SOPHOS NETWORK PROTECTION

Sophos XG - Next Generation Firewall / UTM

Bezpečnostních výzev souvisejících s perimetrem je čím dál tím více. 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 často vedou ke ztrátě kontroly.

Spojení sofistikované bezpečnosti a jednoduchosti

U většiny firewallů se musí použít k nastavení jedné politiky různé moduly či stránky. To však neplatí u firewallu Sophos XG, který nabízí efektivní model konsolidace řízení, náhledu, filtrování a řazení všech uživatelských, aplikačních i síťových politik na jedné stránce.

Sophos XG nabízí velkou flexibilitu nasazení a využití. Lze jej nasadit jako robustní klasický firewall i výkonné UTM nabízející širokou škálu bezpečnostních modulů-funkcí, ke kterým patří např. revoluční systém synchronizace bezpečnosti na perimetru a koncových zařízeních **Security Heartbeat™**, plnohodnotný Web Application Firewall, kompletní webová a emailová bezpečnosti vč. DLP a šifrování poštovní komunikace.

Sophos XG Firewall/UTM byl vyvinut s důrazem na maximální výkon. Hardwarové appliance využívají více jádrové technologie Intel, SSD a akcelerované skenování obsahu přímo v paměti. Navíc paketová optimalizační technologie Sophos FastPath zajišťuje, že propustnost bude vždy dosahovat maxima svých možností.

Sophos XG Firewall v17 nová verze operačního systému SF-OS přináší revoluční funkcionalitu Cloud Application Visibility, která poskytuje přehled a informace o datech, která mohou být v ohrožena v cloudovém prostředí. Díky této funkci se mění XG Firewall na Cloud Access Security Broker (CASB), který upozorní na nežádoucí a neoprávněné aktivity a umožní kontrolu nad aplikacemi. CASB mimo jiné také poskytuje přehledný reporting o nahrávaných a stahovaných datech do cloudového prostředí.

Možnosti nasazení

> **Hardware appliance** – škálovatelná, specializovaná, vysoce výkonná zařízení

> **Software appliance**

> **Virtual appliance** VMware, Citrix, Microsoft Hyper-V a KVM

Každá z variant umožňuje využití všech funkcí.

Snadná správa více firewallů

Sophos Firewall Manager poskytuje jednu konzoli pro kompletní centrální správu mnoha firewallů s SF-OS (Sophos XG). Navíc je možné konsolidovat reporting nad různými firewally SF-OS, Sophos UTM v9.x a Cyberoam OS, a to díky nástroji Sophos iView.

Pro urychlení správy firewallu/ů jsou k dispozici šablony politik určených k zabezpečení běžných služeb, jako jsou MS Exchange, SharePoint, atd. Po výběru politiky je potřeba zadat pouze základní informace a šablona provede automaticky všechna potřebná nastavení pro příchozí i odchozí provoz a zobrazí finální politiku v textové podobě.

Přehled stěžejních funkcí:

> **MANAGEMENT**	Management firewallu	Centrální management	Statusy a upozornění	Reportování a logování
> **ŘÍZENÍ UŽIVATELŮ A APLIKACÍ**	Identita uživatelů	Kontrola aplikací	Kontrola webu	Kontrola obsahu
> **BEZPEČNOST**	Firewall a IPS	Cloud Sandbox	Anti-malware	Webová ochrana
	Ochrana proti pokročilým útokům		**Synchronizovaná bezpečnost mezi koncovými zařízeními a perimetrem**	
	Bussiness aplikace	Email a data	CASB	Antispam
> **NETWORKING**	Routing & Bridging	Segmentace na zóny	Řízení provozu	Řízení Wi-Fi
	Řízení výkonu	VPN	RED VPN	Šifrování provozu

