



Vyatta技術詳細

株式会社まほろば工房 谷津 航

目次

- ▶ Vyattaとは
- ▶ 使用例
- ▶ その他
- ▶ まとめ





Vyattaとは

Linuxをルータっぽく使ったことありますか？

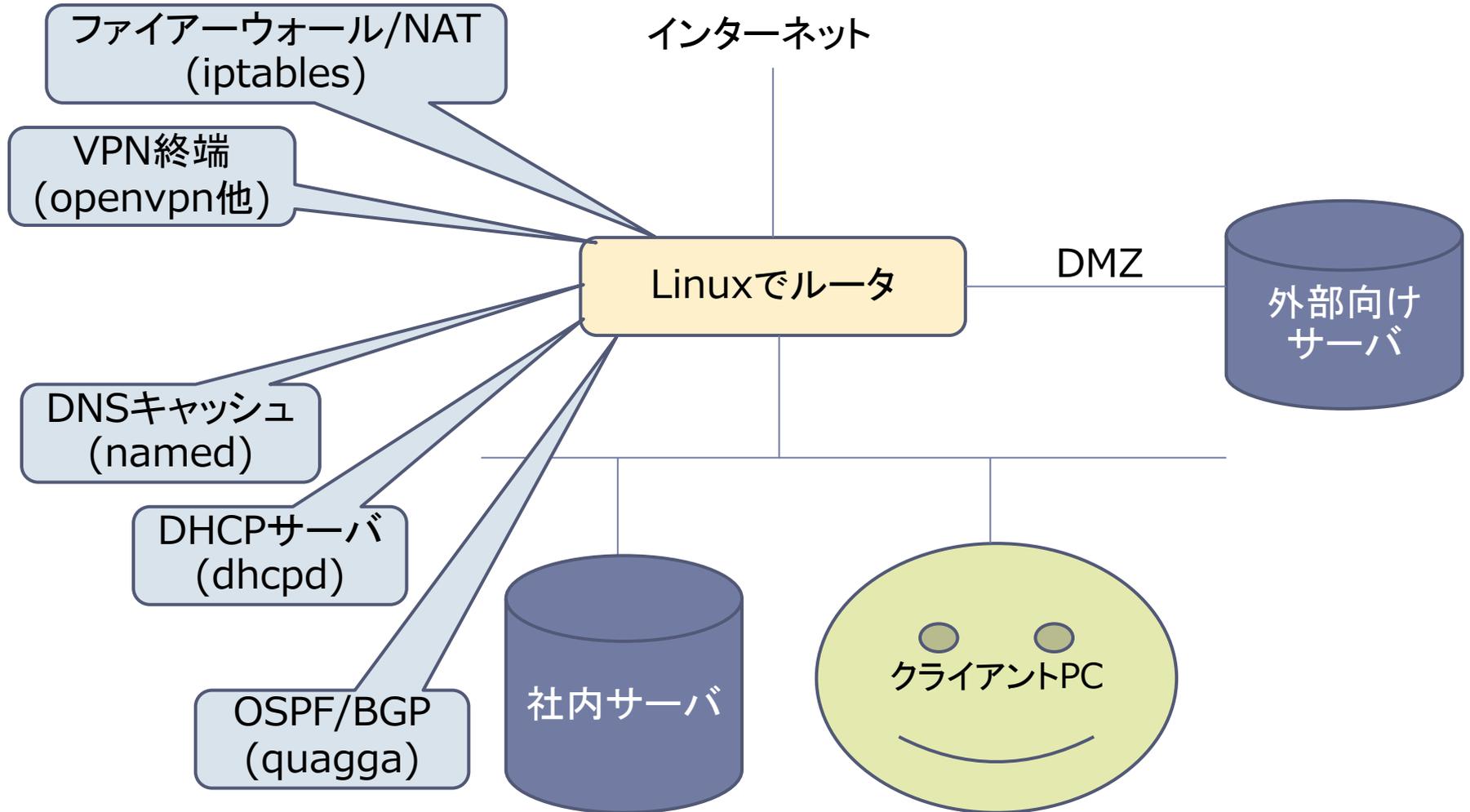
- ▶ ルータ製品を使いたかったけど、ルータ製品で頑張れない場合
 - ▶ 予算と機能のかねあい

サーバマシンに、ルータとして頑張ってもらおう。

- ▶ たぶん、こういう機能を使ったと思います。
 - ▶ iptables
 - ▶ openvpn
 - ▶ tcpdump
 - ▶ named (DNSキャッシュ)
 - ▶ dhcpd
 - ▶ quagga
 - ▶ vrrpd/keepalived
 - ▶ etc...

