SAKURA Internet

www.sakura.ad.jp

クラウド環境における仮想ルーター

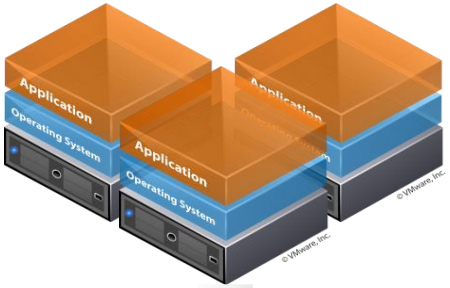
2010年12月09日

さくらインターネット研究所　上級研究員
日本Vyattaユーザー会　運営委員
松本直人

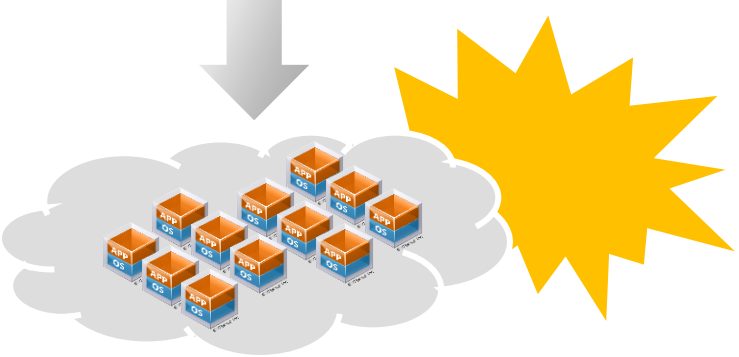
現在起こっているコト

SAKURA Internet

従来のコンピューティング



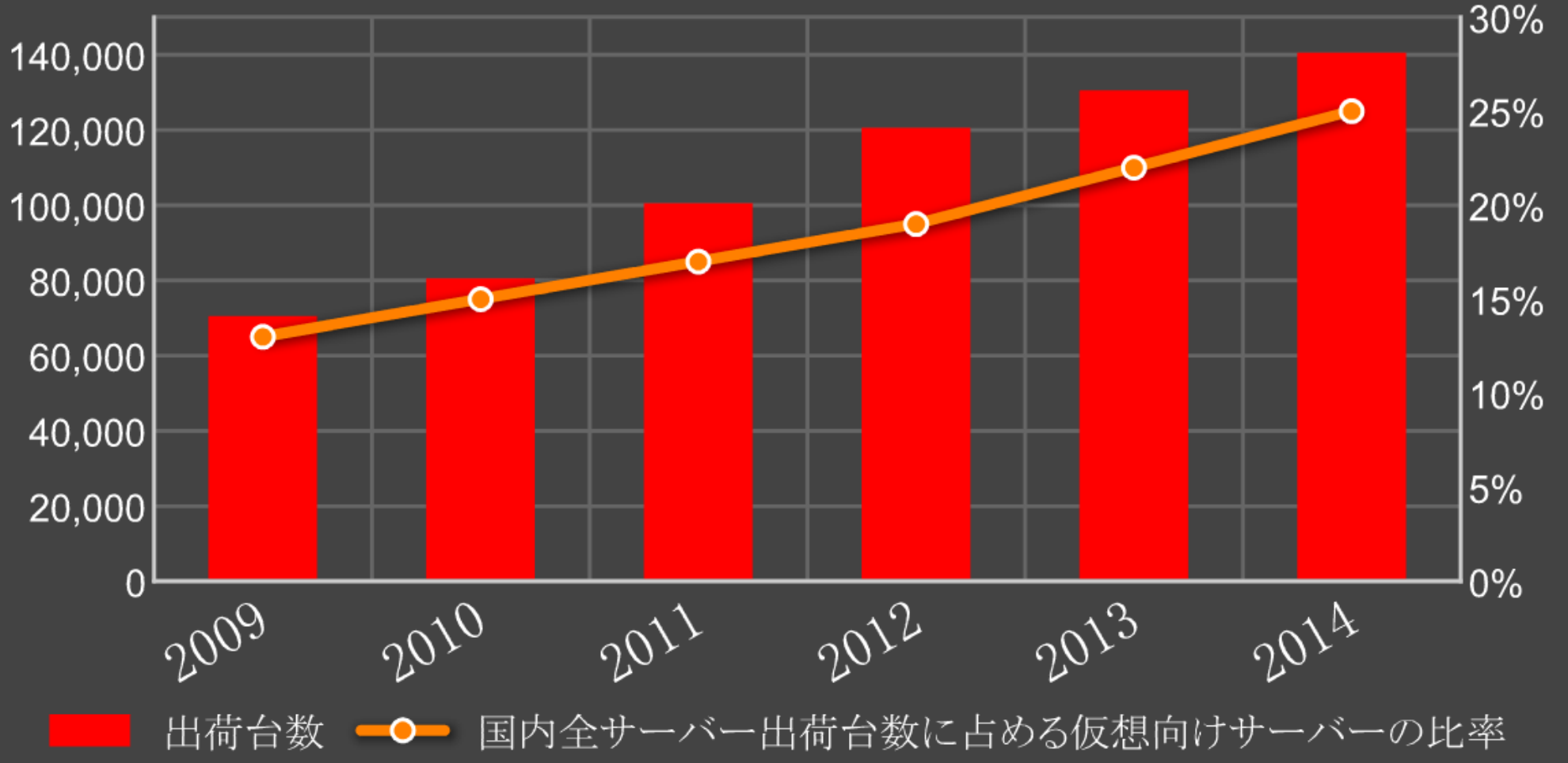
クラウド・コンピューティング



パブリック、プライベートの区別なくクラウドへ移行中

仮想化を取り巻く環境

出典: 国内仮想化サーバー市場 出荷台数予測、2009年～2014年 IDC Japan株式会社 (2010年10月28日作成)



今後5年以内に国内サーバーの1/4が仮想環境となる

ネットワーク機器も仮想化へ

SAKURA Internet

既存のシステム構成

- Firewall Appliance
- VPN Appliance
- SPAM Appliance
- E-Mail Appliance
- VOIP Appliance
- Anti-Virus Appliance
- Search Appliance
- Integration Appliance

仮想化技術で省力化

vmware Virtual Infrastructure

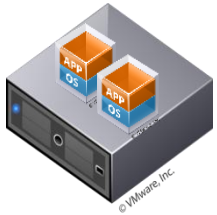
- Firewall Virtual Appliance
- VPN Virtual Appliance
- SPAM Virtual Appliance
- E-Mail Virtual Appliance
- VOIP Virtual Appliance
- Anti-Virus Virtual Appliance
- Search Virtual Appliance
- Integration Virtual Appliance

