Cyberoam
A SOPHOS Company

Next-Generation Firewall for Enterprise network

Data Sheet

Cyberoam Next Generation Firewall

Firewall pro Enterprise

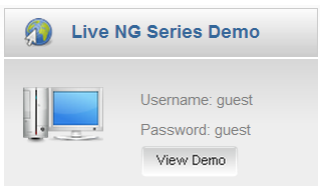
Se stále častější mobilitou firemních zaměstnanců narůstá potřeba mít kdykoli a kdekoli přístup k síťovým zdrojům. Kvůli uživatelům, zákazníkům a partnerům, kteří se připojují k podnikové síti zvenčí, dochází postupně k de-perimetrizaci podnikových sítí. Navíc i trendy, jako je nárůst počtu uživatelů a zařízení v síti, rozšíření aplikací, virtualizace a další vedou ke ztrátě bezpečnostní kontroly v sítích společností.

Cyberoam přichází s řešením v podobě Cyberoam Next-Generation Firewall (NGFW), kde je pro zvýšení zabezpečení přidána do výbavy unikátní schopnost monitorovat a analyzovat provoz na základě identity uživatele, tzv. "layer 8 technology". Pravidla je tak možné aplikovat na jednotlivce nebo vytvořené skupiny uživatelů. K ověřování identity lze využít RADIUS, LDAP, Windows Domain Controller, Active Directory nebo i lokální databázi Cyberoam. Klientská autentifikace prostřednictvím softwarových klientů je podporována jak ve spolupráci se systémy Windows, tak i systémy Linux. Takto aplikovaná bezpečnostní pravidla poskytují dodatečnou úroveň ochrany, ale také možnost kvalitnější správy sítě a omezení zneužívání těchto prostředků.

Cyberoam Next-Generation Firewally jsou vysoce výkoné, škálovatelné a jsou založené na CyberoamOS - inteligentním a výkonném firmwaru, který nabízí bezpečnostní prvky next generation. K těmto prvkům patří inline inspekce, kontrola aplikací, filtrování webových stránek, HTTPS inspekce, Intrusion Prevention System, VPN (IPSec a SSL) a řízení QoS / šířky pásma. Další bezpečnostní prvky jako Firewall Gateway Anti-Virus, Gateway Anti-Spam jsou také k dispozici.

Flexi porty

FLEXI Port (XP) - bezpečnostní zařízení nabízejí flexibilní připojení k síti s I/O sloty, které umožňují další Cooper / Fiber 1G / 10G porty na stejném bezpečnostním zařízení. Umožňují tak podnikům v budoucnu přejít na nové technologie snadno a efektivně. Flexi porty konsolidují počet zařízení v síti, nabízí tak energetickou efektivitu, snížení složitosti sítě a tím i snížení provozních nákladů.



http://ngdemo.cyberoam.com/corporate/webpages/login.jsp

Cyberoam za své řešení získal řadu ocenění:

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

Next-Generation Firewall for Enterprise network

Data Sheet

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, SIP NAT Traversal
- Podpora 802.1q VLAN
- Ochrana proti DoS&DDoS útokům
- MAC & IP-MAC filtrace a prevence spoofingu

Aplikační filtr
- Vestavěná databáze aplikačních kategorií (např. hry, IM, P2P, Proxy, ...)
- Podporováno více než 2000 aplikací
- Časová nastavení / rozvrhování pro uživatele
- Blokuje proxy a tunnrl, přenos souborů, sociální sítě, streaming media
- Důkladná kontrola a řízení 7. vrsty (aplikace) a „8. vrstvy" (uživatel - identity)
- Ochrana systémů SCADA – SCADA/ICS fltrováni signatur pro protokoly –Modbus, DNP3, IEC, Bacnet, Omron FINS, Secure DNP3, Longtalk, controla různých příkazů a funkcí

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
- SCADA – předdefinované kategorie signatur pro ICS a Scada

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

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

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

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
- 1200+ reportů s možností „rozpadu"
- 45+ reportů pro deklaraci shody se standardy
- Historické i real-time reproty
- Vícero Dashboardů
- Speci. 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 klíčových slov
- Časové nastavení automatických reportů

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

Webový filtr
- Vestavěná databáze web kategorií
- Blokuje URL, klíčová slova, typy souborů
- Kategorie: Default(89+) / 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

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

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

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

Gateway Anti-Virus&Spyware
- Detekuje a odstraňuje viry, červi a trojany
- Ochrana proti Spywaru, Malwaru a Phishingu
- Kontrola HTTP/ HTTPS/ FTP/ SMTP/ POP3/ IMAP/ IM/ VPN tunely
- 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

Gateway Anti-Spam
- Příchozí/odchozí skenování
- 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

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

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
- Import konfigurace spojení

* nutno dokoupit

Modelová řada CR	500iNG-XP	750iNG-XP	1000iNG-XP	1500iNG-XP	2500iNG-XP
Cooper GbE porty	8	8	10	10	10
Počet slotů pro Flexi Port moduly	2	2	4	4	4
FleXi porty moduly[1] (1GbE coop./1GbE SPF/10 GbE SPF)	8/8/4	8/8/4	8/8/4	8/8/4	8/8/4
USB porty / HW bypass segmenty[2]	2/2	2/2	2/-	2/-	2/-
Konfig. Internal/DMZ/WAN porty	ano	ano	ano	ano	ano
Propustnost UDP/TCP (Mbps)	18000/16000	22000/18000	27500/22500	32000/26000	60000/36000
Propustnost IPS/NGFW[3] (Mbps)	4500/3250	6500/3600	10500/5000	12500/6000	16000/8000
IPSec/SSL VPN propustnost (Mbps)	1500/650	2250/750	3000/850	4500/1050	9000/1450
Současná spojení	2 500 000	3 000 000	5 500 000	7 500 000	10 000 000
Nová spojení za sekundu	100 000	140 000	240 000	265 000	300 000

[1] Nutno dokoupit [2] Bypass appliance v případě selhání napájení [3] Propustnost při zapnutí všech modulů dle směrnice RFC 3511.

COMGUARD
security & networking

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