



Highlights

- Effiziente Konsolidierung und Vermeidung der kostspieligen unkontrollierten Zunahme von physischen Appliances mithilfe einer virtuellen Plattform für mehr Sicherheitskonvergenz
 - Gleich hoher Schutz gegen unbefugte Zugriffe sowohl für virtuelle als auch konventionelle Netzwerke
 - Minimiert Sicherheits- und Complianceaufwände durch Erkennung und Blockierung von Netzwerkkontakten und nicht autorisiertem Netzwerkzugriff
 - Bereitstellung segmentierter Sicherheitservices in mehrfach genutzten virtuellen Umgebungen durch Cloud-Computing-Service-Provider
 - Vereinfachung von Sicherheitsmaßnahmen durch Einbindung virtueller Sicherheitsmechanismen in den konventionellen Netzwerkschutz
-

IBM Security Network Intrusion Prevention System Virtual Appliance

Mehr Sicherheit und Effizienz für Ihre konventionellen und virtuellen Umgebungen

Das Thema Sicherheit hatte für Unternehmen schon immer eine sehr hohe Priorität. Die zunehmende Komplexität, die Zunahme von Sicherheitsverstößen und die zahlreichen Compiancerichtlinien haben dazu geführt, dass die Forderung nach einem ausgereiften Netzwerkschutz immer lauter wird. Gleichzeitig sind die Unternehmen durch die wirtschaftlichen Gegebenheiten gezwungen, durch entsprechende Konsolidierungs- und Virtualisierungsmaßnahmen den Bedarf an Hardwarekomponenten zu reduzieren. Die Herausforderung besteht darin, diese Prioritäten so aufeinander abzustimmen, dass die Sicherheit in Ihrem Unternehmen einerseits und Ihre Konsolidierungsbemühungen andererseits nicht gefährdet werden.

Die IBM Lösung Security Network Intrusion Prevention System Virtual Appliance bietet umfassenden präventiven Schutz in einer virtuellen Sicherheitsappliance, wodurch ein Maximum an Business-Continuity mit minimalem Ressourceneinsatz erreicht wird. Gestützt durch das IBM X-Force-Forschungs- und Entwicklungsteam wird die IBM Security Network Intrusion Prevention System Virtual Appliance auf virtuellen Plattformen eingesetzt, um sowohl physische als auch virtuelle Netzwerke auf einem gleich hohen Sicherheitsniveau zu schützen. Als virtuelle Appliance ist die IBM Security Network Intrusion Prevention System Virtual Appliance die ideale Lösung für Anbieter von Managed Cloud Services, da sie flexible Implementierungen in mehrfach genutzten virtuellen Umgebungen erlaubt. Eine zentrale Managementkonsole sowie ein breites Angebot an Consulting-Services helfen, die Implementierung und das Management von Sicherheitsmaßnahmen zu vereinfachen. Gleichzeitig bietet die modulare Architektur erweiterbaren Schutz, damit Sie auf die nächste große Bedrohung vorbereitet sind, unabhängig davon, wann oder wo diese auftritt.

Deutlich effizientere Konsolidierung durch eine virtuelle Sicherheitsappliance

Die Netzwerksicherheit bei konventionellen und virtuellen Plattformen erfordert häufig Appliances, die zu höheren Anforderungen im Rechenzentrum führen und das Rechenzentrum komplexer und kostspieliger machen können. Die IBM Security Network Intrusion Prevention System Virtual Appliance bietet hingegen optimale Sicherheit durch ihr hohes Leistungspotenzial und den erweiterten Schutz gegen unbefugte Zugriffe in einer virtuellen Sicherheitsappliance. Hoch entwickelte Erkennungstechnologien und virtuelle Ausgestaltung können dazu beitragen, die unkontrollierte Zunahme von physischen



Appliances auf ein Minimum zu reduzieren und eine effiziente Umsetzung Ihrer Konsolidierungspläne sicherzustellen, ohne die Sicherheit der Netzwerkoperationen zu gefährden. Hoher Durchsatz und niedrige Latenzzeiten regeln den Datenfluss und tragen zu effizienten Netzwerkoperationen bei.

