Global Information Assurance Certification Paper

GSEC PRACTICAL ASSIGNMENT
Version 1.4c, Option 1

Configuring a Cisco PIX 515 to use multifactor authentication of a remote user VPN utilizing pre-shared keys and RADIUS

By Jason Brown
January 28th, 2005

Table of Contents

1.0 Abstract

The purpose of this paper is to configure a Cisco PIX 515 Firewall to use multifactor authentication, pre-shared keys and RADIUS, when authenticating users connected through a Cisco or Microsoft VPN client. Multifactor authentication has become an essential need for any business that requires their data to be secure. This paper will show that utilizing both pre-shared keys and RADIUS to authenticate users is both a low cost and effective solution.

First we will discuss the key features and protocols of VPNs. Then both the Cisco Secure VPN and Microsoft clients will be examined. Next we'll configure the PIX firewall to allow for both types of authentication from both clients. Then we will take a look at IAS on the Windows server.

1.1 Environment Overview

Mainstream software and hardware platforms were chosen for the environment of this paper. By choosing such widely used and available items, it is thought that the information contained within will apply to the majority of the small to medium sized businesses.

- The hardware components that we will be using:
  - Dell PowerEdge 2650
    - Windows Server 2000 Standard, Service Pack 4
  - Dell Dimension 2400
    - Windows XP Professional, Service Pack 2
  - Cisco PIX 515
    - OS Version 6.3(4) with 3DES

- The software components that we will be using:
  - Cisco Secure VPN client version 4.6.00.0049
  - Microsoft PPTP/L2TP VPN client included with Windows XP
  - Internet Authentication Service included with Windows 2000

- The layout of the environment described from hereon in.

