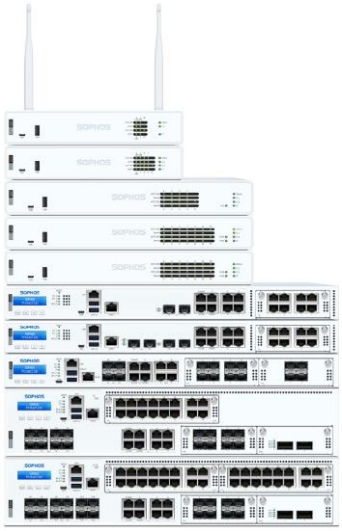
SOPHOS NETWORK PROTECTION

Sophos XGS – Next Generation Firewall / UTM

S narůstajícími nároky na bezpečnost a ochranu perimetru se paralelně zvyšují i nároky na výkon a technologie. Nejmodernější Sophos XGS Firewall/UTM byl vyvinut s důrazem na maximální výkon. Řada XGS používá architekturu založenou na dvouprocesorových čipech Xstream (vícejádrový procesor x86 společně s procesorem Xstream Flow) a nabízí podporu TLS inspekce, včetně nativní podpory TLS 1.3, která je až 6x rychlejší než jiné modely aktuálně dostupné na trhu. To vše společně umožňuje zásadně akcelerovat celkový výkon a úroveň bezpečnosti, včetně kontroly šifrovaného provozu.



Spojení sofistikované bezpečnosti a jednoduchosti

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

Sophos XGS 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 bezpečnost vč. DLP a šifrování poštovní komunikace.

Xstream Architecture vyniká zejména díky třem klíčovým funkcionalitám:

- Dedikované procesory Xstream Flow zrychlují přenos síťové komunikace skrz FastPath – offloading důvěryhodného provozu z FW rychlostí limitovanou pouze kabelem. FW kontroluje tedy jenom provoz, který to skutečně potřebuje.
- Inspekce Xstream TLS 1.3 využívá důkladně přepracovaný ultrarychlý engine, podporuje nejnovější standardy a co je nejdůležitější – je inteligentnější v tom, co je potřeba dešifrovat a co optimalizovat pro potřeby výkonu. I díky tomu je 5-8krát rychlejší v porovnání s předcházející generací.
- Nový optimalizovaný Deep Packet Inspection (DPI) engine pro hloubkovou kontrolu paketů poskytuje kromě nejpokrokovější ochrany před zero-day hrozbami také zvýšenou ochranu vůči aplikacím měnícím hashe jako je např. software Psiphon.

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.

Funkcionalita **Cloud Application Visibility** poskytuje přehled a informace o datech, která mohou být ohrožena v cloudovém prostředí. Díky této funkci se mění XGS 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.

Xstream Protection		Standard Protection
Base License	Síťový firewall, SD-WAN, Wireless, VPN, reporting	Base License
Network Protection	Xstream TLS, DPI, IPS, ATP, Security Heartbeat, vzdálené připojení poboček přes RED zařízení	Network Protection
Web Protection	Xstream TLS, DPI, URL filtering, Web Malware Protection, Application Control sedmé vrstvy	Web Protection
Zero-Day Protection	Statická a dynamická analýza souborů (sandboxing), reporting	
Central Orchestration	NOVINKA: SD-WAN VPN orchestrace, Central Firewall Reporting Advanced (30 dní), připravené pro použití s MTR/XDR technologii	
Enhanced Support	24x7 telefon/e-mail podpora, NBD výměna zařízení	Enhanced Support

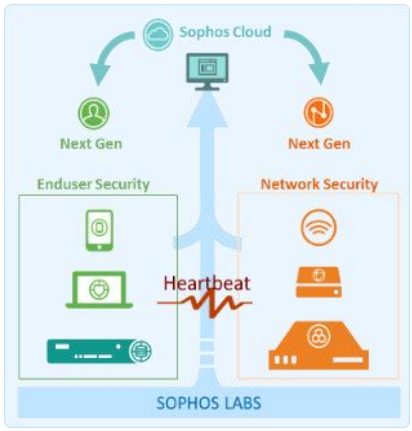
COMGUARD
communication security

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

SOPHOS NETWORK PROTECTION

Funkce synchronizovaného zabezpečení

Synchronized App Control, 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.



