FIX Application Challenges

Financial Information eXchange (FIX) protocol is widely used in the financial community for automating securities trading, and is rapidly gaining adoption in increasing number of organizations. The mission-critical FIX applications demand best response time, always-on connectivity, robust security and rapid disaster recovery. Traditional FIX application infrastructure solutions are inadequate to address these critical requirements.

Connectivity management between FIX clients and FIX Engine servers is static, operationally complex, time consuming and error prone. Financial organizations that offer FIX services statically assign unique TCP/IP endpoint identifiers to each client firm for connecting to and accessing FIX applications. These connection identifiers and the associated client information are maintained in a static and manually operated database. Changes to the network and/or the FIX server farm that impact the TCP/IP connection endpoints used for FIX connectivity will require a complex and time consuming process to implement the changes on the server and the client. Both firms need to collaborate on the changes to their network and security installations to ensure connectivity without negatively impacting network operations. Even simple modifications to TCP/IP connection endpoints require new security clearances and firewall configuration changes, which could take weeks before implementation.

FIX protocol was designed to automate exchange of trade information for real-time execution. But, ironically, FIX implementations use static and manually intensive process for FIX connectivity. Static connectivity management results in increased costs and lost profits due to 1) downtime caused by human errors, 2) lost revenue opportunity due to lengthy service turn-up, 3) service impacting network and server farm changes, and 4) lost business due to poor service and response time. Figure 1 below shows the static mapping of clients to FIX server farms, and highlights the lack of flexibility to make network and server farm changes.

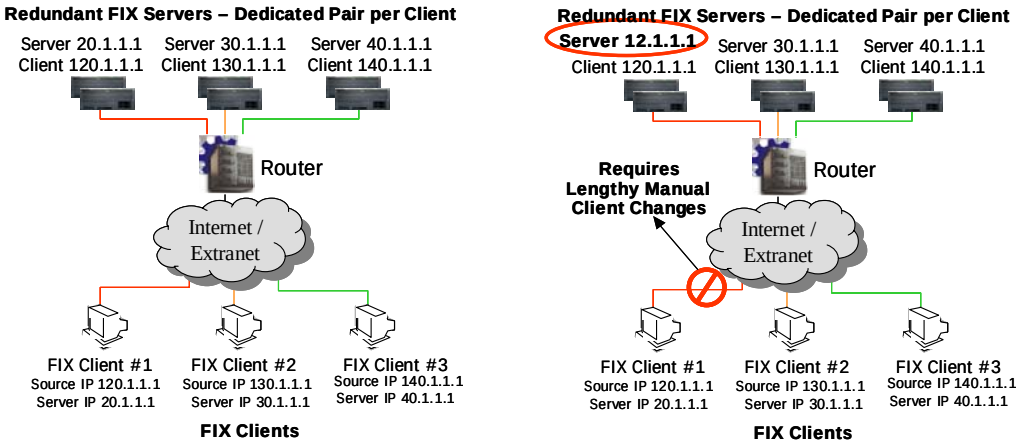

Figure 1: Static FIX Clients and Server Mapping Complicates Connectivity Management

Financial applications require highest reliability and maximum uptime. The network and the application infrastructure must not only be resilient to local failures, but also to catastrophic failures that could wipe out an entire data center. In the event of such disaster, the application infrastructure must be quickly restored at a backup location, and the failover of client connections to the backup location must be quick and transparent. Today's manual management of FIX connectivity does not lend itself to rapid and transparent failover in case of disasters. The result is unreliable service that could lead to lost business.

Current FIX implementations only allow static failover to a redundant data center by configuring the FIX clients with a backup FIX server IP address. Clients connect to the alternate site when connectivity to the primary site fails. Using such client-enforced failover to a disaster recovery site is neither reliable nor consistent. Any failure in connectivity between the client and its corresponding servers will result in the client failing over to the alternate location, and not all clients will consistently failover. To ensure consistent application performance and client service, the FIX application provider must implement rapid, automatic and transparent disaster recovery that operates independent of the clients, and is truly based on the network and application state.

