safe:LINK

TELEKOMUNIKAČNÉ SLUŽBY PRE VÁŠ BIZNIS

- bezpečnosť siete bez veľkých investícií
- bez starostí o správu a aktualizáciu
- pokrytie väčšiny druhov bezpečnostných hrozieb

Chranená sieť – bezpečné podnikanie

Internet sa stal bežným nástrojom, od ktorého závisí vaše podnikanie. S rozvojom jeho využívania prudko vzrástli aj riziká, ktoré túto komunikáciu ohrozujú. Nezabezpečené internetové pripojenie môže využiť zlomyseľný konkurent alebo šikovný hacker na odcudzenie alebo poškodenie citlivých informácií. Veľké firmy do ochrany investujú nemalé finančné prostriedky, no terčom útokov sa čoraz častejšie stávajú aj malé a stredné firmy.

Predíďte hrozbe časových a finančných strát a zabezpečte efektívnu ochranu vašej počítačovej siete a jej používateľov pomocou služby **safe:LINK**!

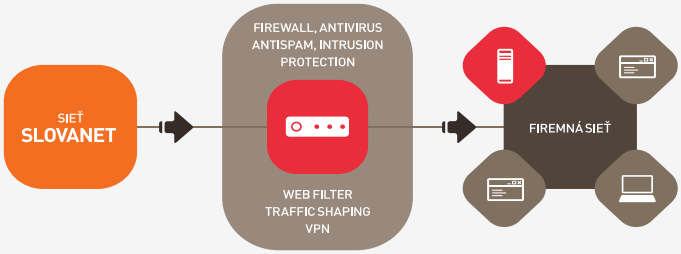
Istota a úspory

- profesionálne zabezpečená sieť bez veľkých investícií
- úspora personálnych nákladov či nákladov na outsourcing IT odborníka na bezpečnosť
- výhodná cena nezávislá od počtu používateľov v sieti
- komplexné integrované riešenie pokrýva ochranu vo všetkých oblastiach bezpečnostných hrozieb

Komplexná ochrana

- získate 12 základných bezpečnostných služieb – firewall, antivírus, prevenciu prienikov (IPS), antispam, antispyware, web filtering, kategorizovaný web filtering, traffic shaping, virtuálnu privátnu sieť, Data Leak Prevention, Network Access Control a Application Control
- vďaka variabilite služby získate riešenie podľa vašich potrieb s možnosťou nastavenia práv
- automatická aktualizácia bezpečnostných aplikácií
- efektívne využívanie pripojenia na pracovné účely
- ochrana pred nevyžiadanými a obťažujúcimi e-mailami

Technické riešenie



safe:LINK

TELEKOMUNIKAČNÉ SLUŽBY PRE VÁŠ BIZNIS

Bezpečnostné funkcie

Základným stavebným prvkom riešenia **safe:LINK** je vždy Next-Generation-Firewall (NGFW) chrániaci perimeter vašej siete. Obsahuje široký **balík bezpečnostných nástrojov**.

Antivírus

- ochrana pred vírusmi, červami a inými nebezpečnými aplikáciami
- kontrola všetkých komunikačných protokolov
- zachytenie nových vírusov už v deň, keď vzniknú vďaka početnému tímu, vyvíjajúcemu antivírusové signatúry po celom svete
- vysoká kvalita potvrdená stopercentným hodnotením od renomovaného časopisu Virus Bulletin

Firewall

- zabezpečenie siete proti útokom z vonkajšieho prostredia
- možné nastavenie na riadenie prístupu do internetu vhodné pre všetky typy sietí

Antispam

- zabezpečenie vašej e-mailovej schránky pred nevyžiadanou alebo obťažujúcou poštou
- úspora času s triedením a vymazávaním pošty
- vynikajúce vlastnosti ocenené cenou Product of the Year (Produkt roka) a cenou časopisu Network Computing

Riadenie internetovej prevádzky (traffic shaping)

- optimálne využitie šírky pásma
- záruka potrebnej rýchlosti pripojenia pre dôležité aplikácie

