VPN Project: Remote Access to a Novell Network

John Porter

VPN Project: Remote Access to a Novell Network

GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b

Option 2: Case Study in Information Security

Author: John Porter

Table of Contents

VPN Project: Remote Access to a Novell Network

Our IT department has often been praised for accomplishing much with limited resources. We often put unique, specialized solutions in place while keeping costs as low as possible. Providing top service to our internal clients has always been our primary objective, and the majority of our resources and time would be allocated to ensure our clientele's visible requirements were met. As a result, some remote services had been put in place without adequate security measures. This problem was identified and we began to focus on tightening the security of our externally accessible IT services and resources. As a senior network administrator, I became project leader and was responsible for directing our security initiative to replace our existing remote access facilities with encrypted Virtual Private Networking (VPN) technology.

Our primary network operating system is Novell Netware. It was imperative that the VPN implementation provide access to the Netware resources our clients had become accustomed to. We decided to implement this service with Cisco's 3030 VPN concentrator as the core device and leverage our existing Netware database of users for authentication. The project covered five primary areas:

- Identification of existing services.
- VPN concentrator.
- Authentication and Encryption.
- VPN Clients.
- VPN Policy.

1. Identification of Existing Services

The first task was to identify our current services and remote access issues. Our 22 IT support staff maintain and manage a complex environment which is summarized as follows:

- One head office, one district office and 35 branch offices
- Approximately 1500 staff.
- 24 File and Print Servers in a variety of locations: Novell (Netware)
- Web Servers: Windows NT, Linux (Apache) and Novell (Apache)
- Application/Database Servers: Solaris (Oracle), Linux (MySql) and NT (Access)
- Approximately 1200 Windows 95 – Windows 2000 client computers.
- Approximately 150 clients which have mobile computers.

- Remote access facilities utilized a variety of dial-up services, GroupWise web access, port mappings in the firewall, FTP, and file synchronization services such as “Novell I-Folder”.

The methods of remote access were inadequate to meet the business requirements of our users.

- Groupwise web access is convenient and functional but users find it cumbersome and lacking in a full client feature set.
- Many of our users work late hours from home or on the road. These users frequently require access to files and databases located on our internal servers.
- Some staff work exclusively from home, and have limited access to internal resources and information.
- Dial-up services are slow, limiting our client’s ability to login to access Netware services.

The methods of remote access were inadequate to meet the security requirements of our network:

- With no suitable alternatives available, users would frequently store copies of confidential material on their notebooks, external email systems and on their home computers. A user could not remotely access their “home” directory on their internal server.
- Once authenticated, dial-up services could provide unmonitored, indiscriminate access into the internal network.
- Port mappings on the firewall put our internal servers at considerable risk.
- Remote access methods were cumbersome to maintain and difficult to monitor.

2. VPN Concentrator

It was clear that the best solution would be obtained by replacing our existing methods with a Virtual Private Network. The key piece of hardware would be the VPN concentrator. We wanted to have an installation that had hardware encryption/decryption capabilities, and also supported Novell NDS. All data was to be encrypted with a strong algorithm, and it was desirable to have this process happen as quickly as possible. If we could leverage our existing database of users (Novell NDS), then we would have fewer administrative headaches both in terms of deployment, and maintenance. We looked at VPN products including:

- Novell's BorderManager
- Nortel's Contivity
- Cisco's VPN 3000 series

We chose to deploy our VPN based on Cisco's 3030 series VPN concentrator. Novell's Bordermanager product runs on a Novell server, and has software based encryption. Both Cisco and Nortel have hardware encryption solutions but neither natively supports Novell NDS authentication. However the Cisco product ties in well with another product, Cisco Access Control Server, which does support NDS authentication. We also have a number of other Cisco devices including routers and switches and had envisioned that these other devices may need to tie into our VPN setup at a future date.

A popular network magazine, Network Computing, posted a recent review that compared various VPN equipment manufacturers. The author of that review rated the Nortel Contivity device as the 'Editor's Choice', and rated the Cisco 3030 second as the 'Best Value'. "Cisco's solution came close to winning this review, partly because the 3030 and Nortel's product are almost identical in interface and features. The 3030 is also significantly less expensive…" (DeMaria). The Cisco 3030 made the best sense for our particular environment and our budget.

