

Unified network traffic monitoring for physical and VMware environments

Applications and servers hosted in a virtual environment have the same network monitoring requirements as applications and servers in a physical environment. For organizational and technical reasons, virtual and physical networks are often monitored independently, making it difficult for network administrators to have a single view of overall network activity. This white paper outlines an approach, based on monitoring network traffic, that delivers a unified view of network activity across virtual and physical components of the network.

Contents

Introduction	1
Why is network monitoring needed?	1
Network monitoring in physical environments.....	2
Network monitoring in a VMware virtual environment.....	4
Unified monitoring of the physical and VMware environment.....	6
NetFort LANguardian	9

Introduction

The principal benefits of virtualization – cost reduction, efficiency, speed of deployment, and energy saving – are well-known to IT and business managers. These benefits have inspired a virtuous circle of increasingly sophisticated VMware technology and increasing adoption of that technology. Despite this, less than 50% of enterprise data center workloads have been virtualized and, while the figure is increasing all the time, it is clear that physical servers will have a significant footing in enterprise IT for many years to come.

The growth in virtualization presents a problem for the IT, network, and security staff who are responsible for keeping the network in good shape. The entire VMware environment appears as a single device on the physical network, so the monitoring tools that are so effective on the physical network are unable to provide any insight into what is happening inside the VMware network. Of course, vSphere provides comprehensive management tools for the VMware environment, but it does not provide the same level of network monitoring capability that is available in the physical environment. And often, the VMware environment is managed as a standalone entity separately from the physical network. The result is, network managers and engineers cannot get a single view of overall network activity.

But, this single view of overall network activity is exactly what network managers need (after all, applications and operating systems hosted in a VMware environment are susceptible to the same network issues that arise in a physical environment), and the lack of this single view is a significant problem. In a 2010 survey published in *Network World* magazine, 36% of network engineers cited the lack of appropriate monitoring tools as the biggest problem with virtualization, while a previous survey in 2008 revealed that 40% considered virtualization as the technology that represents the greatest monitoring challenge.

This white paper outlines a traffic-based approach to network monitoring that enables network engineers to obtain a single view of network activity across their entire environment – physical as well as virtual.

Why is network monitoring needed?

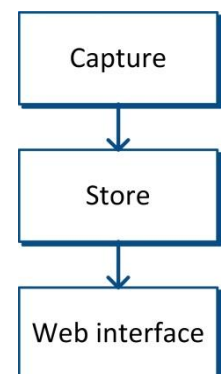
An organization’s network is a business asset that supports user productivity by enabling communication and providing access to data. Productivity suffers whenever the network is down, so it must be available all the time, and it must be kept secure so that sensitive data does not fall into the wrong hands. Yet, the network is vulnerable to all kinds of threats – hackers, viruses, spam, denial of service attacks, bandwidth hogs, illegal downloading, and many more.

To protect this business asset, it is essential to have a robust monitoring solution in place. Network monitoring solutions typically have the three basic components shown in the diagram:

- **Capture** data from the network
- **Store** it in a database on a central server
- Provide a **web interface** for access to the data

Network monitoring has three main benefits:

- It shows you what is happening on your network in real-time.
- It notifies you when an event takes place that requires investigation
- It enables you to troubleshoot problems when they arise
- It provides you with an audit trail of network activity



Although network monitoring is a passive solution that does not modify data or influence how traffic flows in the network, it is a fundamental component of the network security architecture. Its database provides a record of network activity that is independent of the main IT environment and can be used to demonstrate the segregation or separation of duties that is a key requirement for compliance with standards such as SOX and PCI-DSS.

Network monitoring in physical environments

There are many network monitoring products available to the network engineer, ranging from free open-source tools to enterprise management frameworks costing hundreds of thousands of dollars. Essentially, they can be divided into three categories:

- Agent-based

Agent-based tools are usually deployed as part of an enterprise management framework or network management system. Typically, an agent is installed on every device to be included in the monitoring regime. The central management server then communicates with the agent, and vice versa, using a protocol such as SNMP (Simple Network Management Protocol) or WMI (Windows Management Instrumentation). The server can poll the device to determine its status, it can issue configuration commands to control the operation of the device, and the agent can issue alerts to the management server when changes occur or threshold values are breached on the device.

When it comes to network monitoring, agent-based frameworks and tools tend to have a device-centric view of the network. They are really good at monitoring device parameters such as uptime, disk usage, hardware status, bandwidth usage and traffic volume, and they can aggregate the management data from individual devices to give a holistic view of the overall network. However, they do not generally provide detailed information about the network traffic, and when deployed on busy servers or network devices they can sometimes affect performance.

