Skip to main content.

BSD Now

A Weekly BSD Podcast - News, Interviews and Tutorials

Subscribe on Youtube « | Subscribe with iTunes « | RSS: MP3 | Video | HD Video | HD Torrent Feed
Navigation: Home | Episodes | About | Live | Shirt | Contact Us | Tutorials

Using stunnel and SSH to bypass IDS

2013-09-04

Live demo in BSD Now Episode 001 | Originally written by TJ for bsdnow.tv | Last updated: 2014/08/20

NOTE: the author/maintainer of the tutorial(s) is no longer with the show, so the information below may be outdated or incorrect.

Here’s a scenario: say you're on an untrusted network, be it corporate, university or at a foreign hotel. You want to tunnel all your traffic through SSH to your trusted server, right?

We can't have those pesky script kiddies sniffing your traffic. But what's this? You can't get out on port 22! You can't get out on that other random port you used for SSH either! They're filtering everything but ports 80 and 443. Sometimes just running SSH on port 443 will let you get past this, but other times there's deep packet inspection in place to prevent that. Any IDS will be able to easily detect SSH on any port you run it on, so we'll have to find a way to hide it in plain sight. Enter stunnel. It's a simple tool that lets you encapsulate traffic of any protocol in standard SSL/TLS. Your stream of packets will look exactly like a connection to your gmail or anything else. The setup is pretty simple. You'll need stunnel installed on both your client PC and a remote server with sshd already running. Let's install stunnel on the server, make a quick config and setup your key. For FreeBSD, I'll be using ports.

```
# cd /usr/ports/security/stunnel
# make config-recursive install clean
# vi /usr/local/etc/stunnel/stunnel.conf
```

In the config, we're going to put the following:

```
cert=/etc/ssl/stunnel.pem
pid=/var/run/stunnel.pid
setuid = stunnel
setgid = stunnel
[ssh]
accept = your_server_IP:443
connect = 127.0.0.1:22
```

Now we'll generate the key:

```
# cd /etc/ssl
# openssl genrsa 1024 > stunnel.key
# openssl req -new -key stunnel.key -x509 -days 1000 -out stunnel.crt
# cat stunnel.crt stunnel.key > stunnel.pem
# chmod 600 stunnel.pem
# service stunnel onestart
```

Be sure to allow incoming connections to port 443 in your firewall. Now we move over to the client PC. Install stunnel and set up a similar configuration.

```
# cd /usr/ports/security/stunnel
# make config-recursive install clean
# vi /usr/local/etc/stunnel/stunnel.conf
```

In the client config, we put:

```
pid=/var/run/stunnel.pid
client=yes
setuid = stunnel
setgid = stunnel
[ssh]
accept=443
connect=your_server_IP:443
```

