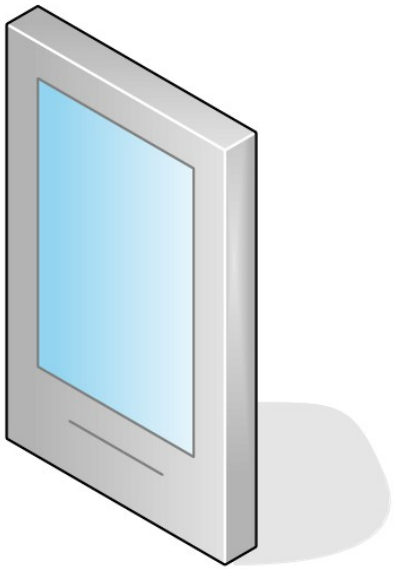
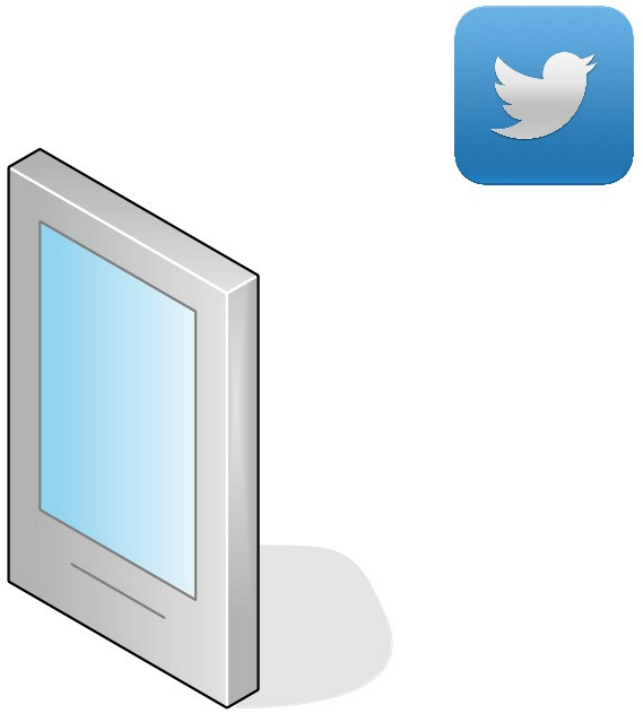
Monitoring Virtual Networks

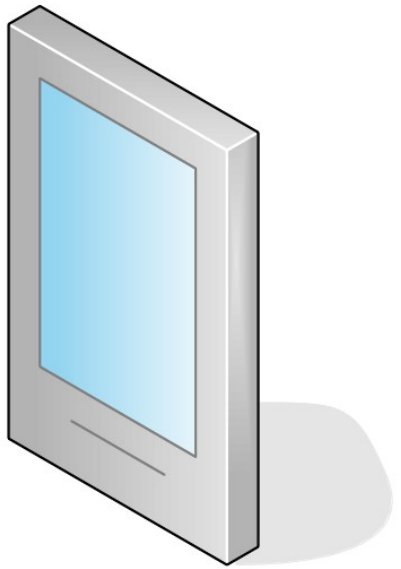
George Warnagiris

Geo@TheTeneoGroup.com
@TeneoGroup

THE TENEO GROUP

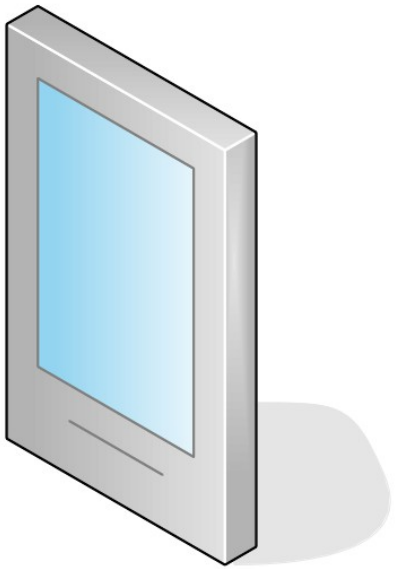






#FloCon2015

@TeneoGroup



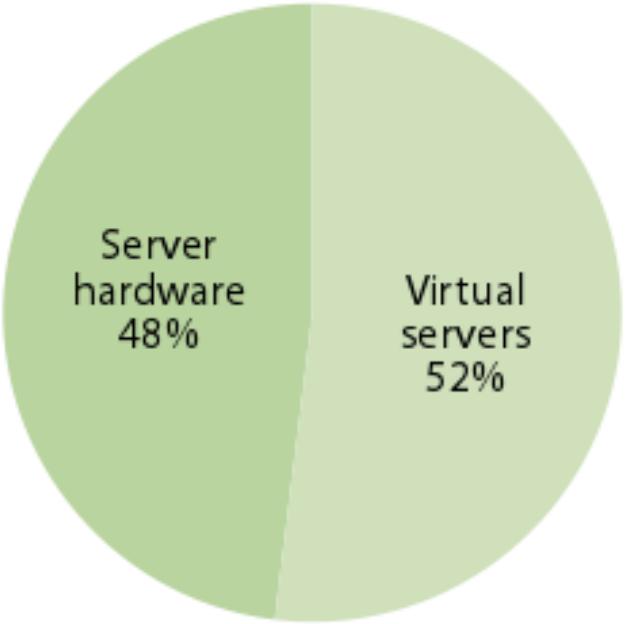
#FloCon2015

Overview

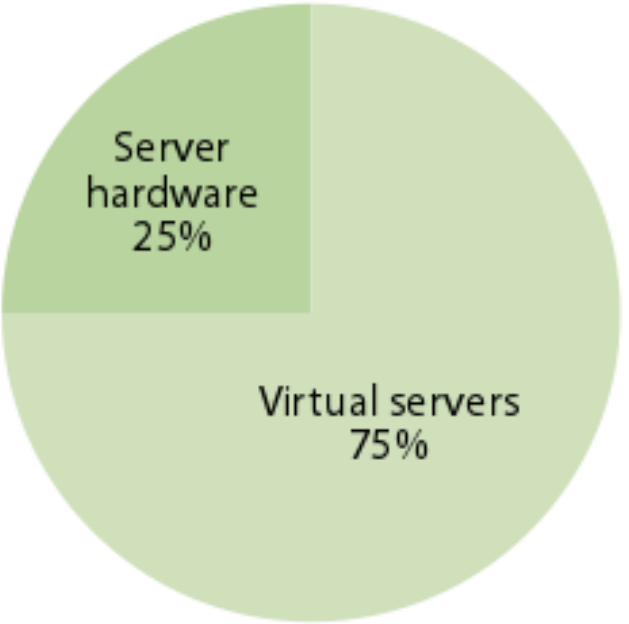
- **Background**
- **The Problem**
- **The Solution**
- **Going Forward**

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

Source: Forrester Research, Inc.

Monitoring Cloud Computing by Layer, Part 1

Jonathan Spring
Software Engineering Institute

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 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- provider must formulate personnel policies with full appreciation of the observed increase in malicious insiders' involvement in security breaches[3] 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-

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

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

DOI:10.1145/1721654.1721672

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."

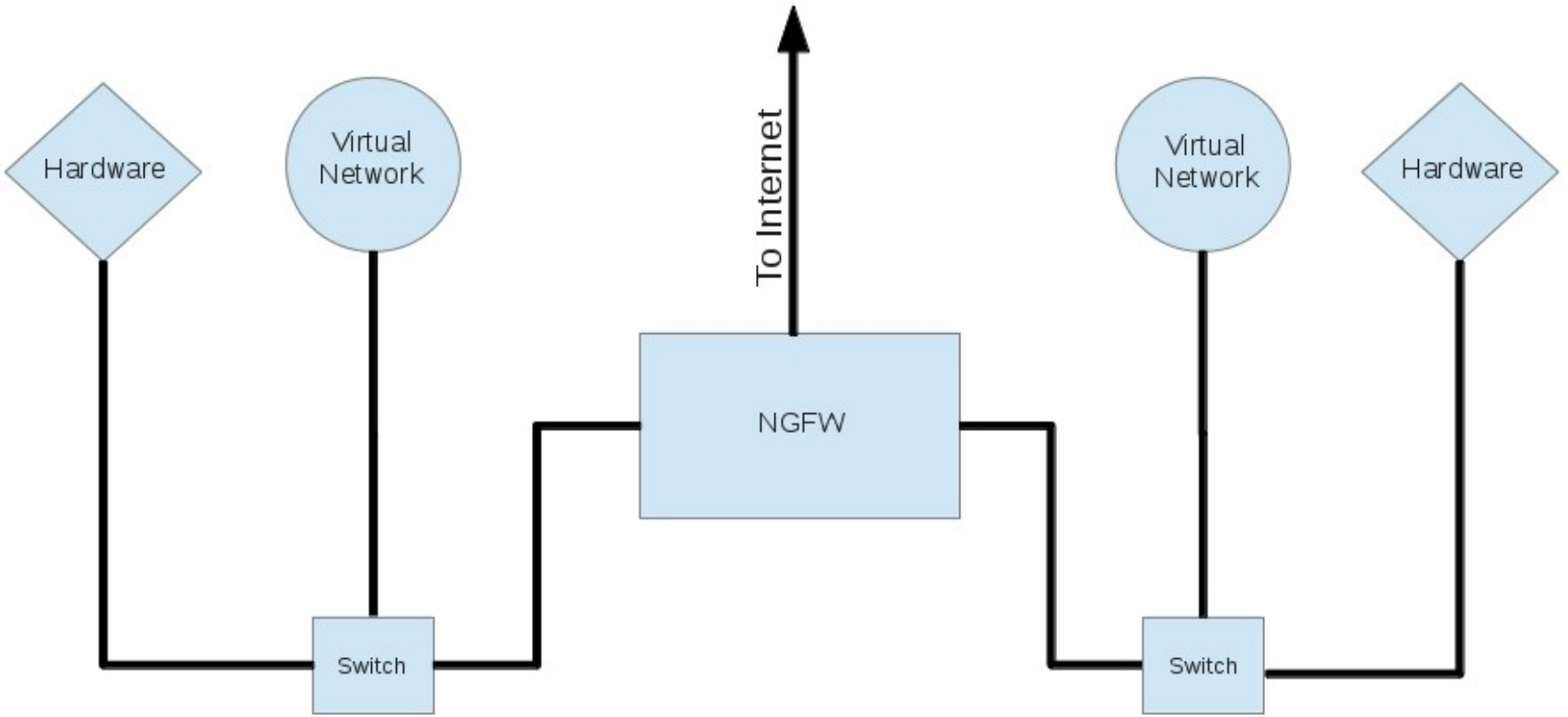
Our goal in this article is to reduce that confusion by clarifying terms, providing simple figures to quantify comparisons between of cloud and conventional computing, and identifying the top technical and non-technical obstacles and opportunities of cloud computing. (Armbrust et al[4] is a more detailed version of this article.)