Interfaces

The Cisco concentrator comes with three built-in Ethernet interfaces. The outside interface would connect into our public segment, where it would be monitored by one of our Intrusion Detection Systems (IDS). The inside interface would connect directly back to our internal network. The third interface has been left unused for the time being, but will eventually provide connection to the concentrator from our management network.

Our implementation closely followed the Typical VPN Concentrator Network Installation as shown in Cisco's Getting Started Guide for Release 3.6. The VPN was setup and configured as shown in Figure 1.

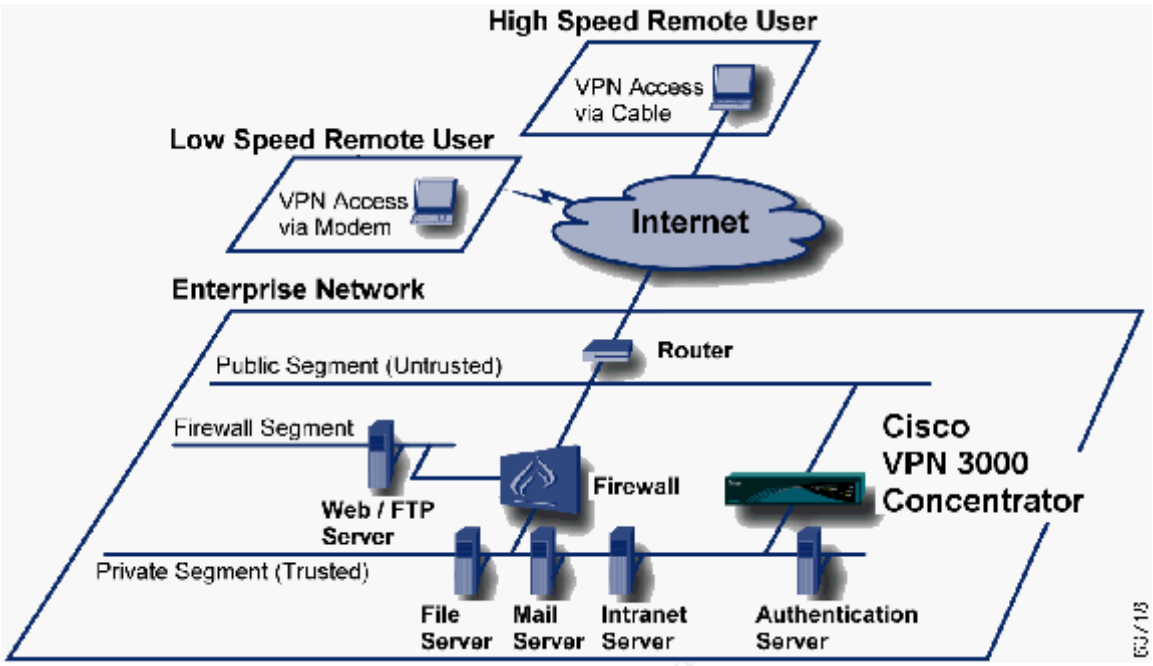

Figure 1 (Cisco Inc. "VPN 3000 Series Concentrator Getting Started", p.1-8)

Groups

A key part of our security strategy was to create user groups with varied levels of access to the internal network. If a user belongs to the 'accounting' group, she would be permitted access to the 'accounting' server, but she should not be able to access the 'executive' server.

Cisco's 3030 concentrator handled this task well, and allowed us to define the different groups with a fine level of control over each. Controls are in place to restrict users from reaching any device on our network unless specifically permitted by a network access list within the concentrator. There is also a base group that allows the default settings to be applied to other groups through optional inheritance, which simplified our global resource settings.

Timeout Values

If a user is connected to the VPN but is not actively using the system, the connection will drop after a period of inactivity. We set this timeout at one hour but we quickly found that the applications our users had running would continually send data back and forth so this timeout would never be reached. The 3030 supports another timeout for maximum time connected. We set this to be 20 hours which would logout users that leave their computers always connected.

