Fireside Fridays

Anatomy of a VPN
Part 3 of 3

Thanks to our sponsors!

ACTIVE | COUNTERMEASURES

BLACK HILLS
Information Security
• 2008 •

WILD WEST
HACKIN' FEST

Antisyphon Training

Lab requirements for this section

- Today is just lecture
- No lab setup needed

Last 2 weeks on Fireside Fridays

- We discussed the components of a VPN
  - Initial authentication
  - Set up a secure channel over an insecure medium
  - Privacy for all transmitted data
  - Authenticate every packet
- This week we'll look at implementations

Common VPNs

- SecureSHell (SSH)
- IPSec
- TLS
- We'll do a brief overview of each

SSH

- Mostly used for secure system administration
- Can function as a rudimentary VPN
- Authentication options
  - Passwords
  - Public/private keys
  - Digital certificates
- Certs - more up front work but easier to manage

Basic SSH

- Can provide a secure terminal session to a remote system
  - Cross platform compatibility
- Can also transfer files securely
  - Syntax on command line is challenging, GUI easier
  - You can even stream audio and video
  - Mount remote file systems via sshfs
  - Sync file systems using rsync

X-Windows support

- Sort of like remote desktop, but not
- Let's you launch graphical apps on a remote server from your desktop
- App actually runs through local emulation but runs as if it's on the server
- You can install X-Windows support for Windows

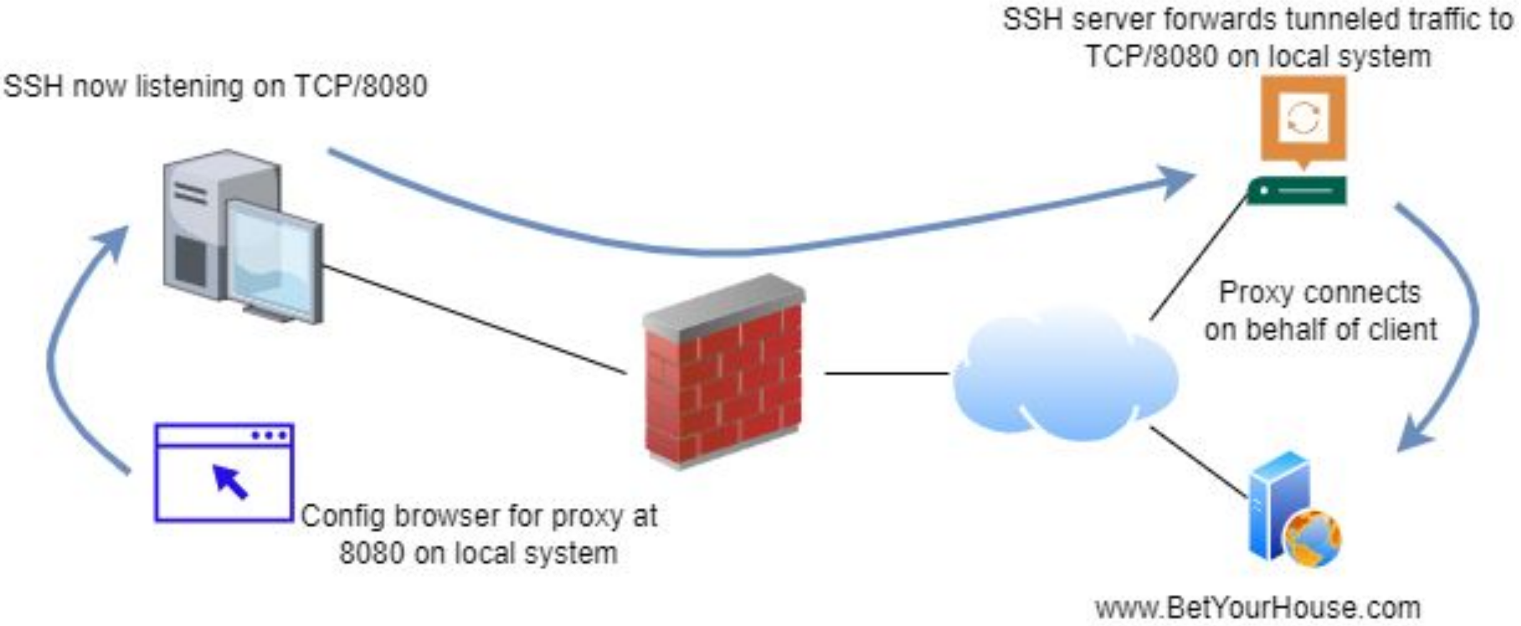
https://sourceforge.net/projects/vcxsrv/

