SOPHOS
Security made simple.

Volle Kontrolle über Ihr Netzwerk

Transparenz über Anwendungen mit Synchronized App Control

Die Evolution der Firewall

Die Rolle der Firewall hat sich mit der Zeit stetig gewandelt: Zunächst sollte sie Netzwerke vor externen Hacks und Angriffen schützen. Mittlerweile hat sich ihr Fokus auf das Innere des Netzwerks verlagert. Hier soll die Firewall potenzielle Risiken erkennen und eliminieren und außerdem die Compliance sicherstellen. Ein Grund für diese Entwicklung ist die veränderte Bedrohungslandschaft: Malware und unbefugte Eindringlinge nutzen immer öfter Schwachstellen in Anwendungen, statt an der Netzwerkgrenze anzugreifen. Dazu kommen immer mehr Verpflichtungen, eine angemessene Compliance zu gewährleisten, vor Sicherheitspannen und Datenverlusten zu schützen und die Netzwerk-Performance zu optimieren. Auch sie haben dazu beigetragen, dass sich der Fokus ins Netzwerkinnere verlagert hat.

Aus dem Bedürfnis heraus, für mehr Transparenz und Kontrolle über Benutzer und deren Anwendungen zu sorgen, wurde daher die Next-Generation Firewall entwickelt. Die Next-Gen Firewall steigt quasi über die Ports und Protokolle früherer Stateful Firewalls zu höheren Ebenen im OSI-Modell auf und sorgt somit für mehr Transparenz über Anwendungen und Benutzer.

Next-Gen Firewalls erkennen Anwendungen anhand von Deep Packet Inspection und ordnen die Anwendungen Benutzern oder Hosts im Netzwerk zu, damit Administratoren angemessene Kontrollen bereitstellen können. Beispielsweise ist es sehr hilfreich, Benutzer zu identifizieren, die P2P-File-Sharing-Anwendungen nutzen, und diese zu blockieren. Außerdem sollten ein extensiver Abruf von Streaming-Medien kontrolliert und wichtige Geschäftsanwendungen wie ERP-Systeme, VoIP-Datenverkehr und CRM-Software priorisiert werden.

Wie Next-Gen Firewall App Control funktioniert

Firewalls identifizieren Anwendungen, indem sie Muster im Datenverkehr mit bekannten Signaturen abgleichen. Dieses Verfahren ist mit einer Gesichtserkennung vergleichbar. Wenn Ihnen das Foto einer Ihnen unbekannten Person vorgelegt wird, können Sie das Foto mit einer Reihe von Fotos vergleichen, die mit Namen versehen sind. Liegt eine Übereinstimmung vor, wissen Sie, mit wem Sie es zu tun haben. Liegt keine Übereinstimmung vor, haben Sie keine Chance, die Person zu identifizieren.

„Durchschnittlich 60 % des Netzwerkverkehrs bleiben unidentifiziert."

Application Control funktioniert genau nach demselben Prinzip. Manche Anwendungen verfügen über eine Art „Namensschild" und lassen sich dadurch leicht identifizieren. Bei den meisten Anwendungen ist das jedoch nicht der Fall und einige Anwendungen versuchen sogar gezielt, unerkannt zu bleiben. Wenn eine Übereinstimmung ermittelt und eine Anwendung identifiziert wird, kann die Firewall die Anwendung kontrollieren – durch Traffic Shaping zur Priorisierung oder Begrenzung des Bandbreitenverbrauchs oder durch eine generelle Blockierung. Wenn jedoch keine Übereinstimmung gefunden werden kann, hat die Firewall keinerlei Informationen darüber, mit welcher Anwendung sie es zu tun hat, und kann diese demzufolge auch nicht kontrollieren.

