10 Cool Things Your Firewall Should Do

Extending beyond blocking network threats to protect, manage and control application traffic

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS®

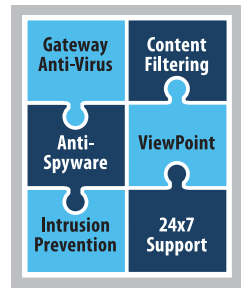
Table of Contents

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS®

The Firewall Grows Up

Traditional firewalls focus on blocking simple threats and intrusions.

Enterprise-class Firewalls have added services such as anti-virus, anti-spyware, intrusion prevention, content filtering and even some anti-spam services to enhance to threat protection.



Most traffic passing through a Firewall is not threat-based, but is instead applications and data. This gave rise to Application Intelligence and Control which can protect, manage and control data and applications that pass through the Firewall.

...but blocking traditional network threats is just the beginning

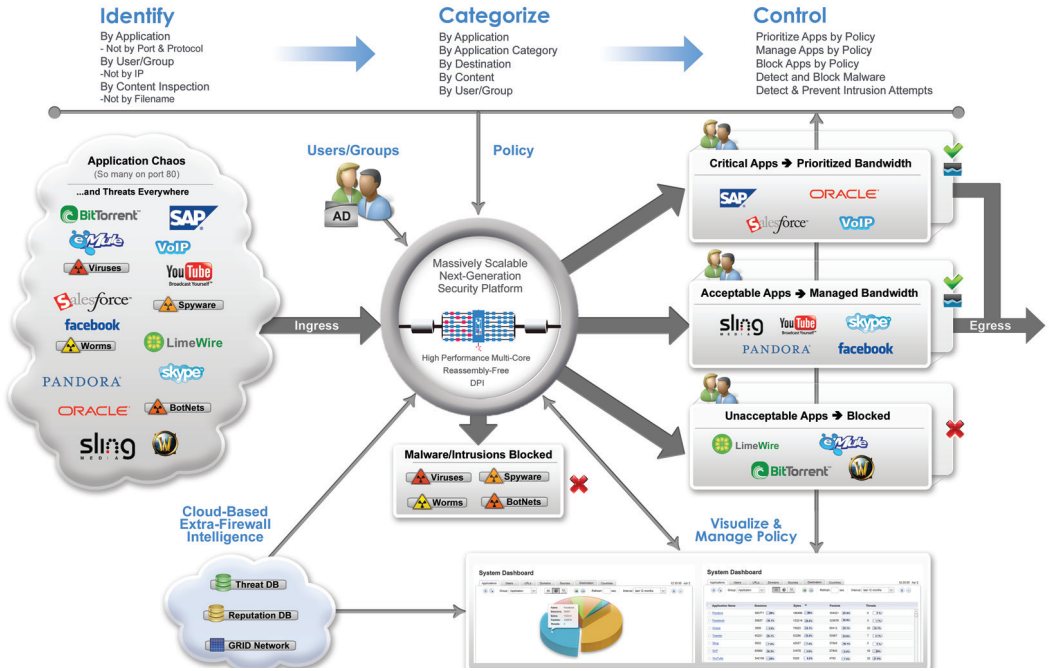
SonicWALL Application Intelligence and Control

What does it do?

Application Intelligence and Control not only blocks traditional network-layer threats, but also extend protection, management, and control over application-layer traffic, enhancing compliance, content filtering and data leakage prevention. It can dedicate throughput for mission-critical or latency-sensitive applications like Live Meeting and restrict productivity-draining applications like YouTube based on user group, time of day, or mobile device type.

How does it work?

Leveraging high-performance Reassembly-Free Deep Packet Inspection, it can identify and control unauthorized browsers, Web 2.0 sites, IM clients, and EXE, PIF, SRC or VBS files—as well as dynamically evolving P2P applications like BitTorrent. Continuously and automatically updated with an industry-leading 1,100+ unique applications, Application Intelligence can identify and control applications traffic regardless of port, protocol, platform or even SSL encryption*. *Optional DPI SSL feature.

