Adatlap

Információ- és adatvagyon-kezelés

Micro Focus Secure Messaging Gateway

A Micro Focus® Secure Messaging Gateway átfogó védelmet biztosít a legújabb vírusok és a kéretlen üzenetek ellen, helyben vagy a felhőben egyaránt. A megoldás a legfrissebb technológiákkal gondoskodik róla, hogy az üzenetkezelő rendszer és a hálózat mentes legyen a vírusoktól, kártékony kódoktól és a kéretlen üzenetektől. A Secure Messaging Gateway a DoS-/DDoS-támadások ellen is véd, és segíti a levelezőrendszert a folyamatos, zökkenőmentes működésben.

Fő termékinformációk

A Micro Focus Secure Messaging Gateway világszerte több ezer szervezet üzleti hálózatát és kommunikációs adatait védi, kormányoktól kezdve oktatási intézményeken, pénzügyi és egészségügyi szolgáltatókon át különféle üzleti vállalkozásokig.

Jellemzők és előnyök

Több rendszer támogatása: Secure Messaging Gateway bármilyen szabványos internetes levelező- vagy csoportmunka-rendszer peremén képes szűrni az üzeneteket. A támogatott platformok közé tartozik a Microsoft Exchange, az Office 365, a Gmail, a Micro Focus GroupWise®, a Vibe, a Lync és az IBM Notes.

Szerepköralapú felhasználói adminisztráció: A szervezetek konkrét szerepköralapú hozzáféréseket oszthatnak ki az egyes felhasználóknak a Secure Messaging Gateway-en belül. A hozzáférésszabályozási lista (Access Control List) segítségével a beállított szerepkör szerint kezelhetik a felhasználók engedélyeit a megoldás egyes funkcióihoz. A kijelölt felhasználók igénybe vehetnek bizonyos adminisztratív funkciókat teljes rendszergazdai jogosultság nélkül is.

Skálázható kialakítás: Amikor a rendszer megközelíti kapacitása határát, vagy túl nagy terhelés éri, új erőforrások (további szerverek) adhatók hozzá a terhelés kiegyenlítésére.

Hibatűrő konfiguráció: A Secure Messaging Gateway több szerveren is használható. Így a rendszer egy vagy több kiszolgáló leállása esetén is működőképes marad.

Könnyen konfigurálható, ad-hoc, testre szabható értesítések: A szervezetek számos különféle értesítést hozhatnak létre a rendszeren belül, például beállíthatnak értesítést kulcsszavakhoz, mellékletekhez, bizonyos tartalmakhoz, vírusokhoz, kéretlen levelekhez vagy más egyéb kategóriákhoz. Ráadásul minden értesítés lokalizálható, így az összes e-mail lokalizált változatban küldhető ki.

Biztonság a felhőben: A Secure Messaging Gateway a helyszínen vagy felhőben is telepíthető. A „több-bérlős" támogatás lehetővé teszi, hogy a vizsgálati beállítások több, egymástól független példányban fussanak ugyanazon a szerveren. Így a szervezetek a Secure Messaging Gateway minden funkcióját kihasználhatják, és több ügyfelet támogatnak egyazon rendszerről. A felhőmegoldás a helyben telepített rendszerekre jellemző többletköltség, kockázat és komplexitás nélkül védi az üzenetkezelő rendszert. Az informatikai, a rendszertámogatási és a hardverköltségek ebben az esetben a Micro Focusra hárulnak.

Bejövő és kimenő forgalom védelme

A Secure Messaging Gateway védi a nagyvállalati hálózati és üzenetkezelő rendszer be- és kifelé irányuló forgalmát a vírusoktól, a kéretlen levelektől, az internetes bűnözéstől és a DoS-/DDoS-támadásoktól.

Védelem a vírusokkal szemben

„Nulladik órás" védelem a vírusokkal szemben: A Secure Messaging Gateway az elérhető legjobb védelmet biztosítja a be- és kifelé irányuló forgalomnál, akár a legfrissebb, „nulladik órás" fenyegetésnek számító vírusokkal szemben is. Még a fertőzés előtt megállítja őket, megelőzve az akár több százezer forintos költséggel járó időkiesést és adatvesztést.

