# 11 nützliche Funktionen, die Ihre Firewall bieten sollte

Next-Generation Firewalls können mehr als nur Netzwerkbedrohungen blockieren:
Sie schützen, verwalten und kontrollieren den Anwendungsverkehr

DELL SonicWALL

# Inhalt

# Die Firewall wird erwachsen

Konventionelle Stateful Packet Inspection Firewalls sind darauf spezialisiert, Bedrohungen über die Netzwerkebene abzuwehren. Dazu evaluieren sie, welche Ports und Protokolle vom Datenverkehr auf der Netzwerkebene verwendet werden. Ganz anders die neuesten Next-Generation Firewalls: Sie prüfen den gesamten Paket-Payload mittels Deep Packet Inspection und bieten auf diese Weise erweiterte Intrusion Prevention- und Content Filtering-Services sowie einen wirksamen Schutz vor Malware und Spam. Da viele Anwendungen über das Web bereitgestellt werden und gängige Ports und HTTP- oder HTTPS-Protokolle nutzen, sind herkömmliche Firewalls „blind" gegenüber diesen Anwendungen: Sie sind nicht in der Lage, geschäftsrelevanten und unbedenklichen Datenverkehr gegenüber unerwünschten und potentiell unsicheren Daten zu priorisieren. Next-Generation Firewalls dagegen liefern detaillierte Informationen über die Anwendungen selbst und bieten Netzwerkadministratoren damit ein äußerst wichtiges Instrument.

**Die zunehmende Verbreitung von Cloud Computing und Web 2.0-Technologien stellt Firewalls nun vor eine neue Herausforderung: Das Erkennen und Kontrollieren von Anwendungen**

## Was bietet Dell SonicWALL Application Intelligence and Control?

Mit den Firewalls von Dell™ SonicWALL™ können Sie sämtliche Anwendungen identifizieren und kontrollieren, die in Ihrem Netzwerk genutzt werden. Diese zusätzliche Kontrolle unterstützt Sie bei der Einhaltung von Compliance-Vorgaben und bietet Ihnen einen erweiterten Schutz vor Datenlecks, da die Anwendungen nicht anhand von Ports oder Protokollen, sondern auf der Grundlage ihrer eindeutigen Signaturen identifiziert werden.

Durch die Visualisierung des Anwendungsverkehrs können Nutzungsmuster bestimmt und somit granulare Regeln für Anwendungen, Benutzer und selbst für Nutzergruppen sowie für Tageszeiten oder andere Variablen definiert werden. Auf diese Weise ist eine flexible Kontrolle in Netzwerken unterschiedlichster Anforderungen möglich.

# Zuweisen von Bandbreite für geschäfts- oder latenzkritische Anwendungen

# Wie funktioniert Dell SonicWALL Application Intelligence and Control?

Dell SonicWALL identifiziert Anwendungen anhand ihrer „DNA“, und nicht anhand weniger eindeutiger Attribute wie Quell- und Ziel-Port oder Protokollart. Dazu greift Dell SonicWALL auf eine umfangreiche, ständig wachsende und automatisch aktualisierte Anwendungssignaturen-Datenbank zurück.

Sie können zum Beispiel Instant Messaging zulassen, aber den Transfer von Dateien blockieren. Oder Sie erlauben den Zugriff auf Facebook, sperren aber Facebook-Spiele. Diese Kontrollen sind auch für SSL-Verkehr verfügbar, der genauso wie unverschlüsselte Verbindungen inspiziert werden muss. Sie können die Ergebnisse Ihrer Kontrollen ganz unkompliziert visualisieren, sodass Sie die Nutzung von Anwendungen auf Ihre Anforderungen abstimmen und die Netzwerkbandbreite optimieren können.

