clavister®

Eine neue Dimension der Netzwerksicherheit für die Cloud mit Clavister

Der Markt für das Cloud Computing wird bis 2015 voraussichtlich auf 7,3 Milliarden Euro anwachsen, denn immer mehr von der Wirtschaftskrise betroffene Unternehmen wissen die Vorteile von Cloud Computing zu schätzen: weniger Kosten und mehr Mobilität und Flexibilität. Dieser Markt boomt zwar, doch am Horizont steht für viele eine große schwarze Wolke.

Laut einer IDC-Umfrage unter Nutzern von Cloud Services nannten 74 Prozent der IT-Verantwortlichen und CIOs die Sicherheit als den wichtigsten Hinderungsgrund für die Einführung von Cloud Services.

Der Gartner-Report „Top End User Predictions for 2012 and Beyond“ (Prognosen der wichtigsten Benutzer für die Jahre ab 2012) unterstreicht diesen Eindruck. Aus dem Report geht hervor, dass bis zum Jahr 2016 die finanziellen Schäden durch Cyberkriminalität mit einer Steigerungsrate von 10 Prozent pro Jahr wachsen werden und dass bis dahin 40 % der Unternehmen den Nachweis einer unabhängigen Sicherheitsprüfung verlangen werden, bevor sie einen Cloud-Dienst nutzen.

Die Cloud Services Provider (CSP) sind besonders von ihrem guten Ruf abhängig, und so ist es von entscheidender Bedeutung, dass sie über absolut zuverlässige Sicherheitsmechanismen und neueste Technik zum Schutz der Kundendaten verfügen. Vertrauenswürdige Sicherheit ist heute das wichtigste Unterscheidungsmerkmal, mit dem sich die CSPs von ihrer Konkurrenz absetzen können.

Sicherheit: ein Türöffner für Cloud-Angebote
Als führender Anbieter von erstklassigen Sicherheitslösungen betrachtet Clavister die effektive Sicherheit im Cloud Computing nicht als Hindernis, sondern vielmehr als Vorteil. Vor diesem Hintergrund wendet sich Clavister mit einem neuen Sortiment cleverer Sicherheitslösungen hauptsächlich an CSPs. Diese neue Produktreihe stößt in ganz neue Dimensionen der Datensicherheit vor und eröffnet den führenden Anbietern die Möglichkeit, mit ihren Netzwerken eine optimale Wertschöpfung zu erzielen.

Geringere Stellfläche und mehr Funktionalität
Die Sicherheitslösungen dieses neuen Sortiments umfassen die Clavister Virtual Series mit vier leistungsstarken Virtual Security Gateways (VSG), welche einen multifunktionalen SaaS-Dienst (Security as a Service) für virtuelle und Cloud-Umgebungen und Hosting Provider anbieten.

Clavister-Produkte werden immer komplett neu entwickelt. Ihr Design ist skandinavisch geprägt, und die Produkte gewähren ein Höchstmaß an Netzwerksicherheit – und das ist es, was die Kunden erwarten.

Die neue Produktreihe bietet das weltweit schnellste Sicherheitssystem in einem Gehäuse mit 1U-Formfaktor. Die Firewall leistet bis zu 240 Gigabit pro Sekunde (Gbps), während Konkurrenzprodukte mit 3U-Formfaktor nur eine Leistung von 150 bis 160 Gbps erzielen. Darüber hinaus verfügen die Geräte über verbesserte Betriebssysteme und eine benutzerfreundliche Bedieneroberfläche.

„Für Provider mit riesigen Räumen und zahlreichen Servern sind die Kosten pro Server-Rack so hoch, dass sie alles so klein wie möglich haben möchten“, sagt Johan Edlund, Vice President Product Management von Clavister. „Sie möchten immer mehr Rechenleistung auf immer kleineren Stellflächen, und genau das machen wir möglich, denn wir bieten größere Firewall-Leistung bei einem Formfaktor von einem Drittel der Größe vergleichbarer Lösungen.”

Mit Lizenzierungs- und Geschäftsmodellen, die speziell für Cloud-Käufer entwickelt wurden, kombiniert die neue Produktreihe vollständig zentralisierte Verwaltung mit reibungsloser Provisionierung und Bereitstellung. Kunden können das Self-Service-Portal nutzen, um die von ihnen gewünschten Dienste zu bestellen. So entfällt ein Großteil der bisherigen manuellen Bedienung, und die Kosten in umfangreichen Cloud-Umgebungen sinken. Sämtliche Leistungsmerkmale stehen auch auf unterschiedlichen Plattformen zur Verfügung. Im Gegensatz zu anderen Sicherheitslösungen, die aus diversen physikalischen und virtuellen Geräten zusammengestellt sind, kann Clavister beides anbieten, sodass sich die Software- und Lizenzverwaltung auf ein Minimum reduziert.