Die Probleme mit Next-Gen Firewall App Control

Wie Sie sich vielleicht vorstellen können, liegt bei vielen Anwendungen keine Übereinstimmung vor. Viele riskante Anwendungen, die in den meisten Unternehmen normalerweise blockiert werden (z. B. BitTorrent Clients), wenden Tricks an, mit denen sie ihre Datenverkehrsmuster und Methoden zur Erstellung von Verbindungen aus dem Unternehmen kontinuierlich ändern. So gelingt es ihnen in vielen Fällen, unerkannt zu bleiben. Das ist in etwas so, als würde eine Person ihre Haarfarbe ändern und sich einen falschen Schnurrbart ankleben, um die Gesichtserkennung zu überlisten.

Andere Anwendungen setzen auf Verschlüsselung, um unerkannt zu bleiben. Dies ist vergleichbar mit einer Person, die eine Sturmhaube trägt. Wieder andere Anwendungen geben sich als Browser aus, damit sie die Firewall unerkannt passieren können. In unserem Vergleichsbeispiel würde sich der Kriminelle hier so verkleiden, dass er wie eine bekannte Persönlichkeit aussieht. Und dann gibt es noch Anwendungen, die erst kürzlich geändert wurden, einmalig in Erscheinung treten, benutzerdefiniert sind oder hoch verschleiert agieren. Für sie lassen sich keine Übereinstimmungen ermitteln. Um zu unserem Beispiel der Gesichtserkennung zurückzukehren: Solche Anwendungen sind mit Personen vergleichbar, für die kein aktuelles Foto vorliegt.

Mit der Zeit haben sich die Funktionen von Firewalls zur Identifizierung und Kontrolle unerwünschter Anwendungen immer weiter verbessert. Doch den Anwendungen gelingt es umgekehrt auch immer besser, die Erkennungsmechanismen von Firewalls zu überlisten. Die Folge: Der meiste Datenverkehr, der heutzutage moderne Firewalls passiert, ist unbekannt, unidentifiziert oder einfach zu generisch, um klassifiziert oder kontrolliert zu werden.

Sieht Ihr App Control Report so aus?

Häufigste Anwendungen

Name der Anwendung	Anteil der Anwendungen
UDP, allgemein	25,45 %
HTTPS MGMT, allgemein	24,26 %
DNS, allgemein	17,8 %
TCP, allgemein	14,39 %
Service RPC Services (IANA)	8,86 %
BitTorrent-Protokoll – UDP-Aktivität 1 (Reqs SIB 5)-63	1,60 %

Konventionelles Firewall-Dashboard mit Anwendungen, die nicht identifiziert werden konnten

Wie groß ist das Problem?

Um zu erfahren, wie weit verbreitet das Problem mit nicht identifizierbaren Anwendungen tatsächlich ist, hat Sophos vor Kurzem mittlere Unternehmen befragt. Wir wollten wissen, wie groß der Anteil ihres Anwendungsverkehrs ist, der nicht identifiziert und nicht kontrolliert wird.

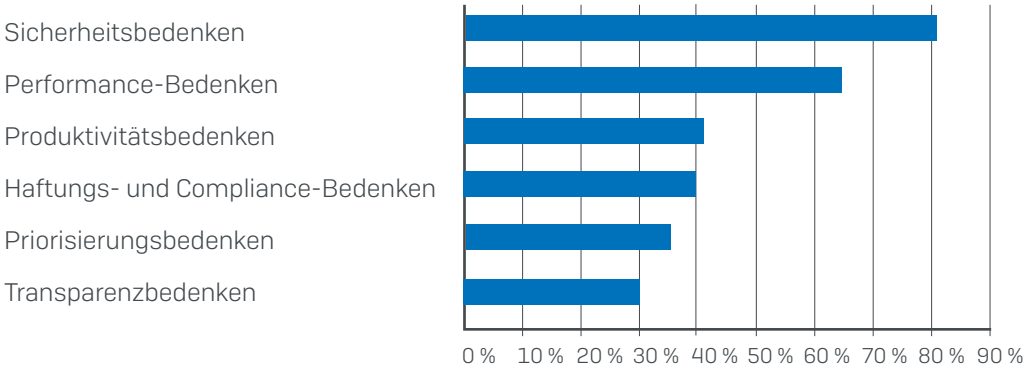
- Fast 70 % der befragten Unternehmen haben eine Next-Gen Firewall oder eine UTM mit Application Awareness.
- Durchschnittlich 60 % des Datenverkehrs bleiben unidentifiziert. Darüber hinaus geben viele Unternehmen an, dass bis zu 90 % ihres Anwendungsverkehrs nicht identifiziert werden.

