GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Implementing “Dual-Sided” VPN’s
Kenneth Boudreaux
September 21, 2001
Version 1.2e

Introduction

In my current position, I am required to provide secure communications to all sites where our project servers are located. Since much of our site-to-site communications are provided by public networks, a solution had to be found that could use a public network for data communications and that could satisfy the security requirements for data transmission that were given.

Several options were evaluated. The first option that was considered was a Leased Line to all sites with servers. Since each server required connectivity to several other sites, the number leased lines was enormous. This was not only expensive, but no guarantee of the security of the data could be achieved. Although leased lines are generally physically secured, there are several vulnerabilities that were discovered. There were concerns that employees or phone company technicians could get access to confidential data by gaining access to the wiring closet. Once inside the wiring closet, the clearly marked leased lines make easy targets. Leased lines transmissions can also traverse satellite, microwave, and other radio frequency links, which are also easy targets for the determined hacker. Frame Relay and ATM connections were also evaluated, but were found to have similar security risks and costs.

Many of the sites in question already had a “Tail Circuit” or leased line that terminated at a central location based on the region that the site was in. These “Tail Circuits” terminated behind a single firewall. We needed to find a way to leverage the existing “Tail Circuits” in a secure manner. The addition of a Virtual Private Network or VPN was chosen. This solution used the existing infrastructure, provided the security we needed, and it was reasonably priced. Problem solved, right? Almost. This solution only provided secure communications from a host behind a firewall, through a leased line behind that same firewall, to another site that is also behind that same firewall. This did not provide secure communications from a remote site outside the firewall to a “Tail Circuit” connected site behind a firewall. There was one restriction in place that prevented us from creating a VPN connection from the remote site to the local site. The restriction was that no VPN ports or protocols were to be allowed to pass through the firewall. This presented a problem. We needed a way to create a VPN connection from one site, through a remote VPN device in parallel to a firewall, to a final VPN device at the destination site. The only way to accomplish this was to install a “Dual-Sided” VPN.

A “Dual-Sided” VPN consists of a minimum of four VPN devices. As seen on Diagram 1, the VPN devices are labeled VPN 1 through VPN 4. VPN 1 sits in front of our main server, Server 1. Data must travel from Server 1 to Server 2, which sits behind VPN 4. To facilitate this, a series of VPN Tunnels must be created. The first tunnel or Secure Association (SA) is created between VPN 1 and VPN 2. When traffic arrives at VPN 1 it is encrypted and sent to VPN 2. When the encrypted traffic is received at VPN 2, it is decrypted and forwarded to VPN 3. VPN 3 receives the traffic, then creates a tunnel with VPN 4 and forwards the traffic to VPN 4. When the traffic is received at VPN 4, it is decrypted and forwarded to Server 2, and the process is complete. Data communications between Server 1 and Server 2 are encrypted in all segments except on Network 2, which lies between VPN 2 and VPN 3. We agreed that this was an

© SANS Institute 2000 - 2005 Author retains full rights.

acceptable risk since VPN's 2 and 3 are directly connected and can be placed in a locked wiring closet or rack that is only accessible by authorized network personnel. It is highly recommended that these two VPN devices not be installed in a building wiring closet, or other closet that does not have controlled access. Unauthorized physical access to these devices would compromise the integrity of the entire VPN. An intruder would simply need to install a hub, set an IP address on a host machine, and plug the VPN devices into the hub. The intruder would then have unrestricted access into the VPN.

As an additional means of security, an Intrusion Detection System could be placed between VPN 2 and VPN 3. This would give the network administrators a means to detect penetrations inside the VPN. Since server-to-server communication ports and protocols are known, communications on any other ports or protocols could be detected, assumed to be a security breach, and logged. Such penetrations would most likely originate from one of the servers inside the VPN. That being said, the attacker would have most likely gained access to one of the project servers. Thus, it is crucial that this activity is detected so that appropriate actions could be taken to block further intrusions and to determine where the intrusion was originating from and who the intruder was.

With that said, this white paper was written to provide a step-by-step procedure to create a "Dual-Sided" VPN. The VPN devices used in our configuration are Alcatel (TimeStep) PERMIT/Gate models 7132 and 7134. The only difference between the two devices is throughput. The 7132 is 2Mbits/second, and the 7134 is 10Mbits/second. Otherwise, configuration of the two devices is identical.