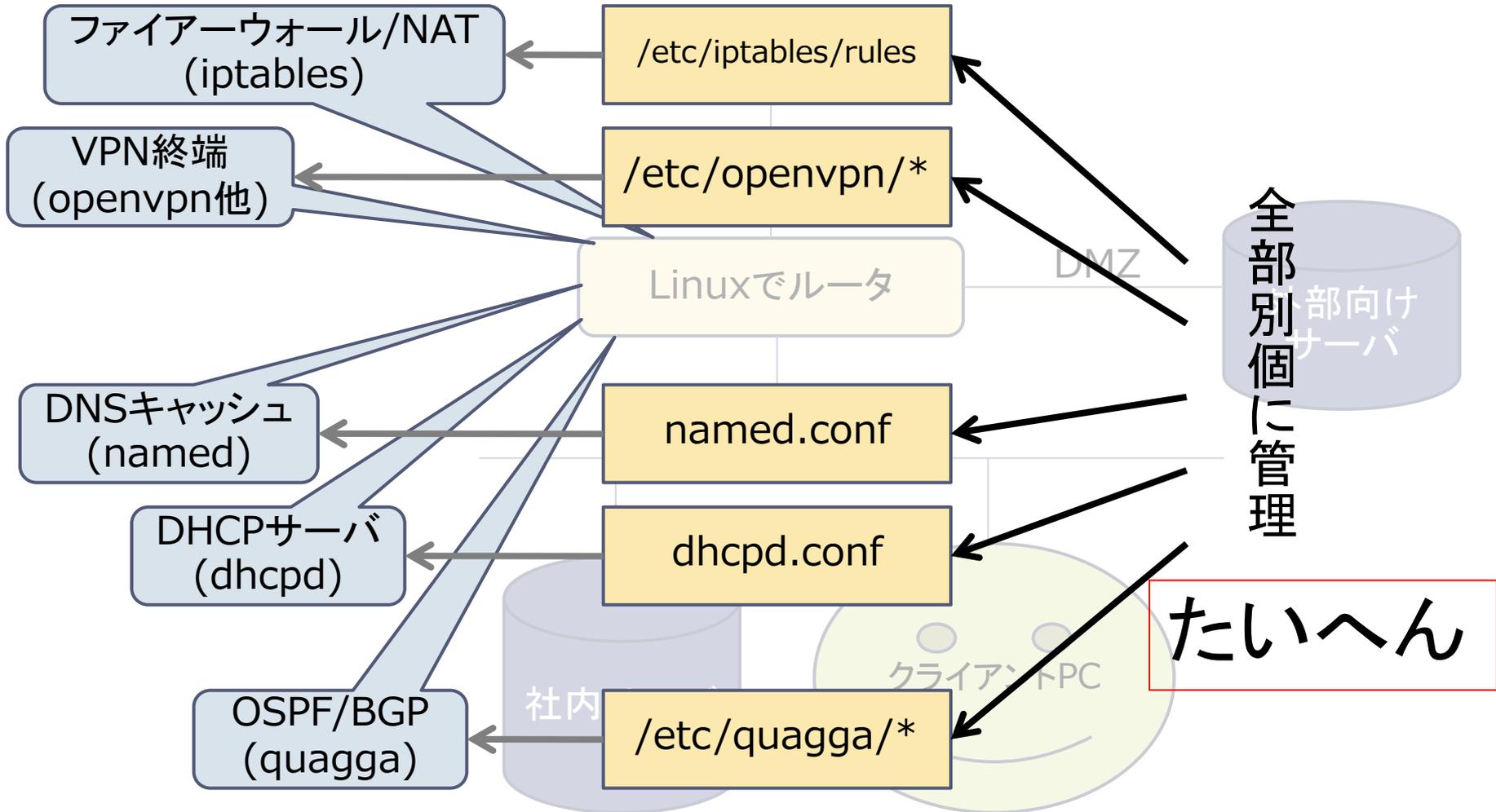


こんなかんじ？