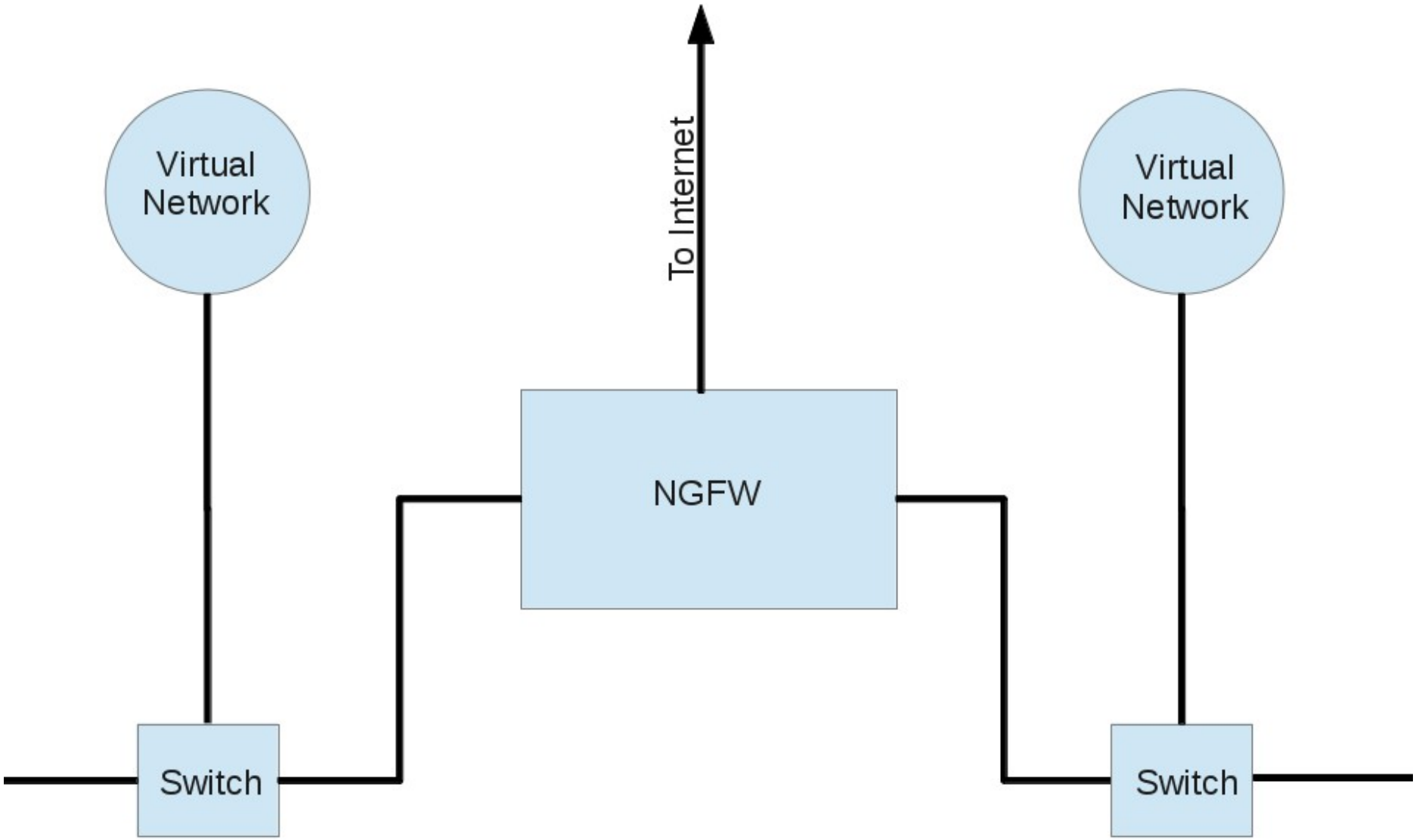
Defining Cloud Computing

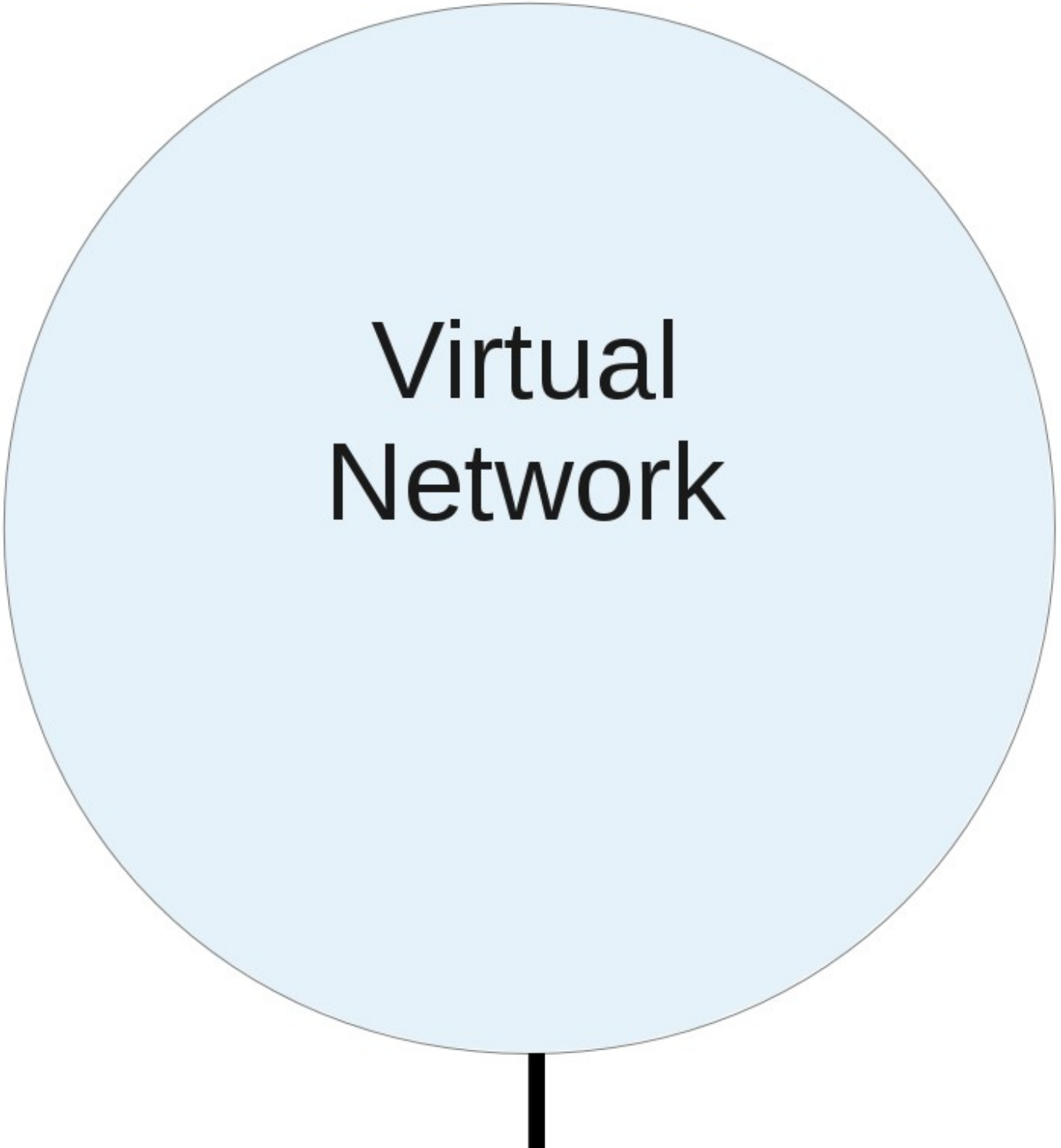
Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS).[a] Some vendors use terms such as IaaS (Infra-

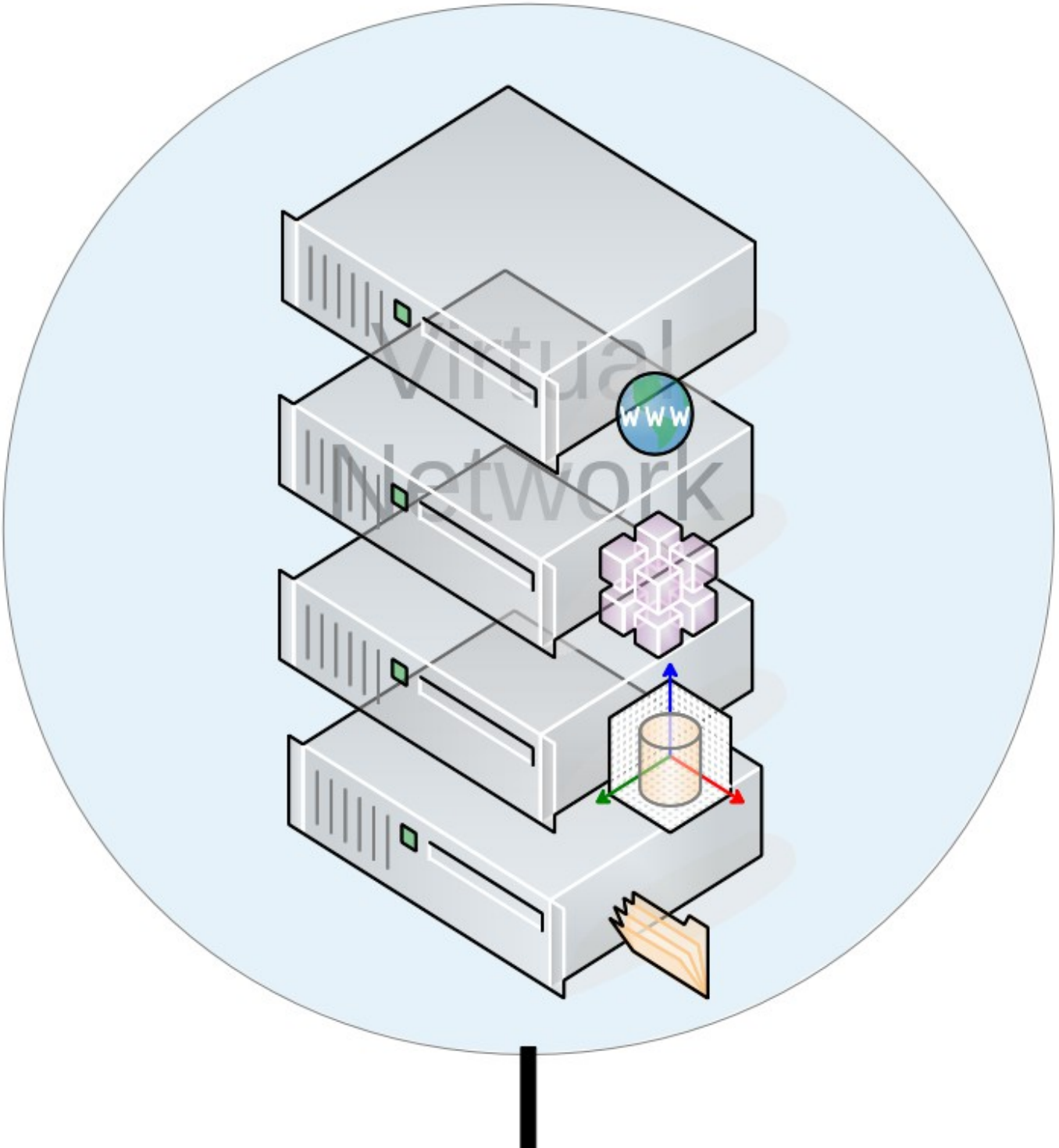
Cloud Computing - The applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.

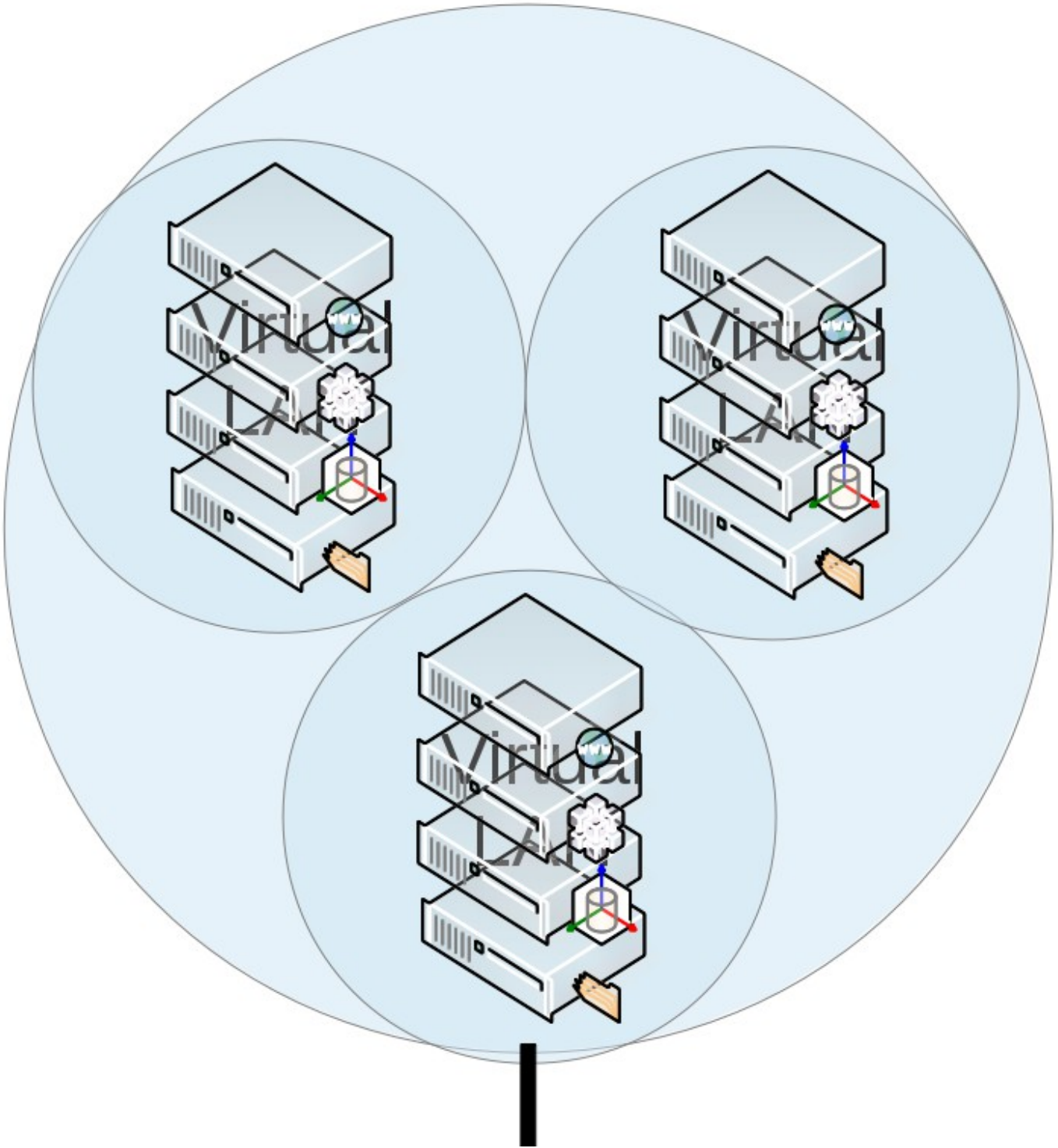
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. 2010. A View of Cloud Computing. Communications of the ACM 53, 50–58.

