A Core Competence White Paper Prepared for

Residential Broadband Access and the Teleworker: Security Considerations for the IT Manager

David M. Piscitello

Background

The teleworker¾the employee who performs a portion of his or her work duties from a residence¾may be the fastest growing part of the corporate work force. For some enterprises, connectivity needs for the majority of its teleworkers may be accommodated using the same technology and security measures used for roaming and remote access. For others, the emergence of **residential broadband services** offers new opportunities for extending the corporate LAN to the residence-based employee. The high bandwidth, low latency, and "always connected" characteristics of services based on **Digital Subscriber Line** (DSL) or **cable modem** technologies allow teleworkers access to corporate LANs using NOS (Network Operating System) file, session, and printer services, including AppleTalk, Microsoft Network, and UNIX/NFS/X. These NOS services are generally impractical to use over traditional dialup services because of dialup's low bandwidth, high latency, and intermittent connectivity. Residential broadband services thus allow a qualitative difference in teleworker activities compared to dialup services, by enabling teleworkers to use the corporate network at home in the same way they do at the office.

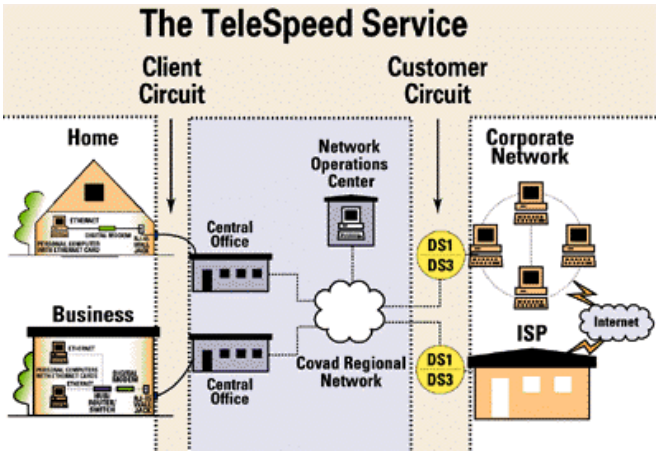
The characteristics of residential broadband services are similar to public, switched data services such as Frame Relay and SMDS, with one noteworthy exception. Most Frame Relay and SMDS connections terminate at remote offices or corporate locations, where some site security policy is typically enforced: employee identification is required, connectivity to the public Internet is restricted and protected by corporate firewalls, etc. Residential broadband service, as the name implies, usually terminates in the home of a corporate teleworker. Because of this difference, the characteristics that make residential broadband service attractive may also raise security concerns for some IT managers.

Why is residential broadband access to a corporate network so different from modem and ISDN dial access from a residence or hotel? Why are some IT managers cautious about bringing DSL or cable modem services into their enterprise? Are there ways to safely integrate residential broadband into an enterprise network? Is one residential broadband technology safer than the rest? Let's take a closer look.

Residential Broadband Services: Digital Subscriber Line & Cable Modem

Digital Subscriber Line (DSL) technology is used to provide layer two (data link layer) access services. There are many different variants of DSL technologies. Covad Communications Company's TeleSpeed^{SM} service is offered using **IDSL, ADSL**, and **SDSL**. The TeleSpeed^{SM} service shares many characteristics with Frame Relay. Both are point-to-point, based on **permanent virtual circuits (PVCs)**. A PVC is conceptually just a bidirectional pipe between two systems; data that is placed in one end of the PVC comes out the other end unmodified. Customers can use any network protocol (AppleTalk, IP, IPX, etc.) over a PVC. PVCs transport data without examination; this means that the data can be encrypted, compressed, or otherwise transformed in ways agreeable to the systems using the PVC, without affecting the PVC itself.

Covad's TeleSpeed[SM] service uses PVCs that originate at the teleworker's residence as a DSL circuit operating over a copper twisted pair. This copper pair is connected to Covad equipment in physically secured Covad facilities in the teleworker's serving Central Office. The PVC is relayed over the Covad Regional Network, and then onto a dedicated circuit to the customer's enterprise network (see figure 1).



