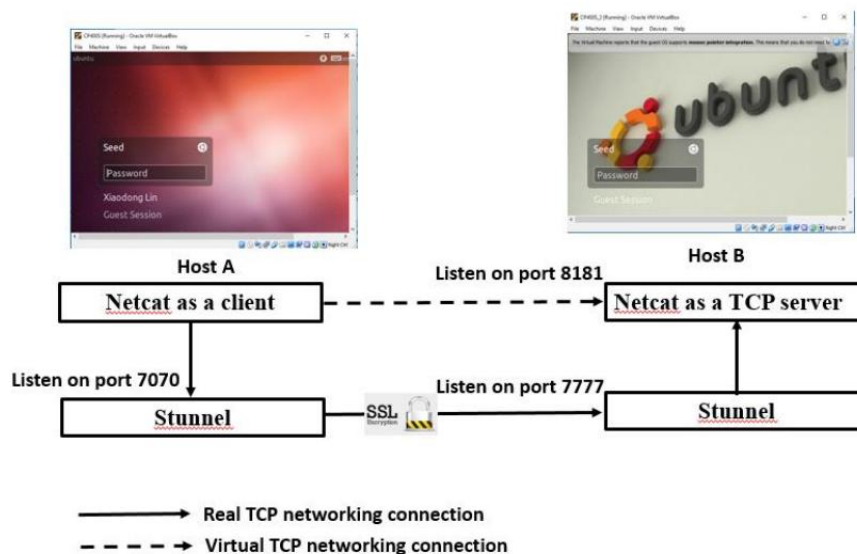


Secure Communication with Stunnel

58119125 JiangZhuoyang

Introduction:

Stunnel is an open source program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows. Stunnel can allow you to secure non-SSL aware daemons and protocols (like POP, IMAP, LDAP, etc) by having Stunnel provide the encryption, requiring no changes to the daemon's code.



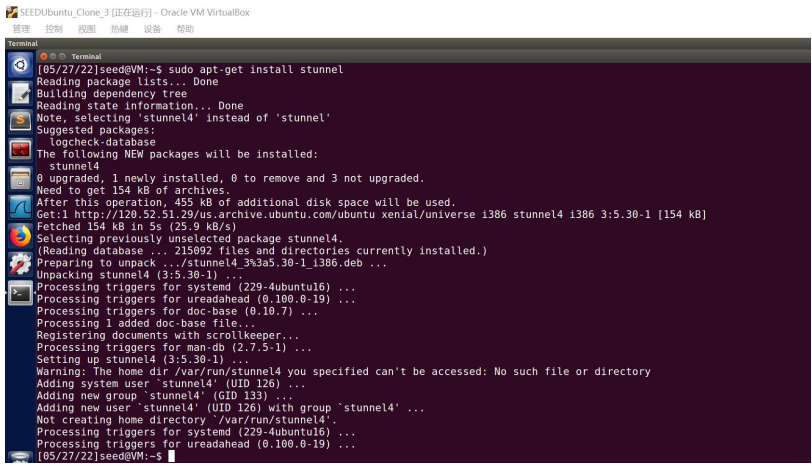
In this lab, we are required to establish a secure channel by using Stunnel, which are shown in the above Figure. In the end, you can use Netcat to listen on a TCP port 8181 on one Ubuntu 16.04 virtual machine (referred to as Host B). Then, you can use Netcat to connect to the Listening TCP port 8181 from another Ubuntu 16.04 virtual machine (referred to as Host A), but over a secure SSL/TLS channel through Stunnel, as shown in the Figure above.

The lab environment:

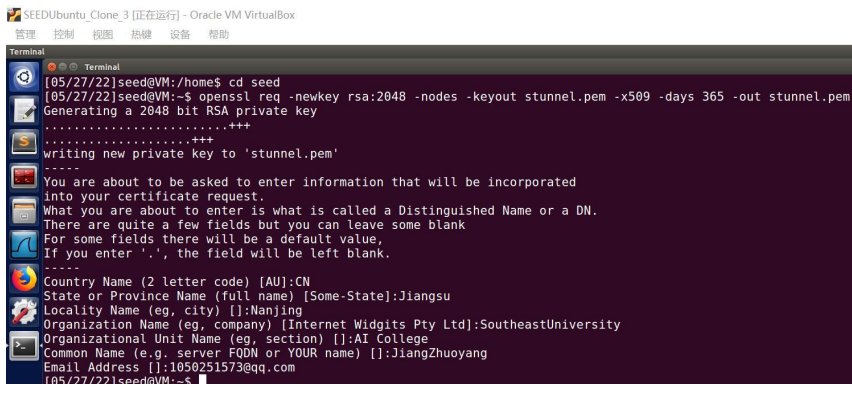
- Ubuntu 16.04 virtual machine HostA as client
- Ubuntu 16.04 virtual machine HostB as sever
- Stunnel and OpenSSL

