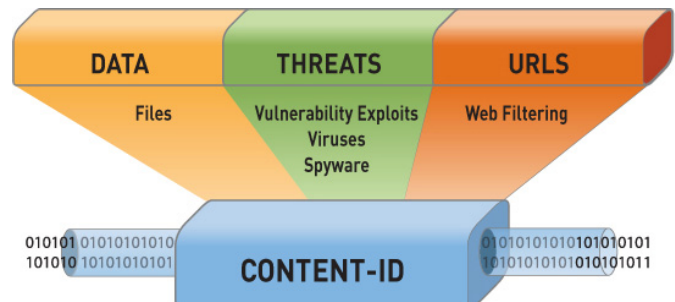


Das Internet ist heutzutage für Unternehmen allgegenwärtig; wir kommunizieren darüber mit Kunden, identifizieren Interessenten und interagieren mit Mitarbeitern. Während das Internet viele Vorgänge verbessert, die Effizienz erhöht und Kosten reduziert, werden Unternehmen immer anfälliger für Bedrohungen wie unerlaubten Zugriff, böswillige Angriffe und den neuesten Bedrohungen durch web-basierte Anwendungen. Zum Schutz vor bestehenden und zukünftigen Bedrohungen müssen Unternehmen von ihren Dienstleistern eine „next generation of protection“ einfordern – beziehungsweise eine Next Generation Managed Cloud Firewall (NGMCF). Dieses Dokument gibt einen Überblick über die 10 wichtigsten Funktionen einer NGMCF, die unabdingbar sind, damit Sie einer solchen Sicherheitslösung vertrauen können.



Die Anwendungstransparenz und -kontrolle ist für Ihre Netzwerksicherheit von entscheidender Bedeutung. Der Grund ist offensichtlich: Anwendungen können traditionelle, port-basierte Firewalls leicht tunneln. Port-basierte Firewalls sind auf dem „Applikations-Auge“ blind. Mitarbeiter, Auftragnehmer und Partner nutzen jede verfügbare Anwendung, die sie benötigen, um ihre Arbeit zu erledigen - oftmals gleichgültig oder nichts ahnend von der Gefahr, die dadurch Ihr Geschäft bedrohen könnte. IT-Sicherheits- und Netzwerk-Experten sind sich einig, dass die effektive Kontrolle von Internet-Applikationen ein immer wichtigerer Teil der Netzwerksicherheit wird. Während die „Next Generation Firewall“ von Gartner als führendes IT-Marktforschungsinstitut genau definiert ist, behaupten viele Netzwerksicherheitsprovider, dass eine Next Generation Firewall eine Mischung von anderen Funktionen wie Unified Threat Management (UTM) oder Intrusion Prevention System (IPS) sei.

Die meisten traditionellen Netzwerksicherheits-Hersteller versuchen Anwendungstransparenz und -kontrolle durch die Verwendung einer begrenzten Anzahl von Anwendersignaturen in deren IPS zu unterstützen oder binden externe Datenbanken an ihre Systeme an. Aber genau wegen dieser mangelnden Integration kann deren Potenzial nicht voll ausgeschöpft werden. Diese Produkte laufen immer noch unter der herkömmlichen „Port-Blocking-Technologie“ und eben nicht auf der „Next Generation Firewall“ Technologie. Es ist wichtig zu verstehen, dass diese Hersteller einen wichtigen Punkt übersehen – es geht nicht darum Internet-Anwendungen zu blockieren, vielmehr geht es darum sie sicher und kontrolliert zuzulassen. Leider ignorieren die angebotenen Lösungen von herkömmlichen Netzwerk-Ausrüstern das, was Unternehmen heutzutage mit Anwendungen/Applikationen machen - sie nutzen sie, um damit ihr Geschäft zu ermöglichen - und deswegen müssen sie sicherstellen, dass diese Anwendungen in einer sicheren Umgebung auch sicher laufen.

Für Unternehmen, die ihre Sicherheit verbessern möchten, ist die wichtigste Überlegung: Wird dieser neue Dienst mein Geschäft unterstützen und stärken, um wichtige Anwendungen zum Nutzen der Organisation sicher zu ermöglichen? Die wichtigsten Kernfragen sind:

- Wird die Transparenz und das Verständnis des Applikations-Traffic verbessert?
- Wird Daten-Traffic-Kontrolle ermöglicht – jenseits von bloßem „allow/deny“?
- Werden Bedrohungen aus dem Internet abgewehrt?
- Wird es keinen Kompromiss zwischen Performance und Sicherheit geben?
- Werden sich die Kosten für meine Organisation reduzieren?
- Werden sich meine IT-Mitarbeiter mit ihren Ressourcen auf unsere geschäftskritischen Prozesse konzentrieren können?
- Wird die Aufgabe des Risikomanagements erleichtert?
- Wird mein Geschäft sicherer - heute, morgen und in der Zukunft?

