

# 10 gave dingen die je firewall moet doen

Een firewall die bedreigingen tegenhoudt is slechts het begin...

**SONICWALL**<sup>®</sup>

PROTECTION AT THE SPEED OF BUSINESS<sup>®</sup>

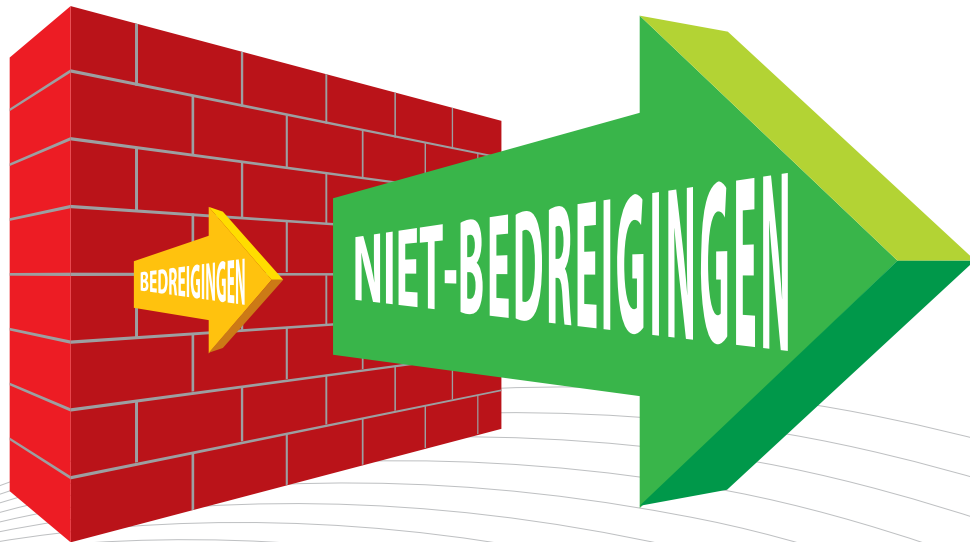
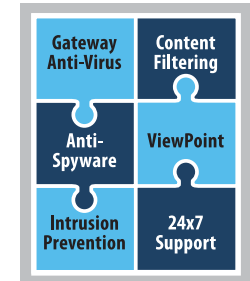
# Inhoud

Een volwassen firewall	1
De toepassingsfirewall	2
1e gave ding: Streaming video beheren	3
2e gave ding: Bandbreedtebeheer per groep	4
3e gave ding: Uitgaande webmail controleren	5
4e gave ding: Gebruik van toepassing forceren	6
5e gave ding: FTP-upload weigeren	7
6e gave ding: P2P-toepassingen onder controle houden	8
7e gave ding: Streaming-muziek beheren	9
8e gave ding: Prioriteit toekennen aan toepassingsbandbreedte	10
9e gave ding: Vertrouwelijke documenten blokkeren	11
10e gave ding: Verboden bestanden blokkeren en dit melden	12
Wanneer je dat bij elkaar optelt, heb je	13

# Een volwassen firewall

Traditionele firewalls concentreren zich op het blokkeren van simpele bedreigingen en indringers.

Bedrijfs-firewalls hebben Unified Thread Management (UTM) services toegevoegd, zoals antivirus, antispysware, intrusion prevention, content-filtering en zelfs enkele antispamservices voor een betere bescherming tegen bedreigingen.



Het meeste verkeer dat door een firewall komt, is niet gebaseerd op bedreigingen, maar zijn toepassingen en gegevens. Hierdoor ontstond de toepassingsfirewall, die gegevens en toepassingen die door de firewall komen, kan beheren en controleren.

