一种廉价的端口复用方案

Poor Man's RedTeaming Skill

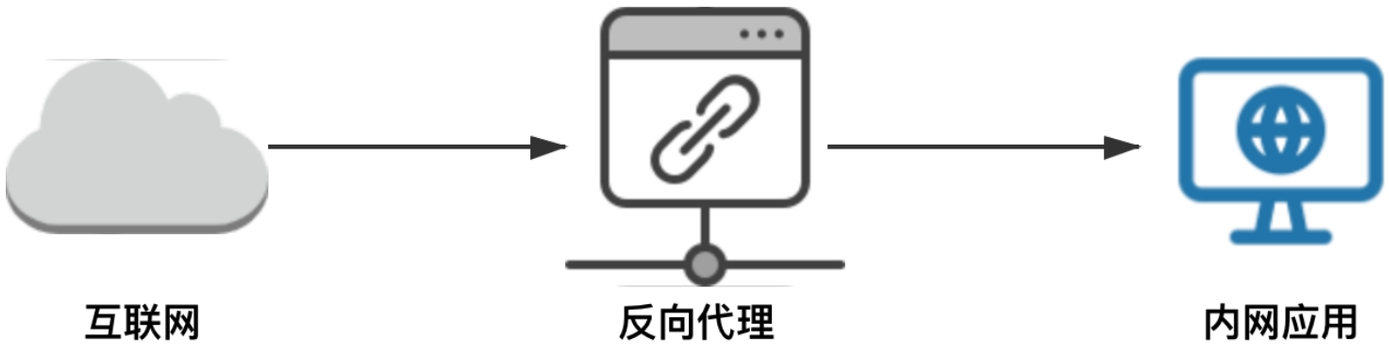
ABOUT ME

- 资深RAT玩家
- 专业后渗透测试QA
- 三流 Pen-Tester & ReadTeamer
- 不入流安全工具Coder
- 键盘艺术工作者
- DarkRay @ Pand0ra & LoopH4ck
- QAX SgLab 观星实验室
- 喜欢说点儿相声界没唱过的饶舌音乐

何谓廉价?

- 几乎没有开发成本
- 尽可能利用已有项目
- 较少配置与操作的过程
- 最重要的是不花钱

常见网络边界拓扑



设备转发类型

- 不带源地址转发
- 带源地址转发
- 反向代理

端口复用的实现原理

- 实现方法：RAW Socket
- 操作系统：几乎通用
- 优点：在Ring3层即可实现
- 缺点：开发成本高，难度大

端口复用的实现原理

- 实现方法：SO_REUSEADDR 与 SO_REUSEPORT 标志
- 操作系统：几乎通用
- 优点：在Ring3层即可实现，开发成本低
- 缺点：只在最后一个调用Bind的进程生效，并且仍然需要对网络数据包进行识别

端口复用的实现原理

- 实现方法：劫持 Socket 句柄
- 操作系统：几乎通用
- 优点：如果程序本身提供接口以供自定义代码访问其进程空间则可大大降低开发成本，如 MySQL UDF；或者利用编程语言本身设计不严谨导致的FD泄露，如PHP的某些漏洞
- 缺点：应用面窄

端口复用的实现原理

- 实现方法：利用应用软件特性
- 操作系统：几乎通用
- 优点：如Apache Mod及IIS ISAPI等，开发成本低；.NET Framework 的WCF提供的 Port Sharing 功能
- 缺点：热加载难度较高，某些特性应用面窄

端口复用的实现原理

- 实现方法：Inline Hook
- 操作系统：几乎通用
- 优点：开发成本低，绝大部分可在Ring3层实现，不同操作系统均有成熟方案，如Linux通过LD_PRELOAD劫持动态链接库或PTRACE进程注入等，Windows也有相应方案 —— 打字太多这里不写了；）
- 缺点：不同引用程序的Hook点不尽相同，绝大部分可以通过Hook Socket相关函数实现，但仍有如 Microsoft IIS6 由于使用了IOCP，故 W3SVC 进程是通过 CreateFile 来操作数据的