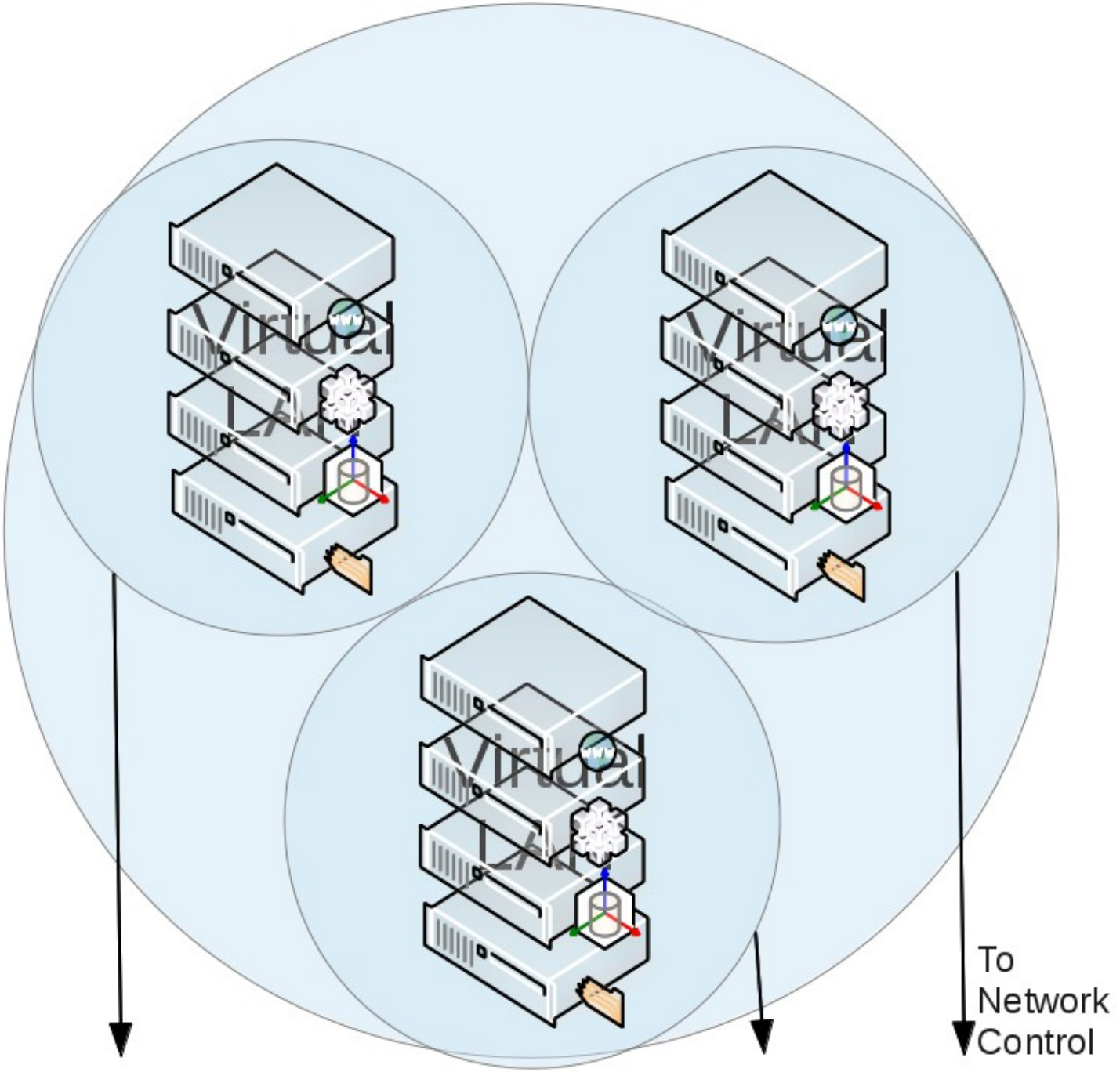

Hardware
Virtual Network
To Internet
Virtual Network
Hardware
NGFW
Switch
Switch

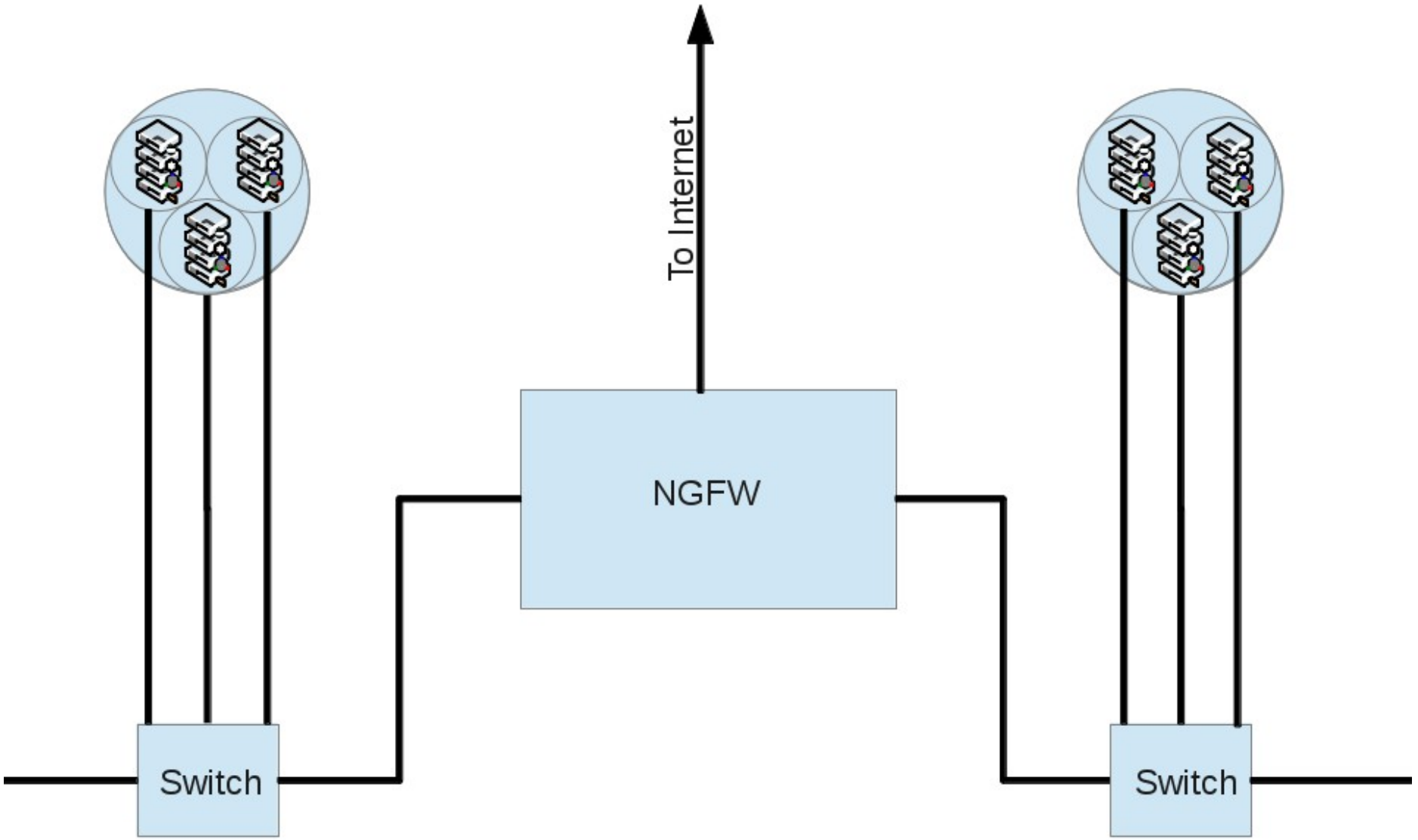

Virtual Network
To Internet
Virtual Network
NGFW
Switch
Switch

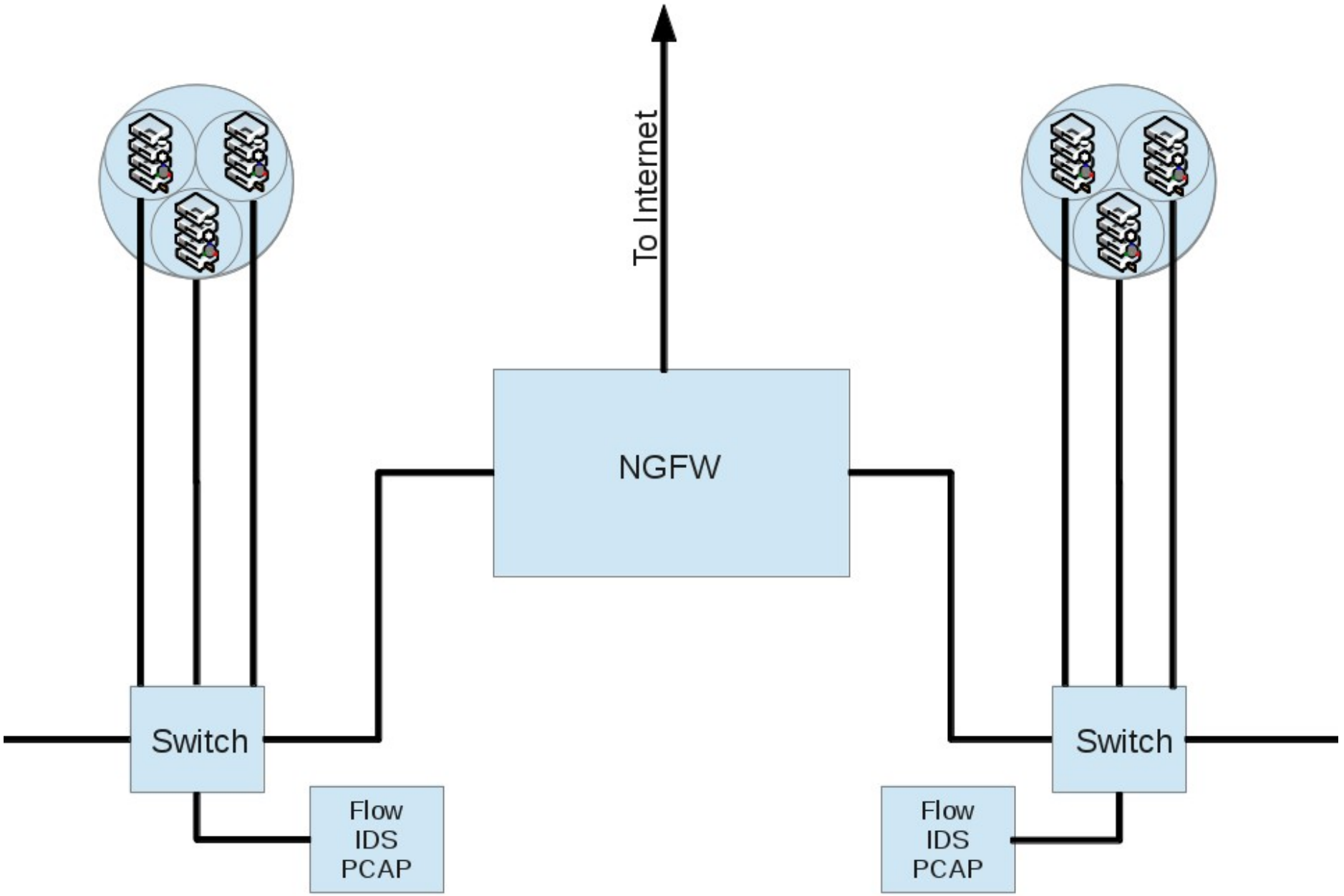

Virtual
Network

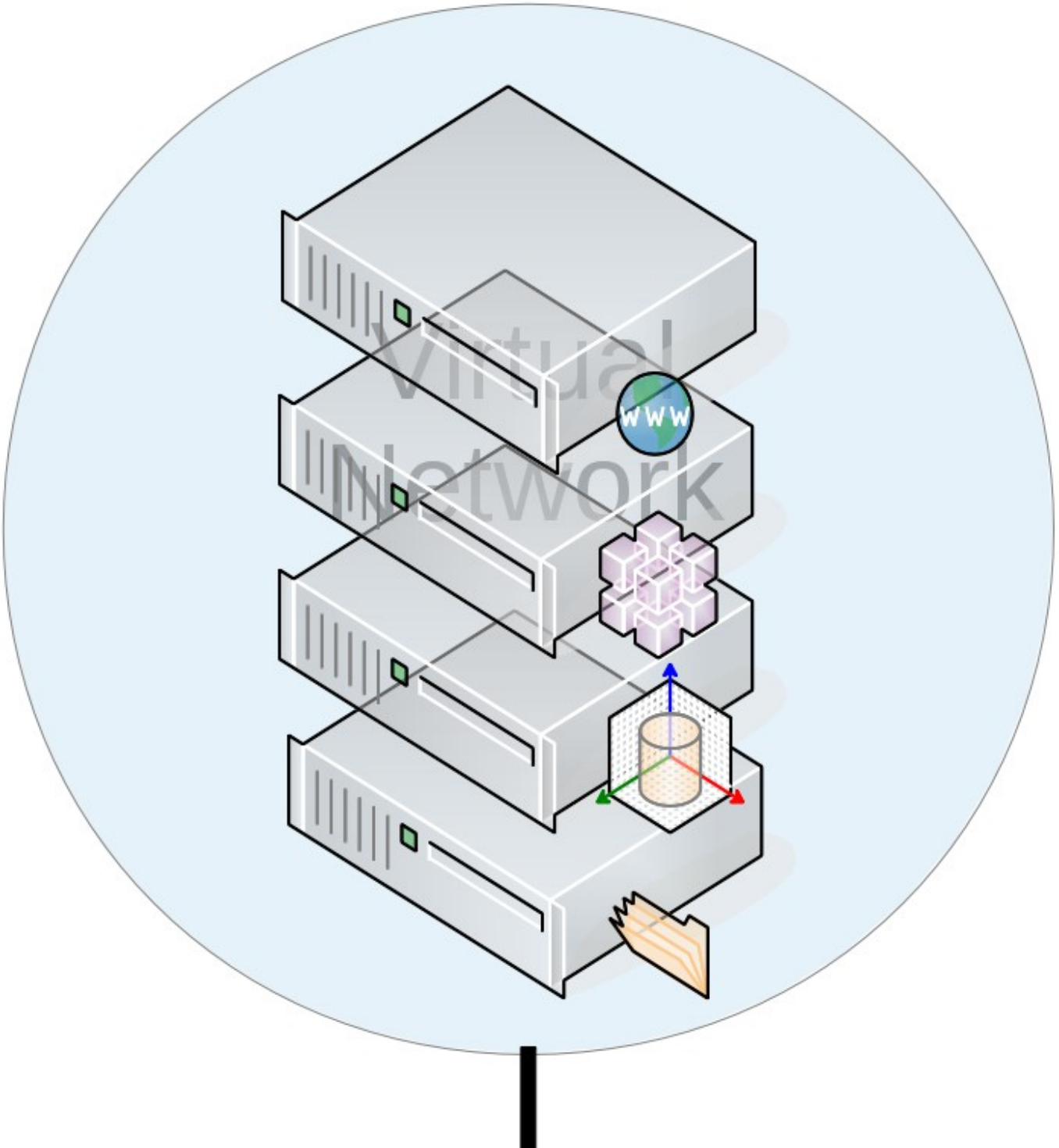