**Kontrolle von Anwendungskategorien, einzelnen Anwendungsfunktionen und bestimmten Funktionen innerhalb von Anwendungen.**

1. nützliche Funktion:

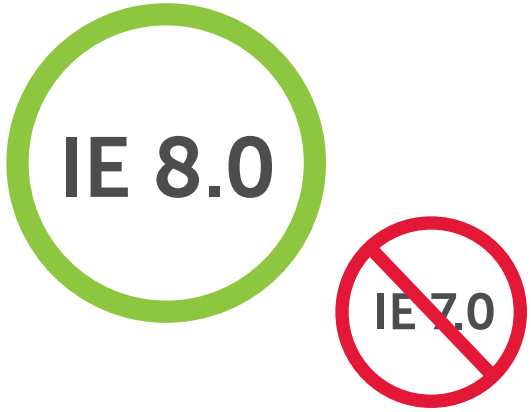
# Kontrolle der im Netzwerk erlaubten Anwendungen

Sie möchten sicherstellen, dass im gesamten Unternehmen nur die aktuelle Internet Explorer-Version verwendet wird. Daher sollen alle Mitarbeiter, die IE6 oder IE7 starten, automatisch auf eine Download-Seite für IE8 weitergeleitet und der Zugriff auf das Internet über IE6 oder IE7 blockiert werden. Es stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Sie prüfen täglich alle Systeme manuell auf die Browser-Version.
- Sie programmieren ein spezielles Skript, das alle Browserversionen automatisch prüft.
- Sie definieren mit Dell SonicWALL Application Intelligence and Control eine Regel und müssen sich weiter um nichts kümmern.

**Erstellen Sie eine Regel, die IE6- oder IE7-Nutzer zum Download der aktuellen IE-Browserversion leitet und den Internetzugriff für IE6 oder IE7 blockiert.**

1. Die Deep Packet Inspection (DPI) Engine sucht im HTTP-Header nach dem User Agent = IE 6.0 oder User Agent = IE 7.0.
2. Die Regel leitet IE6- oder IE7-Nutzer zur Download-Seite von IE8 weiter und blockiert den Zugriff über IE6 oder IE7 auf andere Websites.




## Durch die Anwendungsvisualisierung können Sie die verwendeten Browserversionen ermitteln, bevor Sie eine Regel definieren.

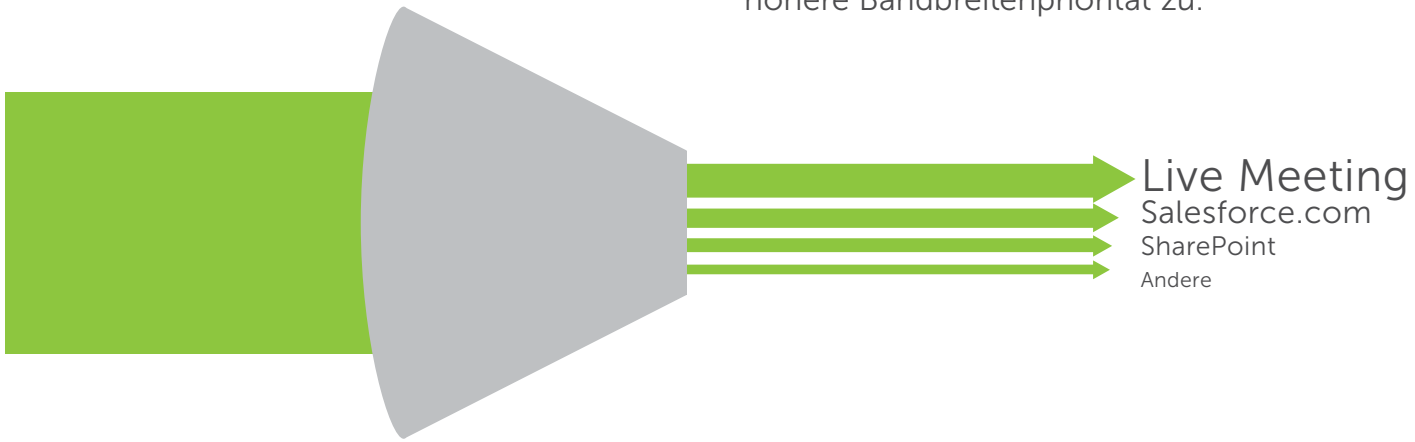
2. nützliche Funktion:

# Bandbreitenverwaltung für kritische Anwendungen

Viele geschäftskritische Anwendungen wie Live Meeting, Salesforce.com® und SharePoint® sind Cloud-basiert oder laufen in geografisch verteilten Netzwerken. Werden diese Anwendungen zulasten von privatem Websurfen priorisiert, lässt sich die Produktivität des Unternehmens verbessern.

