

How To

Security and Remote Access

Practical Ways to Protect Data and Devices Beyond the Corporate LAN

Introduction: The Remote Landscape

Connecting remote workers, branch offices and others to corporate LANs is a business necessity. However, as laptops, handheld computers, smartphones and home computers proliferate, so do the associated security risks.

Remote and mobile users of these devices tend to toggle between “on-net” connections to the corporate network and “off-net” connections to untrusted networks, such as the public Internet and mobile networks. While off-net, endpoint devices may be exposed to viruses, malware and hackers, who might attempt to piggyback onto corporate connections once the device is back on-net.

Remote access security risks exist at three layers in the network: in the endpoint device itself, in the enterprise network, and on the customer premises. This paper will focus primarily on efforts to secure the remote access device and its resident data, but will discuss the other two security layers as they relate to the overall remote access security framework.

What Are the Risks?

The physical enterprise network boundary has dissolved. Enterprise networks extend far beyond physical wired LANs in main offices and data centers to embrace branch and home offices, the Internet, mobile networks and other entities and customer networks. This trend, though convenient and useful, introduces additional points of entry for intruders if the security of the network is compromised.

The boundary-less nature of enterprise networks is being driven by the substantial memory and CPU resources now available in portable devices and by the proliferation of broadband access services. With smart devices and fast access networks, remote access affords unprecedented productivity benefits, empowering users to conduct business from virtually anywhere. They can tap critical information during a sales meeting, for example, more quickly respond to customers and colleagues, and extend their business days as home-based teleworkers. And by distributing users across remote branch and home offices, enterprises gain more hiring flexibility across geographies and can save on real estate costs.

However, in this “virtual network” environment, client endpoint devices are no longer stationary and continually wired to a static Ethernet switch port. As a result, the IT organization faces a greater challenge to retain control over user access – both to data stored in the endpoint computing devices and to the corporate network.

The key IT security challenges associated with remote access include the following:

- Securing sensitive data stored on the remote device
- Ensuring that the endpoint device attempting to access the corporate network is legitimately authorized to connect
- Protecting the device from exploits, such as malicious code. If present during an on-net connection, these could result in performance degradation or denial of service (DoS) for the entire corporate network.
- Protecting data in transit against eavesdropping or data theft

New endpoint security services and tools are now available to help IT departments achieve these goals while also complying with recent mandates that require various security and access tracking features. Among these are authentication protocols, antivirus protection, intrusion prevention, firewall capabilities and data encryption. These functions and protocols should operate at all three network layers described earlier: in the endpoint device, in the WAN cloud and on the customer premises housing corporate network and IT resources.

Creating and Enforcing Policies

The first step toward properly deploying these capabilities is to create a business policy — a set of rules laying out which devices and users have access to which network resources and under what conditions. Among the variables that might go into a policy, for example, are the following:

- The user group/virtual LAN (VLAN) to which the device and its user belong
- The type of device requesting access (a laptop, smartphone, wireless PDA, home computer)
- The type of network connection through which the device is attempting to gain access, such as a wireless LAN, an SSL or IPsec virtual private network (VPN) connection, or a dial-up modem connection
- What minimum version of the endpoint device’s operating system, antivirus, personal firewall and other software must be installed for access to be granted to a given endpoint
- What applications are sanctioned to run on each type of endpoint device and which are disallowed

Keeping your policy updated and ensuring that all access requests are evaluated against the policy and treated appropriately is an ongoing, dynamic operational activity. As such, being able to automate and centralize control over this function is desirable for added security and also for operational practicality.

By contrast, manually keeping remote software, devices and policies synchronized across even a mid-size installation is error-prone and operationally time-consuming and expensive. And if there is no automated check and verification of the device before access is granted, intrusions can make their way onto the enterprise network when devices shift from off-net to on-net.

Once endpoints have been deemed policy-compliant and have gained access, they should be periodically audited for compliance while still connected. Using a so-called “heartbeat” security function, for example, compares policies and what’s actually running on the device at predetermined intervals. Such checks help prevent intrusions resulting from changes that users might make to the endpoint once the device is already on-net, such as the addition of new non-compliant software, USB devices and security key fobs, to name a few.

Recommended Best Practices

Your security strategy for endpoints should aim for consistency in the policies you set among the access categories that you establish based on the variables mentioned in the last section. An arsenal of software security tools is necessary for enforcing your policies across the remote access workforce and meeting the risk-avoidance goals described previously.

Enhanced Personal Firewalls

It is a recommended best practice that endpoints with direct contact to the Internet run a personal firewall to help prevent hackers from gaining control of the endpoint device. As mentioned, hackers can steal data directly from the device or piggyback onto the corporate VPN connection and break into on-net resources.

