



## Securing Financial Services Beyond the Perimeter

*A multi-layered solution is required for securing financial services beyond the perimeter.*

### CONTENTS

The Evolving Financial Services	2
Improving Customer Service Beyond the Perimeter	3
Increasing Revenues Beyond the Perimeter	4
Minimizing Expenses Beyond the Perimeter	5
Regulatory Compliance Concerns	6
Security Beyond the Perimeter: A Clean VPN approach	9
The SonicWALL Solution	10
Conclusion	10

## Abstract

*The traditional financial services network has evolved into a transactional e-commerce model, providing customers with products and services beyond the traditional network perimeter. Conducting financial services beyond the perimeter offers banks and credit unions new opportunities to enhance customer service, increase revenues and lower expenses. However, it can also increase network security complexity, exposes banks to new threats and raises additional concerns for meeting regulatory compliance.*

*To counter these concerns, a viable solution must reduce complexity while providing the utmost security possible. The practice of a “clean VPN” utilizes a centrally-managed, multi-layered approach that integrates intelligent firewall technology such as Unified Threat Management (UTM) with intelligent remote access technology such as SSL VPN to deliver a comprehensive solution. To ensure performance, any clean VPN environments must be architected using high-performance technology such as multi-core processing platforms.*

*SonicWALL® Network Security Appliance (NSA), SSL VPN and Global Management System (GMS) solutions integrate seamlessly to provide a layered solution for securing financial services beyond the perimeter. The entire line of SonicWALL solutions are engineered to reduce the cost and complexity of network security, while delivering comprehensive security and high performance.*

## The Evolving Financial Services Network

The pace of innovation in technology has increased dramatically over the past decade. Broadband access to the Internet has become not merely ubiquitous, but an expected standard, at work, at home and everywhere in between. Mobile devices have proliferated to the point where laptops, PDAs and smartphones are increasing the phase-out of traditional desktop PCs. E-commerce has become a mainstream standard for conducting business—including financial services.

As a result, banks or credit unions are no longer restricted to specific physical locations. In fact, merchants, banking customers and credit union members have all come to expect a full range of financial products and services to be easily available from anywhere online as a matter of course. Deregulation has blurred financial service provider boundaries, with third-party partners, product vendors and consultants playing an increasingly vital a role in banking operations and product offerings, often requiring secure access to “inside” application resources from “outside” networks and endpoint devices, traversing internal and external firewalls.

Broader access to financial services via the Internet has improved customer satisfaction, increased efficiencies and opened new revenue opportunities. However, it has also increased the number of access points, devices and network environments that are outside of the bank IT department’s direct control, leading to greater complexity in administration and security. Breakthroughs in interactive and Web-based technology have extended the value of banking networks, but they have also created new conduits for evolving threats. And yet banks must defend their networks and data within ever-tighter budget restraints.

### **Banking without borders**

In its most fundamental definition, a bank stores and moves numbers, and today those numbers are data. In this digital paradigm, a bank’s vault is analogous to its data center, with its branches opening onto the Internet. The traditional bank network has evolved into a transactional e-commerce model, providing globally-accessible services over the Web. The traditional model has therefore been effectively inverted, transforming what was a closed leased-line WAN to a globally-distributed network that connects employees, partners and customers over multiple Internet and intranet, private and public, wired and wireless networks. The bank’s traditional “network perimeter” has concentrated into a “resource perimeter” around the banking

application data center. IT is focusing more on granular access controls that secure communications to the data center from beyond the perimeter.

This trend departs from prior attempts driven by costly proprietary solutions requiring IT to retrofit their infrastructure in order to ensure security with “smarter” networks. Instead, the focus has shifted to leveraging public networks and shared infrastructure with the operational investments focused on the reliability and transparency of service, with the security investment focused on endpoint control and enterprise resource control.

### **Balancing protection with performance**

With the perimeter contracting around the banking applications data center, it becomes even more important to monitor and manage the traffic flowing both in and out of that perimeter over the virtual network. In practice, IT must balance traffic policy enforcement with system performance. Any solution must enable comprehensive scanning of bandwidth-intensive traffic across the perimeter without diminishing network throughput.