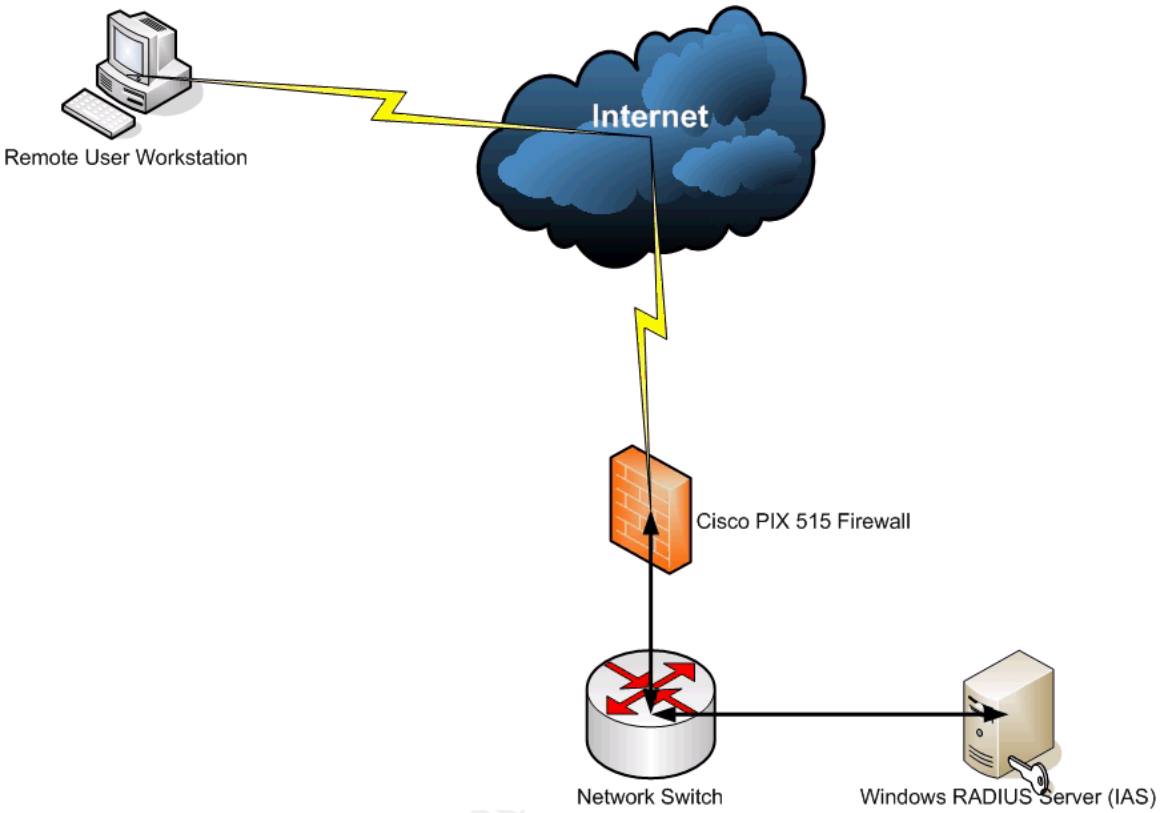

Diagram 1A

2.0 VPN Overview

A VPN typically uses the Internet and tunneling protocols to send data from one address through the tunnel to a receiving address. It is implemented through software on a client workstation and a VPN gateway at the destination network. Depending on the encryption and authentication methods used, this can be either a very secure connection or a huge security risk. A VPN is most widely used as a secured connection between two devices over an unsecured network (like the Internet). The VPN tunnel is secured by encrypting and encapsulating the data packets as data within another packet. The way we ensure that any given packet has not changed from the point where it leaves the client workstation to the VPN gateway is by its message digest. The message digest is a representation of text in the form of a single string of digits created using a process called hashing. This hash is a "one way" function which means it is nearly impossible to derive the original text from the string without the proper algorithm and key. The algorithm and key are shared only between the client and gateway. The client then repeats the same calculations on the return packet and compares that with the message digest it sent on the previous packet. If the two are the same, the packet was not altered. By encapsulating and verifying the data we can be sure we have a secure virtual tunnel for the information to travel through.

Different protocols are used by vendors to create these tunnels. IP Security (IPSec) has two main protocols – Authentication Header (AH) and Encapsulation Security Payload (ESP). AH makes sure the data has not been changed but does not encrypt the data. This is usually used if you want to make sure your data gets back and forth but don't care that it can be caught and read. ESP performs the same functions as AH but also allows for encryption. The Internet Key Exchange (IKE) protocol derived from the Internet Security Association and Key Management Protocol (ISAKMP) and Oakley standards is frequently used to authenticate IPSec connections and establish encryption keys.

Microsoft has implemented its own algorithms and protocols to support PPTP/L2TP. Microsoft has used multiple authentication and encryption methods in the past. Their most recent versions of authentication protocols include Microsoft Challenge-Handshake Authentication Protocol (MS-CHAPv2) and Extensible Authentication Protocol (EAP). MS-CHAPv2 is a revision of the original MS-CHAP (renamed to MS-CHAPv1). This revision fixed quite a few vulnerabilities found in the original protocol. EAP is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

Microsoft uses the Microsoft Point to Point Encryption protocol (MPPE) for its encryption method. As with the older authentication protocols, the older MPPE protocols had some deficiencies. The most recent version has significant changes including using a unique hash key is used in each direction. The older versions did not have this. This allowed hackers to launch an attack by XORing the two streams against each other and then deriving the key.

The key to a secure connection is not only what authentication and encryption methods you use but in what way. The more layers of defense you have against unauthorized intrusions, the better off you are to keep your data protected. For medium to small businesses who need extra layers but don't have the budget to pay for it, Microsoft's solution is easy and affordable. IAS comes as an optional service in Windows 2000 and almost every Microsoft OS comes with the PPTP/L2TP client. Combine that with pre-share keys on the PIX, and you have added an extra layer of defense at a very affordable cost.

2.1 Cisco Secure VPN Client Overview

The Cisco Secure VPN client creates a secure and reliable connection to the VPN gateway. Cisco learned from the deficiencies that Microsoft encountered and improved on security with their VPN solution. Using the Cisco secure VPN client in combination with a Cisco PIX firewall, you have total control over the encryption, authentication, group, and hashing methods used. This allows for the administrator to decide how secure they want the VPN to be. The newest version of the Cisco Secure VPN client allows the client workstation to establish an IPSec tunnel to a VPN gateway with any number of authentication methods.

A connection within the VPN client must be created. This will allow the client and the gateway to agree on the rules of the conversation. These rules include what authentication to use, timeouts, certificates, what Internet Protocols to communicate over, etc.

Diagram 2.1A shows the first tab in the client setup. As mentioned earlier, we will be using two forms of authentication. The first form of authentication is the group name and password. This group name and password has to match a group name and password listed on the VPN gateway. Without this, the first part of the two part authentication will fail.

