

STONESOFT

Whitepaper

Server Consolidation Security - Firewall and VPN Solutions for IBM eServers

Table of Contents

Executive Overview	1
Server Consolidation	1
Concepts	1
Issues	2
New Solutions for Proven Technology	3
StoneGate Advantages	4
Security	4
Manageability	5
Availability	6
Scalability	7
Conclusions	8

Executive Overview

Today's on-demand enterprise can gain significant benefits by consolidating servers into their mainframe and midrange systems. Whether an organization uses IBM® eServer® iSeries model 800s or the IBM eServer zSeries® z990, consolidation of servers is now possible, yielding substantial return on investment. Whether it's mainframes or midrange, organizations can reduce administration, infrastructure, and systems costs significantly by running many virtual servers inside a single eServer zSeries or iSeries machine, instead of using tens or hundreds of x86-architecture based PC servers.

For more information on server consolidation and the IBM eServer family, please see: <http://www.ibm.com/servers/eserver/>

The conversion to server consolidation, although very beneficial to the on-demand organization, is not without concerns. Traditional mainframes and midrange systems were considered very secure. But the introduction of Linux® and Microsoft® Windows® based systems inside these machines, and TCP/IP networking connecting them all together on virtual LANs, introduces the same security concerns that physical servers and LANs have had for many years.

Stonesoft's StoneGate firewall and VPN solution for IBM eServer zSeries and iSeries provides a unique security solution to address the network security needs of this new architecture design. StoneGate excels in security, manageability, availability and security. This whitepaper will explore the issues surrounding server consolidation on the mainframe and midrange systems, and detail how StoneGate can address the security concerns—providing for a secure, on demand workplace, a significant return on investment and the enablement of new business processes.

Server Consolidation

To begin to understand the power and importance of a network security solution such as Stonesoft's StoneGate firewall and VPN solution, it is first important to have an understanding of the fundamentals behind server consolidation as a concept, and the issues that surround it.

Concepts

Server consolidation is based on virtual machine technology developed by IBM over thirty years ago. First on the mainframe, and now on the midrange iSeries systems, many systems can be run on a single physical machine, as illustrated in Figure 1. Each system thinks it is running on its own hardware, with its own resources, yet it is actually running as a virtual server within a larger system. Actual resources, such as storage, networking, and processors can be dynamically assigned and shared among the different systems. With the advent of Linux on the mainframe, modern business applications can take advantage of this virtual machine approach. By consolidating many physical servers, organizations can significantly reduce costs.

Cost reductions through server consolidation are realized in several ways. First, the virtual servers no longer require physical hardware. Related to this, there are lower cooling requirements, lower electrical needs, less cabling and less physical space required to store the equipment. By reducing the cabling and electrical requirements, the reliability of the

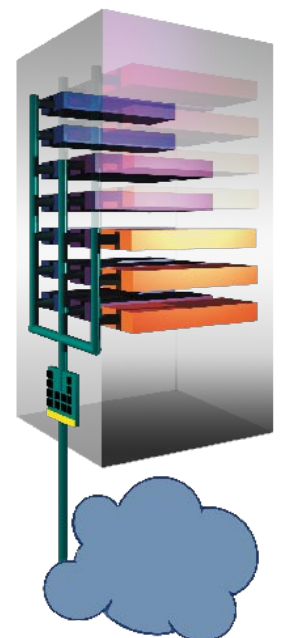


Figure 1: Virtual servers consolidated onto the mainframe creates significant optimization in resources and administrative work.

systems is dramatically increased (eliminating accidental power loss because a system was unplugged inadvertently, for example) while reducing the complexity of the datacenter.

Through consolidation, a great number of systems can run on a proven, reliable piece of hardware, with resources dynamically assigned to individual server instances as necessary. If a particular application requires greater processing power to complete a transaction, for example, resources can be assigned to compensate, while a system running idle can free resources that are not required.

To learn more about the 40 years of innovation in the mainframe product line, please see: <http://www.ibm.com/servers/eserver/zseries/timeline/>

The consolidated servers can also communicate more efficiently—both between other virtual servers, and also with back end systems running on conventional z/OS or OS/400 systems. New technologies—such as Hipersockets for the zSeries, or advanced virtual Ethernet for iSeries—enable very efficient communication between systems within the eServer machine. Since physical cables are no longer required, the physical limitations of such cables—including security risks (wire taps), damaged wires, loose connectors, being unplugged—are also removed.

