Global Information Assurance Certification Paper

Tunneling PPTP Through SSH2 Connections

Defense-in-Depth

By

Nicholas Lee Capace
GSEC v. 1.2e

April 28, 2001

Introduction

As the importance of remote access to network resources grows, so does the desire and ability for certain types of people to attempt to access those resources without authorization. The most powerful weapon in a Network Security Administrator's arsenal is a layered diversification of technology, or "Defense-in-Depth." As the number of different technologies used to secure a network increases, so does the possibility that an attacker will not have the expertise to subvert all of them. For this very reason, when setting up Virtual Private Network (VPN) connections, tunneling Point-To-Point Tunneling Protocol (PPTP) connections through Secure Shell version 2 (SSH2) connections adds another level of encryption and increases the "depth" of security of the connection.

Brief Overview of the Protocols

SSH was developed for computers running UNIX-based Operating Systems to be able to connect and transfer data in a secure environment. SSH2 is the newer, more secure version of SSH that can now be used by most operating systems. SSH2 requires user authentication before establishing an encrypted tunnel and granting access to network resources.

> "Public key authentication is based on the use of digital signatures. Each user creates a public / private key pair for authentication purposes. The server knows the user's public key, and only the user has the private key. The filenames of private keys that are used in authentication are set in *$HOME/.ssh2/identification*. When the user tries to authenticate himself, the server checks *$HOME/.ssh2/authorization* for filenames of matching public keys and sends a challenge to the user end. User is authenticated by signing the challenge using the private key."[1]

SSH2 authentication and encryption is handled by different components of the protocol. "The SSH protocol consists of three major components: The Transport Layer Protocol provides server authentication, confidentiality, and integrity with perfect forward secrecy. The User Authentication Protocol authenticates the client to the server. The Connection Protocol multiplexes the encrypted tunnel into several logical channels." [2] SSH2 has the ability to use 3DES, Twofish, Blowfish, Arcfour, and CAST128 encryption algorithms.

"Point to Point Tunneling Protocol (PPTP) was developed by the PPTP Forum. The forum consists of the following organizations: Ascend Communications, Microsoft Corporation, 3Com/Primary Access, ECI Telematics, and U.S. Robotics." [3] PPTP was developed for Microsoft-based computers to securely connect to a corporate network over the internet. Linux and several other versions of UNIX now also support PPTP connections. PPTP also requires user authentication before establishing an encrypted tunnel and granting access to network resources.

> "MS-CHAP (PPP authentication) is used to validate the user credentials against Windows NT domains and the resulting session key is used to encrypt user data. RAS inherently supports a shared secret between the

> RAS client and the RAS server— essentially, a user-supplied password at the client to derive the same MD4 hash as that stored password stored in the Windows NT security database at the server. By using this shared secret between the RAS client and the RAS server, we are able to elegantly solve a major encryption problem: key distribution. If encryption is negotiated, RSA RC4 is used with a 40-bit session key derived as a result from the earlier user authentication. Microsoft will also offer 128-bit encryption for RAS in the United States, as governed by export law." [4]

Configuring the Connection

This VPN solution will appeal mainly to the small to mid-sized companies that cannot afford to spend a large amount of money on network security, but still want to allow key personnel to access the Corporate network from home. It will also provide them with a higher level of security at very little additional expense.