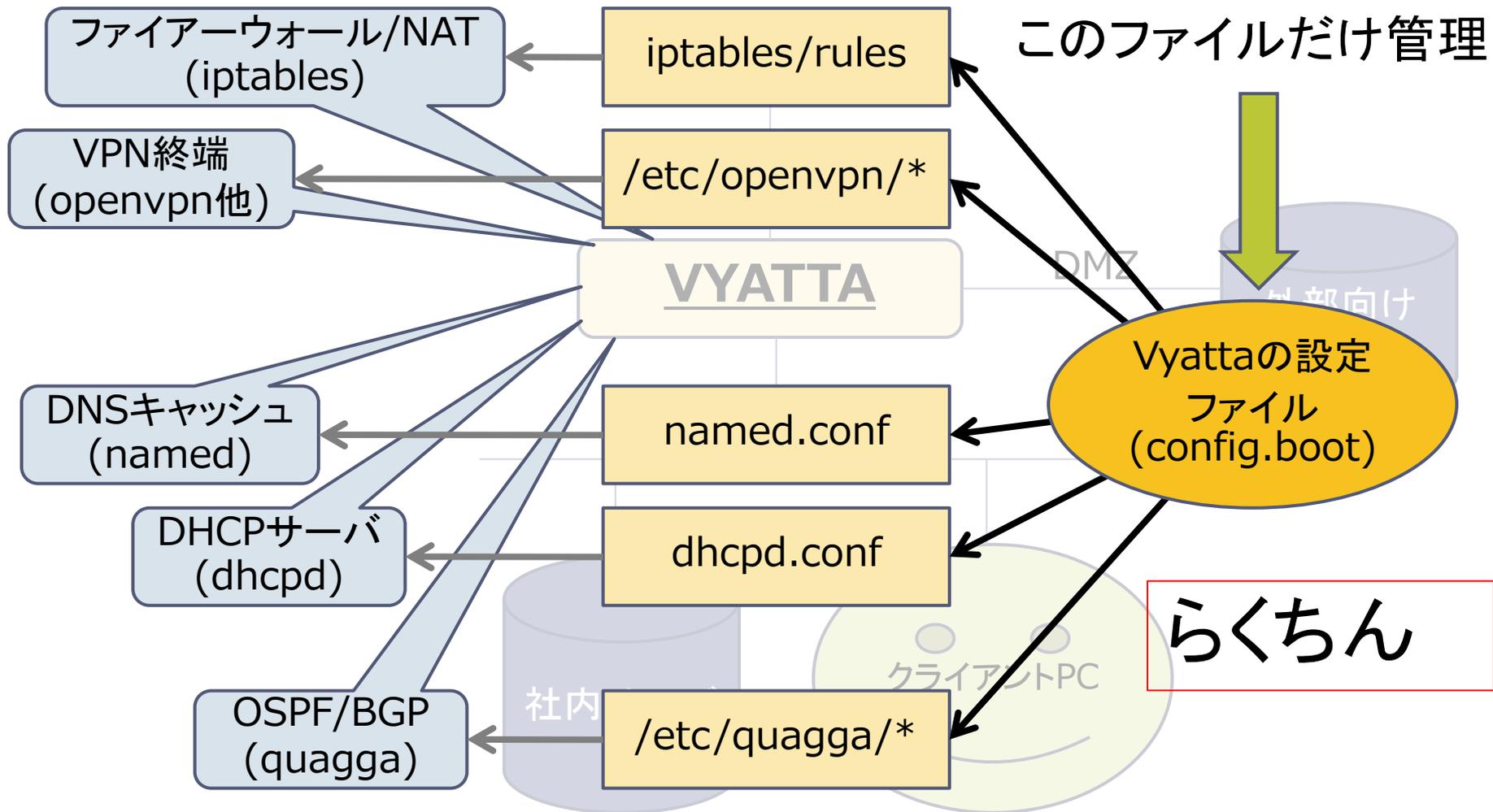


こんなかんじ？

(debianの場合のファイル名)