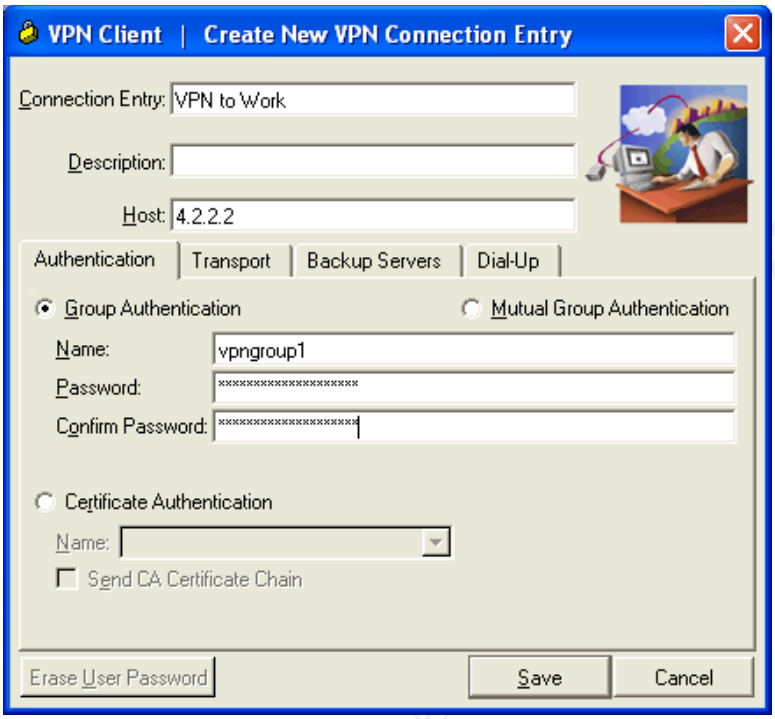

Diagram 2.1A

Diagram 2.1B shows the second and last tab pertaining to this paper. This tab shows what protocols to connect with (TCP or UDP), whether or not allow local LAN access when connected and the number of seconds for the peer timeout.

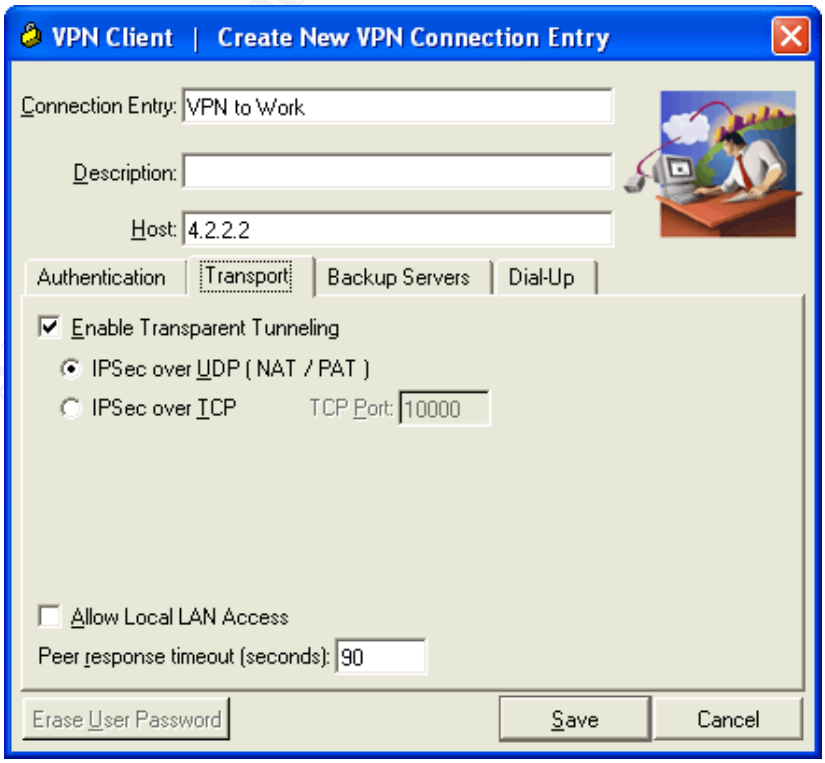

Diagram 2.1B

2.2 Microsoft VPN Client Overview

Microsoft has worked to improve their VPN client and in recent years it has seen some significant advances. Moving from protocols that didn't support encryption (PAP & CHAP) to protocols that did (MS-CHAP & EAP) and then improving protocols to make them secure (MS-CHAPv2). While there are still security reasons for not using Microsoft's VPN client, it is arguably the most popular VPN client with users. This is mainly because it is included with Operation System and doesn't require any additional software. It is easy to setup, easy to maintain, and doesn't cause problems within the OS that a lot of the other clients can. Unfortunately some of the upsides to the users of the client are downfalls to the administrator. You are able to configure a VPN with no encryption and no authentication. If you do not have the gateway configured correctly and a client connects in this way, you have opened up your network for the world to see.