## **Improving Customer Service Beyond the Perimeter**

Arguably, a bank’s primary asset is not its money; rather, it is the trust of its customers. Satisfied banking customers and credit union members are more likely to purchase new products, increasing revenues. They are also less likely to defect to other banks, reducing customer attrition and re-acquisition costs. Extending financial services beyond the perimeter improves customer service and satisfaction by enhancing the customer’s experience and maximizing customer offerings. Depending upon its size and strategic resources, a bank can extend beyond the perimeter to competitively differentiate themselves by offering more personalized customer service, or by offering greater breadth of online products.

### **Enhancing customer experience**

Access is crucial to customer satisfaction. Customers expect bank to have a 360° view of their accounts. Customers want to be able to interact with their bank regardless of location or time of day by leveraging comprehensive online banking capabilities. Larger commercial customers have come to expect real-time self-service to banking information and operations across the perimeter, allowing them to more tightly manage their cash and draw on their lines of credit as needed.

Much of this customized experience is supported by technology-enabled CRM systems and data-driven personalization. However, these in turn require high-granular security solutions based upon personalized policy controls.

### **Maximizing customer offerings**

Customers are becoming more demanding, consolidating their business at banks that offer robust portfolios of services. To meet this demand, banks have to onboard new services quickly. In order to satisfy these customer demands and keep up with the rate of change in the industry, many banks are drawing on outside suppliers to deliver products. This is especially the case for products outside a bank’s core business. This allows banks to focus on their core business, quickly deliver the products best suited to their customers’ needs and to change more quickly as their business requirements change.

## **Buoying customer confidence**

Customer satisfaction can be negatively impacted by broader issues such as consolidation and restructuring. IT is challenged with ensuring that products and services remain seamlessly available to customers during times of corporate transition. A bank's reputation can also be potentially damaged by phishing and pharming attacks that can significantly undermine brand credibility.

Additionally, customers count on their banks to safeguard their online financial transactions and data by meeting compliance with various government and industry regulations. Merchants also expect banks to partner with them to help comply with regulations that relate to their own financial management as well. IT must select and implement security solutions that can best support these compliance guidelines.

## **Increasing Revenues Beyond the Perimeter**

Tighter lending restrictions have limited opportunities for banks to generate revenue. By extending financial services beyond the perimeter, banks gain additional opportunities for increasing revenue, both by making it easier for customers to purchase and use products online, and by offering extended products online via third-party partnerships.

### **Selling to customers beyond the perimeter**

Today's private and business banking customers are not only Internet savvy, they expect to receive products online, and will choose banks that offer the most comprehensive and user-friendly online banking product lines. To stay competitive, banks now must ensure the security and integrity of a broad range of confidential online banking transactions extending beyond the network perimeter, including:

- Bill payment
- Inter-account fund transfer
- Financial data downloads (e.g., to Quicken®, Microsoft® Money and Quickbooks®)
- Viewing of statements and balances
- Viewing of loan status information
- Management of Certificates of Deposit (CDs)
- Automated alerts based on balances, transactions and other activities

In these cases, IT effectively becomes an online service provider. To protect the network and their customers, IT must adhere to the most stringent e-commerce security practices, implementing the most robust Internet threat protection solutions available.

### **Partnering beyond the perimeter**

In order to satisfy these customer demands and competitively keep up with the rate of change in the industry, banks are increasingly reliant upon outsourced partnerships with third-party suppliers to deliver new revenue-generating products. This allows banks to focus on their core business, quickly deliver the products best suited to their customers' needs and to change more quickly as their business requirements change. Frequently, a bank merely provides a branded online storefront "skin" through which the customer clicks, and the actual product transaction takes place via the partner's network, outside the bank's network perimeter. These out-of-perimeter online products can include:

- Payroll services
- Automated Clearing House (ACH) fraud-protection
- Electronic Data Interchange (EDI) tracking and reporting

- Internet merchant services
- Tax payment
- Accounts management and reporting services
- Identity theft protection

The ongoing challenge for IT is to provide technology to monitor and safeguard data communications between the bank's core data center and these third-party providers, to prevent intrusion and contamination, and protect its customers and its reputation.

## Minimizing Expenses Beyond the Perimeter

In order to maintain lower Federal Deposit Insurance Commission (FDIC) rates, banks must also look to ways technology can lower their FDIC Commission Expense-to-Revenue (ER) ratio. This ratio measures the proportion of net operating revenues that are absorbed by overhead expenses, so that a lower value indicates greater efficiency.