Wenn Sie befürchten, dass sich dies negativ auf die Sicherheit, Haftbarkeit oder Leistungsfähigkeit Ihres Unternehmens auswirken könnte, befinden Sie sich in guter Gesellschaft:

- 82 % der Umfrageteilnehmer fürchten zu Recht Sicherheitsrisiken infolge der mangelnden Transparenz über Anwendungen
- 65 % fürchten negative Folgen für ihre Netzwerk-Performance
- 40 % fürchten Haftungs- und Compliance-Risiken

Häufigste Bedenken in Hinblick auf den aktuellen Mangel an Anwendungstransparenz:

Welche Bedenken haben Sie in Bezug auf unidentifizierten Netzwerkverkehr? (Multiple Choice)



Die wichtigsten evasiven und unidentifizierten Anwendungen

Die folgenden Anwendungen stellen aufgrund von Schwachstellen ein hohes Sicherheitsrisiko dar, bergen Compliance-Risiken infolge unangemessener und illegaler Inhalte und können sich negativ auf die Produktivität und den Bandbreitenverbrauch auswirken:

- IM- und Konferenzanwendungen (z. B. Skype, TeamViewer)
- BitTorrent- und andere P2P-Clients (z. B. uTorrent, Vuze, Freenet)
- Proxy- und Tunnel-Clients (z. B. Ultrasurf, Hotspot Shield, Psiphon)
- Games (z. B. Valve und Steam)

Leider ist es nahezu unmöglich festzustellen, ob solche Anwendungen in Ihrem Netzwerk ausgeführt werden – weil Firewall-Signaturen in den meisten Fällen einfach nicht in der Lage sind, eine Übereinstimmung zu finden.

Neben den genannten Anwendungen gibt es noch zahllose weitere Anwendungen, die zwar unbedenklich, jedoch potenziell unerwünscht sind, und generische HTTP- und HTTPS-Verbindungen nutzen, um über die Firewall nach außen zu kommunizieren. Solche Anwendungen vertrauen auf die Tatsache, dass fast alle Unternehmen ihre Firewall für den Internetzugriff auf Port 80 und 443 öffnen. In Ihren Reports tauchen diese einfach als HTTP, HTTPS, SSL, Web Browsing oder andere allgemeine und wenig aussagekräftige Kategorien auf.

Und vielleicht am wichtigsten: Es gibt vertikale Anwendungen, ERP-Lösungen, CRM-Software sowie weitere wichtige und ggf. unternehmensspezifische Geschäftsanwendungen, die unerkannt bleiben. Hierdurch besteht die Gefahr, dass diese Anwendungen nur deshalb nicht die notwendige Priorität erhalten, weil für sie keine Signatur vorliegt.

Doch für dieses Problem gibt es eine ziemlich elegante Lösung.

