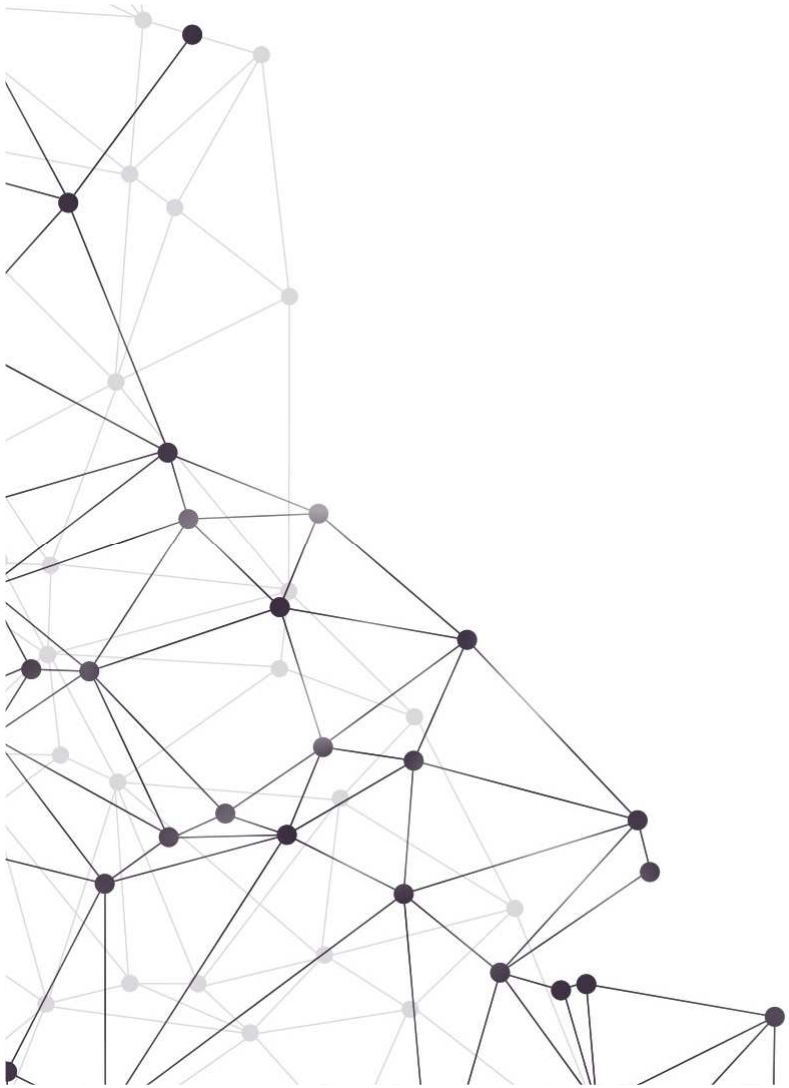


Budowa wirtualnego Data Center w oparciu o technologie Open Source

Marcin Motylski
MITVision

NGSec 2017 30.05.2017

Budowa VDC – historia DC w Polsce

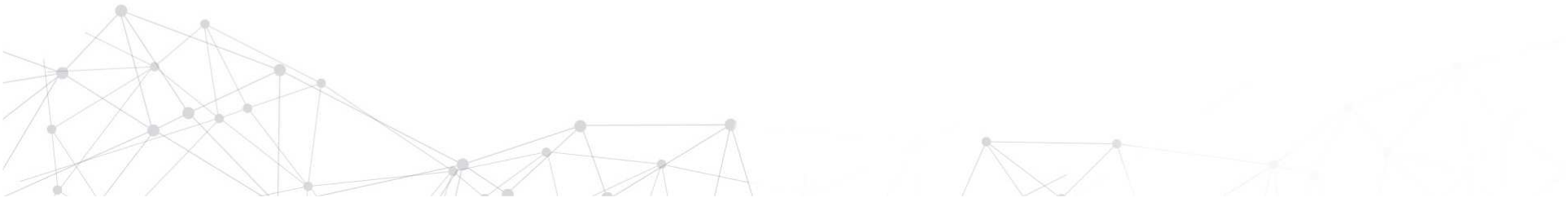
1995 – Novell Netware, SGI/Irix, 10Mbps

2000 – boom Data Center, pierwsze ASP (Application Service Providers)

2004 – zarządzany hosting, duże instalacje HW

2009 – wirtualizacja, VMWare, LDOM, LPAR, KVM

2017 – Cloud, 10Gbps peering EU, EU Zones, Global Regions



Budowa VDC – historia Internetu w Polsce

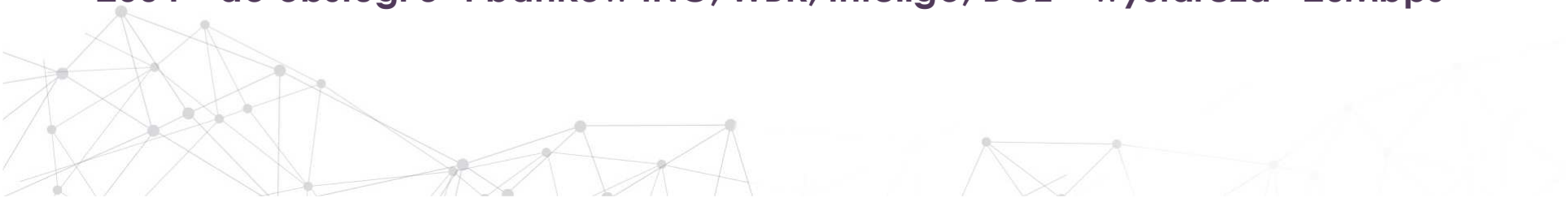
~1995 – pobieranie 1Mb (goblins.zip) Kraków <-> Lublin 8-12 godzin (DOS)

~1997 – zarządzanie serwerami z Polski w USA z opóźnieniem ~200ms (prędkości po USA ~35Mbps) (ascii / konsola)

~1999 – łącza do prywatnych Data Center – 20-40 Mbps – dzierżawy łącza dla klientów na poziomie 1-2Mbps CIR/EIR

2000 – pierwsze internetowe serwisy muzyczne, boom portali internetowych

2004 – do obsługi 3-4 banków ING, WBK, Inteligo, BGŻ – wystarcza ~20Mbps

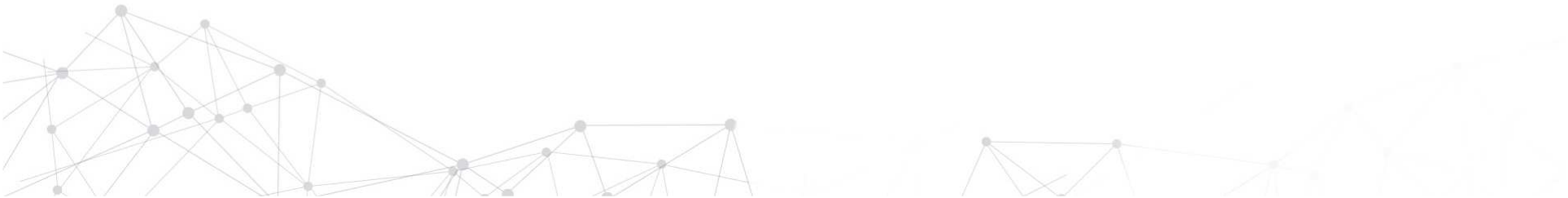


Budowa VDC – historia Internetu w Polsce

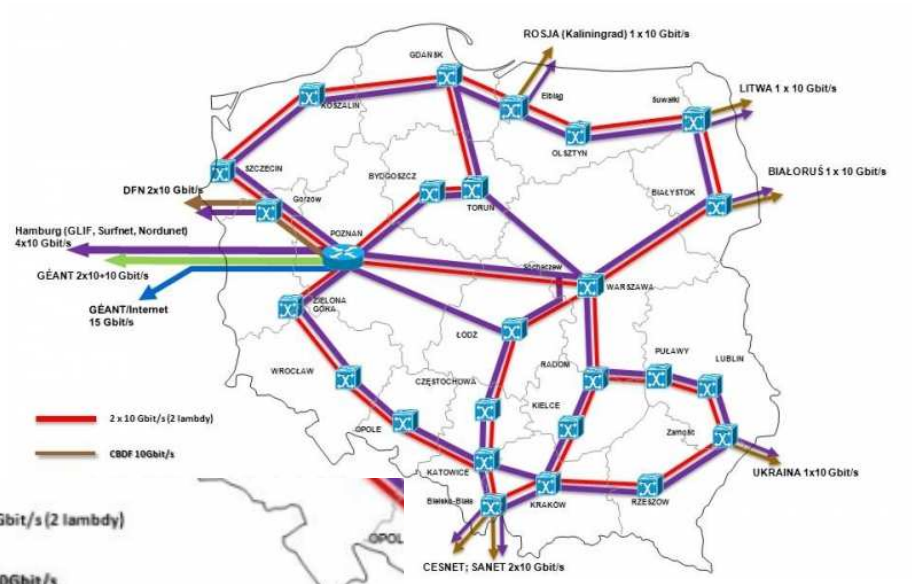
2016 – UPC ofertuje łącza 300/30 Mbps ~150PLN modem kablowy,

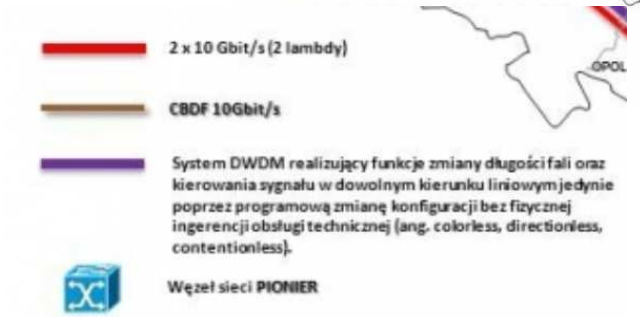
Orange ofertuje łącza 600/60 Mbps światłowód ~110PLN (duże miasta – łącze domowe)

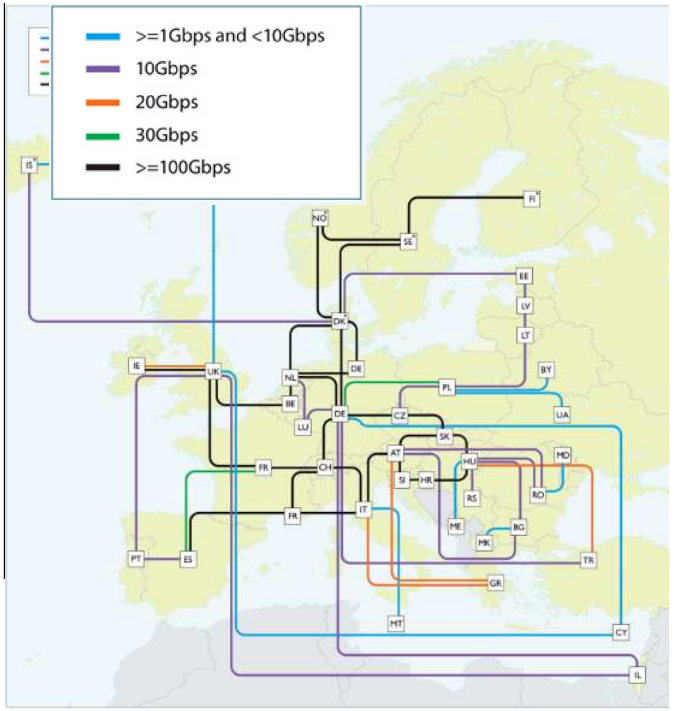
2016 – OVH daje możliwość podłączenia serwerów Francja <-> Warszawa/LIM/Mariott łączem 10Gbps.