In Diagram 2.2A you will see the security tab for a VPN connection. For this paper, we will only look at the security tab. By default, the tab requires data encryption. The client, in this configuration, will try to connect at the highest level of authentication and encryption and then work its way down.

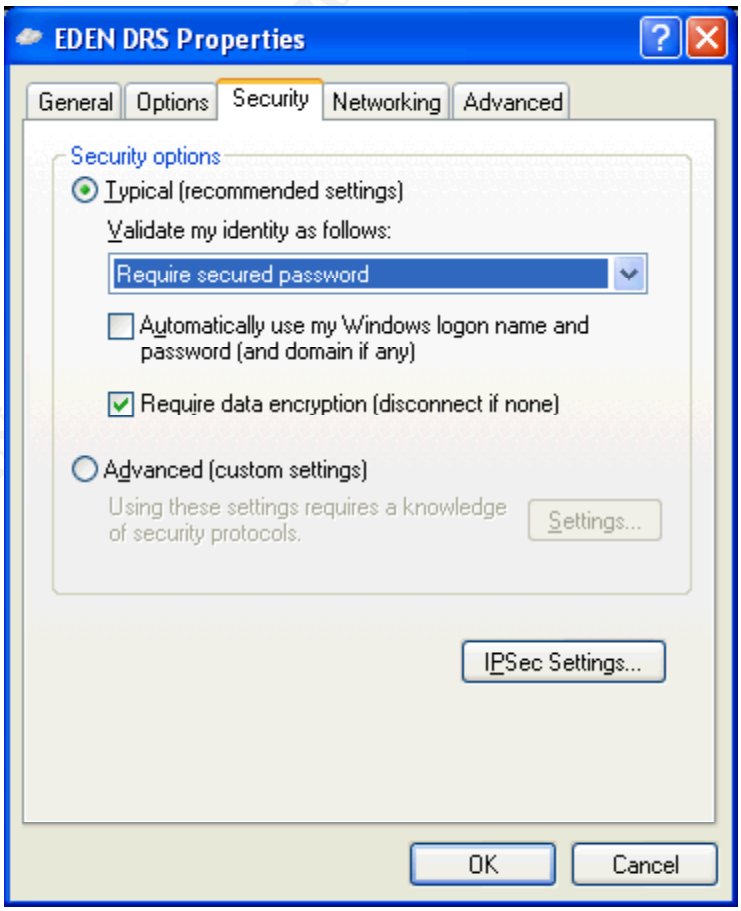

Diagram 2.2A

Diagram2.2B shows the IPSec setting where you can set a pre-share key for this VPN connection. This is the first part of the multifactor authentication.

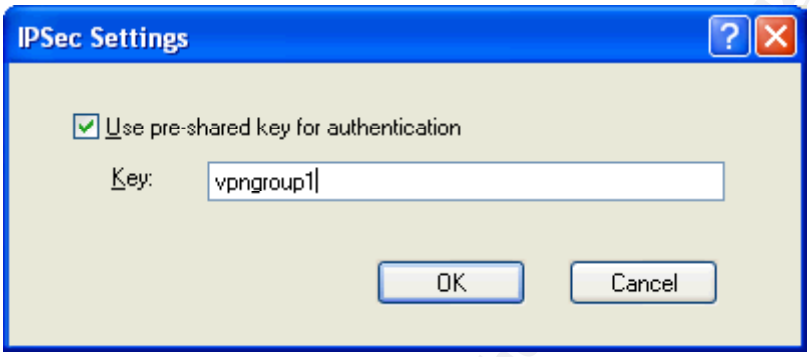

Diagram2.2B

If you were to choose Advanced (custom settings) and click the 'Settings' button, you would see the screen in Diagram2.2C. This screen allows you to choose how strongly you want the client to decide on encryption. The default is 'Require Encryption' but you can choose everything from 'No encryption, disconnect if it is required' to 'Maximum Encryption, disconnect if server declines'. You have the option of either EAP or choosing specific protocols. If not using EAP, MS-CHAP v2 is the most secure protocol. Unfortunately, MS-CHAP (version 1) is the most widely used for backwards compatibility with older clients. PAP, SPAP, and CHAP do not support encryption and should not be an option if you are transmitting any sensitive data.

