

Unified Threat Management:
Flexible, hochintegrierte Sicherheitsfunktionen zum
Schutz vor immer häufigeren Mischangriffen

Die Unified Threat Management-Lösung (UTM) von SonicWALL® bietet Unternehmen mit verteilten Netzwerken intelligenten Echtzeitschutz gegen contentbasierte Bedrohungen sowie gegen Angriffe über die Anwendungsebene und überwacht gleichzeitig die verschiedensten Kommunikationsvorgänge im Netzwerk, wie E-Mail, Instant Messaging und Web-Zugriffe.

INHALT

Eine kurze Geschichte der Firewall	3
Herausforderungen für heutige Unternehmensnetzwerke	4
Unified Threat Management – Erweiterte Netzwerksicherheit	5
Die Unified Threat Management-Lösung von SonicWALL	6
– Nicht alle UTM-Lösungen sind gleich	7
– Unternehmensnetzwerke für die Zukunft wappnen	8
– Optimaler ROI	9
Resümee	9

Angriffe auf Computersysteme gibt es schon seit über 25 Jahren, und auch heute gelingt es Hackern immer wieder, mit neuen und komplexen Angriffen verheerende Schäden in Unternehmensnetzwerken anzurichten. Seit über zwei Jahrzehnten nutzen Organisationen Firewall-Systeme, und seit einiger Zeit auch punktuelle Lösungen wie Viren-Erkennung, Viren-Schutz, Verschlüsselungstechnologien sowie Patch-Management, um Daten vor Computerkriminellen zu schützen. Doch da Netzwerkbedrohungen inzwischen gleich mehrere Angriffsarten kombinieren und dadurch noch größere Schäden verursachen, bieten punktuelle Lösungen heute keinen ausreichenden Netzwerkschutz mehr. Zwar werden die Schutzvorkehrungen immer komplexer, doch Hacker finden gerade deswegen immer raffiniertere Methoden, um sämtliche Schutzschichten mit Mischangriffen zu umgehen. Außerdem werden ständig neue Technologien wie VoIP entwickelt, die überall im Unternehmensnetzwerk eingesetzt werden, wodurch neue Schwachstellen entstehen. Auch einfache Internetdienste wie Web-Zugriff, Instant Messaging und Peer-to-Peer File Sharing-Netzwerke (wie beispielsweise die Tauschbörse Kazaa) sind nicht nur bekannt dafür, unnötig Bandbreite zu verbrauchen und sich negativ auf die Mitarbeiterproduktivität auszuwirken, sie sind auch für mögliche Sicherheitslücken im Netzwerk verantwortlich.

Sicherheitsexperten sind sich einig, dass schon eine einzige Schwachstelle das gesamte Sicherheitssystem gefährden kann. Daher benötigen Unternehmen ganzheitliche Sicherheitslösungen, die Netzwerke und Benutzer vor Mischangriffen und dem Missbrauch von Unternehmensressourcen schützen und gleichzeitig die Ausgaben für Netzwerkschutz senken. Da sich Sicherheitsbedrohungen ständig weiterentwickeln, verzeichnet Unified Threat Management (UTM) inzwischen die höchsten Zuwachsraten auf dem Markt für Security Appliances. UTM steht für Sicherheitslösungen, die verschiedene Sicherheitsfunktionen – Firewall-Technologie, Anti-Virus, Intrusion Detection and Prevention sowie Content-Überwachung und -Filtering – in einer einzigen Hardware-Plattform kombinieren und so umfassenden Netzwerkschutz bieten. Die Bezeichnung UTM wurde von IDC geprägt, einem der weltweit wichtigsten Anbieter im Bereich IT-Marktbeobachtung und Beratung. Laut Branchenanalysten haben vor allem der rapide Anstieg von Mischangriffen und der mobile Zugriff auf Informationen die Nachfrage nach flexiblen und hochintegrierten Funktionen, wie sie in UTM integriert sind, zunehmend steigen lassen. Die Unified Threat Management-Lösung (UTM) von SonicWALL® bietet Unternehmen mit verteilten Netzwerken intelligenten Echtzeitschutz gegen contentbasierte Bedrohungen sowie gegen Angriffe über die Anwendungsebene und überwacht gleichzeitig die verschiedensten Kommunikationsvorgänge im Netzwerk wie E-Mail, Instant Messaging und Web-Zugriffe. UTM wird dabei als eine "intelligente" Lösung bezeichnet, da sie außerordentlich lösungsorientiert arbeitet: Die SonicWALL-Technologie setzt sich von Standard-Firewall-Lösungen durch seine ganzheitliche Multi-Layer-Architektur ab und bietet einen besseren Einblick in die Netzwerk-Nutzung. Außerdem identifiziert die SonicWALL-Technologie mögliche Netzwerk-Einbrüche und missbräuchliche Netzwerk-Nutzung in Echtzeit.

