DELL SonicWALL

Ten easy steps to secure your small business

Small business network administrators need a workable plan to provide comprehensive security against today's sophisticated threats without spending too much time or money. This white paper presents a simple step-by-step approach to leveraging advanced protection technology in ways that are affordable, fast and easy.

Abstract

Small business networks face the same threats as large enterprise networks. However, they also contend with the challenge of limited budgets for IT expenditures. The role of administering the network in a small business often falls on the business owner or on the default in-house "techie," both of whom wear many other hats in the organization and usually do not have the time, resources or expertise to work on complex deployments and administration. Fortunately, the problem of securing a small business network can be addressed by taking advantage of modern network security technologies. The following 10 steps describe the primary challenges facing small network administrators today, and the solutions now available to resolve these challenges.

Step 1: Layer your security

Your challenge: bolster your defense against new threats at every layer

Every year, network attacks become more widespread, more intelligent and more difficult to detect. Entry points into the network, besides publically facing servers, may now include employees' laptops, desktops and smartphones accessing many of the media and content rich applications on the Internet. Because many of today's attacks are blended attacks which use multiple techniques at different layers to try to infiltrate your network, they can bypass outdated firewalls that only provide Stateful Packet Inspection for network traffic. With Stateful Packet Inspection, firewalls mainly ensure that connections are valid. However, they perform absolutely no inspection beyond the first few networking layers and thus do not concern themselves with the content carried within these data streams, allowing both desired and malicious data through.

Your solution: Unified Threat Management

The best way to secure your small business network today is with a Unified Threat Management (UTM) approach. UTM is the latest advancement in network security, bringing a new level of scrutiny to network traffic passing into an organization. Simply put, UTM firewalls combine the effectiveness of various point defenses to add protection at every networking layer.

The power of UTM comes from its simplicity: a single appliance that provides a powerful defense against a wide range of security threats, while extending beyond, the capabilities of regular Stateful Packet Inspection firewalls. This makes network protection more complete, affordable and easy to manage.

Step 2: Secure your gateway

Your challenge: block threats before they enter your network

The most effective place to block threats is at the network perimeter, before they can even enter your network. Threats can gain entry into the network over commonly used communication protocols which many businesses rely on today. Malware can hide in email, instant messaging (IM), peer-to-peer (P2P), file sharing, games or harmless-looking utility programs, and can often trick traditional client-based security.

Your solution: deep packet inspection at your gateway

Stopping today's ever-evolving threats such as viruses, spyware, malware-laden spam and key loggers at the gateway requires deep packet inspection that is capable of complete and comprehensive data inspection. When Deep Packet Inspection technology is properly deployed at the gateway, it scans the entirety of the data packets that come into the network, instead of just looking at packet headers, and thus provides an insight into the contents of the data stream. It is then capable of catching threats that are hidden inside files, applications and attachments.

Step 3: Keep it simple

Your challenge: cut out the cost of complexity

The total cost you pay for security isn't only measured in its list acquisition price. It's also in the cost of installing, using, managing and maintaining your solution. Small businesses do not have to tie themselves down with complicated technology that demands extensive training, endless add-on features and consulting services to operate.

Your solution: simplify your technology

Modern security appliances can make set-up and management easy, using features like intuitive web-based interfaces and object-based policy management; automatic synchronization with existing user directories; and easy-to-use configuration wizards designed to guide users through the configuration steps for most common network setup scenarios. Configuration can be made even simpler by combining what would otherwise be several appliances from different vendors into a single appliance with a coherent configuration interface for all networking tasks. Centralized or hosted management can further ease administration and ultimately lower ongoing cost of ownership.

Step 4: Keep it affordable

Your challenge: avoid having to buy and maintain multiple security products

Threats online continue to proliferate and become more sophisticated as our lives become increasingly digital with the use of Web 2.0 applications. Purchasing traditional standalone point products to protect against all these threats can quickly drive up IT costs with separate expenses for each device's purchase, installation, operation, training, administration and maintenance. Additionally, point products may not work seamlessly together to provide full protection, and therefore need a great deal of manual integration and countless administrative hours to even come close to providing a coordinated defense. Managing many different security tools can be overwhelming, inefficient and expensive.

Your solution: consolidated security

Reduce your costs for hardware, set-up, operations and administrative overhead by consolidating multiple security tools in one easily managed, affordable appliance. Consolidated UTM solutions let you deploy broader and better-coordinated security within your budget. However, you need to make sure your UTM solution comes with enough features, so that it doesn't force you to purchase separate appliances to fill in the holes. For example, with some UTM solutions, features such as SSL VPN for remote access, secure wireless, comprehensive anti-spam and application filtering could require separate appliances, taking away the benefits of consolidation.

Step 5: Get rid of bottlenecks

Your challenge: fully utilize your network bandwidth

Bandwidth is more affordable and available than ever. The amount of traffic being scanned by your firewall—as well as the increasing amount of threats and malware lurking in that traffic—is quickly becoming more than many firewalls can handle. Inspecting every byte of every packet can overwhelm some firewalls and bottleneck network performance.. Some UTM solutions also need file caching for Deep Packet Inspection, which can create new bottlenecks and force administrators into making a difficult tradeoff between security and performance.