The Alcatel brand of VPN devices uses the IPSec protocol suite to create Secure Associations or Tunnels. The two functions that IPSec defines are data encryption and data integrity. Towards that end, the Authentication Header (AH) protocol provides authentication and integrity without encryption and the Encapsulating Security Payload (ESP) protocol provides encryption in addition to authentication and integrity. Tunnel negotiation is provided by the Internet Key Exchange (IKE) protocol, which provides authenticated keying material for Security Associations (SAs) in a protected manner.

Since the focus of this paper is the creation of a "Dual-Sided" VPN, only brief definitions of the components required for the IPSec protocol will follow. More in depth explanations of the key configuration features of the Alcatel (TimeStep) VPN gates is also included to give readers some insight into the configurations that have been made.

I will start by defining some terms that will be used throughout this paper. Some of the terms are common to all VPN's, and others are specific to the Alcatel brand of VPN devices.

Secure Virtual Private Network (VPN) – an enterprise network that traverses a shared or public infrastructure, like the Internet, and establishes private and secure connections over an untrusted network, with geographically dispersed users, customers, and business partners.

IPSec – an Internet Draft Standard developed by the Internet Engineering Task Force (IETF) to ensure secure transfer of information across a public IP network.

Tunnel – a connection between two IPSec devices that uses the negotiated security method to encapsulate and encrypt entire IP packets for secure transfer across a private or public internetwork.

© SANS Institute 2000 - 2005 Author retains full rights.

Secure Association (SA) – a simplex "connection" that affords security services to the traffic carried by it.

Internet Key Exchange (IKE) – negotiates the security association between two entities and securely exchanges key material.

Encapsulating Security Payload (ESP) - a protocol that may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service.

Authentication Header (AH) - provides connectionless integrity, data origin authentication, and an optional anti-replay service.

Public Key Infrastructure (PKI) - the complete system of software, hardware, policies, standards and technologies for the life cycle management of digital identities, known as digital certificates, and data encryption passwords called keys.

Red Security Policy Table – a table on the PERMIT/Gate, much like a routing table, that specifies addresses of nodes protected by the PERMIT/Gate, routing information for the nodes, and security procedures for protecting nodes. The Red Security Policy Table consists of seven pieces of information. The IP Address/Range value specifies which host or range of hosts can communicate through the device. The range can specify a single host, a subnet, a network, or a specific set of hosts when enclosed in square brackets []. The IP Address Mask field specifies the subnet mask of the host. If the subnet mask of the subnet to which the host belongs is given, all hosts in the subnet will be allowed. If a subnet mask of all 255's is given, only the host specified will be allowed. If a range of hosts is specified with square brackets, the IP Address Mask field is grayed out. The Mode field specifies whether or not the host or range can communicate outside the network protected by the VPN device. If so, it specifies whether communications can occur in the clear, or require certificates or shared secrets for authentication. The Policy ID specifies a policy name. For purposes of this paper, Policy ID's are not necessary. The Red Router field specifies the default router for the host or range of hosts. A value of "0.0.0.0" means the host or range is in a directly connected network. The Secure Map field specifies whether or not the host or range should be included in the Secure Map file. Finally, the Allow Clear field specifies whether or not the host or range of hosts is allowed to initiate communications in the clear.

Secure Map – a text file stored on the PERMIT/Gate that maps out nodes and subnets throughout the secure VPN and links them to the security measures they use during communications, and to the proxy device (another PERMIT/Gate), if any, that secures their communications. An example of a typical Secure Map is:

```
begin static-map
        name   "Server 2"
        target   "192.168.3.0/255.255.255.0"
        mode   "ISAKMP-Shared"
        tunnel  "172.16.2.1"
```


© SANS Institute 2000 - 2005 Author retains full rights.

end

The "name" field specifies an arbitrary name given to this entry in the Secure Map. This value is optional. The "target" field specifies the destination host, range of hosts, or network. The "mode" field specifies how communications will be established. The "tunnel" field specifies the IP address of the remote VPN device that secures the "target" host, range of hosts, or network. The "begin" and "end" fields denote the beginning and ending of a Secure Map entry.

Security Descriptor File – a text file stored on the PERMIT/Gate that defines one or more security levels. Each security level definition includes a name for the security level and maps that security level name to specific compression methods, authentication types, encryption types, and negotiation algorithms. An explanation of the options available in the Security Descriptor File is not necessary for purposes of this paper.

Shared Secret Table – a table on the PERMIT/Gate that contains shared secret entries for other VPN devices. The table consists of three entries. The Black IP Address/Range specifies the IP address of a remote VPN device. A range of IP addresses may also be specified if there are multiple VPN devices all using the same shared secret. The "*" wildcard character may also be used to specify any value in that octet. The Black Network Mask field specifies the subnet mask for the Black IP Address/Range. If a range is specified, the Black Network Mask field is grayed out. The Black ID field specifies an ID string for the black host. For purposes of this paper, the Black ID is not required.

