Global Information Assurance Certification Paper

VPN Authentication Solution for the mobile workforce
Practical Assignment version 1.4b
Greg Krause 10/30/02

Introduction:
This paper is intended to demonstrate how a real-world information security risk was addressed and what technology was put in-place. Virtual Private Networks (VPN's) and remote access, is a very broad topic with several security issues. This paper is intended to focus on remote access VPN **authentication,** and the need for positive user identification and protection of valuable corporate information.

In this case, remote access was being provided to mobile users via a VPN using a common shared secret for authentication. Administrators had minimum logging capabilities for security auditing. This paper will discuss problems and vulnerabilities with this technology and what was done to minimize the security risk. It will also cover the decision process that was used to determine what product was chosen and any problems that were encountered during the deployment. IP addresses in the network drawings have been changed to protect the actual network that this case study was built on.

Before:
Remote access for limited amount of users (approximately 25) was being provided via a Timestep Permit Gate model 7520 VPN connections. Timestep VPN gateways are IPSec-compliant and have been IPSec-certified by the International Computer Security Association (ICSA). IPSec is an extension to the Internet Protocol (IP) that provides authentication and encryption at the OSI Reference Model transport layer. IPSec has been mandated into the IETF's specification of IP version 6 (IPv6). IPSec has become the standard for most VPN venders. It's important that the industry has come up with a standard with VPN technology. This becomes very important when configuring clients for remote access. Having a standard is also imperative when connecting a gate-to-gate tunnel. One reason IPSec has become so popular with VPN's is because the client doesn't require much knowledge. The client is not user based, meaning it doesn't require tokens, ID's or Crypto Cards. Instead, the security comes from the workstation's IP address or its certificate, establishing the user's identity and ensuring the integrity of the network. An IPSec tunnel basically acts as the network layer protecting all the data packets that pass through, regardless of the application.

Our VPN authentication was being carried out using MD5 digests. MD5 is often referred to as a shared secret or shared key. The shared key could be a mutually agreed upon character string or RSA private keys. New requirements demanded that we were able to provide additional remote access to an additional 75 users. During the SANS Security Essentials course we discussed several security

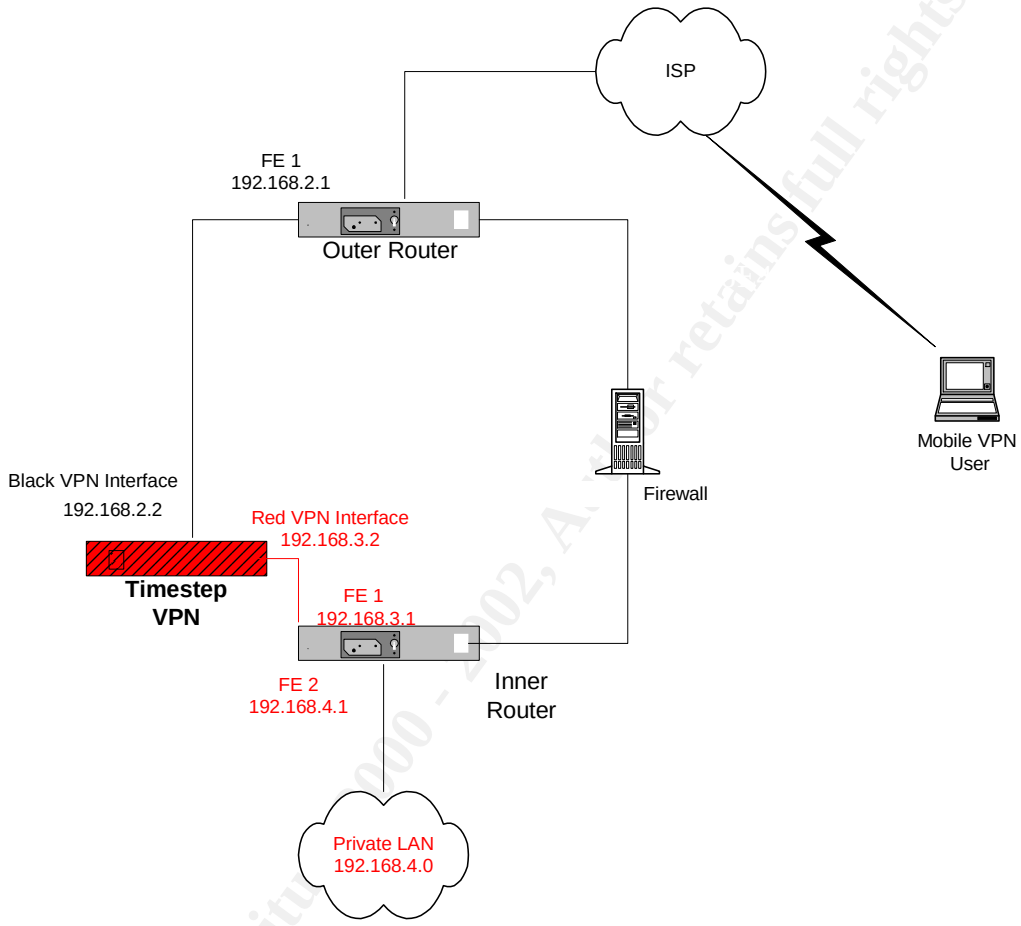
issues with VPN's. There seems to be a misconception that if you're on a VPN every thing must be secure. VPN tunnels only ensure that the data is secure while the data is being transmitted. The most important things to remember about VPN's are simple. VPN's protect against eavesdropping and insertion attacks. A VPN doesn't stop an attack from being passed through it. One important overlooked security issue with remote connectivity over a VPN is the "authentication". Authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

