RESOURCE AND PATIENT MANAGEMENT SYSTEM

Encrypt Data in Flight; Disable Telnet Access.

Installation Guide

MARCH 2019

Office of Information Technology (OIT)

Rockville, Maryland

Table of Contents

Table of Contents....i

1.0 Document Overview....1

1.1 Historical Information....1

1.2 Project Overview....1

2.0 Acquire Software....1

2.1 Software Description....1

2.2 Download Software (Windows)....1

2.3 Download Software (AIX)....1

3.0 Configure & Install Server Software....2

3.1 Choose New Port....2

3.2 Configure & Install Software (Windows Server)....3

3.3 Configure & Install Software (AIX Server)....3

3.4 Configure Software (Windows Client)....3

4.0 Configure Firewall Access....4

4.1 Configure Windows Server Firewall....4

4.2 Configure AIX Server Firewall....4

5.0 Install Workstation Software....4

5.1 Configure stunnel.conf file for workstations....4

5.2 Install & Test Windows Workstation Software....5

5.3 Test connectivity to the RPMS server....6

6.0 Disable Telnet access to Servers....7

6.1 Disable Telnet on Windows....7

6.2 Disable Telnet on AIX....7

7.0 Appendices

7.1 Appendix A: Helpdesk Contact Information....8

1.0 Document Overview

1.1 Historical Information

When computers first started being used to store medical information, there would be one central computer called a mainframe and "dumb" display terminals that interfaced with that one computer.

As computers improved to the point where it was more economical to have individual PCs on the desktop, the paradigm of 'connecting to a central server' still existed and the server software itself was still quite useful, so programs were written so these computers could emulate the display terminals of long ago to communicate with the medical server. The currently used protocol for this communication is called ***Telnet.***

Unfortunately, as computers and networks progressed, so did ways of accessing this data inappropriately, and Telnet is a protocol that sends data "in the clear" or unencrypted. Another way to state this is "easily accessed by people that shouldn't."

There are ways of encrypting network traffic so nefarious users can't access it, however, RPMS isn't currently compatible with the most used standards. So, we have to install an "invisible" workaround to encrypt the traffic. There are free programs that will create an encrypted tunnel – then all we have to do is "point" our unencrypted network traffic at the tunnel and verify it works; then once all workstations are set up with the tunnel software, disable the unencrypted connectivity via an Access Control List or firewall.

1.2 Project Overview

We're going to install encrypted tunneling software (called 'stunnel') on the RPMS server and workstations, test it, install the stunnel software on the workstations, verify all Telnet traffic is now encrypted, then disable the Telnet port on the server disallowing any unencrypted data transmission.

2.0 Acquire Software

2.1 Software Description

The required software is called 'stunnel' and is completely free to use in a commercial setting and open source. So, outside of the time & personnel required for the project, there won't be any capital outlay. Be sure to download the latest version of the software

2.2 Download Software (Windows)

The software can be downloaded here: https://www.stunnel.org/downloads.html

2.3 Download Software (AIX)

The software can be downloaded here: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.html

3.0 Configure and Install Server Software

3.1 Choose New Port

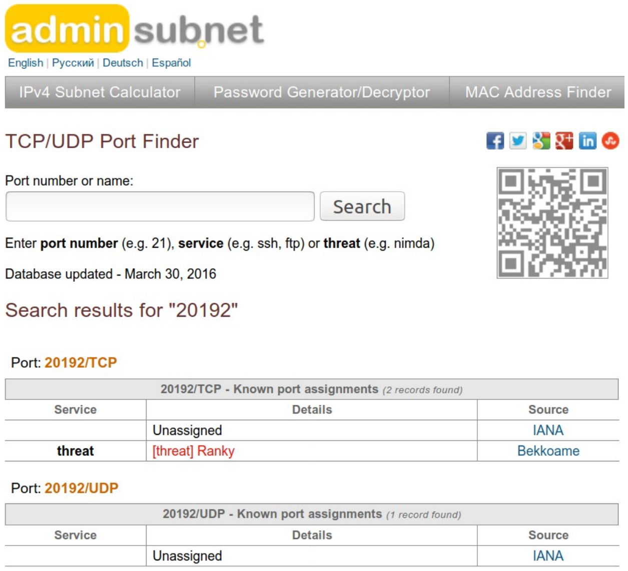
To tunnel the Telnet traffic, we need to choose a new, unused port on the server. Assigned ports are controlled by the IANA, or Internet Assigned Numbers Authority. There are many utilities on the web that can tell you if a port is assigned or not, here's one such website:

http://www.adminsub.net/tcp-udp-port-finder/

It's not a bad idea to use a port that would be easy to remember – in this case, 20190 would work fine. It's not assigned, and chances are good that it's not in use on your server, but always doublecheck!

One reason is that certain ports may have been 'hijacked' by malware – if you use these ports and open your firewall to them, that may allow a malware attack vector into your server. The most descriptive term for this is **"Bad Mojo!"** See the attached image to the right.

For the rest of this document, we're going to use the port 20190 in our examples.


admin subnet
English | Русский | Deutsch | Español
IPv4 Subnet Calculator
Password Generator/Decryptor
MAC Address Finder
Search

TCP/UDP Port Finder

Port number or name:

Enter **port number** (e.g. 21), **service** (e.g. ssh, ftp) or **threat** (e.g. nimda)

Database updated - March 30, 2016

Search results for "20192"

Port: 20192/TCP

20192/TCP - Known port assignments *(2 records found)*		
Service	Details	Source
	Unassigned	IANA
threat	[threat] Ranky	Bekkoame

Port: 20192/UDP

20192/UDP - Known port assignments *(1 record found)*		
Service	Details	Source
	Unassigned	IANA

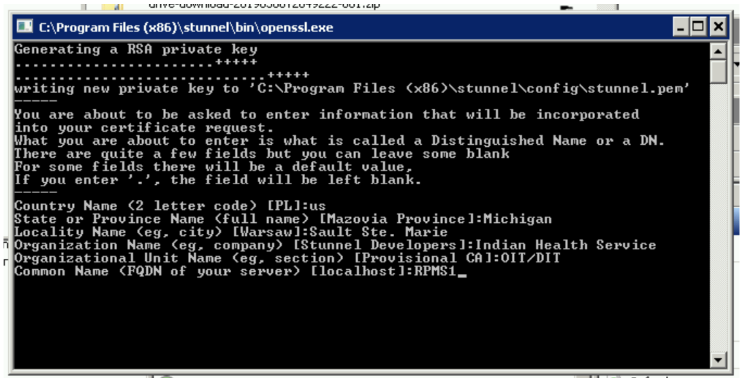
3.2 Configure and install Software (Windows Server)

Verify you are a server administrator, as full administrative rights are required to install this software.

Locate the software installer you downloaded in section 2.2 and double-click on it. If you receive a pop-up asking to make changes to the server, click 'Yes.'

You will see several screens, you can choose the default for each screen, until the very last screen, which is a command prompt window. It will ask you for several pieces of information to build a key – the fields should be populated with information respective to your local system. There's an example of the screen to the right.

The very last field will be "Common Name" – put the name of your server there, and when you hit {Enter} the window will disappear and it will build your SSH key for you.



```
Generating a RSA private key
.......................+++++
..............................+++++
writing new private key to 'C:\Program Files (x86)\stunnel\config\stunnel.pem'
-----
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) [PL]:us
State or Province Name (full name) [Mazovia Province]:Michigan
Locality Name (eg, city) [Warsaw]:Sault Ste. Marie
Organization Name (eg, company) [Stunnel Developers]:Indian Health Service
Organizational Unit Name (eg, section) [Provisional CA]:OIT/DIT
Common Name (FQDN of your server) [localhost]:RPMS1_
```

Once installed, you'll need to install the service – this can either be done from the Start Menu with this icon: stunnel Service Install Or with this command issued in an Administrator Command Prompt:

```
"c:\Program Files (x86)\stunnel\bin\stunnel.exe" -install
```