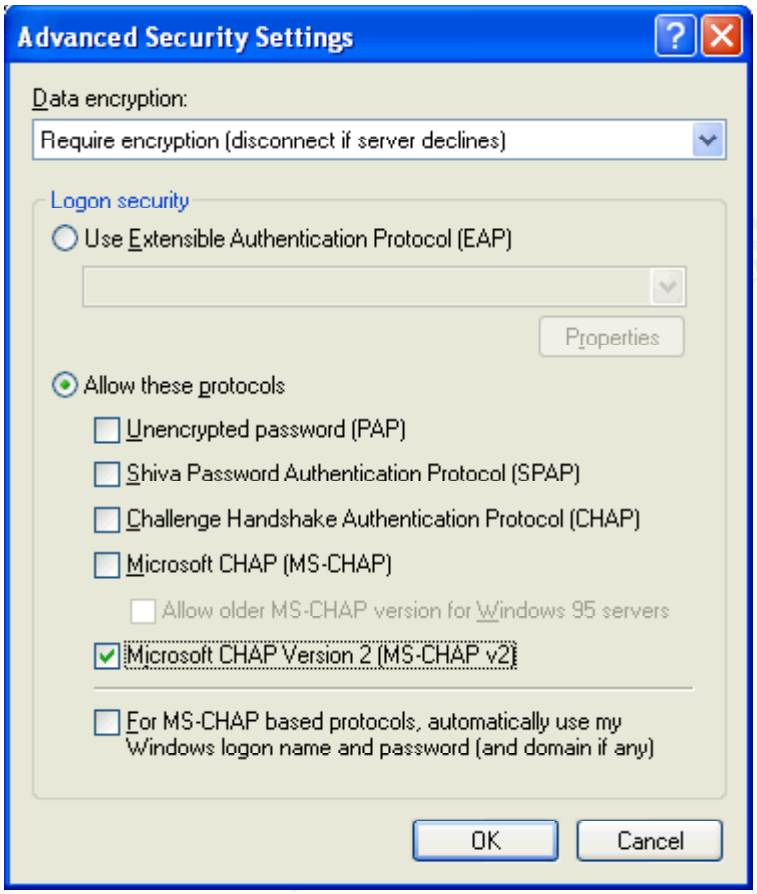

Diagram2.2C

3.0 Cisco PIX 515 VPN Configuration

The Cisco PIX 515 Firewall will act as a gateway and can push the required settings such as encryption, group, key lifetime, etc. to the client during the initial connection. This allows you to set the gateway to whatever security level you desire. In the following pages you will see what commands are needed in order to terminate the VPNs on the PIX and perform a multifactor authentication.

Using IKE the gateway can perform authentication of peers, negotiation, and establish the keys used for encryption for IPSec. IKE has two phases. During the first phase the client is authenticated and a secure tunnel is setup between the client and gateway. Phase one can operate in two modes, “main” or “aggressive”. The main mode is default on the PIX and is more secure. The aggressive mode could be used if a small performance boost was needed as it only has two two-way exchanges.

Main mode has three two-way exchanges between the client and the gateway.

- First exchange: The algorithms and hashes used to secure the IKE communications are agreed upon in matching IKE SAs in each peer.
- Second exchange: Uses a Diffie-Hellman exchange to generate shared secret keying material used to generate shared secret keys and to pass nonces.
- Third exchange: Verifies the other side's identity. The identity value is the IPSec peer's IP address in encrypted form. The main outcome of main mode is matching IKE SAs between peers to provide a protected pipe for subsequent protected ISAKMP exchanges between the IKE peers. The IKE SA specifies values for the IKE exchange: the authentication method used, the encryption and hash algorithms, the Diffie-Hellman group used, the lifetime of the IKE SA in seconds or kilobytes, and the shared secret key values for the encryption algorithms. The IKE SA in each peer is bi-directional.

The purpose of phase two is to negotiate IPSec SAs to set up the IPSec tunnel. Phase two only has one mode - “quick mode”. It negotiates a shared IPSec policy, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec SAs. The keys used for these Sas and tunnels are different than the phase one keys and are independently configured.

There are a few lines we need to add to the PIX in order to connect. While I prefer using the names command which maps names to IP addresses for easier reading, for this paper I will use the IP address itself.

