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

How to build an SSL-based VPN network with AmritaVPN

By Dan L'Heureux
November 18, 2003

© SANS Institute 2004, Author retains full rights.

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

Introduction

This paper will describe how to build an SSL-based VPN network using the software called AmritaVPN (amvpn) on a Linux platform. Amvpn is a software package that connects two separate networks together via a VPN (Virtual Private Network) tunnel. It uses the openssl libraries for encryption of data over a public network that segments two internal networks. The openssl libraries are also used for authenticating and encrypting the connection between the VPN gateways using public keys.

The purpose of building this type of network is to provide an easy-to-use secure path to send data to a remote network. This is especially helpful when needing to ensure the privacy of data over a public network, like the Internet.

Setup

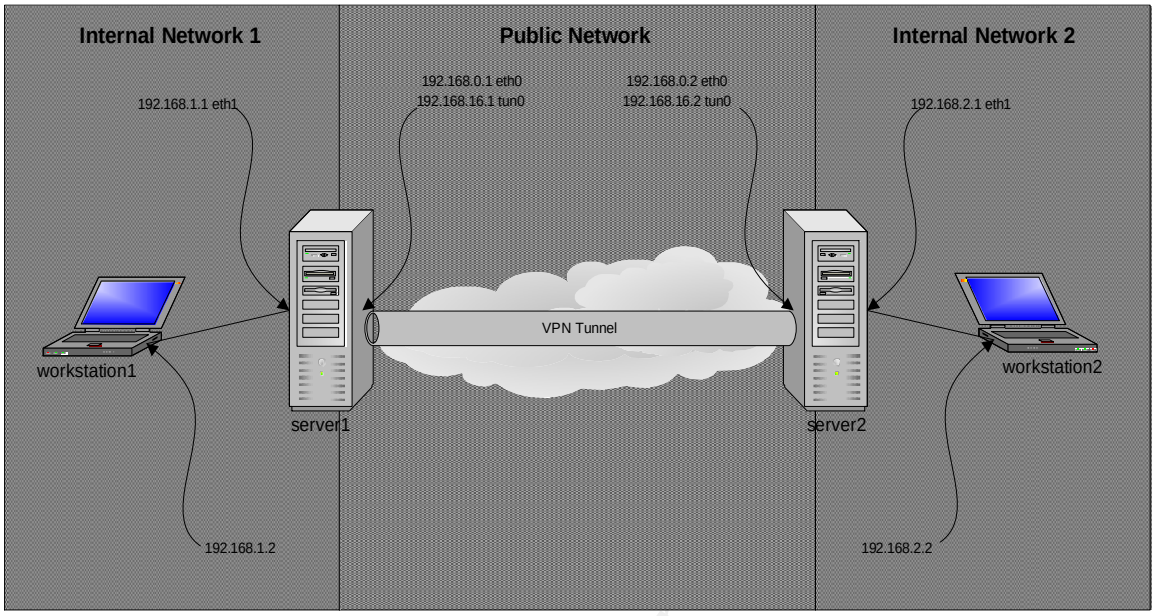
Note: This paper does not cover the proper ways to install/harden a Linux machine, as well as, Windows XP workstations. The assumption is that these machines are installed, hardened, and have the current patches applied.

For simplicity, a minimal amount of equipment will be used for this example network. This network will consist of two Linux machines running Slackware Linux v9.0. On the internal side of each Linux machine will be a Windows XP workstation. In this network, there are two Ethernet adapters in each Linux machine, (one to the public network, and one to the internal network). To connect everything together, a crossover cable connects the Linux machines together, as well as, connecting the XP workstations to the Linux machines. The hostnames given to the Linux machines are server1 and server2. The hostnames given to the XP workstations are workstation1 and workstation2. A common domain of "domain.com", and a common workgroup of "workgroup" have been given to the XP workstations.

The network addressing has been simplified as much as possible, as well. The public network is addressed as 192.168.0.0/24. 192.168.0.1 is the address assigned to the public network adapter of server1 and 192.168.0.2 is assigned to the public network adapter of server2. The internal network 1 and the internal network 2 are addressed as 192.168.1.0/24 and 192.168.2.0/24 respectively. 192.168.1.1 has been assigned to the internal network adapter of server1 and 192.168.1.2 has been assigned to workstation1. Lastly, 192.168.2.1 has been assigned to the internal network adapter of server2 and 192.168.2.2 has been assigned to workstation2. The public network adapters of the Linux machines are designated as eth0 and the internal network adapters are designated as eth1. The tun0 interfaces are dynamically created and will be explained later.

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

The network diagram follows:



A standard load of Linux is all that is needed for the base system. However, some required software is needed to make them each into a VPN gateway for the internal machines to traverse their data through to the remote internal network. This software is amvpn which was mentioned earlier. It can be found from a link on their homepage (http://amvpn.sourceforge.net). Installation is accomplished the same way any other software would be installed on a Linux system (Appendix A.1).

Once the VPN software is installed, it needs to be configured. From the default installation the configuration file is located under the /etc directory. It is called amvpn.conf and contains various parameters. A minimal amount of configuration needs to be done to get the tunnel up and running. First, on server1 you only need to define tunnel-ip, route-ip, and route-mask. For tunnel-ip it will be defined as 192.168.16.1. This IP address is attached to a special kernel device, tun0, which is created dynamically when amvpn is launched. This device is our tunneling interface where all of our VPN traffic will travel through. The next parameters are route-ip and route-mask, which will be defined as 192.168.2.0 and 255.255.255.0, respectively. These parameters will define what to do with packets destined for internal network 2. The route table of the system will define this network to be attached to the special interface tun0. (Appendix B.1, B.1a)

On server2, there is a slightly different configuration. First, the tunnel-ip needs to be changed to 192.168.16.2. An additional parameter, server-ip, needs to be set. This should be set to the public network-facing interface IP address of server1. In this case, it is 192.168.0.1. However, a hostname could be used if DNS was present and available. Routing must be setup on server2 to deal with packets going to and coming from internal network 1. The parameters of route-ip and route-mask will be defined as 192.168.1.0 and

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

255.255.255.0, respectively. This configuration sets up server2 to be a "client". The "client" is the machine that initiates the connection to setup the tunnel. In this case, server1 is the "server" waiting for incoming connections and server2 is the "client" that initiates the connection. (Appendix B.2, B.2a)

The default configuration file that comes with v0.98-2 states that the default port is 7071, however, this is incorrect. By default, amvpn listens on TCP port 7171, but can be configured to listen on any TCP port. For this network, it is left as the default.

Now that the configuration file is setup, authentication needs to be setup. This is accomplished with certificates. Amvpn has created a tool to streamline this process. This tool is called amvpn-keytool. First, we need to create the signing authority called the root Certificate Authority, or root CA. There is only one machine that needs to accomplish this task; this will be handled on server1. To generate this certificate, the command "amvpn-keytool genca" is run. Launching this command will require some user input (Appendix C.1).

Next, certificates need to be created on both server1 and server2. To start, on server1, run the command "amvpn-keytool genkey". This will create the private VPN key for server1 and create the Certificate Signing Request (CSR). The CSR needs to be signed by the root CA. To do this, run the command "amvpn-keytool gencert". This signs the CSR and results in the creation of the public key.

Server2 will be handled slightly different. Since the root CA is on server1, special arrangements need to be made to get the CSR of server2 signed. The amvpn-keytool will be used to overcome this issue. The command "amvpn-keytool genkey" is run on server2 to create the private key and CSR for server2. Once the private key and CSR for server2 are created, the CSR needs to be signed to be mutually inclusive in the root CA's span of trust. The command "amvpn-keytool -r root@192.168.0.2:/usr/share/amvpn gencert" is launched from server1. This uses the ssh/sftp protocol to login to server2, retrieve the CSR, produce the effective certificate, and upload it to server2 along with the CA's public key. Thus uniting server1 and server2 under a single umbrella of trust. (Appendix D.1)

It is essential that server1 and server2 have the correct date and time. If the date and time are incorrect, authentication problems may occur when trying to establish the tunnel. Amvpn has provided a command to verify any clock skewing. The command "amvpn-keytool validate" is run on both server1 and server2 to do this verification. This skew can be reduced greatly if a network time protocol daemon (ntpd) is used to automatically set the server's clock.

This process works great for server2 when you have access to both systems. However, this is not always the case. To get server2 a signed certificate without having access, the openssl commands can be used manually (Appendix D.2). These commands must be performed on the machine where the root CA resides. Once the files are created, they need to be securely transmitted to the non-accessible server2. Methods like encrypted

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

email can be used to transfer the files over. When the files are received on the non-accessible server2, all other copies need to be securely destroyed to prevent them from leaking out to other people. These are the keys to the kingdom.

Once the private keys are all created and in place, there is one last step that needs to be performed before bringing up the tunnel. Amvpn uses a less-privileged user to run the daemon on the system and to own the files. Since the user that was being used to create all these files was root, the ownership of the files is root. Again, amvpn has a command-line option that helps to alleviate this problem. The command "amvpn-keytool secure amvpn" is run on both server1 and server2 to change ownership of all files located in /usr/share/amvpn from root to amvpn. The user amvpn was created as part of the installation process.

Finally, the last step now is to bring up the tunnel. Although either side can be brought up first, it is best to bring server1 up first and wait for connections from server2. When server2 is brought up, the configuration is set to try to connect to server1 automatically. If server1 is not available, server2 retries at regular intervals. The default is set to 30 seconds.

To bring up the daemon on server1 the command "amvpn -d" is run and amvpn begins to listen in the background (daemonized) for incoming connections on port 7171. It is recommended that the "-V" option is used instead on first launch to increase the verbosity (Appendix E.1). This can lead to some good information if something should go wrong. Now that server1 is listening, server2 now can try to connect. Similarly, server2 is brought up with the command "amvpn -d" (Appendix E.2). Launching this causes server2 to attempt a connection to server1. Once the connection is established each server verifies the other's certificate, since these are both valid and signed by the root CA, a connection is established. The special kernel device, tun0, is brought up on each server at this point as the tunnel endpoint. The tunnel is now established and traffic can now traverse encrypted over the public network.

NOTE: This is a very easy and basic way to setup an encrypted tunnel between two or more networks. Amvpn has some more nice features that were not demonstrated in this paper; features like traversing a proxy server, including using username/password authentication. There is also even a feature to route SMB packets over the tunnel for file sharing.

Encryption/Privacy

Now that the tunnel is setup, a closer look at the actual encryption and privacy will be given. The core encryption engine is based on the openssl package available for Linux. This encryption is equivalent to the same encryption that is used between your browser and an SSL web server. This encryption is strong and fast. The following is an example of the encryption in action.

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

Untunneled vs. Tunneled using FTP

When setting up a regular FTP session over the Internet, many people do not realize that the password is sent to the FTP server in clear text. This is very easily captured en route to the FTP server. The following examples demonstrate the differences between tunneled and non-tunneled traffic. To see what is going on between each machine, a sniffer will be placed on workstation1 and server1. A sniffer captures the raw packets as they travel from machine to machine. On the workstation, ethereal will be used. On the server, tcpdump will be the sniffer of choice. To read the output of both the ethereal and tcpdump traces, tcpdump will be used since it can display text on a command-line.

A tap will also be placed on the public network between server1 and server2. This device will only be placed into promiscuous mode and basically only listen to the conversation of network traffic taking place between these two servers. This tap device is running tcpdump on a Linux platform.

There will be two examples that will be performed. One will be done without the tunnel being active and one will be done with the tunnel being active. For these examples, server1 and server2's default gateway points to each other's external interface, ie. server1's default gateway is 192.168.0.2 and vice-versa. This is mainly for the untunneled example so that packets are routed properly into the internal networks. When the tunnel is active, routes are automatically created.

FTP Example #1 –Untunneled

On workstation1 there is an FTP server running awaiting connections on port 21. A connection will be attempted from workstation2 to connect onto workstation1 via the FTP protocol. The command "ftp 192.168.1.2" is run on workstation2 from a command prompt. This should bring up a prompt for login. Anonymous login is turned on for this server. The login of "anonymous" and the password of "guest@" are used as the credentials. This is the extent that is needed to demonstrate what is seen traveling over the network.

What is seen at workstation1 is that packets are initiating inbound on port 21 and everything is in clear text, including the password. This is also true at workstation2 where the packets are instead initiating outbound and again everything including the password is clear text. On server1 and server2, the packets are also seen at both interfaces and again everything is in clear text. (Appendix F.1, F.2, F.3)

For example, on the tap this packet is seen:

```
10:10:51.874327 192.168.2.2.1053 > 192.168.1.2.ftp: P 17:30(13) ack 127 win 64114 (DF)
0x0000   4500 0035 16e6 4000 7f06 6088 c0a8 0202        E..5..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a731 7e07 5768        .........;.1~.Wh
0x0020   5018 fa72 f705 0000 5041 5353 2067 7565        P..r....PASS.gue
0x0030   7374 400d 0a                                   st@..
```


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

If you look closely in the ASCII translation of the tcpdump reading, the password is displayed for any eavesdropper to see. Although this is an anonymous login, what if a higher privileged user had logged in? The eavesdropper would be able to steal this password and potentially use it for indecorous purposes.