Virtual
Network
WWW

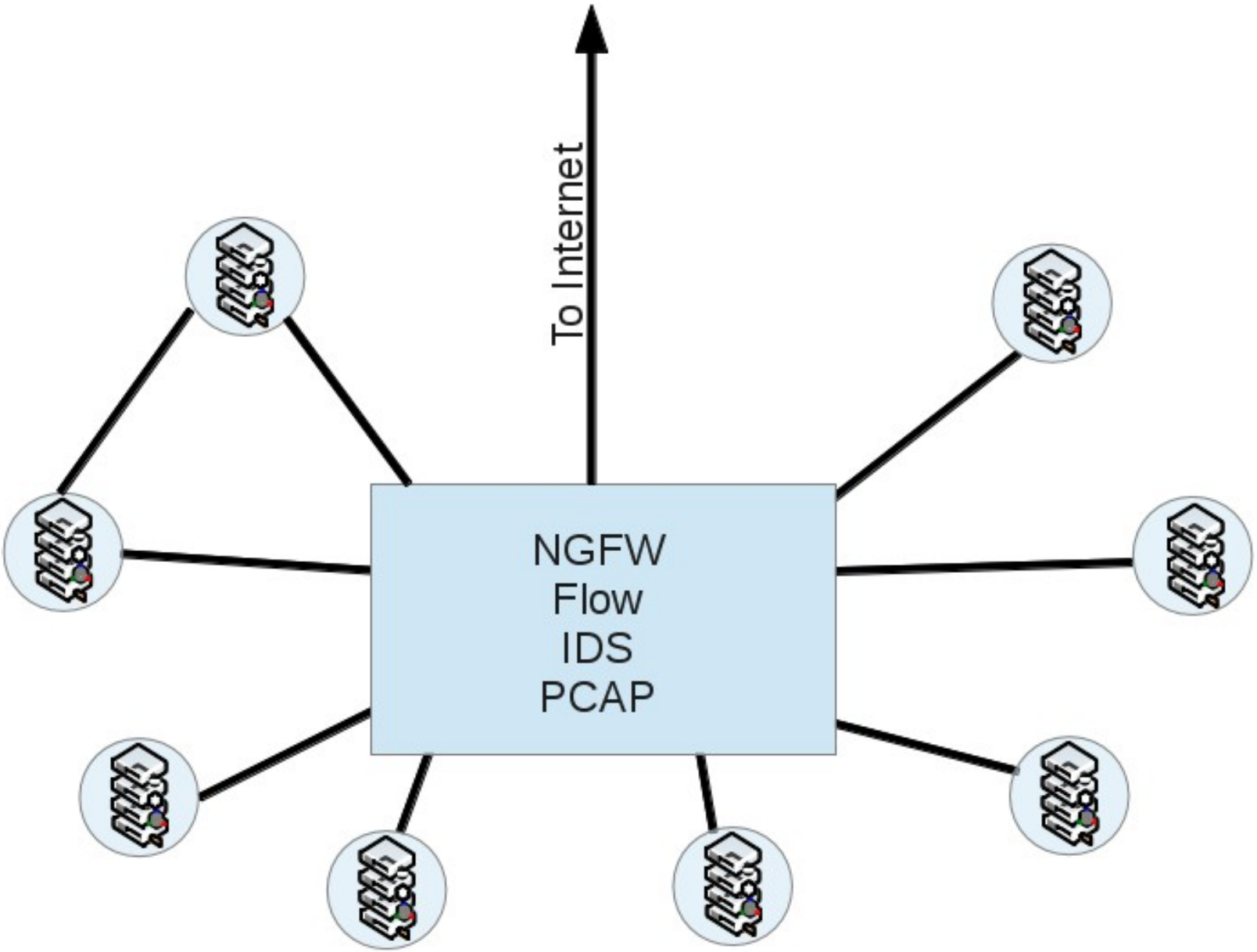

Virtual
LAN
Virtual
LAN
Virtual
LAN

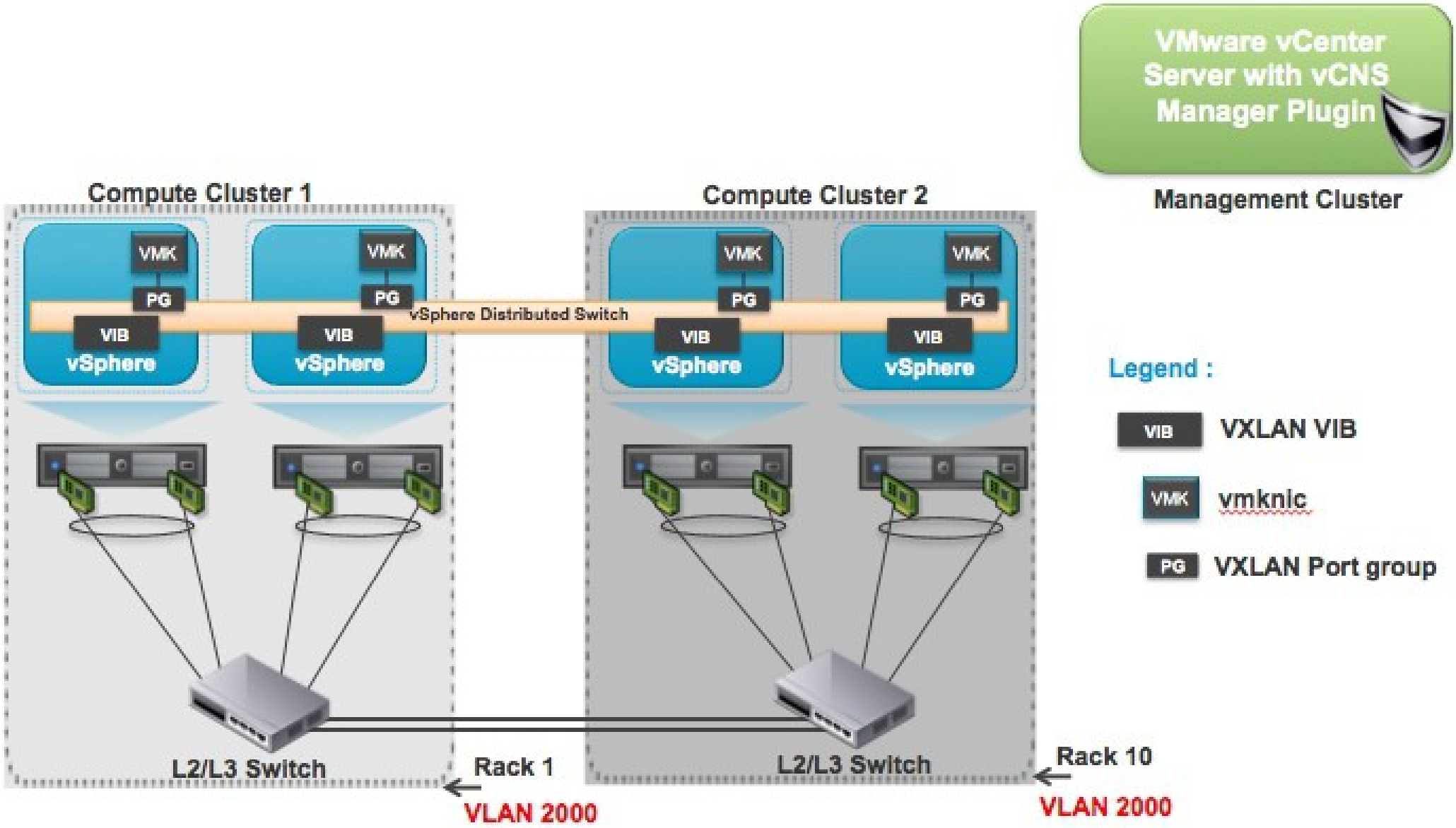

To
Network
Control


To Internet
NGFW
Switch
Switch

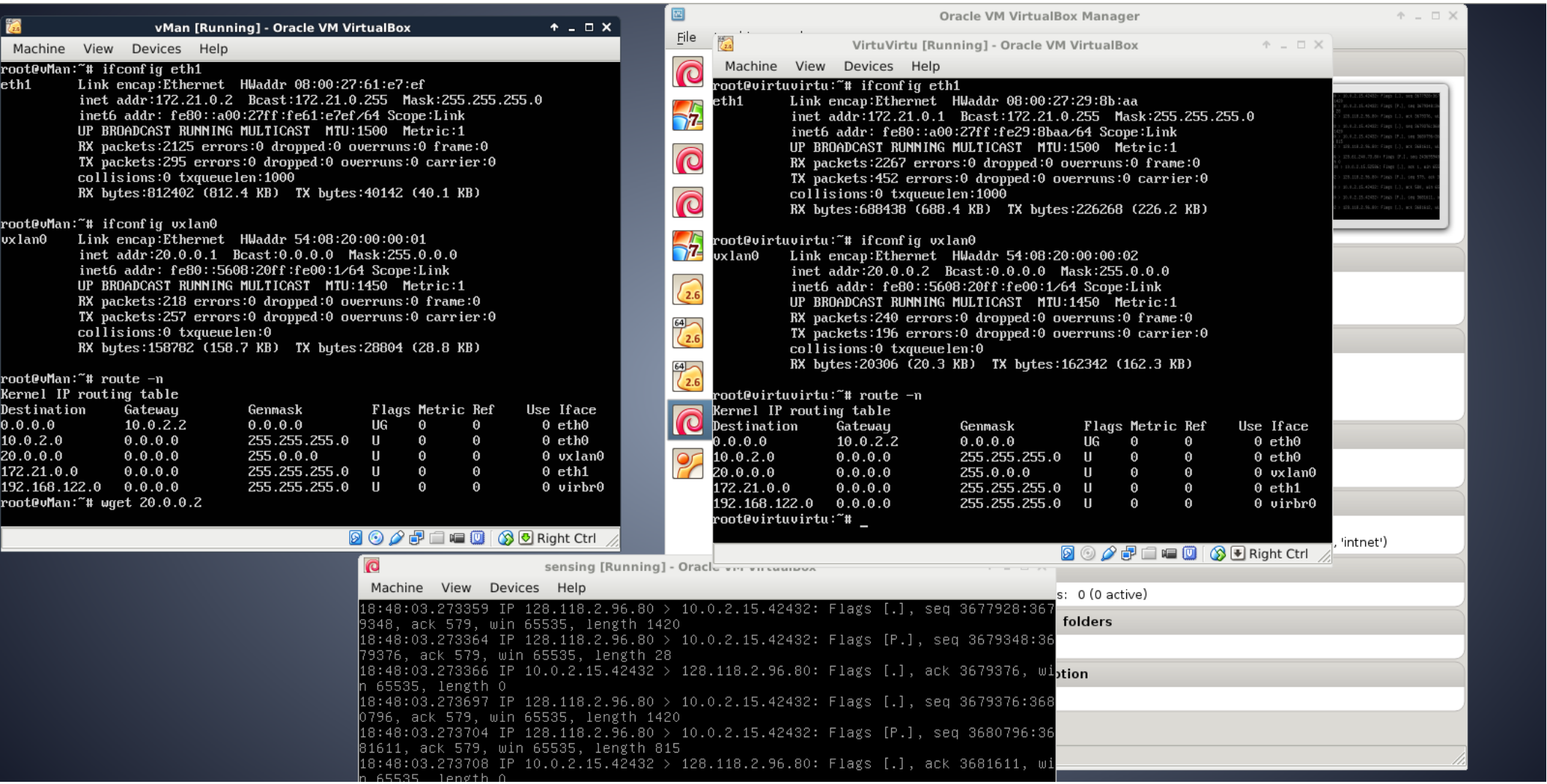

To Internet
NGFW
Switch
Switch
Flow
IDS
PCAP
Flow
IDS
PCAP

