11 COOLE FUNKTIONEN, DIE IHRE FIREWALL BIETEN SOLLTE

Über den Schutz vor Netzwerkbedrohungen hinausgehen und auch den Anwendungsverkehr schützen, verwalten und kontrollieren

SONICWALL®

Inhalt

SONICWALL®

Die ausgereifte Firewall

Herkömmliche Stateful Packet Inspection-Firewalls blockieren Netzwerklayer-Bedrohungen, indem sie die vom Netzwerklayer-Verkehr verwendeten Ports und Protokolle analysieren. Die neuesten Next-Generation-Firewalls (NGFWs) verwenden eine tiefgreifende Paketinspektion, bei der die gesamte Paketnutzlast geprüft wird, um einen erweiterten Schutz vor unbefugten Eingriffen sowie Antimalware, Inhaltsfilterung und Anti-Spam zu bieten. Viele Anwendungen werden durch das Web über gemeinsam genutzte Ports und HTTP- oder HTTPS-Protokolle zugestellt. Herkömmliche Firewalls können diese Anwendungen nicht erkennen und somit auch nicht zwischen produktivem und sicherem oder unproduktivem und möglicherweise gefährlichem Verkehr unterscheiden. Next-Generation-Firewalls ermöglichen dagegen einen Einblick in die Anwendungen selbst, was besonders für Netzwerkadministratoren von großer Bedeutung ist.

Mit der Verbreitung von Cloud-Computing und Web 2.0-Technologien werden Firewalls auch mit den Herausforderungen der Anwendungskontrolle konfrontiert.

SONICWALL®

Welchen Zweck hat die SonicWall Anwendungsintelligenz und -kontrolle?

SonicWall Firewalls ermöglichen die Identifizierung und Kontrolle aller in Ihrem Netzwerk verwendeten Anwendungen. Mit dieser zusätzlichen Kontrolle werden Konformität und Datenleckverhinderung optimiert, da Anwendungen nicht anhand der Ports oder Protokolle, sondern auf Basis ihrer eindeutigen Signaturen identifiziert werden. Dies wird durch die Visualisierung des Anwendungsverkehrs ermöglicht. Dabei werden Nutzungsmuster aufgezeigt und dann granuläre Richtlinien für Anwendungen, Benutzer oder sogar Benutzergruppen sowie Tageszeiten und andere Variablen erstellt. Das Resultat ist eine flexible Kontrolle, die für jede Netzwerkanforderung angepasst werden kann.

Zuweisung von Bandbreite für aufgabenkritische oder latenzempfindliche Anwendungen.

Wie funktioniert die SonicWall Anwendungsintelligenz und -kontrolle?

Mithilfe einer umfassenden, konstant wachsenden und automatisch aktualisierten Datenbank identifiziert SonicWall Anwendungen an deren DNA, anstatt die weniger eindeutigen Attribute, wie Port, Zielport oder Protokollart, zu verwenden. Sie können beispielsweise Instant Messaging erlauben aber Dateitransfer blockieren oder Facebook-Zugang erlauben aber den Zugang zu Facebook-basierten Spielen blockieren. Diese Kontrollen sind auch für jeden TLS/SSL-verschlüsselten Verkehr verfügbar, der allerdings genau wie nicht verschlüsselte Verbindungen inspiziert werden muss. Die Resultate Ihrer Kontrollen lassen sich leicht visualisieren, z. B. um die Nutzung von Anwendungen abzustimmen und die Netzwerkbandbreite zu optimieren.

Sie können Anwendungskategorien, einzelne Anwendungen und bestimmte Funktionsmerkmale innerhalb von Anwendungen kontrollieren.

Anhand der Anwendungsvisualisierung können Sie vor dem Erstellen der Richtlinie „sehen“, welche Browser verwendet werden.