FTP Example #2 – Tunneled

On workstation1 the FTP server is still enabled and awaiting connections. A connection will once again be attempted from workstation2 via FTP. This time the tunnel is brought up and is verified to be up. Again, the command "ftp 192.168.1.2" is run on workstation2 from a command prompt. The prompt should appear and the same credentials are used.

Traces are taken on the same points as before. The same result occurs on both workstation1 and the internal interface of server1. However, this time on the tap, something different is seen. Instead of seeing clear text being sent over the line, now there is garbled text. This garbled text is called cipher text. The tunnel encryption is creating this cipher text based on the previously-entered configuration that was setup for the tunnel. (Appendix G.1, G.2, G.3)

Here is what is seen on the tap:

```
11:50:33.253421 192.168.0.2.1054 > 192.168.0.1.7171: P 1328:1450(122) ack 893 win 8328
<nop,nop,timestamp 302626097 640614> (DF)
0x0000   4500 00ae f29c 4000 4006 c659 c0a8 0002        E.....@.@..Y....
0x0010   c0a8 0001 041e 1c03 0db4 f624 0bee 5fb4        ...........$.._.
0x0020   8018 2088 c1df 0000 0101 080a 1209 b531        ...............1
0x0030   0009 c666 1703 0000 203e 9a1c 2049 1b0e        ...f.....>...I..
0x0040   f60e 7a51 2567 5f8f 1994 5c65 9d45 35f7        ..zQ%g_...\e.E5.
0x0050   45ea 4483 e1ed 67db 2317 0300 0050 0809        E.D...g.#....P..
0x0060   fbb1 18ff bb54 4f71 62e1 2aad 8a05 fa29        .....TOqb.*....)
0x0070   5487 c3e2 bcbe 06d5 0d46 9236 a244 c806        T........F.6.D..
0x0080   5cb1 ab9b 5467 1616 261b cf71 8a52 ebf9        \...Tg..&..q.R..
0x0090   5074 b375 b96c dd35 f3b2 0e8d f56a 349f        Pt.u.l.5.....j4.
0x00a0   4cf4 ed9f f5d2 0e24 c1a2 a1fd 48ae             L......$....H.
```

As you can see, it is a complete mess. Nothing can be interpreted on the data payload of this packet. The only thing that is seen is the header, which includes the source and destination ip addresses and ports. If you notice, the destination port being used in this instance is port 7171. This port was defined in our default configuration of amvpn. Also, the ip addresses are 192.168.0.1 (server1) and 192.168.0.2 (server2), instead of 192.168.1.2 (workstation1) and 192.168.2.2 (workstation2). Since the tunnel is terminated on server1 and server2 that is the only source and destination of the packet communication that is taking place. All the data is encapsulated inside these packets that are being encrypted with amvpn and sent across the wire.

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

Competing VPN Tunneling Packages

Amvpn is not the only product available to do VPN tunneling. There are quite a few other competing products that have the same type of functionality. Below is a comparison between two of the more popular open source packages available today against amvpn.

Amvpn vs. FreeS/WAN Overview

Although amvpn is one type of tunneling software, there are others available that have different functionality. One such software is titled FreeS/WAN. This stands for Free Secure/Wide Area Network. It is another tunneling program available for Linux. It can be found at http://www.freeswan.org. This package uses IPSec and IKE within this Linux operating system to do the encryption. This is unlike amvpn which uses SSL as its encryption engine.

The Internet Key Exchange (IKE) is used at the beginning of a connection setup for IP Security (IPSec). IKE is used to authenticate then setup the encryption suite that would be used to encapsulate the data. Unfortunately, this package has different dependencies than what amvpn needs. It requires some kernel shims, whether it is compiled in, or via a kernel module. Amvpn does not require any kernel modification whatsoever.

The configuration of FreeS/WAN is somewhat cryptic at best. There are options like leftsubnet, rightsubnet, leftid, and rightid. This can get quite confusing quickly. The authentication consists of either a pre-shared key or a certificate. The pre-shared key is an option not found in amvpn. With FreeS/WAN you cannot connect to the gateway that is terminating the tunnel from the remote internal network. You can only communicate between internal networks. This may require an adjustment in certain network designs if connections are needed to the gateway from the remote internal network.

As far as the throughput is concerned, amvpn seems to perform much better. In my experience and others, there seems to be a lot of overhead with FreeS/WAN than with amvpn. While amvpn performs at near line speed, FreeS/WAN seems to fall short of that. It seems to perform at about 50 to 75 percent of line speed.

Overall, the technology is similar between these two different tunneling suites. The difference between these suites lies in the ease of use and encryption techniques. Amvpn seems to be easier to install and configure than FreeS/WAN. Also, because of the efficient use of strong and fast encryption, amvpn has more effective bandwidth than FreeS/WAN. Amvpn seems to come out ahead.

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

Amvpn vs. OpenVPN Overview

After doing a lot of research and implementation with amvpn, I stumbled upon a different tunneling package called OpenVPN, found at http://openvpn.sourceforge.net. This appears to be an up and coming tunneling suite of choice. From the information provided on this software it looks to be very robust and very portable.

The underlying protocol that OpenVPN uses is SSL, just like amvpn. It appears the creator of this software product had the same mentality as the amvpn creator - use a fast, strong encryption suite to tunnel traffic through securely to a remote site.

As for the security that is used for OpenVPN, there are choices of no security, a pre-shared secret, or certificates. With no security, there is no authentication that takes place and probably should only be used to debug and troubleshoot. With a pre-shared secret, you can generate an alphanumeric key to create the tunnel. Finally, with certificates, this is the same idea as with amvpn. You can use X.509 certificates as your authentication enforcement. Unfortunately, there is no nice utility that comes with OpenVPN and does all the backend openssl calls. However, the OpenVPN website provides a lot of good information on this.

The encryption of this package includes all the ciphers that amvpn uses, because it uses the same openssl backend. I would imagine the throughput would be similar because of the same encryption techniques used.

The configuration seems to be straight-forward. It appears that all the configuration parameters can be tweaked on the command-line. Also, there seems to be a lot of parameters that can be tweaked. There are options that are similar to amvpn like using an http proxy with and without authentication, and running as a non-privileged user. There are also many options that are not included with amvpn, like traffic shaping and chroot'ing the program to a jailed directory.

Overall, on paper this solution looks very promising. Also, the development seems to be quite rapid. The creator has also released a version of this program for Win32. This opens a lot of opportunities for tunneling windows applications without the need for a separate machine for use as a gateway. And with the plethora of options, it is more than likely that this program will do what is needed to satisfy tunneling requirements. Definitely, this is an option to keep in mind.

Conclusion

In the setup of this example network many things were defaulted to show off the features and encryption of amvpn. In the grand scheme of an actual secure network, all systems would be hardened and patched; and firewall rules would be implemented on the

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

gateways, especially those that touch the Internet. It would also be beneficial in some situations to place a personal firewall on internal systems that may need a little extra security. Host-based IDS would also give even more benefit if it is warranted.

In a real world situation, the public-facing network adapter of the Linux machine would be connected to some sort of network device like a hub or switch which leads out to a service provider like an ISP (Internet Service Provider). The internal-facing network adapter of the Linux machine would be connected to another network device like a hub or switch that would be connected to an internal network.

Installation of amvpn turns out to be very easy. As long as there is a basic knowledge of how to move around in a *nix environment, it is quite simple. The package is small, but yet robust. The compiling is as straight-forward as it would be for any other package that would need to be compiled. The installation into the proper directory structure requires little effort, as well. The location of all the needed programs and utilities are placed in directories that are in the system's global path, meaning you can specify the command from anywhere in the directory structure of the system. This is especially helpful when first debugging and needing to be in different directories on the system.

Configuration has been made to be very simple as well. Many of the configuration options are defaulted, if they are not defined. This leads to a very quick configuration, if time is of the essence, in getting a solution together expediently. And the good thing is, it is still quite secure in a default configuration.

The heart and soul of the security mechanism lies within the certificates that are created for each machine that will be an endpoint. The certificates first need to be created with a helper program provided by amvpn, called amvpn-keytool. This utility front ends the openssl/ssh toolkits and produces the certificates. The certificates are the basis for the authentication and encryption of the tunnel.

Once the tunnel is created it encapsulates all packets that are being transmitted to the remote internal network. This prevents unauthorized access to the data that is being transmitted over the networking that is separating these two networks. This might be as close as within the same building, and might be as far away as the other side of the globe. In either case, the same result will occur; the data will be privatized and will only be usable by authorized members of the internal networks.

Overall, amvpn is a great product if getting a secure method of communication up and running in a short amount of time is required. The installation and configuration have been made to be very simple and straight-forward. The encryption used is strong, but is lightweight enough to be used in low-bandwidth situations. Even though there are competing packages out there, amvpn can be used to secure the transport.

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

Appendix A.1
Installation
(commands are in italics and launched from the command line in Linux)

Obtain the source code

- *wget http://umn.dl.sourceforge.net/sourceforge/amvpn/amvpn-0.98-2.tar.gz*

Untar the package

- *tar –zxvf amvpn-0.98-2.tar.gz*

Configure and make the package

- *cd amvpn-0.98-2; ./configure; make*

Install the package

- *make install*

© SANS Institute 2004, Author retains full rights.

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

Appendix B.1
Configuring /etc/amvpn.conf on server1

change:
tunnel-ip 192.168.16.1
add (after first route-ip/route-mask):
route-ip 192.168.2.0
route-mask 255.255.255.0

Effective configuration (excluding commented fields):

```
tunnel-ip 192.168.16.1
route-ip  192.168.16.0
route-mask 255.255.255.0
route-ip  192.168.2.0
route-mask 255.255.255.0
run-as-user amvpn
private-key-file /usr/share/amvpn/vpn_key.pem
cert-file /usr/share/amvpn/vpn_cert.pem
ca-cert-path /usr/share/amvpn/ca_cert.pem
```

© SANS Institute 2004, Author retains full rights.

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

Appendix B.1a
Route table of server1

```
root@server1:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt   Iface
192.168.2.0     0.0.0.0         255.255.255.0   U        40 0          0   tun0
192.168.1.0     0.0.0.0         255.255.255.0   U        40 0          0   eth1
192.168.0.0     0.0.0.0         255.255.255.0   U        40 0          0   eth0
192.168.16.0    0.0.0.0         255.255.255.0   U        40 0          0   tun0
127.0.0.0       0.0.0.0         255.0.0.0       U        40 0          0   lo
0.0.0.0         192.168.0.3     0.0.0.0         UG       40 0          0   eth0


*NOTE: An additional line would be present if you were using a provider for your gateway.
A line like this might appear, where 1.1.1.1 is the IP of your provider's gateway:

0.0.0.0         1.1.1.1     0.0.0.0         UG       40 0          0       eth0
```

© SANS Institute 2004, Author retains full rights.

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

Appendix B.2
Configuring /etc/amvpn.conf on server2

change:
tunnel-ip 192.168.16.2
server-ip 192.168.0.1
add (after first route-ip/route-mask):
route-ip 192.168.1.0
route-mask 255.255.255.0

Effective configuration (excluding commented fields):

```
tunnel-ip 192.168.16.2
server-ip  192.168.0.1
route-ip  192.168.16.0
route-mask 255.255.255.0
route-ip  192.168.1.0
route-mask 255.255.255.0
run-as-user amvpn
private-key-file /usr/share/amvpn/vpn_key.pem
cert-file /usr/share/amvpn/vpn_cert.pem
ca-cert-path /usr/share/amvpn/ca_cert.pem
```

© SANS Institute 2004, Author retains full rights.

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

Appendix B.2a
Route table of server2

```
root@server2:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt   Iface
192.168.2.0     0.0.0.0         255.255.255.0   U        40 0          0   eth1
192.168.1.0     0.0.0.0         255.255.255.0   U        40 0          0   tun0
192.168.0.0     0.0.0.0         255.255.255.0   U        40 0          0   eth0
192.168.16.0    0.0.0.0         255.255.255.0   U        40 0          0   tun0
127.0.0.0       0.0.0.0         255.0.0.0       U        40 0          0   lo


*NOTE: An additional line would be present if you were using a provider for your gateway.
A line like this might appear, where 1.1.1.1 is the IP of your provider's gateway:

0.0.0.0         1.1.1.1     0.0.0.0         UG       40 0          0       eth0
```

© SANS Institute 2004, Author retains full rights.

