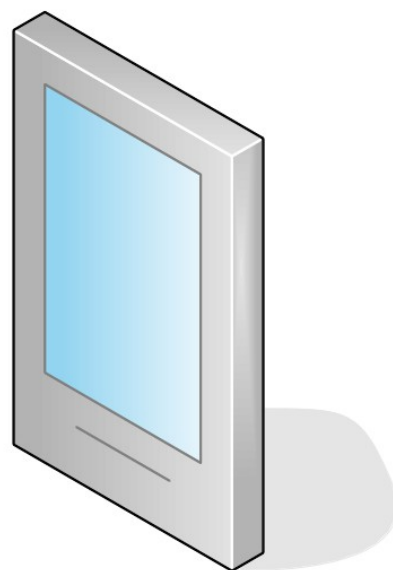
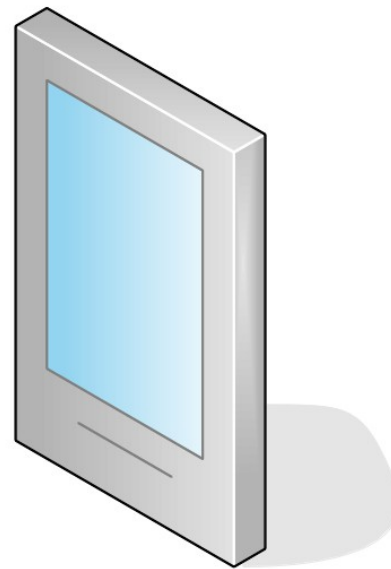


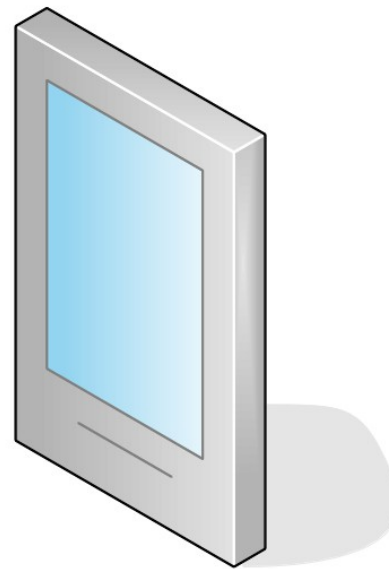
Monitoring Virtual Networks

George Warnagiris

Geo@TheTeneoGroup.com
@TeneoGroup



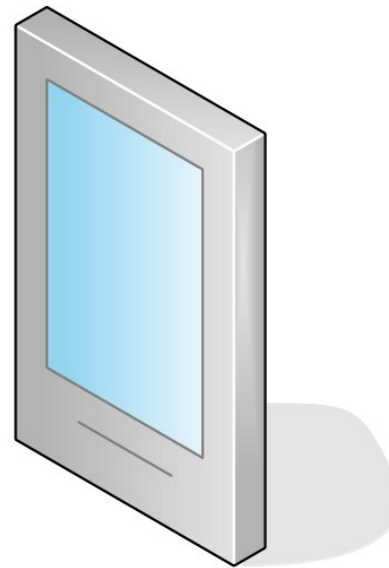




#FloCon2015



@TeneoGroup



#FloCon2015



Overview

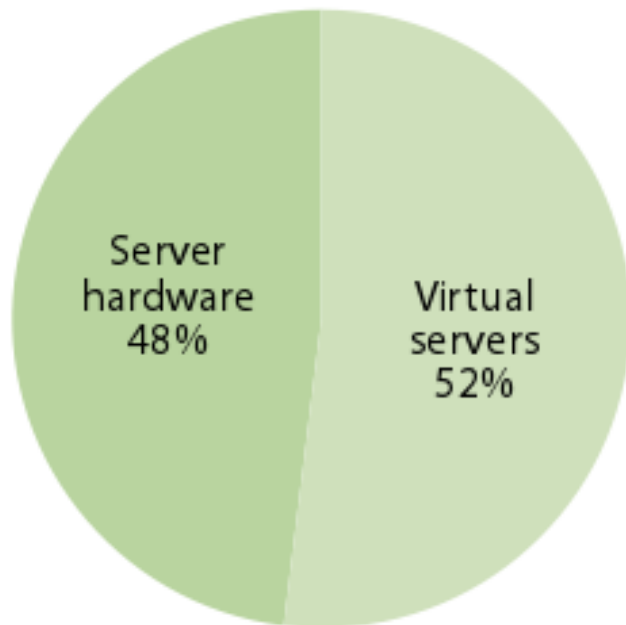
- **Background**
- **The Problem**
- **The Solution**
- **Going Forward**



1-2 The percentage of x86 server virtualization

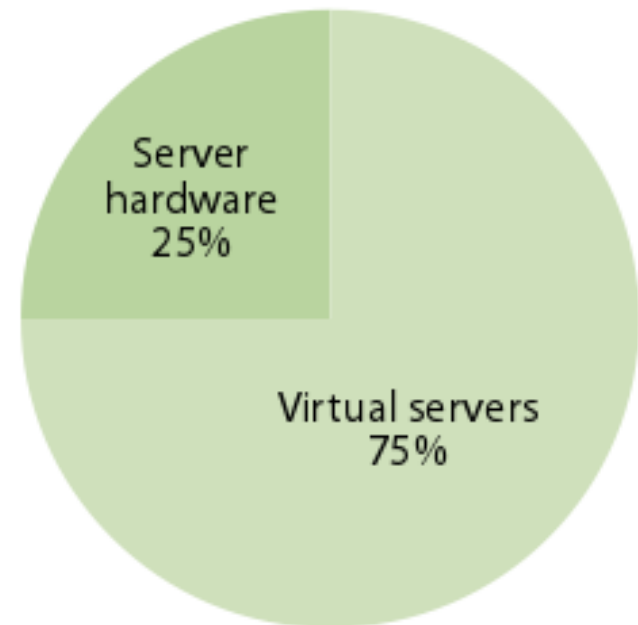
“Today, approximately what percentage of your x86 server OS instances are operated as virtual servers rather than run directly on server hardware?”

(N = 771)



“In two years, approximately what percentage of your x86 server OS instances do you believe will be operated as virtual servers rather than run directly on server hardware?”

(N = 768)



Base: North American and European executives and technology decision-makers at companies with 20-plus employees and who are responsible x86 servers

Source: Forrsights Hardware Survey, Q3 2011



Monitoring Cloud Computing by Layer, Part 1

The general characteristics of cloud computing's three service models—software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)—include on-demand self service, broad network access, pooling of resources, rapid

provider must formulate personnel policies with full appreciation of the observed increase in malicious insiders' involvement in security breaches³ and the potentially huge impact a malicious insider could have by exfiltrating or manipulating data. The provider should follow best practices in separation of privileges, least privilege, access control systems, alarm systems, administrator logging, two-factor authentication, codes of conduct, confidentiality agreements, background checks, and visitor access.

Operating a data center is a complex process that must take into account many environmental con-

elasticity of provisioning resources, and service or resource monitoring.¹ On the basis of the Cloud Security Alliance's work, a cloud is modeled in seven layers: facility, network, hardware, OS, middleware, application, and the user.² These layers can be controlled by

highest risk of data exposure and compromise owing to the less-controlled environment and must be handled with the appropriate caution. Any cloud project will have idiosyncrasies, and each requires its own risk assessment.

Here, I present a set of recom-

JONATHAN
SPRING
*Software
Engineering
Institute*



Layer	Service model		
	Software as a service	Platform as a service	Infrastructure as a service
Facility	✓	✓	✓
Network	✓	✓	✓
Hardware	✓	✓	✓
OS	✓	✓	?
Middleware	✓	?	—
Application	✓	—	—
User	—	—	—



Layer	Service model		
	Software as a service	Platform as a service	Infrastructure as a service
Facility	✓	✓	✓
Network	✓	✓	✓
Hardware	✓	✓	✓
OS	✓	✓	?
Middleware	✓	?	—
Application	✓	—	—
User	—	—	—



Clearing the clouds away from the true potential and obstacles posed by this computing capability.

BY MICHAEL ARMBRUST, ARMANDO FOX, REAN GRIFFITH, ANTHONY D. JOSEPH, RANDY KATZ, ANDY KONWINSKI, GUNHO LEE, DAVID PATTERSON, ARIEL RABKIN, ION STOICA, AND MATEI ZAHARIA

A View of Cloud Computing

CLOUD COMPUTING, THE long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the

hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT.

As a result, cloud computing is a popular topic for blogging and white papers and has been featured in the title of workshops, conferences, and even magazines. Nevertheless, confusion remains about exactly what it is and when it's useful, causing Oracle's CEO Larry Ellison to vent his frustration: "The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do.... I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads."

Our goal in this article is to reduce that confusion by clarifying terms, providing simple figures to quantify comparisons between of cloud and conventional computing, and identifying the top technical and non-technical obstacles and opportunities of cloud computing. (Armbrust et al⁴ is a more detailed version of this article.)


Defining Cloud Computing

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS).² Some vendors use terms such as IaaS (Infra-

Cloud Computing - The applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.

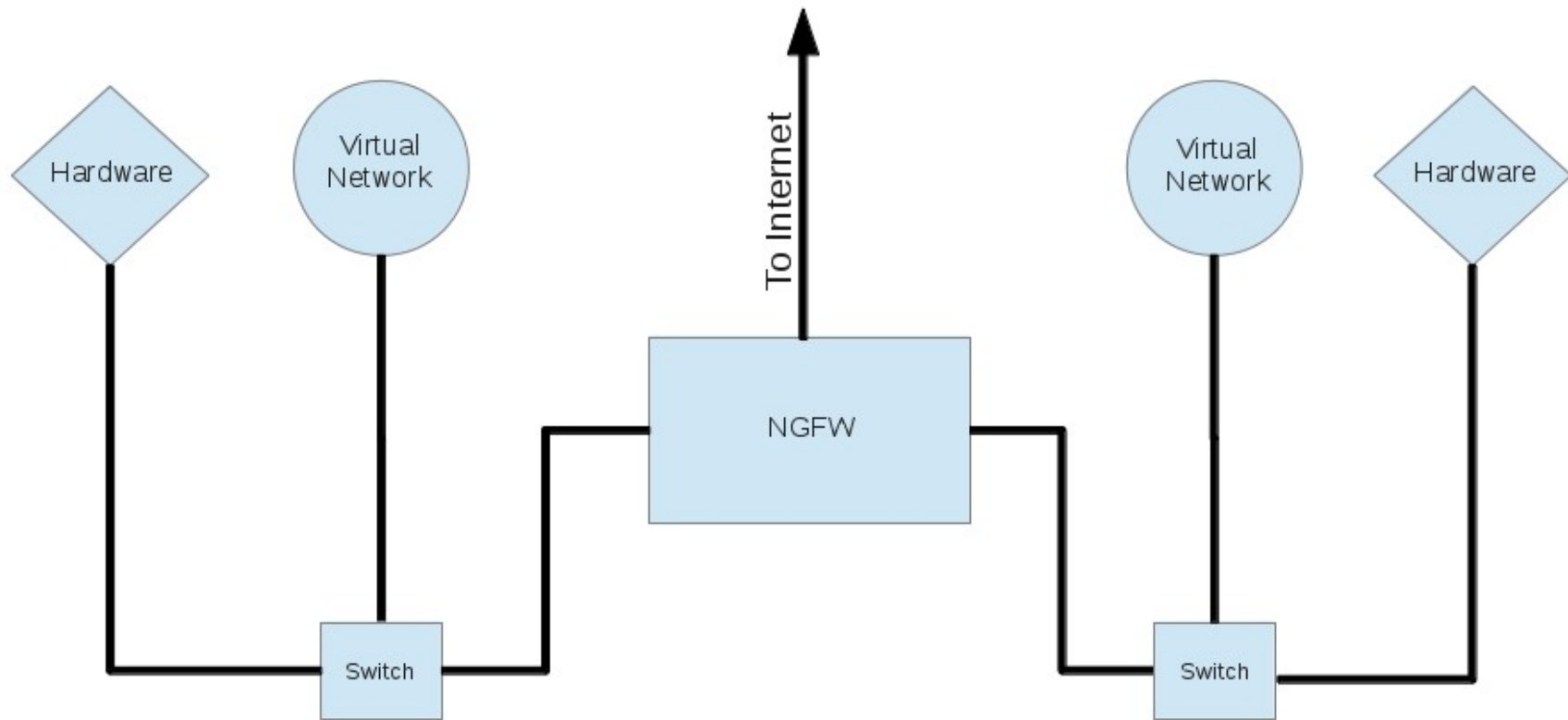
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. 2010. A View of Cloud Computing. Communications of the ACM 53, 50–58.