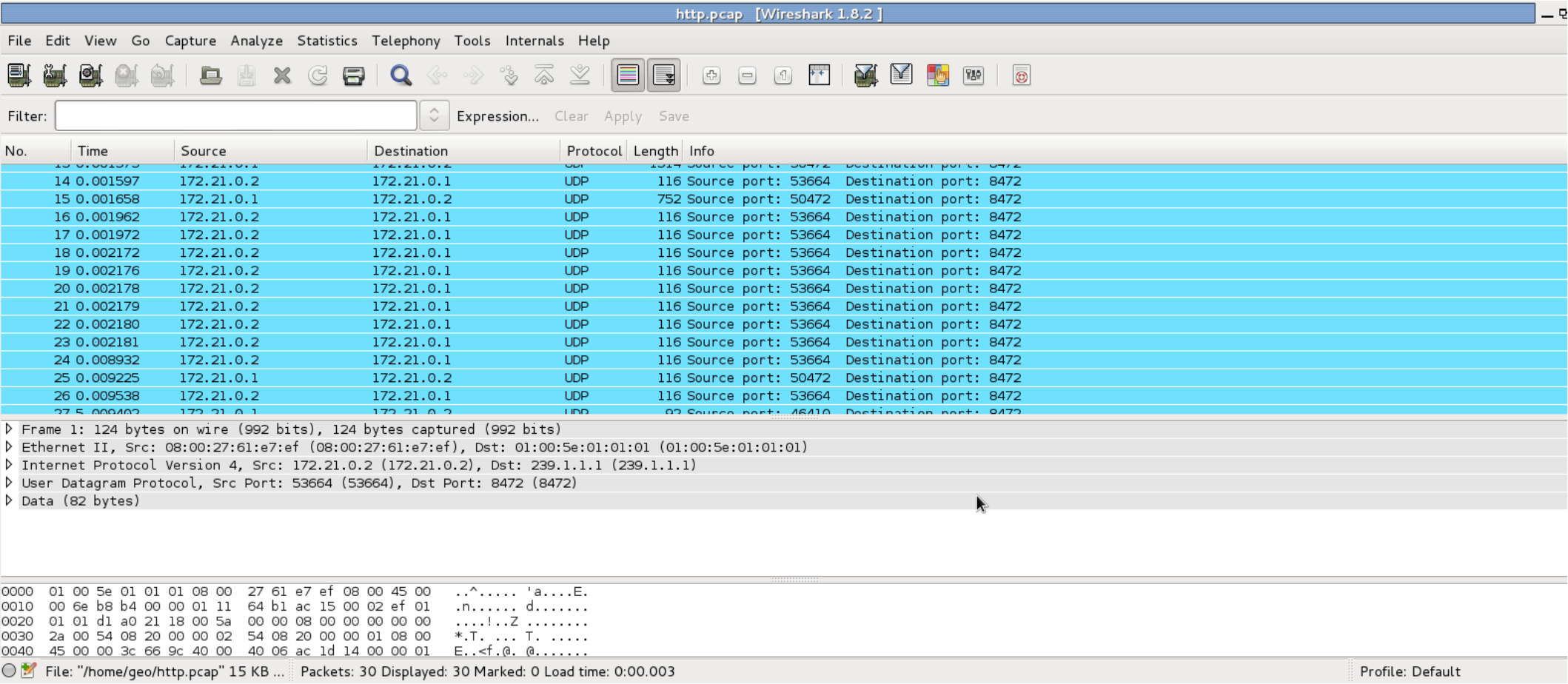

Virtual
Network
WWW

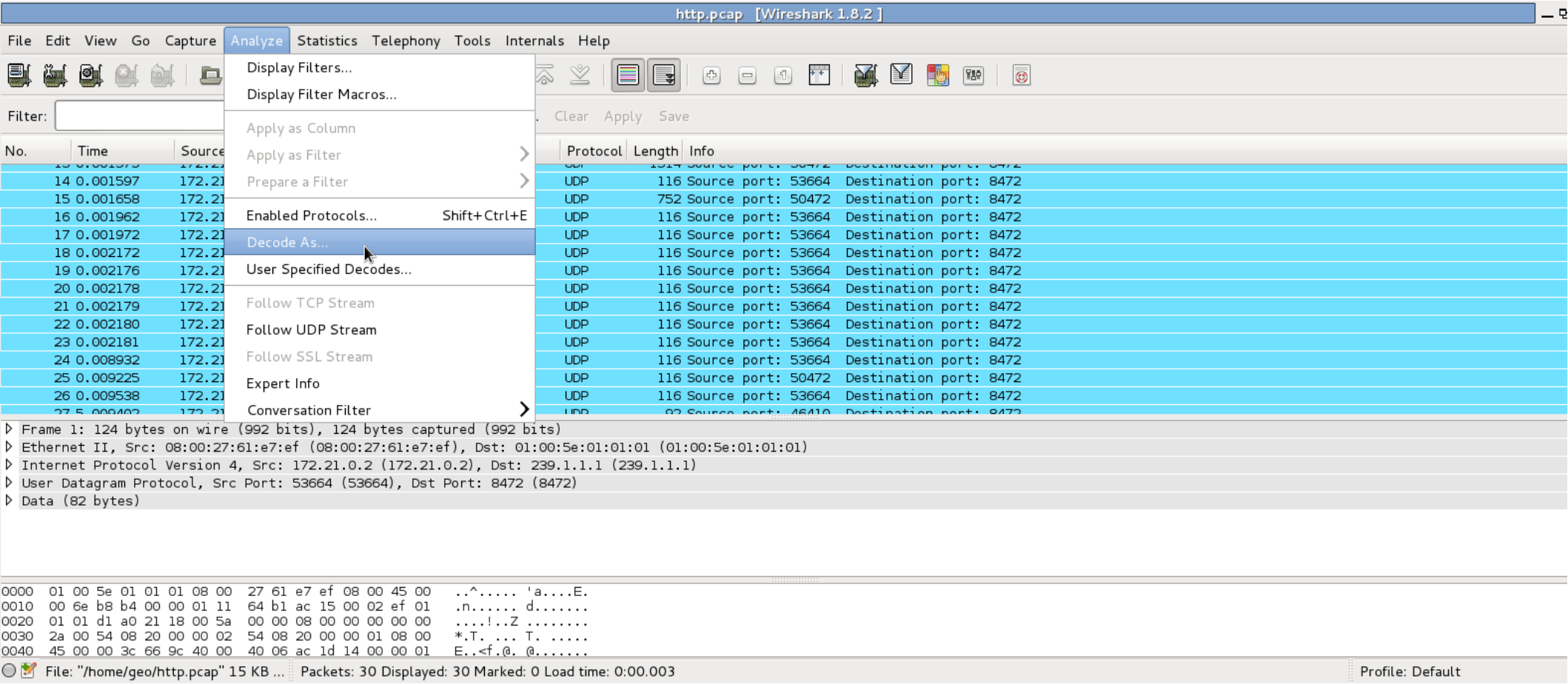

To Internet
NGFW
Flow
IDS
PCAP

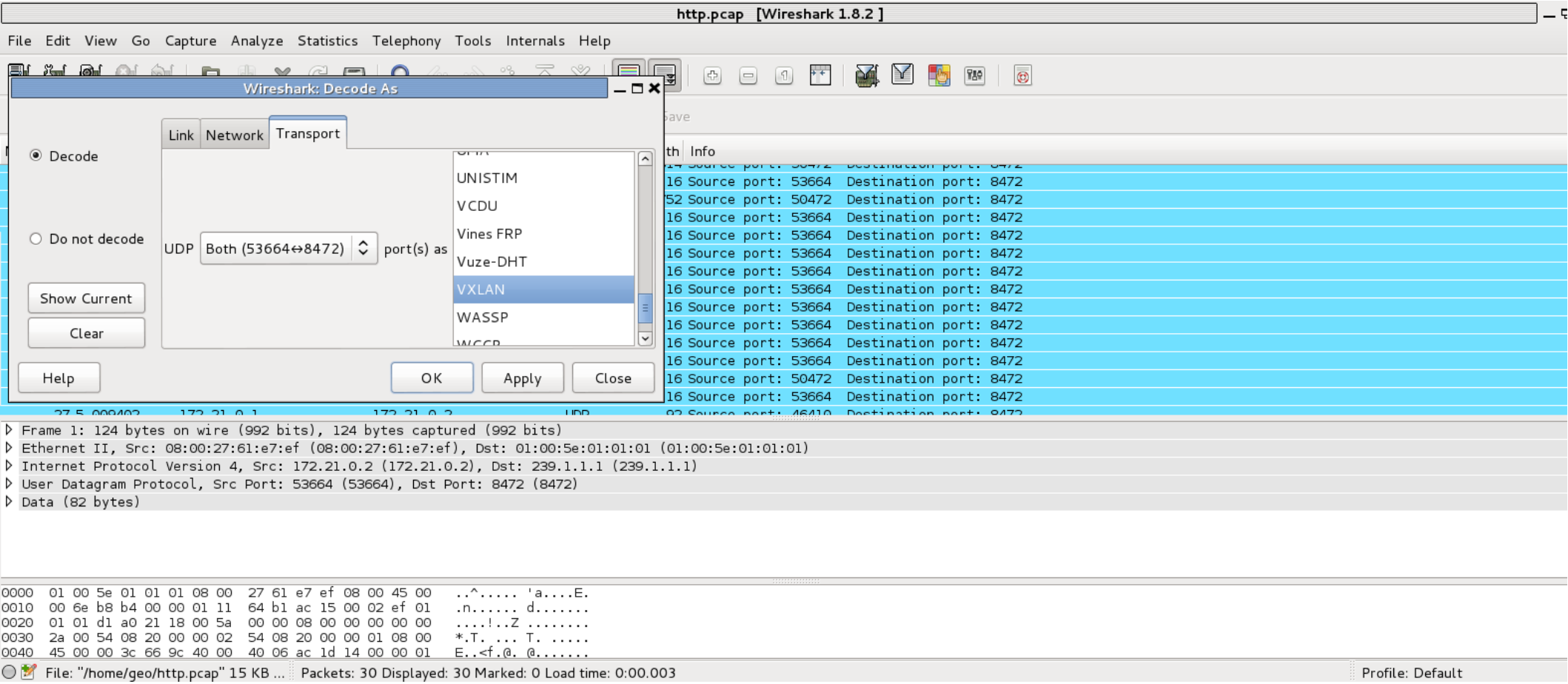


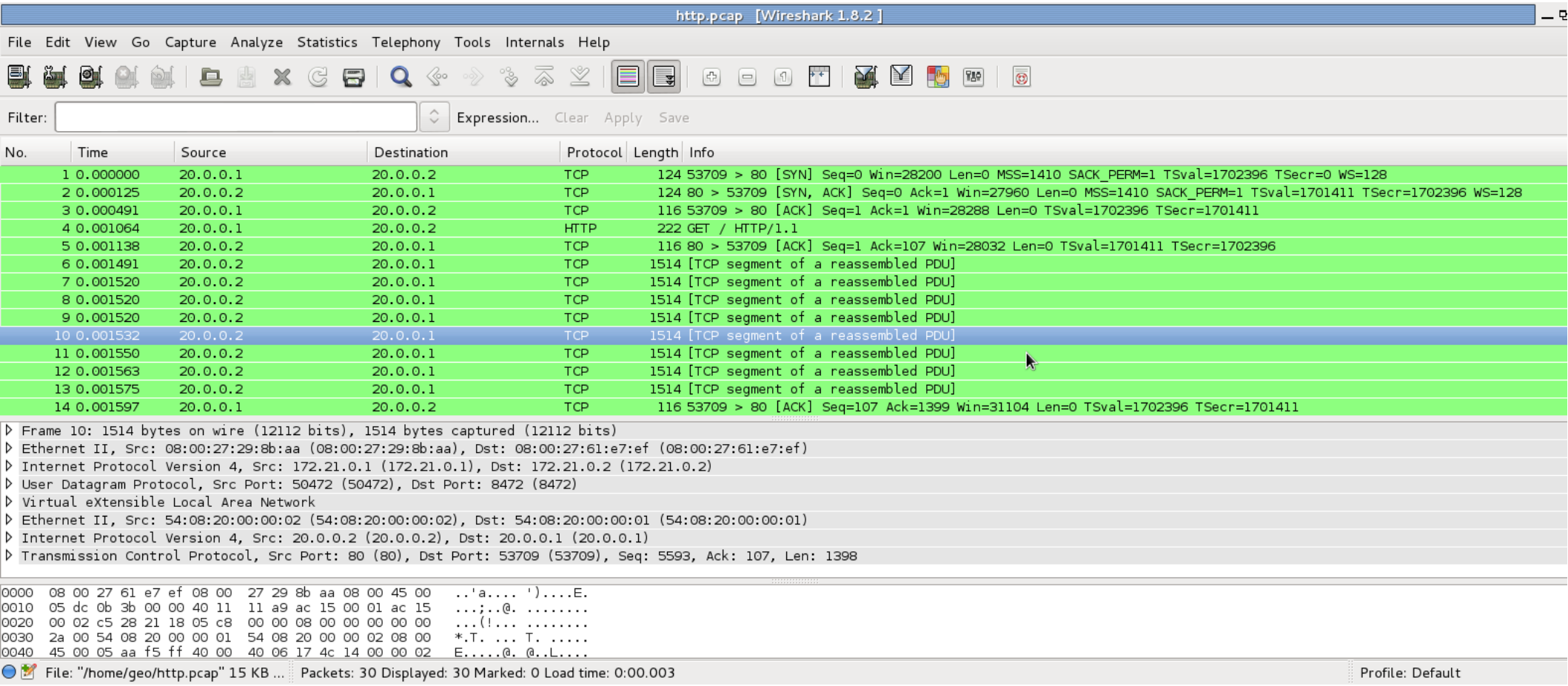
http://blogs.vmware.com/vsphere/2013/04/vxlan-series-different-components-part-1.html





