

Provisioning and Managing Large-Scale Security Deployments

A White Paper by
NetScreen Technologies Inc.



NETSCREEN

Data Security Management Trends

Corporations have historically been concerned about protecting their internal data from prying eyes and accidents, but only recently have they begun to recognize their data as both vulnerable to attack and something worth protecting, even if at a high cost. Initial corporate presence on the Internet—often comprised only of static information repositories—was something to guard but not overprotect, and downtime was an inconvenience but didn't cut into corporate revenues. As businesses turn into e-businesses, however, they find that doing business over the Internet causes a substantial increase in their Web site traffic levels, which can quickly reach volumes that outstrip their ability to manage networks themselves. Exacerbating this situation is the absolute need for reliable network solutions to support the increasingly mission-critical status of their e-commerce applications. As data flowing over the network is increasingly related to e-commerce, and as it grows in volume and value, e-businesses find that network downtime is much more than an inconvenience: It decreases revenues and destroys customer confidence.

As they continue to seek complete solutions, companies outsource more and more of their operations, enabling them to focus more exclusively on their core businesses. This trend is visible both in the move toward Application Service Providers (ASPs) and Internet Data Centers (IDCs). Companies rely on ASPs to manage their application deployments, support, and upgrades. With IDCs, a company's whole body of information—including core operations data—is neither managed nor housed on-site, but rather stored off-site and managed by a specialized body of technical personnel who work for the IDC. Internet data centers must be able to guarantee continual operation and availability of this data, so their clients can conduct their businesses. Without it, trucks can't move, inventory can't be ordered, and the assembly line stops.

On the other side of the outsourcing coin are companies that elect to keep their data on-site but still recognize the need for a specialized group of personnel to manage the increasingly complex issues regarding data security. Managed Security Service Providers (MSSPs) have even more unique requirements, because they are responsible for monitoring and protecting data at remote sites. With firewalls and other security solutions, as well as the data stored on their customers' sites—be they IDCs or corporate users—MSSPs need the ability to monitor and configure these devices remotely. Sending staff out to remote sites is expensive and time-consuming. Customers don't want to wait for travel time before a technician can effect necessary configuration changes. And if there are security issues, problems need to be resolved *now*, not hours later.

And as the value of the data itself increases, security issues grow increasingly complex. Partnering and data sharing with certain allied companies, electronic data interchange, and so forth require data to be all "on the net," while at the same time not easily accessible to just anyone. In addition to the well-meaning but uninformed corporate user who might inadvertently delete or modify certain data, a company's information has to be protected from the malicious intent of outside intruders, who now have a pathway to the data via the Internet. While the various data-sharing trends offer companies improved means of doing business, these same trends make them even more vulnerable to hackers, prey to performance issues, and increasingly uneasy about the security of their corporate data treasure.

Before these outsourcing trends, most companies stored their data on-site and had a staff trained to recommend and support security solutions, perform data backups, configure various devices, and monitor performance. As companies opened themselves up to the Internet and partner companies, the staff saw the need for and implemented even greater security precautions to protect their data. A wide range of products grew up to support these needs, and they too—in keeping pace with the trends—are becoming more numerous and complex. It is harder and harder for companies to keep qualified staff adequately trained on all the devices and disciplines required to satisfy their ever-broadening IT security needs.

Needed: New Solutions for a New Way of Doing Business

The trends toward IDCs and MSSPs are pushing security solutions companies to provide more flexible devices capable of meeting the unique and changing needs they are bringing about. Security management solutions that have proven effective in the past are rapidly becoming inadequate because of their single-user orientation, lack of scalability, and their inability to integrate with third-party software products.