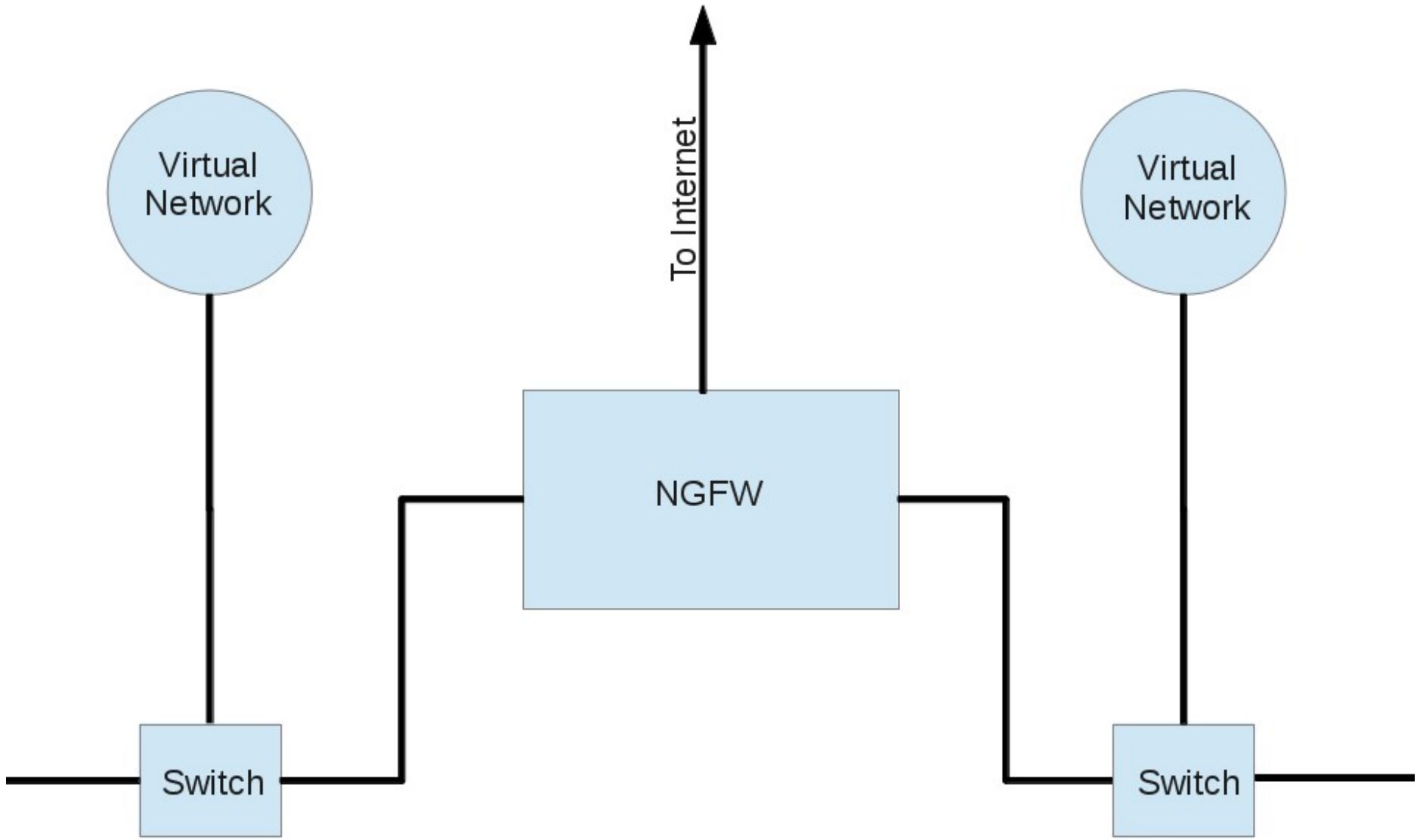


A black and white photograph of a server room. The room is filled with rows of server racks. Two people are walking through the aisle, their figures blurred to suggest motion. The floor is made of large square tiles. The lighting is bright, coming from overhead fixtures.