In this case, the VPN is providing strong triple DES encryption. DES has been around for approximately twenty years and has been approved by the U.S. government as a encryption method This technology has been regarded as less secure than more recent encryption systems. Triple DES has corrected many of the flaws of the original version of DES. Encapsulated Security Payload encrypts data while using a checksum to verify its integrity. Encryption translates data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption also called public key encryption and symmetric encryption.

A common shared secret was used for all users to establish a secure tunnel. This was the only means of authentication to establish a secure tunnel. If the shared secret were compromised, the shared secret would have to be changed immediately. Changing the shared secret would terminate all remote sessions to users that were using the compromised shared secret. All mobile users would have to obtain the new-shared secret to reestablish remote connectivity. This would basically cause a denial of service. Because our company works in a very secure environment, and company policy states, "That no passwords can be transmitted over voice and data lines." New passwords can only be obtained face to face. This posed a serious problem for remote users and administrators. Mobile users on travel would not be able to obtain the new-shared secret until there return back to the corporate office. We needed a way to force a secure independent user authentication. Individual authentication would allow for better accounting and logging of individual accounts. We also needed a way to disabled individual accounts with out affecting other users.

There are multiple ways to implement a VPN into your network infrastructure and you could write a paper on this topic alone. With our current VPN architecture, the VPN is configured parallel to our firewall. (*See figure 1.0*.) This is a very popular configuration and is one of several typologies recommended from Timestep corp.

Figure 1.0
Before VPN typology



A problem we were having with a shared secret authentication method. We found that most users were writing down the password on a piece of paper that was either stuck to the portable computer or stowed away in the travel case. Even though are passwords where built around a phrase to help users remember lengthy passwords, this was still a problem. When portable computers where recalled from the mobile workforce to patch or update software, the IT staff would often find these passwords somewhere in the travel cases. If a portable computer was stolen or lost, users access could be used for unauthorized access. 1.2 million laptops were reported lost or stolen by U.S. companies in 2000, this is a 33 percent increase over 1999. (ZDNET Stop the Thief By: Brian Ploskina) Our current authentication process had no way to verify that the user is who he says he is. We needed an authentication mechanism that was not so vulnerable to possible unauthorized access.

Our attended goal was to engineer a secure authentication method, enhance our logging capabilities, provide a user-friendly environment, and to engineer a system that could scale to hundreds and possible thousands of remote users.

During:
After attending the SANS Security Essential class it was clear that one of the weakest links when providing remote access via a VPN is the authentication method. Having one shared-secret to establish a VPN tunnel into our private network was like leaving the back door unlocked. While attending the Security Essential course it was also made clear that extended authentication was a good solution to securing a VPN connection.

User friendliness is imperative. Our helpdesk is not staffed 24x7. The helpdesk was staffed only during normal business hours. The mobile work force tended to travel to different time zones making the helpdesk unreachable for these traveling users. Authentication solutions only provide security if they're used. Products that require technically demanding and intrusive user intervention at the desktop are more likely to be subverted than products that operate with little end user interaction. We looked at multiple authentication methods, like, PKI, Microsoft's Certificate Server, and RSA's Secur ID.

Enterprise PKI is the collection of policies, roles, responsibilities, decisions, services and controls for using public-key cryptography within an enterprise, across applications. Enterprise PKI takes over the functions of enrolling users to applications one-by-one. PKI is about knowing that if you can decrypt with a key that you believe belongs to a user, which in fact sent the message. PKI is directory service and certificate service software, and hardware, and copies of keys are secured. These are components of a PKI enterprise infrastructure. PKI is the technology that still appears to be in a state of flux. A standard for setting up PKI is currently evolving and there is no single PKI or even a single agreed upon PKI. However, nearly everyone agrees that reliable PKI will become necessary before electronic commerce can become widespread. Finding knowledgeable people on PKI deployment and administration is also difficult.

Microsoft Windows 2000 built-in certificate authentication uses Extensible authentication Protocol (EAP). Windows 2000 uses a mutual authentication process. A user's computer and the network server present their certificates to each other. A public key verifies the user's digital signature that is contained in a trusted root server. The root certificates are the basis for certification and verification. System administrators manage all certificates. While the use of certificates is fairly simply, the deployment and implementation process is anything but easy. We felt that creating and implementing the necessary

processes and procedures for key and certificate management would be labor intensive.

RSA Secur ID uses a two-way authentication method. Two-way authentication is something you know and something you have. (I.e. Pin number, and token display number) Our current Timestep VPN's supports extended authentication by communicating of means of RADIUS, port 1812. RSA Secur ID ACE server also communicates via RADIUS.