Issues

Although server consolidation creates new robust systems, it also shares similar issues with physical environments. Each system consolidated includes an operating system and TCP/IP networking to connect it to the enterprise organization or even the Internet, and therefore carries the security risks associated with such systems.

To learn more about the best practices for securing servers consolidated with IBM eServers, please see the IBM Redbook Linux on IBM eServer zSeries and S/390: Best Security Practices (SG24-7023-00).

These risks include the increased accessibility TCP/IP creates. Mainframes and midrange systems traditionally were accessed with direct coaxial connections with the SNA protocol, using 3270 or 5250 terminals. Since physical access to the terminals was required to access the server systems, a measure of physical security and user authentication were all that was required to secure the mainframe. To take advantage of the lower cost of networking and the increasing connectivity of systems on local area networks, SNA was later encapsulated, or packaged, in TCP/IP, referred to as SNI. But the increased connectivity of the mainframe alone was still not as risky as the addition of new operating systems and more common applications, such as Web servers, application middleware systems and other services based on Windows or Linux. Now, physical security is no longer sufficient, as these systems communicate over networks that are linked to networks that connect to the Internet, and therefore the world. Figure 2, “Typical network design of today’s enterprise,” illustrates the connectivity issues of today’s modern enterprise network.

With consolidated servers, the virtual operating systems are vulnerable to denial of service and other attacks, just as they would be on standard x86 servers. Hackers from untrusted networks, or even an organization’s own employees on a trusted LAN can now poke and prod at these systems running on the iSeries or zSeries. Should a system be compromised, it can then serve as a springboard to attack other systems on the virtual network. If the compromised system was designed to access other application components, backend systems or MVS or OS/400 applications, then those are now attackable as well. Though the traditional midrange and mainframe systems have proven security, denial of service or even distributed denial of service attacks can be launched against them that, although they do not compromise security render the systems inaccessible for legitimate use.

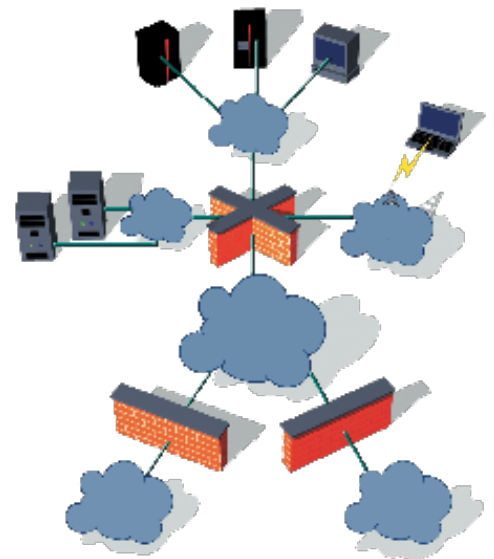


Figure 2: Typical network design of today's enterprise. Corporate and branch offices protected by perimeter firewalls, but have weak internal and remote user security.

Whether denial of service, worms, trojans or viruses, each represents threats against virtual as well as physical systems. In conventional networking, best practices now hold that networks should be segmented into multiple parts. Just as the compartments and doors of a submarine or cargo ship reduce the risk that a hull breach can sink the boat, the segmentation of the network can reduce the risk of a compromise affecting all systems. Thus, trusted networks are separated from untrusted ones, and the trusted networks themselves are further compartmentalized into DMZs (from de-militarized zone; here a network that is semi-trusted, not fully trusted). By dividing the networks, a layered defense can be developed and maintained. Bandwidth and service consuming attacks can be isolated to the affected segments, protecting the access to, and function of other network systems.

New Solutions for Proven Technology

There are numerous technologies available to segment networks into different spaces to ensure that the compromise or failure of one cannot affect the others. But to be effective, some measure of communication must take place between the networks, so that business process is not interrupted as well. To control the traffic between networks, allowing connections when necessary and blocking them when something goes wrong or looks suspicious, administrators use firewalls.

