T-SYSTEMS ADAPTIVE SECURITY FRAMEWORK (ASF)

T · · Systems ·

A T-Systems Magyarország Zrt. biztonsági terméke az informatikai biztonság egy komplex és egyre gyakrabban jelentkező problémájának megoldásához hozza közelebb ügyfeleit. A biztonsági termékek riasztásainak, naplóadatainak feldolgozása és a megfelelő incidenskezelés a legtöbb szervezet számára nagyon nehezen kezelhető kérdés.

A problémának több oka van:

- A biztonsági termékek nem egységesek az általuk készített naplóadatok külső eszközzel történő feldolgozását illetően.
- A biztonsági eszközök „beszédesek", még a szakemberek számára is nehéz kiszűrni a valós riasztásokat a vaklármák közül.
- A biztonsági rendszerekben keletkező incidensek megfelelő kezelése komoly kihívás elé állítja az ügyfelek szakembereit.

Erre a problémára válaszolva a T-Systems Magyarország Zrt. munkatársai egy olyan keretrendszert terveztek meg, amely az ismert biztonsági megoldások számára biztosítja azt a lehetőséget, hogy – amennyiben az ügyfél szeretné – beköthetőek legyenek a TSystems MIBS (Menedzselt Informatikai Biztonsági Szolgáltatás) rendszerébe. Ez a megközelítés lehetővé teszi, hogy a T-Systems által ajánlott megoldások képesek legyenek naplóadataik és incidenseik szolgáltatás keretében történő feldolgozására.

A megoldás neve ASF (Adaptive Security Framework, vagyis Alkalmazkodó Biztonsági Keretrendszer), amely olyan informatikai biztonsági megoldásokat kínál az ügyfelek számára, amelyek fel vannak készítve egy esetleges incidenskezelési szolgáltatás igénybevételére. Ezek a megoldások modulként épülnek be az ASF keretrendszerébe. A modulok kialakításánál a T-Systems több mint húszéves informatikai rendszer-integrációs tapasztalatára alapozva választotta ki azokat a piaci megoldásokat, amelyek alkalmasak a feladatra. Ezért az elvárható szakmai teljesség jegyében az alkalmazott modulok között megtalálhatóak a biztonsági események megakadályozására, az incidensek jelzésére és a kockázatok további kezelésére alkalmas megoldások. A jelenleg elérhető ASF-termékek az alábbi információbiztonsági területeket fedik le:

- biztonsági incidensek és események kezelése,
- adatszivárgás elleni védelem,
- tűzfalas védelem,
- erős authentikáció,
- biztonságos kulcstárolás,
- időbélyegzés.

A T-Systems abban a reményben dolgozik az ASF-megoldáson, hogy az államigazgatási szervezetek és a vállalatok számára a biztonság megteremtése mellett egyre fontosabbá válik az incidensek kezelése, amelyet a jövőben szolgáltatásként vesznek igénybe. Az ASF egy ilyen szolgáltatás igénybevételének műszaki feltételeire biztosít lehetőséget, miközben olyan világszínvonalú informatikai biztonsági modulokat kínál, amelyek megfelelően kezelik a biztonsági kockázatokat.

MENEDZSELT INFORMATIKAI BIZTONSÁGI SZOLGÁLTATÁSOK (MIBS)

A T-Systems menedzselt informatikai biztonsági szolgáltatását (továbbiakban MIBS) azzal a céllal hoztuk létre, hogy egyetlen szolgáltatás keretében képes legyen biztosítani mindazon informatikai biztonsági tevékenységeket, amelyek hatékony és megbízható végrehajtása speciális, magas szintű, naprakész informatikai biztonsági szaktudást és többéves szakmai tapasztalatot igényel. A komplex szolgáltatáscsomag egyes szolgáltatásai modulárisan, az egyedi igényeiknek megfelelően választhatóak ki és kombinálhatóak.

A T-Systems által nyújtott menedzselt informatikai biztonsági szolgáltatás a hagyományos tanácsadási, rendszer-integrációs és támogatási szolgáltatásokon túlmutatva elsősorban olyan szolgáltatásokat foglal magában, amelyek a felügyelt rendszerek biztonsági állapotának nyomon követését, kiértékelését, valamint egy esetleges biztonsági incidens bekövetkezése esetén az incidens mielőbb elhárításának támogatását biztosítják. Ezenfelül a MIBS olyan szolgáltatások igénybevételére is lehetőséget teremt, amelyek a biztonsági sérülékenységek időben (a sérülékenység kihasználását megelőzően) történő feltárását és elhárítását teszik lehetővé.

Az egyes szolgáltatások egymásra épülését a következő ábra mutatja be:

A továbbiakban a MIBS-hez illeszthető ASF keretrendszer egyes moduljait mutatjuk be.

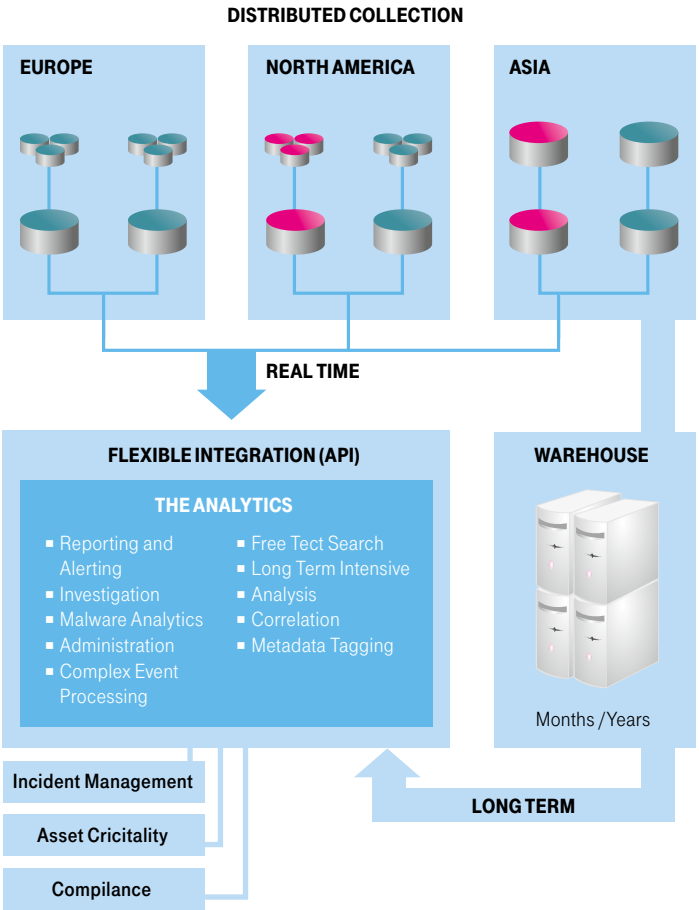
INFORMÁCIÓBIZTONSÁGI INCIDENSEK ÉS ESEMÉNYEK KEZELÉSE – RSA SECURITY ANALYTICS MODULLAL

Ma, a folyamatosan növekvő számú és bonyolultságú fenyegetettségek világában létfontosságú, hogy biztonságos infrastruktúrát üzemeltessünk. Ehhez pedig a logok, sessioninformációk begyűjtése, tárolása, elemzése ugyanúgy hozzátartozik, mint az analízist segítő adattárházak és az intelligens előrejelzések. Mindezek mellett a compliance-követelmények is egyre szigorodnak. Mindez megfűszerezve az egyre komplexebb infrastruktúrával teljes embert kíván. Azonban a Big Data-koncepció és az ezzel járó analizáló és intelligens alkalmazások talán könnyebbé tehetik a szakemberek munkáját. Meg kell érteni a beérkező logokat, azok minél gyorsabb feldolgozása szükséges (és persze tárolni is kell a keletkezett eseményeket). Ezért minél nagyobb segítséget kell nyújtani a szakembereknek, hogy hatékonyan dolgozzanak, a vállalatunk védelme megoldott legyen.

A T-Systems a kihívásokra válaszolva integrálta ASF keretrendszerébe az RSA Security Analytics (továbbiakban SA) platformot, mely almoduljaival segítséget nyújt a feladatok leküzdésében.

Az SA-platform az alábbi almodulokból épül fel:
- Decoder (logokra és teljes hálózati csomagforgalomra)
- Concentrator
- Broker

Mindegyik komponens kulcsfontosságú, hiszen a stabil, skálázható, redundáns kiépítéshez mindhárom részre szükség van. Persze a valós idejű elemzésekhez, alkalmazásszintű logokhoz a megfelelő infrastruktúra is elengedhetetlen. Az SA-megoldás skálázható, hogy az igazán nagy vállalatok igényeit is ki tudja elégíteni, és hierarchikus, hogy könnyen átlátható legyen.