Budowa VDC – peering Polski obecnie

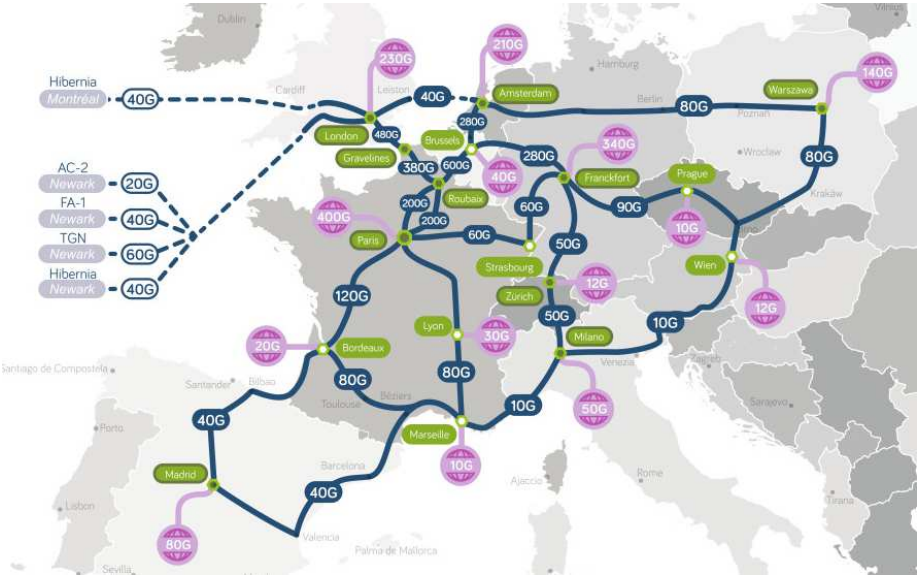






Źródła : https://en.wikipedia.org/wiki/PIONIER
http://www.geant.net

Budowa VDC – peering Polski obecnie



Źródła : https://www.ovh.com/us/about-us/network.xml
http://www.geant.net

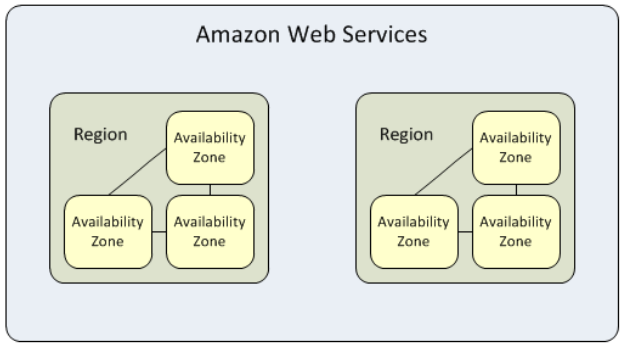
Budowa VDC – peering Polski obecnie

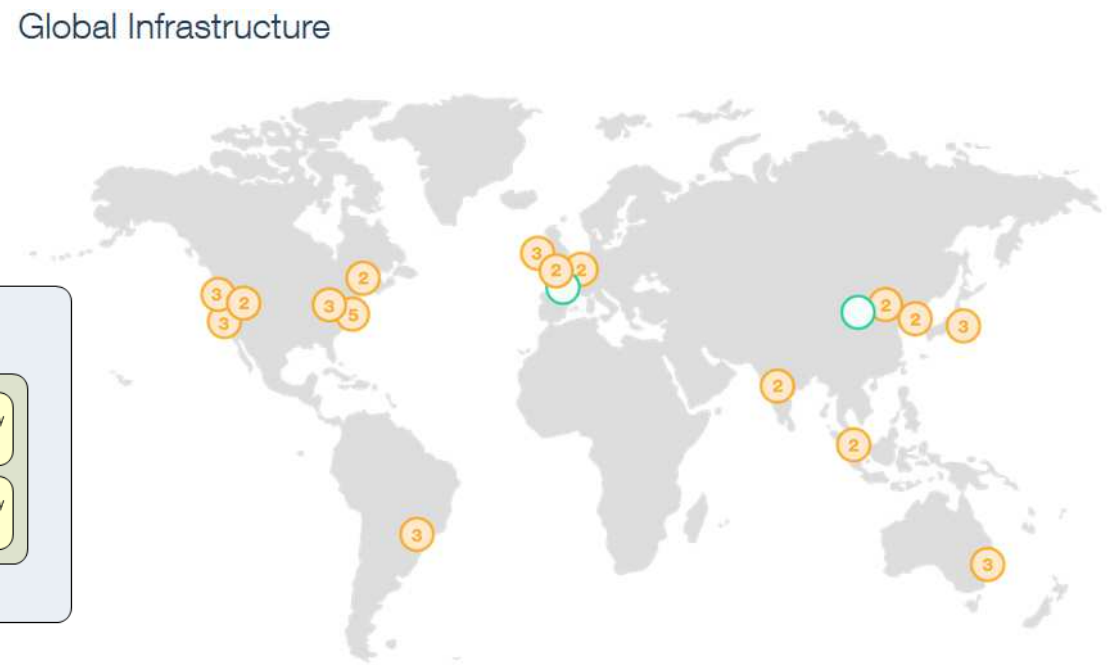
Źródło : http://www.interoute.com/interactive-network-map

Budowa VDC – peering Polski obecnie

Źródło : http://www.interoute.com/interactive-network-map

Budowa VDC – możliwości - obecnie

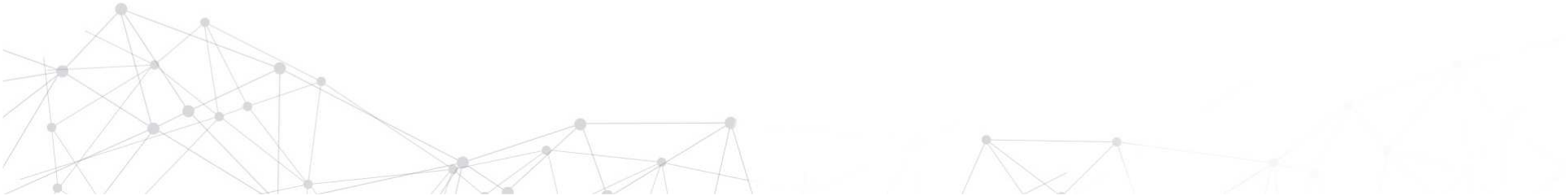




Źródło : https://aws.amazon.com/about-aws/global-infrastructure/

Budowa VDC – Trendy

- Cyberbezpieczeństwo – bezpieczeństwo kluczowych usług
- Chmura obliczeniowa – szybki wzrost migracji do chmury
- Bezpieczeństwo chmury obliczeniowej – duża dowolność
- Dostępność usługi Internet, większa liczba urządzeń, liczba danych, liczba użytkowników, liczba incydentów bezpieczeństwa
- Globalne platformy do obsługi klientów AWS, Azure, IBM, Oracle



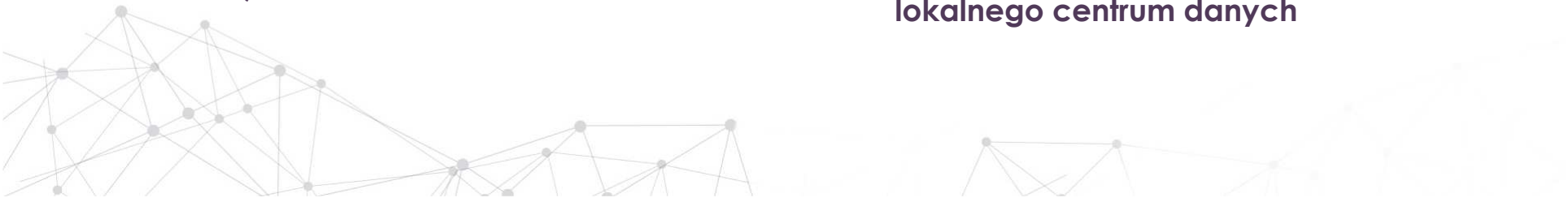
Budowa VDC – wirtualne DC vs fizyczne DC

Fizyczne centrum danych

- Strzeżony budynek
- Zasilanie redundantne, UPSy
- Łącza do sieci Internet
- Serwery fizyczne
- Przełączniki fizyczne
- Przestrzeń dyskowa, macierze
- Tier III, - Tier IV

Wirtualne Data Center

- Bazuje na zasobach fizycznego data center jednego lub wielu
- W lokalnym centrum danych na serwerach, sieci, przestrzeni dyskowej
- Jest instancją hypervisior np. ESX, OpenStack, KVM
- może zawierać elementy fizyczne lokalnego centrum danych



Budowa VDC – czym jest wirtualne Data Center

Wirtualne Centrum Danych

- **instancja hypervisior w jednym lub wielu centrach danych,**
- **może zawierać fizyczne elementy sieciowe, przestrzeń dyskową,**
- **lokalne centrum danych może rozszerzać funkcjonalność wirtualnego centrum danych,**
- **zawiera w sobie komponenty, funkcjonalność centrum danych z ~2000 roku tj. wirtualnych firewall, switch, router, serwer,**

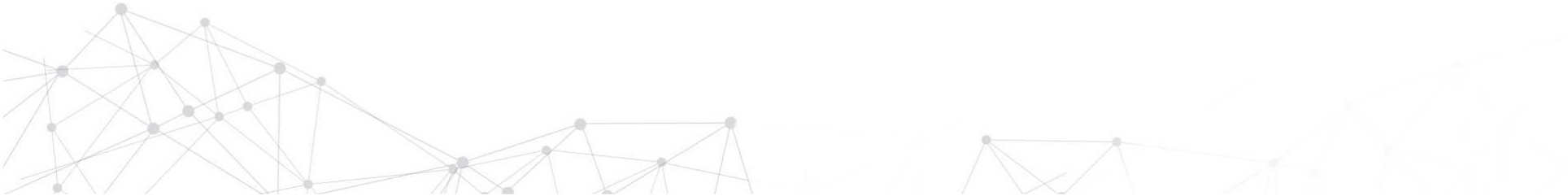
Budowa VDC – czym jest wirtualne Data Center

Wirtualne Centrum Danych

- **… wirtualny dysk, wirtualna macierz dyskowa, wirtualna karta sieciowa, wirtualny TAP, wirtualny IPS, IDS, wirtualne serwery Windows, Linux, AIX, Solaris, BSD, serwery aplikacji, serwery baz danych, instancje kopii zapasowych, systemy monitoringu, DNS, firewall bazy danych, firewall aplikacji.**
- **ograniczenia ? warunki licencyjne, wsparcie produktów.**

Budowa VDC – Open Source

- Czy da się zbudować wirtualne Centrum Danych w oparciu o Open Source ?
- Czy będzie stabilnie, wydajnie, niezawodnie ?
- Czego nie da się zbudować w oparciu o Open Source ?
- Ile to będzie kosztować ?
- Ograniczenia ?



Budowa VDC – Open Source

- Czy da się zbudować wirtualne Centrum Danych w oparciu o Open Source ? - tak
- Czy będzie stabilnie, wydajnie, niezawodnie ? - tak
- Czego nie da się zbudować w oparciu o Open Source ? - czas jest ograniczeniem.
- Ile to będzie kosztować ? – wdrożenie, rozwój oprogramowania
- Ograniczenia ? – wymagania wsparcia - komercyjne produkty

Budowa VDC – Open Source

- **Hypervisior – KVM, Open Stack, PowerKVM, bhyve/FreeBSD**
- **Kontenery – LXC (Docker), Chroot, Jail/BSD**
- **Systemy – Linux Debian, Gentoo, CentOS**
- **Bazy danych – MariaDB, PostgreSQL, MySQL,**
- **Serwery aplikacji, kontenery serwletów – Tomat, WildFly,**
- **Firewall – OpenBSD/PF, NetBSD/PF, FreeBSD/PF/IPF, Linux/IPTables,**
- **Router – Quagga, OpenBGPD, Zebra**

Budowa VDC – Open Source

- **WWW – Apache, Ngnix,**
- **Firewall Aplikacyjny – mod_security,**
- **IPS/IDS – Suricatta, Snort,**
- **Webmail – Roundcube, SOGo, Zimbra/Zarafa [Community],**
- **Serwery poczty – Postfix, Exim,**
- **Antyspam/AV – SpamAssasin, QPSMTPD, ClamAV**
- **Loadbalancer - HAProxy**

Budowa VDC – Open Source

- **Kopie zapasowe - Bacula**
- **Monitoring – Icinga, Nagios Core, Shinken,**
- **Statystyki – Ganglia, Cacti, MRTG**
- **APT – Cuckoo Sandbox**
- **iSCSI - FreeNAS**
- **Storage – CEPH, DRBD**
- **Switch - OpenVSwtich**

Budowa VDC – Komercyjne

- **Hypervisior – RHEV, Open Stack, VMWare, LDOM, LPAR/PowerVM**
- **Kontenery – Docker, Virtuozzo, Solaris/Zones, AIX/WPAR**
- **Systemy – RedHat, SuSE, IBM AIX, Oracle Solaris, MS Windows**
- **Bazy danych – Oracle, IBM DB2, PostgreSQL Enterprise**
- **Serwery aplikacji, kontenery serwletów – JBoss, IBM WLS**
- **Firewall – A10 Networks, Check Point, Palo Alto, Fortinet**
- **Router – Vyatta, Juniper, Cisco**

Budowa VDC – Komercyjne

- **WWW – Apache, Ngnix,**
- **Firewall Aplikacyjny – A10 Networks, Radware, Imperva, F5,**
- **IPS/IDS – Intel/McAfee, Juniper**
- **Webmail – Zimbra, Zarafa**
- **Serwery poczty – Exchange, Zimbra, Zarafa**
- **Antyspam/AV – Symantec**
- **Loadbalancery – A10 Networks, Radware, F5, KEMP (NLB)**

Budowa VDC – Komercyjne

- **Kopie zapasowe – Veritas, IBM Tivoli**
- **Monitoring – Nagios, FlowMon**
- **Statystyki – FlowMon**
- **APT – Blue Coat, Check Point**
- **iSCSI – EMC, IBM, Hitachi, Tintri**
- **Storage –IBM, Hitachi, Tintri**
- **Switch – VMWare NSX, Juniper, Cisco**

Budowa VDC – Komercyjne

- **Cyberbezpieczeństwo – Fidelis, FireEye, DarkTrace**
- **MDM – AirWatch**
- **DLP – Symantec DLP**
- **Klastry – PowerHA, Veritas VCS**
- **TAPy – Gigamon**
- **Nagrywanie sesji administracyjnych – Balabit, CyberArk, Wheel**
- **Firewall DB / anonimizacja danych w DB – Imperva,**

Budowa VDC – Open Source vs Komercyjne

Komercyjne

+ wsparcie producentów

- wykluczenia platform

- licencje / core factor

+ wyższe prawdopodobieństwo dotrzymania SLA – banki, telco

Open Source

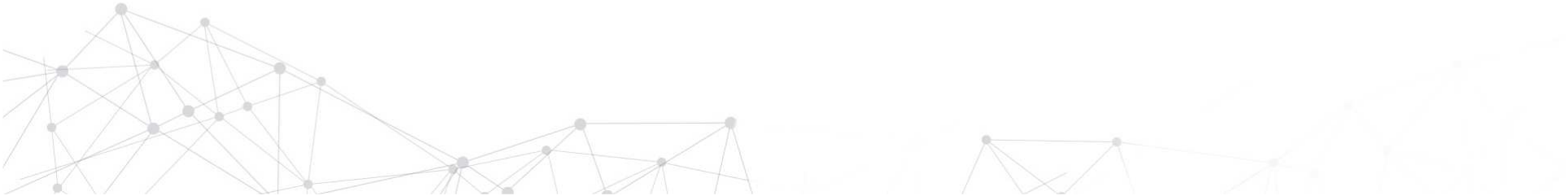
- własny rozwój

+ nowe środowiska bez licencji

- brak wsparcia

+ często szybkie poprawki

- interfejsy graficzne



Najciekawsze Open Source i technologie

- KVM i PowerKVM na IBM/Power
- Ganglia
- VPN – Racoon
- OpenvSwitch
- OpenStack
- Nested Virtualization
- SR-IOV

Najciekawsze Open Source i technologie

- ## KVM, SR-IOV, Linux Kernel, NUMA

numastat –c qemu / sprawdzamy procesy które korzystają z NUMA, NODE1 (CPU1) / NODE2 (CPU2)

```
root@asus1:~# numastat -c qemu
Found no processes containing pattern: "qemu"

Per-node numastat info (in MBs):
                Node 0 Node 1 Total
                ------ ------ -----
Numa_Hit          1835   4186  6021
Numa_Miss           50    205   256
Numa_Foreign        50    205   256
Interleave_Hit     231    231   463
Local_Node        1835   4186  6021
Other_Node           0      0     0
```

Włączamy w Kernelu dla dwóch, dwuportowych kart sieciowych funkcję SR-IOV

```
echo 7 > /sys/devices/pci0000:00/0000:00:02.0/0000:02:00.0/sriov_numvfs
echo 7 > /sys/devices/pci0000:00/0000:00:02.0/0000:02:00.1/sriov_numvfs
echo 7 > /sys/devices/pci0000:80/0000:80:02.0/0000:83:00.0/sriov_numvfs
echo 7 > /sys/devices/pci0000:80/0000:80:02.0/0000:83:00.1/sriov_numvfs
```

Najciekawsze Open Source i technologie

- ## KVM, SR-IOV, Linux Kernel, NUMA

fragment polecenia : dmesg

```
[  311.218028] pci 0000:83:11.5: [8086:10ca] type 00 class 0x020000
[  311.218073] pci 0000:83:11.5: Max Payload Size set to 256 (was 128, max 512)
[  311.218971] iommu: Adding device 0000:83:11.5 to group 78
[  311.219801] igbvf 0000:83:11.5: enabling device (0000 -> 0002)
[  311.221827] igbvf 0000:83:11.5: PF still in reset state. Is the PF interface up?
[  311.222578] igbvf 0000:83:11.5: Assigning random MAC address.
[  311.224510] igbvf 0000:83:11.5: PF still resetting
[  311.243710] igbvf 0000:83:11.5: Intel(R) 82576 Virtual Function
[  311.244478] igbvf 0000:83:11.5: Address: 3a:e8:da:e1:7e:11
[  311.244500] igbvf 0000:83:11.5 enp131s17f5: renamed from eth2
[  311.246032] igb 0000:83:00.1: 7 VFs allocated
```

Izolowanie vCPU / Core w Linux np. na potrzeby KVM i pinowania vCPU do VM w KVM

```
GRUB_CMDLINE_LINUX="clocksource=acpi_pm nousb intel_iommu=on isolcpus=4-11"
```

„Remove the specified CPUs, as defined by the cpu_number values, from the general kernel SMP balancing and scheduler algroithms.”