Mastering VMware vSphere® 5.5

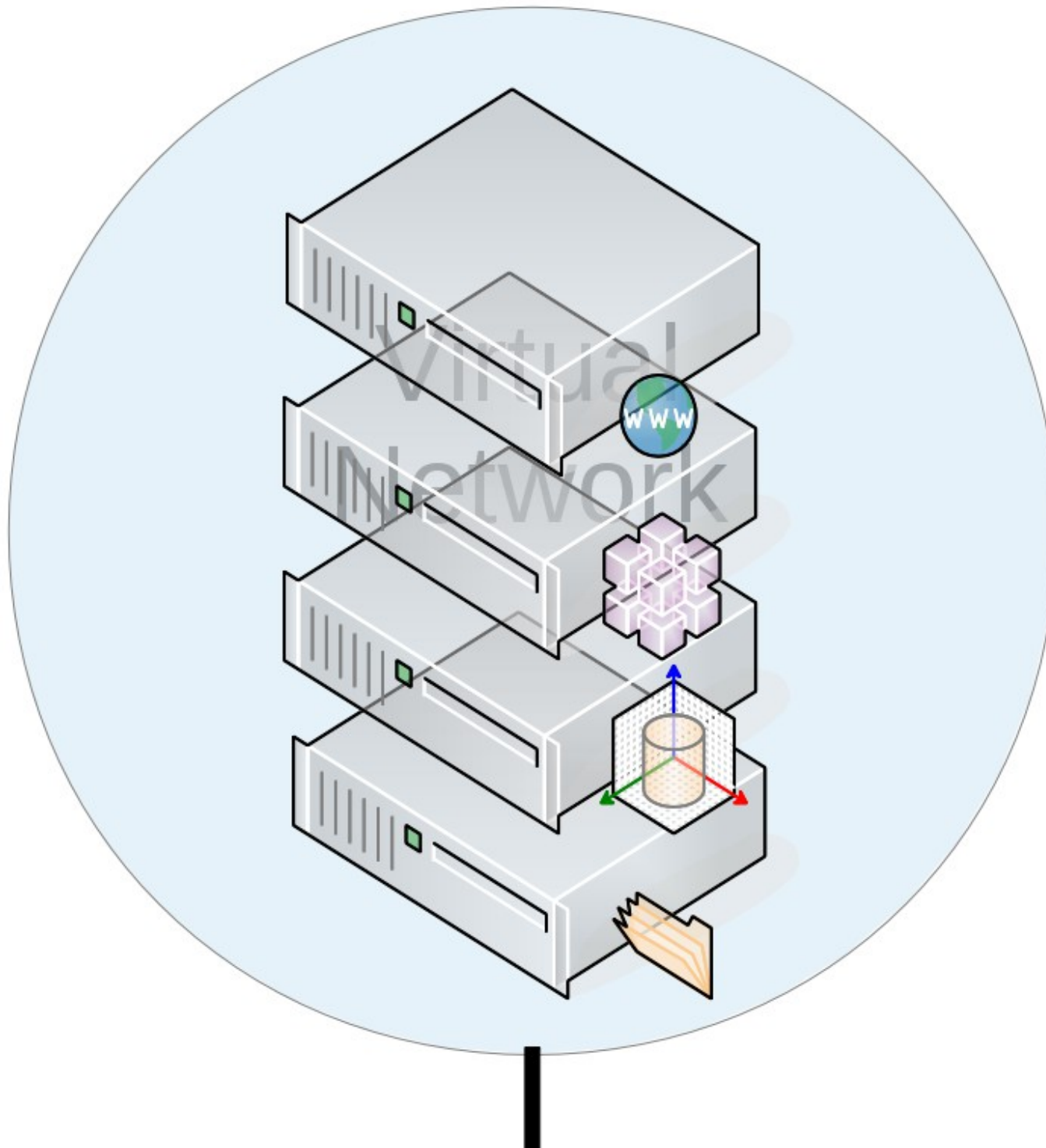


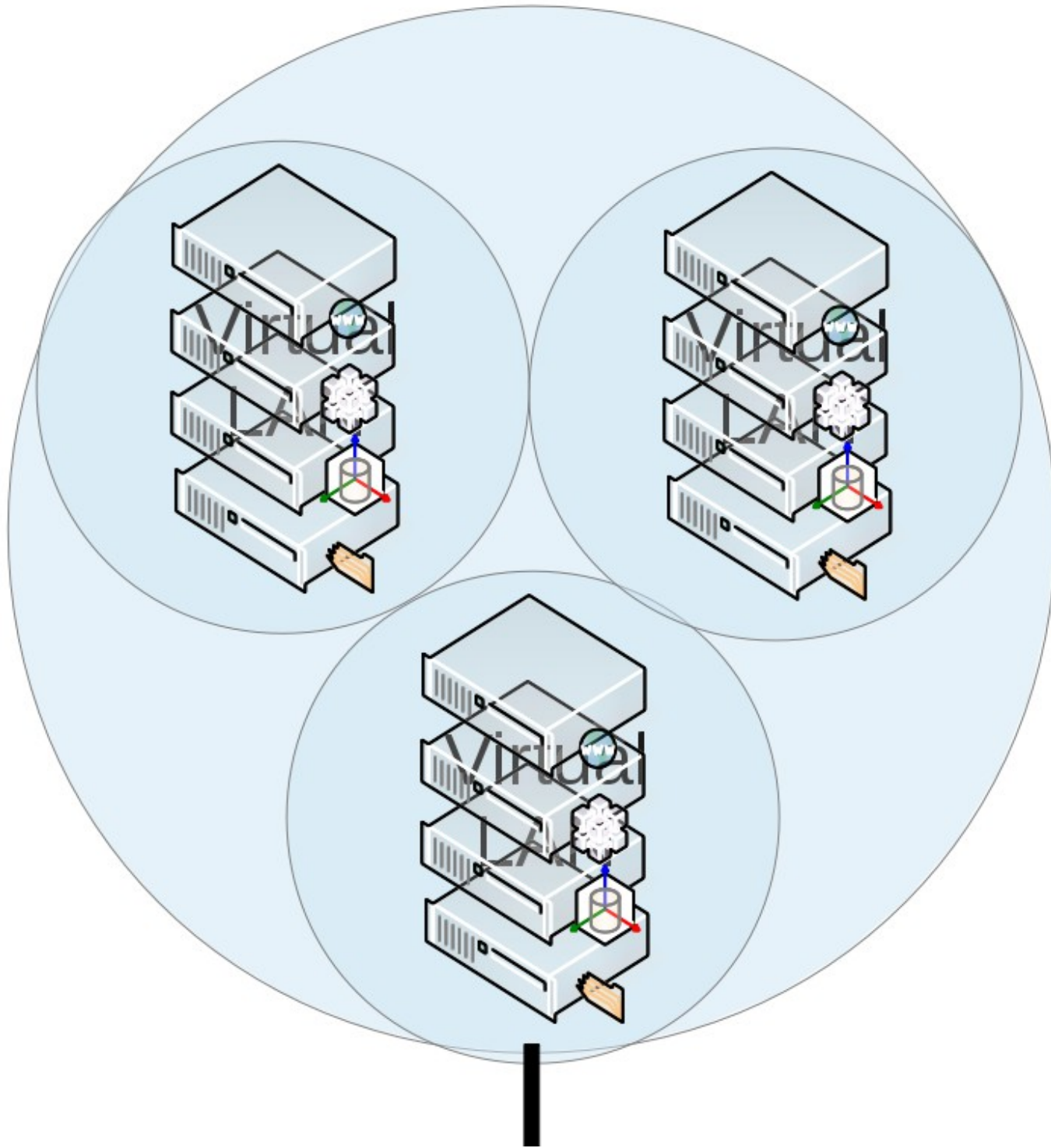


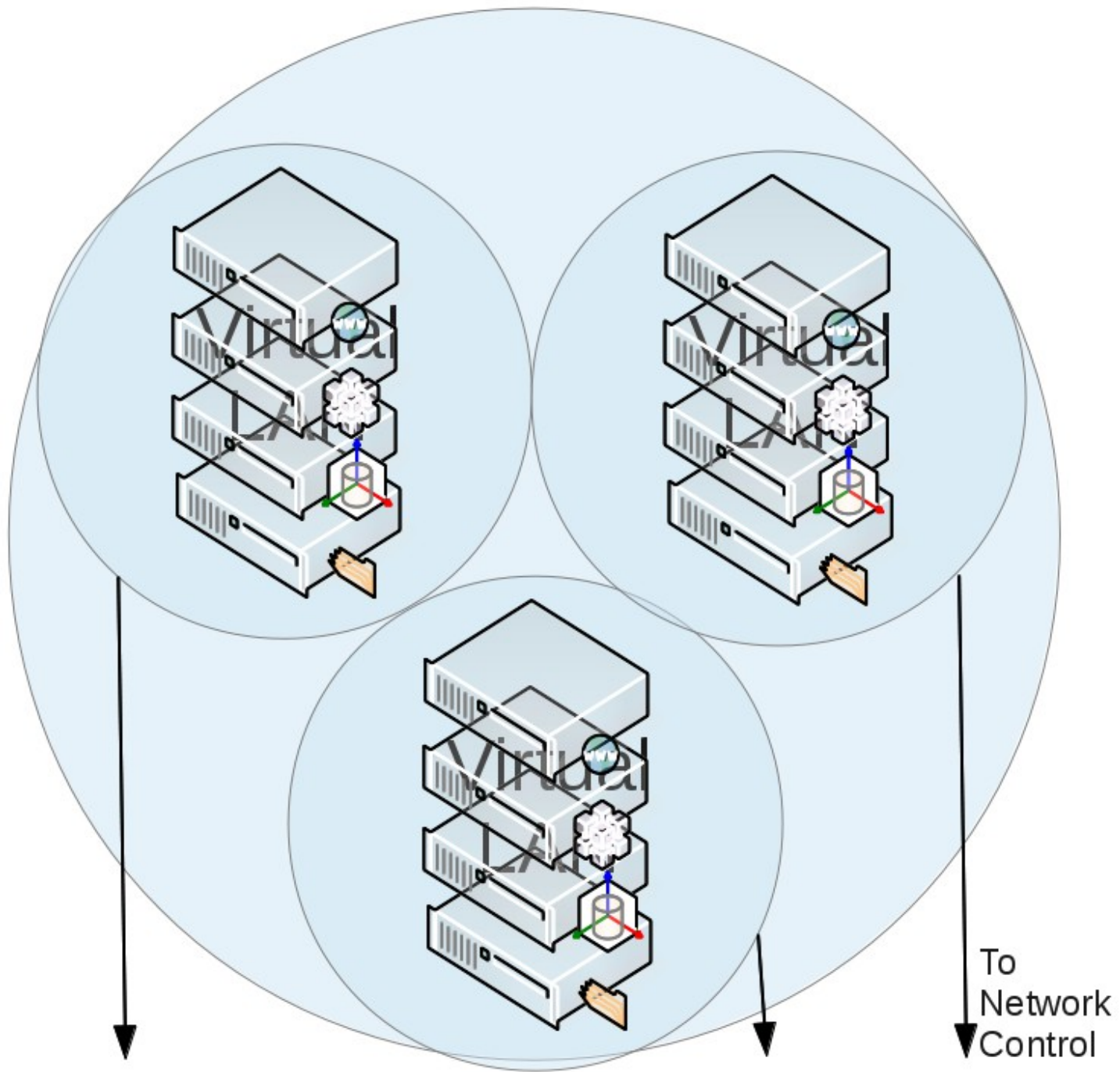


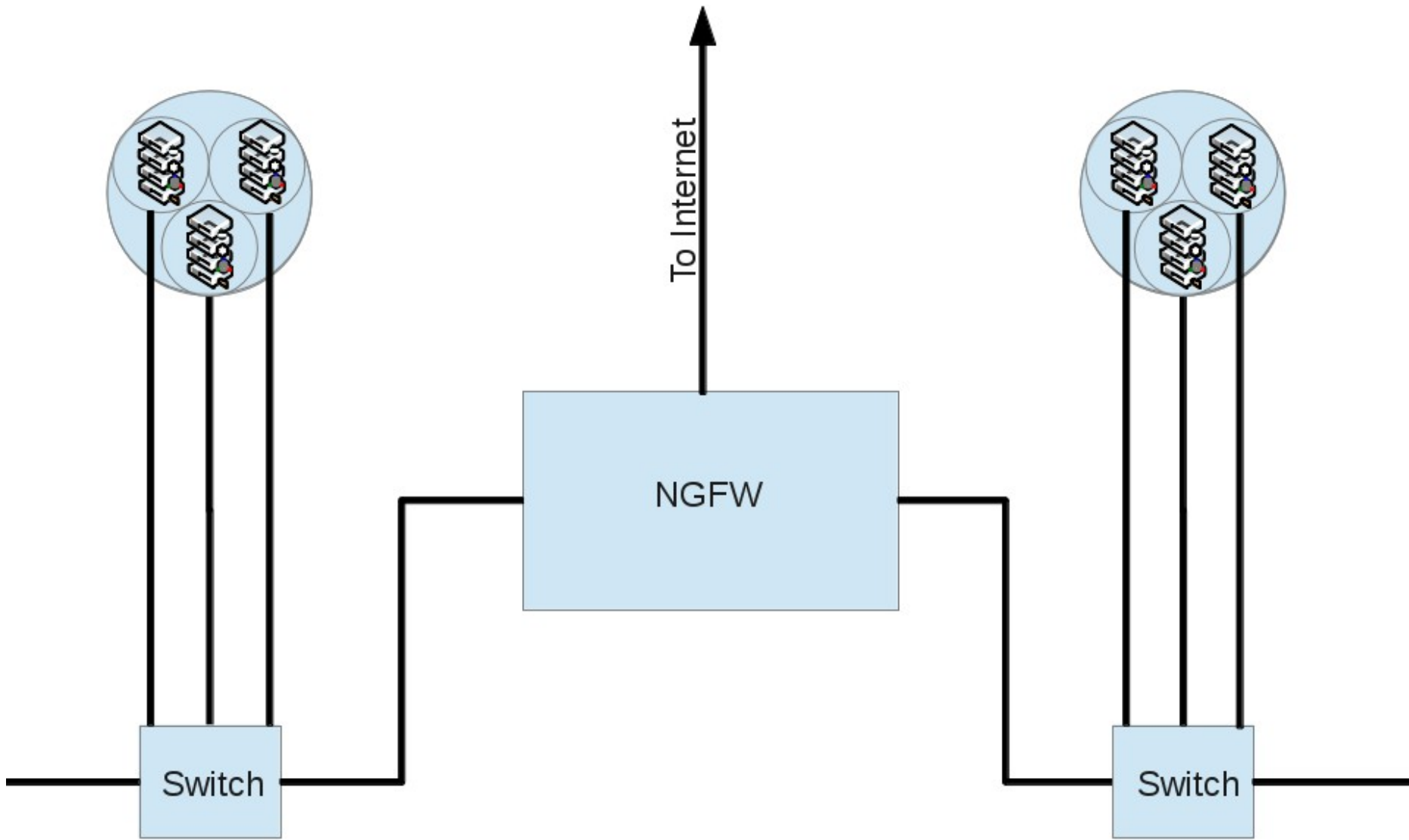


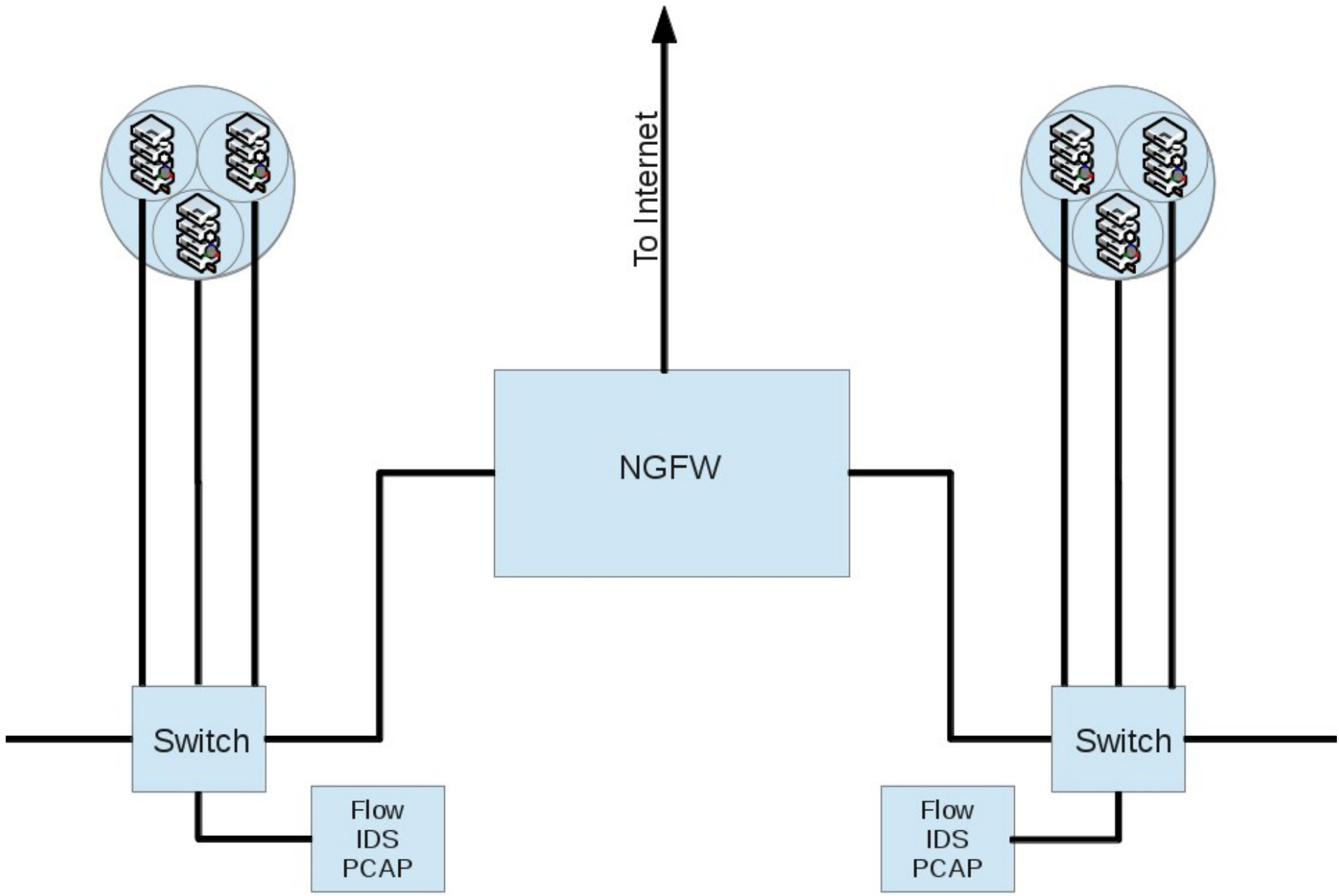
