



DEFENDING THE REMOTE OFFICE:  
WHICH VPN TECHNOLOGY IS BEST?  
AUGUST 2004

## DEFENDING THE REMOTE OFFICE: WHICH VPN TECHNOLOGY IS BEST?

### EXECUTIVE SUMMARY

Using the Internet to connect the distributed small- to mid-size enterprise presents unique challenges for business owners and their satellite offices. This paper presents three models for connecting remote workers and offices: client-based VPN software, a mixed vendor site-to-site VPN solution, and a single vendor solution with integrated firewall. Strengths and weaknesses are also presented for each.

Properly managed, the Internet is a productivity booster that allows workers to work where they're most efficient – whether it's around the globe or across town. There are numerous ways to build distributed networks. Best is an integrated architecture that allows secure remote installation, manageability, and troubleshooting, and can properly enforce your corporate security policy – all of which can save time and money over the long run.

### THREE MODELS FOR CONNECTING REMOTE SITES TO THE MAIN OFFICE NETWORK

The original idea behind a firewall was fairly simple – protect the boundary between a local area network and the Internet by restricting access. But as use of the Internet has grown, so have the number and diversity of threats to computers connected to the Internet.

Small- to mid-size companies, which typically don't have the resources for enterprise-grade network security, are especially vulnerable. If you add remote offices and telecommuter workstations to the mix, the potential for attacks to pass undetected throughout the small enterprise network increases dramatically.

To limit damage, firewalls have extended their protection to all users of the network – including those behind the firewall (at a main office, for example) and those outside it (remote workers). Virtual private network (VPN) solutions are especially attractive because they are designed to provide the security of a private, dedicated, leased-line network, without the cost of actually owning one.

VPNs use cryptography to scramble data so it's unreadable while traveling over the Internet, thus providing privacy over public lines. Companies with remote offices or telecommuters on the network commonly use VPNs to connect multiple locations.

The following table presents three models for connecting a remote site to a main office network, including typical strengths and weaknesses for each:

Model	Strengths	Weaknesses
<b>Client-based VPN software (Mobile User VPN or MUVPN)</b>	Inexpensive; can be used anywhere tunnel traffic is allowed.	No remote management or logging; remote system must be secured separately.
<b>Mixed vendor site-to-site VPN solution (IPSec-capable routers)</b>	Inexpensive initial acquisition; can use whatever is “at hand.” Many IPSec-capable routers come with some firewall capabilities.	More expensive to configure and manage; manual tunnel set up is required; logging isn’t uniform; troubleshooting problems requires integration of two dissimilar data sets.
<b>Single vendor solution with integrated firewall</b>	Less expensive to manage; integrated logging, reporting, and troubleshooting facilitated by common log format and timing; unified management interface/paradigm; added functionality, such as content filtering, is often available.	More expensive in initial acquisition, vendor products might not be available world wide.

**Table 1. Three models for connecting remote sites to the main office network.**

## QUESTIONS TO ASK WHEN CHOOSING A VPN SOLUTION

To understand the full cost and implications of owning and operating a VPN endpoint, you’ll need to consider all aspects of living with it. Not doing so may end up costing you more time, effort, energy, and cash outlay than you originally planned. Before deciding how best to connect your remote offices to your network, ask these questions:

- *Policy control.* Who’s at the other end of the tunnel? Are you comfortable giving them access to your entire trusted network, or do you need to restrict their access?
- *Troubleshooting.* How difficult is it to right things that go wrong on the remote end?
- *Logging.* Does the endpoint support common logging with your firewall/VPN gateway? If not, how are the logs synchronized?
- *Traffic segmentation.* If the VPN endpoint is someone’s home, can they separate business traffic from family traffic?
- *Authentication.* How do you know the traffic coming through the tunnel is from your employee and not his budding hacker teenager?

- *Total Cost of Ownership*. For this paper, TCO includes the cost of acquisition (how steep is the initial purchase price?), deployment (can the proposed solution install without an IPSec expert on the terminating end?), and maintenance (does the proposed solution offer remote management? How are software updates handled?).

## IMPLEMENTING A VPN SOLUTION

### **MOBILE USER VPN (MUVPN) CLIENTS**

The simplest of the three basic options, using individual MUVPN clients, gives the ultimate in flexibility, but at the cost of efficiency in remote management and troubleshooting. In this model, individual software clients running on the remote systems connect back to a central office VPN gateway. To the user of an MUVPN client, access to the corporate network is over the tunnel maintained by the client. Many clients can be configured so that ALL traffic goes through the tunnel. Since all of the remote network traffic goes back to the central office, enforcing a corporate security policy on that traffic is simplified.

#### **Policy Control**

MUVPN is typically either on or off: users at remote sites either get all of your network or none of it. While it's generally possible to configure more restrictive rules on the client for passing traffic, doing so and then maintaining those rules over time is fairly complex and can drive up maintenance costs. If it's required to control what type of traffic comes over the tunnel, consider other solutions.

