



Application Firewall: Die neue Freiheit für Ihr Netzwerk

*Best Practices für die Anwendungskontrolle,
Datensicherheit und Bandbreitenverwaltung
im Zeitalter von Web 2.0.*

INHALT

Einführung	2
Herausforderungen für eine sichere und produktive Arbeitsumgebung	2
Konventionelle Firewalls bieten im Web 2.0 keinen ausreichenden Schutz	3
Best Practices für die Netzwerkkontrolle und Benutzerproduktivität	4
SonicWALL Network Security Appliance	8
Fazit	9

Mitarbeiter können heute auf mehr Informationen, webbasierte Tools und Rich Media-Inhalte zugreifen als je zuvor. In Unternehmensnetzwerken werden immer häufiger Web 2.0-Anwendungen eingesetzt, die neue und effizientere Möglichkeiten versprechen, um Menschen miteinander zu verbinden und Informationen auszutauschen. Doch die verfügbare Bandbreite stößt an ihre Grenzen, wenn Mitarbeiter Streaming-Video- und Musikdateien auf ihren Desktop-Rechnern abspielen. Außerdem können Unternehmen, die auf das neue Modell setzen und von den Vorteilen webbasierter Anwendungen profitieren möchten, Sicherheitsregeln möglicherweise nicht netzwerkübergreifend steuern und durchsetzen. Gleichzeitig finden dynamische und potentiell gefährliche Bedrohungen immer neue Wege in die Unternehmensnetzwerke.

Für viele vorausschauende Unternehmen heißt die Lösung Application Firewall. Die nächste Firewallgeneration bietet weit mehr als den Schutz, den man von konventionellen Firewalls erwarten kann. Mit einer Application Firewall können Unternehmen ihren Mitarbeitern den Zugriff auf nützliche Anwendungen erlauben und der IT-Abteilung helfen, das Unternehmensnetzwerk zu schützen und sicherzustellen, dass ausreichend Bandbreite für geschäftskritische Geschäftsprozesse verfügbar ist.

In diesem Whitepaper beschäftigen wir uns mit den neuen Risiken durch die zunehmende Verbreitung von Webanwendungen und erläutern Best Practices für die Kontrolle von Anwendungen, Daten und Bandbreite. Außerdem stellen wir die Lösungen der SonicWALL® E-Class Network Security Appliance (NSA)- und NSA-Serie vor. Sie wurden entwickelt, um Unternehmen jeder Größenordnung bei der Bewältigung spezieller Herausforderungen im Zusammenhang mit Web 2.0-Anwendungen zu unterstützen. Dazu zählen z. B. unerlaubte Webanwendungen, Streaming-Medien oder Peer-to-Peer-Programme (P2P) und der Schutz von Daten, die in Anhängen und per E-Mail versendet werden.

Einführung

Bessere Zusammenarbeit, höhere Produktivität, niedrigere Kosten: Das sind nur einige der Vorteile, die mit der zunehmenden Verbreitung von Webanwendungen in modernen Unternehmensnetzwerken einhergehen. Doch leider bringen diese Anwendungen auch ganz neue Herausforderungen mit sich. Social Networking- und Streaming Media-Anwendungen z. B. können die Bandbreite und Produktivität beeinträchtigen, wenn sie mit geschäftskritischen Anwendungen konkurrieren. Andere Lösungen, etwa in Verbindung mit Software as a Service (SaaS) und serviceorientierter Architektur (SOA), bieten neue Möglichkeiten zur Geschäftsabwicklung, öffnen dadurch aber auch neuen Bedrohungen die Türen.

Um diese Anwendungen so effizient wie möglich zu nutzen, benötigen Unternehmen einen umfassenden Sicherheitsansatz. In einer modernen Web 2.0-Umgebung können konventionelle Firewalls kritische Informationen und Ressourcen nicht ausreichend schützen. Viele Unternehmen sind sich nicht bewusst, dass ihr gegenwärtiger Netzwerkschutz nicht ausreicht. Und Organisationen, denen die Herausforderungen bekannt sind, scheuen sich, ihren Mitarbeitern den Zugriff auf Webanwendungen zu erlauben. Doch wenn webbasierte Anwendungen sicher und im Rahmen der vorgegebenen Unternehmensrichtlinien eingesetzt werden, bieten sie ungeheure Vorteile.