Wenn die oben gestellten Fragen mit „Ja“ beantwortet werden können, dann ist ein Wechsel zu einer Next Generation Firewall einfach zu rechtfertigen.

ARCHITEKTUR UND SICHERHEITSMODELL: AM BESTEN WIRD DER INTERNET-TRAFFIC IN DER FIREWALL KLASSIFIZIERT

Es gibt erhebliche Unterschiede zwischen einer Next Generation Firewall und UTM-Geräten in Bezug auf deren Architektur und Sicherheitsmodell. Diese Unterschiede haben einen großen Einfluss auf die realen Betriebs-Funktionen und Besonderheiten, Betriebs-Abläufe und Performance. Beim Bau der Next Generation Firewall haben diese Hersteller einen von zwei architektonischen Ansätzen verwendet:

- 1) **Anwendungs-Identifikation in der Firewall als die primäre Klassifizierungs-Engine**
- 2) **Hinzufügen von Anwendungs-Signaturen zu einem Intrusion Prevention System (IPS) oder einem IPS-ähnlichen Muster, die dann um eine Port-basierte Firewall ergänzt werden**

Beide können Anwendungen erkennen, aber mit unterschiedlichem Erfolg, Benutzerfreundlichkeit und Relevanz. Es ist wichtig zu verstehen, dass diese beiden architektonischen Ansätze nur ein (!) spezifisches Sicherheitsmodell für Anwendungsrichtlinien zulassen - entweder positiv (default deny), oder negativ (default allow).

Firewalls verwenden ein positives Sicherheitsmodell, oder „default deny“. „Default deny“ bedeutet, dass Administratoren Policies schreiben um Internet-Traffic zu erlauben (z.B. erlauben von WebEx, GoToMyPC), alles andere wird standardmäßig gesperrt und blockiert.

Negative Policies (z.B. block Limewire) können in diesem Modell verwendet werden, aber es ist eine wichtige Erkenntnis, dass diese Policy in einem positiven Sicherheitsmodell sagt, „all else deny.“ Eine wichtige Schlussfolgerung dieses Ansatzes ist, dass der gesamte Datenverkehr klassifiziert werden muss, um den gewünschten Internet-Traffic zu erlauben.

Dadurch wird Internet-Traffic sichtbar und Policies ermöglichen die Nutzung von Internet-Anwendungen. Ein weiteres wichtiges Ergebnis dieses Ansatzes ist, dass jeder unbekannte Internet-Traffic standardmäßig geblockt wird. Mit anderen Worten: die beste Next Generation Firewall ist eine Firewall.

Intrusion Prevention Systeme (IPS) arbeiten typischerweise nach einem „negativen Sicherheitsmodell“, bzw. „default allow“. „Default allow“ bedeutet, dass das IPS bestimmten Internet-Traffic erkennt und blockiert (typischerweise Bedrohungen bzw. „Threats“), und jeder andere IP-Traffic passieren darf. Traditionelle Netzwerk-Security-Anbieter fügen ihren Firewall-Systemen Applikations-Signaturen hinzu und „basteln“ somit ein IPS, welches sie an eine traditionelle, herkömmliche Port-basierte Firewall „schrauben“. Das Ergebnis ist ein „Application-Prevention-System“. Die Applikationskontrolle befindet sich in einem negativen Sicherheitsmodell - mit anderen Worten, es findet keine echte Applikationskontrolle auf der Firewall statt. Das Ergebnis ist, dass man nur das sieht, was man ausdrücklich sucht – das heißt aber im Umkehrschluss, dass unbekannter IP-Verkehr standardmäßig erlaubt ist.

Dieses Dokument legt sein Augenmerk auf die 10 wichtigsten Dinge, die eine Next Generation Managed Cloud Firewall (NGMCF) beherrschen muss. Es skizziert zudem die oben genannten Voraussetzungen, die wichtig sind für das grundsätzliche Verständnis um die zahlreichen am Markt befindlichen Firewall-Lösungen vergleichbar zu machen. Seien Sie kritisch in der Bewertung der einzelnen Lösungen.

10 DINGE DIE IHRE NEXT GENERATION MANAGED CLOUD FIREWALL BEHERRSCHEN MUSS

Es gibt drei Bereiche, die eine NGMCF unterscheiden: Sicherheitsfunktionen, Bedienungsfreundlichkeit und Performance. Mit den Sicherheitsfunktionen lassen sich entsprechende Sicherheitsmaßnahmen wirksam umsetzen, um alle Risiken im Netzwerkverkehr in den Griff zu bekommen. Von der Betriebsperspektive her stellt sich die große Frage: „Wo und wie kontrolliere ich meine Applikationen und wie schwer oder komplex ist es dies zu managen?“ Der Performance-Unterschied ist einfach: Kann die Firewall das tun, was sie tun soll – ohne Einbußen im Bereich Performance- bzw. Durchsatz?