DECODER

A Decoder a legelső, legalapvetőbb komponense az SA-rendszernek. Nemcsak a logok, de a hálózati csomagok gyűjtésére is alkalmas (ezek azonban külön hardveren futnak alapértelmezetten), sőt a további analízist is segíti. Minden olyan telephelyre, hálózati tartományba, zónába kell egy Decoder, ahonnan logot, sessioninformációt szeretnénk gyűjteni. A Packet Decoder hálózati csomagokat gyűjt, normalizál, indexel, mindezt az OSI 2–7. rétegében. A Packet Decoder folyamatosan képes a forgalom elemzésére. A Log Decoder hálózati logok gyűjtésére, indexelésére lett kifejlesztve, több mint 200 típust és formátumot támogat. A Decoder-eszközök által összegyűjtött információk indexelésével alkalmazás, felhasználó, forrás, cél, esemény, log alapján is kereshetünk, készíthetünk kimutatásokat. Compliance- és tárolási követelmények is kielégíthetők az SA-szerverrel kombinálva.

CONCENTRATOR

A Concentratorok a Decoder-komponensekből származó adatok aggregálására képesek. Hierarchikus felépítésük miatt rugalmasabban skálázhatók. Egyetlen Concentrator több Decoderrel is állhat kapcsolatban, de vagy csak log, vagy csak packet aggregálására alkalmas a dedikált Concentrator.

BROKER ÉS SECURITY ANALYTICS SZERVER

A Broker és a Security Analytics szerver alapértelmezetten egyetlen hardveren futtatható, és ezen komponensek a legmagasabb hierarchiaszinten lévő modulok. A Broker szerver funkciója a lekérdezések, elemzések, kimutatások futtatása, ha több Decoder, Concentrator található a rendszerben. A Brokerek segítségével az összes metadata lekérdezhető, függetlenül a hálózat kiépítésétől (késleltetés, sávszélesség, adatmennyiség). A Security Analytics szerver a felhasználói felületet, konzolt kezeli, ezzel a discovery, investigation, reporting és administration menü érhető el. Támogatja a role based elérést és a kétfaktoros azonosítást is (HMTL5-alapú). Továbbá adattárházak esetén az ezzel kapcsolatos tevékenységek is erről a felületről indíthatóak.

HOSSZÚ TÁVÚ ADATTÁROLÁS ÉS INTENZÍV ANALÍZISEK

Az RSA Security Analytics Warehouse egy opcionális komponens a meglévő SA-rendszer mellé. Hosszú távú archiválásra, előrejelzések, riportok készítésére, testre szabott analízisek futtatására alkalmas. A Hadoop technológiának köszönhetően párhuzamos szálak futtatásával nagyon jól méretezhető nagymennyiségű adathalmaz elemzésére is. Több storage opció is elérhető az adattárházhoz, így illeszthető az elvárásokhoz a tárolórendszer is (akár évekre visszamenőlegesen is képes adattárolásra). Eltérően a hagyományos SIEM-megoldásoktól, itt nemcsak a storage méretezésére van szükség, de az úgynevezett Warehouse node-okra is (elosztott adathalmazokon, szeparáltan futnak az elemzések). Minden egyes node dedikált adathalmazért felel, így a node-ok számának növelésével a teljesítmény növelhető.

További technikai információk:
http://hungary.emc.com/security/security-analytics/security-analytics.htm.

ADATSZIVÁRGÁS ELLENI VÉDELEM – RSA DLP MODULLAL

A vállalatok mindennapi működésük során különböző erőforrásokat használnak fel üzleti céljaik eléréséhez. Az erőforrások közül kiemelt jelentőséggel bír mindaz az információ, amelyet a szervezet napi tevékenysége során rögzít, feldolgoz, továbbít, tárol vagy töröl. Ezek az információk azonban véletlenül (például, ha a munkatárs rossz e-mail címre továbbít egy dokumentumot) vagy szándékosan (például, ha a munkatárs a titkos anyagokat USB-kulcsra lementve elviszi) nyilvánosságra kerülhetnek. Egy ilyen esemény kritikus lehet a szervezet üzletmenet-folytonossága és biztonságos működése szempontjából, mivel egy ilyen jellegű incidens az üzleti pozíció, illetve az ügyfelek bizalmának elvesztését vagy a jó hírnév sérülését eredményezheti. Az adatok kiszivárgásának okai szerteágazóak, azonban közös jellemzőjük, hogy a szervezet által alkalmazott védelmi intézkedések hiányosságai teszik lehetővé az ilyen események bekövetkezését.

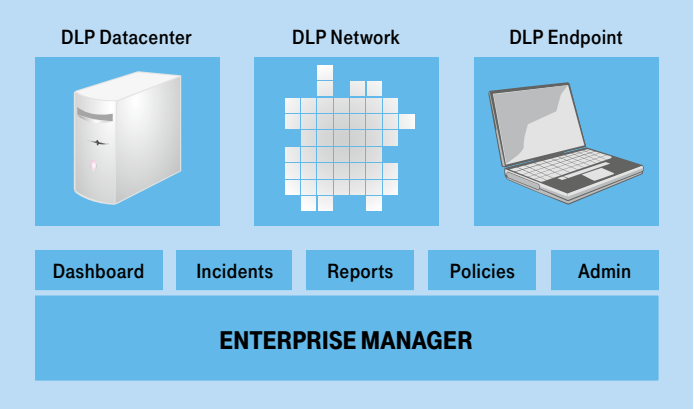
A T-Systems a kihívásokra válaszolva integrálta ASF keretrendszerébe az RSA Data Loss Prevention Suite (továbbiakban DLP) platformot, mely almoduljaival segítséget nyújt a feladatok leküzdésében.

A T-Systems adatszivárgás elleni védelmi moduljának alkalmazásával felismerheti a vállalatánál jelen levő veszélyeket, amelyek bizalmas adatainak elvesztését vagy kiszivárgását eredményezhetik. A megoldás egy szabályalapú eljárással védi meg azokat az adatokat, amelyeket az ügyfél bizalmasnak osztályoz, felügyeli ezeket, majd riportál és auditál, hogy ezzel biztosítsa a biztonsági szabályzatnak való megfelelést. A DLP az alábbiakat nyújtja:

- Bizalmas vállalati adatok meghatározása és védelme: közös policyk alkalmazásával védi meg az adatközpontban, a hálózaton és a végpontokon tárolt bizalmas adatokat.
- Kockázatcsökkentés: a policyk alkalmazásával és betartatásával csökkenti az adatvesztés kockázatát.
- Csökkenti az üzemeltetés (TCO) költségeit: kitűnő skálázhatóságával, a bizalmas adatok automatikus védelmével és a piacon elérhető átfogó policykönyvtárával csökkenti az üzemeltetési költségeket.
- Egyszerűsíti a biztonsági tevékenységeket: összhangba hozza a biztonsági processzeket az incidenskezeléssel és a munkafolyamatokkal.

A DLP MODUL KOMPONENSEI:

- DLP Datacenter – felderíti a file share-eken, adatbázisokban, adattároló rendszerekben (SAN/NAS), Microsoft SharePoint portálokon és egyéb adattárházakban található érzékeny adatokat, és szabályrendszereket alkalmaz rájuk.
- DLP Network – felderíti az e-mailekben, weboldalakon, ftp-szervereken, messagingszolgáltatásokban és webportálokon található érzékeny adatokat, és szabályrendszereket alkalmaz rájuk.
- DLP Endpoint – felderíti a felhasználói munkaállomásokon található érzékeny adatokat, és szabályrendszereket alkalmaz rájuk.



RSA Data Loss Prevention Suite

A DLP Datacenter komponensei:

- Enterprise Coordinator – menedzseli a telepített Site Coordinatorok tevékenységét, feltölti a konfigurációs információkat és a policyket, valamint fogadja a Site Coordinatoroktól a keresési eredményeket.
- Site Coordinator – helyi adminisztratív modul, mely menedzseli az agentek, grid workerek tevékenységét, ütemezi a kereséseket, fogadja az agentek felől a keresési eredményeket és továbbítja azokat az Enterprise Coordinatornak.
- Scanning agents – a végpontokon futó kisméretű ügynökprogram, mely detektálja az érzékeny adatokat.
- Grid workers – speciális célú scanning agent, mely nagy adattárházak analizálását végzi.

Az Enterprise Coordinator menedzseli a földrajzilag szétszórt Site Coordinatorokat. A Site Coordinatorok menedzselik a lokális agent-scan csoportokat, melyek egyenként akár többezer egyedi munkaállomást tartalmazhatnak, melyek mindegyikén fut egy agent. A Site Coordinatorok menedzselik a grid-scan csoportokat, melyek a grid workersek segítségével szkennelik a nagyméretű fájlmegosztásokat. Továbbá a Site Coordinatorok feladata a repository-scan csoportok, valamint a database-scan csoportok menedzselése, melyek védett adattárházakat (SharePoint, Oracle, SQL stb.) és adatbázisokat tartalmaznak.

A DLP Network komponensei:

- Network Controller – a fő appliance, amely karbantartja az információkat az érzékeny adatokról és a tartalomalapú szabályokról.
- Sensor – a hálózat határába telepítendő eszköz, mely folyamatosan monitorozza a kimenő forgalmat és detektálja az érzékeny tartalmakat. Csak monitorozásra alkalmas.
- Interceptor – inline mail transfer agent, mely monitorozza, blokkolja, vagy karanténba helyezi a kimenő érzékeny tartalmú leveleket. Alkalmazható e-mail encryption gatewayjel együtt levéltitkosításra.
- ICAP Server – web proxy szerverhez társítva monitorozza, illetve blokkolja a http, https és ftp protokollokon zajló, érzékeny tartalmú webes feltöltéseket.