*...maar het blokkeren van bedreigingen  
is slechts het begin*

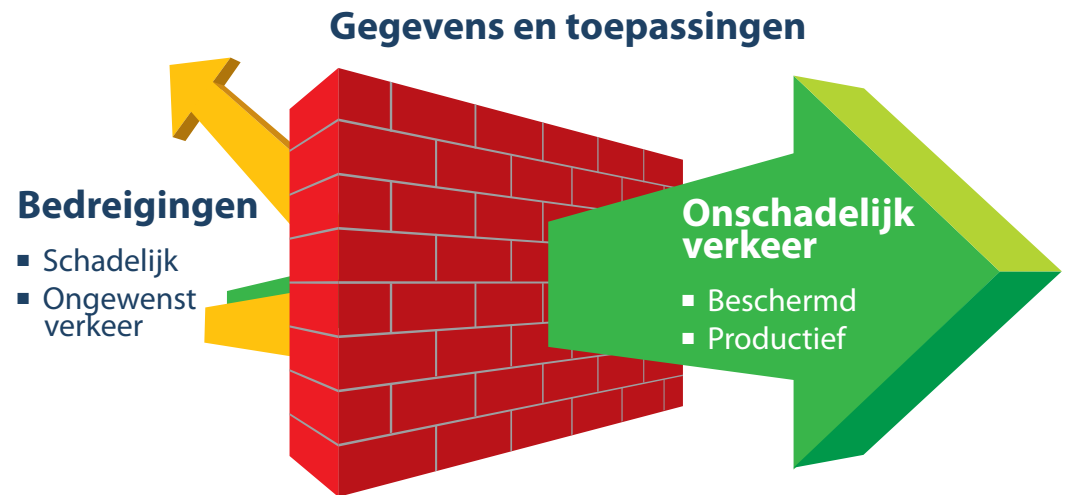
# De toepassingsfirewall

## Wat doet deze firewall?

Een toepassingsfirewall biedt bandbreedtebeheer en -controle, toegangscontroles op toepassingsniveau, controle van datalekage, beperkingen op de overdracht van specifieke bestanden en documenten en nog veel meer.

## Hoe werkt de firewall?

Met een toepassingsfirewall zijn aangepaste toegangscontroles mogelijk op basis van gebruiker, toepassing, schema of IP-subnetniveau. Daardoor kan een beheerder beleiden aanmaken die gelden voor alle toepassingen die toegang kunnen hebben en kan hij die voor het eerst ook echt beheren.



*Je kunt dus toepassingen en gegevens die door je firewall komen, klassificeren, controleren en beheren.*

# 1e gave ding: Streaming video beheren

Toegang tot sites met streaming video, zoals youtube.com is soms handig, maar wordt vaak misbruikt. De site blokkeren, kan werken, maar het zou beter zijn om de bandbreedte die aan streaming video-sites wordt gegeven te beperken.

## **Maak een beleid aan om streaming video te beperken**

- Gebruik de Deep Packet Inspection (DPI)-motor om te zoeken naar **HTTP Host = www.youtube.com** in de HTTP-header.
- Pas bandbreedtebeperkingen toe op het verkeer binnen die header.



The diagram shows a wide green horizontal bar on the left representing 'Gewenste streaming video-bandbreedte'. A grey funnel narrows this bar into a much thinner green horizontal bar on the right representing 'Geboden streaming video-bandbreedte'. Below the funnel, several thin grey lines fan out from the narrow bar towards the right, symbolizing the reduction in bandwidth.

**Gewenste streaming video-bandbreedte**

**Geboden streaming video-bandbreedte**

*Je kunt de **bandbreedte voor toepassingen** op bepaalde tijden van de dag beperken – bijvoorbeeld van 9.00 uur tot 17.00 uur.*

## 2e gave ding: Bandbreedtebeheer per groep

In het 1e gave ding hebben we bandbreedtebeperkingen toegepast voor video streaming-sites zoals youtube.com. Nu klagen je CEO en CFO dat de “zakelijke nieuwsvideo’s” die ze iedere dag bekijken te langzaam zijn. Je kunt de bandbreedtebeperkingen voor iedereen laten vieren, maar nu is er een betere oplossing: bandbreedtebeheer op groepsbasis.

### **Maak een beleid aan om streaming video niet te beperken voor het management**

- Pas dit beleid toe op de groep “management” die is geïmporteerd van uw LDAP-server.
- Gebruik de Deep Packet Inspection (DPI)-motor om te zoeken naar **HTTP Host = www.youtube.com** in de HTTP-header.
- Pas bandbreedtegarantie toe op het verkeer binnen die header.



# 3e gave ding: Uitgaande webmail controleren

Laten we aannemen dat je bestaande spambeveiliging een normale uitgaande e-mail die “Bedrijfsvertrouwelijk” bevat, kan opsporen en blokkeren.

Maar wat gebeurt er als een werknemer een web-mailservice gebruikt, zoals **Yahoo**<sup>®</sup> of **Gmail**<sup>®</sup> om “**Bedrijfsvertrouwelijke**” informatie te verzenden?

