11 cool things your firewall should do

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

Table of contents

The firewall grows up

Traditional stateful packet inspection firewalls focus on blocking network layer threats by evaluating the ports and protocols used by network layer traffic. The latest Next-Generation Firewalls utilize deep packet inspection to scan the entire packet payload to provide advanced intrusion prevention, anti-malware, content filtering and anti-spam. Many applications are delivered over the web sharing common ports and HTTP or HTTPS protocols. This effectively leaves traditional firewalls blind to these applications and unable to prioritize productive and secure versus unproductive and potentially insecure traffic. Next-Generation Firewalls provide insight into the applications themselves, providing a critical capability for networking professionals.

With the proliferation of cloud computing and Web 2.0 technologies, firewalls now have another challenge to contend with—application control.

What does Dell SonicWALL Application Intelligence and Control do?

Dell™ SonicWALL™ firewalls allow you to identify and control all of the applications being used on your network. This additional control enhances compliance and data leakage prevention by identifying applications based on their unique signatures rather than ports or protocols.

This is accomplished by visualizing application traffic to determine usage patterns and then creating granular policies for applications, users or even groups of users, as well as time of day and other variables, for flexible control that can fit any network requirement.

Allocate bandwidth for mission-critical or latency-sensitive applications.

How does Dell SonicWALL Application Intelligence and Control work?

By utilizing an extensive, constantly growing and automatically updated database of application signatures, Dell SonicWALL identifies applications based on their "DNA", rather than less unique attributes, such as source port, destination port or protocol type.

For example, you can allow instant messaging, but block file transfer or allow Facebook access, but block access to Facebook-based games. These controls are available for all SSL traffic as well, which must be inspected just like unencrypted connections. And you can visualize the results of your controls easily, allowing you to fine tune application usage and optimize network bandwidth.

Control categories of applications, individual applications, and specific features within applications.

1st cool thing:

Control the applications allowed on the network

You want to make sure all of your employees are using the latest version of Internet Explorer. Your mission is to ensure all employees launching IE6 or IE7 are automatically redirected to the IE8 download site and restricted from all other Web access. Your possible solutions include:

- Physically check every system each day for the Web browser version
- Write a custom script to automatically check browser versions
- Set up a policy with Dell SonicWALL Application Intelligence and Control—and stop worrying

Create a policy to redirect IE6 or IE7 users to download the latest IE browser, and block Internet access for IE6 or IE7

1. The Deep Packet Inspection (DPI) engine looks for User Agent = IE 6.0 or User Agent = IE 7.0 in the HTTP header
2. The policy redirects IE6 or IE7 users to the IE8 download site, while blocking access for IE6 or IE7 to any other Web sites

Application visualization lets you determine what browsers are being used before you create the policy.

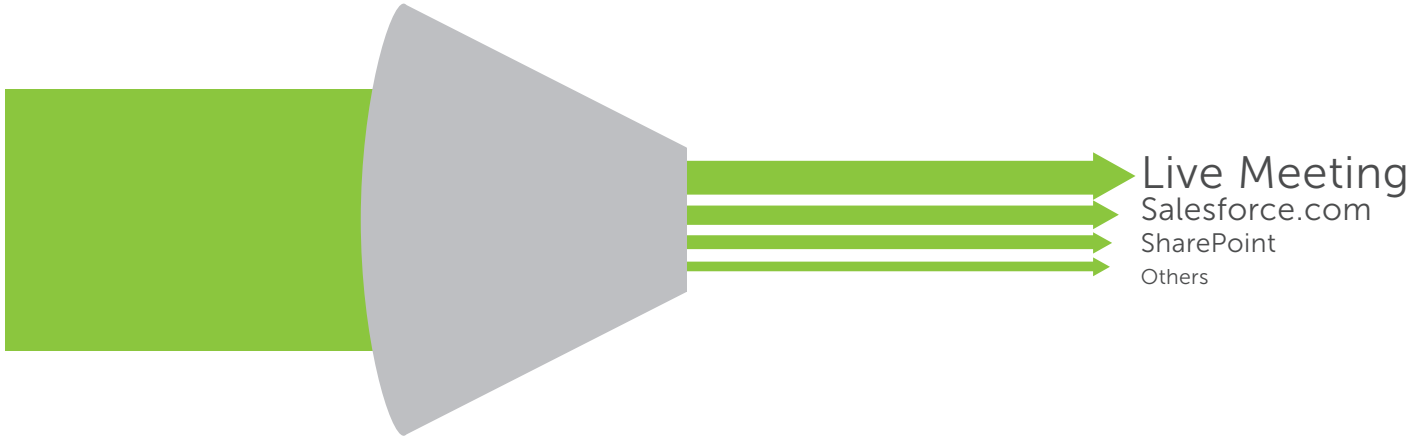
2nd cool thing:

Manage the bandwidth for critical applications

Many mission-critical applications, such as Live Meeting, Salesforce.com® and SharePoint®, are cloud-based, or run across geographically dispersed networks. Ensuring that these applications have priority over unproductive Web surfing improves business productivity.

Create a policy to give bandwidth priority to the Live Meeting application

1. The Deep Packet Inspection (DPI) engine looks for the application signature or application name
2. Assign the Live Meeting application a higher bandwidth priority



Application priority can be date-based (think end-of-quarter priority for sales applications).

3rd cool thing:

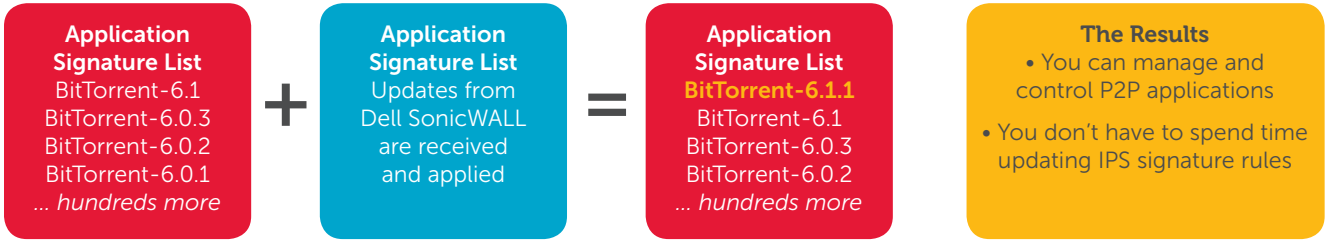
Block peer-to-peer applications

Unproductive peer-to-peer (P2P) applications such as BitTorrent are often used to download unlicensed versions of copyrighted media, and can quickly consume bandwidth or transmit malware. However, the creation of new P2P applications, or simple changes (e.g., version numbers) to the existing P2P applications happen all the time so it is difficult to manually block any single P2P application.

Dell SonicWALL continuously updates the application intelligence and control database to add new P2P apps as soon as they are available. Now you can simply create one policy to block all P2P apps going forward.

Create a policy to block the use of P2P applications

1. The Deep Packet Inspection (DPI) engine uses pre-defined P2P application signatures from the application signature list
2. Choose the P2P applications from the predefined signature list
3. Apply the policy to all users
4. Block P2P applications through bandwidth and time-based restrictions



4th cool thing:

Block unproductive components of applications

Social networking applications such as Facebook, Twitter and YouTube have become new channels of communications for individuals and for companies. While it might be counterproductive to block all social networking applications, you may want to control how they can be used in the workplace.

For example, you may want to let marketing personnel update the company's Facebook page, but not allow them to play Facebook games like Farmville or Mafia Wars. With application intelligence and control, you can create a policy to allow access to Facebook, but block games.

Create a policy to allow Facebook, but block Facebook games

1. Select "All" users
2. Select Facebook games applications as a category
3. Create a single rule to "Block" all users from accessing games within Facebook

You could also allow chat but block file transfers within chat.

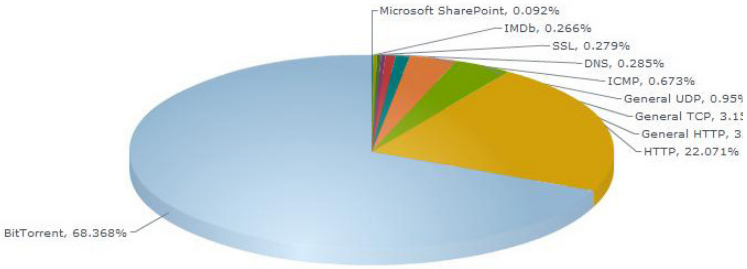
5th cool thing:

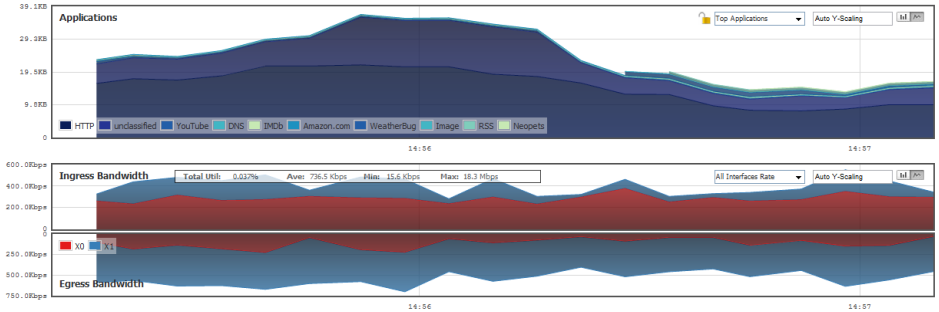
Visualize your application traffic

What's happening on my network? Who's wasting my bandwidth? Why is my network so slow? Have you ever asked yourself any of these questions? You could use a combination of separate tools to try to get answers, but this process is time consuming, and will only provide you with information after-the-fact. With Dell SonicWALL's real-time visualization of application traffic, you can answer these questions instantly, quickly diagnose issues, detect out-of-compliance network usage, create appropriate policies and immediately see the effectiveness of these policies.

View all traffic in real time by logging into the Application Flow Monitor

1. View real-time graphs of all application traffic
2. View real-time graphs of ingress and egress bandwidth
3. View real-time graphs of Web sites visited and all user activity
4. Create your own filtering that gives you the most relevant information





Visualization provides administrators with instant feedback on network traffic flows.

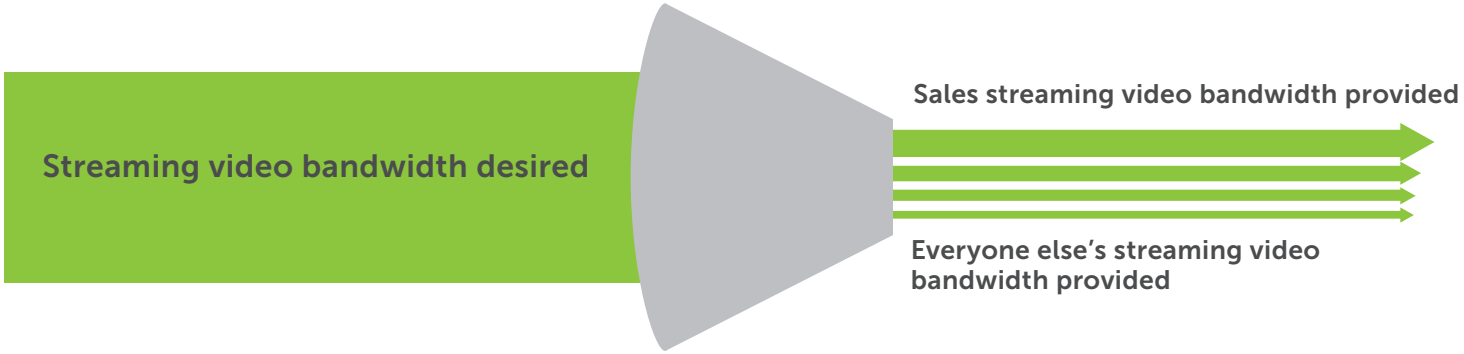
6th cool thing:

Manage bandwidth for a group of users

What do you do if your CEO complains that the business news videos that he wants to watch every morning are choppy and won't play correctly? After investigation, you determine that it's due to a company-wide bandwidth management policy that you implemented for all streaming video? 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 exclude the executive team from streaming video bandwidth management

1. Choose the executive group imported from your LDAP server
2. The Deep Packet Inspection (DPI) engine uses pre-defined streaming video application signatures from the application signature list
3. Apply bandwidth restriction to traffic with that header



Many companies have found that employees are happier if you let them have full access to the web, even if they have reduced bandwidth for unproductive sites.

7th cool thing:

Block viruses from entering your network

Network security must be at the forefront of any IT administrator's focus. The ability to prevent malware such as viruses, spyware, keyloggers, Trojans and intrusion attempts from entering the network at the gateway relieves the organization from great risk and spares potentially wasted resources. Dell SonicWALL security services, running on the high-performance and ultra-low-latency architecture of Dell SonicWALL Next-Generation Firewalls, are capable of blocking millions of threats from entering the network, before they become a danger to your users. If your users connect an infected laptop to the network, Dell SonicWALL Next-Generation Firewalls are capable of blocking the propagation of that malware within the department and within the rest of the organization.

Block viruses, spyware and other malware before it enters your network!

8th cool thing:

Identify connections by country

Is a connection to an IP in a foreign country from your local neighborhood office or a branch site just a benign connection from somebody browsing on the Web, or is it botnet activity? You can use application intelligence as a powerful forensics tool to identify exactly what's happening on your network.

View connections by country or create country-specific filters

1. Check which applications are connecting to IPs in other countries
2. See which users and which computers are connecting to IPs other countries
3. Create filters to restrict traffic to countries specified by you, with exclusion lists

Once you know the answer to the question, you can talk to the user, inspect the machine with the offending IP address, or enable a packet capture utility on the firewall to analyze exactly what's going over that connection. With application intelligence and control, you can identify and address problems that you might not have been aware of otherwise.

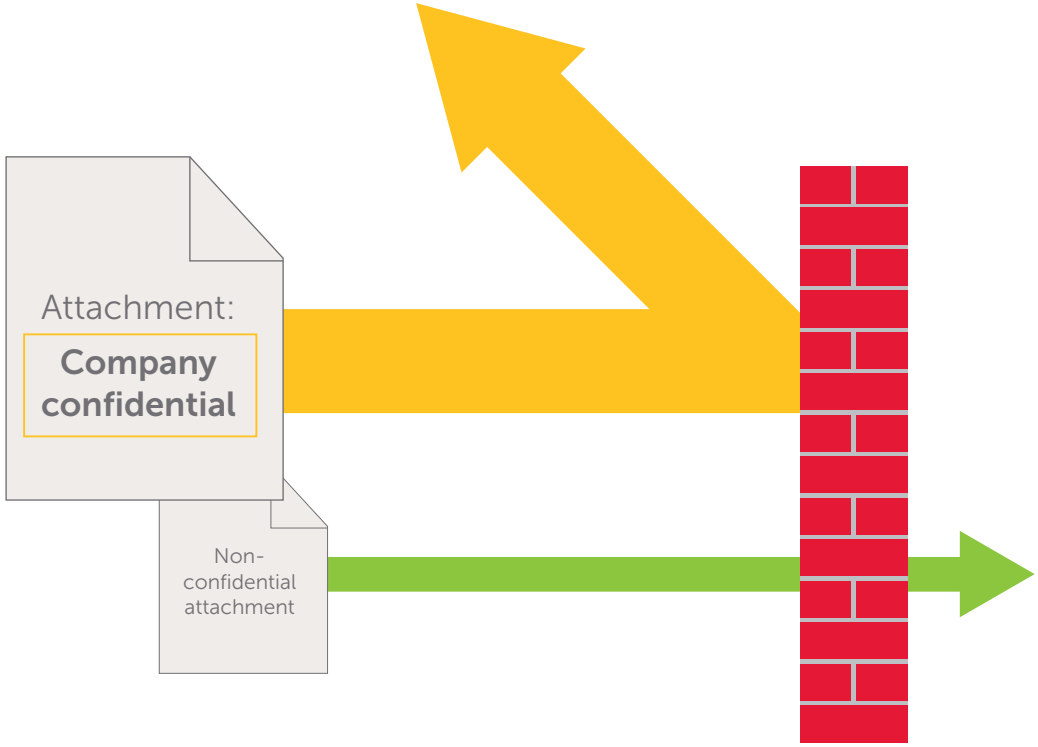
9th cool thing:

Prevent data leaks over email

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
The Deep Packet Inspection (DPI) engine looks for:

1. Email content = "Company confidential" and
2. Email content = "Company proprietary" and
3. Email content = "Private proprietary", etc.



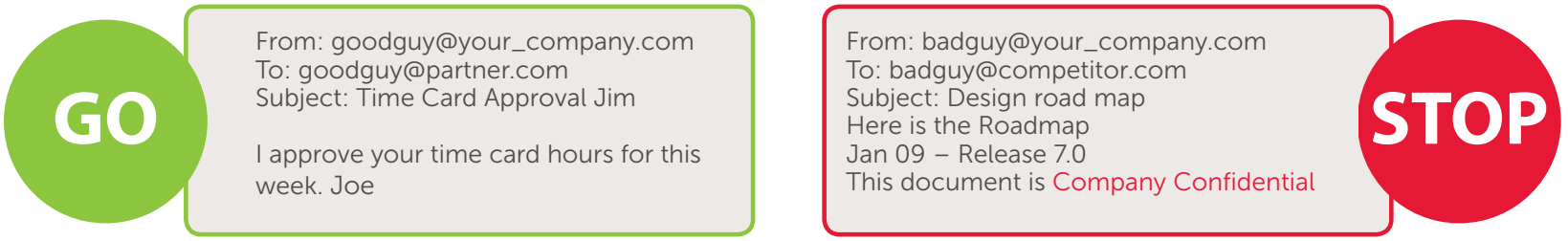
10th cool thing:

Prevent data leaks over web mail

Now 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 "Company Confidential" information?

Create a policy to block "company confidential" attachments in Web traffic

1. The Deep Packet Inspection (DPI) engine looks for "company confidential" on files transferred via http or https
2. Block message and notify the sender that the message is "company confidential"



This can also be done for FTP-based content.

11th cool thing:

Bandwidth manage streaming audio and video

Access to streaming video from sites such as YouTube.com is sometimes useful, but is often abused. Blocking these sites might work, but a preferable approach is to limit the total bandwidth given to streaming video, regardless of where it comes from. This also applies to streaming audio sites such online music radio stations and personalized music playlist sites. This traffic doesn't necessarily need to come from well-known sites, but can also be hosted by blogs. Thus, the goal is to identify this traffic by what it is, rather by its origin. Deep Packet Inspection excels at this process.

Create a policy to limit streaming audio and streaming video by predefined signature list

1. Select Streaming Video and Streaming Audio as application categories
2. Set the amount of bandwidth that you want to allocate to these application categories (e.g., 10%)
3. Create a rule that enforces Streaming Video and Streaming Audio to consume a maximum of 10% of bandwidth for everyone (perhaps excluding particular department groups, such as those in the training group)
4. Optionally, schedule the rule to be effective during standard business hours, but not during lunch hours or after 6 p.m.
5. Confirm the effectiveness of your new policy with real-time Visualization by logging into the Application Flow Monitor

When you add it all up

High performance platform

+ Deep packet inspection

+ Intrusion prevention

+ Application intelligence, control and visualization

Dell SonicWALL Next-Generation Firewall

Performance, protection and application control

How can I learn more?

- Download the white paper, "AimPoint Group: Application Control Defined – The Top 7 Capabilities Required to Restore Firewall Effectiveness"
- View the video
- Download the data sheet

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

Forward to a friend

About Dell SonicWALL

Dell™ SonicWALL™ provides intelligent network security and data protection solutions that enable customers and partners to dynamically secure, control, and scale their global networks. Securing any organization with multi-threat scanning based on global input at wire speed, Dell SonicWALL is recognized as an industry leader by Gartner and NSS Labs. For more information, visit the web site at **www.sonicwall.com**.

05/13 DS 0115L