Herausforderungen für eine sichere und produktive Arbeitsumgebung

Mitarbeiter werden technisch immer versierter, und es kommt häufig vor, dass Webanwendungen heruntergeladen und auf dem Arbeitsplatzrechner installiert werden. Das kann die Produktivität erhöhen, verbraucht aber auch ungeheuer viel Bandbreite und ist ein potentielles Einfallstor für eine ganz neue Art von Sicherheitsbedrohungen. Das Problem wird dadurch verschärft, dass Mitarbeiter Dateien von Social Networking-Seiten wie MySpace herunterladen, Streaming-intensive Medien auf YouTube abspielen, Dateien von privaten E-Mail-Konten wie Yahoo® oder Gmail® abrufen und P2P-Anwendungen nutzen. Oft ist den Mitarbeitern gar nicht bewusst, welchen Schaden sie anrichten können, wenn sie Webanwendungen oder Streaming-Inhalte herunterladen.

Diese Aktivitäten stellen aus mehreren Gründen ein Sicherheitsrisiko dar. Es besteht z. B. die Gefahr, dass Hacker manipulierte Daten in Paketen übermitteln und über Webanwendungen Informationen von den Benutzern „abgreifen“. Cyberdiebe könnten Zugriffskontrollen in eine Anwendung einbauen, um auf bestimmte Inhalte oder Funktionen zuzugreifen, die nur autorisierten Benutzern vorbehalten sind. Außerdem könnten einige Angriffe so hohe Datenverkehrsaufkommen generieren, dass sie bestimmte Anwendungen lahmlegen und berechtigte Benutzer nicht mehr zugreifen können.



Neben den technischen Herausforderungen wie dem Netzwerkschutz müssen auch einige wirtschaftliche Gesichtspunkte berücksichtigt werden. So verschlingen Streaming-Musik- und Video-Seiten eine Menge Bandbreite und können geschäftskritische Anwendungen im Netzwerk verlangsamen. Außerdem kann die Produktivität leiden, wenn sich Mitarbeiter von nicht tätigkeitsrelevanten Web 2.0-Anwendungen wie Streaming-Video, P2P-Downloads und Online-Spielen ablenken lassen.

Angesichts dieser neuen dynamischen Arbeitsumgebung stehen Unternehmen vor einer schwierigen Aufgabe: Sie müssen verhindern, dass sensible Daten nach außen gelangen und gleichzeitig einen sicheren und unterbrechungsfreien Zugriff auf wichtige Unternehmensressourcen gewährleisten. Schließlich kann es passieren, dass Mitarbeiter beim Kommen und Gehen unabsichtlich Malware oder infizierte Daten einschleusen. In extremen Fällen kann es auch so weit gehen, dass verärgerte Mitarbeiter Netzwerkangriffe aus dem Unternehmensinneren starten. Außerdem muss das Firmennetzwerk inzwischen noch mehr Daten von einer wachsenden Zahl von Remote-Mitarbeitern und externen Beratern aufnehmen, was die Sache noch komplizierter macht.

Um die vielen neuen technischen und wirtschaftlichen Herausforderungen zu meistern, müssen Organisationen heute den aktuellen Sicherheitszustand ihres Netzwerkes genauer analysieren und eine Lösung finden, wie sie produktivitätsfördernde Web 2.0-Tools erlauben können, ohne die Geschäftsprozesse zu verlangsamen oder ihr Netzwerk gefährlichen Bedrohungen auszusetzen.

Konventionelle Firewalls bieten im Web 2.0 keinen ausreichenden Schutz

Viele Unternehmen gehen von der falschen Annahme aus, dass ihre Netzwerk-Firewalls die Unternehmensdaten und Netzwerk-Ressourcen im heutigen Geschäftsumfeld ausreichend schützen. Die unbequeme Wahrheit ist aber, dass konventionelle Firewalls Schwierigkeiten haben, Schutz vor Webanwendungsangriffen zu bieten. Manchmal sind sie nicht einmal in der Lage, diese Angriffe als Bedrohungen einzustufen.