Die Lösung

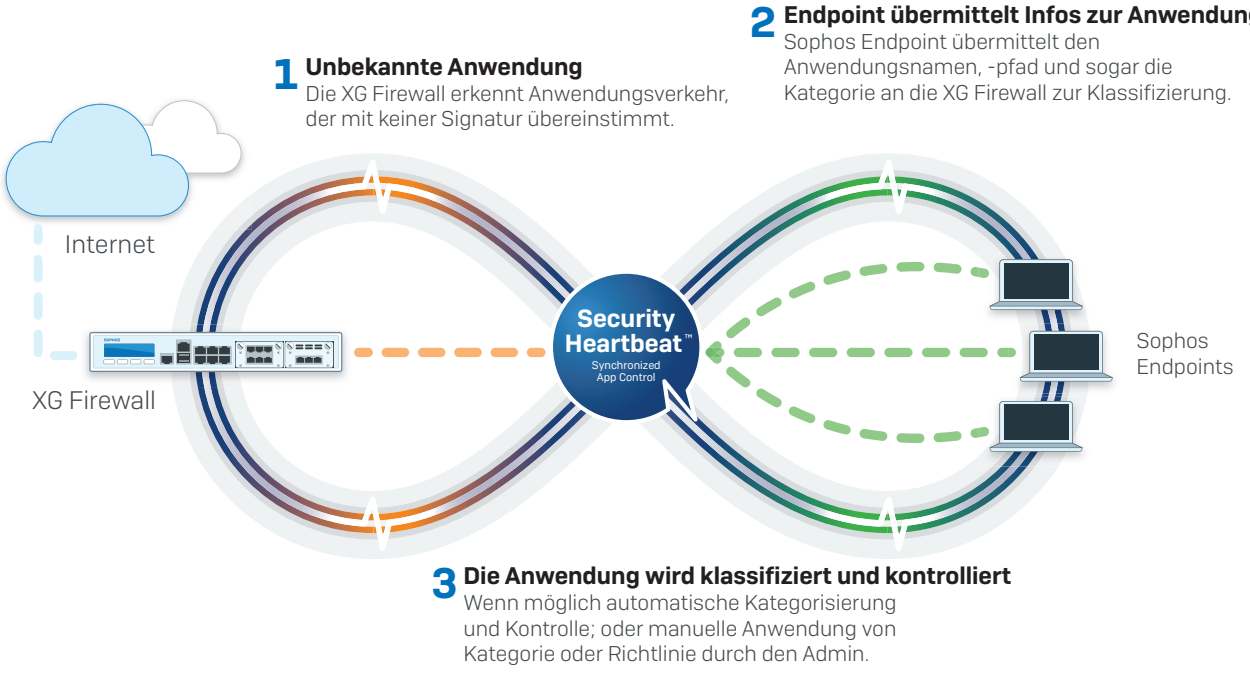
Während Next-Gen Firewalls sich zur Identifizierung von Anwendungen im Netzwerk auf Deep Packet Inspection, Musterabgleiche und Signaturen verlassen müssen, weiß der Endpoint mit absoluter Sicherheit, welche ausführbaren Dateien den Netzwerkverkehr generieren. Daher liegt die Lösung nahe, den Endpoint mit der Firewall zu verbinden, damit die Firewall diese wertvollen Informationen vom Endpoint erhält. Mit unserer revolutionären Synchronized Security bieten wir eine Technologie, die genau dies ermöglicht – einfach und gleichzeitig hocheffektiv..

Sophos Synchronized Security definiert IT Security komplett neu: Die Technologie ermöglicht es Sicherheitsprodukten, Informationen auszutauschen und zusammenzuarbeiten. Dadurch bietet sie einzigartigen Schutz, eine automatische Reaktion auf Vorfälle sowie Echtzeit-Transparenz und -Kontrolle.

Der Security Heartbeat™, eine der ersten Synchronized-Security-Innovationen, verbindet Sophos-Central-verwaltete Endpoints mit der Sophos XG Firewall. So können Informationen zum Integritätsstatus der Endpoints ausgetauscht werden, was eine sofortige Identifizierung gefährdeter Systeme ermöglicht. Wird am Endpoint oder an der Firewall eine Kompromittierung erkannt, erscheinen in Echtzeit Symbole in Ampelfarben sowie Warnhinweise, die den betroffenen Computer, Benutzer und Prozess sofort identifizieren. Ein weiterer großer Vorteil unseres Security Heartbeat™: Die Firewall kann den Endpoint-Integritätsstatus in Firewall-Regeln integrieren. So wird eine automatische Reaktion ermöglicht und der Zugriff auf das kompromittierte System kann bis zur Bereinigung beschränkt oder das System komplett isoliert werden. Hierdurch hat sich die Reaktionszeit von Stunden auf Sekunden verkürzt und die Gefahr, dass Infektionen sich auf andere Bereiche des Netzwerks ausbreiten, wird drastisch reduziert.