Setup

Step	Procedure
1.	1. Install the Stunnel -- Universal SSL Wrapper onto two Ubuntu

	<p>16.04 virtual machines.</p> <p>2. To install Stunnel on Ubuntu, type:</p> <p style="text-align: center;"><i>sudo apt-get install stunnel</i></p> <p>3. The result after downloading.</p> 
2.	<p>1. Create two VM as the experiment machine</p> <p>2. Set VM's identity:</p> <p>(1) Host A(Client): 10.0.2.6</p> <p>(2) Host B(Server): 10.0.2.7</p>

Public key encryption with OpenSSL

Step	Procedure
1.	<p>1. Generate private key and certificate for stunnel server-side proxy using OpenSSL</p> <p style="text-align: center;"><i>openssl req -newkey rsa:2048 -nodes -keyout stunnel.pem -x509 -days 365 -out stunnel.pem</i></p> <p>2. Input the certificate information as below:</p> 
2.	<p>1. View private key information</p>

SEEDUbuntu_Clone_3 [正在运行] - Oracle VM VirtualBox

管理 控制 视图 热键 设备 帮助

Terminal

[05/27/22]seed@VM:~\$ cat stunnel.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC4GU7cPzQ2McDv
x1ULJNB3Cd68GLR10JUIs2Y/UHItwqRN7ctkuTvn70lv3G545u/jQeEH0YsKnF1R
TSstEERYNwz3d0fn5pUZc8LriGm9Rr4GkibflyotZNN81YwkzNxFhgGe8Dl6yeoJ
QdEyo1mVaKizPhhvBmbCy9wy/md8XQwUj+hXHo7UvJu5ZJ4NQ9FRyQCADC0vE3Ge
ueMgb4CV7mVo6qn3nSB61MJCX8KgrikKEuwrqrdBI4a9jWQfzeiN6kgWtMPT7B0
QzD7JXC0F09Ee2deZtQrnDtaIgN9jrvqzIX09Rw+wTzmklZfb6shQsH/KPXWco8k
U7Da0hBHAgMBAAECggEARKX7SBmxaHwJC+BymZUuvxTJH69Zy0zqJgJvoDBpQzMP
fZesfnSsKAKMic/SyfaJgUQY6A3HET/ZdFwoQfeM7mIkzammNwM+me0ZMKX/d/sH
JQAeysVdjuvKdWt2Hmp3YZlVFWVWsqbzdLnKChbVv1Ezgi2YeSlhCvWSzSbif8jLF
0RkykCF1TeD0h2/VvgGaHrAD/E/DdojWIEkTVy+qyBg+S3xq2kvIRtLmR2qLfbKb
1dYJEFdRwtvnM2s41qXg+RMYE6pMx/es2gsnYy+JXPJBG/rWnIBLNB+pQSzFScg
RS1VPTpvrON915x4XkdEBcAVjrRpfXK9psAESG3AMQKBgQDpbCg0dhPQkFWX6AI4
nUCg3JmtDvACrHsvq3sltdWgVbqA6BCL04D0i7xQdIHTpfCAep0+AtfhWg4gPo
722Dz1Q2HcdKlj19iJLJ2TqvHZGUz13Dj3nMWepeiqypJ5IgNvV2xWl0EzncbLLY
r/QtIV1aqREtLycT3XcWuUTqwkBgQDj59WooV8pH8dn9gYYRtnErZiYvggSyRHE
2BR3++G0VpR9qGZnfXXhPiTh2HtTdtApc9PhET73L+CPMMLC/U+90WubadJYZ5A8
Zz+vtaTfKwWtNHjd1qMoJ1IUk0fY01oDgux3hAX2qnQ13L/Lhw0IE6w2+SI8edQ0
ekBZ4zcZ1QKBgBjV71kjvRX61XCv0e9GJAM5LYxUKME8vx3CVBb+8m7+wp8mkeQ0
j7V57o6y3yLx5Mx+06hRe5e7i5eTLLDrEK7ul1ouru6rrxvTdTLOzysKs8Gukp5L
HKN2ia5HePmCgVS2JEXf2UmF0eavFhRiHEvU+fbUeERjePqzesA0JZ2DAoGAwd3Y
mZAJ/Rhp/XnhYJhwgTwL0aELkuDwCb9rj0QNxv7+ZNe5jMKo3zHFHJtImM2/ZVPq
sLiUx/NtbG50DUyqW4CE9syz0E94QYprLFgBJG9jyNMCIrFR2a2N2w5KHPH93iY9
/gxDOY0EHJCX6WqpAD1RY76L4IMRQchKMB4T/mkCgYEAo8fY4J6arv7cgXWAXe
JouMMGWI1cC/w0EKXXLI2+u5MLUZB81PN/GhkaALwyNue0DytYt9v9bJP+2W6KU4
ilwLqI0YYVBVMSVBV2URKB/URN/fL9KgsPhYJqR4qp+JHBp6b362N1W+wQv6gLF
y6eljPGowlyvyCMrR8bZ2Ko=
-----END PRIVATE KEY-----

