

D-Link Solution Brief

Network Security for SMB

Defending Your Network-Dependent Business



Abstract

This brief provides a short introduction to the increasing importance and growing dependence upon reliable networks to carry out today's business processes. Discussed are the computing trends that have placed new requirements on network security for small and medium sized businesses. The security risks and possible network security solutions available to small and medium sized businesses are also covered.

Network Security Requirements

The importance of networking to businesses of all sizes has increased dramatically over the last several years. As companies have continued to enjoy productivity gains through automation and faster access to information for decision support, they have consequently deployed more business processes and applications that rely on network connectivity to key computing resources and data depositories. Networks today provide a key communications infrastructure for mission critical applications and business processes. With more and more mission critical applications running over networks today, the protection of those network-attached resources from exploitation comes to the forefront for many businesses. The challenge at hand for most businesses is trying to effectively balance the needs of making applications and data more accessible to the right people while keeping those same applications and data tougher to access and exploit by the wrong people. Current trends in computing and networking make this balancing act quite difficult for many businesses. Consider some of today's trends that require businesses to open up resources for wider access and as a result generate further requirements for network security.

Mobile Computing, Virtual Offices, and Remote Access

The trend towards pervasive computing continues at a strong pace. Some analyst reports have estimated that for the first time this year, the percentage of notebook and laptop computers has outpaced the sales of desktop computers. In addition, handheld computers, devices, and Personal Digital Assistants (PDA) making connections to IP based networks is also increasing. Other reports have also shown that more people are working from either homes or virtual offices. As a result of more workers performing their tasks outside the office, the demand for further levels of remote access to company resources is increasing. Employees increasingly need to connect to critical computing resources from customer sites, hotspots, homes, remote offices, and other disparate locations. Not only do critical computing resources need to be made available for remote access, the time and location of those access attempts is becoming more varied and unpredictable.

Business Process Collaboration and Dependence

Access to critical computing resources is becoming more important not only to employees, but also to business partners, vendors, and customers. Web applications are commonplace today to support business processes that involve vendors and customers. Customer Care, Logistics, Channel Partner, and other knowledge-based systems and applications have been designed to be accessible over the network and have grown to be mission critical. Collaborative efforts can sometimes lead to unusual partnerships with competitors on certain initiatives. The reality that you need to make your network more secure while opening it up to wider access from potential competitors can appear counterintuitive. That is the reality of business today.

Virtual Private Networks

Another trend that has been in place for some time is the continued migration away from private networking. Businesses have found that eliminating private networking infrastructure in favor of using the existing public Internet to provide WAN connectivity can save significant costs. The result however is that confidential intracompany data may be traversing the open public network where it could become vulnerable to eavesdroppers.

eBusiness Dependence

Transaction speed and lower transaction costs have many more companies conducting some or all of their business over the Internet. These web-based applications can be very critical to their business and in some cases their only stream for revenue generation. On the other hand, these web applications also require deeper levels of access to protected company data in order to carry out the online transactions. Uptime and availability of the key resources enabling revenue generation for a company are paramount and need to be secured and protected.

Laws and Regulations

Another driver for more intensive network security is the necessary compliance to newer laws and regulations. Key regulatory mandates like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act, the Graham-Leach-Bliley Act, and newer Homeland Security initiatives place mandatory directives on the way that companies must maintain and secure data and information. They also require in some cases public disclosure of security breaches. The loss of business, damage to reputation, and bad publicity of such forced disclosures has prompted many companies to re-examine their network security policies and infrastructure.

The real driving force behind all these trends is business competition. As competition in the global economy becomes even more aggressive, the chance for wider and deeper access to a company's computing resources and confidential data is even greater. Out of necessity companies will be forced to open up to further levels of vulnerability. The only option a company has is to protect their network and critical computing resources from the ever-increasing security risks just so that it can effectively compete.

Network Security Risks

Industry news regarding network security risks seems to be more visible and more prevalent every day. The number of incidents has certainly increased, but what is even more concerning is the heightened coordination and sophistication level of more recent security attacks. The types of attacks or network security risks have become more diverse and include many different types. Several of those risks can be broken down into one of several risk types.