A DLP Endpoint komponensei:

- Enterprise Coordinator és Endpoint Coordinator – szükséges egy Enterprise Coordinator, mely menedzseli a földrajzilag szétszórt Endpoint Coordinatorokat, melyek agentek segítségével menedzselik a végponti munkaállomásokat.
- Enforcement agents – a munkaállomásokon futó kis ügynökprogramok, melyek kikényszerítik az érzékeny adatok védelmére beállított szabályrendszert.

AZ RSA DLP ÁLTALÁNOS TULAJDONSÁGAI

- Moduláris bevezethetőség. A modulok egymástól függetlenül bevezethetők.
- Magyar nyelv és speciális karakterkészletek támogatása.
- Valós idejű incidensdetektálás a végpontokon és/vagy a hálózaton.
- Bizonyítékok eltárolásának lehetősége.
- Automatizált és manuális riportkészítési funkciók.
- Együttműködési lehetőség meglévő naplógyűjtő és elemző rendszerekkel.
- Az egyes modulok központi menedzselésének lehetősége.
- Eltávolítható médiák (USB, CD/DVD stb.) szabályozásának – monitorozás, figyelmeztetés, blokkolás – lehetősége.
- Vágólapi műveletek (cut, copy, paste, print screen) szabályozása.
- Webmailre történő feltöltés szabályozása.
- Azonnali üzenetküldés (Skype stb.) szűrésének lehetősége.
- Érzékeny adatok nyomtatásának szabályozása.
- Adatbázis-tartalom felismerésének lehetősége.

További technikai információ:
http://hungary.emc.com/security/rsa-data-loss-prevention.htm

ADATSZIVÁRGÁS ELLENI VÉDELEM – SYMANTEC DLP MODULLAL

A vállalatok mindennapi működésük során különböző erőforrásokat használnak fel üzleti céljaik eléréséhez. Az erőforrások közül kiemelt jelentőséggel bír mindaz az információ, amelyet a szervezet napi tevékenysége során rögzít, feldolgoz, továbbít, tárol vagy töröl.
Ezek az információk azonban véletlenül (például, ha a munkatárs rossz e-mail címre továbbít egy dokumentumot) vagy szándékosan (például, ha a munkatárs a titkos anyagokat USB-kulcsra lementve elviszi) nyilvánosságra kerülhetnek. Egy ilyen esemény kritikus lehet a szervezet üzletmenet-folytonossága és biztonságos működése szempontjából, mivel egy ilyen jellegű incidens az üzleti pozíció, illetve az ügyfelek bizalmának elvesztését vagy a jó hírnév sérülését eredményezheti.
Az adatok kiszivárgásának okai szerteágazóak, azonban közös jellemzőjük, hogy a szervezet által alkalmazott védelmi intézkedések hiányosságai teszik lehetővé az ilyen események bekövetkezését.

A T-Systems a kihívásokra válaszolva integrálta ASF keretrendszerébe az RSA DLP mellett a Symantec Data Loss Prevention (továbbiakban DLP) platformot, mely almoduljaival segítséget nyújt a feladatok leküzdésében.

A T-Systems adatszivárgás elleni védelmi modul alkalmazásával felismerheti a vállalatánál jelen levő veszélyeket, amelyek bizalmas adatainak elvesztését vagy kiszivárgását eredményezhetik. A megoldás egy szabályalapú eljárással védi meg azokat az adatokat, amelyeket az ügyfél bizalmasnak osztályoz, felügyeli ezeket, majd iportál és auditál, hogy ezzel biztosítsa a biztonsági szabályzatnak való megfelelést. A DLP az alábbiakat nyújtja:

- Bizalmas vállalati adatok meghatározása és védelme: közös policyk alkalmazásával védi meg az adatközpontban, a hálózaton és a végpontokon tárolt bizalmas adatokat.
- Kockázatcsökkentés: a policyk alkalmazásával és betartatásával csökkenti az adatvesztés kockázatát.
- Csökkenti az üzemeltetés (TCO) költségeit: kitűnő skálázhatóságával, a bizalmas adatok automatikus védelmével és a piacon elérhető átfogó policykönyvtárával csökkenti az üzemeltetési költségeket.
- Egyszerűsíti a biztonsági tevékenységeket: összhangba hozza a biztonsági processzeket az incidenskezeléssel és a munkafolyamatokkal.

A Symantec Data Loss Prevention integrált DLP-programcsomag az adatokat nyugalmi állapotukban, mozgásuk közben és a végponton általános érvényű, önműködően betartatott DLP-szabályokkal védi, melyeket egy központi platformról szolgáltat. Ezek a DLP-szabályok az észlelés, a folyamatszabályozás és az automatizálás, valamint a jelentéskészítés, a rendszervezérlés és a védelem célját szolgálják.
A végponton a Symantec DLP felderíti a hordozható és asztali gépeken tárolt bizalmas adatokat, a további védelem céljából besorolja a nagy veszélynek kitett végpontokat, valamint megakadályozza a bizalmas adatok USB-eszközre másolását, CD-re vagy DVD-re írását és helyi merevlemezre történő letöltését. A fájlszervereken, adatbázisokban, webszervereken és sok más adattárban levő, veszélynek kitett bizalmas adatok felderítését és megóvását a DLP-re bízó vállalatok az egész cégnél meg tudják találni és meg tudják védeni a veszélyeztetett bizalmas adatokat. A cégek a hálózaton az email, a közvetlen üzenet-, a weblap- és a biztonságos weblap- (HTTPS), az FTP-, a P2P- és az általános TCP-forgalomban történő adatvesztést is minden részletre kiterjedően figyelemmel kísérhetik, illetve megelőzhetik.

A Symantec jelenlegi termékei végponti, valamint hálózati szinten is képesek a bizalmas információk mozgását figyelni, és beavatkozni abban az esetben, ha azokat esetleg valaki notebookon vagy valamilyen adattárolón akarná kijuttatni a védett rendszerből.

A SYMANTEC DLP MEGOLDÁS AZ ALÁBBI KOMPONENSEKBŐL ÁLL:

Symantec Data Loss Prevention Enforce Platform

Egységes átfogó, központosított menedzsmentplatform a szabályrendszer-konfiguráláshoz, detektáláshoz, incidenskezelési workflow- és automatizálási, jelentéskészítési, rendszermenedzsment- és biztonsági feladatok ellátásához.

Symantec Data Loss Prevention Network Discover

Segítségével gyorsan felderíthető a veszélynek kitett bizalmas információ, bárhol is van tárolva a vállalatok által használt adatformákban, tárolókban, beleértve a szervereket, adatbázisokat, dokumentummenedzsment megoldásokat, e-mail tárolókat és webes alkalmazásokat.

Symantec Data Loss Prevention Endpoint Discover

Segítségével feltérképezhetjük a fontos adatainkat, amelyek a végpontokon vannak tárolva, használva, beleértve a laptopokat, munkaállomásokat – hogy leltározhassuk, megvédjük vagy áthelyezzük ezeket az adatokat.

Symantec Data Loss Prevention Network Monitor

Folyamatosan vizsgálja a teljes hálózati kommunikációt, beleértve az e-mail, IM-, web-, FTP-, P2P-, általános TCP-adatforgalmat, hogy felismerje a fontos adatokat és a szabályrendszer alapján megvédje azokat.

Symantec Data Loss Prevention Endpoint Prevent

Megakadályozza a védett adatok átvitelét e-mail, IM-, webcsatornákon, vagy másolásukat USB, CompactFlash, SD vagy egyéb cserélhető adathordozóra, valamint kiírásukat CD/DVD médiára, copy/paste használatát, a print screen funkció használatát, illetve a faxolást vagy nyomtatást. Automatikus értesítést küld a felhasználónak e-mail vagy felugró ablak üzenet formájában, hogy segítse, építse a felhasználó biztonságtudatosságát. Beépített szabályokkal támogatja pl. a PCI-DSS szabályok betartatását. Megelőzi, hogy érzékeny adatokat a dolgozó a védett helyről véletlenül átmásoljon egy nem megbízható környezetbe.

Symantec Data Loss Prevention Network Prevent

Minden olyan hálózati kommunikációt, amely megsérti az adatbiztonsági szabályzatot, proaktívan megakadályoz, feltételrendszer alapján eltávolítva a védett tartalmat, vagy átirányítva a bizalmas adatokat tartalmazó levelezést egy titkosító rendszerhez.

Symantec Data Loss Prevention Network Protect

Automatikusan védi a különféle tárolókban található adatokat, szükség szerint karanténba helyezi, átmásolja, eltávolítja vagy titkosítja.