Your solution: high-performance hardware and software priced for small business

For optimal performance while maintaining maximum security, solutions such as reassembly-free deep packet inspection UTM help to deliver throughput that won't bog down performance. Clever algorithms help to reduce latencies to non-noticeable levels. Also, advances in microprocessor technology, especially those designed for network processing, allow UTM appliances designed for small businesses to gain incredible network efficiency.

Step 6: Keep your systems running

The challenge: don't risk your business on single points of failure

Hard drives fail. Traffic demands can overwhelm available bandwidth. Internet services can drop. These are merely facts of modern life. But when pieces of your critical infrastructure fail, it shouldn't mean your business grinds to a halt. Not only should your firewall prevent threats from entering your network, but it should also be resilient enough to help you keep your business running.

Your solution: integrated duplication and failover

Modern UTM solutions feature integrated redundancy and failover features that make sure your network's operation doesn't rely on a single point of failure, so your business continues without interruption. For example, hardware failover functionality can automatically roll security functions over to an identical UTM appliance should the primary device fail, and revert back once the primary appliance is restored. Load balancing can automatically fail over or balance traffic loads, both on inbound and outbound connections, to allocate resources on both internal servers and Internet links. And while a failure of a primary WAN connection would usually mean complete loss of Internet access, with WAN failover, a secondary link can take over all network operations while the primary link is serviced. The failover can even fail back on 3G wireless or an analog modem when other backup network connections are not available.

Step 7: Keep your network productive

Your challenge: weed out non-productive traffic

Today's business networks can be choked by spam, unauthorized web activity and social networking traffic that have nothing to do with getting work done. If you turn a blind eye to the use of new web-based applications infiltrating your network, you are opening the door to security and productivity issues that will only increase over time. You need to control the potential threats and bandwidth shortages posed by these applications while empowering users to make the best business use of the web. At the same time, blocking ports and protocols is an ineffective way of identifying and controlling these rogue applications.

Your solution: content and application management

Fortunately, modern application layer inspection tools are able to extend protection beyond basic port blocking and inspection and can scan data, communications, file attachments and applications that pass through the network security appliance. These tools rely on a powerful Deep Packet Inspection engine and signature databases to identify applications in real time, providing granular application level controls. Not only can this prevent potential threats, but it can also help you prevent bandwidth shortages created by non-productive applications, while still empowering users to make the best use of the web and email for legitimate business purposes.

Step 8: Stay compliant

Your challenge: meet regulations and avoid penalties

Today, almost every small business must comply with external regulations (such as PCI, HIPAA, GLBA or SOX) or internal regulations (such as polices for protecting intellectual property). For many compliance requirements, encryption and archiving alone are not enough. To make sure your business is in compliance, you need total network security and policy enforcement, as well as robust management and reporting.

Your solution: integrated compliance management

Modern UTM solutions often meet or even exceed regulatory security and enforcement criteria by casting a wider net of advanced security features. At the same time, these solutions often seamlessly integrate with centralized policy management, backup and reporting options to help you track, audit, report on and verify your compliance, if required.

Step 9: Secure your endpoints

Your challenge: manage your endpoint devices

Today, your office is where you are: at home, at the airport, at a café. And, customers, partners and contractors need access to your business from anywhere. You have no control over whether the users keep their anti-virus fully updated, if they have it at all. The chances are higher that these devices might be infected with viruses and other malware that can enter your network as soon as those devices connect to it, whether locally within your building or remotely over VPN.

Your solution: clean endpoint security

New security techniques can check the endpoint devices and verify whether or not they are running an anti-virus solution with the latest signature database, before they connect to your network remotely, and even update the needed security on them automatically. In addition, Clean VPN technology that combines SSL VPN secure remote access with UTM, as well as Clean Wireless technology that combines high-speed wireless with UTM, can ensure that once an authorized connection is secured to your network, all the traffic running over it is also safe, secure and free from threats.

Step 10: Be prepared for the unexpected

The challenge: prepare for unexpected disruptions

Even the best UTM-secured network needs a disaster recovery solution. Major disasters like Hurricane Katrina have demonstrated how exposed small businesses can be to unexpected events. But it's not only headline-grabbing natural disasters, health pandemics or terrorist attacks that can disrupt a business. Building fires, broken water pipes, power outages, equipment failures, or even lost or stolen laptops, can mean disaster for small businesses, and potentially disrupt your operations indefinitely if you are not prepared.

The solution: integrated secure remote access

Modern UTM appliances can feature integrated IPSec or SSL VPN capabilities. SSL VPNs are best suited for secure remote access during an emergency because they allow workers and partners to connect safely to corporate network resources using a web portal, without having to pre-install clients. Modern continuous data protection (CDP) solutions can automatically backup data and applications to discs, avoiding the complexity and human error involved with tape backup. Backup to a secure secondary business location or third-party site means business systems can be restored and operational even in the primary site is compromised. Bare metal recovery (BMR) technology enables entire operating systems, such as database or file servers, be recovered to new or different hardware platforms if the original device can't be restored.