Crackers / Hackers

"Hackers" was a term originally coined to refer to computer programmers who used inventive methods to solve software problems. A "cracker", on the other hand, represents the dark side of hacking and refers to a hacker with malicious intent or motives. The mainstream media today does not discern the difference between hackers and crackers even though the industry does. The objectives of crackers are to break in or gain unauthorized access to a target's computer systems in order to exploit or steal data, application program access, or mask other unauthorized uses of the company's resources. Crackers will exploit your computer systems and commandeer resources for their own malicious intentions. The 2005 CSI/FBI Computer Crime and Security Survey showed that a full 48% of total dollar losses for companies surveyed came as a result of unauthorized access and the theft of proprietary information.

Thus, the survey shows that nearly half of all calculated dollar losses are the result of damage inflicted by crackers. What this tells us is that even though crackers may not be the most prevalent of all the risks in terms of the number of attacks, they can inflict the most financial loss to a company.

Malware

One of the biggest security risks today is posed by the spread of malware, which can include viruses, worms, Trojan horses, spyware, key loggers, and other malicious software that can easily be passed from system to system by ever more complex means. The attack types falling under the category of malware represent the single largest risk to network and system security. The Global State of Information Security 2005 worldwide study by CIO and PricewaterhouseCoopers revealed that 59% of attacks were the result of malware. In addition, the same study found that 68% of all attacks were perpetuated through the use of an email virus.

While viruses and worms have been around for some time causing a nuisance and in some cases causing considerable damage to data, the last couple of years have shown that malware is becoming more widely created for purposes of profit or exploitation. One example is the creation of “zombies” or computers that have been compromised and taken over for use in some illicit activity without knowledge by the computer’s owner or administrator. “Zombies” can be created to send out illegal spam email or to store and transfer illegal copies of copyrighted movies or music. Spyware is another malicious software exploit that can collect information including credit card numbers, Internet usage patterns, file types, and other private data from computer systems. That information is then unknowingly transferred to perpetrators who can use the data for profit or exploitation. The use of malware has definitely migrated from the old stereotypical teenager looking for a challenge and causing some mischief to more sophisticated and organized criminals and networks.

DoS Attacks

Exploitation of resources also comes in the form of Denial of Service (DoS) attacks where a cracker takes control of a resource and makes it unavailable for its intended function. For example, a company may do all of its business online through its ecommerce website. If the server were compromised and taken over by a cracker, that business could essentially be prevented from taking another order for that company’s products. The revenue impact could be crippling and affect the ongoing viability of the business.

Common Denial of Service attacks could also be targeted at server systems used for websites or email. DoS attacks usually render a server useless for its intended function by occupying the server resources with an unlimited number of false requests. The server spends all its time responding to the false requests keeping it from its intended function of responding to normal function such as servicing browser requests or processing email.

Denial of Service attacks can be targeted at servers, systems, routers, firewalls, or any other device on the network and can cause considerable outage and downtime for critical resources.

Internal Threats

Security threats from outside of the business are normally more common and protected against more vigorously. The reality is, however, that attacks can also originate from corrupt or disgruntled employees, former employees, onsite contractors, or guests. Using their inside status as an employee or using their legitimate access to computing resources, they overstep their bounds into sabotage, theft of proprietary information, corporate espionage, or destruction of company records and information. Internal threats, while not great in overall incident numbers, can be very damaging. Internal threats tend to be very targeted and because of the inside knowledge tend to be aimed at high value resources.

Inappropriate Use

A growing risk that has most recently been added to the umbrella of network security is referred to as “inappropriate use.” Inappropriate use refers to employees who are not using company resources, to which they have legitimate access to, in a means for which they were intended. For example, a number of companies have Internet access for which their employees use daily as a part of carrying out their normal business functions or tasks. But that Internet access may also be used for personal matters not related to their job functions. In this case costly network bandwidth could be wasted by employees downloading personal email, swapping music and video files, streaming content for personal use, viewing pornography, using chat programs, visiting questionable web sites, or a host of other potential uses of the network that is not associated with their job.