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

Appendix C.1
Generating the root CA certificate

```
root@server1:/usr/share# amvpn-keytool genca

amvpn-keytool: Please provide appropriate information for generating you CA Certificate

Generating RSA private key, 1024 bit long modulus
...++++++
.....++++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:IL
Locality Name (eg, city) []:Chicago
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SSLVPN
Organizational Unit Name (eg, section) []:SSLVPNOU
Common Name (eg, YOUR name) []:SSLVPNCN
Email Address []:root@rootca

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Signature ok
subject=/C=US/ST=IL/L=Chicago/O=SSLVPN/OU=SSLVPNOU/CN=SSLVPNCN/ema
ilAddress=root@rootca
Getting Private key
VPN CA certificate will be valid for 366 days
```

© SANS Institute 2004, Author retains full rights.

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

Appendix C.2
Generating certificate for server1

root@server1:/usr/share/amvpn# amvpn-keytool genkey

amvpn-keytool: Please provide appropriate information for generating the VPN CSR

Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:IL
Locality Name (eg, city) []:Chicago
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SSLVPN
Organizational Unit Name (eg, section) []:SSLVPNOU
Common Name (eg, YOUR name) []:server1.domain.com
Email Address []:root@server1.domain.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

root@server1:/usr/share/amvpn# amvpn-keytool gencert
Signature ok
subject=/C=US/ST=IL/L=Chicago/O=SSLVPN/OU=SSLVPNOU/CN=server1.domain.c
om/emailAddress=root@server1.domain.com
Getting CA Private Key
VPN certificate will be valid for 366 days

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

Appendix C.3
Generating certificate for server2

root@server2:/usr/share/amvpn# amvpn-keytool genkey

amvpn-keytool: Please provide appropriate information for generating the VPN CSR

Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:IL
Locality Name (eg, city) []:Chicago
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SSLVPN
Organizational Unit Name (eg, section) []:SSLVPNOU
Common Name (eg, YOUR name) []:server2.domain.com
Email Address []:root@server2.domain.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

© SANS Institute 2004, Author retains full rights.

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

Appendix D.1

Using amvpn-keytool to sign the certificate of server2

```
root@server1:~# amvpn-keytool -r root@192.168.0.2:/usr/share/amvpn gencert
Connecting to 192.168.0.2...
root@192.168.0.2's password:
Changing to: /usr/share/amvpn
Fetching /usr/share/amvpn/vpn_req.pem to remote_vpn_req.pem
Signature ok
subject=/C=US/ST=IL/L=Chicago/O=SSLVPN/OU=SSLVPNOU/CN=server2.domain.c
om/emailAddress=root@server2.domain.com
Getting CA Private Key
Uploading remote_vpn_cert.pem to /usr/share/amvpn/vpn_cert.pem
Uploading ca_cert.pem to /usr/share/amvpn/ca_cert.pem

VPN certificate will be valid for 366 days
To ensure that generated Cert has no problems such as clock-skew effects, run 'amvpn-
keytool validate' in the client system.
```

© SANS Institute 2004, Author retains full rights

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

Appendix D.2
Generating additional VPN cert keys manually

```
cd /tmp
openssl genrsa -out vpn_key.pem 1024
openssl req -new -key vpn_key.pem -out vpn_req.pem
openssl x509 -req -in vpn_req.pem -CA /usr/share/amvpn/ca_cert.pem –CAkey \
        /usr/share/amvpn/ca_key.pem -CAcreateserial -out vpn_cert.pem -days 366
```

© SANS Institute 2004, Author retains full rights.

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

Appendix E.1
Startup amvpn on server1

root@server1:/usr/share/amvpn# amvpn -V
Amrita Virtual Private Network Software. AmritaVPN 0.98-2.
Amrita Innovative Technology Foundation Labs, Amrita Institutions, India.
Web: http://aitf.amrita.edu.
All rights reserved.
config_get_value: Configuration option tunnel-if not set. Using the default value: tun0.
config_get_value: Configuration option port not set. Using the default value: 7171.
config_get_value: Configuration option route-smb not set. The option has no default value.
config_get_value: Configuration option max-pending-mails not set. Using the default value: 5.
config_get_value: Configuration option run-as-group not set. Using the default value: 0.
config_get_value: Configuration option tunnel-dev-path not set. Using the default value: /dev/net/tun.
config_get_value: Configuration option reconnect-attempts not set. Using the default value: -1.
config_get_value: Configuration option reconnect-delay not set. Using the default value: 30.
config_get_value: Configuration option notify-sender not set. The option has no default value.
notify_init: Setting notify-sender configuration option to the system-generated value: amvpn@server1
config_get_value: Configuration option smtp-server-ip not set. The option has no default value.
config_get_value: Configuration option proxy not set. The option has no default value.
config_get_value: Configuration option proxy-port not set. Using the default value: 3128.
config_get_value: Configuration option proxy not set. The option has no default value.
config_get_value: Configuration option proxy-port not set. Using the default value: 3128.
vpn_socket_open: Connection accepted from: 192.168.0.2:1025
vpn_ssl_open: Validated user: /C=US/ST=IL/L=Chicago/O=SSLVPN/OU=SSLVPNOU/CN=server2.domain.com/emailAddress=root@server2.domain.com
main_task: SSL handshake succeeded. Negotiating options.
main_task: Option negotiation succeeded. Starting to relay packets.
config_get_value: Configuration option proxy not set. The option has no default value.
config_get_value: Configuration option proxy-port not set. Using the default value: 3128.

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

Appendix E.2
Startup amvpn on server2

```
root@server2:/usr/share/amvpn# amvpn -V
Amrita Virtual Private Network Software. AmritaVPN 0.98-2.
Amrita Innovative Technology Foundation Labs, Amrita Institutions, India.
Web: http://aitf.amrita.edu.
All rights reserved.
config_get_value: Configuration option tunnel-if not set. Using the default value: tun0.
config_get_value: Configuration option port not set. Using the default value: 7171.
config_get_value: Configuration option route-smb not set. The option has no default
value.
config_get_value: Configuration option max-pending-mails not set. Using the default
value: 5.
config_get_value: Configuration option run-as-group not set. Using the default value: 0.
config_get_value: Configuration option tunnel-dev-path not set. Using the default value:
/dev/net/tun.
config_get_value: Configuration option reconnect-attempts not set. Using the default
value: -1.
config_get_value: Configuration option reconnect-delay not set. Using the default value:
30.
config_get_value: Configuration option notify-sender not set. The option has no default
value.
notify_init: Setting notify-sender configuration option to the system-generated value:
amvpn@server2
config_get_value: Configuration option smtp-server-ip not set. The option has no default
value.
config_get_value: Configuration option proxy not set. The option has no default value.
config_get_value: Configuration option proxy-port not set. Using the default value: 3128.
config_get_value: Configuration option proxy not set. The option has no default value.
config_get_value: Configuration option proxy-port not set. Using the default value: 3128.
vpn_socket_open: Connection Succeeded to Server 192.168.0.1:7171
vpn_ssl_open: Validated user:
/C=US/ST=IL/L=Chicago/O=SSLVPN/OU=SSLVPNOU/CN=server1.domain.com/emai
lAddress=root@server1.domain.com
main_task: SSL handshake succeeded.  Negotiating options.
main_task: Option negotiation succeeded. Starting to relay packets.
```


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

Appendix F.1
Trace for FTP on workstation1 using ethereal (readout by tcpdump)

```
10:10:47.762993 192.168.2.2.1053 > 192.168.1.2.ftp: S 3258689312:3258689312(0) win 64240
<mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 16de 4000 7e06 6195 c0a8 0202        E..0..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a720 0000 0000        .........;......
0x0020   7002 faf0 964b 0000 0204 05b4 0101 0402        p....K..........
10:10:47.763131 192.168.1.2.ftp > 192.168.2.2.1053: S 2114410217:2114410217(0) ack
3258689313 win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 4e3c 4000 8006 2837 c0a8 0102        E..0N<@...(7....
0x0010   c0a8 0202 0015 041d 7e07 56e9 c23b a721        ........~.V..;.!
0x0020   7012 faf0 c149 0000 0204 05b4 0101 0402        p....I..........
10:10:47.763696 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 1 win 64240 (DF)
0x0000   4500 0028 16df 4000 7e06 619c c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 56ea        .........;.!~.V.
0x0020   5010 faf0 ee0d 0000 7e7e 7e7e 7e7e             P.......~~~~~~
10:10:47.846892 192.168.1.2.ftp > 192.168.2.2.1053: P 1:62(61) ack 1 win 64240 (DF)
0x0000   4500 0065 4e3d 4000 8006 2801 c0a8 0102        E..eN=@...(.....
0x0010   c0a8 0202 0015 041d 7e07 56ea c23b a721        ........~.V..;.!
0x0020   5018 faf0 904d 0000 3232 302d 4775 696c        P....M..220-Guil
0x0030   6446 5450 6420 4654 5020 5365 7276 6572        dFTPd.FTP.Server
0x0040   2028 6329 2031 3939 372d 3230 3032 0d0a        .(c).1997-2002..
0x0050   3232 302d 5665 7273 696f 6e20 302e 3939        220-Version.0.99
0x0060   392e 390d 0a                                   9.9..
10:10:47.988859 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 62 win 64179 (DF)
0x0000   4500 0028 16e1 4000 7e06 619a c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5727        .........;.!~.W'
0x0020   5010 fab3 ee0d 0000 7e7e 7e7e 7e7e             P.......~~~~~~
10:10:47.989011 192.168.1.2.ftp > 192.168.2.2.1053: P 62:91(29) ack 1 win 64240 (DF)
0x0000   4500 0045 4e3f 4000 8006 281f c0a8 0102        E..EN?@...(.....
0x0010   c0a8 0202 0015 041d 7e07 5727 c23b a721        ........~.W';.!
0x0020   5018 faf0 4bf7 0000 3232 3020 506c 6561        P...K...220.Plea
0x0030   7365 2065 6e74 6572 2079 6f75 7220 6e61        se.enter.your.na
0x0040   6d65 3a0d 0a                                   me:..
10:10:48.189171 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 91 win 64150 (DF)
0x0000   4500 0028 16e3 4000 7e06 6198 c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5744        .........;.!~.WD
0x0020   5010 fa96 ee0d 0000 7e7e 7e7e 7e7e             P.......~~~~~~
10:10:50.306059 192.168.2.2.1053 > 192.168.1.2.ftp: P 1:17(16) ack 91 win 64150 (DF)
0x0000   4500 0038 16e4 4000 7e06 6187 c0a8 0202        E..8..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5744        .........;.!~.WD
0x0020   5018 fa96 6619 0000 5553 4552 2061 6e6f        P...f...USER.ano
0x0030   6e79 6d6f 7573 0d0a                            nymous..
10:10:50.315378 192.168.1.2.ftp > 192.168.2.2.1053: P 91:127(36) ack 17 win 64224 (DF)
0x0000   4500 004c 4e41 4000 8006 2816 c0a8 0102        E..LNA@...(.....
0x0010   c0a8 0202 0015 041d 7e07 5744 c23b a731        ........~.WD.;.1
0x0020   5018 fae0 607e 0000 3333 3120 5573 6572        P...`~..331.User
0x0030   206e 616d 6520 6f6b 6179 2c20 4e65 6564        .name.okay,.Need
0x0040   2070 6173 7377 6f72 642e 0d0a                  .password...
10:10:50.492706 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 127 win 64114 (DF)
0x0000   4500 0028 16e5 4000 7e06 6196 c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a731 7e07 5768        .........;.1~.Wh
0x0020   5010 fa72 edfd 0000 7e7e 7e7e 7e7e             P..r....~~~~~~
10:10:52.397430 192.168.2.2.1053 > 192.168.1.2.ftp: P 17:30(13) ack 127 win 64114 (DF)
0x0000   4500 0035 16e6 4000 7e06 6188 c0a8 0202        E..5..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a731 7e07 5768        .........;.1~.Wh
0x0020   5018 fa72 f705 0000 5041 5353 2067 7565        P..r....PASS.gue
0x0030   7374 400d 0a                                   st@..
10:10:52.482411 192.168.1.2.ftp > 192.168.2.2.1053: P 127:148(21) ack 30 win 64211 (DF)
0x0000   4500 003d 4e42 4000 8006 2824 c0a8 0102        E..=NB@...($....
0x0010   c0a8 0202 0015 041d 7e07 5768 c23b a73e        ........~.Wh.;.>
0x0020   5018 fad3 d364 0000 3233 3020 5573 6572        P....d..230.User
0x0030   206c 6f67 6765 6420 696e 2e0d 0a               .logged.in...
10:10:52.595548 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 148 win 64093 (DF)
0x0000   4500 0028 16e7 4000 7e06 6194 c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a73e 7e07 577d        .........;.>~.W}
0x0020   5010 fa5d edf0 0000 7e7e 7e7e 7e7e             P..]....~~~~~~
```