Źródło : http://www.linuxtopia.org/online_books/linux_kernel/kernel_configuration/re46.html

Więcej informacji : https://codywu2010.wordpress.com/2015/09/27/isolcpus-numactl-and-taskset/

Najciekawsze Open Source i technologie

ifconfig –a | grep –i enp | grep –i enp2s

```
root@asus1:~# ifconfig -a | grep -i enp | grep -i enp2s
enp2s16: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s17: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
enp2s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
enp2s16f1: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s16f2: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s16f3: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s16f4: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s16f5: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s16f6: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s16f7: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s17f1: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s17f2: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s17f3: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s17f4: flags=4098<BROADCAST,MULTICAST>  mtu 1500
enp2s17f5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

```
<hostdev mode='subsystem' type='pci' managed='yes'>
  <source>
    <address domain='0x0000' bus='0x02' slot='0x10' function='0x1'/>
  </source>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
</hostdev>
```

portu SR-IOV do KVM

Najciekawsze Open Source i technologie

```
root@asus1:~# virsh start vsys19
Domain vsys19 started
```

virsh start vsys19

numastat – c qemu

```
root@asus1:~# numastat -c qemu

Per-node process memory usage (in MBs) for PID 5810 (qemu-system-x86)
         Node 0 Node 1 Total
         ------ ------ -----
Huge          0      0     0
Heap         42      0    42
Stack         0      0     0
Private   28775      3 28778
-------  ------ ------ -----
Total     28817      3 28820
root@asus1:~# ps -ef | grep -i 5810
libvirt+  5810     1 76 18:51 ?        00:00:58 qemu-system-x86_64 -enabl
```

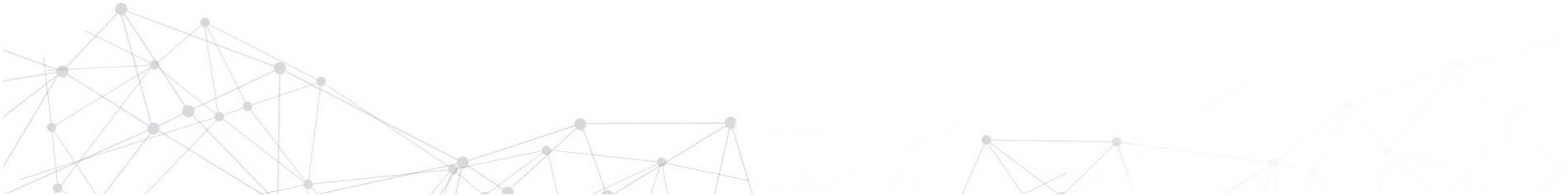
…

```
0,addr=0x2 -device vfio-pci,host=02:10.1,id=hostdev0,bus=pcie.0,addr=0x3
```

Najciekawsze Open Source i technologie

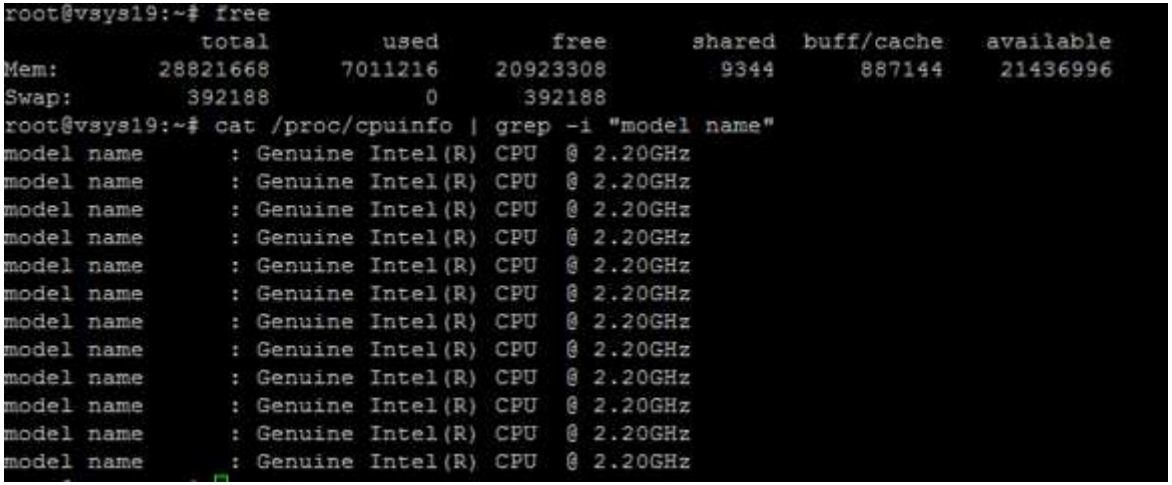
fragment konfiguracji xml wirtualnej maszyny KVM

```
<memory unit='KiB'>29360128</memory>
<currentMemory unit='KiB'>29360128</currentMemory>
<vcpu placement='static'>12</vcpu>
<numatune>
  <memory mode='preferred' nodeset='0'/>
</numatune>
<os>
  <type arch='x86_64' machine='pc-q35-2.7'>hvm</type>
  <boot dev='hd'/>
</os>
<features>
  <acpi/>
  <apic/>
  <pae/>
</features>
<cpu mode='host-passthrough'/>
```



Najciekawsze Open Source i technologie

wirtualna maszyna KVM, wynik poleceń free i cat /proc/cpuinfo



Najciekawsze Open Source i technologie

numastat –c qemu / po uruchomieniu kilku maszyn wirtualnych KVM

```
root@asus1:~# numastat -c qemu

Per-node process memory usage (in MBs)
PID              Node 0 Node 1  Total
---------------  ------ ------ ------
7756 (qemu-syste  28837      3  28841
7844 (qemu-syste  16582      3  16585
7925 (qemu-syste  16590      3  16594
8001 (qemu-syste     17  16575  16592
8078 (qemu-syste     15  16567  16582
8232 (qemu-syste  28918      3  28921
8330 (qemu-syste  12349     16  12366
8469 (qemu-syste   4149     25   4174
8583 (qemu-syste   4295      3   4298
8662 (qemu-syste     16   4271   4287
8732 (qemu-syste     14   4152   4166
8820 (qemu-syste     14  12349  12363
---------------  ------ ------ ------
Total           111798  53970 165768
```

```
root@asus1:~# virsh list
 Id    Name                           State
----------------------------------------------------
 2     vsys19                         running
 3     vsys31a                        running
 4     vsys31b                        running
 5     vsys31c                        running
 6     vsys31d                        running
 7     vsys19b                        running
 8     db1                            running
 9     db2                            running
 10    db3                            running
 11    db4                            running
 12    vsys29                         running
 13    vsys30                         running
```

Najciekawsze Open Source i technologie

Reprezentacja portu karty SR-IOV w hoście KVM

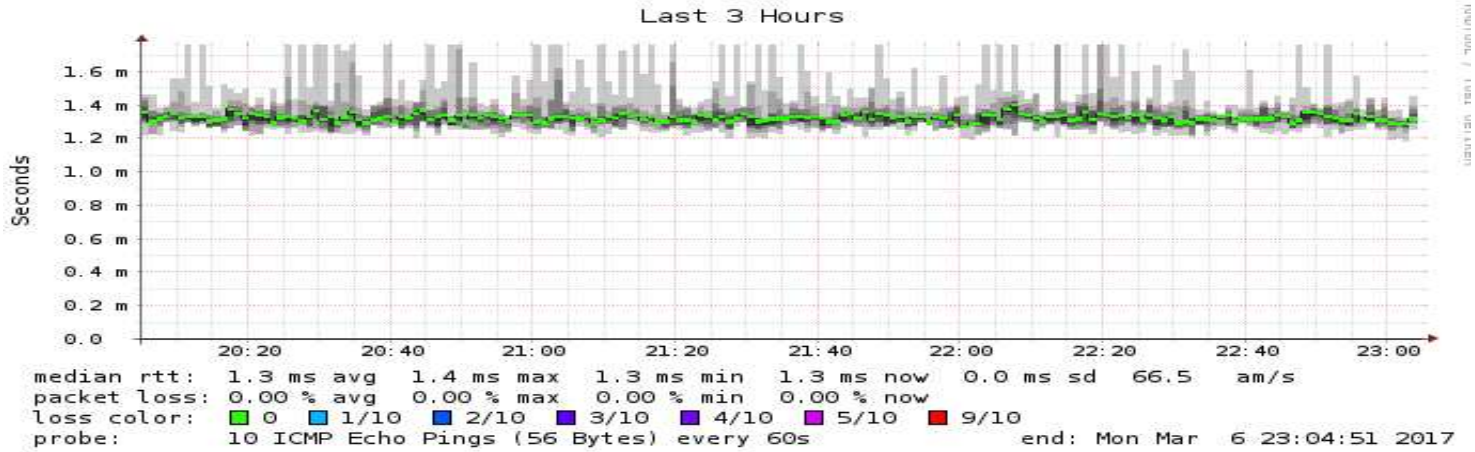
```
root@vsys19:~# dmesg | grep -i igb
[    2.256920] igbvf: Intel(R) Gigabit Virtual Function Network Driver - version 2.0.2-k
[    2.256923] igbvf: Copyright (c) 2009 - 2012 Intel Corporation.
[    2.312097] igbvf 0000:00:03.0: PF still in reset state. Is the PF interface up?
[    2.312099] igbvf 0000:00:03.0: Assigning random MAC address.
[    2.332102] igbvf 0000:00:03.0: PF still resetting
[    2.333093] igbvf 0000:00:03.0: Intel(R) 82576 Virtual Function
[    2.333095] igbvf 0000:00:03.0: Address: 9e:1e:60:1a:dc:7d
[    8.156098] igbvf 0000:00:03.0: Link is Up 1000 Mbps Full Duplex
```

mtr –r –c 20 137.74.124.254 / z host KVM / SR-IOV (0.2ms) – łącze Fiber/Orange do OVH (3,7-4.5ms)

```
root@vsys19:~# mtr -r -c 20 137.74.124.254
Start: Mon Mar  6 20:05:00 2017
HOST: vsys19                      Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.55.20.65               0.0%    20    0.2   0.2   0.1   0.2   0.0
  2.|-- 10.50.61.52               0.0%    20    2.2   3.0   2.1   4.0   0.3
  3.|-- 10.50.61.1                0.0%    20    4.0   3.4   2.3   4.5   0.2
  4.|-- 137.74.1.252              0.0%    20    3.4   3.8   2.5   4.9   0.4
  5.|-- 10.95.97.14               0.0%    20    4.6   3.4   2.6   4.6   0.4
  6.|-- 137.74.124.254            0.0%    20    3.7   3.4   2.2   4.5   0.4
```

Najciekawsze Open Source i technologie

http://waw.smokeping.ovh.net/smokeping?filter=Orange;target=EU.AS5617

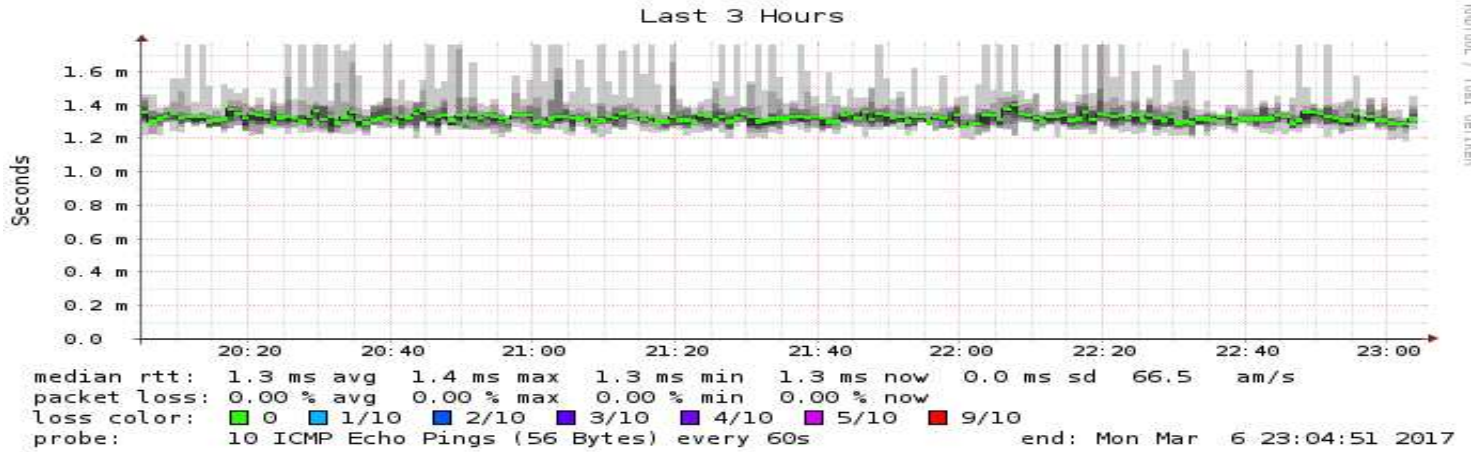


Traceroute - [History]

