10 Cool Things Your Firewall Should Do

A firewall that blocks threats is only the beginning…

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS®

Table of Contents

SONICWALL ®

PROTECTION AT THE SPEED OF BUSINESS®

The Firewall Grows Up

Traditional firewalls focus on blocking simple threats and intrusions.

Business grade Firewalls have added Unified Threat Management (UTM) services such as anti-virus, anti-spyware, intrusion prevention, content filtering and even some anti-spam services to enhance to threat protection.

Gateway Anti-Virus	Content Filtering
Anti-Spyware	ViewPoint
Intrusion Prevention	24x7 Support
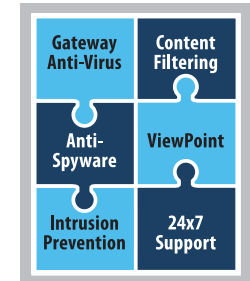
Most traffic passing through a Firewall is not threat-based, but is instead applications and data. This gave rise to the Application Firewall which can manage and control data and applications that pass through the Firewall.

THREATS

NON-THREATS

...but blocking threats

is just the beginning

1

The Application Firewall

What does it do?

An Application Firewall provides bandwidth management and control, application level access controls, data leakage control functionality, restrictions on the transfer of specific files and documents, and much more.

How does it work?

An Application Firewall allows custom access controls based upon user, application, schedule or IP subnet level. This allows an administrator the ability to create polices that address the full range of applications that are available for access and for the first time truly manage them.

Data and Applications

Threats
- Compromised
- Wasteful

Good
- Protected
- Productive
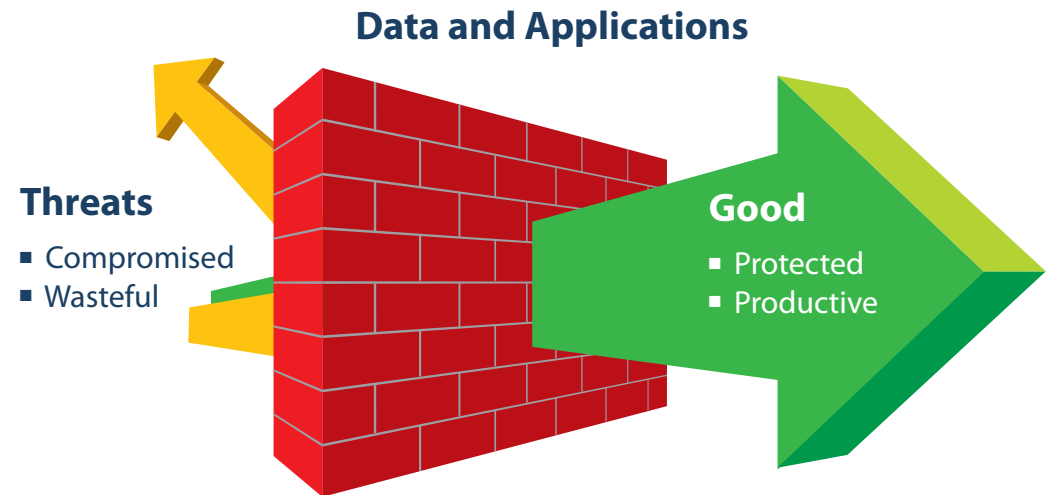
Allows you to classify, control and manage applications and data that pass through your firewall.

1st Cool Thing: Managing Streaming Video

Access to streaming video sites, such as youtube.com is sometimes useful but often abused. Blocking the site might work, but the best answer could be to limit the bandwidth given to streaming video sites.

Create a Policy to limit streaming video
- Use the Deep Packet Inspection (DPI) engine to look for **HTTP Host = www.youtube.com** in HTTP header
- Apply bandwidth restrictions to traffic with that header

Streaming Video Bandwidth Desired　　　　　　**Streaming Video Bandwidth Provided**

You can limit bandwidth for applications

over specified times of day – say from 9:00am to 5:00pm

2nd Cool Thing: Per Group Bandwidth Management

In the 1st Cool Thing, we applied bandwidth restrictions for streaming video sites like youtube.com. Now your CEO and CFO are complaining that the "business news videos" they review each day are too slow. You could ease off on the bandwidth restrictions for everyone, but now there is a better answer—group-based bandwidth management.