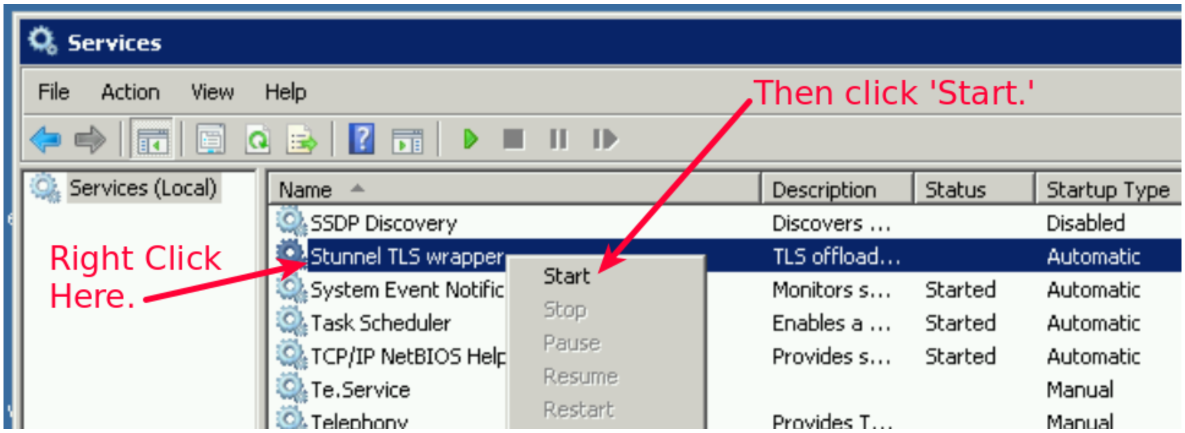
[[If the command fails, try removing the underlined portion of the command above. If that still fails, try the GUI icon instead.]]

Now, we'll need to configure the service. Click this icon in the Start menu: Edit stunnel.conf and it will request permission to start Notepad with Administrator privileges – click "Yes." You can either remove all lines from the file and start from scratch (easier but removes documentation) or 'comment' out all of the existing lines that do not start with a semicolon - ';'. Once that's complete, at the bottom of the file add these lines *[[again, assuming the new port will be 20190]]*:

```
[telnet]
accept = 20190
connect = 23
cert = stunnel.pem
```

and Save the file.

Once that's been saved, then we'll need to start the service. This can either be done from the Start menu with this icon: stunnel Service Start Or, by going to the Services section under "Administrative Tools" and right-clicking on the Stunnel TLS wrapper service and selecting 'Start.' See the screenshot below.



Name	Description	Status	Startup Type
SSDP Discovery	Discovers ...		Disabled
Stunnel TLS wrapper	TLS offload...		Automatic
System Event Notific	Monitors s...	Started	Automatic
Task Scheduler	Enables a ...	Started	Automatic
TCP/IP NetBIOS Help	Provides s...	Started	Automatic
Te.Service			Manual
Telephony	Provides T...		Manual

Right Click Here.

Then click 'Start.'

If you get a pop-up window stating that the service couldn't start, or if the Status for that service above doesn't change to "Started," you may have made an error in the configuration file above, follow the steps again at the beginning of this section and try it again. If that doesn't rectify the situation, please call the Helpdesk and put a ticket in regarding this issue; the contact information is in Appendix A.

3.3 Configure and install Software (AIX Server)

This is a placeholder for the AIX server instructions – although the end product is quite similar to above, the lack of a GUI interface will make the implementation instructions very, very much different.

4.0 Configure Firewall Access

4.1 Configure Windows Server Firewall

With the stunnel application installed, it might set up the Windows Firewall to work, but sometimes it doesn't work correctly. So, just in case, this is an alternate way of setting up the firewall to allow traffic on the stunnel port through.

Start the Windows Firewall application by clicking on this in Control Panel:

and then in that window on the left hand side, click on Advanced Settings:

Then in that window, right-click on the Inbound Rules entry, and click "New Rule…"

When asked for a Rule Type, click "Port", then "Next>"

Leave TCP selected, and under "Specific local ports:" enter 20190 *[[or what port you selected in Section 3.1]]* and click 'Next>'. Keep clicking 'Next>' until you get to the last entry – Name – and enter 'stunnel Port' then click 'Finish.'

Windows firewall should activate the rule and you're good to go.