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

Appendix F.2
Tap trace for FTP using tcpdump (readout by tcpdump)

```
10:10:47.239845 192.168.2.2.1053 > 192.168.1.2.ftp: S 3258689312:3258689312(0) win 64240
<mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 16de 4000 7f06 6095 c0a8 0202        E..0..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a720 0000 0000        .........;......
0x0020   7002 faf0 964b 0000 0204 05b4 0101 0402        p....K..........
10:10:47.240379 192.168.1.2.ftp > 192.168.2.2.1053: S 2114410217:2114410217(0) ack
3258689313 win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 4e3c 4000 7f06 2937 c0a8 0102        E..0N<@...)7....
0x0010   c0a8 0202 0015 041d 7e07 56e9 c23b a721        ........~.V..;.!
0x0020   7012 faf0 c149 0000 0204 05b4 0101 0402        p....I..........
10:10:47.240720 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 1 win 64240 (DF)
0x0000   4500 0028 16df 4000 7f06 609c c0a8 0202        E..(..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 56ea        .........;.!~.V.
0x0020   5010 faf0 ee0d 0000 7e7e 7e7e 7e7e             P.......~~~~~~
10:10:47.324151 192.168.1.2.ftp > 192.168.2.2.1053: P 1:62(61) ack 1 win 64240 (DF)
0x0000   4500 0065 4e3d 4000 7f06 2901 c0a8 0102        E..eN=@...).....
0x0010   c0a8 0202 0015 041d 7e07 56ea c23b a721        ........~.V..;.!
0x0020   5018 faf0 904d 0000 3232 302d 4775 696c        P....M..220-Guil
0x0030   6446 5450 6420 4654 5020 5365 7276 6572        dFTPd.FTP.Server
0x0040   2028 6329 2031 3939 372d 3230 3032 0d0a        .(c).1997-2002..
0x0050   3232 302d 5665 7273 696f 6e20 302e 3939        220-Version.0.99
0x0060   392e 390d 0a                                   9.9..
10:10:47.465816 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 62 win 64179 (DF)
0x0000   4500 0028 16e1 4000 7f06 609a c0a8 0202        E..(..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5727        .........;.!~.W'
0x0020   5010 fab3 ee0d 0000 7e7e 7e7e 7e7e             P.......~~~~~~
10:10:47.466254 192.168.1.2.ftp > 192.168.2.2.1053: P 62:91(29) ack 1 win 64240 (DF)
0x0000   4500 0045 4e3f 4000 7f06 291f c0a8 0102        E..EN?@...).....
0x0010   c0a8 0202 0015 041d 7e07 5727 c23b a721        ........~.W'.;.!
0x0020   5018 faf0 4bf7 0000 3232 3020 506c 6561        P...K...220.Plea
0x0030   7365 2065 6e74 6572 2079 6f75 7220 6e61        se.enter.your.na
0x0040   6d65 3a0d 0a                                   me:..
10:10:47.666108 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 91 win 64150 (DF)
0x0000   4500 0028 16e3 4000 7f06 6098 c0a8 0202        E..(..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5744        .........;.!~.WD
0x0020   5010 fa96 ee0d 0000 7e7e 7e7e 7e7e             P.......~~~~~~
10:10:49.782994 192.168.2.2.1053 > 192.168.1.2.ftp: P 1:17(16) ack 91 win 64150 (DF)
0x0000   4500 0038 16e4 4000 7f06 6087 c0a8 0202        E..8..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5744        .........;.!~.WD
0x0020   5018 fa96 6619 0000 5553 4552 2061 6e6f        P...f...USER.ano
0x0030   6e79 6d6f 7573 0d0a                            nymous..
10:10:49.792650 192.168.1.2.ftp > 192.168.2.2.1053: P 91:127(36) ack 17 win 64224 (DF)
0x0000   4500 004c 4e41 4000 7f06 2916 c0a8 0102        E..LNA@...).....
0x0010   c0a8 0202 0015 041d 7e07 5744 c23b a731        ........~.WD.;.1
0x0020   5018 fae0 607e 0000 3333 3120 5573 6572        P...`~..331.User
0x0030   206e 616d 6520 6f6b 6179 2c20 4e65 6564        .name.okay,.Need
0x0040   2070 6173 7377 6f72 642e 0d0a                  .password...
10:10:49.969446 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 127 win 64114 (DF)
0x0000   4500 0028 16e5 4000 7f06 6096 c0a8 0202        E..(..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a731 7e07 5768        .........;.1~.Wh
0x0020   5010 fa72 edfd 0000 7e7e 7e7e 7e7e             P..r....~~~~~~
10:10:51.874327 192.168.2.2.1053 > 192.168.1.2.ftp: P 17:30(13) ack 127 win 64114 (DF)
0x0000   4500 0035 16e6 4000 7f06 6088 c0a8 0202        E..5..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a731 7e07 5768        .........;.1~.Wh
0x0020   5018 fa72 f705 0000 5041 5353 2067 7565        P..r....PASS.gue
0x0030   7374 400d 0a                                   st@..
10:10:51.959705 192.168.1.2.ftp > 192.168.2.2.1053: P 127:148(21) ack 30 win 64211 (DF)
0x0000   4500 003d 4e42 4000 7f06 2924 c0a8 0102        E..=NB@...)$....
0x0010   c0a8 0202 0015 041d 7e07 5768 c23b a73e        ........~.Wh.;.>
0x0020   5018 fad3 d364 0000 3233 3020 5573 6572        P....d..230.User
0x0030   206c 6f67 6765 6420 696e 2e0d 0a               .logged.in...
10:10:52.072451 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 148 win 64093 (DF)
0x0000   4500 0028 16e7 4000 7f06 6094 c0a8 0202        E..(..@...`.....
0x0010   c0a8 0102 041d 0015 c23b a73e 7e07 577d        .........;.>~.W}
0x0020   5010 fa5d edf0 0000 7e7e 7e7e 7e7e             P..]....~~~~~~
```


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

Appendix F.3

Trace for FTP on server1(eth1) using tcpdump (readout by tcpdump)

```
10:10:47.239883 192.168.2.2.1053 > 192.168.1.2.ftp: S 3258689312:3258689312(0) win 64240
<mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 16de 4000 7e06 6195 c0a8 0202        E..0..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a720 0000 0000        .........;......
0x0020   7002 faf0 964b 0000 0204 05b4 0101 0402        p....K..........
10:10:47.240358 192.168.1.2.ftp > 192.168.2.2.1053: S 2114410217:2114410217(0) ack
3258689313 win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 4e3c 4000 8006 2837 c0a8 0102        E..0N<@...(7....
0x0010   c0a8 0202 0015 041d 7e07 56e9 c23b a721        ........~.V..;.!
0x0020   7012 faf0 c149 0000 0204 05b4 0101 0402        p....I..........
10:10:47.240742 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 1 win 64240 (DF)
0x0000   4500 0028 16df 4000 7e06 619c c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 56ea        .........;.!~.V.
0x0020   5010 faf0 ee0d 0000                            P.......
10:10:47.324131 192.168.1.2.ftp > 192.168.2.2.1053: P 1:62(61) ack 1 win 64240 (DF)
0x0000   4500 0065 4e3d 4000 8006 2801 c0a8 0102        E..eN=@...(.....
0x0010   c0a8 0202 0015 041d 7e07 56ea c23b a721        ........~.V..;.!
0x0020   5018 faf0 904d 0000 3232 302d 4775 696c        P....M..220-Guil
0x0030   6446 5450 6420 4654 5020 5365 7276 6572        dFTPd.FTP.Server
0x0040   2028 6329 2031 3939 372d 3230 3032 0d0a        .(c).1997-2002..
0x0050   3232 302d 5665 7273 696f 6e20 302e 3939        220-Version.0.99
0x0060   392e 390d 0a                                   9.9..
10:10:47.465835 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 62 win 64179 (DF)
0x0000   4500 0028 16e1 4000 7e06 619a c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5727        .........;.!~.W'
0x0020   5010 fab3 ee0d 0000                            P.......
10:10:47.466236 192.168.1.2.ftp > 192.168.2.2.1053: P 62:91(29) ack 1 win 64240 (DF)
0x0000   4500 0045 4e3f 4000 8006 281f c0a8 0102        E..EN?@...(.....
0x0010   c0a8 0202 0015 041d 7e07 5727 c23b a721        ........~.W'.;.!
0x0020   5018 faf0 4bf7 0000 3232 3020 506c 6561        P...K...220.Plea
0x0030   7365 2065 6e74 6572 2079 6f75 7220 6e61        se.enter.your.na
0x0040   6d65 3a0d 0a                                   me:..
10:10:47.666127 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 91 win 64150 (DF)
0x0000   4500 0028 16e3 4000 7e06 6198 c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5744        .........;.!~.WD
0x0020   5010 fa96 ee0d 0000                            P.......
10:10:49.783020 192.168.2.2.1053 > 192.168.1.2.ftp: P 1:17(16) ack 91 win 64150 (DF)
0x0000   4500 0038 16e4 4000 7e06 6187 c0a8 0202        E..8..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a721 7e07 5744        .........;.!~.WD
0x0020   5018 fa96 6619 0000 5553 4552 2061 6e6f        P...f...USER.ano
0x0030   6e79 6d6f 7573 0d0a                            nymous..
10:10:49.792631 192.168.1.2.ftp > 192.168.2.2.1053: P 91:127(36) ack 17 win 64224 (DF)
0x0000   4500 004c 4e41 4000 8006 2816 c0a8 0102        E..LNA@...(.....
0x0010   c0a8 0202 0015 041d 7e07 5744 c23b a731        ........~.WD.;.1
0x0020   5018 fae0 607e 0000 3333 3120 5573 6572        P...`~..331.User
0x0030   206e 616d 6520 6f6b 6179 2c20 4e65 6564        .name.okay,.Need
0x0040   2070 6173 7377 6f72 642e 0d0a                  .password...
10:10:49.969468 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 127 win 64114 (DF)
0x0000   4500 0028 16e5 4000 7e06 6196 c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a731 7e07 5768        .........;.1~.Wh
0x0020   5010 fa72 edfd 0000                            P..r....
10:10:51.874363 192.168.2.2.1053 > 192.168.1.2.ftp: P 17:30(13) ack 127 win 64114 (DF)
0x0000   4500 0035 16e6 4000 7e06 6188 c0a8 0202        E..5..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a731 7e07 5768        .........;.1~.Wh
0x0020   5018 fa72 f705 0000 5041 5353 2067 7565        P..r....PASS.gue
0x0030   7374 400d 0a                                   st@..
10:10:51.959687 192.168.1.2.ftp > 192.168.2.2.1053: P 127:148(21) ack 30 win 64211 (DF)
0x0000   4500 003d 4e42 4000 8006 2824 c0a8 0102        E..=NB@...($....
0x0010   c0a8 0202 0015 041d 7e07 5768 c23b a73e        ........~.Wh.;.>
0x0020   5018 fad3 d364 0000 3233 3020 5573 6572        P....d..230.User
0x0030   206c 6f67 6765 6420 696e 2e0d 0a                .logged.in...
10:10:52.072473 192.168.2.2.1053 > 192.168.1.2.ftp: . ack 148 win 64093 (DF)
0x0000   4500 0028 16e7 4000 7e06 6194 c0a8 0202        E..(..@.~.a.....
0x0010   c0a8 0102 041d 0015 c23b a73e 7e07 577d        .........;.>~.W}
0x0020   5010 fa5d edf0 0000                            P..]....
```