**Definieren Sie eine Regel, um einer Live Meeting-Anwendung Bandbreitenpriorität zuzuweisen.**

1. Die Deep Packet Inspection (DPI) Engine sucht nach der Anwendungssignatur oder dem Anwendungsnamen.
2. Weisen Sie der Live Meeting-Anwendung eine höhere Bandbreitenpriorität zu.




## Anwendungen lassen sich auf der Grundlage eines Datums priorisieren (z. B. Priorität am Quartalsende für Vertriebsanwendungen).

3. nützliche Funktion:

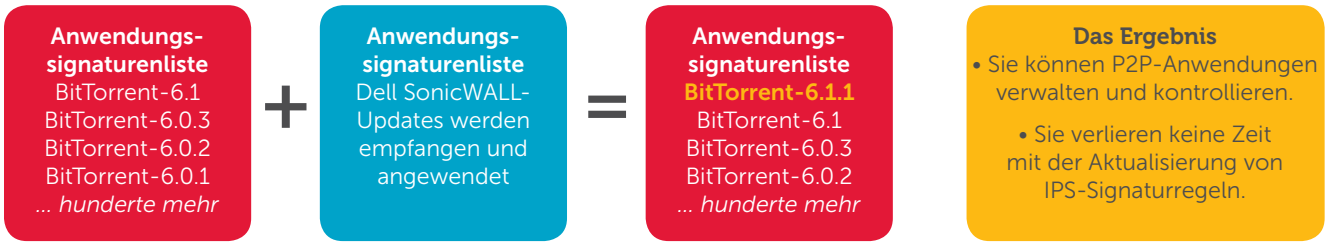
# Blockieren von Peer-to-Peer-Anwendungen

Nicht geschäftsrelevante Peer-to-Peer (P2P)-Anwendungen wie BitTorrent werden oft verwendet, um unlizenzierte Versionen urheberrechtlich geschützter Medien herunterzuladen, und können Bandbreite verschlingen oder Malware übertragen. Da ständig neue P2P-Anwendungen auftauchen oder minimale Änderungen an vorhandenen P2P-Anwendungen (z. B. eine neue Versionsnummer) vorgenommen werden, ist es schwierig, einzelne P2P-Anwendungen manuell zu blockieren.

Dell SonicWALL aktualisiert laufend seine Application Intelligence- und Anwendungskontroll-Datenbank, um neue P2P-Anwendungen hinzuzufügen, sobald sie in Umlauf sind. Mit Dell SonicWALL können Sie jetzt einfach eine Regel erstellen, um alle zukünftigen P2P-Anwendungen zu blockieren.

**Definieren Sie eine Regel, um die Nutzung von P2P-Anwendungen zu verhindern.**

1. Die Deep Packet Inspection (DPI) Engine verwendet vordefinierte P2P-Anwendungssignaturen aus der Anwendungssignaturenliste.
2. Wählen Sie die P2P-Anwendungen aus der vordefinierten Signaturenliste aus.
3. Wenden Sie die Regel auf alle Benutzer an.
4. Blockieren Sie die P2P-Anwendungen anhand bandbreiten- und zeitbasierter Einschränkungen.