4.2 Configure AIX Server Firewall

This is a placeholder for the AIX server instructions – Unix like operating systems have a completely different security model so I will require access to an AIX system to configure before I can complete this section.

5.0 Install Workstation Software

5.1 Configure stunnel.conf file for workstations

Make a copy of the stunnel.conf file that you modified in Section 3.2 (Win) / 3.3 (AIX) to a separate network share or flash drive, and then open it in Notepad (Win) or nano/vim (AIX) – remove the server configuration that you added above, and add this at the bottom of the file:

```
[telnet-client]
client = yes
accept = 127.0.0.1:23
connect = ip_address_of_RPMS_server:20190
cert = stunnel.pem
```

Above, you'll need to replace: `ip_address_of_RPMS_server` with the actual IP address of your RPMS server.

Make a copy of the stunnel.pem file as well, as we need to copy that file to the workstations.

5.2 Install & Test Windows Workstation Software

Verify you are an administrator of the workstation, as full administrative rights are required to install.

Locate the software installer you downloaded in section 2.2 and double-click on it. If you receive a pop-up asking to make changes to the workstation, click 'Yes.'

You will see several screens, you can choose the default for each screen, until the very last screen, which is a command prompt window, just like before. However, this time it won't matter what you enter because we're not going to use the new key, we're going to copy the server key to the workstation. Just hit enter at all the questions until the window disappears.

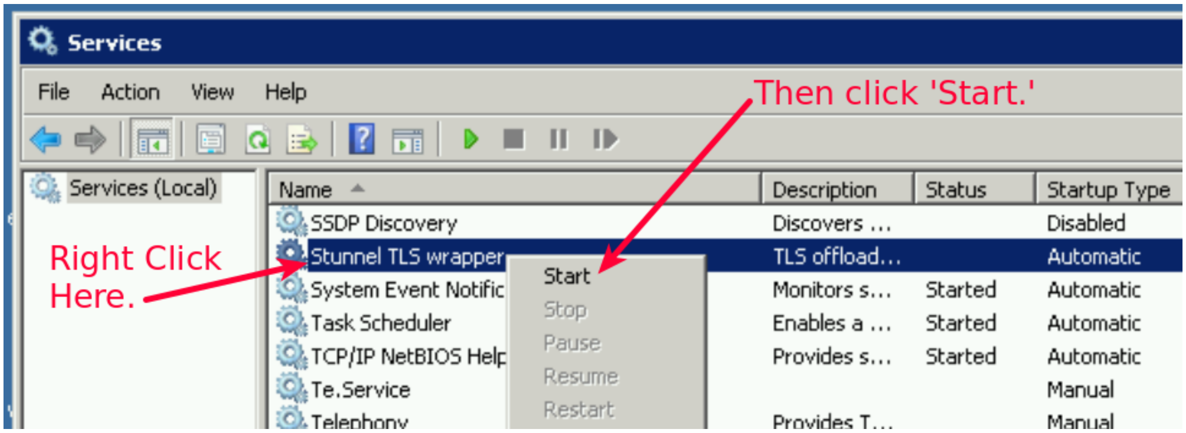
Once installed, you'll need to install the service – this can either be done from the Start Menu with this icon: stunnel Service Install Or with this command issued in an Administrator Command Prompt:

```
"c:\Program Files (x86)\stunnel\bin\stunnel.exe" -install
```

[[If the command fails, try removing the underlined portion of the command above. If that still fails, try the GUI icon instead.]]

Once the software is installed, browse to: `c:\Program Files (x86)\stunnel\conf\` on the workstation and delete the files: stunnel.pem and stunnel.conf. Once those are gone, copy the stunnel.pem file and your modified stunnel.conf (from section 5.1 above) from your network / flash drive to that directory.

Once that's been saved, then we'll need to start the service. This can either be done from the Start menu with this icon: stunnel Service Start Or, by going to the Services section under "Administrative Tools" and right-clicking on the Stunnel TLS wrapper service and selecting 'Start.' See the screenshot below.



