サーバーでパケットルーティングを行いたい (openvpn)

【設定】
-通常-
sysctl net.ipv4.ipforward=1

-特殊- (柔軟な設定は出来ない？ 未検証)
sysctl net.ipv4.conf.*interfacename* .forwarding=1

サーバーでルーティングと言えば、Destination Routing を、真っ先に想像します。
routeコマンドや、ip route add コマンドです。
このコマンドは、自身のサーバーがDefaultGWではなく、他のルーターを介して別セグメント(NW)へ通信したい場合に設定するものであり、
・自身のサーバーが、別セグメントにあるサーバーと通信させたい
・別セグメントにあるサーバーが自身のサーバーと通信させたい(帰りのパケット)
の際に使用します。つまり、起点は自身のサーバーです。

ところが起点とならない場合、つまり中継サーバー的な位置づけの場合です。
クライアントA[192.168.0.100/24] -> [192.168.0.1/24] 中継サーバーX [10.0.0.1/24] ->
目的のサーバー[10.0.0.50/24]
※ 所謂、ルーターと同様なふるまいを中継サーバーXにする必要があります。

単純にパケットルーティングやACLを行いたいのであれば、FWやルーターに置き換えれば良いのですが、
中継サーバーX上で行いたい場合が発生する場合があります。
私の場合は、OpenVPNを実装する際に必要となりました。

冒頭で記述したコマンドは、端的に言うと、ネットワークI/F間のパケットをフォワードするかどうかの設定です。
OpenVPN(tunデバイス)でいえば、tun0とeth0間をフォワードします。
※ OpenVPN(tapデバイス)の場合で、物理NICにブリッジすれば、ルーターやFWでルーティングも可能だと思いますが、
　OpenVPNの機能を使って、証明書でのACLやユーザー毎のVPN-IPを変更するなどやりたかったのでtunデバイスとした。
　tapデバイスでも出来るかもしれないが、ネットの情報ではtunデバイスを使った手法の情報が多かった。
　と、いうかtapデバイスでは調べたい情報は探し出せなかっただけだが。

ただ「net.ipv4.ipforward=1」の利用には、個人的に少々使いたくない感がある。
真面目にACLしないとセキュリティ的に穴になる場合があるから。

Linuxディストリビューションの中には、デフォルトで「net.ipv4.ipforward=1(有効)」となっている場合があるらしいが、
私がメインで利用していたRedhat(CentOS)系は、デフォルトは「net.ipv4.ipforward=0 (無効)」です。
特に最近のサーバー向けOSは、デフォルト状態で最低限のセキュリティは確保されています。

昔のOSはセキュリティ概念が低かったのか、(使わないのに)最初から色々なソフトが起動していたり、管理用デフォルトパスワードも甘々だったりとしていたので「サーバーの要塞化」が必須でした。

OpenVpnを導入するにあたり、最初は既存サーバーにインストールしようと思いましたが、
「net.ipv4.ipforward=1」を設定しないといけないと分かり、lo, eth0, eth1 が既に存在しているので、
eth0 - tun0 のパケットフォワードは行いたいが、eth1 - tun0は行いたくない。
新規サーバーにしても、iptables/nftablesは設定するが、既存サーバーでiptables/nftablesで実は通信止まってました〜。
なんて事は、なりたくないな！と。
すぐに影響が出て気づけば、即修正すれば良いんだけど、かなり後になって「気づきました。止まってました！」は避けたい。
いや、単にすべての通信テストをやるのが面倒なだけです。はい。

添付ファイル::

一意的なソリューション ID: #1011
製作者: n/a
最終更新: 2022-07-03 12:32