Vyattaの場合こんなかんじ



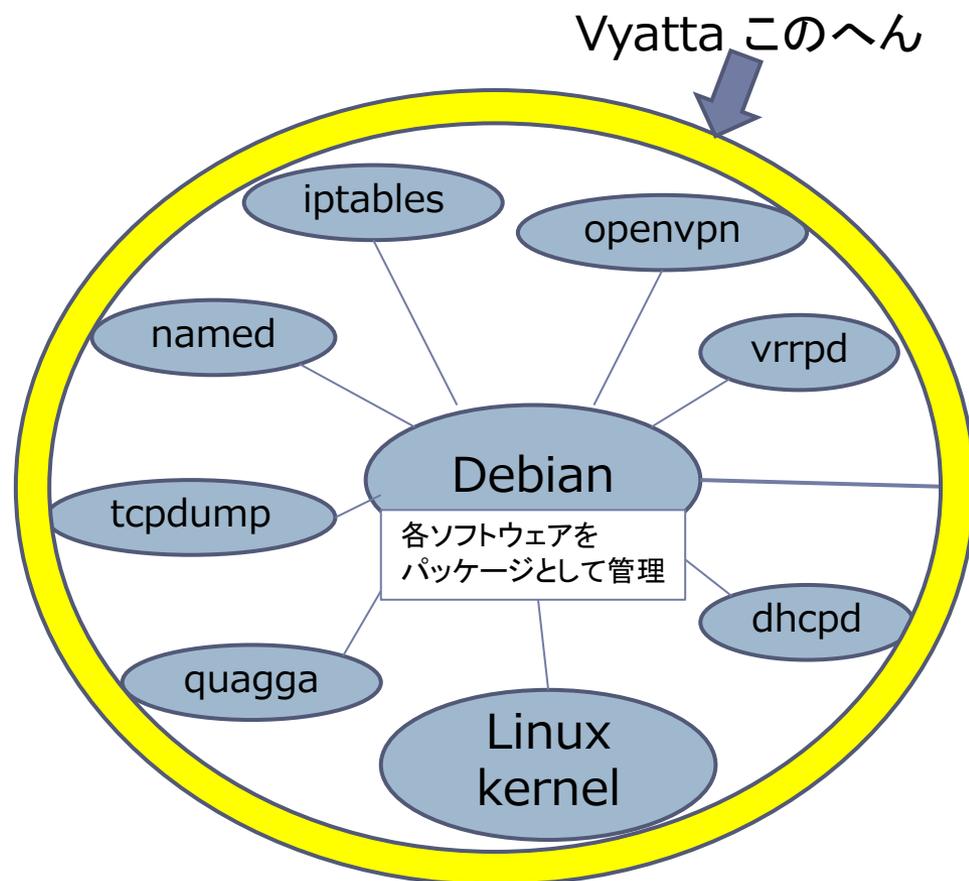
Vyattaとは

▶ ソフトウェアルータ

- ▶ Vyatta自身がルータ機能の全てを提供してはなりません。
- ▶ いろいろなOSSを、Debianパッケージとして搭載することで、各機能を実現しています。
 - ▶ 一部のOSSはVyattaカスタム

▶ Vyattaの役割

- ▶ UI(設定管理/状態表示)
- ▶ 各ソフトウェアの設定ファイルをとりまとめてくれる。
- ▶ 各ソフトウェアのバージョン管理もしている。(APTで)
 - APTを使って独自にソフトウェア追加/更新できちゃう。