Target – the destination host, range of hosts, or network protected by another security gateway.

Tunnel Point – the address of the security gateway that protects the target host, range of hosts, or network.

In my example, I will be establishing a "Dual-Sided" VPN from Server 1 at 192.168.1.2 to Server 2 at 192.168.3.2. Data transferred from Server 1 will traverse VPN's 1-4 on it's way to Server 2. Refer to Diagram 1. The step-by-step procedures for establishing the "Dual-Sided" VPN are as follows.

1. On VPN 1, an entry must be made in the Red Security Policy Table for Red Network 1. This entry designates which hosts may communicate on the secure side of the gate. This entry can be specified as a single host, a range of hosts, a subnet, or a network. It is good practice to only add those devices that need access through the VPN. If a subnet is specified when only one device in that subnet needs access to the VPN, all other devices in that subnet will also have access inside the VPN. This situation would give someone with less than noble intentions, unrestricted access inside the VPN. They would simply need to configure a host with an IP address that falls into the subnet specified.

IP Address/Range	IP Address Mask	Mode	Policy ID	Red Router	Secure Map	Allow Clear
192.168.1.0	255.255.255.0	ISAKMP-Shared	N/A	0.0.0.0	Yes	No

© SANS Institute 2000 - 2005 Author retains full rights.

2. In the Secure Map of VPN 1, a target of Network 3, must be added with a Tunnel Point of VPN 2. As with the Red Security Policy, it is good practice to only specify devices that need to communicate through the VPN. If hosts behind one VPN device need to talk to hosts behind another VPN device, entries for each of the hosts must be included in the Secure Map on both VPN devices. If one of the entries is omitted, no SA's will be created and no communications will take place. On a related note, these entries do not have to specify the same host(s). An entry on VPN 1 may specify only necessary hosts, while the entry on VPN 2 may specify the subnet or network that contains those hosts. A request, by a host behind VPN 2, to talk to a specified host behind VPN 1 will be successful. However, a request, by a host behind VPN 2, to talk to a non-specified host behind VPN 1, will fail since the requested host is not specified in the Secure Map of VPN 1. This will prevent an intruder from plugging in another host, such as a laptop, into the remote network and gaining access to the VPN.

```
begin static-map
        name   "Server 2"
        target   "192.168.3.0/255.255.255.0"
        mode   "ISAKMP-Shared"
        tunnel  "172.16.2.1"
end
```

3. In the Shared Secret table of VPN 1, a shared secret entry must be added with the same shared secret as VPN 2. It is highly recommended that a "Black Network Mask" of 255.255.255.255 be specified in the Shared Secret Table. This network mask will specify only the address that is given in the "Black IP Address/Range" field. If a subnet mask is given, the VPN device will accept communications from any other VPN device that falls into the subnet specified, and has the correct shared secret. This is a security risk since anyone with a VPN device and the correct shared secret can gain entry into the VPN. This may seem far-fetched, but with the price of computer equipment dropping everyday, and the poor password generation and guarding of some network administrators, it's a lot easier than you might think.

Black IP Address/Range	Black Network Mask	Black ID
172.16.2.1	255.255.255.255	N/A

4. On VPN 2, an entry must be made in the Red Security Policy Table for Red Network 2, which resides between VPN 2 and VPN 3.

IP Address/Range	IP Address Mask	Mode	Policy ID	Red Router	Secure Map	Allow Clear
192.168.2.0	255.255.255.0	ISAKMP-Shared	N/A	0.0.0.0	Yes	No

5. On VPN 2, an entry must be made in the Red Security Policy Table to forward traffic, destined for Server 2, to the next hop in the "Dual-Sided" VPN chain. In this case, the traffic will be destined for Red Network 3.

IP Address/Range	IP Address Mask	Mode	Policy ID	Red Router	Secure Map	Allow Clear
192.168.3.0	255.255.255.0	ISAKMP-Shared	N/A	192.168.2.2	Yes	No

© SANS Institute 2000 - 2005 Author retains full rights.

6. In the Secure Map of VPN 2, a target of Network 1 must be added with a Tunnel Point of VPN 1.

```
begin static-map
        name   "Network 1"
        target   "192.168.1.0/255.255.255.0"
        mode   "ISAKMP-Shared"
        tunnel  "172.16.1.1"
end
```

7. In the Shared Secret table of VPN 2, a shared secret entry must be added with the same shared secret as VPN 1.

Black IP Address/Range	Black Network Mask	Black ID
172.16.1.1	255.255.255.255	N/A

8. On VPN 3, an entry must be made in the Red Security Policy Table for Red Network 2, which resides between VPN 2 and VPN 3.

