SoftEther By Hand

Servers, Clusters, Hubs, Clients, and Bridges

SEC 440 / 4-24-2015

Henry Quinn, Liam Callaghan, Matthew Prahl, Charles Iszard, Ahmed Almalki

GENERAL NOTES:

Most of these commands outside of “$ ./vpncmd” need root access. Easier to drop into root rather than keep typing “sudo”.

It is assumed that the network this is installed on already has a working DHCP server.

**SETUP OF SERVER**

Fresh install of Ubuntu Server 14.04

1.) INSTALL LYNX AND DOWNLOAD SOFTETHER

$ apt-get install update && apt-get upgrade (MAY NOT NEED THIS)

$ apt-get install lynx –y

$ lynx<http://www.softether-download.com/files/softether/>

Using the on screen instructions, navigate to the newest version => Linux => SoftEther VPN Server => 64bit – Intel x64 or AMD64 => highlight the tar file

Press “D” to download, choose “Save to Disk” when prompted, and then hit “Q” once file is saved to quit Lynx

2.) INSTALL AND CONFIGURE SOFTETHER

Unzip the SoftEther File and Prepare to Build

$ tar xzvf softether-vpnserver-vwhateverwhateverwhatever.tar.gz

$ apt-get install build-essential –y

$ cd vpnserver

$ make

Accept the terms of the License Agreement

Type “1” and press “Enter” three times

Move the newly created VPNServer to its new home and chmod file permissions

$ cd ..

$ mv vpnserver /usr/local

$ cd /usr/local/vpnserver

$ chmod 600 \*

$ chmod 700 vpnserver

$ chmod 700 vpncmd

3.) CONFIGURE SOFTETHER TO START ON BOOT

Create file /etc/init.d/vpnserver and copy in the highlighted code

$ sudo nano /etc/init.d/vpnserver

#!/bin/sh

# chkconfig: 2345 99 01

# description: SoftEther VPN Server

DAEMON=/usr/local/vpnserver/vpnserver

LOCK=/var/lock/subsys/vpnserver

test -x $DAEMON || exit 0

case "$1" in

start)

$DAEMON start

touch $LOCK

;;

stop)

$DAEMON stop

rm $LOCK

;;

restart)

$DAEMON stop

sleep 3

$DAEMON start

;;

\*)

echo "Usage: $0 {start|stop|restart}"

exit 1

esac

exit 0

Save and exit

CTRL + “O”

“Y”

CTRL + “X”

4.) RUN THE FOLLOWING COMMANDS TO START AND CLEANUP SOFTETHER INSTALLATION

$ sudo mkdir /var/lock/subsys (MAY NOT NEED THIS)

$ chmod 755 /etc/init.d/vpnserver && /etc/init.d/vpnserver start

$ update-rc.d vpnserver defaults

5.) CHECK TO SEE IF VPN SERVER IS WORKING

$ cd /usr/local/vpnserver

$ ./vpncmd

Press “3” to choose “Use of VPN Tools” then type and enter “check” and watch to make sure all of your checks pass. Type “exit” to exit VPN Tools.

6.) CHANGE ADMIN PASSWORD

Connect to the vpncmd interface

$ cd /usr/local/vpnserver

Connect to the local administrator panel

$ sudo ./vpncmd

Press “1” to choose “Management of VPN Server or VPN Bridge” when it asks for a localhost server, type 127.0.0.1:5555 then hit “Enter” twice to get into server admin mode

$ ServerPasswordSet (then follow the prompts – enter password and confirm)

**PROMOTING SERVER TO CLUSTER CONTROLLER**

1.) MAKE VPNSERVER THE CLUSTER CONTROLLER

Connect to the vpncmd interface

$ cd /usr/local/vpnserver

Connect to the local administrator panel

$ sudo ./vpncmd

Press “1” to choose “Management of VPN Server or VPN Bridge” when it asks for a localhost server, type 127.0.0.1:5555 then hit “Enter” twice to get into server admin mode

Promote the server to Cluster Controller

$ ClusterSettingController </WEIGHT:#>

NOTE: Weight defaults to 100. See note below following command.

You can add a weight to the controller and the members of the cluster. The higher the weight, the more of the load of connections that particular machine will receive.

See (Ctrl+F for “ClusterSettingController” and “ClusterSettingMember”:<https://www.softether.org/4-docs/1-manual/6._Command_Line_Management_Utility_Manual/6.3_VPN_Server_%2F%2F_VPN_Bridge_Management_Command_Reference_(For_Entire_Server)>

**SETUP OF CLUSTER MEMBERS**

1.) CREATE ANOTHER SOFTETHER SERVER

Set everything up for a new server the way you would before. Follow the steps under the heading SETUP SERVER verbatim. Use a different server password, if you’d like.