A SYMANTEC DLP ÁLTALÁNOS TULAJDONSÁGAI

- Moduláris bevezethetőség. A modulok egymástól függetlenül bevezethetők.
- Magyar nyelv és speciális karakterkészletek támogatása.
- Valós idejű incidensdetektálás a végpontokon és/vagy a hálózaton.
- Bizonyítékok eltárolásának lehetősége.
- Automatizált és manuális riportkészítési funkciók.
- Együttműködési lehetőség meglévő naplógyűjtő és elemző rendszerekkel.
- Az egyes modulok központi menedzselésének lehetősége.
- Eltávolítható médiák (USB, CD/DVD stb.) szabályozásának – monitorozás, figyelmeztetés, blokkolás – lehetősége.
- Külső adathordozók titkosításának lehetősége.
- Vágólapi műveletek (cut, copy, paste, print screen) szabályozása.
- Webmailre történő feltöltés szabályozása.
- Azonnali üzenetküldés (Skype stb.) szűrésének lehetősége.
- Érzékeny adatok nyomtatásának szabályozása.
- Adatbázis-tartalom felismerésének lehetősége.

További technikai információk:
http://www.symantec.com/data-loss-prevention

ERŐS AUTHENTIKÁCIÓ – RSA AUTHENTICATION MANAGER ÉS SECUREID MODULOKKAL

A T-Systems ASF erős authentikációs moduljai segítségével a felhasználók nemcsak felhasználónév/jelszó párossal azonosítják magukat, hanem az ennél biztonságosabb kétfaktoros azonosítást használják. A megoldás számos előnye közül a legfontosabb, hogy a felhasználókat nem kényszerítjük bonyolult jelszavak megjegyzésére – aminek egyenes következménye a könnyen kitalálható vagy monitor szélére ragasztott, értéktelen jelszó. Mivel a felhasználókat nem terheljük komplex jelszavak megjegyzésével, a megoldás használata kényelmes, nem csak biztonságos. Az üzemeltetés feladatait is csökkenti, mivel az elfelejtett jelszavak visszaállításából fakadó terhelés lényegében megszüntethető.

RSA Authentication Manager

A modul központi eleme az RSA Authentication Manager, amely tárolja a használatban lévő tokenek azonosítóit, a felhasználóneveket (LDAP-integráció is lehetséges), valamint a tokenekre és felhasználókra vonatkozó házirendeket (azaz melyik felhasználóhoz melyik token[ek] vannak hozzárendelve, és az adott felhasználó mely határpontokon jogosult belépni).

Az RSA Authentication Agentek, amelyek egyfajta „kapuőrnek” tekinthetők, továbbítják a felhasználó által megadott felhasználónevet, PIN kódot és a token által generált számsorozatot az RSA Authentication Managernek.

Ezt a komponenst minden egyes olyan szerverre, tűzfalra, kliensre telepíteni kell, amelyen kétfaktoros azonosítást szeretnénk. A támogatott alkalmazások köre rendkívül széles. Szükség esetén RADIUS-os hitelesítés is megvalósítható. Az agentek beágyazásra kerülnek a legtöbb nagyobb hálózati-kommunikációs termékbe, beleértve a legtöbb VPN-képes eszközt, tűzfalat és egyebeket. Az RSA Authentication Manager ideális megoldás azon szervezetek számára, amelyek erős felhasználóazonosítást keresnek Microsoft operációs rendszerekbe történő belépéshez. A Microsoft Windows környezetre fejlesztett SecurID for Microsoft Windows megoldás lehetővé teszi a kétfaktoros azonosítás alkalmazását Microsoft Windows-alapú környezetben akár offline (tartománytól távoli) bejelentkezés esetén is. RSA Authentication Manager szoftvert úgy tervezték, hogy bármilyen méretű szervezet igényeinek megfeleljen. Az RSA Authentication Manager szoftver minimális számú, alig huszonöt felhasználótól kezdve akár több millió felhasználót, valamint akár több száz egyidejű felhasználói azonosítást is képes kezelni szerverenként. Az RSA megoldását világszerte több mint húszezer ügyfélnél vezették be (bankokban, kormányzatban, iparban, egészséggondozásban).

RSA SecureID token

Az RSA SecurID token egy speciális eszköz, mely 60 másodpercenként egy 6 számból álló sorozatot állít elő, ezt kell a felhasználónak azonosítás céljából megadnia. Ezzel a módszerrel elérhető, hogy a felhasználónak biztosan rendelkeznie kell a tokennel, hiszen 60 másodperc elteltével az – esetlegesen – megjegyzett számsorozat már nem érvényes. Minden RSA SecurID token rendelkezik egy nagy teljesítményű algoritmussal kombinált, egyedi szimmetrikus kulccsal, amely 60 másodpercenként új kódot generál. Mivel a szám megjósolhatatlan és dinamikus, a hacker számára kivételesen nehéz feladatot jelent a helyes számot kitalálni bármely adott időben. A megoldás minden tokent összeszinkronizál a biztonsági szerverrel, így garantálva a biztonság magas szintjét.

Kétféle tokentípus ismert:

Hardvertokenek
Az RSA SecurID hardvertokenek előzetes ismereteket nem igénylő megoldások, melyeknek nincs egyéb szoftverre szükségük a felhasználó számítógépén, így az eszközök átvételkor azonnal működőképesek.

Szoftvertokenek
A szoftveralapú megoldások a hardvertokenekkel megegyező algoritmust használnak. Költséghatékony megoldást jelentenek olcsóbb egységáruk és a hardvertokenek esetleges elvesztésével járó többletköltségek megtakarítása révén. A szoftvertokenek rendkívüli kényelmet biztosítanak, mivel telepíthetőek akár a célalkalmazás elérésére használt számítógépekre, akár mobileszközökre.

További technikai információk:
http://hungary.emc.com/security/rsa-securid/rsa-authentication-manager.htm,
http://hungary.emc.com/security/rsa-securid.htm

TŰZFALAS VÉDELEM – FORTINET FORTIGATE MODULLAL

A nagy és kis cégek, nyilvános és magánszektorbeliek egyaránt, új veszélyekkel néznek szembe az általánosan használt és elterjedt alkalmazások frontja felől, ami a közösségi hálózatokban és azok össze- és keresztülkapcsoltságában rejlik. Ezek kiváló táptalajt jelentenek nemcsak a malware-ek terjedéséhez, de ipari kémkedéshez vagy szimpla adathalászathoz is, amely a felhasználókon keresztül benyúlik a cégek belsejébe. Mindeközben a munkavállalók az otthoni és a céges számítógépeiket is előszeretettel használják blogolásra, ismerkedésre, üzengetésre, videózásra, zenehallgatásra, vásárlásra, levelezésre...
Az olyan dolgok, mint a streaming video (YouTube...), P2P és a hosztolt, felhőalapú alkalmazások mind újabb és újabb támadási felületet nyújtanak, amelyek behatolások és adatkiszivárogtatások számára sebezhetővé tehetik a céget, vagy akár hálózati leállásokat, lassulásokat is okozhatnak. Ennek tetejében pedig ezek az alkalmazások komoly sávszélességeket fogyasztanak, versenyeznek a kritikus alkalmazásokkal az erőforrásokért, valamint munkamoráltól függően akár a termelékenységet is gátolhatják. A kockázatok csökkentése érdekében szükség van olyan eszközökre, amelyek intelligens módon képesek vizsgálni, osztályozni, irányítani és védeni mind a kimenő, mind pedig a bejövő adatfolyamokat – de ez nem mehet a sebesség és a termelékenység rovására.

A T-Systems a kihívásokra válaszolva integrálta ASF keretrendszerébe a FortiNet FortiGate UTM-termékcsaládot, mely segítséget nyújt a feladatok leküzdésében.

A Unified Threat Management (UTM) megoldások célja, hogy egy integrált eszközben nyújtsanak olyan hálózatbiztonsági funkciókat, amelyek megvédik a vállalati infrastruktúrát a legösszetettebb fenyegetésekkel szemben is. Azonban a sávszélességek növekedése miatt – hiszen ma már nem ritka a 100-120 Mbit/sec sebességű internetkapcsolat sem – az UTM-eszközök teljesítménye a legtöbb esetben nem elegendő a valós idejű hálózatbiztonsági szolgáltatások megvalósításához.
A probléma magából az UTM-megoldások architektúrájából fakad: a hagyományos 32 vagy 64 bites processzorral szerelt eszközök nem képesek feldolgozni a szélessávú adatkapcsolaton keresztül érkező forgalmat, így minden egyes UTM-funkció bekapcsolásával exponenciálisan csökken az eszközök áteresztőképessége. A Fortinet FortiGate UTM-termékcsaládja azonban szakít a hagyományos architektúrával: A FortiGate-eszközökben saját fejlesztésű ASIC-processzorok (Application-Specific Integrated Circuit) dolgoznak, így a FortiGate-eszközök teljesítménye alig összehasonlítható a hagyományos UTM-megoldásokéval. A FortiGate-termékcsalád minden tagja az ASIC processzorok használatával akár egy időben képes a nagy sebességű adatkapcsolatok kezelésére, tűzfal-, IPS-, antivírus-, Wi-Fi controller, VPN-, SSL-VPN szolgáltatásokra, web- és e-mail tartalom- vagy akár alkalmazásszűrésre is.

FORTIGATE-ARCHITEKTÚRA

A teljesítmény mögött: FortiASIC és FortiOS
Az alkalmazás- és célspecifikus processzorok használata olyan teljesítményre teszi képessé a FortiGate-eszközöket, amelyeket a hagyományos processzorok használatával nem lehet elérni.
A FortiASIC a Fortinet saját fejlesztésű célprocesszorcsaládja, amely a csomagfeldolgozást és a csomagvizsgálatot gyorsítja fel.

