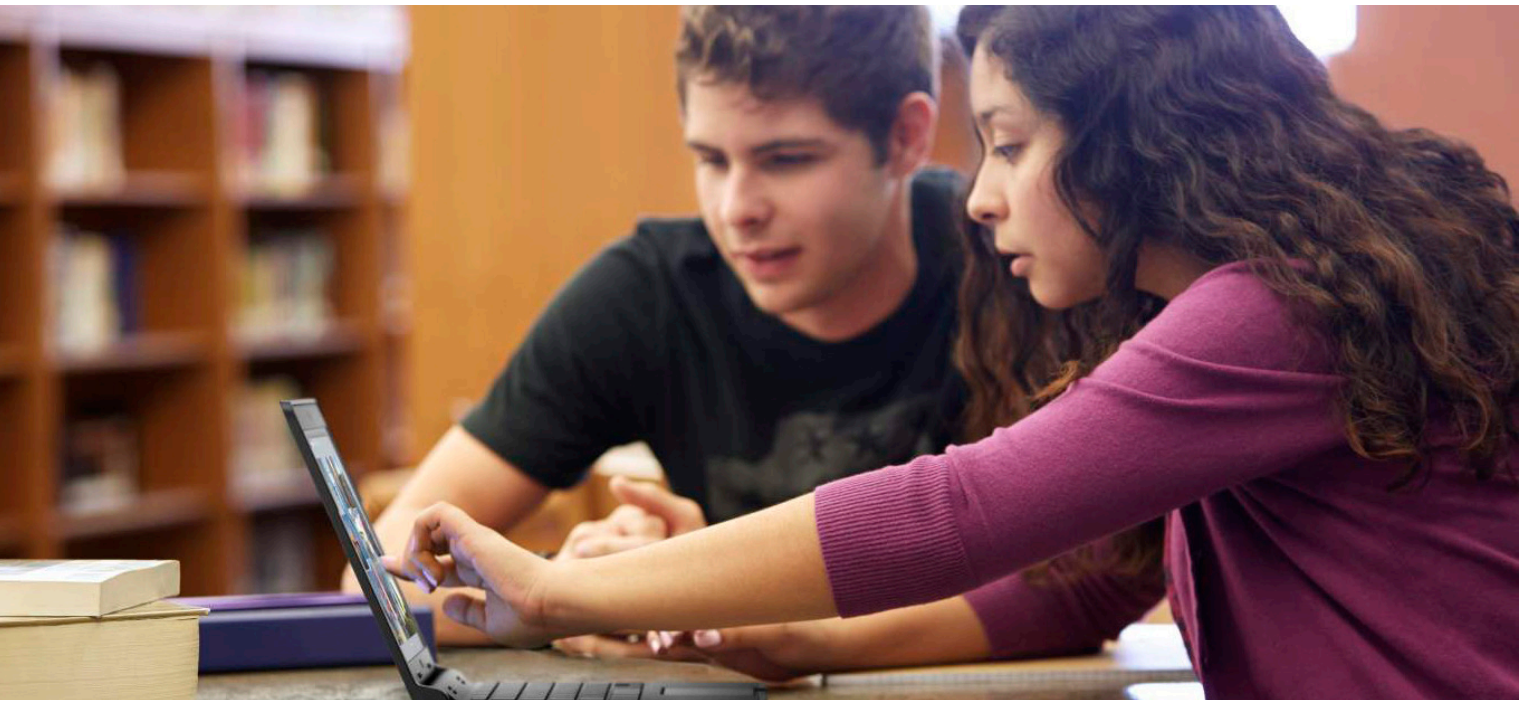
Security

K-12 network security: A technical deep-dive playbook

Five key components to consider in next-generation firewall deployments



Introduction

This paper offers IT directors and administrators at K-12 schools and school districts a deep-dive into deploying highly secure and cost-effective network security. It reviews core requirements, presents five key components to consider when selecting a network security solution to meet those requirements, and then dives into detail on how next-generation firewall (NGFW) technology from Dell SonicWALL delivers those key components.

Core network security requirements for K-12

K-12 school districts share student, faculty and administrative data across local and wide area networks, wireless networks, cloud services and the internet. Districts must protect confidential and sensitive data from cyber-theft, protect students from inappropriate content, and secure the network from threats such as viruses, spyware and intrusions – all without impeding academic performance and productivity.

In order to maintain E-Rate discount eligibility, schools also must comply with the Children's Internet Protection Act (CIPA), by implementing a policy that protects minors from inappropriate web content. District directors of information security (IS) are tasked with selecting and procuring the most effective network security solutions within their budgets, while ensuring the greatest value and return on investment.

An effective K-12 network security solution must therefore:

- Protect students from harmful websites both at school and home on school-issued devices, in line with CIPA
- Comprehensively protect the network from threats
- Provide secure, high-speed wireless access for students, faculty, and staff using either school-issued or personal devices
- Optimize network bandwidth for academic applications to enhance performance and productivity
- Streamline deployment, management, and integration to lower total cost of ownership (TCO)

"The Dell SonicWALL SuperMassive will easily support our district's 5,000 devices connecting to it and surfing the internet at the same time, which was important to us. It doesn't even break a sweat."