```
traceroute to 80.50.248.79 (80.50.248.79), 40 hops max, 60 byte packets  -  Generated at 2017-03-06 23:00:02

 1 > 137.74.124.254                    (137.74.124.254)  [AS16276]  0.117ms    0.171ms    0.123ms
 2 > 10.95.97.0                        (10.95.97.0)      [*]        0.240ms    0.190ms    0.110ms
 3 > be100-1068.var-5-a9.pl.eu         (213.186.32.202)  [AS16276]  0.637ms    0.590ms    0.983ms
 4 >
 5 > war-ar8.tpnet.pl                  (195.117.0.10)    [AS5617]   0.660ms    0.649ms    0.625ms
 6 > 80.50.248.67                      (80.50.248.67)    [AS5617]   1.015ms    1.003ms    0.982ms
 7 > lg.tpnet.pl                       (80.50.248.79)    [AS5617]   1.171ms    1.275ms    1.251ms
```

Najciekawsze Open Source i technologie

http://waw.smokeping.ovh.net/smokeping?filter=Orange;target=EU.AS5617

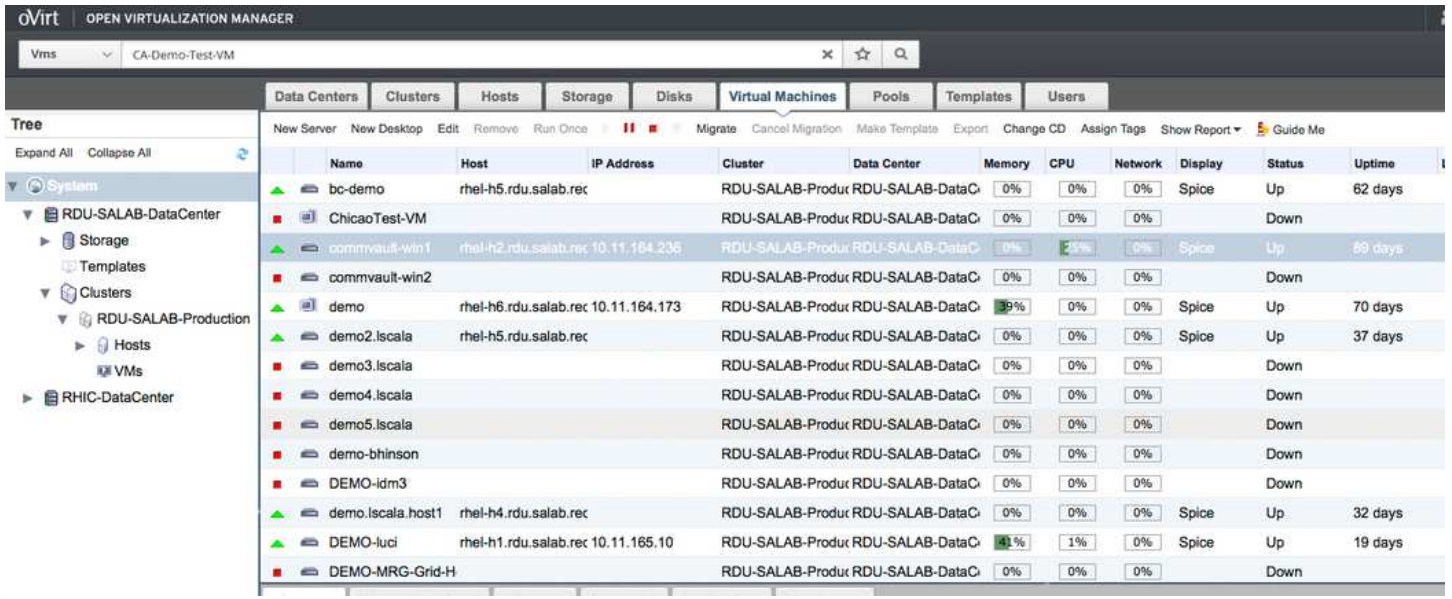


Traceroute - [History]

```
traceroute to 80.50.248.79 (80.50.248.79), 40 hops max, 60 byte packets  -  Generated at 2017-03-06 23:00:02