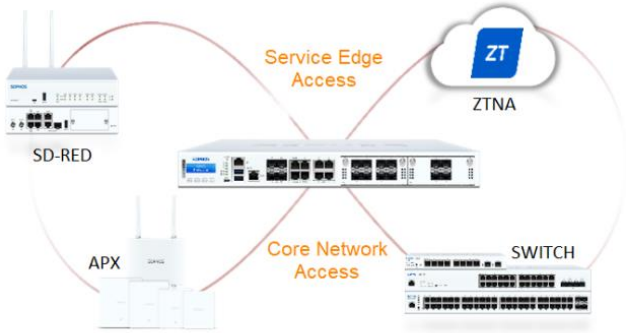
Revoluční přístup k ochraně proti pokročilým hrozbám

Sophos Security Heartbeat™ je první technologií svého druhu, která propojuje koncová zařízení s firewallem a kombinuje jejich schopnosti za účelem identifikace kompromitovaných systémů dosud neznámými hrozbami. Security 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 důvěryhodné. Tato funkce vyžaduje na koncových zařízeních systém Sophos Central Intercept X.

Secure Access Portfolio

Sophos SD-RED VPN | Bezpečná 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 XGS se pouze zadá ID zařízení a po instalaci RED se skrze automaticky sestavenou VPN směruje bezpečně veškerý datový provoz na centrální UTM. Sophos XGS umí pracovat jako centrální „wireless controller". Přístupové body (APX) jsou nastaveny automaticky a dostává se jim plné UTM ochrany.



Flexi Port moduly | I/O porty

Sophos XGS lze osadit dalšími Copper / Fiber 1G / 10G porty na stejné appliance díky použití FleXi Port modulů a je tak možné konfigurovat hardware dle potřeb dané infrastruktury. 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.

Zero Trust Network Access

Sophos ZTNA je sofistikovaně zabezpečené a transparentní připojení vzdálených pracovníků nebo poboček plně kompatibilní s XGS Firewallem a Sophos Intercept X. Koncept „zero trust" řeší rizika, která s sebou nese připojení nového zařízení do korporátní sítě skrz VPN. Pracuje s presumpcí viny a všechny zařízení považuje za rizikové, dokud se neprokážou jako zabezpečené. Každé zařízení získá v síti pouze takové oprávnění, které odpovídá jeho aktuální bezpečnostní připravenosti = bezpečná alternativa k VPN.

Sophos Central Firewall Reporting (CFR)

CFR nabízí široké možnosti přizpůsobení historických reportů síťové aktivity, které zabezpečí potřebný vhled do již proběhlých procesů, jejich hlubší pochopení a díky nastavitelným politikám a pravidlům CFR bude práce administrátorů efektivnější a jednodušší. K dispozici je množství filtrů, které nabízí lehké a rychlé prohledávání logů z XGS firewallu, granulárnost dat v přizpůsobitelných tabulkách a grafech za období až jednoho roku a uživatelsky přívětivé přehledné GUI s možností bohatého přizpůsobování šablon. Tento reportovací nástroj je integrován do platformy Sophos Central, administrátoři mohou tedy z jediné konzole spravovat reporty z FW a také další komponenty bezpečnostní infrastruktury.

COMGUARD
communication security

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 XGS 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 traps

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"
- TLS inspekce s podporou TLS 1.3
- 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

SD-WAN
- Připojení přes VDSL,DSL,4G/LTE a další s možností monitoringu, balancingu a failover mezi nimi
- Volba odchozí WAN brány pro konkrétní aplikace/uživatele/komunikaci
- Centralizovaný VPN orchestrátor
- Sophos SD-RED

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, 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
- Sdílení portu 443 mezi SSL VPN a WAF
- 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
- Komprese tunelovaného provozu
- Možnost konfigurace VLAN na portech (SD-RED 60)

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 (APX) 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)
- 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
- Filtrování typů souborů dle mime-type, přípony a aktivního obsahu (např. Activex, applety, cookies, atd.)

