Ensuring the Success of E-Business Sites

January 2000

NETSCREEN

Executive Summary

Critical to your success in the e-business market is a high-capacity, high-availability and secure web site. And to ensure long-term success, you know you need to move at Internet speed to stay ahead of the competition.

NetScreen Technologies Inc. purpose-built security appliances are used by leading e-businesses to secure their web sites and keep them operating at optimal performance. NetScreen products combine firewall, VPN and traffic shaping functionality in a high performance, ASIC-based security appliance. The NetScreen-100 received Data Communications' Tester's Choice awards for both firewall and traffic shaping. Data Communications found that the NetScreen-100 "offered the best combination of airtight security, screaming performance, and simple management."

NetScreen-100 firewalls are securing the sites of emerging dot.com companies as well as some of the highest traffic portals and e-business sites on the Internet.

Table of Contents

Introduction

Your company's e-business success depends on your web site. First you have to race to get your offering to the market ahead of your competition. Then you work hard to bring a prospect to your site. But after all that effort if they need to wait more than a few seconds to access a web page, they are gone - probably for good. You need to make sure your site will always be available and will deliver the response time your users demand. Internet brownouts and blackouts are unacceptable.

In addition to getting to market quickly and delivering high availability, you need to make sure the site is secure. Hackers can bring down sites with denial of service attacks, or they can break in and compromise sensitive customer data.

A well-designed security architecture is an essential component of any e-business site. The security architecture and security devices must address the needs of an emerging e-business, but then must be able to easily scale to accommodate rapid growth if the business is successful. The security solutions must be secure, easy to deploy, high performance, high capacity and optimized for the co-location environment where most e-business sites are hosted.

NetScreen is working with e-business companies that range from small "dot.com" startups that are putting up their first site to some of the highest-traffic portal and e-business sites on the Internet. This paper discusses the security requirements and solutions for these e-business companies.

Implications of Poor Web Site Availability and Performance

Performance and availability are critical to ensuring a successful web site. Poor performance and availability results in lost customers - and revenue.

A recent report by Zona Research estimates that the average web buyer will wait approximately 8 seconds for a page to download, but the current average download time across a backbone connection on most sites is nearly 10 seconds. Such

unacceptable download times may result in the loss of up to $4.35 billion in U.S. e-commerce sales in 1999, Zona stated.

Outright web blackouts are worse, with Forrester Research estimating that the average cost of site downtime being $8,000 an hour. For large and e-commerce dependent sites, outages are more costly. EBay's 22-hour crash in June 1999, for instance, cost the company more than $5 million in returned auction fees.

The Zona Research study estimated that page load times of eight seconds or more, combined with normal ISP page download and connection failures, could cause as many as 30 percent of online buyers to "bail out" of a site before buying anything. The combined losses of these site problems could be as high as $362 million a month, Zona said. Such Internet brownouts and blackouts affect consumer confidence in the site as well as the value of a company's stock.

Sources of Availability and Performance Problems

Web site availability and performance problems can be caused by a variety of problems including:

Capacity: The site must be designed with the capacity to support peak levels of traffic. Capacity planning is critical for all major components of the site - servers, network connections and firewalls. High-capacity, mirrored web servers and server load balancing are required in most sites. High-bandwidth connections between the site and the Internet are a must. Hosting the site in a co-location facility is generally the best way to get cost-effective, high- bandwidth connection to the site. Equally important is ensuring that the site's firewall security doesn't become a bottleneck. To prevent the firewall from becoming a capacity bottleneck it needs to be capable of supporting (1) the peak bandwidth available to the site, (2) the maximum total number of TCP connections or sessions that the site will need to support, and (3) the maximum burst rate of new TCP connections per second that can be initiated. A firewall that can't scale to address all three types of capacity can become a bottleneck and lead to availability and performance problems.

System Failures: Hardware failures, system crashes, and network failures can all lead to unacceptable availability problems. Crashes are especially costly when the site is located in a co-location facility because often crashes can't be fixed until support personnel can travel across town or across the country to the co-lo facility. To minimize these problems devices need to be selected that are reliable and redundant, high-availability topologies must be implemented. Implementing redundant connections from your cage in the co-location facility to the Internet is a first step. For maximum server availability, this should be combined with a redundant meshed switching fabric providing multiple network paths through the site, as well as mirrored web servers and load balancing. Critical components like the firewall should be implemented on a high availability platform - a hardware-based platform with no moving parts provides the highest device reliability. In addition to a highly reliable platform, the firewall must support redundant high availability (HA) topologies. With HA topology, if one firewall fails the other takes its place. Site security and site availability are maintained giving the support team time to fix problems or replace faulty equipment.