1. coole Funktion:

Kontrolle der im Netzwerk erlaubten Anwendungen

Sie möchten sicherstellen, dass alle Ihre Mitarbeiter die neueste Version von Internet Explorer verwenden. Um das zu erreichen, sollen alle Mitarbeiter, die IE9 oder IE10 starten, automatisch zur Download-Site für IE11 weitergeleitet werden, ohne auf andere Websites zugreifen zu können. Mögliche Lösungen:

- Tägliche manuelle Überprüfung der Webbrowser-Version jedes Systems
- Erstellung eines speziellen Skripts für die automatische Überprüfung der Webbrowser-Versionen
- Einrichten einer Richtlinie mithilfe der SonicWall Anwendungsintelligenz und -kontrolle—und keine Sorgen mehr machen

Erstellen Sie eine Richtlinie, unter der alle IE9- oder IE10-Benutzer umgeleitet werden und den neuesten IE-Browser herunterladen müssen, und IE9- oder IE10- Versionen keinen Internetzugang erhalten

1. Die Deep Packet Inspection (DPI) Engine sucht im HTTP-Header nach User Agent = IE 9.0 oder User Agent = IE 10.0
2. Die Richtlinie leitet IE9- oder IE10-Benutzer an die IE11-Download-Site weiter und blockiert den Zugriff der IE9- oder IE10-Versionen auf andere Websites

SONICWALL

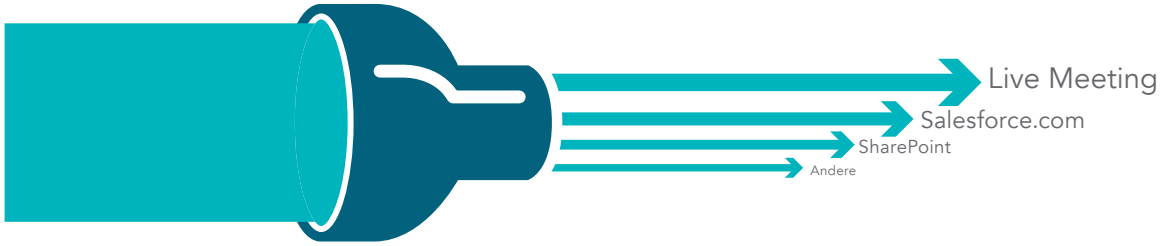
2. coole Funktion:

Verwaltung der Bandbreite für kritische Anwendungen

Viele aufgabenkritische Anwendungen, wie Live Meeting, Salesforce.com® und SharePoint®, sind Cloud-basiert oder werden über geografisch weit verstreute Netzwerke ausgeführt. Zur Gewährleistung optimaler Produktivität müssen diese Anwendungen Priorität gegenüber unproduktivem Websurfing-Verkehr erhalten.

Erstellen Sie eine Richtlinie, unter der die Live Meeting-Anwendung Bandbreitenpriorität erhält

1. Die Deep Packet Inspection Engine sucht nach der Signatur oder dem Namen der Anwendung
2. Weisen Sie der Live Meeting-Anwendung eine höhere Bandbreitenpriorität zu



Die Anwendungspriorität kann auf einem Datum basieren (z. B. für die Zuweisung einer höheren Priorität für Verkaufsanwendungen zum Quartalsende).

SONICWALL®

3. coole Funktion:

Blockierung von Peer-to-Peer-Anwendungen

Unproduktive Peer-to-Peer (P2P)-Anwendungen, wie BitTorrent, werden oft für den Download von nicht lizenzierten Versionen von urheberrechtlich geschützten Medien verwendet und können schnell große Bandbreiten verbrauchen oder Malware übertragen. Da jedoch laufend neue P2P-Anwendungen erstellt oder bestehende P2P-Anwendungen geändert (z. B. Versionsnummern) werden, ist es schwierig, eine einzelne P2P-Anwendung zu blockieren.

SonicWall aktualisiert seine Datenbank für Anwendungsintelligenz- und kontrolle auf laufender Basis und neue P2P-Anwendungen werden sobald sie verfügbar sind aufgenommen. Jetzt können Sie einfach eine Richtlinie erstellen, unter der alle weiteren P2P-Anwendungen blockiert werden.