Address Pools

Each group was given a different range of IP addresses to use while connected to the VPN. These addresses, along with the usual DHCP parameters, are provided to each client on connection. The address given to the client depends on the defined pool of addresses allowed for that user's group. This allows further security controls to be placed in routers and servers to restrict access to unauthorized services. This also gave us a method of accounting and auditing for particular groups by monitoring source IP addresses. The used addresses are unique in our network only to VPN clients, and use the unregistered Class A address space. For example:

- Accounting: 10.10.16.1 – 10.10.16.254 (mask 255.255.255.0)
- Executive: 10.10.17.1 – 10.10.17.254 (mask 255.255.255.0)
- IT: 10.10.32.1 – 10.10.32.254 (mask 255.255.255.0)
- Shipping: 10.10.33.1 – 10.10.33.254 (mask 255.255.255.0)
- Etc.

We can now summarize all VPN access with one router statement (10.10.0.0, mask 255.255.0.0). Accounting and Executive can be grouped together on their own using an address of 10.10.16.0 and a subnet mask of 255.255.240.0. This allows us to create simple access control lists in the routers to control traffic that originates from the VPN, realizing group level control in router access lists in addition to the defined group level control inherent in the 3030 concentrator.

3. Authentication and Encryption

Encryption-Security Associations

Securing our communications was the number one objective. We had to decide the methods of encryption to be used during the authentication process and also chose the encryption methods for data exchange. These parameters formed our primary Security Association (SA) for secure communications.

Encryption-SA (Internet Key Exchange and Pre-shared Keys)

With limited funding, we were not able to use tokens or certificates for authentication but we still required the security of two-factor authentication. The best remaining choice was to deploy our VPN using pre-shared keys as the first level of VPN authentication. A default group was created on the 3030 for use by the VPN users. Authentication into this group required a valid key, or password to be coded into the configuration of the VPN client. This password became our pre-shared key.

Internet Key Exchange (IKE) is the process of encryption negotiation between the client and the concentrator. We configured IKE to use a MD5 hashing algorithm to ensure data integrity and the Diffie-Hellman Group 2 (1024-

bit) algorithm to perform the exchange of the keys. Cisco recommends the use of SHA1 for hashing due to its stronger algorithm and we are currently reviewing the use of SHA1 instead of MD5.

> IPSec provides numerous security features. The following have configurable values for the administrator to define their behavior: data encryption, device authentication and credential, data integrity, address hiding, and security-association (SA) key aging. The IPSec standard requires use of either data integrity or data encryption; using both is optional. Cisco highly recommends using both encryption and integrity. Because single Data Encryption Standard (DES) was hacked in the last competition in 1999 in about 22 hours and 15 minutes with US$50,000 worth of equipment, Cisco recommends that you do not use it for data encryption. Instead, Cisco recommends the use of Triple DES (3DES). Data integrity comes in two types: 128-bit strength Message Digest 5 (MD5)-HMAC or 160-bit strength secure hash algorithm (SHA)-HMAC. Because the bit strength of SHA is greater, it is considered more secure. Cisco recommends the use of SHA because the increased security outweighs the slight processor increase in overhead (in fact, SHA is sometimes faster than MD5 in certain hardware implementations). (Halpern, p.6)

Encryption-SA (Data Encryption)

As noted in the above excerpt by Jason Halpern, the use of DES for data encryption is highly discouraged. 3DES (168bit) is the prevalent secure standard as a data encryption algorithm, and we deployed our IPSEC SA using 3DES and MD5 hashing algorithm.

The anticipated successor to 3DES, Advanced Encryption Standard (AES), has now been finalized and is available with Cisco's 3030 concentrator. AES offers even higher security than 3DES, with available bit strengths of 128 bits, 196 bits and 256 bits. We are currently testing SA's that use AES encryption.

Access Control Server

In order to provide the second level of authentication, we wanted to leverage our existing database of users. These accounts and passwords were already available in Netware Directory Services (NDS). Most of the available VPN products do not natively support authentication against NDS. Both Cisco and Nortel product lines have features to easily integrate the VPN into a Windows based user directory, but do not directly support Novell. Novell's BorderManager is a notable exception and does directly support NDS authentication.