#### **Troubleshooting**

The MUVPN client must survive in the hands of a non-technical colleague, so it's important to consider how your IT staff might fix it when it breaks. The client itself has no remote troubleshooting or management functionality. In order to troubleshoot problems, you'll have to use third party remote management software.

#### **Logging**

The VPN gateway and most MUVPN clients both log connection information. This is vital for troubleshooting. Insure that both systems can accept time correction from a common source and that the different log formats can be reconciled.

#### **Traffic Segmentation**

In most deployments, an MUVPN client handily segments office traffic from non-office traffic. All office traffic is encrypted and routed to the office. The non-office traffic isn't. Moreover, unlike the other two solutions, MUVPN clients can be used almost anywhere there is a connection to the Internet, such as in hotel rooms, internet cafés, and places where dial-up is the only access available.

#### **Authentication**

Most MUVPN clients provide strong authentication for all connections.

### **Total Cost of Ownership**

Acquiring MUVPN clients is easy. A few MUVPN client licenses typically come with your firewall. Additional client licenses can be purchased for as little as USD \$20 a seat.

Costs associated with initial deployment depend on how complex your roll-out plan is. You should budget a week to get comfortable with the configuration and troubleshooting procedures. Plan on spending 30 to 60 minutes with each client system for the actual installation.

No routine maintenance of the MUVPN client itself is required. Remember, though, that an MUVPN client secures nothing except the traffic in the tunnel. The client computer will need, minimally, anti-virus software and a personal firewall. Updates to either of these programs over time can impact the performance of the MUVPN client since they all use the same set of system resources. These interdependencies are one reason to resist using an MUVPN as a permanent solution to the remote office connectivity issue.

### **Summary**

If there are only a few people out of the office, or if a premium is placed on the ability to connect from anywhere, a handful of MUVPN clients might be an adequate solution.

### **THIRD PARTY IPSEC-CAPABLE FIREWALL/ROUTERS**

The mainstreaming of the Internet has led to a host of inexpensive and sometimes surprisingly functional firewall/ routers. Typically in the sub-\$100 dollar price band, these entry level devices offer basic functionality for both IPsec and firewall, but at the cost of ease of remote management, troubleshooting, logging, and content management. The low cost of acquisition is attractive and under certain circumstances can be complimented by low cost of ownership. In a typical architecture, a low cost firewall/router is connected to the main VPN gateway with a manually configured IPsec tunnel.

### **Policy Control**

Different routers offer different capabilities, depending on how much IPsec and firewall software is built in. Generally, policy controls are imposed at the main VPN termination point to reduce the complexity of the overall deployment. All tunnel traffic coming from a VPN endpoint to the firewall should be blocked at the firewall (even if the tunnel itself is open) unless exceptions are specified for individual services to permit that type of traffic.

### **Troubleshooting**

If the remote device *can* be managed securely from the corporate office, the IT department will have two different management interfaces presenting debug information in two different formats. Accurately interpreting the two together can be tricky. Success in doing this depends on how much time and effort is spent learning the peculiarities of the router and its interactions with your main gateway.

### **Logging**

IPsec-capable routers may or may not support traffic logging and may not have "debug" level logs available. If they do, your staff still must integrate information from two sets of logs. Since time synchronization is a key part of debugging IPsec problems, consider systems that will take time information from a common source.

Many devices will log information to syslog, the common format used by UNIX®. While syslog is neither secure nor reliable, it can be used for cross platform log aggregation. If the device doesn't support syslog, then IT must resort to manual synchronization of log data in two formats using two report mechanisms.

**Traffic Segmentation**

Few inexpensive IPSec-capable routers can divide their internal switch into two separate physical networks. Thus, there is no easy way to ensure that only business traffic goes out on the tunnel.

**Authentication**

Is the remote office really a remote worker's house? If so, ensure that ONLY the remote employee accesses the main office network via the tunnel. Most small IPSec-enabled routers don't provide user authentication before granting tunnel access.

**Total Cost of Ownership**

Most retail computer stores sell IPSec-capable routers for about USD \$100. Initial deployment is time consuming, but tends to go more smoothly if employees on both ends of the tunnel are knowledgeable about IPSec. If not, ensure that reliable remote management and troubleshooting capabilities (not dependent on the router itself) are available. If possible, pre-configure the third party device before sending it to the remote location.

It usually costs more in maintenance cycles to have a mix of brands in a network than to standardize on a single vendor and management system. Each software update to one of the devices could bring the change that requires tunnel settings to be rebuilt and tested – a tedious task without meaningful remote management.

**Summary**

Under certain controlled circumstances with experienced administrators available at both ends of the tunnel, IPSec VPN networks built with IPSec-capable firewall/routers can work. But expect higher administrative overhead and support cost surprises.

***SINGLE VENDOR SOLUTION***

The difference between a single and multi-vendor solution for remote and branch offices boils down to manageability. Products from a single vendor are generally made to work together, typically use a common log format, can take advantage of tighter IPSec integration and special tunnel management tools, and incur lower maintenance costs due to common or similar management interfaces.