Create a Policy to not limit streaming video for the executives
- Apply this Policy to the "executive" group imported from your LDAP server
- Use the Deep Packet Inspection (DPI) engine to look for **HTTP Host = www.youtube.com** in HTTP header
- Apply bandwidth guarantee to traffic with that header

Streaming Video Bandwidth Desired

Executive Streaming Video Bandwidth Provided

Everyone Else's Streaming Video Bandwidth Provided

3rd Cool Thing: Web-mail and Data Loss

Let's assume your existing anti-spam protection can detect and block a normal outbound e-mail that contains "Company Confidential" information.

But, what if an employee uses a Web-mail service such as **Yahoo®** or **Gmail®** to **send out** a **"Company Confidential"** information?

Create a Policy to block "Company Confidential" e-mail
- Deep Packet Inspection (DPI) engine looks for **E-mail Body = "Company Confidential"**
- Block message and **notify** the sender that the message is "Company Confidential"

GO

From: goodguy@your_company.com
To: goodguy@partner.com
Subject: Time Card Approval Jim,

I approve your time card hours for this week.
Joe

From: badguy@your_company.com
To: badguy@competitor.com
Subject: Design road map
Here is the Roadmap
Jan 09 – Release 7.0
This document is **Company Confidential**

STOP

4th Cool Thing: Application Use Enforcement

Your Boss: Wants to use Internet Explorer (IE) 7.0 as the standard browser.

Your Mission: Ensure all company systems are using IE 7.0—nothing else!

Your Possible Solutions

1. Physically check everyone's system each day for "Foreign" browsers

2. Set-up some type of script to check everyone's system for "Foreign" browsers and make sure it checks everyone's system everyday

3. Set up a policy in the Application Firewall and stop worrying

Create a "I've got better things to do" Policy

- Deep Packet Inspection (DPI) engine looks for **User Agent = MSIE 7.0** in HTTP header
- Allows IE 7.0 traffic and blocks other browsers

5th Cool Thing: Deny FTP Upload

You set up an FTP site for the exchange of large files with one of your business partners and you want to make sure that only the project manager at the partner and no one else can upload files.

Create a Policy to allow FTP uploads, but only for certain people

- Deep Packet Inspection (DPI) engine looks for **FTP Command = PUT**
- DPI engine looks for **Authenticated User Name = "pm_partner"**
- If both are True then allow PUT

sales_partner: put file
mktg_partner: put file
sales_partner: put file

pm_partner: put file
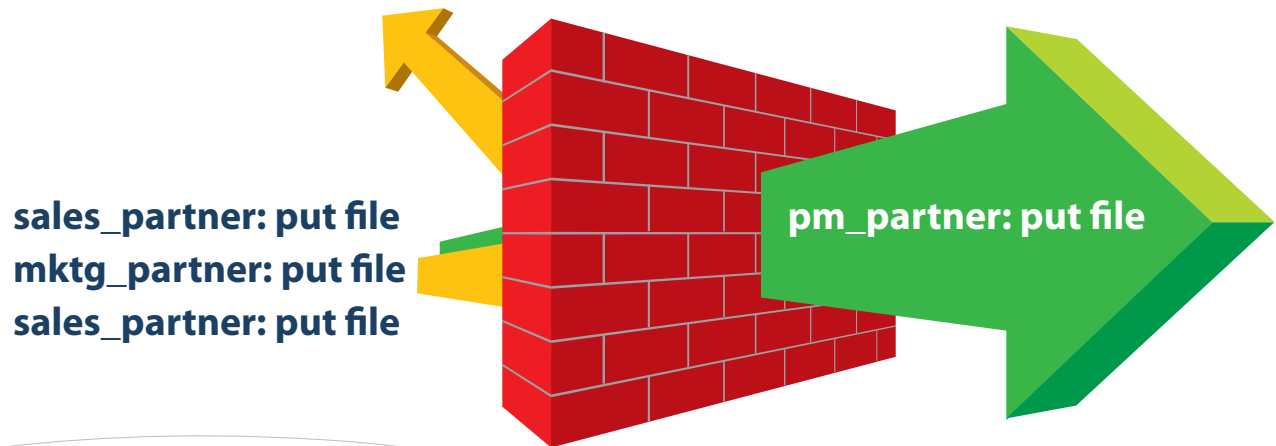
You can also *disallow any FTP commands*
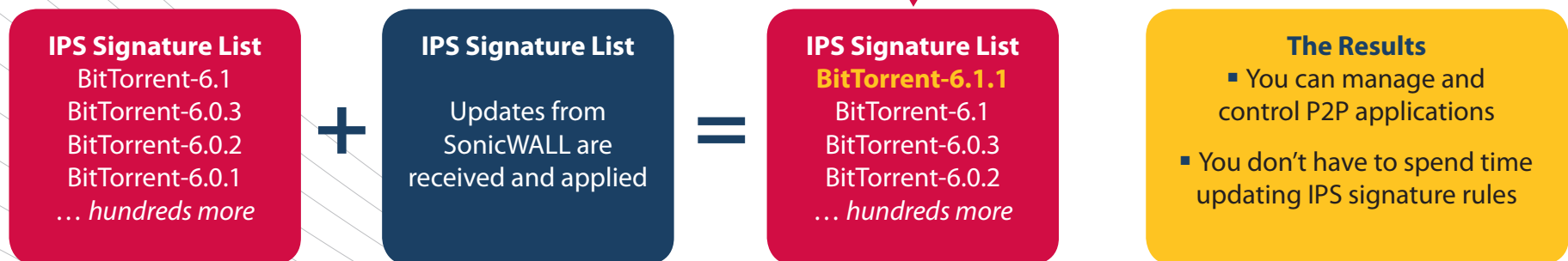*you think are "unnecessary" for a given FTP server*