FortiASIC NP – Network Processor:
A Network Processor feladata a hálózati csomagkezelés felgyorsítása és a tűzfal-, QoS-, virtualizáció-, routing-, traffic shaping szolgáltatások gyorsítása. Az alacsony késleltetésű alkalmazások (pl. multimédia vagy VoIP-forgalom) kiszolgálásáért és a valós idejű csomagfeldolgozásért (pl. IPS) szintén a FortiASIC NP felel. A FortiASIC alkalmazás- és célspecifikus processzorok használatával jól skálázható és elképesztő teljesítményre képes (akár 500 Gbps áteresztés) hálózatbiztonsági megoldás vezethető be.

FortiASIC CP – Content Processor:
Az IPSec- és SSL-VPN kapcsolatok, valamint a kulcsmenedzsment támogatása mellett a VPN-adatkapcsolatok titkosításáért felelős ASIC-processzor. A VPN-szolgáltatásokon túl a FortiASIC CP felel a nagy sebességű és inline antivírusszűrésért, valamint a webes tartalom- és alkalmazásprotokoll-szűrésért és tartalomvizsgálatért.

FortiASIC SP – Security Processor:
A nagyvállalati FortiGate-eszközökben található egy olyan ASIC-processzor is, amely dedikáltan az IPS-modul gyorsításáért felelős. A Security Processor segítségével akár egyetlen eszközzel is lehetséges 20 Gbps IPS-áteresztőképesség biztosítása.

FortiOS – Network Security OS:
A FortiASIC-processzorok kihasználására a Fortinet – szakítva a hagyományos Linux kernelen alapuló megoldásokkal – saját operációs rendszert fejlesztett. A FortiOS szoftveresen támogatja az egyedi fejlesztésű hardvert, így a szolgáltatások maximálisan ki tudják használni a FortiASIC nyújtotta teljesítményt. A FortiOS minden FortiGate-eszközben ugyanazokat a szolgáltatásokat nyújtja (hardverlimitáltan), így a kisebb UTM-eszközök is nagyvállalati funkciókkal támogatják a hálózatbiztonságot.

FORTIOS-SZOLGÁLTATÁSOK

Alkalmazáskontroll
Az alkalmazáskontroll biztosítja az adott protokollon belül felismerhető alkalmazások detektálását és szignatúraalapú szűrését. Az alkalmazások egy adott protokollt használnak (pl. HTTP-n belül Facebook-játékok, webes levelezés stb.), de az alkalmazás felismerésével sokkal pontosabb szűrési szabályok hozhatóak létre (pl. http engedélyezett, Facebook URL-szűrésben engedélyezett, de Facebookon belül nem indítható el a TikiFarm alkalmazás, vagy http engedélyezett, de SSL tunnelben P2P alkalmazás nem engedélyezett).

IPS
Az integrált IPS-modul több mint 4000 támadási formát képes felismerni. A szignatúraalapú IPS-funkciók mellett lehetőség van a protokoll- vagy viselkedési anomáliák észlelésére, így felismeri az olyan támadásokat, amelyek szignatúráját még nem tartalmazza az adatbázis. Az IPS-szignatúrák mellett a FortiOS több mint 1000 alkalmazásmintát képes felismerni, így a protokollon belül képes meghatározni az adatforgalom típusát, és képes beavatkozni nem engedélyezett adatforgalom esetén. A beépített és folyamatosan frissülő szignatúra-adatbázis mellett lehetőség van egyedi szignatúrák SNORT-nyelvű hozzáadására és akár csomagszintű adatforgalom-rögzítésre.

VPN és SSL VPN
A FortiGate-eszközök VPN-koncentrátorként is működhetnek. FortiOS operációs rendszerük támogatja az IPSec, PPTP-, L2TP- és SSL-VPN szolgáltatásokat. SSL VPN esetén egy agent alkalmazás töltődik le a kliensszámítógépre, amely automatikusan kiépíti az SSL-tunnelt, és biztosítja a VPN-kapcsolatot. SSL-portál alkalmazásával a felhasználók HTTPS-protokollon keresztül a FortiGate-eszközbe jelentkeznek be, és manuálisan le tudják tölteni az agentet, vagy a portálra kihelyezett alkalmazások használatával agentless és tunnel nélküli kapcsolatot kezdeményezhetnek a vállalati levelezőszerverrel (OWA), Windows-szerverekkel vagy UNIX-kiszolgálókkal.

SSL-szűrés
Az SSL-forgalom man-in-the-middle terminálásával a FortiGate UTM-eszközök képesek kicsomagolni és megvizsgálni az SSL/HTTPS csatornák adatforgalmát, így nemcsak a rosszindulatú kódok szűrhetők ki a titkosított adatforgalomból, de csökkenthető az adatszivárgás kockázata is.

Teljes eszközvirtualizáció
A FortiOS lehetővé teszi, hogy a fizikai FortiGate UTM-eszközökön teljesen virtualizált UTM-eszközöket hozhassunk létre. A virtualizáció kiterjed az összes UTM-szolgáltatásra és a fizikai portokra is, így a fizikai FortiGate-en belül létrehozhatók a különálló hálózatokat önállóan menedzselő, eltérő konfigurációjú UTM-eszközök. A virtualizáció a FortiASIC-architektúrának köszönhetően nem csökkenti az eszköz(ök) teljesítményét.

Antivírus/Antispyware
A FortiGate UTM-eszközök gateway-szintű antivírus-szolgáltatásokkal erősítik a vállalati vírusvédelmet. FortiOS-rendszer támogatja a hagyományos fájlalapú (a vizsgálathoz a fájlnak le kell töltődnie) és az inline/flow-based (az átfolyó adat folyamatos ellenőrzése) antivírus-ellenőrzéseket is.

DLP
Az adatszivárgás kockázatát csökkentő modul precíz mintaillesztéssel vizsgálja az adatfolyamot, és megakadályozza, hogy érzékeny adatok távozzanak a hálózatból. Mivel az összes forgalom a FortiGate UTM-eszközön folyik át, így a webes, FTP-, SSL-, e-mail adatforgalmak egyszerűen ellenőrizhetőek, de a gyakran használt protokollok mellett lehetőség van bármely protokoll DLP-szempontú vizsgálatára is.

Web- és URL-szűrés
A FortiGate web- és URL-szűrő megoldása szolgáltatás (FortiGuard) alapú. A 76 kategóriából és több mint 2 milliárd URL-ből álló adatbázis nem a FortiGate-eszközökön, hanem a Fortinet szolgáltatásfelhőjében található. URL-szűréskor az UTM-eszköz a szolgáltatásfelhőben ellenőrzi a lekért URL besorolását, majd a helyi szabályrendszer alapján blokkolja vagy engedélyezi a felhasználó számára az URL elérését. Támogatja a helyi saját URL-adatbázis létrehozását, a kulcsszavas vagy reguláris kifejezéseken alapuló szabályrendszereket, a quota- és override-funkciókat is.

Felhasználó- vagy csoportszintű tűzfal
A FortiOS felhasználó- vagy csoportszintű (identity-base) tűzfalszolgáltatást biztosít a FortiGate-eszközök számára. A FortiGate-eszközt a vállalati autentikációs adatbázissal (AD, LDAP stb.) integrálva lehetőség van olyan flexibilis szabályrendszerek létrehozására, ahol nemcsak a csomagok forráscímére vagy céljára, de akár magára a felhasználóra vagy csoportjára is létrehozhatunk szabályrendszert.

E-mail szűrés
A FortiGate UTM-eszközök spam-, antivírus- és e-mail tartalomszűrő szolgáltatásokat nyújtanak a POP3(S), SMTP(S) és IMAP(S) protokollokhoz. Az e-mail szűrő funkciók mögött a Fortinet saját fejlesztésű spamadatbázisa dolgozik, amelyet a Fortinet szolgáltatásfelhőjéből (FortiGuard) lehet igénybe venni. Nagyvállalati e-mail tartalomszűréshez vagy extrém e-mail terheléshez a Fortinet egy külön appliance-alapú eszközt, a FortiMail megoldást ajánlja, amely a szűrések mellett e-mail archiválás szolgáltatást is nyújt.

FORTIOS HÁLÓZATI SZOLGÁLTATÁSOK

L2/L3 routing
A FortiGate-eszközök a FortiOS-be integrált routingszolgáltatásoknak köszönhetően támogatják a statikus és dinamikus (BGB, RIP, OSPF, IS-IS, Multicast stb.) routingot.A routolási szolgáltatások akár biztonsági zónánként is eltérhetnek, támogatott a zone-to-zone routing vagy akár a policy-based routing is. Virtualizáció esetén a fizikai UTM-szközben létrehozott virtuális UTM-eszközök között is megvalósítható a routing.

QoS és traffic shaping
A FortiOS QoS és traffic shaping szolgáltatással támogatja az alacsony válaszidejű (VoIP, multimédia stb.) protokollokat. Akár felhasználónként vagy csoportonként és protokollonként külön forgalommenedzsment-szabályok hozhatók létre.