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

Appendix G.1
Trace for FTP on wokstation1 using ethereal (readout by tcpdump)

```
11:50:28.476816 192.168.2.2.1062 > 192.168.1.2.ftp: S 449048905:449048905(0) win 64240
<mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 1753 4000 7e06 6120 c0a8 0202        E..0.S@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f149 0000 0000        .....&.....I....
0x0020   7002 faf0 f391 0000 0204 05b4 0101 0402        p...............
11:50:28.476956 192.168.1.2.ftp > 192.168.2.2.1062: S 3600064008:3600064008(0) ack
449048906 win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 4f0c 4000 8006 2767 c0a8 0102        E..0O.@...'g....
0x0010   c0a8 0202 0015 0426 d694 9e08 1ac3 f14a        .......&.......J
0x0020   7012 faf0 7ee3 0000 0204 05b4 0101 0402        p...~...........
11:50:28.478730 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 1 win 64240 (DF)
0x0000   4500 0028 1754 4000 7e06 6127 c0a8 0202        E..(.T@.~.a'....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e09        .....&.....J....
0x0020   5010 faf0 aba7 0000 7e7e 7e7e 7e7e             P.......~~~~~~
11:50:28.570809 192.168.1.2.ftp > 192.168.2.2.1062: P 1:62(61) ack 1 win 64240 (DF)
0x0000   4500 0065 4f0d 4000 8006 2731 c0a8 0102        E..eO.@...'1....
0x0010   c0a8 0202 0015 0426 d694 9e09 1ac3 f14a        .......&.......J
0x0020   5018 faf0 4de7 0000 3232 302d 4775 696c        P...M...220-Guil
0x0030   6446 5450 6420 4654 5020 5365 7276 6572        dFTPd.FTP.Server
0x0040   2028 6329 2031 3939 372d 3230 3032 0d0a        .(c).1997-2002..
0x0050   3232 302d 5665 7273 696f 6e20 302e 3939        220-Version.0.99
0x0060   392e 390d 0a                                   9.9..
11:50:28.712533 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 62 win 64179 (DF)
0x0000   4500 0028 1756 4000 7e06 6125 c0a8 0202        E..(.V@.~.a%....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e46        .....&.....J...F
0x0020   5010 fab3 aba7 0000 7e7e 7e7e 7e7e             P.......~~~~~~
11:50:28.712677 192.168.1.2.ftp > 192.168.2.2.1062: P 62:91(29) ack 1 win 64240 (DF)
0x0000   4500 0045 4f0f 4000 8006 274f c0a8 0102        E..EO.@...'O....
0x0010   c0a8 0202 0015 0426 d694 9e46 1ac3 f14a        .......&...F...J
0x0020   5018 faf0 0991 0000 3232 3020 506c 6561        P.......220.Plea
0x0030   7365 2065 6e74 6572 2079 6f75 7220 6e61        se.enter.your.na
0x0040   6d65 3a0d 0a                                   me:..
11:50:28.912827 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 91 win 64150 (DF)
0x0000   4500 0028 1757 4000 7e06 6124 c0a8 0202        E..(.W@.~.a$....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e63        .....&.....J...c
0x0020   5010 fa96 aba7 0000 7e7e 7e7e 7e7e             P.......~~~~~~
11:50:31.477934 192.168.2.2.1062 > 192.168.1.2.ftp: P 1:17(16) ack 91 win 64150 (DF)
0x0000   4500 0038 1759 4000 7e06 6112 c0a8 0202        E..8.Y@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e63        .....&.....J...c
0x0020   5018 fa96 23b3 0000 5553 4552 2061 6e6f        P...#...USER.ano
0x0030   6e79 6d6f 7573 0d0a                            nymous..
11:50:31.487123 192.168.1.2.ftp > 192.168.2.2.1062: P 91:127(36) ack 17 win 64224 (DF)
0x0000   4500 004c 4f11 4000 8006 2746 c0a8 0102        E..LO.@...'F....
0x0010   c0a8 0202 0015 0426 d694 9e63 1ac3 f15a        .......&...c...Z
0x0020   5018 fae0 1e18 0000 3333 3120 5573 6572        P.......331.User
0x0030   206e 616d 6520 6f6b 6179 2c20 4e65 6564        .name.okay,.Need
0x0040   2070 6173 7377 6f72 642e 0d0a                  .password...
11:50:31.616719 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 127 win 64114 (DF)
0x0000   4500 0028 175a 4000 7e06 6121 c0a8 0202        E..(.Z@.~.a!....
0x0010   c0a8 0102 0426 0015 1ac3 f15a d694 9e87        .....&.....Z....
0x0020   5010 fa72 ab97 0000 7e7e 7e7e 7e7e             P..r....~~~~~~
11:50:33.449633 192.168.2.2.1062 > 192.168.1.2.ftp: P 17:30(13) ack 127 win 64114 (DF)
0x0000   4500 0035 175b 4000 7e06 6113 c0a8 0202        E..5.[@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f15a d694 9e87        .....&.....Z....
0x0020   5018 fa72 b49f 0000 5041 5353 2067 7565        P..r....PASS.gue
0x0030   7374 400d 0a                                   st@..
11:50:33.535620 192.168.1.2.ftp > 192.168.2.2.1062: P 127:148(21) ack 30 win 64211 (DF)
0x0000   4500 003d 4f12 4000 8006 2754 c0a8 0102        E..=O.@...'T....
0x0010   c0a8 0202 0015 0426 d694 9e87 1ac3 f167        .......&.......g
0x0020   5018 fad3 90fe 0000 3233 3020 5573 6572        P.......230.User
0x0030   206c 6f67 6765 6420 696e 2e0d 0a               .logged.in...
11:50:33.719748 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 148 win 64093 (DF)
0x0000   4500 0028 175d 4000 7e06 611e c0a8 0202        E..(.]@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f167 d694 9e9c        .....&.....g....
0x0020   5010 fa5d ab8a 0000 7e7e 7e7e 7e7e             P..]....~~~~~~
```


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

Appendix G.2
Tap trace for FTP using tcpdump (readout by tcpdump)

```
11:50:28.280233 192.168.0.2.1054 > 192.168.0.1.7171: P 229961972:229962094(122) ack
200170552 win 8328 <nop,nop,timestamp 302625600 633552> (DF)
0x0000   4500 00ae f28e 4000 4006 c667 c0a8 0002        E.....@.@..g....
0x0010   c0a8 0001 041e 1c03 0db4 f0f4 0bee 5c38        ..............\8
0x0020   8018 2088 cb8f 0000 0101 080a 1209 b340        ..............@
0x0030   0009 aad0 1703 0000 20e1 8212 4548 58a9        ............EHX.
0x0040   b42c 0cf8 46e9 b3fd 0682 221d c4ae 99c2        .,..F.....".....
0x0050   ced1 8b87 4133 0bfa 8f17 0300 0050 03ee        ....A3.......P..
0x0060   ac65 3372 456d f933 9bb6 169f e0ad cff4        .e3rEm.3........
0x0070   46f0 c45d 269f 1fb8 46c5 2e02 dd6a 1402        F..]&...F....j..
0x0080   73f5 1892 ed23 a954 04ae 602b dc38 bb0a        s....#.T..`+.8..
0x0090   f265 0287 d580 ea72 f7c5 590c 2151 f461        .e.....r..Y.!Q.a
0x00a0   dfcb f584 a54e 0cdd abb8 f67d 9b59             .....N.....}.Y
11:50:28.280324 192.168.0.1.7171 > 192.168.0.2.1054: . ack 122 win 17376
<nop,nop,timestamp 640296 302625600> (DF)
0x0000   4500 0034 0a63 4000 4006 af0d c0a8 0001        E..4.c@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5c38 0db4 f16e        ..........\8...n
0x0020   8010 43e0 9fa3 0000 0101 080a 0009 c528        ..C............(
0x0030   1209 b340                                      ...@
11:50:28.281572 192.168.0.1.7171 > 192.168.0.2.1054: P 1:123(122) ack 122 win 17376
<nop,nop,timestamp 640296 302625600> (DF)
0x0000   4500 00ae 0a64 4000 4006 ae92 c0a8 0001        E....d@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5c38 0db4 f16e        ..........\8...n
0x0020   8018 43e0 ae09 0000 0101 080a 0009 c528        ..C............(
0x0030   1209 b340 1703 0000 208a 1476 eba4 05b9        ...@.......v....
0x0040   df97 60d6 67be 99eb cb11 5046 3a83 1da2        ..`.g.....PF:...
0x0050   10ca 46ad 9b41 e222 7117 0300 0050 ad7e        ..F..A."q....P.~
0x0060   1044 9b43 6dae 579b 5bd8 88da 959b a99d        .D.Cm.W.[.......
0x0070   032e c1b1 5ffc 9acc 4c86 a8b8 bacd e084        ...._...L.......
0x0080   5ec6 42f6 b9ea 0f7d abb9 7123 6a87 5889        ^.B....}..q#j.X.
0x0090   280a ba10 a880 d531 eb56 9f55 1b1c 6a77        (......1.V.U..jw
0x00a0   f2c7 46ca 0f5a d39c b100 5cea 3cd3             ..F..Z....\.<.
11:50:28.281650 192.168.0.2.1054 > 192.168.0.1.7171: . ack 123 win 8328
<nop,nop,timestamp 302625600 640296> (DF)
0x0000   4500 0034 f28f 4000 4006 c6e0 c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f16e 0bee 5cb2        ...........n..\.
0x0020   8010 2088 c281 0000 0101 080a 1209 b340        ..............@
0x0030   0009 c528                                      ...(
11:50:28.282523 192.168.0.2.1054 > 192.168.0.1.7171: P 122:228(106) ack 123 win 8328
<nop,nop,timestamp 302625600 640296> (DF)
0x0000   4500 009e f290 4000 4006 c675 c0a8 0002        E.....@.@..u....
0x0010   c0a8 0001 041e 1c03 0db4 f16e 0bee 5cb2        ...........n..\.
0x0020   8018 2088 a388 0000 0101 080a 1209 b340        ..............@
0x0030   0009 c528 1703 0000 20d2 a56d 6f12 2af2        ...(.......mo.*.
0x0040   f61b 934c b20d 6864 02d7 ebec 1a5e 1272        ...L..hd.....^.r
0x0050   7ce8 b45f fb50 d80f 6917 0300 0040 fa45        |.._.P..i....@.E
0x0060   2b65 bd33 2c70 c3cd 40f5 625b 1300 61e1        +e.3,p..@.b[..a.
0x0070   9f4d 3526 b79e da75 67e1 feac 79ed 2750        .M5&...ug...y.'P
0x0080   88b7 8a63 1523 c019 3b20 047a bad5 3acd        ...c.#..;..z..:.
0x0090   03fe 188a 0b05 d6dd 21d4 4894 96c4             ........!.H...
11:50:28.318112 192.168.0.1.7171 > 192.168.0.2.1054: . ack 228 win 17376
<nop,nop,timestamp 640300 302625600> (DF)
0x0000   4500 0034 0a65 4000 4006 af0b c0a8 0001        E..4.e@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5cb2 0db4 f1d8        ..........\.....
0x0020   8010 43e0 9ebb 0000 0101 080a 0009 c52c        ..C............,
0x0030   1209 b340                                      ...@
11:50:28.375480 192.168.0.1.7171 > 192.168.0.2.1054: P 123:293(170) ack 228 win 17376
<nop,nop,timestamp 640305 302625600> (DF)
0x0000   4500 00de 0a66 4000 4006 ae60 c0a8 0001        E....f@.@..`....
0x0010   c0a8 0002 1c03 041e 0bee 5cb2 0db4 f1d8        ..........\.....
0x0020   8018 43e0 24f9 0000 0101 080a 0009 c531        ..C.$..........1
0x0030   1209 b340 1703 0000 2002 2405 5fa0 bf88        ...@...... $._...
0x0040   8fd6 5035 876f f385 24ca bd4c e71d c891        ..P5.o..$..L....
0x0050   53fb 8c92 fdc7 1db7 4817 0300 0080 fe4b        S.......H......K
0x0060   dced 923a 58c6 2359 a61b e109 c1d5 a945        ...:X.#Y.......E
0x0070   f88d 6fd0 7487 589f 43a1 c7f9 c068 b8da        ..o.t.X.C....h..
```