These lines are used for the creation of the phase one tunnel for IKE.

```
isakmp policy 5 authentication pre-share
isakmp policy 5 encryption 3des
isakmp policy 5 hash md5
isakmp policy 5 group 2
isakmp policy 5 lifetime 86400
isakmp enable outside
```

Each line consists of the “isakmp policy” statement, the priority number (ranging from 1 to 65534) and the command. From these lines we can see that the gateway is expecting to authenticate with a pre-share key. It is using triple des, hashing with MD5, using group 2 (1024-bit Diffie-Hellman), and has a lifetime of 86400 seconds (24 hours). The last line tells the PIX to enable these settings on the outside interface or the interface facing the internet.

The next step is to create a DHCP scope of IP’s to assign to the incoming connections. The line to create this consists of the ‘ip local pool’ statement, the name of the pool, and the range of the pool.

```
ip local pool vpnpool 192.168.1.200-192.168.1.254
```

Most likely you do not want the PIX to NAT/PAT the IP addresses in the VPN pool. To disable this, you must add the IP's to a NAT 0 (zero) group. This command consists of the 'nat' statement, the interface, the group, and the range.

```
nat (inside) 0 192.168.1.0 255.255.255.0
```

3.1 Cisco Secure VPN Client

The next step is to protect the data and this is where dealing with the Microsoft and Cisco client differs. The clients differ in the commands they are using and the PIX differs in the commands to accept the clients.

A transform set, or the group of transforms to be used to encrypt text, needs to be setup using the crypto ipsec statement. This consists of the statement, the command, the transform-set name (vpnset for this example) and up to three individual transforms, one AH and two ESPs.

```
crypto ipsec transform-set vpnset esp-3des esp-md5-hmac
```

The following transforms are supported by the PIX –

esp-des	ESP encryption with 56 bit DES
esp-3des	ESP encryption with 168 bit triple DES
esp-md5-hmac	ESP with MD5 authentication
esp-sha-hmac	ESP with SHA authentication
ah-md5-hmac	AH with MD5 authentication
ah-sha-hmac	AH with SHA authentication

The next step is to create a dynamic crypto map. Dynamic crypto maps are policy templates used when processing negotiation requests for new security associations from a remote IPSec peer. In this I am using the crypto dynamic-map statement, naming the map, giving it a priority, and assigning it the transform-set created above.

```
crypto dynamic-map VPNMap 5 set transform-set vpnset
```

Then the dynamic crypto map needs to be bound with a static crypto map. Using the crypto map statement we name the static map, give it a priority, tell it to use IKE (ipsec-isakmp), specify it is for a current dynamic map and the name of the dynamic map.

```
crypto map StaticVPNmap 5 ipsec-isakmp dynamic VPNMap
```

Now for the two factor authentication to work, we have to setup the RADIUS server using Authentication, Authorization, and Accounting

services (AAA). An AAA server is a database that will be checked by the PIX to complete the second authentication. In this case, we will be using RADIUS as the protocol to communicate with the Windows 2000 Server running IAS and using Active Directory as its authentication database.

```
aaa-server ias-server protocol radius
aaa-server ias-server max-failed-attempts 3
aaa-server ias-server deadtime 10
aaa-server ias-server (inside) host 192.168.1.2 timeout 10
```

These lines show the aaa-server statement, the alias of the aaa-server, and the separate commands. The aaa-server is using radius, will allow you up to three attempts to login before disconnecting, the amount of minutes before declaring the aaa server unresponsive, and the host to authenticate with.

With that set, we can finish the crypto commands and tell the PIX what aaa-server to authenticate to and apply the crypto map to the outside interface.

```
crypto map StaticVPNmap client authentication ias-server
crypto map StaticVPNmap interface outside
```

The final set of information the PIX needs in order to terminate IPSec VPNs is the actual vpngroup information.

```
vpngroup VPNUsers address-pool vpnpool
vpngroup VPNUsers dns-server 192.168.1.3
vpngroup VPNUsers idle-time 1800
vpngroup VPNUsers password ********
```

In these commands the group name is defined (VPNUsers) what address-pool to use (vpnpool), the dns-server, timeout, and the group password. You can also assign secondary dns servers, wins servers, etc.

The last step is to allow ipsec connections to come into the PIX.

```
sysopt connection permit-ipsec
```

3.2 Microsoft VPN Client

In order to configure L2TP clients to connect to the PIX, a few additional statements must be entered in.

```
vpdn group 1 accept dialin l2tp
vpdn group 1 ppp authentication mschap
vpdn group 1 client configuration address local vpnpool
vpdn group 1 client configuration dns 192.168.1.3
vpdn group 1 client authentication aaa ias-server
```

The vpdn statement is fairly straightforward. Using the 'vpdn group' statement we are assigning a group (1) and then allowing the group to accept l2tp. The group is allowed to authenticate only MS-CHAP. Other protocols can also be entered in such as PAP and CHAP. It will be using the same pool and DNS as the Cisco client VPN connections. The vpdn statement can also support the secondary DNS and WINS servers. The last line states that, like the Cisco IPSec connections, after the pre-share key, the user with authenticate to the ias-server.