Hacker Attacks: Another source of web site performance and availability problems comes from malicious hacker attacks. An unprotected site is vulnerable to hackers compromising the security of the servers and is also vulnerable to denial of service attacks. A well-implemented, multi-layer security solution should utilize firewalls to provide controlled access to front end web servers, while denying access to back-end servers. OS and application level security then needs to be layered above this network security infrastructure. This firewall solution must also have the capability and capacity to protect against denial of service attacks. Common attacks like SYN attacks, ICMP floods and UDP floods can bring most firewalls and sites to the ground. In a SYN attack, a hacker sends a large number of TCP SYN requests at a host without completing the rest of the TCP three-way handshake. This can lead the host to open up excessive numbers of TCP connections, leading to a system crash or preventing the host from being available to handle legitimate traffic. Attackers can flood a site with thousands of SYN packets per second, so the firewall must be able to detect these attacks and deter them at very high traffic levels.

Technical Requirements for E-Business Security Products

Implementing the right security solution is critical to your e-business success. Selecting the right firewall and designing the right topology is essential. Some important considerations in the selection of your e-business firewall should include:

Airtight security: ICSA certification, sophisticated access policy definition capabilities, network address translation, port address translation and robust support for typical hacker attacks are essential. It is also critical to ensure that the firewall is properly installed and configured. Running a scanner after installation is recommended. If the firewall is running on a general purpose OS and computing platform, the installation process must ensure that the underlying OS is appropriately "hardened" to remove any security vulnerabilities in the OS.

Performance: The firewall should be scaled to support the bandwidth required today and as the site grows. To accommodate peak bursts of traffic, a 100 Mbps firewall is typically used. Larger sites will require multiple 100 Mbps firewalls often deployed in a "firewall sandwich" utilizing load balancing devices and multiple firewalls.

Total Capacity: An e-business site firewall must be scaled to handle a large number of simultaneous TCP connections. A single user hitting the web site could result in the opening up of 10 or 20 TCP connections - one per item (e.g, GIF) on the web page. Software-based firewalls running on general-purpose operating systems and PC/workstation platforms are subject to the limitations of the OS and TCP stack they are running on. Most of these software-based firewalls can only scale to 10,000 or maybe 20,000 total connections. A purpose-built, e-business firewall should be able to scale to 50,000 or more total connections to accommodate heavy traffic loads.

Peak Capacity: Peak capacity, or number of new TCP connections that can be opened per second, is as important, and in many cases, more important than total firewall capacity. Bursts of traffic are common and hard to predict. If a large number of users hits a site at the same time, the firewall is likely to become overwhelmed.

High Availability: To maintain security, a firewall should be designed so that in the event of a failure it will always fail "closed" - meaning that a failure must block traffic and continue to protect the site. While this is great for maintaining security, it makes the site unavailable. To maximize device availability the firewall should be implemented on a hardware-based platform with no moving parts - for example, no hard disks to fail. It must also be implemented on a secure and highly reliable operating system. A purpose-built Internet security appliance provides this. In addition to a highly reliable platform, the firewall must support redundant high availability (HA) topologies. With HA topology, if one firewall fails the other takes its place.

Form Factor and Rack Space: Most e-business sites are implemented in co-location facilities where the company rents a cage and rack space from the hoster. Rack space is expensive. A low-profile firewall can save on rack space and reduce on going operating costs.

Remote Management: Secure remote management is essential for firewalls implemented in a remote co-location facility. Web-based management can make installation and configuration far easier, but a command line interface (CLI) can be more powerful for the experienced user. Support for central management of multiple devices from a single management application is important in larger sites with multiple firewalls, or for sites that are mirrored across multiple co-location facilities. If the firewall includes IPSec VPN capabilities, remote management can be performed through IPSec tunnels for maximum security.