The solution was found with a Cisco software product called Secure Access Control Server (ACS). ACS is basically a Radius/TACACS+ server that has an added benefit for Novell installations: it can proxy authentication between a Radius device and Novell's NDS. The ACS server also provides us with a central logging and administrative tool. ACS is designed to be used in a VPN authentication scenario, and has many other Cisco features that we plan to make use of such as TACACS+ for router authentication and IOS user permission definitions. ACS is easily integrated into other authentication schemes such as tokens or certificates, which is important so that we expand and revise our authentication methods if funding becomes available.

Login Process Summary

As a user attempts connection into the VPN, a number of processes occur in the course of establishing the secure IPSec tunnel. Here is a summary of the events as Joe in accounting attempts to connect to the VPN:

- Joe's VPN client and the VPN concentrator negotiate on a security association. They settle on the available option: 3DES using MD5 hashing.
- The VPN client authenticates using the default group and supplies the pre-shared key. The default group provides no access to the internal network.
- The encrypted tunnel is established. Joe is then prompted for a username and password.
- Joe's username and password are relayed from the concentrator, over to the ACS server for verification using Radius.
- The ACS server queries the Novell NDS to verify:
    - Is Joe's account found in the list of valid NDS contexts?
    - Is the password valid?
    - What NDS group membership does Joe have?
- Joe's account is located, and his password is valid. Joe belongs to the 'nwaccounting' NDS group. ACS then determines which VPN group Joe belongs in. ACS has a group mapping definition that maps his NDS group membership of 'nwaccounting' to the VPN group membership of 'accounting'.
- ACS sends the concentrator information that the Joe is a valid and authenticated user, and Joe belongs to the 'accounting' VPN group.
- The concentrator finishes authenticating Joe, and changes his group from 'default' to 'accounting'.
- The concentrator then applies all the rules and restrictions that are applicable to the accounting group. Joe is not able to reach the executive server, but has access to reach the resources he requires.

Joe is now connected to the internal network using a secure IPSec tunnel.

4. VPN Clients

The Cisco 3030 concentrator allows a number of client configurations and even supports some other vendor's clients. The 3030 includes an unlimited software client license, so there was little requirement to explore other vendor client offerings. We were in a good position to standardize the VPN clients. In our installation, there are two primary access scenarios for VPN Clients to connect:

- Cisco VPN client software on a home/mobile computer.
- Cisco VPN hardware client (Cisco 3002) connecting a remote location.

Software VPN Client

The Cisco software VPN client that is available for use with the 3030 concentrator is full of features and configurations (including a built in light version of Zone Labs firewall product), but the client is still subject to the policies defined in the VPN concentrator, the 3030 can override most client settings. This gave us the ability to centralize our policy control, a feature we quickly took advantage of.

The parameters that we defined to be pushed down from the concentrator to the software client are as follows:

- **Split-tunneling.** While a user is connected to the corporate network through the VPN, all TCP/IP communication travels through the VPN first before reaching its final destination. Clients wishing to directly access services such as SMTP services from an ISP will be forced to disconnect from the corporate network first. This will help prevent a remote cracker from leveraging a compromised user's computer to gain access to the corporate LAN.
- **Password caching** (VPN client password). We disabled the client's ability to save their password on the local computer for an automated (and insecure) login.
- **NAT Transparency.** IPSec tunnels created using either TCP or UDP connections are permitted to facilitate the home user with a small router or personal firewall appliance. This option permits tunneling from a location that uses network address translation.
- **Firewall Policy.** The firewall policy is pushed down from the 3030 to the Zone Labs firewall built into the Cisco VPN client, overriding any other firewall policies installed on the computer. The policy basically denies all traffic unless the session is initiated by the VPN client.
- **Local LAN access.** Local LAN access is currently disabled, however this is a controversial point as a number of users have local LANs with networked printers and shared directories. If this is enabled, the end result could potentially be as insecure as allowing split-tunneling.