Next we have to do enable the vpdn function to the outside interface and allow the L2TP connection to come into the PIX.

```
vpdn enable outside
sysopt connection permit-l2tp
```

Below is a configuration of a single authentication PPTP connection. Note the differences between the security enhancements with the IPSec VPNs and the PPTP VPNs.

```
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp encryption mppe 40
vpdn group 1 client configuration address local vpnpool
vpdn group 1 client configuration dns 10.128.64.200
vpdn group 1 client authentication aaa ias-server
vpdn group 1 pptp echo 60
vpdn enable outside
sysopt connection permit-pptp
```

You'll notice that since IPSec is not controlling the encryption, this has the additional 'encryption' line. This can be set to 40bit, 128bit, or auto for client negotiation. This is not as secure as the L2TP option because there is no two factor authentication. The IPSec key is not an option in the Microsoft client when the connection is setup as PPTP only.

4.0 RADIUS (IAS) Configuration

The IAS configuration is simple and straightforward. IAS can be installed through add/remove programs on any Windows 2000 server. It is a free service that acts as a RADIUS server for the PIX firewall. On the IAS server you setup the PIX as a client and assign policies to it. Diagram 4.0A shows the main clients screen of IAS server.

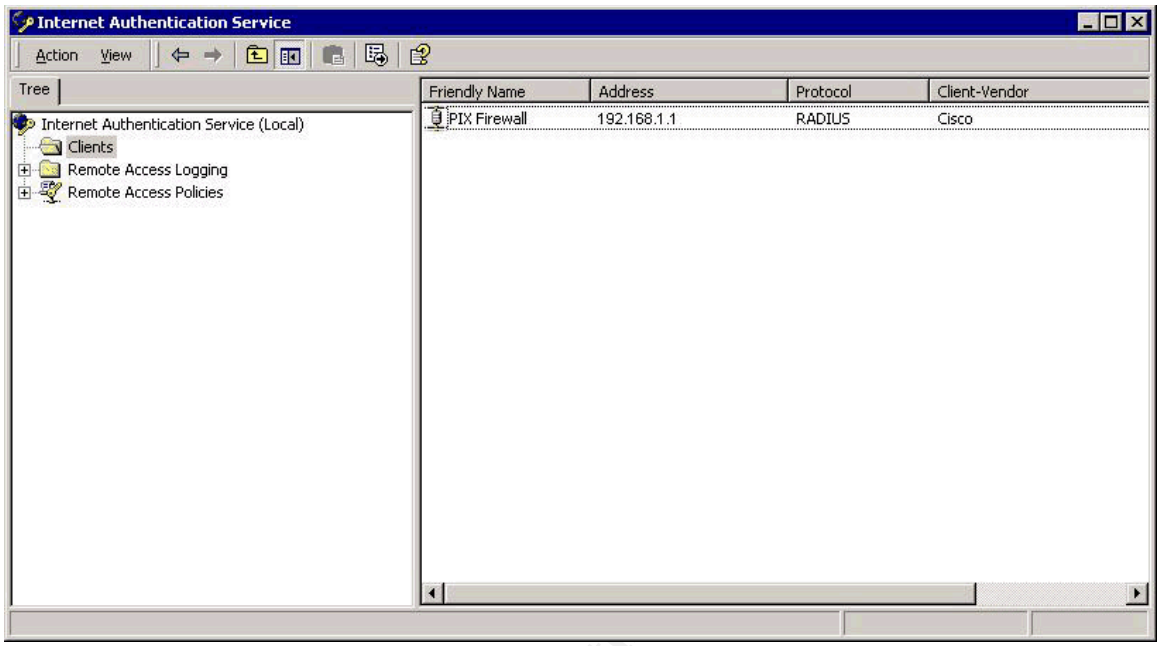

Diagram 4.0A

The settings for the client are shown in Diagram 4.0B. The client is assigned a friendly name; the IP Address is entered as well as the vendor and the pre-share key.