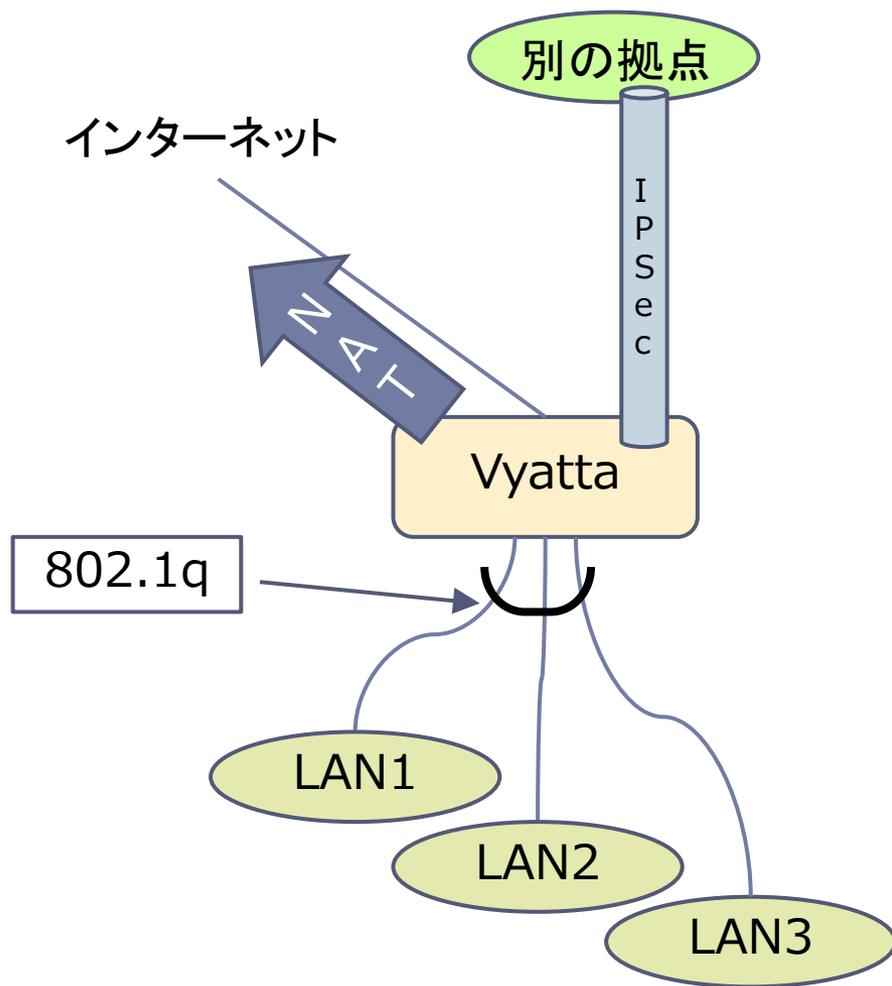


Vyatta使用例

使用例1

▶ 拠点/オフィスに設置の ルータ

- ▶ IPSec
- ▶ NAT
- ▶ VLAN



使用例1

▶ vyatta設定(IPSec部分)

```
vpn {  
  ipsec {  
    (snip)  
    ipsec-interfaces {  
      interface eth1  
    }  
    site-to-site {  
      peer 10.0.100.1 {  
        authentication {  
          mode pre-shared-secret  
          pre-shared-secret vyatta  
        }  
        ike-group ike1  
        local-ip 10.0.100.2  
        tunnel 10 {  
          allow-nat-networks disable  
          esp-group esp1  
        }  
      }  
    }  
  }  
}
```

▶ /etc/ipsec.conf

```
# generated by  
/opt/vyatta/sbin/vpn-config.pl  
(snip)  
conn peer-10.0.100.1-tunnel-10  
  left=10.0.100.2  
  right=10.0.100.1  
  ike=aes128-sha1!  
  ikelifetime=28800s  
  keyingtries=%forever  
  esp=aes128-sha1!  
  keylife=3600s  
  rekeymargin=540s  
  type=tunnel  
  pfs=yes  
  compress=no  
  authby=secret  
  auto=start  
#conn peer-10.0.100.1-tunnel-10
```

使用例1

▶ vyatta設定(NAT)

```
service {  
  nat {  
    rule 100 {  
      outbound-interface eth1  
      type masquerade  
    }  
  }  
}  
(snip)  
}
```

commitすると

(vyatta独自の保存形式)

iptablesを実行

```
# /sbin/iptables -t nat -A POSTROUTING  
-s 192.168.1.0/24 -j MASQUERADE
```

▶ vyatta設定(VLAN)

```
interfaces {  
  ethernet eth0 {  
(snip)  
    vif 1000 {  
      address 10.0.0.2/24  
    }  
  }  
}
```