4. nützliche Funktion:

# Blockieren von nicht geschäftsrelevanten Anwendungskomponenten

Soziale Netzwerke wie Facebook, Twitter und YouTube haben sich zu neuen Kommunikationsplattformen für Privatpersonen und Unternehmen entwickelt. Doch statt alle sozialen Netzwerke vollständig zu blockieren, ist es effektiver zu kontrollieren, wie diese Netzwerke am Arbeitsplatz genutzt werden.

Marketing-Mitarbeiter benötigen beispielsweise Zugriff auf Facebook um den Unternehmensauftritt zu aktualisieren, aber sie sollen nicht auf Facebook-Spiele wie Farmville oder Mafia Wars zugreifen können. Mit der Funktion Application Intelligence and Control lässt sich eine Regel erstellen, die den Zugriff auf Facebook freigibt, aber Spiele sperrt.

**Definieren Sie eine Regel, die den Zugriff auf Facebook freigibt, aber Facebook-Spiele sperrt.**

1. Wählen Sie „alle" Benutzer.
2. Wählen Sie Facebook-Spiele als Kategorie aus.
3. Definieren Sie eine einzige Regel, um den Zugang zu Facebook-Spielen zu blockieren.


Sie könnten ebenso die Chat-Funktion freigeben, aber den Transfer von Dateien im Chat blockieren.

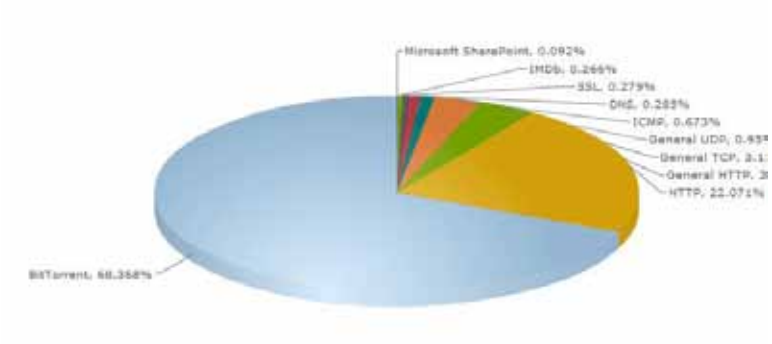
5. nützliche Funktion:

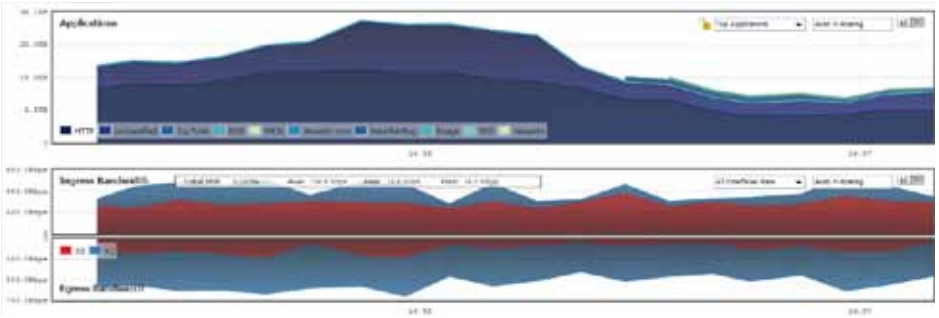
# Visualisierung Ihres Anwendungsverkehrs

Was passiert im Netzwerk? Welcher Benutzer verschwendet Bandbreite? Warum ist das Netzwerk so langsam? Kommen Ihnen diese Fragen bekannt vor? Sie könnten einzelne Tools kombinieren, um Antworten auf diese Fragen zu finden, doch dafür brauchen Sie viel Zeit und erhalten die gewünschten Informationen erst, nachdem die Fakten vorliegen. Mit Dell SonicWALLs Echtzeit-Visualisierung des Anwendungsverkehrs erhalten Sie umgehend eine Antwort. Sie können Probleme schnell identifizieren und erkennen, wenn die Netzwerknutzung nicht den Compliance-Vorgaben entspricht. Außerdem haben Sie die Möglichkeit, entsprechende Regeln zu definieren und sofort zu prüfen, wie sich diese auswirken.