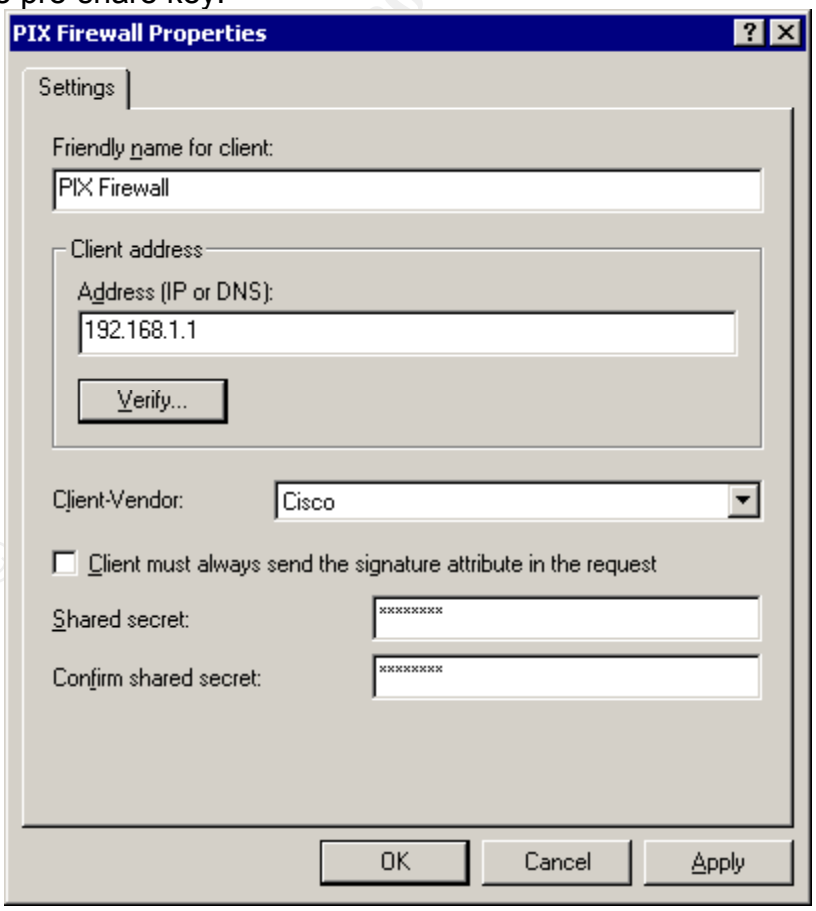

Diagram 4.0A

You can then assign policies to anyone connecting to the IAS server. You are able to pick from any of the following settings. From these settings you can allow only the PIX to connect and only allow users belonging to certain Windows groups to authenticate.

Called-Station-ID	Phone number dialed by user
Calling-Station-ID	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (IAS only)
Client-IP-Address	IP address of RADIUS client. (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS. (IAS only)
Day-And-Time Restrictions	Time periods and days of the week during which user is allowed to connect
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originating the request (IAS-only)
NAS-IP-Address	IP address of the NAS originating the request (IAS-only)
NAS-Port-Type	Type of physical port used by the NAS originating the request
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used
Windows-Groups	Windows groups that user belongs to

You are able to lock down what tunnels are allowed, the time and days they can connect, and what protocols they use.

5.0 Conclusion

Defense in depth is the key to maintaining security in any instance. This is especially essential when clients are connecting to your internal network while traversing the internet. Having multiple layers between you and the general public is crucial when sending confidential data through the VPN tunnel. While some options can strain the budget of a small to medium sized company, solutions such as the one stated in this document give you security without the financial headache.

6.0 References

Bruce Schneier. 1999. Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). http://www.schneier.com/paper-pptpv2.html

Cisco Systems Inc. "Configuring IPSec and Certification Authorities" http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/ipsecint.htm (July 22nd, 2004)

Cisco Systems Inc. "Managing VPN Remote Access" http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/basclnt.htm (October 29th, 2004)

Cisco Systems Inc. "Configuration Examples for Other Remote Access Clients" http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/vpncl11.htm (July 22nd, 2004)

Microsoft "IAS Authentication" http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/windows/2000/server/reskit/en-us/intwork/inbc_ias_IRHI.asp 2005

Mason, Andrew. CCSP Self-Study : Cisco Secure Virtual Private Networks (CSVPN) (2nd Edition) Indianapolis: Cisco Press, 2004

Quiggle, Adam. Implementing Cisco VPNs Osborne Media: McGraw-Hill, 2001

Deal, Richard. Cisco(R) PIX (TM) Firewalls Osborne Media: McGraw-Hill, 2002