Die 10 Dinge, die Ihre Next Generation Managed Cloud-Firewall vereinen muss, sind:

- 1) Identifizieren und kontrollieren von Anwendungen auf jedem beliebigen Port
- 2) Identifizieren und kontrollieren von Applikationen, die sich nicht auf einen bestimmten Port festlegen lassen
- 3) Entschlüsselung von ausgehendem SSL-Traffic
- 4) Scan auf Viren und Malware in erlaubten Anwendungen/Applikationen
- 5) Zurechtkommen mit unbekanntem Verkehr durch entsprechende Policies
- 6) Identifizieren und Kontrolle von Anwendungen die sich die gleiche Verbindung teilen
- 7) Sichtbarkeit und Kontrolle aller Anwendungen auch für Remote-Benutzer
- 8) Applikationskontrolle ohne Durchsatz- und Performance- Einbußen trotz aktivierter Policies
- 9) Kostengünstig
- 10) Schutz Ihres Netzwerks heute, morgen und in der Zukunft

1 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS ANWENDUNGEN AUF JEDEM BELIEBIGEN PORT IDENTIFIZIEREN UND KONTROLLIEREN, NICHT NUR STANDARD-PORTS (einschließlich Anwendungen die HTTP oder andere Protokolle verwenden)

Business Case: Anwendungsentwickler halten sich nicht mehr an Standard-Ports, Protokolle oder die Zuordnung von Anwendungen. Anwendungen wie Instant Messaging, Peer-to-Peer-Filesharing oder Voice-over IP arbeiten mit „Non-Standard-Ports“ oder beherrschen das „Port-Hopping“. Darüber hinaus haben Benutzer genug Erfahrung, um Anwendungen wie „Non-Standard-Ports“ zu betreiben (z.B. Microsoft Remote Desktop Protocol, SSH). In einer Welt, in der Ports immer irrelevanter werden, lassen sich anwendungsspezifische Regeln nur mit einer Firewall der neuesten Generation durchsetzen. Anwendung laufen auf jedem beliebigen Port. Dies ist einer der grundlegenden Technologie-Treiber, die eine Next Generation Firewall zur absoluten Notwendigkeit macht, während traditionelle, portbasierte Firewalls zunehmend überflüssig werden. Dies zeigt auch, warum eine „negative Kontrolle“ das Anwendungsproblem nicht lösen kann. Wenn eine Anwendung über jeden beliebigen Port läuft, muss eine Firewall die auf der negativen Kontrolle basiert, alle Signaturen auf zehntausenden Ports überprüfen, was wiederum weder skalierbar noch überschaubar ist.

Voraussetzungen: Das ist einfach – wenn eine Anwendung über jeden beliebigen Port laufen kann – dann muss Ihre zukünftige Firewall Internet-Traffic klassifizieren können, je nach Anwendung – zu jeder Zeit. Ansonsten erübrigen sich Sicherheitsmaßnahmen und Sie sind den gleichen Bedrohungen ausgesetzt, wie Sie sie schon seit Jahren kennen.

2 IHRE NEXT GENERATION MANAGED CLOUD-FIREWALL MUSS UMGEHUNGSMÖGLICHKEITEN IDENTIFIZIEREN UND KONTROLLIEREN: PROXIES, REMOTE ACCESS UND VERSCHLÜSSELTE TUNNEL-ANWENDUNGEN

Business Case: Die meisten Organisationen haben Sicherheitsrichtlinien - und Maßnahmen mit denen sie diese Sicherheitsrichtlinien durchsetzen. Mit Proxies, Remote Access Lösungen und verschlüsselten Tunnel-Anwendungen lassen sich Sicherheitsmaßnahmen wie Firewalls, URL-Filter, IPS und Web-Security-Gateways umgehen. Wenn Organisationen die Umgehungsmöglichkeiten nicht kontrollieren können, sind Sicherheitsrichtlinien nicht durchsetzbar. Dann setzen sich Organisationen Risiken aus, von denen Sie dachten, dass Sie diese mit ihren Sicherheitsrichtlinien im Griff hätten. Nicht alle Anwendungen sind gleich. Remote Access Lösungen haben berechtigte Benutzer und einige verschlüsselte Tunnel-Anwendungen. Dagegen haben externe, anonyme Proxies wie „Ultrasurf“ und „Tor“, welche die Kommunikation über SSL auf zufälligen Ports oder Anwendungen tunneln, nur einen wirklichen Zweck – die Umgehung Ihrer Sicherheits-Kontrollen und -Maßnahmen.