**Virtual
Network**

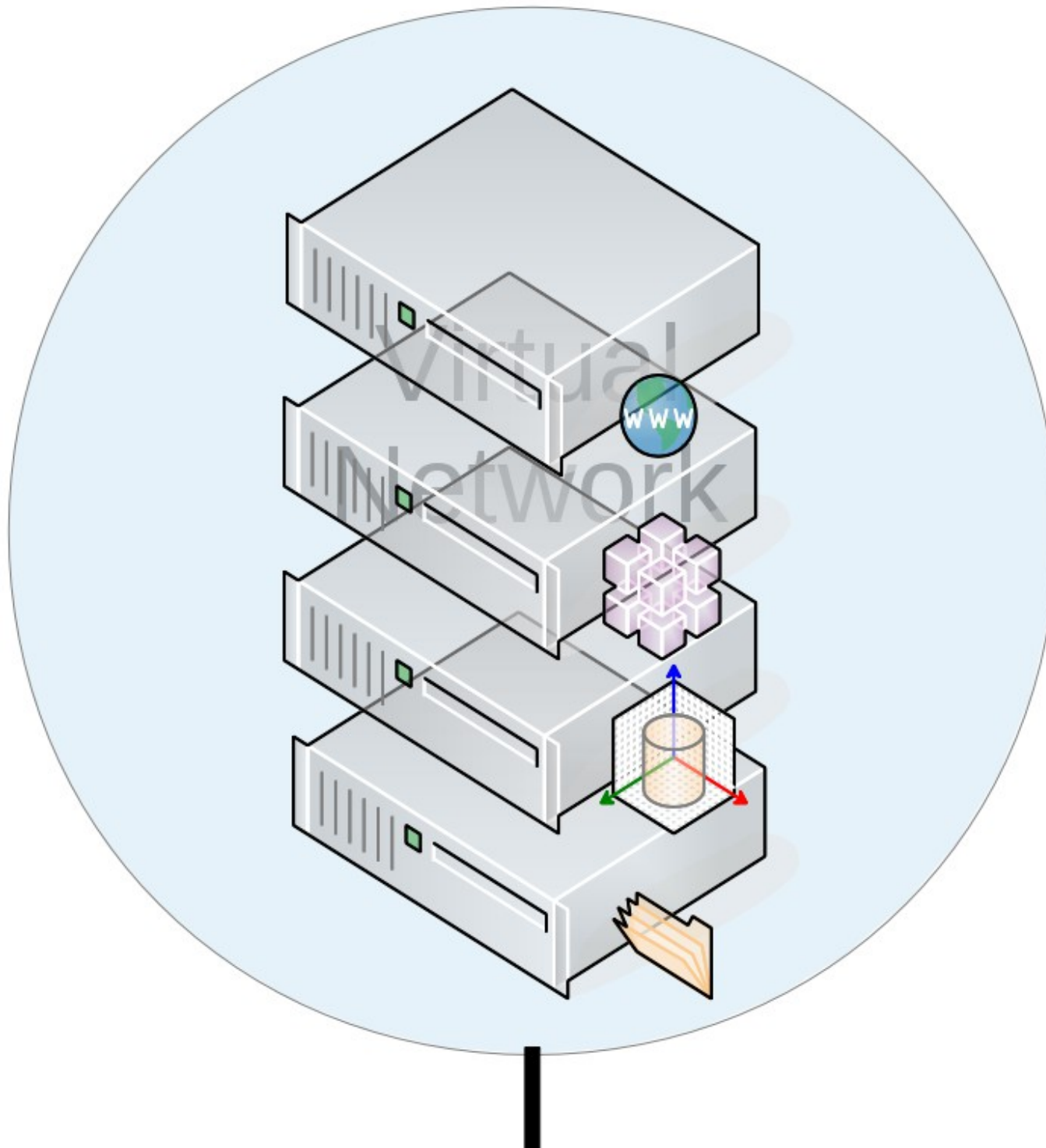


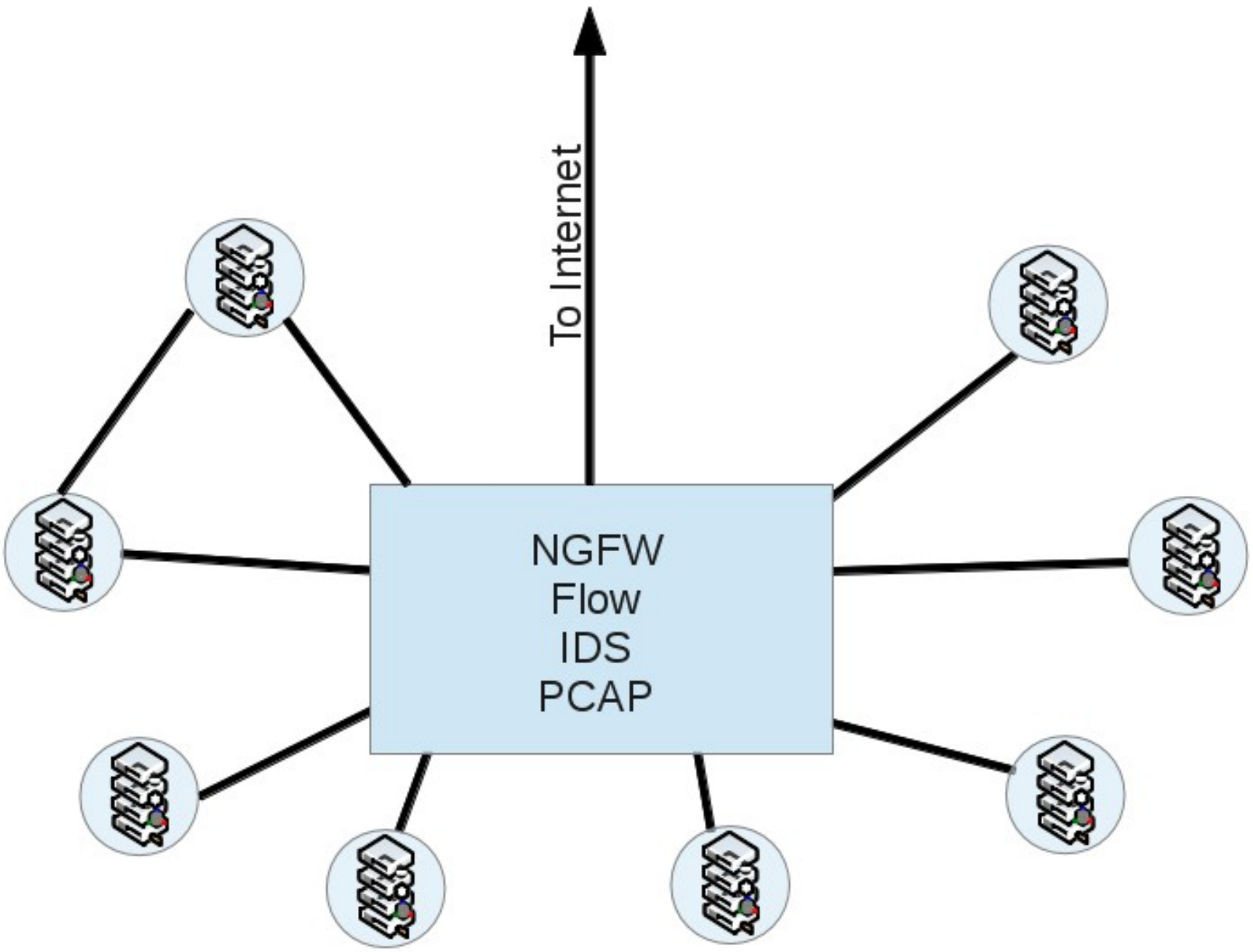






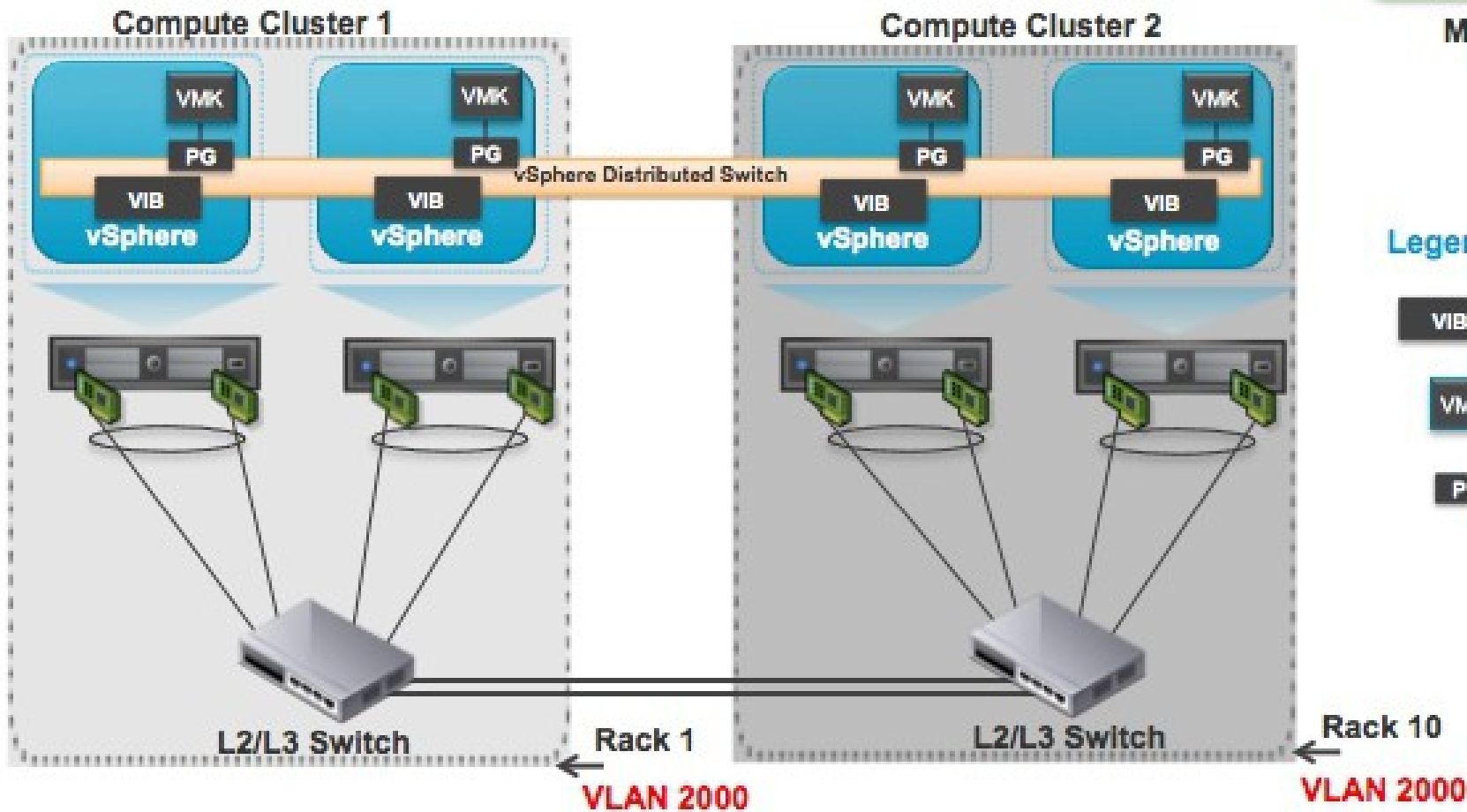






VMware vCenter
Server with vCNS
Manager Plugin

Management Cluster



Legend :

