

Bezpečnosť obsahu sieťovej prevádzky

Modul služieb Cisco ASA 5500 Series Content Security a Control Security CSC-SSM

Modul služieb CSC-SSM pre firewall Cisco ASA 5500 kombinuje komplexnú ochranu pred výskytom škodlivého kódu malware spolu so sofistikovanou kontrolou sieťovej prevádzky. Výsledkom je výkonné a vysoko bezpečné riešenie pre podniky a organizácie, ktoré zamedzí hrozbám ako sú vírusy, wormy, spyware, spam a phishing, zahŕňa kontrolu neželaných návštevníkov a kontrolu obsahu web stránok pri redukcii prevádzkových nákladov.

Prehľad vlastností

Cisco ASA 5550 bezpečnostný modul CSC SSM prináša bezpečnostnú ochranu na úrovni priemyselných štandardov a kontrolu obsahu pre internetové pripojenie komplexnou kombináciou prostriedkov ako antivírus, anti-spyware, blokovanie súborov, antispam, anti-phishing, URL blocking a filtering ako i content filtering, v efektívnom ľahko administrovateľnom riešení od popredných dodávateľov informačnej bezpečnosti. CSC-SSM modul rozširuje vysokú mieru bezpečnosti Cisco ASA 5500 firewallu o možnosti ochrany a kontroly obsahu firemnej komunikácie.

Prínosy CSC-SSM modulu:

- **Komplexná ochrana pred výskytom škodlivého kódu malware:** Zahŕňa špičkový antivírus a anti-spyware od spoločnosti Trend Micro. CSC-SSM zabráni virtuálne akémukoľvek škodlivému kódu preniknúť do vnútropodnikovej siete. Vysoká miera bezpečnosti Trend Micro technológie chráni pred výpadkami siete, garantuje plynulý chod biznis kritických aplikácií a minimalizuje riziko nákladov spojených s odstraňovaním následkov bezpečnostného incidentu.
- **Sofistikované filtrovanie obsahu:** Zahŕňa URL filtering, content filtering a anti-phishing technológie, vďaka ktorým sú dôležité procesy a senzitívne dáta chránané ako i individuálni užívatelia chránení pred bezpečnostnými rizikami úniku dát v súlade s bezpečnostnou politikou vo firme zosúladenou s legislatívou.
- **Integrovaná bezpečnosť správ a mailov:** Zahŕňa anti-spam technológiu, vďaka ktorej sa odstráni nevyžiadaná elektronická pošta spam, čo šetrí náklady na mail server prevádzku, zvyšuje produktivitu zamestnancov a eliminuje riziko plyvania sieťovou priepustnosťou a kapacitami dátových úložísk.
- **Customizácia a konfigurovateľnosť nastavení:** Poskytuje administrátorom priestor na špecifikáciu bezpečnostnej politiky spoločnosti v súvislosti so spamom a kontrolou obsahu.
- **Efektívny manažment a automatická aktualizácia:** Dodáva sa v prednastavenom móde, ktorý je možné jednoducho upraviť podľa svojich potrieb vďaka intuitívnemu administratívemu rozhraniu (nástroj Adaptive Security Device Manager ASDM). Automatické aktualizácie a updaty vrátane scanning enginov a signatúr garantujú, že sieť je neustále zabezpečená proti najnovším typom útokov s minimálnou administratívnou záťažou.

Kľúčové vlastnosti a prínosy riešenia:

vlastnosť	Prínos
Antivírus	Špičková antivírusová technológia chráni internú sieť pred hrozbou šírenia vírusov v najefektívnejšom mieste infraštruktúry, na hranici internetového pripojenia. Vyčistenie mailovej a webovej komunikácie na perimetri garantuje kontinuitu podnikových procesov a eliminuje nákladné odstraňovanie následkov šírenia malware infekcie.
Anti-Spyware	Blokuje spyware pred vstupom do siete prostredníctvom mailovej a webovej komunikácie. Dovoľuje tak ušetriť podporné prostriedky IT v spoločnosti zamedzením nákladného odstraňovania následkov škodlivej funkcie spyware zablokovaním na úrovni internet brány.

Anti-Spam	Efektívne blokuje nevyžiadajú poшту spam. Výskyt falošne označených správ je skutočne minimalizovaný. Zvýši sa tak efektívnosť mailovej komunikácie, takže kontakt so zákazníkmi, dodávateľmi a partnermi nie je narušený neželanými efektami.
Anti-Phishing	Ochrana pred zneužitím cudzej identity s aktívnou ochranou pred phishing útokmi formou nastražených web stránok zabráni užívateľom vo firme vyraziť senzitivne údaje a heslá, čím sa zamedzí výskytu finančných škôd a pod.
Automatické aktualizácie z TrendLabs	S profesionálnou podporou 24x7 jedného z najväčších tímov expertných špecialistov na hrozby typu vírusy, spyware a spam je garantovaná neustála automatická ochrana.
Centrálna administrácia	Jednoduchá administrácia formou – nastav a zabudni – cez web konzolu a automatické aktualizácie, čo šetrí náklady na prevádzku pri garancii stálej bezpečnosti.
Ochrana v reálnom čase pre web, mail a prenos súborov	Dokonca aj pri zabezpečenom firemnom emaili si zamestnanci zvyknú pristupovať na rôzne webmail služby z firemných PC, čo predstavuje ďalší zdroj bezpečnostných rizík. Zamestnanci sa môžu tiež pokúšať sťahovať rôzne neautorizované programy alebo kontaminované súbory z netu. Ochrana v reálnom čase pre všetku web komunikáciu na úrovni internetovej brány dokáže tieto riziká eliminovať a zredukovať ich dopady na minimum.
Plný URL Filtering s kategorizáciou, plánovaním a vyrovnávacou pamäťou (Caching)	URL filtering umožňuje kontrolovať používanie internetu zamestnancom pomocou blokovania nevhodných stránok, čím sa zvyšuje produktivita a obmedzí riziko stiahnutia škodlivého kódu, či návštevy stránky s nelegálnym obsahom.
E-Mail Content Filtering	E-mail filtering minimalizuje právne riziká spôsobené prenosom ofenzívnych správ v mailoch a prináša súlad s legislatívnymi normami ako i bezpečnostnou politikou spoločnosti.

Viac informácií nájdete na stránke www.cisco.com/go/asa