SSH port forwarding

- Permits you to map/forward TCP ports between SSH client and server
- Access the network from the perspective of each endpoint
- Two kinds of port forwarding
  - Local port - Local listener forwarded to the server
  - Remote port - Remote listener forwarded to the client

Local port forwarding example

```
ssh -L 8080:localhost:8080 <user@server name or IP>
```



SSH now listening on TCP/8080

SSH server forwards tunneled traffic to TCP/8080 on local system

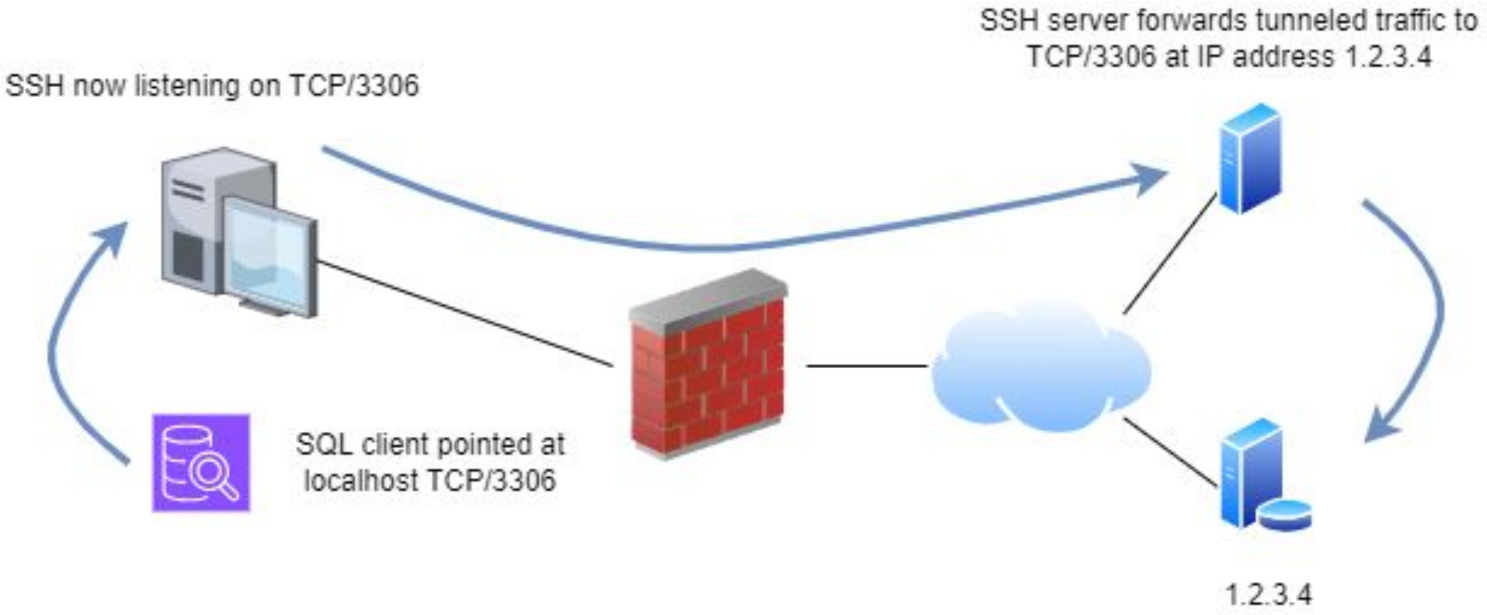
Proxy connects on behalf of client

Config browser for proxy at 8080 on local system

www.BetYourHouse.com

Local port forwarding to remote server

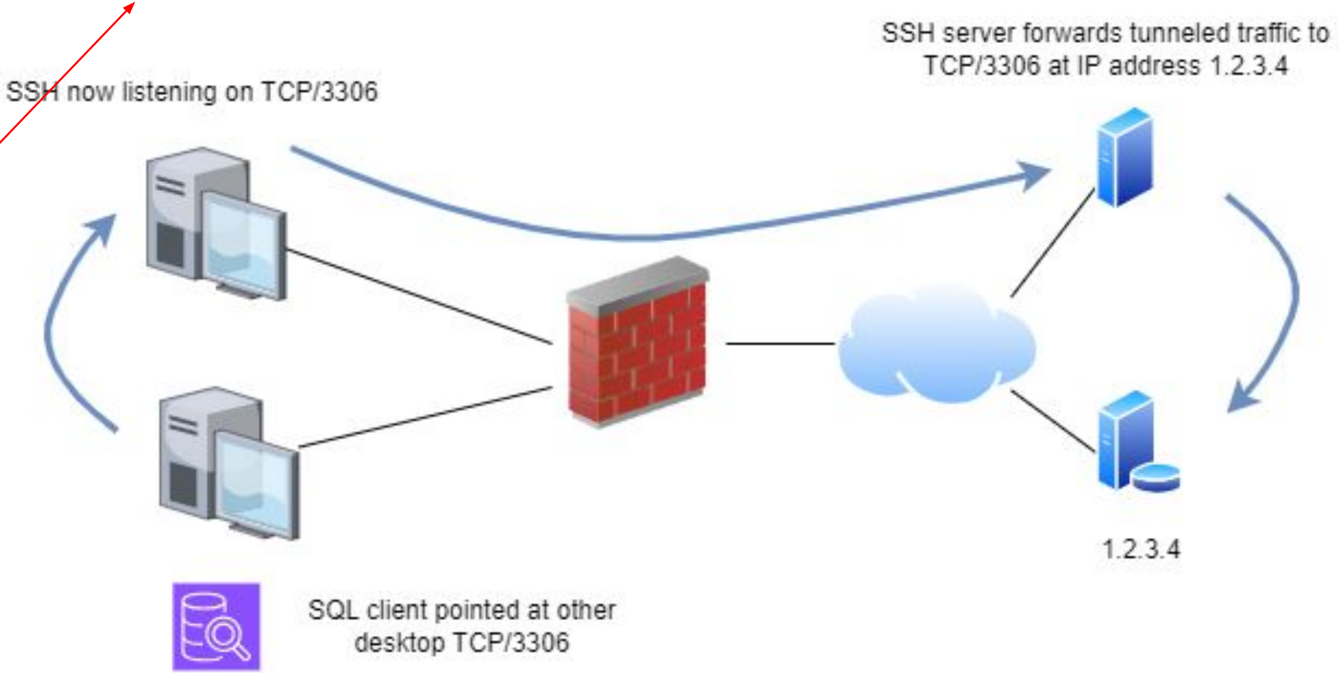
```
ssh -L 3306:1.2.3.4:3306 <user@server name or IP>
```


SSH server forwards tunneled traffic to TCP/3306 at IP address 1.2.3.4
SSH now listening on TCP/3306
SQL client pointed at localhost TCP/3306
1.2.3.4