Since revenue is under constant competitive pressure, the surest way to increase profitability and lower ER is by cutting costs. This can be achieved by taking advantage of partnerships beyond the network perimeter to lower product development and delivery costs, and by reducing IT overhead through greater efficiencies in system acquisition, deployment and management.

### **Reducing product development and delivery costs**

Cost-containment opportunities provided through outsourcing are particularly evident in products outside a bank's core business. For instance, equities and securities offerings, online products and integrations with commercial customers can all be obtained more quickly and cost-competitively from third-party managed service providers. The result is ultimately better margins and higher quality, but at the cost of greater potential exposure to threats from across the perimeter from third-party environments that are beyond the direct control of the bank's IT department.

### **Reducing system acquisition costs**

In the past, banks had to settle for esoteric security solutions targeting single-point threats like viruses, spam and intrusions as they arose, often adding complexity and expense without corresponding value. Today, security technology has evolved and IT can lower acquisition costs by selecting simpler, well-engineered and cost-effective solutions that leverage industry-standard hardware architectures.

### **Reducing system deployment costs**

The endpoint devices of banking networks have evolved from terminals to desktops to laptops. Not only does this open new security concerns, but can complicate deployment of security solutions, especially those requiring installation and upkeep of resident client agents on the endpoint device. IT can streamline deployment using technically superior and highly integrated solutions that simplify complex designs, leverage Web technology and easily scale to demanding and distributed network infrastructures. For example, IT might ease deployment costs by selecting an access control solution that integrates seamlessly with pre-established policy domain architectures such as RADIUS and LDAP.

### **Reducing system management overhead**

To lower total cost of ownership, IT should deploy products and services that deliver real time threat and data protection solutions with minimal administrative overhead. Systems administration, policy management and reporting should be centralized through a uniform console interface, to minimize training and ramp-up costs. To minimize help desk requests and lower support costs, security operations should be transparent to end-users, and endpoint interfaces should be friendly and intuitive. IT must also sustain operational

efficiency by leveraging high-performance processing capacity for faster throughput and improved responsiveness, to ensure network service levels, increase productivity and provide a greater overall return on technology investment.

## Regulatory Compliance Concerns

Banks are mandated by a host of governmental and industry regulations to protect sensitive data under penalty of significant fines, increased insurance rates, or discontinued transaction capabilities. As compliance becomes an essential factor in every decision made regarding operations of a bank's business, IT departments no longer have final say on whether to implement effective measures to adequately enforce these regulations. As a result, IT increasingly considers technology-enabled aspects of regulatory compliance a key factor in selecting any security solution.

### **GLBA mandates**

Of significant concern to banks is compliance with the Gramm-Leach-Bliley Act of 1999 (GLBA). GLBA requires (along with other mandates) that a bank's information security program must be designed to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity
- Protect against unauthorized access to or use<sup>1</sup>

The Federal Financial Institutions Examination Council (FFIEC) recognizes the National Institute of Standards and Technology (NIST) as an acceptable source for guidance on meeting compliance<sup>2</sup>. NIST criteria recommendations for technical security<sup>3</sup> include:

- Communications (e.g., dial-in, system interconnection, routers)
- Cryptography
- Discretionary access control
- Identification and authentication
- Intrusion detection
- Object reuse
- System audit

Best practices warrant that IT select and implement security solutions that employ:

- Encrypted communications
- Granular access control
- Verified identification and authentication (e.g., SSL VPN)
- Comprehensive intrusion detection (e.g., Unified Threat Management network security appliances)

---

<sup>1</sup> Gramm-Leach-Bliley Act of 1999, Appendix B

<sup>2</sup> Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook

<sup>3</sup> Risk Management Guide for Information Technology Systems, NIST SP 800-30, Table 3-3

- Object-based, centralized management systems

## PCI standard

The Payment Card Industry Data Security Standard (commonly referred to simply as PCI) was designed to provide the baseline requirements for how vendors should protect cardholder data to ensure it is not stolen or compromised. Classifications for participants are as follows:

- Issuers: Member banks and financial institutions who issue credit cards to individuals or corporations.
- Acquirers: Member banks and financial institutions who acquire and manage merchants accepting cardholder payments / transactions
- Service Providers: Entities that provide any service requiring the processing, storage or transmission of card information/transaction information on behalf of member organizations, acquirers or issuers.