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 emailu
- Black/white listy adres a domén dle uživatelů/globálně
- Skenování emailů pro SMTP, POP3 a IMAP
- 2 nezávislé antivirové enginy (Sophos & Avira)
- Blokuje nechtěné typy souborů
- Karanténa pro neskenovatelné či nadměrně objemné zpráv
- Neomezený počet domén/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 communication security

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

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 (TLS/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 XGS	XGS 87 rev. 1	XGS 107 rev. 1	XGS 116 rev. 1	XGS 126 rev. 1	XGS 136 rev. 1	XGS 2100 rev. 1	XGS 2300 rev. 1	XGS 3100 rev. 1	XGS 3300 rev. 1	XGS 4300 rev. 1	XGS 4500 rev. 1	XGS 5500 rev. 1	XGS 6500 rev. 1
	Desktop	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	1U	1U	1U	2U	2U
Maximální počet portů	5 4x GE 1x SFP	9 8x GE 1x SFP (shared)	10 8x GE 1x SFP 1x GE PoE	14 10x GE 2x SFP 2x GE PoE	14 10x GE 2x SFP 2x 2,5GE PoE	18 8x GE 2x SFP 1x module	18 8x GE 2x SFP 1x module	20 8x GE 2x SFP 2x SFP+ 1x module	20 8x GE 2x SFP 2x SFP+ 1x module	28 4x GE 4x 2,5GE 4x SFP+ 2x moduly	28 4x GE 4x 2,5GE 4x SFP+ 2x moduly	48 8x GE 8x SFP+ 3x moduly	68 8x GE 12x SFP+ 4x moduly
Rozšiřující moduly	-	SFP DSL (VDSL2)	SFP DSL (VDSL2), 3G/4G	SFP DSL (VDSL2), 3G/4G	SFP DSL (VDSL2), 3G/4G	FlexiPort (1)	FlexiPort (1)	FlexiPort (1)	FlexiPort (1)	FlexiPort (2)	FlexiPort (2)	FlexiPort + High-density (2+1)	FlexiPort + High-density (2+2)
Úložná kapacita	16 GB eMMC	64 GB SSD	64 GB SSD	64 GB SSD	64 GB SSD	120 GB SSD	120 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD	2*240 GB SSD (SW RAID-1)	2*480 GB SSD (HW RAID-1)	2*480 GB SSD (HW RAID-1)
DDR4 RAM (GB)	6	6	8	10	12	12	12	16	20	40	40	86	92
Propustnost firewallu (Mbps)	3 700	7 000	7 700	10 500	11 500	30 000	35 000	38 000	40 000	75 000	80 000	100 000	115 000
Propustnost IPsec VPN (Mbps)	750	900	1 100	-	-	3 000	3 500	5 200	6 500	9 800	16 000	21600	26 000
Propustnost IPS (Mbps)	1 015	1 355	2 000	2 600	3 300	5 800	7 000	9 820	13 440	25 000	35 690	40 000	48 000
Threat Protection propustnost (Mbps)	240	330	685	900	1 000	1 250	1 400	2 000	2 770	4 800	8 390	12 390	17 050
Propustnost Xstream SSL/TLS (Mbps)	375	420	650	800	950	1 100	1 450	2 470	3 130	8 000	10 600	13 500	16 000
Latence (64 byte UDP)	6 µs	6 µs	8 µs	8 µs	8 µs	6 µs	4 µs	4 µs	4 µs	3 µs	4 µs	5 µs	5 µs
Nová spojení/s (	35 700	44 400	61 500	69 900	74 500	134 700	148 000	186 500	257 800	368 000	450 000	468 000	496 000
Současná spojení (tis.)	1 600	1 600	1 600	5 000	6 400	6 500	6 500	12 260	13 700	16 600	17 200	32 400	39 900
Xstream SSL/TLS souč. spoj.	8 192	8 192	8 192	12 288	18 432	18 432	18 432	55 296	102 400	276 480	276 480	512 000	768 000
Redundantní zdroj	-	volitelně	volitelně	volitelně	volitelně	volitelně	Volitelně	volitelně	volitelně	volitelně	volitelně	ano (hot-swap)	ano (hot-swap)