2. View certificate information

SEEDUbuntu_Clone_3 [正在运行] - Oracle VM VirtualBox

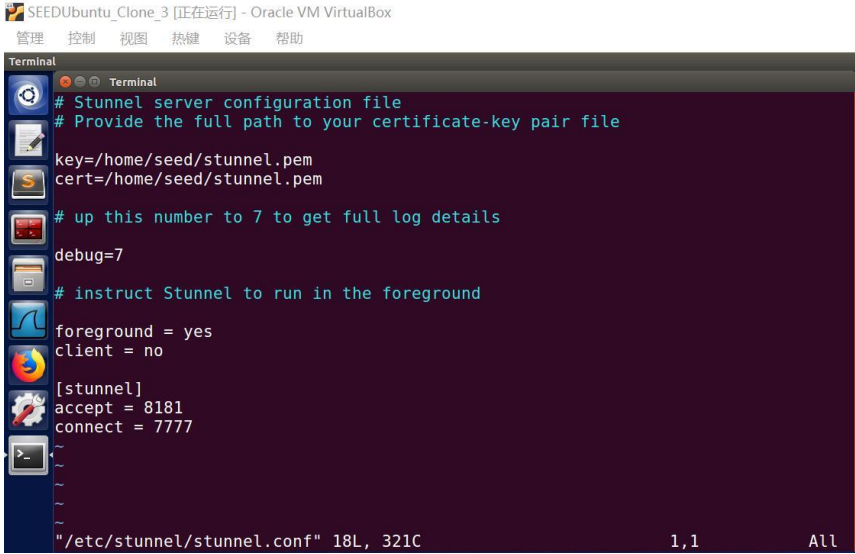
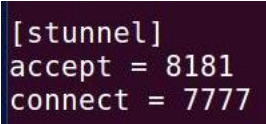
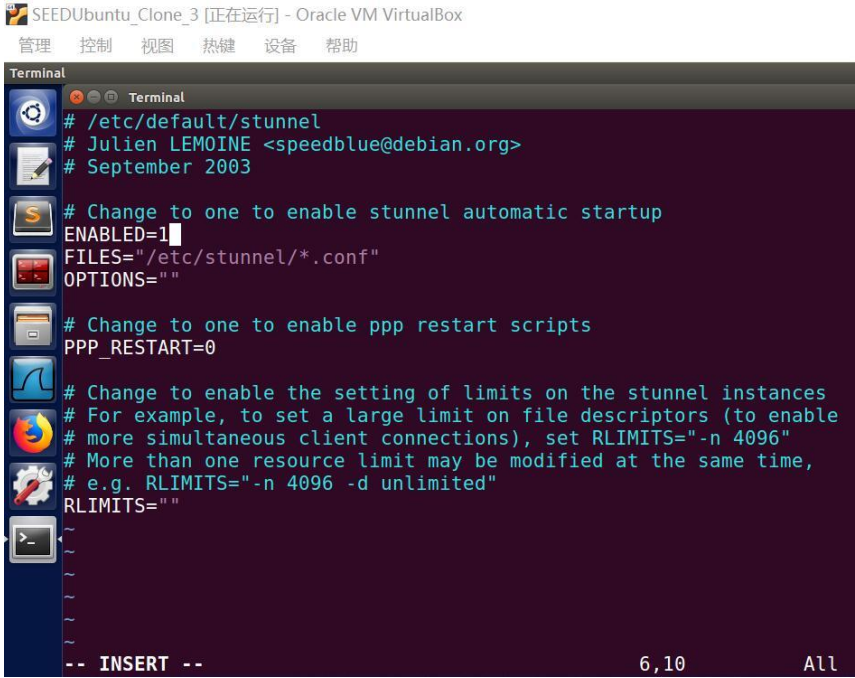