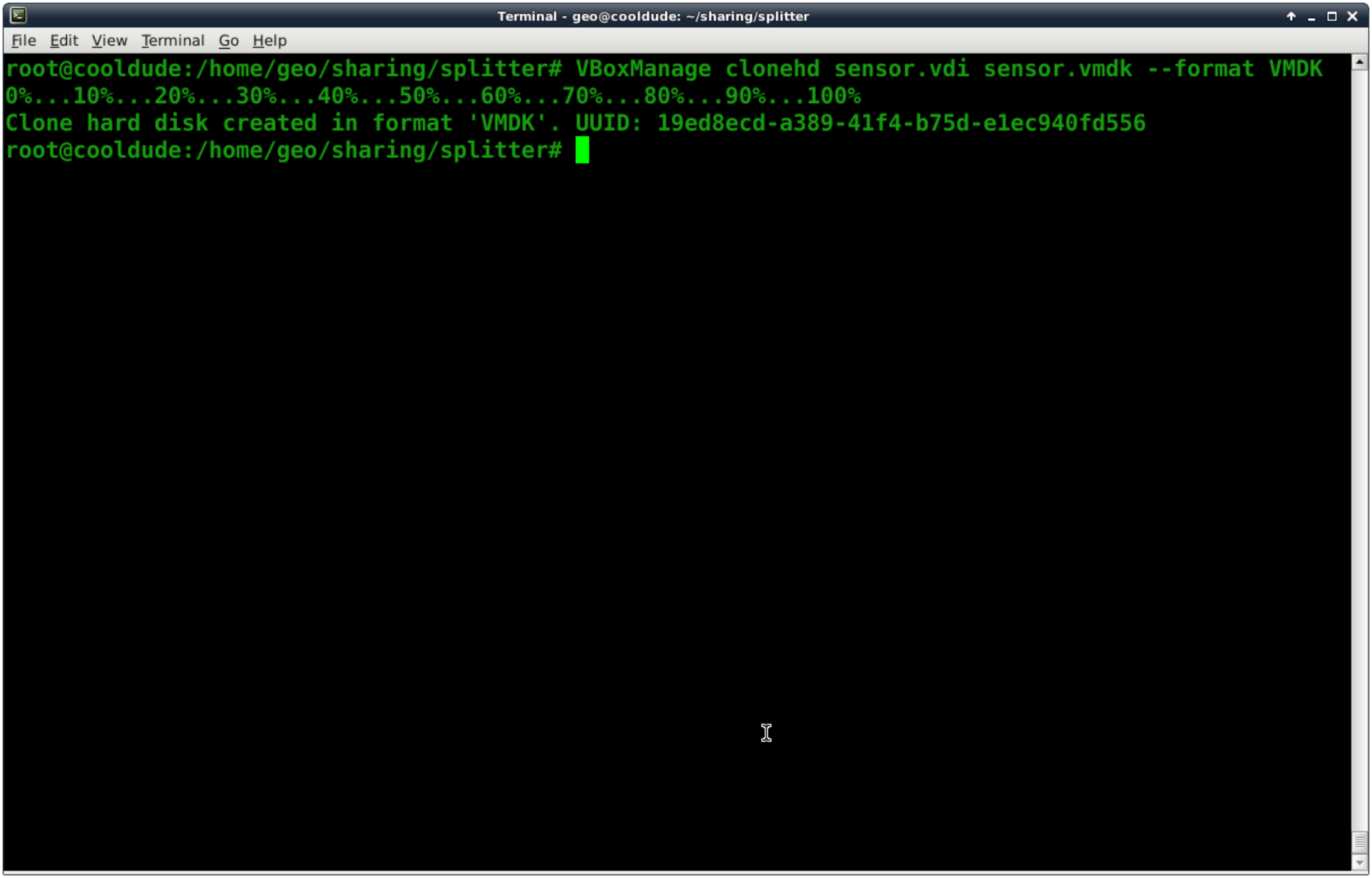


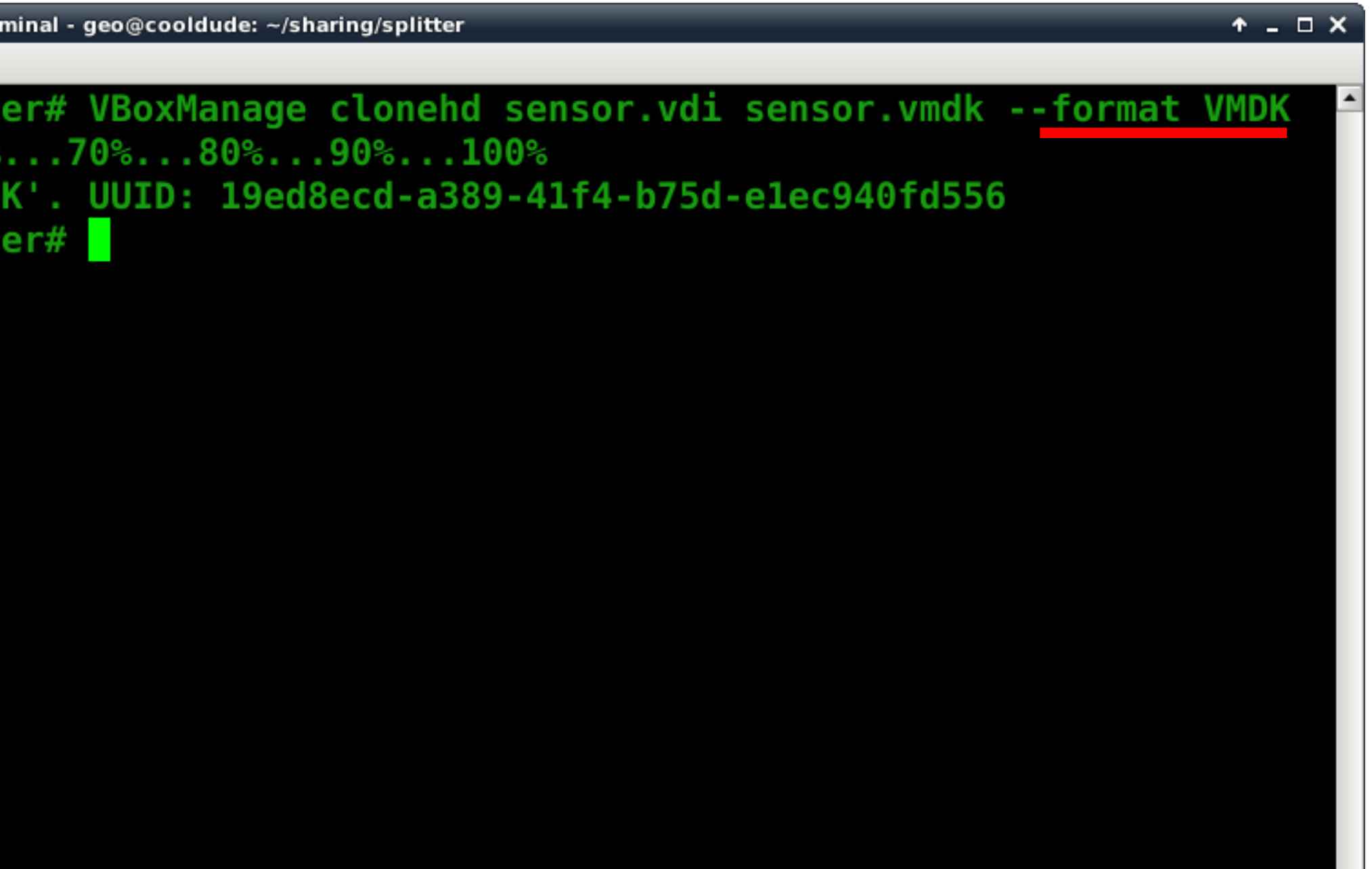




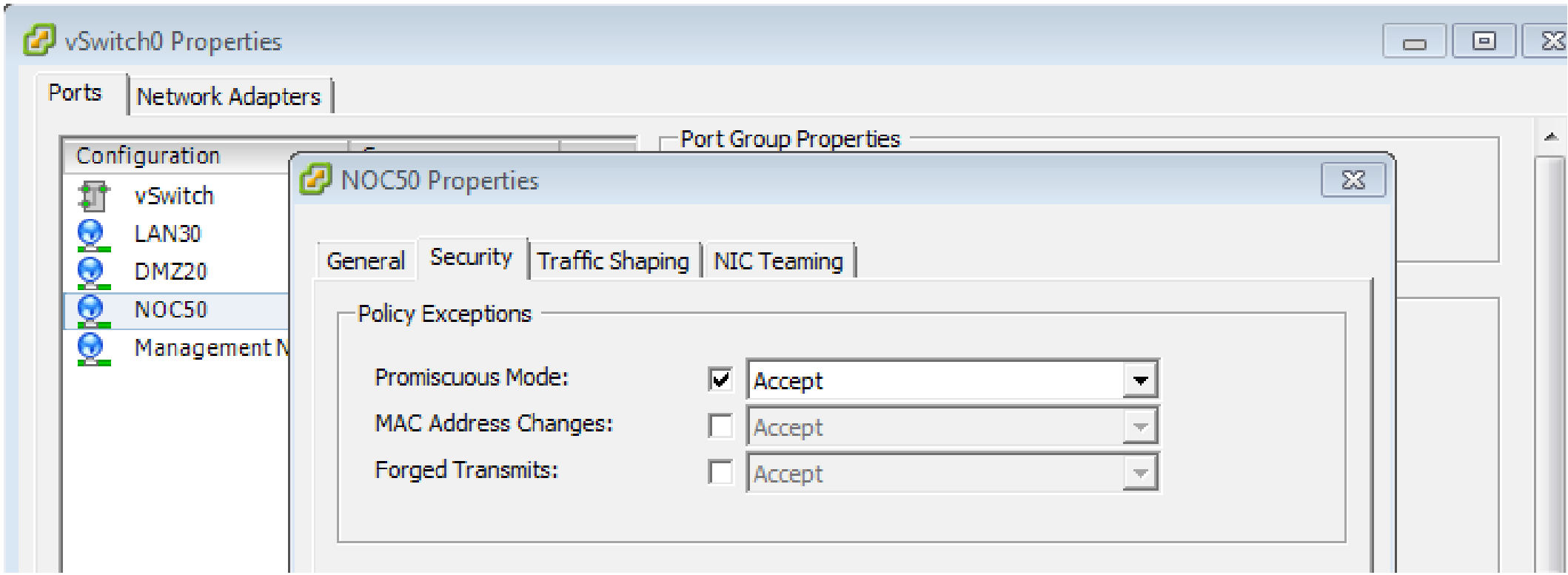
Monitoring Virtual Networks

Virtual Sensors

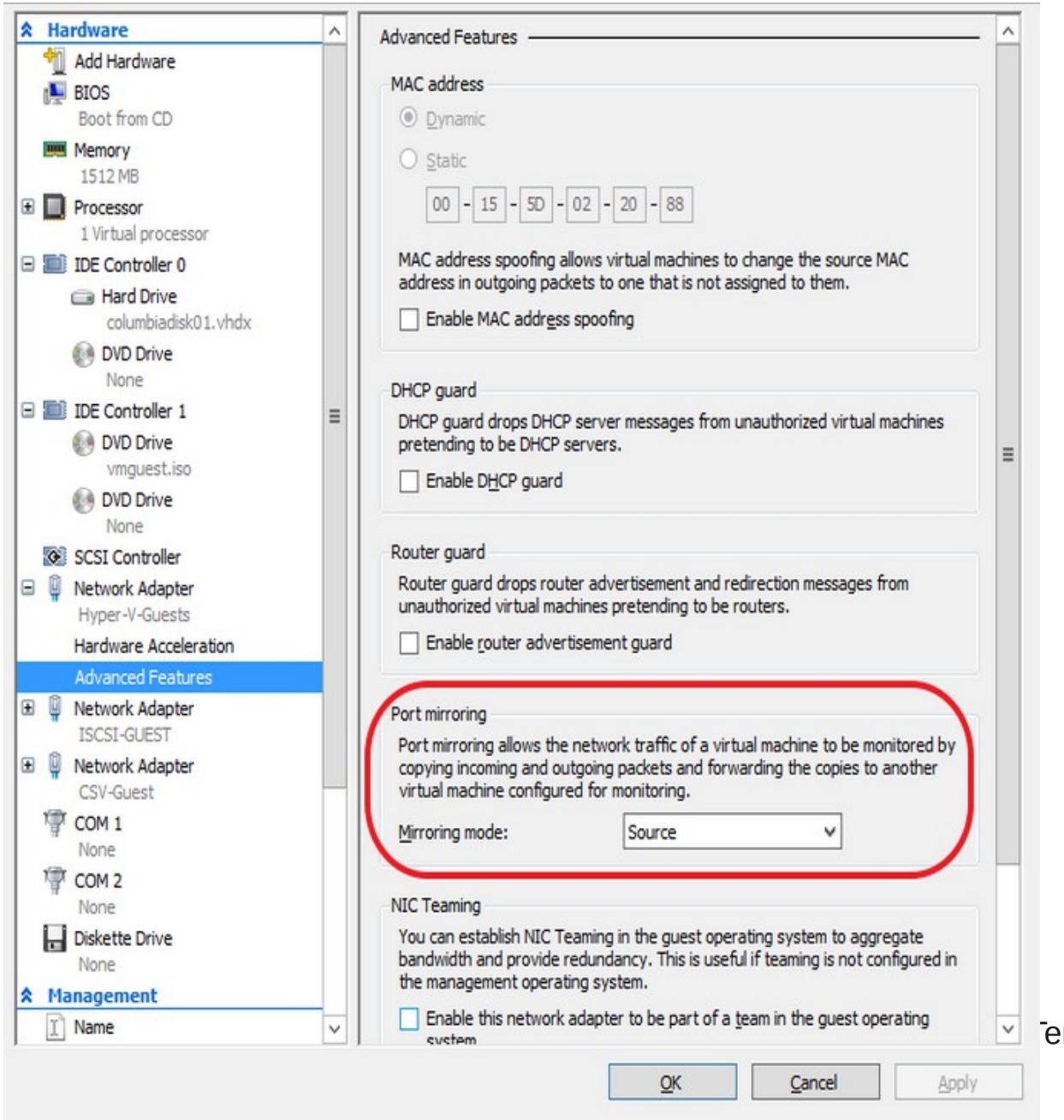



minal - geo@cooldude: ~/sharing/splitter
er# VBoxManage clonehd sensor.vdi sensor.vmdk --format VMDK
...70%...80%...90%...100%
K'. UUID: 19ed8ecd-a389-41f4-b75d-e1ec940fd556
er#