Jon Graves, Technology Services, Coordinator, Walton County Public Schools

Five key components to consider

In order to meet all of these core requirements, five key components stand out for consideration when selecting a network security solution:

1. **Content filtering:** To protect students from harmful web content
2. **DPI-SSL:** To provide Deep Packet Inspection (DPI) of encrypted Secure Sockets Layer (SSL) traffic
3. **Gateway security services:** To prevent intrusions, block malware and spyware, and provide application intelligence and control
4. **Wireless network security:** To scan and protect Wi-Fi device traffic
5. **WAN acceleration:** To optimize network performance and productivity

In addition, these components should be easily deployed, managed and integrated via centralized global management.

K-12 deployment scenario

The following sections present a technical deep-dive into how Dell SonicWALL NGFW technology addresses each of these five key components.

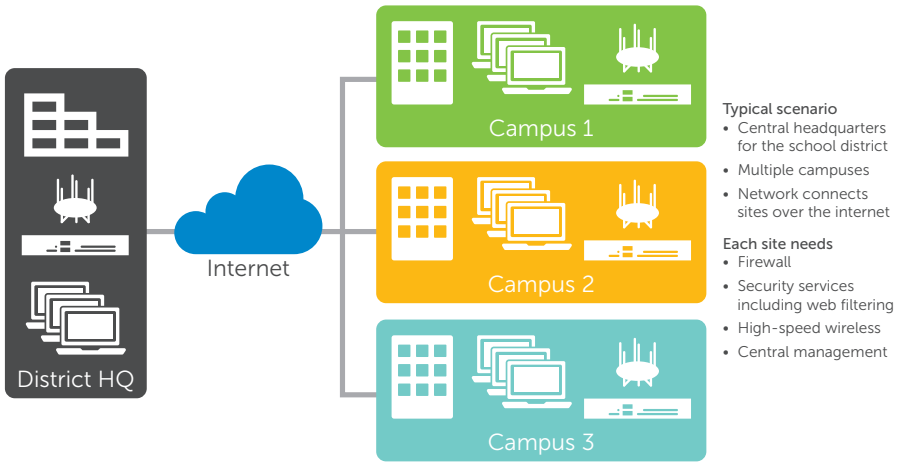
Content filtering

Dell SonicWALL Content Filtering Service (CFS) enables schools to create and enforce internet use policies that block IT-issued computers, located behind the firewall, from accessing inappropriate and unproductive websites over a LAN, wireless LAN (WLAN), or VPN.

Deployed and managed through a Dell SonicWALL firewall, CFS eliminates the need for additional hardware or deployment expenditures on a separate dedicated filtering server. A dynamically updated rating architecture cross-references all requested websites against a highly accurate database categorizing millions of URLs, IP addresses and domains. The Dell SonicWALL firewall receives ratings in real time, and then compares each rating to the local policy setting. The appliance will then either allow or deny the request based on the administrator's locally configured policy.

Administrators can block or apply bandwidth management to all or any combination of more than 56 pre-defined categories. Administrators can apply User Level Authentication (ULA) and Single Sign-On (SSO) to enforce username and password logon. CFS can block potentially harmful content such as Java™, ActiveX®, and cookies, as well as schedule filtering by time of day, such as during school hours. CFS also enhances performance by filtering out IM, MP3s, streaming media, freeware and other files that drain bandwidth.

School district



Dell SonicWALL content filtering solutions architecture

IP-based HTTPS content filtering allows administrators to use an SSL certificate common name, in addition to server IP addresses, to control user access to websites over encrypted HTTPS. Multimedia, social networking, malware, and the Child Abuse Image Content list (CAIC), maintained by the Internet Watch Foundation (IWF), are included in the CFS list. HTTPS filtering is based on the categorical rating of websites containing information or images that are objectionable or unproductive, such as violence, hate, online banking, or shopping. For even more comprehensive URL filtering for HTTPS, we recommend using client DPI-SSL (see DPI-SSL section, below).

Easy-to-use web-based management enables flexible policy configuration and complete control over internet usage. Administrators can enforce multiple custom policies for individual users, groups, or specific category types. Local URL filtering controls can allow or deny specific domains or hosts. To block objectionable and unproductive material more effectively, administrators can also create or customize filtering lists.

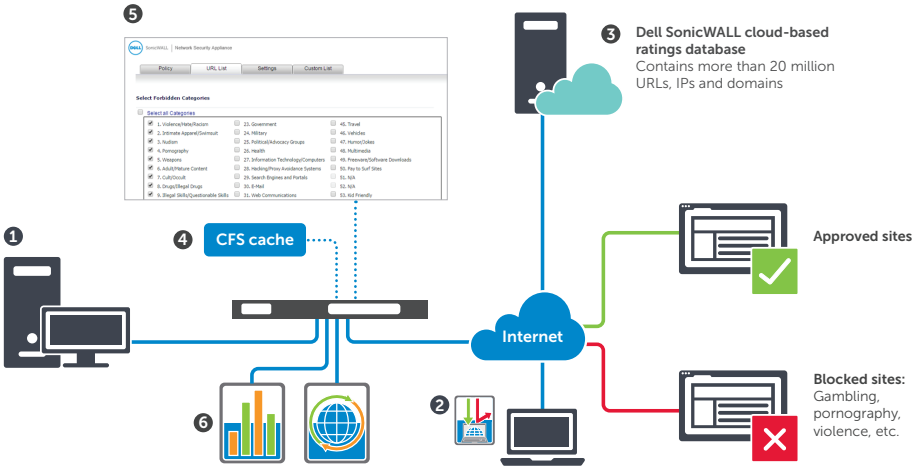
High-performance web caching and rating architecture allows administrators to block sites easily and automatically by category. URL ratings are cached locally on the Dell SonicWALL firewall, so response time for subsequent access of frequently visited sites is only a fraction of a second.

