MICRO FOCUS

Datenblatt

Secure Messaging Gateway
GroupWise
WebAccess
Vibe

Micro Focus Secure Messaging Gateway

Micro Focus Secure Messaging Gateway bietet Zero-Hour-Antiviren- und Antispam-Schutz lokal oder in der Cloud. Die Lösung nutzt neueste Technologien, um sicherzustellen, dass Ihr Nachrichtensystem sowie Ihr Netzwerk frei von Viren, Schadprogrammen und Spam sind. Weitere Vorteile: Überwachung des Netzwerkverkehrs, um pornografische Bilder zu blocken, Blockieren des Zugriffs auf bösartige Websites und Inhalte und Schutz vor Internetkriminalität und DoS-/DDoS-Angriffen.

Produkthighlights

Micro Focus Secure Messaging Gateway wird bei Tausenden von Organisationen auf der ganzen Welt in Behörden, in Bildungseinrichtungen, in der Finanzdienstleistungsbranche, im Gesundheitswesen sowie in privatwirtschaftlichen Unternehmen zum Schutz von Unternehmensnetzwerken und Kommunikationsdaten eingesetzt.

Die wichtigsten Funktionen und Vorteile

Unterstützung für mehrere Systeme: Secure Messaging Gateway kann Nachrichten am Netzwerkrand jedes standardbasierten Internet-E-Mail- oder Collaboration-Systems filtern. Dies umfasst Plattformen wie Microsoft Exchange, Office 365, Gmail, Micro Focus GroupWise, Vibe, Lync oder IBM Notes.

Rollenbasierte Benutzerverwaltung: Gewähren Sie Ihren Benutzern einen bestimmten rollenbasierten Zugriff direkt in Secure Messaging Gateway. Mit der neuen Zugriffssteuerungsliste können Sie den Benutzerzugriff auf Merkmale und Funktionen von Secure Messaging Gateway basierend auf den von Ihnen festgelegten Rollen verwalten. Aufgeführte Benutzer können nun Zugriff auf bestimmte Verwaltungsfunktionen erhalten, ohne vollständige Administratorrechte besitzen zu müssen.

Skalierbares Design: Wenn Ihr System langsam seine Kapazitätsgrenze erreicht oder unter hoher Belastung arbeitet, können Sie neue Ressourcen (zusätzliche Server) zum Ausgleich der Last in Ihrem Secure Messaging Gateway-System hinzufügen.

Fehlertolerante Konfiguration: Secure Messaging Gateway kann auf mehreren Servern eingerichtet werden. Dadurch kann Ihr System weiterhin ausgeführt werden, auch wenn ein oder mehrere Server ausfallen.

Einfach zu konfigurierende, anpassbare Ad-Hoc-Benachrichtigungen: Erstellen Sie spezielle Benachrichtigungen, die Sie haben möchten oder benötigen. Die Arten von Benachrichtigungen, die Sie erstellen können, sind nahezu unbegrenzt. Sie können durch Schlüsselwörter, Anlagen, Inhalte, verbotene Bilder, Viren, Spam und andere Elemente ausgelöst werden. Zudem können alle Benachrichtigungen lokalisiert werden, sodass Sie die generierten lokalisierten Versionen der E-Mails bereitstellen können.

Cloud-Sicherheit: Secure Messaging Gateway kann lokal oder in der Cloud bereitgestellt werden. Dank der Mehrmandantenfähigkeit von Secure Messaging Gateway können mehrere unabhängige Instanzen der Scan-Konfigurationen auf demselben Server ausgeführt werden. So können Sie alle Funktionen von Secure Messaging Gateway nutzen und gleichzeitig Support für eine Vielzahl von Kunden über ein System bieten. Die Cloud-Lösung sichert Ihr Nachrichtensystem ohne die zusätzlichen Kosten und Risiken sowie ohne den zusätzlichen Aufwand in Zusammenhang mit einem lokalen Messaging-Security-System. Überlassen Sie die IT-, Hardware- und Supportkosten Micro Focus.

Schutz von eingehenden und ausgehenden Daten

Secure Messaging Gateway bietet Schutz von eingehenden und ausgehenden Daten für das Netzwerk- und Nachrichtensystem Ihres Unternehmens, einschließlich Antivirenschutz, Antispam-Schutz, Schutz vor Cyberkriminalität, DDOS-Schutz und Blockieren von pornografischen Inhalten durch integrierte Bildanalysen.

Antivirenschutz

Zero-Hour-Antivirenschutz: Secure Messaging Gateway bietet den besten Zero-Hour-Antivirenschutz, der für eingehenden und ausgehenden Datenverkehr verfügbar ist. Viren werden gestoppt, bevor sie Unheil anrichten, sodass Sie Tausende Dollar für Zeit- und Datenverlust sparen.