Voraussetzungen: Es gibt verschiedene Arten der Anwendungsumgehung mit jeweils leicht unterschiedlichen Techniken. Es gibt sowohl öffentliche als auch private externe Proxies (siehe proxy.org für eine große Datenbank von öffentlichen Proxys), die sowohl HTTP als auch HTTPS verwenden können. Private Proxies werden oft auf dynamischen IP-Adressen aufgesetzt (z.B. Heimcomputern) mit Anwendungen wie PHPProxy oder CGIProxy. Remote Access Anwendungen wie GoToMyPC oder LogMeln haben ihre Berechtigung, sollten aber wegen der damit verbundenen Gefahren kontrolliert und verwaltet werden. Die meisten anderen Umgehungstechniken (z.B. Ultrasurf, Tor, Hamachi) haben keinen legitimen Geschäftszweck. Zudem gibt es unbekannte Umgehungstechniken – siehe unten Punkt Nr. 6. Unabhängig davon, ob Sie Sicherheitsmaßnahmen im Einsatz haben, benötigt Ihre zukünftige Firewall spezielle Techniken, um mit all diesen Anwendungen, unabhängig von Port, Protokoll, Verschlüsselung oder anderen Ausweichmanövern, klar zu kommen. Eine weitere Überlegung: diese Anwendungen werden regelmäßig aktualisiert, damit sie schwerer zu erkennen und zu kontrollieren sind. Deshalb ist es wichtig, dass Ihre zukünftige Firewall diese Anwendungen identifizieren kann, und dass sichergestellt ist, dass die Applikations-Intelligenz auf der Firewall permanent aktualisiert und laufend gepflegt wird.

3 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS AUSGEHENDEN SSL-TRAFFIC ENTSCHLÜSSELN KÖNNEN

Business Case: Heute sind mehr als 15% des Netzwerkverkehrs SSL-verschlüsselt und in einigen Branchen wie Finanzdienstleistungen oder im Gesundheitswesen können es auch mehr als 50% sein. Angesichts der zunehmenden Verbreitung von HTTPS für viele hoch riskante und gerne verwendete Anwendungen (z.B. Gmail, Facebook) und der Möglichkeit der Benutzer, SSL auf vielen Websites auszuwählen, haben Netzwerksicherheit-Teams einen großen und wachsenden blinden Fleck ohne Entschlüsselung, Klassifizierung, Kontrolle und Erkennen von SSL-verschlüsseltem Datenverkehr. Selbstverständlich muss Ihre zukünftige Firewall flexibel genug sein, um bestimmten SSL-verschlüsselten Datenverkehr zuzulassen (z. B. Web-Datenverkehr von Finanzdienstleistungen oder Organisationen im Gesundheitswesen), während andere Arten (z.B. SSL auf Nicht-Standard-Ports, HTTPS von nicht klassifizierten Webseiten aus Ost-Europa) mittels Policies entschlüsselt werden können.

Voraussetzungen: Die Fähigkeit ausgehenden SSL-Traffic zu entschlüsseln ist ein zentraler und kritischer Punkt. Nicht nur weil immer mehr IP-Traffic verschlüsselt wird, sondern auch, weil andere wichtige Funktionen ohne die Fähigkeit zur Entschlüsselung von SSL unwirksam würden (z.B. Kontrolle von Umgehungsmöglichkeiten, Anwendungskontrolle, Scannen von erlaubten Anwendungen und Kontrolle von Anwendungen, die sich dieselbe Verbindung teilen. Achten Sie bei der Auswahl auch darauf, dass SSL auf jedem beliebigen Port entschlüsselt und kontrolliert werden kann, und die Lösung die notwendigen Funktionen in Hard- und Software mitbringt, um SSL-Entschlüsselung über zehntausende, gleichzeitige SSL-Verbindungen ohne Leistungseinbußen und mit hohem Durchsatz auszuführen.

4 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS IN ERLAUBTEN KOLLABORATIONSANWENDUNGEN NACH BEDROHUNGEN SUCHE

Business Case: Unternehmen arbeiten zunehmend mit gehosteten kollaborativen Anwendungen wie: Microsoft SharePoint, Google Docs, Box.net, Microsoft Office 365 oder einer gehosteten Extranet-Anwendung bzw. verschiedenster File-Sharing-Anwendungen. Diese Anwendungen bergen ein hohes Bedrohungsrisiko, da viele infizierte Dokumente in Kollaborationsanwendungen abgelegt sind, zusammen mit Dokumenten, die sensible Kundendaten wie Kreditkarten-Informationen enthalten können. Darüber hinaus hängen Microsoft SharePoint Anwendungen von Technologien ab, die regelmäßig Ziele für Exploits sind - einschließlich Microsoft SQL Server oder IIS. Das vollständige Blocken dieser Anwendungen ist nicht ideal oder realistisch, aber Kollaborationsanwendungen bergen ein Risiko für Ihr Unternehmen.

Voraussetzungen: Ein Teil der sicheren Anwendungsunterstützung ist es, die Anwendungen zu erlauben und darin nach Bedrohungen zu suchen. Diese Anwendungen kommunizieren über verschiedene Protokolle (z.B. SharePoint - HTTPS und CIFS, siehe oben Anforderung Nr. 3) und erfordern eine differenziertere Maßnahme als „blockieren der Anwendung“. Der erste Schritt ist es, die Anwendung zu identifizieren, unabhängig vom genutzten Port oder einer Verschlüsselung. Dann muss die Anwendung erlaubt werden und anschließend wird sie nach Bedrohungen, Exploits, Viren/Malware oder Spyware durchsucht ... oder sogar nach vertraulichen, sensiblen Informationen.

