VyOS(ヴィワイオーエス)の次期バージョンを試してみた +EdgeOSについて調べてみた。

– ENOG28 Meeting –

2014/9/5 (株)創風システム　外山　文規

今日のおはなし

- VyOSについて簡単に紹介
- VyOSの次期バージョンである1.1(Helium)について
- VyOS 1.1でL2TPv3を試してみた
- EdgeOSについて

VyOS（ヴィワイオーエス）について

VyOSってなに？

- Vyatta Core 6.6からFork
- 1.0.0が2013/12/22にリリース
- 最新安定板は1.0.4（Hydrogen）

詳しくは、ニフティ(株)の日下部さんの資料をご参考ください。
参考: http://www.janog.gr.jp/meeting/janog34/program/lt_vyos.html
http://www.slideshare.net/higebu/20140727-vyos-users-meeting-japan-1

Vyatta Coreは？

2013年開発停止！

※Vyattaの有償版（Vyatta SE）は、
vRouter 5400/5600として継続している

VyOSの登場

Vyatta Coreとの互換性は？

現時点ではVyatta CoreのJunosライクなコマンドと基本的な設定方法は変わっていなんで、Vyatta Coreの知識はほぼ通用する。

Vyatta Coreを使い続けていいの？

先ほどの通り既に開発は停止
strongSwan等のセキュリティFIXは
されていない状態

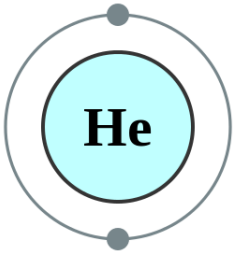
引越し先候補:

サポートやvPlaneが必要なあなた　　－＞ vRouter 5400/5600
オープンでVC相当の機能でよいあなた －＞ VyOS

VyOSの次期バージョンについて

次期バージョン1.1(Helium)

1.0(Hydrogen)から1.1(Helium)へ



2014/8/7に1.1 Beta版を公開
2014年夏?にリリース予定

Beta版入手先とインストール手順

1. ISOの入手
   http://dev.packages.vyos.net/iso/preview/1.1.0-beta1/
   から自分の環境にあったイメージをダウンロード
   ※仮想環境で動かす場合は、 amd64またはi586-virtを使用すること

2. ISOイメージ(または、CDに焼いて)からブート
3. インストールコマンドを実行

login: vyos / password: vyos でログイン後
$ install image
を実行

次期バージョン1.1(Helium)

Kernelの更新と幾つかの機能追加とバグ修正がありました。

・kernel 3.13（iproute2も合わせて）
・802.3ad QinQ VLAN stacking
・Unmanaged L2TPv3
・Event handler
・IGMP proxy (pulled from EdgeOS).
・Dummy interfaces (same functionality to multiple loopbacks).
・IPsecがIKEv2、hash256、SHA2をサポートなど

etc...

参考: http://vyos.net/wiki/1.1.0/release_notes

次期バージョン1.1(Helium)

Kernelの更新と幾つかの機能追加とバグ修正がありました。

・kernel 3.13（iproute2も合わせて）
・802.3ad QinQ VLAN stacking
・Unmanaged L2TPv3 ← これ
・Event handler
・IGMP proxy (pulled from EdgeOS).
・Dummy interfaces (same functionality to multiple loopbacks).
・IPsecがIKEv2、hash256、SHA2をサポート

etc...

参考: http://vyos.net/wiki/1.1.0/release_notes

Unmanaged L2TPv3を試してみた

L2TPv3?

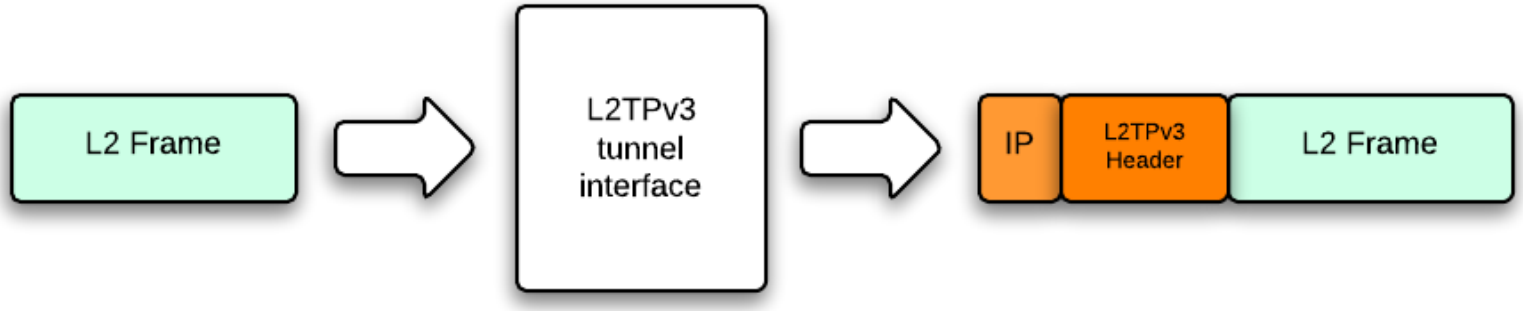
L2フレームをIPまたはUDPでカプセリングしてVPNを実現できるトンネリングプロトコル。

unmanged L2TPv3?