Using Dell SonicWALL Analyzer or Dell SonicWALL Global Management System (GMS), administrators can create real-time and historical reports, including websites blocked and visited by user. Configuration of the YouTube for Schools service (which allows customized YouTube access for students, teachers, and administrators) depends on the method of content filtering you are using. Users that are members of multiple groups, where one policy allows unrestricted access to YouTube, and the other policy restricts access to YouTube for Schools, are filtered by the YouTube for Schools policy and are not allowed unrestricted access to YouTube.

The basic default behavior for CFS policies assigned to different groups is to follow standard most specific/least restrictive logic, meaning the most specific rule is always given the highest priority. In contrast, the basic default behavior for CFS policies within the same group is to enforce rules following an additive logic.

Content filtering client

For Windows, Chrome OS and Mac OS endpoint devices that are used outside the firewall perimeter, the Dell SonicWALL Content Filtering Client (CFC) extends content filtering controls to block harmful and unproductive web content, regardless of where the connection is established. In addition to providing IT administrators the tools to control web-based access for roaming devices, the client can be configured to automatically switch enforcement to the internal policy once the device reconnects to the network firewall. In the event an outdated client attempts to connect to the internal network to access the internet, the connection is denied and the user receives a message with steps for remediation. The client is automatically deployed and provisioned through a Dell SonicWALL firewall, and is managed and monitored using a powerful policy and reporting engine in the cloud, that is accessed seamlessly from the firewall interface.



1. Dell SonicWALL CFS user behind the firewall
2. Roaming CF Client user outside the firewall perimeter
3. Distributed Dell SonicWALL CFS ratings database
4. Local ratings cache of acceptable sites
5. Set URL polices to block objectionable or counter productive web sites
6. Real-time and historical reports using Dell SonicWALL Analyzer or GMS

Points for consideration:

- Does your solution comply with CIPA mandates to be eligible for E-Rate discounts?
- Does your solution work when the student takes a school-issued device home?

DPI-SSL

Dell SonicWALL DPI-SSL provides advanced protection against encrypted threats. DPI-SSL extends Dell's patented Reassembly-Free Deep Packet Inspection® (RFDPI) technology to allow inspection of encrypted HTTPS traffic and other SSL-based traffic. DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted traffic. The full-stack-stream inspection technology of RFDPI scans SSL-encrypted traffic (including HTTPS, SMTPS, NNTPS, LDAPS, FTPS, TelnetS, IMAPS, IRCS, and POPS), regardless of the port being used. The SSL traffic is decrypted transparently, scanned for threats, and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found.

DPI-SSL requires minimal configuration and complexity. For high-traffic deployments, administrators can exclude trusted sources to maximize network performance. Additionally, administrators can target specific traffic for SSL inspection by customizing a list that specifies address, service or user objects or groups. All Dell SonicWALL firewall appliances support DPI-SSL. Comprehensive support includes intrusion prevention, malware prevention, application intelligence and control, content/URL filtering, and prevention of malware command-and-control communication.

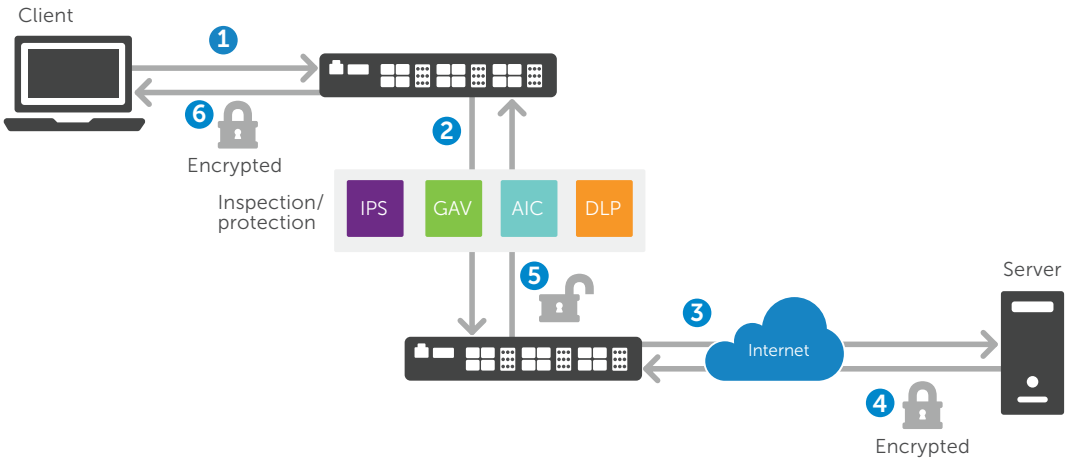
By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure inclusion/exclusion lists to customize which traffic DPI-SSL inspection applies. The inclusion/exclusion lists provide the ability to specify certain objects or groups. In deployments that process a large amount of traffic, to reduce the CPU impact of DPI-SSL, and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections, it can be useful to exclude trusted sources. DPI-SSL has two main deployment configurations: Client DPI-SSL and Server DPI-SSL.