Eine weitere Synchronized-Security-Innovation ist Synchronized App Control. Synchronized App Control nutzt das einzigartige Synchronized-Security-System von Sophos und löst damit das Problem, unbekannten, evasiven oder benutzerdefinierten Anwendungsverkehr im Netzwerk zu erkennen. Da Informationen mit dem Endpoint ausgetauscht werden können, ist Synchronized App Control in der Lage, den Ursprung von unidentifiziertem Anwendungsverkehr im Netzwerk zu ermitteln. Dadurch wird ein großer Unsicherheitsfaktor in Netzwerken beseitigt.

Synchronized App Control in Aktion



Synchronized App Control ist der erste große Durchbruch im Bereich Transparenz und Kontrolle über Netzwerkanwendungen seit Entwicklung der Next-Gen Firewall.

Verbindet sich ein Sophos-Central-verwalteter Endpoint mit einem Netzwerk, in dem auch eine XG Firewall zum Einsatz kommt, baut er eine Security-Heartbeat™-Verbindung zur Firewall auf und tauscht darüber Infos zum Integritäts- und Sicherheitsstatus sowie Telemetrie-Daten aus. Zusätzlich nutzt der Endpoint diese Verbindung auch, um die Identität aller Netzwerkanwendungen an die Firewall zu übermitteln.

Wenn die Firewall die Identität der Anwendung nicht mithilfe herkömmlicher Signaturtechniken bestätigen kann, weil die Anwendung evasiv, benutzerdefiniert oder neu ist oder eine generische Verbindung nutzt, verwendet sie die vom Endpoint bereitgestellten Informationen, um die Anwendung zu identifizieren, klassifizieren und kontrollieren. Wenn möglich werden die vom Endpoint übermittelten Anwendungen automatisch einer geeigneten Kategorie zugeordnet („Klassifizierung"). Hierdurch werden auf die neu identifizierte und klassifizierte Anwendung automatisch alle App-Control-Richtlinien angewendet, die bereits auf der Firewall durchgesetzt werden.

Beispielsweise wird ein evasiver BitTorrent Client automatisch der Peer-to-Peer-Anwendungskategorie zugewiesen. Falls auf der Firewall zudem eine Application-Control-Richtlinie zur Blockierung von P2P-Anwendungen aktiv ist, wird der neue BitTorrent-Datenverkehr automatisch blockiert – ohne jegliches Eingreifen des Netzwerkadministrators.

Die Vorteile:

Identifizierung unbekannter Anwendungen

Synchronized App Control identifiziert alle Anwendungen, die im Netzwerk bislang nicht erkannt wurden, einschließlich aller neuen Anwendungen sowie Tunneling-, Proxy- und VPN-Anwendungen, die Firewall-Kontrollen häufig mittels Verschlüsselung umgehen. All diese Anwendungen stellen eine enorme Schwachstelle dar und bergen eine ganze Reihe von Compliance-, Performance- und Sicherheitsrisiken. Falls bereits Richtlinien zur Blockierung oder zum Traffic Shaping solcher Anwendungstypen vorhanden sind, werden auf neu identifizierte Anwendungen, die in diese Kategorie fallen, automatisch dieselben Richtlinien angewendet. Gleichzeitig werden die betroffenen Benutzer und Hosts einfach identifiziert, sodass im Bedarfsfall eingegriffen und ggf. Schulungsmaßnahmen durchgeführt werden können.

Priorisierung benutzerdefinierter Anwendungen

Synchronized App Control erkennt benutzerdefinierte Geschäftsanwendungen (z. B. Finanz- CRM-, ERP-, Fertigungsanwendungen und andere Netzwerkanwendungen), die für Ihre aktuelle Firewall komplett unsichtbar sind, für Ihr Unternehmen jedoch hohe Priorität haben. Erstmals bietet sich mit Synchronized App Control die Möglichkeit, Traffic-Shaping- und QoS-Richtlinien anzuwenden, mit denen sichergestellt werden kann, dass unternehmenskritische Anwendungen angemessen priorisiert werden und mit optimaler Performance ausgeführt werden können.

