Replacing Complex Internet VPN Networks

Case Study - Kirkland's

A Cybera White Paper

Regional and growing national based retailers, restaurants and physicians practices have looked for cost effective ways to securely connect their growing businesses and practices. The need to connect sensitive data driven by payment, accounting, settlement and patient record applications that are bandwidth hungry requires robust connectivity. Dedicated private network alternatives tend to be too bandwidth limited at acceptable price points. Thus traditional broadband solutions provide the best value, but pose security challenges.

Limited IT staff and operating cost budgets push businesses to what appear to be affordable Internet VPN solutions. This typically requires the purchase of a firewall/VPN router at each location and establishing dedicated VPNs between sites. However, the cost and complexities of Internet VPN solutions quickly become problematic as broadband outages occur and hidden costs of dedicated IP addressing and configuration changes add up. This white paper proposes an alternative solution to traditional Internet VPN solutions that reduces complexities and lowers costs, while improving security. This white paper takes a look at how a regional retailer Kirkland's adopted Cybera ONE and achieved more stability, network simplicity and cost savings.

What Are Internet VPNs?

Internet VPNs are Virtual Private Networks established over public Internet bandwidth. VPNs are semi-permanent tunnels established between two points, typically two routers, servers, software clients or a combination of two of these. A VPN tunnel defines a specific path in which encrypted data travels securely between the two points. The two points can connect in a geographically agnostic manner, as long as the two sites have Internet connectivity.

An Internet VPN at a minimum requires five primary elements:

1. Public Internet access
2. A static public IP address at each end of the tunnel
3. Two Internet VPN devices (routers, servers, software clients), one at each end, that have compatible VPN standards settings
4. A secret password that establishes a valid "hand shake" or authentication between each end of the tunnel.
5. A qualified technician to setup and maintain the configurations in each end device/client.

Internet VPN networks can either be homegrown or facilitated by a service provider. Homegrown VPNs are typically strung together by an internal IT technician or by an outside contractor. Service provider facilitated VPN networks are developed and managed by a third-party that typically supplies all of the Internet connections at each site for a monthly management fee.

Benefits of Internet VPNs

Internet VPNs are a relatively cost effective solution compared to dedicated private networks such as MPLS, Frame Relay or VSAT (satellite) networks. Internet VPNs allow for the use of public broadband services at each site which typically offer greater bandwidth for a lower price than private line networks. The primary costs associated with Internet VPNs are the one-time charge of purchasing a firewall/VPN router and the cost of IT personnel or contractors to setup the VPNs. These charges are incurred at each site in the VPN network. Typically there is a monthly management fee for administering the VPN networks, although this may be bundled with other monthly retainer charges for additional IT services. Costs could also be incurred through the salary of an internal IT staff, but these costs are typically spread over a variety of other IT tasks such as computer maintenance, server maintenance and local area network (LAN) management. Still, the aggregate costs of an Internet VPN network are typically lower than the cost of dedicated private line networks because of the circuit costs. This holds true even when contracted or internal IT staff costs are accounted for across both methodologies.

Internet VPNs provide very secure transport between two end points, and thus, reasonably secure network architecture. Data in transit over a VPN is encrypted and requires fairly sophisticated methodology for a third party to capture and decipher. A variety of different VPN security algorithms can be deployed that make deciphering data in transit even more difficult since not just one method of encryption can be deployed. As long as the end point device is not compromised by an outside party, VPN networks are a fairly cost effective network solution.

Drawbacks of Internet VPNs

As secure as Internet VPNs may be for data in transit between two end points, they can also provide unprecedented access to a hacker that compromises one of the VPN end point devices. If a computer with a VPN client or a server is infected with malware or viruses, the device can become compromised. Once compromised the hacker can gain access to the VPN tunnel itself and use the tunnel, or series of tunnels, to navigate the entire private network across all sites. Game over.

As stated previously, Internet VPNs require public IP addresses in order to establish the tunnels over the Internet and route traffic between the two end points. It is the public IP address that is targeted by hackers, because it is public and broadcast over the Internet. Therefore a very robust firewall with very strict parameters is a requirement for Internet VPNs to be secure. But a robust firewall in and of itself is not enough when a stringent security policy is not defined and enforced. The addition of public facing services such as Wi-Fi, or the downloading of content from infected web sites, or a virus on a flash memory card (USB storage device) can facilitate a network breach. These are very common occurrences, especially in networks that do not have a full time IT staff to manage and monitor all users on the network. Simply put, VPNs can provide a false sense of security if they are not implemented as part of a comprehensive security plan with the appropriate resources to actively manage the network.