L2TPv3ではトンネルの接続、管理のためにcontorl messageをやりとりしています。unmanaged L2TPv3ではconrtrol messageで動的に設定されるパラメータを手動で設定して通信を確立させます。

unmanged L2TPv3

つまりこれだけ(encap ipの場合)



※ここからL2TPv3と記載しているL2TPv3は、unmanaged L2TPv3のことを指します。

iprouteコマンドでL2TPv3

・iprouteコマンドでの設定例

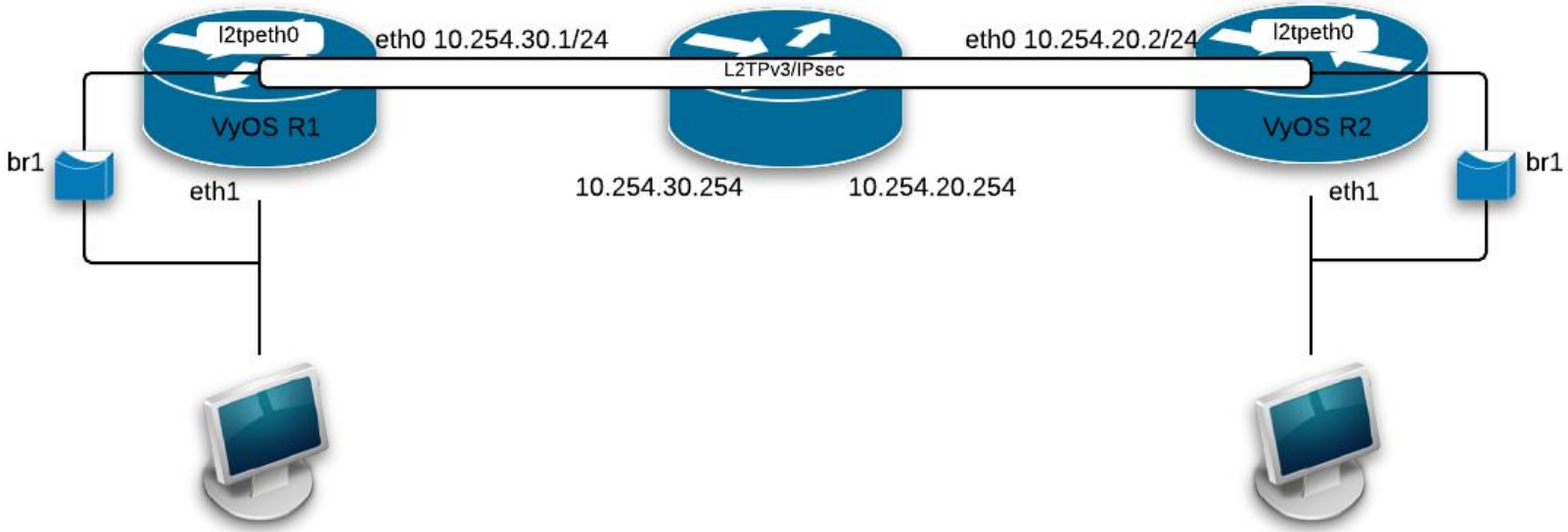
```
ip l2tp add tunnel tunnel_id 200 peer_tunnel_id 200 ¥
            encap udp local 192.0.2.1 remote 203.0.113.24 ¥
              udp_sport 9000 udp_dport 9001

ip l2tp add session tunnel_id 200 session_id 100 ¥
              peer_session_id 200

ip link set l2tpeth0 up mtu 1488
```

VyOSのL2TPv3コマンド

- 設定例(L2TPv3 over UDP):

```
l2tpv3 l2tpeth0 {
    destination-port 9001
    encapsulation udp
    local-ip 192.0.2.1
    peer-session-id 100
    peer-tunnel-id 200
    remote-ip 203.0.113.24
    session-id 100
    source-port 9000
    tunnel-id 200
}
```

VyOS - VyOS L2TPv3/IPsec



L2TPv3/IPsecの設定概要

・L2TPv3
 - encapsulationにUDP(1701)を使用
・IPsec
 - 事前共有鍵
 - UDP(1701)をIPsecする条件として設定
 - IKE　aes256, sha1, hd-group 5
 - ESP　aes256, sha1, transport mode, pfs enable

VyOS R1 基本設定

```
$ configure
# set interfaces ethernet eth0 address 10.254.30.1/24
# set system gateway-address 10.254.30.254
# set interfaces ethernet eth1 bridge-group bridge br0
# commit
# save
```