Antiviren-Untersuchungen: Secure Messaging Gateway sucht nach Viren in der Betreffzeile, im Nachrichtentext und in den Anhängen einer E-Mail. Wenn der Anhang ein Virus enthält, wird die E-Mail-Nachricht am Gateway gestoppt. Wenn der Nachrichtentext oder die Betreffzeile der E-Mail einen schädlichen Link oder ein Virus enthält, wird die E-Mail von Secure Messaging Gateway blockiert.

Richtlinienbasierte Mehrmandanten-Konfiguration: Secure Messaging Gateway ermöglicht das Erstellen und Konfigurieren von einzelnen Nachrichten-Richtlinien auf Basis der Sendeinformationen der einzelnen Nachrichten. Verwenden Sie Kriterien wie den Empfänger, die Quelladresse und die Nachrichtenrichtung zum Erstellen von einzelnen Nachrichten-Richtlinien für eingehende und ausgehende E-Mails, für einzelne Benutzer, Domänen oder mehrere Sätze von Benutzern. Unterstützt wird zudem eine volle Mehrmandanten-Untersuchung von E-Mails über einzelne Messaging-Gateways. In Verbindung mit der regelbasierten Steuerung können Partner und Dienstanbieter Secure Messaging Gateway als gehostete Lösung nutzen.

Schutz von eingehenden und ausgehenden Daten: Viren und Schadprogramme sind Bedrohungen, die von einer Vielzahl von Einstiegspunkten in Ihr Netzwerk eindringen können. Durch die Untersuchung ein- und ausgehender Daten bietet Secure Messaging Gateway einen einzigartigen Schutz, durch den sichergestellt ist, dass Bedrohungen und Schäden minimiert werden.

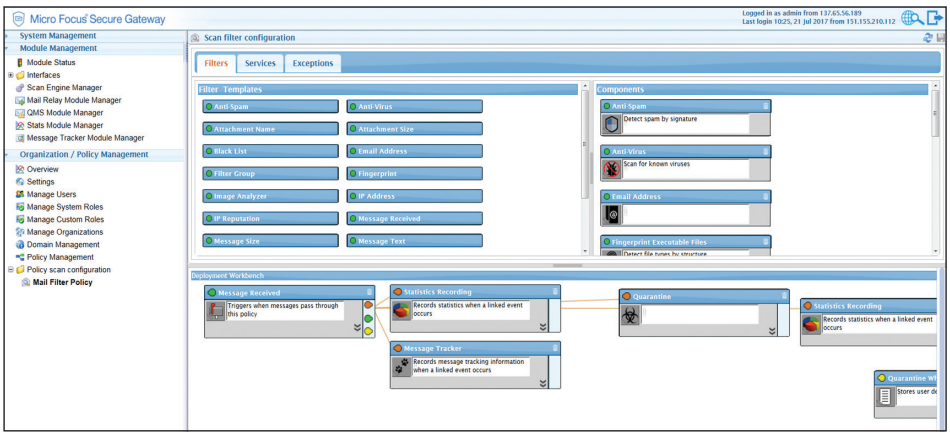
Leistungsstarke Multi-Thread-Untersuchungen: Stellen Sie mit asynchronen Thread-Untersuchungen über alle verfügbaren Ressourcen auf dem Server einen leistungsstarken Schutz Ihrer E-Mails sicher.

Musterabgleich: Secure Messaging Gateway unterstützt standardbasierte reguläre Ausdrücke für den Musterabgleich. Es können Muster angewendet und die vollständige Domäne untersucht werden. Beispiel: Bei der Suche nach Mustern in E-Mail-Inhalten wird *companydomain.com für alle E-Mail-Adressen angewendet, die diese Domäne verwenden.

Antispam-Schutz

Secure Messaging Gateway bietet einen mehrschichtigen Spam-Schutz für E-Mails und hält unerwünschten Datenverkehr von Ihrem Collaboration-System fern.

Zuverlässige Inhaltsfilterung: Secure Messaging Gateway filtert E-Mail-Inhalte auf Basis von E-Mail-Adresse, Betreff, Header, Textkörper, Raw-MIME, Fingerabdruck, Anlagen, Anlagennamen, Bildern (über Image Analyzer), Negativ- und Positivlisten, Nachrichtengröße und IP-Adresse.