**Loggen Sie sich am Application Flow Monitor ein und überwachen Sie den gesamten Anwendungsverkehr in Echtzeit**

1. Lassen Sie sich Echtzeit-Grafiken des gesamten Anwendungsverkehrs anzeigen.
2. Lassen Sie sich Echtzeit-Grafiken der ein- und ausgehenden Bandbreite anzeigen.
3. Lassen Sie sich Echtzeit-Grafiken der besuchten Websites und der Benutzeraktivitäten anzeigen.
4. Erstellen Sie Ihre eigenen Filter, um gezielt auf relevante Informationen zuzugreifen



# Durch die Visualisierung erhalten Administratoren umgehend Informationen zum Datenverkehr im Netzwerk.

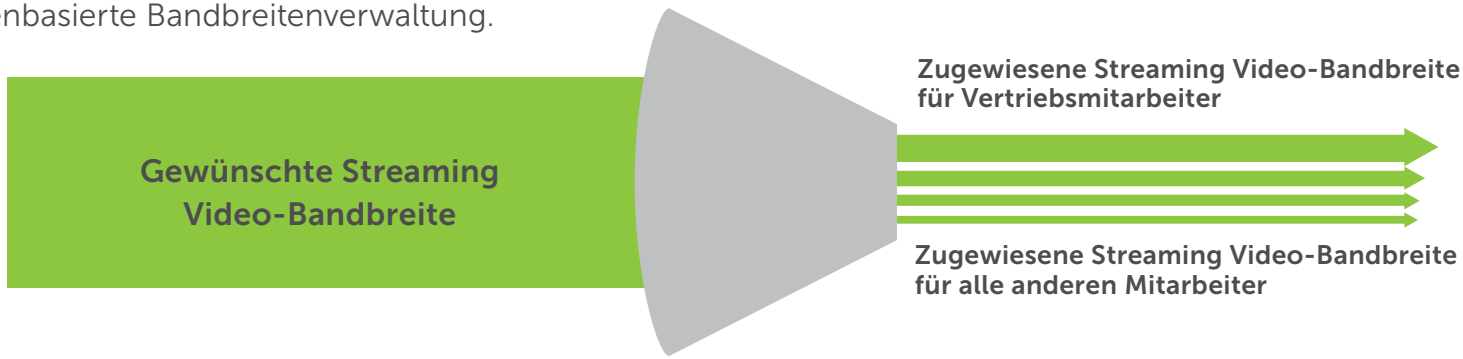
6. nützliche Funktion:

# Bandbreitenverwaltung für Benutzergruppen

Was tun Sie, wenn sich Ihr CEO beschwert, dass die Videoseiten mit den Wirtschaftsnachrichten, die er/sie jeden Morgen aufruft, ruckeln und nicht richtig abgespielt werden? Sie gehen der Sache auf den Grund und stellen fest, dass die Ursache dafür eine unternehmensweite Regel zur Bandbreitenverwaltung ist, die Sie für alle Streaming-Seiten implementiert haben. Eine Möglichkeit wäre nun, die Bandbreitenbeschränkungen für alle Mitarbeiter zu lockern, doch es gibt eine bessere Lösung: gruppenbasierte Bandbreitenverwaltung.

**Definieren Sie eine Regel, die Führungskräfte bei der Streaming Video-Bandbreitenverwaltung ausnimmt.**

1. Wählen Sie die von Ihrem LDAP-Server importierte Gruppe der Führungskräfte aus.
2. Die Deep Packet Inspection (DPI) Engine verwendet vordefinierte Anwendungssignaturen für Streaming-Video aus der Anwendungssignaturenliste.
3. Wenden Sie die Bandbreitenbeschränkung auf Datenverkehr mit diesem Header an.




Viele Unternehmen haben die Erfahrung gemacht, dass ihre Mitarbeiter Wert darauf legen, vollen Zugriff auf das Web zu erhalten, selbst wenn die Bandbreite für nicht geschäftsrelevante Seiten eingeschränkt ist.