Vírusvizsgálat: A Secure Messaging Gateway az e-mail tárgyát, szövegtestét és mellékleteit is megvizsgálja, vírusok után kutatva. Ha a melléklet vírust tartalmaz, a rendszer még az átjárónál megállítja az e-mail üzenetet. Ha a levél szövegében vagy tárgyában található kártékony hivatkozás vagy vírus, a Secure Messaging Gateway letiltja az e-mailt.

Szabályalapú, „több-bérlős" konfiguráció: A Secure Messaging Gateway lehetővé teszi a szervezetek számára, hogy egyéni üzenetszabályokat állítsanak be az egyes üzenetek kézbesítési adatai alapján. A címzett, a feladó, az irány és hasonló feltételek alapján külön üzenetszabályok hozhatók létre a bejövő és kimenő üzenetekhez, az egyes felhasználókhoz, tartományokhoz vagy felhasználói csoportokhoz. A rendszer a levelezőátjárón végzett teljes, „több-bérlős" e-mail vizsgálatot is támogatja. Szabályalapú ellenőrzéssel kombinálva a partnerek és a szolgáltatók hosztolt megoldásként is használhatják a Secure Messaging Gatewayt.

Bejövő és kimenő forgalom védelme: A vírusok és a kártékony kódok olyan fenyegetések, amelyek sokféle belépési ponton képesek bejutni a hálózatba. A be- és kifelé irányuló forgalom vizsgálatával a Secure Messaging Gateway egyedülálló védelmet nyújt, és minimalizálja a kockázatokat és az esetleges károkat.

Többszálú, nagy teljesítményű vizsgálat: A szervezetek nagy teljesítményű e-mail vizsgálatot is végezhetnek aszinkron módon, több szálon indítva a vizsgálati folyamatot, a kiszolgálón elérhető összes erőforrásra kiterjesztve.

Minták egyeztetése: A Secure Messaging Gateway támogatja a szabványos kifejezések használatát a minták egyeztetésénél, és a teljes tartományra nézve lehetővé teszi a minták alkalmazását és a vizsgálatot. Például alkalmazhatja a *ceg.hu kifejezést a tartományt használó összes e-mail címre, miközben az e-mail tartalomban keres a mintákra.

Kéretlen üzenetek elleni védelem

A Secure Messaging Gateway többszintű védelmet nyújt a kéretlen üzenetek ellen. Megvédi a levelezést, és távol tartja a nemkívánatos forgalmat a csoportmunka-rendszertől.

Robusztus tartalomszűrés: A Secure Messaging Gateway képes szűrni az e-mail tartalmat e-mail cím, tárgysor, fejléc, szövegtest, nyers MIME, ujjlenyomat, melléklet, mellékletnév, képek (Image Analyzer), feketelista/fehérlista, üzenetméret és IP-cím alapján egyaránt.

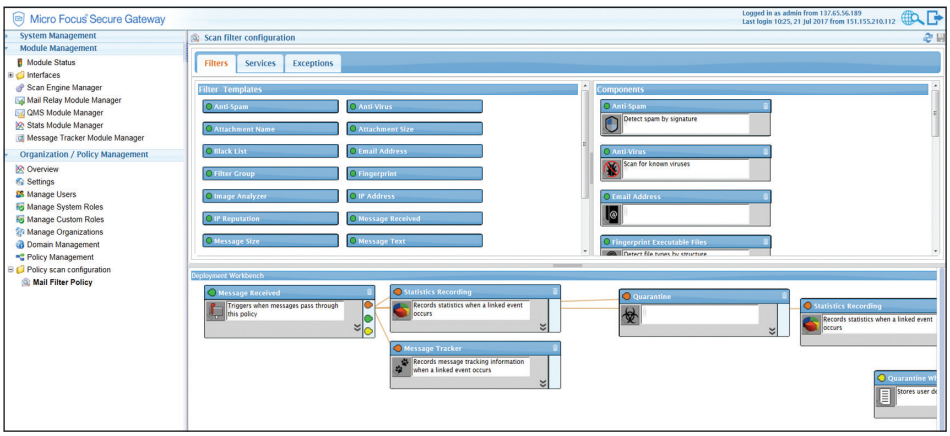
Peremvédelmi vizsgálat: A Secure Messaging Gateway még azelőtt elfogja a kéretlen üzenetet, hogy az bejutna az üzenetkezelő rendszerbe. Kéretlen üzeneteket letiltó funkciója támogatja a címek blokkolását, a tartalomszűrést, a heurisztikát, a SURBL-technológiát, az IP-megbízhatóság szerinti vizsgálatot, a konverziókövetést és a TLS-t. A kéretlen üzenetektől mentes e-mail rendszer így zökkenőmentesen és hatékonyan működhet.