VyOS R1 IPsecの設定 1

```
# set vpn ipsec ike-group IKE-1
# set vpn ipsec ike-group IKE-1 proposal 1 encryption aes256
# set vpn ipsec ike-group IKE-1 proposal 1 hash sha1
# set vpn ipsec ike-group IKE-1 proposal 1 hd-group 5
# set vpn ipsec ike-group IKE-1 lifetime 3600
# set vpn ipsec esp-group ESP-1
# set vpn ipsec esp-group ESP-1 mode transport
# set vpn ipsec esp-group ESP-1 pfs enable
# set vpn ipsec esp-group ESP-1 lifetime 3600
# set vpn ipsec esp-group ESP-1 proposal 1 encryption aes256
# set vpn ipsec esp-group ESP-1 proposal 1 hash sha1
```

VyOS R1 IPsecの設定2

```
# set vpn ipsec site-to-site peer 10.254.20.2
# set vpn ipsec site-to-site peer 10.254.20.2 authentication mode pre-shared-secret
# set vpn ipsec site-to-site peer 10.254.20.2 authentication pre-shared-secret
secret123
# set vpn ipsec site-to-site peer 10.254.20.2 ike-group IKE-1
# set vpn ipsec site-to-site peer 10.254.20.2 local-address 10.254.30.1
# set vpn ipsec site-to-site peer 10.254.20.2 tunnel 1 esp-group ESP-1
# set vpn ipsec site-to-site peer 10.254.20.2 tunnel 1 local port 1701
# set vpn ipsec site-to-site peer 10.254.20.2 tunnel 1 remote port 1701
# set vpn ipsec ipsec-interfaces interface eth0
# commit
```

VyOS R1 L2TPv3の設定

```
# set interfaces l2tpv3 l2tpeth0
# set interfaces l2tpv3 l2tpeth0 encapsulation udp
# set interfaces l2tpv3 l2tpeth0 source-port 1701
# set interfaces l2tpv3 l2tpeth0 destination-port 1701
# set interfaces l2tpv3 l2tpeth0 local-ip 10.254.30.1
# set interfaces l2tpv3 l2tpeth0 remote-ip 10.254.20.2
# set interfaces l2tpv3 l2tpeth0 tunnel-id 3000
# set interfaces l2tpv3 l2tpeth0 peer-tunnel-id 4000
# set interfaces l2tpv3 l2tpeth0 session-id 1000
# set interfaces l2tpv3 l2tpeth0 peer-session-id 2000
# set interfaces bridge br0
# set interfaces l2tpv3 l2tpeth0 bridge-group brigde br0
# commit
# save
```

VyOS R2 基本設定

```
$ configure
# set interfaces ethernet eth0 address 10.254.20.2/24
# set system gateway-address 10.254.20.254
# set interfaces ethernet eth1 bridge-group bridge br0
# commit
# save
```

VyOS R2 IPsecの設定 1

```
# set vpn ipsec ike-group IKE-1
# set vpn ipsec ike-group IKE-1 proposal 1 encryption aes256
# set vpn ipsec ike-group IKE-1 proposal 1 hash sha1
# set vpn ipsec ike-group IKE-1 proposal 1 hd-group 5
# set vpn ipsec ike-group IKE-1 lifetime 3600
# set vpn ipsec esp-group ESP-1
# set vpn ipsec esp-group ESP-1 mode transport
# set vpn ipsec esp-group ESP-1 pfs enable
# set vpn ipsec esp-group ESP-1 lifetime 3600
# set vpn ipsec esp-group ESP-1 proposal 1 encryption aes256
# set vpn ipsec esp-group ESP-1 proposal 1 hash sha1
```

VyOS R2 IPsecの設定2

```
# set vpn ipsec site-to-site peer 10.254.30.1
# set vpn ipsec site-to-site peer 10.254.30.1 authentication mode pre-shared-secret
# set vpn ipsec site-to-site peer 10.254.30.1 authentication pre-shared-secret secret123
# set vpn ipsec site-to-site peer 10.254.30.1 ike-group IKE-1
# set vpn ipsec site-to-site peer 10.254.30.1 local-address 10.254.20.2
# set vpn ipsec site-to-site peer 10.254.30.1 tunnel 1 esp-group ESP-1
# set vpn ipsec site-to-site peer 10.254.30.1 tunnel 1 local port 1701
# set vpn ipsec site-to-site peer 10.254.30.1 tunnel 1 remote port 1701
# set vpn ipsec ipsec-interfaces interface eth0
# commit
```