Secur ID was are product of choice for securing are VPN authentication. RSA is the world's leading two-factor authentication system and it has a very large customer base. RSA Secur ID has deployed more than 10 million RSA Secur ID's to end users and 12,000 authentication installations worldwide.

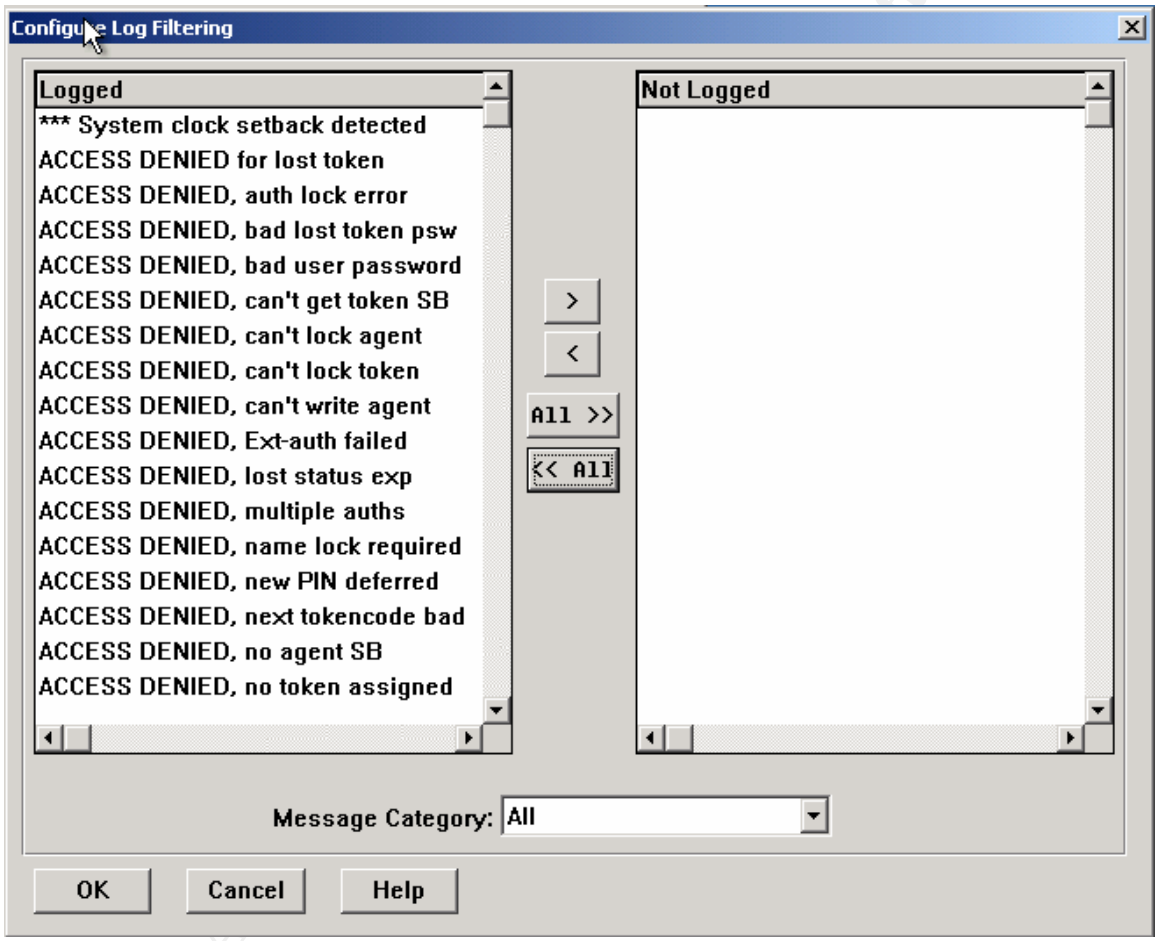
RSA was contacted and they confirmed that Timestep VPN's was an interoperability partner with Timestep Permit Gate Enterprise VPN's. RSA referred us to a document that supported the interoperability and configuration of Timestep Permit GATE and RSA ACE server.
http://www.rsasecurity.com/support/guides/imp_pdfs/TimeStep.pdf

RSA's ACE Server is a very scalable product. RSA Security claims that a single server can support millions of users on one server by load balancing by replicating the database to another server. Replicating servers work by routing authentication requests to a faster performing server, resulting in more efficient authentication performance. RSA ACE Agent software provides this load balancing by detecting server response times and routing authentication requests accordingly. You can also define manual load balancing sequences. RSA ACE server has high Availability system support for increased failover and disaster recovery support RSA ACE Server is certified to run on HP Service Guard and IBM HACMP high availability hardware systems.