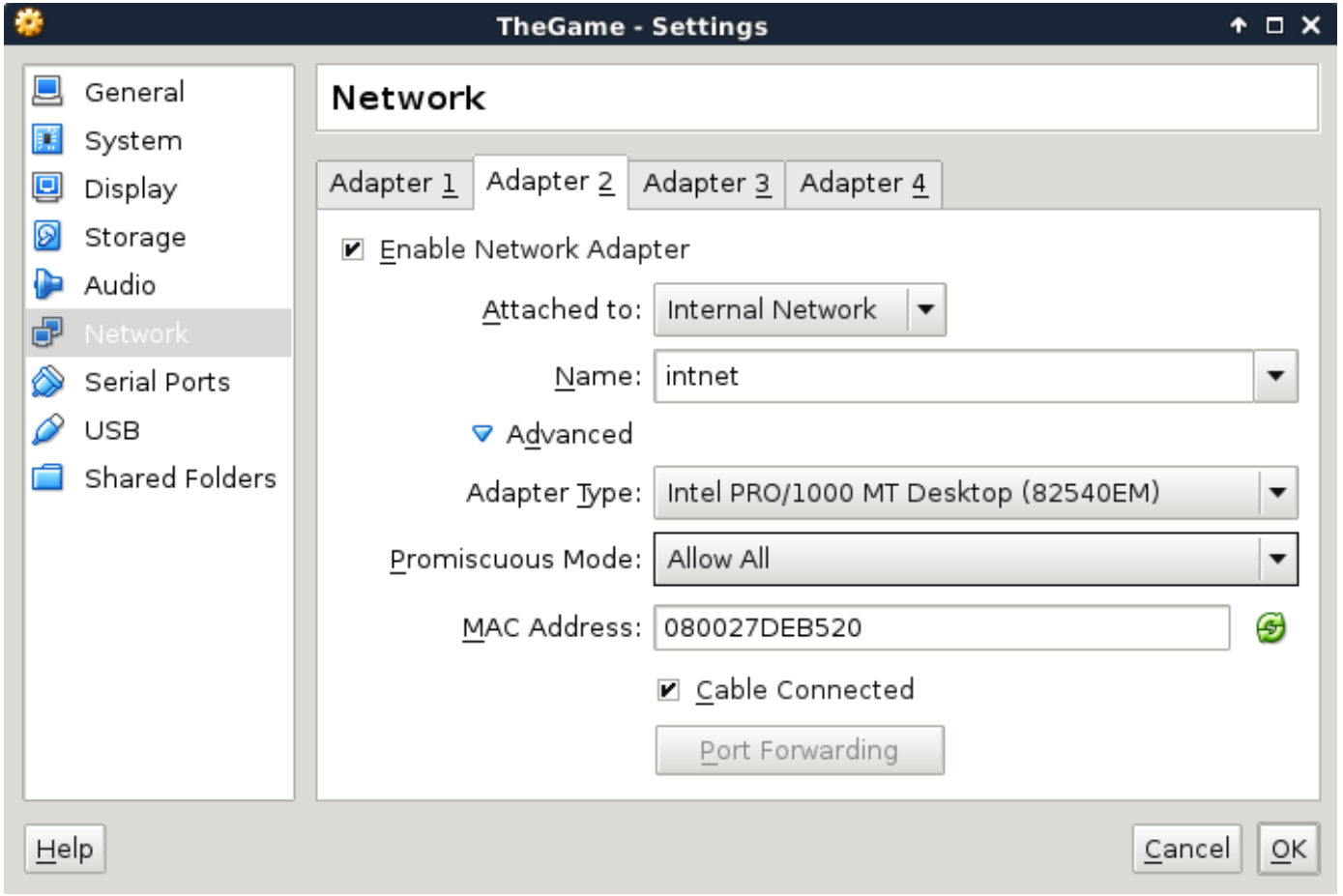
VMware Port Groups

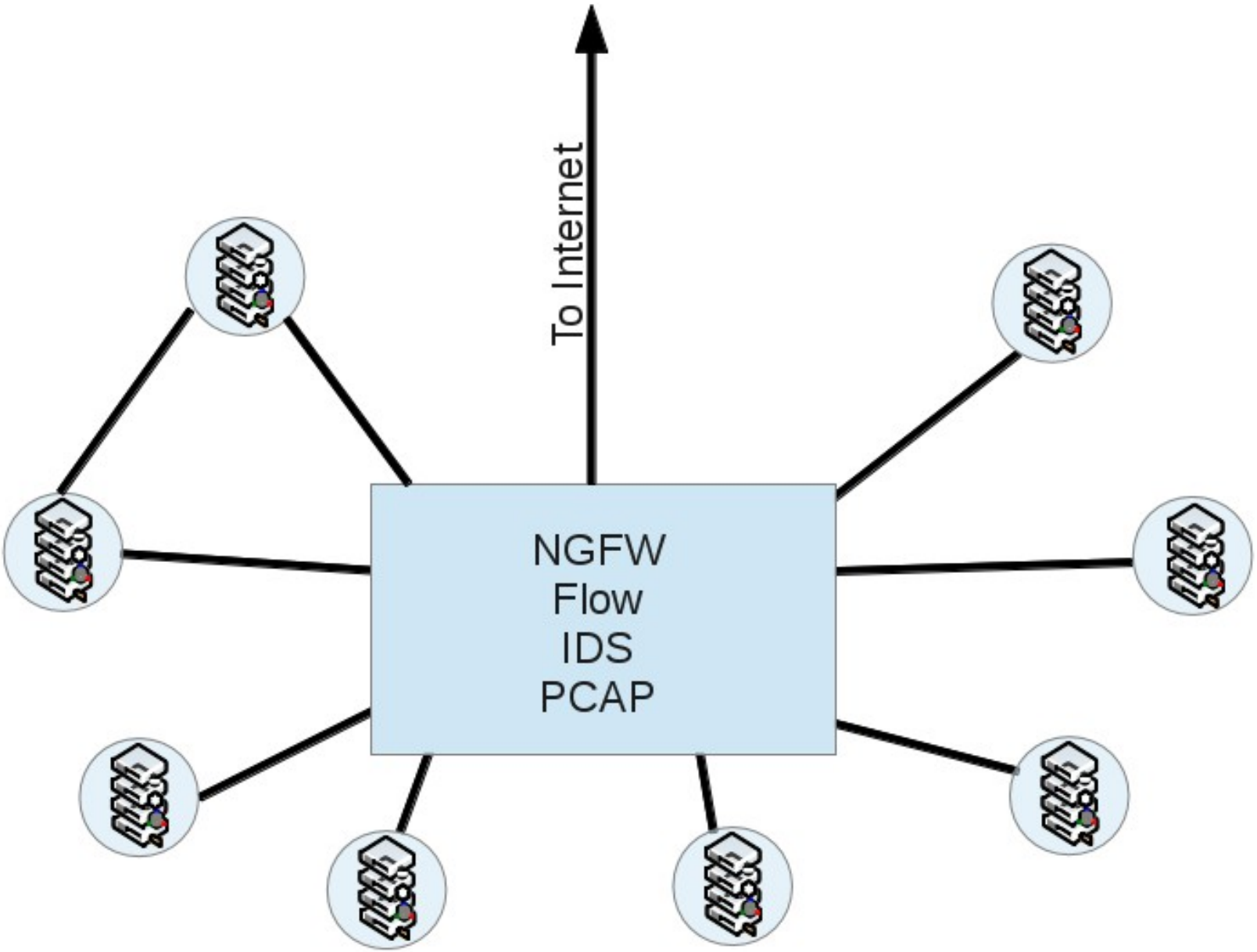


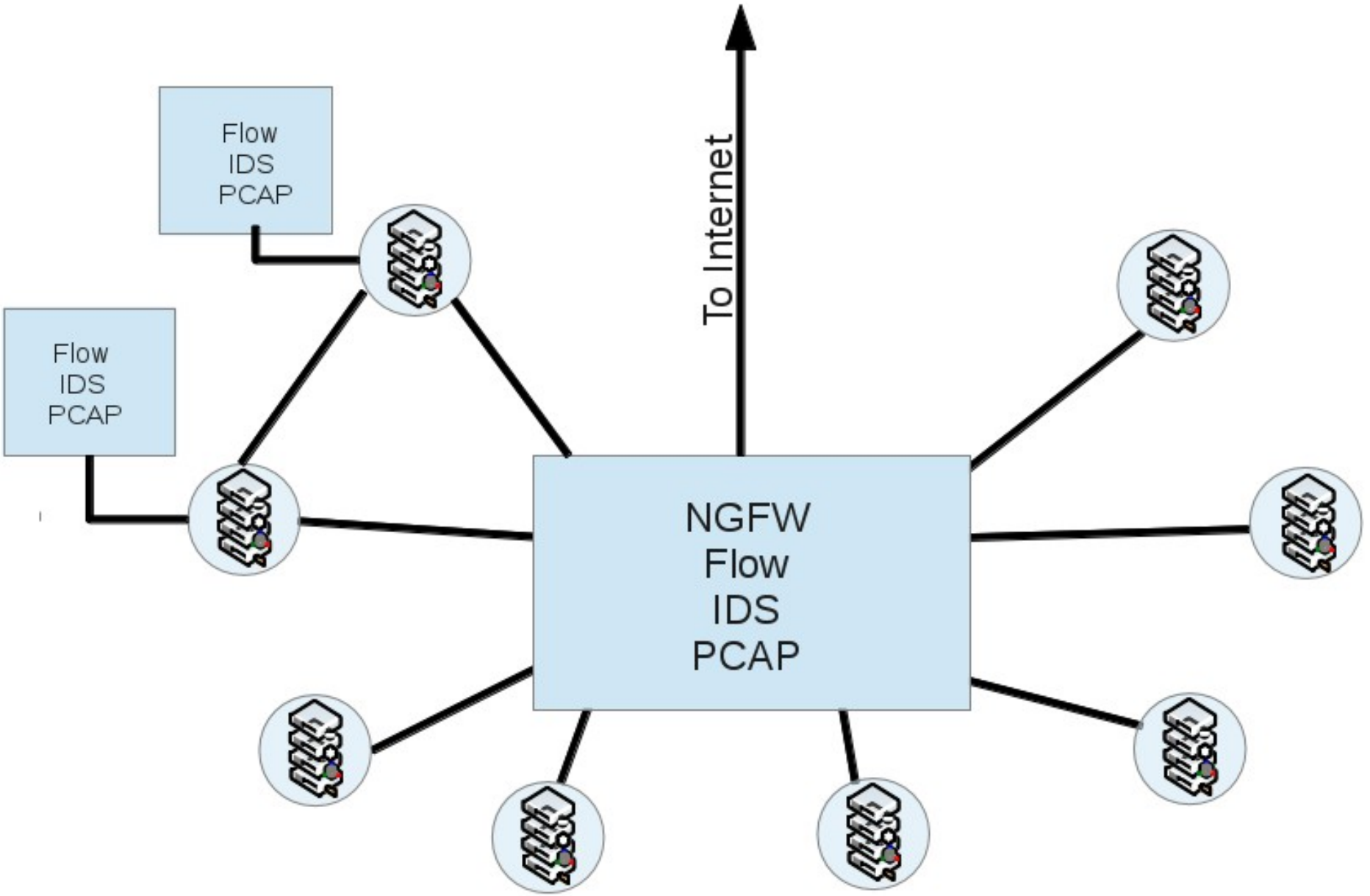
Hyper-V Port Mirroring

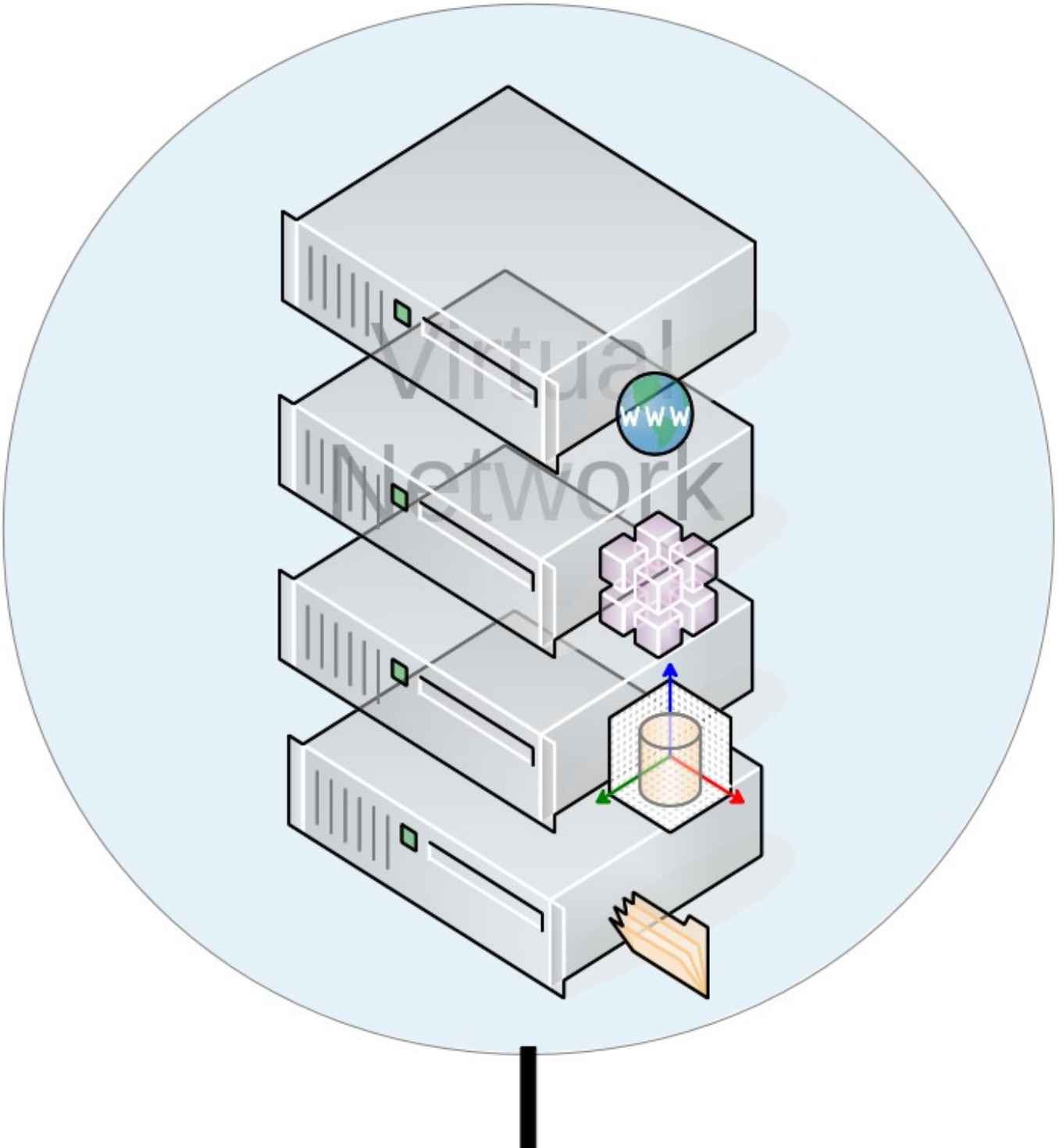


Vbox Promiscuous Mode




To Internet
NGFW
Flow
IDS
PCAP

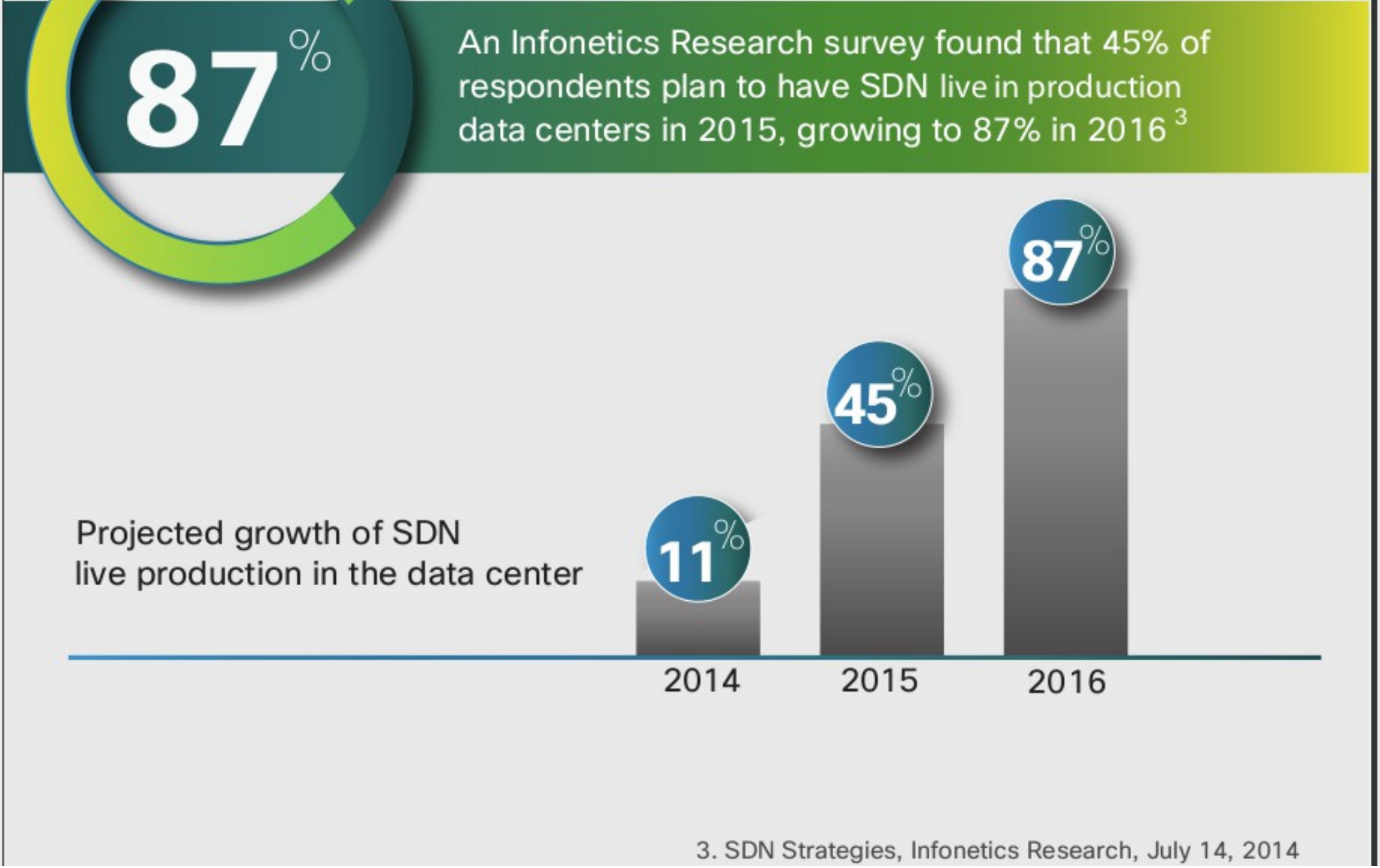

Flow
IDS
PCAP
Flow
IDS
PCAP
To Internet
NGFW
Flow
IDS
PCAP


Virtual
Network
WWW

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



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

