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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

GIAC Certification
GSEC Practical Assignment Version 1.4b

© SANS Institute 2004, Author retains full rights.

Implementing CISCO PIX firewall VPN for SOHO networks and DSL

Case Study

Prepared by: Vadim Dostman

Submitted: 12/30/2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The advance of high speed DSL brings new choices for companies looking to establish connectivity to their geographically dispersed business partners, customers, suppliers, branches or remote office (SOHO) networks. One of the most popular solutions is establishing a VPN (Virtual Private Network) using DSL broadband. It is relatively easy to implement and it is considerably more cost effective in comparison with dedicated circuit or leased line. This case study will examine benefits and risks associated with VPN solution and also assist in getting started configuring a CISCO PIX firewall on a SOHO network connected to a central office.

Introduction

Let's consider a company is looking to establish a new office close to a location of a major client. The office is going to contain approximately 20 workstations that would require access to corporate Email and windows file shares located in the main office of the company. Among the biggest concerns is security, cost and total time required for the implementation. After some consideration, a choice was made to proceed by connecting SOHO network to the Internet via a DSL and a Virtual Private Network connection to central office.

Network layout

DSL modem (which was provided by the phone company as part of the DSL Internet access package) is connected directly to the external interface of the CISCO PIX firewall. Internal interface of the PIX is then connected to an Ethernet switch or a hub (switch is preferred for better performance), which is in the end connected to the user workstations and local file server. DSL link provides a dual functionality – the primary is allowing the SOHO network to safely connect to the Internet while the secondary is VPN connectivity to the central office of the company. IPSec protocol is used to allow authentication and encryption for the VPN tunnel:

> IPSec is needed whenever there is a requirement for strong encryption or strong authentication. It also supports multiplexing and a signaling protocol - IKE.

Bryan Gleeson et. al. "RFC 2764 - A Framework for IP Based Virtual Private Networks" [1]

Please see network diagram in Appendix I.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk Analysis

While implementing a new security solution with strong defense in mind, it is always a good practice to perform some risk analysis. Here are some of the points that we have encountered:

- Risk of a remote attack or eavesdropping – since a VPN connection is using public IP network, there is a risk coming from spoofing, session hijacking, sniffing or man-in-the-middle attacks. The word "virtual" is the key – VPN tunnel data is traveling over the public network. In order to reduce this risk, VPN connections use encryption protocols such as IPSec in our case.
- Physical security compromise – it is often overlooked that remote VPN sites are usually less physically secure than the central site. This is a major risk because once someone gains physical access to a remote site they can use VPN connection to access information on the central site. It is also reasonable to mention that security of remote site is affecting security of the central office even if the connection is a dedicated one and not a VPN. Physical security of remote sites should always be thoroughly addressed.

System Policy

In order to successfully address the risks of implementing VPN it is advisable to write a system specific security policy. Here are some points to be emphasized in that policy:

- Ownership of the VPN configuration and maintenance. There should be a designated person or a team responsible for maintaining the firewall and performing maintenance and upgrades. Access to firewall configuration should be restricted to that person or team.
- Physical access to remote office (where the VPN is connected) should be restricted to personnel with proper permissions and valid access not only to the resources in that office, but those accessible via the VPN.
- VPN access network policy. Network access via VPN should be restricted to only those resources that are required for the business. For example if remote office only needs access to E-Mail server in the central office, a firewall rule should be in place to enforce such restriction limiting traffic to specific ports and IP addresses.
- IDS systems should be used to monitor suspicious activity originating from VPN for added protection.
- Network devices and computers on remote site should be regularly audited, patched for latest vulnerabilities and protected with anti-virus

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

system. CISCO IOS (operating system) should be upgraded to the latest version and configuration should be audited on a regular basis (please see Ongoing Maintenance section below).

Step by Step Guide

1. Physical site assessment

Because of the risk associated with breach of security in the remote office, physical access should be controlled (i.e. alarm systems, security guards, etc.). All network equipment - firewall, network switch and local file server should be located in a server room with access restricted to IT staff responsible for maintaining the systems.

2. Ordering DSL line

A business DSL line can be ordered from a local phone company. Please make sure to order a “fixed IP” option, this will slightly increase the cost, however it is important since the VPN configuration is based on fixed IP information. Here’s what the phone company should provide with the contract:

- Username & password for PPPOE (Point-to-Point Protocol authentication over Ethernet)
- Fixed IP address assigned for your connection
- Technical support phone number

3. Connecting DSL and PIX firewall

Connect DSL modem with provided RJ-11 cable to the phone jack, connect the power and, if possible, ensure that the modem connects to the provider. Use the manual that comes with modem to figure out which lights should be on in normal operation.