Even a seemingly innocent email forwarding of a joke results in the use of email resources, network bandwidth, and additional storage that a company must waste. More companies are taking stronger action against inappropriate use by establishing company policies and creating acceptable use policies and agreements for its employees. Some companies view these acceptable use policies as liability protection against employees carrying out illegal or offending activities with company resources.

Network Security Solutions

As we can see by the growing industry requirements for network security and the ever-increasing complexity of network security risks, companies are faced with the difficult decision of not “if” they should deploy network security, but “how” they should deploy network security. If companies want to compete, they will be forced to provide wider access to their business processes. This will mean wider access to their networked computing resources.

Network security is therefore a necessity for any sized business. The risks, however, are magnified even greater in small and medium sized businesses where the stakes are higher. The financial loss associated with a security breach can have a much greater impact to the ongoing viability of a small or medium

sized business than it would with a larger company. Security breaches in small and medium sized businesses could be catastrophic. Therefore, small and medium sized businesses need to develop and execute a network security strategy.

That strategy should include a layered approach of protecting networks as well as systems. The strategy should consider the risks not only from external means but also factor in the risks of internal exploits. The network security strategy should include protection against all the major risks. The defense that a small or medium sized business implements should consider the following solution sets as a part of their overall network security strategy.

Firewalls

Firewalls are a necessary and basic layer of defense for both the network and attached resources. Firewalls can be deployed in either a dedicated perimeter device or on individual computers. A layered defense would include both system-based firewalls as well as dedicated firewall hardware for perimeter protection. A dedicated network firewall is positioned between two networks and acts as a monitoring device to check all traffic coming into and out of a trusted network. A typical firewall application would be used to connect a company network to the Internet. The firewall would monitor all traffic against a set of security policies set up in the firewall. If any traffic were flagged by the firewall as not meeting the configured policies, then that traffic would be filtered and not allowed to pass from the Internet to the trusted network. Normally standard firewalls can filter and pass/block traffic based on the checking of certain parameters like IP addresses, domain names, or UDP and TCP ports.

By filtering traffic with malicious intent, a firewall can protect the trusted network from unauthorized remote access, unsolicited traffic, and denial of service attempts. Firewalls may also be considered to protect against internal threats as well. A perimeter firewall alone cannot protect against exploits generated from the internal network towards other internal systems. That is why companies are now deploying firewalls to protect critical resources within the trusted network from internal attacks. A layered approach to security would consider the deployment of both perimeter and internal firewalls for full protection.

Intrusion Detection & Prevention

Firewalls alone cannot always protect against most Trojan horses, worms, and other malware. Intrusion Detection and Intrusion Prevention technology are more effective against malware risks. Intrusion Detection contains a level of intelligence above that of firewalls that filter packets based on certain fields. Crackers have learned how to mask their malware in packets that can pass through a firewall. The method that an exploit uses to penetrate the network, however, will leave a "footprint" or "signature".

Intrusion Detection Systems (IDS) look for patterns of usage and traffic that match a known signature. For instance, a typical tool or method for crackers is to do a “port scan” against a particular host in order to determine what applications that host may be running. Simply speaking, a port scan can tell a cracker what doors are open for possible penetration of a system. A typical port scan, however, will result in a traffic pattern of many successive packets requesting connections to several different port numbers of the same host. While each of these properly formatted and normal appearing packets could successfully pass through a firewall, an IDS could look beyond the packet level scope and notice and detect the overall traffic pattern. If the traffic pattern or signature matches the signature in the IDS database of a known exploit, then the IDS device can flag and/or filter the traffic from the trusted network.

The key for IDS devices is that they can only match against a list of known signatures. Therefore, signature updates or pattern files must be updated on an ongoing basis in order to keep pace with new viruses, worms, Trojan horses, and DoS exploits as well as the new methods deployed by crackers. While IDS functionality was initially introduced in a separate dedicated IDS product, the market is now delivering IDS function in some combined firewall products. One should never assume, however, that a firewall has IDS functionality or that an IDS device has firewall functionality.

