COMGUARD

Skyhigh Security

# Skyhigh Web Gateway

## Komplexní ochrana proti webovým nástraham

*Pro většinu současných organizací je internet základní a nepostradatelný funkční nástroj. Využitelnost webu pro prosperitu organizace se zvětšuje každým rokem. Bohužel přímou úměrou také narůstá potenciální bezpečnostní riziko, které tento mocný nástroj představuje. Každým dnem vznikají stovky nových, více či méně sofistikovaných vzorků malwaru, které jsou do éteru distribuovány právě přes webové prostředí. Skyhigh Web Gateway zaručí organizacím komplexní ochranu proti webovým nástrahám, poskytne patřičný vhled do využití webu v rámci organizace pomocí přehledných reportů a v neposlední řadě také zaručí vynucení organizační politiky. Díky možnosti využití cloudového nasazení mohou být uživatelé chráněni i mimo podnikovou síť.*

### Klíčové charakteristiky

- **#1 proti nebezpečným kódům** s více než 99% úspěšností (HTTP, HTTPS, FTP).
- **Hybridní ochrana** – Skyhigh Web Protection nabízí možnost kombinovaného propojení ochrany webového provozu pomocí fyzické nebo virtuální appliance a cloudové služby. Software pro virtuální prostředí je v ceně řešení.
- **DLP pravidla** – nástroj pro vynucení a naplnění cílů bezpečnostních politik v oblasti ochrany citlivých dat.
- **Global Threat Intelligence** – proaktivní detekce s napojením na systém globálních reputací Skyhigh TrustedSource.
- **Web & DNS Cache** – proaktivní kontrola a testy reputace objektů před doručením uživatelům.
- **AntiMalware** – hloubkový výkon proaktivní antimalware ochrany proti virům, červům, trojským koním a špiónům.
- **Aplikační kontrola** – umožňuje nastavit granulární pravidla pro více jak 1000 webových aplikací.
- **URL filtrace** – výkonné, vícejazyčné filtrování webového obsahu s využitím databáze Skyhigh GTI a hodnocením webů za pomoci globální reputační technologie Skyhigh TrustedSource.
- **Inspekce HTTPS** (SSL šifrovaného provozu) – dočasné dešifrování odchozího i příchozího https provozu, následná kontrola obsahu včetně kontroly certifikátů a opětovné zašifrování, čímž je zachována důvěrnost dat.
- **Skyhigh client proxy** – umožňuje chránit uživatele i když se nacházejí mimo podnikovou síť, dostupné i pro smartphony a tablety.
- **Streaming Proxy** – nativní ochrana streamovaných médií s podporou pro RTSP – doručování dat v reálném čase (zvuk, video); MMS s děleným streamováním a cachováním.
- **Šifrování souborů** – při nahrávání na Google Drive, Microsoft Skydrive, Dropbox a Box
- **Možnost propojení s Advanced Threat Defense (ATD)** – Sandboxing malwaru – simulace reálného prostředí, kde se vyhodnocuje chování hrozby a tím i její nebezpečnost. Objekty už jednou zkontrolované pomocí ATD, se znovu neskenují. Výsledky prvního testu se používají ke klasifikaci objektu jako bezpečný nebo infikovaný.
- **Možnost integrace s Threat Intelligence Exchange –** zkráceně TIE, technologie pro reputační hodnocení souborů a výměnu informací mezi jednotlivými zařízeními bezpečnostní infrastruktury (webová brána <–> endpoint klient).

### Skyhigh nabízí komplexní integrované zabezpečení

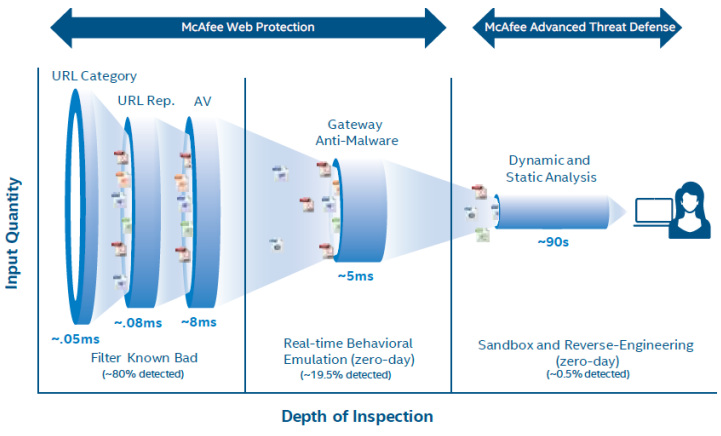
Skyhigh Web Gateway posiluje „bojeschopnost" stěžejních modulů (Anti-Virus a Web Filter) integrací zabezpečené cache (i pro DNS), napojení na systém globální Inteligence a dešifrace HTTPS protokolu uvnitř zařízení. Navíc díky proaktivnímu modulu Anti-Malware lze zdvojit ochranu proti zákeřným kódům a filtrovat tak provoz dvěma nezávislými systémy najednou. Jako další možné rozšíření klasické ochrany lze jednoduše integrovat fyzický (ATD) či cloudový sandbox. Pro komplexní ochranu od koncového zařízení až ke cloudu lze Skyhigh Web Gateway doplnit řešením **Skyhigh Security Cloud (CASB)**, které zajistí ucelený vhled do cloudových aktivit korporace.