Einfache Bereitstellung
Die Clavister Virtual Series ist in den verschiedensten Szenarien rasch implementierbar, beispielsweise in Virtualisierungs-Umgebungen mit VMware oder mit anderen Virtualisierungspaketen und sogar in einer Kombination aus beidem.

Im Unternehmen kann die Clavister Virtual Series in einer virtualisierten Umgebung eingesetzt werden, um in einer ansonsten offenen Umgebung Schutzzonen einzurichten. Dies bedeutet, dass mit VSG in einem virtuellen Unternehmensrechenzentrum Sicherheitszonen für unterschiedliche Bereiche des virtuellen Netzwerks eingerichtet werden können. Es ist zum Beispiel möglich, mit Hilfe der Virtual Series für die Abteilungen Personal, Forschung und Entwicklung, Vertrieb und Finanzen in derselben Cloud eigene geschützte Zonen einzurichten.

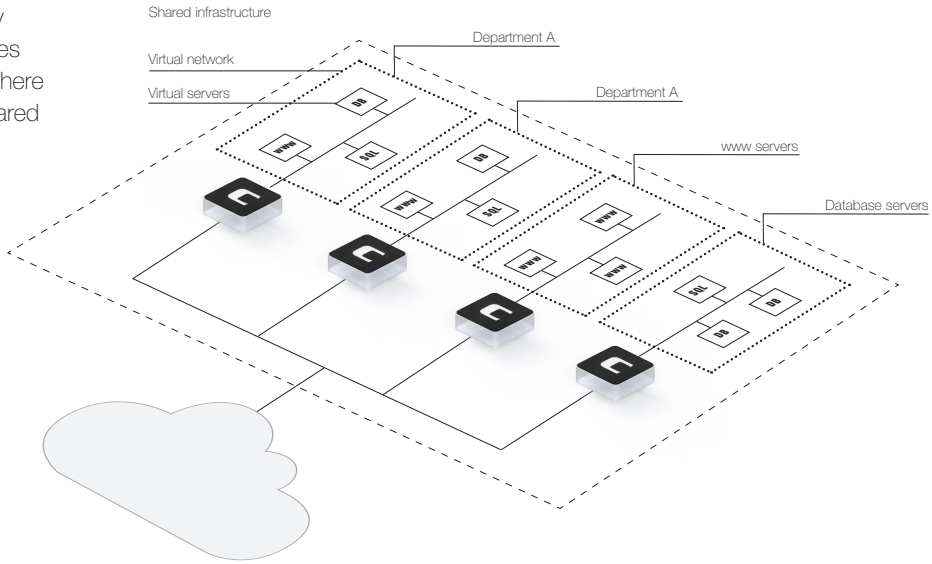


Fig. 1 The Virtual Security Gateway establishes protected zones where infrastructure is shared

Es können aber auch bestimmte Funktionen, wie etwa Internet-Server, Datenbank-Server und ERP-Systeme, in eigene geschützte Bereiche gelegt werden. Jede Abteilung kann ihre eigene Firewall betreiben, was die Berechnung und Aufteilung der Kosten vereinfacht.

ISPs können mit der Clavister Virtual Series ihren Internetkunden individuell konfigurierbare Sicherheitsdienste anbieten und zusätzlich abrechnen. Für den ISP ergeben sich höhere durchschnittliche Umsätze pro Kunde, wenn er allen seinen Bestandskunden kostengünstige Sicherheitsdienstleistungen anbieten kann. Aufgrund der extremen Skalierbarkeit der Lösung kann ein ISP seine kundenorientierten Service-Pakete genau auf das jeweilige Kundensegment zuschneiden.

Viele Probleme von Hosting-Providern, die durch gemeinsam genutzte Firewalls verursacht werden, können mit Hilfe von Clavister VSGs gelöst werden.

„Die meisten Hosting-Anbieter geraten in Schwierigkeiten, wenn sie eine von vielen Kunden gleichzeitig genutzte Firewall betreiben, weil fast alle Kunden eigene Sicherheitsrichtlinien integrieren möchten", erklärt Andreas Åsander, CEO von Clavister APAC (Asien-Pazifik). „Manche Kunden wünschen komplizierte Regelwerke, während sich andere mit grundlegenden Einstellungen zufrieden geben. Wenn man aber die Wünsche von ca. 10.000 Kunden berücksichtigen muss, bekommt man mit einer gemeinsam genutzten Firewall schnell Probleme.