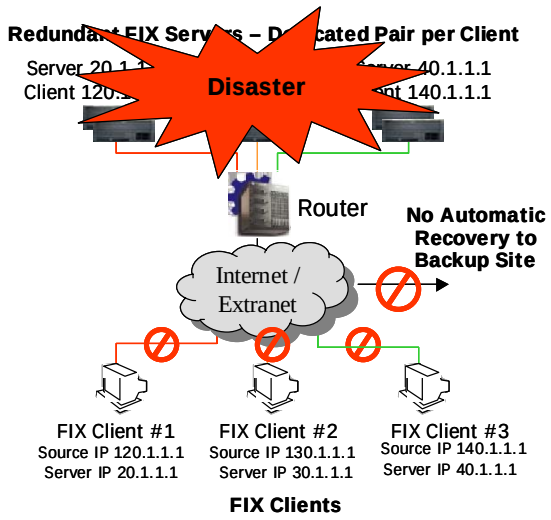

Figure 2: Lack of Rapid Disaster Recovery with Traditional FIX Application Solutions

Financial applications are a high value target for malicious users, and are routinely subject to attacks. FIX applications are especially vulnerable to many forms of Denial of Service (DoS) and Distributed DoS (DDoS) attacks because these applications expose several TCP/IP endpoints over the extranet or the Internet. These endpoints, exposed through the firewalls for client connectivity, could be exploited by malicious users to launch devastating attacks that could cripple the mission-critical FIX application infrastructure. Few firewalls provide protection against these attacks, and none deliver high-performance protection required for new types of attacks.

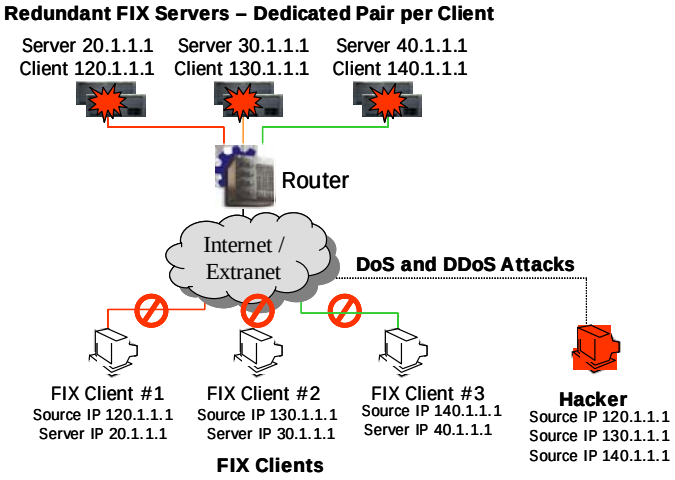

Figure 3: Threat of Denial of Service Attacks on Application Exposed to External Hosts

Foundry ServerIron FIXSWITCH

Foundry Networks' market-leading ServerIron Layer 4-7 switches uniquely enable connectivity automation, rapid disaster recovery, and robust security for FIX applications. With integrated support for the FIX protocols and applications, the ServerIron switches can be deployed transparently into existing FIX implementations for quick benefits. Foundry's Layer 4-7 switches are used by over 1600 customers worldwide, and have been the leading choice of the most demanding enterprise, financial and service provider customers to improve application availability, scalability, security and manageability for over five years. By providing a complete solution to the critical FIX application challenges outlined above, Foundry's ServerIron solution helps maximize productivity and profits, and reduce the cost of managing FIX applications.

Based on Foundry's innovative Layer 2/3 switching architecture and rich Layer 4-7 features, ServerIron switches offer wire-speed Gigabit rate protection against DoS attacks, and provide highest availability and maximum transparency to mission-critical applications. The comprehensive ServerIron product line is designed to meet a range of customer needs from the smaller financial firms to the largest multinational giants.