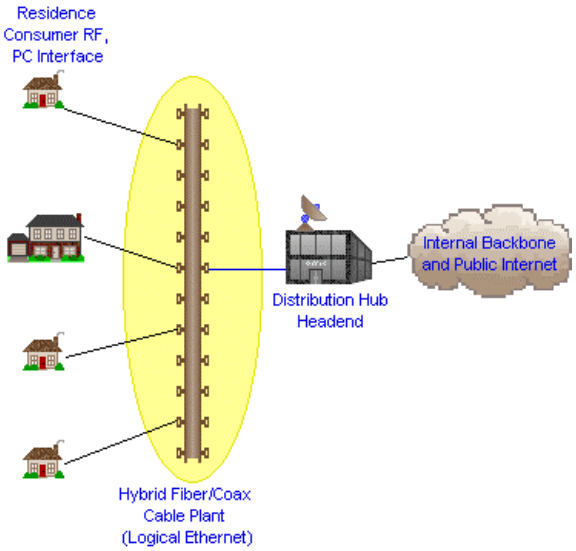
If your enterprise has already completed a risk assessment for Frame Relay, the **security measures deemed appropriate for Frame Relay transport can probably be applied to DSL-based services**. For example, if your enterprise uses encryption over Frame Relay links, you can do so over TeleSpeed service links as well. This is true for many configuration and management issues as well. Covad is an alternative public data service provider. The same **third party trust model** that companies understand and accept when dealing with other telephone and Frame Relay providers applies to Covad as well. Basically, everything related to customer service is done at customer request. Covad sets up new PVCs only when the customer submits an authorized service order. Furthermore, Covad setting up a new PVC is not enough to create a new connection into the customer's network; the customer also has to set up their own router or switch to handle the PVC. Like telephony providers, Covad facilities are physically secured, and only authorized Covad personnel monitor and administer Covad's equipment.

Cable modem technology offers another method for providing residential broadband services. Cable modems use two radio frequency carrier signals ("channels") from the CATV spectrum to provide high-bandwidth, low latency **shared** access service to residential customers. Cable modem operates a layer two service over a hybrid fiber-coax plant that passes residences in neighborhood to reach a cable company's central office for relay to a distribution hub (the "headend"). Cable companies often collaborate with (or franchise services from) public Internet Service Providers for layer three (i.e., IP) service. Service offerings of this kind are best compared against Covad's Small Business Internet Access service.

Whereas the DSL-based services offered by Covad are point-to-point services, services based on cable modems are multi-point services. Cable modem service is similar to LAN service provided by shared-media (i.e., traditional, non-switched) Ethernet. In security terms, shared-media Ethernet and cable modem systems (in the most common deployment configuration) are **promiscuous media**: all stations sharing the same media can read frames transmitted over the media, and can write frames to the media.

Unlike PVC-based services, shared media services rely on stations to honestly identify themselves when transmitting data. Passive monitoring, forgery, and denial of service attacks are thus all greater risks with cable modem services than with DSL services.

When using cable modem services, data encryption is often warranted to assure message privacy and integrity; this adds complexity and expense, and can impact performance.



Residential Broadband Services and Security

Characteristics that residential broadband services share that may be associated with security risk are:

1. The residence is not a physically secured premises, at least not in the same way as other corporate facilities.
2. The residence has an "always connected" link to the enterprise network.
3. The connection from residence to the enterprise network is a high speed link.

The first and second concerns are related, and are problems common to all communications services used by teleworker and roaming employees who access corporate information resources remotely. Regardless of whether it is via analog modem, ISDN, or dialup bridge/router access, connectivity is typically automated. Because of this automated connectivity, the physical security of a teleworker's premises should be a concern for the IT manager regardless of whether access to the enterprise is achieved using on-demand or always-connected services.

For example, is DSL service a greater risk than remote LAN access using dialup ISDN service because DSL is "always connected", given that ISDN router automatic dial-on-demand features are generally used by teleworkers? The answer, of course, depends on other factors, including the security measures in place at the corporate network and at the host computer(s) in the teleworker's residence; if all other factors are equal, the answer is usually "no, always-connected DSL service is no greater risk than automatic dial-on-demand ISDN service". In many ways, in fact, always-connected DSL may be a *lesser* risk, because it can only be used from a single premises; dial-on-demand ISDN can be accessed from any ISDN-connected site anywhere in the world.