## **Maak een beleid aan om “Bedrijfsvertrouwelijke” e-mails te blokkeren**

- Deep Packet Inspection (DPI)-motor blokkeert **E-mail Body = “Bedrijfsvertrouwelijk”**.
- Blokkeer het bericht en **meld** de afzender dat het bericht “Bedrijfsvertrouwelijk” is.



Van: goeiegast@jouw\_bedrijf.com  
Aan: goeiegast@partner.com  
Onderwerp: Goedkeuring tijdkaart Jan,  
Ik ga akkoord met je tijdkaarten van deze week.  
Kees

Van: slechtegast@jouw\_bedrijf.com  
Aan: slechtegast@concurrent.com  
Onderwerp: Ontwerp routekaart  
Hier is de routekaart  
Jan 09 – Versie 7.0  
Dit document is **Bedrijfsvertrouwelijk**



# 4e gave ding: Gebruik van toepassing forceren



**Je baas:** Wil Internet Explorer (IE) 7.0 gebruiken als standaardbrowser.

**Jouw missie:** Ervoor zorgen dat alle bedrijfssystemen IE 7.0 gebruiken – en niets anders!

## Je mogelijke oplossingen

1. Controleer letterlijk de systemen van alle werknemers iedere dag op “Andere” browsers.
2. Stel een script op om ieders systeem te controleren op “Andere” browsers en zorg ervoor dat dit alle systemen iedere dag controleert.
3. Stel een beleid op in de toepassingsfirewall en maak je geen zorgen meer.

## Maak een “Ik heb wel wat beters te doen”-beleid

- Deep Packet Inspectie (DPI)-motor zoekt naar **Gebruikersagent = MSIE 7.0** in HTTP-header.
- Laat IE 7.0-verkeer toe en blokkeert andere browsers.

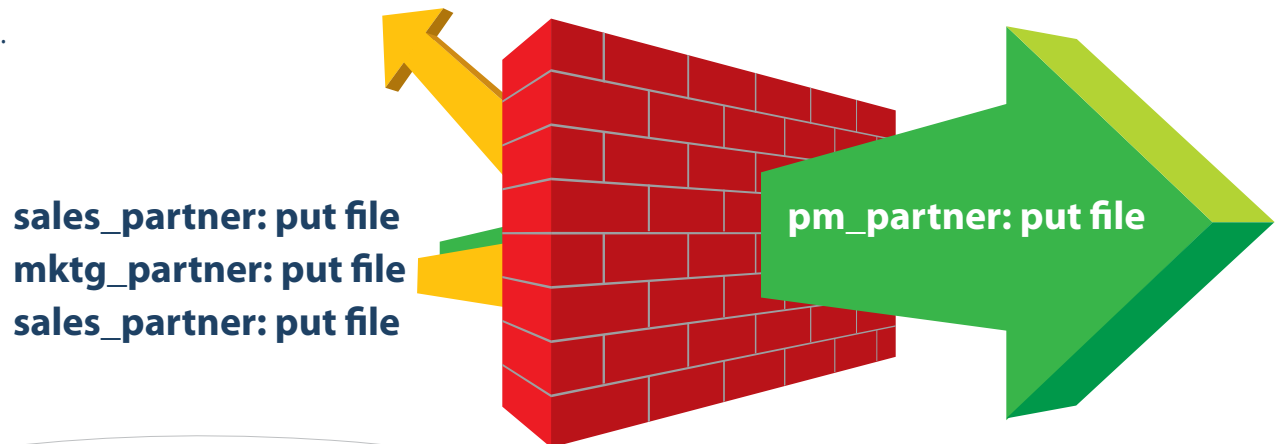


# 5e gave ding: FTP-upload weigeren

Je stelt een FTP-site op voor de uitwisseling van grote bestanden met één van je business-partners en je wilt zeker weten dat alleen de projectmanager en niemand anders bij de partner bestanden kan uploaden.

## Maak een beleid om FTP-uploads toe te staan, maar alleen voor bepaalde mensen

- Deep Packet Inspection (DPI)-motor zoekt naar **FTP Command = PUT**.
- DPI-motor zoekt naar **Naam geïdentificeerde gebruiker = "pm\_partner"**.
- Als beide waar zijn, is PUT toegestaan.



