
- Vícero Dashboardů
- Spec. monit. Dashboardy pro Username, Host, Email ID
- Reporty o útocích/přenosu dat dle uživatele/skupiny/IP
- Různé formáty reportů – tabulkové / grafické
- Export do PDF, Excel
- Vyhledávání dle klíčových slov
- Automatické plánované reporty

Vysoká dostupnost (HA) *****
- Active/Active
- Active/Passive se synchronizací stavu
- Stateful Failover
- Výstrahy při změně stavu zařízení

* není k dispozici u CR15iNG a CR15wiNG
** filtrace příchozí/odchozí pošty není možná zároveň
*** není součástí standardní licence
**** u CR15iNG a CR15wiNG pouze do předchozího dne (lze exportovat)
***** není podporováno u CR15iNG, CR15wiNG, CR25wiNG a CR35wiNG

COMGUARD
security & networking

COMGUARD s.r.o.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz