Dell SonicWALL application risk management (SWARM) report

Prepared for:
General Hospital, LLC

Report on firewall:
Cisco ASA 5520 with IPS module

Report generated:
05/16/2014 10:53:47

Version:
02
This report has been prepared by Dell™ SonicWALL™ Laboratories as an example of a fictitious organization for three reasons.

• First, to give you a general understanding of the threats your network and your business face today.

• Second, to give you an understanding of how a Cisco ASA like yours performed when tested at SonicWALL Laboratories against the same threats that your Cisco firewall faces every day, in order to give you a clear picture of your current vulnerabilities.

• Third, to introduce you to a Next-Generation Firewall option that you might find both superior to the Cisco ASA and more affordable.

Today, intrusion and malware propagation techniques have evolved beyond simple port-based attacks. Security threats now come in the form of embedded viruses and malware, and often leverage the user populations of social networking hubs. Stateful packet inspection - the primary method of first-generation firewalls in detecting threats - cannot provide adequate protection against intruders piggy-backing on legitimate traffic.

Dell SonicWALL’s Next-Generation Firewalls, leaving behind the first-generation model of stateful packet inspection, offer a flexible and easily maintainable solution. Integrating multiple features onto a single platform, Dell SonicWALL bundles together a set of powerful security management tools on a single physical device with an easy-to-understand licensing structure.

For auditing needs, personal logs are kept by the Dell SonicWALL firewall. In providing a high-level overview of the fictitious General Hospital’s network, this report will:

• Identify vulnerabilities detected
• List high-risk applications and protocols
• Present traffic distribution statistics by URL category and traffic type
• Highlight the top 20 high-risk applications found
• Highlight the top 20 high-bandwidth applications found

The appendix contains:

• Risk definitions
• In-use application descriptions
• Detected vulnerabilities descriptions
• Complete application list
Vulnerabilities detected

Integrating traditional endpoint security protection into the firewall, Dell SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention provides a platform for additional protection at the network boundary. Security definitions are automatically delivered by Dell SonicWALL, ensuring both ease of use and up-to-date monitoring. Dell SonicWALL scrutinizes both inbound and outbound traffic. By monitoring internal traffic, Dell SonicWALL is able to identify infections on the internal network, rather than simply detecting attacks from external sources.

Laboratory failures of Cisco ASA 5520

In a laboratory setting, the Cisco ASA 5520 was subjected to the types and severity of attacks that your firewall can be expected to face over the course of a typical year in your business.

This is the report of the specific actual security vulnerabilities that were found to be exploited, as well as those breaches actually found under laboratory conditions when testing the Cisco ASA 5520.

As you can see the ASA failed to stop most of the MU application attacks in our laboratory environment. The Dell SonicWALL Network Security Appliance (NSA) was placed in bridge mode on the outside (WAN) of the ASA which is in NAT mode (most common gateway firewall deployment). The reason for placing the NSA on the outside vs. the inside of the ASA is to reveal the amount of applications and vulnerabilities that are leaking out of the network protected by a Cisco ASA. Even with all of the security features turned on the stateful packet inspection engine of the ASA failed to prevent and even detect these forms of applications and application attacks. A network safeguarded by such insecure technology can potentially be utilized as a safe haven for hackers and utilized by botnet masters for DDOS attacks.

Intrusion events

Intrusion detection is comprised of a multitude of events, ranging from scanning attacks to suspected botnet behavior. Dell SonicWALL IDP has detected the following intrusion attempts at the gateway:

Total intrusion events: 72
Sample events: 16 / 72

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious HTTP Content-Length Header 14</td>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>Adobe Reader eBook Format String Attack</td>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>Suspicious HTTP Content-Encoding Header</td>
<td>Intrusion</td>
<td>1</td>
</tr>
</tbody>
</table>
## Dell SonicWALL application risk management (SWARM) report

<table>
<thead>
<tr>
<th>Vulnerability Description</th>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Java Plugin Sandbox Security Bypass</td>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft Outlook OLE Object Security Bypass 2</td>
<td>Intrusion</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft SMB Client Remote Code Execution 1 (MS10-006)</td>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>Client Application Shellcode Exploit 1</td>
<td>Intrusion</td>
<td>8</td>
</tr>
<tr>
<td>Mozilla Firefox nsTreeRange Use-After-Free</td>
<td>Intrusion</td>
<td>2</td>
</tr>
<tr>
<td>Windows IE urlmon.dll Heap Buffer Overflow (MS06-042)</td>
<td>Intrusion</td>
<td>3</td>
</tr>
<tr>
<td>Windows Media Player -- ActiveX Instantiation</td>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>MS IE Uninitialized Object Memory Corruption (MS09-072)</td>
<td>Intrusion</td>
<td>2</td>
</tr>
<tr>
<td>Client Application Shellcode Exploit 2</td>
<td>Intrusion</td>
<td>6</td>
</tr>
<tr>
<td>Suspicious ActiveX Method 2</td>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>Client Application Shellcode Exploit 7</td>
<td>Intrusion</td>
<td>5</td>
</tr>
<tr>
<td>Macrovision InstallShield ActiveX DownloadAndExecute Method Invocation</td>
<td>Intrusion</td>
<td>1</td>
</tr>
<tr>
<td>Destination Unreachable (Port Unreachable)</td>
<td>Intrusion</td>
<td>8</td>
</tr>
</tbody>
</table>

*Vulnerability descriptions are provided in Appendix 3.*
Top URL categories in use

Web traffic is often one of the largest contributors to total network traffic. Dell SonicWALL’s Content Filtering Service splits web destinations into over 50 dynamically updated categories. Both traditional and next-generation traffic management options are available for each category, resulting in robust and granular control.

The top 6 categories of web destinations detected during the audit period are presented below:

Network traffic by type

Different types of network traffic perform different purposes. While infrastructure traffic between devices is a necessary component of every network, other forms of traffic may be unwanted. By differentiating between types of traffic, Dell SonicWALL identifies possible improvements for the allocation of resources on your network. You may want to identify bandwidth thresholds and implement application controls for each type of traffic.

*Note: Traffic by Geographic Source was not reported in this test given 100% of the traffic came from our USA lab. This report will typically also show geographic sources.*
The top 4 types of network traffic detected during the audit period are presented below:

![Pie chart showing network traffic categories]

### Top 25 applications by risk factor

Application vulnerabilities are often exploited by hackers to infiltrate private networks. SonicWALL tracks, logs and ranks traffic flowing through your network.

These applications represent the 25 most vulnerable applications on General Hospital’s network:

<table>
<thead>
<tr>
<th>Application</th>
<th>Category</th>
<th>Sessions</th>
<th>Kilobytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eMule</td>
<td>P2P</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>HTTP Proxy</td>
<td>PROXY-ACCESS</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>SOCKS 5</td>
<td>PROXY-ACCESS</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Wget</td>
<td>DOWNLOAD-APPS</td>
<td>2</td>
<td>1,822</td>
</tr>
<tr>
<td>SSH</td>
<td>REMOTE-ACCESS</td>
<td>5</td>
<td>268</td>
</tr>
<tr>
<td>Remote Frame Buffer (VNC)</td>
<td>REMOTE-ACCESS</td>
<td>4</td>
<td>140</td>
</tr>
<tr>
<td>Skype</td>
<td>IM</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>Facebook</td>
<td>SOCIAL-NETWORKING</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Executable</td>
<td>FILE-TYPES-HTTP</td>
<td>12</td>
<td>29,983</td>
</tr>
<tr>
<td>Encrypted Key Exchange</td>
<td>PROXY-ACCESS</td>
<td>798</td>
<td>1,007</td>
</tr>
<tr>
<td>CUPS</td>
<td>MISC-APPS</td>
<td>9</td>
<td>909</td>
</tr>
<tr>
<td>Archive</td>
<td>FILE-TYPES-HTTP</td>
<td>7</td>
<td>344</td>
</tr>
</tbody>
</table>

Generated: 05/16/2014 10:53:47
Dell SonicWALL application risk management (SWARM) report

<table>
<thead>
<tr>
<th>Document</th>
<th>FILE-TYPES-HTTP</th>
<th>12</th>
<th>162</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft CryptoAPI</td>
<td>MISC-APPS</td>
<td>13</td>
<td>119</td>
<td>✓</td>
</tr>
<tr>
<td>QuickTime</td>
<td>MULTIMEDIA</td>
<td>2</td>
<td>107</td>
<td>✓</td>
</tr>
<tr>
<td>Nullsoft Winamp</td>
<td>MULTIMEDIA</td>
<td>2</td>
<td>42</td>
<td>✓</td>
</tr>
<tr>
<td>LDAP v3</td>
<td>MISC-APPS</td>
<td>2</td>
<td>37</td>
<td>✓</td>
</tr>
<tr>
<td>vsFTpd FTP Server</td>
<td>MISC-APPS</td>
<td>60</td>
<td>36</td>
<td>✓</td>
</tr>
<tr>
<td>MySQL Server</td>
<td>DATABASE-APPS</td>
<td>20</td>
<td>30</td>
<td>✓</td>
</tr>
<tr>
<td>AOL Radio</td>
<td>MULTIMEDIA</td>
<td>2</td>
<td>21</td>
<td>✓</td>
</tr>
<tr>
<td>RealMedia</td>
<td>MULTIMEDIA</td>
<td>9</td>
<td>19</td>
<td>✓</td>
</tr>
<tr>
<td>RTSP</td>
<td>MULTIMEDIA</td>
<td>5</td>
<td>17</td>
<td>✓</td>
</tr>
<tr>
<td>MS SQL Server</td>
<td>DATABASE-APPS</td>
<td>4</td>
<td>17</td>
<td>✓</td>
</tr>
<tr>
<td>Microsoft Remote Desktop</td>
<td>REMOTE-ACCESS</td>
<td>2</td>
<td>15</td>
<td>✓</td>
</tr>
<tr>
<td>Telnet</td>
<td>REMOTE-ACCESS</td>
<td>4</td>
<td>13</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Risk type definitions provided in Appendix 1. Application descriptions provided in Appendix 2.
Dell SonicWALL application risk management (SWARM) report

Top 25 applications by bandwidth consumed
Excessive demand, often the result of large downloads or streaming of video, can produce an unacceptable strain on your network infrastructure.

These applications represent the 25 biggest consumers of General Hospital's network bandwidth:

<table>
<thead>
<tr>
<th>Application</th>
<th>Category</th>
<th>Sessions</th>
<th>Kilobytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executable</td>
<td>FILE-TYPES-HTTP</td>
<td>12</td>
<td>29,983</td>
</tr>
<tr>
<td>Wget</td>
<td>DOWNLOAD-APPS</td>
<td>2</td>
<td>1,822</td>
</tr>
<tr>
<td>Encrypted Key Exchange</td>
<td>PROXY-ACCESS</td>
<td>798</td>
<td>1,007</td>
</tr>
<tr>
<td>CUPS</td>
<td>MISC-APPS</td>
<td>9</td>
<td>909</td>
</tr>
<tr>
<td>Archive</td>
<td>FILE-TYPES-HTTP</td>
<td>7</td>
<td>344</td>
</tr>
<tr>
<td>SSH</td>
<td>REMOTE-ACCESS</td>
<td>5</td>
<td>268</td>
</tr>
<tr>
<td>Document</td>
<td>FILE-TYPES-HTTP</td>
<td>12</td>
<td>162</td>
</tr>
<tr>
<td>Remote Frame Buffer (VNC)</td>
<td>REMOTE-ACCESS</td>
<td>4</td>
<td>140</td>
</tr>
<tr>
<td>Microsoft CryptoAPI</td>
<td>MISC-APPS</td>
<td>13</td>
<td>119</td>
</tr>
<tr>
<td>QuickTime</td>
<td>MULTIMEDIA</td>
<td>2</td>
<td>107</td>
</tr>
<tr>
<td>Nullsoft Winamp</td>
<td>MULTIMEDIA</td>
<td>2</td>
<td>42</td>
</tr>
<tr>
<td>LDAP v3</td>
<td>MISC-APPS</td>
<td>2</td>
<td>37</td>
</tr>
<tr>
<td>vsFTpd FTP Server</td>
<td>MISC-APPS</td>
<td>60</td>
<td>36</td>
</tr>
<tr>
<td>MySQL Server</td>
<td>DATABASE-APPS</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>Skype</td>
<td>IM</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>AOL Radio</td>
<td>MULTIMEDIA</td>
<td>2</td>
<td>21</td>
</tr>
<tr>
<td>RealMedia</td>
<td>MULTIMEDIA</td>
<td>9</td>
<td>19</td>
</tr>
<tr>
<td>RTSP</td>
<td>MULTIMEDIA</td>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>MS SQL Server</td>
<td>DATABASE-APPS</td>
<td>4</td>
<td>17</td>
</tr>
<tr>
<td>Microsoft Remote Desktop</td>
<td>REMOTE-ACCESS</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>Telnet</td>
<td>REMOTE-ACCESS</td>
<td>4</td>
<td>13</td>
</tr>
<tr>
<td>Kerberos Kadmin</td>
<td>INFRASTRUCTURE</td>
<td>2</td>
<td>13</td>
</tr>
</tbody>
</table>
Dell SonicWALL application risk management (SWARM) report

<table>
<thead>
<tr>
<th>Application</th>
<th>Category</th>
<th>NDMP</th>
<th>INFRASTRUCTURE</th>
<th>7</th>
<th>7</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP</td>
<td>VoIP-APPS</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>SOCIAL-NETWORKING</td>
<td>2</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Risk type definitions provided in Appendix 1. Application descriptions provided in Appendix 2.

Application intelligence, control and visualization

Dell SonicWALL puts network control back into the hands of IT administrators. While some applications are business critical and require access to large amounts of bandwidth, other applications are non-productive and require throttling or blocking. Rulesets based on port or protocol require constant updates as applications evolve. Dell SonicWALL makes the job easy for administrators with a robust identification scheme, granular control options and detailed visualization tools.

Application intelligence

Scanning every byte of every packet of network traffic, Dell SonicWALL identifies applications without relying on port or protocol specific rules.

- Deep Packet Inspection of traffic tunneling over SSL
- Supports custom application signatures
- Integrated data leakage prevention and logging

Application control

Bandwidth management policies are placed at the administrator’s fingertips, and pre-defined logical categories are available alongside traditional application and user options. Application signatures are pushed by Dell SonicWALL and eliminate the hassle of ruleset updates.

- Dynamically updated database containing thousands of application and content-based signatures
- Customizable actions, such as Set User Message
- Predefined actions, such as Bypass DPI

Application visualization

Flow Monitor provides visuals for application traffic, ingress and egress bandwidth, web traffic, and general user activity, supplying administrators with the crucial information necessary for maintaining a productive network under rapidly changing conditions.

- Real-time data on everything from potential network threats to URLs visited
- Customizable filter views for repeat access
- Widget creation, such as a pie chart view

Generated: 05/16/2014 10:53:47
Appendix 1: Risk definitions

- This application is resource hungry and can contribute significantly to network bandwidth. The application is also a well known facilitator of malicious activity, and is often used to infect end points. Some peer to peer services, such as eMule, fall into this category.