Foundry's ServerIron FIXSWITCH helps create and manage virtual FIX application server farms, which completely decouple client connectivity management from internal network and server farm management. FIX application providers simply need to expose a single virtual IP address to all external clients to connect to the FIX servers. This virtual IP address is logically bound to multiple real server addresses belonging to redundant pairs of FIX servers. Client connection requests are first received by the ServerIron FIXSWITCH, which then identifies the client and re-directs the request to the corresponding pair of redundant FIX servers assigned to the specific client. Client identity may be based on a choice of Layer 3 (IP), Layer 4 (TCP Port) and Layer 7 (FIX header SenderCompID field) information. The ServerIron FIXSWITCH, with the intelligent application-aware load balancing and content switching capabilities, uniquely inspects deep into the FIX application messages to identify the FIX clients and send connection requests to the corresponding redundant FIX servers. Switching client connections to the servers based on FIX message content as opposed to the traditional TCP/IP information gives added flexibility, scalability, and security to the FIX application infrastructure. ServerIron FIXSWITCH supports both the "TAG=VALUE" and FIXML formats for inspecting FIX messages.

Foundry's patented Global Server Load Balancing (GSLB) solution allows geographic scalability and rapid disaster recovery for mission-critical FIX applications. Using the Foundry GSLB solution, financial firms can rapidly and automatically re-direct client connections to the backup data center during disastrous failures of the primary datacenter. Organizations can use GSLB to scale applications beyond one data center by geographically distributing and simultaneously utilizing multiple server farms. The ServerIron switches, with their intelligent GSLB controller function, direct client connections to different sites using many sophisticated site selection algorithms, starting with the static mapping of client IP addresses to a site to the most advanced round trip time based site selection. The failure of one or more sites does not impact the overall application availability. Client requests are automatically sent to other available sites.

Security is especially critical for financial businesses, and the threat of a security breach is even more severe for FIX applications because of the many TCP/IP ports exposed to external clients through the Firewalls. ServerIron FIXSWITCH has intelligent features and superior performance to reliably protect server farms and applications against many forms of DoS, DDoS, Virus and Worm attacks. The ServerIron switches provide wire-speed Gigabit rate DoS attack protection at 1.5 million attack packets a second. With the application and content intelligence built in, Foundry switches provide application level Firewall security by detecting and discarding messages with undesirable content. Because ServerIron switches are built for high-performance, they continue to efficiently service legitimate clients even while preventing and defeating attacks.

ServerIron FIXSWITCH Benefits

FIX Connectivity Automation and Manageability

FIX applications use TCP/IP connections for session layer connectivity between FIX clients and the FIX engine servers. These connections are then used to exchange messages related to securities trading. Typically, two FIX engine servers are deployed in a redundant configuration with full session data replication between the two servers. Each pair of servers may serve one or more clients depending on the resources and the client's utilization. Clients are statically assigned a destination IP address and a TCP port for connecting to the servers, and once the client and server TCP/IP endpoints are determined, the enterprise security layer is configured to allow connections between the end points through the firewalls. Statically assigned client-server address and port information is maintained in a manual database for tracking. While the static connectivity management meets the core requirements of the application behavior, it is extremely inefficient and inflexible. Changes to the network and/or the FIX server farms require all the clients to change the information used to connect for FIX services. Changing the TCP/IP information is made even more complex and time consuming due to the layers of enterprise security and business processes. Turning up new clients is equally complex and time consuming, which further increases the time to generating revenue and provides poor service to the end customer.

Foundry ServerIron FIXSWITCH solves these challenges by automating FIX connectivity management. It significantly shortens the time to implement network and server farm changes, and to turn up FIX services to new clients. The complex coordination between the FIX provider and client organizations to establish connectivity is eliminated, resulting in faster connectivity and improved service.