COMGUARD security & networking

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

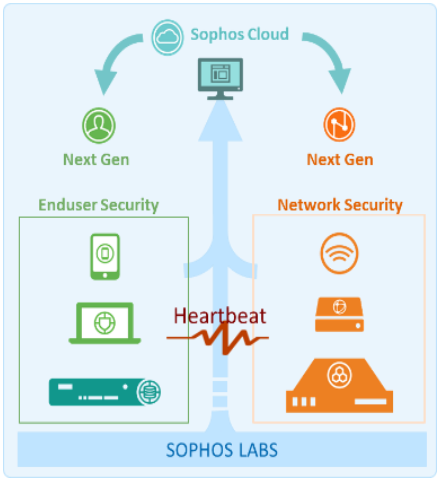
SOPHOS NETWORK PROTECTION

Patentovaná technologie řízení identity jako „8. vrstvy"

Uživatelská identita je prosazována jako celá nová vrstva, což umožňuje řídit aplikace, šířku pásma a další atributy s ohledem na konkrétní uživatele či skupiny, a to bez ohledu na IP adresy, lokality, sítě či zařízení.

Řízení uživatelského a aplikačního rizika

Sophos User Threat Quotient (UTQ) je velmi užitečná a unikátní funkce, která poskytuje okamžitě využitelné informace o chování uživatelů. Firewall koreluje obvyklé chování na webu každého uživatele s aktuálními prahovými hodnotami pro identifikaci hrozeb i jejich historií a identifikuje tak uživatele s rizikovým profilem chování. Další funkcí je „**Application Risk Meter**" vyjadřující rizikovost aplikace v síti.



Funkce synchronizovaného zabezpečení

Synchronized App Control, která umožňuje identifikovat, klasifikovat a kontrolovat dříve neznámé aplikace, které jsou využívány na koncových zařízeních. Správci mají možnost přidělit neznámým aplikacím kategorie. Na základě toho mohou být blokovány nebo upřednostňovány podle jejich potřeby. Interaktivní reportování aplikací poskytuje detailní přehled o denním toku dat.

Revoluční přístup k ochraně proti pokročilým hrozbám

Sophos Security Heartbeat™ je první technologií svého druhu, která propojuje koncová zařízení s firewallem a kombinuje jejich schopnosti za účelem identifikace systémů kompromitovaných dosud neznámými hrozbami. Status Heartbeat je integrován v rámci nastavení bezpečnostních politik a okamžitě spouští akce na koncových zařízeních i síťové úrovni ve smyslu izolace či omezení přístupu napadených systémů do doby, než jsou opět důvěryhodná. Tato funkce vyžaduje na koncových zařízeních systém Sophos Cloud Endpoint Protection Advanced nebo Sophos Cloud Enduser Protection.

Flexi Port moduly | I/O porty

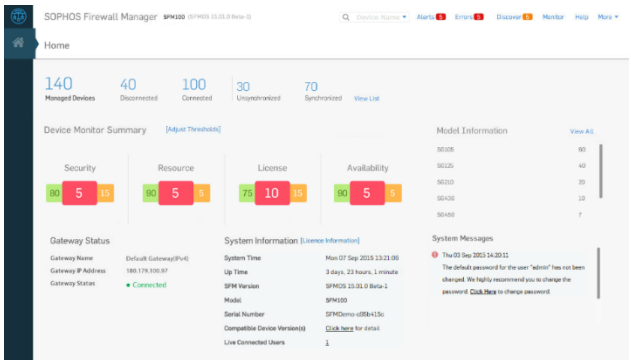
Sophos XG lze osadit dalšími Cooper / Fiber 1G / 10G porty na stejné appliance díky použití FleXi Port modulů a je tak možné konfigurovat hardware dle potřeb dané infrastruktury. Zároveň to přináší organizacím možnost v budoucnu přejít na nové technologie snadno a efektivně. Flexi porty konsolidují počet zařízení v síti, nabízí energetickou efektivitu, snížení složitosti sítě a tím i snížení provozních nákladů. Navíc jsou Flexi Port moduly kompatibilní i napříč modelovou řadou (např. v rámci 1U zařízení). Každý z modelů je rovněž vybaven různými I/O porty (USB, COM (RJ45), eth, VGA), které jsou nezbytné pro pohodlnou správu bezpečnostního zařízení.