- VIB** VXLAN VIB
- VMK** vmknic
- PG** VXLAN Port group

<http://blogs.vmware.com/vsphere/2013/04/vxlan-series-different-components-part-1.html>



©The Teneo Group 2015

```

vMan [Running] - Oracle VM VirtualBox
Machine View Devices Help
root@vMan:~# ifconfig eth1
eth1  Link encap:Ethernet HWaddr 08:00:27:61:e7:ef
      inet addr:172.21.0.2 Bcast:172.21.0.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe61:e7ef/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:2125 errors:0 dropped:0 overruns:0 frame:0
      TX packets:295 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:812402 (812.4 KB) TX bytes:40142 (40.1 KB)

root@vMan:~# ifconfig vxlan0
vxlan0 Link encap:Ethernet HWaddr 54:08:20:00:00:01
      inet addr:20.0.0.1 Bcast:0.0.0.0 Mask:255.0.0.0
      inet6 addr: fe80::5608:20ff:fe00:1/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1450 Metric:1
      RX packets:218 errors:0 dropped:0 overruns:0 frame:0
      TX packets:257 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:158782 (158.7 KB) TX bytes:28804 (28.8 KB)

root@vMan:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.0.2.2 0.0.0.0 UG 0 0 0 eth0
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
20.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 vxlan0
172.21.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0

root@vMan:~# wget 20.0.0.2

```

```

Oracle VM VirtualBox Manager
VirtuVirtu [Running] - Oracle VM VirtualBox
Machine View Devices Help
root@virtuvirtu:~# ifconfig eth1
eth1  Link encap:Ethernet HWaddr 08:00:27:29:8b:aa
      inet addr:172.21.0.1 Bcast:172.21.0.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe29:8baa/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:2267 errors:0 dropped:0 overruns:0 frame:0
      TX packets:452 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:688438 (688.4 KB) TX bytes:226268 (226.2 KB)

root@virtuvirtu:~# ifconfig vxlan0
vxlan0 Link encap:Ethernet HWaddr 54:08:20:00:00:02
      inet addr:20.0.0.2 Bcast:0.0.0.0 Mask:255.0.0.0
      inet6 addr: fe80::5608:20ff:fe00:1/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1450 Metric:1
      RX packets:240 errors:0 dropped:0 overruns:0 frame:0
      TX packets:196 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:20306 (20.3 KB) TX bytes:162342 (162.3 KB)

root@virtuvirtu:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.0.2.2 0.0.0.0 UG 0 0 0 eth0
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
20.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 vxlan0
172.21.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0

root@virtuvirtu:~#

```

```

sensing [Running] - Oracle VM VirtualBox
Machine View Devices Help
18:48:03.273359 IP 128.118.2.96.80 > 10.0.2.15.42432: Flags [.], seq 3677928:367
9348, ack 579, win 65535, length 1420
18:48:03.273364 IP 128.118.2.96.80 > 10.0.2.15.42432: Flags [P.], seq 3679348:36
79376, ack 579, win 65535, length 28
18:48:03.273366 IP 10.0.2.15.42432 > 128.118.2.96.80: Flags [.], ack 3679376, wi
n 65535, length 0
18:48:03.273697 IP 128.118.2.96.80 > 10.0.2.15.42432: Flags [.], seq 3679376:368
0796, ack 579, win 65535, length 1420
18:48:03.273704 IP 128.118.2.96.80 > 10.0.2.15.42432: Flags [P.], seq 3680796:36
81611, ack 579, win 65535, length 815
18:48:03.273708 IP 10.0.2.15.42432 > 128.118.2.96.80: Flags [.], ack 3681611, wi
n 65535, length 0

```

intnet)

s: 0 (0 active)

folders

ation





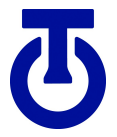
Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
14	0.001597	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
15	0.001658	172.21.0.1	172.21.0.2	UDP	752	Source port: 50472 Destination port: 8472
16	0.001962	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
17	0.001972	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
18	0.002172	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
19	0.002176	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
20	0.002178	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
21	0.002179	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
22	0.002180	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
23	0.002181	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
24	0.008932	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
25	0.009225	172.21.0.1	172.21.0.2	UDP	116	Source port: 50472 Destination port: 8472
26	0.009538	172.21.0.2	172.21.0.1	UDP	116	Source port: 53664 Destination port: 8472
27	5.009402	172.21.0.1	172.21.0.2	UDP	82	Source port: 46410 Destination port: 8472

▶ Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
 ▶ Ethernet II, Src: 08:00:27:61:e7:ef (08:00:27:61:e7:ef), Dst: 01:00:5e:01:01:01 (01:00:5e:01:01:01)
 ▶ Internet Protocol Version 4, Src: 172.21.0.2 (172.21.0.2), Dst: 239.1.1.1 (239.1.1.1)
 ▶ User Datagram Protocol, Src Port: 53664 (53664), Dst Port: 8472 (8472)
 ▶ Data (82 bytes)

```

0000 01 00 5e 01 01 01 08 00 27 61 e7 ef 08 00 45 00  ..^.... 'a...E.
0010 00 6e b8 b4 00 00 01 11 64 b1 ac 15 00 02 ef 01  .n.... d.....
0020 01 01 d1 a0 21 18 00 5a 00 00 08 00 00 00 00 00  ...!..Z .....
0030 2a 00 54 08 20 00 00 02 54 08 20 00 01 08 00  *.T. ... T. ....
0040 45 00 00 3c 66 9c 40 00 40 06 ac 1d 14 00 00 01  E..<f.@. @.....
  
```



http.pcap [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

Clear Apply Save

No.	Time	Source	Protocol	Length	Info
13	0.001575	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
14	0.001597	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
15	0.001658	172.21.0.2	UDP	752	Source port: 50472 Destination port: 8472
16	0.001962	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
17	0.001972	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
18	0.002172	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
19	0.002176	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
20	0.002178	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
21	0.002179	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
22	0.002180	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
23	0.002181	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
24	0.008932	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
25	0.009225	172.21.0.2	UDP	116	Source port: 50472 Destination port: 8472
26	0.009538	172.21.0.2	UDP	116	Source port: 53664 Destination port: 8472
27	5.009403	172.21.0.2	UDP	82	Source port: 46410 Destination port: 8472

▷ Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
 ▷ Ethernet II, Src: 08:00:27:61:e7:ef (08:00:27:61:e7:ef), Dst: 01:00:5e:01:01:01 (01:00:5e:01:01:01)
 ▷ Internet Protocol Version 4, Src: 172.21.0.2 (172.21.0.2), Dst: 239.1.1.1 (239.1.1.1)
 ▷ User Datagram Protocol, Src Port: 53664 (53664), Dst Port: 8472 (8472)
 ▷ Data (82 bytes)

```

0000  01 00 5e 01 01 01 08 00 27 61 e7 ef 08 00 45 00  ..^.... 'a...E.
0010  00 6e b8 b4 00 00 01 11 64 b1 ac 15 00 02 ef 01  .n.... d.....
0020  01 01 d1 a0 21 18 00 5a 00 00 08 00 00 00 00 00  ...!..Z .....
0030  2a 00 54 08 20 00 00 02 54 08 20 00 00 01 08 00  *.T. ... T. ....
0040  45 00 00 3c 66 9c 40 00 40 06 ac 1d 14 00 00 01  E..<f.@. @.....
  
```

File: "/home/geo/http.pcap" 15 KB ... Packets: 30 Displayed: 30 Marked: 0 Load time: 0:00.003 Profile: Default



http.pcap [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Wireshark: Decode As

Decode

Do not decode

Show Current

Clear

Help

Link Network Transport

UDP Both (53664↔8472) port(s) as

- UNISTIM
- VCDU
- Vines FRP
- Vuze-DHT
- VXLAN
- WASSP
- WCCP

OK Apply Close

th Info

14	Source port: 50472	Destination port: 8472
16	Source port: 53664	Destination port: 8472
52	Source port: 50472	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 53664	Destination port: 8472
16	Source port: 50472	Destination port: 8472
16	Source port: 53664	Destination port: 8472
82	Source port: 46410	Destination port: 8472

Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)

Ethernet II, Src: 08:00:27:61:e7:ef (08:00:27:61:e7:ef), Dst: 01:00:5e:01:01:01 (01:00:5e:01:01:01)

Internet Protocol Version 4, Src: 172.21.0.2 (172.21.0.2), Dst: 239.1.1.1 (239.1.1.1)

User Datagram Protocol, Src Port: 53664 (53664), Dst Port: 8472 (8472)

Data (82 bytes)

```

0000 01 00 5e 01 01 01 08 00 27 61 e7 ef 08 00 45 00  ..^..... 'a....E.
0010 00 6e b8 b4 00 00 01 11 64 b1 ac 15 00 02 ef 01  .n..... d.....
0020 01 01 d1 a0 21 18 00 5a 00 00 08 00 00 00 00 00  ....!...Z .....
0030 2a 00 54 08 20 00 00 02 54 08 20 00 01 08 00  *.T. ... T. ....
0040 45 00 00 3c 66 9c 40 00 40 06 ac 1d 14 00 00 01  E..<f.@. @.....

```

File: "/home/geo/http.pcap" 15 KB ... Packets: 30 Displayed: 30 Marked: 0 Load time: 0:00.003 Profile: Default





Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.0.0.1	20.0.0.2	TCP	124	53709 > 80 [SYN] Seq=0 Win=28200 Len=0 MSS=1410 SACK_PERM=1 TSval=1702396 TSecr=0 WS=128
2	0.000125	20.0.0.2	20.0.0.1	TCP	124	80 > 53709 [SYN, ACK] Seq=0 Ack=1 Win=27960 Len=0 MSS=1410 SACK_PERM=1 TSval=1701411 TSecr=1702396 WS=128
3	0.000491	20.0.0.1	20.0.0.2	TCP	116	53709 > 80 [ACK] Seq=1 Ack=1 Win=28288 Len=0 TSval=1702396 TSecr=1701411
4	0.001064	20.0.0.1	20.0.0.2	HTTP	222	GET / HTTP/1.1
5	0.001138	20.0.0.2	20.0.0.1	TCP	116	80 > 53709 [ACK] Seq=1 Ack=107 Win=28032 Len=0 TSval=1701411 TSecr=1702396
6	0.001491	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
7	0.001520	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
8	0.001520	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
9	0.001520	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
10	0.001532	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
11	0.001550	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
12	0.001563	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
13	0.001575	20.0.0.2	20.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
14	0.001597	20.0.0.1	20.0.0.2	TCP	116	53709 > 80 [ACK] Seq=107 Ack=1399 Win=31104 Len=0 TSval=1702396 TSecr=1701411

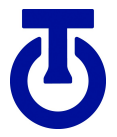
> Frame 10: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
 > Ethernet II, Src: 08:00:27:29:8b:aa (08:00:27:29:8b:aa), Dst: 08:00:27:61:e7:ef (08:00:27:61:e7:ef)
 > Internet Protocol Version 4, Src: 172.21.0.1 (172.21.0.1), Dst: 172.21.0.2 (172.21.0.2)
 > User Datagram Protocol, Src Port: 50472 (50472), Dst Port: 8472 (8472)
 > Virtual eXtensible Local Area Network
 > Ethernet II, Src: 54:08:20:00:00:02 (54:08:20:00:00:02), Dst: 54:08:20:00:00:01 (54:08:20:00:00:01)
 > Internet Protocol Version 4, Src: 20.0.0.2 (20.0.0.2), Dst: 20.0.0.1 (20.0.0.1)
 > Transmission Control Protocol, Src Port: 80 (80), Dst Port: 53709 (53709), Seq: 5593, Ack: 107, Len: 1398

```

0000 08 00 27 61 e7 ef 08 00 27 29 8b aa 08 00 45 00  ..'a.... ')....E.
0010 05 dc 0b 3b 00 00 40 11 11 a9 ac 15 00 01 ac 15  ...;.@. ....
0020 00 02 c5 28 21 18 05 c8 00 00 08 00 00 00 00 00  ...(!... ....
0030 2a 00 54 08 20 00 00 01 54 08 20 00 00 02 08 00  *.T. ... T. ....
0040 45 00 05 aa f5 ff 40 00 40 06 17 4c 14 00 00 02  E.....@. @..L....
  