DKIM-támogatás (DomainKeys Identified Mail): Az elküldött és fogadott e-mailek védelméről DKIM-támogatás is gondoskodik. A Secure Messaging Gateway ellenőrzi, hogy az adott tartományból érkező e-mailt a tartomány tulajdonosa engedélyezte-e. Így a hamisított feladói címről érkező adathalász vagy kéretlen üzenetek nem jutnak be az e-mail rendszerbe.

A téves eredmények számának minimalizálása: A Secure Messaging Gateway kéretlen üzeneteket kezelő motorját folyamatosan új spam-aláírásokkal frissítjük. Ez az innovatív technológia észleli a fals pozitív eredményeket, és ügyel rá, hogy a valóban szükséges üzenetek a bejövő üzenetek mappába kerüljenek, és a rendszer csak a kéretlen leveleket szűrje ki.

Kéretlen üzenetek elleni védelem a kimenő forgalomnál: A végfelhasználók munkaállomásait megfertőzhetik bizonyos vírusok, amelyek átjutnak a peremvédelmen. Ezek a munkaállomások kéretlen üzeneteket küldhetnek a hálózaton keresztül, több ezer kimenő kéretlen üzenet forrásává téve a céges rendszert. A Secure Messaging Gateway segít megelőzni a kiküldött kéretlen üzenetek jelentette kockázatokat, beleértve az IP-cím letiltását, a hír csorbulását, az erőforrások kiesését és az üzenetkezelő rendszer működési zavarait.

Szűrésszabályzás irány alapján: A Secure Messaging Gateway lehetővé teszi az üzenet iránya alapján történő szűrést (kifelé vagy befelé irányuló forgalom szűrői). Így eltérő szűrőt lehet alkalmazni a bejövő és a kimenő forgalomra.

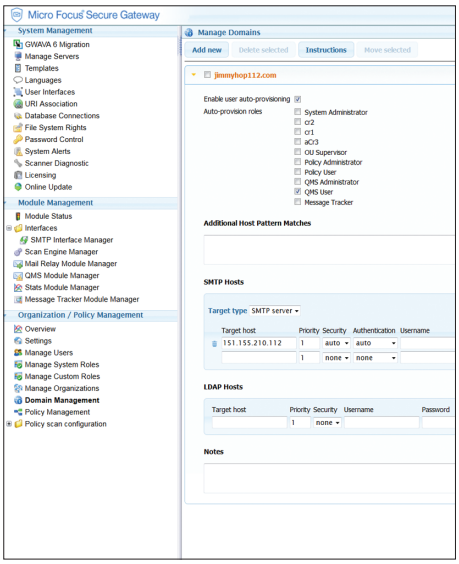


„Az ügyfeleim többségénél a kéretlen üzenetek jelentik a legnagyobb problémát. Különösen az állami szektorban, ahol nyilvánosak az e-mail címek, és ezért valamilyen termékkel védekezniük kell a kéretlen üzenetek ellen. Jelentős tapasztalattal rendelkezem a Micro Focus termékekkel kapcsolatban. Megbízom bennük, és magam is használom őket."

DIETHMAR RIMSER
a BrainAgents vezérigazgatója

Kapcsolatfelvétel:
www.microfocus.com

Tetszik amit olvas? Ossza meg.



„Envelope" szűrés: A Secure Messaging Gateway lehetővé teszi a felhasználó jogosultsága szerinti szűrők létrehozását. Ha egy felhasználó megfelelő jogosultsággal rendelkezik a Micro Focus rendszerében, és e-mail üzenetet küld, a rendszer előre meghatározott módon kezeli az üzenetet. Beállítható például, hogy az adott felhasználótól érkező összes üzenet bejusson a rendszerbe. A Secure Messaging Gateway a jogosultsággal nem rendelkező felhasználók összes üzenetét le tudja tiltani.