ネットワーク機器の仮想アプライアンス化は発展途上

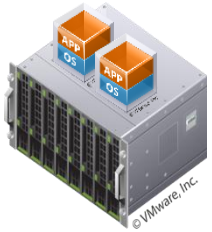
仮想化・クラウドを取り巻く方向性

SAKURA Internet

仮想化



プライベート・クラウド



パブリック・クラウド

用途に応じた選択が、ユーザーによって行われる

Vyattaが持つ機能

SAKURA Internet

IPv4 / IPv6 Routing	» BGPv4, BGPv6 » OSPFv2, OSPFv3*	» RIPv2 » Static Routes	» IPv6 Policy » IPv6 SLAAC
IP Address Management	» Static » DHCP Server » DHCP Client	» DHCP Relay » Dynamic DNS » DNS Forwarding	» DHCPv6 Server » DHCPv6 Client » DHCPv6 Relay
Encapsulations	» Ethernet » 802.1Q VLANs » PPP	» PPPoE » IP in IP » Frame Relay	» MLPPP » HDLC » GRE
Firewall	» Stateful Inspection Firewall » Zone-based Firewall » P2P Filtering	» IPv6 Firewalling » Time-based Firewall Rules » Rate Limiting	» ICMP Type Filtering » Stateful Failover
Tunneling / VPN	» SSL-based OpenVPN » Site to Site VPN (IPSec) » Remote VPN (PPTP, L2TP, IPSec)	» OpenVPN Client Auto-Configuration » Layer 2 Bridging over GRE » Layer 2 Bridging over OpenVPN	
Additional Security	» Network Address Translation » Sourcefire VRT Intrusion Prevention » VyattaGuard Web Filtering	» DES, 3DES, AES Encryption » MD5 and SHA-1 Authentication » RSA, Diffie Helman Key Mgmt	» NAT Traversal » Role based access control
WAN / LAN Device Drivers	» WAN Device Drivers - ADSL, T1, T3 » Intel 10/100Mbps - 10Gbps	» IEEE 802.11 wireless » Drivers in 2.6.31 Linux Kernel	» Synchronous Serial - V.35, X.21, RS-422, EIA530
Performance Optimization	» WAN Link Load Balancing » Ethernet Link Bonding » Web Caching	» MLPPP » ECMP » Bandwidth Management	
QoS Policies	» Priority Queuing » Network Emulator » Round Robin	» Random / Weighted Random » Classful Queuing » Ethernet Header Matching	» VLAN Tag » IPv6 Address » Port Mirroring
High Availability	» Stateful Firewall / NAT Failover » VRRP » HA Clustering	» Configuration Replication » RAID 1	» IPSec VPN Clustering » Protocol Fault Isolation
Administration & Authentication	» Integrated CLI » Web GUI » Vyatta Remote Access API	» Telnet » SSHv2 / SSH Public Key » Binary Image Install	» RADIUS » TACACS+* » Single Configuration File
Diagnostics & Logging	» tcpdump » Wireshark Packet Capture » BGP MD5 Support	» Serial Loopback Commands » Netflow / sFlow » LLDP	» Syslog » SNMPv2c » SNMP for IPv6