Member organizations are responsible for the security of cardholder data and cannot store certain types of data on their systems or the systems of third-party service providers. Member organizations are also responsible for any damages or liability that may occur as a result of a data security breach or non-compliance with PCI. PCI applies three methods of verifying compliance:

- Independent audit by a Qualified Security Assessor (QSA)
- Self-validated Assessment Questionnaires (SAQ)
- Network scans by a qualified independent scan vendor

Depending upon an organization's transaction volume, payment channels and potential exposure, PCI classifies merchants into four levels of required compliance verification:

- **Level 1:** These are merchants processing over 6 million transactions per year or compromised in the past year, regardless of acceptance channel. To comply with PCI, Level 1 merchants are required to conduct annual onsite review by a Qualified Data Security Company (CDSC) or internal audit; as well as quarterly network scans by a qualified independent scan vendor.
- **Level 2:** These are merchants processing 1-6 million transactions per year, regardless of acceptance channel. To comply with PCI, Level 2 merchants are required to conduct annual self-validated assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.
- **Level 3:** These are merchants processing 20,000 to 1 million transactions per year. To comply with PCI, Level 3 merchants are also required to conduct annual self-assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.
- **Level 4:** These are merchants processing under 20,000 e-commerce transactions per year, and all other merchants processing up to 1 million transactions per year. To comply with PCI, Level 4 merchants are also required to conduct annual self-assessments and an annual network scan.

Additionally, PCI sets three levels for service providers:

- **Level 1:** These are service providers including all VisaNet processors (member and non-member), and all payment gateways. To comply with PCI, Level 1 service providers are required to conduct annual onsite review by a Qualified Data Security Company (CDSC) or internal audit; as well as quarterly network scans by a qualified independent scan vendor.
- **Level 2:** These are service providers not in Level 1 that store, process or transmit over 1 million Visa accounts/transactions per year. To comply with PCI, Level 2 service providers are required to conduct annual self-assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.

- **Level 3:** These are service providers not in Level 1 that store, process or transmit less than 1 million Visa accounts/transactions per year. To comply with PCI, Level 2 service providers are required to conduct annual self-assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.

	Levels	Annual Criteria	Audit via QSA	Annual SAQ	External Scans
<b>Merchants</b>	1	6M+ transactions OR security breach	x		x
	2	150K-6M transactions		x	x
	3	20K-150K transactions		x	x
	4	<20K transactions		x	x
<b>Service Providers</b>	1	All processors and payment gateways	x		
	2	1M+ accounts/ transactions	x		
	3	<1M accounts/ transactions		x	x

The PCI standard is broken down into twelve fundamental requirements that are designed to be relatively intuitive to follow:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data and do not store card and transaction data unnecessarily
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly maintain secure systems and applications
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Establish and maintain high level security principles and procedures

These standard principles and mandated requirements offer an overall guideline for security best practices that should be applied not only to your credit card information, but as part of your organization's entire business data security program.

## Security Beyond the Perimeter: A Clean VPN Approach

As the traditional banking network perimeter contracts further into an applications resource perimeter, and endpoint devices become increasingly outside direct IT control, it is more important than ever to monitor and secure both the traffic flowing through that perimeter and the endpoints beyond the perimeter. Best practices warrant a defense-in-depth approach utilizing multiple layers for thorough protection.

A “clean VPN” approach integrates a layer of intelligent remote access technology such as a Secure Sockets Layer virtual private network (SSL VPN) to secure users and devices beyond the perimeter, with layer of intelligent firewall technology such as Unified Threat Management (UTM) to secure data traffic penetrating the perimeter. Optimally, this clean VPN would be controlled via a centralized management and reporting interface. To be practically effective, an integrated clean VPN should be able to comprehensively:

- Detect the integrity of all endpoints, users and data traffic
- Protect resources against unauthorized access and malware attacks
- Connect authorized users easily to mission-critical resources in real time

### **Detect the integrity of endpoints, users and traffic**

Certain SSL VPNs employing End Point Control (EPC) technology can interrogate the endpoint to verify the presence or absence of required attributes (e.g., operating systems, applications, domain membership, certificates, files, anti-virus, anti-spyware, personal firewalls, etc.) that are required to adhere to the bank’s security policy, all before authorizing VPN access. By integrating certain high-performance UTM solutions with the SSL VPN, IT could ensure that all traffic is scanned and decontaminated before it can traverse the bank’s resource perimeter. Because malicious attacks can penetrate stateful packet inspection without detection, the UTM firewall should optimally conduct deep packet inspection on all traffic.