Hamisításszűrés SPF-vizsgálattal: Az e-mail hamisítás megállításához a Secure Messaging Gateway „Sender Policy Framework" (SPF) vizsgálatot végez. Az SPF megvizsgálja a MIME-fájlban a feladóra vonatkozó tartományinformációt, majd a tartomány SPF-rekordjának ellenőrzésével megállapítja, hogy az e-mail által jelzett tartomány egyezik-e az adott tartományhoz tartozó levelezőszerverekkel. Az SPF segítségével a Secure Messaging Gateway a tartomány tulajdonosának küldési szabályzatában közölt információk alapján azonosítja azokat az üzeneteket, amelyek számára engedélyezett, illetve nem engedélyezett a tartománynév használata az SMTP HELO és MAIL FROM parancsoknál.

Internetes bűnözés elleni védelem: Az internetes bűnözés, a kiberterrorizmus és a kártékony kódok komoly fenyegetést jelentenek a szervezetek számára. A Secure Messaging Gateway speciális többszintű védelemmel akadályozza meg, hogy a kiberbűnözők e-mailen keresztül megtámadják az infrastruktúrát.

DoS-/DDoS-támadások elleni védelem: A megoldás megelőzi az SMTP elleni DoS- (Denial of Service) és DDoS- (Distributed DoS) támadásokat, amelyek a levelezőszerver összeomlásához vezethetnek. Az ilyen leállásokkal járó üzemkiesés pénz- és időveszteséget jelent a vállalat számára.

Végfelhasználói fekete- és fehérlisták: A megoldás segítségével a vállalatok jogosultságokat biztosíthatnak a végfelhasználóknak, és egyúttal csökkenthetik az adminisztráció idő- és költségigényét. A végfelhasználók megjelölhetnek bizonyos tartományokat és e-mail címeket, és egyes e-mail címeket vagy akár teljes tartományokat is rátehetnek a fekete- vagy fehérlistára. Ezzel meghatározhatják, hogy a rendszer átengedje vagy letiltsa az üzeneteket a lista alapján

Teljes körű GroupWise-támogatás*

A Micro Focus Secure Messaging Gateway képes teljes körű vizsgálatot végezni a Micro Focus GroupWise üzenetkezelő platformon. A megoldás valós időben kezeli a GroupWise MTA, POA, GWIA, WebAccess és GMS rendszereken áthaladó összes üzenetet, és ellenőrzi, hogy mentesek-e a vírusoktól, a kéretlen tartalomtól és a kártékony kódoktól.

GroupWise WebAccess: Mivel a GroupWise WebAccess az SMTP-t és az MTA-t kikerülve közvetlenül kommunikál a levelezőrendszerrel, a WebAccessen keresztül zajló kommunikáció nem védett és közvetlenül megfertőzheti a rendszert. A Secure Messaging Gateway a GroupWise WebAccess Gateway mellett kiszűri a kéretlen tartalmakat, mielőtt még azok elérnék a rendszert. Ahhoz, hogy a teljes Micro Focus-portfólióval képes legyen együttműködni, a megoldás Vibe-bővítőmodult is tartalmaz.

Kiegészített védelem a GroupWise Mobility Service számára: A Secure Messaging Gateway megvizsgálja a GroupWise Messaging Service-hez csatlakoztatott mobileszközökről küldött összes üzenetet, és még azelőtt megállítja a vírusokat, hogy azok bejutnának a GroupWise rendszerbe. Így a szervezet gondoskodhat a mobilüzenetek védelméről, és megakadályozhatja a vírusok továbbterjedését a belső GroupWise felhasználókra.

Micro Focus Vibe támogatás: A Secure Messaging Gateway megvizsgálja a Vibe-on közzétett összes üzenetet és feltöltést, és még azelőtt megállítja a vírusokat, hogy bejutnának a hálózatba. Így a szervezet gondoskodhat a Vibe védelméről, és megakadályozhatja a vírusok továbbterjedését a belső rendszerfelhasználókra.

** Ez a funkció csak a Secure Messaging Gateway for GroupWise 18+ verzióban áll rendelkezésre. A GroupWise 8, 2012, és 2014 esetében ez a funkció csak a GWAVA 6.x-en keresztül elérhető. Ez a funkció csak a Secure Messaging Gateway for GroupWise 18+ verzióban áll rendelkezésre. A GroupWise 8, 2012, és 2014 esetében ez a funkció csak a GWAVA 6.x-en keresztül elérhető.*