Virtuálna privátna sieť

- ochrana internej komunikácie vo vnútrofiremnej sieti
- bezpečná komunikácia pracovníkov v pobočkách v rôznych mestách, zamestnancov pripojených z domu alebo obchodných zástupcov na cestách

Filter obsahu webových stránok (web content filter)

- nastavenie prístupu vašich zamestnancov na webové stránky v závislosti od ich obsahu
- zvýšenie efektivity práce
- obrana pred neúčelným pripojením, ktoré môže zaťažovať vašu sieť
- nastaviteľné rôzne stupne filtrovania pre rôzne typy používateľov
- filtrovanie webstránok môže byť statické, dynamické na základe obsahu alebo na základe kategorizácie
- k dispozícii je 79 kategórií a zároveň možnosť vytvárať vlastné

Systém prevencie útokov IPS (intrusion preventing system)

- sledovanie a vyhodnocovanie prichádzajúcej komunikácie
- odvrátenie prichádzajúcich útokov ešte pred vstupom do siete
- parametre ocenené cenou za najlepšie IDS a IPS riešenie - Best Intrusion Detection and Prevention Solution

safe:LINK

TELEKOMUNIKAČNÉ SLUŽBY PRE VÁŠ BIZNIS

Nadstavbové piliere bezpečnosti

Analýza sieťovej prevádzky

Mať prehľad o tom, čo sa deje vo vašej sieti, môže byť v niektorých situáciách kriticky dôležité. Väčšina firiem sa na kontrolu „logov" obráti, až keď sa niečo deje. Vtedy je už ale spravidla neskoro.

Riešením je nástroj na efektívne sledovanie a vyhodnocovanie diania vo firemnej sieti. **FortiAnalyzer (FAZ)** dokáže v reálnom čase analyzovať logy z rôznych sieťových zariadení či ďalších prvkov riešenia **safe:LINK**. Umožňuje tak odhaľovať podozrivé správanie, identifikovať potenciálne hrozby a vytvárať komplexné reporty o bezpečnostných udalostiach.

Pokročilá analytika a upozornenia v reálnom čase umožňujú proaktívne riešenie potenciálnych zraniteľností.

Multi-faktorová autentifikácia (MFA)

Viacfaktorová autentifikácia (multi-factor authentication) je zásadným nástrojom pre zabezpečenie prístupu k dôverným informáciám, informačným systémom či vnútornej podnikovej sieti.

Zatiaľ čo tradičná jednofaktorová autentifikácia (meno a heslo) môže byť ľahko prelomená, viacfaktorová autentifikácia pridáva ďalšiu vrstvu ochrany. Kombinuje rôzne autentifikačné faktory, ako je biometria, tokeny alebo jednorazové kódy. Takáto kombinácia minimalizuje riziko neoprávneného vstupu.

Endpoint Management System (EMS)

Jedným z najčastejších zdrojov hrozieb v sieti sú koncové zariadenia. Podceniť ich zabezpečenie sa preto nevypláca.

Riešením je softvérový agent, ktorý koncovému zariadeniu (PC, mobilné zariadenia) poskytuje okrem antivírovej ochrany, aj dodržiavanie súladu s predpismi a bezpečný prístup v jednom modulárnom ľahkom klientovi.

Okrem samotnej ochrany agent umožňuje tiež bezpečné vzdialené pripojenie k vašej virtuálnej privátnej sieti (VPN).

V kombinácii s ďalšími piliermi **safe:LINK** možno automaticky presunúť infikované zariadenie do karantény, a zamedziť tak šíreniu hrozieb v sieti.

Data-Loss Prevention (DLP)

Data-Loss Prevention (DLP) je výkonný nástroj na ochranu dát pred únikom alebo nesprávnym použitím.

Monitoruje, analyzuje a kontroluje pohyb dát vo firemných sieťach a aplikáciách. Dokáže identifikovať citlivé informácie, ako sú osobné údaje, finančné údaje alebo obchodné tajomstvá, a uplatňovať prísne politiky ich ochrany. Ak sa zistí neoprávnený pohyb dát, ako napr. pokus o ich presun mimo internej siete alebo zdieľanie cez neautorizovaný kanál, DLP dokáže takýto pokus blokovať a upozorniť správcov siete.