WAN-optimalizáció
A WAN-optimalizációs modul az összekapcsolt branch- és központi hálózatok közötti kommunikációt képes protokolloptimalizációval és cache-szolgáltatással támogatni A WAN-optimalizáció használatával kisebb sávszélesség mellett is gyorsabb adat- és szolgáltatáselérés valósítható meg.

További technikai információ:
http://www.fortinet.com/products/fortigate/index.html

TŰZFALAS VÉDELEM – JUNIPER MODULLAL

A Juniper Networks Integrált Biztonsági Átjárók termékcsaládja célhardveralapú biztonsági megoldás, amely egyesíti magában a negyedik generációs biztonsági „alkalmazásspecifikus integrált áramköröket" (ASIC), a Gigascreen3-at és a nagy sebességű processzorokat a páratlan tűzfal és VPN-teljesítmény elérése érdekében. A TSystems ASF Juniper SRX (SRX Service Gateway), ISG (Integrated Security Gateway) és SSG (Secure Service Gateway) moduljai különösen alkalmasak kis, közepes és nagyvállalati, adatközponti és internetszolgáltatókat kiszolgáló környezetekben, ahol szükség van konzisztens, méretezhető teljesítményre az olyan fejlett alkalmazások futtatásához, mint például a streaming media vagy az internetalapú telefonálás (VoIP).

INTEGRATED SECURITY GATEWAY

Az ISG-sorozat upgradelhető integrált IDP (Intrusion Detection and Prevention) támogatásúra, ezáltal pedig robusztus védelmet nyújt a hálózati és alkalmazásszintű aktuális és felbukkanó fenyegetésekkel szemben. A Juniper Networks IDP-megoldásain is futó szoftver ScreenOS-be integrálásával az ISG-sorozat tűzfal, virtuális magánhálózat és behatolásdetektáló megoldásokat egyesít egyetlen eszközben. A dedikált feldolgozó egységeknek (a Juniper terminológiájában biztonsági moduloknak) köszönhetően az alkalmazásspecifikus feldolgozás is megvalósulhat a több gigabites tűzfal-, VPN-, IDP-teljesítmény szavatolására. Az ISG-sorozat tehát védelmezheti a hálózatok külső oldalára telepített eszközöket és a belső hálózat eszközeit egyaránt. Mindez pedig az egyedülálló biztonsági feldolgozási potenciálnak és a gazdag hálózatszegmentációs tulajdonságoknak köszönhető.

TULAJDONSÁGOK ÉS ELŐNYÖK

- Lineáris gigabites átvitel tűzfal és IPSec VPN funkcióban minden csomagmérethez, különböző típusú alkalmazások védelmére. Ez különösen akkor előnyös, ha alacsony késleltetés, ugyanakkor méretezhető „kiscsomag-teljesítmény" szükséges (streaming media és VoIP).
- A Gigascreen3-as céláramkörök és a nagy teljesítményű processzorok segítségével párhuzamos feldolgozás lehetséges. Így az alkalmazásszintű és a hálózati szintű védelemhez, a központi menedzsmenthez, valamint a több gigabites tűzfal-, VPN- és IDP-sebesség szavatolásához elegendő teljesítmény áll rendelkezésre.
- Az opcionális IDP upgrade lehetővé teszi a kritikus, nagy sebességű hálózati szegmensek hatékony védelmét a létező és frissen keletkező, alkalmazásszintű fenyegetések ellen.
- Méretezhetőség és bővíthetőség a későbbiekben felmerülő igényeknek való megfelelés jegyében, lehetővé téve a kezdeti befektetések és a teljes birtoklási költség (TCO) közötti egyensúly megteremtését.
- Átfogó, magas rendelkezésre állású megoldások interfész- és eszközszinten.
- „Full mesh" (teljes kiválthatóság) konfiguráció a redundáns fizikai útvonalak kialakításához, ezáltal nyújtva maximális rugalmasságot és üzemidőt.
- Olyan „virtuális rendszerek" támogatása, melyek lehetővé teszik az eszközök több hálózati domainre történő felosztását, ahol mindegyikhez egyedi adminisztrátorlista, házirend, tűzfal/VPN és címjegyzék rendelhető.
- Széles körű fizikaiinterfész-kínálat a könnyebb rendszerbe illeszthetőség kedvéért.
- A „virtuális routerek" támogatják a belső, privát és közösen használt IP-címek új, „külső" IP-címmé alakítását, alternatív útvonalat nyújtva ezzel a célállomáshoz, anélkül hogy a hálózati struktúra nyilvánossá válna.
- Testre szabható biztonsági zónák, a kiegészítő hardverkiadások nélküli interfészsűrűség növeléséért, alacsonyabb házirend-létrehozási költségek (melyek tartalmazzák a jogosulatlan felhasználók és támadások kiszűrését), továbbá egyszerűsített menedzsment a tűzfalnak és a VPN-nek.
- Transzparens módban is telepíthető az eszköz, amely ennek köszönhetően layer 2-es IP-biztonsági hídként működhet tűzfal-, VPN- és DoS-védelmet nyújtva, mindezt a már meglévő hálózatunk konfigurációjának minimális megváltoztatásával.
- Grafikus webes felhasználói felületen, parancssoron keresztül, illetve a Juniper Networks Security Manager szoftveren keresztül is irányítható az eszköz.
- Házirendalapú menedzsment a központi, életciklus-alapú vezérlés biztosítására.

SRX SERVICE GATEWAY

A Juniper Networks SRX sorozatú integrált végponti átjárói biztonságos útválasztók, amelyeknek fontos képessége, hogy összekapcsolnak, védenek és menedzselnek végpontokat maréknyi vagy akár több ezres felhasználószámmal. Egyetlen eszközben konszolidálva a gyors, magas rendelkezésre állású kapcsoló, útválasztó, biztonságos átjáró alkalmazási lehetőségeit, a nagyvállalatok gazdaságosan kapnak új szolgáltatásokat, biztonságos kapcsolódást és kielégítő végfelhasználói élményt. Minden SRX sorozatú integrált végponti átjáró – beleértve az egyetemi és az adatközponti alkalmazásokhoz méretezetteket – a Juniper Networks Junos operációs rendszert használja, amely páratlan összhangot, jobb teljesítményt és szolgáltatásokat, valamint piacvezető infrastruktúra-védelmet nyújt alacsony fenntartási költségek mellett.

TULAJDONSÁGOK ÉS ELŐNYÖK

Biztonságos útválasztás

A SRX sorozat megépítésével az útválasztó és tűzfalképességek egyetlen eszközben egyesülnek. Az SRX sorozatú végponti átjárók ellenőrzik a forgalmat, hogy jogos-e, és csak akkor továbbítják azt, ha igen. Ez csökkenti a hálózat terheltségét, és sávszélességet biztosít más kiemelt fontosságú alkalmazásoknak, valamint védi a hálózatot a hackertámadásoktól. Egy biztonságos útválasztó fő célja az, hogy tűzfalas védelmet nyújt és szabályokat alkalmaz az útválasztás közben. A tűzfal(zóna) funkció vizsgálja az adatforgalmat, és biztosítja, hogy egy munkamenet eredeti és visszaérkező információi abba a zónába érkezzenek, ahol vártak és engedélyezettek. A biztonsági szabály meghatározza, hogy egy munkamenet származhat-e egy adott zónából, és áthaladhat-e egy másikba. A felépítés alapján történő kiválasztási eljárás csomagokat fogad sokféle klienstől és szervertől, és nyomon követi az összes felhasználó és alkalmazás minden egyes munkamenetét. Ez biztosítja, hogy a hálózaton csak jogos forgalom legyen, és az is csak a meghatározott irányba haladjon. A konfigurálás megkönnyítésének érdekében az SRX sorozatú végponti átjárók két funkciót használnak: zónákat és szabályokat. Míg ezek meghatározhatóak a felhasználó által, az alapkonfiguráció tartalmazza a minimális – megbízható és megbízhatatlan – zónákat. A megbízható zóna a helyi hálózat konfigurálására és csatlakoztatására használatos, míg a megbízhatatlan zóna a kiterjedt hálózat vagy az internet interfésze. A telepítés egyszerűsítésére és a beállítás megkönnyítésére egy alapértelmezett szabály került elhelyezésre, amely engedélyezi a megbízható zónából származó forgalom áthaladását a megbízhatatlan zónába. Ez a szabály blokkol minden megbízhatatlan zónából származó forgalmat a megbízható zóna irányába. Ezzel ellentétben egy hagyományos útválasztó minden forgalmat továbbít tűzfal (munkamenet-tudatosság) és szabály (egy munkamenet származásának és célállomásának vizsgálata) nélkül. A webinterfészt vagy a parancssort használva könnyedén létrehozható biztonsági szabályok sorozata, amelyek a meghatározott módon irányítják a forgalmat a zónák között. Bármilyen típusú adat engedélyezhető bármilyen biztonsági zónából bármilyen más célállomásba, mindenféle ütemezési korlátozás nélkül. Ezzel szemben a legszigorúbb szabályok is felállíthatók, amelyek egyetlen fajta forgalmat engedélyeznek egy adott zóna előre meghatározott küldője és egy másik zóna meghatározott fogadója között, egy ütemezett időperiódusban.