Erstellen Sie eine Richtlinie, um die Verwendung von P2P-Anwendungen zu blockieren

1. Die Deep Packet Inspection Engine verwendet die in der Liste von Anwendungssignaturen vordefinierten Signaturen für P2P-Anwendungen
2. Wählen Sie die P2P-Anwendungen aus der Liste vordefinierter Signaturen aus
3. Wenden Sie die Richtlinie auf alle Benutzer an
4. Blockieren Sie P2P-Anwendungen durch bandbreiten- und zeitbasierte Einschränkungen

Anwendung Signaturenliste

BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
BitTorrent-6.0.1
... und Hunderte mehr

+

Anwendung Signaturenliste

Updates von SonicWall werden empfangen und angewendet

=

Anwendung Signaturenliste

BitTorrent-6.1.1
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
... und Hunderte mehr

Resultat

- Sie können P2P-Anwendungen verwalten und kontrollieren
- Sie können sich den für das Aktualisieren von IPS-Signaturregeln erforderlichen Zeitaufwand sparen

4. coole Funktion:

Blockierung von unproduktiven Komponenten der Anwendungen

Social Networking-Anwendungen, wie Facebook, Instagram und YouTube, sind heute sowohl für den privaten als auch den unternehmerischen Bereich wichtige Kommunikationskanäle. Eine komplette Blockierung sämtlicher Social Networking-Anwendungen wäre deshalb nicht sinnvoll, doch die Kontrolle über deren Verwendung am Arbeitsplatz würde der Produktivität zugutekommen.

Marketing-Mitarbeiter sollten beispielsweise Zugang haben, um die Facebook-Seite des Unternehmens zu aktualisieren, doch das Spielen von Facebook-Spielen, wie Texas HoldEm Poker oder Candy Crush Saga, sollte nicht möglich sein. Mit der Anwendungsintelligenz und -kontrolle können Sie eine Richtlinie erstellen, unter der Facebook zugänglich ist, während alle Spiele blockiert sind.

Erstellen Sie eine Richtlinie, unter der Facebook zugänglich ist, aber Facebook-Spiele blockiert sind

1. Wählen Sie „Alle“ Benutzer
2. Wählen Sie „Facebook-Spieleanwendungen“ als Kategorie
3. Erstellen Sie eine Regel für die „Blockierung“ des Zugriffs aller Benutzer auf Spiele innerhalb von Facebook

Sie können auch Chats erlauben, aber mit Chats verbundene Dateitransfers blockieren.

5. coole Funktion:

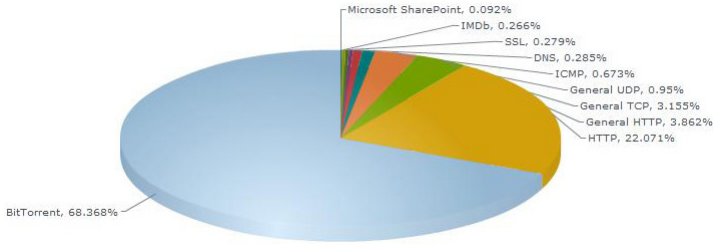
Visualisierung des Anwendungsverkehrs

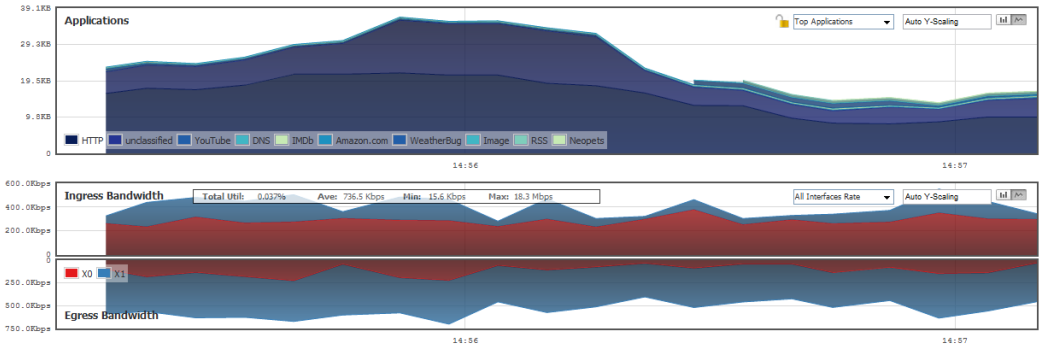
Was läuft in meinem Netzwerk ab? Wer verschwendet meine Bandbreite? Warum ist mein Netzwerk so langsam? Sind das Fragen, auf die Sie gerne Antworten hätten? Um diese Antworten zu erhalten, könnten Sie eine Kombination aus verschiedenen Tools verwenden, was mit großem Zeitaufwand verbunden wäre und lediglich nachträgliche Informationen liefern würde. Mit SonicWalls Echtzeitvisualisierung des Anwendungsverkehrs erhalten Sie sofort Antworten auf Ihre Fragen und Sie können Probleme schnell diagnostizieren, nicht-konforme Netzwerknutzungen erkennen, entsprechende Richtlinien erstellen und die Effektivität dieser Richtlinien sofort sehen.