RSA is easy to implement with minimum training to end users and Administrators. Secur ID has a very intuitive administrative interface for easy administration. RSA ACE Server Quick Admin allows RSA ACE Server help desk administrators to handle approximately 80% of daily RSA Secur ID user and token management calls through a browser-based interface and Provides centralized easy and cost-effective administration. Quick Admin provides a subset of the tasks available through Remote Admin and focuses on user and token management tasks that are often performed by first-tier helpdesks. The default number of concurrent remote administration sessions supported is 32. ACE Server has very extensive logging capabilities. RSA ACE/Server administrators can maintain user records in the directory and token records in RSA ACE Server. Import and synchronization utilities let administrators bring data from the directory into RSA ACE Server and keep the data synchronized. Simplified administration with new administration tools. The RSA ACE Server can

log all transactions and user activity. You can utilize RSA ACE Server as an auditing and accounting tool and it has a report template that can be easily tailored to your needs, including activity, exception, incident and usage summaries. Filtering tools allow administrators to define which Server events to capture in both the RSA ACE Server and the operating system event logs. *See figure 2.0*

Figure 2.0
Log Filtering



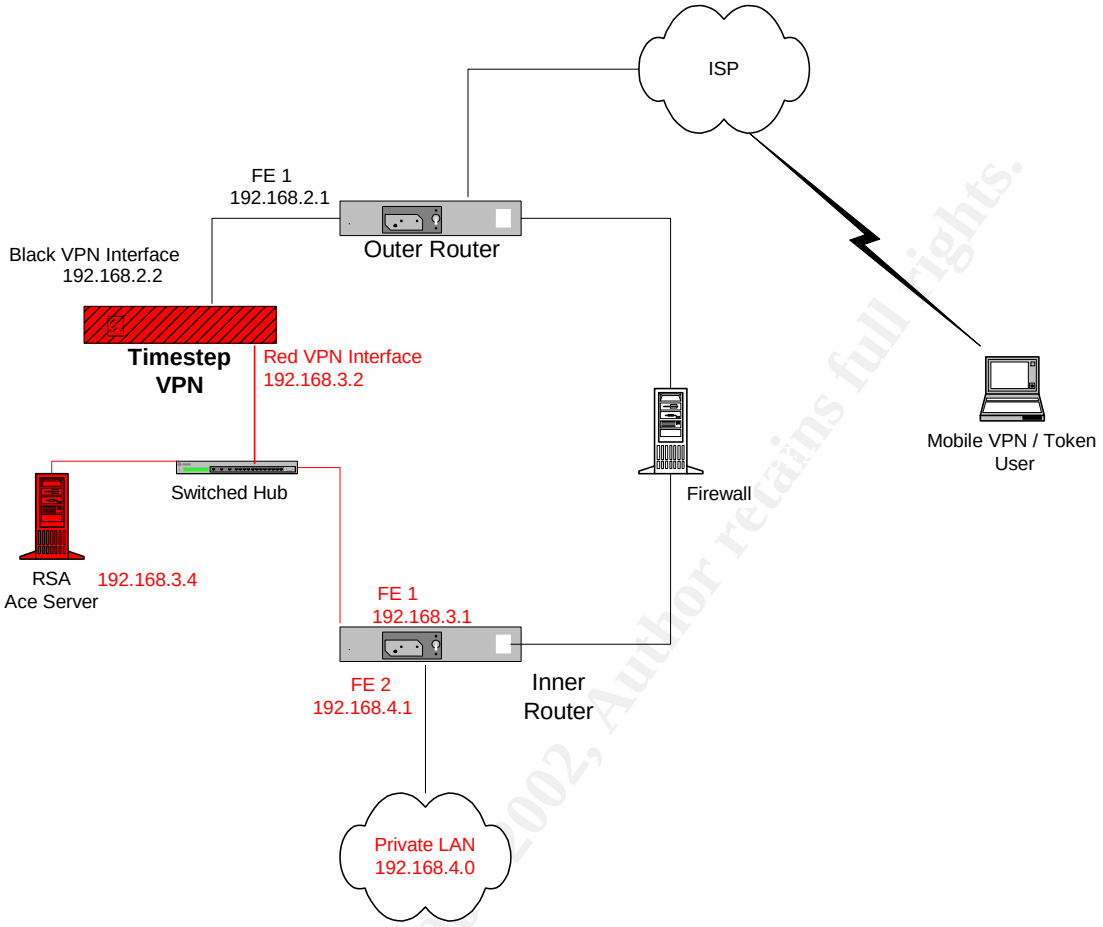
ACE server uses a two-way authentication that has a time synchronized Secur-ID card that displays a LCD screen with a string of numbers that changes every sixty seconds. This number is unique one time token and must be entered along with a 4-digit pin number. This is a typical ATM banking scenario - you combine something you know (your password) with something you have (your ATM card) to prove that you are who you say you are. A Secur ID token card comes in two form factors. *See figure 3.0*

Figure 3.0
Secur- ID card form factors

In time-synchronous authentication, both the token and the ACE server have internal clocks that are synchronized. Both token and ACE server also has a generation routine to create a random number. This is also called a seed. This seed is embedded within a token and generates a new token code every 60 seconds. The seed record is also stored within the RSA ACE Server software and generates the same token code at the same time. When the user enters the number, the server validates that this code matches its records at that point in time. If the both numbers match, the user is authenticated and granted access to protected resources.