```

File: "/home/geo/http.pcap" 15 KB ... Packets: 30 Displayed: 30 Marked: 0 Load time: 0:00.003

Profile: Default



Monitoring Virtual Networks

Virtual Sensors



vmware®



Microsoft
Hyper-V



VirtualBox



CERT NetSA Security Suite

Monitoring for Large-Scale Networks

Projects

- [Analysis Pipeline 4.4.1](#)
- [fixbuf 1.6.1](#)
- [IPA 0.5.2](#)
- [iSiLK 0.6.2](#)
- [netsa-python 1.4.3](#)
- [Orcus 1.0.1](#)
- [Rayon 1.4.3](#)
- [SiLK 3.9.0](#)
- [SiLK IPset 3.9.0](#)
- [snarf 0.2.2](#)
- [super_mediator 0.4.0](#)
- [YAF 2.6.0](#)

The [Network Situational Awareness \(NetSA\)](#) group provides tools for monitoring large-scale networks using flow analysis. This project, the SiLK project and the effort to integrate them into a single analysis platform.

CERT is a part of the [Software Engineering Institute](#) (SEI) (FFRDC) operated by [Carnegie Mellon University](#).

Featured Projects

SiLK 3.9.0

[Download Now](#)

The System for Internet Level Knowledge (SiLK) is an efficient network flow collection and storage infrastructure that will accept flow data from a variety of sensors. SiLK also provides a suite of efficient command-line tools for analysis.



```
root@cooldude:/home/geo/sharing/splitter# VBoxManage clonehd sensor.vdi sensor.vmdk --format VMDK
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone hard disk created in format 'VMDK'. UUID: 19ed8ecd-a389-41f4-b75d-e1ec940fd556
root@cooldude:/home/geo/sharing/splitter# █
```

I

Terminal - geo@cooldude: ~/sharing/splitter



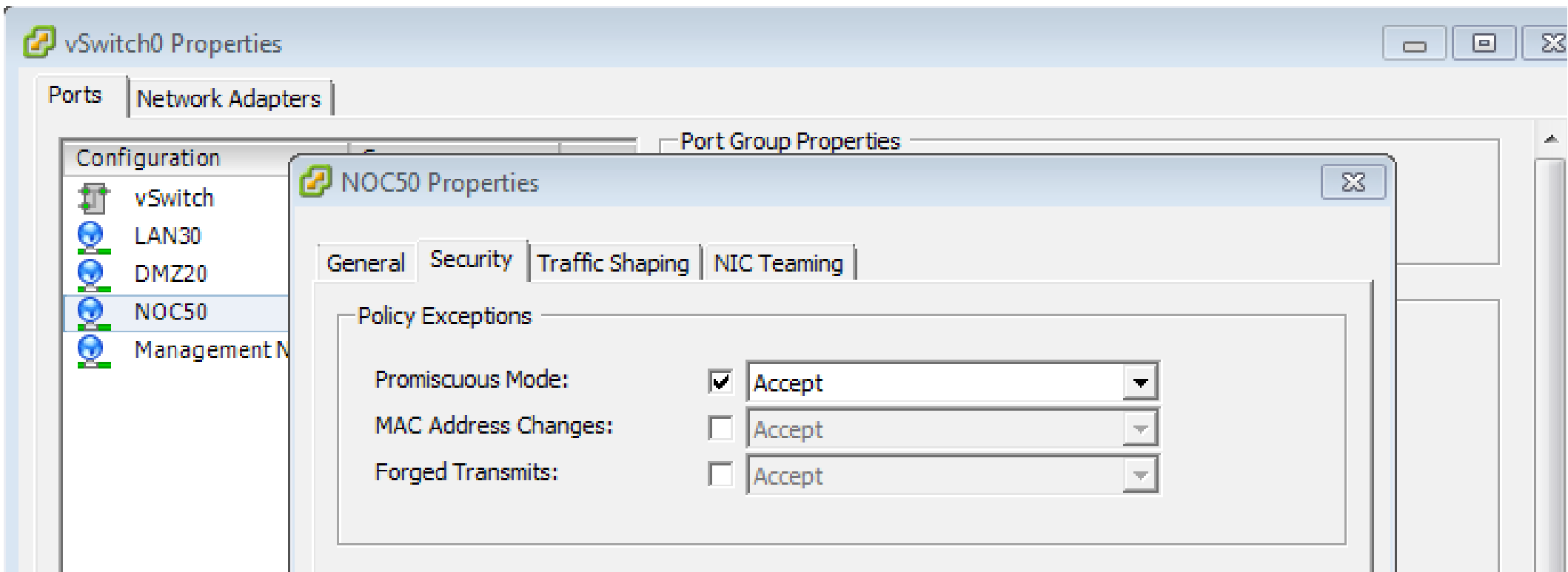
```
er# VBoxManage clonehd sensor.vdi sensor.vmdk --format VMDK
```

```
...70%...80%...90%...100%
```

```
K'. UUID: 19ed8ecd-a389-41f4-b75d-e1ec940fd556
```

```
er# █
```

VMware Port Groups



Hyper-V Port Mirroring

The screenshot shows the Hyper-V Advanced Features settings for a network adapter. The left sidebar lists hardware components, with 'Advanced Features' selected. The main panel shows several settings, with 'Port mirroring' highlighted by a red oval. The 'Port mirroring' section includes a description and a dropdown menu for 'Mirroring mode' set to 'Source'.

Hardware

- Add Hardware
- BIOS
Boot from CD
- Memory
1512 MB
- Processor
1 Virtual processor
- IDE Controller 0
 - Hard Drive
columbiadisk01.vhdx
 - DVD Drive
None
- IDE Controller 1
 - DVD Drive
vmguest.iso
 - DVD Drive
None
- SCSI Controller
- Network Adapter
Hyper-V-Guests
Hardware Acceleration
- Advanced Features**
- Network Adapter
ISCSI-GUEST
- Network Adapter
CSV-Guest
- COM 1
None
- COM 2
None
- Diskette Drive
None
- Management**
- Name

Advanced Features

MAC address

Dynamic

Static

00 - 15 - 5D - 02 - 20 - 88

MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.

Enable MAC address spoofing

DHCP guard

DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.

Enable DHCP guard

Router guard

Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.

Enable router advertisement guard

Port mirroring

Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.

Mirroring mode: Source

NIC Teaming

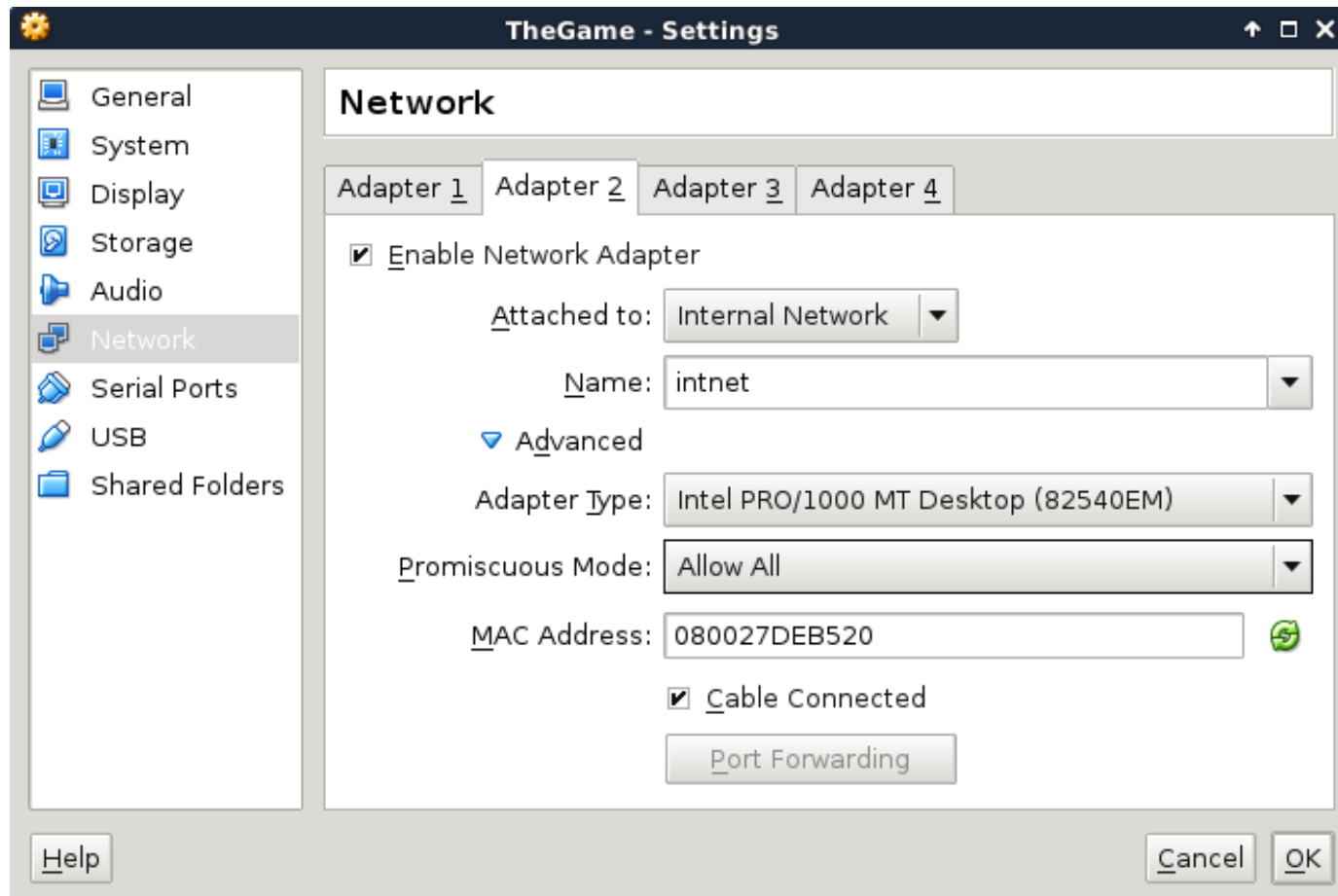
You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.