Client DPI-SSL

Client DPI-SSL deployment mode enables inspection of SSL traffic when the client is on the firewall's LAN and accesses content located on the WAN. In this scenario, the firewall typically does not own the certificates and private keys for the content it is inspecting. After the appliance has decrypted and inspected the SSL-encrypted traffic, it rewrites the certificate sent by the remote server and signs the newly-generated certificate with the user-specified certificate.

Points for consideration:

- Dell SonicWALL has greater performance and scalability than solutions from other security vendors when it comes to decrypting SSL traffic and scanning it for threats.



1. Client initiates SSL handshake with server
2. NGFW intercepts request and establishes session using its own certificates in place of server
3. NGFW initiates SSL handshake with server on behalf of client using admin defined SSL certificate
4. Server completes handshake and builds a secure tunnel between itself and NGFW
5. NGFW decrypts and inspects all traffic coming from or going to client for threats and policy violations
6. NGFW re-encrypts traffic and sends along to client

Client DPI-SSL deployment

By default, this is the appliance certificate authority (CA), although a different certificate can be selected. By default, when DPI-SSL is enabled, it applies to all traffic on the appliance. Administrators can customize which traffic DPI-SSL inspection applies:

- Exclusion/inclusion lists (exclude/include specified objects and groups)
- Common name exclusions (exclude specified host names)

Server DPI-SSL

Alternatively, Server DPI-SSL deployment mode enables inspection of SSL traffic when remote clients connect over the WAN to access content located on the firewall's LAN, allowing the administrator to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client. In this scenario, the owner of the Dell SonicWALL NGFW owns the certificates and private keys of the origin content servers.

Afterward, if the pairing defines the server to be clear text, then a standard TCP connection is made to the server on the original (post-NAT remapping) port. If the pairing is not defined to be clear text, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the connection.

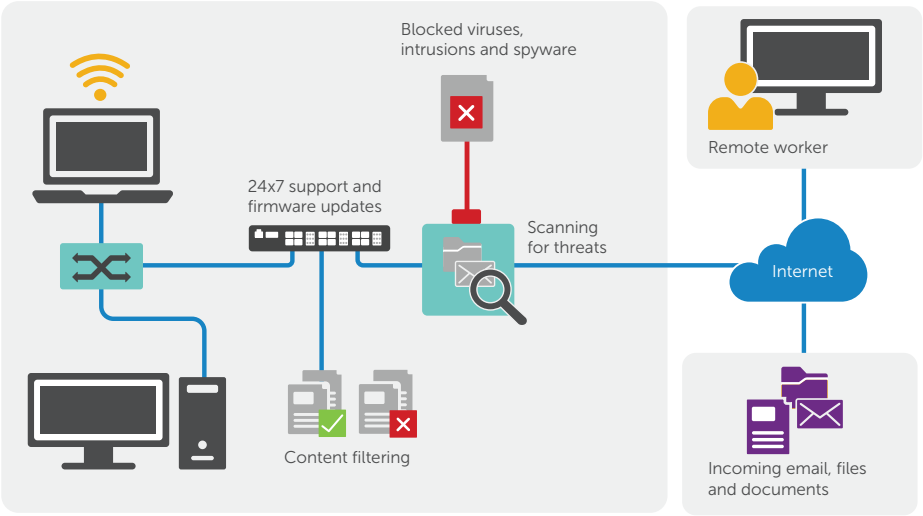
In this deployment scenario, the owner of the firewall owns the certificates and private keys of the origin content servers. Administrators would have to import the server's original certificate onto the appliance and create an appropriate server IP address to server certificate mappings in the Server DPI-SSL UI. Server DPI-SSL inspection requires that you specify which certificate is used to sign traffic for each server that has DPI-SSL inspection performed on its traffic.

Gateway security services

In addition to CFS, detailed above, the Dell SonicWALL Comprehensive Gateway Security Suite (CGSS) also includes:

- Gateway anti-virus, anti-malware, and anti-spyware
- Intrusion prevention service (IPS)
- Application intelligence and control

These services (detailed individually below) integrate everything needed for comprehensive protection from threats such as viruses, intrusions, botnets, spyware, worms, Trojans, adware, keyloggers, malicious mobile code (MMC), and other dangerous applications and web content.



As soon as new threats are identified, and often before software vendors can patch their software, Dell SonicWALL firewalls and the cloud database are automatically updated with signatures that protect against these threats.