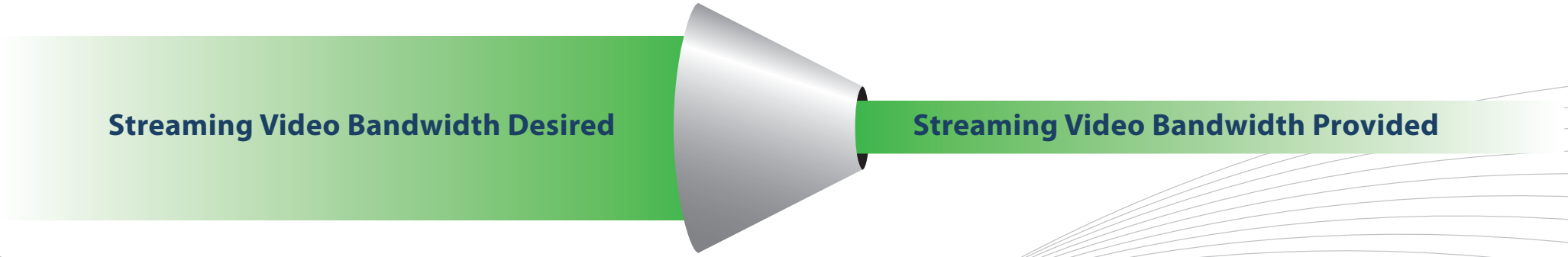


1st Cool Thing: Managing Streaming Video

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 applications

- Deep Packet Inspection (DPI) engine uses pre-defined streaming video application signatures from the application signature list
- Apply bandwidth restrictions to traffic with that header



*You can **limit bandwidth for applications***

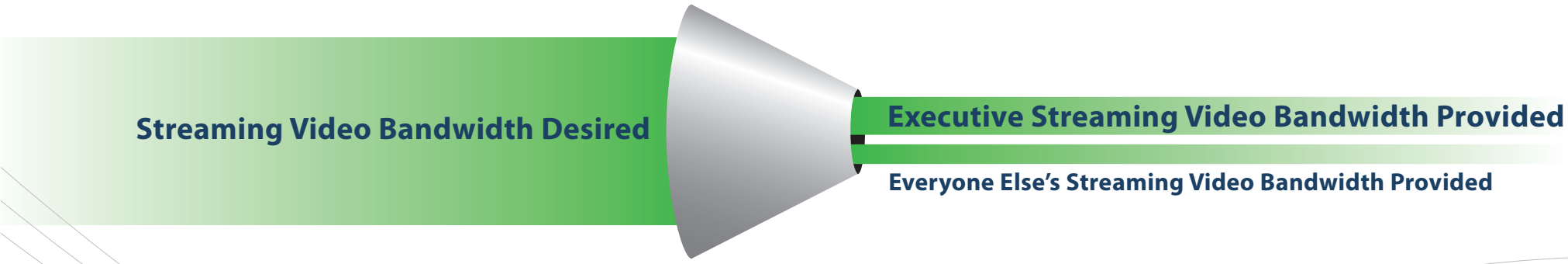
over specified times of day – say from 9:00am to 5:00pm

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
- Deep Packet Inspection (DPI) engine uses pre-defined streaming video application signatures from the application signature list
- Apply bandwidth guarantee to traffic with that header



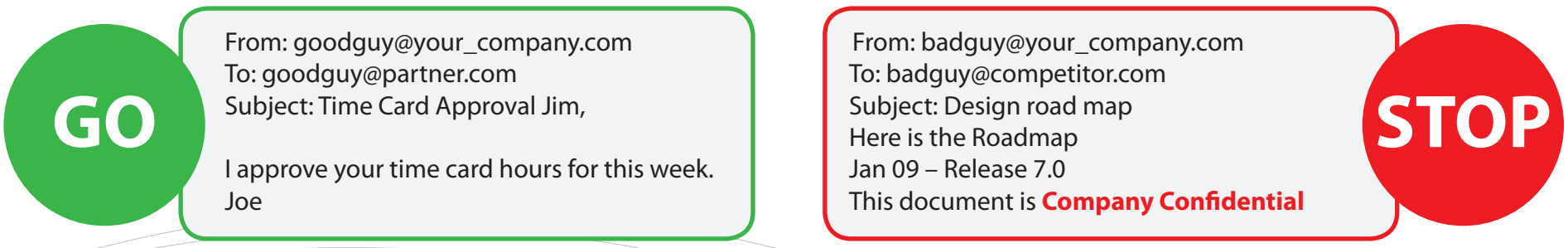
3rd Cool Thing: Web-mail and Data Loss

Let's assume your existing anti-spam protection can detect and block a normal outbound email 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" email

- Deep Packet Inspection (DPI) engine looks for **Email Body = "Company Confidential"**
- Block message and **notify** the sender that the message is "Company Confidential"



4th Cool Thing: Application Use Enforcement

IE 7.0

Your Boss: Wants employees to stop using the IE6 (Internet Explorer 6) Web browser and upgrade to IE7

Your Mission: Ensure all employees launching IE6 are automatically redirected to the IE7 download site, and restricted from all other Web access over IE6

IE 6.0

Your Possible Solutions

1. Physically check everyone's system each day for IE6 browsers
2. Set up some type of script to check everyone's system for IE6 browsers and make sure it checks everyone's system everyday
3. Set up a policy with Application Intelligence and stop worrying

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

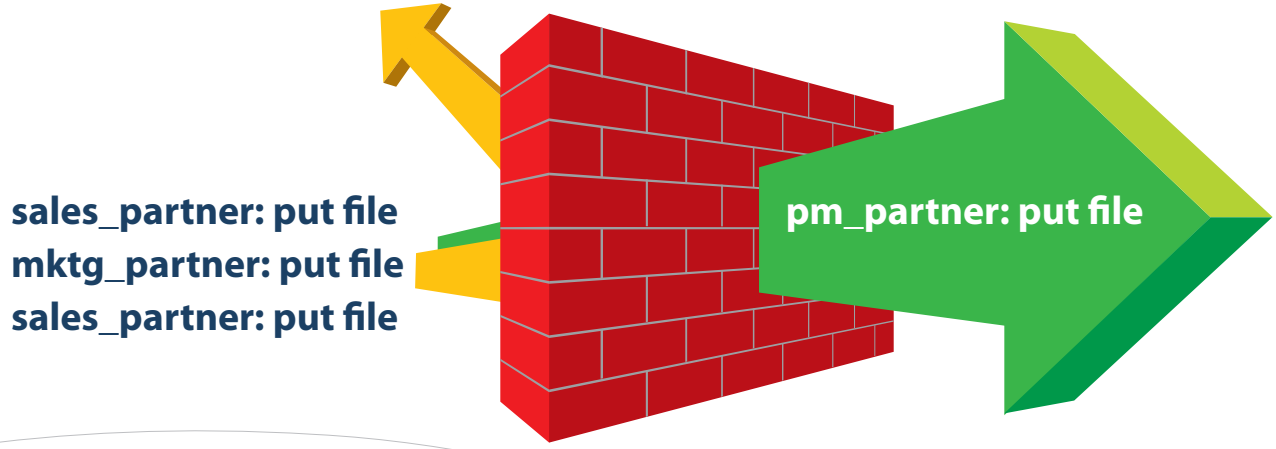
- The Deep Packet Inspection (DPI) engine looks for **User Agent = IE 6.0** in the HTTP header
- Redirects IE6 users to the IE7 download site, while blocking access over IE6 to any other Web sites

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



You can also disallow any FTP commands you think are "unnecessary" for a given FTP server

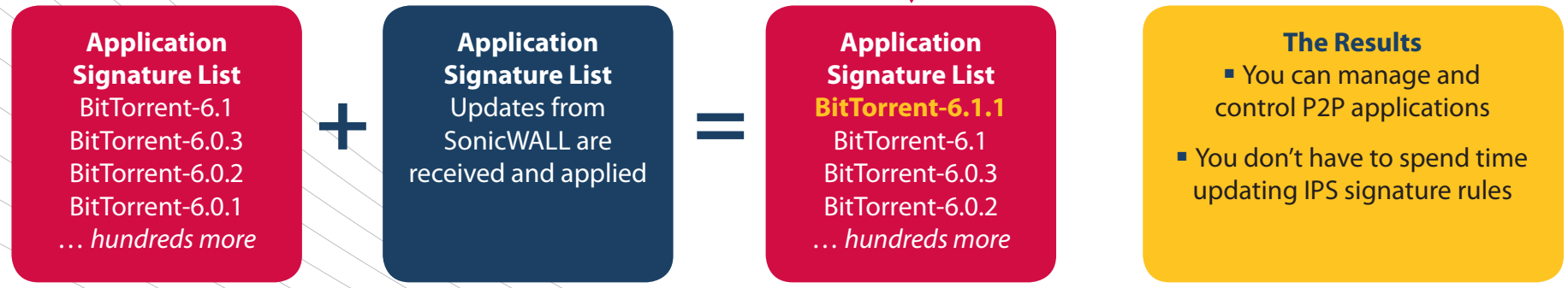
6th Cool Thing: Keep P2P Apps Under Control

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 uses pre-defined P2P application signatures from the application signature list



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

7th Cool Thing: Manage Streaming Audio

Streaming media application 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.

PANDORA®

last.fm

Control by Predefined Signature List

Create a Policy to limit streaming audio applications

- Deep Packet Inspection (DPI) engine looks for a **Streaming Audio Application signature on the application signature list.**
- Apply bandwidth restrictions to traffic with that header
- Deep Packet Inspection (DPI) engine uses pre-defined streaming audio application signatures from the application signature list

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

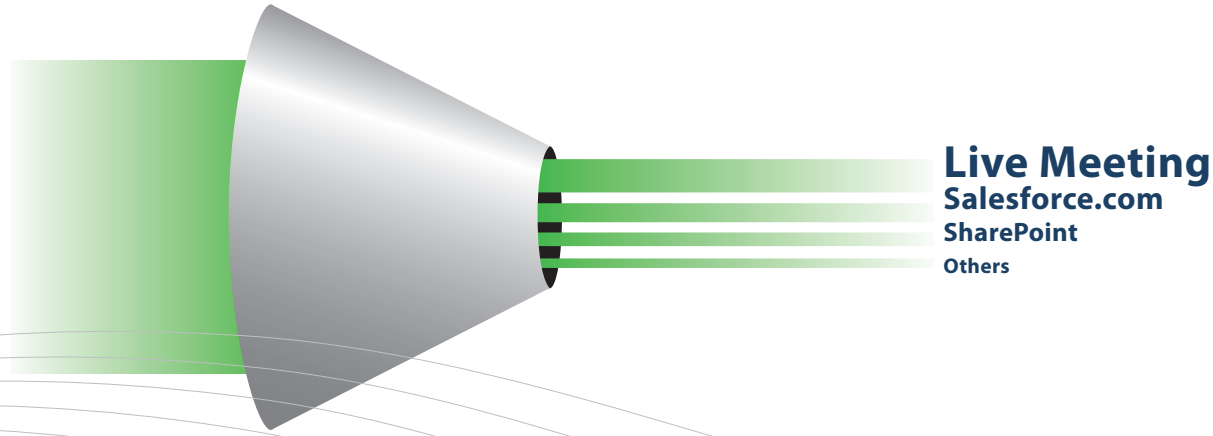
the streaming audio.

8th Cool Thing: Prioritize Application Bandwidth

Today many **mission-critical** applications, such as Live Meeting, 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 Live Meeting application

- Deep Packet Inspection (DPI) engine looks for **the application signature or application name**
- Assign the Live Meeting application a higher bandwidth priority



Application priority can be date based

(think end-of-quarter priority for sales applications)

9th Cool Thing: Blocking Confidential Documents

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

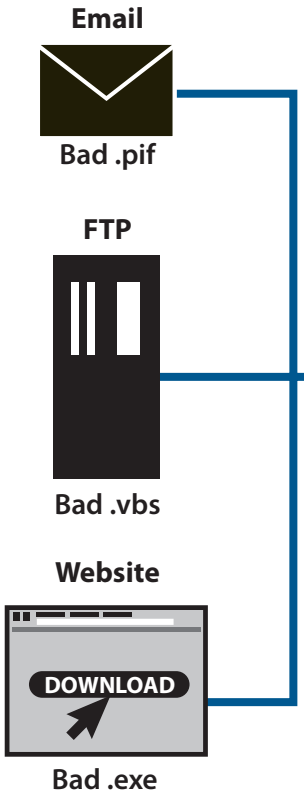
Since outbound network traffic goes through your firewall, you can detect and block this "data-in-motion".

Create a Policy to block email attachments which contain the "Company Confidential" watermark

- Deep Packet Inspection (DPI) engine looks for
  Email Content = "Company Confidential" and also
  Email Content = "Company Proprietary" and also
  Email Content = "Private Proprietary" and …

This can also be done for FTP-based content!

10th Cool Thing: Block Forbidden Files and Notify



Can your Firewall block any of the following?

- An EXE file from being downloaded from a Web page (HTTP/HTTPS)
- An EXE file as an email attachment
- An EXE file from being transferred via FTP

How about PIF, SRC or VBS files?

SonicWALL NSA with Application Intelligence and Control

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.

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/HTTPS, Email Attachment or FTP = Forbidden File Extensions**

If file blocked, send Notification

When You Add it All Up

High Performance Platform

+ Deep Packet Inspection

+ Application Intelligence and Control

SonicWALL Network Security Appliance

Performance, Protection and Application Control

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS®

How Can I Learn More?

- Comparison of the SonicWALL NSA models which include Application Intelligence
- Download the datasheet
- Practical examples of the Application Intelligence with product examples
- Application Intelligence and Control user guide

For feedback on this e-book or other SonicWALL e-books or whitepapers, please send an email 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**.

SonicWALL's line-up of dynamic security solutions

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com