The third concern (that the connection from residence to the enterprise network is a high speed link) often proves to be the most troubling, especially in the case of remote or teleworker access to corporate servers. When corporate security is evaluated, the speed of a link is a weighting factor in determining risk. Simply put, if a low–speed link is compromised, information could be leaked from the enterprise network, but not nearly as fast as if a high speed link is compromised. The rate at which a motivated intruder can access or collect sensitive information from a corporate server is more worrisome than whether the intruder is dialing in or is using facilities from a physically unsecured premises.

Let's examine several scenarios where these characteristics become issues for the IT manager and consider how they might be addressed. How an organization addresses security in these scenarios is greatly influenced by the perceived and real risks to corporate resources, the organization's financial and technological abilities to reduce or mitigate these risks, and the ability of an organization to implement and enforce security measures chosen.

Scenario #1: The teleworker operates systems that do not fall under the purview of corporate desktop administration.

By definition, teleworkers work outside the physically secured workplace. The IT manager may have little control over equipment at the teleworker's residence. The teleworker who runs unauthorized services (e.g., a web, file, or mail server) and unapproved software may create vulnerabilities and compromise a secure perimeter established for an enterprise network. Network anti-virus and intrusion detection measures can be circumvented, and mail distribution, name resolution, or enterprise routing could be disrupted. Whether the result of accidental misconfiguration or malicious attack, activities initiated over the residential connection can interfere with or deny service to fellow corporate workers.

Recommended Policy and best practices for Desktop Security

It's easy to get caught up with concern over theft or modification of data transported over a network and overlook the more mundane issue of protecting stored information. Information isn't any less sensitive because it's recorded on a removable medium (a Jazz drive) or hard disk of a laptop than if it's electronically. A security policy for both teleworker and mobile employee should consider:

a) **Desktop authentication**. This can be as simple as requiring that all PCs, irrespective of location, use login and screen saver passwords for with a small idle timeout. It can also be a sophisticated as requiring a security token, key or card to access a PC or a removable medium. Cylink Corporation offers products that require a physical token and password to access a PC. If you are interested in authentication based on biometrics, NEC and others offer affordable fingerprint recognition systems.

b) **Anti-virus utilities.** Teleworker PCs should run anti-virus software to prevent the spread of email-borne viruses from the residential PC into enterprise networks. This is probably consistent with your corporate desktop security, but it's especially important if your network relies on network antivirus measures at your secure perimeter. MacAfee, Symantec, IBM corporation, and several others offer fine antivirus products.

c) **Secure file storage, stored file encryption**. There are a number of easy and effective applications for encrypting files stored on PCs and removable media. Often, the same application provides file deletion that prevents recovery ("electronic shredding"). Pretty Good Privacy, Entrust Solo, and EMD Worldwide's Encryptor can be used for secure file storage and secure electronic mail. RSA SecurPC from Security Dynamics Technologies, EMD Worldwide, Software Shelf International and Symantec offer products that are aimed at protecting enterprises from the loss or compromise of sensitive information resulting from the theft of laptops, and these alternatives are appropriate for teleworker PCs as well.

A good review of stored file encryption applications for Windows95 systems can be found at Network Computing Magazine, and several good white papers on these subjects can be found at Security Dynamics and Symantec.

d) **Desktop file security, access controls**. File (folder) sharing on Windows95 is simple to use, but too often ignored. Insist that teleworkers assign passwords to network users, and discourage them from allowing full access privileges to entire disks and partitions. Consider a centrally administered user-level access control list for network domains that include teleworker PCs. Use third party products, e.g., EMD Armor 97, that offer advanced access control features for Windows95. For increased file security, consider Windows NT, which has a Win95 look-and-feel, but its file system (NTFS) ACLs can be used to assign user permissions to files, directories, or other secured objects (devices, ports), and so offers more effective and granular access controls.

One way to motivate any worker to take file security seriously is to explain that personal or sensitive information stored on a PC in a residence or on a corporate LAN could easily be viewed by ***anyone*** in the corporation who sees that PC through Microsoft's Network Neighborhood.