Kontrolle evasiver Anwendungen

Synchronized App Control erkennt automatisch alle evasiven Anwendungen, die ihre Verbindungsmethoden und Kommunikationswege stetig ändern, um einer Erkennung und Kontrolle zu entgehen. Synchronized App Control schiebt diesen Verschleierungstaktiken ein für alle Mal einen Riegel vor. Unabhängig davon, wie evasiv Anwendungen auftreten: Sie haben keine Chance, die Synchronized App Control zu überlisten und unerkannt zu bleiben.

„Synchronized App Control ist der erste bedeutende Durchbruch auf dem Gebiet der Transparenz und Kontrolle von Netzwerk-anwendungen seit der Entwicklung der Next-Gen Firewall."

Welche Sophos-Produkte erforderlich sind:

Sophos hat ein komplettes System von IT-Security-Produkten im Angebot, die sich zur Bereitstellung von Synchronized Security einfach integrieren lassen. Die Aktivierung von Security Heartbeat™ und Synchronized App Control ist einfach und komfortabel – inklusive aller zusätzlichen Sicherheitsfeatures, die diese Lösungen in Bezug auf Sicherheit, Transparenz und Kontrolle bieten. Es sind mindestens die Sophos XG Firewall und Intercept X erforderlich. Beide Produkte lassen sich jedoch parallel und ergänzend zur bestehenden IT-Security-Infrastruktur bereitstellen. Die Implementierung von Synchronized Security ist also ohne Störung oder Erneuerung der bestehenden Infrastruktur möglich.

Die Sophos XG Firewall kann entweder inline mit Ihrer bestehenden Firewall oder als Ihr Haupt-Firewall-Gateway bereitgestellt werden. Darüber hinaus ist auch ein Betrieb im reinen Reporting- und Visibility-Modus möglich, wenn die XG Firewall im Discover-Modus (auch bekannt als TAP-Modus) an einen Switch Mirror Port angeschlossen wird.

Am Endpoint kann Intercept X parallel zu Ihrer bestehenden Desktop-AV-Lösung bereitgestellt werden. Alternativ können Sie mit Sophos Central Endpoint Advanced Ihren gesamten Endpoint-Schutz von Sophos beziehen. Beide Produkte unterstützen Synchronized Security beim gemeinsamen Einsatz mit der XG Firewall auf Windows- und Mac-Plattformen.

Zusammenfassung

Next-Gen-Firewalls sind oft nicht in der Lage, mittels Application Awareness für Transparenz über Anwendungen zu sorgen, da die Effektivität signaturbasierter Erkennungstechniken für Anwendungen naturgemäß beschränkt ist. Ein Großteil des Anwendungsverkehrs in heutigen Netzwerken wird daher weder identifiziert noch überprüft. Die Folgen für die Sicherheit, Produktivität, Performance und Compliance können verheerend sein.

Doch es gibt eine elegante und effektive Lösung: Synchronized App Control nutzt die einmalige Sophos-Security-Heartbeat™-Verbindung zwischen Sophos-Central-verwalteten Endpoints und der XG Firewall und ermöglicht so den Austausch eindeutiger Informationen über Netzwerkanwendungen.

Mit Synchronized App Control ist die XG Firewall in der Lage, den gesamten unbekannten Anwendungsverkehr im Netzwerk automatisch zu identifizieren, zu klassifizieren und zu kontrollieren. Synchronized App Control ist ein bedeutender Durchbruch auf dem Gebiet der Netzwerktransparenz und -kontrolle und hebt sich damit entscheidend von anderen Next-Gen Firewalls ab.

Jetzt kostenlos online testen unter www.sophos.de/demo

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

22-09-17 WPDE (NP)

SOPHOS