管理 控制 视图 热键 设备 帮助

Terminal

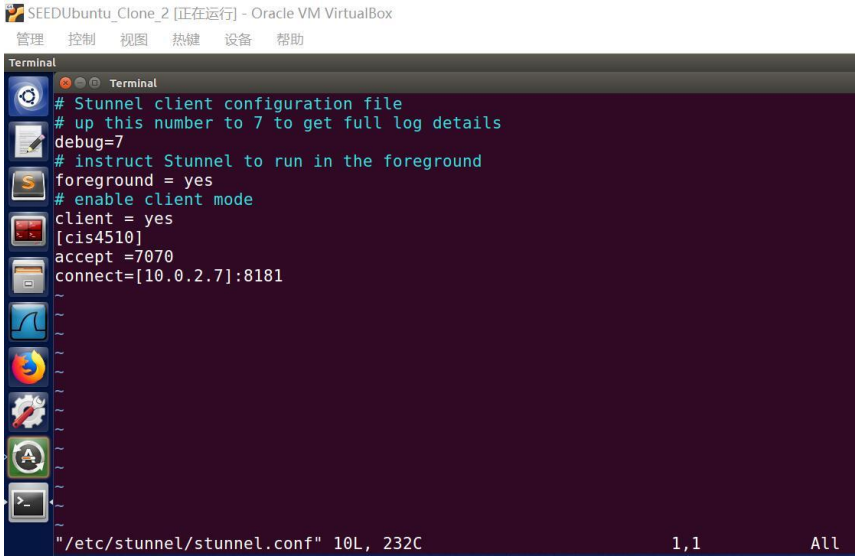
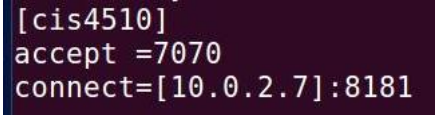
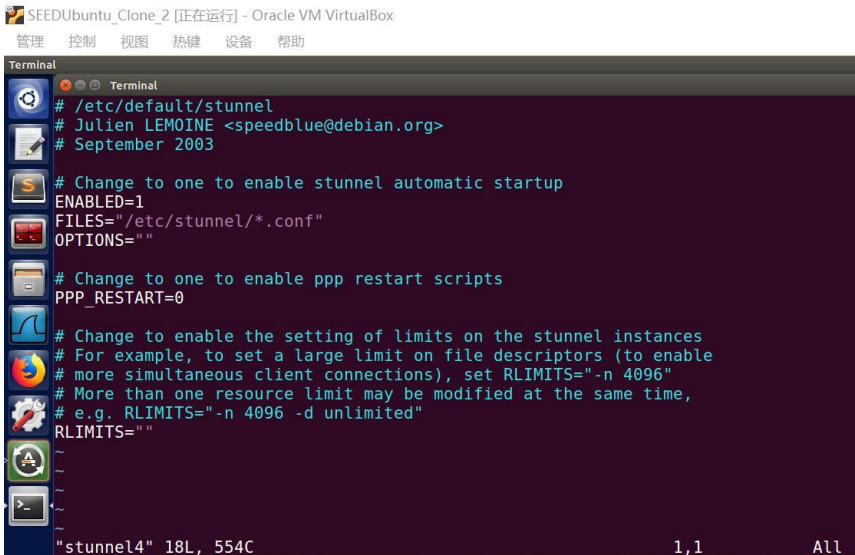
-----BEGIN CERTIFICATE-----
MIIEETCCAvmgAwIBAgIJA0Iy0oWgS1QkMA0GCSqGSIb3DQEBCUAMIGeMwswCQYD
VQ0GEwJDTjEQMA4GA1UECAwHSm1hbmdzdTEQMA4GA1UEBwwHTmFua1uZzEcMBoG
A1UECgwTU291dGhLYXN0VW5pdMlVyc2l0eTETMBEGA1UECwwKQ0929sbGVnZTEW
MBQGA1UEAwwNsm1hbmdaaHVveWVufuZzEgMB4GCSqGSIb3DQEJARYRMTA1MDI1MTU3
M0BxcS5jb2wHhcnMjIwNTI3MDg0NDA0WmcNMjIwNTI3MDg0NDA0WjCBnjELMAK6
A1UEBhMQ04xEDA0BgNVBAGMB0ppYw5nc3UxEDA0BgNVBACMB05hbmppbmcxHDAa
BgNVBAoME1NvdXR0ZWZzdFVuaXZlcnNpdHkxZARBgNVBAcMCKFJIEUvNGxLZ2Ux
FjAUBGNVBAMMDUppYw5nWmh1b31hbmcxIDAeBgkqhkiG9w0BCQEWEWNTAyNTE1
NzNAcXEuY29tMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuB103D80
NjHA78dVJSTQdwneVpUddCVCLNmP1ByLcKkTe3LZLk75+9Jb9xue0bv40BHzmL
CpxdU00rLRBECjCM93UH5+aVGXPJa4hpVua+BpIm35cqlWTZ/JWMJMzcR34BnvA5
esnqCUHRMqNZLWiosz4YbwZmwsvcMv5nfF0MFI/oVx601LYbuWSeDUPRa2EAgAwj
rxNxnrrnIG+AlE51a0qp950getTCQL/CoK4pChLsEaq3Q50GvY1kH83ojepBsE8D
D0+wdEMw+yQLzhTvrHtnXmbUK5w7WiIDfY676syF9PUcPsE85pJWX2+rIULB/yj1
1nKPJF0w2kIQRwIDAQABA1AwTjAdBgNVHQ4EFgQUwITxm0E89Nsa3F8jpIRBqCpB
ifwWwHYDVR0jBBgwFoAUwITxm0E89Nsa3F8jpIRBqCpBifwWwHYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQsFAAOCAQEALyRSc+rMD9H0t/1qb64PK5LRb95JC0xXbTp
uuAa715BD81wofYE2nP00wtLntKfYmlyrEoAWJ17/hvUEh5Tv0bWFZerDFsvN1c
8bssfqVTknLqBKq2odfTALabayqAam3/YQtLVgpPKtgiPoc3MQG1uL6f8mhUYaaU
Dqd5jkCblKXnYXR84LXf4YdjVuNigCDC+1pb6zeXB53kRKWF6XBGUFYennIAGw
l0I4tV7c0gXpVHgMwveeNYqt5G3UZD0z0HaV0+LTpHfb0WvDGD0dpM2xxHnc/JUL
3g45v8k5D11vJYLnr3yjK5c4ejFxdsusRMYLGV3YvX110V7/Ng==
-----END CERTIFICATE-----
[05/27/22]seed@VM:~\$