Connect the external interface of the PIX to the DSL modem. This connection and all of the remaining use Ethernet CAT5, RJ-45 Ethernet cables.

4. Configuring PIX firewall

PIX Configuration can be performed using several methods, among them:

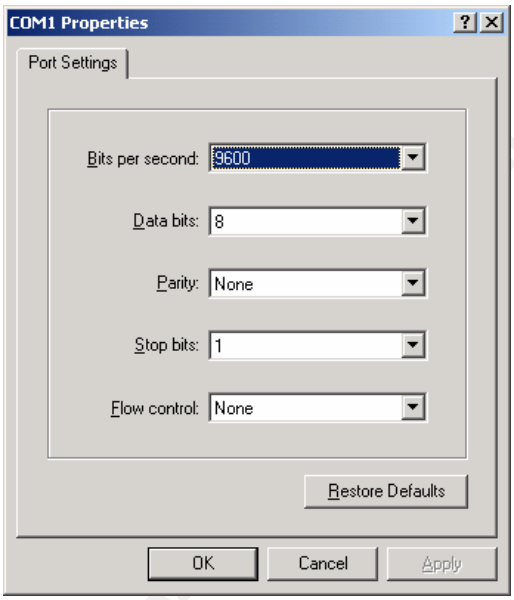
- Using provided serial console cable
- Using telnet access

Initially use the console connection in order to configure IP addresses and accept telnet, telnet access can later be used to finish the configuration.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. Connecting to serial console of the PIX

Use your laptop or a desktop computer to connect to the serial port of the PIX. Any serial terminal software can be used here, most MS Windows computers will already have HyperTerminal installed, it can be started by going to Start Menu Programs | Accessories | Communications. Set the connection properties to 9600 bps, 8 Data bits, No Parity, 1 Stop bits and No Flow control:



Connect the serial cable from your computer's serial interface (9 pins) to the PIX serial port. You may need to find a terminal adapter to go from 9-pin connector to RJ-45. Once everything is connected you can power on the PIX and you should be able to see IOS banner on your serial terminal.

6. Viewing and editing configuration

CISCO has two levels of authentication for administration purposes – first you need to enter username (if you are using telnet) and password and then enter another password for "enable" or privileged mode. Here's an example of connecting to console:

```
User Access Verification

Password: *******
pixfw> enable
Password: *******
pixfw#
```

Note: each command prompt contains the hostname assigned to the PIX. We will explain how to change it below.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CISCO IOS commands can be abbreviated. For example:

Instead of “write terminal” we can use “wr term”.

After logging in and entering the “enable” mode, enter the following command to view the current configuration:

```
pixfw# wr term
Building configuration…
: Saved
: Written by enable_15 at 14:44:30.886 EDT Fri Oct 10 2003
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password hkjhUUH76fg56 encrypted
passwd k76hgjh8jhg7k87 encrypted
hostname pixfw
…
```

To edit any of the configuration lines, enter the terminal configuration mode, type new lines and type “exit” to close configuration mode:

```
pixfw# conf t
pixfw(config)# <new line here>
pixfw(config)# <new line here>
pixfw(config)# exit
pixfw#
```

To replace an existing line from the configuration, type “no” and the line that you want to delete and then enter new line:

```
pixfw(config)# no <existing line here>
pixfw(config)# <new line here>
```

To save new configuration to make sure it doesn’t get lost after a reboot or a loss of power, type “wr mem”:

```
pixfw# wr mem
Building configuration…
Cryptochecksum: 4nj44765 u76k8y89 u88dsfuy7 8ejkh9s90
[OK]
pixfw#
```

7. Setting new passwords

One of the first things to do is to replace the default passwords:

```
pixfw# conf t
pixfw(config)# enable password <new password here>
pixfw(config)# passwd <telnet password here>
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8. Setting new hostname and domain name

You can also set a new hostname for the PIX (which will immediately appear at the command prompt) and the domain name assigned to your company:

```
pixfw(config)# hostname <new hostname here>
<new hostname>(config)# domain-name <your domain name here>
```

9. Configuring DSL connection and internal IP

Even though we have a fixed IP assigned to us by the ISP, we still need to obtain it using DHCP protocol from the modem; we will also specify the username and password, which we got along with the DSL contract:

```
ip address outside pppoe setroute
ip address inside 172.19.1.1 255.255.255.0
vpdn group DSL request dialout pppoe
vpdn group DSL localname <username here>
vpdn group DSL ppp authentication pap
vpdn username <username here> password <your password here>
```

Note:

RFC 1918 describes non-routable subnet designations, which we can use for our SOHO network addresses:

> The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets:
>
> 10.0.0.0 - 10.255.255.255 (10/8 prefix)
> 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
> 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

[2] Rekhter, Y. et. al. "RFC 1918: Address Allocation for Private Internets."

In this example we assigned 172.19.1.1 class C to our internal network, but you can pick any private (non-routable) subnet for this purpose.
Should your ISP ever change the fixed IP address (which is unfortunate because it would cause an outage, however sometimes it can happen) you would need to reboot your PIX and inform the administrator of the central office firewall of the new IP to reconfigure their firewall and get the VPN connection working again.

10. Configuring NAT

In order to allow a number of workstations (and servers) on our SOHO network to access the Internet, each computer needs to be assigned a unique IP address. However we only get one IP from our provider, this is where NAT comes in handy, it allows us to use a whole subnet (172.19.1.x class C in this example)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and translate it to the single IP:

```
global (outside) 1 interface
nat (inside) 1 172.19.1.0 255.255.255.0
```

11. Configuring DHCP server

PIX Firewall can function as a DHCP server (although you may prefer your local file server), to enable this feature enter:

```
dhcpd address 172.19.1.1-172.19.1.100 inside
dhcpd enable inside
```

12. Configuring to accept telnet connections

In order to allow incoming telnet connections for administering PIX, enter the following command:

```
telnet 172.19.1.0 255.255.255.0 inside
telnet timeout 10
```

The above will allow telnet connections coming from the internal subnet and set timeout for inactive sessions to 10 minutes. It is not advisable to allow telnet from outside subnets, however after VPN is configured we can allow connections from the central office network:

```
telnet <IP subnet of the central office> <netmask> outside
```

To configure a username for telnet connections, enter:

```
username <telnet username> password <telnet password> privilege 2
```

The above command allows to login via telnet, however the user still needs to enter “enable” mode to be able to view or edit configuration.

13. Configuring VPN

There are two steps in CISCO VPN configuration:

1. IKE – defines method to be used in order to establish the VPN tunnel
2. IPSec – defines the tunnel itself

13.1 IKE

You will need to find out from the administrator of the central firewall the following information:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. IKE Encryption method (DES, 3DES)
2. Hashing method (md5)
3. Authentication method (pre-shared keys, RSA signature) and pre-shared key if used
4. Identification method (IP, hostname)
5. Public IP of the central firewall

The above methods can differ depending on the firewall that is being used by the central office. In our case we used a SonicWall firewall, which uses des, md5, pre-shared keys and IP identification:

```
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 authentication pre-share
isakmp key <pre-shared key> address <public IP of central firewall>
netmask 255.255.255.255
isakmp identity address
isakmp enable outside
```

13.2 IPSec

Here as well you need to contact the central firewall administrator and find out which encryption and hashing methods should be used for the VPN transform set. Most likely it will be either DES or 3DES and MD5. Here we define a 3DES - MD5 set and name it “T3DESMD5”:

```
crypto ipsec transform-set T3DESMD5 10 esp-3des esp-md5-hmac
```

Next we need to define the valid VPN traffic and map the transform set to it and the central firewall:

```
access-list VPN-ACL permit ip <SOHO network subnet> <netmask> <central
office subnet> <netmask>
crypto map VPN-MAP 10 match address VPN-ACL
crypto map VPN-MAP 10 set peer <public IP of the central firewall>
crypto map VPN-MAP 10 set transform-set T3DESMD5
```

We also need to apply the same ACL to the NAT configuration to ensure that the VPN traffic does not get translated:

```
nat (inside) 0 access-list VPN-ACL
```

14. Troubleshooting VPN connections

To show IKE status (first phase of establishing VPN) use “show crypto isakmp sa” command:

```
pixfw# show crypto isakmp sa
Total     : 1
Embryonic : 0
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
        dst             src          state       pending     created
     169.47.62.19    169.173.151.9    QM_IDLE         0           0
```

The above shows a successful key exchange and the IP's for both ends of a VPN connection.

"show crypto ipsec sa" command shows the second phase of VPN connection – tunnel status. Here we see a successful IPSec tunnel:

```
pixfw# sh crypto ipsec sa

interface: outside
    Crypto map tag: VPN-MAP, local addr. 169.47.62.19

   local  ident (addr/mask/prot/port): (172.19.1.0/255.255.0.0/0/0)
   remote ident (addr/mask/prot/port): (172.19.2.0/255.255.0.0/0/0)
   current_peer: 169.173.151.9
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 45136, #pkts encrypt: 45136, #pkts digest 45136
    #pkts decaps: 73072, #pkts decrypt: 73072, #pkts verify 73072
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 169.47.62.19, remote crypto endpt.:
169.173.151.9
     path mtu 1492, ipsec overhead 56, media mtu 1492
     current outbound spi: 968b43cf

     inbound esp sas:
      spi: 0xec54084(247808132)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4606144/2577)
        IV size: 8 bytes
        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:
      spi: 0x968b43cf(2525709263)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4606798/2580)
        IV size: 8 bytes
        replay detection support: Y
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
outbound ah sas:

outbound pcp sas:
```

15. Securing PIX

Here are some additional configuration changes to protect SOHO network:

```
access-list soho permit ip 172.19.1.0 255.255.255.0 172.19.2.0
255.255.255.0
access-list soho deny tcp any any eq 135
access-list soho deny udp any any eq 135
access-list soho deny icmp any any echo
access-list soho deny icmp any any echo-reply
access-list soho deny udp any any eq tftp
access-list soho deny tcp any any eq 137
access-list soho deny udp any any eq netbios-ns
access-list soho deny tcp any any eq 138
access-list soho deny udp any any eq netbios-dgm
access-list soho deny tcp any any eq netbios-ssn
access-list soho deny udp udp any any eq 139
access-list soho deny tcp any any eq 445
access-list soho deny tcp any any eq 593
access-list soho permit ip any any
access-group soho in interface inside
```

The above ACL allows all traffic to the central office subnet (172.19.2.0) and restricts other unnecessary protocols, which could have exposed SOHO subnet to the Internet. In addition it protects against Cisco Pix Firewall DoS (NAT Pool Depletion) vulnerability and Nachi worm. Please see “Nachi Worm Mitigation Recommendations” for more information. 3

In addition we can also limit which servers in central office can be accessed from SOHO network:

Replace

```
access-list soho permit ip 172.19.1.0 255.255.255.0 172.19.2.0
255.255.255.0
```

With

```
access-list soho permit ip 172.19.1.0 255.255.255.0 172.19.2.4
255.255.255.0
access-list soho permit ip 172.19.1.0 255.255.255.0 172.19.2.7
```

The above rule will open all ports to only two IP’s in the central office subnet (172.19.2.4 and 172.19.2.7). In most cases the central firewall would also require additional rules with similar functionality. As we mentioned in the System Policy section above, it is necessary to define which IP’s in the central office should be

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

open to the SOHO network.

16. Connecting workstations and servers

Connect internal interface of the PIX to an Ethernet hub or switch. Connect user workstations and servers (if any) to the hub/switch.

Ongoing Maintenance

Audit PIX Firewall using Router Audit Tool (RAT)

RAT is a great tool that allows parsing configuration for any errors and vulnerabilities using a policy or benchmark. RAT was created by George M. Jones, at the time of writing this paper, CISecurity were finishing PIX benchmark and scoring tool for RAT, it should be available late January on CIS website. [4]

RAT creates output in form of text files containing suggested configuration changes and HTML files showing the results and explanations for each passed or failed rule. Make sure to review each suggested change before writing it into configuration.

It is recommended to regularly audit configuration using RAT to ensure mitigation of the latest vulnerabilities.

Update IOS

Update IOS (PIX operating system) regularly. To see which version is installed run the following command in enable mode:

```
pixfw# sh version

Cisco PIX Firewall Version 6.2(2)
Cisco PIX Device Manager Version 2.1(1)
…
```

IOS is available for registered users at CISCO website – http://cisco.com/software You will need to install a TFTP server in order to be able to load the new software into the firewall. Once the TFTP server is up, use the following command to load the configuration:

copy tftp[:[[**//***location*] [**/***tftp_pathname*]]] **flash**

For more information please read Cisco PIX Firewall and VPN Configuration Guide. [6]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Subscribe to a mailing list

On of the best sources of information about the latest PIX vulnerabilities is Cisco Product Security Advisories and Notices web page. [7]

Additionally you can join one or more of the following mailing lists:

SANS Computer Security Newsletters and Digests
Refer to: http://www.sans.org/newsletters/

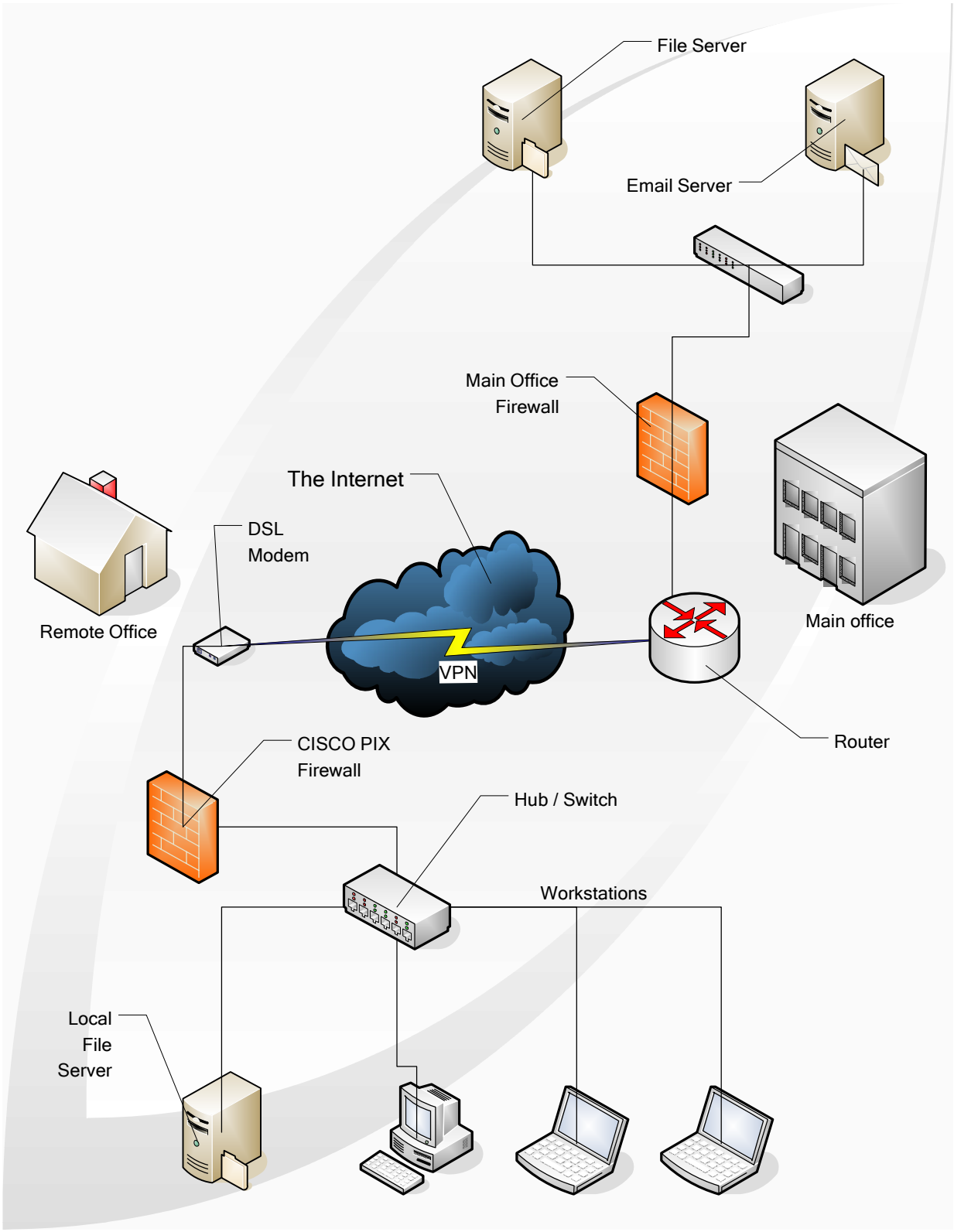
SecuriTeam
Refer to: http://www.securiteam.com/mailinglist.html

CERT Coordination Center
Refer to: http://www.cert.org/contact_cert/certmaillist.html

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix I – Network Diagram



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1. Bryan Gleeson et. al. "RFC 2764 - A Framework for IP Based Virtual Private Networks" February 2000 URL: http://www.faqs.org/rfcs/rfc2764.html (15 December 2003).
2. Rekhter, Y. et. al. "RFC 1918: Address Allocation for Private Internets." February 1996. URL: http://www.ietf.org/rfc/rfc1918.txt?number=1918 (15 December 2003).
3. Cisco Systems “Cisco Security Notice: Nachi Worm Mitigation Recommendations” 14 October 2003 URL: http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml (15 December 2003).
4. Center for Information Security “The Router Audit Tool and IOS Benchmark” URL: http://www.cisecurity.org/bench_cisco.html (15 December 2003).
5. Cisco Systems “Cisco PIX Firewall and VPN Configuration Guide” 1992-2004 URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_configuration_guides_list.html (15 December 2003).
6. Cisco Systems “Cisco PIX Firewall and VPN Configuration Guide" http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_configuration_guides_list.html (15 December 2003).
7. Cisco Systems “Cisco Product Security Advisories and Notices” URL: http://www.cisco.com/warp/public/707/advisory.html (15 December 2003).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.