SonicWALL Unified Threat Management

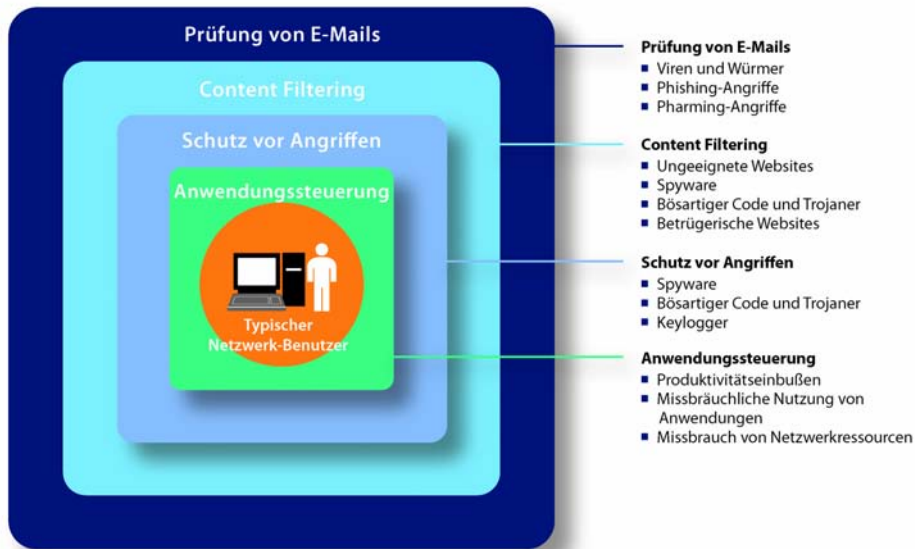


Abbildung 1. Uneingeschränkter Zugriff auf das Internet macht Unternehmen anfällig für Bedrohungen

Eine kurze Geschichte der Firewall

Seit einiger Zeit bilden Firewalls das zentrale Element innerhalb einer IT-Sicherheitsinfrastruktur. Firewalls wurden Anfang der achtziger Jahre entwickelt und unterbinden seitdem unberechtigte Zugriffe auf Netzwerke. Dabei haben sich mit der Weiterentwicklung der Netzwerke auch die Sicherheitstechnologien gewandelt: Aus einfachen Zugriffssteuerungsmethoden auf Basis von IP-Adresslisten wurden Systeme, die auf mehreren Ebenen wirken und den Verkehr in vertrauenswürdigen Zonen freigeben können, während sie gleichzeitig Bedrohungen wie Computerviren ausschalten.

Mit dem Einzug moderner Netzwerktechnologien, die als Grundlage für Ethernet-basierte LANs (Local Area Networks) dienen, mussten Firewalls plötzlich in der Lage sein, eine neue Art Sicherheitsbedrohung abzuwehren: Internetwürmer. Um dieser Bedrohung zu begegnen, stattete man Firewalls mit paketbasierten Filtern aus, die den Netzwerkverkehr auf den untersten Ebenen verarbeiteten: Jedes einzelne Paket wurde anhand seiner Ursprungs- und Zielinformationen mit einem Satz von Sicherheitsregeln abgeglichen, die rudimentären Schutz boten. Mit dem Aufkommen der ersten Internetbrowser konnten Unternehmen weltweit Verbindungen über das Internet herstellen. Nun benötigte man eine neue Generation von Firewalls, die eine Schutzschicht bildeten, indem sie jedes einzelne Datenpaket mit einer Tabelle von gültigen Netzwerksitzungen abglichen. Schon bald waren Firewalls so weit entwickelt, dass sie Pakete analysieren konnten und die Prüfung zusätzlicher sicherheitsrelevanter Elemente zuließen.