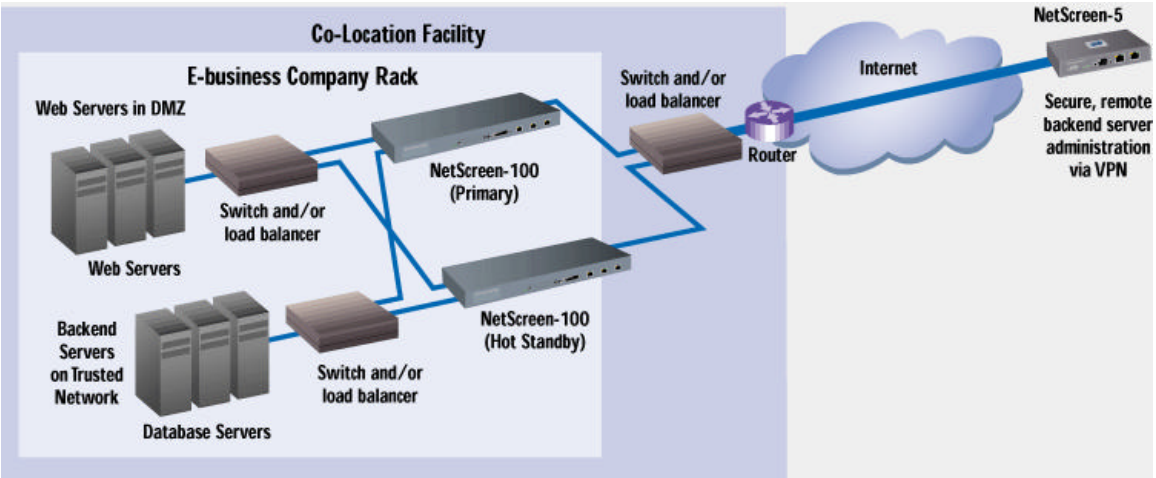
VPN for back end server administration and management: A typical e-business site will include front-end web servers available to the public, and will have back-end servers performing critical database functions to support the e-business site. The firewall security should protect these servers, but the site operator is likely to need to get access to these servers for data collection or administration. Being in remote co-location facilities requires that a secure connection be established between the corporate site and the company's cage in the co-location facility. This is often implemented with a private leased line, but the monthly cost can get expensive. With site-to-site IPSec VPN capability in the firewall, a secure, encrypted tunnel can be created between the co-

location facility cage and the corporate site to allow for remote administration. This utilizes the existing Internet connections for the two sites and eliminates the cost of an expensive leased line.

Deployment Example: Emerging E-Business

As an e-business gets off the ground, the site needs to be rolled out quickly and securely. A basic topology creates two security domains, a "demilitarized zone" (DMZ) supports front-end web servers accessible to site visitors, and a second "trusted" domain is used to secure back-end database servers holding sensitive customer data. Policies can be implemented to restrict access to web servers to only allow for web protocols, such as HTTP. Even more restrictive policies can be implemented on the Trusted network to only allow for communication between the web servers and the back-end servers and only with specific services.

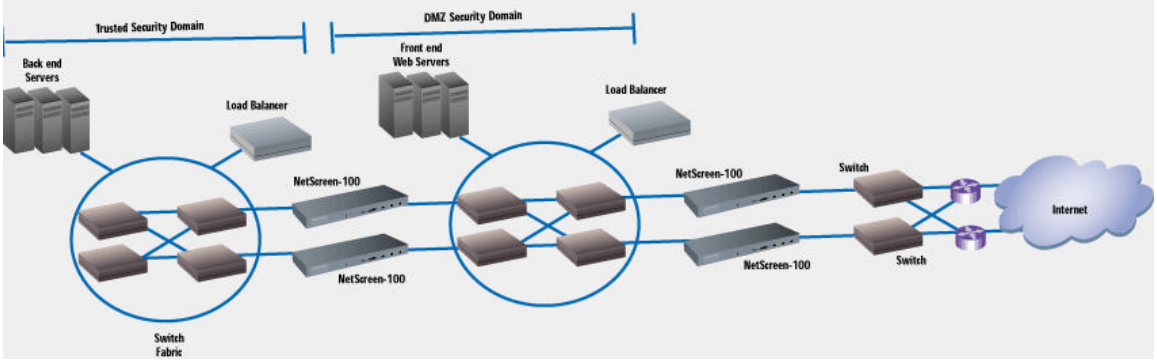
VPN access policies can be added to create a secure VPN tunnel from a remote location (corporate HQ) into the Trusted domain to allow for the back-end server maintenance and access. For high availability, firewalls should be implemented in redundant pairs. If one fails the other one can become active and keep your site available.