 1 > 137.74.124.254                    (137.74.124.254)  [AS16276]  0.117ms    0.171ms    0.123ms
 2 > 10.95.97.0                        (10.95.97.0)      [*]        0.240ms    0.190ms    0.110ms
 3 > be100-1068.var-5-a9.pl.eu         (213.186.32.202)  [AS16276]  0.637ms    0.590ms    0.983ms
 4 >
 5 > war-ar8.tpnet.pl                  (195.117.0.10)    [AS5617]   0.660ms    0.649ms    0.625ms
 6 > 80.50.248.67                      (80.50.248.67)    [AS5617]   1.015ms    1.003ms    0.982ms
 7 > lg.tpnet.pl                       (80.50.248.79)    [AS5617]   1.171ms    1.275ms    1.251ms
```

Najciekawsze Open Source i technologie

oVirt – GUI / zarządzanie m.in. KVM. Inne GUI dla KVM libvirt to np.: virt-manager



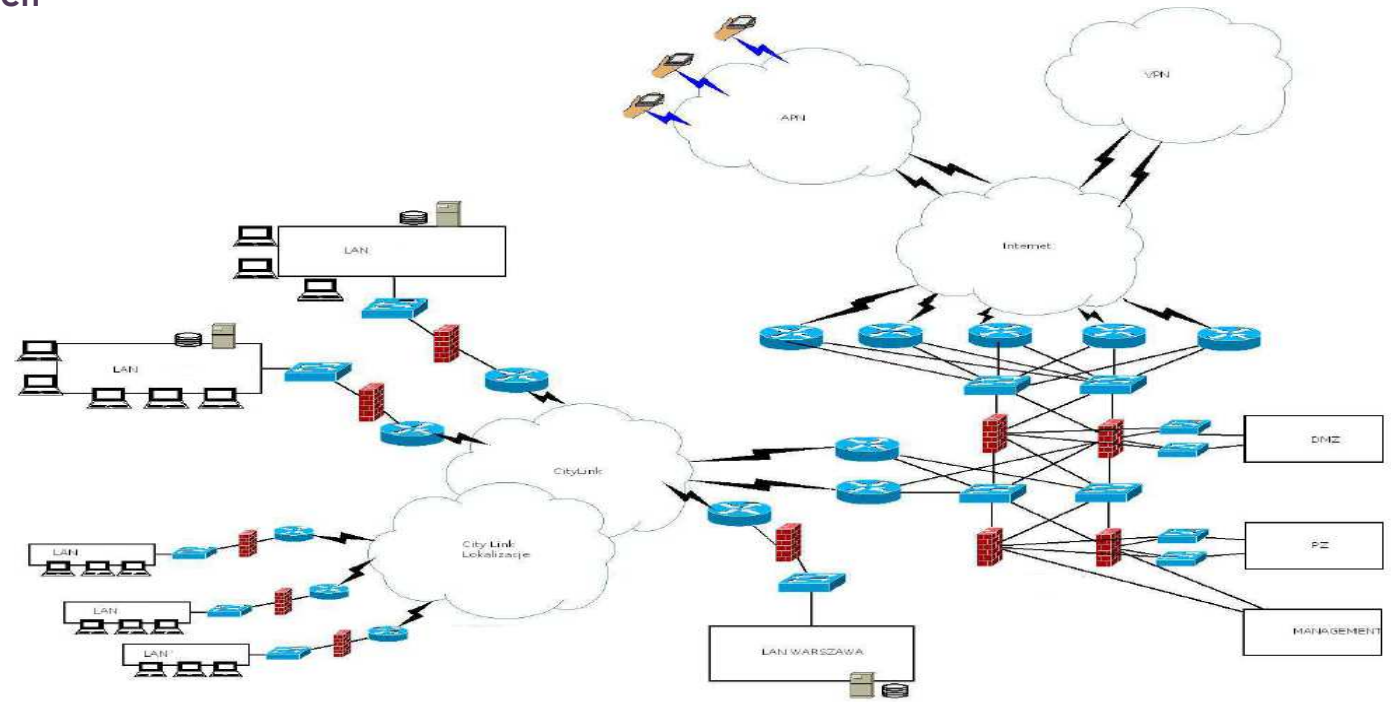
Źródło : https://blog.yvonet.com

Budowa VDC – UseCase

Migracja obecnych

usług do nowej

architektury

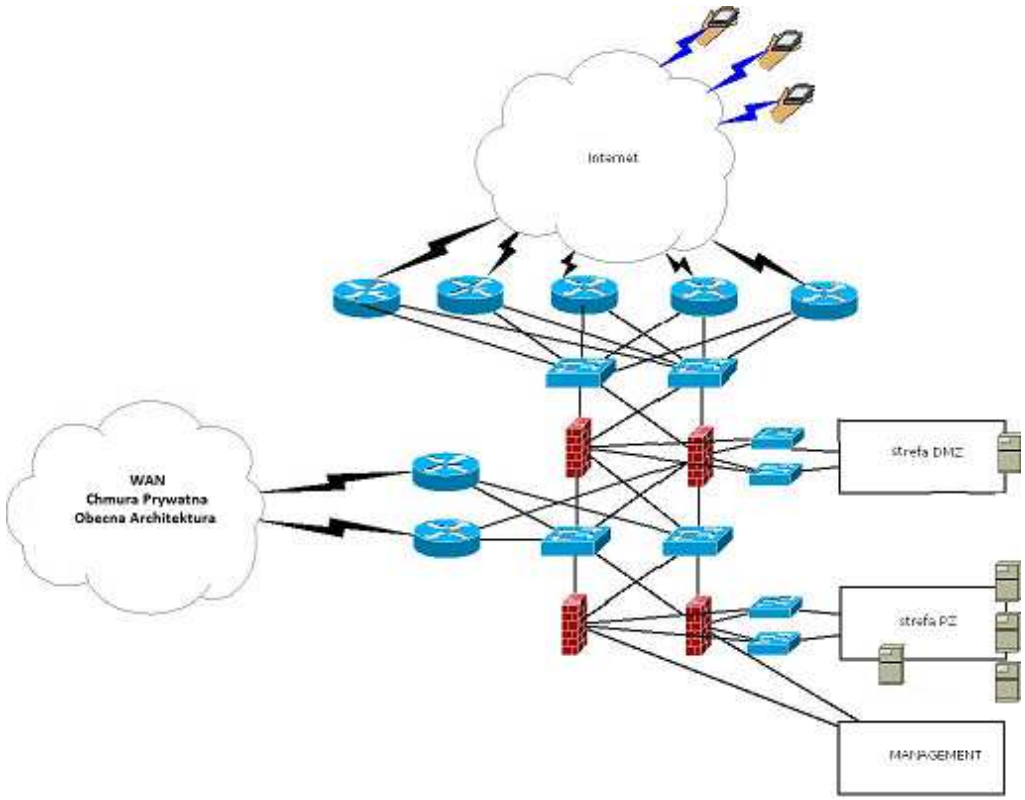


Budowa VDC – UseCase

Szybka budowa

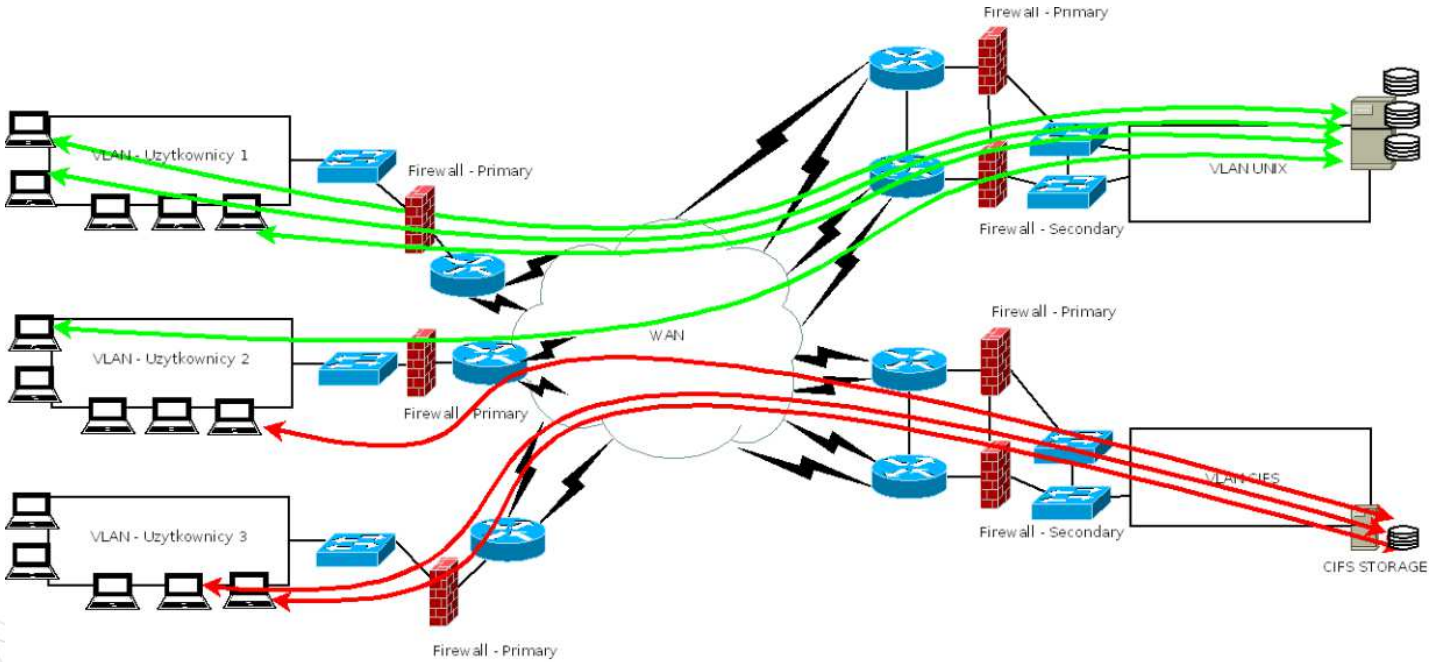
nowego styku

z siecią Internet



Budowa VDC – UseCase

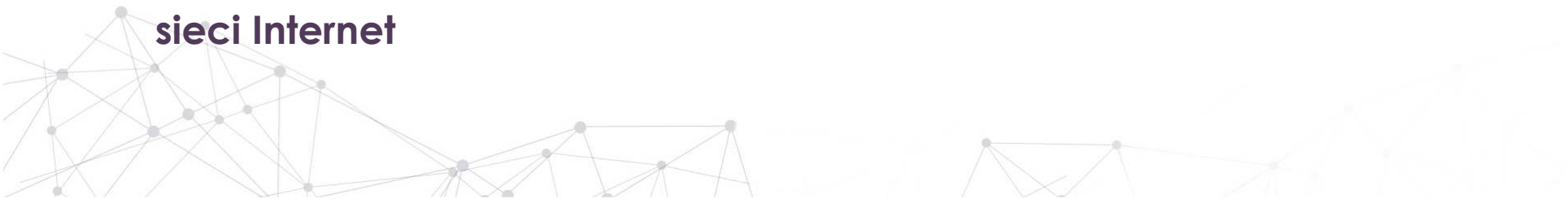
Szybka budowa środowiska developerskiego



Budowa VDC – Migracja

Migracje – do chmury, z chmury, kolokacji, hostingu

- **Klasyfikacja usług**
- **Czas życia projektu**
- **Lokalizacja i bezpieczeństwo DC,**
- **Dostępność łączy do sieci Internet.**
- **Procesory, pamięć RAM, przestrzeń dyskowa, sieć – szybkie łącza do sieci Internet**



Budowa VDC – Migracja

- Power8 24C, 512GB RAM, 750Mbps 1 500 USD/m (online.net)
- Xeon 24C (E5-2690v3), 256GB RAM, 500Mbps ~860 USD/m
- ARM 12C, 24GB RAM, 100Mbps 20 USD/m (beta projekt)
- Oracle T5 (?)
- Obecnie Oracle Cloud M7, IBM Cloud (Power8), Azure/AWS – x86
- Tanie alternatywy do nauki – SoYouStart, Kimsufi.

klasyczne bezpieczeństwo wymaga przeniesienia części funkcjonalności do chmury

świadome przeniesienie odpowiedzialności za część usług na dostawcę chmury obliczeniowej, monitorowanie, zarządzanie, backup

Budowa VDC – Projekt Techniczny

Główne strefy bezpieczeństwa :

- **siec INET.**
- **sieci DMZ.**
- **sieci PZ.**
- **siec CORE.**
- **siec BACKUP.**
- **siec MGMT.**
- **siec WAN.**

Elementy infrastruktury konieczne

do budowy bezpiecznego

ośrodka obliczeniowego :

- **Połączenia głownie 10Gbps (PROD, BACKUP).**
- **Połączenia management 1Gbps.**
- **Separacja sieciowa stref funkcjonalnych tj. PROD, MGMT, BACKUP.**

Budowa VDC – Projekt Techniczny

- Zapasowy ośrodek obliczeniowy
- Połączenie ośrodków dwoma niezależnymi łączami (szyfrowanie L2).
- Architektura sieciowa – bezpieczeństwa – zdefiniowanie i nazwanie najważniejszych stref
- Architektura sieciowa – schemat główny – wysoki poziom
- Architektura sieciowa.
- Główne założenia polityki bezpieczeństwa
- Główne założenia dot. bezpieczeństwa – standardy.
- Główne założenia dot. bezpieczeństwa – rekomendacje.
- Warstwa sieciowa – szkielet rozwiązania.
- Routery brzegowe – styk z siecią Internet.
- Routery brzegowe – styk z siecią WAN.
- Switche brzegowe.

Budowa VDC – Projekt Techniczny

- Firewalle brzegowe styk z siecią Internet.
- Firewalle brzegowe styk z siecią WAN.
- Firewalle wewnętrzne – ochrona sieci PZ, MGMT.
- Systemy czasu.
- Systemy autoryzacji.
- Systemy Firewall Zewnętrzne DMZ.
- Systemy Firewall Wewnętrzne DMZ.
- Systemy Firewall Zewnętrzne PZ.
- Systemy Firewall Wewnętrzne PZ.
- Systemy Firewall WAN.
- Systemy Firewall INET.

Budowa VDC – Projekt Techniczny

- Systemy wirtualizacji DMZ.
- Systemy wirtualizacji PZ.
- Systemy monitoringu.
- Systemy logowania zdarzeń (osobne dla stref DMZ i PZ).
- Systemy proxy.
- Systemy WAF.
- Systemy IDS/IPS.
- Systemy TAP.
- Systemy SIEM.
- Systemy terminacji tuneli VPN – użytkownicy.
- Systemy terminacji tuneli VPN – inne firmy (ew. dedykowane łącza).

Budowa VDC – Projekt Techniczny

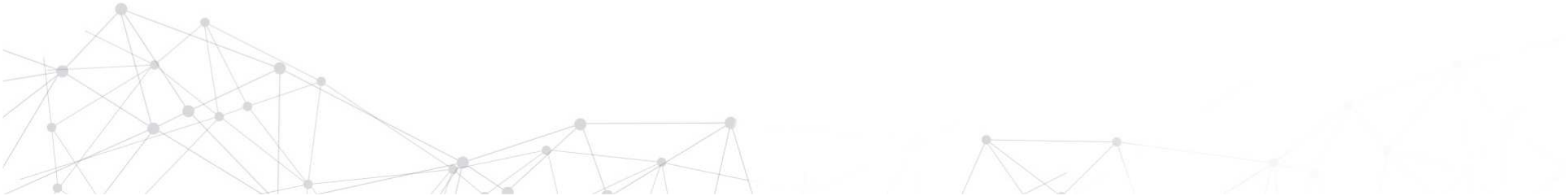
- Systemy terminacji tuneli VPN – połączenia WAN (inne lokalizacje).
- Systemy Firewall DB.
- Systemy backupu konfiguracji.
- Systemy DNS.
- Switche storage SAN DMZ.
- Switche storage SAN PZ.
- Switche storage SAN Interconnect DR (DWDM).
- Switche LAN Interconnect DR (DWDM).
- Switche LAN – szkielet CORE.
- Switche LAN – szkielet DMZ.
- Switche LAN – szkielet PZ.

Budowa VDC – Projekt Techniczny

- Switche LAN – szkielet WAN.
- Switche LAN – szkielet INET.
- Switche LAN – szkielet MGMT (każda sieć funkcjonalna musi posiadać osobną strefę MGMT realizowana na osobnych fizycznych przełącznikach).
- Switche LAN – szkielet BACKUP.
- Switche LAN – akceleracja i wsparcie wirtualizacji DMZ
- Switche LAN – akceleracja i wsparcie wirtualizacji PZ
- Macierze dyskowe DMZ (układ HA).
- Macierze dyskowe PZ (układ HA).
- Systemy równoważenia obciążenia (load balancers).
- Systemy optymalizacji ruchu TCP.

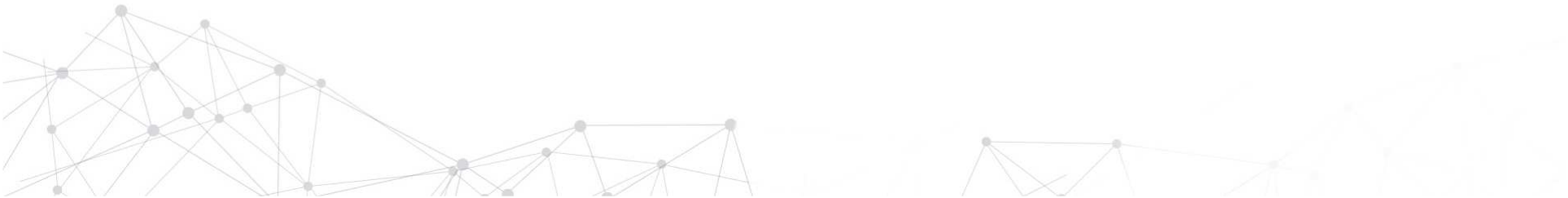
Budowa VDC – Projekt Techniczny

- Systemy akceleracji ruchu.
- Systemy anty DDOS (Internet).
- Centralny system DLP.
- Centralny system AV.
- Systemy APT.
- Systemy automatycznych audytów bezpieczeństwa.
- Systemy analizy sum kontrolnych.
- Systemy analizy NetFlow.
- Systemy akceleracji SSL.
- Systemy ReverseProxy.

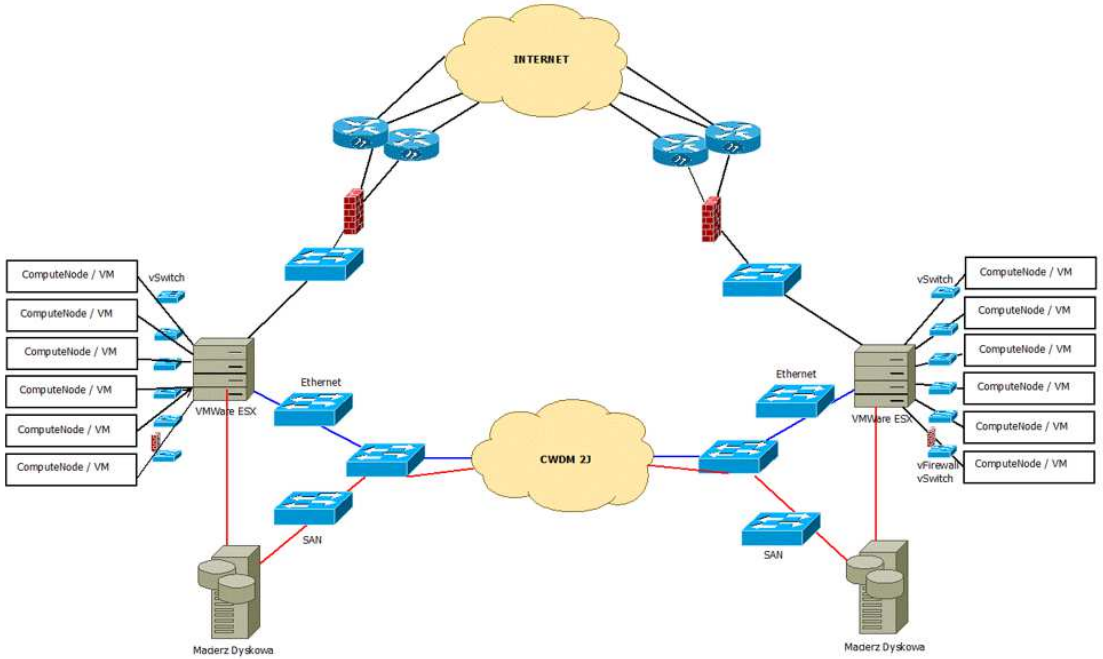


Budowa VDC – Projekt Techniczny

- Systemy deszyfracji SSL.
- Akceleratory aplikacyjne.
- Systemy QoS.
- Systemy kompresji i cache HTTP.
- Systemy nagrywania ruchu IP.
- Dedykowana infrastruktura do obsługi VoIP.
- Centralny system utrzymania i kontroli nad kontami użytkowników w systemach.



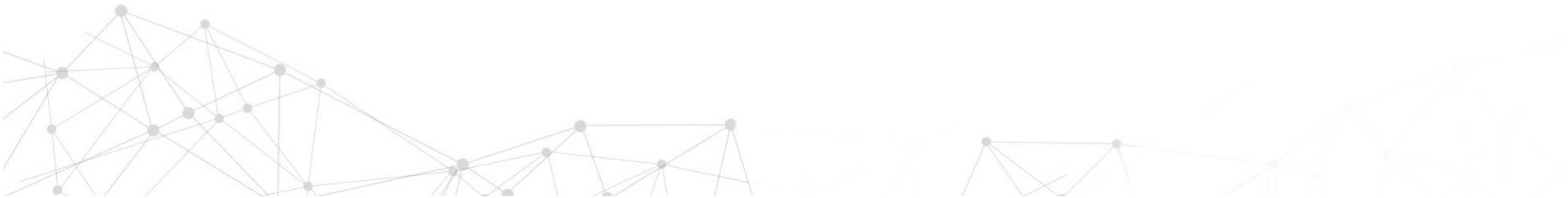
Budowa VDC – Projekt Techniczny



Dwie architektury wirtualnego data center – połączone w jedno środowisko.

Budowa VDC – Open Source DC

- zapraszam do współpracy przy budowie projektu wirtualnego centrum danych w oparciu o technologie Open Source,
- darmowa alternatywa dla startup, organizacji non-profit,
- rozwój, testy do dużych projektów, stosujących technologie Open Source



Budowa VDC – Open Source DC - OpenBSD

- **OpenBSD – www.openbsd.org / obecnie 6.1**
- **CARP (***Common Address Redundancy Protocol)* **+ pfsync**
- **Packet Filter, AuthPF**
- „Only two remote holes in the default install, in a heck of a long time!"
- New vmmci(4) VMM control interface / Support for Linux guest VMs.

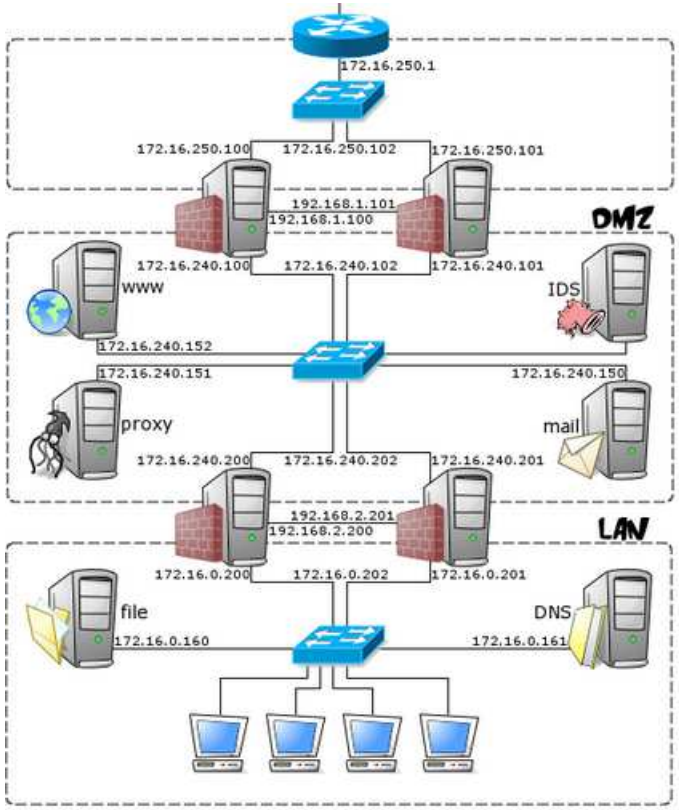
Budowa VDC – Open Source DC - OpenBSD

- Przykład architektury opartej

o Firewall OpenBSD / klastry z CARP

- Projekt OpenBSD skoncentrowany

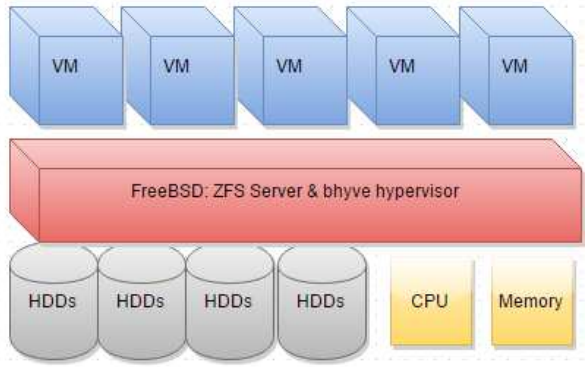
na bezpieczeństwie



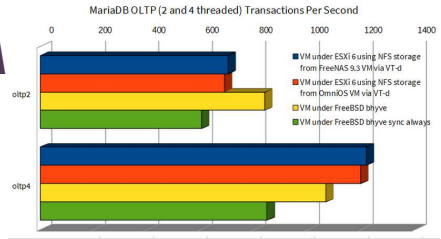
Źródło : http://www.kernel-panic.it/openbsd/carp/carp2.html

Budowa VDC – Open Source DC – bhyve / FreeBSD

- bhyve – www.bhyve.org (obecnie FreeBSD 10.3/11)
- start od FreeBSD 7.2/8.1 ~2011
- BHyVe – a Native FreeBSD Hypervisor
- funkcjonalny system z kernelem BSD
- Firewall, WWW, LB, VM
- GNU/kFreeBSD



Simpler bhyve design



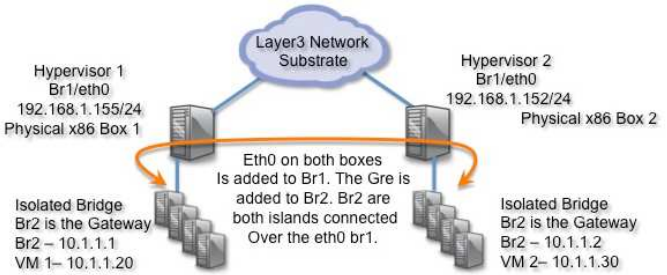
Żródło : https://b3n.org/vmware-vs-bhyve-performance-comparison/

Budowa VDC – Open Source DC - KVM

- **KVM – www.linux-kvm.org**
- **19/04/2017 v2.9 http://wiki.qemu-project.org/ChangeLog/2.9**
- virtio-crypto „The crypto subsystem now includes support for HMAC algorithms, which are used in virtio-crypto."
- **obsługa wielu systemów operacyjnych Windows, Linux, BSD**
- **obsługa NUMA, SR-IOV**
- **alternatywa PowerKVM na serwerach IBM Power**

Budowa VDC – Open Source DC – Open vSwitch

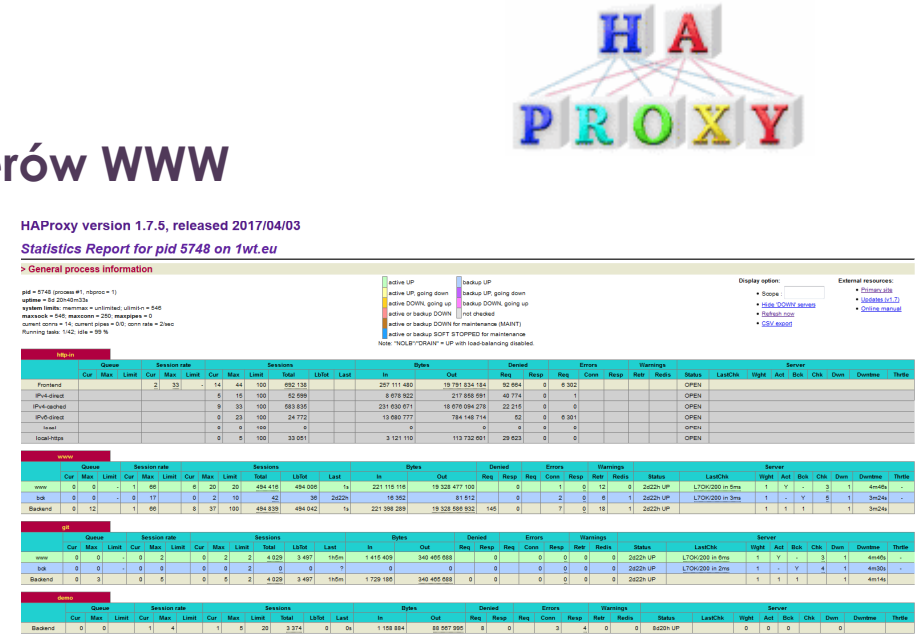
- **Open vSwitch – openvswitch.org**
- alternatywa dla bridge w Linux
- obsługa VLAN, SPAN Port, VxLAN
- możliwość połączenia 2 lokalizacji w L2
- prosta konfiguracja
- ovs-vsctl add-br ovs-lan0; ovs-vsctl add-port ovs-lan0 eth-x



źródło : http://networkstatic.net/open-vswitch-gre-tunnel-configuration/

Budowa VDC – Open Source DC – HAProxy

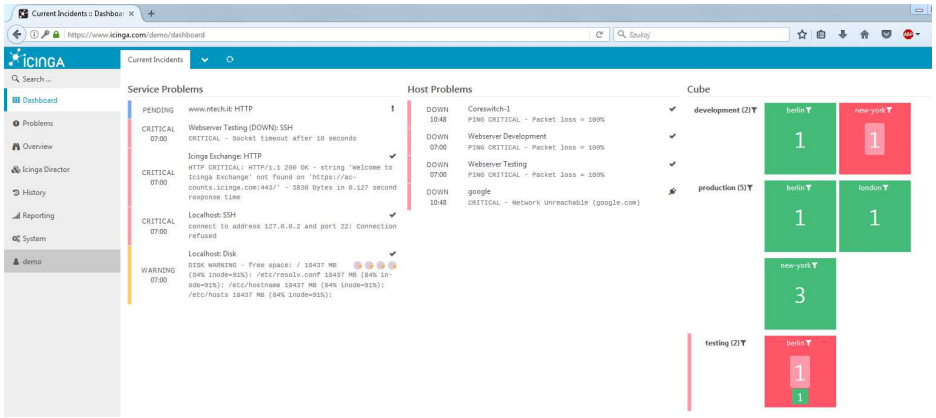
- **HAProxy– hdproxy.org**
- **Load Balancer nie tylko dla serwerów WWW**
- TCP/HTTP Load Balancer
- roundrobin, latestconn, source
- aplikacje, bazy danych



źródła : http://demo.haproxy.org/
https://www.digitalocean.com/community/tutorials/an-introduction-to-haproxy-and-load-balancing-concepts

Budowa VDC – Open Source DC – ICINGA

- ICINGA – icinga.com
- darmowy monitoring fork Nagios
- obsługa konfiguracji z Nagios



Budowa VDC – Open Source DC – Shinken

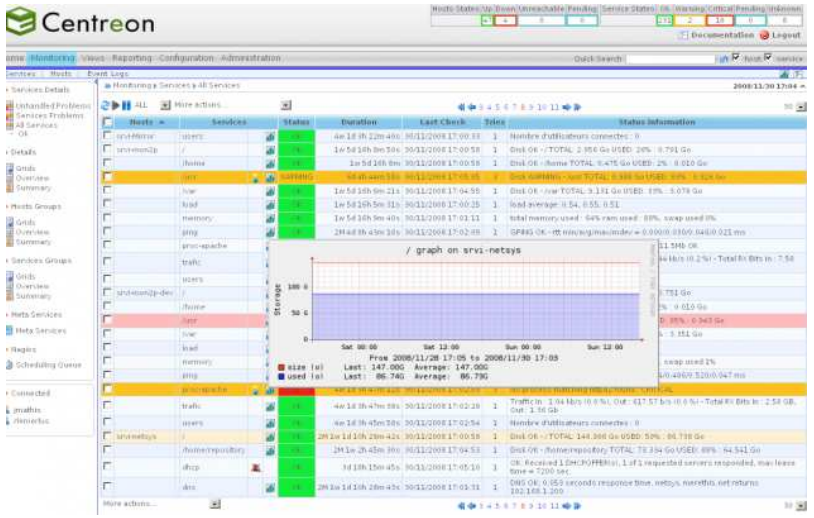
- **Shinken – shinken-monitoring.org**
- darmowy monitoring
- wspiera rozproszone architektury

tj. separacje sieciową WAN/DMZ/Core

idealny jako lekki alternatywny

system monitoringu

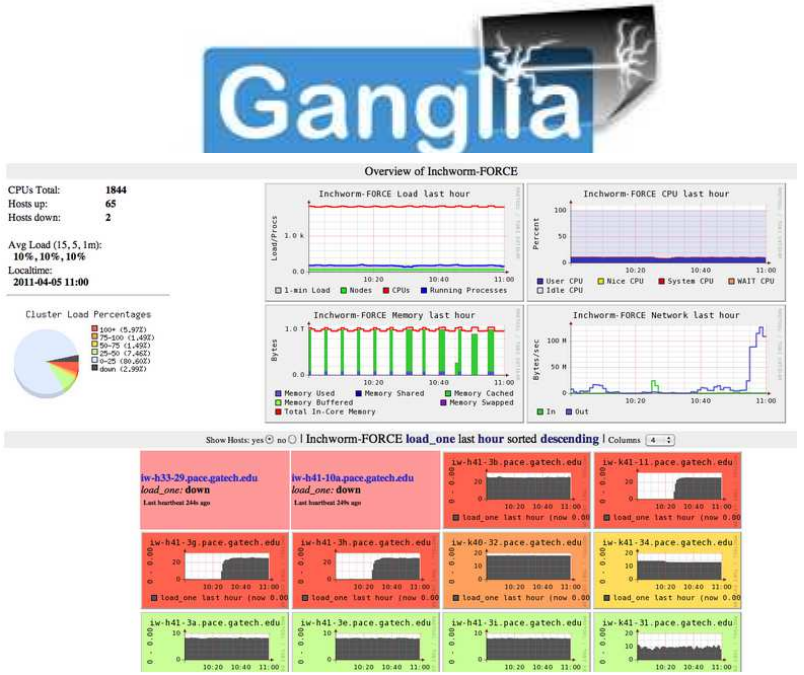
- Shinken + Centreon



Źródło : http://shinken.readthedocs.io/en/latest/11_integration/centreon.html

Budowa VDC – Open Source DC – Ganglia

- Ganglia – ganglia.sourceforge.net
- alternatywa dla LPAR2RRD na AIX
- statystyki dla dużych architektur
- agregacja, prezentacja klastry,
- pakiety dla Linux, AIX

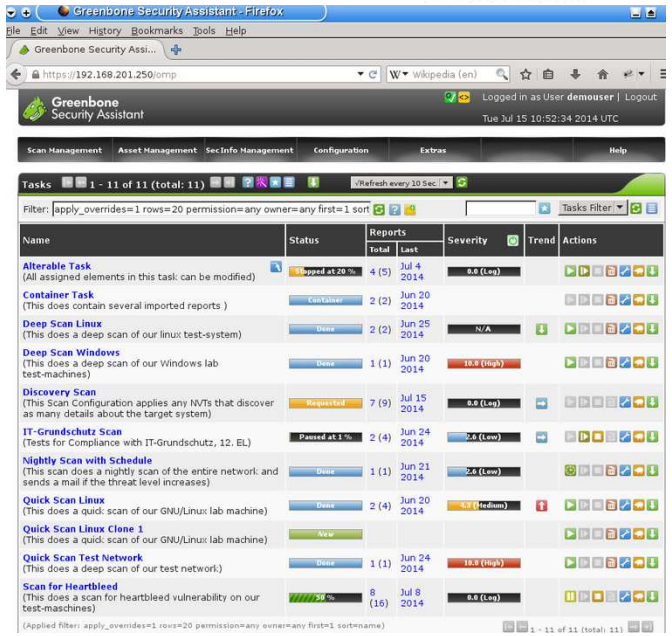


źródło : http://www.pace.gatech.edu/cluster-performance-monitoring

Budowa VDC – Open Source DC – OpenVAS

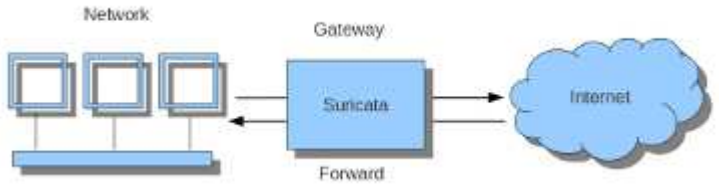
- OpenVAS – openvas.org
- alternatywa darmowa dla Nessus
- możliwa kompilacja na Linux@IBM_Power
- automatyczne testy podstawowych

podatności skany zewnętrzne/wewnętrzne



Budowa VDC – Open Source DC – Suricata

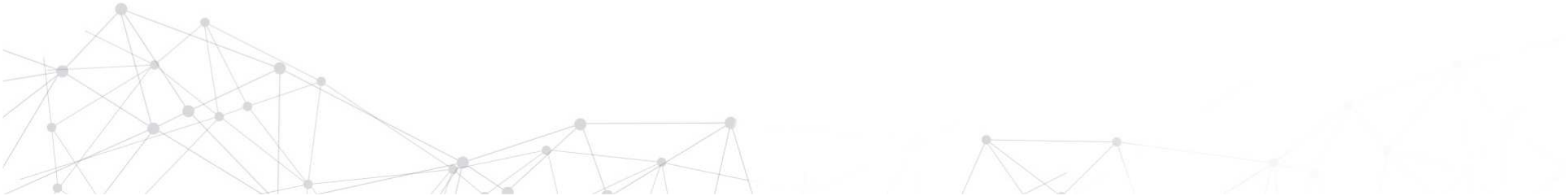
- Suricata – suricata-ids.org
- IPS/IDS
- możliwość połączenia z TAP na Open vSwitch
- dobre uzupełnienie Apache + mod_security + Cuckoo
- możliwość pracy w IPS/inline
- Możliwość akceleracji GPU



źródła : https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Setting_up_IPSinline_for_Linux
https://www.sans.org/reading-room/whitepapers/intrusion/open-source-ids-high-performance-shootout-35772

Budowa VDC – Open Source DC – Racoon2

- Racoon2 http://www.racoon2.wide.ad.jp/w/?TheRacoon2Project
- VPN/IPSEC – protokoły ESP, UDP/500
- prosta konfiguracja, obsługa kluczy x.509, DPD, NAT-T
- konfiguracje „road-warrior” dla lokalizacji z dynamicznymi-IP
- alternatywa dla StronSwan* od kernela ~2.5.56
- Linux / FreeBSD



Budowa VDC – Open Source DC – Racoon2

- $mtr www.ovh.pl (przez tunnel VPN terminowany w VPS/OVH - SBG)
- Transmisja PL/WAW -> FR/SGB

