



SOPHOS

KOMPLEXNÍ ZABEZPEČENÍ ICT A SÍŤOVÉ INFRASTRUKTURY

SÍŤOVÁ INFRASTRUKTURA

Sophos reprezentuje ucelený bezpečnostní systém evropské provenience (GB,D), který kombinuje proprietární zařízení (UTM) s možností nasazení softwarové ochrany typu Endpoint na všechna koncová zařízení včetně mobilních (tablety, telefony, notebooky), ale i na servery.



PETR ODVÁRKA VEDOUcí ODDĚLENí SÍŤOVÉ INFRASTRUK- TURY

Petr vystudoval České vysoké učení technické, obor automatizované systémy řízení. Svou kariéru začal jako technik propojení podpory serverů LAN, nejdříve pro společnost Themos, poté pro DB. Ve společnosti RSM CZ Petr pracuje od roku 1992. V současnosti má na starosti předprodejní a prodejní podpory komunikací, je systémový specialista a vedoucí oddělení Síťové infrastruktury. Petr je expert na vývoj aplikací pro správu, dohled a management sítí a systémů. Podílel se například na designu a implementaci podpory LAN a WiFi pro Ahold ČR, Kiekert-CS a na dalších projektech například pro společnosti Tatra a Pojišťovna České spořitelny.

Zakoupením tohoto systému klient získá kromě základních bezpečnostních funkcionalit typu firewall, NAT (network address translation) a VPN (klientská, pobočková) i možnosti aktivace dalších následujících bezpečnostních funkcionalit:

- Web content filtering, neboli kontrola web stránek (rozdělení do kategorií, zákaz některých kategorií)
 - Download antivirus (tedy antivirová kontrola stahovaných souborů a detekce malware na web stránkách)
 - Kontrola přenosu souborů s přílohou (zamezení downloadu souborů s konkrétní přílohou z Internetu / zamezení uploadu konkrétních příloh na Internet)
 - Kontrola aplikací a zamezení vybraným, případně omezování pásma na základě aplikace (např. skype, facebook, atd. – tedy hlubší inspekce procházejících dat s tím, že je kontrolován i obsah; nejen to, že jde o port 80 protokolu TCP)
 - Automatická detekce uživatele podle účtu v AD a jeho zařazení do skupin
 - Detekce škodlivého kódu (bot) ve vnitřní síti
- ATP (Advanced Threat Protection) – funkcionalita, která vede k odhalení infikovaných stanic (botů) a je založena analýze provozu; někteří výrobci (stejně tak Sophos) nabízejí použití tzv. sand-boxu, tedy cloud prostředku do něhož je možné podezřelé aplikace posílat; zde je provedena analýza jejich chování a následně je UTMku odeslána zpráva o bezpečnosti aplikace
 - Omezování přístupu na web stránky podle jejich pověsti (reputace)
 - DLP (Data Leak Protection) neboli ochrana před ztrátou dat (souvisí i s funkcí kontrola přenosu souborů s přílohou)
 - Mailová brána s kontrolou škodlivého kódu v mailech, spamů a phishing mailů
 - Zabezpečení serverů publikovaných do internetu pomocí Web Application Firewall (WAF) funkcionality s ověřováním uživatelů

RSM CZ preferuje z velkého množství výrobců UTM technologii právě Sophos kvůli:

- Široké škále vlastností (jedna z nejširších na trhu)
- Vysokému výkonu (a tím pádem dobrému poměru cena / výkon)
- Unikátnímu řešení download anitviru – jako jediný výrobce umožňuje pro kontrolu použít dva nezávislé antiviry
- Snadné integraci do active directory
- Nejlepší možnosti náhrady Microsoft ISA / TMG díky integrovanému WAF

Sophos je společnost, která nabízí ucelenou škálu bezpečnostních prostředků, zaměřených na ochranu:

- Perimetru (sítě)
- Koncových stanic (anitvirus / HIPS / ...)
- Serverů – včetně virtualizovaného prostředí

Základní licenční informace

UTM Sophos může být buď formou:

- **Fyzické appliance;** pak není nijak omezeno množství IP v chráněné síti
- **Virtuální appliance** (nebo serverový modul včetně OS instalovaný přímo na server bez virtualizační vrstvy); pak je licenční omezení a platí se za počet uživatelů (v určité škále)



RSM CZ a.s.
Amazon Court – Karolinská 661,
186 00 Praha 8, Česká republika
T: +420 226 219 000
E: info@rsm.cz
W: www.rsm.cz
NONSTOP servisní linka:
+420 844 171 171