A personal firewall is a software application that helps protect an individual Internet-connected computer from intruders by examining each network packet to determine whether to forward it toward its destination. Fundamentally, firewalls make a “yes” or “no” decision to grant access based on the sender’s IP address or source network domain. However, today’s firewalls – both personal firewalls and the appliance- and router-based firewalls that guard network resources at the customer premises – are growing more sophisticated in that they now combine multiple endpoint security functions.

Today, basic source-route filtering is combined with scans for viruses and other known dangerous signatures, so that malicious code is filtered out alongside unauthorized users. Some will also filter based on URL; disallowing users, for example, to access or download content from certain Web pages. Some will also detect and filter spyware, programs that help gather information about a person or organization without their knowledge.

Personal firewalls are particularly useful for users with “always-on” broadband connections, which use static IP addresses that make them especially vulnerable to hackers. Firewalls can run alongside, or be integrated with, VPN client software for encrypting data and authentication messages traversing a wide-area network (WAN).

User Authentication to the Device

Users, devices and networks should be authenticated that they are, indeed, who or what they represent themselves to be. When a user logs on to the remote access device, for example, a user ID and password

help authenticate that the user is indeed the appropriate individual to be using that computer. For stronger security, two-factor authentication can also be used. This is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. Some security procedures are even beginning to use three-factor authentication, which involves possession of a physical token and a password used in conjunction with biometric data, such as a fingerprint scan or a voiceprint.

Authentication to the Network(s) — and Vice Versa

This step involves the carrier VPN service, if one is being used, and your own enterprise’s backend authentication, authorization and accounting infrastructure. The server side of the endpoint security scanning functions on the device – which can be run in an appliance, as router-based software, or as server software – first checks the device for infection, then that it complies with all required OS and application software versions, then that it isn’t running any programs disallowed by your policy. If the device doesn’t comply, the option remains for access to be blocked or for the connection to be redirected to a URL so that patches can be applied or software remediation can otherwise take place.

Once the device is deemed compliant, an authentication exchange using the 802.1X and Extensible Authentication Protocol (EAP) takes place between the VPN service provider’s network and the device. This exchange can also be between the device and the enterprise authentication, authorization and accounting infrastructure, or it can take place between device and both back ends, depending on what network services are used and whether you are managing endpoint of your network in house or outsourcing it to a service provider. User credentials are sent to a router at the service provider’s NOC or at the edge of the private network. From there, they are passed to a Remote Access Dial-In User Service (RADIUS) or other authentication server. Once the server verifies the user credentials, it sends a message to the router that the user is legitimate, and a VPN session is established between device and router.

Depending on what flavor of the EAP algorithm is used, mutual authentication can provide an extra measure of security. In this situation, the 802.1X exchange happens in two directions, verifying not only that the user and device are legitimate, but also verifying that the network to which the user thinks he or she is connecting is, indeed, that network. This capability helps avoid malicious attempts to redirect users to a network or Web site other than the one they think they are accessing for fraudulent purposes, such as phishing or otherwise gathering user credentials and personal information.

Local Data Encryption

Encryption of any sensitive data stored on the endpoint is also considered a best practice. Encryption converts data into a form called a cipher so that it cannot be understood by unauthorized people.

Encrypting either the entire hard drive of the device or certain files and folders flagged for encryption helps prevent intruders who find a lost or stolen device from accessing private information. It also allows network administrators to troubleshoot devices without seeing certain data. This capability might be a requirement of the Healthcare Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, or other compliance mandate, depending on what industry your organization is in. Encryption methods for preventing unwanted access to local resident data include Advanced Encryption Standard (AES), Triple Data Encryption Standard (DES), Blowfish 128, and others.

Network Encryption

Encryption is also important for helping to protect the privacy of both data and user authentication credentials sent over a public Internet connection. Your strategy for encrypting data and authentication message exchanges in transit may depend on whether your organization uses a network-based VPN (one that uses an infrastructure separate from the public Internet) or a CPE-based VPN that sends traffic exclusively over the Internet.

CPE-based Internet VPNs tend to encrypt both authentication messages and data in transit end to end: from the edge of one site or device across the last-mile link to the back-end authentication system at the data center.

Enterprises with the strongest security requirements (financial, healthcare and government organizations, for example) are most likely to use data encryption over a network-based VPN service. Network-based VPN users include those who access corporate resources from remote or branch offices via a Multiprotocol Label Switching (MPLS), IP-enabled frame relay, frame relay or ATM service.

These services already provide a per-customer virtual circuits through a single-operator network; encryption is an added layer of protection. By contrast, the Internet VPN traverses network links run by myriad operators, so security control is more difficult to maintain.