Stunnel configuration on Server VM

Step	Procedure
1.	1. create a "stunnel.conf" file in the “/etc/stunnel” directory: <i>sudo vi /etc/stunnel/stunnel.conf</i> 2. Modify the server VM’s "stunnel.conf" file:

	<div data-bbox="496 208 1353 759"><pre>SEEDUbuntu_Clone_3 [正在运行] - Oracle VM VirtualBox 管理 控制 视图 热键 设备 帮助 Terminal # Stunnel server configuration file # Provide the full path to your certificate-key pair file key=/home/seed/stunnel.pem cert=/home/seed/stunnel.pem # up this number to 7 to get full log details debug=7 # instruct Stunnel to run in the foreground foreground = yes client = no [stunnel] accept = 8181 connect = 7777 ~/etc/stunnel/stunnel.conf 18L, 321C 1,1 All</pre></div> <p>3. Configure port information:</p> <div data-bbox="793 835 1059 958"><pre>[stunnel] accept = 8181 connect = 7777</pre></div>
<p>2.</p>	<p>1. Enabling Stunnel by modifying the /etc/default/stunnel4 file, firstly open the file:</p> <p style="text-align: center;"><i>sudo vi stunnel4</i></p> <p>2. Modify the server VM's "stunnel4" file:</p> <div data-bbox="496 1164 1353 1839"><pre>SEEDUbuntu_Clone_3 [正在运行] - Oracle VM VirtualBox 管理 控制 视图 热键 设备 帮助 Terminal # /etc/default/stunnel # Julien LEMOINE <speedblue@debian.org> # September 2003 # Change to one to enable stunnel automatic startup ENABLED=1 FILES="/etc/stunnel/*.conf" OPTIONS="" # Change to one to enable ppp restart scripts PPP_RESTART=0 # Change to enable the setting of limits on the stunnel instances # For example, to set a large limit on file descriptors (to enable # more simultaneous client connections), set RLIMITS="-n 4096" # More than one resource limit may be modified at the same time, # e.g. RLIMITS="-n 4096 -d unlimited" RLIMITS="" -- INSERT -- 6,10 All</pre></div> <p>3. Set ENABLED to 1:</p> <div data-bbox="831 1912 1021 1957"><pre>ENABLED=1</pre></div>