5 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL ERSTELLT RICHTLINIEN FÜR UNBEKANNTEN TRAFFIC

Business Case: Es wird immer unbekanntem IP-Traffic geben, und dieser stellt ein erhebliches Risiko für jede Organisation dar. Es gibt einige wichtige Punkte im Zusammenhang mit unbekanntem IP-Traffic zu berücksichtigen – ihn zu minimieren, charakterisieren selbst erstellter Anwendungen und ihn somit „bekannt“ und sichtbar machen für Policies.

Voraussetzungen: Zuerst sollte ihre zukünftige Firewall standardmäßig den gesamten Datenverkehr klassifizieren. Dies ist ein Bereich, in dem die obigen Ausführungen über Architektur und Sicherheit wichtig werden. Positive (default deny) Modelle klassifizieren alles, negative (default allow) Modelle klassifizieren nur das, was man ihnen sagt, dass sie es klassifizieren sollen. Zweitens sollte es für speziell entwickelte Anwendungen eine Möglichkeit geben, diesen IP-Traffic exakt zu identifizieren, damit er als bekannter Traffic sichtbar wird. Drittens spielt das Sicherheitsmodell erneut eine wichtige Rolle - ein positives Modell kann jeden unbekanntem IP-Verkehr verweigern - was man nicht kennt, kann einem auch nicht wehtun bzw. Schaden zufügen. Ein negatives Modell erlaubt jeglichen unbekanntem IP-Traffic - was man nicht kennt, wird Ihnen Schaden zufügen. Viele Botnetze verwenden zum Beispiel Port 53 (DNS), um eine Kommunikation zu deren Control-Servern aufzubauen. Wenn Ihre zukünftige Firewall nicht in der Lage ist unbekanntem IP-Traffic zu erkennen und zu kontrollieren, können Botnetze ungehindert auf Ihr Netzwerk zugreifen.

6 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS ANWENDUNGEN, DIE SICH EINE VERBINDUNG TEILEN, IDENTIFIZIEREN UND KONTROLLIEREN

Business Case: Anwendungen teilen sich „sessions“. Um sicherzustellen, dass Benutzer eine Anwendungs-„Plattform“ verwenden, sei es Google, Facebook, LinkedIn oder Yahoo, integrieren Anwendungsentwickler zahlreiche weitere Anwendungen, die wiederum andere Risiken bergen – aber auch Nutzen bieten. Werfen wir einen Blick auf das obige Beispiel Gmail. Gmail hat die Möglichkeit eine Google Talk Session innerhalb der Gmail Session zu öffnen. Gmail und Google Talk sind grundverschiedene Anwendungen und Ihre zukünftige Firewall sollte die beiden auseinanderhalten und über das Firewall-Regelwerk kontrollieren können.

Voraussetzungen: Die einfache Klassifizierung einer Plattform oder Website reicht nicht. In anderen Worten: die „schnelle Lösung“ ist keine Option – eine „einmal-erkannt-und-erledigt“-Klassifizierung ignoriert die Tatsache, dass sich Anwendungen Sessions teilen. IP-Traffic muss kontinuierlich evaluiert werden, um die Anwendung zu verstehen, gerade wenn der Benutzer innerhalb der Session die Anwendung wechselt. Schauen wir uns die technischen Anforderungen nochmal am Gmail/Google Talk Beispiel an: Gmail verwendet standardmäßig HTTPS, also ist der erste Schritt die Entschlüsselung. Diese muss aber kontinuierlich erfolgen, genauso wie die Anwendungsklassifizierung, weil der Nutzer zu jeder Zeit einen Chat starten könnte, der wiederum mit einem völlig anderen Regelwerk verbunden ist.

7 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS FÜR MOBILE BENUTZER DIE GLEICHE ANWENDUNGSTRANSPARENZ UND -KONTROLLE ERMÖGLICHEN WIE FÜR BENUTZER AN UNTERNEHMENSSTANDORTEN

Business Case: Benutzer sind zunehmend mobil und außerhalb des Unternehmens unterwegs. Früher waren das lediglich die „Road Warriors“, heute sind es ganz normale Mitarbeiter, Auftragnehmer, Partner und Dienstleister, die aus der Ferne zusammen arbeiten. Ob sie nun von einem Café, von zu Hause oder von einem Kunden aus arbeiten, Ihre Benutzer erwarten, dass Ihnen Ihre Anwendungen via Wi-Fi, Wireless-Breitband, oder auf anderen Wegen zur Verfügung stehen. Unabhängig davon, wo sich der Benutzer oder die Anwendung befindet, sollte derselbe Standard bzgl. der Kontroll- und Security-Möglichkeiten gelten. Wenn Ihre zukünftige Firewall lediglich die Sichtbarkeit und Kontrolle von Anwendung nur innerhalb der vier Wände des Unternehmens aber nicht außerhalb ermöglicht, dann verkennen Sie die Tatsache von hohem und riskantem IP-Traffic, der von mobilen Benutzern ausgeht.