Seit sich Netzwerke mit Technologien wie Wireless und Virtual Private Network (VPNs) erweitern lassen und Anwender nicht mehr auf Kabel angewiesen sind, um auf das Internet zuzugreifen, sind Unternehmensnetzwerke noch größeren Sicherheitsgefahren ausgesetzt. Mit VPN und anderen neuen Technologien können Anwender das Netzwerk besser nutzen. Auch wenn der VPN-Datenverkehr verschlüsselt ist, ergeben sich damit neue Möglichkeiten für Hacker und Mischangriffe, um Firewalls zu umgehen. Seit 2005 haben die meisten VPNs immer noch Sicherheitsschwachstellen. Das ist besonders gefährlich, weil die meisten VPN-Benutzer das System für unbezwingbar halten und deswegen möglicherweise zusätzliche Sicherheitsmaßnahmen außer Acht lassen. Während Anwender mit VPN von neuen Zugriffsmöglichkeiten auf das Netzwerk profitieren, stellt jeder neue Zugriffspunkt ein weiteres

Angriffsziel für Hacker dar. Auch wenn punktuelle Lösungen inzwischen sehr weit entwickelt sind, haben neue Exploits verheerende Schäden und Produktivitätsverluste im Wert von mehreren Hundert Milliarden Dollar verursacht.

Herausforderungen für heutige Unternehmensnetzwerke

Unternehmen und Organisationen haben heute mit hochkomplexen Virenattacken und anderen bösartigen Angriffen zu kämpfen, die einen mehrschichtigen Ansatz verfolgen, um maximale Zerstörung anzurichten. Diese neuen Mischangriffe kombinieren Viren- und Wurm-Technologie in einem einzigen, extrem unberechenbaren Angriff. Der Computerwurm MyDoom wurde über E-Mail übertragen und gehört zu den aktuellsten Bedrohungen, die verschiedene Spielarten kombinieren. Dabei machte sich myDoom weltweit Millionen von Computern zunutze, um einen DoS-Angriff auf ein ausgewähltes Unternehmen auszuführen. Schätzungen zufolge wurden in den ersten fünf Tagen nach Ausbruch des Wurms weltweit Schäden im Wert von über 60 Milliarden Dollar verursacht.

Mischangriffe stellen aber nicht nur eine Bedrohung für die Sicherheit dar. Zusätzlich verlangsamen sie das Netzwerk und erschweren die Priorisierung des Netzverkehrs, was zu Lasten der Effizienz geht. Performance-Probleme treten häufig auf, wenn zu viele Anwender das Netzwerk privat nutzen und beispielsweise die Tauschbörse Kazaa, Peer-to-Peer- Instant Messaging- oder Multimedia-Anwendungen aufrufen. Diese Anwendungen wirken sich nicht nur negativ auf die Produktivität und die Bandbreitenauslastung aus, sondern verursachen Sicherheitslücken im internen Netzwerk.

Auch die zunehmende geschäftliche und private Nutzung des Internets durch interne Benutzer, stellt eine ernstzunehmende Herausforderung für Unternehmen dar. So führt mangelnde Kontrolle bei der Internetnutzung immer wieder zu Produktivitäts- und Bandbreitenverlusten, oder zu rechtlichen Problemen durch den Zugriff auf unerwünschte oder illegale Webinhalte. Auch der unkontrollierte Zugang zum Internet macht das interne Netzwerk anfällig für Bedrohungen wie Spyware, Malicious Mobile Code (MMC), Key-Logging-, VoIP- und Phishing-Angriffe sowie betrügerische Websites. Der Zugriff auf Informationen sollte individuell für jeden einzelnen Benutzer kontrolliert werden – nur so lässt sich die Sicherheit des Netzwerks gewährleisten.

Viele Unternehmen verteilen punktuelle Lösungen über das gesamte Netz, um ihre Netzwerke vor Sicherheitsbedrohungen und Produktivitätsverlusten zu schützen. Auf diese Weise hoffen sie, alle potentiellen Gefahren auszuschalten. IT-Experten verwenden punktuelle Lösungen beispielsweise zum Schutz vor internen Angriffen. Laut einer Studie des FBI ist die Anzahl interner Angriffe höher als die Menge der externen Angriffe. (Siehe Abb. 2) Daher verwenden viele Unternehmen interne Intrusion Detection-Lösungen in Form von Überwachungssystemen für Abteilungen oder E-Mail Antiviren-Systemen, die dafür sorgen, dass sich Viren nicht ausbreiten können. Auch Bedrohungen, die von verteilten oder Remote-Standorten ausgehen, bereiten IT-Administratoren Kopfzerbrechen: beispielsweise, wenn Mitarbeiter von einem Hotel, HotSpot oder von unterwegs über einen VPN-Client auf das Unternehmensnetzwerk zugreifen und das Netz so den unterschiedlichsten Bedrohungen aussetzen. Um dieses Bedrohungsszenario auszuschalten, werden zunehmend separate VPN-Lösungen für Remote-Benutzer eingesetzt, die den Remote-Datenverkehr vom Hauptnetzwerk abtrennen.