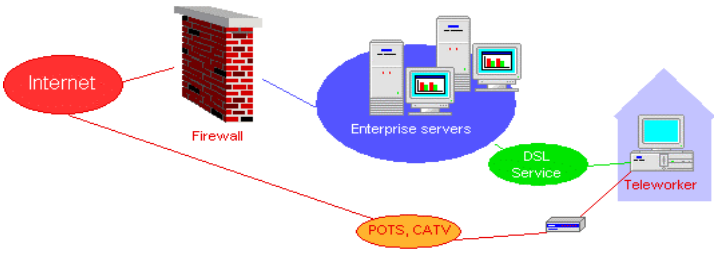
e) **Unauthorized services**. Consider a security policy that expressly prohibits services operating on desktop PCs that can expose the corporate network to attacks. It is not uncommon for IT managers to expressly prohibit FTP server applications, or nominally, prohibit anonymous FTP access from operating on all desktop PCs, including teleworker PCs. Web hosting applications present a number of security issues when operated on desktop PCs. Entire file systems can be browsed if file permissions on a web server are not appropriately set, and the IT manager cannot exercise adequate control over the features, CGI scripts and services operated, nor can he or she control the use applets and downloadable programs.

The IT manager may wish to prohibit the operation of mail, telnet, tftp, route, and domain name servers on teleworker LANs. Consider blocking or **filtering** of routing protocol updates, name server announcements, and SMTP messages used between mail transfer agents emanating from a teleworker connection. Note that this is only a partial list of servers that may be inappropriate for operation from an uncontrolled desktop.

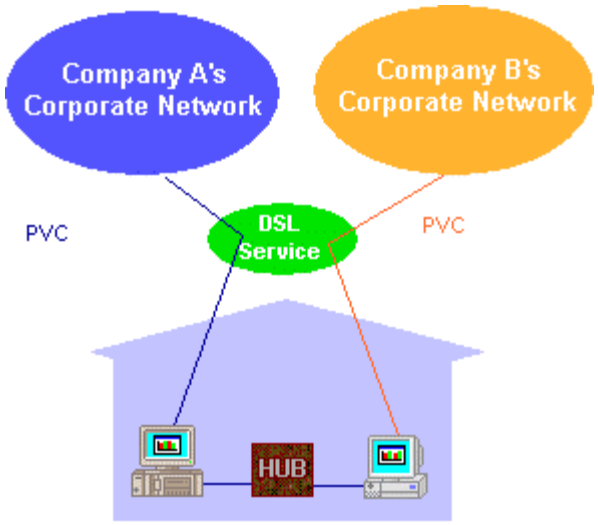
Scenario #2: The teleworker's residence has multiple physical connections.

Depending on how residential broadband services are terminated at the corporate network, a second connection in the teleworker's residence can provide an unprotected access or **backdoor** into the corporation. There are several ways multiple physical connections can be introduced:

· The teleworker has a PC with a modem, incoming calls are accepted by the modem, and software operating on the PC (e.g., PC Anywhere, Netopia Virtual Office, UNIX shell, telnet) is compromised to allow an outsider to gain control of the PC. An extreme case of this configuration is one in which the teleworker has a second LAN NIC and uses this to connect to the public Internet via the DSL or cable modem.



- The teleworker of Company A operates a PC LAN at his or her residence, and a second system, for example, a house partner's host or router, is connected to both the PC LAN and the public Internet. In this scenario, anyone who gains access to the house partner's PC may also gain unauthorized access to Company A. An extreme case of this scenario is where Company A's teleworker and a housemate share a PC LAN in the residence, and where the housemate has a separate Internet connection, or a connection to the housemate's corporate network (Company B).



Recommended Policy and Best Practices for Multiple Connections to the Residence

The most commonly encountered second or alternative connection a teleworker may have is an analog modem or ISDN Terminal Adapter on the teleworker's PC. An IT manager can expressly prohibit modems and TA's, but a less stringent but more readily enforceable alternative is to prohibit incoming (data) calls.