2.) ADD SERVER TO CLUSTER AS MEMBER

Connect to the vpncmd interface

$ cd /usr/local/vpnserver

Connect to the local administrator panel

$ sudo ./vpncmd

Press “1” to choose “Management of VPN Server or VPN Bridge” when it asks for a localhost server, type 127.0.0.1:5555 then hit “Enter” twice to get into server admin mode

$ ClusterSettingMember <ServerIP:Port> </IP:none> </PORTS:443,5555> </PASSWORD:ClusterControllerPassword> </WEIGHT:#>

Where

$ ClusterSettingMember IPOfClusterController:5555 /IP:none /PORTS:443,5555 /PASSWORD:PasswordOfClusterController

Again, weight defaults to 100, which is fine for us.

That should honestly be that. There are plenty more cluster commands to get you more troubleshooting information. If you feel like you need anything, hit the link below and CTRL+F “Cluster”. There will be a really match heavy block towards the top of the page, which will be your diagnostic commands.

**CREATING HUBS**

1.) CREATE A VIRTUAL HUB

GENERAL NOTE: Only create the hubs from the Cluster Controller if you can help it. It makes everything work more smoothly. It’ll automatically disperse computational load to the cluster members based on the weight assigned to each member. The higher the weight, the more of the computational load that particular cluster member takes takes. However, by default, everything gets a weight of 100.

Connect to the vpncmd interface

$ cd /usr/local/vpnserver

Connect to the local administrator panel

$ sudo ./vpncmd

Press “1” to choose “Management of VPN Server or VPN Bridge” when it asks for a localhost server, type 127.0.0.1:5555 then hit “Enter” twice to get into server admin mode

2.) CREATE HUB

$ HubCreate <NameOfHub>

Where <NameOfHub> is whatever you would like to name your hub.

Enter an administrator password for the hub and fill out other prompted information.

3.) SELECT VIRTUAL HUB TO WORK WITH

Enter the following command

$ HUB <NameOfHub>

Where <NameOfHub> is the name of the hub you would like to administer

4.) CREATE USERS ON HUB

$ UserCreate <NameOfUser>

Where <NameOfUser> is the username you would like to create

Fill out the prompted information.

$UserPasswordSet <NameOfUser>

Where <NameOfUser> is the username you would like to create a password for

Fill out the prompted information

**SETUP OF CLIENT TO SERVER CONNECTIONS**

Fresh install of Ubuntu Server 14.04

1.) INSTALL LYNX AND DOWNLOAD SOFTETHER

$ apt-get install update && apt-get upgrade (MAY NOT NEED THIS)

$ apt-get install lynx –y

$ lynx<http://www.softether-download.com/files/softether/>

Using the on screen instructions, navigate to the newest version => Linux => SoftEther VPN Client => 64bit – Intel x64 or AMD64 => highlight the tar file

Press “D” to download, choose “Save to Disk” when prompted, and then hit “Q” once file is saved to quit Lynx

2.) INSTALL AND CONFIGURE SOFTETHER

Unzip the SoftEther File and Prepare to Build

$ tar xzvf softether-vpnclient-vwhateverwhateverwhatever.tar.gz

$ apt-get install build-essential –y

$ cd vpnclient

$ make

Accept the terms of the License Agreement

Type “1” and press “Enter” three times

Move the newly created VPNSClient to its new home and chmod file permissions

$ cd ..

$ mv vpnclient /usr/local

$ cd /usr/local/vpnclient

$ chmod 600 \*

$ chmod 700 vpnclient

$ chmod 700 vpncmd

3.) CONFIGURE SOFTETHER TO START ON BOOT

Create file /etc/init.d/vpnclient and copy in the highlighted code

$ sudo nano /etc/init.d/vpnclient

#!/bin/sh

# chkconfig: 2345 99 01

# description: SoftEther VPN Client

DAEMON=/usr/local/vpnclient/vpnclient

LOCK=/var/lock/subsys/vpnclient

test -x $DAEMON || exit 0

case "$1" in

start)

$DAEMON start

touch $LOCK

;;

stop)

$DAEMON stop

rm $LOCK

;;

restart)

$DAEMON stop

sleep 3

$DAEMON start

;;

\*)

echo "Usage: $0 {start|stop|restart}"

exit 1

esac

exit 0

Save and exit

CTRL + “O”

“Y”

CTRL + “X”

4.) RUN THE FOLLOWING COMMANDS TO START AND CLEANUP SOFTETHER INSTALLATION

$ sudo mkdir /var/lock/subsys (MAY NOT NEED THIS)

$ chmod 755 /etc/init.d/vpnclient && /etc/init.d/vpnclient start

$ update-rc.d vpnclient defaults

5.) START UP THE CLIENT

Connect to the vpncmd interface

$ cd /usr/local/vpnclient

$ sudo ./vpncmd

Connect to the local client panel

Type “2” to enter “Management of VPN Client” then hit enter.