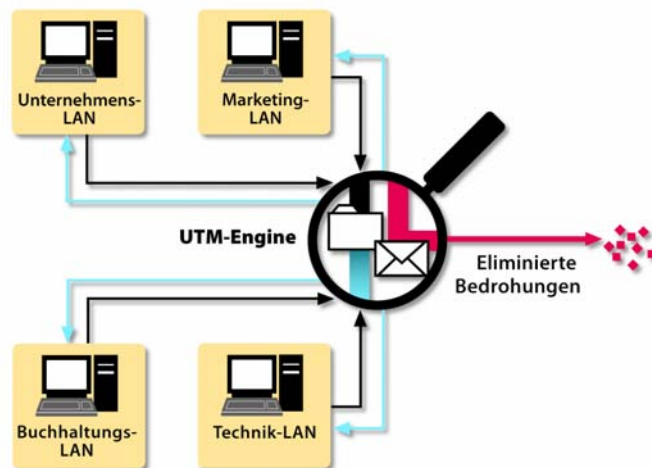


Abb. 2. UTM von SonicWALL blockiert interne und externe Bedrohungen

Da viele Unternehmen noch Sicherheitsbedenken im Umgang mit neuen Wireless-Technologien haben, implementieren sie häufig separate Wireless-Netzwerke und trennen den drahtlosen Datenverkehr vom internen Netzwerk ab. Außerdem werden Content Filtering-Lösungen eingesetzt, um Produktivitätsprobleme in den Griff zu bekommen und Spware zu eliminieren. Spam wird dabei mittels Filter-Software blockiert und Viren werden durch Firewall-Portüberwachung eingegrenzt. Außerdem installieren IT-Experten regelmäßig Patches für Server, Workstations, Router, Switches und Firewalls. Zwar können Patches Probleme mit bestehender Software beheben, doch häufig werden sie zu spät oder gar nicht implementiert. Da der ordnungsgemäße Einsatz von Patches langwierige Testläufe erfordert, ist es sinnvoller, Patches nicht einzeln zu installieren, sondern stattdessen einen Patch-Schutz auf Netzwerkebene zu installieren.

Punktuelle Lösungen haben sich in der Vergangenheit als äußerst effektiv erwiesen, jedoch zeigt sich immer deutlicher, dass sie heute keinen ausreichend schnellen und ganzheitlichen Schutz mehr bieten können. Außerdem sind sie häufig kompliziert zu installieren, können nicht zentral verwaltet werden und müssen manuell aktualisiert werden. Die Folge ist eine enorm aufwändige Handhabung, die zu spürbar höheren Kosten führt.

Unified Threat Management – Erweiterte Netzwerksicherheit

Organisationen benötigen heute integrierte und ganzheitliche Netzwerksicherheitslösungen, bei denen die Verwaltung der unterschiedlichen Sicherheits- und Produktivitätstechnologien in einem einzigen System kombiniert ist. Genau hier setzt Unified Threat Management an: UTM steht für einen neuen Trend auf dem Firewall-Markt und verkörpert die konsequente Weiterentwicklung der konventionellen Firewall in ein Produkt, das nicht nur Intrusion Prevention, sondern auch Content Filtering, Spam Filtering, Intrusion Detection und Antivirenschutzfunktionen bietet.

UTM ist so gesehen ein zwingender Meilenstein in der Evolution der Informationssicherheit, eine Bündelung unterschiedlicher Technologien, die eine Antwort auf die zunehmenden Herausforderungen unseres Jahrhunderts beim Schutz von Informationen darstellt. Effizientes Unified Threat Management bietet:

Total Cost of Ownership – Die Kosten für das gesamte System sollten niedriger sein, als der geschätzte Verlust durch Sicherheitseinbrüche aufgrund mangelnder Kontrolle. Außerdem sollte die Lösung die Reaktionszeiten für Sicherheitsmaßnahmen beschleunigen und den Verwaltungsaufwand reduzieren, so dass die TCO gesenkt werden können. Sicherheitsgefahren ändern sich ständig, daher sollte sich das System konstant auf diese Änderungen einstellen – und zwar so, dass der Benutzer gar nicht oder nur geringfügig einschreiten muss.

Koordination – Sicherheitseinbrüche können auf unterschiedlichen Technologieebenen stattfinden, daher sollte ein mehrschichtiger Sicherheitsansatz gewählt werden. Da viele Bedrohungen mehrere Angriffssignaturen haben, sollte eine Ebene den ersten Teil des Angriffes abfangen und eine weitere den Rest. Der gesamte Abwehrmechanismus muss dabei wie ein einziges, konsolidiertes Bollwerk funktionieren, um das Netzwerk umfassend schützen zu können.