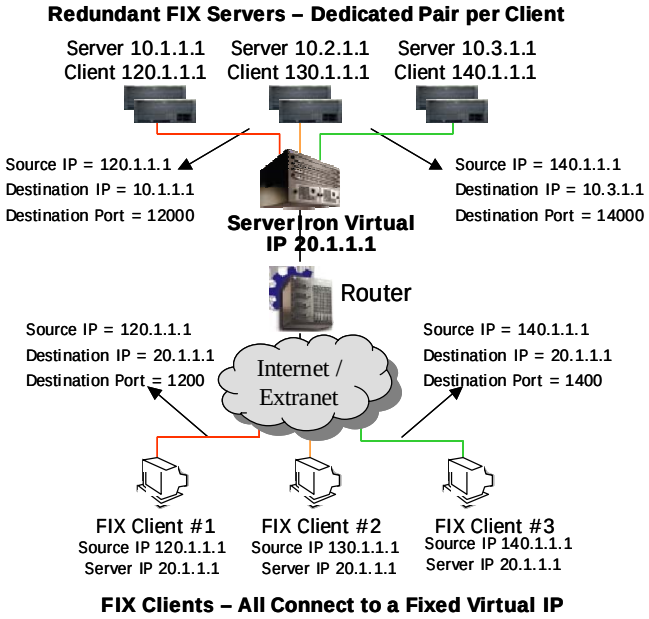

Figure 4: Virtual FIX Server Farm for Easy Manageability and Connectivity Automation

ServerIron FIXSWITCH exposes a single virtual IP address and TCP port for all clients to connect to the FIX application and the clients' corresponding pair of FIX servers. The use of virtual IP and TCP port completely decouples client-side configuration from the internal FIX network and server farm implementation. All clients send connection requests to the FIXSWITCH, which intelligently distributes them to the FIX servers assigned to a specific client. The FIXSWITCH is configured with the bindings of real server IP address and TCP port

information to the client identifier, which can be based on the client source IP or Layer 7 FIX field SenderCompID. The clients and FIX servers are completely transparent to the presence of the ServerIron FIXSWITCH in the network. Figure 4 above shows a sample network using ServerIron FIXSWITCH with a virtual IP connecting clients to multiple redundant FIX servers.

Turning up FIX service to a new client simply involves allowing the client to connect to the virtual IP, and configuring the FIXSWITCH to re-direct connections from this new client to the corresponding FIX servers. No network security and configuration changes are required. ServerIron switches support full Layer 2/3/4 ACLs (Access Control Lists), including extended ACLs, to allow connection requests only from authorized clients to pass through to the FIX servers. Figure 5 below shows adding a new client to an existing FIX network with the ServerIron FIXSWITCH providing connectivity management and automation.

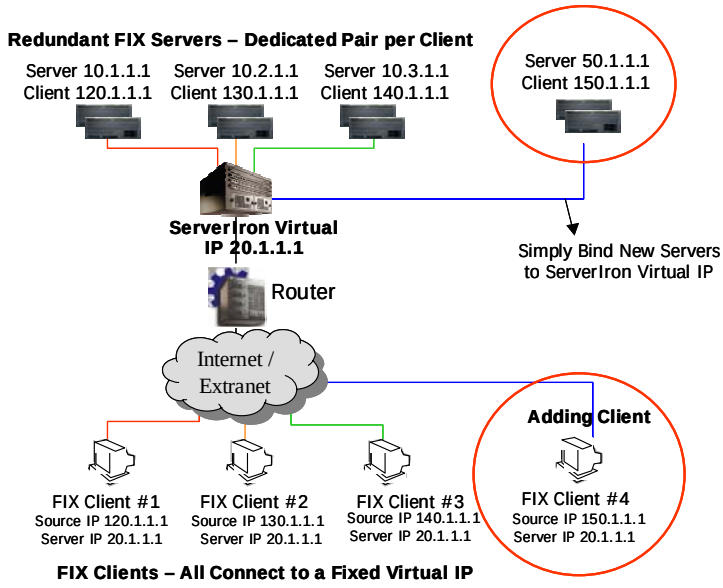

Figure 5: Turning Up a New FIX Client Simplified by ServerIron FIXSWITCH Virtual IP

Changing TCP/IP information in the internal network is completely transparent to the clients. The changes are localized to the organization with no time-consuming collaboration with all the client firms. The clients continue to connect to the virtual IP. Configuration changes to the ServerIron FIXSWITCH resulting from client IP changes can be eliminated by using the SenderCompID field in the FIX messages for client identification.