Sophos RED (Remote Ethernet Device) VPN | Bezpečnost Wi-Fi

Sophos RED poskytuje bezpečné připojení/vzdálený přístup k jakýmkoli off-site lokacím organizace (pobočky, obchodní místa, atp.) a ve vzdálené lokalitě nevyžaduje po obsluze téměř žádné technické dovednosti. Na centrálním Sophos XG se pouze zadá ID zařízení a po instalaci RED se skrze automaticky sestavou VPN směruje bezpečně veškerý datový provoz na centrální UTM. Sophos XG rovněž pracuje jako centrální „wireless controller". Přístupové body (AP) jsou nastaveny automaticky a dostává se jim plné UTM ochrany.

Sophos Firewall Manager (SFM)

SFM poskytuje výkonnou centralizovanou správu pro všechny Sophos XG firewally napříč všemi lokalitami organizace, a to na jediné obrazovce. Správa je snadnou pro administrátory poskytovatelů služeb i společnosti s několika málo firewally. SFM účinně snižuje nároky na čas administrátorů a tím i náklady, jelikož jednoduchá aplikace politik i získaní dokonalého konsolidovaného přehledu, je kdykoli k dispozici.



K dalším charakteristikám patří možnost definice rolí administrátora a také variabilita nasazení, kdy je SFM možné nasadit jako
samostatnou hardwarovou appliance, software, či virtuální appliance.

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

SOPHOS NETWORK PROTECTION

Funkce a vlastnosti Sophos XG Firewall / UTM

Management
> Uživatelsky komfortní rozhraní s interaktivním řídícím centrem (Control Center)
> Navigace v GUI na 3 kliky kdekoli
> Kontextová nápověda u každé položky menu
> Pokročilé nástroje pro řešení problému v GUI (např. Packet Capture)
> Administrace dle rolí – selektivní definice oprávnění
> Automatické upozornění na aktualizace
> Objektově orientovaný systém definice pro sítě, služby, hosty, časové úseky, uživatele a skupiny, klienty a servery
> Sledování změn v konfiguraci
> Upozorňování skrze email nebo SNMP trapy

Routing a služby firewallu
> Vytváření zón a podpora politik dle zón
> Přednastavené zóny pro LAN, WAN, DMZ, LOCAL, VPN a WiFi
> Nastavitelné zóny LAN nebo DMZ
> Routing: statický, multicast (PIM-SM) a dynamický (BGP, OSPF)
> Bridging s podporou STP a ARP broadcast forwarding
> WAN link balancing: více internetových připojení, automatická kontrola funkčnosti linky, automatické překlopení (failover), automatický a vážený balancing a podrobná vícecestná pravidla
> Plná konfigurace DNS, DHCP a NTP
> Podpora Sophos RED
> Podpora a tagování VLAN DHCP

Pokročilá ochrana před hrozbami a synchronizovaná bezpečnost
> Detekuje a blokuje síťový provoz snažící se kontaktovat Command and Control servery využitím vícevrstvé DNS, AFC, HTTP proxy a firewallu
> Sophos Security Heartbeat okamžitě identifikuje kompromitované koncové body a zaznamenává hosty, uživatele, procesy, počty a časy incidentů
> Politiky Sophos Security Heartbeat můžou omezovat přístup k síťovým zdrojům nebo kompletně izolovat kompromitované systému do doby jejich nápravy

Síťová bezpečnost
> Stavový firewall s hloubkovou inspekcí paketů
> Optimalizace „FastPath Packet"
> Ochrana proti narušení: výkonný IPS systém s hloubkovou inspekcí paketů
> Ochrana proti zahlcení: blokovaní DoS, DDoS a skenování portů
> Blokování na základě zemí (geo-IP)
> „Site-to-site VPN": SSL, IPSec, 256-bit AES/3DES, PFS, RSA, X.509 certifikáty, „pre-shared key"
> Vzdálený přístup: podpora SSL, IPsec, iPhone/iPad/Cisco VPN klientů
> QoS (traffic shaping) dle sítě, uživatele, webu
> Optimalizace VoIP v reálném čase