*Je kunt ook alle FTP-opdrachten weigeren die je "onnodig" vindt voor een bepaalde FTP-server.*

# 6e gave ding: P2P-toepassingen onder controle houden

**Probleem 1:** Peer-To-Peer (P2P)-toepassingen, zoals BitTorrent kunnen veel bandbreedte opeisen en allerlei schadelijke bestanden binnenhalen.

**Probleem 2:** Er worden onophoudelijk nieuwe P2P-toepassingen gemaakt of eenvoudige veranderingen aangebracht aan de bestaande P2P-toepassingen, zoals een ander versienummer.

## **Maak een beleid om P2P-toepassingen op te sporen**

Deep Packet Inspection (DPI)-motor zoekt naar een **P2P-toepassings**signatuur op de IP-signatuurlijst. ....



***P2P-toepassingen kunnen worden geblokkeerd  
of beperkt via op bandbreedte en tijd gebaseerde beperkingen***

# 7e gave ding: Streaming-muziek beheren

Sites met streaming audio en streaming radio gebruiken waardevolle bandbreedte, maar er bestaan wel legitieme bedrijfsredenen om dergelijke sites te openen. Er zijn twee manieren om met deze uitdaging aan te pakken.

## **Controle per website**

**Maak een lijst met streaming audio sites die je wilt beheren**

**Maak een beleid om streaming audio sites te detecteren**

- Gebruik de Deep Packet Inspection (DPI)-motor om te zoeken naar **HTTP Host = Blokkeringslijst van Streaming Audio sites** in de HTTP-header.

## **Controle per bestandsextensie**

**Maak een lijst met audiobestandsextensies die je wilt beheren**

**Maak een beleid om streaming audio content te detecteren**

- Gebruik de Deep Packet Inspection (DPI)-motor om te zoeken naar **File extension = Blokkeringslijst van Streaming Audio extensies** in de HTTP-header.

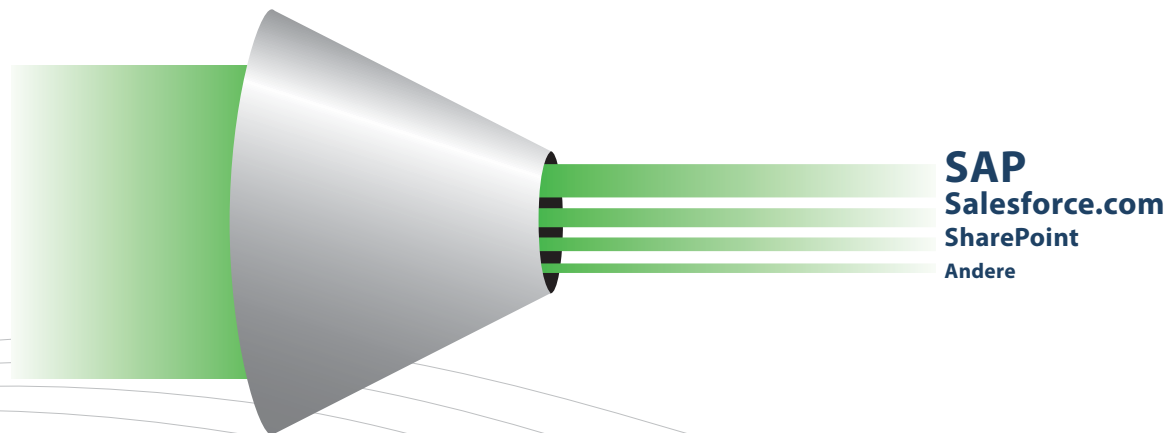
*Zodra ze zijn “gedetecteerd” kan je de streaming audio blokkeren of alleen de bandbreedte ervan beheren.*

# 8e gave ding: Prioriteit toekennen aan toepassings-bandbreedte

Vandaag de dag zijn veel **missie-kritieke** toepassingen zoals SAP®, Salesforce.com® en SharePoint® internet-gebaseerd of lopen over geografisch verspreide netwerken. Door ervoor te zorgen dat deze **toepassingen** met voorrang de netwerkbandbreedte krijgen die ze nodig hebben om te kunnen werken, kan de bedrijfs**productiviteit** verbeteren.