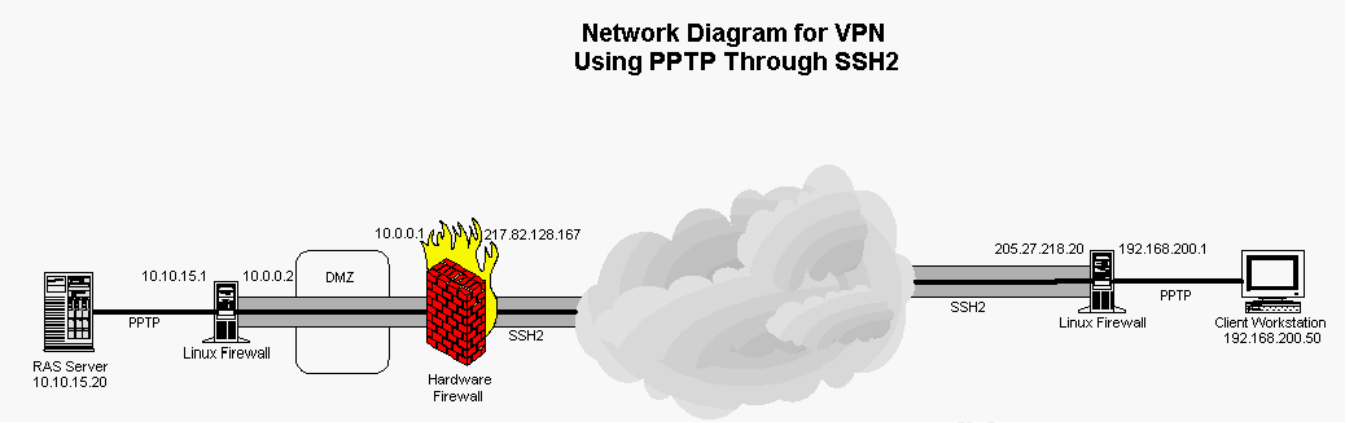
The secure tunnel must be set up in three phases. The first phase is the physical configuration of the Corporate network. This will be the most difficult phase and should be completed and tested first. The second phase is the physical setup of the Remote network(s). Although this will be easier than the Corporate configuration, the Remote sites also must be tested before continuing. Finally, the third phase involves making the connections between the two networks. Testing the setup and configuration of each site as it is completed will help to reduce the time troubleshooting errors in the third phase.

The Corporate Configuration

The Corporate network should have a hardware firewall as the first, or outermost, layer of defense. Several different hardware firewalls can be purchased for less than $1500 and can be set up relatively easily. The next layer should be the DMZ (literally demilitarized zone). DMZ is the space between the internal and external firewalls that contains the company's web and e-mail servers that provide the public with access to corporate data and services. A software firewall, built on a relatively inexpensive PC, running Linux with IP Chains, should be placed on the inside of the DMZ. The final level should be a Windows NT Server with Remote Access Server (RAS) services placed inside of the software firewall.

The Remote Configuration

The remote network should consist of a software firewall, built on a relatively inexpensive PC, running Linux with IP Chains. Inside of the firewall would be the client PC. The client PC should be running the most secure OS available to the company, preferably Windows 2000 Professional or Windows NT workstation. The client machine must also have the Microsoft VPN client installed.



Making the Connections

First, the SSH2 client and server portions will have to be configured on the two Linux firewalls. Then, the client firewall will have to initiate the SSH2 connection, through the hardware firewall, to the internal Corporate firewall. Configure the SSH2 connection to forward port 1723 (PPTP authentication port) and 47 (PPTP data transfer port). Then establish the PPTP connection between the client and the RAS server.

Configuring SSH2

After installing the SSH2 server and client portion on each respective firewall and generating the public/private keys, a forwarding tunnel can be created between the two machines. For additional security, the SSH2 server can be configured to allow only specific hostnames to authenticate. "The AllowHosts and DenyHosts keywords permit or prevent (respectively) SSH connections from given hosts."[5] Log into the SSH server as root and type:

AllowHosts "Client_Machine_Name"

Log into the client firewall as root. At the command prompt, type:

ssh –L 1723:10.10.15.20:1723 217.82.126.167

where 1723 is the port on the client firewall that will make the PPTP connection, 10.10.15.20 is the destination RAS server, and 217.82.126.167 is the public address of the Corporate firewall that will forward port 1723 to the internal firewall.

Then type:

ssh –L 47:10.10.15.20:47 217.82.126.167

where 47 is the port that PPTP will transfer the data.