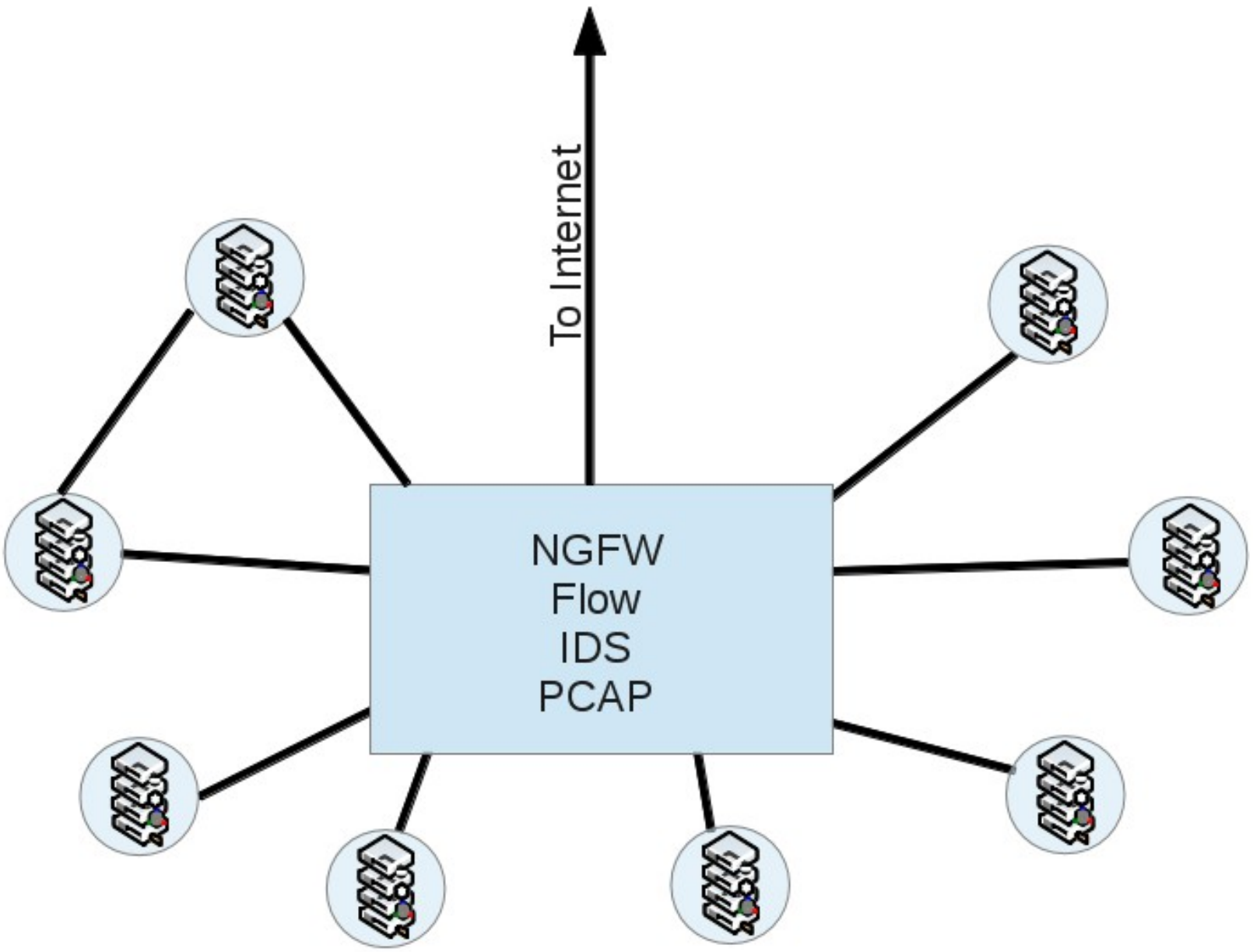
Enable this network adapter to be part of a team in the guest operating system