- This application may be either resource hungry or may provide a service that circumvents normal network rules. Allowing this application to run may result in users unknowingly downloading malicious files. Some proxy services, such as Potential Ultrasurf, fall into this category. It also includes some peer to peer applications, such as BitComet.

- This application may not have a legitimate purpose on the network. The application can also be a source of unwanted traffic to the internal network. Some messenger services, such as Meebo, fall into this category.

- This application is a common source of network traffic.
Appendix 2: Application descriptions

AOL radio
AOL radio is a no-cost multimedia player and service from AOL. As with many streaming media services users may find this application to be bandwidth heavy.

Archive
RPM files are software files packaged by the RPM Package Manager system.

CUPS
The Common Unix Printing System (CUPS) is a modular computer printing system that lets a local computer operate as a print server accepting and processing print jobs from other clients.

Document
The PDF file format or Portable Document Format was created by Adobe Systems to help users in facilitating the exchange of document files.

Encrypted Key Exchange
Encrypted Key Exchange (also known as EKE) is a family of password-authenticated key agreement methods described by Steven M. Bellovin and Michael Merritt. Although several of the forms of EKE in this paper were later found to be flawed the surviving refined and enhanced forms of EKE effectively make this the first method to amplify a shared password into a shared key where the shared key may subsequently be used to provide a zero-knowledge password proof or other functions.

Executable
Executable and Linking Format files (.exe) are a common standard file format for executable files and libraries.

Facebook
Facebook is an enormously popular social networking site that lets users build a profile page and then seek out and connect with other friends on the service. Users can also join networks for various interests or geographic locations upload digital media content and even play games online through the site. Facebook is subject to blocking and censure in some countries and the site appears to continually be re-vamping their privacy policy in an effort to balance user security and business needs.

HTTP Proxy
While this event may not represent an attack such activity may represent application usage against company policies.
Kerberos Kadmin
Kerberos is a network authentication protocol that allows nodes to prove their identity to one another while communicating over non-secure networks while ensuring that messages are not vulnerable to eavesdropping.

LDAP v3
LDAP or Lightweight Directory Access Protocol is an application protocol for querying and modifying directory services running over TCPIP.

MS SQL Server
Microsoft SQL Server is a relational database management system produced by Microsoft Corporation. SQL Server is available in a wide number of editions and its primary query languages are MS-SQL and T-SQL.

Microsoft CryptoAPI
The Microsoft Cryptographic Application Programming Interface (or CAPI) is an application programming interface that is part of Microsoft Windows operating systems.

Microsoft Remote Desktop
Microsoft Terminal Services also known as Remote Desktop Services extends distributed computing by allowing PCs to operate in a server-based computing environment. Remote Desktop Services are cross-platform functional.

MySQL Server
MySQL is a relational database management system that runs as a server providing multi-user access to a number of databases.

NDMP
Network Data Management Protocol (NDMP) is a protocol that provides for the efficient transport of data between network area storage and other backup devices.

Nullsoft Winamp
Winamp is a client application that downloads digital content of all forms over HTTP. The client also supports a variety of multimedia protocols and standards.

QuickTime
The QuickTime client uses HTTP to download digital content for users to view in the QuickTime player. QuickTime is an application that supports a number of media standards.

RTSP
RTSP (Real-Time Streaming Protocol) is a protocol for streaming media that lets a client system remotely control a media server. RTSP is often used with QuickTime and RealMedia players.
RealMedia
This event indicates that a RealMedia compatible client application is attempting to download content. RealPlayer for example is a multimedia client application supporting a broad range of media standards.

Remote Frame Buffer (RFB)
Remote Frame Buffer (RFB) is a protocol to provide remote access to graphical user interfaces. RFB can be used by users with both Windows and Mac operating systems. More recent iterations of RFB contain more advanced compression security and file transfer features. RFB is used is Virtual Network Computing and while it has great flexibility as it pixel-based other protocols such as RDP have a greater understanding of the desktop and send simpler higher-level commands.

