

## Branch Office Security: Triple Threat Protection

Recent advances in multi-function security switches offer streamlined security models for branch and remote offices (BROs). Hub and spoke architectures in which BROs tunnel all traffic back through headquarters are being replaced with modified architectures in which the BRO offers highly secure direct connectivity to the Internet while continuing to maintain VPN connections to corporate application resources at headquarters. In addition to offering secure tunnels and faster and more secure browsing, the new model increases dramatically the level of internal BRO security through segmented security zones and per-segment security policy application. Because this can be accomplished with a single or paired security switch the result is a safer and simpler BRO security model that is also more cost effective than existing models.

### A Quick Overview of the Problem

Most BRO security architectures are the result of a security appliance, usually a firewall/VPN device, “stapled” onto the side of a network. The network architecture is built to deliver traffic efficiently inside the BRO and consists of the minimum number of access layer switches required. This network connects back to headquarters via a VPN that may or may not be coupled with a firewall. Thus, traffic inside the branch office stays local and fast while traffic back to headquarters operates across one or several full or fractional T1/T3 lines (connected through a Frame Relay network or through an IP/VPN across the Internet).

But the model has problems.

First, “backhauled” connections create inherent slowdowns and unacceptable latencies especially at those times when end users are most aware of them. The reason for this is that BRO-HQ traffic spikes at certain obvious times such as the morning email rush, the mid-morning and early afternoon web surfing rush, and the end of the financial quarter when everything is due. Multi-homed connections to the Internet protected only by a firewall solve the speed problem but introduce a myriad of Port 80 security threats.

Second, and more seriously, the dramatic rise in security breaches has rendered the BRO network architecture itself vulnerable. Worms that travel in on laptops do as much or more damage in a BRO as they do at headquarters. This is because the IT staff on site is less trained in security topics and less capable of both preventing and controlling security threats. Thus, a network architecture that simply “delivers bits fast” is also a network that “delivers attacks fast.” Existing BRO security appliances don’t solve the problem because their designs assume a slow T1-T3 Internet connection and not multiple 100Mbps segments. The asymmetrical requirements of WAN and LAN are lost in these older “one speed fits all” models.

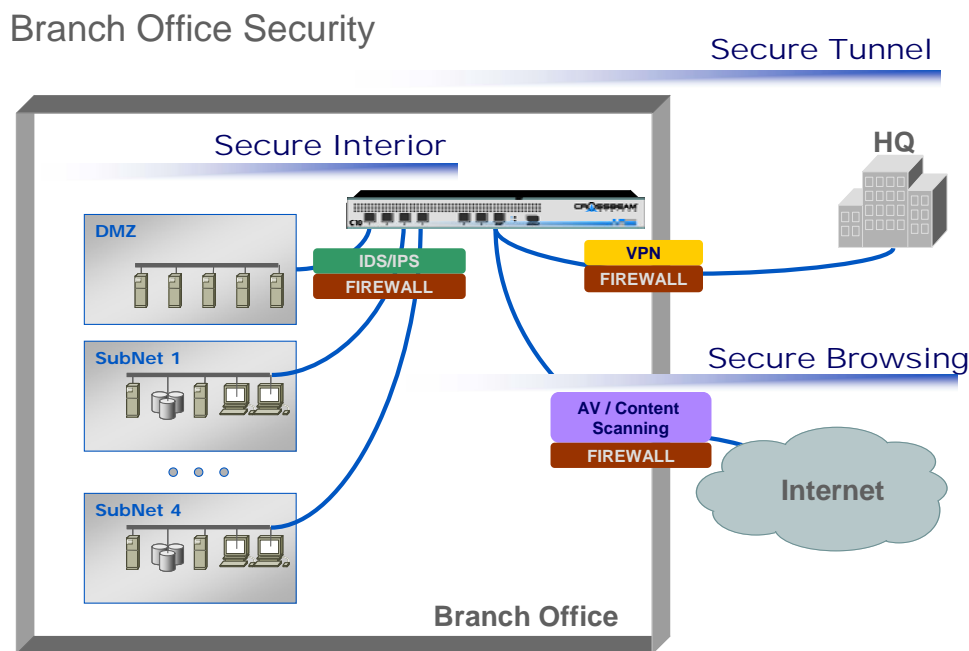
These problems, while distinct and separate in principle, find an integrated resolution in the deployment of multi-function security switches such as those built by Crossbeam Systems.

## The New BRO Secure Network Architecture

The three key requirements of the new BRO security model can be summarized as follows:

1. Provide fast and secure site-to-site VPN from BRO to headquarters
2. Provide fast and secure Internet usage (primarily browsing and FTP) directly from the BRO
3. Increase the interior BRO security posture for worm prevention

Crossbeam C-Series security switches provide both the speed, security and multiple functions required by these criteria. The overall solution is best described by the diagram below:



In the diagram, the large enclosing frame represents the branch office (note: for simplicity's sake, the WAN router has been omitted from the diagram). Internally, the branch office consists of one to several subnets. Each of these is fed into the security switch, in this case a Crossbeam C10. Because each of the C10 ports supports 10/100/1000 connections, the BRO internal LAN can be upgraded to gigabit Ethernet at any time without equipment swap. The C10 firewalls each of the LAN segments from each other so that PCs on one segment may not attack PCs on other segments. The security switch then connects out to headquarters via a combination of firewall and site-to-site VPN. The switch also provides the dual functions of firewall and content scanning for the direct BRO-to-Internet connection.

Notice how simply the single security switch solves both the performance and security requirements of both the internal and external connections. On the LAN side, the C10 offers two gigabit throughput so that end users don't experience delays often associated with security boxes. Why gigabit speeds? Because even multiple 10/100 segments at

peak utilization can put tremendous strain on the processing resources of a security device. On the WAN side, where speeds typically range from 1.5Mbps to 45Mbps security performance becomes much less of an issue. However, now the raw connection to HQ itself becomes a bottleneck when all traffic is backhauled to the HQ network. To remedy this situation, companies can move all Internet browsing back to the BRO. The reason is that the Crossbeam security switch offers secure high speed browsing without speed bottlenecks (again, usually associated with security devices). Furthermore, no proxy management is required to accomplish this task since Crossbeam uses a transparent proxy solution based on Aladdin eSafe.

An important feature of the security switch in all three scenarios – internal, VPN, Internet – is that security policies can be pushed from a central HQ administrative group. There is no need to visit the device onsite for management upgrades. In addition, Crossbeam offers seamless patch and upgrade management via its SecureShore management platform.

## **Conclusion**

Security switches offer a safe and simple solution to the performance/security tradeoff that security and network teams everywhere are facing. By delivering services on a per-segment basis with speeds matching both LAN and WAN requirements, the security services switch provides a real investment with lower total cost of ownership, higher security and satisfied end users.