Obwohl einige Netzwerksicherheitsanbieter das Ausmaß der neuen Bedrohungen langsam verstehen, ergreifen sie keine adäquaten Sicherheitsmaßnahmen. Da herkömmliche Firewalls z. B. keinen ausreichenden Schutz vor den neuen Bedrohungen durch Social Networking- und andere potentiell gefährliche Web 2.0-Anwendungen bieten, haben viele Anbieter angefangen, Funktionen wie Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS) in ihre Produkte zu integrieren und werben mit Application-Layer Sicherheit. Doch aus zwei wesentlichen Gründen haben sich diese Lösungen im Kampf gegen Webanwendungsangriffe nicht als wirksam erwiesen: Sie greifen auf statische Angriffssignaturen zurück und arbeiten auf den Netzwerkebenen.

Statische Angriffssignaturen können nichts gegen viele Webanwendungsbedrohungen ausrichten, da die Sicherheitssignaturen so programmiert sind, dass sie Angriffe anhand der Verhaltensmuster bekannter Bedrohungen abwehren. Doch leider werden statische Signaturen erst nach Identifizierung der Bedrohung geschrieben und funktionieren reaktiv. Außerdem müssen Sicherheitsprodukte kontinuierlich mit neuen Signaturen aktualisiert werden, damit sie die neuesten Bedrohungen abwehren können. Folglich sind Netzwerke nicht vor Angriffsarten geschützt, die noch nicht identifiziert wurden und als normaler

Datenverkehr getarnt sind. Noch gravierender ist aber, dass Systeme schutzlos ausgeliefert sind, wenn Angriffe, für die es keine allgemeinen Muster gibt, auf bestimmte Anwendungsschwachstellen abzielen.

Diese Defizite wiegen noch schwerer, weil Lösungen, die auf den Netzwerkebenen arbeiten, grundsätzlich auf die Informationen beschränkt sind, die sie interpretieren können. Da konventionelle Firewalls und IPS-Systeme Daten paketweise scannen und Anfragen bzw. Benutzersitzungsdaten nicht in einem Stück prüfen, verfügen sie nicht über die erforderlichen anwendungsspezifischen Informationen, um legitime Anfragen von gefährlichen zu unterscheiden. Trotz dieser Probleme gibt es Möglichkeiten, um potentielle Risiken zu erkennen, Netzwerkangriffe zu verhindern und gleichzeitig die Mitarbeiterproduktivität zu steigern.

Best Practices für die Netzwerkkontrolle und Benutzerproduktivität

Da sich das Arbeitsumfeld in Unternehmen rasant weiterentwickelt, sind Organisationen gut beraten, wenn sie die nötigen Netzwerksicherheitsmaßnahmen ergreifen, damit ihre Mitarbeiter von den Vorteilen webbasierter Anwendungen profitieren können. Um diese Herausforderungen zu meistern und die Mitarbeiterproduktivität zu steigern, setzen Unternehmen Application Firewalls ein und ermöglichen damit die Zugriffskontrolle für Anwendungen, die Regulierung von Web-Datenverkehr, E-Mails, E-Mail-Anhängen und Dateitransfers sowie die Verwaltung der Bandbreite. Im Folgenden stellen wir einige Best Practices vor, mit denen Sie Bedrohungen reduzieren, den Bandbreitenverbrauch kontrollieren und die Mitarbeitereffizienz steigern können.

1) Anwendungsverwaltung mit individuellen Zugriffskontrollen

Mit einer Application Firewall können Administratoren individuelle Zugriffskontrollen nach Benutzer, Anwendung, Zeitplan oder IP-Subnetz-Ebene definieren. Sie haben damit die Möglichkeit, alle verfügbaren Anwendungen umfassend zu verwalten. Insbesondere können sie durchsetzen, dass nur zugelassene Anwendungen eingesetzt werden und behalten gleichzeitig die Kontrolle über P2P-Anwendungen.



Abbildung 1: Ermöglicht die Klassifizierung, Kontrolle und Verwaltung von Anwendungen und Daten, welche die Firewall passieren.