VyattaCore提供方式

SAKURA Internet

http://www.vyatta.org/downloads

virt.ISO

VMware OVF

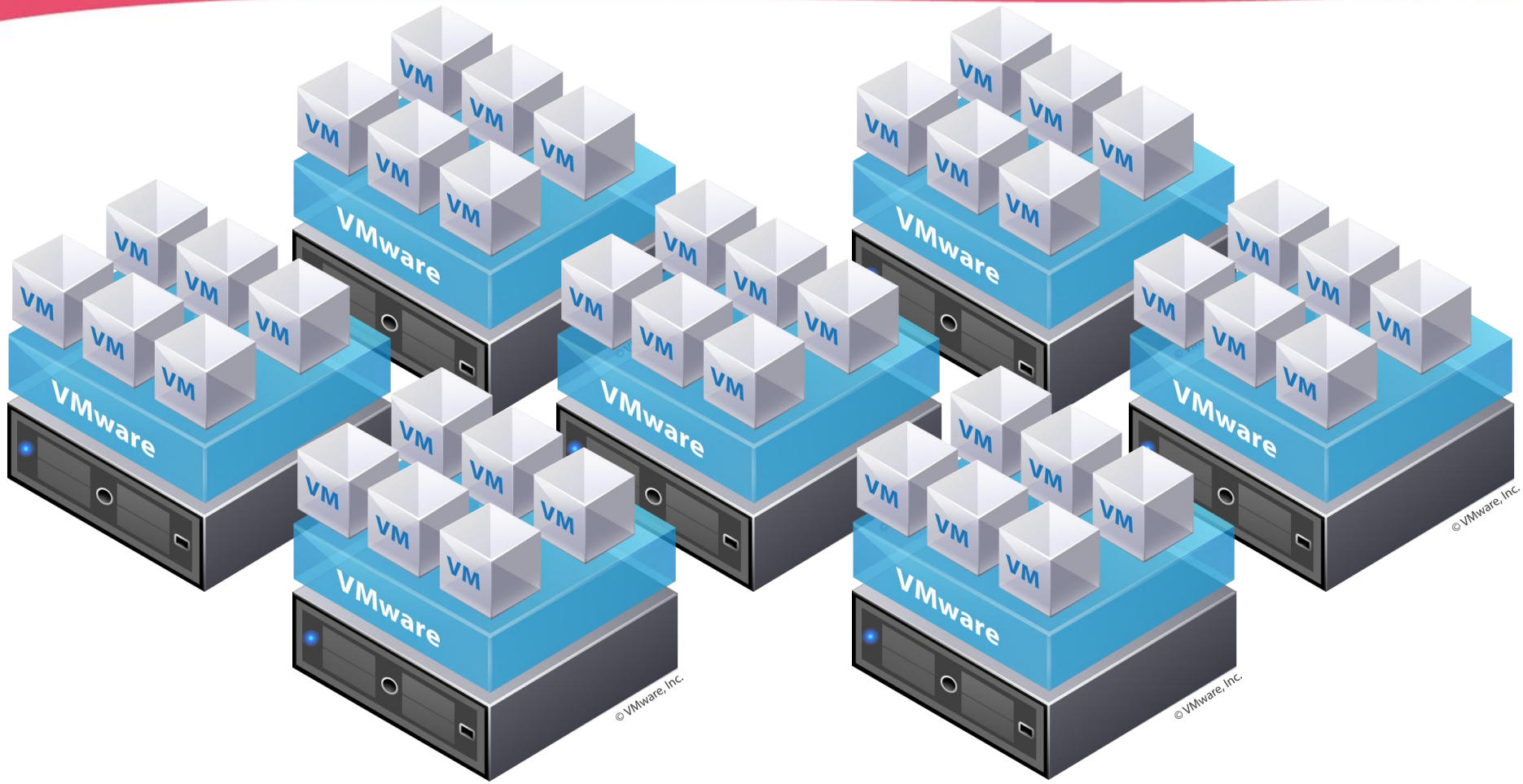
XenServer XVA

LiveCD

ユーザー環境に応じて、システム・イメージを選択が可能

クラウド時代のVyattaの使われ方

SAKURA Internet



仮想ルーターとして、クラウド環境で場所を選ばず利用できる

BASIC Configuration

SAKURA Internet

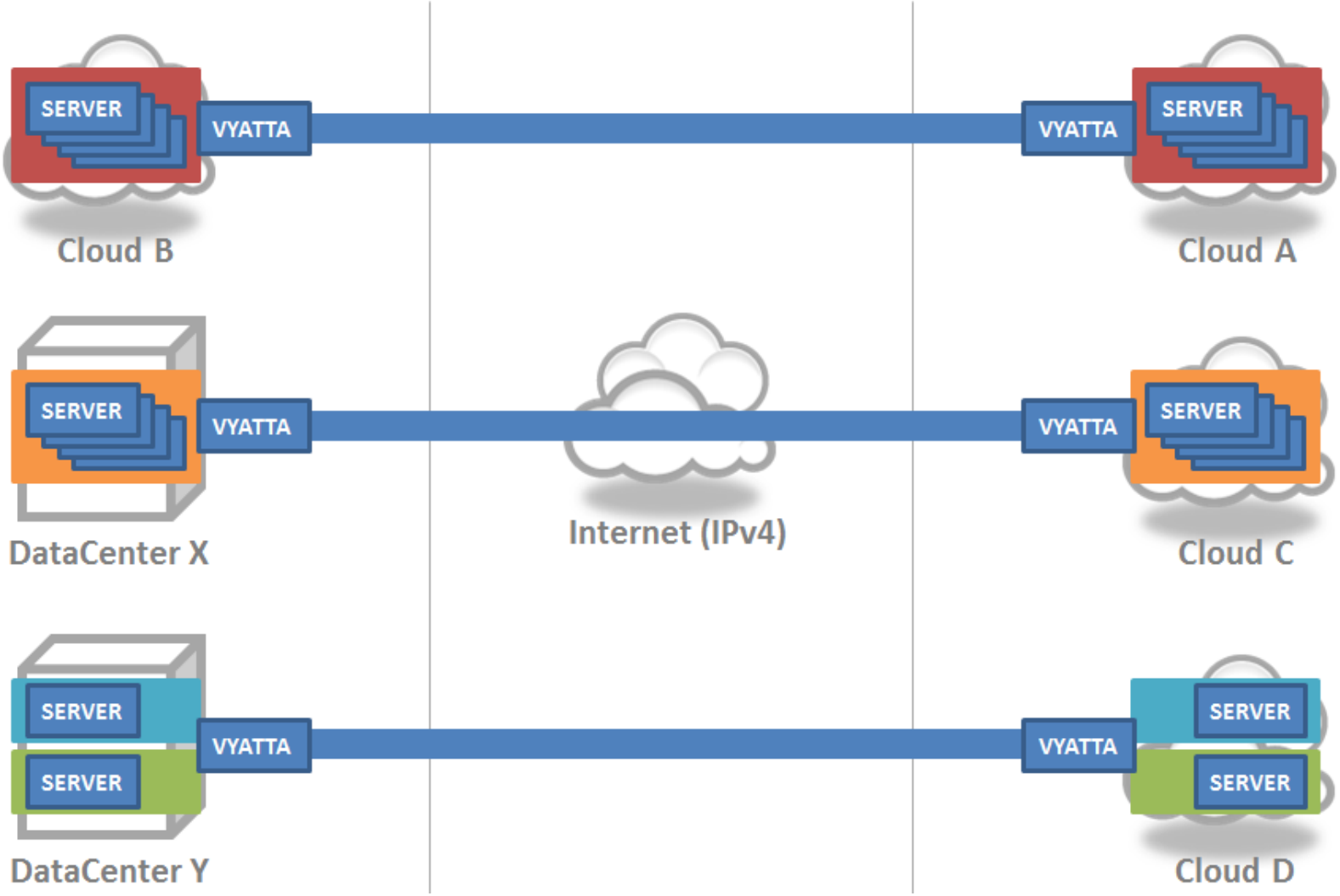
```
set interfaces ethernet eth0 address 10.10.10.10/24
set system gateway-address 10.10.10.1

set system name-server 10.10.10.99
set system name-server 10.10.10.88
set interfaces ethernet eth1 address 192.168.168.10/24
set service ssh
set system time-zone Asia/Tokyo
set system syslog host 10.10.10.222 facility all level info
commit
```