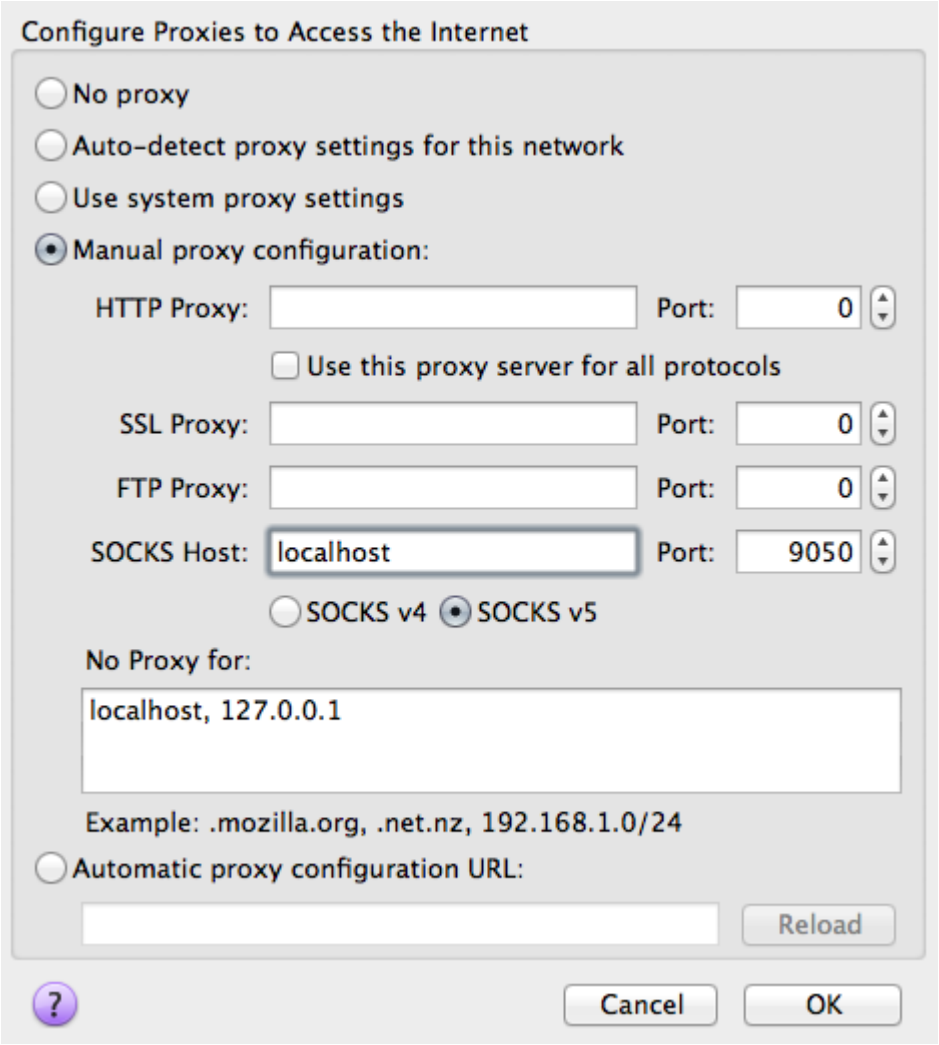
Start the service and test it out:

```
# service stunnel onestart
$ ssh -vp 443 youruser@localhost
```

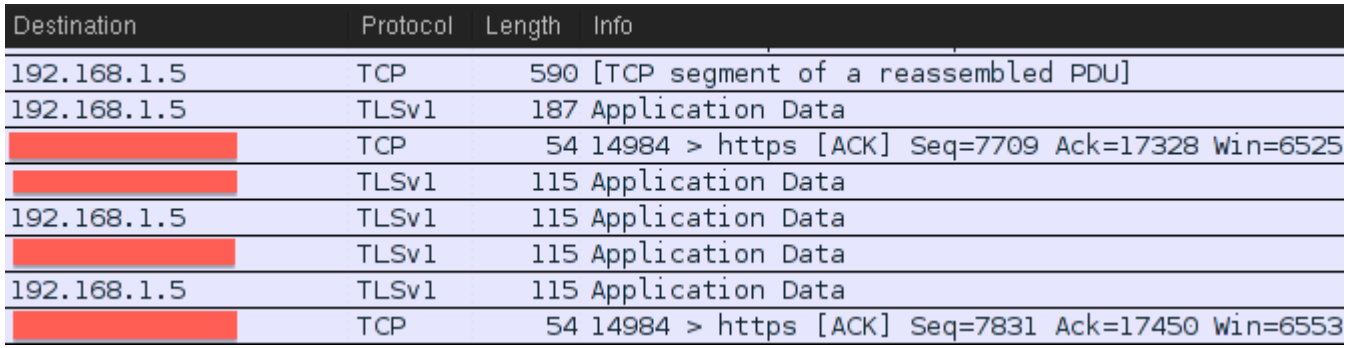
At this point you should be SSHed into your remote server, but all the traffic is tunneled through SSL. Now, say you want to tunnel all your web browsing traffic through this. With stunnel running on both systems, run this on the client:

```
$ ssh -Cv -ND localhost:9050 localhost
```