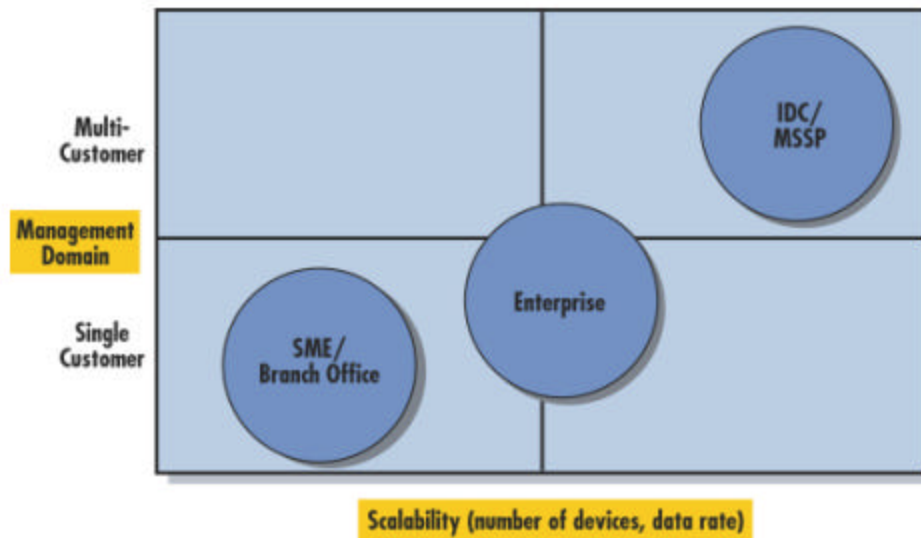


Figure 1. Enterprise versus Service Provider Solutions

To stay abreast of new trends, next-generation security management solutions will need to overcome these limitations to meet service provider-level management needs. These include scalability in terms of thousands of devices and multiple customers, multiple administrator accounts, flexibility, ease of configuration, and the ever-present need for robust and fault-tolerant systems.

Important considerations and questions when evaluating a next-generation data security management system:

- ❑ Existing security management products are designed for a single “user” with a single administrator account. A next-generation management system must address
 - Letting users configure the aspects of the environment they should control while protecting other users’ configuration management.
 - How can the service provider modify those aspects that *it* needs to control?
 - Visualization of multiple customer domains from a single console.
- ❑ Existing security management products are not scalable. A next-generation management system must address
 - Whether the security management system allows data collection from thousands of devices.
 - Monitoring this data.
 - Handling peaks of network usage.
- ❑ Existing security management products do not integrate with other tools—they were designed as standalone applications. A next-generation management system must address

- Easily supplying historical usage information to third-party management applications.
- Effectively storing historical performance information and the security and re-usability of that information.
- Monitoring usage and spot trends in a timely manner.

NetScreen Security Management

NetScreen Technologies' high-performance security solutions are designed for the unique requirements of growing IDC and MSSP environments. NetScreen offers service providers the ability to quickly safeguard customer data and ensure reliable accessibility while best meeting diverse customer needs. Customers demand performance levels that exceed their in-house capabilities at a more affordable price and with a greater level of customer support. At the same time, providers need to address their own operational needs while ensuring the ability to grow quickly, move into new markets, and add services without destroying profit margins. NetScreen security management solutions are designed with all of these needs in mind.



Figure 2. NetScreen's Security Management Strategy

Rapid Deployment

Once customers have made the decision to outsource their data storage and security needs, they will want to have it done immediately. Service providers can differentiate themselves with the ability to bring new customers on-line quickly and deploying the required service options in an easily configurable manner. NetScreen understands that a service provider's goal is to manage customers and services—not to spend extensive efforts managing the devices required to service them. Providers want their customers to have appropriate levels of policy control to offload low-level tasks, such as adding or modifying user accounts and so forth.

Rapid Problem Resolution

The speed and reliability of alerts are critical. Being able to tell the difference between a sudden burst of traffic through a customer's firewall due to a sales promotion and one caused by a distributed denial of service attack is crucial. When there is a security breach, service providers need the tools to react quickly and efficiently to close the hole.

NetScreen security management solutions offer real-time performance monitoring, reports on attacks by source address and type, and integration with leading fault management and intrusion detection systems such as Micromuse Netcool™, allowing providers to leverage their existing problem resolution tools. Centralized device configuration makes it possible to quickly change policies and services as necessary in response to problems.