The ACE Server was installed on the same subnet as the red side of the VPN interface and directly connected to the inner router interface fast Ethernet interface 1 (FE1) via a switched eight-port hub. *See Figure 5.0*

Figure 5.0
ACE server placement



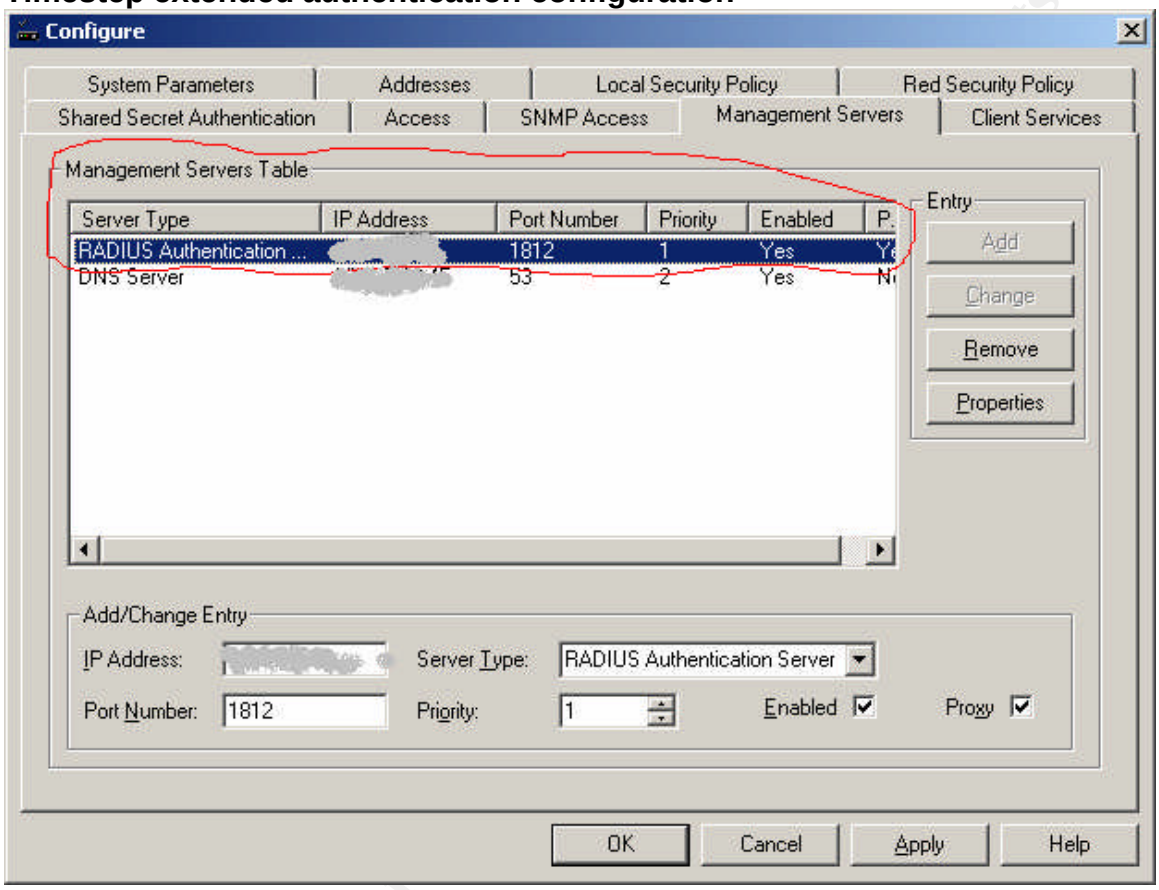
Secur ID ACE Server was installed on a Compaq Proliant DL360 Pentium 4 with 1 gigabyte of RAM running Windows 2000 server with service pack 2
http://www.compaq.com/products/servers/proliantdl360/index.html
The following list shows the minimum Windows NT and Windows 2000 hardware platform requirements for ACE Server Version 5

Single Intel Pentium 266 MHz processor
Hard disk drive with 200 MB of free space for programs, documentation, and examples.
Additional free space needed for database and log files: 1 MB per 1,000 users.
NTFS file system (not a requirement for remote administration)
Monitor display set to a minimum of 800 x 600 pixels
100 MB of physical memory + 1 MB per 1,000 users
2 times physical memory swap file

All Timestep VPN gateway's come with a remote administration utility is called "*Permit Config*." Timestep VPN gateways also have command line configuration capability from the console port. Command line interface or GUI can do most administration. In this case we demonstrate using the Permit config GUI utility. A RADIUS server must be added to the list of management servers and enabled.