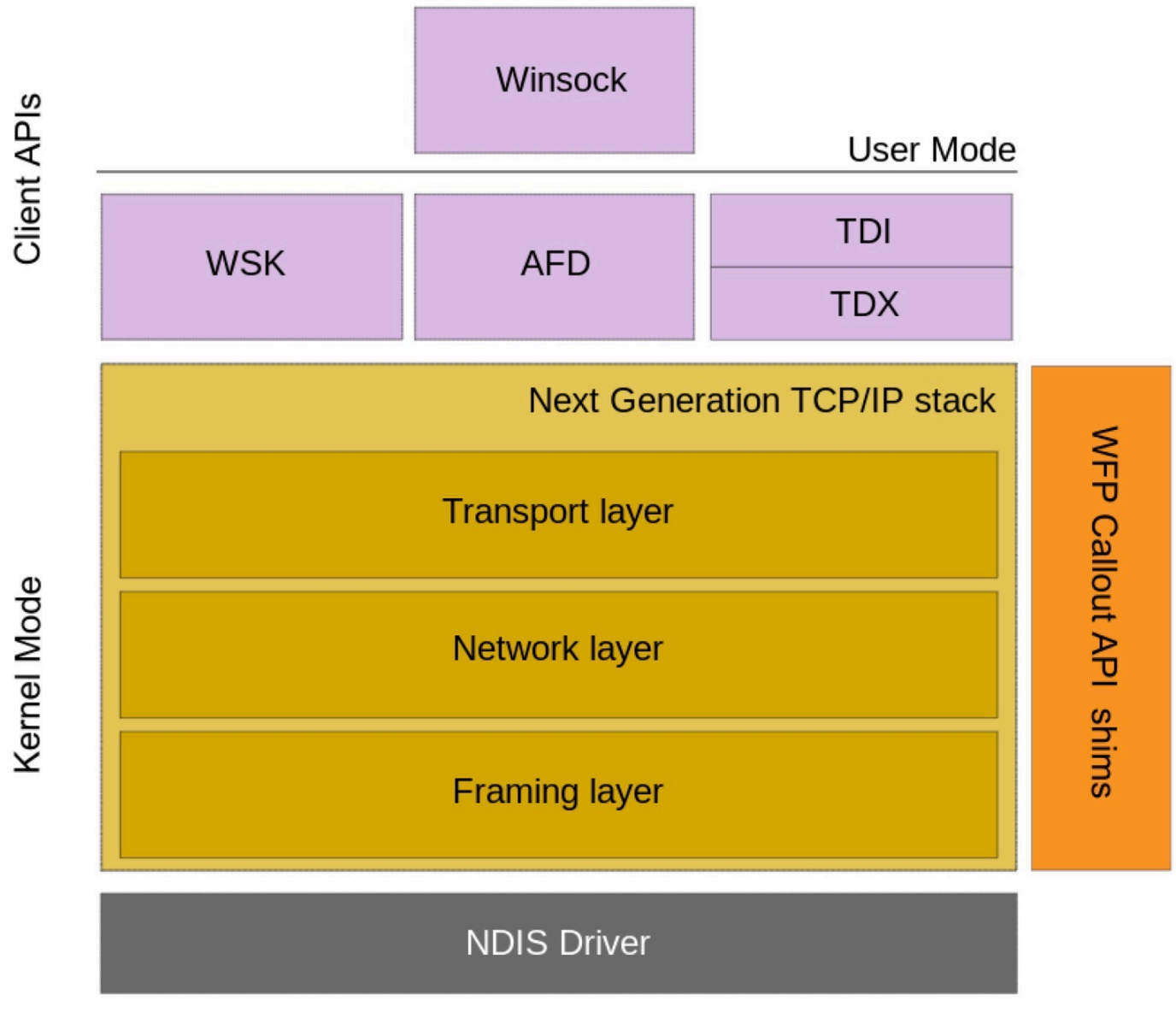
端口复用的实现原理

- 实现方法：利用系统网络协议栈提供的接口
- 操作系统：几乎通用
- 优点：如 Linux Net Filter 以及 Windows NDIS、TDI、WCF 等
- 缺点：几乎只能Ring0层实现，NT6以后Windows驱动穷人难以驾驭