6th Cool Thing: Keep P2P Apps Under Control

Problem 1: Peer-To-Peer (P2P) applications such as BitTorrent can steal bandwidth and bring with them all kinds of mischievous files.

Problem 2: The creation of new P2P applications or simple changes to the existing P2P applications, like a version number changes, happen all the time.

Create a Policy to detect P2P applications
Deep Packet Inspection (DPI) engine looks for a **P2P Application signature on the IPS signature list**

IPS Signature List
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
BitTorrent-6.0.1
… *hundreds more*

+

IPS Signature List

Updates from SonicWALL are received and applied

=

IPS Signature List
BitTorrent-6.1.1
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
… *hundreds more*

The Results
- You can manage and control P2P applications
- You don't have to spend time updating IPS signature rules

P2P applications can be blocked or just limited through bandwidth and time-based restrictions

7th Cool Thing: Manage Streaming Music

Streaming audio sites and streaming radio sites consume precious bandwidth, but there are legitimate business reasons to access such sites. There are two ways to manage this challenge.

Control by Web Site

Create a list of streaming audio sites you'd like to manage

Create a Policy to detect streaming audio sites

- Use the Deep Packet Inspection (DPI) engine to look for **HTTP Host = Streaming Audio Site block list** in HTTP header

Control by File Extension

Create a list of audio file extensions you'd like to manage

Create a Policy to detect streaming audio content

- Use the Deep Packet Inspection (DPI) engine to look for **File extension = Streaming Audio Extensions block list** in HTTP header

Once "detected"
you can block or just bandwidth manage
the streaming audio.

8th Cool Thing: Prioritize Application Bandwidth

Today many **mission-critical** applications, such as SAP®, Salesforce.com® and SharePoint®, are cloud-based or they are running across geographically dispersed networks. Ensuring these **applications** have priority to get the network bandwidth they need to operate can improve business **productivity**.

Create a Policy to give bandwidth priority to the SAP application
- Deep Packet Inspection (DPI) engine looks for **the application signature or application name**
- Assign the SAP application a higher bandwidth priority