Virtual Private Networks

With the growth in notebook and laptop usage combined with greater numbers of employees working outside the office, the need for a more secure level of remote access to company resources and data is required. Remote workers are accessing company networks and resources while using the public Internet as the infrastructure to carry out that communications. Those communications could include company proprietary and confidential information, trade secrets, and private customer data. In order to better secure the information being sent across the public Internet, Virtual Private Network (VPN) technology can be used. VPNs allow for the encrypted tunneling of traffic from one location to another location across the Internet. By encrypting the traffic, it is rendered useless to anyone who may intercept the traffic on the public network and does not have the proper encryption keys. Encrypted tunnels are initiated by a VPN client that can run on an individual computer or on a network device such as a router. Encrypted tunnels are then terminated with a VPN gateway. Note that a firewall could also have VPN gateway function built in.

Anti-Virus Solution

Virus protection is an important component of network security. Anti-Virus solutions protect a system, a server, or a network from the threat of worms and other malware. Anti-Virus protection can be deployed on individual systems, email servers, or at the network perimeter. A layered security plan would deploy multiple types of Anti-Virus protection in order to protect from both external and well as internal risks for viruses. The Anti-Virus protection deployed will scan

files, especially email, for infected files or attachments. The use of a perimeter device or gateway scanner can only provide protection from external threats, but is easier to manage and administer than Anti-Virus software on every system in your network. Since new worms appear frequently it is important to have an Anti-Virus solution that is constantly updated with signatures or pattern files for new attacks and exploits. Perimeter Anti-Virus solutions can be deployed as part of a combination firewall device.

Application Security & Policy Enforcement

One area of network security that is most recently increasing in visibility and importance is the acceptable use of the network by a company's employees. In an effort to define how company resources should be used and to attempt to limit its own liability, more companies are establishing acceptable use policies and guidelines. Companies are looking to protect themselves against potentially illegal or offending use of the network and Internet by its employees.

Another driver for companies is cost control and efficient utilization of its computing and networking resources. Internet connectivity is a recurring monthly expense for businesses and the cost is based on the speed and capacity of the link. When the capacity needs to be increased, then the costs will also increase. This has focused more companies on taking steps to ensure efficient utilization of the link. Some companies have written restrictions into their acceptable use policies that attempt to limit employee usage of the Internet for personal, non-work related activities. Companies would rather not waste their Internet bandwidth with employee's personal email, music downloads, streaming content, instant messaging, or pornography and other offending material.

The reality for businesses however is that until recently the tools to monitor and enforce these policies have been limited and required a manual and time intensive effort. Only recently have vendors started to deliver products to address application level security and policy enforcement. This new class of Application Security Gateways can help to both manage and control the use of instant messaging, peer-to-peer, personal email, streaming media, and other applications. Application Security Gateways can effectively aid in bandwidth management and also help eliminate the spread of malware and the external leaks of company information through these applications. In addition Application Security Gateways can help enforce browsing policies by blocking access to questionable or offensive websites. Since seven-layer application security capabilities are fairly new, it is unlikely that you will find this capability built into firewall devices at this time. The other important feature that you want to consider for Application Security Gateways is the real-time traffic monitoring and reporting capabilities. These reports are important for trending and the identification of new risks and the need for further policies.

Implementing Network Security

With the growing requirements for deeper levels of access to company networks and the increasing number of risks and exploits, small and medium businesses have no choice but to deploy network security. There really is no choice on whether to deploy network security or not. The risks of not deploying network security are too great and the loss from just a single security breach can be catastrophic to a small or medium-sized business.

So, all businesses concerned with their ongoing viability will deploy network security solutions. In those deployments there are considerations and options that should be evaluated. Some of those deployment options are discussed further in the following sections.