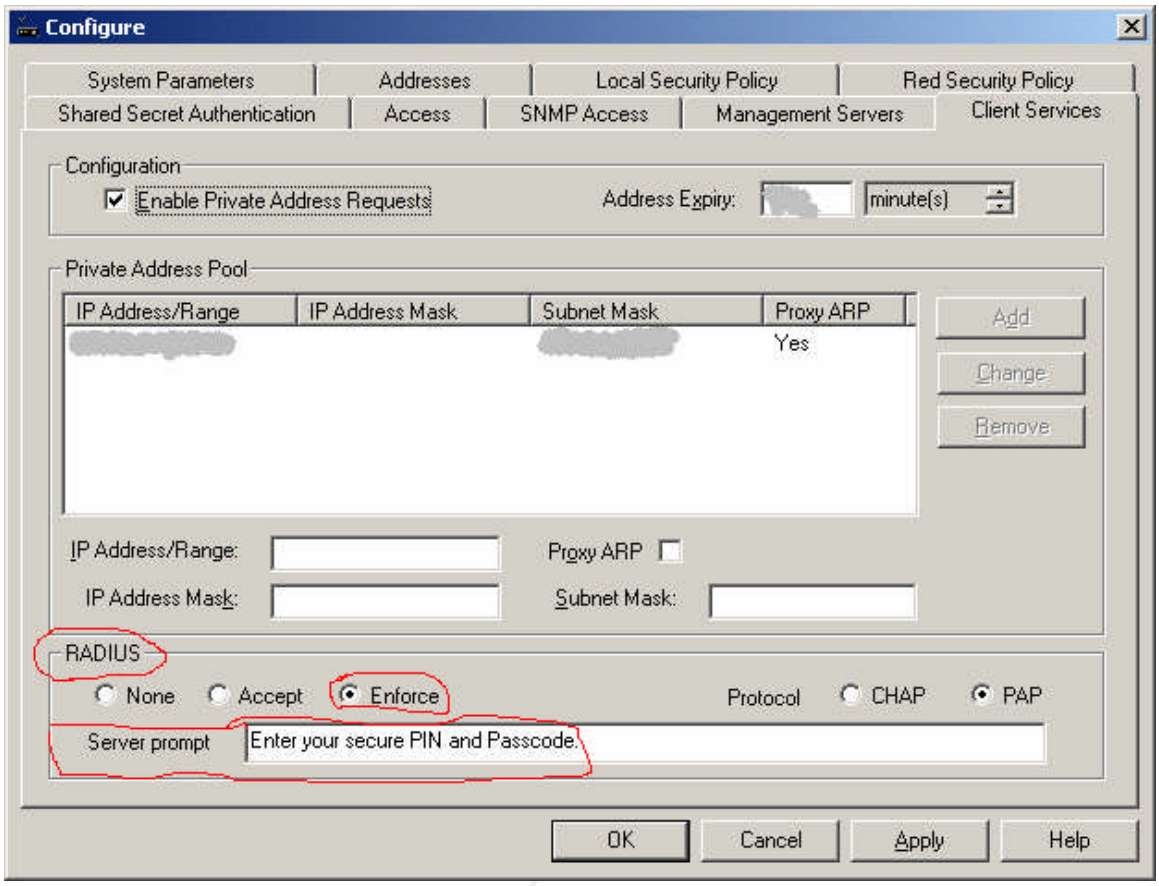
This is also where the UDP port number is configured. These RADIUS configuration settings can be found on the " Management Servers" tab. *See figure 4.0*

Figure 4.0
Timestep extended authentication configuration



In order that all VPN connections are required to use extended authentication to establish a secure tunnel, you must enable the "*Enforce*" RADIUS button. By enforcing Timestep VPN to use extended authentication, a request is sent to the RADIUS server via port 1812 forcing an extended authentication. Configuration to force extended authentication with a Timestep Permitgate can be accomplished in the Timestep Permit config utility on the "client services" tab. *See Figure 5.0*

