Lippis Report

White Paper

# Network Security 2.0

## Deploying Teleworking Solutions in Scale: Part 2

Issue 5

by

Nicholas John Lippis III
President, Lippis Consulting

October 2008

## Deploying Teleworking Solutions in Scale

In Part One of Deploying Teleworking Solutions in Scale we discussed business and IT problems plus the benefits of teleworking. Here we provide business and IT leaders with an architectural view of today's teleworking solutions that scale to home and small office environments. These environments may be home workers, call center agents working from home, small branch offices equipped with a few people, small retailers, etc.

**American Century Investments Invests In Cisco Virtual Office Solution**

Listen to the Podcast

Today's teleworker solutions provide many benefits as described in Part One of our series. But teleworking solutions are becoming more realistic in order to accommodate all users of home internet connections such as family sharing of broadband internet services through the use of split tunnels. A split tunnel allows family members to directly access the Internet and not the corporate IT infrastructure separating work and family.

Another teleworking use is for small branch offices. For example, a food services industry restaurant such as those distributing at sports stadiums or airports, or a small retail outlet are perfect for teleworking solutions. Their use profile may be different than the home worker, as small branch office sites may need to support more than one user, or may not need mission-critical voice or video applications or perhaps might require an inventory back-up link. Today's teleworking solutions can support these use cases too.

For example, the distributed call center agent model is very popular today as it taps into a previously inaccessible labor pool – work at home parents. Many airlines equip their ticketing agents with teleworking solutions so they may work from home, reducing commercial real estate office expense, increasing hours of coverage, etc. In short they are able to deliver a better service at a lower operational cost.

But while the small office and special use cases are interesting, the major teleworking market is to create a virtual office at home. Many IT leaders are asking how to scale their IT resources, especially the movement to home working. In short, IT leaders want to be assured that their deployment performs effectively and their teleworking solution scales. Further, IT leaders seek to receive the ultimate long-term return of investment promised during acquisition. To achieve these goals, the teleworking solution needs to incorporate these architecture components and attributes.

**Cisco Virtual Office Deployment Guide**

Get the Case Study

### Three Architectural Components

For any teleworker solution that scales there are three basic components. First is the remote site or teleworking solution. This is and should be simple, a small router loaded with services such as WLAN, security, UC, etc., and an IP phone, typically. Second and most important for scale is the head end. The head end includes VPN routers for aggregation and also a series of management servers that provide a diverse set of functions, including policy definition, automated configuration management plus identity controls. One head end footprint should support thousands of teleworkers to deliver scale. This centralization of complexity and ability to scale delivers a recurring return on investment as a single head end footprint can scale without the need for new equipment when new teleworkers are added to the network. The third component is a professional service offering that assists IT management with envision, design, deployment and management/monitoring/optimizing of the teleworking service.

We offer a teleworking architectural view from an attributes perspective to help guide business and IT leaders as they consider options. We are impressed with Cisco's new Cisco Virtual Office (CVO) and many of the attributes

below can be found in that offering. What makes CVO different from previous teleworking offerings is the level of service integration including mobility, unified communications, management and security in the teleworking equipment. It's the layering of security into the teleworker environment that makes executives comfortable that they're not opening up back doors surrounding their organization. But perhaps most important is its ability to scale which makes it perfect for large enterprise organizations, multi-nationals and global operations.

**Multiple Security Technologies**

Security is the number one concern of business leaders when considering large-scale teleworking solutions. The concern is wrapped up in compliance, threat management, policy and control initiatives and requirements. To address these security issues and concerns the teleworking solution needs multiple levels of security technology distributed between head end and teleworking network device, i.e., a router with multiple security services embedded.

The router needs to support a wide range of security technologies for voice, video and data. Security technologies such as identity-based authentication, firewall, content filtering, intrusion prevention, content filtering, WLAN authentication, automated public key infrastructure (PKI), SDP, AAA, 802.1x, worm and virus protection and hacker lockout. The scenarios are relatively simple; if the device is compromised, lock it out from the corporate network and mitigate virus and worms from propagating into the corporate network. Ensure identity of device and user before access is allowed. Ensure that router configuration changes are not done at the home office thanks to PKI and if changes are made, the device is locked out. Control and distribute policy and configuration changes at the head end to all teleworking routers. Further, voice sessions should be isolated via their own VLAN. Hardware encryption is important too, to keep communication secure without paying a performance penalty.