7. nützliche Funktion:

# Virenschutz am Gateway

Für IT-Administratoren sollte der Netzwerkschutz an erster Stelle stehen. Sie müssen dafür sorgen, dass Malware wie Viren, Spyware, Keylogger, Trojaner und andere Eindringlinge am Gateway abgewehrt wird und nicht ins Netzwerk gelangt. Damit schützen sie ihr Unternehmen vor Risiken und verhindern, dass Ressourcen unnötig verschwendet werden. Kombiniert mit unserer hochleistungsfähigen und äußerst latenzarmen Next-Generation Firewall-Technologie können die Dell SonicWALL-Sicherheitsservices Millionen von Bedrohungen blockieren, bevor sie in das Netzwerk gelangen und einen Schaden anrichten. Wird z. B. ein infiziertes Laptop an das Netzwerk angeschlossen, können die Next-Generation Firewalls von Dell SonicWALL die Verbreitung von Malware innerhalb der Abteilung und der gesamten Organisation stoppen.

**Blockieren Sie Viren, Spyware und andere Malware am Gateway, bevor sie in Ihr Netzwerk gelangen!**

8. nützliche Funktion:

# Verbindungen nach Ländern sortieren

Handelt es sich bei einer Verbindung zu einer IP-Adresse im Ausland von einem benachbarten Büro oder einer Niederlassung nur um eine unbedenkliche Verbindung von einem Nutzer, der im Web surft, oder um eine Botnet-Aktivität? Application Intelligence bietet Ihnen ein leistungsfähiges forensisches Tool, um herauszufinden, was genau in Ihrem Netzwerk passiert.

**Lassen Sie sich Verbindungen nach Ländern sortiert anzeigen oder erstellen Sie länderspezifische Filter**

1. Prüfen Sie, welche Anwendungen Verbindungen zu IP-Adressen im Ausland herstellen.
2. Prüfen Sie, welche Benutzer und welche Rechner Verbindungen zu IP-Adressen im Ausland herstellen.
3. Erstellen Sie Filter, die mittels Ausschlusslisten den Datenverkehr für bestimmte Länder einschränken.

Sobald Sie die Antwort auf diese Frage kennen, können Sie mit dem Benutzer sprechen und das Gerät mit der angreifenden IP-Adresse inspizieren oder ein Paketerfassungsprogramm auf der Firewall aktivieren, um genau zu analysieren, welche Daten über diese Verbindung übertragen werden. Mit der Funktion Application Intelligence and Control können Sie Probleme erkennen und beheben, von denen Sie möglicherweise gar nichts gewusst hätten.

9. nützliche Funktion:

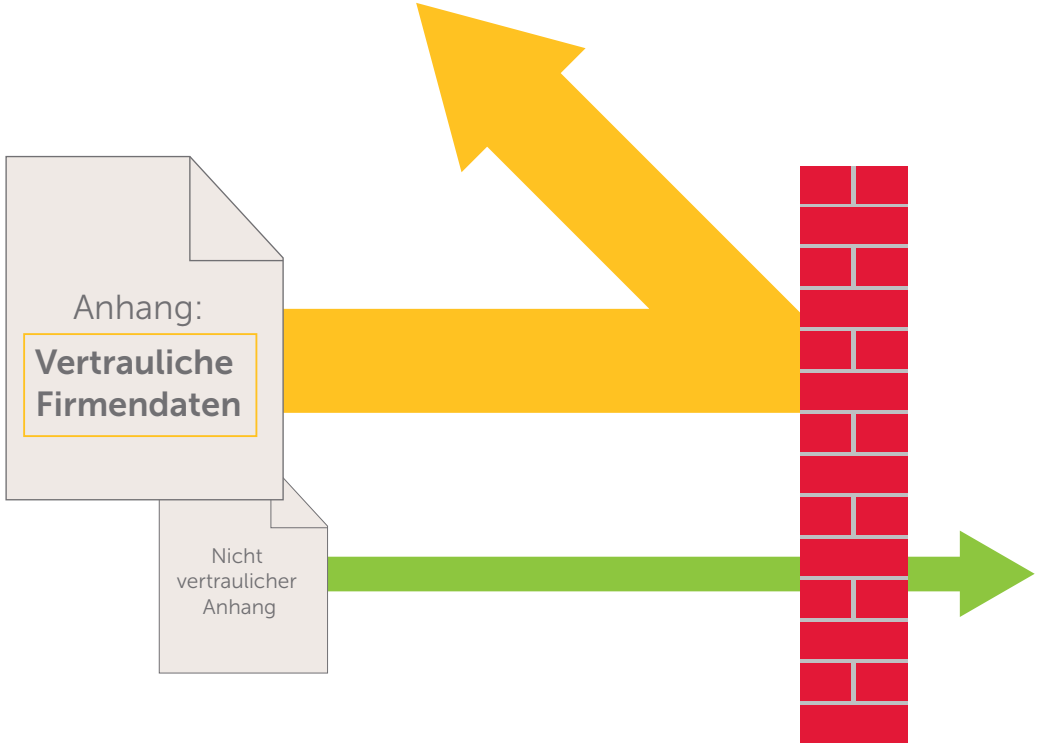
# Verhindern von E-Mail-basierten Datenlecks

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" problemlos nach außen gelangen. Nicht so bei Dell SonicWALL: Da der ausgehende Netzwerkverkehr Ihre Firewall passiert, können Sie diese Daten während der Übertragung („Data in Motion") erkennen und blockieren.

**Definieren Sie eine Regel, um E-Mail-Anhänge mit dem Wasserzeichen „Vertrauliche Firmendaten" zu blockieren.**

Die Deep Packet Inspection (DPI) Engine sucht nach dem

1. E-Mail-Inhalt = „Vertrauliche Firmendaten" und dem
2. E-Mail-Inhalt = „Firmeneigentum" und dem
3. E-Mail-Inhalt = „Privateigentum" und ...



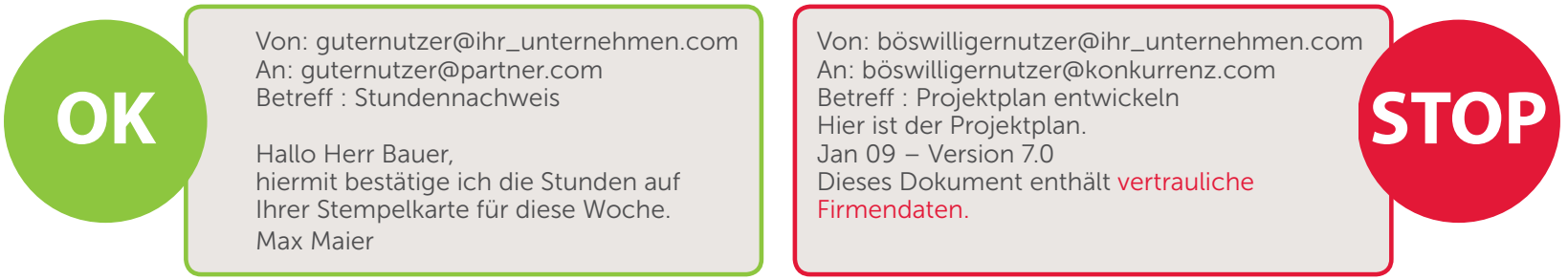
10. nützliche Funktion:

# Verhindern von Web-Mail-basierten Datenlecks

Nehmen wir einmal an, dass Ihre bestehende Anti-Spam-Lösung normale ausgehende E-Mails mit „vertraulichen Firmendaten“ erkennen und blockieren kann. Was aber geschieht, wenn ein Mitarbeiter „vertrauliche Firmendaten“ über einen Web-Mail-Service wie Yahoo® oder Gmail® versendet?