**Policy Control**

Single vendor firewall/VPN networks are typically designed to work together. This is demonstrated best by special global management and VPN configuration tools. As with the IPSec-capable routers, egress of traffic from the tunnel is typically managed by the VPN gateway at the corporate office, centralizing control and simplifying management.

**Troubleshooting**

Devices from a single vendor typically have a common management suite, terminology, log format, etc. These strong family resemblances assist in debugging the issues that inevitably arise.

**Logging**

If the vendor has implemented a custom log format to overcome the lack of reliability and confidentiality inherent in syslog, both devices typically support this custom log format assisting in troubleshooting.

### Traffic Segmentation

More sophisticated remote office devices offer separate physical segments for a home and office network. In the case of the remote office actually being the basement of the employee's house, the family's traffic is kept on one network segment; the other segment is used only for office work. Thus, a virus on the home system can't infect the office via the tunnel.

### Authentication

More sophisticated remote office devices authenticate individuals before allowing them access to either the Internet or a tunnel. This is particularly useful for wireless network segments in an un-trusted environment. Since many wireless networks are easy to tap into, the ability to authenticate the person sending the traffic is crucial.

### Total Cost of Ownership

Initial acquisition of a single vendor network is typically more expensive than choosing the lowest-priced device. In most cases, however, this is more than made up for in lower labor costs for maintenance, deployment and management.

Deploying single vendor networks means that administrators can make full use of specialized tools and capabilities designed to speed network roll outs and improve reliability. To promote ease of maintenance, more sophisticated devices include robust support for secure remote management, remote installation of new software, and remote logging.

### Summary

Despite the higher initial cost, an integrated single vendor solution generally provides the best reliability, management, and lowest total cost of ownership. Better, more sophisticated product lines have numerous features to make it even easier and typically less expensive overall to configure, manage, and support.

## FIREBOX® X EDGE SECURES SMALL BUSINESS NETWORKS

WatchGuard® Technologies' Firebox® X Edge is a line of model-upgradeable integrated firewalls that can be used as a standalone appliance or as VPN endpoints. Designed specifically for small businesses, Firebox X Edge secures small business networks, remote offices, and telecommuter workstations. It's also easy to manage, even for businesses with limited in-house networking experience.

Firebox X Edge provides the following benefits:

- **“Plug-and-play” setup:** Intuitive Web-based user interface and quick-start wizards make it easy to set up and configure.
- **Fastest performance in its class:** Designed to support all network traffic without degrading network performance.
- **10 Ethernet ports:** Connects users to networked devices, including printers, fax machines, and servers, quickly and easily.

## DEFENDING THE REMOTE OFFICE: WHICH VPN TECHNOLOGY IS BEST?

- **Dynamic stateful packet inspection:** Delivers commercial-grade security that protects your business and networks.
- **Virtual Private Networking (VPN):** Extends a secure tunnel from Firebox X Edge to safely connect telecommuters and remote offices.
- **Managed desktop anti-virus:** Provides centrally managed desktop protection against known viruses, web attacks, and e-mail intrusions.
- **WAN failover:** Enables a second Internet connection if the primary connection or provider fails.

### SUMMARY

The three types of endpoints discussed in this paper all have their place. For most deployments where the endpoint is stationary, the single vendor approach offers considerable advantages at a modest increase in up-front costs.

Much of the integrity of your core systems and the productivity of your employees depends on how well you secure your remote offices and how efficiently that remote connection is managed. When deciding what sort of VPN network you'll deploy, remember that your IT staff will be responsible for maintaining it and fixing it – in addition to all that they currently do. Tunnel problems tend to erupt with a poor sense of timing. As you design your tunnel network, optimize it for stability and ease of maintenance.

For more information about WatchGuard security solutions, visit us at [www.watchguard.com](http://www.watchguard.com), or contact your reseller.

---

#### ADDRESS:

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

#### WEB:

[www.watchguard.com](http://www.watchguard.com)

#### E-MAIL:

[information@watchguard.com](mailto:information@watchguard.com)

#### U.S. SALES:

+1.800.734.9905

#### INTERNATIONAL SALES:

+1.206.521.8340

#### FAX:

+1.206.521.8342

#### ABOUT WATCHGUARD

WatchGuard network security solutions provide small- to mid-sized enterprises worldwide with effective, affordable network protection. Our Firebox line of extendable, integrated security appliances is designed to be fully upgradeable as an organization grows, and to deliver the industry's best combination of security, performance, intuitive interface, and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently, and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of security with vulnerability alerts, software updates, expert security instruction, and superior customer care.

#### FOR MORE INFORMATION

Please visit us on the Web at [www.watchguard.com](http://www.watchguard.com) or contact your reseller for more information.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis.

©2004 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, and Firebox are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners.

Part No. WGCE66123\_0804