Beobachten Sie den gesamten Verkehr in Echtzeit, indem Sie sich im Application Flow Monitor anmelden

1. Betrachten Sie Echtzeitdiagramme des gesamten Anwendungsverkehrs
2. Betrachten Sie Echtzeitdiagramme der Ingress- und Egress-Bandbreite
3. Betrachten Sie Echtzeitdiagramme der besuchten Websites und aller Benutzeraktivitäten
4. Erstellen Sie Ihre eigenen Filter, damit Sie stets Zugriff auf relevante Informationen erhalten

Durch Visualisierung erhalten Administratoren sofortiges Feedback zum Fluss des Netzwerkverkehrs.





SONICWALL

6. coole Funktion:

Verwaltung der Bandbreite für eine Gruppe von Benutzern

Was tun Sie, wenn sich der Firmenchef beschwert, weil seine morgendlichen Wirtschaftsnachrichten-Videos verzerrt sind oder nicht richtig abgespielt werden? Sie untersuchen die Sache und stellen fest, dass die Ursache in einer von Ihnen erstellten Richtlinie zur unternehmensweiten Bandbreitenverwaltung für alle Streaming-Videos liegt. Sie könnten die Bandbreiteneinschränkungen für alle etwas lockern, oder Sie verwenden die beste Lösung: Gruppenbasierte Bandbreitenverwaltung.

Erstellen Sie eine Richtlinie, unter der das Führungsteam des Unternehmens von den in der Bandbreitenverwaltung vorgesehenen Einschränkungen für Streaming-Videos ausgenommen ist

1. Wählen Sie die von Ihrem LDAP-Server importierte Führungsteamgruppe
2. Die Deep Packet Inspection Engine verwendet die in der Liste von Anwendungssignaturen vordefinierten Signaturen für Streaming-Video-Anwendungen
3. Wenden Sie die Bandbreiteneinschränkungen auf den Verkehr mit diesem Header an

Viele Unternehmen haben erkannt, dass ihre Mitarbeiter zufriedener sind, wenn sie vollen Webzugang erhalten, auch wenn die Bandbreite für unproduktive Sites eingeschränkt ist.

SONICWALL

7. coole Funktion:

Blockierung von Ransomware-Angriffen und Einbrüchen

Netzwerksicherheit ist für jeden IT-Administrator oberste Priorität. Die Fähigkeit, durch Malware und Eindringversuche ausgeführte Ransomware-Angriffe und Einbrüche zu blockieren, führt zu einer maßgeblichen Reduzierung der Risiken und Ressourcenverschwendung von Unternehmen. Die SonicWall Sicherheitsdienste werden auf der leistungsstarken, praktisch latenzfreien Architektur der Sonic Wall Next-Generation-Firewalls ausgeführt und können Millionen von bekannten und unbekannten Bedrohungen von Ihrem Netzwerk abwenden, bevor diese zur Gefahr für Ihre Organisation werden könnten. SonicWall Capture erweitert die Verhinderungskapazität der Firewall durch Erkennung und Blockierung unbekannter und Zero-Day-Attacken durch einen cloudbasierten Multi-Engine-Sandbox-Dienst.

Blockieren Sie Malware-Attacken und Eindringversuche, bevor diese in Ihr Netzwerk gelangen!

SONICWALL®

8. coole Funktion:

Identifizierung von Verbindungen nach Land

Handelt es sich bei einer Verbindung zwischen Ihrem lokalen Büro oder einer Zweigstelle und einem IP in einem fremden Land lediglich um eine gutartige Websurfing-Verbindung oder ist es eine Botnet-Aktivität? Verwenden Sie die landesspezifische Verkehrsidentifizierung GeoIP, um den Netzwerkverkehr von und zu bestimmten Ländern zu identifizieren und zu kontrollieren. So können Sie sich vor Attacken von bekannten oder verdächtigen Bedrohungsquellen schützen oder den vom Netzwerk abgehenden verdächtigen Verkehr untersuchen.