Therein lies one of the largest hidden costs of Internet VPN networks. The need for the appropriate IT staff, or a qualified contractor organization, that can assure an allocation of resources to your network. Often contractors are busy securing additional clients and cannot cost effectively allocate the consistently focused resources your network needs to remain secure. Even internal IT resources tend to be stretched with many projects and have a difficult time allocating the focus of monitoring network logs to ensure the network has not been compromised. With increasingly sophisticated hacking methodologies arising at greater frequencies, VPN networks are inherently vulnerable. Internet VPN networks are also vulnerable because of their complexity. A simple point to point VPN is not very complex. But when VPN networks begin to scale across more and more sites, complexity increases in a linear manner. Each site requires a discrete configuration, and every configuration change on the network can have a cause and effect relationship that is difficult to foresee.

Another hidden cost of VPN networks is the need for static public IP addresses. Static public IP addresses are provided by your Internet Service Provider (ISP) for a monthly charge. The alternative is to use a dynamic IP (referred to as DHCP) address service which is much lower in cost. DHCP services carry significant impacts on

Internet VPN configuration because each time a router is restarted it will likely grab a new public IP address and the Internet VPN configuration will no longer be valid, resulting in the VPN not working. Remember that each Internet VPN end-point requires a deterministic public IP address, and when the address changes, the configuration must be updated. There are some methods of getting around this by using advanced tools such as Dynamic DNS, but this requires additional costs and results in long delays of the VPN rediscovering its new route. Therefore, most companies opt for static public IP addresses.

Moving from a DHCP based service to a static IP service immediately changes the price of the broadband service, as it moves the customer from a residential pricing plan to a business pricing plan. These cost increases can range from $20.00 a month to over $150.00 per month depending on your ISP and the speed of service purchased. The cost of the public IP address is then added on top of the circuit cost. A single static IP address is an additional cost of $10.00 to $20.00 a month depending on the same factors as the circuit price increase. If a customer requires multiple static IP addresses, costs can increase from $20.00 to $35.00 or more based on how many IP addresses are needed. ISPs usually provide multiple static IP addresses in "blocks" of addresses, so if you only need two additional addresses, you will end up paying for a block of five addresses. The result is typically unexpected costs that make Internet VPN networks more expensive than originally planned.

If all of these issues were not enough already, there is still another dynamic that can increase the costs and complexities of Internet VPN Networks. All broadband services are not made the same. Some broadband Internet services are straightforward and simple. The simple services are where the IP address that you are assigned always stays the same. But broadband services based on PPPoE technology, such as those from AT&T, are not so easy. The problem is that PPPoE (Point-to-Point Protocol over Ethernet) requires a user name and password authentication device at the customer premise. Typically in residential type services this is handled by the AT&T DSL modem. Although, the AT&T modem has a firewall which commonly blocks services such as VPNs, VOIP and other applications. As a result, companies are forced to reconfigure the AT&T modem and place them into bridge mode to stop the blocking. This requires the customer router to perform the PPPoE authentication instead. If a business purchased a single static IP address, the IP address will stay the same even after a router power cycle. But if it purchased multiple static IP addresses, then the firewall/VPN router will not retain the static IP address after each power cycle. The VPN router may lose the static IP address at any time, even if power is not removed or lost from the router. The only way to keep a static IP is to purchase an additional router to perform the VPN functionality, as only the routers behind the PPPoE authentication device will retain static IP addresses. This increases cost and complexity, and creates variability between site implementations based on the specific DSL provider. Complexity is vulnerable and is more costly to support.

There are a lot of hidden costs and complexities associated with Internet VPN networks. The net result is that Internet VPN networks can provide a false sense of security. They are vulnerable and require constant maintenance. The price tag of Internet VPN networks is typically much higher than estimated when all associated costs are accounted for and totaled.