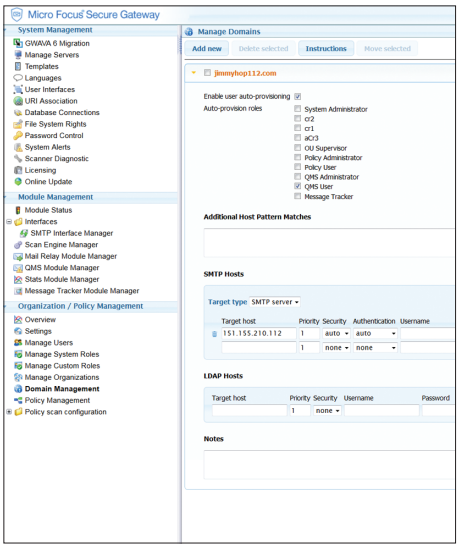
Perimetersicherheits-Untersuchung: Die Secure Messaging Gateway Soft-Appliance fängt Spam ab, bevor er Ihr Nachrichtensystem erreicht. Die Spam-Blockier-Funktionen umfassen Adressenblockierung, Filterung von Inhalten, Heuristik, SURBL-Technologie, IP-Reputationsanalysen, Conversion-Tracking und TLS-Unterstützung. Durch die Eliminierung von Spam läuft Ihr E-Mail-System reibungslos und effizient.

DomainKeys Identified Mail (DKIM)-Unterstützung: Schützen Sie gesendete und empfangene E-Mails durch DKIM-Unterstützung. Secure Messaging Gateway sorgt dafür, dass E-Mails von einer Domäne vom Eigentümer dieser Domäne autorisiert werden. Dadurch wird verhindert, dass E-Mails von gefälschten Absendern in Ihr E-Mail-System gelangen, wodurch Phishing- und Spam-Angriffe eliminiert werden.

Minimierung von falsch-positiven Ergebnissen: Die Antispam-Engine von Secure Messaging Gateway wird fortlaufend mit neuen Spam-Signaturen aktualisiert. Diese innovative Technologie gewährleistet, dass falsch-positive Ergebnisse erkannt werden, d. h., dass die E-Mails, die Sie benötigen, auch wirklich in Ihrem Posteingang landen und nur Spam gefiltert wird.

Ausgehender Antispam-Schutz: Workstations von Endbenutzern können mit Viren infiziert werden, die die Perimetersicherheit durchdringen. Diese Workstations können dann den Spam über Ihr Netzwerk verteilen und das System zu einer Quelle für Tausende von ausgehenden Spam-Nachrichten machen. Secure Messaging Gateway eliminiert Risiken durch ausgehende Spam-Nachrichten, einschließlich einer blockierten IP-Adresse, Reputationsverlust, Verlust von Ressourcen und lahmgelegter Nachrichtensysteme.

Direktionale Filterungssteuerung: Mit Secure Messaging Gateway können Sie Filter basierend auf der Nachrichtenrichtung (Filter für ausgehende bzw. eingehende Nachrichten) erstellen. Sie können für eingehenden Datenverkehr andere Filter anwenden als für ausgehenden Datenverkehr.



Umschlag-Filterung: Mit Secure Messaging Gateway können Sie Filter basierend auf der Authentifizierung von Benutzern erstellen. Wenn ein im Micro Focus System authentifizierter Benutzer eine E-Mail sendet, kann das System diese Nachricht in einer bestimmten Weise verarbeiten. Beispielsweise können Sie erlauben, dass alle Nachrichten von diesem Benutzer im System eingehen, und Secure Messaging Gateway kann alle Nachrichten blockieren, die von einem nicht authentifizierten Benutzer gesendet werden.

Anti-Spoofing mit SPF-Untersuchung: Zur Vermeidung von E-Mail-Spoofing führt Secure Messaging Gateway eine Sender Policy Framework (SPF)-Untersuchung durch. SPF prüft die Domäne, die im Absenderbereich der MIME-Datei zu finden ist, und überprüft dann die SPF-Datensätze dieser Domäne, um sicherzustellen, dass die Domäne, die die E-Mail berichtet, den Mailservern entspricht, die die Domäne senden. Durch SPF kann Secure Messaging Gateway basierend auf in einer Absenderrichtlinie des Domänen-Anbieters veröffentlichten Informationen Nachrichten identifizieren, die autorisiert bzw. nicht autorisiert sind, den Domänennamen in den Befehlen „SMTP-HELO“ und „MAIL FROM“ zu verwenden.

Schutz des Netzwerks

Secure Messaging Gateway überwacht Ihr Netzwerk aktiv zum Schutz vor Cyberkriminalität, pornografischen Dateien und DoS-/DDoS-Angriffen. Das System bietet auch die Filterung von Internetdatenverkehr und Webinhaltsuntersuchungen, um sicherzustellen, dass schädliche Websites und ähnliche Inhalte nicht auf Ihr Netzwerk zugreifen können.