Betrachten Sie Verbindungen nach Land oder richten Sie landesspezifische Filter ein

1. Prüfen Sie, welche Anwendungen mit den IP der anderen Länder Verbindungen herstellen
2. Sehen Sie, welche Benutzer und welche Computer mit den IP anderer Länder Verbindungen herstellen
3. Richten Sie Filter ein, um den Verkehr zu den von Ihnen vorgegebenen Ländern einzuschränken und Ausnahmelisten einzurichten

Nachdem Sie die Antwort gefunden haben, können Sie mit dem Benutzer sprechen, den Rechner mit der fraglichen IP-Adresse inspizieren oder eine Paketerfassung an der Firewall aktivieren, um genau zu analysieren, was über diese Verbindung abläuft. Mit der landesspezifischen Verkehrsidentifzierung GeoIP von SonicWall können Sie Probleme erkennen und beheben, derer Sie sich sonst nicht bewusst gewesen wären.

9. coole Funktion:

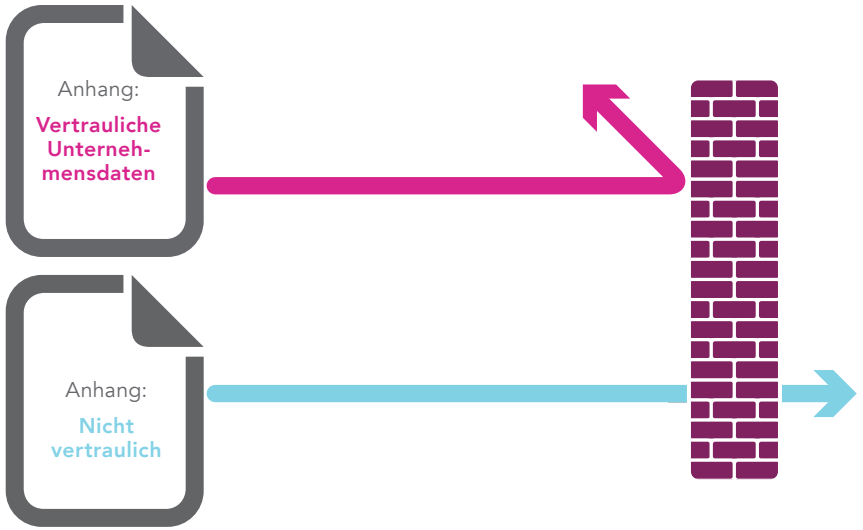
Verhinderung von Datenlecks via E-Mail

In manchen Unternehmen wird die abgehende E-Mail nicht durch das E-Mail-Sicherheitssystem geleitet oder der Inhalt von E-Mail-Anhängen wird vom Sicherheitssystem nicht geprüft. Unter beiden Umständen können Anhänge mit „vertraulichen Unternehmensdaten“ das Unternehmen verlassen. Da der abgehende Netzwerkverkehr durch Ihre Firewall geleitet wird, können Sie diese „Datenbewegung“ erkennen und blockieren.

Erstellen Sie eine Richtlinie für die Blockierung von E-Mail-Anhängen, die das Wasserzeichen für „vertrauliche Unternehmensdaten“ tragen

Die Deep Packet Inspection Engine sucht nach:

1. E-Mail-Inhalt = „Vertrauliche Unternehmensdaten“ und
2. E-Mail-Inhalt = „Proprietäre Unternehmensinformationen“ und
3. E-Mail-Inhalt = „Privat proprietär“ etc.



SONICWALL®

10. coole Funktion:

Verhinderung von Datenlecks via Web-Mail

Nehmen wir an, dass Ihr bestehender Anti-Spam-Schutz eine normale abgehende E-Mail erkennen kann, die „vertrauliche Unternehmensdaten“ enthält. Was geschieht jedoch, wenn ein Mitarbeiter einen Webmail-Service, wie Yahoo® oder Gmail® verwendet, um „vertrauliche Unternehmensdaten“ an eine externe Stelle zu senden?