- Log-based

Operating systems such as Windows and all flavors of UNIX maintain detailed log files of all activity on the system – shutdowns, startups, logins, logouts, network connections, database accesses, and so on. Using the syslog format, which was first developed for the Sendmail program on UNIX servers in the 1980s, it is possible to route all logging information to a centralized server. The syslog format is supported by many network switches and there are tools available to export Windows event logs to a syslog server, thereby making it possible for the network administrator to monitor the entire network from a single location.

Centralized logging is a good way to strengthen the security of a networked environment. If an attacker gains access to a server that stores log files locally, he can modify the log files to hide all traces of his activity. If the log files are stored on a secure central system, the attacker will not be able to access them.

- Traffic-based tools

Every time network users access a website, database, file share or other networked resource, they send information in data packets across the network – for example, the address of the website, the content of a SQL query, or the name and location of a file to be deleted. Modern network switches allow monitoring devices to be plugged into the switch and take a snapshot of the data flowing through it. Because this is made possible through the switch hardware and software, traffic analysis does not require agents to be installed and has no performance impact on the systems being monitored.

There are two common approaches to traffic-based monitoring:

- Flow analysis

In computer networks, a sequence of data packets flowing from the same source to the same destination, using the same protocol, is defined as a flow. Many switches support the IPFIX (IP Flow Information Export) standard, NetFlow (the Cisco-developed protocol on which IPFIX is based), and sFlow (an industry-standard packet-sampling protocol). Flow-enabled devices export information about each flow to a flow collector, a software application that processes the flow data and presents it for analysis in graphical or tabular format.

The traffic data exported to a NetFlow collector is based on the packet headers only. It is highly condensed, usually about 1% to 5% of the switched network traffic. Nonetheless, it contains sufficient information to enable detailed analysis of traffic patterns and network utilization. Many collectors store the flow data in a database, creating a historical record that makes it possible to monitor changes and identify

trends in network activity over a period of time.

- Full packet capture

Full packet capture works on the same principle as flow analysis, except that it takes a copy of each data packet flowing through the switch. Full packet capture is possible only with switches that support port mirroring (see sidebar). With full packet capture, it is possible to analyze network data in more depth than is possible with flow analysis, which captures only summarized packet headers.

Traffic analysis systems usually incorporate a database that acts as a historical record of network activity and enables network engineers to forensic analysis and troubleshooting that is impossible with a real-time instantaneous view of network activity. They are typically deployed on a dedicated machine because of the high network traffic throughput. Many full packet capture systems require bespoke hardware although there are some, such as NetFort LANguardian, that can run on any industry standard PC or server.

Figure 1 shows a typical traffic-based network monitoring setup.

What is port mirroring?

Most network core switches have the ability to copy network traffic from one port on the switch to another. This feature, which is called **port monitoring** or **port mirroring**, enables packet capture applications to capture traffic data for analysis.

Port monitoring is given different names by different switch vendors:

- On a Cisco Systems switch, port monitoring is called Switched Port Analyzer (SPAN). You will often see references in the documentation to a SPAN port.
- On 3Com switches, it is called a Roving Analysis Port (RAP).
- HP switches use the term trunk monitoring.