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

```
0x0080   68c8 bd0f dffa 4e87 0886 57d5 a5af 154e        h.....N...W....N
0x0090   cb85 3e9d 3cc6 65a1 f233 411b 676a 5020        ..>.<.e..3A.gjP.
0x00a0   e4b3 9e00 47c3 68d9 b04e 5d88 1cd9 b408        ....G.h..N].....
0x00b0   a5bf 1fb3 bb12 bcf6 07ea b617 bc61 b42a        .............a.*
0x00c0   ee6d 8234 244d 2c0d 4fa3 edf0 cc56 6e5e        .m.4$M,.O....Vn^
0x00d0   8a62 6994 3424 9067 5495 a79d c10a             .bi.4$.gT.....
11:50:28.414759 192.168.0.2.1054 > 192.168.0.1.7171: . ack 293 win 8328
<nop,nop,timestamp 302625614 640305> (DF)
0x0000   4500 0034 f291 4000 4006 c6de c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f1d8 0bee 5d5c        ..............]\
0x0020   8010 2088 c156 0000 0101 080a 1209 b34e        .....V.........N
0x0030   0009 c531                                      ...1
11:50:28.415086 192.168.0.1.7171 > 192.168.0.2.1054: P 293:447(154) ack 228 win 17376
<nop,nop,timestamp 640309 302625614> (DF)
0x0000   4500 00ce 0a67 4000 4006 ae6f c0a8 0001        E....g@.@..o....
0x0010   c0a8 0002 1c03 041e 0bee 5d5c 0db4 f1d8        ..........]\....
0x0020   8018 43e0 1e5a 0000 0101 080a 0009 c535        ..C..Z.........5
0x0030   1209 b34e 1703 0000 2093 34c0 174f b59e        ...N......4..O..
0x0040   56a3 64be 2abd dd13 c70c 2c83 9948 81e8        V.d.*.....,..H..
0x0050   f1e4 c9d2 b2c7 7eff 9917 0300 0070 cb0f        ......~......p..
0x0060   49a9 e930 e593 da2a 38dd d733 2841 ab51        I..0...*8..3(A.Q
0x0070   7a94 59ad c308 bec2 b245 20ec c307 3595        z.Y......E....5.
0x0080   8ffc 3619 e4e5 a4eb 35b7 c295 bbb5 c4f6        ..6.....5.......
0x0090   c72a 2c49 1b21 5105 2df8 8f84 de2f df43        .*,I.!Q.-..../.C
0x00a0   6d47 3852 9f06 7e4c 6f32 4129 4e1c f213        mG8R..~Lo2A)N...
0x00b0   97a6 c902 00fe 9322 b35e c54d f21e b405        .......".^.M....
0x00c0   ec8f 674e 6b26 8690 d4a4 ba34 e7a8             ..gNk&.....4..
11:50:28.415329 192.168.0.2.1054 > 192.168.0.1.7171: . ack 447 win 8328
<nop,nop,timestamp 302625614 640309> (DF)
0x0000   4500 0034 f292 4000 4006 c6dd c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f1d8 0bee 5df6        ..............].
0x0020   8010 2088 c0b8 0000 0101 080a 1209 b34e        ..............N
0x0030   0009 c535                                      ...5
11:50:28.416423 192.168.0.2.1054 > 192.168.0.1.7171: P 228:558(330) ack 447 win 8328
<nop,nop,timestamp 302625614 640309> (DF)
0x0000   4500 017e f293 4000 4006 c592 c0a8 0002        E..~..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f1d8 0bee 5df6        ..............].
0x0020   8018 2088 8fa3 0000 0101 080a 1209 b34e        ..............N
0x0030   0009 c535 1703 0000 20dd 47c6 10f7 6619        ...5......G...f.
0x0040   2f4e 779d 2696 fdf7 bb90 4abe f4eb 6c08        /Nw.&.....J...l.
0x0050   402d b393 c707 1053 3617 0300 0120 45b1        @-.....S6.....E.
0x0060   8d48 6360 b0ca 446d 117d 8bbd bae6 9621        .Hc`..Dm.}.....!
0x0070   9320 3114 ccba b587 6987 99cb 4d39 4f97        ..1.....i...M9O.
0x0080   e05e eeba 83af bdfd 8f08 749f ce0d 6f9e        .^........t...o.
0x0090   cf5f 15ba 9305 3580 49f0 09f3 15ef 7e84        ._....5.I.....~.
0x00a0   ddaf 15e7 6eac 0f32 64e0 f8d8 3676 ac55        ....n..2d...6v.U
0x00b0   d163 cc25 430c 6f14 024b fe65 4a3b 2487        .c.%C.o..K.eJ;$.
0x00c0   9c7c 17c9 143e 7f76 d3f7 8a89 ea0a f793        .|...>.v........
0x00d0   35b5 c7fb 51ec 541e e8ea 6a8b c35c e236        5...Q.T...j..\.6
0x00e0   29be a7e2 c691 037b 16e9 16b9 d8b4 650c        ).......{......e.
0x00f0   ecea cb00 20d2 a756 623b 8b91 54ae 8a5c        .......Vb;..T..\
0x0100   6c7b 215a c446 028f 90a0 7d79 b986 2022        l{!Z.F....}y..."
0x0110   fb54 8e6c d7da 0eec e8ac 9deb 02b6 ee46        .T.l...........F
0x0120   ac42 e1d6 72f5 01a6 6d5f c434 cb3b 9036        .B..r...m_.4.;.6
0x0130   85b1 a3db d3f7 e3cc f063 73e5 3f25 67bf        .........cs.?%g.
0x0140   794c 3099 603a 0894 a41c 6c45 14a5 ab5a        yL0.`:....lE...Z
0x0150   81eb 4eff 85ff e762 83fb d795 270d 2221        ..N....b....'."!
0x0160   903d 8b49 eb7f 8043 fdf4 9021 5b2f 3aeb        .=.I...C...![/:.
0x0170   53e0 f5ed 9683 c827 69f4 5917 b098             S......'i.Y...
11:50:28.416458 192.168.0.1.7171 > 192.168.0.2.1054: . ack 558 win 17376
<nop,nop,timestamp 640309 302625614> (DF)
0x0000   4500 0034 0a68 4000 4006 af08 c0a8 0001        E..4.h@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5df6 0db4 f322        ..........]....."
0x0020   8010 43e0 9c16 0000 0101 080a 0009 c535        ..C............5
0x0030   1209 b34e                                      ...N
11:50:28.516250 192.168.0.2.1054 > 192.168.0.1.7171: P 558:664(106) ack 447 win 8328
<nop,nop,timestamp 302625624 640309> (DF)
0x0000   4500 009e f294 4000 4006 c671 c0a8 0002        E.....@.@..q....
0x0010   c0a8 0001 041e 1c03 0db4 f322 0bee 5df6        ..........."..].
0x0020   8018 2088 90a0 0000 0101 080a 1209 b358        ..............X
0x0030   0009 c535 1703 0000 20fa 42a0 eba2 eb84        ...5......B.....
```


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

```
0x0040   4008 4d89 bd50 d2b6 63fe 7872 1d3c e4a0        @.M..P..c.xr.<..
0x0050   7bbb 27e5 5e8e 7d89 2517 0300 0040 f7d3        {.'.^.}.%....@..
0x0060   03eb 99d5 a770 d197 8a6b 6a8e dcb6 27c3        .....p...kj...'.
0x0070   9f3d fff4 67f3 d8d8 8274 835d d60e e1f0        .=..g....t.]....
0x0080   cec5 4253 66a9 7e34 3e42 53f8 db85 38f8        ..BSf.~4>BS...8.
0x0090   389f f902 7b84 d59d fd40 30d9 4526              8...{....@0.E&
11:50:28.516446 192.168.0.1.7171 > 192.168.0.2.1054: . ack 664 win 17376
<nop,nop,timestamp 640319 302625624> (DF)
0x0000   4500 0034 0a69 4000 4006 af07 c0a8 0001        E..4.i@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5df6 0db4 f38c        ..........].....
0x0020   8010 43e0 9b98 0000 0101 080a 0009 c53f        ..C............?
0x0030   1209 b358                                      ...X
11:50:28.517296 192.168.0.1.7171 > 192.168.0.2.1054: P 447:585(138) ack 664 win 17376
<nop,nop,timestamp 640319 302625624> (DF)
0x0000   4500 00be 0a6a 4000 4006 ae7c c0a8 0001        E....j@.@..|....
0x0010   c0a8 0002 1c03 041e 0bee 5df6 0db4 f38c        ..........].....
0x0020   8018 43e0 d24a 0000 0101 080a 0009 c53f        ..C..J.........?
0x0030   1209 b358 1703 0000 20b6 fb95 19a7 8162        ...X.........b
0x0040   8cf3 4b62 0f64 5823 596d b74c 6b40 4168        ..Kb.dX#Ym.Lk@Ah
0x0050   366f 59f1 0c7c 2af4 e517 0300 0060 cb68        6oY..|*......`.h
0x0060   b227 3073 2118 ee4a 8204 03fa a4c9 a4de        .'0s!..J........
0x0070   3fbb f20f 8d72 9bb9 9ec3 9ce1 f57d eec7        ?....r.......}..
0x0080   bcdc d68b 16e4 293b 7e54 c21f 71a4 290c        ......);~T..q.).
0x0090   b201 f141 43a2 471b de8e dfdb cf84 c13f        ...AC.G........?
0x00a0   b63e d1da ac34 602c da7a bebe 983b 4a1b        .>...4`,.z...;J.
0x00b0   1947 2a1b 60dc 5958 1d6b 0b74 e28b              .G*.`.YX.k.t..
11:50:28.554761 192.168.0.2.1054 > 192.168.0.1.7171: . ack 585 win 8328
<nop,nop,timestamp 302625628 640319> (DF)
0x0000   4500 0034 f295 4000 4006 c6da c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f38c 0bee 5e80        ..............^.
0x0020   8010 2088 be62 0000 0101 080a 1209 b35c        .....b.........\
0x0030   0009 c53f                                      ...?
11:50:28.716583 192.168.0.2.1054 > 192.168.0.1.7171: P 664:770(106) ack 585 win 8328
<nop,nop,timestamp 302625644 640319> (DF)
0x0000   4500 009e f296 4000 4006 c66f c0a8 0002        E.....@.@..o....
0x0010   c0a8 0001 041e 1c03 0db4 f38c 0bee 5e80        ..............^.
0x0020   8018 2088 b523 0000 0101 080a 1209 b36c        .....#.........l
0x0030   0009 c53f 1703 0000 20ec 1c88 05bb 0bdf        ...?............
0x0040   7c23 4a2e f0c1 cbc3 62e9 4058 453b 4c5e        |#J.....b.@XE;L^
0x0050   76a6 1e03 ba55 e699 7917 0300 0040 300b        v....U..y....@0.
0x0060   090d 0c7f c613 5f05 becf 8601 31e1 1185        ......_.....1...
0x0070   9b66 5870 f3e5 af42 47b1 8cec bf32 bcf2        .fXp...BG....2..
0x0080   1a40 4fcb 6938 f0ba 133c 7d11 837a a9bb        .@O.i8...<}..z..
0x0090   8655 f533 64e6 366f 5980 8508 e772              .U.3d.6oY....r
11:50:28.748110 192.168.0.1.7171 > 192.168.0.2.1054: . ack 770 win 17376
<nop,nop,timestamp 640343 302625644> (DF)
0x0000   4500 0034 0a6b 4000 4006 af05 c0a8 0001        E..4.k@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5e80 0db4 f3f6        ..........^.....
0x0020   8010 43e0 9a78 0000 0101 080a 0009 c557        ..C..x.........W
0x0030   1209 b36c                                      ...l
11:50:28.848908 192.168.0.1.7171 > 192.168.0.2.1054: P 585:739(154) ack 770 win 17376
<nop,nop,timestamp 640353 302625644> (DF)
0x0000   4500 00ce 0a6c 4000 4006 ae6a c0a8 0001        E....l@.@..j....
0x0010   c0a8 0002 1c03 041e 0bee 5e80 0db4 f3f6        ..........^.....
0x0020   8018 43e0 5faf 0000 0101 080a 0009 c561        ..C._..........a
0x0030   1209 b36c 1703 0000 204d fc4a f72d 7882        ...l.....M.J.-x.
0x0040   c4a9 6e50 7480 6bd7 0038 ef7a 054a ffcd        ..nPt.k..8.z.J..
0x0050   f932 6481 9f22 ba2f 0b17 0300 0070 12ed        .2d.."./.....p..
0x0060   d583 9ba5 9592 9bfc 7bd7 6dff a87b e7dc        ........{.m..{..
0x0070   81b4 a69b beb8 f632 f537 2035 1d2b bf37        .......2.7.5.+.7
0x0080   a833 4521 d5d7 babb 006f 878b ac52 dd08        .3E!.....o...R..
0x0090   dba3 39bc 22a4 7525 c1d8 2566 c512 dabd        ..9."u%..%f....
0x00a0   2f7d 8f62 a9f6 3d0d eec2 c75d 2c1a a3e8        /}.b..=....],...
0x00b0   5abf e0ec fe6e d5d9 0f0f 3642 3285 ed38        Z....n....6B2..8
0x00c0   2d0b 3d27 2ec8 23d2 09e6 2f46 6fc9              -.='..#.../Fo.
11:50:28.848982 192.168.0.2.1054 > 192.168.0.1.7171: . ack 739 win 8328
<nop,nop,timestamp 302625657 640353> (DF)
0x0000   4500 0034 f297 4000 4006 c6d8 c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f3f6 0bee 5f1a        ..............._.
0x0020   8010 2088 bd1f 0000 0101 080a 1209 b379        ..............y
0x0030   0009 c561                                      ...a
```