Sicherheitsmaßnahmen vereinfachen und erweitern

Die IBM Security Network Intrusion Prevention System Virtual Appliance bietet denselben umfassenden präventiven Schutz für Ihre virtuellen Operationen, wodurch Sicherheitsrisiken in diesen Umgebungen blockiert werden können. Darüber hinaus entzerrt diese Lösung komplexe Prozesse, da sich virtuelle Sicherheit, konventionelle Unternehmenssicherheit und Sicherheitslücken über eine zentrale Managementschnittstelle verwalten lassen. Mehr Konsistenz lässt sich dabei nicht nur durch weniger Einzellösungen und -ressourcen erreichen, sondern auch durch die Fähigkeit, Netzwerkrichtlinien und Best Practices für Sicherheitsmaßnahmen sowohl im virtuellen als auch im physischen Netzwerk zu nutzen.

Immer einen Schritt voraus – bei wachsenden Bedrohungen und Compliance-Maßnahmen

Die IBM Security Network Intrusion Prevention System Virtual Appliance basiert auf dem vom IBM X-Force-Team entwickelten IBM Protocol Analysis Module (PAM), einer leistungsfähigen, erweiterbaren Protection-Engine, die neue Dimensionen beim Schutz gegen wachsende Sicherheitsrisiken eröffnet. Diese leistungsfähige PAM-Technologie macht die IBM Security Network Intrusion Prevention System Virtual Appliance zur umfassenden Lösung für den Netzwerkschutz mit folgenden Leistungsmerkmalen:

- IBM Virtual Patch-Technologie – Schutz gegen das Ausnutzen von Sicherheitslücken, unabhängig von einem Software-Patch
- Clientseitiger Anwendungsschutz – schützt Endbenutzer gegen Angriffe auf Anwendungen und Dateien, die jeden Tag genutzt werden, z. B. Microsoft Office-Dateien, Adobe PDF-Dateien, Multimediadateien und Web-Browser

- Erweiterter Netzwerkschutz – erweiterter Schutz gegen unbefugte Zugriffe einschließlich DNS-Schutz
- Datensicherheit – Überwachung und Identifikation nicht verschlüsselter, personenbezogener Daten und anderer vertraulicher Daten
- Webanwendungssicherheit – Schutz für Webanwendungen, Web 2.0 und Datenbanken (gleicher Schutz wie bei Webanwendungs-Firewalls)
- Anwendungssteuerung – Rückgewinnung von Bandbreite und Blockierung von Skype, Peer-to-Peer-Netzwerken und Tunnelung

Durch die Konsolidierung von Sicherheitsanforderungen wie Erkennung und Vermeidung von Sicherheitsrisiken, Datensicherheit, Webanwendungsschutz und Anwendungssteuerung trägt die IBM Security Network Intrusion Prevention System Virtual Appliance dazu bei, die Kosten für die Implementierung und das Management von Einzellösungen zu senken. Diese modular aufgebaute Technologie kann dazu beitragen, Ihr Netzwerk gegen die unterschiedlichsten Angriffe und Sicherheitsrisiken wie die folgenden zu schützen:

- Computerwürmer und Spyware
- Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)
- Bot-Netze
- Gezielte Angriffe auf Webanwendungen
- Proprietäre oder sensible Daten, die das Netzwerk verlassen

Sicherheitsservices beim Cloud-Computing

Die IBM Security Network Intrusion Prevention System Virtual Appliance ermöglicht Anbietern von Managed Cloud Services, spezielle Segmente im virtuellen Netzwerk zu schützen und optional angepasste Sicherheitsrichtlinien oder vertrauenswürdige „X-Force“-Standardkonfigurationen zu nutzen. Durch die Möglichkeit, neue Services zur Umsatzgenerierung mit X-Force-Sicherheitsfunktionen anbieten zu können, schaffen Anbieter von Cloud-Services sichtbare Alleinstellungsmerkmale und gleichzeitig das hohe Maß an Zuverlässigkeit, das ihre Kunden fordern.