Definieren Sie eine Regel, um E-Mail-Anhänge mit „vertraulichen Firmendaten“ im Webverkehr zu blockieren.

1. Die Deep Packet Inspection (DPI) Engine sucht nach „vertraulichen Firmendaten“ in Dateien, die per HTTP oder HTTPS übermittelt werden.
2. Blockieren Sie die Nachricht und informieren Sie den Absender, dass die Nachricht „vertrauliche Firmendaten“ enthält.




## Dies lässt sich auch für FTP-Inhalte umsetzen.

11. nützliche Funktion:

# Bandbreitenverwaltung für Streaming-Audio und -Video

Streaming Video-Seiten wie z. B. youtube.com können zwar manchmal nützlich sein, doch häufig werden sie für private Zwecke genutzt. Eine Möglichkeit wäre, die Seiten komplett zu sperren. Die bessere Lösung ist aber, die für Streaming Video verfügbare Bandbreite einzuschränken, egal von welcher Seite die Videos stammen. Dies gilt auch für Streaming-Audio-Seiten, wie Online Musik-Radiosender und personalisierte Musik-Playlist-Seiten. Dieser Datenverkehr kommt nicht unbedingt von bekannten Seiten – er kann auch in Blogs gehostet werden. Es ist also nicht entscheidend zu wissen, woher der Datenverkehr stammt, sondern um welche Daten es sich handelt. Deep Packet Inspection ist hierfür besonders gut geeignet.

**Definieren Sie eine Regel zur Einschränkung von Streaming-Audio und Streaming-Video nach einer vordefinierten Signaturenliste.**

1. Wählen Sie Streaming-Video und Streaming-Audio als Anwendungskategorien aus.
2. Setzen Sie die Bandbreite fest, die Sie für diese Anwendungskategorien bereitstellen möchten (z. B. 10 %).
3. Definieren Sie eine Regel, die dafür sorgt, dass alle Mitarbeiter für Streaming-Video und Streaming-Audio höchstens 10 % der Bandbreite erhalten (bestimmte Gruppen innerhalb von Abteilungen können eventuell ausgenommen werden, z. B. Mitarbeiter, die an Schulungen teilnehmen).
4. Sie können die Regel auch so definieren, dass sie für die normalen Bürozeiten gilt, aber nicht für die Mittagszeiten oder nach 6 Uhr abends.
5. Loggen Sie sich am Application Flow Monitor ein und vergewissern Sie sich mittels Echtzeit-Visualisierung, dass Ihre neue Regel greift.

## Unter dem Strich

High Performance-Plattform

+ Deep Packet Inspection

+ Intrusion Prevention

+ Application Intelligence, Anwendungskontrolle und -visualisierung

---

**Dell SonicWALL Next Generation Firewall**

## Performance, Schutz und Anwendungskontrolle

**Weitere Informationen**

- Laden Sie das Whitepaper „AimPoint Group: Anwendungskontrolle im Blickpunkt – Die 7 wichtigsten Funktionsanforderungen an eine effiziente Firewall" herunter
- Sehen Sie sich unser Video an.
- Laden Sie sich das Datenblatt herunter.

Wenn Sie uns Feedback zu diesem E-Book, anderen E-Books oder Whitepapers von Dell SonicWALL geben möchten, senden Sie eine E-Mail an folgende Adresse: feedback@sonicwall.com.

Weiterempfehlen

**Über Dell SonicWALL**

Dell™ SonicWALL™ bietet intelligente Netzwerksicherheits- und Datenschutzlösungen, mit denen Kunden und Partner ihre globalen Netzwerke dynamisch sichern, überwachen und skalieren können. Das weltweite Dell SonicWALL-Frühwarnsystem garantiert dabei ultraschnellen Schutz vor unterschiedlichsten Bedrohungen. Von Gartner und NSS Labs wird Dell SonicWALL als einer der Marktführer anerkannt. Weitere Informationen erhalten Sie auf der Website **www.sonicwall.com**.



SonicWALL