### Ochrana proti hrozbám z externích zdrojů (ICAP Deployment)

Spousta organizací nabízí možnost na své file servery nahrávat soubory přes webové rozhraní kdekoliv z internetu. Skyhigh Web Gateway řeší tuto bezpečnostní problematiku pomocí nasazení své webové brány jako reversní proxy, kdy je webová brána nasazena před file server a skenuje všechen obsah, který proudí směrem do interních systémů společnosti.

### Přínosy

- **Dokonalá ochrana informačních aktiv** – ucelené portfolio preventivních i reaktivních nástrojů v několika vrstvách proti veškerým formám nebezpečného a nechtěného obsahu webového provozu generovaného uživateli.
- **Rychlá návratnost investice** – okamžitý růst produktivity zaměstnanců díky omezení nepracovního využití internetu, méně bezpečnostních incidentů v síti, úspora nákladů za internetovou konektivitu.
- **Příjemné admin prostředí a reporty** – volitelné nastavení politik uživatelů s přehlednými reporty (reportovací nástroj Web Reporter Basic v ceně řešení, možnost volby Web Reporter Premium).




COMGUARD
communication security

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

COMGUARD

Skyhigh Security

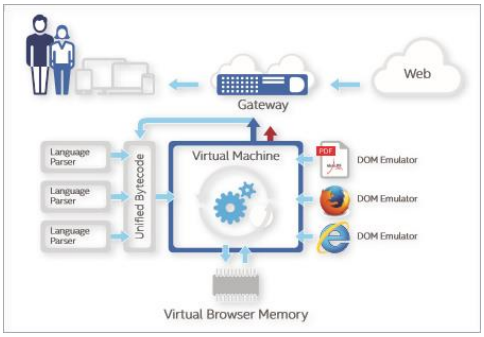
# Skyhigh Web Gateway

## Technologie / funkce / vlastnosti

**Hybridní ochrana** – součástí licence Web Protection je i hostovaná služba Skyhigh Web Gateway Cloud Service, která umožňuje URL a anti-malware filtraci webového provozu v cloudu. Toto nasazení je velmi výhodné zejména pro uživatele, kteří často cestují a přistupují na web mimo podnikovou síť. Skyhigh uvedl nový standard proaktivní ochrany a napojil bezpečnostní brány na systém globální inteligence Skyhigh „Global Threat Intelligence" založeného na cloud computingu. Tento systém využívá patentované technologie a zpravodajské služby laboratoří Skyhigh Labs. Nejznámější je reputační technologie Skyhigh TrustedSource s hodnocením obsahu webových stránek a zobrazující informace nejen o geografickém umístění jednotlivých webů (Geo-location). Díky exponenciálně rostoucí znalosti chování subjektů na internetu, v prostředí neustále se vyvíjejících hrozeb, identifikuje systém podezřelé či zcela nelegitimní chování entit (např. IP adres, URL, domén, DNS serverů atd.), přičemž se opírá o síť více než 10000 senzorů v 80+ zemích světa včetně ČR a SR.

**Web Filter URL a Aplikační Filter** se opírá o kooperaci lokální databáze a Skyhigh GTI s globálním reputačním (hodnotícím) systémem TrustedSource. Nabízí řízení uživatelů pro zvýšení produktivity práce, pro bezpečnost webového provozu a pro optimalizaci využití šířky pásma. Dostupné akce jsou: monitoring, blokování, učení a objemové a časové kvóty. Zákazníci mají na výběr z lokálních, cloudových i kombinovaných dotazů. Filtrace je doplněna **kontrolou aplikací**, takže lze jednoduše řídit přístup k aplikacím typu Facebook, Xing a další. Pro zajištění nejvyšší úrovně bezpečnosti brána dokáže rozpoznat **streamové formáty** (typu RealMedia, Flash, MS WMSP a další) a následně regulovat jejich využívání. V neposlední řadě lze pro filtraci využít regulární výrazy, kde jsou zohledněny uživatelsky zadané kategorie a stránky, jsou analyzovány nevhodné obrázky, a probíhá kontrola html obsahu a URL. Multijazyčná webová filtrace navíc dokáže rozpoznat nevhodný obsah, i když je např. stažen z cache vyhledávacích portálů. Vše je podporováno reportovacím nástrojem **Content Security Reporter**.