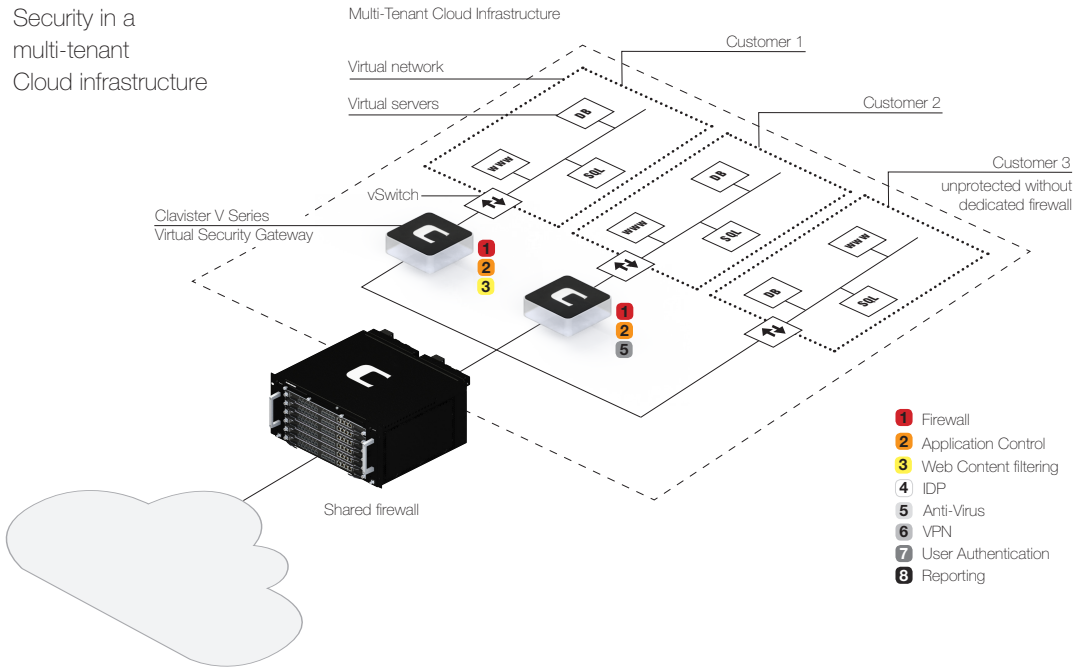
Letztendlich möchten die Anbieter überhaupt keine Einstellungsänderungen an der Firewall mehr vornehmen, weil sich jede für einen bestimmten Kunden vorgenommene Änderung auf alle Kunden auswirken kann. Schließlich gelangt man an einen Punkt, wo man nicht mehr weiß, welche Regeln zu welchem Kunden gehören, und die ganze Sache ist nicht mehr praktikabel. Wenn ein Kunde auf die Nutzung des Service verzichten möchte, wagt man es nicht, Regeln zu entfernen, da zu befürchten ist, dass auch andere Kunden in Mitleidenschaft gezogen werden. Die Firewall wird zu einem Engpass und zu einer tickenden Zeitbombe, die jeden Moment explodieren kann."

Kontrolle von Risiken

Die VSG-Lösungen von Clavister verhindern diese Risiken. Die gemeinsam genutzte Firewall bleibt weiterhin Eigentum des Hosting-Providers, stellt jedoch nur einen Überbau mit nur sehr wenigen Regeln dar, da die einzelnen Kunden keine eigenen Sicherheitsregeln mehr definieren können. Jeder Kunde hat sein eigenes VSG, mit dem er sich verbindet, um eigene Regelwerke zu implementieren. Auf diese Weise wird die Verantwortung für die Implementierung eines funktionierenden Regelwerks an den Kunden zurückgegeben. Daraus ergibt sich eine größere Kundenzufriedenheit, denn vereinzelte Eingriffe wirken sich kaum mehr auf die gesamte Firewall aus, Verstöße gegen Service-Level-Vereinbarungen werden vermieden, und der gute Ruf des Providers wird gestärkt.

„Sie werden als ein Unternehmen wahrgenommen, welches ausgezeichneten Datenschutz bietet. Um Geld zu verdienen, darf man nicht nur Sicherheit verkaufen, sondern muss sein Ansehen als zuverlässiger Provider stärken; danach kann man auch andere Dienste verkaufen", erklärt Åsander. „Unsere homogene Plattform bietet eine Fülle von Funktionen. So können Hosting-

Fig. 2 Security in a multi-tenant Cloud infrastructure



Anbieter zum Beispiel Firewall-Dienste, Dienste für die Kontrolle der Nutzung von Anwendungen und Virenschutz anbieten.