IP Address/Range	IP Address Mask	Mode	Policy ID	Red Router	Secure Map	Allow Clear
192.168.2.0	255.255.255.0	ISAKMP-Shared	N/A	0.0.0.0	Yes	No

9. On VPN 3, an entry must be made in the Red Security Policy Table to forward traffic, destined for Server 1, to the next hop in the "Dual-Sided" VPN chain. In this case, the traffic will be destined for Red Network 1.

IP Address/Range	IP Address Mask	Mode	Policy ID	Red Router	Secure Map	Allow Clear
192.168.1.0	255.255.255.0	ISAKMP-Shared	N/A	192.168.2.1	Yes	No

10. In the Secure Map of VPN 3, the target network, Network 3, must be added with a Tunnel Point of VPN 4.

```
begin static-map
        name   "Server 2"
        target   "192.168.3.0/255.255.255.0"
        mode   "ISAKMP-Shared"
        tunnel  "172.16.4.1"
end
```

11. Also in the Secure Map of VPN 3, Network 2 must be added with a Tunnel Point of VPN 3.

```
begin static-map
        name   "Server 2"
        target   "192.168.3.0/255.255.255.0"
        mode   "ISAKMP-Shared"
        tunnel  "172.16.4.1"
```


© SANS Institute 2000 - 2005 Author retains full rights.

end

12. In the Shared Secret table of VPN 3, a shared secret entry must be added with the same shared secret as VPN 4. It is recommended that a different shared secret be used for this VPN connection. This is just one more step in the process of trying to stop intruders.

Black IP Address/Range	Black Network Mask	Black ID
172.16.4.1	255.255.255.255	N/A

13. On VPN 4, an entry must be made in the Red Security Policy Table for Red Network 3.

IP Address/Range	IP Address Mask	Mode	Policy ID	Red Router	Secure Map	Allow Clear
192.168.3.0	255.255.255.0	ISAKMP-Shared	N/A	0.0.0.0	Yes	No

14. In the Secure Map of VPN 4, Network 2 must be added with a Tunnel Point of VPN 3.

```
begin static-map
        name   "Network 2"
        target   "192.168.2.0/255.255.255.0"
        mode   "ISAKMP-Shared"
        tunnel  "172.16.3.1"
end
```

15. In the Shared Secret table of VPN 4, a shared secret entry must be added with the same shared secret as VPN 3.

Black IP Address/Range	Black Network Mask	Black ID
172.16.3.1	255.255.255.255	N/A

When steps 1-15 have been successfully completed, secure communications from Server 1 to Server 2 will be established.

The process of setting up secure VPN connections may differ from vendor to vendor, but the idea behind the "Dual-Sided" VPN will not change. Secure VPN connections must be established between all VPN devices in the chain. When configuring the VPN devices, it is important to only allow access to those devices that must communicate through the VPN. Also, using different shared secrets for each VPN tunnel will slow potential intruders down.

As stated earlier, the purpose of the "Dual-Sided" VPN is to establish a secure connection from one site to another site that gets it's connectivity from a leased line that terminates behind a firewall. The "Dual-Sided" VPN solution accomplished all of our goals. We were able to leverage existing leased lines and get secure data communications from one site to another without passing any VPN ports or protocols through the firewall at the site.

© SANS Institute 2000 - 2005 Author retains full rights.