Service Assurance

The unique requirements of service providers call for the ability to access vast amounts of accurate and timely data, so their Network Operations Center (NOC) staff can fine-tune the network to meet customer needs. To manage multiple customers and value-added service offerings, providers need security management solutions that ensure their capability to do so profitably. NOC staff should not have to guess how to best tune the network for lack of access to the information necessary to making intelligent decisions. They need a security management solution designed from the ground up to manage the hundreds of domains, thousands of virtual private networks, and hundreds of thousands of TCP sessions their staffs need to support. In addition, they must be able to supply customers with timely and robust performance reports.

Flexibility

This paper has described baseline requirements for market evolution. In order to survive, organizations need rapid deployment, performance and service assurance, and the ability to quickly resolve problems as they arise. These are givens. If service providers don't take care of the basics, customers won't care how many bells and whistles they offer in addition.

Of course, all customers are not alike. Providers need the ability to offer the right differentiated services to the right customers—whether they rely on secure Web-hosting services, complex e-commerce transactions, or application hosting solutions. Each type of customer has unique needs and is willing to pay for those services they see as most critical. Usage-based billing, for example, provides the flexibility to offer different services, priced appropriately, to different customers.

Building New Revenue-Generating Services from the Basics

Once a service provider has in place a data security management system that performs the basic necessary functions, it can serve as a springboard for a myriad of value-added, revenue-generating capabilities and services. Among them, the ability to monitor customer usage closely enough to spot trends and recommend changes before they become the cause of poor performance. Such monitoring capability also means a provider could offer a discounted rate to certain low-end price-sensitive customers who don't need the "extras." It also allows identification of customers who would be willing to pay more for premium services (e.g., video conferencing) because of their service and high-data-rate usage patterns

Usage-based billing, made possible through powerful network system monitoring functionality, will allow all of this and more. Service providers can flexibly offer various capacity allocations that change as their customers' needs change. Usage-based billing and monitoring also enables them to spot trends, rapidly re-configure both local and remote devices as needed, and automate certain actions based on

defined events. In short, the more providers know about their customers, the better able they are to provide excellent service—the right service at the right time, and the kind that makes them stand out from the competition.

Introducing NetScreen-Global PRO

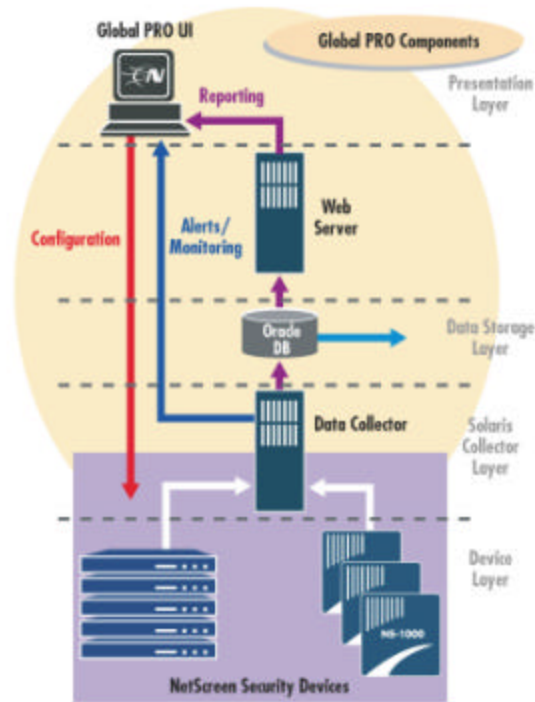


Figure 3. NetScreen-Global PRO Architecture

Service providers have unique needs, and NetScreen has designed its NetScreen-Global PRO™ software specifically to meet their specialized requirements:

- ❑ Multi-customer features ease administration, management, and reporting on multiple customers, multiple devices, and multiple sites.
- ❑ NetScreen-Global PRO features scalable performance in terms of bandwidth, the number of devices it supports, and customizable access levels and views.
- ❑ The software integrates with service providers' existing applications to make the best use of both live and historical data through the open database schema.

Multi-Customer Management

NetScreen has designed its newest generation of security management products to allow the service provider to support multiple customers, each with different needs. Customers who have outsourced the management of their data still want to feel like they own their information and have as much access to it as they did when it was stored on-site in their own data centers. While executives can't walk downstairs and look at the blinking red lights, providers can let them know they are still in charge, and

their data is secure. They can assign individual customers access to their own specific real-time data without having to manually collect and upload individual device log data.