端口复用的核心方法论

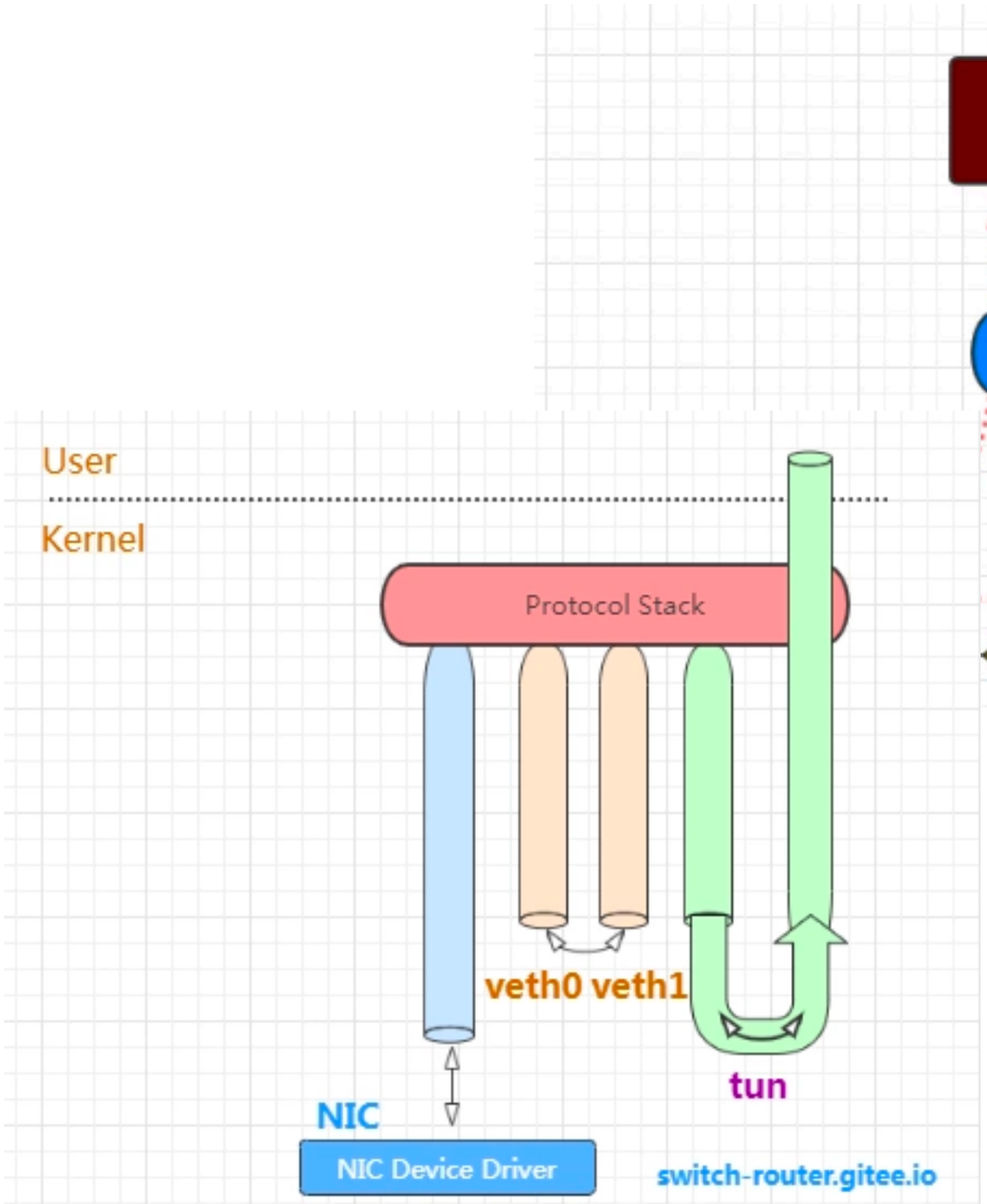
- 在恰当的时机，选择恰当的网络数据包，并同时进行转发

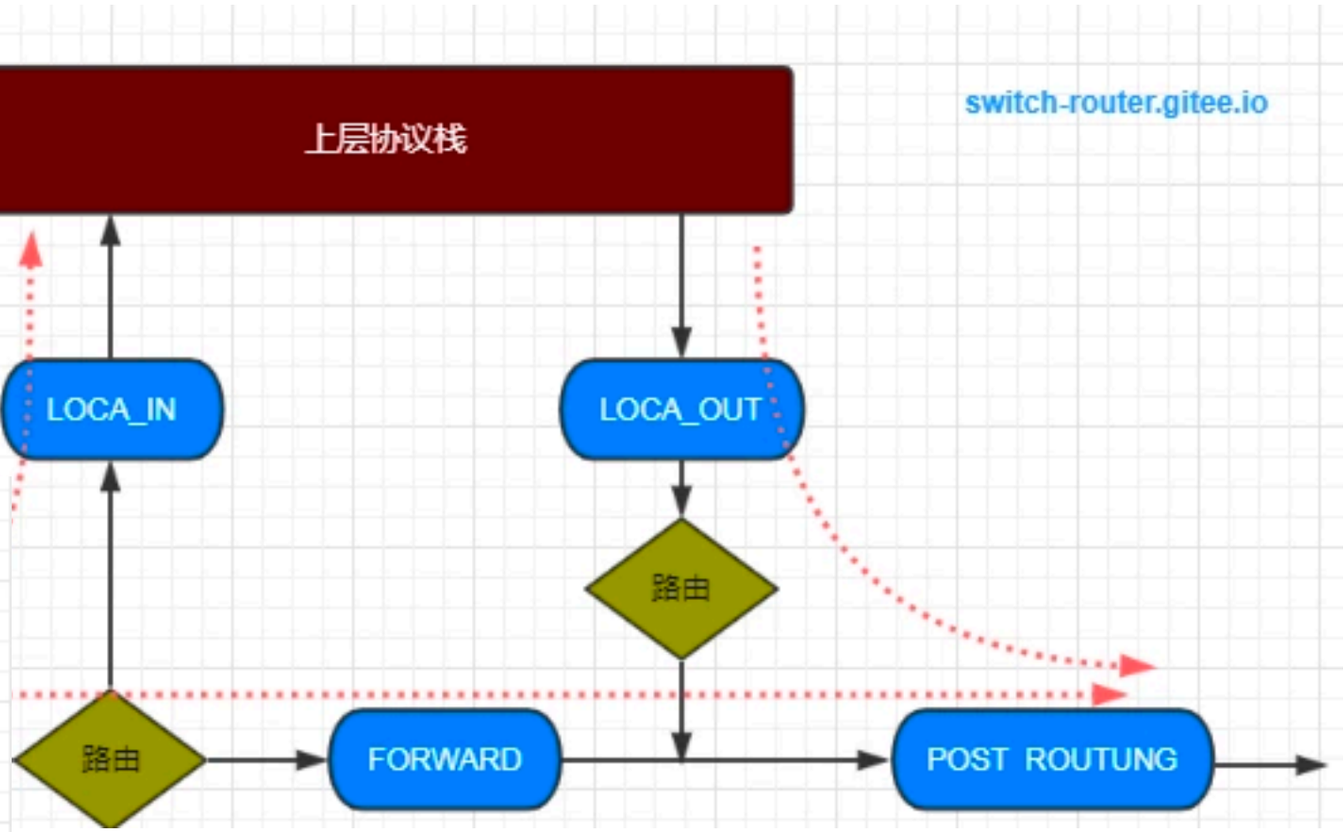
WINDOWS 网络协议栈架构



- Pic from https://zhuanlan.zhihu.com/p/91495819

LINUX 网络协议栈架构





Pic from https://segmentfault.com/a/1190000021227338

富人的方案

- Linux Iptables Extionsion
- Windows NDSI Driver https://www.ntkernel.com/windows-packet-filter/
- Windows WFP Driver https://www.reqrypt.org/windivert.html
- Windows TDI & WFP Driver http://netfiltersdk.com/