Figure 5.0
Timestep Permit config utility enforcing extended authentication



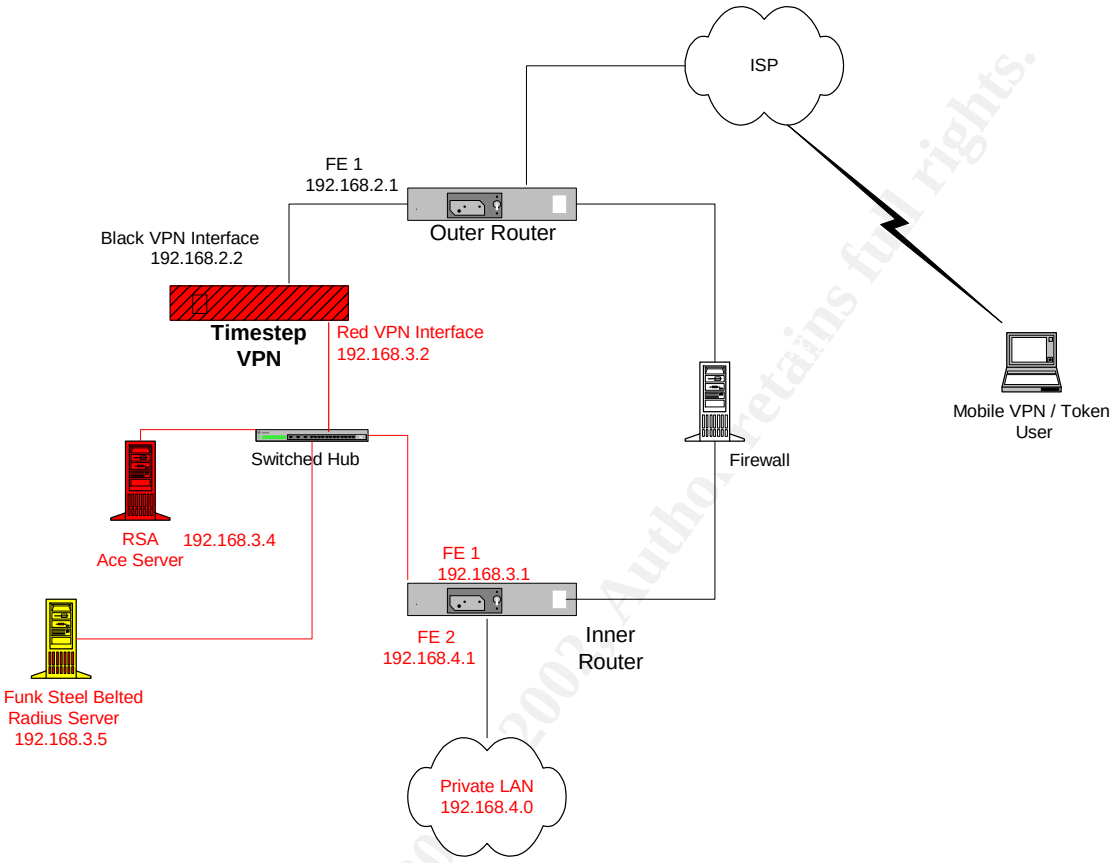
Before forcing extended authentication. VPN users were only prompt for a shared secret to gain a tunnel. Now with forced extended authentication, the user is prompt for a username, pass code, (six digit code on token display) followed by a pin number. *See figure 6.0* The user usually creates the pin number. Although the RSA RADIUS Server can be configured to allow system-generated user Pin's, this option is turned off by default in ACE server 5.0 and should never be turned on. A system-generated PIN is not encrypted when it is sent back to the user in a RADIUS packet. Because the transmission of unencrypted Pins to users on remote systems involves a clear security risk, RSA Security strongly recommends against allowing system-generated Pins for remote users who are authenticated through a RADIUS server. Normal pin transmissions use RC5 encryption went it is sent back to the user.

Figure 6.0
Extended authentication user interface

All this sounds easy right? Everything always looks good on paper, but those of us who work in the information technology field know that there is usually some kind of unexpected incompatibility issue when implementing new network architecture. When we installed RSA ACE server into our VPN architecture we discovered interoperability with Timestep VPN's and RSA ACE server 5.0. Even though RSA published interoperability configuration guide on the Timestep Permit Gate VPN. It turns out that the ACE server had problems communicating RADIUS request from the Timestep. The published interoperability report from RSA was completed with ACE server version 4. One of the changes with ACE server version 5.0 was RSA's embedded RADIUS engine.

The work around: Funks Software's Steel Belted RADIUS server has very advanced RADIUS capabilities. It can act as a proxy target server, and can forward proxy requests to other RADIUS servers. Forwarding RADIUS request is exactly what we needed. Steel Belted RADIUS server was installed on a Dell Optiplex GX150 running Windows 2000 Professional workstation. This system resides between the Timestep Permitgate VPN and the RSA Secur ID ACE Server. (*See Figure 7.0*) Funk's Steel Belted RADIUS server now takes all RADIUS request from the Timestep VPN and forwards all RADIUS request to the RSA Secur ID ACE Server, acting as a proxy. This configuration worked successfully. In addition to making the access possible, Steel-Belted RADIUS gave us more control over remote users once they're authenticated. Along with the authentication Steel-Belted RADIUS can send connection attributes what network resources the user is allowed to access, by what port, and for how the users remote session was. It can also gather accounting data describing the entire session for our records. Even though this was not part of our original configuration and budget we were still able to complete our deployment of securing VPN authentication.

Figure 7.0
Final Architecture



After: Prior to the implementation of our extended authentication with our VPN remote access. Management, and the IT security staff were very resistant to allow full deployment of remote access to the mobile workforce. Remote access was only given to a small group of users. Attending the SANS Security Essential course and implementing a stronger authentication system had a directed impact on the entire company. Future IT budgets will now include funds for additional potable computers and tokens in order to deploy remote access to the entire staff. The mobile work force can now access corporate networks services and resources with the same efficiency and functionality as if they were in the corporate office in a secure manner. For organizations employing VPN's, the technology helps improve productivity through an inexpensive conduit. The benefits of virtual private networks (VPN's) are clear why they have become very popular. VPN's enable organizations to utilize cost-effective third-party Internet transport to connect to remote offices, thus eliminating expensive dedicated WAN links and modem banks. High-bandwidth technologies like DSL, and broadband has allowed remote users to access corporate LAN's with good performance. VPN's can reduce connectivity costs while simultaneously

increasing productivity. Cisco Corporation offers an on-line calculator that calculates your savings by deploying a Cisco VPN. This application calculates the approximate savings realized by converting to a VPN solution. The calculation is based upon the least expensive Cisco solution deployable VPN Savings Calculator.

