2020年5月24日 投稿者: YSATO@DELEGATE.ORG

ipマスカレードで快適e環境

社長：それで、VPN のほうはどうなりましたかね。

基盤：VPN はやめようと思います。

社長：ご…

基盤：基本、素で IP をフォワードした場合よりも大幅に遅くなるのは目に見えていますし、意味なく複雑、リスクも増す、かつお金もかかる。

開発：素性も中身も知れたアプリケーション・プロトコルだけを、特定のターゲットに中継するのは安全ですからねぇ。

社長：つまり NAT というか、**NAPT するルータだけ社外のクラウドに置こう**ということですか。なんか、出発点に戻りましたね。

開発：元々公海をやってきたパケットを公海を通って転送するだけですので、セキュリティ上のリスクは増しませんね。

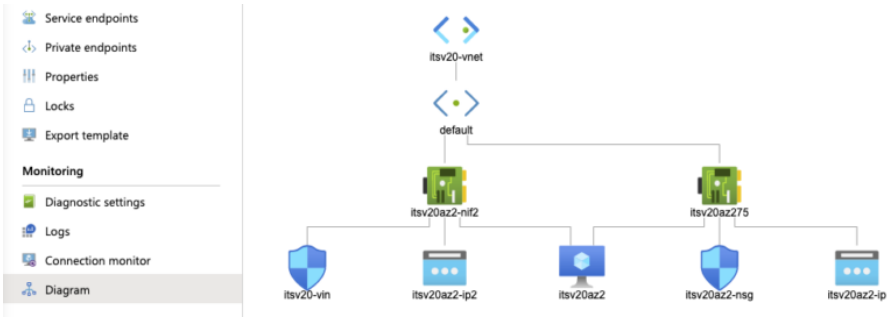
社長：どうもそういうサービス、レンタルクラウドルータみたいなのが見当たらないので、何か技術的に困難な問題があるのかと思っていたのですが。

営業：需要が少ないからじゃ無いですかね。クラウド業者の儲けにもならなそう。

基盤：とりあえず、Azure で2つ IP を買ってあったので、やってみました。使った道具は Linux の ip route と iptables。結果的には、いたってカンタンでした。

社長：iptables、懐かしス。

基盤：ただともかく昔にちょこっと使ったきりなので、使い方を全く覚えていなくて、苦労しました。問題はまず、マルチホームでのルーティングの問題です。うちの Azure 上の仮想ネットはこうなってるわけです。VMをもう一つ買うのをためらったので、一つに2枚挿しにしました。



社長：マルチホーム、超懐かしス。行きと帰りが違う道になっちゃって迷子になる問題ですね。

基盤：それです。2つのネットワークインタフェースからやって来たTCPの接続に、それぞれ元来た道で帰ってもらうというあれです。TCPの場合、帰りのパケットのソースは自動的についてますから、IPのソースルティングだけでできるはずです。実際、答えはこうでした。

```
#  ip route add from X.X.X.X oif ethX
```

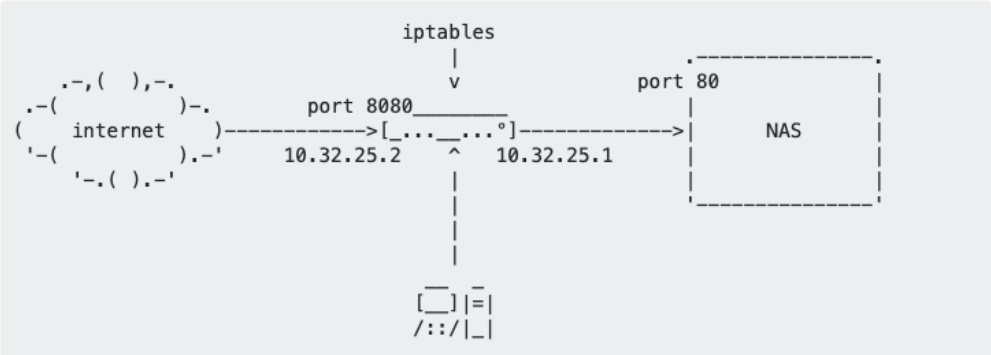
社長：そうですか…　私がやってたころはまだ BSD が元気で、あちらはあちらで流儀が違ったよね。