**Anti-Malware** – **nová** generace skeneru provádí proaktivní kontrolu webového obsahu v reálném čase. Sofistikovaný Anti-Malware engine dokáže odhalit jakékoli skryté útoky, viry, červy, trojské koně, přetečení zásobníku aj. Zároveň posuzuje chování mobilních kódů a hodnotí jejich potenciální škodlivé aktivity. V rámci **Skyhigh GTI** jsou shromažďovány veškeré nové hrozby a škodlivé aktivity, které jsou neustále automaticky korelovány ve Skyhigh laboratořích, čehož zpětně využívá každá Skyhigh Web Gateway.




**Web & DNS Cache** – Skyhigh je prvním výrobcem, který vyvinul proxy/cache pro zabezpečení Web 2.0 prostředí. Revoluční technologie podrobuje sledované objekty proaktivní kontrole a hodnocení (reputace) z hlediska bezpečnosti dříve, než jsou doručeny koncovým uživatelům. Odpadá také nutnost znovu načítání cache při aktualizaci signatur v porovnání s tradičními řešeními.

**Integrace se Skyhigh Enterprise Authentication Services** umožňuje dosáhnout stejných bezpečnostních parametrů pro přístup uživatelů ke cloudovým službám jako při jejich přístupu přes webovou bránu. Modul One Time Password nabízí multifaktorovou autentizaci jak pro uživatele, tak i pro administrátory ve formě jednorázových hesel zasílaných pomocí emailu, SMS nebo přes mobilní aplikaci. Cloud SSO na Web Gateway podporuje nové konektory http a poskytuje obecnou šablonu ty, které mohou být nakonfigurovány i pro aplikaci, která není Web Gateway podporována. Aktualizace katalogu SSO podporovaných konektorů lze dodat jako službu. Po aktualizaci jsou zastaralé konektory zvýrazněny v uživatelském rozhraní.

**Mobile Security s Autentizací pomocí certifikátu** – tradičně se pro přístup k interním aplikacím využívá SSL VPN spojení, to však může být problém v důsledku různorodosti mobilních zařízení. Skyhigh Web Gateway přichází s alternativou, která převádí dotazy HTTP na HTTPS. Pro autentizaci mobilních uživatel se využívá certifikátu, který lze importovat přímo do prohlížeče. Pro své zaměstnance tak zajistíte bezpečný přístup bez nutnosti VPN.

**SSL Scanner** – šifrovaný SSL provoz lze snadno použít jako tunel pro infiltraci malware do „zabezpečených" sítí, jelikož je za normálních okolností nekontrolovatelný (např. free mail via https). SSL Scanner dočasně dešifruje odchozí i příchozí https provoz a umožní zkontrolovat obsah proti malware a dodržení firemních zásad. Následně provoz opět šifruje a odesílá do cíle bez narušení integrity.

**Prevence úniku citlivých dat (DLP)** – pomocí filtrace odchozího provozu (včetně šifrovaného). Je Skyhigh Web Gateway nástrojem pro vynucení a naplnění cílů bezpečnostní politiky organizace v oblasti ochrany citlivých dat. Umožňuje řídit shodu se standardy, provést forenzní analýzu v případě incidentu a poskytuje obsáhlý reporting (pro organizace využívající cloudová uložiště).

**Content Security Reporter** je jednotný reportovací nástroj pro všechny Skyhigh produkty, který je k dispozici jako add-on k ePolicy Orchestrator. Přináší detailní pohled na chování uživatelů na internetu včetně podrobného rozpadu na hodinové aktivity. Dále reportuje špičky, trendy a události spojené se síťovými aktivitami a to vč. cache, přenosu multimédií a webu.

| Modelová řada |  |  |  |
|---|---|---|---|
| | **WG-4500** (1U) | **WG-5000** (1U) | **WG-5500** (1U) |
| Procesor | 1 x Intel Xeon 4 cores | 2 x Intel Xeon 8 cores | 2 x Intel Xeon 14 cores |
| Paměť | 64 GB | 96 GB | 128 GB |
| Rozhraní | 6 x 10/100/1000 Mbit/s | 6 x 10/100/1000/10000 Mbit/s | 6 x 10/100/1000/10000 Mbit/s |
| RAID | RAID 1 | RAID 1 | RAID 10 |
| HDD | 2 x 1 TB SATA | 2 x 600 GB SAS | 6 x 300 GB SAS |
| Napájecí zdroj | jeden | redundantní | redundantní |

COMGUARD
communication security

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