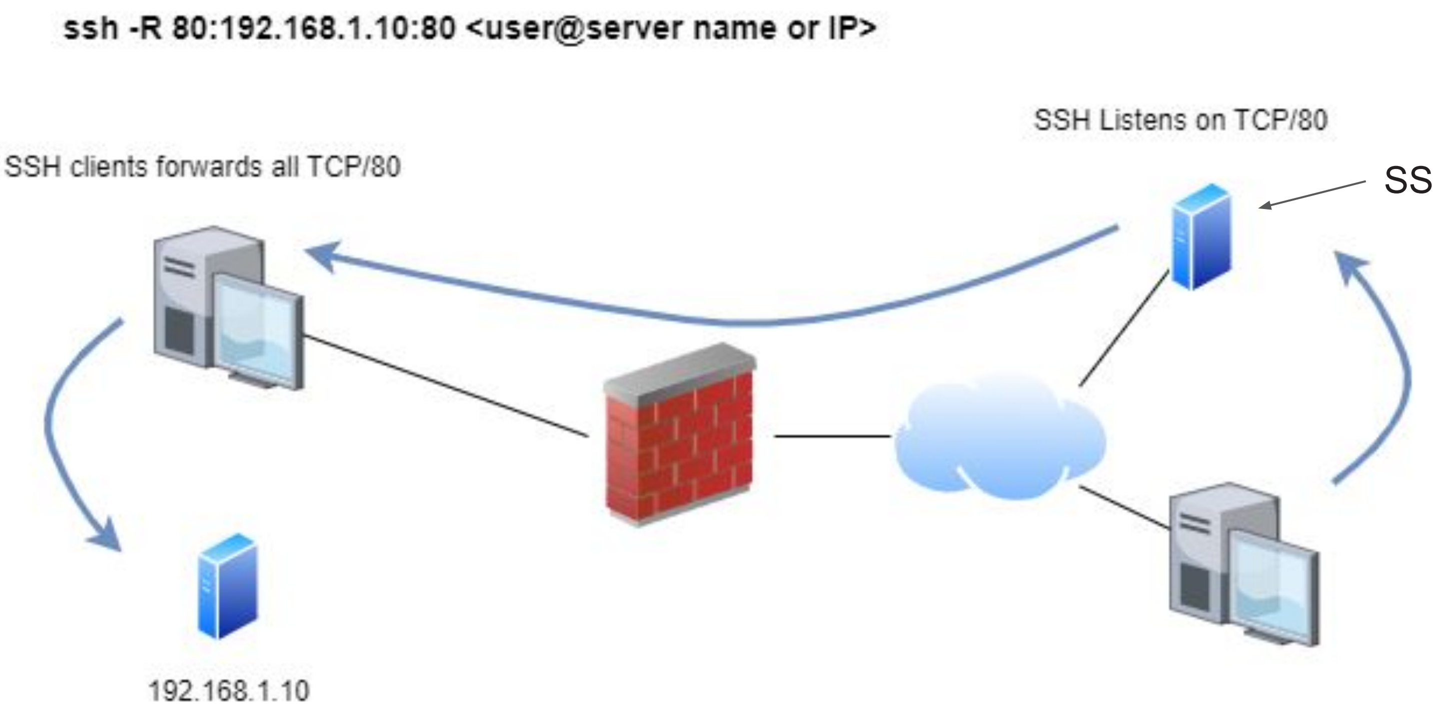
Running through local tunnel

```
ssh -L *:3306:1.2.3.4:3306 <user@server name or IP>
```

Bind to all interfaces


SSH now listening on TCP/3306
SSH server forwards tunneled traffic to TCP/3306 at IP address 1.2.3.4
1.2.3.4
SQL client pointed at other desktop TCP/3306