Deployment Example: High-Traffic E-Business Site

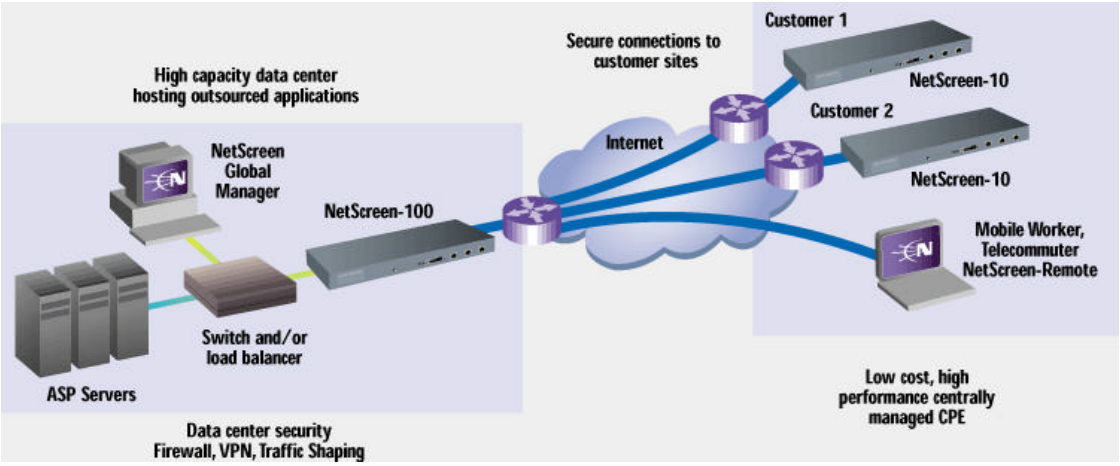
As the business grows, and user traffic to the site grows, the security architecture needs to be migrated to a higher capacity and higher redundancy topology. In this case, instead of utilizing the DMZ and Trusted ports on the same firewall to create the two

security domains, multiple firewalls can be used to create two or more security domains with redundant, high-performance paths into each security domain.



Deployment Example: Multi-Site E-Business Using VPN Technology

More and more e-businesses are creating secure connections between their co-location-hosted servers and remote offices or customer sites. ASPs are one example of this where an ASP hosts applications in a central site for a number of customers. They need firewall security combined with the ability to create a VPN to their customer sites using their central security appliance and low-cost CPE. Other e-business companies are using VPN tunnels to transfer sensitive customer information between their data center and their "brick and mortar" facilities that are spread across the country.



NetScreen-100: Optimized for the E-Business Environment

The NetScreen-100 combines firewall, VPN and traffic shaping functionality in a high-performance, ASIC-based security appliance optimized for e-business environments. The NetScreen-100 received Data Communications' testers choice awards for both firewall and traffic shaping. Data Communications found that the NetScreen-100 "offered the best combination of airtight security, screaming performance, and simple management."

NetScreen-100 firewalls are securing numerous new dot.com web sites as well as some of the highest traffic portals and e-business sites on the Internet. For example, it is the firewall solution for TIBCO.net, a service that enables portals such as Yahoo, Lycos, AltaVista, NetScape NetCenter and CBS Sportsline to deliver custom stock, news and weather data to their visitors. When a portal visitor requests a stock price, they get a page served up by TIBCO and secured by a NetScreen-100.

The NetScreen-100 is being selected for these sites because it meets the needs of demanding e-business sites. It delivers:

Airtight security: ICSA certification, sophisticated access policy definition capabilities, network address translation, port address translation and robust support for typical hacker attacks. Since it is a purpose built security appliance running a specialized OS, there is no need to worry about hardening the OS or other security holes in general purpose operating systems.

Performance: Wire-speed 100 Mbps firewalling and NAT in addition to 85 Mbps 3DES IPSec VPNs.

Total Capacity: 64,000 simultaneous TCP connections, 4 times the capacity of leading software-based firewalls.

Peak Capacity: 19,600 new TCP connections can be opened up in 1 second to handle even the heaviest traffic bursts.

High Availability: A purpose-built security appliance with no moving parts to fail. Support for redundant topologies and failover to a hot stand-by unit.

Form Factor and Rack Space: Slim 1U form factor uses minimum co-lo rack space.

Remote Management: Integrated web server allows browser-based management in addition to CLI-based management via Telnet or a dial up connection. Management can be implemented via a VPN tunnel for maximum security.

VPN for back end server administration and management: IPSec VPN capability for secure, encrypted communication between the co-location cage and the corporate site to allow for remote administration.

And perhaps best of all, the NetScreen-100 is a phenomenal value at a U.S. price of less than $10,000.