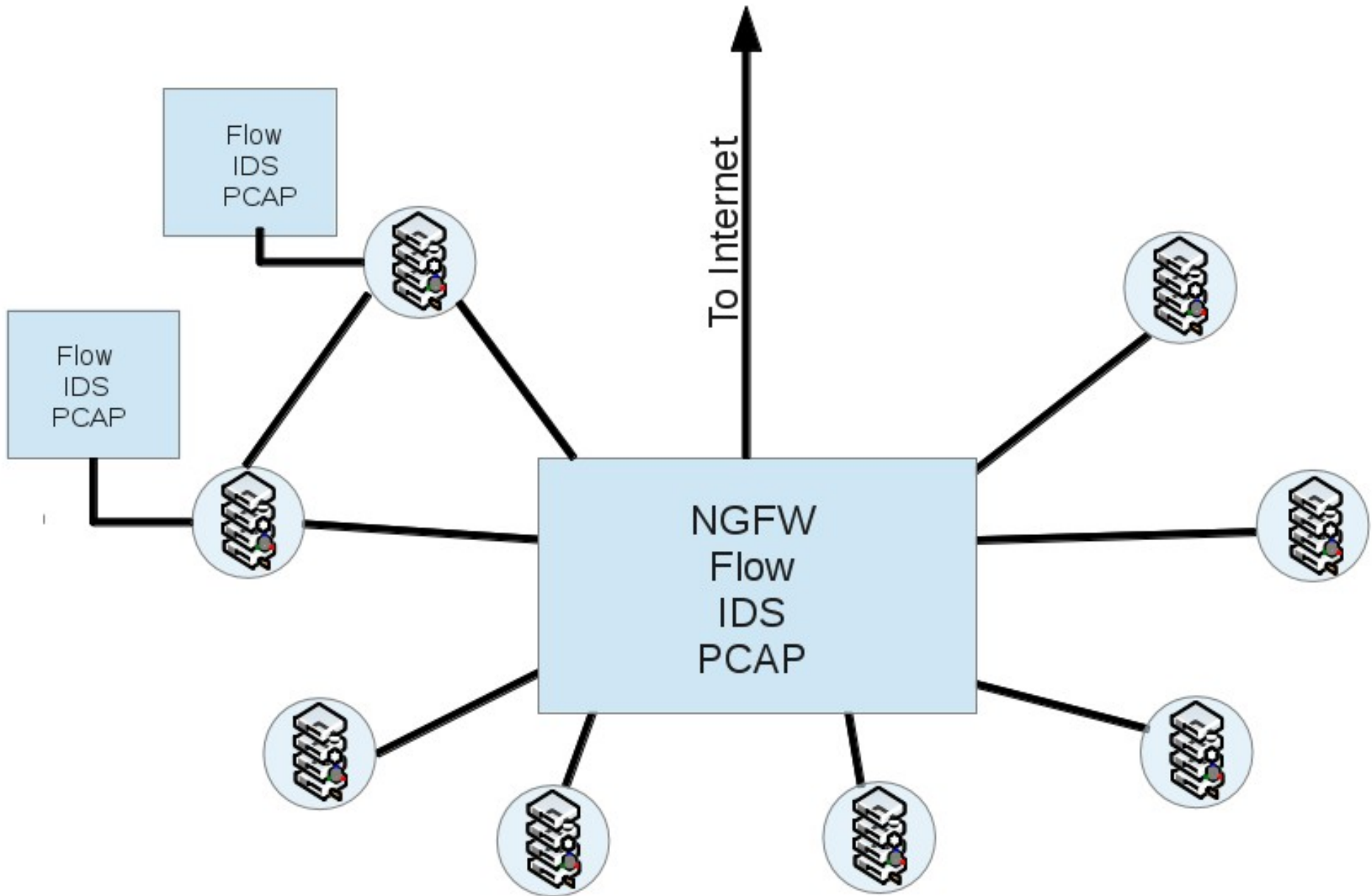
OK Cancel Apply

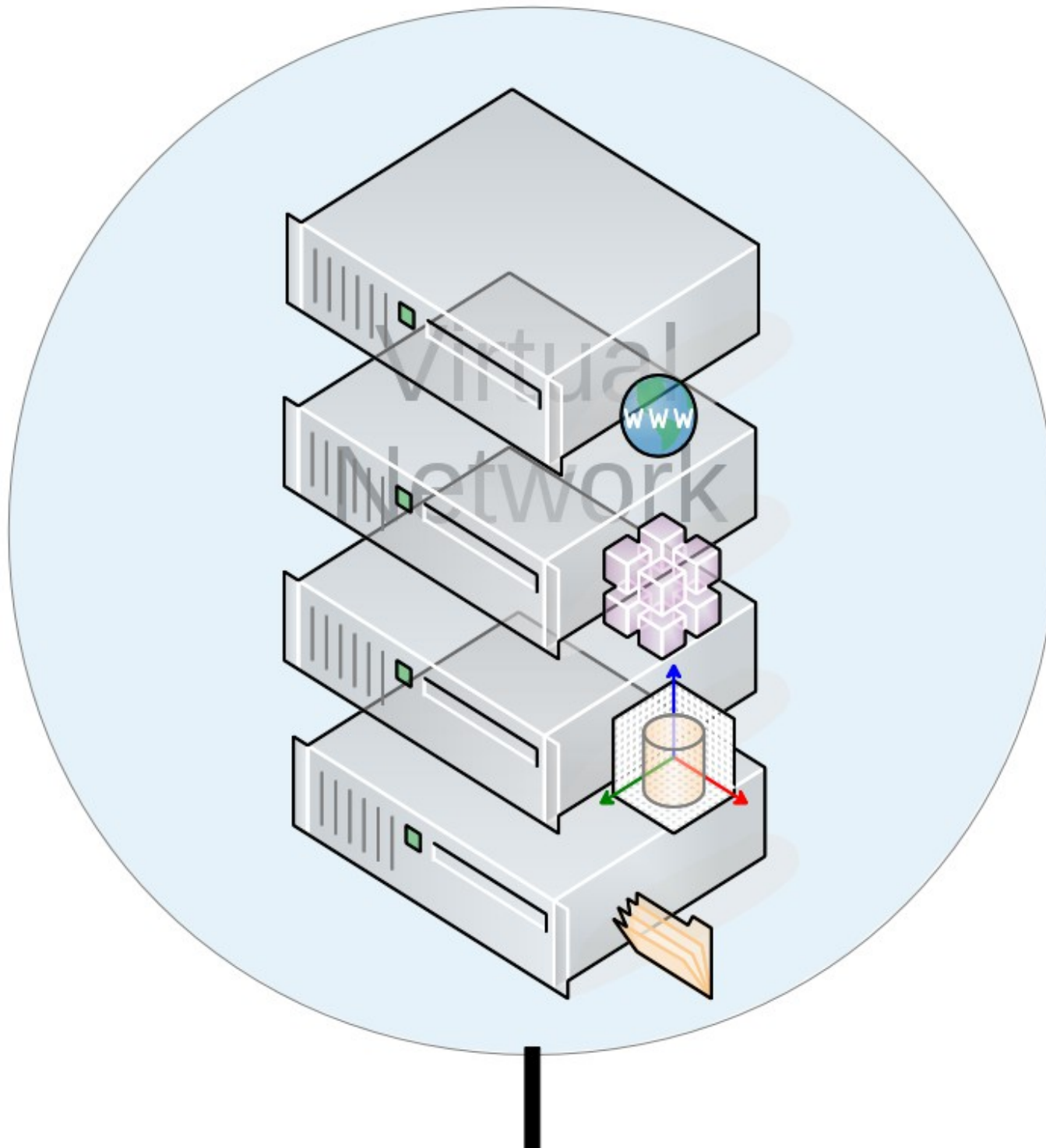


Vbox Promiscuous Mode









172.20.30.11	172.20.50.200	53	53128	17	1	89		2014/12/01T19:52:37
172.20.50.200	172.20.130.11	19117	445	6	16	7459	SRPA	2014/12/01T19:52:37
172.20.130.11	172.20.50.200	445	19117	6	12	1753	S PA	2014/12/01T19:52:37
172.20.130.11	172.20.50.200	88	19118	6	4	280	SRPA	2014/12/01T19:52:37
172.20.50.200	172.20.130.11	19118	88	6	4	1544	FS PA	2014/12/01T19:52:37
172.20.130.11	172.20.50.200	88	19119	6	4	1556	SRPA	2014/12/01T19:52:37
172.20.50.200	172.20.130.11	19119	88	6	4	1557	FS PA	2014/12/01T19:52:37
172.20.107.16	172.20.50.200	0	2048	1	358	21480		2014/12/01T19:55:25
172.20.50.200	172.20.50.255	137	137	17	6	468		2014/12/01T19:57:13
172.20.50.200	172.20.30.11	0	2048	1	2	120		2014/12/01T19:57:15
172.20.30.11	172.20.50.200	0	0	1	2	120		2014/12/01T19:57:15
172.20.30.11	172.20.50.200	137	137	17	2	442		2014/12/01T19:57:15
172.20.50.200	172.20.30.11	137	137	17	2	156		2014/12/01T19:57:15
172.20.50.200	172.20.30.11	138	138	17	1	204		2014/12/01T19:57:15
172.20.50.200	172.20.30.11	53262	53	17	1	73		2014/12/01T19:57:15
172.20.30.11	172.20.50.200	53	53262	17	1	89		2014/12/01T19:57:15
172.20.50.200	172.20.30.11	52833	53	17	1	73		2014/12/01T19:57:18
172.20.30.11	172.20.50.200	53	52833	17	1	89		2014/12/01T19:57:18
172.20.30.11	172.20.50.200	139	19120	6	10	1634	FS PA	2014/12/01T19:57:18
172.20.50.200	172.20.30.11	19120	139	6	12	1495	FS PA	2014/12/01T19:57:18
172.20.30.11	172.20.50.200	53	59318	17	1	89		2014/12/01T19:57:18
172.20.50.200	172.20.30.11	59318	53	17	1	73		2014/12/01T19:57:18
172.20.30.11	172.20.50.200	139	19121	6	11	1723	FS PA	2014/12/01T19:57:18
172.20.50.200	172.20.30.11	19121	139	6	13	1519	FS PA	2014/12/01T19:57:18
172.20.30.11	172.20.50.200	139	19122	6	12	1391	FS PA	2014/12/01T19:57:18
172.20.50.200	172.20.30.11	19122	139	6	14	4344	FS PA	2014/12/01T19:57:18
172.20.130.11	172.20.50.200	389	59319	17	1	215		2014/12/01T19:57:18
172.20.50.200	172.20.130.11	59319	389	17	1	193		2014/12/01T19:57:18
172.20.50.200	172.20.130.11	19123	88	6	4	1544	FS PA	2014/12/01T19:57:18
172.20.130.11	172.20.50.200	88	19123	6	4	280	SRPA	2014/12/01T19:57:18
172.20.130.11	172.20.50.200	88	19124	6	4	1556	SRPA	2014/12/01T19:57:18
172.20.50.200	172.20.130.11	19124	88	6	4	1557	FS PA	2014/12/01T19:57:18
172.20.30.11	172.20.50.200	53	58714	17	1	147		2014/12/01T19:57:18
172.20.50.200	172.20.30.11	58714	53	17	1	84		2014/12/01T19:57:18
172.20.50.200	172.20.30.11	56928	53	17	1	73		2014/12/01T19:57:18
172.20.30.11	172.20.50.200	53	56928	17	1	89		2014/12/01T19:57:18
172.20.30.11	172.20.50.200	389	56929	17	1	215		2014/12/01T19:57:18
172.20.50.200	172.20.30.11	56929	389	17	1	194		2014/12/01T19:57:18
172.20.50.200	172.20.50.255	138	138	17	2	464		2014/12/01T20:01:41
172.20.50.200	172.20.130.11	19125	445	6	18	8881	SRPA	2014/12/01T20:07:37
172.20.130.11	172.20.50.200	445	19125	6	13	1805	S PA	2014/12/01T20:07:37
172.20.130.11	172.20.50.200	88	19126	6	4	280	SRPA	2014/12/01T20:07:37
172.20.50.200	172.20.130.11	19126	88	6	4	1544	FS PA	2014/12/01T20:07:37
172.20.130.11	172.20.50.200	88	19127	6	4	1556	SRPA	2014/12/01T20:07:37
172.20.50.200	172.20.130.11	19127	88	6	4	1557	FS PA	2014/12/01T20:07:37
172.20.130.11	172.20.50.200	0	772	1	2	112		2014/12/01T20:07:37
172.20.50.200	172.20.50.255	137	137	17	6	468		2014/12/01T20:09:18
172.20.50.200	172.20.30.11	63035	53	17	1	73		2014/12/01T20:09:20
172.20.30.11	172.20.50.200	53	63035	17	1	89		2014/12/01T20:09:20
172.20.50.200	172.20.30.11	0	2048	1	2	120		2014/12/01T20:09:20
172.20.30.11	172.20.50.200	0	0	1	2	120		2014/12/01T20:09:20
172.20.50.200	172.20.30.11	137	137	17	2	156		2014/12/01T20:09:20
172.20.30.11	172.20.50.200	137	137	17	2	442		2014/12/01T20:09:20
172.20.50.200	172.20.30.11	138	138	17	1	204		2014/12/01T20:09:20

Monitoring Virtual Networks

The Future

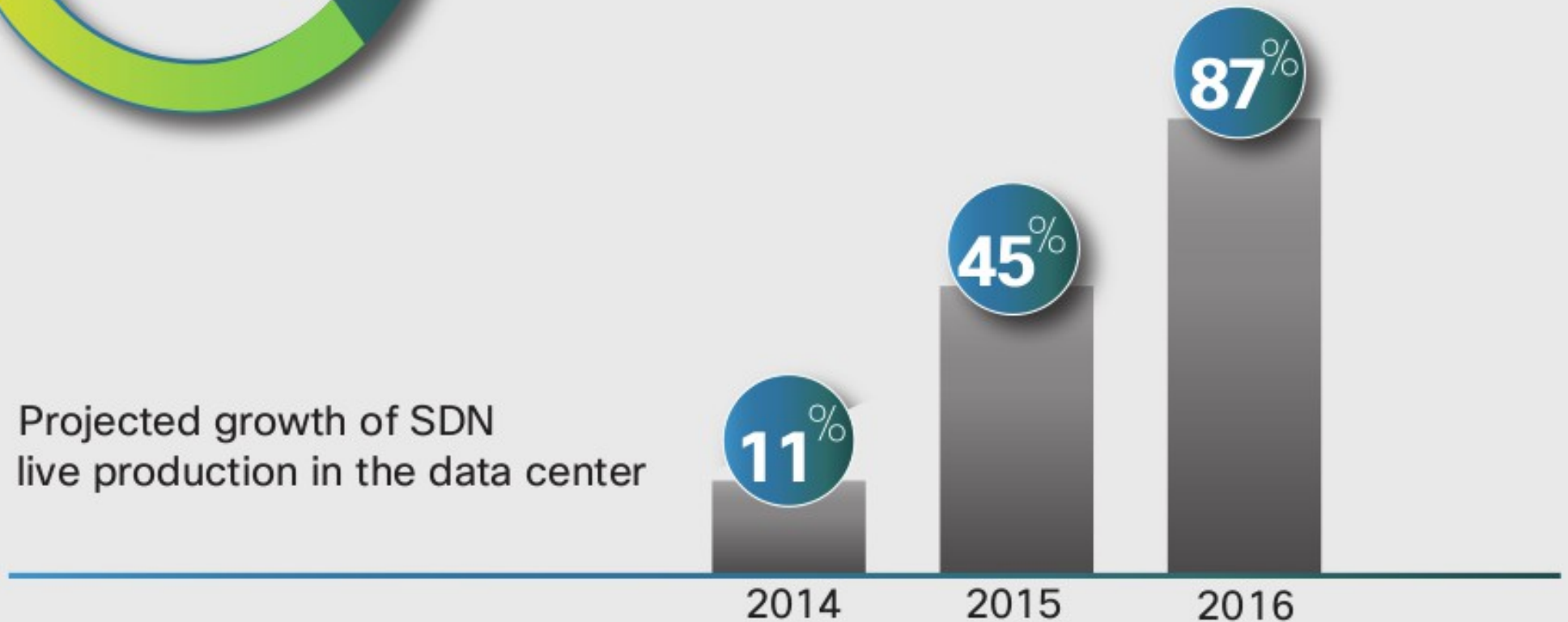




87%

An Infonetics Research survey found that 45% of respondents plan to have SDN live in production data centers in 2015, growing to 87% in 2016³

Projected growth of SDN live production in the data center



3. SDN Strategies, Infonetics Research, July 14, 2014

<http://www.cisco.com/web/solutions/trends/sdn/index.html>



©The Teneo Group 2015





About Us

- Company Information
- Events & Training
- Public Relations
- Investor Relations
- Careers

Check Point Introduces Software-defined Protection Security Architecture

Revolutionary Security Blueprint Powered by Collaborative Intelligence

581 [Retweet](#) [Share](#) [Send](#) [Print](#) [Subscribe](#)

SAN CARLOS, CA - RSA Conference 2014 — Tue, 25 Feb 2014

[Check Point® Software Technologies Ltd.](#) (Nasdaq: CHKP), the worldwide leader in securing the Internet, today introduced Software-defined Protection (SDP), a revolutionary security architecture that can protect organizations in today's fast-evolving IT and threat landscape. Software-defined Protection offers modern security today that can effectively protect against tomorrow's threats, through a design that is modular, agile and most importantly, secure.

SDP is a three-layer security architecture comprised of enforcement, control and management layers. This framework decouples the control layer from the enforcement layer, enabling robust and highly-reliable enforcement points that obtain real-time protection updates from a software-based control layer. SDP converts threat intelligence into immediate protections and is managed by a modular and open management structure.

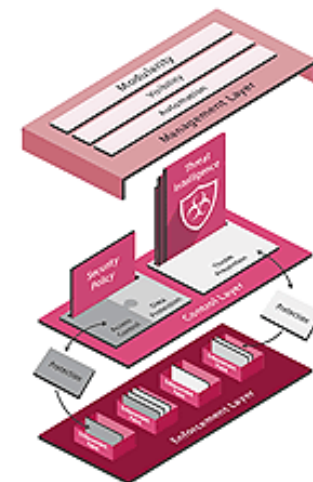
"The threat landscape has become far more sophisticated while at the same time, enterprise IT environments have grown in complexity. Enterprises are looking for advice on how they can become more

SOFTWARE-DEFINED PROTECTION

MANAGEMENT LAYER
Integrates security with business process

CONTROL LAYER
Delivers real-time protections to the enforcement points

ENFORCEMENT LAYER
Inspects traffic and enforces protection in well-defined segments



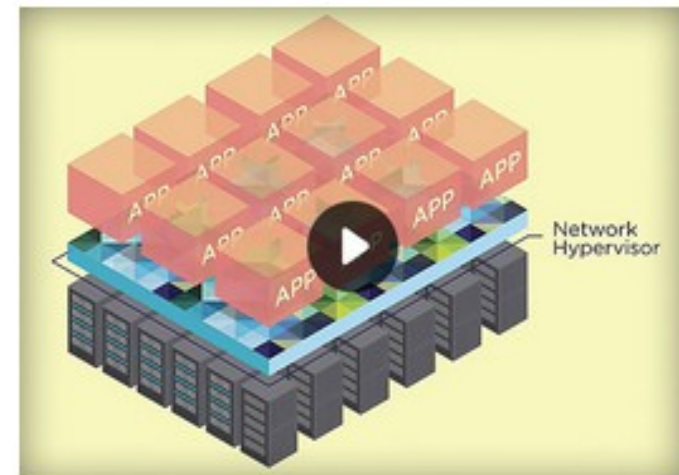
[Home](#) / [Products](#) / [NSX](#)

NSX

[Overview](#)[Features](#)[Resources](#)[Getting Started](#)

VMware NSX™ is the network virtualization platform for the Software-Defined Data Center (SDDC).

By bringing the operational model of a virtual machine to your data center network, you can transform the economics of network and security operations. NSX lets you treat your physical network as a pool of transport capacity, with network and security services attached to VMs with a policy-driven approach.



NSX technology reduces network provisioning time from days to seconds. (4:08 min)

Monitoring Virtual Networks

George Warnagiris

**www.TheTeneoGroup.com
[@TeneoGroup](https://twitter.com/TeneoGroup)**