Anforderungen und technische Spezifikationen				
	GV1000	GV200		
Prozessor	2x Quad Core Intel® Xeon® E5440 @ 2,83 GHz			
Betriebssystem	VMware ESX Infrastructure3 Version 3.5	VMware ESX Infrastructure 3 Version 3.5, VMware ESXi 3.5. VMware Server 2.0		
VM-Gastsystemunterstützung	Nicht zutreffend	Nicht zutreffend		
Arbeitsspeicher	1 GB RAM	1 GB RAM		
Netzwerkverbindung	Jede VMware-unterstützte NIC	Jede VMware-unterstützte NIC		
Plattenspeicher	10-GB-Festplattenlaufwerk	10-GB-Festplattenlaufwerk		
Leistungsmerkmale*		ESX 3.5	ESXi 3.5	VMware Server 2.0
Durchsatz	Bis zu 700 Mbps	Bis zu 200 Mbps	Bis zu 150 Mbps	Bis zu 50 Mbps
Verbindungen pro Sekunde	19.000	19.000	19.000	12.000
Gleichzeitige Sitzungen (max. Rate)	500.000	500.000	500.000	400.000
Betriebsmodi	GV 1000	GV 200		
Aktivschutz	Ja	Ja		
Passiverkennung	Ja	Ja		
Inline Simulation	Ja	Ja		
Geschützte Netzwerksegmente	1	1		
*Die Leistungswerte wurden mit der folgenden Konfiguration erzielt	IBM BladeCenter HT-Gehäuse, Blade IBM eServer HS21 – 8853AC1, NICs NetXtreme Broadcom5704S, Prozessor 2x Quad Core Intel Xeon E5440 @ 2,83 GHz, Betriebssystemversion ESX 3.5.0 Build 123630 Update 3	IBM BladeCenter HT-Gehäuse, Blade IBM eServer HS21 – 8853AC1, NICs NetXtreme Broadcom5704S, Prozessor 2x Quad Core Intel Xeon E5440 @ 2,83 GHz		

Einfache Implementierung und Verwaltung

Die IBM Security Network Intrusion Prevention System Virtual Appliance ist so konzipiert, dass sie neben der einfachen Installation, Konfiguration und dem einfachen Management dazu beiträgt, den eigentlich konträren Prioritäten „Mitarbeiterbedarf“ und „Netzwerksicherheit“ gerecht zu werden. Als eigenständige Virtual Appliance-Lösung bietet diese IBM Lösung hohe Sicherheit, ohne

Server-Images, virtuelle Server, Anwendungen oder die virtuelle Infrastruktur ändern zu müssen. Sie können aus verschiedenen Betriebsmodi auswählen:

- Aktiv – Intrusion Prevention: Schutz gegen unbefugte Zugriffe mit Blockierung
- Inline Simulation – zeigt die unbefugten Zugriffe an, die blockiert würden
- Passiv – Intrusion Detection: für die Ausgabe von Warnungen ohne Blockierung



Wenn Sie den Schutz Ihres Netzwerks auf einen zuverlässigen Anbieter von Sicherheitslösungen übertragen wollen, bietet Ihnen IBM bewährte Consulting und Managed Services über qualifizierte Service Solution-Teams an, die sich um Bewertung, Entwurf, Implementierung und Management kümmern.

Warum IBM?

Die IBM Security Network Intrusion Prevention System Virtual Appliance stellt erstklassige, auf die Erkennung von Sicherheitslücken ausgerichtete Sicherheitstechnologien für virtuelle Umgebungen bereit. So lassen sich Umgebungen mit virtuellen und physischen Netzwerken schützen und die angestrebten Konsolidierungsziele umsetzen. Neben den vorbeugenden Schutzmechanismen für alle Netzwerkebenen, der einfachen Implementierung und dem integrierten Management kennzeichnet diese umfassende Sicherheitsplattform die hervorragende Unterstützung des IBM X-Force-Forschungs- und Entwicklungsteams.

Weitere Informationen

Wenn Sie mehr über die IBM Security Network Intrusion Prevention System Virtual Appliance erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner oder besuchen Sie uns unter:

ibm.com/tivoli/solutions/threat-mitigation

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:

ibm.com

IBM, das IBM Logo, ibm.com und X-Force sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter

ibm.com/legal/copytrade.shtml

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation oder deren Tochtergesellschaften in den USA oder anderen Ländern. Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Die Produktdaten wurden zum Datum ihrer ersten Veröffentlichung auf ihre Korrektheit überprüft. Die Produktdaten können von IBM jederzeit ohne vorherige Mitteilung geändert werden. Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

Der Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen auswirken können, die er im Hinblick auf die Einhaltung solcher Bestimmungen durchführen muss. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit jeglichen relevanten Gesetzen und Verordnungen.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

© Copyright IBM Corporation 2010
Alle Rechte vorbehalten.



Bitte der Wiederverwertung zuführen