Gateway anti-virus and anti-spyware

Dell SonicWALL gateway anti-virus (GAV) service provides comprehensive, multi-layered anti-virus protection for the network, the desktop, and at remote campus sites. Its ICSA-certified gateway anti-virus and anti-spyware protection combines network-based anti-malware with a cloud database of more than 12 million malware signatures. It enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network. GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic.

GAV can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because GAV does not have to perform reassembly, there are no file size limitations imposed by the scanning engine. GAV delivers threat protection directly on the Dell SonicWALL security appliance by matching downloaded or emailed files against an extensive and dynamically updated database of threat virus signatures, without ever buffering any of the bytes within the stream. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of Dell SonicWALL's SonicAlert Team, third-party virus analysts, open source developers, and other sources.

GAV can be configured to protect against internal threats, as well as those originating outside the network. It operates over a multitude of protocols, including TCP streams, SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications, and dozens of other stream-based protocols. This provides administrators with comprehensive network threat prevention and control. It also closes potential backdoors that could be used to compromise the network, while also improving employee productivity and conserving internet bandwidth.

Because files containing malicious code and viruses can also be compressed, and therefore inaccessible to conventional anti-virus solutions, GAV integrates advanced decompression technology. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) are automatically decompressed and scanned on a single-pass, per-packet basis. Along with GAV, Dell SonicWALL anti-spyware protects networks from intrusions by cutting off spyware installations and delivery at the gateway, and denying previously installed spyware from communicating collected information outbound. It works with other anti-spyware programs, such as those that remove existing spyware applications from hosts.

The anti-spyware service analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware.

If spyware has been installed on a LAN workstation prior to installing the anti-spyware service, the service will examine outbound traffic for streams originating at spyware infected clients, and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the firewall identifies that traffic and resets the connection.

Intrusion Prevention Service (IPS)

Dell SonicWALL IPS delivers a configurable, high-performance DPI engine for extended protection of key network services such as web, email, file transfer, Windows services and DNS. IPS is designed to protect against application vulnerabilities as well as worms, Trojans, peer-to-peer, spyware, and backdoor exploits. The extensible signature language used in the DPI engine also provides proactive defense against newly discovered application and protocol vulnerabilities.

The DPI engine looks at the data portion of the packet. The DPI technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it by preventing the traffic from passing through. DPI allows a firewall to classify passing traffic based on rules.

These rules include information about Layer 3 and Layer 4 content of the packet, as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the firewall, as well as prevent them (such as dropping a packet or resetting a TCP connection). Dell SonicWALL DPI also correctly handles TCP fragmented byte stream inspection, as if no TCP fragmentation has occurred. IPS can be configured by status, global settings, or policies.

Application intelligence and control

Application intelligence and control is a set of granular, application-specific policies, providing application classification and policy enforcement to help administrators control and manage both school- and non-school-related applications.

Application control allows administrators to set policy rules for application signature. These include global policies, as well as policies that are more targeted. As a set of application-specific policies, this enables granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. This allows administrators to regulate web browsing, file transfer, email, and email attachments.

Dell SonicWALL firewalls integrate application control with standard network control features to provide more powerful control over all network traffic. The ability to control application layer traffic is significantly enhanced by the ability to view real-time application traffic flows, access the application signature database, and to create application layer rules. Application intelligence and control is available on all SuperMassive, NSA Series, and TZ400/TZ500/TZ600 appliances.

There are three flexible ways to create application control policies.

- The AppFlow Monitor dashboard enables the administrator to quickly configure policies for application blocking, bandwidth management, or packet monitoring. This allows the administrator to rapidly apply an action to an application that he or she notices while using the firewall visualization and application intelligence features. The policy is automatically created and displayed.
- The App Control Advanced page provides a simple and direct way of configuring global App Control policies. Administrators can quickly enable blocking or logging for a whole category of applications, and can easily locate and do the same for an individual application or individual signature. Once enabled, the category, application, or signature is blocked, or logged globally, without the need to create a policy.
- The App Rules page provides the third way to create a policy. Policies created using App Rules are more targeted because they combine a match object, action object, and possibly email address object, into a policy. For flexibility, policies can access the same application controls for any of the categories, applications, or signatures available on the App Control Advanced page.

Points for consideration:

- Dell SonicWALL IPS, anti-malware and application control outperform products that use a proxy-based approach because SonicWALL is not bound by file size limitations.

Wireless network security

Dell SonicWALL wireless network security solutions combine the performance of Dell SonicWALL firewalls and Dell SonicPoint wireless access points. Dell SonicWALL firewalls feature an integrated wireless controller that automatically detects and configures Dell SonicPoints across the network. Plus, Dell SonicPoints have a plenum-rated chassis for safe installation in a wide variety of environments, such as air-handling spaces, or above suspended ceilings.

The Dell SonicPoint ACe and Dell SonicPoint ACi are based on the 802.11ac standard, which can achieve a data rate of up to 1.3 Gbps, or 3x that of 802.11n, while maintaining a higher performance level at greater ranges, depending on environmental conditions. Dell SonicPoints support a wide range of wireless standards and security protocols, including 802.11 a/b/g/n/ac, WPA2 and WPA. This allows organizations to leverage prior investments in devices that are incapable of supporting higher encryption standards, while easing migration to 802.11ac.