VyOS R2 L2TPv3の設定

```
# set interfaces l2tpv3 l2tpeth0
# set interfaces l2tpv3 l2tpeth0 encapsulation udp
# set interfaces l2tpv3 l2tpeth0 source-port 1701
# set interfaces l2tpv3 l2tpeth0 destination-port 1701
# set interfaces l2tpv3 l2tpeth0 local-ip 10.254.20.2
# set interfaces l2tpv3 l2tpeth0 remote-ip 10.254.30.1
# set interfaces l2tpv3 l2tpeth0 tunnel-id 3000
# set interfaces l2tpv3 l2tpeth0 peer-tunnel-id 4000
# set interfaces l2tpv3 l2tpeth0 session-id 1000
# set interfaces l2tpv3 l2tpeth0 peer-session-id 2000
# set interfaces bridge br0
# set interfaces l2tpv3 l2tpeth0 bridge-group brigde br0
# commit
# save
```

IPsecの確認

```
vyos@vyos:~$ show vpn ike sa
Peer ID / IP                            Local ID / IP
------------                            -------------
10.254.30.1                             10.254.20.2

    State  Encrypt  Hash    D-H Grp  NAT-T  A-Time  L-Time
    -----  -------  ----    -------  -----  ------  ------
    up     aes256   sha1    5        no     2438    3600


vyos@vyos:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
10.254.30.1                             10.254.20.2

    Tunnel  State  Bytes Out/In   Encrypt  Hash    NAT-T  A-Time  L-Time  Proto
    ------  -----  -------------  -------  ----    -----  ------  ------  -----
    1       up     0.0/0.0        aes256   sha1    no     1510    1800    ip
```

VyOS以外とのL2TPv3/IPsec

unmanaged L2TPv3で必要なパラメータが決め打ちができるルータ（ＯＳ）であることが必要。

Ciscoはできるらしい

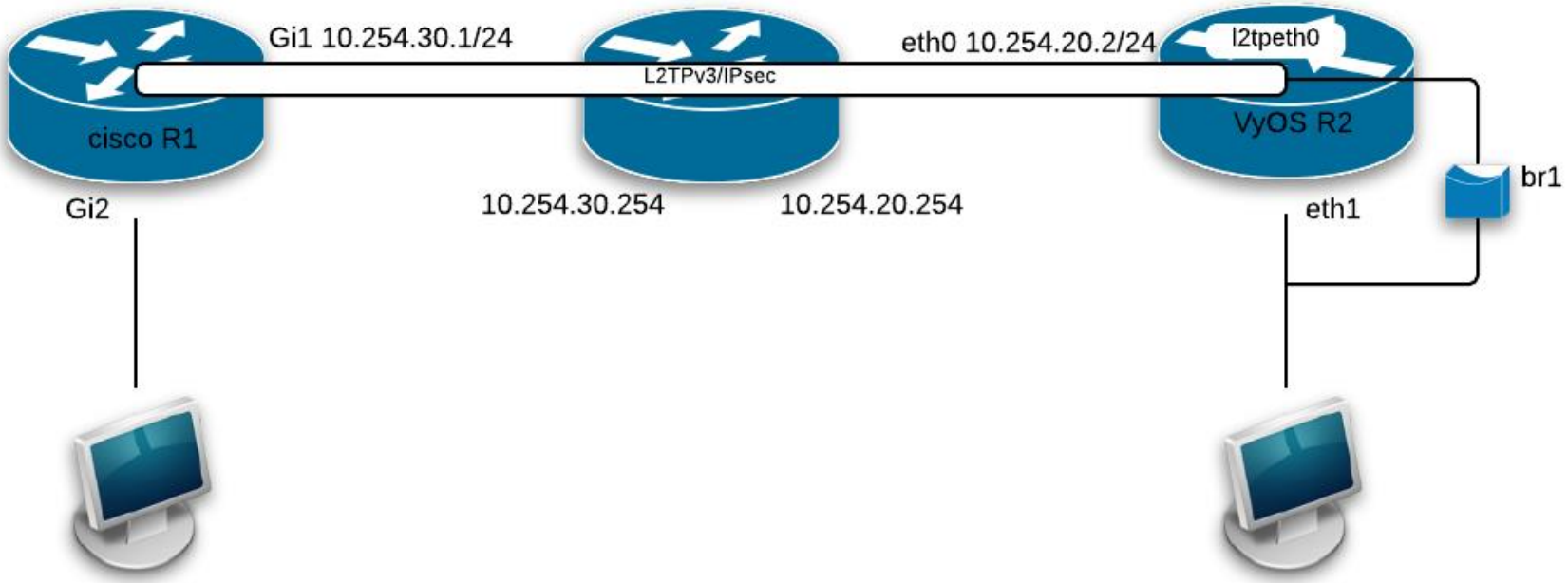
- L2TPv3でmanualというモードを使う
- CiscoではencapsulationはIPのみ
- L2-Specific Sublayer headerがない