基本的なルーター設定は、既存のルーター製品と全く同じ

インタークラウドで設備のシームレス化

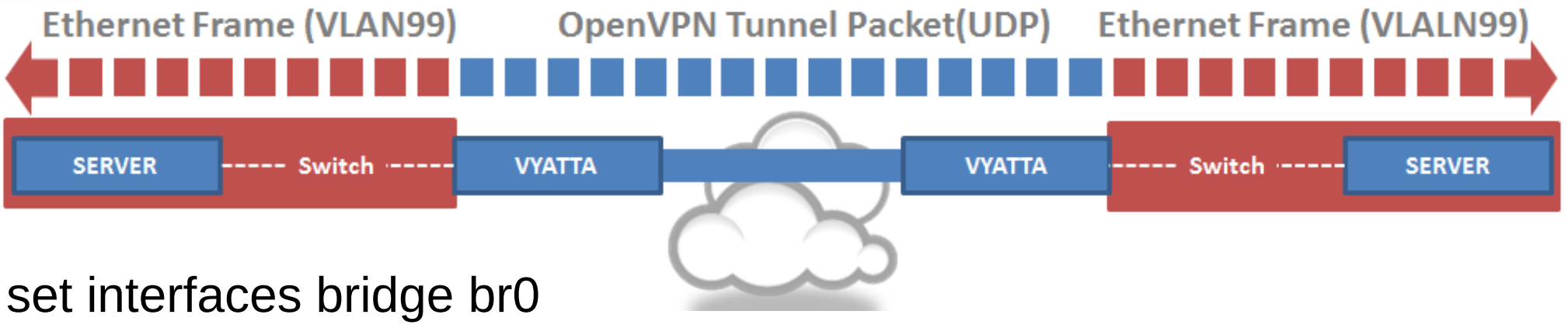
SAKURA Internet

Inter-Cloud Networking Model



Layer2 Bridging Configuration

SAKURA Internet

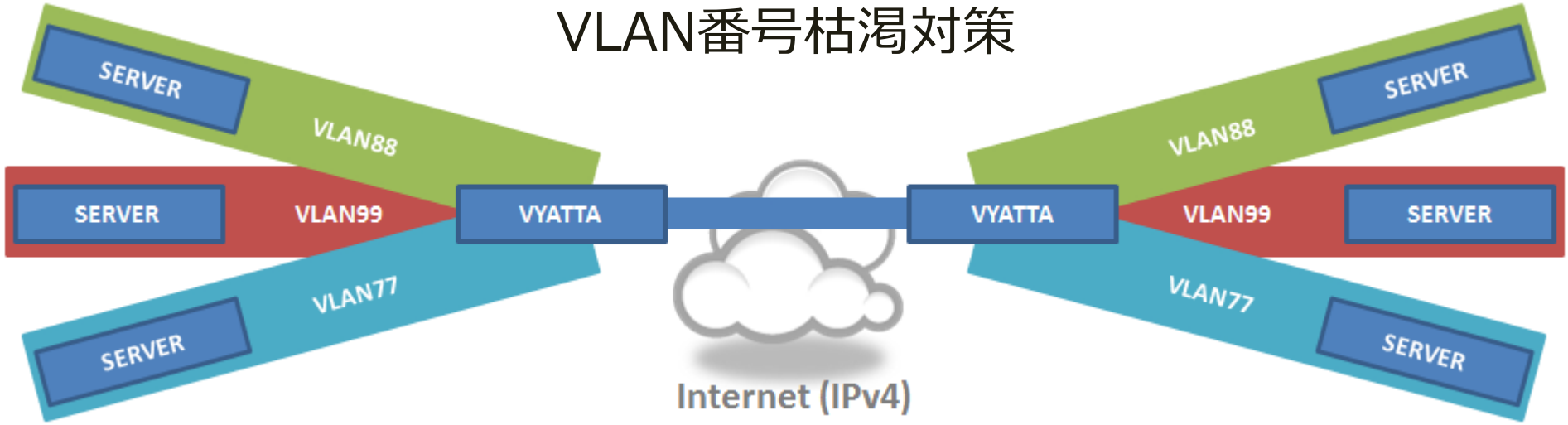



```
set interfaces bridge br0
set interfaces ethernet eth1 bridge-group bridge br0
set interfaces openvpn vtun0 bridge-group bridge br0
set interfaces openvpn vtun0 mode site-to-site
set interfaces openvpn vtun0 remote-host X.X.X.X
run vpn openvpn-key generate /root/key
set interfaces openvpn vtun0 shared-secret-key-file /root/key
```

Ethernetフレームを遠隔地まで飛ばし、シームレスにつなぐ

Against VLAN Exhaustion

SAKURA Internet



set interfaces ethernet eth0 vif 66 address A.A.A.A/24
set interfaces ethernet eth0 vif 77 address B.B.B.B/24
set interfaces ethernet eth0 vif 88 address C.C.C.C/24
set interfaces ethernet eth0 vif 99 address D.D.D.D/24

管理セグメントのVLAN番号の制約を受けないネットワーク設計

IPv6 Networking

SAKURA Internet

```
set interfaces ethernet eth0 address 2001:db8:a::1/64
set interfaces ethernet eth1 address 2001:db8:b::2/64
delete system ipv6 disable-forwarding

set protocols static route6 ::/0 next-hop 2001:db8:a::99/64

set firewall ipv6-name FWv6 default-action reject
set firewall ipv6-name FWv6 rule 66 source address 2001:db8:a::0/64