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

```
11:50:28.850211 192.168.0.2.1054 > 192.168.0.1.7171: P 770:1100(330) ack 739 win 8328
<nop,nop,timestamp 302625657 640353> (DF)
0x0000   4500 017e f298 4000 4006 c58d c0a8 0002        E..~..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f3f6 0bee 5f1a        ..............._.
0x0020   8018 2088 7d04 0000 0101 080a 1209 b379        ....}..........y
0x0030   0009 c561 1703 0000 20a7 26a4 734a 9003        ...a......&.sJ..
0x0040   2c0d 9474 5450 f4c2 be18 46ea 950d 8d38        ,..tTP....F....8
0x0050   2ef2 ad83 1bef c129 5f17 0300 0120 4475        .......)_.....Du
0x0060   f33d af53 0904 26ab c2c9 756a 185d 6f30        .=.S..&...uj.]o0
0x0070   1e92 72f4 d262 34bf 52a6 8cf0 fcd8 1cac        ..r..b4.R.......
0x0080   b980 627e f9d7 9f39 0214 ea22 7e40 d984        ..b~...9..."~@..
0x0090   3250 7efd 1b5e 459c ca71 c57b f8cb 87ed        2P~..^E..q.{....
0x00a0   73a0 9504 65ce 634f 2550 900f c303 cac9        s...e.cO%P......
0x00b0   80e3 5abc dc50 7df1 db47 fe16 0b51 6273        ..Z..P}..G...Qbs
0x00c0   dd0a 8c78 0b6d 52f1 0c95 8923 d8f8 c690        ...x.mR....#....
0x00d0   f4a2 08e6 3c6b 203e c391 3534 fec5 e5c5        ....<k.>..54....
0x00e0   a212 64ab e4f2 50b1 902c 4b18 3d24 4fc6        ..d...P..,K.=$O.
0x00f0   aa7d 842a 9063 a5e3 2204 9179 176e 2941        .}.*.c.."..y.n)A
0x0100   d96b 5dbe 4db9 f3c9 f23b 3677 f2f0 c909        .k].M....;6w....
0x0110   0f70 b26e 3205 a2d0 04d4 b8a5 15da 2c9c        .p.n2.........,.
0x0120   53d9 3ee8 4c7b 5664 278b 3988 5f25 5a40        S.>.L{Vd'.9._%Z@
0x0130   c03c a0bf c7c5 57ab fa7e 3d28 182c c56a        .<....W..~=(.,.j
0x0140   e6fe e688 7f9a 8cd7 f699 1f9f 0e97 b2fc        ................
0x0150   c5ea 1a0c 3c5f d7f1 8cc1 e109 b9a4 20e6        ....<_.........
0x0160   f0d5 a328 c3e0 5fdf f7b3 80c2 73c3 1312        ...(.._.....s...
0x0170   9d14 a18d bad7 466e 05ef 7727 0ad0              ......Fn..w'..
11:50:28.850296 192.168.0.1.7171 > 192.168.0.2.1054: . ack 1100 win 17376
<nop,nop,timestamp 640353 302625657> (DF)
0x0000   4500 0034 0a6d 4000 4006 af03 c0a8 0001        E..4.m@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5f1a 0db4 f540        ..........._....@
0x0020   8010 43e0 987d 0000 0101 080a 0009 c561        ..C..}.........a
0x0030   1209 b379                                      ...y
11:50:31.281620 192.168.0.2.1054 > 192.168.0.1.7171: P 1100:1222(122) ack 739 win 8328
<nop,nop,timestamp 302625900 640353> (DF)
0x0000   4500 00ae f299 4000 4006 c65c c0a8 0002        E.....@.@..\....
0x0010   c0a8 0001 041e 1c03 0db4 f540 0bee 5f1a        ...........@.._.
0x0020   8018 2088 d243 0000 0101 080a 1209 b46c        .....C.........l
0x0030   0009 c561 1703 0000 2008 5fac cc9f 6bc1        ...a...._...k.
0x0040   012a 78c4 d45b 1659 284f 0545 b665 cdf3        .*x..[.Y(O.E.e..
0x0050   c510 c912 b523 5d52 2417 0300 0050 31ab        .....#]R$....P1.
0x0060   7fc7 0c53 562e 986e d675 a816 d77d bd4d        ...SV..n.u...}.M
0x0070   ad5e 7c8b 14c3 aef7 c4ae 65f3 c8c3 0f27        .^|.......e....'
0x0080   41b2 66d7 4e36 328b 113a 1773 ffe6 e7c9        A.f.N62..:.s....
0x0090   7ece abb7 9602 8485 2753 dc7f d7c0 df61        ~.......'S.....a
0x00a0   59f6 60ad 107b 05c7 e70d 457c 5368              Y.`..{....E|Sh
11:50:31.281704 192.168.0.1.7171 > 192.168.0.2.1054: . ack 1222 win 17376
<nop,nop,timestamp 640596 302625900> (DF)
0x0000   4500 0034 0a6e 4000 4006 af02 c0a8 0001        E..4.n@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5f1a 0db4 f5ba        ..........._.....
0x0020   8010 43e0 961d 0000 0101 080a 0009 c654        ..C............T
0x0030   1209 b46c                                      ...l
11:50:31.291876 192.168.0.1.7171 > 192.168.0.2.1054: P 739:893(154) ack 1222 win 17376
<nop,nop,timestamp 640597 302625900> (DF)
0x0000   4500 00ce 0a6f 4000 4006 ae67 c0a8 0001        E....o@.@..g....
0x0010   c0a8 0002 1c03 041e 0bee 5f1a 0db4 f5ba        ..........._.....
0x0020   8018 43e0 6ce9 0000 0101 080a 0009 c655        ..C.l..........U
0x0030   1209 b46c 1703 0000 2093 a4fe 8558 c052        ...l.........X.R
0x0040   d4f1 93a6 ce59 79c3 1567 c501 7bd6 6c40        .....Yy..g..{.l@
0x0050   b4d0 ce56 6132 5137 9417 0300 0070 bc71        ...Va2Q7.....p.q
0x0060   b1bc 5d9f 4f9f a5e1 ee11 8569 5aa0 2d64        ..].O......iZ.-d
0x0070   e8f2 b54b f9da a71d 9267 1f55 1a0c 3f6d        ...K.....g.U..?m
0x0080   9547 f73d 5e7c 8d5b 2509 8e00 0923 6974        .G.=^|.[%....#it
0x0090   c8e9 abf1 7498 633d 2c2d 6ea3 ab0e 182c        ....t.c=,-n....,
0x00a0   6a4b 58f6 f74d 595a dbc7 cbdb dc4f f11e        jKX..MYZ.....O..
0x00b0   e603 7694 ac6d e3e1 dbed cc7a 7c18 88bc        ..v..m.....z|...
0x00c0   cfd1 d457 fe65 fbf1 9d74 385d de95              ...W.e...t8]..
11:50:31.324823 192.168.0.2.1054 > 192.168.0.1.7171: . ack 893 win 8328
<nop,nop,timestamp 302625905 640597> (DF)
0x0000   4500 0034 f29a 4000 4006 c6d5 c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f5ba 0bee 5fb4        ..............._.
0x0020   8010 2088 b8d5 0000 0101 080a 1209 b471        ..............q
```


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

```
0x0030   0009 c655                                        ...U
11:50:31.420514 192.168.0.2.1054 > 192.168.0.1.7171: P 1222:1328(106) ack 893 win 8328
<nop,nop,timestamp 302625914 640597> (DF)
0x0000   4500 009e f29b 4000 4006 c66a c0a8 0002        E.....@.@..j....
0x0010   c0a8 0001 041e 1c03 0db4 f5ba 0bee 5fb4        ..............._.
0x0020   8018 2088 8f2c 0000 0101 080a 1209 b47a        ....,.........z
0x0030   0009 c655 1703 0000 20e8 0fc9 3851 caea        ...U........8Q..
0x0040   50ec d979 a7f9 39d2 f61c ecb7 0ffd d463        P..y..9........c
0x0050   7c38 bc2e 229c 7e80 8617 0300 0040 cb01        |8.."."~.......@..
0x0060   9928 158c c843 cb3c 9ee6 d428 db4e 1708        .(...C.<...(.N..
0x0070   7a30 26df 041e a173 5059 bd91 e315 558c        z0&....sPY....U.
0x0080   7029 00fd d0c8 258c b10f 0739 9f1d 1d2d        p)....%....9...-
0x0090   dc1a b26f a462 82b1 9c69 56b0 2367              ...o.b...iV.#g
11:50:31.458188 192.168.0.1.7171 > 192.168.0.2.1054: . ack 1328 win 17376
<nop,nop,timestamp 640614 302625914> (DF)
0x0000   4500 0034 0a70 4000 4006 af00 c0a8 0001        E..4.p@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5fb4 0db4 f624        ..........._....$
0x0020   8010 43e0 94f9 0000 0101 080a 0009 c666        ..C............f
0x0030   1209 b47a                                      ...z
11:50:33.253421 192.168.0.2.1054 > 192.168.0.1.7171: P 1328:1450(122) ack 893 win 8328
<nop,nop,timestamp 302626097 640614> (DF)
0x0000   4500 00ae f29c 4000 4006 c659 c0a8 0002        E.....@.@..Y....
0x0010   c0a8 0001 041e 1c03 0db4 f624 0bee 5fb4        ...........$.._.
0x0020   8018 2088 c1df 0000 0101 080a 1209 b531        ...............1
0x0030   0009 c666 1703 0000 203e 9a1c 2049 1b0e        ...f.....>...I..
0x0040   f60e 7a51 2567 5f8f 1994 5c65 9d45 35f7        ..zQ%g_...\e.E5.
0x0050   45ea 4483 e1ed 67db 2317 0300 0050 0809        E.D...g.#....P..
0x0060   fbb1 18ff bb54 4f71 62e1 2aad 8a05 fa29        .....TOqb.*....)
0x0070   5487 c3e2 bcbe 06d5 0d46 9236 a244 c806        T........F.6.D..
0x0080   5cb1 ab9b 5467 1616 261b cf71 8a52 ebf9        \...Tg..&..q.R..
0x0090   5074 b375 b96c dd35 f3b2 0e8d f56a 349f        Pt.u.l.5.....j4.
0x00a0   4cf4 ed9f f5d2 0e24 c1a2 a1fd 48ae              L......$....H.
11:50:33.253488 192.168.0.1.7171 > 192.168.0.2.1054: . ack 1450 win 17376
<nop,nop,timestamp 640793 302626097> (DF)
0x0000   4500 0034 0a71 4000 4006 aeff c0a8 0001        E..4.q@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 5fb4 0db4 f69e        ..........._.....
0x0020   8010 43e0 9315 0000 0101 080a 0009 c719        ..C.............
0x0030   1209 b531                                      ...1
11:50:33.340413 192.168.0.1.7171 > 192.168.0.2.1054: P 893:1031(138) ack 1450 win 17376
<nop,nop,timestamp 640802 302626097> (DF)
0x0000   4500 00be 0a72 4000 4006 ae74 c0a8 0001        E....r@.@..t....
0x0010   c0a8 0002 1c03 041e 0bee 5fb4 0db4 f69e        ..........._.....
0x0020   8018 43e0 d2cc 0000 0101 080a 0009 c722        ..C.............."
0x0030   1209 b531 1703 0000 2041 c3d9 d71e d3a6        ...1.....A......
0x0040   38e9 7615 365f 50d2 9db6 db38 5827 d087        8.v.6_P....8X'..
0x0050   d34e 239e 3615 9d8b e217 0300 0060 492c        .N#.6........`I,
0x0060   2b0b af30 f57e 9fe1 bf7e 55c7 58ce 13dc        +..0.~...~U.X...
0x0070   3257 ee95 01b8 b1a9 3646 1501 d263 fb27        2W......6F...c.'
0x0080   f8d0 82c1 7020 cadf 6c01 f395 3ca7 dbcd        ....p...l...<...
0x0090   2a8c f667 2d14 279e 7b38 1735 9add 7d59        *..g-.'.{8.5..}Y
0x00a0   3d7d 4202 c830 644d 67b7 3df6 11dc 57a0        =}B..0dMg.=...W.
0x00b0   21c8 58b9 9ed3 32da 980c d3f7 a7d4              !.X...2.......
11:50:33.340493 192.168.0.2.1054 > 192.168.0.1.7171: . ack 1031 win 8328
<nop,nop,timestamp 302626106 640802> (DF)
0x0000   4500 0034 f29d 4000 4006 c6d2 c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f69e 0bee 603e        ..............`>
0x0020   8010 2088 b5d1 0000 0101 080a 1209 b53a        ...............:
0x0030   0009 c722                                      ..."
11:50:33.425727 192.168.0.1.7171 > 192.168.0.2.1054: P 1031:1185(154) ack 1450 win 17376
<nop,nop,timestamp 640810 302626106> (DF)
0x0000   4500 00ce 0a73 4000 4006 ae63 c0a8 0001        E....s@.@..c....
0x0010   c0a8 0002 1c03 041e 0bee 603e 0db4 f69e        ..........`>....
0x0020   8018 43e0 6868 0000 0101 080a 0009 c72a        ..C.hh.........*
0x0030   1209 b53a 1703 0000 2051 897f c6b0 4c41        ...:.....Q....LA
0x0040   4efa ca1c 4304 83db 1d97 aef6 c8ee bb8a        N...C...........
0x0050   3d65 d782 d14c 3cf0 e217 0300 0070 462d        =e...L<......pF-
0x0060   7603 b797 cc00 7449 7cf2 1ff9 9624 dfc0        v.....tI|....$..
0x0070   49e0 ba7b 85ee 7d9b 2864 8c43 d650 e082        I..{..}.(d.C.P..
0x0080   9e0a c0e7 7984 7e27 2f0f 99fc c89e 7d22        ....y.~'/.....}"
0x0090   29e3 e46c 2b56 c641 f198 95f3 88be 4b46        )..l+V.A......KF
0x00a0   8d33 5a98 3a44 c584 e479 8933 3ac4 b847        .3Z.:D...y.3:..G
```