※ L2-Specific Sublayerはoptionalなので必須ではない

Cisco側のcookieの設定を調整するとVyOS側がこれを回避できる。

参考: http://man7.org/linux/man-pages/man8/ip-l2tp.8.html
http://www.spinics.net/lists/netdev/msg254630.html

CSR1000v - VyOS L2TPv3/IPsec



L2TPv3/IPsecの設定概要

・L2TPv3
 - encapsulationにIPを使用
・IPsec
 - 事前共有鍵
 - IPのプロトコルタイプ115(l2tp)をIPsecする条件として設定
 - IKE　aes256, sha1, hd-group 5
 - ESP　aes256, sha1, transport mode, pfs enable

CSR1000v R1基本設定

(config 抜粋)

```
interface GigabitEthernet2
  ip address 10.254.30.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 10.254.30.254
```

CSR1000v R1 IPsecの設定1

(config 抜粋)

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key secret123 address 10.254.20.2
crypto isakmp keepalive 30 periodic
!
crypto ipsec transform-set IPSEC esp-aes 256 esp-sha-hmac
 mode transport
```

CSR1000v R1 IPsecの設定2

(config 抜粋)

```
crypto map L2TPv3-IPSEC_to_VyOS 1 ipsec-isakmp
 set peer 10.254.20.2
 set transform-set IPSEC
 match address 100
!
access-list 100 permit 115 host 10.254.30.1 host 10.254.20.2
```

CSR1000v R1 L2TPv3の設定

(config 抜粋)

```
pseudowire-class PSE-L2TPv3
 encapsulation l2tpv3
 interworking ethernet
 protocol none
 ip local interface GigabitEthernet1
interface GigabitEthernet2
 no ip address
 negotiation auto
 xconnect 10.254.20.2 1000 encapsulation l2tpv3 manual pw-class PSE-L2TPv3
  l2tp id 4000 3000
  l2tp cookie local 4 0
  l2tp cookie remote 4 0
!
```

VyOS R2 基本設定

```
$ configure
# set interfaces ethernet eth0 address 10.254.20.2/24
# set system gateway-address 10.254.20.254
# set interfaces ethernet eth1 bridge-group bridge br0
# commit
# save
```

VyOS R2 IPsecの設定 1

```
# set vpn ipsec ike-group IKE-1
# set vpn ipsec ike-group IKE-1 proposal 1 encryption aes256
# set vpn ipsec ike-group IKE-1 proposal 1 hash sha1
# set vpn ipsec ike-group IKE-1 proposal 1 hd-group 5
# set vpn ipsec ike-group IKE-1 lifetime 3600
# set vpn ipsec esp-group ESP-1
# set vpn ipsec esp-group ESP-1 mode transport
# set vpn ipsec esp-group ESP-1 pfs enable
# set vpn ipsec esp-group ESP-1 lifetime 3600
# set vpn ipsec esp-group ESP-1 proposal 1 encryption aes256
# set vpn ipsec esp-group ESP-1 proposal 1 hash sha1
```

VyOS R2 IPsecの設定2

```
# set vpn ipsec site-to-site peer 10.254.30.1
# set vpn ipsec site-to-site peer 10.254.30.1 authentication mode pre-shared-secret
# set vpn ipsec site-to-site peer 10.254.30.1 authentication pre-shared-secret
secret123
# set vpn ipsec site-to-site peer 10.254.30.1 ike-group IKE-1
# set vpn ipsec site-to-site peer 10.254.30.1 local-address 10.254.20.2
# set vpn ipsec site-to-site peer 10.254.30.1 tunnel 1 esp-group ESP-1
# set vpn ipsec site-to-site peer 10.254.30.1 tunnel 1 protocol l2tp
# set vpn ipsec ipsec-interfaces interface eth0
# commit
```

VyOS R2 L2TPv3の設定