Die Nutzung vorgegebener Anwendungen durchsetzen

Als Erstes möchten Unternehmen meistens den Einsatz bevorzugter Anwendungen vorgeben und durchsetzen. Wenn sich eine Firma beispielsweise entschieden hat, standardmäßig einen bestimmten Internet-Browser zu verwenden, bieten sich die folgenden Strategien an:

1. Tägliche physische Prüfung aller Systeme auf unerlaubte Browser
2. Programmierung und tägliche Ausführung eines Skripts, das alle Systeme auf unerlaubte Browser prüft

3. Definition einer Application Firewall-Regel, die den Datenverkehr auf bevorzugten Browsern freigibt und automatisch auf unerwünschten Browsern blockiert

Die beiden ersten Optionen sind nicht unbedingt ideal und belasten die IT-Abteilung mit zeitaufwändigen manuellen Arbeiten. Außerdem gewährleisten die beiden ersten Ansätze nicht den erforderlichen Sicherheitsstandard. Selbst wenn ein Administrator nur ein einziges System überwacht, kann sich Malware so schnell wie ein Flächenbrand ausbreiten. Die dritte Option bietet Unternehmen ein zuverlässiges Tool, um Sicherheitslücken zu schließen und IT-Mitarbeiter zu entlasten, damit sie sich auf strategische Aufgaben konzentrieren können.

Die Kontrolle über Peer-to-Peer-Anwendungen behalten

Darüber hinaus ist es vielen Unternehmen wichtig, dass sie P2P-Anwendungen wie BitTorrent kontrollieren können. Diese Anwendungen können jede Menge Bandbreite verschlingen und alle möglichen Arten schädlicher Dateien in das Unternehmensnetzwerk einschleppen. Für Netzwerkadministratoren, die P2P-Anwendungen in ihren Netzwerken verwalten möchten, besteht die Herausforderung darin, dass ständig neue P2P-Anwendungen auftauchen oder minimale Änderungen an vorhandenen P2P-Anwendungen (z. B. eine neue Versionsnummer) vorgenommen werden. Das macht es fast unmöglich, den Überblick zu behalten.

Durch die Implementierung von Application Firewall-Regeln können Unternehmen solche Anwendungen blockieren oder anhand von Bandbreiten- und Zeitbeschränkungen eingrenzen. Und da ausgereifte Application Firewalls automatisch IPS-Signatur-Updates bereitstellen, müssen Systemadministratoren keine Zeit dafür aufwenden, IPS-Signaturregeln zu aktualisieren, und können sich auf wichtigere, geschäftskritische Aufgaben konzentrieren.

2) Proaktive Regeln verhindern, dass Daten nach außen dringen und Bedrohungen ins Netzwerk gelangen

Sind die Anwendungen unter Kontrolle, müssen Unternehmen dafür sorgen, dass keine sensiblen Informationen (absichtlich oder versehentlich) nach außen dringen oder von Mitarbeitern, Lieferanten oder Partnern gestohlen werden. Application Firewalls verfügen über die nötigen Kontrollfunktionen, mit denen Unternehmen den Verlust von Web-Mails und Daten minimieren, den FTP-Upload einschränken, vertrauliche Dokumente schützen und verbotene Dateien blockieren können.

Den Verlust von Web-Mails und Daten minimieren

Um Daten zu kontrollieren, fängt man am besten mit E-Mail an – dem mit Abstand beliebtesten Arbeitstool. Fakt ist, dass Anti-Spam-Lösungen nicht verhindern können, dass Daten nach außen dringen, wenn Mitarbeiter oder Partner Informationen über Web-Mail-Services wie Yahoo oder Gmail versenden. Mit Application Firewall-Regeln dagegen können Unternehmen ausgehende E-Mails mit sensiblen oder vertraulichen Daten aufspüren und blockieren.

Vertrauliche Dokumente schützen

Unternehmen müssen dafür sorgen, dass sowohl der Inhalt von Web-Mail-Nachrichten als auch die Anhänge von E-Mails geschützt werden. Die meisten Unternehmen können verhindern, dass Viren und Spam-Mails über gängige E-Mail-Programme wie Microsoft Outlook® ins Netzwerk gelangen. Doch wenn es um den Schutz von E-Mail-Anhängen geht, sind sie meistens ratlos. Es gibt Unternehmen, in denen ausgehende E-Mails kein E-Mail-Sicherheitssystem durchlaufen, oder bei denen der Inhalt von E-Mail-Anhängen nicht geprüft wird. In beiden Fällen können Dateianhänge mit vertraulichen Informationen ohne Probleme nach außen gelangen.