An IDC that supports multiple ASPs as clients, who in turn support multiple end customers, needs the ability to service its clients invisibly and to easily maintain the overall security infrastructure behind the scenes. ASP clients want to brand their service offerings and give their own clients the ability to add and delete users as needed without jumping through endless hoops.

An MSSP supporting multiple end customers or even IDCs as clients needs the capacity to manage large numbers of remote security clients over a diverse set of networks. NetScreen-Global PRO allows them to do this. MSSPs can quickly set up and configure remote devices, and they can monitor performance while quickly pinpointing the root causes of any network issues and resolving the problems.

Service providers that offer service level agreements require appropriate reporting and analysis to ensure they are meeting their obligations and that customers know they are doing so. NetScreen-Global PRO can generate detailed exception reports as well as executive summary level reports for each customer or grouping of customers to better monitor usage trends and make informed decisions to best meet their individual needs.

Role-based monitoring enables providers to deliver customizable performance reports to customers, allowing them to learn more about their own usage as well as that of their customers. In addition to serving customer needs, the flexible, usage-based reports allow service providers to detect trends and plan for the future, monitor individual customer usage patterns, and offer a more suitable set of services. NetScreen-Global PRO ensures providers will not be caught without the necessary resources to assure continued premium performance.

Scalability

Scalability needs to be addressed in several areas. Not only do service providers need to handle the increased traffic loads and bursts of traffic (burstable bandwidth), but they must also monitor and report on this traffic. To customers, bursts of traffic are usually the sign of a successful Web site. IDCs that can handle their customers' successes will be successful themselves. Failure to support customers at the peak of their success will leave providers in the difficult position of trying to rebuild their trust.

Traditional security management products require data centers to manually process individual firewall log files for different customers to generate customer-specific reports. This puts an extreme burden on the support staff, resulting in the inability to respond as quickly as necessary to current problems. NetScreen's client/server architecture delivers automated, high-performance data collection and reporting without burdening NOC staff.

True scalability means service providers can handle more clients and more devices with fewer staff resources of their own. And it means they can get new customers on-line quickly and expand infrastructure for the prompt service delivery to meet customer demand, while increasing their own revenue potential in the process.

Third-Party Integration

NetScreen's open database schema means NetScreen-Global PRO can easily integrate with other third-party solutions, including many existing billing and reporting applications. Because NetScreen-Global PRO stores real-time and historical trending data in an Oracle® database and Solaris™-based data collectors, service providers get both the scalable performance reporting and event logging they need. The product's data collection functionality allows providers to report on security attacks, usage

by type and by customer, and a variety of critical performance measurements that provide third-party management products with the information required to perform complex diagnoses.

Browser-based reporting allows access from multiple locations by multiple administrators. NetScreen-Global PRO includes templates that enable providers to quickly create their own customized Crystal Report™-based views to meet individual needs. The software supports other reporting packages as well, allowing service providers to integrate NetScreen devices and data with existing packages that are compatible with the data storage schemas discussed above.

Problem resolution requires good management combined with the ability to pinpoint the root cause of a problem. Through integration of NetScreen device data with trouble ticketing or other existing fault management systems, not only can service providers solve problems quickly, but they can track and report on the status of problems for both customers and internal management.

Data Security Management with a Commitment

NetScreen is committed to providing industry-leading, hardware-based security solutions. As NetScreen continues in its mission to provide increasingly innovative solutions, its customers can expect access to even more performance, flexibility, scalability, and manageability. NetScreen understands that success as a service provider today means keeping pace with customers' ever-increasing expectations. NetScreen aims to make this job easier by providing industry-leading data security management solutions, so its clients can stay ahead of the game.

©2001 NetScreen Technologies Inc. All rights reserved. Information in this document is subject to change without notice. NetScreen Technologies, Inc assumes no responsibility for errors that appear in this document. NetScreen Technologies, Inc, the NetScreen logo, and NetScreen-Global PRO are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.