開発：当時は BSD のがスッキリしてたような記憶もありますけどね。トランスペアレントプロキシとかやるのに。

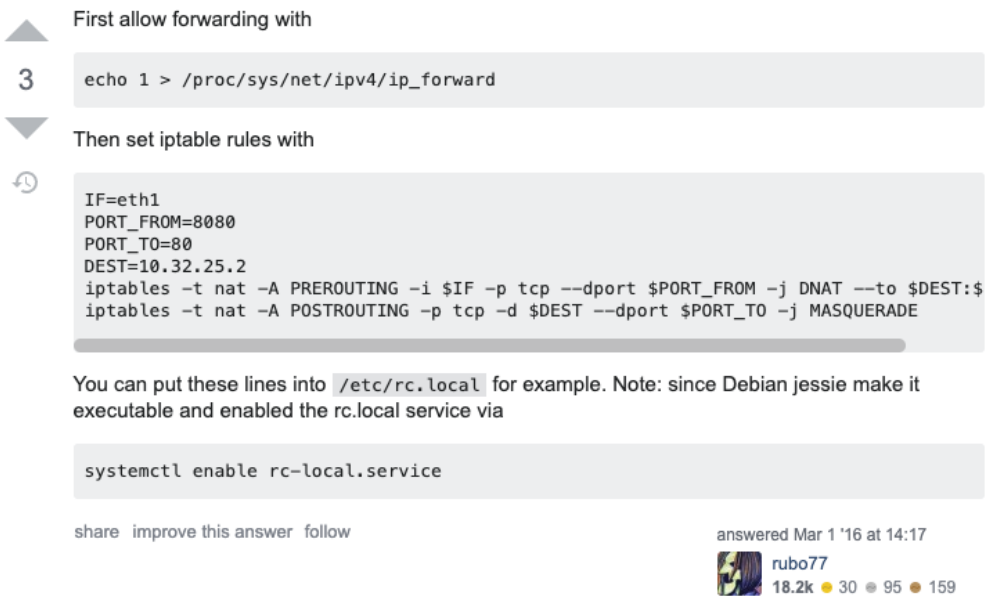
基盤：あとは、IP のフォワーディングなのですが、これは iptables でやりました。インタエース XX に来たのを IP アドレス YY に丸投げするのは、こうなります。

```
# iptables -t nat -A PREROUTING -i XX –to YY -j DNAT
# iptables -t nat -A POSTROUTING -j MASQUARADE
```

基盤：ポート番号を変えたり、実際にフォワーディングを有効にしたりするのは、もう少しだけやらないといけないことはあります。Stackexchange で見つけた、そのものスバリの具体例と完璧な解答がこれです。



質問（要件）



First allow forwarding with

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Then set iptable rules with

```
IF=eth1
PORT_FROM=8080
PORT_TO=80
DEST=10.32.25.2
iptables -t nat -A PREROUTING -i $IF -p tcp --dport $PORT_FROM -j DNAT --to $DEST:$
iptables -t nat -A POSTROUTING -p tcp -d $DEST --dport $PORT_TO -j MASQUERADE
```

You can put these lines into `/etc/rc.local` for example. Note: since Debian jessie make it executable and enabled the rc.local service via

```
systemctl enable rc-local.service
```

share improve this answer follow

answered Mar 1 '16 at 14:17
rubo77
18.2k 30 95 159

回答（ソリューション）

▶ Linux での IPマスカレードの設定方法

IPTables – Port to another ip & port (from the inside)
https://unix.stackexchange.com/questions/76300/iptables-port-to-another-ip-port-from-the-inside

基盤：これの設定って一瞬で終了なのに、うちのおまけルータ、設定して変えるのに90秒かかるんですが、一体全体何やってるんでしょう？

開発：FPGA構成を生成してしてFlashに書いているとか？

社長：それにしてもこういう基盤系の人たちって、徹頭徹尾CLIだね。ウェブでカンタンインタフェースをつけてやれば楽々設定なのに。

開発：素人には教えたく無い秘伝の技みたいな。

基盤：作っておきます。CGIで十分ですよね（笑）

開発：設定用のHTTPサーバでは、公開鍵を使ったクライアント認証があったほうが良いですね。

営業：それ、売れませんかね？

社長：需要が少なくて、儲けにもならなそうですが。

社長：てか、iptables を双方向にしたら、分散プライベートネットできるよね。ルータなんだし。

開発：リアルプライベーットネットですね。RPNというか。

社長：隠さないといけないプライバシーも無けりゃ無問題かな。

開発：まあ、隠したいデータはトランスポート層でもアプリケーション層でも暗号化されてますしね。要はHTTPだけ通すネットワークみたいない。

社長：で、それならHTTPプロキシ、つまりアプリケーション層のルータだけでできたネットワークでいいんじゃね？ってのが当時の私の考えでしたね。SSHだって必要なの？SSLトンネルでいいんじゃね？とか。その考えは今も変わらないけど。まあ、あとはソーシャルエンジニアリング対策ってやつかなぁ…

開発：ただ、いずれ世の中アプリケーションプロトコルはHTTPSだけになるって予感は当たりませんでしたね。

社長：いやいや、この先どうなるかわからんよ。HTTP の最大の問題は効率だと思うんだけど、HTTP2でのパイプラインとか、プロトコルの等価バイナリ化で、かなりイケるんじゃないかと思うんだけどね。

—

2020-0523 SatoxITS

ipマスカレードで快適e環境---株式会社-ITS-more