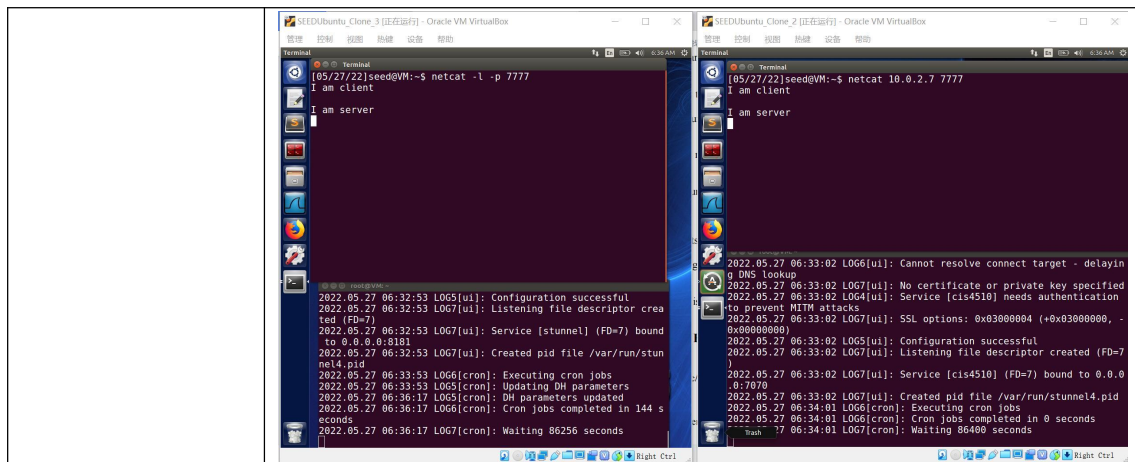
Stunnel configuration on Client VM

Step	Procedure
1.	<p>1. create a "stunnel.conf" file in the “/etc/stunnel” directory: <i>sudo vi /etc/stunnel/stunnel.conf</i></p> <p>2. Modify the client VM's "stunnel.conf" file:</p>  <pre># Stunnel client configuration file # up this number to 7 to get full log details debug=7 # instruct Stunnel to run in the foreground foreground = yes # enable client mode client = yes [cis4510] accept =7070 connect=[10.0.2.7]:8181</pre> <p>3. Configure port information:</p>  <pre>[cis4510] accept =7070 connect=[10.0.2.7]:8181</pre>
2.	<p>1. Enabling Stunnel by modifying the /etc/default/stunnel4 file, firstly open the file: <i>sudo vi stunnel4</i></p> <p>2. Modify the client VM's "stunnel4" file:</p>  <pre># /etc/default/stunnel # Julien LEMOINE <speedblue@debian.org> # September 2003 # Change to one to enable stunnel automatic startup ENABLED=1 FILES="/etc/stunnel/*.conf" OPTIONS="" # Change to one to enable ppp restart scripts PPP_RESTART=0 # Change to enable the setting of limits on the stunnel instances # For example, to set a large limit on file descriptors (to enable # more simultaneous client connections), set RLIMITS="-n 4096" # More than one resource limit may be modified at the same time, # e.g. RLIMITS="-n 4096 -d unlimited" RLIMITS=""</pre> <p>3. Set ENABLED to 1:</p>

ENABLED=1

Test TCP information transmission under stunnel agent

Step	Procedure
1.	<div><div>1. Test run stunnel on the server VM</div><div></div><div>2. Test run stunnel on the client VM</div><div></div></div>
2.	<div><div>1. Establish TCP connection with stunnel on the client and connect to the server:</div><div></div><div>2. Using stunnel to establish the TCP connection with the client on the server:</div><div></div><div>3. The connection is successful. Start the communication test. The test results are as follows:</div></div>



Analyze our results:

We were puzzled when setting the port number of the stunnel configuration file. However, after deeply understanding the principle of the stunnel agent, we understood the true meaning of accept and connect, and successfully set the port. Finally, we ran stunnel on two virtual machines at the same time, established a TCP connection between the client and the server, and successfully completed secure communication.