```
                             My traceroute  [v0.86]
vsys31a (0.0.0.0)                                Thu Apr 20 14:31:42 2017
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                 Packets               Pings
 Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.55.20.61                 0.0%    13    0.3   0.3   0.2   0.9   0.0
 2. 223.ip-92-222-84.eu         0.0%    13   25.5  25.9  25.0  27.0   0.4
 3. old.zk-1.sbg.spinoff.ovh.net 0.0%   13   27.2  26.2  24.9  27.2   0.4
 4. 164.132.232.222             0.0%    13   26.4  26.1  25.2  27.2   0.4
 5. 51.255.186.254              0.0%    13   25.6  26.1  25.1  27.1   0.4
 6. 10.99.168.209               0.0%    13   27.5  26.1  25.1  27.5   0.6
 7. be1-120.sbg-g2-a9.fr.eu     0.0%    13   26.5  26.1  24.9  27.1   0.5
 8. vl1251.rbx-g2-a75.fr.eu     0.0%    13   35.0  35.0  34.1  36.4   0.5
 9. be7.rbx-iplb1a-a70.fr.eu    0.0%    13   34.6  35.1  34.2  36.4   0.4
10. www.ovh.pl                  0.0%    12   36.8  35.2  33.9  36.8   0.7
```

Budowa VDC – Open Source DC – Racoon2

- $mtr www.ovh.pl (bez tunelu VPN)
- Transmisja PL/WAW -> FR/SGB

