Zscaler Cloud Firewall

Wegweiser für eine sichere Migration in die Cloud

zscaler™

Nutzen Sie die Vorteile der Zscaler Cloud Firewall bei Ihrer Migration in die Cloud

Die Tatsache, dass Anwendungen mithilfe von Webprotokollen in die Cloud verlagert werden, ist keine Neuigkeit. Bei Zscaler haben wir diese Verschiebung im Jahr 2008 vorhergesehen, als wir mit dem Aufbau unserer Security Cloud begannen. Heute gibt uns unsere massiv skalierbare Cloud die Flexibilität, den gesamten Traffic zu untersuchen und festzustellen, was in den Daten für HTTP- und HTTPS-Sessions passiert.

Mit der Auslagerung von Applikationen aus zentralisierten Rechenzentren wird das Modell des zentralen Backhauling problematisch – es ist nicht nur teuer, sondern führt auch zu Latenzen bei der Nutzererfahrung. Wenn Sie beispielsweise Ihr DNS durch eine herkömmliche Firewall an einem zentralen Ort leiten, erfolgt die Antwort am Standort der Firewall und nicht an dem des Benutzers, was sich auf die Echtzeitleistung der Anwendung auswirkt.

Cloud-Anwendungen sind leistungsstarke Business-Enabler, bringen jedoch auch Herausforderungen mit sich. Office 365 öffnet beispielsweise mehrere Verbindungen pro Benutzer und erhöht die Bandbreite, was die Port- und Durchsatzkapazität der herkömmlichen Firewall erschöpft. Laut einer von Zscaler in Auftrag gegebenen neuen Umfrage zu den Auswirkungen des Deployment von Office 365 kam es häufig zu Netzwerkproblemen und Latenzen. Obwohl viele Organisationen ihre Firewalls vor dem Deployment aktualisiert hatten, verzeichneten 69 Prozent nach der Bereitstellung immer noch Latenzen. Auch das Erhöhen der Bandbreite für zurückgeleiteten Traffic funktionierte nicht. 69 Prozent der Befragten berichteten von wöchentlichen, 30 Prozent von täglichen Leistungsproblemen.

Wie kann die Zscaler Cloud Firewall helfen?

Zscaler Cloud Firewall meistert diese Herausforderungen auf die gleiche Weise, wie der Cloud-Proxy beim Web-basierten Traffic hilft. Sie ermöglicht schnelle und sichere Internet-Breakouts für alle Ports und Protokolle, ohne dass Appliances aktualisiert oder bereitgestellt werden müssen, und all dies mit zentraler Verwaltung. Wie die gesamte Plattform von Zscaler skaliert die Zscaler Cloud Firewall elastisch je nach Verbrauch, und Ihre Kosten richten sich ausschließlich nach der Anzahl der Benutzer.

Mit Zscaler sind Richtlinien nicht an einen physischen Standort gebunden. Stattdessen folgen die Richtlinien den Benutzern, um ihnen unabhängig von Gerät oder Verbindungsort identischen Schutz zu bieten. Dies bedeutet, dass die Führungskräfte Ihres Unternehmens überall denselben Zugang und Schutz erhalten, egal, ob sie in der Firmenzentrale arbeiten, Niederlassungen besuchen oder weltweit auf Geschäftsreise sind.

Zscaler bietet zwei Cloud-Firewall-Services an: Eine standardmäßige Cloud Firewall, die in jedem Abonnement von Zscaler Internet Access enthalten ist, und eine erweiterte Cloud Firewall, die im Transformationspaket eingeschlossen ist oder als separates Upgrade erworben werden kann.

Was ist der Unterschied zwischen „standardmäßiger“ und „erweiterter“ Cloud Firewall?

Die standardmäßige Zscaler Cloud Firewall ist in Ihrem Abonnement der Services von Zscaler Internet Access enthalten. In der folgenden Beschreibung finden Sie einige der Richtlinienfunktionen, die Ihnen bereits zur Verfügung stehen. Wir werden auch auf die erweiterte Zscaler Cloud Firewall eingehen, ein Service, der Bestandteil des Transformationspakets ist, aber auch als einzelnes Upgrade erworben werden kann.

Lassen Sie uns zunächst einen Blick auf die Richtlinien werfen, die Sie in beiden Produkten finden

STANDARD CLOUD FIREWALL

Anwendung von Sicherheitsrichtlinien zum Zulassen/Blockieren basierend auf IP-Adressen von Quelle und Ziel, Ports und Protokollen. Folgendes steht für Ihren gesamten ausgehenden Traffic zur Verfügung:

- Einheitliche Richtlinien (5 Tupel pro Standort)
- Einzelne Verwaltungskonsole
- Ein Satz von Logs für all Ihre Standorte und Benutzer

ADVANCED CLOUD FIREWALL

Anwendung granularer Sicherheitsregeln zum Zulassen/Blockieren basierend auf Applikationen mithilfe einer DPI-Engine (Deep Packet Inspection):