SAP
Salesforce.com
SharePoint
Others
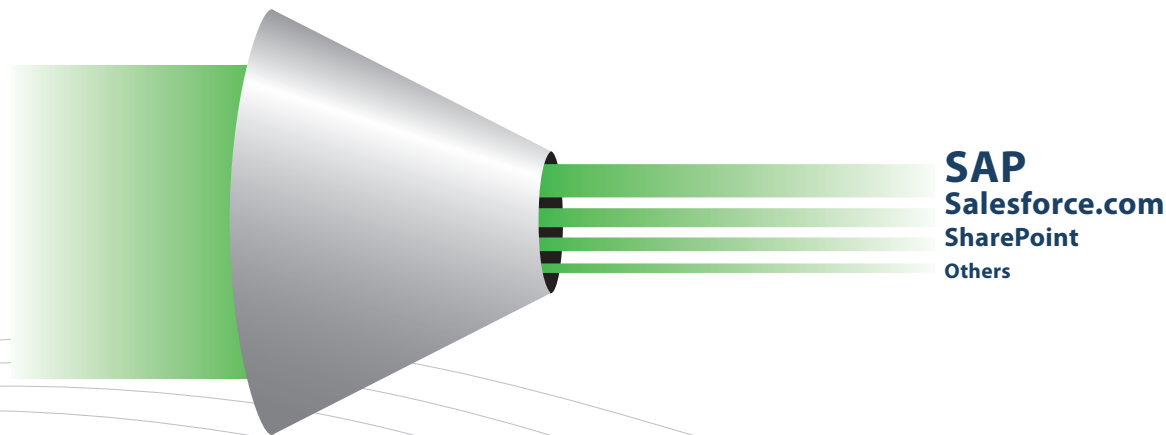
Application priority can be date based
(think end-of-quarter priority for sales applications)

9th Cool Thing: Blocking Confidential Documents

In some companies, outbound e-mail does not pass through their E-mail Security system or that system does not check the content of e-mail attachments. In either case **"Company Confidential"** attachments can easily leave the organization.

Since outbound network traffic goes through your firewall, you can detect and block this "data-in-motion".

Create a Policy to block e-mail attachments which contain the "Company Confidential" watermark
- Deep Packet Inspection (DPI) engine looks for
  E-mail Content = "Company Confidential" and also
  E-mail Content = "Company Proprietary" and also
  E-mail Content = "Private Proprietary" and …

This can also be done for **FTP-based content!**

10th Cool Thing: Block Forbidden Files and Notify

Email

Bad .pif

FTP

Bad .vbs

Website

DOWNLOAD

Bad .exe
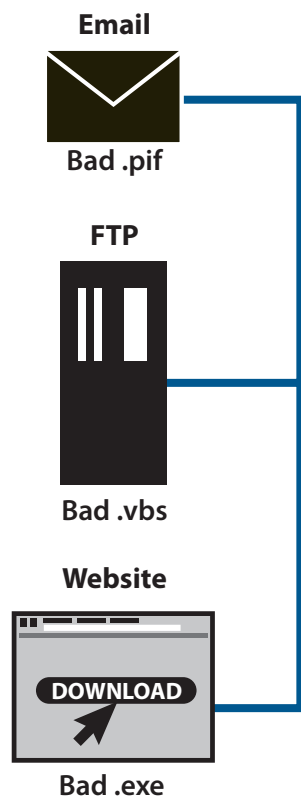
Can your Firewall block any of the following?

- An EXE file from being downloaded from a web page
- An EXE file as an e-mail attachment
- An EXE file from being transferred via FTP

How about PIF, SRC or VBS files?

SonicWALL NSA with
Application Firewall

Create a Forbidden File Extensions list

Create a Policy to block forbidden file extensions

- Deep Packet Inspection (DPI) engine looks for **File Extension in HTTP, Email Attachment or FTP = Forbidden File Extensions**

If file blocked, send Notification

Security Risk

Activity: You are attempting to download or receive a file with a forbidden file extension (.exe, .pif, .src or .vbs).

Action: Per corporate policy, this file has been blocked.

More info: Please refer to the Security section of the corporate intranet for a complete list of the files which are forbidden.

When You Add it All Up

High Performance Firewall

\+ Unified Threat Management

\+ Application Firewall

SonicWALL Network Security Appliance

Performance, Protection and Pin-Point Control

How Can I Learn More?
- For a comparison of the SonicWALL NSA models which include the Application Firewall
- To download the datasheet
- Practical examples of the Application Firewall with product examples
- Application Firewall user guide

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an e-mail to **feedback@sonicwall.com.**

Forward to a Friend

About SonicWALL
SonicWALL® is a recognized leader in comprehensive information security solutions. SonicWALL solutions integrate dynamically intelligent services, software and hardware that engineer the risk, cost and complexity out of running a high-performance business network. For more information, visit the company Web site at **www.sonicwall.com**.