Mehr Transparenz – Um maximalen Netzwerkschutz erzielen zu können, sollten die Lösungen transparent und unkompliziert bei der Implementierung sein. Außerdem sollten die einzelnen Komponenten reibungslos zusammenarbeiten, anderenfalls ist es schwierig oder gar unmöglich, dass Bedrohungen erkannt und bekämpft werden. Eine besondere Bedeutung kommt dabei den Reaktionszeiten und der Automatisierung passender Schutzmaßnahmen zu.

Unified Threat Management erfüllt diese und andere Anforderungen, da es wichtige Informationen und Sicherheitsfunktionen bündelt und die Verwaltung vereinfacht. Durch die effiziente Integration und Bereitstellung in einem einzigen Gerät trägt es außerdem dazu bei, die Kosten zu senken und die Zuverlässigkeit von Sicherheitsstrategien im Unternehmen zu erhöhen.

Unified Threat Management-Lösung von SonicWALL

Die UTM-Komplettlösung von SonicWALL bietet intelligenten Echtzeitschutz gegen contentbasierte Bedrohungen und Angriffen über die Anwendungsebene. Mit seiner UTM-Lösung vereint SonicWALL Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention Service und bietet Schutz vor externen und internen Bedrohungen. Dabei werden potenzielle Einfallstore für Angriffe überwacht und sämtliche Netzwerkebenen gründlich gescannt. Die leistungsfähige Deep Packet Inspection Engine überprüft das Netzwerk auf verschiedene Anwendungs- und Protokollarten und gleicht die Dateien mit einer umfangreichen Signaturrendatenbank ab. Auf diese Weise wird das Netzwerk direkt am Sicherheits-Gateway geschützt.

Viele punktuelle Lösungen, mit denen Unternehmen heute arbeiten, verwenden eine Firewall-Architektur, die als Stateful Packet Inspection bekannt ist. Diese Architektur wird hauptsächlich auf der Netzwerkebene eingesetzt und prüft, ob Datenpakete angefordert wurden und ob sie in das Netzwerk gelassen werden. Dies erlaubt einen selektiven aber gleichzeitig flexiblen Netzwerkzugriff von Außen und eine relativ uneingeschränkte Datenübertragung aus dem Inneren des Netzwerkes. Ein entscheidender Nachteil von Stateful Packet Inspection ist allerdings, dass der größte Teil des Datenverkehrs, der die Firewall passiert, nicht überprüft werden kann. Die "Stateful"-Ebene bietet damit einen eher durchlässigen Schutz, da viele Bedrohungen über interne Anwendungen (wie z.B. E-Mail), verbreitet werden.

SonicWALL greift dagegen auf eine durchgängige Lösung zurück, die als Echtzeit-Deep Packet Inspection (DPI) bekannt ist, und die den gesamten Netzwerkverkehr, einschließlich kodierten, komprimierten, verschlüsselten und drahtlosen Verkehr, mit einer umfassenden und kontinuierlichen Signaturrendatenbank abgleicht. Das SonicALERT-Team arbeitet zusammen mit anderen Anbietern rund um die Uhr an der Entwicklung von neuen Signaturen. Diese werden regelmäßig aktualisiert, um Echtzeit-Scans durchzuführen und versteckte und sichtbare Bedrohungen zu erkennen und zu blockieren.

Dank DPI-Technologie kann SonicWALL Informationen auf der Anwendungsebene prüfen und Angriffe abwehren, die auf Anwendungsschwachstellen abzielen. Die DPI Engine überprüft das Netzwerk auf verschiedene Anwendungs- und Protokollarten, wie SMTP, POP3, IMAP, FTP, HTTP, NetBIOS sowie zahlreiche andere streambasierte Protokolle und auf über 50 Anwendungsarten. Die SonicWALL-Engine prüft außerdem alle Netzwerkebenen, einschließlich Verknüpfungen, IP, TCP/UDP, statische Ports, dynamische Ports und gängige Benutzeranwendungen, wie beispielsweise Instant Messaging und Peer-to-Peer-Anwendungen, so dass alle Remote-Site-Gateways, internen Netzwerke, Dateidownloads, Server und Desktop-Rechner innerhalb von Unternehmensnetzen geschützt sind. Als zusätzliche Schutzschicht bietet SonicWALL umfassende Sicherheit sowohl vor internen als auch vor externen Netzwerkbedrohungen.