6.) CREATE VIRTUAL ADAPTER

$ NicCreate <NameOfAdapter>

Where <NameOfAdapter> is the name you would like to call your new adapter

7. CREATE AND CONFIGURE A VPN CONNECTION

$ AccountCreate <NameOfConnection>

Where <NameOfConnection> is the name you would like to call your new connection

Then enter the VPN Cluster Controller’s IP and Port Number

xxx.xxx.xxx.xxx:5555

“Destination Virtual Hub Name:” <NameOfHub>

Where <NameOfAdapter> is the name of your preferred hub on the Cluster Controller

“Connecting User Name:” <NameOfUser>

Where <NameOfUser> is the name of a user on the selected hub

“Used Virtual Network Adapter Name:” <NameOfAdapter>

Where <NameOfAdapter> is the name is the name of the adapter you just created

8. PASSWORD PROTECT YOUR CLIENT TO SERVER CONNECTION

$ AccountPasswordSet <NameOfConnection>

Where <NameOfConnection> is the name of the newly created connection

“Specify standard or radius:” standard

9. BRING THE CONNECTION UP

$ AccountConnect <NameOfConnection>

Where <NameOfConnection> is the name of the newly created connection

10.) TEST THE CONNECTION

$ AccountStatusGet <NameOfConnection>

Where <NameOfConnection> is the name of the newly created connection

If the connection shows as being ONLINE, you’re all set.

**SETUP OF SITE TO SITE CONNECTIONS**

Fresh install of Ubuntu Server 14.04

1.) INSTALL LYNX AND DOWNLOAD SOFTETHER

$ apt-get install update && apt-get upgrade (MAY NOT NEED THIS)

$ apt-get install lynx –y

$ lynx<http://www.softether-download.com/files/softether/>

Using the on screen instructions, navigate to the newest version => Linux => SoftEther VPN Server => 64bit – Intel x64 or AMD64 => highlight the tar file

Press “D” to download, choose “Save to Disk” when prompted, and then hit “Q” once file is saved to quit Lynx

2.) INSTALL AND CONFIGURE SOFTETHER

Unzip the SoftEther File and Prepare to Build

$ tar xzvf softether-vpnserver-vwhateverwhateverwhatever.tar.gz

$ apt-get install build-essential –y

$ cd vpnserver

$ make

Accept the terms of the License Agreement

Type “1” and press “Enter” three times

Move the newly created VPNServer to its new home and chmod file permissions

$ cd ..

$ mv vpnserver /usr/local

$ cd /usr/local/vpnserver

$ chmod 600 \*

$ chmod 700 vpnserver

$ chmod 700 vpncmd

3.) CONFIGURE SOFTETHER TO START ON BOOT

Create file /etc/init.d/vpnserver and copy in the highlighted code

$ sudo nano /etc/init.d/vpnserver

#!/bin/sh

# chkconfig: 2345 99 01

# description: SoftEther VPN Server

DAEMON=/usr/local/vpnserver/vpnserver

LOCK=/var/lock/subsys/vpnserver

test -x $DAEMON || exit 0

case "$1" in

start)

$DAEMON start

touch $LOCK

;;

stop)

$DAEMON stop

rm $LOCK

;;

restart)

$DAEMON stop

sleep 3

$DAEMON start

;;

\*)

echo "Usage: $0 {start|stop|restart}"

exit 1

esac

exit 0

Save and exit

CTRL + “O”

“Y”

CTRL + “X”

4.) RUN THE FOLLOWING COMMANDS TO START AND CLEANUP SOFTETHER INSTALLATION

$ sudo mkdir /var/lock/subsys (MAY NOT NEED THIS)

$ chmod 755 /etc/init.d/vpnserver && /etc/init.d/vpnserver start

$ update-rc.d vpnserver defaults

5.) CHECK TO SEE IF VPN SERVER IS WORKING

$ cd /usr/local/vpnserver

$ ./vpncmd

Press “3” to choose “Use of VPN Tools” then type and enter “check” and watch to make sure all of your checks pass. Type “exit” to exit VPN Tools.