Schutz vor Cyberkriminalität: Cyberkriminalität, Cyberterrorismus und Schadprogramme sind ernste Bedrohungen für Ihr Unternehmen. Secure Messaging Gateway bietet spezielle Schutzmaßnahmen auf mehreren Ebenen, damit Cyberkriminelle Ihre Infrastruktur nicht per E-Mail angreifen können.

Schutz vor pornografischen Inhalten: Secure Messaging Gateway nutzt Image Analyzer zur Untersuchung der Zusammensetzung von Bildern und Videos. Anstelle der häufig verwendeten Signatur-Datenbanken untersucht die ausgefeilte Wahrscheinlichkeits-Engine eingehende Bilder, unterscheidet zuverlässig pornografische von nichtpornografischen Inhalten und stoppt derartige Inhalte vor dem Eingang in Ihr Nachrichtensystem.

DoS-/DDoS-Schutz: Verhindern Sie Denial-of-Service(DoS)- und Distributed DoS(DDoS)-Angriffe auf die SMTP, die Ihren Mail-Server lahmlegen können. Dies führt zu Systemausfällen und Ausfallzeiten und kostet Ihr Unternehmen Zeit und Geld in Form von verlorener Produktivität.

Negativ- und Positivlisten von Benutzern: Geben Sie Benutzern mehr Rechte, und verringern Sie dadurch Verwaltungsaufwand und -kosten. Micro Focus bietet eine Benutzeroberfläche, mit der Benutzer Domänen und E-Mail-Adressen kennzeichnen können. Die Benutzer können einzelne E-Mail-Adressen oder komplette Domänen auf ihre Negativ- und Positivlisten setzen, sodass Nachrichten auf Grundlage dieser Liste empfangen oder blockiert werden.

Umfassende Unterstützung für GroupWise

GroupWise

Micro Focus Secure Messaging Gateway bietet umfassende Untersuchungen Ihrer Micro Focus GroupWise Messaging-Plattform. Secure Messaging Gateway untersucht alle Nachrichten, die GroupWise MTA, POA, GroupWise Mobility Service (GMS) und WebAccess durchlaufen, in Echtzeit, um sicherzustellen, dass sie frei von Viren, Spam, Schadprogrammen und illegalen Bildern sind. Darüber hinaus kann Secure Messaging Gateway in festgelegten Abständen E-Mails untersuchen und Viren unter Quarantäne stellen.

GroupWise WebAccess: Da GroupWise WebAccess direkt mit dem Post-Office kommuniziert und SMTP und MTA umgeht, ist die Kommunikation über WebAccess ungeschützt und könnte das Post-Office direkt infizieren. Um WebAccess zu verwalten, befindet sich der Secure Messaging Gateway am GroupWise WebAccess Gateway und filtert unerwünschte Inhalte, bevor diese Ihr System erreichen. Um alle Micro Focus Produkte abzudecken, umfasst Secure Messaging Gateway zudem ein Vibe-Modul.

Erhöhter Schutz für GroupWise Mobility Service: Secure Messaging Gateway untersucht alle Nachrichten, die von mobilen Geräten gesendet werden, die mit dem GroupWise Messaging Service verbunden sind, und stoppt Viren, bevor diese in das GroupWise-System eindringen. Auf diese Weise können Unternehmen sicherstellen, dass mobile Nachrichten sicher sind und keine Viren an interne GroupWise-Benutzer verteilt werden.

Micro Focus Vibe Unterstützung: Secure Messaging Gateway untersucht alle Nachrichten und in Vibe hochgeladenen Elemente, und stoppt Viren, bevor diese ins Netzwerk eindringen. Dadurch wird sichergestellt, dass Vibe sicher ist und keine Viren an interne Benutzer des Systems verteilt werden.

„Das größte Problem bei den meisten meiner Kunden ist Spam. Es ist vor allem ein Problem für Menschen im öffentlichen Sektor, da deren E-Mail-Systeme öffentlich geworden sind, und sie deshalb ein Produkt zum Schutz vor Spam benötigen. Ich habe viel Erfahrung mit Micro Focus. Ich vertraue den Produkten von Micro Focus. Und ich verwende sie auch selbst.“

DIETHMAR RIMSER
CEO
BrainAgents

www.microfocus.com

Micro Focus
Deutschland
Fraunhoferstraße 7
D-85737 Ismaning
00 800-58102130

Micro Focus
Schweiz
Merkurstrasse 14
8953 Dietikon
Switzerland
00 800-58102130

Micro Focus
Firmenhauptsitz
Vereinigtes Königreich
+44 (0) 1635 565200

www.microfocus.com