Name	Description	Status	Startup Type
SSDP Discovery	Discovers ...		Disabled
Stunnel TLS wrapper	TLS offload...		Automatic
System Event Notific	Monitors s...	Started	Automatic
Task Scheduler	Enables a ...	Started	Automatic
TCP/IP NetBIOS Help	Provides s...	Started	Automatic
Te.Service			Manual
Telephony	Provides T...		Manual

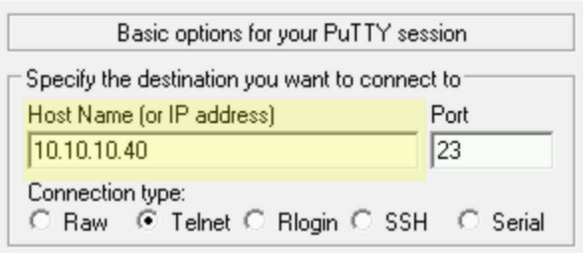
If you get a pop-up window stating that the service couldn't start, or if the Status for that service above doesn't change to "Started," you may have made an error in the configuration file above, follow the steps again at the beginning of this section and try it again. If that doesn't rectify the situation, please call the Helpdesk and put a ticket in regarding this issue; the contact information is in Appendix A.

5.3 Test connectivity to the RPMS server

Unfortunately, this section can't cover every instance of every terminal emulation software package. To mention a few, there's Putty, NetTerm, SecureCRT, AnyConnect, etc. Including instructions for every possible terminal emulator would be problematic at best, so I will demonstrate the setting change in Putty (it's quite simple, actually) and hopefully the local IT folks will be able to translate the information below into instructions applicable to your local software standard.

Anyway, in your terminal emulation software, there will be an IP address or name of your RPMS server in the configuration, like the image to the right.

The highlighted portion is the IP address of a test server – the IP address or name will be different for your local configuration.



Basic options for your PuTTY session

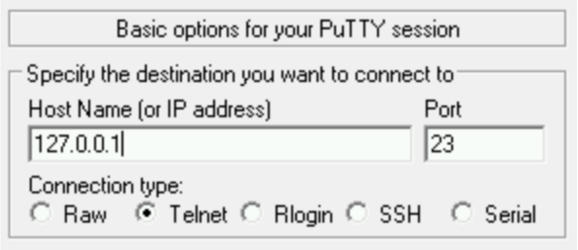
Specify the destination you want to connect to

Host Name (or IP address): 10.10.10.40

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

All that needs to change, is that Host Name needs to be changed to the Loopback IP Address of the computer, which is 127.0.0.1. So, for my demo screen, it would look like this:



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 127.0.0.1

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

That's it! Once you save the configuration change, go ahead and test this by trying to log into RPMS.

If successful, repeat section 5 for every other workstation that connects to the RPMS server.

6.0 Disable Telnet access to Servers

6.1 Disable Telnet on Windows

With the stunnel application installed on all of the workstations, now we need to disable the Telnet protocol from any external access. Windows Firewall is the method we'll use to do this.

Start the Windows Firewall application by clicking on this in Control Panel:

Windows Firewall

and then in that window on the left hand side, click on Advanced Settings:

Advanced settings

Click on the Inbound Rules and scroll to the right until you see a heading called 'Local Port.' Click on the heading so that it will sort on the local port. Scroll through and see if there's a local port rule with 23, if so, then that's your Telnet rule and you should disable that rule.

If you don't see one, then you'll need to disable it specifically. Right-click on the Inbound Rules entry, and click "New Rule…"

When asked for a Rule Type, click "Port", then "Next>"

Leave TCP selected, and under "Specific local ports:" enter 23 and click 'Next>'.

Under the Action step, click "Block the Connection" and click 'Next>.'

Keep clicking 'Next>' until you get to the last entry – Name – and enter 'Block Telnet,' then click 'Finish.'

Windows firewall should activate the rule and you're good to go.

6.1 Disable Telnet on AIX

This is a placeholder for the AIX server instructions – Unix like operating systems have a completely different security model so I will require access to an AIX system to configure before I can complete this section.

7.0 Appendices

7.1 Appendix A: HelpDesk Contact Information

OIT HELP DESK

Phone: (888) 830-7280

Web: http://www.ihs.gov/helpdesk/

Email: support@ihs.gov