**The Ability To Scale Without Additional Operational Spend**

Solving a teleworking problem that includes 20 home offices versus an organization that wishes to provide 40% of their 100,000 employees with home offices are different problems with different scale dimensions. 40,000 teleworkers is a large population and IT may not be ready to deploy a system that large in short order, but they need to know that the solution that they deploy today can scale to accommodate their requirements. In addition IT needs to know that they will be able to manage such a highly distributed and pervasive remote access solution. One of the largest teleworking deployments is at Cisco Systems, which includes some 13,000 teleworkers, which is growing at 1,000 new teleworkers per month until it reaches a projected 30,000. Cisco IT operates on a very tight budget and this solution has let them keep their headcount constant while growing at 8% per month.

It's the management tools at the head end that delivers scale without adding operational expense. One of the most unique features assisting scale without additional operational spend is zero-touch deployment. Automating the provisioning process of initial configuration and deployment of teleworking devices scales IT resources. In addition ongoing maintenance is eased too as new software images or configurations are pushed to remote teleworking devices in bulk versus one at a time. Imagine how difficult this would be if IT depended on some 5,000 teleworkers to initiate this process versus IT initiating an automatic push from the centralized IT head end.



**IT Management**

The management of the head end and teleworking device is the technology that enables scale with minimal operational expense. The ability to configure and develop polices which are pushed to teleworking devices minimizes operational spend and removes this task from home office workers yielding a zero-touch deployment and management model. Look for a policy server to control teleworking devices. A server that performs device provisioning securely plus authenticates and registers new devices as they communicate to the head end is favorable. A configuration engine for teleworking devices to pull policy updates, software updates, configuration changes, etc., simplifies patch management operations. A certificate authority server that automates much of the

process associated with pre-shared keys restricting management access to teleworking devices and an AAA server for authentication, authorization and access of profiles ensures system security.

**VPN Support**

At the head end multiple VPNs need to be accommodated. There are layer 3 VPNs for high availability applications, a dedicated “always on” session for voice, video and QoS tunnels plus on-demand tunnels with the ability to create full meshes between teleworker sites. This is an important attribute as traditionally inter-teleworking communications traversed from teleworker-to-head end-to-teleworker. Now direct tunnels between teleworkers can be established increasing application performance such as video conferencing while reducing the load on the head end for this form of traffic, increasing performance for all teleworkers.

In addition to the above user application VPN tunnels, management tunnels are needed too. For example, a VPN for policy push with integrated firewalling plus IPsec client interoperability provides direct access between teleworking router and head end for security and management. An SSL VPN at layer 7 for behavior-based end-point protection and full-tunnel client download provides additional security. A layer 2/3 VPN for mobile end-points such as iPhones and dual-mode phones enables model end-points to share the teleworking solution. With support for multiple VPNs at the head end and teleworking sites, business resiliency or continuity is ensured, as there are multiple connectivity options to leverage in the case of a man-made or natural disaster.



**Advanced Network Services**

We mentioned above that teleworking devices are being equipped with advanced network services such as security, routing, switching, WLANs, unified communications, etc. While these are powerful network services, look for application optimization too which increases application performance over broadband links. Enabling QoS technologies should be built within teleworking devices to ensure an excellent voice and video experience while prioritizing mission-critical traffic. QoS plays an important role in teleworking environments where family members share a single broadband connection. QoS prioritizes phone and business traffic, which may be flowing over the wireless network while youngsters download content or play internet-based games on Ethernet attached devices.

The value proposition of electronic communications has always been to allow people to communicate over distance. Modern corporate communications is not only a mandatory requirement for corporations to conduct business but with advances in teleworking solutions, communications is now a major contributor to green initiatives too. Teleworking initiatives have a unique set of business attributes such as reducing real estate requirements, increasing labor pool access, improved employee lifestyle options, plus enabling greater employee productivity. Never before have there been so many motivating factors favoring teleworking, including high energy cost, government initiatives, business benefits, collaboration/social networking and green initiatives. Advanced teleworking technology is now being packaged to allow business and IT leaders to develop and deploy massive teleworking initiatives. The architectural approach above can help IT leaders deploy teleworking in scale while achieving the goals outlined above.