## **Maak een beleid om bandbreedteprioriteit te geven aan de SAP-toepassing.**

- Deep Packet Inspection (DPI)-motor zoekt naar de **toepassingssignatuur of -naam**.
- Ken een hogere bandbreedteprioriteit toe aan de SAP-toepassing



***De toepassingsprioriteit kan op datum gebaseerd zijn  
(bijvoorbeeld prioriteit voor einde-kwartaal bij salestoepassingen)***

# 9e gave ding: Vertrouwelijke documenten blokkeren

In sommige bedrijven gaan uitgaande e-mails niet door het e-mailbeveiligingssysteem of controleert dat systeem de inhoud van e-mailbijlagen niet. In beide gevallen kunnen **“bedrijfsvertrouwelijke”** bijlagen het bedrijf makkelijk verlaten.

Aangezien uitgaand netwerkverkeer door je firewall gaat, kan je deze “gegevens-in-beweging” opsporen en blokkeren.

## **Maak een beleid aan om e-mailbijlagen met het watermerk “Bedrijfsvertrouwelijk” te blokkeren**

- Deep Packet Inspection (DPI)-motor zoekt naar  
E-mail-inhoud = **“Bedrijfsvertrouwelijk”** en ook naar  
E-mail-inhoud = **“Bedrijfseigendom”** en ook naar  
E-mail-inhoud = **“Privé-eigendom”** en ook naar



*Dit kan ook worden gedaan voor FTP-content!*

# 10e gave ding: Verboden bestanden blokkeren en dit melden



## Kan je firewall de volgende zaken blokkeren?

- Een EXE-bestand dat van een webpagina wordt gedownload
- Een EXE-bestand als e-mailbijlage
- Een EXE-bestand dat wordt overgedragen via FTP

## Hoe zit het met PIF-, SRC- of VBS-bestanden?

### Veiligheidsrisico

**Activiteit:** U probeert een bestand met een verboden bestandsextensie (.exe, .pif, .src of .vbs) te downloaden of te ontvangen.

**Actie:** Volgens het bedrijfsbeleid is dit bestand geblokkeerd.

**Meer info:** Raadpleeg het gedeelte over de veiligheid van het bedrijfsintranet voor een complete lijst van de bestanden die verboden zijn.

## Maak een lijst met verboden bestandsextensies

## Maak een beleid aan om verboden bestandsextensies te blokkeren

- Deep Packet Inspection (DPI)-motor zoekt naar **Bestandsextensie in HTTP, E-mailbijlage of FTP = Verboden bestandsextensies.**

## Stuur melding als bestand wordt geblokkeerd

# Wanneer je dat bij elkaar optelt



**Firewall met hoge prestaties  
+ Unified Threat Management  
+ Application Firewall**  

---

**SonicWall netwerkbeveiliging**

***Prestaties, beveiliging en zeer nauwkeurige controle***



### Hoe kom ik meer te weten?

- Voor een vergelijking van de SonicWall NSA-modellen met de Application Firewall:  
[http://www.sonicwall.com/us/products/NSA\\_Series.html](http://www.sonicwall.com/us/products/NSA_Series.html)
- Om het informatieblad te downloaden:  
[http://www.sonicwall.com/downloads/NSA\\_Series\\_DS\\_US.pdf](http://www.sonicwall.com/downloads/NSA_Series_DS_US.pdf)
- Praktische voorbeelden van de Application Firewall in productvoorbeelden:  
[http://www.sonicwall.com/downloads/SonicOS\\_Application\\_Firewall\\_Practical\\_Examples\\_Guide\\_technote.pdf](http://www.sonicwall.com/downloads/SonicOS_Application_Firewall_Practical_Examples_Guide_technote.pdf)
- Gebruiksaanwijzing Application Firewall:  
[http://www.sonicwall.com/downloads/Application\\_Firewall\\_5.1e\\_Feature\\_Module.pdf](http://www.sonicwall.com/downloads/Application_Firewall_5.1e_Feature_Module.pdf)

Voor feedback op dit e-book of andere SonicWALL e-books of whitepapers kunt u een e-mail sturen naar [feedback@sonicwall.com](mailto:feedback@sonicwall.com).

### Info over SonicWALL

SonicWALL® is een erkend leider in veelomvattende oplossingen voor informatieveiligheid. De SonicWALL-oplossingen integreren dynamisch intelligente diensten, software en hardware die de risico's, kosten en complexiteit van bedrijfsnetwerken met hoge prestaties regelen. Bezoek voor meer informatie de website van het bedrijf op [www.sonicwall.com](http://www.sonicwall.com).