穷人的方案

- 回顾一下我们对于廉价的定义 —— 最简单的实现方式莫过于利用操作系统的机制，与现有的开源软件相结合，实现端口复用的操作

- Windows Netsh + Haproxy
- Linux Iptables + Haporxy

WINDOWS 重定向方案

- 利用 Netsh 进行端口转发 *netsh interface portproxy add v4tov4 listenport=80 connectport=51025 connectaddress=x.x.x.x*
- 由于 smb.sys 及 http.sys 均为内核驱动，故针对SMB服务和IIS服务，需要做一些小的处理，非内核驱动相关的服务则无需做额外处理
- 以SMB为例，首先我们需要通过 **sc config smb start= demand** 将 SMB 这个内核驱动设定为禁止自动运行，然后添加一张本地回环网卡，并且将跃点数修改为一个较大值，同时取消 Netbios 协议在此网卡上的注册，为了保证原SMB服务的正常运行，我们需要在计划任务中添加一个SMB的自启动 **sc start smb**，最后通过Netsh添加转发规则即可，**重启即可生效**
- Haproxy 将监听在 51025 端口进行分流

LINUX 重定向方案

- 利用 Iptables 进行端口转发 *iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 51025*

- Haproxy 将监听在 51025 端口进行分流

HAPROXY TCP/IP 三层分流

```
frontend main
        mode tcp
        bind *:9999

        tcp-request inspect-delay 3s
        #GET POS(T) PUT DEL(ETE) OPT(IONS) HEA(D) CON(NECT) TRA(CE)
        acl is_http req.payload(0,3) -m bin 474554 504f53 505554 44454c 4f5054 484541 434f4e 545241
        tcp-request content accept if is_http
        tcp-request content accept
        use_backend http if is_http
        use_backend socks5

backend socks5
        mode tcp
        timeout server 1h
        server ss 127.0.0.1:51025

backend http
        mode tcp
        server ngx 127.0.0.1:80
```