Magas rendelkezésre állás

A Junos operációs rendszer redundanciaprotokollja (JSRP – Junos OS Services Redundancy Protocol) az egyik alapfunkciója az SRX sorozatú végponti átjáróknak. A JSRP lehetővé teszi egy biztonsági rendszerpár magas rendelkezésre állást megvalósító hálózati architektúrába történő könnyed integrálását, redundáns fizikai összeköttetéssel a rendszerek és a szomszédos hálózati kapcsolók között. A redundáns kapcsolattal a Juniper Networks képes kezelni a rendszerhibák leggyakoribb okait – így a sérült fizikai portokat, vagy ha egy kábel nem csatlakozik megfelelően –, anélkül hogy hibatűrő lenne a teljes hálózat. Ez konzisztens az általános aktív/készenléti természetű hibatűrő (failover) útválasztó protokollokkal.Amikor az SRX sorozatú végponti átjárók aktív/aktív párba vannak konfigurálva, a forgalom és a konfiguráció automatikusan tükrözésre kerül, hogy hiba esetén aktív tűzfal- és VPN-munkamenetet nyújtson. Az SRX sorozatú eszközök már szinkronizálják a konfigurációs és a futási információkat. Ennek eredményeként hibatűrő üzemmódban a következő információk kerülnek szinkronizálásra: kapcsolat/munkamenet állapot- és folyamatinformáció, IPsec biztonsági társítások, hálózati címfordítás (NAT) forgalma, címjegyzékkel kapcsolatos információk, konfigurációs változások stb. Ezzel szemben az általános aktív/készenléti hibatűrő útválasztó protokollok esetén, mint a virtuális útválasztó redundanciaprotokoll (VRRP), minden dinamikus folyamat és munkamenet információja elvész, és visszaállítandó. Néhány vagy akár az összes alkalmazás munkamenete újraindítást igényelhet a végpontok vagy a kapcsolatok konvergenciaidejétől függően. Az állapottartásnak köszönhetően nemcsak a munkamenet kerül konzerválásra, de a biztonság is folyamatos. Egy instabil hálózat esetén az aktív/aktív konfiguráció csökkenti a kieső kapcsolatok hatását a munkamenet teljesítményére.

Sessionalapú továbbítás a teljesítmény csökkenése nélkül

A kombinált útválasztó és tűzfal áteresztőképességének és a lappangási idejének optimalizálására a Junos operációs rendszer munkamenet-alapú továbbítást alkalmaz, egy olyan fejlesztést, amely kombinálja egy általános tűzfal munkamenet-állapot információit és egy klasszikus útválasztó következő állomásra (next-hop) történő csomagtovábbítását egyetlen műveletbe. A Junos operációs rendszer esetén egy munkamenet, amely megengedett a továbbítási szabály által, hozzáadódik a továbbítási táblához egy mutatóval a következő állomásra. A fennálló munkamenetek egyetlen táblán történő kereséssel ellenőrzésre kerülnek, hogy engedélyezettek-e, és mi a következő állomásuk. Ez a hatékony algoritmus javítja a teljesítményt, és kisebb lappangási időt biztosít egy munkamenet forgalmazásához, összehasonlítva egy klasszikus útválasztóval, amely több táblás keresést végez, hogy ellenőrizze a munkamenet információját, és aztán megtalálja annak a következő állomását. Amikor egy új munkamenet feláll, a munkamenet-alapú architektúrával a Junos operációs rendszer ellenőrzi, hogy a munkamenet engedélyezett-e a továbbítási szabályok szerint. Amennyiben igen, a Junos operációs rendszer megkeresi a következő állomást az útválasztó táblában. Aztán beszúrja a munkamenetet és a következő állomást a munkamenet- és továbbítási táblába, és továbbítja a csomagot. A későbbi csomagok a fennálló munkamenethez csak egyszeri keresést igényelnek a munkamenet- és továbbítási táblában, aztán továbbításra kerülnek a kijárati interfésznek.

További technikai információ:
http://www.juniper.net/us/en/products-services/security/isg-series/,
http://www.juniper.net/us/en/products-services/security/srx-series/,
http://www.juniper.net/us/en/products-services/security/ssg-series/

TŰZFALAS VÉDELEM – WATCHGUARD MODULLAL

A T-Systems ASF egy következő UTM-kategóriába tartozó modulja – a FortiGate mellett – a WatchGuard XTM tűzfalak, melyek UTM-tűzfalakként nemcsak a hagyományos tűzfalfeladatokat látják el, hanem rendelkeznek antivirus, antispam, behatolásmegakadályozás, webtartalomszűrés, alkalmazáskontroll (application control) és VPN hálózatkialakítás komponensekkel is. A WatchGuard XTM tűzfalak stabilitását és megbízhatóságát a gyártó a tűzfalon futó operációs rendszer és hardver együttes fejlesztésével éri el. A siker titka továbbá az alkalmazásproxy szemléletmód, hiszen a hálózati védelem során fontos szempont a tűzfalon áthaladó csomagok mély elemzése, mely lehetőséget biztosít a különböző támadások kivédésére és az adatszivárgás megakadályozására is. A WatchGuard XTM termékek ugyanazt az erős védelmet biztosítják a kis- és nagyvállalatok részére egyaránt.

A WATCHGUARD ALKALMAZÁS PROXYTŰZFALAK FUNKCIÓI

A WatchGuard XTM tűzfal főbb funkciói választ adnak napjaink legfontosabb biztonsági kihívásaira.

Antivírus: A protokollok vizsgálatával képes kiszűrni a kommunikáció során érkező kártékony kódokat (pl. vírusokat, trójai programokat, spyware alkalmazásokat). Képes a https-csatornában folyó adatok vizsgálatára is, ami azért jelentős, mert számos esetben a támadók https-oldalakon rejtik el a kártékony kódokat, melyek szűrését a csomagalapú tűzfalak nem képesek elvégezni, így a kód könnyedén eljut a felhasználó számítógépére.

Antispam: A kéretlen levelek mailszerverhez jutásuk előtt blokkolódnak, így tehermentesítve a mailszerveren futó spamszűrő megoldást.

Web filtering: A felhasználók, illetve felhasználói csoportok által megnézhető weboldalak korlátozásával csökkenthető a kártékony kódok hálózatba jutásának esélye, valamint biztosítható a sávszélesség ésszerűbb kihasználása is.

Behatolásmegelőzés: A kommunikáció vizsgálatával kiszűri a hackertámadásokra utaló hálózati forgalmat.

Alkalmazásfelügyelet (application control): Ez a funkció biztosítja, hogy a tűzfalon keresztül csak az engedélyezett alkalmazások kommunikáljanak. Az alkalmazott és folyamatosan bővülő adatbázisban jelenleg közel 2000 alkalmazás található, melyek tűzfalon keresztül történő kommunikációjára szabály alakítható ki felhasználónként vagy felhasználói csoportonként egyaránt. A proxytulajdonság (bizonyos protokollokban lévő forgalmat ellenőrizni tud) és a https „hack” miatt lehetőség nyílik a kommunikálni akaró alkalmazás felismerésére és blokkolására, anélkül hogy más alkalmazás hálózati forgalmát megakadályoznánk.

A WATCHGUARD TŰZFAL TOVÁBBI TULAJDONSÁGAI

Teljesítmény: akár 20 Gbps tűzfal és 10 Gbps tartalomszűrés.

Csomagszűrés: A tűzfalra érkező csomagok folyamatos ellenőrzésével biztosítja, hogy csak az engedélyezett irányú és jellegű forgalom haladhasson keresztül a tűzfalon.

Alkalmazásproxy: A WatchGuard Firebox tűzfalak SMTP, HTTP, HTTPS, FTP, DNS és TCP proxyval rendelkeznek. Képesek a csomagok tartalmát vizsgálva kiszűrni az ártalmas kódrészleteket, a protokollba nem illeszkedő parancsokat, szükség szerint megváltoztatni a felsőbb szintű protokollokba ágyazott információkat, elfedni a szerverek sebezhetőségét, verzióját, a

konfiguráció hiányosságai által nyitva hagyott kiskapukat. A szabálytalan csomagokat küldő támadó számítógép automatikusan kizárható a kommunikációból.

Behatolásdetektáló és -megelőző rendszer (IPS+IDS): A WatchGaurd XTM tűzfalak lehetőséget adnak a különféle módokon veszélyt jelentő külső, internetes IP-címek kommunikációjának tiltására, meggátolva ezzel a címekről érkező esetleges további támadási kísérleteket. Lehetőséget biztosít a különféle portok megkeresésére, protokoll-rendellenességek észlelésére, a címtiltási akciónak DoS- (denial -of-service) és egyéb támadásokhoz történő kötésére. A WatchGuard Firebox System monitoringrendszeren keresztül az adminisztrátor képes a kapcsolatok lebontására, a végpontok kizárásának beállítására.