And set your browser proxy settings to tunnel all traffic through a SOCKS host of localhost:9050



To verify everything is working, fire up Wireshark or tcpdump:



Destination	Protocol	Length	Info
192.168.1.5	TCP	590	[TCP segment of a reassembled PDU]
192.168.1.5	TLSv1	187	Application Data
[redacted]	TCP	54	14984 > https [ACK] Seq=7709 Ack=17328 Win=6525
[redacted]	TLSv1	115	Application Data
192.168.1.5	TLSv1	115	Application Data
[redacted]	TLSv1	115	Application Data
192.168.1.5	TLSv1	115	Application Data
[redacted]	TCP	54	14984 > https [ACK] Seq=7831 Ack=17450 Win=6553

Done! It's recommended that you stop the stunnel service when you're not planning on using it, since all SSH connections appear to come from 127.0.0.1, and it can be annoying if someone is trying to bruteforce your login.

Latest News

New announcement

2017-05-25

Hi, Mr. Dexter. Also, we understand that Brad Davis thinks there should be more real news....

Two Year Anniversary

2015-08-08

We're quickly approaching our two-year anniversary, which will be on episode 105. To celebrate, we've created a unique t-shirt design, available for purchase until the end of August. Shirts will be shipped out around September 1st. Most of the proceeds will support the show, and specifically allow us to buy...

New discussion segment

2015-01-17

We're thinking about adding a new segment to the show where we discuss a topic that the listeners suggest. It's meant to be informative like a tutorial, but more of a "free discussion" format. If you have any subjects you want us to explore, or even just a good name...

How did you get into BSD?

2014-11-26

We've got a fun idea for the holidays this year: just like we ask during the interviews, we want to hear how all the viewers and listeners first got into BSD. Email us your story, either written or a video version, and we'll read and play some of them for...

1 | 2 | 3 | 4 | 5 | Next >

Episode 228: The Spectre of Meltdown

2018-01-10

Direct Download:HD VideoMP3 AudioTorrent This episode was brought to you by Headlines Meltdown Spectre Official Site Kernel-memory-leaking Intel processor design flaw forces Linux, Windows redesign Intel’s official response The Register mocks intels response with pithy annotations Intel’s Analysis PDF XKCD Response from FreeBSD FreeBSD's patch WIP Why Raspberry Pi isn’t vulnerable to Spectre or Meltdown Xen mitigation patches Overview of affected FreeBSD Platforms/Architectures Groff's response We’ll...

Episode 227: The long core dump

2018-01-03

Direct Download:HD VideoMP3 AudioTorrent This episode was brought to you by Headlines NetBSD 7.1.1 released The NetBSD Project is pleased to announce NetBSD 7.1.1, the first security/critical update of the NetBSD 7.1 release branch. It represents a selected subset of fixes deemed important for security or stability reasons. Complete source and binaries for NetBSD 7.1.1...

Episode 226: SSL: Santa's Syscall List

2017-12-27

Direct Download:HD VideoMP3 AudioTorrent This episode was brought to you by Headlines FreeBSD Q3 Status Report 2017 FreeBSD Team Reports FreeBSD Release Engineering Team Ports Collection The FreeBSD Core Team The FreeBSD Foundation Projects FreeBSD CI Kernel Intel 10G iflib Driver Update Intel iWARP Support pNFS Server Plan B Architectures AMD Zen (family 17h) support Userland Programs Updates to GDB Ports FreeBSDDesktop OpenJFX 8 Puppet Documentation Absolute FreeBSD, 3rd Edition Manual Pages Third-Party Projects The nosh Project FreeBSD...

Episode 225: The one true OS

2017-12-20

Direct Download:HD VideoMP3 AudioTorrent This episode was brought to you by Headlines TrueOS stable release 17.12 We are pleased to announce a new release of the 6-month STABLE version of TrueOS! This release cycle focused on lots of cleanup and stabilization of the distinguishing features of TrueOS: OpenRC, boot speed, removable-device...