"Dual-Sided" VPN

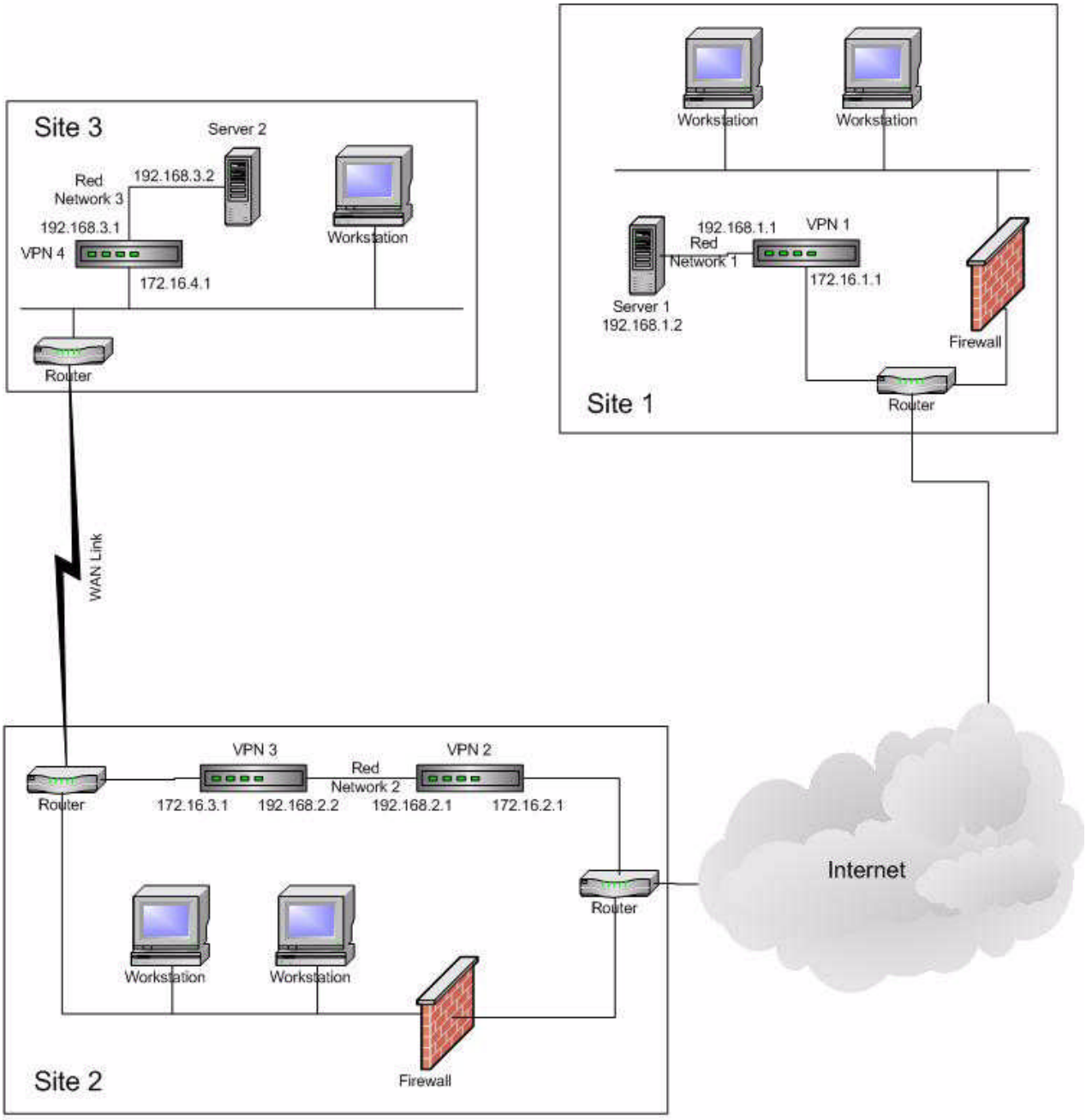


Diagram 1

© SANS Institute 2000 - 2005 Author retains full rights.

References

1. Ciolek, Gregory J. "Virtual Private Network (VPN) Security." 4 January 2001. URL: http://www.sans.org/infosecFAQ/encryption/VPN_sec.htm (11 August 2001)

2. Microsoft, Inc. "Virtual Private Networking: An Overview." 19 April 1999. URL: http://www.microsoft.com/windows2000/docs/VPNoverview.doc (11 August 2001)

3. Kent, S. and Atkinson, R. "Security Architecture for the Internet Protocol." November 1998. URL: http://www.ietf.org/rfc/rfc2401.txt?number=2401 (12 August 2001)

4. Fraser, Moye. " Understanding Virtual Private Networks (VPN). 3 March 2001. URL: http://www.sans.org/infosecFAQ/encryption/understanding_VPN.htm (10 August 2001)

5. Newbridge Networks. "PERMIT Enterprise secure VPN overview". Chapter 1. PERMIT Enterprise Secure VPN Primer. Newbridge Networks May, 2000 VPN Primer.

6. Newbridge Networks. "Configuring the PERMIT/Gate". Chapter 4. PERMIT/Gate Version 3.0 Administrator's Guide. 2000.

7. Quinby, Joe. "Remote Access—Protecting the Internal Network, or, How to Allow "Them" in While Keeping "Them" out" 16 January, 2001. URL:http://www.sans.org/infosecFAQ/firewall/remote_access.htm.

8. Cylink Corporation. "Is Your Wide Area Network Really Secure?" September 2000. URL:http://www.cylink.com/library2/wansecure9-00.pdf.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.