```
# set interfaces l2tpv3 l2tpeth0
# set interfaces l2tpv3 l2tpeth0 encapsulation ip
# set interfaces l2tpv3 l2tpeth0 local-ip 10.254.20.2
# set interfaces l2tpv3 l2tpeth0 remote-ip 10.254.30.1
# set interfaces l2tpv3 l2tpeth0 tunnel-id 1000
# set interfaces l2tpv3 l2tpeth0 peer-tunnel-id peer 1000
# set interfaces l2tpv3 l2tpeth0 session-id 3000
# set interfaces l2tpv3 l2tpeth0 peer-session-id 4000
# set interfaces l2tpv3 l2tpeth0 bridge-group brigde br0
# commit
```

既知の問題的な何か

- L2tpv3/IPsecで疎通できた後に、IPsecの設定を変更したりすると疎通できなくなることがある。

- peer ipが疎通状態にない場合にコマンドがエラーになる
  特に両端のVyOSを再起動する時はよく起こる

- IPv6かつencupにipを指定した場合に必要モジュールがロードされない

※IPv6の問題については、指摘すればすぐ修正されるかも

Q-in-Qとか

Wikiに設定例があるから見てね。

※(2014/8時点)設定例はMTU未調整なので注意

参考:
http://vyos.net/wiki/1.1.0/release_notes

次次期Ver VyOSについて

・Ver 1.2
- ベースを**squeeze から wheezyに更新**

心配？

少ないメンバーで
果たして無事にwheezy更新できるか？

EdgeOSについて

次期バージョン1.1(Helium)

Kernelの更新と幾つかの機能追加とバグ修正がありました。

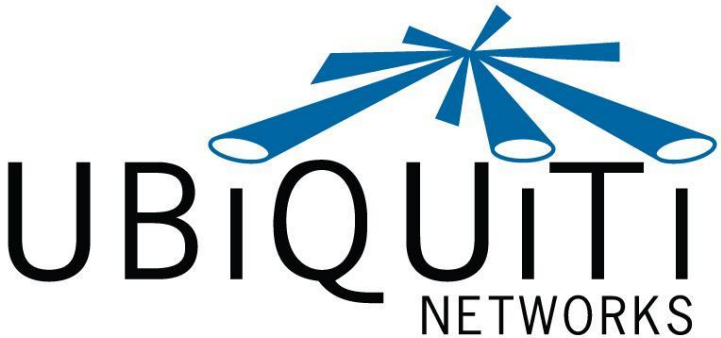
・kernel 3.13（iproute2も合わせて）
・802.3ad QinQ VLAN stacking
・Unmanaged L2TPv3
・Event handler
・IGMP proxy (pulled from EdgeOS). ← これ
・Dummy interfaces (same functionality to multiple loopbacks).
・IPsecがIKEv2、hash256、SHA2をサポート

etc...

参考: http://vyos.net/wiki/1.1.0/release_notes

EdgeOSとは

Ubiquiti NetworksのEdgeRouterというルータ製品に乗っているＯＳ



参考:EdgeRouter Lite

こんなの

参考:EdgeRouter Lite

CPU : Cavium OCTEON+
RAM : 512MB RAM
ストレージ : USB 2.0 2GBフラッシュ
NIC : 1GbE x 3 port(eth0 - eth2)
コンソール : RJ45シリアルポート（CiscoのでＯＫ）
性能: 100万PPS
価格: 日本円で1万円ちょい(個人輸入)

EdgeOSとは

Vyatta Core6.3からFork
EdgeRouterに搭載されているMIPSで動作することを想定されている
EdgeOSコミュニティもあってそこから意見も取り入れて開発されている(参加ユーザ数はVyOSより多い)
企業のバックがある

基本部分は同じ

・configure、commit、saveは同じ
・bashに入ることもできる

EdgeOSとVyOSの関係

EdgeOSの成果が一部取り込まれたりする。
交流はあるが、上下関係ではないらしい。

None of the systems commits to closely follow the other, i.e. EdgeOS is not the "upstream" for VyOS or vice versa.
(略)