The 802.11ac standard operates in the 5 GHz frequency band, which has fewer wireless devices competing for airspace and is therefore less prone to signal interference. In addition, 802.11ac uses wider 80 MHz channels and has more non-overlapping channels than 802.11n, which operates in the 2.4 GHz frequency band. All of these features combined yield a higher quality signal. The increase in bandwidth capacity and greater number of spatial streams, combined with 3x3 MIMO and the improved processing offered by 802.11ac, result in more reliable wireless coverage. Dell SonicPoints also support FairNet, which guarantees a minimum amount of bandwidth to each wireless client, to prevent disproportionate bandwidth consumption by a single user.

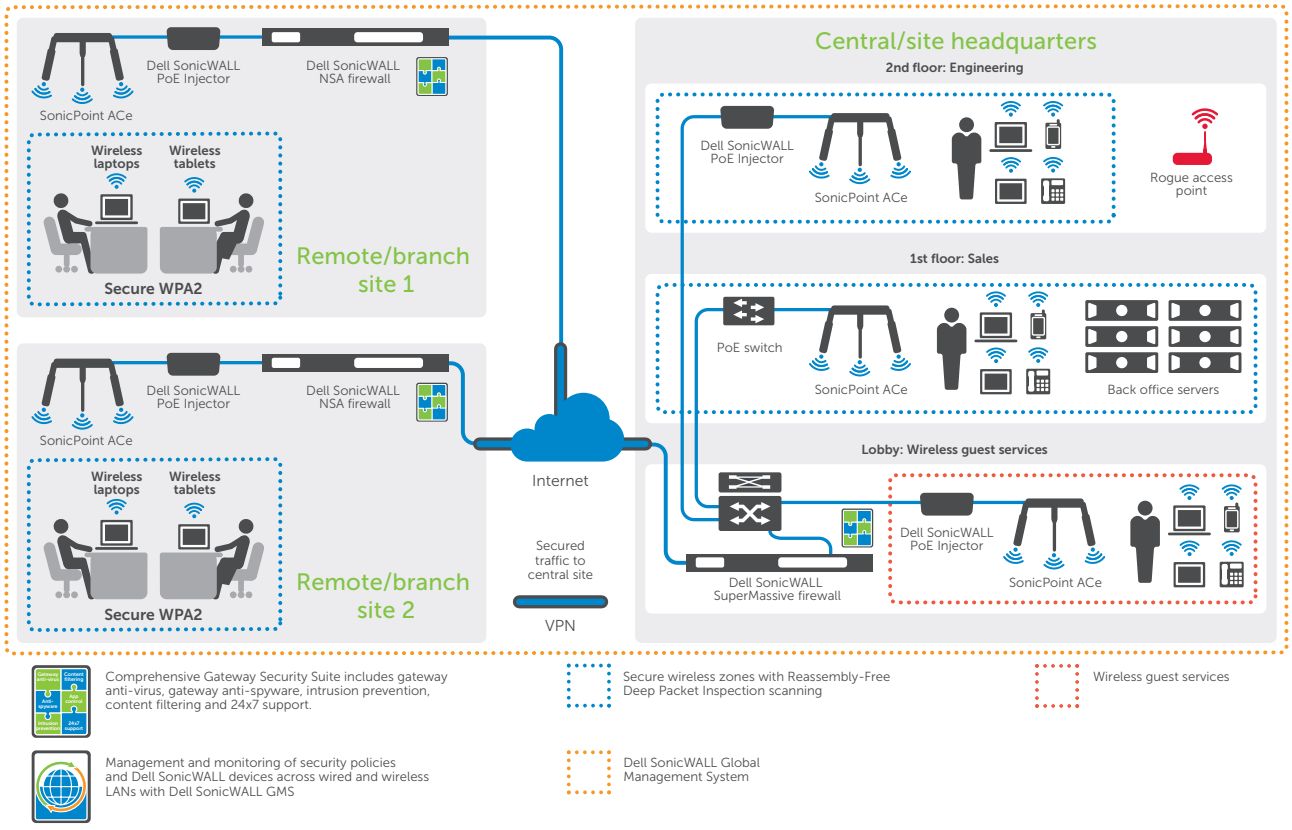
Wireless network security deployment

Dell SonicPoints are automatically detected, provisioned and updated by the wireless controller in the managing Dell SonicWALL SuperMassive, NSA, or TZ Series firewall. WLAN administration is also handled directly from the managing firewall, simplifying setup and centralizing ongoing management. Ongoing management and monitoring of Dell SonicPoints and security are handled centrally through the firewall or through the Dell SonicWALL GMS, providing administrators with a single pane of glass from which to manage all aspects of the network — both wired and wireless.