Remote port forwarding



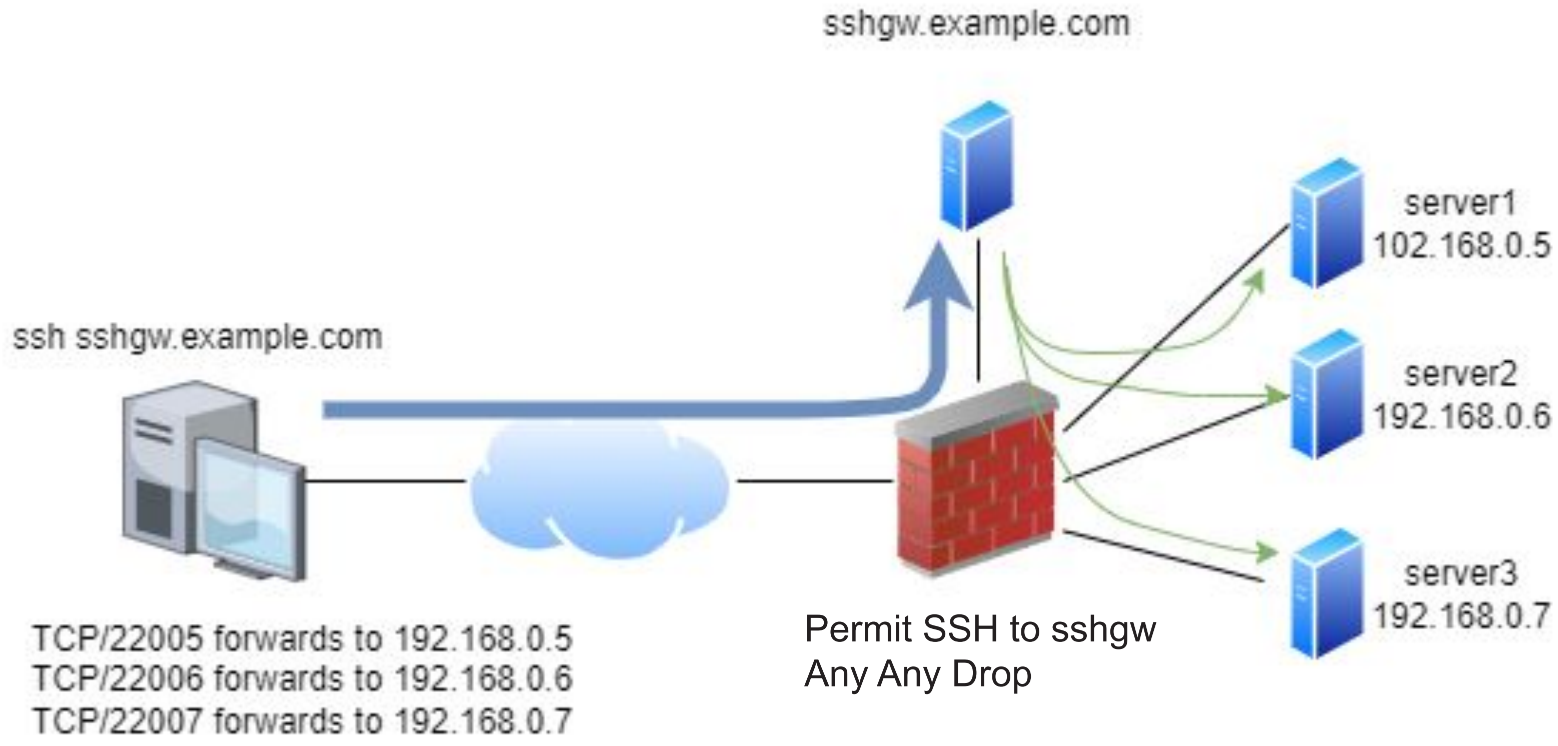
```
ssh -R 80:192.168.1.10:80 <user@server name or IP>
```

SSH server

SSH gateway with port forwarding

- SSH can expose administrative access
- Especially if you are still using passwords
- SSH gateway
  - Funnels all SSH through a single host
  - Central point of management
  - Only host exposed to the Internet
  - Opens options like one time password

SSH forwarding gateway



TCP/22005 forwards to 192.168.0.5
TCP/22006 forwards to 192.168.0.6
TCP/22007 forwards to 192.168.0.7

Permit SSH to sshgw
Any Any Drop

Sample ~./ssh/config

```
Host *
      User mylogin
      IdentityFile /home/mylogin/.ssh/id_dsa

Host sshgw.example.com
#server1
      LocalForward22005 192.168.0.5
#server2
      LocalForward22006 192.168.0.6
#server3
      LocalForward22007 192.168.0.7

Host server1
      Hostname    localhost
      Port        22005
      HostKeyAliasserver1
Host server2
      Hostname    localhost
      Port        22006
      HostKeyAliasserver2
Host server3
      Hostname    localhost
      Port        22007
      HostKeyAliasserver3
```

More info: http://www.stearns.org/doc/ssh-techniques-two.current.html

IPSec

- Designed from the ground up to be a VPN
- Host to network or network to network
  - Can support remote users
  - Can support site to site
- Protocols
  - TCP/500 - IKE negotiations
  - ESP - Protocol 50
  - AH - Protocol 51

AH or ESP, which to use?