On the eServer zSeries and iSeries, the StoneGate firewall and VPN solution represents the most secure, manageable, available and scalable answer to maintaining secure connectivity between virtual networks and servers within a mainframe or midrange platform. With StoneGate, virtual networks can be secured from one another, and from networks external to the eServer system, as well as from other logical partitions (LPARs), while fully realizing the benefits of virtual server technology by running the firewall/VPN gateway as one also.

For the IBM zSeries, StoneGate runs either natively, consuming a logical partition, or as a z/VM guest. Since it includes its own integrated and hardened operating system, there is no need to install a Linux distribution in VM first. In addition to simplifying the installation process itself, this integration of the operating system also reduces the administrative time, as there is no need to remove extraneous packages and services, users, groups, and files, and to verify filesystem permissions, download and install appropriate patches, and all the other work that goes into installing the operating system first. Figure 3, "StoneGate for IBM zSeries architecture," illustrates a possible zSeries architecture with StoneGate, where the virtual firewalls protect the systems from the Internet, and from each other. In this example, the application server is secured from the Web server (and the database from the application server). Should the Web server be compromised, the hacker has not gained access to the data or the middleware logic. StoneGate can prevent unauthorized connections to the application or database servers, and generate an alert when such an anomaly takes place, so that the administrator can immediately take action.

For the IBM iSeries, StoneGate runs in a logical partition of its own, and links multiple LPARs with advanced virtual Ethernet networks. Traffic to the other systems or partitions is controlled through StoneGate, which protects each subsystem from each other, and from external systems. Just as StoneGate for zSeries includes an integrated operating system, so does the iSeries edition.

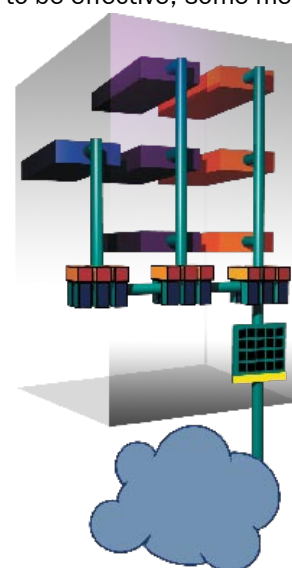


Figure 3: StoneGate for IBM zSeries Architecture.

StoneGate requires the support of OS/400 on the server in general, in much the same way that StoneGate for the zSeries typically uses z/VM, yet StoneGate does not run on top of OS/400, a Linux system or a Windows partition. Figure 4, “StoneGate for IBM iSeries architecture,” illustrates the architecture within the iSeries system. In this example, LPAR 2 runs StoneGate and protects the other five partitions from the outside networks. It also controls traffic between the three virtual LANs, connected with virtual Ethernet. For example, traffic from the Apache Web server on the first virtual LAN must go through the firewall and pass the security policy in order to access the database on the third virtual LAN.

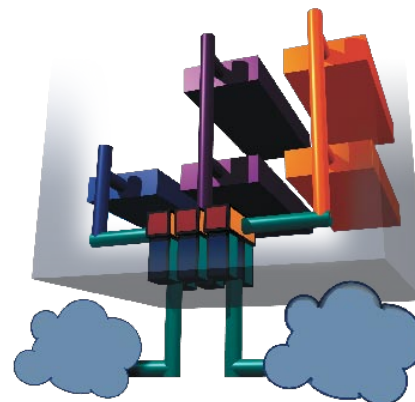


Figure 4: StoneGate for IBM iSeries architecture.

StoneGate Advantages

StoneGate in either eServer architecture provides significant advantages over other security options. It excels in providing a superior mixture of security, manageability, availability and scalability.

Security

StoneGate is designed from the ground up to be a secure system. It operates under the principle that what is not expressly permitted is denied. StoneGate provides the iSeries and zSeries systems with a true stateful inspection firewall. But StoneGate goes beyond stateful inspection. It provides Multi-Layer Inspection, where the firewall can function as a basic packet filter, a stateful inspection firewall, or perform deeper packet inspection at the application layer—each available on a rule-by-rule basis as selected by the administrator.

StoneGate’s integrated operating system contributes to the security of the overall solution. The work of hardening and securing the operating system has been carried out by experts, and is packaged in the installation. Furthermore, configuration of operating system functions, such as routing, are handled through the user interface and management system. And the configuration data on the gateway is stored in an encrypted and tamper-proof format by default.