- **Access hours.** There were no restrictions placed here, our internal users can legitimately connect at any time of day or night.
- **Idle Timeout / Maximum Connection Time.** The idle timeout was set to terminate the tunnel after 60 minutes of inactivity. However, the Novell client sends data every few seconds which resets this timer and the idle timeout is never reached. In response to this issue, I set the Maximum connection timeout to be 20 hours in order to logout users that leave their computers always connected.
- **Simultaneous connections.** The maximum number of simultaneous tunnels allowed for each user was set to be one. This would make it inconvenient for a user to share their password with other computers or people, and more difficult for a stolen password to be used undetected. The legitimate user would not be able to log in at the same time as the unauthorized computer, which would likely result in a trouble ticket bringing the issue to our attention.

Novell Access

The Cisco VPN software client had provided us with another challenge. Again, we ran into an issue with the lack of native Novell Netware support. The software client has functions and abilities to use the reuse the username and password to authenticate into a Microsoft Windows network, but no native support to log into Novell resources. Key to our security strategy was to make it very easy for our users to gain access to their server based home directories. This would allow them to save their documents on the server rather than their local hard drives, allowing us to back up critical documents and reducing our vulnerability if a computer was stolen or lost. We had to find a way to streamline this login.

To solve this issue, I wrote a batch file to automatically launch the Novell client after the VPN client connected. The batch file launches the Cisco VPN client. If the tunnel is successfully established, the batch file will then launch the Novell client. The batch file follows below:

```
@echo off
c:
rem Connect to VPN using Corporate profile
rem profile must be named 'Corporate' without the quotes
c:\progra~1\ciscos~1\vpncli~1\vpnclient connect "Corporate"
if errorlevel 200 goto ok
:failed
rem login failed, show errors
echo ERROR %errorlevel%
pause
goto done
:ok
```

```
rem login successful: show vpn status, and launch netware client
if exist C:\NOVELL\CLIENT32\LOGINW32.EXE goto win98
:winnt
%SystemRoot%\System32\loginw32.exe
goto done
:win98 will automatically launch on its own
:done
```

In addition to the lack of native Novell support in Cisco's VPN client are some other Novell Netware and general VPN complications. Netware networks using Netware version 5 and above can run on pure TCP/IP networks, but it quickly became apparent that some issues have yet to be worked out with Netware access over TCP/IP. IPSec VPNs do not support Novell's native protocol, IPX, so we had to make TCP/IP work regardless.

We already had configured, operational Novell Directory Agent (DA) and Service Location Provider (SLP) servers. These servers are required by TCP/IP Netware clients in order to locate the correct services. The Novell clients still had problems reliably locating their resources, and it became necessary to address the Novell NDS tree and servers with IP addresses instead of names, even in the login scripts! This was a fairly major operation (remember the 24 Novell servers?). Novell reports that this issue is now fixed, and we are currently testing the latest Novell and Cisco client combinations:

> Novell engineering has investigated this issue and has implemented a new mechanism to allow VPN vendors to trigger the Novell client when their tunnel has successfully initialized. Once triggered the Novell client will flush all caches so that network resources can be located. This new interface is available in client support pack 1 for both NT (4.83) and 9x (3.32) platforms. (Novell Inc. "Cannot login to Novell network through a Cisco VPN. - TID10068795")

Each remote computer was required to have virus scanning software installed and running. This would help reduce the level of risk associated with user's activities while they were not connected to the corporate network. Although the VPN concentrator has abilities to integrate with a virus management server, we have no such server and were relying on polices to ensure this requirement would be met.

Hardware VPN Client

Cisco's software VPN client was to be the primary method for users to remotely access the VPN. Cisco's 3002 hardware client was to be used in the event we required a small branch office or other site connectivity. The 3002 hardware client provides hardware encryption/decryption, providing 3DES throughput of up to 2.2Mbps. We have no current deployments of this type, but

plan to convert several small branch office connections from Frame Relay/ISDN over to the VPN using a local ISP for network service. This scenario is also ideal for off-site conferences and other events requiring network access.