Even with incoming call handling disabled, and with a security policy that prohibits server operation from a desktop (including routing services, e.g., UNIX gated, NT R&RAS), the IT manager must consider the security implications of client applications, especially web browsers. Executable programs carried over an HTTP stream are especially dangerous in those situations where a teleworker has multiple connections, because the teleworker may unknowingly download active content using a web browser. The downloaded executable might contain code designed to circumvent firewall or web proxy defenses and provide an intruder with access from the outside. It may contain a virus, or other undesirable software and this could be propagated onto the corporate network. One security measure to consider is to require that teleworkers disable the download of active content (e.g., Java, ActiveX) to browsers, or require that they utilize anti-virus software to filter it out. Disabling active content should include disabling download of executables and archive files containing executables. Seemingly harmless applications can contain "easter eggs" or other suspicious code. A better long-term policy and practice is to implement strong public-key based authentication between servers and clients (see the section entitled "Universal Precautions").

Local area networks in the teleworker's residence can pose additional security problems. Covad TeleSpeed service is commonly offered through a two port router or bridge. One port is connected to the DSL service, and another to the Ethernet segment to which the teleworker's PC(s) and perhaps printers are connected. Ethernet is commonly implemented in a residence using inexpensive hub technology. Unauthorized equipment attached to the hub can be used to gain access to the corporate LAN through the DSL router or bridge.

We have mentioned how LANs shared between housemates are yet another form of multiple, unsecured connections in a residence (see "Residential Broadband Access and Security"). There are several ways to address this problem as a matter of policy or practice:

1. Do not permit the use of shared hubs, instead **use Ethernet crossover cabling** between the DSL router and the teleworker's PC. This limits systems at the residence with DSL access to the router and the teleworker's PC.

2. **Use managed hubs**, port switching hubs, or workgroup Ethernet switches at the teleworker's residence. Disable all but the authorized number of Ethernet ports on the hub using administrative controls only accessible to authorized IT staff. SNMP-manage the hubs and enable traps so that unauthorized attempts to modify the hub configuration are forwarded to IT management systems.

Think of an always-connected medium as an asset rather than a liability. You don't have to enable and manage incoming calls at the teleworker's residence to **manage hubs remotely** over an ***always-connected*** DSL service.

3. Consider hubs or switches that offer **advanced security features**. Some equipment (e.g., 3COM port switch hubs and workgroup switches) has the ability to learn the MAC address of a station attached to one of its ports. Once learned, the hub or switch will disable the port and generate an alarm (to console or as an SNMP Trap) should any address other than the learned address is seen on that port.

4. **Use packet and MAC frame filtering**. IT managers may wish to pre-configure network level packet filters on routers or bridges to block access to well known services ports of teleworker's PCs, to block traffic from unauthorized addresses originating at the teleworker's LAN, and to block network protocols other than authorized protocols. Where bridging is used, IT managers may wish to configure filters that only permit forwarding of LAN frames originating from authorized MAC addresses.

5. **Restrict routing and bridging protocols**. For the majority of teleworker environments, static routing is sufficient and should be the only routing used between routers at a teleworker's residence and corporate routers. Similarly, a static Forwarding Database can be configured in many bridges, and learning can be disabled.

Scenario #3: The teleworker requires access to application servers and NOS services that would otherwise be blocked by a corporate firewall.

The kinds and locations of enterprise servers and NOS services that a teleworker may need to access depends on the nature of the work the teleworker is expected to perform from a residence, and include:

- Intranet web servers
- File and print servers accessed using Network Operating System (NOS) protocols
- Client-server remote login
- Internal database and other networked application servers.

In this scenario, the IT manager may have to terminate residential broadband services behind the corporate firewall, or make exceptions to an existing security perimeter to accommodate access to, for example, intranet file servers. Such actions introduce vulnerabilities. Existing methods for compartmentalizing LAN communications within the enterprise may not be accommodated from a common termination point within the corporate network.