Autentizace
> Transparentní, proxy autentizace (NTLM/Kerberos) nebo klientská autentizace
> Autentizace s podporou: Active Directory, eDirectory, RADIUS, LDAP a TACACS+
> Transparentní autentizace formou serverového agenta (STAS, SATC) s podporou Active Directory
> Transparentní autentizace formou klientského agenta s podporou pro Windows, Mac OS X, Linux 32/64
> Autentizační certifikáty pro iOS a Android
> Single sign-on: Active directory, eDirectory
> Autentizační služby pro IPSec, L2TP, PPTP, SSL

Možnosti VPN
> IPSec, SSL, PPTP, L2TP, Cisco VPN (iOS), OpenVPN (iOS a Android)
> Bezklientský portál využívající unikátní Sophos šifrovaný HTML5 samoobslužný portál s podporou pro RDP, HTTP, HTTPS, SSH, Telnet a VNC
> Podpora Sophos Remote Ethernet Device (RED)

VPN IPsec klient
> Autentizace: „Pre-Shared Key" (PSK), PKI (X.509), smartkarty, tokeny a XAUTH
> Šifrování: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (až do 2048 Bit), DH skupiny 1/2/5/14, MD5 a SHA-256/384/512
> Inteligentní „split-tunneling" pro optimální směrování provozu
> Podpora NAT-traversal

VPN SSL klient
> Osvědčené zabezpečení založené na SSL (TLS)
> Možnost customizovat SSL VPN port pro naslouchání
> Minimální systémové požadavky
> Podpora MD5, SHA, DES, 3DES a AES
> Průchodnost přes všechny firewally bez ohledu na proxy či NAT
> Podpora iOS a Android

Remote Ethernet Device (RED) VPN
> Centrální správa pro všechna RED zařízení
> Žádná konfigurace: automatické spojení skrze cloudovou službu
> Bezpečný šifrovaný tunel užívající digitální X. 509 certifikáty a AES256 šifrování
> Lokality s RED jsou plně chráněny licencemi firewallu (Network, Web and Mail security subscriptions)
> Virtuální ethernet pro spolehlivý přenos provozu mezi lokalitami
> IP Address Management s centrální konfigurací DHCP a DNS služeb
> Vzdálená deautorizace RED zařízení po zvolené lhůtě neaktivity
> Komprese tunelovaného provozu (RED 50, RED 10 revize 2, 3)
> Možnost konfigurace VLAN portu (RED 50)

Bezpečnost Wi-Fi sítě
> Jednoduché „plug-and-play" nasazení bezdrátových přístupových bodů Sopohos – automatické přidání do control centra firewallu
> Centrální monitoring a správa všech přístupových bodů (AP) a bezdrátových klientů přes bezdrátový kontroler
> Integrovaná bezpečnosti: Veškerý Wi-Fi provoz je automaticky směrován přes firewall
> Silné šifrování podporuje nejvyspělejší autentizační metody vč. WPA2-Enterprise a IEEE 802.1X (RADIUS)
> Bezdrátový přístup do internetu pro hosty s funkcí „walled garden"
> Časově definovaný přístup do sítě přes Wi-Fi
> Podpora přihlášení přes HTTPS

Webová bezpečnost
> Plně transparentní webová filtrace dle uživatelů bez potřeby nastavování proxy
> Databáze URL filtrace obsahuje miliony stránek v 92 kategoriích vyvíjených a udržovaných od SophosLabs
> Politiky dle uživatelů, skupin, času či sítě
> Skenování malwaru: blokuje veškeré formy škodlivého kódu v rámci HTTP/S, FTP a webových emailů
> Pokročilá ochrana před malwarem ve webovém provozu díky emulaci JavaScriptů
> Live Protection – dotazy přes cloud v reálném čase pro nejnovější informace o hrozbách
> Druhý nezávislý antimalwarový engin od Aviry – dvojí skenování provozu
> Ochrana proti pharmingu
> Skenování HTTP a HTTPS
> Detekce a ochrana před tunelováním provozu skrze SSL
> Ověřování certifikátů
> Vynutitelné kešování pro updaty Sophos Endpoint
> Filtrování typů souborů dle mime-type, přípony a aktivního obsahu (např. Activex, applety, cookies, atd.)
> Možnost vynucení YouTube pro školy
> Možnost vynucení „SafeSearc