### **Protect resources against unauthorized access and attacks**

A clean VPN can protect resources through enforced authentication, data encryption, granular access policy and gateway threat protection. The VPN policy engine should control admission based upon the level of trust for each remote user and end point device, and control access based upon the applications that each user is authorized to access. Different access policy should be enforced depending upon whether the endpoint is a fully IT-managed device, or an unmanaged public or personal device. While access controls are critical to protecting resources, even the most granular access controls could be potentially undermined by ultra-sophisticated criminal attacks and evolving threats. Best practices warrant the additional layered protection of a comprehensive UTM firewall on the resource perimeter that can deliver auto-updating anti-virus, anti-spyware, intrusion prevention, anti-spam and content filtering.

### **Connect users to resources easily in real-time**

Based upon device interrogation, user authentication and access policy, the clean VPN should then intelligently and seamlessly connect users to authorized resources, employing an access method and interface appropriate to the specific endpoint device (e.g., laptop, PDA, smartphone, hotel kiosk, etc.). To prevent performance bottlenecks, best practices must also balance traffic policy enforcement with system performance. The UTM firewall should also allow administrators to be alerted to bandwidth anomalies that could infer policy abuse and trigger appropriate use restrictions. Any clean VPN environments must be architected using ultra-high-performance architecture platforms to enable comprehensive scanning of bandwidth-intensive mobile traffic in real time, without bringing network throughput to a standstill. Multi-core processor architecture offers flexible scalability, high performance and low power consumption when compared against general purpose and ASIC processor platforms.

## Centralized management and reporting

In order to ensure compliance beyond the perimeter, it is also crucial for IT to have centralized management that can generate comprehensive event reporting, proactive alerts, rapid forensic analyses and complete audit trails. Integrating dedicated security management oversight simplifies administration, helps identify gaps or anomalous activity, and facilitates regulatory compliance audits.

## The SonicWALL Solution

To enhance customer service and open new opportunities for revenue generation via the Internet and third-party outsourcing, and with the perimeter contracting ever more tightly around the banking applications data center, it becomes even more important than ever for IT to monitor, manage and secure the traffic flowing both in and out of that perimeter. This level of protection requires a layered approach that integrates intelligent firewall technology with intelligent remote access technology to deliver a comprehensive, centrally-managed solution. SonicWALL engineers dynamically intelligent services, software and hardware that seamlessly integrate into a comprehensive offering of high-performance security solutions.

### Implementation scenario: a SonicWALL Clean VPN

A SonicWALL® Clean VPN™ integrating SonicWALL Aventail® SSL VPN, SonicWALL Network Security Appliance (NSA) and SonicWALL Global Management System (GMS) products can provide a bank with a single comprehensive solution for defense-in-depth security. SonicWALL Aventail SSL VPN End Point Control (EPC) allows banks to establish trust for users, devices and traffic before allowing a connection to any sensitive information on the network, while the SonicWALL NSA ensures that all VPN traffic is scanned in real-time and decontaminated before it can traverse the bank's resource perimeter.

### Unparalleled value and efficiency

To provide even deeper layers of security for financial services organizations, SonicWALL offers SonicWALL Email Security spam protection and SonicWALL Continuous Data Protection (CDP) backup and recovery. SonicWALL helps IT break free from premium-priced, complex legacy systems with easy, affordable solutions that are robust enough to support the needs of any financial institution. By relentlessly innovating to drive the costs and complexity out of building and running high-performance secure infrastructure, SonicWALL offers financial services organizations exceptional value, minimizing operational overhead and lowering ER through eliminating costs associated with:

- Acquisition—by standardizing to commercially-available hardware, maximizing supply chain efficiencies and leveraging SonicWALL's leading-edge software development across the entire product line
- Deployment—by delivering elegant, simplified solutions that are quickly and easily set up, even in the most demanding network infrastructures
- Management—by providing globally-managed, centrally-administered products and dynamic security services that deliver real-time threat and data protection

## Conclusion

Banking beyond the perimeter is a competitive reality, which IT must secure with comprehensive solutions that do not increase administrative overhead or diminish network performance. SonicWALL streamlines the complexity out of security, allowing banks to extend products and partnerships beyond the traditional network perimeter, while maintaining the confidentiality, integrity and security of their information assets in order to meet regulatory demands.

©2008 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.