Recommended Policy and Best Practices for Teleworker access to Enterprise servers

AppleTalk, Microsoft Network (SMB/CIFS), and UNIX/NFS/X cannot be used effectively over traditional dialup services, but residential broadband services easily satisfy bandwidth and delay characteristics for teleworkers, so they will naturally want access to the same LAN environment from home as they have in their office. There are several ways to accommodate LAN access. These should be implemented in conjunction with the best practices already described, and include the following techniques:
For teleworker access to Intranets, consider products that allow you to build community of interest networks (COINs) based on strong user authentication.
For NOS protocol support, use Virtual Private Network techniques to securely extend file, print and other NOS services from enterprise networks to the teleworker (see "Encrypted Data Transport" and "Strong Authentication").
For client-server remote login, consider secure shell and secure telnet applications.

Universal Precautions

The measures described in the previous sections can greatly reduce risks associated with common configuration scenarios associated with teleworker residences. They are largely based on security measures that are generally understood to be among the "best practices" in building secure networks. They are **universal precautions** and,

where implemented, will be effective for mitigating and reducing certain risks, whether the user is a teleworker, mobile, or office employee. Let's examine these more closely.

Strong Authentication

Strong authentication is perhaps the most important security measure you can implement. Access controls, accounting, message confidentiality and message integrity are all based on the ability to require a user to prove that he or she is who he or she claims to be. If a user's or server's authenticity can demonstrated with a high degree of confidence (assurance), IT managers can control access to specific hosts, information, and applications. They can exercise considerable control over the kinds of actions users can perform on secured objects, and they can dictate when message exchanges between users and objects should be conducted using encryption for privacy and integrity.

There are a number of strong authentication systems to choose from, and you may have already implemented these over corporate LANs and for remote access. These include Kerberos, one time passwords such as Bellcore S/Key or RSA SecurPCTM (SoftID), and authentication token systems from Security Dynamics Technologies (SecurIDâ).

An increasing number of organizations that require strong authentication for web-enabled applications make use of the Secure Sockets Layer (SSL) and Secure Hypertext Transfer (S-HTTP) Protocols between web servers and clients. SSL can be enabled on most commonly used browsers and servers to provide mutual, strong authentication between clients and servers. For applications that operate over TCP, strong end-to-end session encryption can be negotiated and employed as well. SSL uses public-key cryptography for strong authentication. Aventail Corporation maintains an good reference site on SSL and SOCKS security resources. Secure HTTP (S-HTTP), an extension to HTTP, provides strong client/server authentication, "spontaneous encryption" and message integrity, and Request/Response Non-repudiation.

A good resource for information about S-HTTP can be found at Terisa Systems.

The use of a public key based authentication requires an infrastructure, e.g., a Certificate Authority (CA) for assigning personal and server certificates. A CA not only issues certificates, but is used to assert the trustworthiness and validity of certificates as well. You can outsource Certificate Authority to third parties such as GTE, Verisign, CyberTrust, and Thawte Consulting, or enterprises can use Certificate Servers from companies like Xcert, Netscape, or Entrust to implement private CAs. Once implemented, teleworkers (indeed, all workers) acquire personal certificates for use, and configure their browsers to only permit downloads of active content from servers that present trusted and valid certificates.

A good resource for general white papers on public key infrastructure can be found at Entrust.

Encrypted Data Transport

Certain organizations may find it necessary to use encryption over any communications link that is not physically secured, and security policy may dictate that any intra-enterprise communications exchanged over unsecured link must be encrypted. Consider VPN products based on IP Security (IPSEC) standards to fill this need. Layer 3 IPSEC **tunnels** provide IP-based **virtual, secure connections**. In this IPSEC mode, normal IP packets are routed between tunnel endpoints. Host systems or IPSEC routers can terminate tunnels. Tunnel endpoints can operate over any intervening network topology. Encapsulated within tunneled IP packets are IETF-specified security protocol headers that provide packet-level authentication (AH – authentication header) and data integrity and confidentiality (ESP – encapsulating security payload). These protocol extensions are IPv4 and IPv6 compatible. When used in conjunction with an Internet Key Management Protocol (IKMP), IPSEC protocols can be used with any authentication or encryption algorithm (MD5, SHA1, RC5, DES, 3DES, etc). Products based on draft standards for tunnel or transport mode IPSEC include the Cisco IOS routers, Compatible Systems IntraPort, RedCreek Ravlin, Timestep PERMIT, VPNet VSU-1010, and FTP Software Secure Client.