Aplikační bezpečnost
> Vylepšené řízení aplikací dle signatur a vzorů na 7. vrstvě pro tisíce aplikací
> Řízení aplikací dle kategorií, charakteristik (např. šířka pásma, ztráta produktivity), technologií (např. P2P) a úrovně rizika
> Vynucení pravidel aplikační kontroly dle uživatele nebo sítě
> Kategorické řazení nově objevených aplikací
> Možnost řízení šířky pásma pro aplikaci za účelem omezit nebo garantovat priority pro upload/download

Emailová bezpečnost
> Reputační služba s monitoringem spamových kampaní založená na patentované technologii Recurrent-Pattern-Detection
> Blokuje spam a malware v SMTP provozu
> Detekuje phishingové URL uvnitř emailů
> Black/white listy adres a domén dle uživatelů/globálně
> Skenování emailů pro SMTP, POP3 a IMAP
> 2 nezávislé antivirové enginy (Sophos & Avira)

Skenuje vložená data: blokuje nebezpečné a nechtěné soubory s kontrolou typu souborů (MIME type) Karanténa pro neskenovatelné či nadměrně objemné zprávy Filtrace pošty pro neomezený počet domén a poštovních schránek
> Automatické aktualizace signatur a vzorů
> Možnost vytváření Allow listů pro Bypass politiky, kde lze přidat jednotlivé uživatele, či domény
> Propojení s cloudovou službou Sophos Live Anti-Virus pro dotazy na aktuální hrozby v reálném čase

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

SOPHOS NETWORK PROTECTION

Šifrování emailů a prevence úniku citlivých dat (DLP)
> Patentovaná technologie SPX (Secure PDF Exchange) pro jednosměrné šifrování zpráv
> Samoobslužná registrace SPX hesel příjemců
> Transparentní de/šifrování a podepisování SMTP emailů
> Kompletně transparentní, není třeba další software či klient
> Umožňuje skenovat obsah/viry i u šifrovaných emailů
> Centrální správa všech klíčů a certifikátů – není třeba žádné distribuce klíčů či certifikátů
> DLP engine s automatickým vyhledáváním citlivých dat v emailech a přílohách
> Předpřipravený kontrolní list citlivých dat (CCLs) pro PII, PCI, HIPAA a další, připravený a udržovaný od SophosLabs

Uživatelský samoobslužný portál
> SMTP karanténa: prohlížení a uvolňování zpráv z karantény
> Blacklist/whitelist odesilatelů
> Informace o přístupu k hotspotům
> Stažení Sophos Authentication Agenta (SAA)
> HTML5 VPN portál pro sestavení bez klientského VPN spojení k definovaným službám
> Stažení HTTPS Proxy CA certifikátů

Bezpečnost webových aplikací - Web Application Firewall (WAF)
> Reverzní proxy
> Systém zabezpečení URL proti útokům typu „deep-linking" a „directory traversal"
> Systém zabezpečení formulářů
> Ochrana proti „SQL injection" útokům
> Ochrana proti „Cross-site scripting" útokům
> 2 nezávislé antivirové enginy (Sophos & Avira)
> Převzetí šifrování HTTPS (SSL) - offloading
> Podepisování Cookie souborů digitálními podpisy
> Směrování dle obsahu (Path-based routing)
> Reverzní autentizace (offloading) pro basic autentizaci i založenou na formuláři u serverových přístupů
> Integrovaný systém rozkladu zátěže rozděluje návštěvníky na jednotlivé servery
> Porovnává požadavky ze zdrojových síti nebo specifických cílových URL
> Podpora logických and/or operátorů
> Možnosti měnit parametry ovlivňující výkonnost WAF
> Možnost omezit velikost skenovaných dat
> Možnost povolit/blokovat IP rozsahy