Check Point
SOFTWARE TECHNOLOGIES LTD.

Global Sites | My Account

Home | Products & Services | Buy | Support | About Us

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

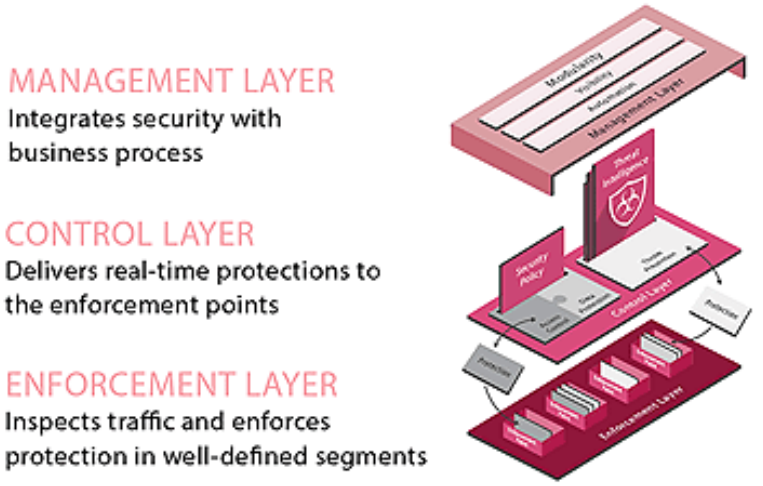
581 Retweet | Share | Send | Print | Subscribe

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



vmware®

Products Support Downloads Consulting

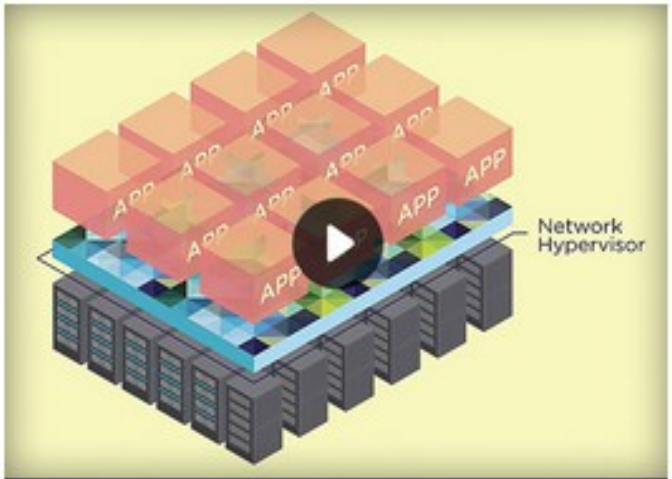
Home / Products / NSX

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

THE TENEO GROUP