Mit einer Application Firewall können Organisationen diese Sicherheitslücke proaktiv beim Versand über gängige E-Mail-Programme schließen. Der IT-Administrator des Unternehmens braucht nur eine Application Firewall-Regel zu erstellen, um E-Mail Anhänge zu blockieren, die mit einem Wasserzeichen als Indikator für sensible Informationen versehen sind. Die Firewall verhindert dann, dass diese Dateien das Unternehmensnetzwerk verlassen. Selbst beim Datenaustausch über einen FTP-Server können diese Regeln eingesetzt werden.

Den FTP-Upload einschränken

Es gibt viele Einsatzmöglichkeiten für FTP-Services, doch meistens werden sie für den Austausch großer Dateien in Anspruch genommen. Dabei besteht das Risiko, dass FTP-Sites als Einfallstor für unerwünschte Inhalte dienen. Um dem entgegenzuwirken, können Unternehmen die FTP-Upload-Berechtigungen auf vertrauenswürdige Quellen beschränken, wie z. B. dem Projektmanager einer Partnerfirma. Mit bestimmten Application Firewalls lassen sich Regeln erstellen, die FTP-Uploads nur für autorisierte Benutzer zulässt. Gleichzeitig können Unternehmen mit diesen Firewalls FTP-Befehle zurückweisen, die auf bestimmten FTP-Servern für unnötig erachtet werden.

Verbotene Dateien blockieren

Obwohl die bisher vorgestellten Best Practices einen großen Beitrag zum Schutz von Geschäftsdaten leisten, müssen sich Organisationen bewusst sein, dass trotzdem böartige oder unerwünschte Dateien ins Netzwerk gelangen können. So sind viele herkömmliche Firewalls beispielsweise nicht in der Lage, potentiell gefährliche Dateien zu blockieren, wie z. B. EXE-Dateien mit ausführbarem Code. Egal, ob ausführbare Dateien von einer Website heruntergeladen, als E-Mail-Anhang empfangen, oder über FTP übertragen werden: Sie können bewirken, dass ein Rechner verschlüsselte Anweisungen befolgt.

Darüber hinaus gibt es PIF (Personal Information Files)-Dateien, die dem Betriebssystem vorgeben, wie Anwendungen ausgeführt werden sollen, und Visual Basic Scripts (VBS), die Daten auf dem Rechner des Benutzers abrufen und modifizieren können. Doch es besteht kein Grund, vor diesen Bedrohungen zu kapitulieren. Unternehmen können für ihre Application Firewall eine Liste mit verbotenen Dateiendungen erstellen und mithilfe einer entsprechenden Regel diese Dateien blockieren und die damit verbundenen Risiken mindern.

3) Bandbreitenverwaltung zur Gewährleistung der Anwendungs- verfügbarkeit

Um sicherzustellen, dass beim Einsatz von Webanwendungen die Verfügbarkeit und Performance von geschäftskritischen Anwendungen nicht leiden, müssen Unternehmen die Netzwerkbandbreite verwalten. Wenn z. B. einige Mitarbeiter Streaming-Video- und Musik-Dateien auf ihrem Rechner abspielen, kann das nicht nur die Produktivität, sondern auch die Verfügbarkeit von Geschäftsanwendungen für andere Mitarbeiter beeinträchtigen. Aus diesem Grund hat die Bandbreitenverwaltung eine sehr wichtige Rolle übernommen. Ausgereifte Application Firewalls bieten Funktionen, mit denen sich der Bandbreitenverbrauch innerhalb des gesamten Unternehmens kontrollieren lässt. Damit kann der Zugriff auf Streaming-Video und -Musik überwacht und die Verfügbarkeit von geschäftskritischen Anwendungen gewährleistet werden.



Abbildung 2 : Sorgt dafür, dass genügend Netzwerkbandbreite verfügbar ist, damit geschäftskritische Anwendungen effizient laufen und zur Produktivität des Unternehmens beitragen.

Zugriffskontrolle für Streaming-Media

Streaming Video-Seiten, wie z. B. YouTube können zwar manchmal nützlich sein, doch in den meisten Fällen werden sie für private Zwecke genutzt. Man könnte das Problem kurzfristig lösen, indem man diese Seiten sperrt, aber noch effizienter ist es, die verfügbare Bandbreite für Streaming Video-Seiten mithilfe einer Application Firewall einzuschränken.