Logování a reportování
> Stovky reportů na zařízení s možnostmi vlastního nastavení
> Anonymizuje data
> Plánování reportů pro různé příjemce dle skupin reportů s flexibilní periodou
> Nastavitelná délka uchování logů dle kategorií
> Dashboardy pro síťový provoz, bezpečnost a ukazatel rizik spojených s uživateli
> Aplikační reporty pro rizika uživatelských aplikací, blokované uživatelské aplikace, webová rizika, blokované přístupy na web, vyhledávací enginy, využití webového serveru, ochranu webového serveru, přenos uživatelských dat, FTP provoz
> Síťové reporty a reporty hrozeb pro útoky-narušení sítě, pokročilou síťovou ochranu, Wi-Fi a Security Heartbeat
> Reporty využití a ochrany emailu
> reporty shody pro HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3 a CIPA

Všechny funkce mají konfigurační API pro RMM/PSA integraci

Modelová řada Sophos XG	XG 86 rev. 1	XG 106 rev. 1	XG 115 rev. 3	XG 125 rev. 3	XG 135 rev. 3	XG 210 rev. 3	XG 230 rev. 2	XG 310 rev. 2	XG 330 rev. 2	XG 430 rev. 2	XG 450 rev. 2	XG 550 rev. 2	XG 650 rev. 2	XG 750 rev. 2
	Desktop	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	1U	1U	1U	2U	2U	2U
Maximální počet portů	4	4x GE + 1xSFP (shared)	4x GE + 1xSFP (shared)	8x GE + 1xSFP	8x GE + 1xSFP	16 (6 + 2 SFP plus 1 module)	16 (6 + 2 SFP plus 1 module)	20 (8 + 2 SFP + 2 SFPplus + 1 module)	20 (8 + 2 SFP + 2 SFPplus + 1 module	26 (8+2SFP+ 2 moduly) + IPMI	26 (8+2SFP+ 2 moduly) + IPMI	32 (8 + 4 moduly)	32 (8 + 6 moduly)	64 (8 + 8 moduly)
Rozšiřující moduly	-	SFP DSL (VDSL2)	SFP DSL (VDSL2)	SFP DSL (VDSL2), 3G/4G	SFP DSL (VDSL2), 3G/4G	FleXiPort (1)	FleXiPort (1)	FleXiPort (1)	FleXiPort (1)	FleXiPort (2)	FleXiPort (2)	FleXiPort (4)	FleXiPort (6)	FleXiPort (8)
Úložná kapacita	16 GB eMMC	64 GB M.2 SSD	64 GB M.2 SSD	64 GB M.2 SSD	64 GB M.2 SSD	120 GB SSD	120 GB SSD	180 GB SSD	180 GB SSD	240 GB SSD	2*240 GB SSD (RAID-1)	2*300 GB SSD (RAID-1)	2*480 GB SSD (RAID-1)	2* 480 GB SSD (RAID-1)
RAM (GB)	4	4	4	4	6	8	8	12	12	16	16	24	48	64
Propustnost firewallu (Mbps)	3000	3500	4000	6500	8000	16000	20000	28000	33000	41000	50000	65000	85000	100 000
Propustnost VPN (Mbps)	225	360	490	700	1180	1450	1700	2750	3200	4800	5500	8400	9000	11000
Propustnost IPS (Mbps)	580	970	1220	1530	2480	2700	4200	5500	8500	9000	10000	17000	20000	22000
Propustnost AV-proxy (Mbps)	360	450	600	700	1580	2300	2800	3300	6000	6500	7000	10000	13000	17000
Nová spojení/s (tis.)	15	28	35	35	85	135	140	200	200	200	200	220	240	300
Současná spojení (tis.)	3200	3200	6000	6000	6000	8200	8200	17500	17500	20000	20000	30000	30000	30000
Redundantní zdroj	-	volitelně	volitelně	volitelně	volitelně	volitelně	Volitelně	volitelně	volitelně	volitelně	volitelně	ano	ano	ano