```
                             My traceroute  [v0.87]
vlsbg1 (0.0.0.0)                                        Thu Apr 20 14:34:13 2017
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                  Packets               Pings
 Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.50.21.1                  0.0%    10    0.5   0.4   0.3   0.5   0.0
 2. war-bng4.tpnet.pl           0.0%     9    1.1   2.2   1.1   3.5   0.7
 3. war-r1.tpnet.pl             0.0%     9    3.0   2.2   1.0   3.3   0.5
 4. be100-158.var-5-a9.pl.eu    0.0%     9    2.5   2.6   1.6   3.7   0.6
 5. vl2.var-1-a72.pl.eu         0.0%     9    1.7   2.4   1.5   3.7   0.4
 6. be100-1102.fra-1-a9.de.eu   0.0%     9   23.9  23.5  22.4  24.3   0.4
 7. ???
 8. ???
 9. po5.rbx-iplb1b-a70.fr.eu    0.0%     9   30.7  30.1  28.9  30.9   0.4
10. www.ovh.pl                  0.0%     9   30.6  30.4  29.4  31.2   0.4
```

Budowa VDC – Open Source DC – Racoon2

- $mtr www.ovh.pl (bez tunelu VPN)
- Transmisja PL/WAW -> FR/SGB

```
                             My traceroute  [v0.87]
vlsbg1 (0.0.0.0)                                        Thu Apr 20 14:34:13 2017
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                  Packets               Pings
 Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.50.21.1                  0.0%    10    0.5   0.4   0.3   0.5   0.0
 2. war-bng4.tpnet.pl           0.0%     9    1.1   2.2   1.1   3.5   0.7
 3. war-r1.tpnet.pl             0.0%     9    3.0   2.2   1.0   3.3   0.5
 4. be100-158.var-5-a9.pl.eu    0.0%     9    2.5   2.6   1.6   3.7   0.6
 5. vl2.var-1-a72.pl.eu         0.0%     9    1.7   2.4   1.5   3.7   0.4
 6. be100-1102.fra-1-a9.de.eu   0.0%     9   23.9  23.5  22.4  24.3   0.4
 7. ???
 8. ???
 9. po5.rbx-iplb1b-a70.fr.eu    0.0%     9   30.7  30.1  28.9  30.9   0.4
10. www.ovh.pl                  0.0%     9   30.6  30.4  29.4  31.2   0.4
```

Budowa VDC – Open Source DC – Racoon2

- $mtr www.ing.pl (z tunelem VPN PL/WAW@Orange -> PL/WAW@OVH)
- Transmisja PL/WAW -> PL/WAW ~5ms

```
                                My traceroute  [v0.86]
vsys31c (0.0.0.0)                                        Thu Apr 20 14:38:36 2017
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                     Packets               Pings
 Host                              Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.55.20.65                     0.0%     2    0.3   0.3   0.3   0.3   0.0
 2. 10.50.61.52                     0.0%     2    3.5   3.5   3.5   3.5   0.0
 3. 10.50.61.1                      0.0%     2    3.8   3.4   3.1   3.8   0.0
 4. 137.74.1.252                    0.0%     2    4.6   4.8   4.6   5.1   0.0
 5. 10.95.97.14                     0.0%     1    4.1   4.1   4.1   4.1   0.0
 6. vl1067.var-1-a72.pl.eu          0.0%     1    4.5   4.5   4.5   4.5   0.0
 7. incapsula.plix.pl               0.0%     1    3.5   3.5   3.5   3.5   0.0
 8. 192.230.78.108.ip.incapdns.net  0.0%     1    4.8   4.8   4.8   4.8   0.0
```

Budowa VDC – Open Source DC – Racoon2

- $mtr www.ing.pl (bez VPN PL/WAW@Orange -> www.ing.pl via telia)
- Transmisja PL/WAW -> PL/WAW via telia ~30ms

```
                           My traceroute  [v0.87]
vlwaw1 (0.0.0.0)                                    Thu Apr 20 14:38:32 2017
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                 Packets                Pings
 Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. 10.50.21.1                  0.0%     2    0.3   0.3   0.3   0.4   0.0
 2. war-bng4.tpnet.pl           0.0%     2    1.2   1.9   1.2   2.7   1.0
 3. war-r1.tpnet.pl             0.0%     2    1.8   1.8   1.8   1.9   0.0
 4. war-b2-link.telia.net       0.0%     2   34.7  33.5  32.2  34.7   1.7
 5. war-b1-link.telia.net       0.0%     2   37.3  39.7  37.3  42.1   3.3
 6. imperva-ic-322003-war-b1.c.telia  0.0%     2   36.6  36.6  36.6  36.6   0.0
 7. 192.230.78.108.ip.incapdns.net    0.0%     1   20.7  20.7  20.7  20.7   0.0
```

Budowa VDC – Open Source DC – Racoon2

- przykład użycia Racoon via OVH/VPS

```
root@vlsbg1:/etc/racoon# cat /root/vr.sh
setkey -FP
setkey -F
killall -9 racoon
/etc/racoon/vpn1.sh
racoon -f /etc/racoon/racoon.conf -l /va
root@vlsbg1:/etc/racoon#
```

```
#path certificate "/usr/local/etc/racoon/easy-rsa/keys" ;
path pre_shared_key "/etc/racoon/psk.txt" ;
path certificate "/etc/racoon/certs";
log info;
#log debug;

listen {
        isakmp 10.50.21.50;
        isakmp_natt 10.50.21.50[4500];
}

timer
{
        counter 5;
        interval 20 sec;
        persend 1;
        natt_keepalive  15 sec;
        phase1 30 sec;
        phase2 15 sec;
}
```

Budowa VDC – Open Source DC – Racoon2

```
remote 92.222.84.223
{
        exchange_mode main;
        lifetime time 168 hour;
        proposal_check obey;
        nat_traversal   off;
        dpd_delay 5;
        dpd_retry 5;
        dpd_maxfail 5;
        rekey   on;
        generate_policy on;
        doi ipsec_doi;
        certificate_type x509 "mgmt1.public" "mgmt1.private";
        my_identifier asn1dn;
        peers_certfile x509 "mgmt3.public";
        send_cert on;
        send_cr on;
        initial_contact on;
        passive off;
#        my_identifier keyid tag "client-test";
        proposal {
                encryption_algorithm camellia;
                hash_algorithm sha256;
                authentication_method rsasig;
                dh_group 14;
        }
}
```

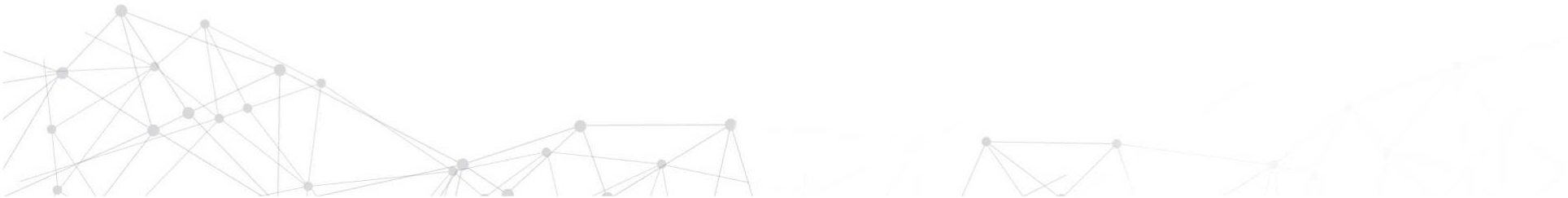
Budowa VDC – Open Source DC – Racoon2

-
```
sainfo address 10.55.20.128/25 any address 0.0.0.0/0 any
{
        pfs_group 14;
        lifetime time 120 hour;
        encryption_algorithm camellia;
        authentication_algorithm hmac_sha256;
        compression_algorithm deflate;
}
```

```
root@vlsbg1:/etc/racoon# cat vpn1.sh
#!/bin/sh

setkey -FP
setkey -F

setkey -v -c << END

spdadd 0.0.0.0/0 10.55.20.128/25 any -P in ipsec esp/tunnel/92.222.84.223-10.50.21.50/require;
spdadd 10.55.20.128/25 0.0.0.0/0 any -P out ipsec esp/tunnel/10.50.21.50-92.222.84.223/require;