HAPROXY TCP/IP 四层分流

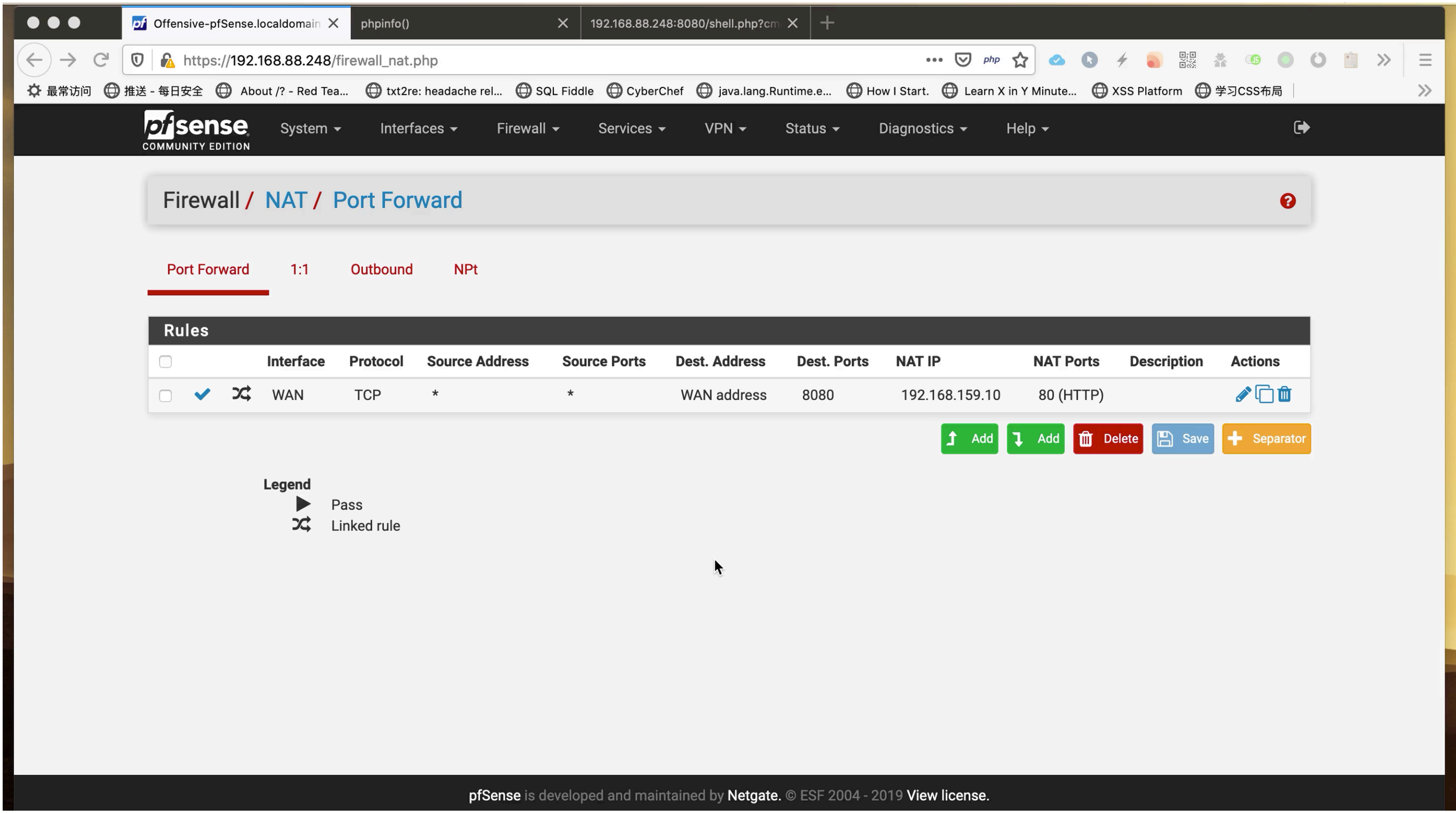
```
frontend main
        mode tcp
        bind *:9999

        option forwardfor except 127.0.0.1
        option forwardfor header X-Real-IP

        acl is-proxy-now urlp_reg(proxy) ^(http|https|socks5)$
        # http-request set-var(req.proxy) urlp(proxy) if is-proxy-now

        use_backend socks5 if is-proxy-now
        use_backend http

backend socks5
        mode tcp
        timeout server 1h
        server ss 127.0.0.1:51025

backend http
        mode tcp
        server ngx 127.0.0.1:80
```

DEMO LAB SETUP

- PfSense 模拟防火墙，IP为 192.168.199.248 不带源地址转发，映射内网 Ubuntu 的80端口到192.168.199.248的8080端口

- Ubuntu 上跑了Web应用，内网IP为192.168.159.10，为了演示方便分流后直接连接SSH

DEMO及武器化


Offensive-pfSense.localdomain
phpinfo()
192.168.88.248:8080/shell.php?cm
https://192.168.88.248/firewall_nat.php
最常访问
推送 - 每日安全
About /? - Red Tea...
txt2re: headache rel...
SQL Fiddle
CyberChef
java.lang.Runtime.e...
How I Start.
Learn X in Y Minute...
XSS Platform
学习CSS布局
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / NAT / Port Forward
Port Forward
1:1
Outbound
NPt
Rules
Interface
Protocol
Source Address
Source Ports
Dest. Address
Dest. Ports
NAT IP
NAT Ports
Description
Actions
WAN
TCP
*
*
WAN address
8080
192.168.159.10
80 (HTTP)
Add
Add
Delete
Save
Separator
Legend
Pass
Linked rule
pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.

参考与讨论

- http://squidarth.com/networking/systems/rc/2018/05/28/using-raw-sockets.html
- https://www.slideshare.net/hugolu/the-linux-networking-architecture
- https://zhuanlan.zhihu.com/p/91319628 & https://zhuanlan.zhihu.com/p/91495819
- https://x-c3ll.github.io/posts/Pivoting-MySQL-Proxy/
- http://www.91ri.org/6642.html

THE END

- 感谢实验室小伙伴 @Beee（https://www.imbeee.com/）提供的实现思路 ☺