Even StoneGate’s management architecture demonstrates security designed into the product from the ground up. All communications between components are encrypted and authenticated, as illustrated in Figure 5. Where other products include Web-based interfaces that default to an unsecured configuration, StoneGate provides SSH-based interaction with the gateways; but this too is not enabled by default, and the security policy must permit such communication as well.

StoneGate can also leverage backend mainframe security systems, such as RACF® or CA-ACF2® to perform additional user authentication. Whether basic authentication is required, or an organization wishes to deploy advanced encryption of network traffic all the way into the eServer, StoneGate can authenticate the users requesting system access through LDAP.

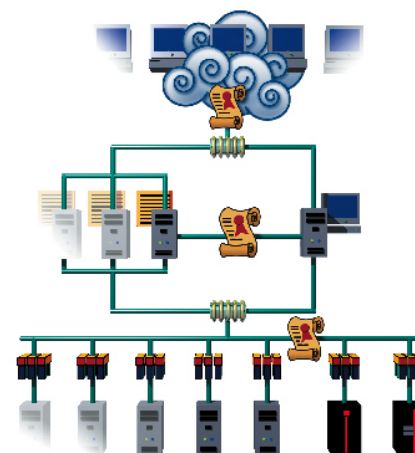


Figure 5: StoneGate’s secured management system architecture. The StoneGate Management Center uses encrypted communications between all components, including the firewall engines for any platform, the log servers and the GUI clients. It also uses advanced PKI digital certificates to authenticate the connections.

With advanced logging capabilities and auditing built-in, StoneGate can further enhance the security of the mainframe or midrange system by providing logs of traffic in and out of the system, and between LPARs. Powerful filtering capabilities allow an administrator to quickly isolate the particular entries they are looking for, based on a number of different criteria, such as source or destination IP address, user authentication information, time of day, and more. Auditing features track access to, and modifications of security policies and network elements, including the firewall/VPN gateway properties and routing information. Combined with different administrator permission levels, an organization can have very strict controls on the security of the eServer systems.

Alert notification management in StoneGate

The logging features of StoneGate can also be used to provide alert notifications in the event that unauthorized access is attempted. Administrators can configure custom alert messages, which are triggered by individual rules in the security policy, and then transmit those alerts through any number of alert methods, including combinations of e-mail, SNMP traps, alpha-numeric pages, or SMS text messages through GSM phones.

With StoneGate for the eServer line, organizations can also enhance security through the use of VPNs on the internal networks. Since the VPN endpoint can be placed as close to the applications as possible, even data on the internal networks can be encrypted all the way into the mainframe or midrange system itself. By deploying the StoneGate VPN client on internal workstations, encryption can take place across the entire physical medium. As an additional bonus, the VPN client includes an active traffic filter, which can protect the client machine from unauthorized traffic on the network as well. The client supports multiple authentication methods, including certificates, simple user ID/password, RADIUS or TACACS+, or LDAP.

Manageability

StoneGate's architecture also provides the only commercially available solution capable of running across most of the eServer line, including xSeries, iSeries and zSeries. This architectural flexibility yields further benefits for those wishing to centrally manage not only the iSeries or zSeries instances, but also the entire enterprise security architecture from one platform. The StoneGate Management Center can manage instances of all of the platforms, and enable unified policy management for each. Administrators can monitor, control and change software versions for perimeter clusters on xSeries, StoneGate appliances at remote locations, multiple zSeries instances, and iSeries instances all from within the same user interface, and the same central management system.

StoneGate includes robust logging and log data management capabilities, including centralized log collection. Whether from zSeries, iSeries or other platforms, all StoneGate firewalls and VPNs can log to a single log server, or each gateway or gateway cluster can be assigned its own log server instead. Log data is stored in a relational database, enabling unique filtering options and data management operations, such as the ability to prune certain log data from the database, yet still have it displayed in any active log browser. All log servers can also forward log data as standard syslog to other log data management solutions. And the Log Data Manager provides the ability to define and manage tasks such as archives, exports, and deletions, and to schedule these to occur on a regular interval, and to cover a specific time range.