Auch Streaming Audio- und Streaming Radio-Seiten beanspruchen wertvolle Bandbreite. Doch meistens ist der Zugriff auf diese Seiten arbeitsrelevant. Hier haben Unternehmen die Möglichkeit, anhand von Kontrollfunktionen den Datenverkehr nach Website und Dateiendung zu filtern. Eine Application Firewall-Regel kann die für Streaming Audio-Seiten und -Dateien verfügbare Bandbreite ermitteln, blockieren oder einschränken.

Die Verfügbarkeit von geschäftskritischen Anwendungen und Inhalten sicherstellen

Da der Bandbreitenbedarf für wichtige Geschäftsanwendungen und Inhalte ständig zunimmt, leidet die Produktivität empfindlich, wenn Netzwerkressourcen für private Zwecke beansprucht werden. Mitarbeiter, die das Netzwerk für P2P-Datei-Downloads und Online-Spiele nutzen, können Bandbreitenengpässe verursachen, so dass andere Mitarbeiter, Geschäftspartner oder Lieferanten Probleme beim Zugriff auf wichtige Informationen und Ressourcen bekommen. Manche Organisationen reagieren darauf, indem sie die Bandbreitenbeschränkung im gesamten Unternehmen lockern. Als sinnvollerer Ansatz bietet sich hier eine gruppenbasierte Bandbreitenverwaltung an. Beispielsweise könnte man eine Application Firewall-Regel definieren, die uneingeschränkten Zugriff auf Streaming-Videos für Führungskräfte und Entscheider garantiert und den Zugriff für andere Mitarbeiter während der Geschäftszeiten einschränkt.

Ebenso sind viele geschäftskritischen Anwendungen wie z. B. Salesforce.com®, SharePoint® und SAP®-Anwendungen Cloud-basiert oder werden in geografisch verteilten Netzwerken eingesetzt. Die Priorisierung der Netzwerkbandbreite für diese Anwendungen trägt entscheidend zur Produktivität des Unternehmens bei. Auch hier können Organisationen eine Application Firewall-Regel definieren, um die Bandbreite für kritische Anwendungen zu priorisieren. Mit ausgereiften Application Firewalls können IT-Administratoren sogar die Bandbreitenverfügbarkeit nach einem bestimmten Datum festlegen, wie z. B. das Quartalsende für Vertriebsanwendungen.

SonicWALL Network Security Appliance:

Performance, Schutz und punktgenaue Netzwerkkontrolle

Die vorgestellten Best Practices leisten einen großen Beitrag zur Netzwerksicherheit und Mitarbeiterproduktivität. Darüber hinaus gibt es eine Application Firewall-Lösung, die modernen Unternehmen eine Antwort auf ihre anspruchsvollen Anforderungen liefert und dort ansetzt, wo konventionelle Netzwerk-Firewalls an ihre Grenzen stoßen. Die SonicWALL® Network Security Appliance (NSA)-Serie setzt neue Maßstäbe bei der Netzwerksicherheit und -kontrolle und bietet eine Reihe konfigurierbarer Tools, mit denen sich Anwendungen gezielt überwachen lassen und die Weitergabe vertraulicher Informationen verhindert werden kann. Die Lösung ist mehr als nur ein Sicherheitsansatz und bietet mehrere Sicherheitsfunktionen, wie eine Firewall, Unified Threat Management und eine Application Firewall zum Schutz vor zahlreichen Bedrohungen. Mithilfe einer High-Speed Inspection- und Classification Engine werden Echtzeit-Anwendungen, Dateien und contentbasierter Verkehr geprüft, ohne dass die Netzwerkperformance oder die Skalierbarkeit beeinträchtigt wird. Damit können IT-Abteilungen wiederverwendbare und adaptierbare Regelkontrollen erstellen, ohne dass sie einen Kompromiss zwischen Sicherheit und Produktivität eingehen müssen.