Dell SonicPoints are powered from a Dell SonicWALL IEEE 802.11at Power over Ethernet (PoE) Injector or third-party device for easy deployment where electrical outlets are not readily

Distributed Networks

Enterprise/campus deployments



> "With Dell SonicWALL, we can stay at the forefront of this changing landscape. We have a great business relationship with Dell SonicWALL, and its customer service and engineering support was outstanding."
>
> *C.J. Daab, Technology Support Coordinator, Hall County Schools*

accessible. The SonicPoint ACe can also be powered directly through an AC adapter. Dell SonicPoints are certified by the Wi-Fi Alliance. This validates them as interoperable with a diverse sampling of other certified equipment operating in the same frequency band. In addition, Dell SonicPoints enable both radios to enter sleep mode for power-saving when no clients are actively connected. The Dell SonicPoint will exit sleep mode once a client attempts to associate with it. With dimmable LEDs (excluding power), Dell SonicPoints fit perfectly into environments that need discreet wireless coverage.

Multi-RADIUS Authentication provides enterprise-class redundancy by enabling organizations to deploy multiple RADIUS servers in active/passive mode for high availability. Should the primary RADIUS server fail, the managing Dell SonicWALL firewall discovers the failure and switches to the secondary server, ensuring wireless devices can continue to authenticate. Further, multi-RADIUS authentication can be supported on each virtual access point and configured for WPA-Enterprise, WPA2-Enterprise, or WPA2-Auto-Enterprise mode. Administrators can create up to eight SSIDs on the same access point, each with its own dedicated authentication and privacy settings. This provides logical segmentation of secure wireless network traffic and secure customer access.

Wireless guest services enable administrators to provide internet-only access for guest users. This access is separate from internal access and requires guest users to securely authenticate to a virtual access point before access is granted. Lightweight hotspot messaging extends the Dell SonicWALL wireless guest services model of differentiated internet access for guest users, enabling extensive customization of the authentication interface, and the use of any kind of authentication scheme. Captive portal forces a user's device to view a page and provide authentication through a web browser before internet access is granted.

Dell SonicWALL NGFWs scan all inbound and outbound traffic on wired and wireless networks and eliminate intrusions, spyware, viruses, and other threats, before they enter the network. The same set of security policies can be enforced over both wired and wireless networks. An extension to local ACL, cloud ACL is deployed, and managed from a centralized RADIUS server in the cloud. This eliminates local ACL scalability issues, enabling organizations to configure authentication accounts based on their specific requirements. In addition, MAC authentication can be enforced on all Wi-Fi-enabled devices, even if they are not capable of 802.1x support. This adds another layer of protection to the wireless network.

For increased flexibility, Dell SonicPoints even allow for the dedication of one radio for wireless intrusion detection and prevention scanning to meet compliance mandates, while the other continues to support users. Wireless intrusion detection and prevention scans the wireless network for unauthorized (rogue) access points and then the managing firewall automatically takes countermeasures, such as preventing any connections to the device. In addition to intrusion prevention, SSL decryption and inspection, application control and content filtering, the wireless network security solution also integrates additional security-related features, including wireless intrusion detection and prevention, virtual access points, wireless guest services, cloud access control list, and more.

Points for consideration:

- Do you provide wireless access in classrooms today?
- Do you utilize the 802.11ac standard?
- Are you providing students with Wi-Fi-enabled devices, such as Dell Chromebooks?

WAN acceleration

The Dell SonicWALL WAN Acceleration Appliance (WXA) solution reduces application latency and conserves vital bandwidth, significantly enhancing WAN application performance, and improving the experience and productivity of faculty, staff, and students. WXA optimizes performance and reduces latency by transmitting only new or changed data across the network after initial file transfer, resulting in dramatically reduced traffic volumes. In addition, the managing firewall enables administrators to identify and prioritize application traffic, while the WXA minimizes traffic between sites.

Unlike standalone WAN acceleration products that are deployed either behind the firewall, or between the firewall and WAN router, the WXA series is an integrated add-on to the Dell SonicWALL NGFW. The solution enables comprehensive scanning for intrusions and malware, before accelerating the traffic across the VPN or dedicated WAN link, thus maximizing security and performance.

WXA dramatically reduces bandwidth consumption through byte and file caching. It decreases the amount of data transferred when downloading or accessing files from a shared drive, using Windows File Sharing (WFS) acceleration. Moreover, WXA client software allows traffic initiated from remote Windows PCs, or laptops running NetExtender, to be accelerated.