Erstellen Sie eine Richtlinie für die Blockierung von Anhängen mit „vertraulichen Unternehmensdaten“ im Web-Verkehr

1. Die Deep Packet Inspection Engine sucht in den via http oder https übertragenen Dateien nach „vertraulichen Unternehmensdaten“
2. Blockieren Sie die Nachricht und informieren Sie den Absender darüber, dass die Nachricht „vertrauliche Unternehmensdaten“ enthält

i.O.

Von: guteabsicht@Ihr_Unternehmen.com
An: guteabsicht@Partner.com
Betreff: Genehmigung der Stechkarte von Jim
Ich habe die Stunden der Stechkarte für diese Woche genehmigt. Joe

n.i.O.

Von: böseabsicht@Ihr_Unternehmen.com
An: böseabsicht@Konkurrenzunternehmen.com
Betreff: Entwicklungsplan
Hier ist unser Entwicklungsplan
09. Jan – Version 7.0
Dieses Dokument enthält **vertrauliche Unternehmensdaten**

Diese Funktion kann auch für FTP-basierte Inhalte verwendet werden.

1. coole Funktion:

Bandbreitenverwaltung für das Streamen von Audio und Video

Der Zugang zu Streaming-Videos von Sites wie YouTube.com kann nützlich sein, wird aber oft missbraucht. Eine Blockierung dieser Sites ist eventuell hilfreich, doch ein besserer Ansatz ist die Einschränkung der Gesamtbandbreite für Streaming-Videos jeden Ursprungs. Das Gleiche gilt für Audio-Streaming-Sites, wie Online-Radiosender und Musik-Streaming-Dienste wie Spotify und Apple Music. Diese Art von Verkehr muss nicht unbedingt von gut bekannten Sites stammen, sondern kann auch durch Blogs gehostet werden. Deshalb sollte dieser Verkehr an seiner Art erkannt werden, nicht an seinem Ursprung. Für diesen Fall ist die Deep Packet Inspection unübertrefflich.

Erstellen Sie eine Richtlinie, unter der Streaming-Audio und Streaming-Video durch vordefinierte Signaturenlisten eingeschränkt werden

1. Wählen Sie Streaming-Video und Streaming-Audio als Anwendungskategorien
2. Setzen Sie eine Bandbreite fest, die Sie diesen Anwendungskategorien zuweisen möchten (z. B. 10 %)
3. Erstellen Sie eine Regel, unter der durchgesetzt wird, dass für Streaming-Video und Streaming-Audio maximal 10 % der Bandbreite genutzt werden können und die Regel für alle gilt (eventuell unter Ausnahme bestimmter Abteilungsgruppen, z. B. im Schulungsbereich)
4. Optional kann die Regel auch so eingerichtet werden, dass sie nur während normaler Geschäftszeiten gilt, aber nicht während der Mittagspause oder nach 18 Uhr.
5. Bestätigen Sie die Effektivität Ihrer neuen Richtlinie durch Echtzeitvisualisierung, indem Sie sich im Application Flow Monitor anmelden

SONICWALL®

Das Resultat

Leistungsstarke Plattform
+ Tiefgreifende Paketinspektion
+ Verhinderung von Eingriffen
+ Anwendungsintelligenz, Kontrolle und Visualisierung

SonicWall Next-Generation-Firewalls

Sicherheit, Performance und Kontrolle

SONICWALL®

Über uns

Seit über 27 Jahren verteidigt SonicWall kleine und mittelständische Unternehmen weltweit im Kampf gegen Cyberkriminalität. Unsere Kombination von Produkten und Partnerschaften liefert Echtzeit-Cyberschutzlösungen, die auf die spezifischen Bedürfnisse der über 500.000 Unternehmen in mehr als 215 Ländern und Gebieten abgestimmt sind. Das Ergebnis: Sie können sich beruhigt ganz auf Ihr Geschäft konzentrieren. Weitere Informationen finden Sie auf www.sonicwall.com oder folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram.

Bei Fragen zu Ihrer möglichen Verwendung dieses Materials setzen Sie sich bitte mit uns in Verbindung:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

Ebook-11CoolThings-Firewall-US-VG-MKTG5084

SONICWALL