The Kirkland's Story

Kirkland's is a home décor retailer with 292 stores across 30 states and does not have a large internal IT staff. Kirkland's initially built their own Internet VPN network, but after discovering many of the complexities of operating the network decided to outsource their Internet VPN solution. Kirkland's looked at private network alternatives but the total cost was prohibitive. As a result, they selected to use the Net VPN from AT&T as an outsourced Internet VPN solution. The cost was reasonable, but generally higher than operating the network themselves. The main advantage of the AT&T solution was that AT&T would manage the network and not Kirkland's limited IT staff.

Over time, the inherent issues associated with the complexities of Internet VPN continued to present themselves, even with AT&T's management. Outages were common and frequent configuration changes added to the fixed monthly cost per site for the service. The AT&T service was limited to site-to-site VPN connectivity and did not address the need for additional services such as secure payment services. They needed network security solution that they could implement across their enterprise footprint to meet PCI compliance standards along with their core private network. Kirkland's started looking at secure payment solutions for its stores and evaluated Cybera ONE.

Kirkland's engaged Cybera to provide a secure network that could easily be deployed and managed across their enterprise footprint. With Cybera ONE, the company gained security services including hosted VPN services with managed concentrators, authentication and encryption, wireless IDS, application segmentation, and remote archiving. In addition, Cybera ONE was able to improve resiliency and redundancy for secure payment processing through its built-in backup 3G wireless application. As a result, Kirkland's improved their payment security process, improved reliability and lowered their infrastructure costs.

Cybera ONE's unique architecture addressed the inherent security vulnerabilities of Internet VPN through the following technological advancements.

1. Cybera ONE utilized a secure application appliance (SCA-315) that facilitated persistent VPN connections with the Cybera Secure CORE cloud. All of Kirkland's sites were connected to Cybera's data centers instead of using point-to-point tunnels. Store VPNs were connected to regional VPN concentrators that provided aggregation and activity logging. Then traffic was aggregated onto a single VPN going to Kirkland's headquarters which reduced the complexity of the network topology.

2. Cybera ONE did not use public IP addressing. The SCA-315's unique functionality allowed it to be installed behind a DSL or cable modem and only use a private NAT based IP address. As a result, the Kirkland's VPN network was virtually invisible to hackers. Even if someone hacked the DSL or cable modem, the SCA-315 was not accessible from the modem IP route. The VPN to the secure core served as a secure overlay network over the public broadband that was not dependent on public IP addressing at all. This eliminated all the complexities associated with PPPoE, deterministic VPN configuration and the costs associated with static IP addressing from ISPs.

3. Cybera ONE enabled secure connections to corporate and card processing gateways. This eliminated the need for multiple network devices, reducing cost and complexity.

4. Cybera ONE incorporated integrated wireless failover functionality onto 3G/4G networks, eliminating the reliability issues they experienced with DSL only solutions. The cost savings achieved from using DHCP only circuits easily covered the cost of the wireless backup service.

5. Cybera ONE's fully managed service was supported by Cybera's Solutions Management Center (SMC). In addition, Kirkland's had access to Cybera's Smartview management system which maintained logs of all activities on their network and alerted their IT personnel of actionable

events on the network that required their attention. All network logs were stored and filed for future use in the event of a PCI compliance audit, with documentation that logs had been reviewed daily by Cybera. Cybera ONE enabled Kirkland's IT staff with useful and actionable data such as a map of all network sites, their up/down status, fail-over state, and bandwidth utilization performance.

Cybera ONE addressed the shortcomings of Internet VPN networks, while reducing the total cost versus both internally managed and outsourced Internet VPN solution. "With Cybera, we know our network is secure and we have a platform to expand our network security services in the future." Kirkland's was able to add new services using Cybera ONE such as adding secure Wi-Fi to its stores for customer use without compromising security. "Cybera understands the security needs of our business and delivers excellent services and resources to protect our network effectively and efficiently." The simplicity of the Cybera ONE architecture allowed for a scalable and replicable solution that did not tax Kirkland's IT staff. "Cybera has helped Kirkland's develop a standardized network security solution across our enterprise to protect against cybercrime and meet PCI compliance standards."