In situations where corporations wish only to encrypt certain data, application-specific or circuit-level encryption may be appropriate. Aventail VPN server encrypts application data transmitted over TCP connections. InfoExpress offer a VPN solution that proxies Windows Internet Naming Service (WINS) and Microsoft File Sharing for Windows environments. InfoExpress recently added AppleTalk proxy support to its Virtual TCP Secure Remote

VPN product. Electronic mail applications from Microsoft, Netscape, Network Associates and others support either Secure MIME or Pretty Good Privacy. These products let you digitally sign and encrypt mail and attachments.

Intrusion Detection, Attack recognition and Response

Where you terminate residential broadband services in the corporate network and the services you expect to provide to teleworkers may change the way you proactively monitor for intrusions and attacks. If you are already performing monitoring, logging and auditing activities on all internal segments, subnets, and systems, consider extending the practice to include teleworker connections. If you only proactively monitor systems on DMZ subnets or systems on subnets that can be accessed by outsiders or partners, consider how these same practices can be extended to subnets where teleworker connections are terminated.

Proactive monitoring systems and software products represent one of the fastest growing segments in the security industry. FireWatch from Bellcore, UNIX tcpwrapper and tcpdump, provide administrative assistance in collecting logs and creating reports for network auditing purposes. PingWare from Bellcore, Internet Scanner from ISS, or UNIX COPS, proactively scan networks for known configuration flaws that are exploited by intruders. Products from Cisco Systems, Network Associates and ISS take intrusion detection to the next level. These products scan networks searching for traffic patterns and content that match known attack signatures. NetSonarä from Cisco Systems, ISS SafeSuiteä and Network Associates' (formerly TIS) Stalker3.0 products can intervene and reconfigure firewalls, screening routers, and servers when they detect an attack or misuse of a network.

Network Anti-Virus Protection, Content Filtering

Blocking and intercepting executable code from sources outside the enterprise is a persistent concern for IT managers. Again, where you terminate residential broadband services in the corporate network and the services you expect to provide to teleworkers may change the segments and subnets you choose to restrict downloads and filter content (see "Intrusion Detection, Attack Recognition and Response").

Firewall-based VPN products from vendors such as Aventail Corporation, CheckPoint, Raptor, and Network Associates, can monitor application data and can enforce security policies at a more granular level, for example, by blocking application protocol content like Java and ActiveX. Products that focus entirely on Web security and management to provide URL and content access controls can also be obtained from companies such as Netegrity (SiteMinder) and Caravelle (Webwatcher).

Symantec's Norton AntiVirus for Firewalls and McAfee NetShield Security Suiteâ work with any firewall that supports the Content Vectoring Protocol (CVP), a standard interface used by firewall clients (e.g., the Gauntletâ Firewall 4.0 from Trusted Information Systems) to validate message content by passing requests to a scan server. The scan server checks HTTP, FTP, and SMTP requests for known virus signatures and repairs or deletes infected messages before they can be propagated inside the firewall. McAfee NetShield Security Suiteâ performs similar security services from a Windows NT server or workstation.

Conclusions

In this report, we've provided background information for IT managers who must maintain tight security while also introducing new access technologies into the enterprise. We've explained how residential broadband services based on Digital Subscriber Line and cable modem operate. We have identified potential vulnerabilities that are sometimes associated with DSL-based services, but are in many cases, vulnerabilities exposed by many if not all services used by remote workers and mobile employees. We have discussed deployment scenarios you may wish to consider as you re-evaluate corporate security policies regarding remote access and teleworker arrangements. Through examples, we describe how risks can be mitigated or reduced using commercially available security products.

Hopefully, we have alleviated your concerns about DSL-based services and security, and have helped you move one step closer towards a successful teleworker deployment.

This report offers considerations for implementing security in enterprise networks where DSL-based services are applied. It does not profess to address every security issue for every enterprise IT manager. In the course of this report, we mention security products that may satisfy a security need for an IT manager, and may direct the IT manager to a review of certain products. Any such mention does not represent an endorsement of any kind by Covad Communications.