

10 ways to secure borderless networks

Date: October 9th, 2007

Author: Debra Littlejohn Shinder

Category: 10 things, Security, Network administration

Tags: Firewall, Microsoft Access, Network, Operating System, Data, Encryption, User, Authentication, Computer, Identity Management, IPSec, Federated Identity Management System, Encrypting File System, PGP NetShare, Entrust Entelligence Media Security, Transport Layer Security, Microsoft Windows, Security, Authentication/Encryption, Networking, Operating Systems, Software, Debra Littlejohn Shinder

Company networks are undergoing so-called “de-perimeterization,” as online collaboration with partners, customers, telecommuters, and others outside the physical LAN becomes more and more important to doing business. At the same time, these users are able to connect to company resources with a wider variety of devices, including smartphones, Blackberries, and other handheld devices. This is great in terms of access, but not so great in terms of security. The old security model is dependent on “border patrol” via firewalls, intrusion detection and prevention systems, DMZs, and other perimeter protection methods. In the new, borderless network, the focus shifts to protection of the data itself.

Here are 10 technologies you should be looking at to help secure your borderless network.

Note: This information is also available as a PDF download.

#1: Strong and multi-factor authentication

User authentication focuses on who is requesting access, rather than where they're located. But when users can access internal resources from anywhere, it becomes more important than ever to ensure that the authentication process can't be circumvented.

Strong authentication methods include more than just providing a password; for example, a user might be required to answer multiple challenge questions before being given access to sensitive data. Multi-factor authentication adds another element: The user must provide a card, token (something you *have*), or biometric identifier, such as a fingerprint or iris scan (something you *are*), as well as the “something you *know*” element of passwords and successful answers to questions.

Some companies, such as SafeNet, have developed entire security platforms targeted at protecting borderless networks.

#2: Cross-company identity management

Closely related to authentication is the dilemma of identity management. Identity management systems tie particular people to particular accounts, names, and attributes. The problem with traditional identity management systems is that they work well within the borders of an organization but not as well with users outside the organization. That's where cross-organization, or *federated*, identity management comes in.

A federated identity management (FIM) system allows partner companies to authenticate each others' users. Microsoft's Identity Integration Server (MIIS) and its successor, Identity Lifecycle Manager (ILM), are examples of products that can provided for federation-wide identity management. Another option is RSA's Federated Identity Manager.

#3: Host-based security software

A borderless network doesn't mean the firewall is dead; it's just moved. Actually, most companies aren't doing away with their perimeter firewalls — we haven't gotten quite *that* de-perimeterized yet. But when those borders aren't as tight as they used to be, it's a good idea to install/use

host-based firewalls, antivirus, and other security products to catch those threats that make it past the edge firewalls. This gives you a double dose of protection.

The latest versions of Windows client and server operating systems come with firewall and anti-spyware programs built in, and numerous third-party host-based products are available.

#4: Application-level security

Application-level security is integrated into the user or business application program and can provide cryptographic services, such as non-repudiation through digital signatures or selective field encryption. This gives you good protection against “insider” attacks (which becomes even more important in the borderless network, where the lines between insider and outsider are blurred).

#5: Policy-based integrity enforcement

When users are connecting to your internal resources from various locations via computers you don't control, it becomes especially important to ensure the integrity of those systems. You want to be assured that they are running that host-based security software (firewall, antivirus, etc.) and have installed security updates to minimize the chances that an infected remote system will spread malware or attacks to other computers on your network.

To do this, you can use policy-based integrity systems, such as Microsoft's Network Access Protection (NAP), which is a policy enforcement system built into Windows Server 2008, Vista, and Windows XP Service Pack 3, or Cisco's Network Admission Control (NAC), which likewise restricts connection of devices that aren't compliant or trusted.

#6: Data-centric access controls

File-level access controls, such as NTFS permissions, help protect data whether it's accessed from a remote computer, an internal computer, or the local machine, making protection more data-centric. Access is granted or denied based on individual user accounts or group membership and is not dependent on the physical location of the user.

#7: File-level encryption

Encryption of individual data files can be accomplished using the Encrypting File System (EFS) built into modern Windows operating systems. The latest versions of EFS allow the creator/owner of the file to specify other users who can share/access the encrypted file. EFS is certificate based, and users can export their EFS certificates and private keys to removable media so that it does not remain on the computer when they're not using it.

Alternatively, third-party data encryption software, such as Cypherix, can be used to encrypt individual files, folders, e-mail messages, etc., including the data on removable media. PGP NetShare is designed to encrypt files and folders used by collaboration teams. Entrust Entelligence Media Security is a file encryption application that will automatically encrypt data saved to specific folders. Many other file encryption products are available.

#8: Full disk encryption

Full disk encryption protects both portable and desktop computers in the borderless network environment by encrypting entire volumes. An example is the BitLocker feature that's included in Windows Vista Ultimate and Enterprise editions. It can be used in conjunction with a Trusted Platform Module (TPM) hardware chip to prevent someone who steals or gains physical access to a computer from being able to boot the operating system or access the files on the volume, even by booting another instance of an OS.

BitLocker, unlike some disk-level encryption programs, encrypts the operating system partition, not just data partitions. This means the page file and temp files, which often contain copies of data that might be sensitive, are encrypted.

Third-party products, such as SafeGuard's Easy Hard Disk Encryption, are also available.

#9: End-to-end encryption

File-level and full disk encryption protect the data only while it's on the hard disk. To protect data when it's traveling over the network, you can use IPsec, which operates at the network layer of the OSI model and thus requires no changes to or awareness of applications. IPsec can provide data encryption/confidentiality, authentication, or both, using public key encryption and digital certificates. IPsec is an open standard and is supported by modern Windows operating systems.

Data can also be protected in transit over the network by using a higher level encryption protocol, such as SSL/TLS. Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL). Also based on public key encryption, SSL/TLS is often used for sending secure data to Web servers.

#10: Rights management

In the borderless network, security problems arise not just in regard to what data can be accessed by whom, but also in regard to what those with legitimate access do with that data once they receive it. Rights management attempts to control what a recipient of an e-mail message or document can do with it.

Windows Rights Management Services (RMS) can restrict the recipient's ability to save, forward, copy, or change the data and can even set an expiration date so that the recipient can no longer even access the data after a specified time period. This helps prevent security leaks caused by deliberate or inadvertent mishandling of sensitive data.

Cross-company solutions for RMS are available from third-party companies such as GigaTrust.

Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

Trackbacks

The URI to TrackBack this entry is:

<http://blogs.techrepublic.com.com/10things/wp-trackback.php?p=244>

No trackbacks yet.

Copyright © 2007 CNET Networks, Inc. All Rights Reserved.

0