Log data is useful only if it can be interpreted and acted upon. To that end, the StoneGate Management Center 3.0 includes a Report Manager. This new tool allows an administrator to define, manage and generate reports on a wide variety of data points, and schedule the automated generation of reports on a recurring interval. Available output types include PDF, making viewing and portability of the reports an effortless task.

Multiple administrators can be logged into the management system at the same time. And each can work with elements, and be assigned different access control levels. So an iSeries administrator can be given access to the iSeries firewall instance and its associated security policy, yet they would not have access to the zSeries instances or their policies. Other administrators can be granted access to the zSeries firewalls, and the overall firewall team can manage the entire solution.

The goal of security solutions is to enforce an organization's security policy. StoneGate improves the manageability of this task as well, with a flexible, hierarchical rule base design. An administrator can create a template rule base, which defines a set of rules for the entire organization. Such a template might include rules to deny peer-to-peer (P2P) file sharing traffic, access to instant messaging services (IM), and redirects outbound Web traffic (HTTP) through a content inspection system to block undesired URLs. Then security policies can be defined for the perimeter firewall/VPN gateway clusters, the zSeries policy, and an iSeries policy. Each of these inherits rules from the organizational template, while at the same time allowing for flexible configuration for the particular instances in each case. When combined with multiple administrator logins and different administrator access rights control, the assignment of policies in templates and rule bases becomes a very powerful and effective means of enforcing security policies.

Availability

Mainframe and midrange systems from IBM are legendary for their reliability. Administrators of iSeries and zSeries machines are familiar with the many availability features of the systems and their ability to keep services up and running. Combined with a disciplined approach to systems management, downtime for the mainframe is almost non-existent.

Stonesoft also has demonstrated expertise in availability, starting with pioneering high availability solutions for firewalls back in 1995. From that simple solution, StoneGate was eventually created. StoneGate supports full load balancing and clustering of up to sixteen nodes on standard x86 architecture equipment, such as the IBM xSeries machines.

For the mainframe and midrange, StoneGate also supports availability. In addition to inheriting the availability and reliability of the legendary zSeries and iSeries platform, StoneGate for zSeries can run with a hot standby high availability instance, as illustrated in Figure 6. Should an instance need to be brought down for maintenance, or in the unlikely event of an instance failure, traffic is transparently failed over to the standby instance.

Regardless of platform, every StoneGate system is equipped with Stonesoft's patented Multi-Link technology, which enables load balancing across multiple network providers. This increases both performance and availability, as the failure of an ISP or network link does not require administrator intervention for traffic to resume. If Multi-Link VPNs are used, traffic is transparently failed over to the remaining active sub tunnels.

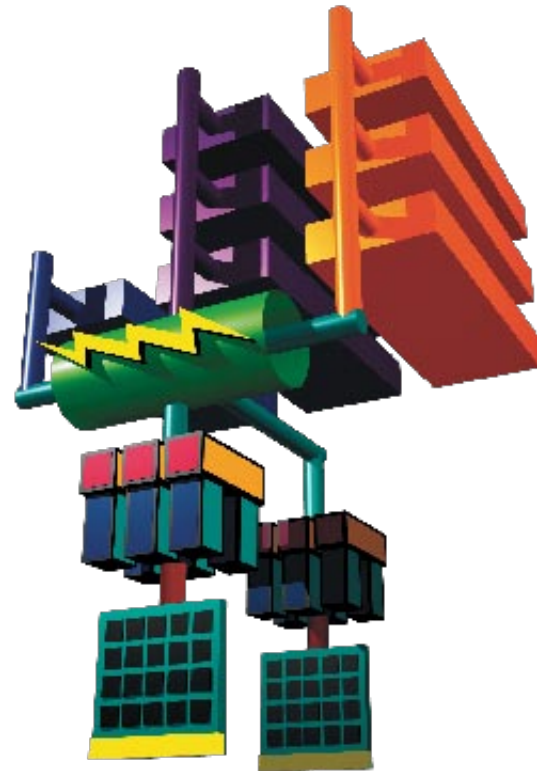


Figure 6: StoneGate high availability in IBM's zSeries.