set firewall ipv6-name FWv6 rule 66 action accept
set interfaces ethernet eth0 firewall in ipv6-name FWv6
commit
```

小規模なIPv6 Networkingから開始できる機能を保持

Add New media type / Infiniband

SAKURA Internet

```
sudo full-upgrade -k
sudo apt-get update
sudo aptitude install module-assistant
sudo apt-get install rpm zlib1g-dev zlib1g-dbg
sudo aptitude intall byacc bison flex
sudo module-assistant prepare
sudo /opt/OFED-1.5.2/install.pl
sudo vi /etc/udev/rules.d/75-persistent-net-generator.rules
 :

set interfaces inifniband ib0 address 1.1.1.1/24
commit
```

OpenFabrics Enterprise Distribution (OFED)でIPoIB機能追加

Against Denial of Service Attack

SAKURA Internet

```
set firewall name STOP-DoS default-action accept

set firewall name STOP-DoS rule 99 protocol tcp
set firewall name STOP-DoS rule 99 destination port 80
set firewall name STOP-DoS rule 99 state new enable
set firewall name STOP-DoS rule 99 recent count 99
set firewall name STOP-DoS rule 99 recent time 10

set firewall name STOP-DoS rule 99 action drop
set interfaces ethernet eth0 firewall in name STOP-DoS
```

VyattaCore version 6.1 2010.08.20
Build ID 1008200448-170b446

同一IPアドレスから10秒間に99回以上のトラフィックは遮断

SAKURA Internet

www.sakura.ad.jp

ご静聴誠にありがとうございました