Voraussetzungen: Konzeptionell ist es einfach. Ihre zukünftige Firewall muss konsequent für Transparenz und Kontrolle des IP-Traffic sorgen, unabhängig davon, ob sich der Benutzer innerhalb oder außerhalb Ihres Netzwerks befindet. Das soll aber nicht heißen, dass es ein und dieselbe Policy für beide Benutzergruppen gibt. Es muss möglich sein, dass mobile Mitarbeiter Skype verwenden – es muss aber auch möglich sein, Skype in der Unternehmenszentrale zu verbieten. Wiederum andere verlangen eine Security-Policy, die es außerhalb des Büros verhindert salesforce.com-Anhänge herunterzuladen, es sei denn, sie haben die Festplattenverschlüsselung eingeschaltet. Dies sollte mit Ihrer zukünftigen Firewall möglich sein ohne: 1) signifikante Latenzzeit für den Benutzer, 2) unnötigen operationellen Aufwand für den Administrator, oder 3) erhebliche zusätzlichen Kosten für die Organisation. Außerdem soll die Lösung eine sichere Virtual Private Network (VPN)-Verbindung zwischen Remote-Benutzern, Dienstleistern oder Partnern aufbauen und zusätzliche Sicherheit und Produktivität ermöglichen, wenn mobil auf das Firmennetzwerk zugegriffen wird. Das VPN arbeitet auf Netzwerk-Ebene des OSI-Modells und sichert alle Daten, die sich zwischen dem Remote-Benutzer und dem Firmennetzwerk befinden. Ein SSL VPN für Remote-Benutzer stellt den sicheren Zugriff auf das Netzwerk über einen Web-Browser her, ohne vorher eine Client-Anwendung zu installieren, um eine zusätzliche Sicherheitsebene einzuziehen, um Ihr Unternehmen zu schützen.

8 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS DEN GLEICHEN DURCHSATZ UND LEISTUNG BEI VOLLSTÄNDIG AKTIVIERTER APPLIKATIONSKONTROLLE HABEN

Business Case: Viele Unternehmen haben mit dem erzwungenen Kompromiss zwischen Leistung und Sicherheit zu kämpfen. Allzu oft würden die aktivierten Sicherheitsfunktionen den Durchsatz und die Performance ab. Wenn Ihre Next Generation Firewall richtig aufgesetzt wurde, ist dieser Kompromiss nicht notwendig.

Voraussetzungen: Die Bedeutung der richtigen Firewall-Architektur ist hier offensichtlich. Das „Hinbasteln“ von verschiedenen Sicherheitsfunktionen und Technologien an eine Port-basierte Firewall, bedeutet in der Regel zusätzliche Komplexität in der Administration und schlechtere Performance. Die Firewall-Software muss aus einem Guss sein. Selbst rechenintensive Aufgaben (z.B. Anwendungsidentifikation) müssen selbst bei hohem IP-Traffic in kritischen Infrastrukturen ohne Latenz laufen. Dafür bedarf es eines speziellen Designs für Netzwerk, Sicherheit (einschließlich SSL-Terminierung) und Content-Scanning.

9 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS KOSTENEFFIZIENT SEIN

Business Case: Betriebskosten im Zusammenhang mit der Bereitstellung und Verwaltung der Informationssicherheit sind Overhead-Kosten und setzen sich aus zahlreichen einzelnen Kostenblöcken, einschließlich folgenden, zusammen:

- Die Kapitalkosten für die Beschaffung von Hard- und Software
- Die Kosten für die Installation und Konfiguration der Software durch Ihre Mitarbeiter oder Dienstleister
- Die jährlichen Kosten für Wartung der Hardware sowie Software-Updates und -Upgrades
- Die jährlichen Kosten für die Verwaltung und Überwachung der Systeme und der Infrastruktur
- Die Kosten für die Fortbildung Ihrer Mitarbeiter oder Dienstleister
- Die Kosten, um neue Lösungen für Ihr Unternehmen zu evaluieren, um künftigen Bedrohungsszenarien gerecht zu werden

Investitionskosten, Wartungskosten, Personalkosten – die meisten Unternehmen verstehen, dass ihr Geld besser in die Entwicklung und Einführung neuer Produkte oder Dienstleistungen investiert wäre. Netzwerksicherheit ist Overhead und es ist kein Ende in Sicht. Zahlreiche Unternehmen sind mit den Kosten einer Security-Lösung überfordert, noch bevor diese läuft. Eine NGMCF Lösung hilft Unternehmen ihr Kapital effektiver und effizienter einzusetzen.