SIP
The Session Initiation Protocol (SIP) is an application-layer signaling protocol widely used for establishing and tearing down multimedia communication sessions for voice and video transmission over the Internet.

SOCKS 5
SOCKS 5 is an updated version of the SOCKS Internet protocol that allows data packets to travel between client server applications via a proxy server. SOCKS 5 also provides for UDP and IPv6 support.

SSH
Secure Shell (SSH) is both a set of standards and a network protocol for opening a secure channel between a remote and local computer. SSH provides encryption to aid in security for users connecting to a remote system over the Internet.

Skype
Skype is an application that allows users to make voice calls over the Internet using a proprietary VoIP network called the Skype protocol. After a user installs client software calls to fellow Skype users are free-of-charge while calls to landlines and mobile phones can be made for a fee. Additional features include instant messaging file transfer and video conferencing. Skype is owned by eBay Inc.

TELNET
TELNET Protocol provides a basic eight-bit bi-directional protocol that can be used for communications on LANs and the Internet. Due to its lack of encryption it is advised that the use of Telnet be blocked.

Wget
GNU Wget is an application that retrieves content from web servers and completes downloads using the HTTP HTTPS and FTP protocols.

eMule
eMule is a de-centralized peer-to-peer file sharing application for Microsoft Windows. eMule connects to multiple networks including eDonkey and Kad. eMule allows for direct exchange of sources between client
nodes quick recovery of corrupted downloads and the use of a credits to reward uploaders. eMule transmits data in zlib-compressed form to save bandwidth.

**vsFTPD FTP Server**

vsFTPD (Very Secure FTP Daemon) is an FTP server for UNIX-based systems. vsFTPD also supports IPv6 and SSL.

**Appendix 3: Vulnerability descriptions**

**Suspicious HTTP Content-Length Header 14**

This signature indicates a suspicious Content-Length header within an HTTP response.

**Adobe Reader eBook Format String Attack**

This signature detects a suspicious byte pattern in XML documents that may be an attempt at exploiting a vulnerability in Adobe Reader.

**Suspicious HTTP Content-Encoding Header**

This signature indicates a suspicious Content-Encoding header within an HTTP response.

**Oracle Java Plugin Sandbox Security Bypass**

The Sun Java Plugin capability in Java 2 Runtime Environment (JRE) 1.4.2_01 1.4.2_04 and possibly earlier versions does not properly restrict access between Javascript and Java applets during data transfer which allows remote attackers to load unsafe

**Microsoft Outlook OLE Object Security Bypass 2**

Microsoft Outlook 2003 allows remote attackers to bypass the default zone restrictions and execute script within media files via a Rich Text Format (RTF) message containing an OLE object for the Windows Media Player which bypasses Media Player’s setting

**Microsoft SMB Client Remote Code Execution 1 (MS10-006)**

The SMB client implementation in Microsoft Windows 2000 SP4 XP SP2 and SP3 and Server 2003 SP2 does not properly validate response fields which allow remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted response.

**Client Application Shellcode Exploit 1**

This signature detects and blocks a suspicious byte pattern sent from a server upon connection establishment.
Dell SonicWALL application risk management (SWARM) report

Mozilla Firefox nsTreeRange Use-After-Free

Windows IE urlmon.dll Heap Buffer Overflow (MS06-042)
Heap-based buffer overflow in URLMON.DLL in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1 with versions the MS06-042 patch before 20060824 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long U

Windows Media Player -- ActiveX Instantiation
Windows Media Player (WMP) is a digital media player and media library application developed by Microsoft that is used for playing audio video and viewing images on Microsoft operating systems. P This SonicWALL signature can help detect and identify

MS IE Uninitialized Object Memory Corruption (MS09-072)

Client Application Shellcode Exploit 2
This signature detects and blocks a suspicious byte pattern sent from a server upon connection establishment.

Suspicious ActiveX Method 2
This signature indicates malicious ActiveX control in the web page.