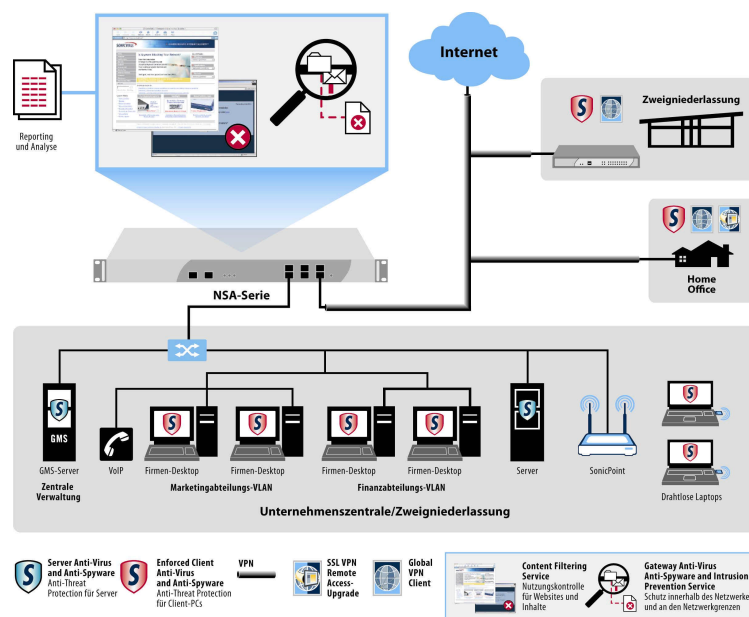


Abbildung 3. Die NSA-Serie von SonicWALL kombiniert leistungsstarke Application Firewall-Kontrollmöglichkeiten mit High-Speed Intrusion Prevention und Funktionen zur Prüfung von Dateien und Dateiinhalten sowie mit zahlreichen erweiterten flexiblen Netzwerk- und Konfigurationsfeatures

Die Application Firewall von SonicWALL verfügt über eine Reihe individuell anpassbarer Sicherheitstools und ermöglicht Administratoren eine detaillierte Kontrolle und Überwachung des Netzwerkverkehrs. Ein Firewall-Assistent erleichtert die Konfiguration und hilft bei den häufigsten Szenarien, die beim Einsatz der Application Firewall denkbar sind. Administratoren können Regeln unkompliziert ändern und an individuelle Situationen anpassen. Außerdem können IT-Administratoren granulare Kontrollen erstellen und durchsetzen, um sicherzustellen, dass genügend Bandbreite für kritische Prozesse zur Verfügung steht.

Diese einzigartige Kombination aus Kontrolle und Flexibilität verbessert die Produktivität im ganzen Unternehmen.

Fazit

Webanwendungen spielen eine immer größere Rolle an unserem Arbeitsplatz. Unternehmen, die vor dieser Entwicklung die Augen verschließen, müssen mit Sicherheits- und Produktivitätsproblemen rechnen, die mit der Zeit immer deutlicher zutage treten. Denn Mitarbeiter, Lieferanten und Partner werden auch weiterhin Webanwendungen nutzen, um möglichst effizient zu arbeiten. Daher sollten Unternehmen eine Lösung finden, um potentielle Gefahren und Bandbreitenengpässe unter Kontrolle zu bekommen, so dass Benutzer die Vorteile von Webanwendungen auch in ihrem Arbeitsalltag bestmöglich einsetzen können.

SonicWALL ist ein führender IT-Sicherheitsanbieter und hat mit der SonicWALL Network Security Appliance (NSA)-Serie neue Maßstäbe bei der Sicherheit und Netzwerkkontrolle gesetzt. Als Sicherheitslösung der nächsten Generation bietet die NSA-Serie die Multi-Threat-Sicherheit und granulare Kontrolle, die Unternehmen benötigen, um die speziellen Herausforderungen beim Einsatz von Webanwendungen zu meistern. Die gigabitschnellen Appliances mit mehrstufigen Schutzmechanismen helfen dabei, Bedrohungen zu identifizieren und zu blockieren, ohne die Performance zu beeinträchtigen. Eine Reihe individuell anpassbarer Sicherheitstools ermöglicht eine detaillierte Kontrolle und Überwachung des Netzwerkverkehrs, gewährleistet die Bandbreitenverfügbarkeit für kritische Prozesse und lässt sich unkompliziert an veränderte Geschäftsbedingungen anpassen.