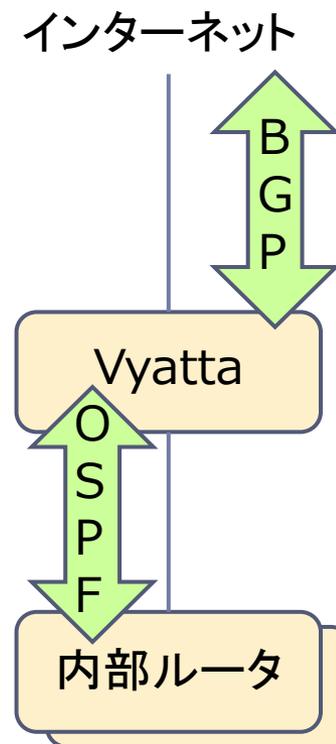
(vyatta独自の保存形式)

vconfigを実行

```
# /sbin/vconfig add eth0 1000
```

使用例2

- ▶ ISP網内のAS境界ルータ
 - ▶ OSPF
 - ▶ BGP



使用例2

▶ vyatta設定(BGP&OSPF)

```
protocols {  
  bgp 65001 {  
    neighbor 10.1.1.2 {  
      remote-as 65004  
      soft-reconfiguration {  
        inbound  
      }  
    }  
  }  
  parameters {  
    log-neighbor-changes  
  }  
}  
ospf {  
  area 0.0.0.0 {  
    network 10.1.0.0/16  
  }  
}
```

commitすると

(vyatta独自の保存形式)

vtysh実行

```
/usr/bin/vtysh -c configure terminal ¥  
-c router bgp 65001 ¥  
-c neighbor 10.1.1.2 remote-as 65004 ¥  
-c neighbor 10.1.1.2 soft-reconfiguration inbound ¥  
-c bgp log-neighbor-changes
```

```
/usr/bin/vtysh -c configure terminal ¥  
-c router ospf ¥  
-c network 10.1.0.0/16 area 0.0.0.0
```

その他の使用例(SNMP)

▶ vyatta設定(SNMP)

```
service {
  snmp {
    community vyatta {
      authorization ro
      network 192.168.0.0/24
    }
    contact someone@example.jp
    description VC6.1
    location somewhere
    trap-target 192.168.0.4 {
      community vyatta
      port 162
    }
  }
}
(snip)
}
```

▶ /etc/snmp/snmpd.conf

```
# autogenerated by vyatta-snmp.pl
(snip)
rocommunity vyatta 192.168.0.0/24
syscontact "someone@example.jp"
sysdescr "VC6.1"
syslocation "somewhere"
(snip)
trap2sink 192.168.0.4:162 vyatta
```





その他

保守性

- ▶ 故障時の筐体交換
 - ▶ 交換用の機器でvyattaを起動する。
 - ▶ ログインする。
 - ▶ 事前にバックアップしておいたvyatta設定ファイル(config.boot)を、交換用の機器の /opt/vyatta/etc/config/ に置く。
 - ▶ scpなど
 - ▶ load config.boot コマンドを実行する。
- ▶ バージョンアップ
 - ▶ ログインする。
 - ▶ サービスを停止させる。
 - ▶ sudo full-upgrade -k コマンドを実行する。
 - ▶ (再起動される)
 - ▶ ログインする。
 - ▶ サービスを再開する。

アプライアンス機みたいな使用感



インストール

- ▶ Live CDで起動して、
- ▶ install-systemコマンドを実行したら、
- ▶ 7つの質問に答えて、
- ▶ ログインパスワードを入れて、
- ▶ reboot。

これだけ

7つの質問:

Would you like to continue? (Yes/No) [Yes]: (**ENTER**)

Partition (Auto/Union/Parted/Skip) [Auto]: (**ENTER**)

Install the image on? [sda]: (**ENTER**)

Continue? (Yes/No) [No]: **Yes**

How big of a root partition should I create? (1000MB - 8590MB) [8590]MB: (**ENTER**)

Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]: (**ENTER**)

Which drive should GRUB modify the boot partition on? [sda]: (**ENTER**)



まとめ

Vyattaとは - まとめ

▶ 実体は、

- ▶ Debianをベースにして、
- ▶ OSSやVyatta社独自のソフトウェアを追加して、 ←
- ▶ さらに独自のUI(CLI、GUI、、、)を追加した、 ←
- ▶ ソフトウェアルータ

Debianパッケージの形式で追加

▶ 本質は、

IA機を、ルータのアプライアンス機に変えるおまじない





まほろば工房

<http://www.ate-mahoroba.jp/>