Global Information Assurance Certification Paper

Remote Access Solutions for the Digital Age in Government Computing
Robert Ellison
December 21, 2000

Introduction:

Government and Corporate networks alike suffer from the same administrative and fiscal issues of implementing and managing remote access. Users have difficulty accessing resources when they are away from the office, and the network administrators must maintain extra equipment, modify firewall policies and usually incur hefty circuit costs to maintain these access points.

Because I work for the government and am responsible in part for the design, administration and security of our network and it's resources, I have to deal with these situations. I also have the added task of being able to access my own network from a remote log cabin under the shadows of the Blue Ridge Mountains.

Initial Approach:

The solutions that we have tried are varied and some worked better than others. Five years ago we had racks of full dedicated dial-up hardware. The up side of this solution is that it was inherently secure because our users dialed directly into the network. By utilizing this approach we did not have to add any holes to our existing firewall, and we had the ability to add additional security measures such as dial-back connections to authorized user phone numbers. The downside was that this approach required many dedicated phone lines to support peak user demand, a fact not immediately definable since we previously lacked this ability to dial into our network. In addition, we established early on that specific travel, and/or trade shows overloaded our systems capacity, and it was too costly to maintain for the overall sporadic usage, which generally was much lower. There are several mature solutions in the current marketplace that are easy to implement, but you really need to evaluate the overall costs involved since this type of solution winds up being expensive in the long run and limits it's overall value to businesses. Given that the initial solutions were cumbersome and expensive we decided to try a two-pronged approach that utilized existing Government owned dial-in access points and our own users Internet Provider accounts from home.

Security and User Considerations:

This is a list of some of the hurdles that we had to overcome in order to make this a usable and relatively secure system:

- Unauthorized Access to dial-in servers
- Account Policies and Maintenance procedures
- Holes in the firewall to accommodate remote access from home users
- Different Operating Systems to contend with
- Users who did not have Government Systems
- Encryption standards not set
- Validation of data and users
- Support Issues on whatever system we deploy
- User perception of past services

Password policy, the bane of any security administrator's existence, is even more critical when those passwords grant remote access to internal networks. Remote users must employ strong passwords in order to keep the privilege, and a password usage policy should be enforced which provides for periodic assessment of password strength. Consider two-factor authentication mechanisms, such as smartcards or hardware tokens. [1]

We have implemented a tough standard on our two-stage username password authentication scheme. The NT Based Network underneath the dial-in has passfilt.dll installed on all network servers and workstations, in addition it has been modified to meet in-house policies which consists of: minimum password length is eight characters, a minimum of six alpha-numeric letters two of which must be capitals, and the other two must be special characters, it also cannot begin or end with a numeric. We have also upgraded our network to NT workstations and have disabled LANMAN authentication[2]

How to access the Network:

We have also decided that we have two categories of users, who in general want the "Works" or a "No Frills"

approach to the network resources they want to access. To accommodate the "No Frills" group we have deployed a Web Based Outlook E-Mail Client through the use of a NT 4.0's Internet Information Server Web Server and add-on Exchange Web Connector. To encrypt the information coming and going to the web server we installed a Server based 2048-Bit Triple DES Digital Certificate, and employ a two-stage NT username/password/domain Authentication model to login. Our Internet Site that contains the link to our Outlook Web E-Mail Access also includes FAQ's and links to troubleshooting to help any users who cannot contact our support people after hours or during holidays. We have employed all of the Internet Information Server patches and security fixes noted on Microsoft's, the SANS and CIAC Websites. This approach mimics an article that I have recently read entitled "Secure Messaging Concepts with Exchange Clients[3]," with respect to our Web Based E-Mail implementation. Additionally we have paid special attention to the SANS Institute Resources, specifically "How to eliminate the ten most Critical Internet Security Threats," seeing as how Threat #4, RDS Hole in the Microsoft Internet Information Server (IIS) could be used against our design. [4]

In the group that we identified as wanting the "Works" will access the network through our deploying a Windows NT-Based ICA-Citrix Meta-Frame Client that creates a VPN (Virtual Private Network) for our users. By utilizing this client we have effectively given internal Network Access to our users and administrators alike in a costly and effective manner in an encrypted secure network tunnel via the Internet. Both services (Citrix and WebBased E-Mail Access only) are implemented by connecting to the Internet either by their own Internet provider or a shared pool of Shiva LanRovers that our Government facility owns. Once the initial connection and first level of username/password authentication is made, the user must launch the ICA-Citrix Meta-Frame Client, which forces IP Security and the Layer 2 Tunneling Protocol, as well as secondary NT username/password authentication. It should be noted that the initial dial-in access we offer has a separate username/password authentication scheme from our internal network. By deploying the two access points, (Internet dial-in & VPN Authentication) and enforcing the VPN connection, we can control the applications, desktop and access to network resources by policies and login scripts.

Logon Restriction/Policies:

Clearly stated policies regarding the use of all Government Computing resources is a mandatory read for our users prior to granting any remote access software or usernames/passwords. We require all of the Federal Employees and Contractors to sign a statement indicating that they have read and understand our policies, and that they may be monitored and have their sessions recorded when they use remote access systems. Essentially we are using the same criteria, policies and warning banners for our remote access computing regardless where they logon.