- Alle Funktionen der standardmäßigen Zscaler Cloud Firewall
- Alle Vorteile einer Next-Generation Firewall (NGFW) – sowie Cloud-Intelligenz und -Verwaltung von Zscaler – ohne dass teure Appliances gekauft oder gewartet werden müssen
- DNS-Sicherheit und -Kontrolle – Optimiert die DNS-Auflösung und führt granulare Kontrollen zum Erkennen und Verhindern von DNS-Tunneling durch
- Auf NGFW- und Kontext bezogene Richtlinien – Granulare Zugangs- und Sicherheitsrichtlinien für das Zulassen/Blockieren basierend auf Anwendung, Benutzer, Identität, Gruppe und Standort
- Vollständig qualifizierte Domain-Name-Richtlinien – Zugangsrichtlinien für Anwendungen, die unter mehreren IPs gehostet werden
- Umfassendes Dashboard – Einschließlich Echtzeiteinsicht in Traffic-Nutzung, Bedrohungen und Anwendungen nach Benutzern, Gruppen und Standorten
- Komplettes Logging und Reporting Session-für-Session
- Cloud-IPS – Permanent verfügbarer IPS-Schutz vor Bedrohungen und vollständige Transparenz, unabhängig von Verbindungsart oder Standort; Überprüfung des gesamten Internet-Traffic (selbst SSL)
- Automatische Weiterleitung für nicht standardmäßige Ports – Automatische Identifikation und Absicherung von Applikationen, die keine standardmäßigen Ports und Protokolle verwenden

Die Standardversion der Zscaler Cloud Firewall wird wahrscheinlich Ihren Anforderungen entsprechen, wenn Sie auf Protokollen basierte Angriffe mit bekannten Protokollnummern stoppen wollen. Sie können beispielsweise die Verwendung eines alternativen DNS-Servers verhindern, indem Sie Port 53 blockieren.

Was geschieht jedoch, wenn die Anwendung zwar mit der Port-Nummer übereinstimmt, aber nicht die Anwendung ist, für die Sie sie halten? Ähnlich, wie der Proxy eine kritische Rolle bei Anwendungen spielt, die über HTTP und HTTPS ausgeführt werden, ist eine erweiterte Cloud Firewall erforderlich, wenn Sie detailliertere Informationen wünschen. Wenn Sie wissen möchten, was an einem von Ihnen geöffneten Port ausgeführt wird und was Ihre Benutzer beabsichtigen, sollten Sie zur erweiterten Zscaler Cloud Firewall wechseln.

Überdenken der Richtlinien

Als die Branche von Zugangskontrolllisten (Access Control Lists – ACLs) zu Stateful Firewalls zu NGFWs wechselte, war das grundlegende Verfahren dasselbe. Wir wollten die Firewall „durchlöchern", um Traffic durchzulassen, den wir für akzeptabel hielten, und alles andere blockieren. Die Standardregel „alle ablehnen" steht am Ende fast aller vorhandenen Firewall-Regeln.

In Bezug auf den ausgehenden Traffic der Organisation mag dies zwar noch stets ein praktikables Entwurfsmuster sein, hinsichtlich des eingehenden Traffic ist jedoch ein Umdenken erforderlich. Sie sollten eine Änderung ihrer letzten Regel in Betracht ziehen und diese stattdessen in „alle zulassen" umkehren. Dieses Muster zielt darauf ab, das zu stoppen, was sie nicht wollen, und den Rest wie gewohnt fortfahren zu lassen.

Warum sollte man etwas ändern, das jahrzehntelang funktioniert hat und von Sicherheitsexperten empfohlen wurde? Weil das Wesen unserer Arbeit die Art und Weise, wie wir mit dem Internet interagieren, im Laufe der letzten 20 Jahre völlig verändert hat.

Heutzutage haben unterschiedliche Organisationen unterschiedliche Anforderungen in Bezug auf Richtlinien und Vorschriften, die Entscheidungen über das Zulassen oder Blockieren von Traffic beeinflussen. Wie entscheiden Sie, was das Richtige für Sie ist? Ein Blick auf die Funktionsweise Ihrer Organisation und die von Ihnen angebotenen Dienstleistungen ist oftmals hilfreich bei der Wahl.

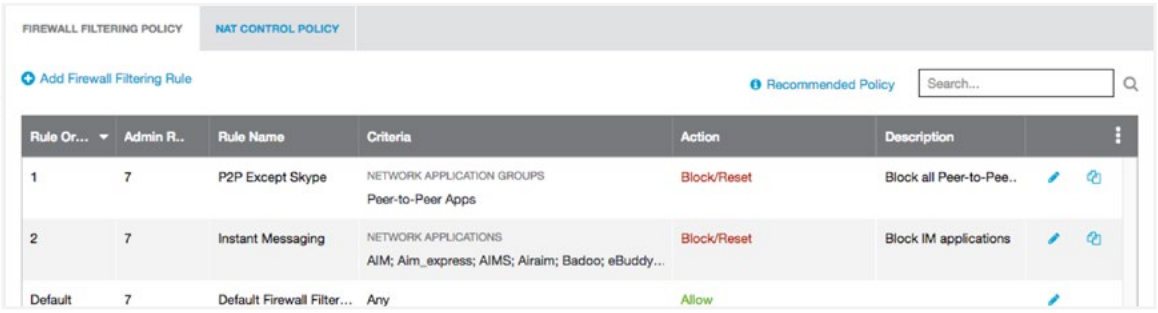

Abbildung 1. Beispiel einer Standardregel „alle zulassen"