ServerIron High Availability and Stateful Failover

FIX server farm and application infrastructure require the highest availability, and must be resilient to catastrophic failures of the ServerIron FIXSWITCH. ServerIron switches feature three modes of advanced high availability in which two switches back each other up from failures, and provide rapid, stateful and transparent failover of client connections. A ServerIron switch failure will not result in the loss of client connections. In high availability mode, ServerIron switches synchronize their session tables (mapping of client connection to the real servers and the corresponding state) to each other in real-time to ensure that failure of one does not cause FIX connections to fail. The second ServerIron switch automatically detects failures, gains control and continues to serve active client connections by sending messages to the corresponding FIX server(s). No client connections are lost and there is no need for clients to reestablish or retransmit any critical information.

In the active-standby mode, two ServerIron switches are configured to manage the same Virtual IP and act as primary and backup switches. One switch acts as the primary and serves all the active client connections while

the second switch acts as a backup and awaits the failure (or degradation) of the primary switch. The backup ServerIron switch takes over when the primary one fails or degrades in its ability to serve client traffic. All sessions are synchronized from the primary to the backup switch in real time, and when the backup switch takes control and becomes the primary switch, existing client connections continue to function transparently. Hot standby mode is simple and provides the fastest failover time.

The active-active mode maximizes ServerIron switch utilization by having both the switches actively serve client traffic during normal operations. The two switches back each other up during failures. Session synchronization is bi-directional in this mode where each ServerIron switch synchronizes sessions to the other. Any ServerIron failure is automatically detected and all sessions are maintained by the remaining ServerIron without any loss of connectivity between the client and server.

Rapid Disaster Recovery

Rapidly recovering service during a disaster is a critical business requirement, especially in the financial industry. Foundry's ServerIron switches uniquely meet this need with the advanced Global Server Load Balancing (GSLB) solution. They use the highly sophisticated Route Health Injection (RHI) feature to inject route entries to the virtual IP on the ServerIron switch into the network depending on the health of the server farm. During normal operation, the ServerIron switch at the primary site injects the route to the VIP and receives client connection requests. The ServerIron switch at the backup site monitors the health of the switch at the primary site, and also the health of the local FIX servers. When the switch at the primary site is down and the local servers at the secondary site are available, the switch at the backup site performs RHI, and starts receiving client requests. Failover between the sites is completely transparent to the clients and is quick.

Network managers have immense flexibility in customizing the conditions that cause the secondary ServerIron switch to inject routes to the VIP. Failover can be controlled manually by not configuring automatic RHI based on health checks. The user can activate RHI when the backup site is deemed ready to service FIX application clients.