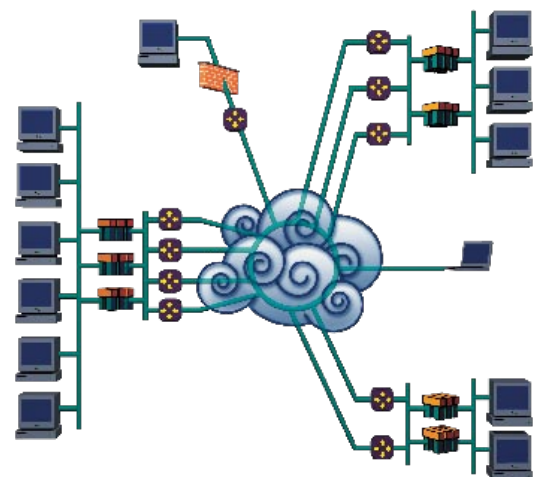


Figure 7: StoneGate's patented Multi-Link technology enables always-on communications between sites, load balancing connections to the Internet to aggregate bandwidth, and provide transparent VPN failover in the event of an ISP outage. The IBM eServer platform editions of StoneGate also support this revolutionary technology to ensure business continuity.

For the IBM zSeries and iSeries this technology can provide additional availability, even if the system is not connected to the Internet or near the perimeter. Multi-Link technology operates at an IP address level, so it is possible to load balance and have redundancy on internal network links within an organization too.

A second feature available on all platforms is the ability to do server load sharing. This feature, though complimentary to Multi-Link, can independently share traffic load destined for a pool of servers. Server pool load sharing is performed with

the gateway presenting a single IP address to the systems on one side, and then distributing the traffic to multiple servers on the other side. This feature performs a simple round robin of connections by default, and availability is only determined by the response of the server to test packets. A more robust solution is also available, which uses an agent (a piece of software that performs monitoring) on each server to perform additional monitoring and service verification.

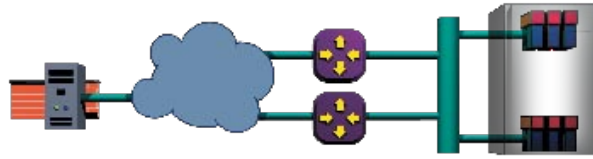


Figure 8: Multi-Link can also be used internally, allowing for multiple gateways to connect the mainframe or mid-range system to other systems within an organization. StoneGate will load balance between routes, and if one path is unavailable, connections will be re-routed to the remaining operational paths.

Scalability

The IBM eServer line demonstrates great scalability. In particular, the mainframe and midrange lines provide many options for future growth. Additional processors and memory can be allocated to existing systems, and storage and networking are also easily expanded.

Stonesoft's StoneGate firewall and VPN for the IBM zSeries and iSeries also demonstrates great scalability. StoneGate can grow across the entire server line, from xSeries clusters to both zSeries and iSeries hardware. StoneGate can also easily take advantage of dynamic resource allocation on the zSeries, for example. Multiple instances of StoneGate can be run on the zSeries or iSeries, ensuring that future growth is possible, while preserving security. Since each is distributed by the firewall amongst a pool instance can be managed through the same user interface, the scalability is not of servers within the system. Unavailable systems will no longer receive traffic.



Figure 9: Traffic coming in from multiple IP addresses (represented by the colored balls) is distributed by the firewall amongst a pool of servers within the system. Unavailable systems will no longer receive traffic.

Conclusions

In the on-demand workplace, new technologies and traditional systems are combining to provide significant return on investment, enabling business processes, and leveraging powerful system architectures. Server consolidation is a realization of this convergence, allowing an organization to run modern network architectures and multiple server systems within a single mainframe or midrange system.

With that consolidation, new risks are also introduced, in terms of system and network security. Stonesoft's StoneGate firewall and VPN for the IBM iSeries and zSeries can clearly mitigate these risks, by providing a secure, manageable, available and scalable solution to protect these systems.

STONESOFT

Stonesoft Corp.

Itälahdenkatu 22 A
00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 712 34

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 770 6681 125
fax. +1 770 6681 131

Copyright 2006 Stonesoft Corp. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products described in this document are protected by one or more of U.S. patents and European patents: U.S. Patent No. 6,650,621, European Patents No. 1065844, 1289202, and may be protected by other U.S. patents, foreign patents, or pending applications. Specifications subject to change without notice.