Die UTM-Lösung von SonicWALL bietet detaillierte Einblicke in den Netzwerkverkehr, so dass IT-Administratoren das Unternehmensnetz ständig überwachen und verbessern können. Übersichtliche Echtzeitreports und historische Reports liefern Administratoren aktuelle Informationen zur Netzwerksicherheit, unterstützen sie bei der Erkennung von potentiellen Gefahren sowie bei der Einschätzung von Risiken und bieten detaillierte Daten über die Internetnutzung der Mitarbeiter, um den künftigen Bandbreitenbedarf zu planen.

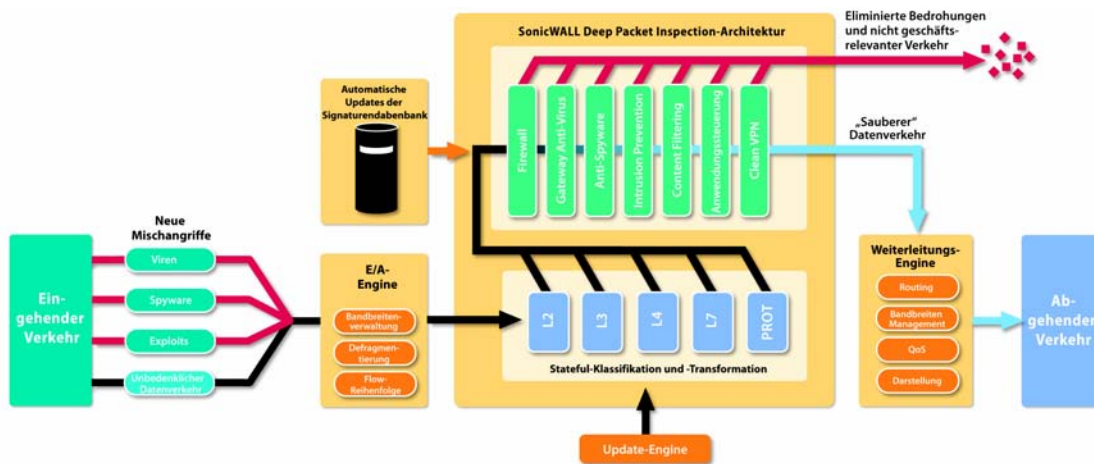


Abb. 3. Die Echtzeit-Unified Threat Management-Engine von SonicWALL

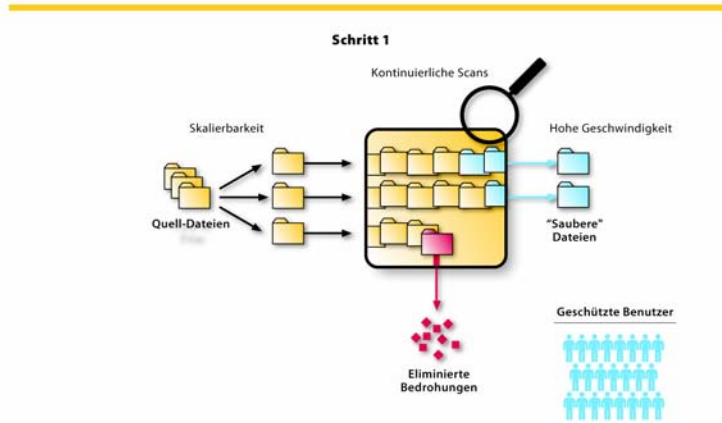
Nicht alle UTM-Lösungen sind gleich

Eines scheint klar: Die aktuell erhältlichen Stateful Packet-Lösungen bieten Unternehmensnetzwerken keinen ausreichenden Schutz vor Mischangriffen. Tatsächlich prüfen Stateful-Firewalls nur ca. 2 % des Datenverkehrs, der die Firewall passiert, während UTM-Lösungen mit Deep Packet Inspection den gesamten Datenverkehr scannen. Aber selbst bei UTM-Lösungen mit DPI gibt es Unterschiede. So sind beispielsweise UTM-Produkte mit "begrenzter" DPI und mit "umfassender" DPI auf dem Markt. SonicWALL hebt sich dabei gleich mehrfach von anderen Anbietern ab: Keine andere Lösung bietet genügend Leistung, um alle Benutzer in einem Netzwerk gleichzeitig abzudecken, den gesamten Datenverkehr, der die Appliance passiert, auf Bedrohungen zu prüfen und alle Verbindungen, die Dateien jeder Größe und nahezu aller Dateitypen transportieren, zu berücksichtigen. Die umfassende DPI von SonicWALL gewährleistet maximalen Schutz und garantiert gleichzeitig die Skalierbarkeit und Performance, die für wachsende Netzwerke nötig ist.