Voraussetzungen: Eine NGMCF sollte Ihre Kapital- und Betriebskosten reduzieren und gleichzeitig Ihren Schutz für Ihre Organisation und Ihr Geschäft deutlich verbessern und alle folgenden Punkte durch eine einfache monatliche Gebühr ersetzen:

- Upfront-Investitionen für Hard- und Software
- Jährliche Hardware-Wartungsverträge
- Jährliche Software-Update Verträge
- Personalkosten für Installation und Konfiguration Ihrer Lösung
- Personalkosten für Konfigurationen weil sich ihr Unternehmen verändert
- Personalkosten für die Suche nach Lösungen für zukünftige Bedrohungsszenarien
- Laufende Schulungs- und Zertifizierungskosten für Ihre Mitarbeiter
- Personalkosten für die Überwachung

Darüber hinaus ermöglicht eine NGMCF für Sie das Verteilen der Gemeinkosten für ein Network Operation Center (NOC). Sie müssen keine Forschung & Entwicklung betreiben, um zukünftigen Bedrohungsszenarien gewachsen zu sein – Sie nutzen unsere Erfahrungen aus Bedrohungen, die alle Organisationen betreffen. Wenn Ihr Unternehmen wächst können sich Sicherheitsbedürfnisse verändern oder erhöhen. Ihre NGMCF sollte in der Lage sein, sich Ihrem Geschäft anzupassen. Mit der richtigen NGMCF sind Sie in der Lage Ihre Kosten zu reduzieren, während Sie gleichzeitig Ihr Sicherheitsniveau anheben.

10 IHRE NEXT GENERATION MANAGED CLOUD FIREWALL MUSS SIE SCHÜTZEN - HEUTE, MORGEN UND IN ZUKUNFT

Business Case: Die meisten Unternehmen sind nicht statisch. Sie müssen sich ständig weiterentwickeln und neu erfinden und sich an neue Anforderungen des Marktes und den Wettbewerbsdruck anpassen. Diese sich ständig ändernden Parameter schaffen immer wieder neue Herausforderungen für Unternehmen, deren Mitarbeiter und deren Infrastruktur für neue Anwendungen und neue Geschäftsmodelle. Unternehmen sollten in Wachstumsbereiche wie Vertrieb, Marketing und die Entwicklung neuer Produkte investieren – und nicht in einen Overhead-Bereich wie Informationssicherheit. Die meisten Organisationen adressieren Informationssicherheit als reaktives Projekt. Dabei sollte sie als 24/7-Aufgabe behandelt werden, um den laufenden Veränderungen in der Geschäftswelt und den damit verbundenen Bedrohungen gerecht zu werden. Allzu oft ist IT-Sicherheit eine reaktive Aufgabe aufgrund eines IT-Security Problems, anstatt sich permanent mit der Bedrohungslage auseinanderzusetzen. Die richtige NGMCF sollte Ihr Unternehmen proaktiv schützen, egal wie sich Ihr Unternehmen entwickelt und egal, was die Bedrohung ist. Schutz Ihrer Geschäfte rund um die Uhr.

Voraussetzungen: Eine NGMCF sollte einen proaktiven Security-Ansatz bieten. Ihre NGMCF soll nicht nur Ihre Unternehmung heute schützen, sie muss sich kontinuierlich weiterentwickeln, um auf zukünftige Bedrohungsszenarien und technologische Entwicklungen rechtzeitig reagieren zu können. Genauso wie Haus-Alarmanlagen werden Sie durch ein erweitertes Team von zertifizierten Fachleuten in einem geschützten NOC betreut, die da sind, wenn Sie es nicht sind. Selbst wenn Sie ein eigenes IT- oder Security-Team haben, das diese Funktionen ausübt, ist es schwer, die komplette Bandbreite auf der Suche nach zukünftigen Bedrohungen abzudecken. Wenn Ihr Unternehmen sich entwickelt und wächst, kann sich Ihr NGMCF Anbieter mit Ihnen entwickeln und wachsen. Sie beziehen einen Service, der sich Ihrem Unternehmen anpasst.

FAZIT: Ihre Next Generation Managed Cloud Firewall muss Anwendungen sicher zur Verfügung stellen und Sie in Ihrem Geschäft unterstützen

Benutzer, Dienstleister und Geschäftspartner werden weiterhin neue Anwendungen und Technologien entwickeln mit denen Bedrohungen einhergehen. Anwendungen ermöglichen es den Mitarbeitern Ihre Arbeit zu erledigen. Deswegen ist die sichere Anwendungskontrolle so wichtig. Um dies zu ermöglichen, müssen Netzwerk-Security-Teams entsprechende Richtlinien und Kontrollmöglichkeiten haben, um entsprechende Unternehmensregeln durchzusetzen. Die 10 hier beschriebenen Anforderungen sind kritische Funktionen, die angesichts einer sich verändernden Bedrohungslandschaft berücksichtigt werden müssen. Ohne einer Netzwerk-Sicherheitsinfrastruktur, welche diese Bedrohungen in ihrer Vielfalt und Tiefe bewältigt, können Sicherheits-Teams Business-Anwendungen nicht sicher zur Verfügung stellen. Um Ihrem Unternehmen die Sicherheit und den Anwendungs-Schutz, den Sie brauchen, zu gewährleisten, müssen Sie nicht länger warten. Eine NGMCF kann Ihnen den gewünschten Schutz mit entsprechender Performance/Leistung bei gleichzeitiger Kosteneffizienz und Wirtschaftlichkeit zur Verfügung stellen.