The configurations for the 3002 hardware client paralleled the software client's settings and restrictions with some exceptions:

- **Password caching** (VPN client password). The 3002 client would have its static username and password coded into its local configuration.
- **Firewall Policy.** The 3002 hardware client does not support the software client's firewall policy. In fact, if a software policy was even was applied to a group that had a hardware client in it, that hardware client would not be able to connect.
- **Local LAN access.** Local LAN access is enabled with 3002 configurations.
- **Idle Timeout / Maximum Connection Time.** The 3002 was configured to connect 24/7 with no timeout values set.
- **Novell Batch Files.** No longer required in a 3002 setup as the VPN is connected prior to the computer booting up. The Novell resources are available when the computer requires them.

5. Policy

Perhaps the most important but easiest to implement task in this project, was to establish a VPN security policy to provide parameters governing the utilization of this new service. The primary goal of the policy was to bring security awareness to our clients. The policy also serves as an educational tool for our VPN's configuration. Each user is required to sign a copy of the VPN policy and solicit their manager's written authorization prior to receiving access to the VPN.

We used the VPN Security Policy available on the SANS web site as the foundation for our security policy. The availability of this great resource for public consumption is what made this critical part of our project so easy. Only minor changes were required to the original document to align the policy with the parameters we defined for this project (as indicated in the above sections). The original policy can be found on the SANS web site at: http://www.sans.org/newlook//resources/policies/Virtual_Private_Network.pdf**.**

Project Conclusion

The project's primary objective was met at the after the conclusion of the installation/configuration phase of the project and we starting bringing users

online. We were successful in tightening the security of our remote services. Our users now had a secure, encrypted means to access resources within our corporate network.

We have increased our awareness of vulnerabilities in our network, and have removed many of them. We removed the port mappings on the firewall, and reduced the dependency on dial-up remote access services. VPN users have discovered that if they save their work on the servers rather than on local hard drives, they can access that information from work, home or on the road which has reduced the amount of confidential material stored on vulnerable hard drives. We have removed other remote file access services such as FTP and I-Folder, as they have been made redundant by the VPN.

Staff are much happier as they can now use the full version of Groupwise from home and they are impressed with the speed and improved capabilities provided by the VPN. The benefits to the users have made it easier to implement our new policy and tighter restrictions. IT staff and managers are pleased with the enhanced security of our new service. We can all sleep easier at night, except for that accounting guy that connects from home and works until 3:00 AM!

Our remote access security has been substantially improved but we have more work left to achieve. The VPN has yet to be deployed to all staff that work on the road, so there is some continued dependence on dial-up services. Users still occasionally save critical material on hard drives and new features and technologies such as AES encryption will have to be examined and incorporated into the VPN if found viable. We still have our initial problem: insufficient resources and control mechanisms to prevent further security holes. Implementing change control procedures will have to be our next security project. Nevertheless, the VPN project has been an outstanding success.

List of References

DeMaria, Michael J. "Contivity Captures VPN Crown". March 18, 2002. http://www.networkcomputing.com/1306/1306f22.html (December 08, 2002)

Cisco Systems, Inc. "VPN 3000 Series Concentrator Getting Started". Release 3.6. August 2002. http://www.cisco.com/application/pdf/en/us/guest/products/ps2283/c1692/ccmigration_09186a00800b4811.pdf (December 08 2002).

Halpern, Jason "SAFE VPN: IPSec Virtual Private Networks in Depth". September 08, 2002. http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8bc.shtml (December 08, 2002)

SANS Institute (Michele Crabb-Guel, Director, SANS Security Policy Project). "VPN Security Policy**"** http://www.sans.org/newlook//resources/policies/Virtual_Private_Network.pdf (December 08, 2002)

Cisco Systems, Inc. "Data Sheet - Cisco Secure Access Control Server Software for Windows". Version 3.1 http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_data_sheet09186a00800887d5.html (December 08, 2002)

Cisco Systems, Inc. "VPN 3000 Series Concentrator Reference Volume I: Configuration". Version 3.6 http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_6/config/index.htm (December 08, 2002)

Cisco Systems, Inc. "VPN Client Administrator Guide, Release 3.6". Version 3.6 http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_6/admin_gd/index.htm (December 08, 2002)

Novell Inc. "Cannot login to Novell network through a Cisco VPN. - TID10068795". October 29, 2002 http://support.novell.com/cgi-bin/search/searchtid.cgi?/10068795.htm (December 08, 2002)