The Cybera ONE Secure Application Architecture Solution

Cybera ONE provides a solution to the complexities and vulnerabilities faced by retailers, and has been deployed by many of the world's largest retailers. Cybera ONE is a secure application and networking solution that allows retailers to securely embrace public broadband services. Cybera ONE securely hosts retail applications locally on its embedded Linux server appliance or within the Cybera Secure CORE data centers. Cybera ONE can securely connect to the retailers' own corporate data centers and payment processors. Cybera ONE can cost effectively expand services through a common architecture that is fully managed. Cybera ONE also maintains an easy-to-use network logging database to identify any anomalies that occur on any retail store networks and alert IT personnel of any threshold or actionable event.

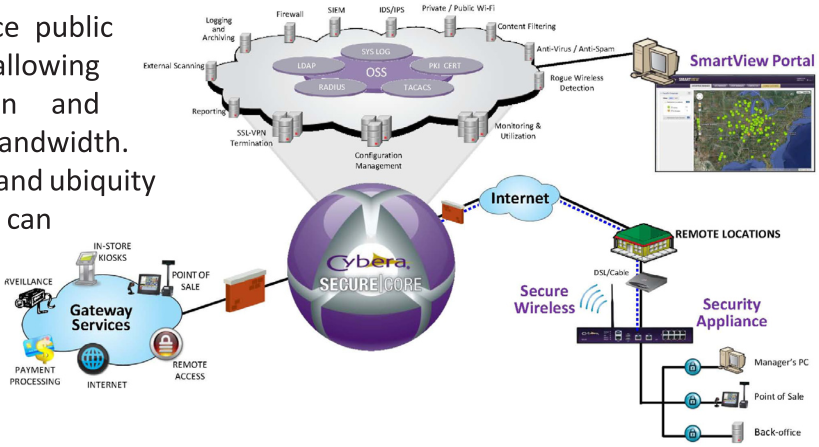
Cybera ONE is composed of five primary elements:

- Cybera ONE SCA-315 Appliance
- Cybera ONE Secure CORE & Cybera ONE Gateway Services
- Optimized Broadband Connectivity & Wireless Redundancy
- SmartView Network Management System
- Cybera Solutions Management Center

- **SCA-315 Secure Application Appliance** – Cybera's unique secure application appliance which serves as the primary site router, incorporates multiple other functionalities into a single manageable platform. The SCA-315 also enables Ethernet switch, VPN client, integrated 3G/4G back-up, integrated Wi-Fi HotSpot, and a secure Intel based Linux server. The SCA-315 does not use a public IP address, and maintains an overlay network that is completely independent of the local public IP address. The SCA-315 can be turned up behind any DSL modem, cable modem or Internet router depending on the type of connectivity to the site. The SCA-315 is a plug-and-play device that can be installed by store personnel and will automatically reach out to the Cybera Secure CORE and auto-configure itself. Applications can be securely hosted on the SCA-315's embedded Linux Server or broker with applications hosted in the Cybera Secure CORE or at a retailer's data center. Each port on the SCA-315 is a distinctly defined physical port that is hard coded to the specific application's use. This eliminates the ability to plug in an unauthorized device as it will not work.

  The SCA-315 also provides serial port conversion services enabling apps such as POS and Loyalty to be integrated securely and efficiently. The SCA-315 has an embedded dual band Wi-Fi server that can segment customer Wi-Fi services from closed corporate Wi-Fi services. The Cybera ONE SCA-315 is a single appliance that can consolidate multiple networking devices and servers into a single manageable device, reducing the complexity and vulnerability of your network.

- **Optimized Broadband Connectivity** – Cybera ONE allows the best broadband solution available at the site. The customer can select the highest speed, lowest price or best overall value broadband option, and Cybera ONE will work. Cybera ONE is bandwidth agnostic, allowing for the rightsizing of the broadband options for the site's needs. Retailers can securely embrace public broadband, allowing for optimization and expansion of bandwidth. The high speeds and ubiquity of broadband can eliminate the bandwidth bottleneck that stunts application deployment. The fact that the SCA-315 does not utilize a public IP address and is not locally accessible to hackers, keeps the retail network completely hidden from the public Internet, much like an MPLS network. The ability to securely embrace public broadband not only increases bandwidth, but it also reduces costs. These cost reductions typically provide a compelling return on investment (ROI) and actually saves the retailer money.