- ESP
- All day, every day
- Authentication header
  - Provides no data privacy (no encryption)
  - Some value in areas where encryption cannot be used
  - Broken by NAT as it tries to authenticate IP header
- Most IPSec implementation leverage ESP

IPSec history

- Open standard
- Created for IPv6, adopted to IPv4
- Snowden leaks - weakened by the NSA?
- Dead peer detection issues between vendors
  - Does not always work
  - May require restarts every few days
- Ensure both ends are properly time synced
- Troubleshooting can be challenging

IPSec host to host

- Run racoon to manage IKE and generate encryption key
- Pre-shared secret for initial authentication
- Configure ifcfg for each tunnel
  - /etc/sysconfig/network-scripts/ifcfg-<uniquename>
- Can connect to network on other side if target has ip_forward=1

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/4/html/security_guide/s1-ipsec-host2host#s1-ipsec-host2host

IPSec network to network

- Similar info as host to host
- Define networks on both ends of the tunnel
- Ensure there is no overlap in address space
- ip_forward=1 on both sides
- Configure DHCP, dynamic routing, etc. per networks on both sides

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/4/html/security_guide/s1-ipsec-net2net#s1-ipsec-net2net

TLS

- Designed to secure TCP applications
  - Typically on an alternate port
  - Example: Insecure HTTP=TCP/80, secure = TCP/443
  - Vendor specific tunnel options available
- Replaces SSL
  - TLS 1.2 is currently most popular (2008)
  - TLS 1.3 is coming (2018) but has issues

TLS - App specific

- Agentless - no specific client needed
- But application specific support is needed
- Most popular applications support it
  - Web
  - Email
  - Messaging
  - VoIP
- Always good to check

Does TLS always encrypt?

- No!
- Some countries ban private use of encryption
- Still want to provide some value
- Cipher suite to:
  - Authenticate both ends of the connection
  - Authenticate against changes (but not sniffing)
  - Protect against replay attacks
- Similar to IPSec AH implementation

TLS 1.3 improvements

- Faster handshake
    - Saves 2 packets
- Removes known vulnerable cipher suites
- Faster connect for frequently accessed server
    - Zero Round Trip Time Resumption (0-RTT)
- Support for perfect forward secrecy
    - No relation between encryption keys
    - Cracking one key does not make it easier to crack others

TLS 1.3 challenges

- 0-RTT vulnerable to replay attacks
  - Poor tradeoff for speed
- Server Name Indication (SNI) can now be encrypted
  - Blind to traffic going to 3rd party proxies
  - Proxy must remain inline
    - Creates a central point of security/privacy failure
    - You probably don't want all of your bank info decrypted in transit
- Encrypting the SNI is optional

Should I use TLS 1.2 or 1.3?

- Most 1.2 issues can be mitigated
  - Remove support for poor ciphers like RC4
- Can't mitigate 1.3 issues
  - WTF were they thinking???
- Many sites sticking with TLS 1.2 for now
- Forcing 1.2 requires config control of clients
- For low security networks this may not matter

DNS over HTTPS/TLS (DoH/DoT)

- Suppose to provide additional privacy
  - Simply shifts who can collect your DNS data
  - ISP can still see where you connect
- Bad for security
  - We can no longer leverage DNS for visibility
  - Why did the user connect to that IP address?
- Feels like a power grab by browser vendors
- Malware/C2 already hiding in this channel

Disabling DoH/DoT

- Root issue is browsers ignoring DNS config
- Today this is only a problem with browsers
  - Chrome, Firefox, Edge
  - Maybe others
- DoH uses TCP/443
- DoT uses TCP/853
- Config changes need to be done on a per browser basis
  - Not just a problem on Windows

Next week on Fireside Fridays!

- Authentication, passwords & password cracking
- We'll do a walk through on password racking
    - John the Ripper
- I'll post instructions the day before the webcast
- Check the Fireside Fridays #fire-content channel for details and instructions

Wrap up

- Thank you for attending!
- Certs & video will go out by Monday
- If you have any lingering questions, the Discord channel will remain active
  - Also a good chance to socialize with others in the class
  - Have other tips and tricks? Please share with others!
- **Thank you** for sharing your time with us!