Wenn Sie in einem öffentlichen Raum ein Gästenetzwerk bereitstellen, werden Sie wahrscheinlich die Regel „alles zulassen" wählen, nachdem sie nicht akzeptable Inhalte blockiert und potenziell schädliche oder illegale Aktivitäten durch Sperren von Protokollen wie P2P verhindert haben. Da die Benutzer eines Gästenetzwerks auf das Internet und nicht auf Ihr Rechenzentrum zugreifen, ist der restliche Traffic für Ihre Organisation vermutlich akzeptabel.

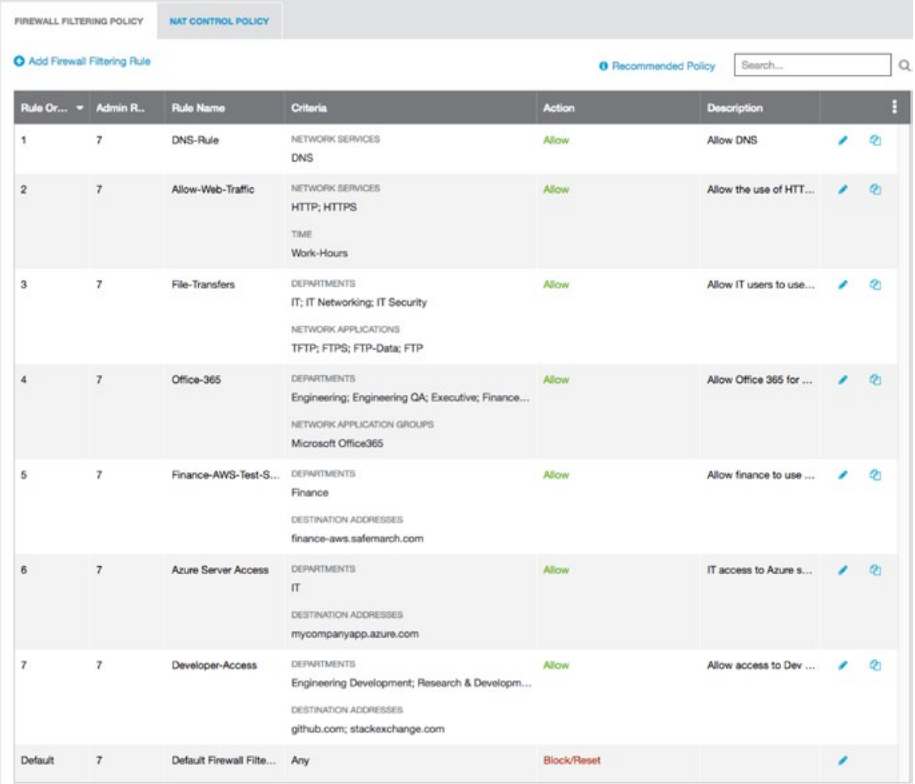

Abbildung 2. Beispiel einer Standardregel „alle ablehnen“

Wenn Ihre Organisation allerdings in einer stark regulierten Branche wie dem Gesundheits- oder Bankwesen tätig ist, wollen Sie möglicherweise nur genehmigte Anwendungen zulassen. In diesem Fall ist es am besten, nur bestimmte Anwendungen freizugeben und alle anderen lokal aufzubewahren. Ausschließlich auf Applikationen zugreifen zu lassen, für deren Ausführung Internetzugang erforderlich ist und auf alle anderen die Regel „alle ablehnen“ anzuwenden, wäre hier der beste Richtlinienrahmen.

Weitere Informationen über die Zscaler Cloud Firewall und deren Konfiguration finden Sie in unserer Dokumentation unter: https://help.zscaler.com/zia/about-firewall-control

Fazit

Der Arbeitsplatz verändert sich rasant. Rechenzentren werden in Zukunft durch Infrastrukturen und Dienste in der Cloud ersetzt werden. Teures Backhauling wird durch lokale Breakouts ersetzt. Und Benutzer befinden sich zunehmend außerhalb des Netzwerks und des Büros. Zur Absicherung dieser Zukunft benötigen Sie eine Sicherheitsplattform mit integrierten Services und Richtlinien, die Benutzern überall hin und zu jeder gewünschten Arbeitsweise folgen. Die Zscaler Cloud Firewall ermöglicht schnelle, sichere lokale Internet-Breakouts für alle Ports und Protokolle, ohne Appliances. Die Cloud-Sicherheitsplattform von Zscaler mit standardmäßiger oder erweiterter Cloud Firewall bringt den gesamten Security Stack näher an die Benutzer heran, um an jedem beliebigen Verbindungsort identischen Schutz zu gewährleisten. Sie skaliert elastisch, um den gesamten Traffic Ihrer Cloud-Anwendungen zu verarbeiten.

Zscaler, Inc.
120 Holger Way
San Jose, CA
+1 408 533 0288
www.zscaler.com