Wir offerieren auch verschiedene Abrechnungsmodelle für unterschiedlich strukturierte Kundengeschäfte, beispielsweise Pay-per-Use, Pay-per-Feature oder Finanzausgleich, abhängig von den Kosten- und Einnahmestrukturen. Mit unserem personalisierten Kundenportal können Hosting-Anbieter ihren Kunden maßgeschneiderte Nutzungslizenzen anbieten. Über dieses Portal können die Abrechnungssysteme des Kunden mit unseren Abrechnungssystemen kommunizieren, sodass daraus eine geschlossene Kette von Geschäftsprozessen entsteht."

Die Attraktivität eines VSG als Mittel der Wertschöpfung besteht in der einfachen Installation und in dem von Clavister angebotenen Vertriebsmodell. Es kann vollautomatisch, d. h. ohne Benutzerintervention, installiert und implementiert werden. Der Kunde meldet sich am Bedienerportal an und kann dann den oder die gewünschten Services auswählen, wie etwa Firewall, VPN und andere. Die gewählten Dienste werden automatisch im Kernnetz des Service Provider-Rechenzentrums implementiert und sind innerhalb von einer Stunde einsatzbereit.

„Der Vorteil für den Betreiber besteht darin, dass die Kosten nur einen Bruchteil der physikalischen Hardware-Installationskosten ausmachen, weil die Implementierung virtuell erfolgt", sagt Åsander. „Auch die so wichtige Skalierbarkeit ist gegeben, denn je nach Setup können 10 bis 100.000 Gateways auf einem einzigen physikalischen Server mit Standardausstattung implementiert werden.

Das bedeutet, dass der Service Provider weitere teure Dienste anbieten kann, da außer der Integration neuer Hardware in die virtuelle Infrastruktur nahezu keine Wartungsarbeiten oder manuelle Eingriffe anfallen. Wir bieten dem Service Provider neue Einkommensquellen und ein neues Abrechnungsmodell, denn für ein VSG ist nun keine Vorauszahlung mehr erforderlich. Eine Bezahlung muss erst bei Installation erfolgen.

Dies ermöglicht es den Service-Providern, Umsatzerträge und Investitionskosten aufeinander abzustimmen, da Vorleistungen und die damit einhergehenden Risiken entfallen. Zahlungen fallen erst dann an, wenn die Lösung beginnt, Erträge abzuwerfen.

Clavister betrachtet dieses Geschäftsmodell als langfristige Zusammenarbeit mit den Hosting-Providern als Partner."

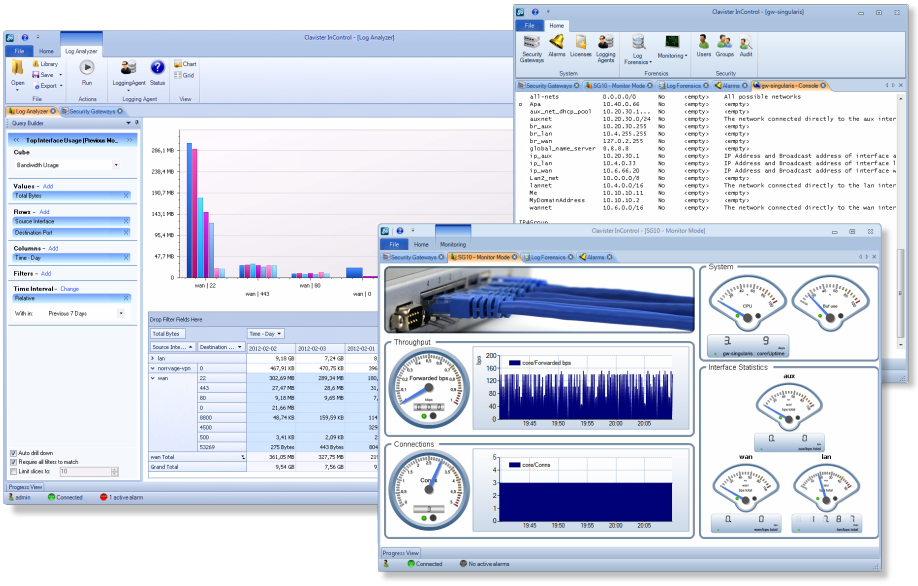
Mit InControl haben Sie Ihr Netzwerk im Griff

Das preisgekrönte Betriebssystem für Netzwerksicherheit von Clavister ist das Herzstück der Virtual Series. Es wurde in Clavister cOS Core 10 und cOS Stream 1.2 umbenannt und zeichnet sich durch eine stark vereinfachte Benutzeroberfläche aus.