END
```

Budowa VDC – Open Source DC – StrongSwan

- **StrongSwan – strongswan.org**
- **obecnie wspierany, rozwijany projekt IPSEC dla Linux**
- **w teorii obsługa multi-core**
- ***obsługa Linux, Android, FreeBSD, Mac OS X***



Budowa VDC – Open Source DC – OpenStack

- OpenStack – openstack.org

- na start RedHat RDO / packstack- https://www.rdoproject.org/
- ciekawe projekty Magnum – API dla kontenerów np. Docker, Mesos, Kubernetes
- TripleO (OpenStack On OpenStack)
- Warto rozpocząć od KVM + Open vSwitch

Budowa VDC – Open Source DC – OpenStack

- **OpenStack / Havana – Debian / Wheezy**
- OpenStack, Havana, Debian, Wheezy,

Multi, Node, Neutron, Nova, Keystone,

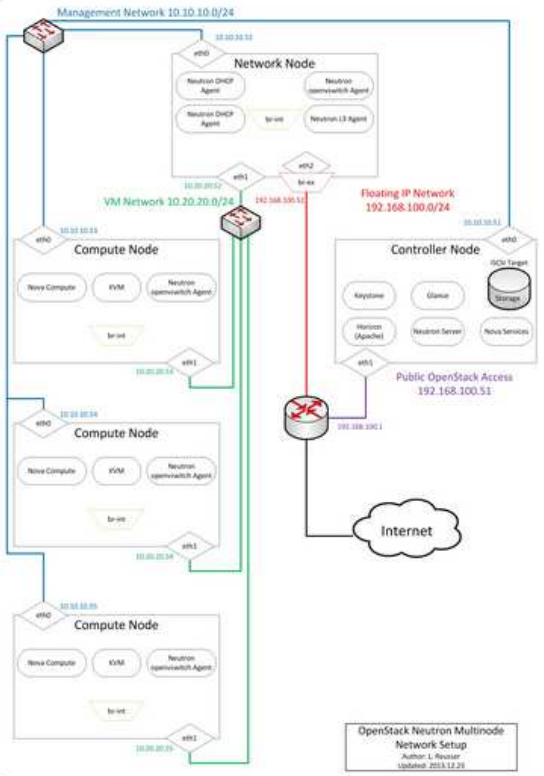
Glance, Horizon, Cinder, OpenVSwitch, KVM

- OpenStack obecnie wiele szybko

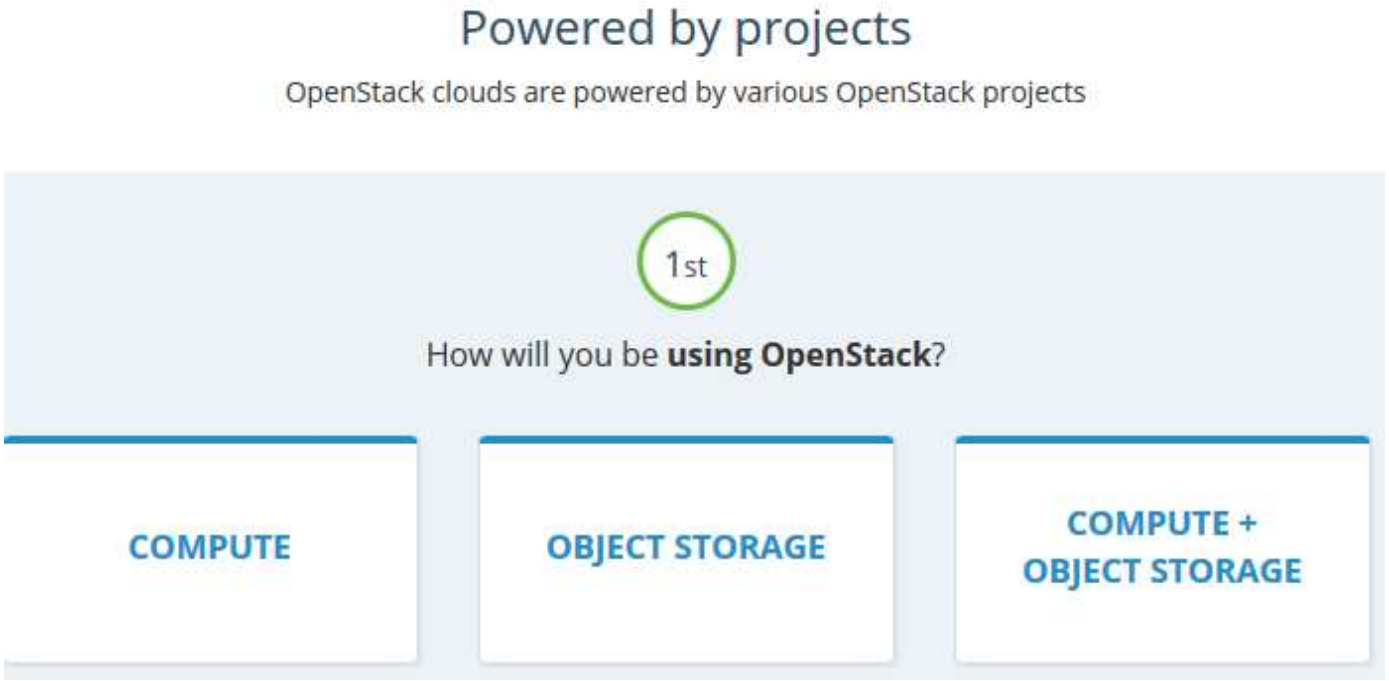
Rozwijanych modułów, coraz lepiej

udokumentowany projekt

Żródło : https://github.com/reusserl/OpenStack-Install-Guide



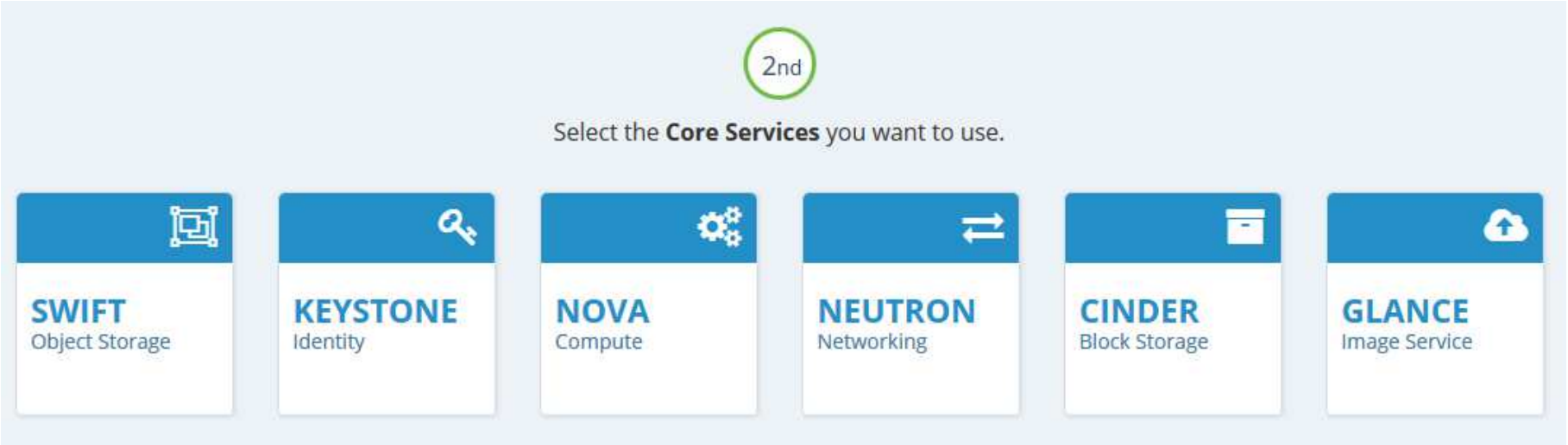
Budowa VDC – Open Source DC – OpenStack



Żródło : https://www.openstack.org/software/

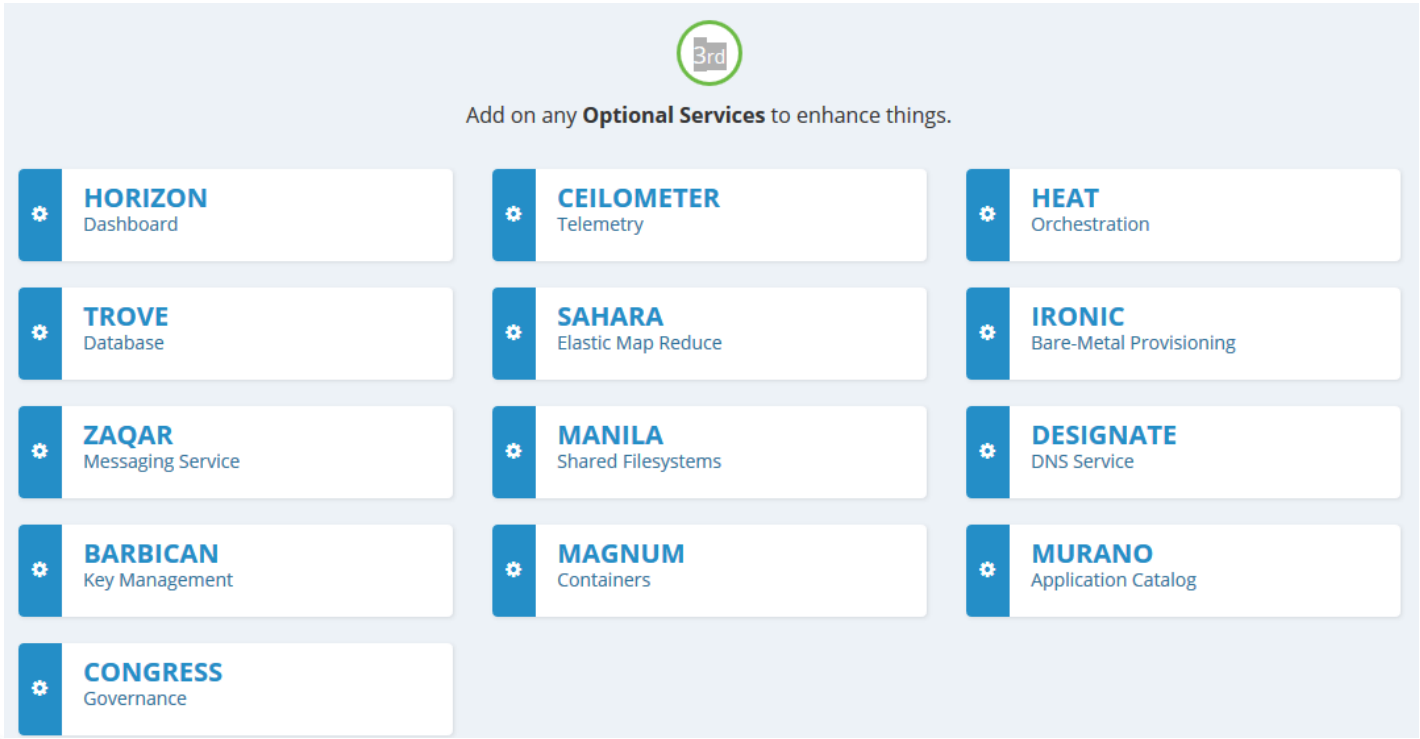
Budowa VDC – Open Source DC – OpenStack

- **OpenStack**



Żródło : https://www.openstack.org/software/

Budowa VDC – Open Source DC – OpenStack



Żródło : https://www.openstack.org/software/

Budowa VDC – Podsumowanie

- jakie usługi chcemy uruchomić w chmurze – czym będą za 2-4 lata
- koszt pobrania/migracji danych
- klasyfikacja danych / planowanie / rozwój
- wirtualne data center / prywatna chmura

Budowa VDC – ciekawostka

- **Wirtualizacje / Cloud – jak uczyć ?**

Running BuildTools (top)

1. Download BuildTools.jar from https://hub.spigotmc.org/jenkins/job/BuildTools/lastSuccessfulBuild/artifact/target/BuildTools.jar.

- Code (Latest Version):

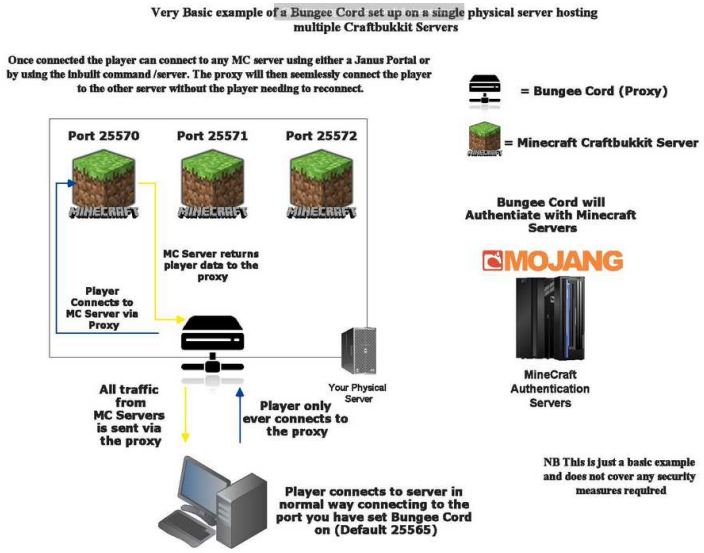
```
java -jar BuildTools.jar --rev latest
```

MULTIVERSE 2
THE BUKKIT WORLD MANAGEMENT PLUGIN

Źródło :
https://www.spigotmc.org/wiki/buildtools/ | https://www.technicpack.net/
https://github.com/Multiverse/Multiverse-Core/wiki | http://www.computercraft.info/

Budowa VDC – ciekawostka

- **Wirtualizacje / Cloud – jak uczyć ?**



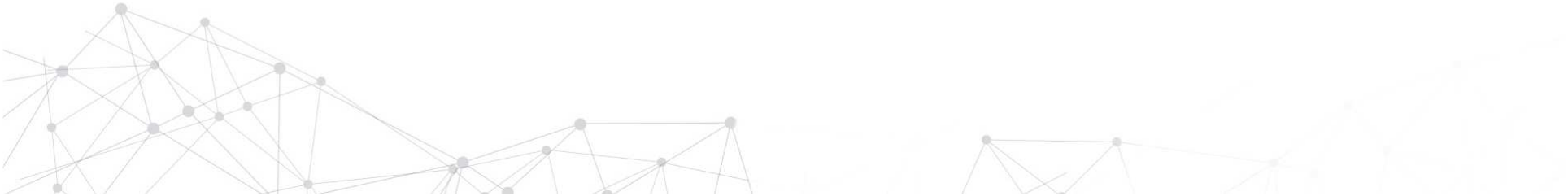
Źródło :
https://www.spigotmc.org/wiki/bungeecord/

Q&A

Marcin Motylski
MITVision
email: marcin.motylski@mitvision.com
www.mitvision.com

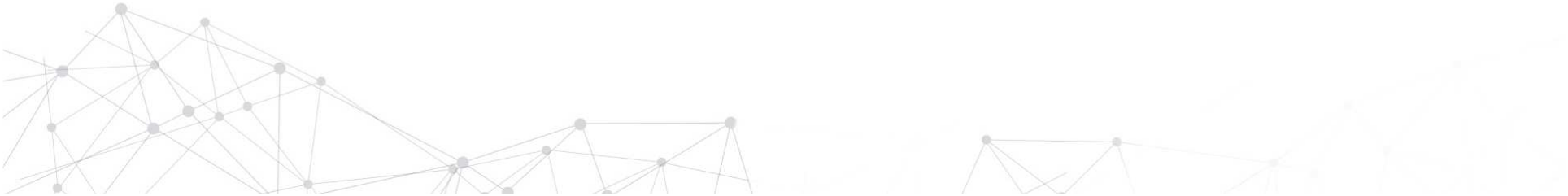
Budowa VDC – praktycznie

- architektura
- kompilacja kernel Linux
- Linux KVM
- KVM guest host
- KVM / Linux tunning
- przykłady połączeń IPSEC / GRE



Budowa VDC – praktycznie

- Linux jako host brzegowy (router)
- Firewall brzegowy FreeBSD / OpenBSD / Linux
- Firewall NAT (połączenia IPSEC / GRE)
- ręczne przeniesienie host KVM
- przykłady routingów w IPSEC / GRE (możliwości styk z Internetem)
- Instalacja kernel Linux



Budowa VDC – praktycznie

- monitoring host KVM, narzędzia takie jak iostat, dstat, iptraf, mtr
- tworzenie Open vSwitch i podłączenie host do Open vSwitch
- przykład konfiguracji IPSEC Racoon / GRE (speedtesty)
- monitoring Munin / Icinga
- Instalacja kernel / upgrade KVM