You can choose to license, deploy and maintain client software that performs the filtering and encryption functions described in conjunction with network- and premises-based security tiers. Or you can elect to procure your endpoint security measures in the form of a service that takes advantage of a service provider's economies of scale for patch deployment and technology refreshment.

Executing your Strategy: Outsourcing vs. Do-it-Yourself

As mentioned, if you choose to deploy and manage endpoint security yourself, it is advisable to both automate and centralize the process. Otherwise, you will be hard-pressed to keep disparate devices synchronized and policies updated and enforced, even if you are fortunate enough to have substantial local IT staff. The reason is

that new exposures are constantly emerging, and there is a time delay associated with patching remote devices one at a time – a delay that could rapidly affect network operations should an infection sneak onto the network before updates can be completed.

For the same reason, it can be attractive – particularly in very large, dynamic enterprise environments – to take advantage of a service provider's network operations center (NOC) and continual product and technology upgrades. From an outsourcing perspective, you can opt for either a managed or unmanaged endpoint security service.

Managed services entail purchasing a portfolio of remote access connectivity services from a carrier and also licensing client software from the carrier for each remote computing device. The client software provides a common interface for accessing the available services to which each user is entitled by means of your central policy. The software also bundles in most, if not all, of the security services described.

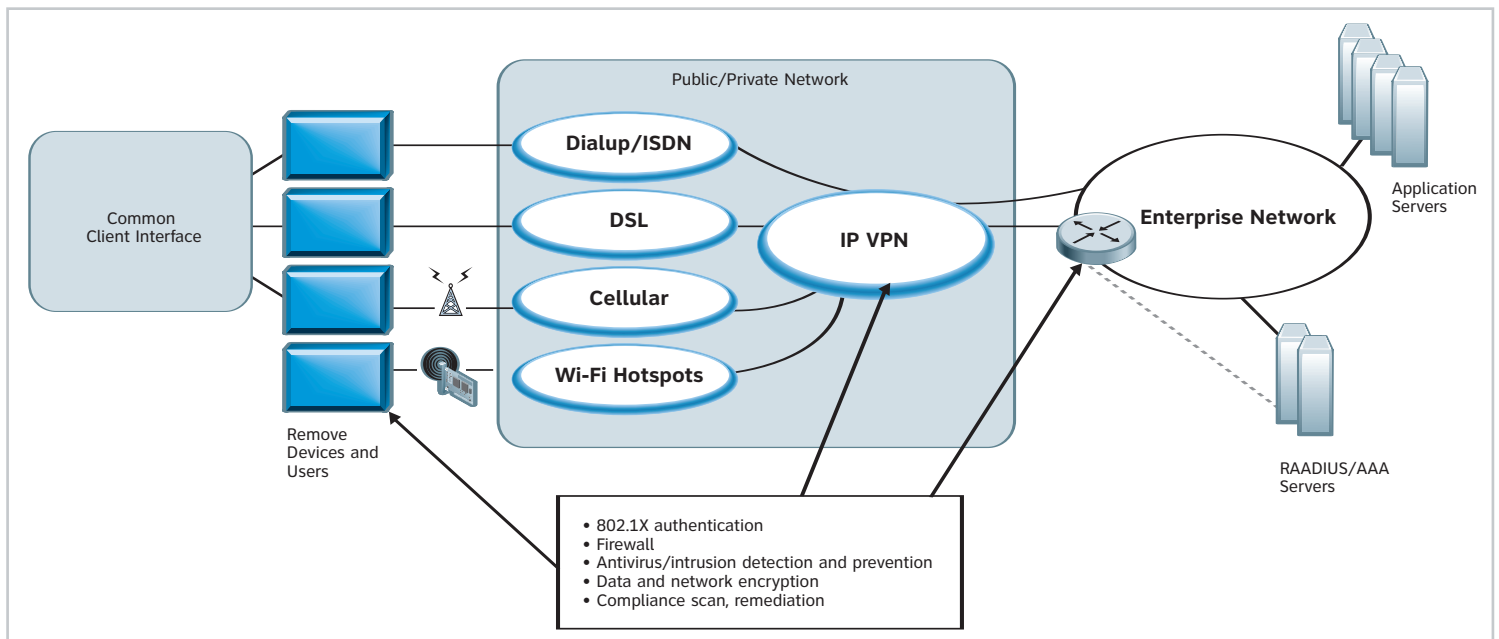
Under the auspices of a managed service, your fleet of remote users can access corporate resources using the carrier's various connectivity services under a single common billing umbrella. They can also access other providers' services that use the same network protocols – in cases, for example, when the carrier might not have a local service available – that will generate separate service bills.