Die UTM-Engine von SonicWALL hebt sich hauptsächlich dadurch von den Produkten anderer Anbieter ab, dass sie als einzige Lösung keine Pause einlegen muss, um Datenverkehr in einem Speicher abzulegen (was bei allen anderen Lösungen auf dem Markt der Fall ist). Die Engine kann sämtliche Dateigrößen ohne Einschränkung, sowie unbegrenzt viele Netzwerkverbindungen in Echtzeit scannen. Skalierbarkeit und Performance basieren auf der leistungsstarken Reassembly-Free Deep Packet Inspection Engine, die dafür ausgelegt wurde, komplexe Bedrohungen in Hochgeschwindigkeit zu prüfen. Im Unterschied zu anderen Lösungen, gibt es bei der UTM-Technologie von SonicWALL weder Einschränkungen bei der Größe von Dateien, die Benutzer herunterladen können, noch bei der Anzahl der Benutzer, die gleichzeitig geschützt werden. Fremdanbieterprodukte bieten Administratoren nur zwei Optionen: Entweder passiert der Datenverkehr bei sehr hoher Netzauslastung das Netzwerk ohne Prüfung, oder der gesamte Verkehr wird blockiert, auch wenn es sich dabei um normale geschäftliche Daten handelt.

Die Deep Packet Inspection-Architektur von SonicWALL bietet nicht nur mit Abstand die größte Skalierbarkeit – sie ist auch die einzige Lösung, die tatsächlich Unified Threat Management in Echtzeit abwickelt.

Speicherunabhängige Engine von SonicWALL



Speicherabhängige Engine

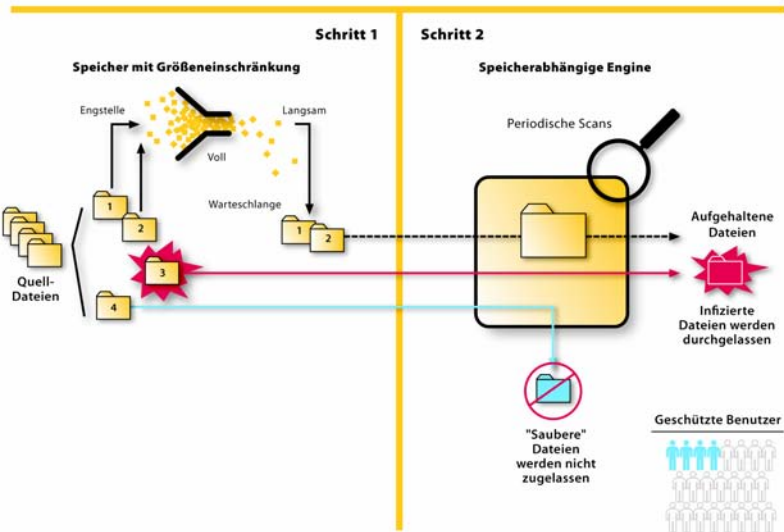


Abb. 4. Reassembly-Free Deep Packet Inspection-Technologie von SonicWALL

Unternehmensnetzwerke für die Zukunft wappnen

IT-Administratoren haben es nicht leicht: Jeden Tag tauchen neue Bedrohungen, wie Viren und Spyware auf, die eine ernstzunehmende Gefahr darstellen. Schaffen sie es nicht, die entsprechenden Sicherheitsupdates rechtzeitig zu installieren, so kann dies schwerwiegende Folgen haben. Einige dieser Bedrohungen können sich innerhalb von wenigen Stunden ausbreiten und Computer und Netzwerke jeder Größenordnung lahm legen. Da diese Angriffe immer raffinierter und dynamischer werden, brauchen Unternehmen eine zuverlässige Lösung die effektiven Schutz bietet. Genau hier kommen Unified Threat-

Lösungen ins Spiel: sie gewährleisten umfassenden Schutz vor aktuellen und neuen Bedrohungen, ohne dass Sicherheitsvorkehrungen manuell vorgenommen werden müssen.

Im Gegensatz zu anderen UTM-Produkten reagiert die SonicWALL-Lösung auf neue Sicherheitsgefahren, sobald diese auftauchen. Die Security Appliance passt sich an die ständig neuen Bedrohungen an und verändert ihre Sicherheitseinstellungen proaktiv. So schützt die SonicWALL-UTM-Lösung das Netzwerk effektiv vor den neuesten Bedrohungen – egal, ob sie von Übersee, von nebenan oder aus dem Inneren des Netzwerks kommen. Und was noch wichtiger ist: Dank automatisierten Updates, müssen Administratoren nicht manuell eingreifen, sondern profitieren von einer proaktiven Sicherheitslösung.