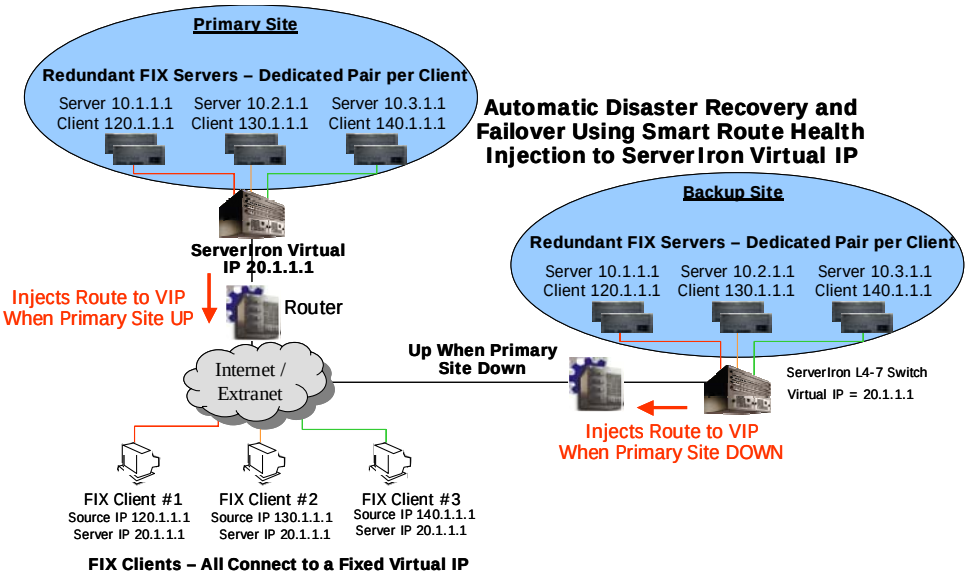

Figure 6: Rapid Disaster Recovery for FIX Applications with Foundry ServerIron FIXSWITCH

Foundry ServerIron switches also support advanced GSLB features that allow operating multiple sites simultaneously serving active clients. Financial organizations can distribute applications in multiple geographic

locations, and direct clients to the "nearest" and the "best" location. Site selection can be based on a static mapping of client IP addresses to a specific site, which may be more suitable for the FIX applications. Distributing applications ensures geographic redundancy, localizes traffic and optimizes network usage.

Security

Foundry's intelligent ServerIron Layer 4-7 switches are industry leaders in security and performance, and meet the security needs of the most demanding financial organizations in the world. The switches support a wide variety of intelligent security features, and combine these features with high performance to act as a reliable last-line-of-defense for the server farms in financial networks.

The innovative SYN-Guard feature defeats and prevents most DoS and DDoS attacks that take advantage of TCP connection handshake mechanisms. The ServerIron switch shields the servers completely from any TCP connection requests until the connection is successfully completed with the three-way handshake. The ServerIron switch forwards the connections to the real servers only after the connection is legitimately established and the application messages are validated. The servers do not receive any partially established connections, which are reset by the ServerIron switch upon expiration of a user-configured timeout. Figure 7 below shows the operation of SYN-Guard feature on the ServerIron switch and how it protects real servers and their resources to serve legitimate application clients.

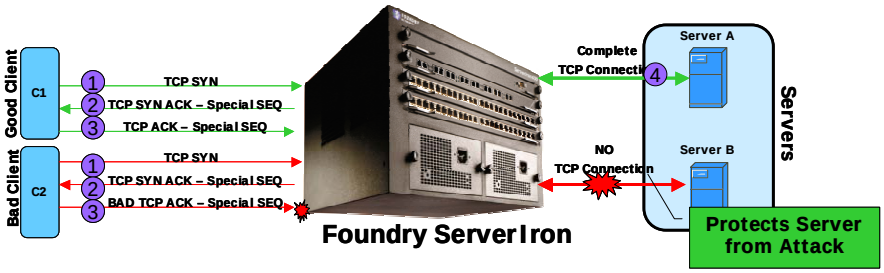

Figure 7: SYN-Guard to Defeat DoS Attacks Against FIX Servers

ServerIron FIXSWITCH acts as a connection proxy to the server farm and shields the servers from initial client communications. Only after receiving sufficient application information from the client to validate the legitimacy of the requests does the ServerIron switch forward client connections to FIX servers. By leveraging high-speed FIX content inspection, the switches also discard malicious FIX messages against user-configured filters that identify illegitimate content.

Scalability

As an increasing number of financial firms rely on FIX applications and the FIX transaction volume increases, organizations require a FIX application infrastructure that scales on demand without significantly increasing management complexity. Many FIX application implementations require a pair of redundant servers with session replication for correct application behavior. In this model, scalability beyond two servers requires that the client connections be distinguished and distributed to multiple pairs of FIX servers. Foundry ServerIron FIXSWITCH can distinguish client connections using Source IP address or the SenderCompID field in the FIX message header. By using different Source IP addresses and/or SenderCompID values, large clients' scalability needs can be met with commodity servers. ServerIron FIXSWITCH automatically switches multiple connections from the same client firm to the designated groups of servers for scalability.