As part of the managed service, the carrier can also resell and manage the CPE needed to work in conjunction with the personal firewall, authentication, and other endpoint security functions. For example, the carrier could provide, install, and maintain the following at the head end on the customer premises:

- A firewall
- A VPN encryptor/decryptor
- An intrusion detection/prevention system

These functions can take place either in standalone appliance form factors or as software capabilities directly embedded into the head-end WAN router on the corporate premises.

Layered Endpoint Security



A mix of firewall filtering, authentication, encryption, and client compliance scanning is necessary to secure remote workforces.

AT&T as Security Service Provider

Enterprises can turn to AT&T for security services, either managed or unmanaged. AT&T managed services integrate access connectivity with security-layer services. They enable users to connect from 40,000 AT&T Wi-Fi, dial and wired Ethernet access points, as well as from other providers' access points.

For endpoint security, AT&T offers the AT&T Personal Firewall Service. This service is most often layered onto one of AT&T's VPN services (described below). It bundles two-factor authentication, firewall, antivirus and intrusion scanning, and software patch management into a common software client that runs on all of an enterprise's remote access devices.

Compliance scans and authentication take place at the AT&T NOC according to enterprise policy, filtering out unauthorized users and devices and checking devices for software version policy compliance before granting users access to the enterprise customer's back-end authentication, authorization and accounting resources.

Among AT&T's services:

- **Premises-Based VPN Service** – A VPN service that protects data traversing the public Internet. The service supports the same software client used with AT&T Personal Firewall Service for gaining access to corporate information via broadband, dial, Wi-Fi or wired Ethernet connections. For site-to-site connectivity, an appliance or router supporting encryption, such as IPsec, is installed on customer sites to protect data in transit.
- **Network-Based VPN Service** – A site-to-site, network-based IP service that utilizes MPLS for added privacy and quality-of-service (QoS) control, or, alternatively, uses frame relay or ATM technology.
- **Network-Based Firewall Service** – With this service, the firewall functionality resides in the AT&T MPLS network. This allows control over employee access to the Internet and helps prevent unauthorized access into the corporate network without the expense of premises equipment.
- **Network-Based IP-VPN Remote Access** – A remote access service that offers access to a customer's AT&T frame relay, IP-enabled frame relay, ATM or VPN using the same software client used with AT&T Personal Firewall Service via broadband, dial, Wi-Fi or wired Ethernet connections.

An unmanaged service provides the same security features but doesn't bundle in the connectivity services at the access layer or, necessarily, CPE at the enterprise head end. This option allows users to access any carriers' remote services. In this scenario, users incur costs with various service operators, so the enterprise billing management function is more complex, and volume discount opportunities with any one carrier are reduced.

The most compelling reason to use the resources of a service provider for security services is that do-it-yourself total cost of ownership (TCO) is high for installing and maintaining the complex and dynamic remote access infrastructure. Managed carrier services can build in future-proofing and technology refreshes into the service contract for all three layers of remote access security services: the endpoint device, the WAN cloud and the customer premises. This substantially reduces the cost and operational complexity challenging enterprise IT staff as new threats and exposures continually emerge.

Summary

Remote access connections have become integral to mainstream business, offering unprecedented productivity and flexibility benefits. Protecting devices and the data they contain when they are disconnected from the corporate LAN, however, is a challenge that has resulted from the dissolution of physical enterprise network boundaries.

Successful endpoint security measures involve remote client software containing a bundle of security functions that filter out access attempts from intruders and malicious code. The software also performs the level of authentication the enterprise deems appropriate, verifying that the user, device, and network are all legitimate. These tools correspond to the same security capabilities in the WAN services point of presence and on the customer premises for a layered, defense-in-depth approach to security issues.

In addition, endpoint security involves protecting the corporate network by scanning devices for policy compliance before granting access.

Enterprises can opt to build and maintain the remote-access security infrastructure themselves, which can be complex and expensive from a TCO standpoint, given the ever-changing dynamics of remote-access risks and solutions. Conversely, they can outsource endpoint security to a carrier that offers automatic technology refreshments and product upgrades as conditions change. Carrier services can be managed or unmanaged. Managed services usually entail also buying connectivity access services along with the security services and might also involve the carrier installing and maintaining premises-based security equipment, such as firewalls and intrusion detection/prevention systems.

Whether you opt to run your own endpoint security infrastructure or outsource it to a carrier, be sure to create a centralized set of policies that can be quickly and automatically checked each time a remote device attempts connection. Distributed approaches to securing the remote workforce generally make it difficult to keep policies and software versions in sync, creating time lags between detection and patching that could cause serious security breaches to your devices or your corporate network resources.

For more information contact an AT&T Representative or visit www.att.com.