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

```
0x00b0   fd51 6622 7178 df95 1dd1 ecfe 8654 c97a        .Qf"qx.......T.z
0x00c0   bbd7 90ba 64ac 112c 1013 b3a9 4334             ....d..,....C4
11:50:33.425795 192.168.0.2.1054 > 192.168.0.1.7171: . ack 1185 win 8328
<nop,nop,timestamp 302626115 640810> (DF)
0x0000   4500 0034 f29e 4000 4006 c6d1 c0a8 0002        E..4..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f69e 0bee 60d8        ..............`.
0x0020   8010 2088 b526 0000 0101 080a 1209 b543        .....&.........C
0x0030   0009 c72a                                      ...*
11:50:33.427028 192.168.0.2.1054 > 192.168.0.1.7171: P 1450:1780(330) ack 1185 win 8328
<nop,nop,timestamp 302626115 640810> (DF)
0x0000   4500 017e f29f 4000 4006 c586 c0a8 0002        E..~..@.@.......
0x0010   c0a8 0001 041e 1c03 0db4 f69e 0bee 60d8        ..............`.
0x0020   8018 2088 cb82 0000 0101 080a 1209 b543        ...............C
0x0030   0009 c72a 1703 0000 204e 90e1 35a4 59a8        ...*.....N..5.Y.
0x0040   e59d c2f8 7ce4 cc4f 2fb5 4f54 4c21 1560        ....|..O/.OTL!.`
0x0050   8483 a9ea 9a62 1a42 e817 0300 0120 1475        .....b.B.......u
0x0060   6160 5d6f 1491 7b28 9be1 cf3d 16b1 c584        a`]o..{(...=....
0x0070   46eb ff2b 8436 ddda 1f32 5022 8791 dfe1        F..+.6...2P"....
0x0080   c774 1791 7fb8 9dfd bb67 531a ae0a dd9e        .t.......gS.....
0x0090   96b0 769a 7653 95ec fc32 b246 bd94 7bde        ..v.vS...2.F..{.
0x00a0   be1b 2da3 eb28 50b8 9d4e fc0c e094 0162        ..-..(P..N.....b
0x00b0   dcb6 c153 a1e5 a1ed 0973 0bf8 0f4b c034        ...S.....s...K.4
0x00c0   44be d904 56f7 ad0b a0bb 04a5 fdda dffe        D...V...........
0x00d0   749c cb7c a1ca 7d8f 4c5f c599 a215 ae5b        t..|..}.L_.....[
0x00e0   ef39 bec1 59b9 be22 2533 221b d966 3411        .9..Y.."%3"..f4.
0x00f0   02f3 be98 03f0 74da be0a 44d6 2fba 0938        ......t...D./..8
0x0100   a5b1 7dfc 71f3 c6bd 585e a41f 6640 c902        ..}.q...X^..f@..
0x0110   dccc b250 5954 cdce 5e78 bc79 62ed 021a        ...PYT..^x.yb...
0x0120   6691 e60d abb2 2cf3 b287 f3c7 4438 1a3d        f.....,.....D8.=
0x0130   c9e6 9bc6 eee8 ab19 7bb7 2bf4 7142 add8        ........{.+.qB..
0x0140   7669 fd37 e568 f36a 6e74 bc18 8033 0508        vi.7.h.jnt...3..
0x0150   69c6 1a31 4123 d88f 5b43 2b50 cb3a f9bc        i..1A#..[C+P.:..
0x0160   3cee 9293 162d f063 622f b28d b1ab 5e94        <....-.cb/....^.
0x0170   c6ae 914e cfe8 ba85 eadc 82c4 ecbf             ...N..........
11:50:33.427063 192.168.0.1.7171 > 192.168.0.2.1054: . ack 1780 win 17376
<nop,nop,timestamp 640810 302626115> (DF)
0x0000   4500 0034 0a74 4000 4006 aefc c0a8 0001        E..4.t@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 60d8 0db4 f7e8        ..........`.....
0x0020   8010 43e0 9084 0000 0101 080a 0009 c72a        ..C............*
0x0030   1209 b543                                      ...C
11:50:33.523641 192.168.0.2.1054 > 192.168.0.1.7171: P 1780:1886(106) ack 1185 win 8328
<nop,nop,timestamp 302626124 640810> (DF)
0x0000   4500 009e f2a0 4000 4006 c665 c0a8 0002        E.....@.@..e....
0x0010   c0a8 0001 041e 1c03 0db4 f7e8 0bee 60d8        ..............`.
0x0020   8018 2088 87ad 0000 0101 080a 1209 b54c        ...............L
0x0030   0009 c72a 1703 0000 20bf 90cb 23e5 efa9        ...*........#...
0x0040   fcbc a04c a279 e63f 23ba 116b c5cf 0a37        ...L.y.?#..k...7
0x0050   74d9 6d13 26db 3bb4 8d17 0300 0040 e903        t.m.&.;......@..
0x0060   5aec 032b 96e0 5a95 cc52 c1c9 73fe 527c        Z..+..Z..R..s.R|
0x0070   80b0 9358 ac53 7bbf 5163 7204 34c1 8ac6        ...X.S{.Qcr.4...
0x0080   02cf 3ccf d2fb ef25 0cfc 2899 9f31 767f        ..<....%..(..1v.
0x0090   a74f c543 edb6 6d81 4e8f 3b6a 64d4             .O.C..m.N.;jd.
11:50:33.523722 192.168.0.1.7171 > 192.168.0.2.1054: . ack 1886 win 17376
<nop,nop,timestamp 640820 302626124> (DF)
0x0000   4500 0034 0a75 4000 4006 aefb c0a8 0001        E..4.u@.@.......
0x0010   c0a8 0002 1c03 041e 0bee 60d8 0db4 f852        ..........`....R
0x0020   8010 43e0 9007 0000 0101 080a 0009 c734        ..C............4
0x0030   1209 b54c                                      ...L
```

© SANS Institute 2004, Author retains full rights.

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

Appendix G.3

Trace for FTP on server1(eth1) using tcpdump (readout by tcpdump)

```
11:50:28.006974 192.168.2.2.1062 > 192.168.1.2.ftp: S 449048905:449048905(0) win 64240
<mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 1753 4000 7e06 6120 c0a8 0202        E..0.S@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f149 0000 0000        .....&.....I....
0x0020   7002 faf0 f391 0000 0204 05b4 0101 0402        p...............
11:50:28.007461 192.168.1.2.ftp > 192.168.2.2.1062: S 3600064008:3600064008(0) ack
449048906 win 64240 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 4f0c 4000 8006 2767 c0a8 0102        E..0O.@...'g....
0x0010   c0a8 0202 0015 0426 d694 9e08 1ac3 f14a        .......&.......J
0x0020   7012 faf0 7ee3 0000 0204 05b4 0101 0402        p...~...........
11:50:28.009045 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 1 win 64240 (DF)
0x0000   4500 0028 1754 4000 7e06 6127 c0a8 0202        E..(.T@.~.a'....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e09        .....&.....J....
0x0020   5010 faf0 aba7 0000                            P.......
11:50:29.101324 192.168.1.2.ftp > 192.168.2.2.1062: P 1:62(61) ack 1 win 64240 (DF)
0x0000   4500 0065 4f0d 4000 8006 2731 c0a8 0102        E..eO.@...'1....
0x0010   c0a8 0202 0015 0426 d694 9e09 1ac3 f14a        .......&.......J
0x0020   5018 faf0 4de7 0000 3232 302d 4775 696c        P...M...220-Guil
0x0030   6446 5450 6420 4654 5020 5365 7276 6572        dFTPd.FTP.Server
0x0040   2028 6329 2031 3939 372d 3230 3032 0d0a        .(c).1997-2002..
0x0050   3232 302d 5665 7273 696f 6e20 302e 3939        220-Version.0.99
0x0060   392e 390d 0a                                   9.9..
11:50:29.242817 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 62 win 64179 (DF)
0x0000   4500 0028 1756 4000 7e06 6125 c0a8 0202        E..(.V@.~.a%....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e46        .....&.....J...F
0x0020   5010 fab3 aba7 0000                            P.......
11:50:29.243175 192.168.1.2.ftp > 192.168.2.2.1062: P 62:91(29) ack 1 win 64240 (DF)
0x0000   4500 0045 4f0f 4000 8006 274f c0a8 0102        E..EO.@...'O....
0x0010   c0a8 0202 0015 0426 d694 9e46 1ac3 f14a        .......&...F...J
0x0020   5018 faf0 0991 0000 3232 3020 506c 6561        P.......220.Plea
0x0030   7365 2065 6e74 6572 2079 6f75 7220 6e61        se.enter.your.na
0x0040   6d65 3a0d 0a                                   me:..
11:50:29.343100 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 91 win 64150 (DF)
0x0000   4500 0028 1757 4000 7e06 6124 c0a8 0202        E..(.W@.~.a$....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e63        .....&.....J...c
0x0020   5010 fa96 aba7 0000                            P.......
11:50:32.908117 192.168.2.2.1062 > 192.168.1.2.ftp: P 1:17(16) ack 91 win 64150 (DF)
0x0000   4500 0038 1759 4000 7e06 6112 c0a8 0202        E..8.Y@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f14a d694 9e63        .....&.....J...c
0x0020   5018 fa96 23b3 0000 5553 4552 2061 6e6f        P...#...USER.ano
0x0030   6e79 6d6f 7573 0d0a                            nymous..
11:50:32.917658 192.168.1.2.ftp > 192.168.2.2.1062: P 91:127(36) ack 17 win 64224 (DF)
0x0000   4500 004c 4f11 4000 8006 2746 c0a8 0102        E..LO.@...'F....
0x0010   c0a8 0202 0015 0426 d694 9e63 1ac3 f15a        .......&...c...Z
0x0020   5018 fae0 1e18 0000 3333 3120 5573 6572        P.......331.User
0x0030   206e 616d 6520 6f6b 6179 2c20 4e65 6564        .name.okay,.Need
0x0040   2070 6173 7377 6f72 642e 0d0a                  .password...
11:50:33.046954 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 127 win 64114 (DF)
0x0000   4500 0028 175a 4000 7e06 6121 c0a8 0202        E..(.Z@.~.a!....
0x0010   c0a8 0102 0426 0015 1ac3 f15a d694 9e87        .....&.....Z....
0x0020   5010 fa72 ab97 0000                            P..r....
11:50:33.179848 192.168.2.2.1062 > 192.168.1.2.ftp: P 17:30(13) ack 127 win 64114 (DF)
0x0000   4500 0035 175b 4000 7e06 6113 c0a8 0202        E..5.[@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f15a d694 9e87        .....&.....Z....
0x0020   5018 fa72 b49f 0000 5041 5353 2067 7565        P..r....PASS.gue
0x0030   7374 400d 0a                                   st@..
11:50:34.966165 192.168.1.2.ftp > 192.168.2.2.1062: P 127:148(21) ack 30 win 64211 (DF)
0x0000   4500 003d 4f12 4000 8006 2754 c0a8 0102        E..=O.@...'T....
0x0010   c0a8 0202 0015 0426 d694 9e87 1ac3 f167        .......&.......g
0x0020   5018 fad3 90fe 0000 3233 3020 5573 6572        P.......230.User
0x0030   206c 6f67 6765 6420 696e 2e0d 0a               .logged.in...
11:50:35.150051 192.168.2.2.1062 > 192.168.1.2.ftp: . ack 148 win 64093 (DF)
0x0000   4500 0028 175d 4000 7e06 611e c0a8 0202        E..(.]@.~.a.....
0x0010   c0a8 0102 0426 0015 1ac3 f167 d694 9e9c        .....&.....g....
0x0020   5010 fa5d ab8a 0000                            P..]....
```


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

References

1. Amrita Innovative Technology Foundation Labs. "AmritaVPN – A Virtual Private Networking Tool for GNU/Linux" 11/10/2003. URL: http://amvpn.sourceforge.net/amvpn.html.

2. Dunston, Duane. "OpenVPN: An Introduction and Interview with Founder, James Yonan" 11/10/2003. URL: http://www.linuxsecurity.org/feature_stories/feature_story-152.html.

3. Engelschall, Ralf S. "Welcome to the OpenSSL Project" 10/2003. URL: http://www.openssl.org.

4. Jacobson, Van. "tcpdump – dump traffic on a network" 11/2003. URL: http://www.tcpdump.org/tcpdump_man.html.

5. Khanvilkar, Shashank. "Setting up VPN using Amrita VPN" 9/2003. URL: http://mia.ece.uic.edu/~papers/volans/amvpn.html.

6. Unknown. "Ethereal" 11/3/2003. URL: http://www.ethereal.com.

7. Unknown. "FreeS/WAN Documentation" 4/15/2003. URL: http://www.freeswan.org/freeswan_trees/freeswan-2.04/doc/index.html.

8. Unknown. "NTP: The Network Time Protocol" 10/2003. URL: http://www.ntp.org.

9. Yonan, James. "OpenVPN" 11/04/2003. URL: http://openvpn.sourceforge.net.

© SANS Institute 2004, Author retains full rights.

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