Migration of Existing FIX Deployments

While the challenges confronting FIX application implementations are profound, migrating to any solution to these challenges must not disrupt business operations. Foundry ServerIron switches are field proven for non-

disruptive migration of existing applications. Current static FIX application connectivity can be preserved in the new architecture by simply configuring existing FIX server IP addresses as virtual IP addresses on the ServerIron FIXSWITCH. Clients continue to connect at the same IP addresses, and will be unaware that the server addresses are configured as virtual IP addresses on the ServerIron FIXSWITCH. A new virtual IP address can be assigned for new clients to connect.

Always-On Traffic Monitoring

Complete network management has always been a goal for network managers in companies of all sizes. Trying to understand all the possible traffic flows, the bandwidth requirements, performance implications, security threats, and billing allocations are just a few of the challenges that network managers face with modern networks. As networks grow in size, speed, and capacity, it is getting much more difficult to monitor and manage with traditional tools that rely on RMON or NetFlow based counters and statistics.

sFlow is a modern standards-based network export protocol (RFC 3176) that addresses many of the challenges that network managers face today. By embedding sFlow technology into network router and switch ASIC hardware, sFlow becomes an "always-on" technology that operates without any network or switch performance impact. Cost of implementation is driven down dramatically when compared to traditional network monitoring solutions using mirrored ports, probes, and line tap technologies. A full enterprise-wide monitoring capability for every port in the corporate network is now possible using sFlow.

Foundry is the first vendor to integrate the sFlow network monitoring technology into the Layer 4-7 switches. With sFlow network monitoring, application traffic can be monitored and measured, and any network-based attacks can be quickly identified and prevented. Armed with real-time information provided by sFlow, administrators can take quick corrective action to protect the critical resources in the network. . The sFlow data can also be collected to gather statistics, providing details about client/server usage patterns and changes over time. Additional information on sFlow is available at www.sflow.org.

Summary

FIX applications are at the heart of financial business operations. Currently, FIX applications suffer from static connectivity management, poor disaster recovery, and severe vulnerability to security threats. Foundry ServerIron FIXSWITCH, with its unique Layer 4-7 switching and FIX protocol integration, solves these challenges. It automates and simplifies FIX connectivity management by allowing all the clients to connect using a virtual IP address. By providing stateful failover in a high availability implementation to ensure that the client connections are not disrupted even during catastrophic switch failures, the ServerIron switches deliver a strong and always-on foundation to the FIX application infrastructure. The intelligent SYN-Guard and Layer 7 content filtering capabilities of the ServerIron FIXSWITCH coupled with the high-performance architecture help defeat wire-speed Gigabit rate Denial of Service (DoS) attacks, and various virus and worm attacks. Unauthorized intruders are prevented from gaining access to restricted critical services. Rapid disaster recovery and geographic scalability is achieved by the industry's most scalable and innovative ServerIron Global Server Load Balancing (GSLB). And, with always-on standards-based sFlow network monitoring, one gains improved network security and visibility into the overall application health.

Appendix B – Reference Documents and Links

The Tolly Group Independent ServerIron Test Report for Security and Connection Performance
http://www.foundrynet.com/products/webswitches/serveriron/PDFs/Tolly%20Foundry%20ServerIron%20Report%20-%20Sep%202003.pdf

Foundry ServerIron White Papers and Application Notes

http://www.foundrynet.com/products/webswitches/serveriron/appnotes.html

ServerIron Data Sheet
http://www.foundrynet.com/products/webswitches/serveriron/productInfo.html

ServerIron ISP Link Load Balancer Data Sheet
http://www.foundrynet.com/products/webswitches/serveriron/PDFs/ServerIron_LB%20FINAL.pdf