ÜBER INDEVIS CLOUD FIREWALL SERVICE:

Der indevis Cloud Firewall Service ist einer von zahlreichen Cloud Security Services von indevis. Er schützt Ihr Unternehmen und stellt einen sicheren ein- und ausgehenden Internet-Zugang über ein sicheres managed Firewall-Gateway zur Verfügung. Dieser Managed Firewall-Service sorgt auch für eine konsequente Durchsetzung Ihrer Sicherheitsrichtlinien für alle Ihre Standorte und mobilen Mitarbeiter – ohne Vor-Ort-Geräte oder spezielles IT-Personal. Der indevis Cloud Firewall Service bietet höchste Sicherheit und Schutz bei gleichzeitiger Reduzierung der Verwaltungskosten, er beseitigt Investitionskosten und bietet rund um die Uhr 24/7-Überwachung. Wir verbessern die Produktivität Ihrer Mitarbeiter und verbessern die Netzwerk-Performance und den Schutz sensibler Unternehmensdaten. Mit dem indevis Cloud-Firewall-Dienst sind Sie bereit für die Herausforderungen der aktuellen und zukünftigen Bedrohungen. Der indevis Cloud-Firewall-Dienst steht in drei Optionen zur Auswahl, um Ihrem speziellen Schutzbedarf gerecht zu werden. Für weitere Informationen besuchen Sie bitte www.indevis.de.

Der indevis Cloud-Firewall-Dienst wird mit der Technik von Palo Alto Networks™ betrieben. Palo Alto Networks Next Generation Firewalls ermöglichen Visibilität und granulare Policy-Kontrolle von Anwendungen und Inhalten - per Benutzer, nicht nur per IP-Adressen - von bis zu 20Gbps ohne Leistungseinbußen. Basierend auf der patentierten App-ID™-Technologie kann Palo Alto Networks Firewall-Anwendungen genau identifizieren und kontrollieren, anwendungsunabhängig von Port, Protokoll, ausweichender Anwendung oder SSL-Verschlüsselung. Sie scannt Inhalte, um Bedrohungen zu stoppen und ungewollten Datenabfluss zu verhindern. Unternehmen können damit erstmalig sicher mit Web 2.0 Anwendungen arbeiten und erhalten vollständige Transparenz und Kontrolle, bei gleichzeitiger deutlicher Reduzierung der Gesamtbetriebskosten durch Konsolidierung auf ein Gerät. Für weitere Informationen besuchen Sie bitte www.paloaltonetworks.com.

ÜBER INDEVIS

Die indevis GmbH ist ein international, national und regional tätiges Unternehmen auf dem Feld der Informationstechnologie und Netzwerkkommunikation, das Lösungen und Dienste für sichere Datennetze anbietet, welche alle Anforderungen sowohl der Wirtschaft als auch von öffentlichen Behörden und Hochschulen erfüllen.

Unsere Kunden unterstützen wir in der Analyse, Konzeptionierung, Realisierung, Betrieb und Betriebsunterstützung von IT-Sicherheits- und -Netzwerkinfrastruktur und Informationssicherheit.

Seit 1999 versteht sich die indevis GmbH als Lösungsanbieter für komplexe IT-Sicherheits- und Netzwerk-Infrastrukturen und steigert die Effizienz von Organisationen in den verschiedensten Branchen.

Zu unseren zufriedenen Kunden zählen namhafte Unternehmen in den Bereichen:

- Automobil- und Zulieferindustrie
- Beratungsunternehmen (RAe, WP, StB, UB, PAe)
- Dienstleistungsunternehmen
- Fertigungsindustrie
- Finanzdienstleister
- Gesundheitswesen
- Lebensmittelindustrie
- Maschinenbau
- Medizintechnik
- Öffentliche Hand/Verwaltung/Behörden
- Universitäten, Hochschulen und Wissenschaft

indevis versteht sich als Partner dieser Organisationen, der seinen Kunden Lösungen für sichere Netzwerke bietet oder ihm komplexe Netzwerkaufgaben abnehmen kann. Dies wird durch professionelle Management- und Supportdienste abgesichert. Ziel von indevis ist es Ihnen eine perfekte Beratung zu unseren sehr guten Produkten, Dienstleistungen und neuester Technologie zu liefern – zu wettbewerbsfähigen, fairen Preisen! Seit 1999 machen und verstehen wir dieses Geschäft.

Weitere Informationen zu unseren Produkten und Dienstleistungen finden Sie im Internet unter:

www.indevis.de

Kontaktperson: Herr Andreas Mayer

Telefon: +49 (89) 45 24 24-100

E-Mail: sales@indevis.de