- **Cybera ONE Secure CORE** – The Cybera ONE Secure Core is based on an MPLS backbone connecting nationwide secure data centers which enable hosted security services such as firewall, intrusion detection, SEIM, event logging, VPN and content filtering. A variety of higher-memory footprint customer applications can be hosted in the secure core and securely made available to all sites in the customer network. This dramatically reduces site complexity, deployment costs and support complexity. Secure gateways to payment processors, POS vendors, ERP providers and other strategic partners facilitate an always-on secure connectivity for critical applications.

- **SmartView Network Manager** – Cybera ONE's SmartView network management application provides real-time status of all network connections and alerts retailers to critical events on its network. SmartView will proactively notify a retailer if its primary broadband goes down and when wireless back-up is engaged, and when it reverts back to the primary connectivity. SmartView maintains a log of all actions taken on a network and reviews logs everyday to maintain a record for verifying this aspect of PCI compliance. SmartView provides a list view or a map view of networks for easy drill down to specific sites.

- **Solutions Management Center** – Cybera's Solutions Management Center (SMC) provides 24x7 monitoring and management of our customers' networks. The SMC also supports the troubleshooting and repair of customers' network connectivity. Cybera ONE is a fully managed service helping to control the customer IT support staff costs. The Cybera SMC works with critical partners such as payment processors and POS vendors to troubleshoot the entire network, not just site connectivity.

The Internet VPN Versus Cybera ONE Business Case

The business case for comparing the alternatives of Outsourced Internet VPN or Cybera ONE with a 7 Mbps DSL solution requires a comparison of both the monthly recurring costs and the initial one-time costs.

Cost Element	Outsourced Internet VPN Cost	Cybera ONE Cost w/3G
Recurring Costs		
Primary DSL Circuit Cost	$129.95 - 5 Static IPs	$59.95 DHCP
Back-Up Circuit Cost	NA	$10.00 - 3G
VPN Configuration Change Cost	$57.00 Avg. per Month	$0.00
Basic Security Package Cost	NA	$24.95
POS Support App Cost	NA	$7.95
Wi-Fi Cost	NA	$7.95
Total Recurring Costs	**$186.50**	**$110.80**
Non-Recurring Costs		
Cybera ONE Appliance	NA	$450.00
Cisco 18xx	$1,100.00	NA
Cisco 53xx Switch	$1,200.00	NA
Cisco 1131AG Access Point	$600.00	$600.00
3G Wireless Cradle Point	$149.99	NA
Cisco IOS	$250.00	NA
Cisco SmartNet	$175.00	NA
Installation	$1,500.00	NA
Total Non-Recurring Costs	**$4,974.99**	**$1,050.00**

Savings Analysis

Cybera ONE Versus	Monthly Savings	% Savings	Upfront Savings	% Savings
Outsourced Internet VPN	($76.15)/Mo.	**41%**	($3,924.99)	**79%**

Summary

Cybera ONE provides a cost effective Internet VPN replacement solution as a fully managed service. Cybera ONE offers a unique security and application deployment architecture that provides a scalable and manageable methodology for large distributed retailers to grow their businesses. The Cybera ONE solution integrates multiple services into a single network appliance solution such as POS payment, POS support, Site-to-Site VPN, Wi-Fi and much more. Cybera ONE offers several compelling advantages over existing Internet VPN architectures, including:

- **Simplicity** – Cybera ONE consolidates multiple devices into a single secure application appliance that is easily installed and requires limited integration.
- **Cost Effectiveness** – Cybera ONE allows retailers to securely embrace public broadband to reduce network costs, operations costs and future deployment costs.
- **Security** – Cybera ONE provides a secure overlay network on top of public broadband connections that keeps the retail network invisible to hackers. Cybera ONE provides secure logs of all events on the network and notifies IT administrators of any priority actionable events.
- **Compliance** – Cybera ONE keeps your payment apps secure and provides automatic daily log review to demonstrate PCI compliance. Cybera ONE also supports other compliance requirements such as HIPPA, CIPA and EPA compliance.
- **Future Growth** – Cybera ONE provides a platform for future application expansion and is a cost effective and scalable architecture.

Simply put, Cybera ONE simplifies the complex task of deploying and operating a multi-site retail environment. Complexity is costly and vulnerable. Cybera ONE provides simplicity and cost savings.