Client Firewall Rules

All of the rules are based on the IP Addresses from the diagram above.

```
#!/bin/sh

# variables
LOCALNET=192.168.200.0/24
INT_NIC=eth1
LPBK=lo

EXT_NIC=eth0

# start port forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

# Flush current rules
/sbin/ipchains -F

# forward rules
/sbin/ipchains -F forward
/sbin/ipchains -P forward DENY
/sbin/ipchains -A forward -j MASQ -s $LOCALNET -d 0.0.0.0/0

# Inbound connections
/sbin/ipchains -A input -l -j DENY -i $EXT_NIC -s 0.0.0.0/0 -d $LOCALNET ! -p
tcp
/sbin/ipchains -A input -l -j DENY -i $EXT_NIC -s 0.0.0.0/0 -d $LOCALNET ! -p
udp
/sbin/ipchains -A input -l -j DENY -i $EXT_NIC -s 0.0.0.0/0 -d $LOCALNET ! -p
icmp

# Spoof proof
/sbin/ipchains -A input ! -i $LPBK -s 127.0.0.0/255.0.0.0 -j DENY
```

Corporate Hardware Firewall

The configuration of the hardware firewall will vary greatly depending on the type of firewall used and the company's need for public access to company data. For this specific connection to work, regardless of the rest of the settings, the hardware firewall will have to forward ports 1723 and 47 to the internal firewall.

Internal Corporate Firewall Rules

The internal Corporate firewall could also have a similar set of rules as the client firewall, with IP Address modifications for the Corporate private address scheme.

```
#!/bin/sh

# variables
LOCALNET=10.10.0.0/24
INT_NIC=eth1
LPBK=lo
```

```
EXT_NIC=eth0

# start port forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

# Flush current rules
/sbin/ipchains -F

# forward rules
/sbin/ipchains -F forward
/sbin/ipchains -P forward DENY
/sbin/ipchains -A forward -j MASQ -s $LOCALNET -d 0.0.0.0/0

# Inbound connections
/sbin/ipchains -A input -l -j DENY -i $EXT_NIC -s 0.0.0.0/0 -d $LOCALNET ! -p
tcp
/sbin/ipchains -A input -l -j DENY -i $EXT_NIC -s 0.0.0.0/0 -d $LOCALNET ! -p
udp
/sbin/ipchains -A input -l -j DENY -i $EXT_NIC -s 0.0.0.0/0 -d $LOCALNET ! -p
icmp

# Spoof proof
/sbin/ipchains -A input ! -i $LPBK -s 127.0.0.0/255.0.0.0 -j DENY
```

Configuring RAS

Install the Microsoft RAS services and configure the appropriate number of VPN connections. Install the MS VPN client on the client machine. For the address of the VPN server, the user MUST use the internal IP Address of the client firewall.

Summary

Following the above configuration and implementation procedures, tunneling PPTP connections through SSH2 tunnels, will provide double encryption and an increased "depth" of security. The possibility that people will have the expertise to gain access to your corporate resources is greatly reduced by the multiple layers of several different technologies.

Cited Resources

1 SSH Communications Security Ltd., "Manpage of SSH2" http://www.employees.org/~satch/ssh/faq/manpages/ssh2_man.html

2 T. Ylonen, T. Kivinen, M. Saarinen, T. Rinne, and S. Lehtinen, "SSH Protocol Acrhitecture" (9, January, 2001) http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-07.txt

3 K. Hamzeh, G. Pall, W. Verthein, Jeff Taarud, and W. Little, "Point to Point Tunneling Protocol (PPTP) Technical Specifications" (June, 1996) http://support.3com.com/infodeli/tools/remote/general/pptp/pptp.htm

4 Microsoft, "Point-to-Point Tunneling Protocol (PPTP) FAQ" (December 11, 1998) http://www.microsoft.com/NTServer/commserv/deployment/moreinfo/PPTPfaq.asp

5 D. Barrett and R. Silverman, SSH, The Secure Shell (Sebastopol, CA: O'Reilly, February, 2001), 182.

Additional Resources

http://www.microsoft.com/ntserver/commserv/deployment/moreinfo/pptpfaq.asp

http://www.counterpane.com/pptp.html

http://www.employees.org/~satch/ssh/faq/ssh-faq.html

http://kb.indiana.edu/data/aelc.html

http://www.openssh.org/

http://www.knowplace.org/pptp-hints.html

http://www.linux-firewall-tools.com/linux/faq/index.html

http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/IPCHAINS-HOWTO.html#s1

http://msdn.microsoft.com/library/winresource/ssreskit/rk_fltrset_fpnd.htm

http://www.linuxdoc.org/LDP/nag2/

Last Updated: October 22nd, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event