DELL SonicWALL

The Dell SonicWALL solution for SMB network security

Dell SonicWALL® can help you to execute all 10 steps to securing your small network with affordable, effective, easily deployed solutions.

The Revolutionary Dell SonicWALL TZ Series

Engineered specifically for small networks and distributed sites, the state-of-the-art Dell SonicWALL TZ Series, including the TZ 105, TZ 205 and TZ 215 firewall appliances, simply offers the most comprehensive Unified Threat Management (UTM) solution available for under $1000.

The revolutionary TZ Series appliances shatter the performance limitations of other UTM products by offering the fastest multi-layered network security in their class. Combining Dell SonicWALL's industry-leading UTM—featuring gateway anti-virus, anti-spyware, intrusion prevention, enforced desktop anti-virus, content filtering, and Application Firewall—and patented[1] Reassembly-free Deep Packet Inspection™ technology, the TZ Series delivers in-depth protection at unparalleled performance. The all new TZ Series dramatically expands the comprehensive protection critical for securing distributed environments and SMBs, at a performance level that will not compromise network throughput. Additionally, TZ Series appliances cost-effectively integrate IPSec and SSL VPN remote access, Voice over IP (VoIP), and optional 802.11b/g/n wireless with optional 3G wireless broadband failover. Built to meet the needs of small- to medium-sized businesses, retailers, managed service providers, distributed enterprise sites and branch offices, the TZ Series is the first affordable solution that can maximize the highest speeds available from modern ISPs while delivering full UTM protection. Each TZ appliance is also available as a Dell SonicWALL TotalSecure™ solution, conveniently bundling all hardware and services needed for comprehensive protection from continually-evolving network threats.

Dell SonicWALL Comprehensive Anti-Spam Service

The Dell SonicWALL Comprehensive Anti-Spam Service utilizes real-time sender IP reputation analysis and cloud-based Advanced Content Management techniques to remove spam, phishing and virus laden messages from inbound SMTP-based email before they reach your network. This service eliminates the need for less effective, slow responding and error prone real-time black list services.

Dell SonicWALL VoIP

Dell SonicWALL's robust capabilities for Voice over IP (VoIP) offer secure, standards-based support for sending voice (audio), streaming video and other media over IP-based networks. All VoIP traffic between third-party VoIP telephony devices can be easily secured with UTM over SSL VPN or IPSec VPN tunnels using the TZ Series appliance

Dell SonicWALL Clean VPN

Dell SonicWALL Clean VPN delivers the innovative dual protection of SSL VPN combined with the high-performance UTM on TZ Series appliances.

Dell SonicWALL SonicPoints™

Dell SonicWALL SonicPoint™ and SonicPoint-N™ Dual-Band (802.11n and 802.11a/b/g) wireless access point devices and Dell SonicWALL Power over Ethernet (PoE) Injectors complement UTM to flexibly extend comprehensive security across wireless networks.

Dell SonicWALL Clean Wireless

Dell SonicWALL Clean Wireless unites high-speed secure wireless and high-performance UTM through the deployment of Dell SonicWALL TZ appliances with SonicPoints.

Dell SonicWALL Continuous Data Protection

Dell SonicWALL Continuous Data Protection (CDP) Series offers the only complete end-to-end backup and recovery solution for small business networks. An ideal replacement for tape-based systems, CDP provides foolproof, intuitive, continual protection. Policy-driven CDP is transparent to the end-user, ensuring that data, applications and systems are reliably protected. Because most recovery involves a single file, CDP's self-directed restore by the end-user helps meet service levels while reducing burden on IT support. Dell SonicWALL CDP takes the complexity out of safeguarding your data by automating tedious tasks to provide a true low-touch solution. CDP provides flexible Offsite Data Backup, Site-to-Site Data Backup, Local Archiving and Bare Metal Recovery with Dell SonicWALL Universal Restore options to address any disaster recovery scenario.

Dell SonicWALL Global Management System (GMS®)

Dell SonicWALL's award-winning GMS provides network administrators with the tools for simplified configuration, enforcement and management of multiple global security policies, VPN and services for multiple systems, all from a central location. Dell SonicWALL Analyzer reporting software graphically illustrates network activity, such as bandwidth utilization, VPN reporting, threats observed, web site usage, and more. .

---

[1]U.S. Patent 7,310,815–A method and apparatus for data stream analysis and blocking.

Conclusion

In order to counter all of today's sophisticated Web 2.0 threats, a network administrator would need to upgrade their protection and deploy several different defensive techniques. However, small businesses do not have the budgets for maintenance contracts or personnel necessary that can purchase, configure and maintain these point solutions. At the same time, small businesses cannot afford to skimp on security. In fact, little security can be worse than no security at all, since a false sense of security in a network protected by a minimal firewall can lead people to be more likely to fall victim to attack. Dell SonicWALL TZ Series Unified Threat Management firewalls, especially when under GMS management, offer all the steps necessary to secure today's small networks and stay ahead of sophisticated Web 2.0 type threats in a single, consolidated multi-layered security solution that is it easy to afford, deploy and maintain.

DELL SonicWALL