The problem for most organizations is providing a secure and scalable means of authenticating VPN users. In this case study having only a common shared secret for all users authenticating to establish a VPN connection causes some serious security risk. Before deploying RSA Secur ID we had no way to disable individual accounts. Our accounting and logging capabilities were minimal. Implementing forced extending authentication has addressed several issues. The first being authentication. Two-way authentication is virtually hacker proof. Authentication is commonly overlooked security issue with VPN's. Most VPN clients are readily available for download and can be easily obtained for hackers. Extending authentication for remote VPN users provides individual authentication. RSA ACE Server also provides better accounting and logging capabilities. If a token is loss or stolen administrators now can disable an individual user account making it transparent to other users. The extensive logging capability with ACE server allows us to perform unique individual logging this compliments the minimal logging that Timestep Permitgate offers.

What is the total cost of ownership (TCO) with the implementation of extended Authentication? Trying to figure out a correct answer for this is very difficult. Most estimates place the TCO at about 3 to 4 times the actual purchase cost of the hardware and software. In general, however, we believe that the benefit from extended authentication significantly outweighs the costs of a potential intrusion. The startup cost to implement extended authentication for 100 users was approximately $25,000. The hardware tokens that we purchased from RSA Security are good for two years. Token life can be extended for additional cost from RSA Security. Cost varies depending on the length required.

With the implementation of extended authentication, it's very hard to come up with a return on investment (ROI) figure. When protecting valuable corporate and personal information, estimates could be in the millions. A recent study from the Computer Security Institute and the FBI's San Francisco computer crime squad found 90 percent of 540 respondents surveyed detected computer security breaches during 2001. Around half of these respondents where able to come up with a dollar figure claimed a total loss of $455.8 million dollars to hack attacks.

This paper focused on VPN Authentication. Many security experts agree that authentication is the weakest link when deploying a VPN solution to the mobile work force. Authentication is one link of the chain. Microsoft recent and highly publicized hack is a good example of this. In the summer of 2000, a hacker penetrated the Microsoft Corporate network by sneaking through an authorized VPN tunnel. The attacker installed a Trojan Horse that captured keystrokes of a

authorized Microsoft employee working from home. These keystrokes were e-mailed to an address in Russia. The attacker was able to capture keystrokes that included the username and password necessary to use the VPN, and the username and password needed to authenticate to the Microsoft internal domain account. This unauthorized penetration and others could have been avoided by putting other security measures in place. Before deploying an enterprise remote access system. Personal firewalls, virus prevention, Intrusion detection systems (IDS) and vulnerability scans are just a few of many security issues that need to be addressed. Having a policy that requires remote users, whether they're working at home or on the road, to use properly configured and updated firewall and anti-virus software is important. Forget about all the security jargon, protecting a network is about preventing unauthorized use of a system, and determining accountability if this occurs. Without strong user identification, you don't have real security. Your audit trails are worthless if you can't confirm the identity of the person behind the keyboard. It seems like just about every time you open a IT trade magazine a or watch the news another system is being knocked over due to automated attacks on weak static passwords. Strong authentication should be on the top of our list of security concerns Remote Access to your private LAN can be secure if implemented properly.

References:

RSA SECURITY, RSA SecurID Tokens
http://www.rsasecurity.com/products/securid/tokens.html

Information Security Magazine TUNNEL VISION July 2000 CURTIS E. DALTON
http://www.infosecuritymag.com/articles/july00/features1b.shtml

Information Security Magazine April 2001 REACH OUT AND ID SOMEONE ACCESS CONTROL BY Mandy ANDRESS
http://www.infosecuritymag.com/articles/april01/cover.shtml

Information Security Magazine The 8 Hurdles to VPN Deployment BY CHRISTOPHER M. KING
http://www.infosecuritymag.com/articles/1999/vpn.shtml

Network Magazine 06/05/02 VPN Vulnerabilities, VPNs might be tunneling more through your firewall than you'd like BY RICK FARROW
http://www.networkmagazine.com/article/NMG20020603S0004

Information Security Magazine SPECIAL REPORT PKI: The Myth, the Magic and the Reality BY CHARLES REED
http://www.infosecuritymag.com/articles/1999/junepki.shtml

ZDNET Stop the Thief By: Brian Ploskina
http://www.caveo.com/news/htmlmags/stopthief.htm

Network Computing Securing Remote Access
by Peter Stephenson
http://www.networkcomputing.com/602/602work2.html

Creating and Implementing Virtual Private Networks: The All-encompassing Resource for Implementing VPNs
by Casey Wilson, Peter Doak
http://www.amazon.com/exec/obidos/tg/detail/-/1576104303/ref=lib_dp_TFCV/102-4288115-2342550?v=glance&vi=reader#reader-link

Funk Software Getting Twice the Security with Half the Effort
http://www.funk.com/RADIUS/Solns/unisys_us.asp

ZDNET VPN users: The weakest link By John McCormick Tech Republic July 29, 2002
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2875784-1,00.html

Microsoft, Ask Us About... Security - December 15, 2001
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/askus/aus1201.asp