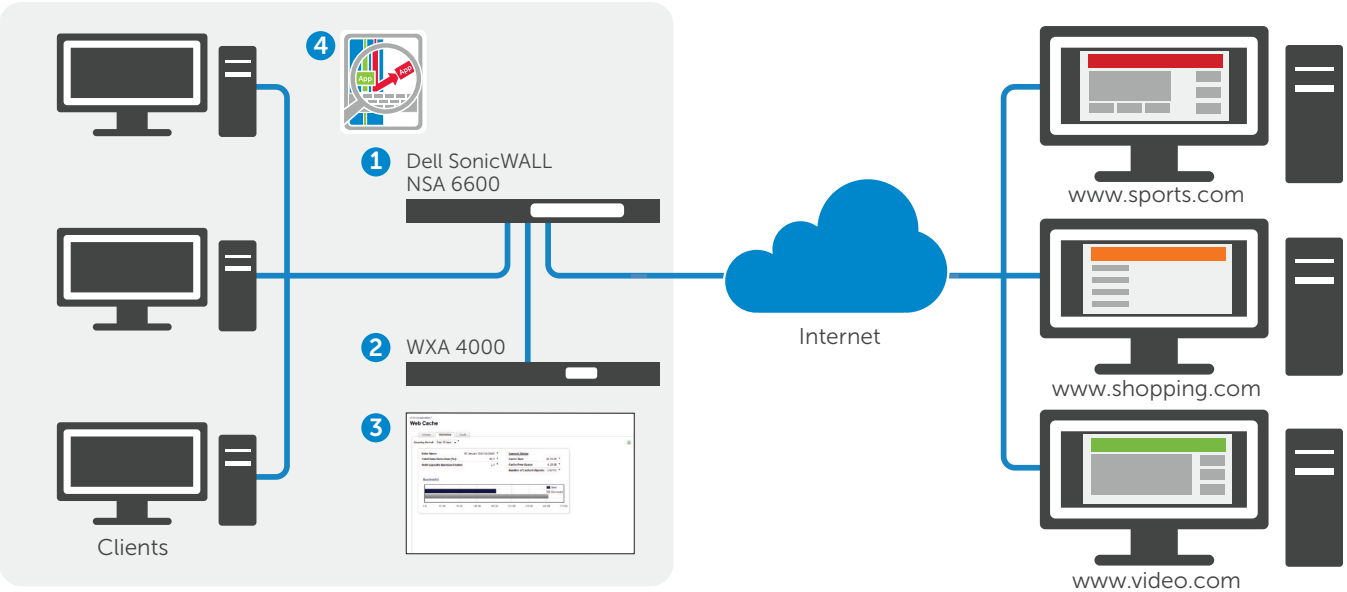
The Dell SonicWALL architecture streamlines the placement, deployment, configuration, routing, management, and integration of WXA with other components, such as VPNs. Consolidating WAN acceleration with core NGFW technologies, including intrusion prevention, anti-malware, and application intelligence, control and visualization at the gateway, significantly increases security, while lowering the TCO. There are a variety of WXA platform options, including hardware, virtual appliances, and software.

Districts can also scale to meet the WAN acceleration needs of a growing user population through clustering, which enables several WXA solutions to be linked together at each location.

For clustering, when a WXA is detected, and the default group has been set, the WXA is assigned to the default group. There can be any number of groups. A group can be assigned to each VPN or Route Policy. Traffic on that VPN is accelerated by the WXAs in that group. The same group can be assigned to more than one VPN or Route Policy, but each policy can have only one group. Each WXA in a group is given the same configuration, which is stored on the firewall. The configuration is set up on each WXA when the WXA first connects to the firewall, whenever the WXA is probed by the firewall (every 60 seconds), and whenever any aspect of the configuration is changed.

Web caching

Of particular value in K-12 environments, WXA can also improve browser response times with web caching. This feature behaves as proxy server for outgoing and incoming web connections. The web cache feature stores copies of frequently-visited HTTP web pages passing through the network. When a user requests one of these web pages, it is retrieved



from the local web cache instead of going out to the internet. This reduces the response time, while also saving bandwidth. Web caching is done transparently, without requiring users to reconfigure their browsers.

Minimal, moderate, and aggressive caching strategy options are available. These determine the objects that are placed into the web cache and how long they stay there. The web cache feature is capable of caching YouTube videos (currently only Flash video format is supported). This feature is only available when using moderate and aggressive web caching strategies.

WXA statistics graphs display the web cache data for the selected covering period and chart. The conveyed data is the number of bytes that would be sent from a web server without the use of the WXA series appliance's web cache. The sent data is the bytes that are actually sent from web servers, in response to the user's web request, with the remainder being served from the cache. A "hit" is when an object is served from the web cache instead of fetched from the internet. Charts can display data by summary, time, breakdown by individual WXA, and number of requests and hits over a period of time.

Conclusion

In summary, when evaluating a comprehensive network security solution, K-12 school districts should require the five key components of content filtering, SSL inspection, gateway security services, wireless network security, and WAN acceleration, as well as global management of all five. Content filtering protects students from harmful websites both at school and home on school-issued devices, in line with CIPA requirements. DPI-SSL enables the detection of increasing amounts of encrypted threats, while gateway security services prevent intrusions, block malware and spyware, and provide application intelligence and control, all needed to comprehensively protect the network from threats. Wireless network security extends that protection to provide secure, high-speed wireless access for students, faculty, and staff, using either school-issued or personal devices. In addition, WAN acceleration optimizes network bandwidth for academic applications to enhance performance and productivity, while an integrated global management system streamlines deployment, administration, and integration, to lower TCO.

Learn more: Read the brochure "Helping schools secure their networks."

"With two SuperMassives in an HA cluster, we have achieved 99.9 percent uptime, which is critical for our digital curriculum — while also saving $80,000 in operating expenses over the 18 months we've had them."

Tom Condo, Supervisor of IS Operations, Seminole County Public Schools

For More Information

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security

If you have any questions regarding your potential use of this material, contact:

Dell
5455 Great America Parkway,
Santa Clara, CA 95054
www.dell.com/security

Refer to our Web site for regional and international office information.