In a nutshell, it's much like FreeBSD and OpenBSD. They exchange patches when it's reasonable to achieve common goals, but they are independent and each is going in its own direction.

参考:http://blog.vyos.net/post/71030817586/relationship-with-edgeos

VyOSと共通の追加/修正

例:

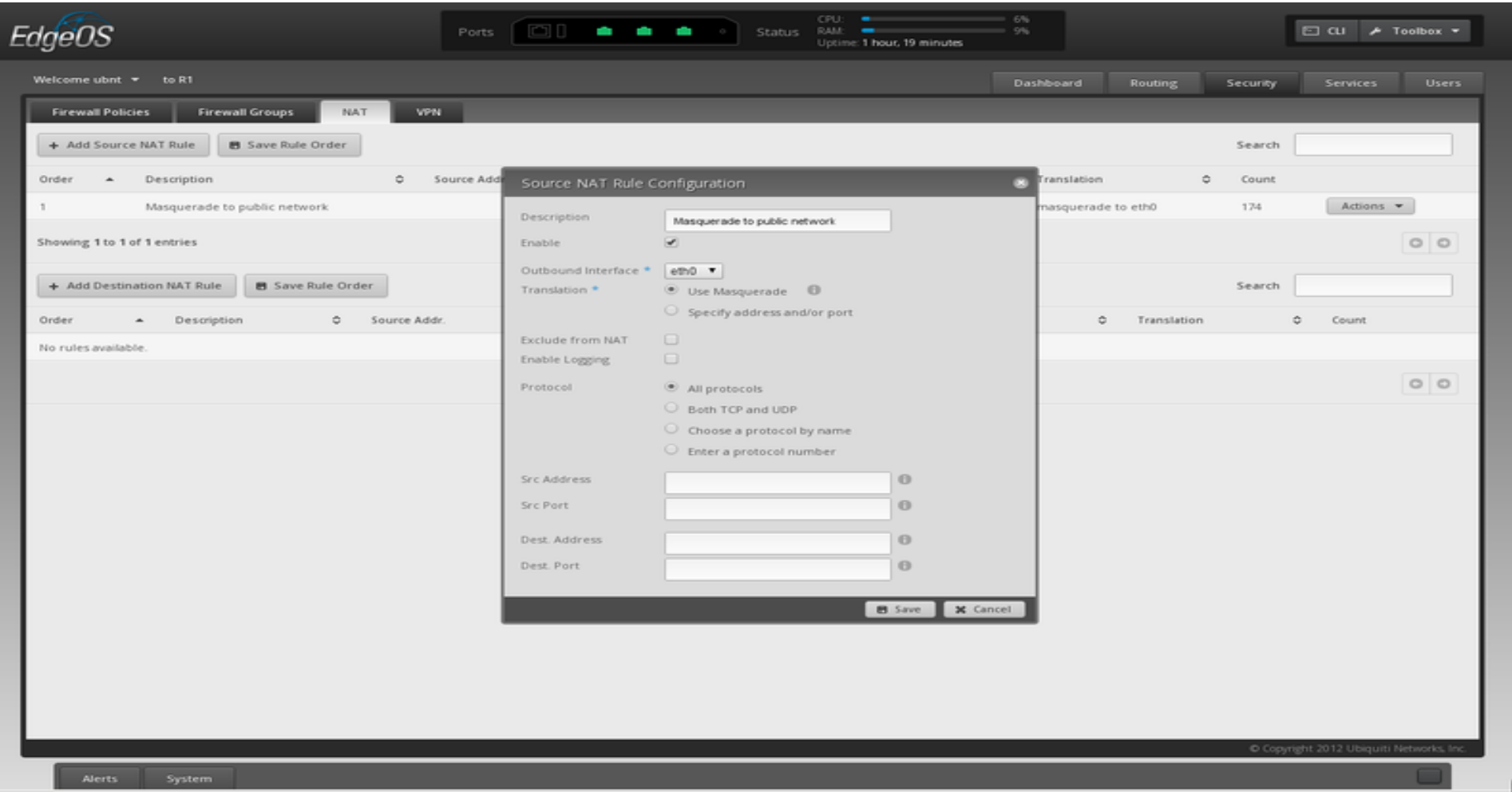
- IGMP Proxy
- Task scheduler (cron) CLI
- Command Scripting
- IPv4 BGP peer groupsのバグFIX
- DHCPv6 relayのバグFIX

EdgeOS固有の機能など

例 EdgeOS最新版v1.5の場合(2014/8時点):

- 6RD
- UPnP?
- Linux kernel 3.4.27
- WebUIの強化

参考:
https://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMax-software-release-v1-5-0/ba-p/888586


EdgeOS
Ports
Status
CPU: 6%
RAM: 9%
Uptime: 1 hour, 19 minutes
CLI
Toolbox
Welcome ubnt
to R1
Dashboard
Routing
Security
Services
Users
Firewall Policies
Firewall Groups
NAT
VPN
+ Add Source NAT Rule
Save Rule Order
Search
Order
Description
Source Addr.
Translation
Count
1
Masquerade to public network
masquerade to eth0
174
Actions
Showing 1 to 1 of 1 entries
+ Add Destination NAT Rule
Save Rule Order
Search
Order
Description
Source Addr.
Translation
Count
No rules available.
Source NAT Rule Configuration
Description
Masquerade to public network
Enable
Outbound Interface *
eth0
Translation *
Use Masquerade
Specify address and/or port
Exclude from NAT
Enable Logging
Protocol
All protocols
Both TCP and UDP
Choose a protocol by name
Enter a protocol number
Src Address
Src Port
Dest. Address
Dest. Port
Save
Cancel
© Copyright 2012 Ubiquiti Networks, Inc.
Alerts
System

EdgeOS v1.6(alpha2時点)

- New kernel (3.10-based)
- Change base system to Debian wheezy
- basic DHCPv6 PD support

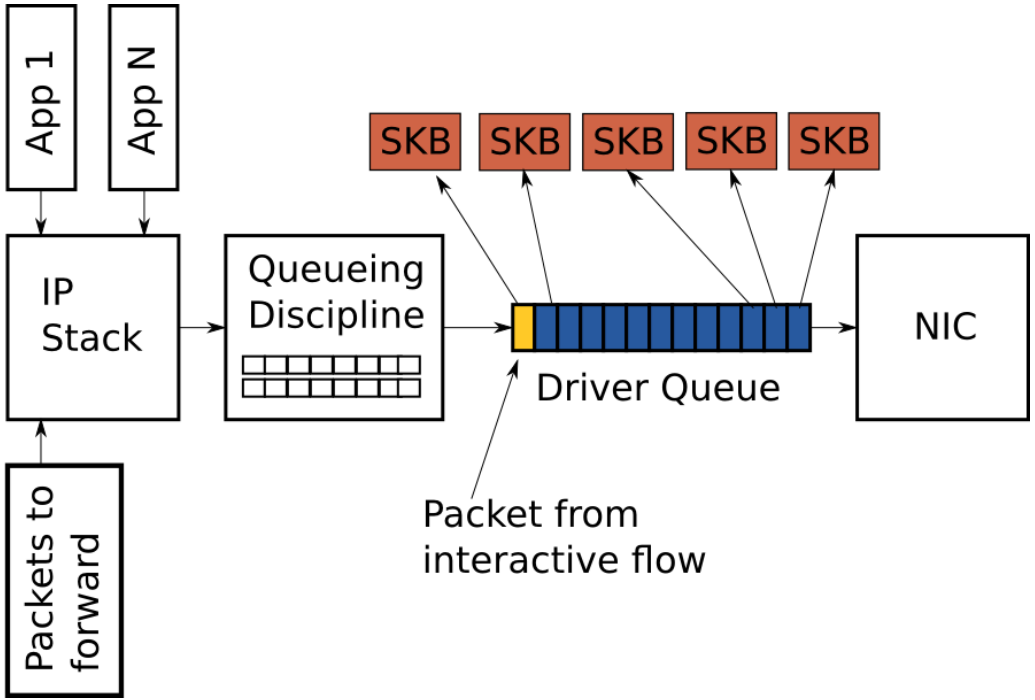
alpha1 Release Notes:
http://community.ubnt.com/t5/EdgeMAX/Alpha-software-release-v1-6-0alpha1-now-available-in-the-beta/m-p/949025#U949025

alpha2 Release notes:
http://community.ubnt.com/t5/EdgeMAX-Beta/Alpha-release-v1-6-0alpha2/m-p/973015#U973015

その他実装が試されている機能

- VRF
- fq_codel/HTB（Bufferbloat対策）

Linuxの送信側イメージ



参考: http://www.coverfire.com/articles/queueing-in-the-linux-network-stack/