Die UTM-Lösung von SonicWALL ist eine zukunftssichere und anpassungsfähige Lösung, die Sie heute, morgen und auch in Zukunft zuverlässig schützt.

Optimaler ROI

Die SonicWALL UTM-Lösung wurde entwickelt, um bei der Prävention und Eliminierung von Sicherheitsbedrohungen Verwaltungskosten einzusparen. IT-Administratoren profitieren von einer integrierten Lösung und dem Know-how eines führenden Anbieters: Hunderte SonicWALL-Sicherheitsexperten arbeiten täglich daran, neue Technologien zum Schutz von Unternehmensnetzwerken zu entwickeln. Mit der SonicWALL UTM-Lösung lassen sich Verwaltungskosten reduzieren, der ROI verbessern und die Produktivität steigern. SonicWALL UTM schützt nicht nur geschäftskritische Daten, sie sorgt gleichzeitig für sichere Kommunikationen und eine effiziente Nutzung der Web-Ressourcen und verhindert, dass Netzwerke durch unerwünschte Anwendungen und Datenverkehr verlangsamt werden.

SonicWALL-Lösungen sind für Organisationen jeder Größenordnung erschwinglich und bieten kleinen und großen Unternehmen die sichersten Netzwerkfunktionen auf dem Markt.

Resümee

Seit die ersten Firewalls Anfang der achtziger Jahre auf dem Markt kamen, ist im Security-Bereich für Computernetzwerke viel passiert. Dennoch ist heute die Sicherheit von Netzwerken so wichtig wie nie zuvor: Netzwerkbedrohungen und Angriffe werden immer komplexer und schneller und entwickeln sich dabei ständig weiter. Während punktuelle Lösungen in der Vergangenheit Unternehmensnetze effektiv schützen konnten, bieten sie heute keine ausreichende Sicherheit mehr. Unternehmen benötigen heute ein effektives und mehrschichtiges Abwehrsystem gegen die ständig wechselnden aktuellen Sicherheitsbedrohungen – sie brauchen Unified Threat Management.

UTM von SonicWALL verwendet eine hochskalierbare, Reassembly-Free Deep Packet Inspection-Architektur, die direkt am Sicherheitsgateway umfassenden Schutz vor Bedrohungen bietet. Dabei scannt die Deep Packet Inspection- und UTM-Architektur das Netzwerk auf Viren, Würmer, Trojaner, Spyware, neue Bedrohungen und VoIP-Verkehr. Durch integrierte Content-Kontroll- und Filterfunktionen für Internetdienste, wie Webzugang, Instant Messaging und Peer-to-Peer File Sharing, lassen sich Haftungsrisiken reduzieren und die Produktivität verbessern.

Die UTM-Architektur von SonicWALL wird regelmäßig von einem Signaturen-Team aktualisiert, das rund um die Uhr Schutzmaßnahmen für die aktuellsten Sicherheitsschwachstellen von Betriebssystemen und Netzwerken sowie Kontrollmaßnahmen für gängige Benutzeranwendungen entwickelt. UTM von SonicWALL sorgt für Sicherheitsmechanismen, die an allen Unternehmensstandorten ohne Einschreiten der Anwender zum Schutz vor den aktuellsten Bedrohungen eingesetzt werden können – egal ob es sich dabei um große Unternehmensnetze, kleine Remote-Standorte, Home Offices oder Zweigniederlassungen handelt. UTM von SonicWALL eignet sich für alle Benutzer, unabhängig davon, ob sie sich an Unternehmensstandorten oder zwischen Netzwerkzonen aufhalten. Dabei können Dateien ohne Größeneinschränkung die Firewall passieren, während der Netzwerkschutz erhalten bleibt.

2005 wurde SonicWALL mit dem Grand Prize in der Kategorie Network Security bei der Interop in Tokio ausgezeichnet – dem wichtigsten Forum für Telekommunikation und Netzwerk-Technologie. Prämiiert wurde SonicWALLs einzigartige Kombination aus innovativen Technologien, optimaler Performance, Kosteneffizienz und Zuverlässigkeit. Als weltweit führender Anbieter im Bereich Unified Threat Management

unterstützt SonicWALL Unternehmen dabei, Netzwerkangriffe abzuwehren, ihre Produktivität und Effizienz zu steigern, die TCO für Netzwerk-Sicherheitslösungen zu senken und die Administration dank einer einzigen, benutzerfreundlichen Management-Oberfläche zu vereinfachen.