Client Application Shellcode Exploit 7
This signature detects and blocks a suspicious byte pattern sent from a server upon connection establishment.

Macrovision InstallShield ActiveX DownloadAndExecute Method Invocation
There exists a vulnerability in Macrovision InstallShield Update Service isusweb.dll ActiveX control. The vulnerability is due to insufficient verification of user input to the DownloadAndExecute function. An attacker can host a crafted web page and entice interaction.

Destination Unreachable (Port Unreachable)
Internet Control Message Protocol (ICMP) is part of the Internet Protocol Suite. ICMP messages are typically generated in response to errors in IP datagrams or for diagnostic or routing purposes. BRBR ICMP traffic may be used to map a network or help
Dell SonicWALL application risk management (SWARM) report

Appendix 4: Complete application list

42 applications have been identified on General Hospital's network. They are ranked in descending order of kilobytes transferred. Applications in red indicate a risk level of yellow or higher.

1. Executable (29,983)
2. Wget (1,822)
3. Encrypted Key Exchange (1,007)
4. CUPS (909)
5. Archive (344)
6. SSH (268)
7. Document (162)
8. Remote Frame Buffer (VNC) (140)
9. Microsoft CryptoAPI (119)
10. QuickTime (107)
11. Nullsoft Winamp (42)
12. LDAP v3 (37)
13. vsFTPd FTP Server (36)
14. MySQL Server (30)
15. Skype (30)
16. AOL Radio (21)
17. RealMedia (19)
18. RTSP (17)
19. MS SQL Server (17)
20. Microsoft Remote Desktop (15)
21. Telnet (13)
22. Kerberos Kadmin (13)
23. NDMP (7)
24. SIP (5)
25. Facebook (5)
26. Serv-U FTP Server (5)
27. DRDA (4)
28. IBM DB2 (4)
29. MP3 (4)
30. Microsoft Windows (3)
31. GDS DB (3)
32. RSYNC (3)
33. eMule (3)
34. HTTP Proxy (2)
35. Non-SSL traffic over SSL port (2)
36. PostgreSQL Server (2)
37. WS_FTP Server (2)
38. NNTP (2)
39. Icecast (1)
40. X Font Server (1)
41. SOCKS 5 (1)
42. NetFlow v9 (1)

In summary

If your network security perimeter more than three years old, it is time to move to a Next-Generation Firewall. As you have seen, threats are now coming into your network through the application layer where older firewalls cannot detect them. Social networking and streamed media open new vulnerabilities and personal Internet consumption saps productivity. In addition, your old firewall is a bottleneck and is likely slowing down your entire network.
There are three main reasons to upgrade to a Next-Generation Firewall:

1. to prevent threats from entering your network through the application layer
2. to improve network performance getting all the bandwidth you’re paying for
3. to see and control who is doing what on your network which can help keep employees focused

Here are 5 important things to look for when considering a replacement for your Cisco ASA firewall:

1. **Does the firewall scan any size files across all protocols?**
   Fortinet, Cisco, Juniper and WatchGuard firewalls have file size limitations

2. **Does the firewall perform deep packet inspections?**
   Cisco and Check Point firewalls require additional modules or “blades.”

3. **Does the firewall’s performance degrade when security services are turned on?**
   Palo Alto Networks, Fortinet, Cisco, Juniper, Check Point, and WatchGuard firewalls experience performance degradation when security services are enabled

4. **Does the firewall enable application throttling, analysis and visualization?**
   None of these vendors provides all these services.

5. **Is it affordable to own?**
   Not if you are forced to purchase additional hardware and you can’t manage everything yourself.

The Dell SonicWALL Customer Advantage program makes it affordable to move up to a Next-Generation Firewall. In fact, you’ll get a sizable credit for your old firewall. Our [Secure Upgrade Plus](#) offers provides an upgrade path from current SonicWALL products as well as a trade-in path from competitors’ products. Click [here](#) to get the details.