```
[ftoyama@localhost ]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP qlen 1000
    link/ether 00:0c:xx:xx:xx:xx brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.xxx/24 brd 192.168.1.255 scope global eth0
    valid_lft forever preferred_lft forever
```

Bufferbloatについて

ここらへんを参考にしてください。

Bufferbloat:
http://www.slideshare.net/kazuhitoohkawa/bufferbloat
http://events.linuxfoundation.jp/events/linuxcon-japan/program/slides
のBufferbloat: are we there yet? By stephen hemminger

FQ_CoDel(Fair Queue Controlled Delay):
https://www.bufferbloat.net/projects/codel/wiki/Technical_description_of_FQ_CoDel
http://manpages.ubuntu.com/manpages/raring/man8/tc-fq_codel.8.html

HTB(Hierarchical Token Bucket):
http://linuxjf.sourceforge.jp/JFdocs/Adv-Routing-HOWTO/lartc.qdisc.classful.html
http://luxik.cdi.cz/~devik/qos/htb/

参考: /usr/share/doc/ubnt-platform-e100/fqcodel-example をそのまま実行すると投入されるtcコマンド

```
#WAN upload traffic
/sbin/tc qdisc add dev eth1 root handle 1: htb default 10
/sbin/tc class add dev eth1 parent 1: classid 1:1 htb quantum 1500 ¥
        rate 8000000 ceil 8000000
/sbin/tc class add dev eth1 8000000 parent 1:1 classid 1:10 htb quantum 1500 ¥
        rate 8000000 ceil
/sbin/tc qdisc add dev eth1 parent 1:10 handle 100: fq_codel quantum 300 target 5ms

#WAN download traffic
/sbin/tc qdisc add dev ifb_eth1 root handle 1: htb default 10
/sbin/tc class add dev ifb_eth1 parent 1: classid 1:1 htb quantum 1500 ¥
        rate 10000000 ceil 10000000
/sbin/tc class add dev ifb_eth1 parent 1:1 classid 1:10 htb quantum 1500 ¥
        rate 10000000 ceil 10000000
/sbin/tc qdisc add dev ifb_eth1 parent 1:10 handle 100: fq_codel quantum 300 target 5ms

/sbin/ip link set ifb_eth1 up
/sbin/tc qdisc add dev eth1 handle ffff: ingress # download  traffic
/sbin/tc filter add dev eth1 parent ffff: protocol all prio 10 u32 match u32 0 0 flowid 1:1 ¥
          action mirred egress redirect dev ifb_eth1
```

まとめ

・unmanaged L2TPv3は、control messageの実装がされていないのでその前提で使うこと

・EdgeOSが存続する限り、VyOSは現状の少ないメンバーでも続いてくれそうかも？

・CSR1000vも良いけどVyOSも使ってみよう（コワクナイヨー）

おわり