6.) CHANGE ADMIN PASSWORD

Connect to the vpncmd interface

$ cd /usr/local/vpnserver

Connect to the local administrator panel

$ sudo ./vpncmd

Press “1” to choose “Management of VPN Server or VPN Bridge” when it asks for a localhost server, type 127.0.0.1:5555 then hit “Enter” twice to get into server admin mode

$ ServerPasswordSet (then follow the prompts – enter password and confirm)

COMPLETE THE FOLLOWING STEPS ON THE MAIN SERVER

7.) CREATE A LOCAL HUB

GENERAL NOTE: Only create the hubs from the Cluster Controller if you can help it. It makes everything work more smoothly. It’ll automatically disperse computational load to the cluster members based on the weight assigned to each member. The higher the weight, the more of the computational load that particular cluster member takes takes. However, by default, everything gets a weight of 100.

A.) CONNECT TO THE VPNCMD INTERFACE

$ cd /usr/local/vpnserver

Connect to the local administrator panel

$ sudo ./vpncmd

Press “1” to choose “Management of VPN Server or VPN Bridge” when it asks for a localhost server, type 127.0.0.1:5555 then hit “Enter” twice to get into server admin mode

B.) CREATE HUB

$ HubCreate <NameOfSiteToSiteHub>

Where <NameOfSiteToSiteHub> is whatever you would like to name your hub.

Enter an administrator password for the hub and fill out other prompted information.

C.) SELECT VIRTUAL HUB TO WORK WITH

Enter the following command

$ HUB <NameOfSiteToSiteHub>

Where <NameOfSiteToSiteHub> is the name of the hub you would like to administer

D.) CREATE USERS ON HUB

$ UserCreate <NameOfUser>

Where <NameOfUser> is the username you would like to create

Fill out the prompted information.

$UserPasswordSet <NameOfUser>

Where <NameOfUser> is the username you would like to create a password for

Fill out the prompted information

COMPLETE THE FOLLOWING STEPS ON THE LOCAL BRIDGE

8.) CONNECT TO THE VPNCMD INTERFACE

$ cd /usr/local/vpnserver

Connect to the local administrator panel

$ sudo ./vpncmd

Press “1” to choose “Management of VPN Server or VPN Bridge” when it asks for a localhost server, type 127.0.0.1:5555 then hit “Enter” twice to get into server admin mode

9.) CONNECT TO THE BRIDGE

$ Hub BRIDGE

10.) CREATE YOUR CASCADE CONNECTION

This is similar to the Cascade Connection created for the client earlier in the tutorial. It will allow information to flow between the computer the Bridge is housed on (acting as a physical ethernet network segment at a remote location), through the cloud, and ultimately to where the main server is hosted.

$ CascadeCreate <NameOfCascadeConnection> /SERVER:<IPOfMainServer>:5555 /HUB:<NameOfHubCreatedInLastSegment> /USERNAME:<UsernameFromThatHub>

Where <NameOfCascadeConnection> is whatever you would like to name this new connection, <NameOfHubCreatedInLastSegment> is the name of the hub created in Step 7B of this heading, and <UsernameFromThatHub> is a valid username from that same hub.

11.) INPUT A VALID PASSWORD FOR THE CASCADE CONNECTION

$ CascadePasswordSet <NameOfCascadeConnection> /PASSWORD:<UserPassword>

Where <NameOfCascadeConnection> is the name of the Cascade Connection you are working with, and <UserPassword> is the valid password for whatever user you selected in the previous step.

12.) BRING THE CASCADE CONNECTION ONLINE

$ CascadeOnline <NameOfCascadeConnection>

Where <NameOfCascadeConnection> is still the name of the Cascade Connection you are working with.

13.) CHECK TO MAKE SURE YOUR CONNECTION IS ONLINE

$ CascadeList

Make sure that the status for your newly created Cascade Connection states “Online (Established)”.

**TROUBLESHOOTING**

If troubles come up with creating Nic’s on the Client computer (we saw error 31 once or twice, and there was remarkably little help available on the internet), we found that rebooting the VM then going back to the VPNCMD console seemed to fix the problem.

We found that if you run this tutorial on Virtual Machines that get suspended and then brought back online, there can sometimes be problems where the server times don’t match up. The solution we found was to run the following command as root on each machine connected to the cluster to get the clocks synchronized again.

$ sudo ntpdate ntp.ubuntu.com