Tűzfalszolgáltatások: Előre definiált tűzfalszolgáltatások egyszerűsítik a tűzfal beállítását és kezelését. A WatchGuard Firebox® modellek tudásbázisa több, előre definiált tűzfalszolgáltatást (protokollon alapuló forgalom-ellenőrzést) tartalmaz, melyekből gyorsan összeállítható a felhasználó igényeinek megfelelő szabálygyűjtemény.

Felhasználóazonosítás: A megszokott IP-alapú azonosítás helyett személyre szabott tűzfalszabályok hozhatók létre (cím, címtartomány, hálózat, felhasználónév és jelszó). A felhasználók azonosításával a tűzfal számítógéptől függetlenül, a személyhez tartozó jogok alapján vizsgálja az illető tűzfalon keresztül zajló forgalmát. Korlátozhatja a megtekinthető oldalak és a használt, interneten keresztül kommunikáló szoftverek körét.

Riportok: Webes felületen is készíthetünk az igényeknek megfelelő riportokat. Ezen keresztül könnyedén ki tudjuk választani azt, hogy miről szeretnénk jelentést készíteni.

Menedzsment: A Watchguard eszközök menedzseléséhez többféle lehetőség közül választható ki az igényeknek és a helyzetnek leginkább megfelelő. Ezen felületek a WatchGuard System Manager, a parancssoros felhasználói felület és a Web UI, amelyek segítségével az eszköz bárhonnan és bármikor menedzselhető.

Bővíthetőség: Nem szükséges az igények növekedésével új hardvert vásárolni. Egyszerűen, szoftverlicenckulcsok segítségével új funkcionalitás és megnövelt védelmi képesség nyerhető a hálózat igényei szerint.

További technikai információ:
http://www.watchguard.com/products/xtm-main.asp

BIZTONSÁGOS KULCSTÁROLÁS – THALES MODULLAL

A vállalaton belül található érzékeny információ mennyisége folyamatosan nő (ügyféladatok, pénzügyi eredmények, kimutatások, kutatások stb.). Ma már ugyan sok vállalat használ külön védelmet, esetleg titkosítást ezen információk védelmére, azonban maga a titkosító kulcs is ugyanolyan (sőt sokkal jobban!) védendő adat, mint a fent felsoroltak. Ezért is kiemelten fontos ezen kulcsok megfelelő kezelése, tárolása, megújítása. A mai modern adatvédelmi megoldásoknak már nemcsak a hálózaton kívüli támadások ellen kell védelmet nyújtaniuk, de a vállalaton belüli támadások ellen is. A belső támadások ellen azonban a pusztán szoftveres megoldások már kevésbé védettek, míg a hardveres megoldások (ahol a védendő kulcs nem is hagyhatja el az eszközt) elegendő biztonságot nyújtanak.

A T-Systems a kihívásokra válaszolva integrálta ASF keretrendszerébe a Thales nShield-termékcsaládot, mely segítséget nyújt a feladatok leküzdéséhez. Az nShield biztonságos, tamper-resistent környezetet biztosít a védendő kulcsok számára. A PCIExpress-alapú/PCI-alapú eszköz támogatja a secure code executiont (ez esetben a kívánt kód is az eszközön belül fut) és a kulcstárolást is az eszközön belül, így növelve a biztonságot. A kritikus információk nem hallgathatóak le, nem módosíthatók (ez a titkosítás miatt rögtön kiderülne). A Thales nShield eszköze tehát mind a logikai, mind a fizikai támadások ellen védelmet nyújt.

A BIZTONSÁGOS KULCSTÁROLÓ MEGOLDÁS ELŐNYEI:

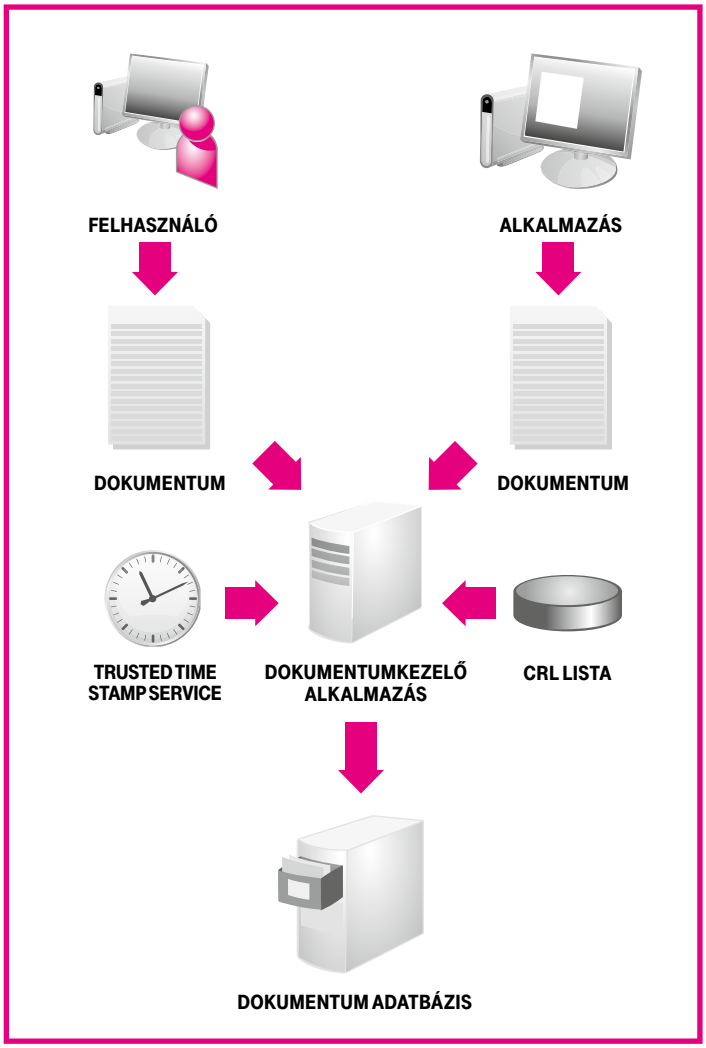
- Költséghatékony hardveres kulcsmenedzsment megoldás, mely rugalmasan kezelhető, legyen szó akár klasszikus adatközpontról, akár felhőalapú technológiákról.
- Compliance-igényeknek könnyen megfeleltethető kiépítés.
- Nagyvállalati környezetben használható (skálázható, redundáns, hibatűrő rendszer építhető).
- Egyszerű mentés, visszaállítás.
- Központosított menedzsment, hálózati elérés.
- Üzleti folyamatok védelme (PKI, titkosítás, felhasználói azonosítás, adatbázis-titkosítás, webszerverek védelme, digitális aláírás, DNSSEC, kódellenőrzés esetén használható megoldás).
- Megbízható, tanúsítványokkal elismert (FIPS validated security) megoldás.
- Egyszerű integráció külső gyártók megoldásaival.
- Szerepköralapú adminisztráció (ki, mihez, hogyan férhet hozzá), akár többfaktoros azonosítással is.
- Nagy teljesítménye miatt másodpercenként több száz kulcslekérdezésre is lehetőség van.
- SEE (secure execution engine) biztonságos kódfuttatás akár az eszközön belül.
- SOA-támogatás.
- ECC- (elliptic curce cryptography) támogatás.

További technikai információ:
http://www.thales-esecurity.com/products-and-services/products-and-services/hardware-security-modules/general-purpose-hsms/nshield-solo

IDŐBÉLYEGZÉS – THALES TIME STAMP SERVER MODULLAL

A Time Stamp Server appliance, mely a Thales nagy biztonságú adatvédelmi megoldásai közé tartozik, képes hálózaton keresztül időbélyegek generálására. A pontos időt hálózaton keresztül kérdezi le, így az időbélyeggel együtt az utolsó módosítás ideje és bármilyen elektronikusan tárolt dokumentum eredetisége is igazolható. A független szervezetek által minősített appliance (FIPS 140-2 Level 3, Common Criteria EAL 4+) segítségével hitelesíthető a digitális record és az utolsó módosítás ideje is, akárcsak egy lepecsételt, aláírt, papíralapú megoldásnál. A hardveres kivitelnek (tamper resistant hardware) köszönhetően az időbélyegek nem módosíthatóak vagy manipulálhatóak – még az adminisztrátorok által sem –, így pluszbiztonság érhető el a szoftveralapú megoldásokkal szemben. Más megoldásokhoz viszonyítva további előnye, hogy kompatibilis a Microsoft Authenticode-dal, mely a Microsoft által fejlesztett code-signing szabvány. A Thales Time Stamp Source Master Clock segítségével integrálva pedig külön hálózati elérésre sincs szüksége, hiszen képes ezen eszköztől lekérdezni a pontos időt. A megoldás használható:

- Karchiválásra – hosszú távú megoldás, akár dokumentum-ellenőrzésre is,
- public key infrastructure keretében – biztosítja a küldő, a címzett, a tartalom és az időpont sérthetetlenségét,
- e-business alkalmazások esetén – digitális számlák/online banki tranzakciók,
- postai szolgáltatásoknál,
- e-mail küldésnél,
- log file kezelésnél.



Időbélyegzés általános felhasználása

További technikai specifikáció:
http://www.thales-esecurity.com/products-and-services/products-and-services/time-stamping-appliances/time-stamp-server