Zu diesem neuen und verbesserten Software-Paket gehört auch InControl 1.3. Damit können Tausende von Geräten mit demselben Management-Tool zentral verwaltet werden. Benutzer können von einer einzigen Konsole aus Sicherheitsregeln festlegen und anwenden, den Status in Echtzeit überwachen, Software-Upgrades verwalten, Datensicherungen vornehmen sowie Daten wiederherstellen. InControl beinhaltet außerdem vielseitige forensische Tools für das Data-Mining und für Abweichungs- sowie Trendanalysen.

„Die zugrunde liegende Architektur macht es möglich, InControl 1.3 vollkommen ortsunabhängig zu betreiben und trotzdem eine hochwertige Verschlüsselung des Datenverkehrs zu gewährleisten", erklärt Edlund. „InControl 1.3 verfügt über moderne Fehlersuchfunktionen für die Geräte mit direktem Zugriff auf Protokolle, Snoops

Fig.3 InControl features a far simpler user interface.



und Befehlszeile. Wenn Sie einen Fehler lokalisiert haben, können Sie ihn mit InControl gleich beheben. Das Paket verfügt auch über ein integriertes Monitoring-Dashboard, mit dem man sich einen Überblick über den Netzwerkverkehr verschaffen kann. Mit dem Protokoll-Agent steht eine Lösung zur Verfügung, die innerhalb eines Unternehmens verteilt werden kann und zu einer Minimierung der Netzlast beiträgt. Für CSPs, Betreiber von Rechenzentren und ISPs haben wir auch ein umfangreiches Application Programming Interface (API), mit der InControl in die eigene Netzwerkinfrastruktur integriert und die Netzwerkkonfiguration automatisiert werden kann."

Kontrollieren Sie die wachsende Nutzung sozialer Medien

Clavister Application Control ist Bestandteil des cOS-Kerns und dient dazu, die wachsende Nutzung von sozialen Netzwerken unter Kontrolle zu halten. Das System ermöglicht die Nutzungskontrolle von Anwendungen wie Skype, YouTube und Facebook.

„Die Nutzung sozialer Netzwerke während der Arbeitszeit stellt einen riesigen Kostenfaktor für die Unternehmen dar", sagt Edlund. „Wenn ein Unternehmen zum Beispiel 500 Mitarbeiter beschäftigt, die Lohnkosten im Durchschnitt 60 Euro pro Stunde betragen, wenn man von 200 Arbeitstagen pro Jahr ausgeht und sich jeder Mitarbeiter im Durchschnitt nur 30 Minuten pro Tag mit den sozialen Netzwerken beschäftigt, entstehen dem Unternehmen jährliche Kosten in Höhe von 3 Millionen Euro.

Mit Application Control können Sie ermitteln, in welchem Umfang soziale Netzwerke in Ihrem Netzwerk genutzt werden; Sie können Diagramme und Analysen erstellen und Gegenmaßnahmen ergreifen. Wenn zum Beispiel die Marketingabteilung soziale Netzwerke geschäftlich nutzt, können sie für diese Abteilung die Nutzung vollständig freigeben, die Nutzung in anderen Abteilungen zeitlich einschränken und an berufliche Aufgaben binden, um Kosten zu sparen und das Netzwerk zu optimieren."

Vorteile für Unternehmen

Über die rein technischen Vorteile der Netzwerksicherheitslösungen von Clavister hinaus profitieren Kunden auch finanziell, denn sämtliche Produkt-Updates sind bereits im Abonnement für die Sicherheitslösungen und in den Cloud-Lizenzen enthalten. So erhalten die Kunden ein komplettes Sicherheitsökosystem; dieses wird regelmäßig aktualisiert, damit sichergestellt ist, dass ihre Sicherheitslösung immer auf dem neuesten Stand ist.

Das Abonnementsystem basiert auf fünf Säulen:

- Content-Sicherheit rund um den Virenschutz für Anwendungen sowie Intrusion Detection and Prevention (IDP)
- Netzwerksicherheit einschließlich Firewall, Virtual Private Networks (VPN) und Tunneling
- Netzwerkoptimierung für hohe Verfügbarkeit, Bandbreiten-Management und Traffic-Shaping
- Zentrale Verwaltung einschließlich Web-Benutzeroberfläche (WUI) und Befehlszeilen (CLI)
- Support und Wartung 24/7

Weitere Informationen

Wenn Sie mehr über Clavister Cloud-Security-Lösungen wissen möchten, besuchen Sie uns unter: www.clavister.com/solutions/cloud.

clavister®

WE ARE NETWORK SECURITY