We have chosen Microsoft Outlook 2000 as our primary in-house E-mail Client and Internet Explorer 5.5 for all home users that wish to access e-mail only via our Outlook Web-Based E-Mail. Outlook 2000 includes security features that allow you to send and receive secure e-mail messages over the Internet and prevent unauthorized access to your computer. To answer the call of the digital age and the government's direction to provide authentication, verification and non-repudiation of e-mails from users we are deploying Entrust on our LAN Based E-Mail systems and offering transportable certificates for home Users in specific instances, such as Government owned laptops or systems. We decided to limit ourselves to Microsoft's Outlook E-Mail Client and Internet Explorer to simplify our support and installation base. In analyzing the vendors of PKI products, we decided that Entrust Technologies offered an affordable and Enterprise scalable product that goes well beyond our initial E-Mail based needs. It is S/Mime compatible and interoperates with our current Entrust CA client certificates that we are deploying site-wide. This gives our users the granular abilities to set security levels on e-mail messages from Exchange to Exchange recipients attachments, messages from Exchange to Internet recipients, control html content that is received with their e-mail messages and set security levels on attachments. By deploying an accepted PKI, (Public Key Infrastructure) solution on our Enterprise we have successfully meet the NIST standards and are following the Federal PKI Steering Committee guidance documents. [5]

Digital signatures and digital certificates are encryption-based methods for providing the identities of users (user authentication), the origin of messages (message authentication), and the integrity of the documents. They can also provide non-repudiation as well as digital time stamping, which effectively binds a document to the time it was created or sealed[6]

Entrust/Express, an Entrust-Ready application plug-in for Microsoft Outlook, provides additional levels of functionality over the core email application, including advanced trust management. Entrust/Express properly handles certificates that have been issued by a Microsoft CA or an Entrust CA.

Bottom line: Entrust/Express provides powerful and easy-to-use S/MIME capabilities with Microsoft's Outlook and Exchange e-mail clients. Entrust managed certificates are also available to native Outlook and Outlook Express through Entrust/Unity.[7]

Benefits from our deployed PKI E-Mail solution:

- **Authentication Digital certificates issued as part of your PKI solution allow individual users and organizations the ability to confidently validate the identity of each party in an Internet transaction.**
- **Verification A digital certificate ensures that the message or document the certificate "signs" has not been changed or corrupted in transit online.**
- **Ensure privacy. Digital certificates protect information from interception during Internet transmission.**
- **Authorize access. PKI digital certificates replace easily guessed and frequently lost user IDs and passwords to streamline intranet login security - and reduce the MIS overhead.**
- **Authorize transactions. With PKI solutions, your enterprises can control access privileges for specified online transactions.**
- **Nonrepudiation. Digital certificates validate their users' identities, making it nearly impossible to at a later date repudiate a digitally "signed" transaction; this is an acceptable standard in courts now for document validity and verification.**

Use of PKI products allows the government to meet accepted criteria within our Nation's Court Systems for time stamping and identification/verification of documents and user's who have sent and received them. This also works within our requirements for time stamping of materials that must be archived and remain sensitive well into the future.

Password Validation:

On a monthly basis we run LophtCrack on our NT server's SAM Database to see if anyone has easily cracked passwords. If the passwords are cracked easily they receive an e-mail notice from our support group indicating that they must change their password on the next login. We also make the selection in User Manager on the Domain's BDC to reflect this change to the user's account.

Analysis:

By leveraging our assets to meet the needs of our two disparate groups of customers we have deployed a workable and scalable Enterprise Model for Remote Network access that remains independent of most hardware requirements.[8] Although I did not specify, we do cater to Macintosh and Windows based clients accessing our internal NT Based Network. With the ICA-Citrix Meta-Frame NT and Macintosh Clients, we can cater to the lowest common denominator, that being modem speed at this point and still grant fairly unencumbered access to all of network resources in a relatively safe and secure environment. The key to making this effort a success was to identify our requirements and develop a solution based upon their specifics. It is a foregone conclusion that Network Security, especially from a remote access standpoint is a strategy of risk mitigation, and that given enough time and effort, our network could be attacked and accessed. With that said, the solution that we have deployed has enough safeguards and authentication levels to meet our security and working requirements at this point in time. We will always have to remain cognizant of new threats and how they will affect our Networks and make adjustments to the architecture as required.

Footnotes:

1 Mcclure, Stuart. Scamray, Joel. Kurtz, George. "Hacking Exposed: Network security Secrets and Solutions." 1999, P.287

2 O'Dwyer, Frank. "Ensuring Password Quality on NT Networks," Revision 90, Wednesday, April 7, 1999. http://www.brd.ie.ntsecurity/

3 Hall, Monty, "Secure Messaging Concepts with Exchange Clients," Last Updated, Monday Aril 17, 2000 http://www.securityfocus.com/templates/library.html?id=242

4 "How To Eliminate The Ten Most Critical Internet Security Threats The Experts' Consensus," Version 1.30 November 17, 2000 http://www.sans.org/topten.htm

5 Polk, William, "The National Institute of Standards and Technology (NIST)" Last Modified: December 15, 2000, http://csrc.ncsl.nist.gov/pki/

6 Winkler, Ira S. "Internet Security Professional Reference Second Edition." 1997, P. 572

7 Entrust ® and Microsoft ® Windows ® 2000: An Interoperability Overview, Date: September 1, 2000 Version:

2.0

8 Fratto, Mike. Network Design Manual, "Building Scalable Remote Access," Updated January 17, 1997
http://www.networkcomputing.com/netdesign/sraa.html

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event