Perimeter Firewall Deployment

The most common security solution deployment for small and medium sized businesses will be for perimeter firewalls. A perimeter firewall should be the absolute minimum level of security deployed by a business. An important point to consider is that not all firewalls are created equal. Firewalls come in different makes and models and many available today are combining functions to also include VPN gateway function, intrusion detection, and anti-virus. The features available in the perimeter device need to be considered against the security risks and requirements of the business.

A perimeter firewall is normally positioned at points of the network where external connections are made. The most common situation is to place a perimeter firewall on the Internet access link for a business. A perimeter firewall is normally located just inside the network router that handles the link to the outside world. It is put in this location to filter and examine all traffic destined to and from the external network connection. Note that in some cases it may be necessary to host an email or web server "in front" of the firewall providing it direct unprotected Internet access on a special network called a DMZ. Perimeter firewalls can also be deployed in redundant configurations for an extra level of resiliency.

Interior Firewall Deployment

While a perimeter firewall may protect company resources from the outside world, it cannot help with defending against internal attacks. That is why some businesses will choose to deploy interior firewalls to shield important resources from internally generated attacks. Interior firewalls represent a deployment of layered defenses and add additional security protection to a company looking to defend against all situations. A consideration for Interior firewalls is that they must be high performance. Every frame destined for key high usage computing resources will need to traverse the firewall. Wire speed processing is required for interior firewalls.

Host Protection VPNs

When a company decides that it needs secured remote access in order to protect confidential information on the Internet, it will deploy a Virtual Private Network. How that VPN is deployed will be based on the requirements for access. VPNs can offer host privacy where the encryption and the VPN client reside on a particular computer. VPN Client software is required for the computer that in most cases is a mobile notebook computer. The client software on the computer will create a secure tunnel across the Internet with a VPN gateway on the perimeter of the company network. The advantage to host-based VPN clients is that the host can be moved to any network with Internet access including customer networks, public hotspots, or residential broadband connections. The most important consideration when using host VPNs is the compatibility of the VPN client software with the VPN server running in the perimeter VPN gateway. If the client software and the VPN gateway are from different vendors, then you need to ensure compatibility before wide scale deployment.

Network Protection VPNs

The alternative to a host-based VPN is a network-based VPN. In a network-based VPN, the privacy for all computers on the network is secured across the public Internet. The VPN client for a network-based VPN is contained within a network connectivity device. That device is most often a VPN router. The router will receive traffic from any host and will create encrypted tunnels with the VPN gateway located on the company's network perimeter. The advantage of network VPNs is that many computers can have secured privacy without any special software installed on those computers. The router does the encryption for all the computers and thus removes the processing burden from those computers. The restriction is that any computers moved to another network without a VPN router are no longer protected. As a result network based VPNs are usually deployed for home, branch, or satellite offices where multiple computers in a single location need secured remote access.

Application Security

Application level security can be deployed in a multifunction firewall at the network perimeter or it can be deployed in a separate gateway. If application security is deployed in a separate device, then that device should be positioned inside the perimeter firewall. Most application security gateways are two port inline devices. A feature to look for in dedicated application security gateways is a bypass function for resilient network connectivity if the application security gateway were to fail or become powered down.

D-Link Network Security Solutions

VPN Client Software

DS-601 NETDEFEND VPN Client Software (1-User License)
Recommended Retail price R230.00

DS-605 NETDEFEND VPN Client Software (5-User License)
Recommended Retail price R700.00

VPN Firewalls

DFL-800 NETDEFEND Desktop VPN Firewall
Recommended Retail price R5,900.00

DFL-1600 NETDEFEND Rackmount VPN Firewall
Recommended Retail price R26,300.00

Application Security Gateways

DFL-M510 NETDEFEND Application Security Gateway
Recommended Retail price R8,999.00

For more information on the D-Link product range, please contact D-Link Africa on 08600 DLINK (35465) or (012) 665-2165 or visit our website at www.d-link.co.za

For PR/marketing questions: Karien Wood karien@d-link.co.za 083 556 4443
For product specific questions: Tobie van Schalkwyk tobie@d-link.co.za 083 276 1627

The D-Link product range is distributed in South Africa through Comztek, Mustek and Pinnacle Micro.