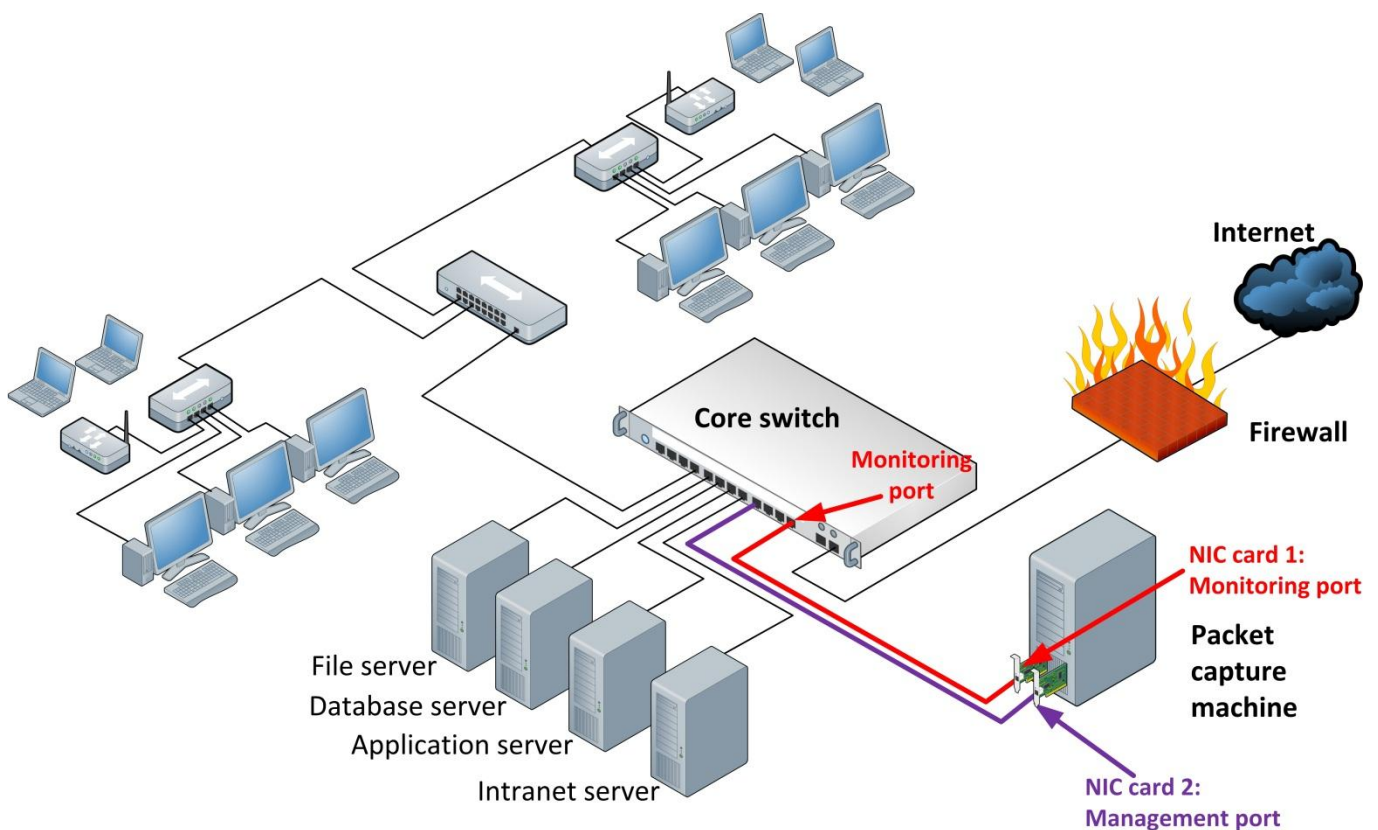


Figure 1 Typical traffic-based monitoring setup

The steps involved in setting up a traffic-based monitoring environment for the physical network are:

1. Set up a monitoring port on the core switch.
2. Decide which network ports you want to monitor, and map them to the monitoring port on the switch.

3. Connect the packet capture system to monitoring port.
4. Connect the management port to a different port on the switch. Typically, to cope with the amount of network traffic involved and to prevent packet loss, the collector is installed on a dedicated machine.

Network monitoring in a VMware virtual environment

The success of VMware is built on its ability to faithfully emulate a physical server and network environment, so it should come as no surprise that it emulates the security and monitoring requirements too. Just as in a physical environment, it is necessary to monitor the servers in the virtual environment to diagnose and prevent application performance bottlenecks, security threats, unauthorized user behavior, and regulatory non-compliance.

A VMware environment also poses additional technical challenges:

- Problems that affect one virtual server in the VMware host can affect all others on the same host.
- Shared disk and memory structures can facilitate cross-appliance infection.
- Individual virtual machines are only as strong as the underlying host.
- When virtual servers are moved to new environments, they can potentially compromise the security of their new environment.
- Virtual machine images that have been unused for a while might not have the latest operating system updates and security patches installed.

In addition to these technical challenges, there is often the very real organizational challenge that arises from the virtual environment and the network environment being managed by different teams. The physical network can be affected by events in the virtual environment and vice versa. Without insight into both, it is difficult to monitor the overall network effectively.

Addressing the organizational challenge is beyond the scope of this white paper, but the technical challenge can be addressed by applying the principles of physical network monitoring to the virtual environment.

In keeping with its faithful emulation of the physical environment, VMware ESX includes virtual network interface cards (NICs) and virtual switches that replicate, in a virtual environment, the role of NICs and network switches in a physical network. The virtual switch interfaces with a physical NIC to provide the connection between the VMware environment and the physical network.

Figure 2 shows a typical VMware setup:

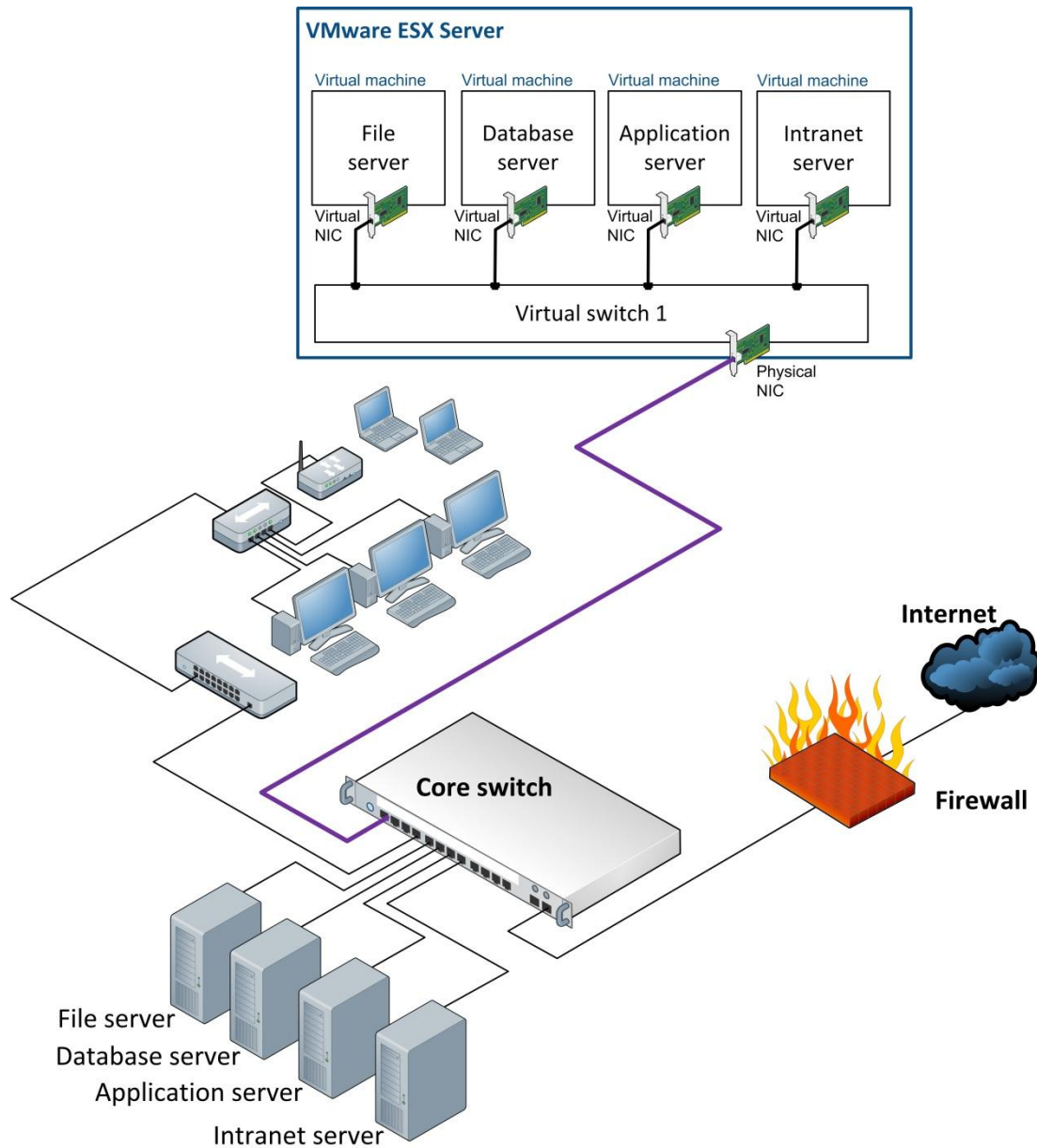


Figure 2 Typical VMware setup

In this setup, the virtual environment is simply another network connection as far as the core switch is concerned. Monitoring tools connected to the core switch can see traffic entering and leaving the virtual environment, but they cannot see what is happening inside it. To overcome this limitation, it is necessary to implement network monitoring in the virtual environment.

The network monitoring options that are available for physical networks are, in principle, also available for VMware virtual networks:

- **Agent-based logging**
VMware ESX supports SNMP, enabling virtual servers to be monitored in the same way as physical servers.
- **Log-based**
Network monitoring based on log files works in the exact same way on VMware virtual machines as it does on physical machines.

- Traffic-based monitoring

Flow analysis and packet capture techniques can be implemented in a VMware environment.

- Flow analysis

VMware ESX Server supports NetFlow but only in a way that is described by VMware as “experimental”. It supports a limited set of the NetFlow features that are available on physical switches. According to VMware, “*although activation of NetFlow should not create stability issues, overall performance of the ESX Server host may be affected.*”

- Full packet capture

Just like vendors of physical switches implement the port mirroring capability that makes full packet capture possible, VMware provides a similar capability on virtual switches. Many network monitoring vendors take advantage of this capability to support full packet capture in VMware environments. Generally, the monitoring capability is provided by a virtual appliance that is connected to the virtual switch and takes a snapshot of all traffic data passing through it. The captured data is then stored in the virtual appliance.

The key to setting up packet capture in a VMware environment is to set the virtual NIC of the packet capture appliance to operate in promiscuous mode. By default, a NIC is configured to accept only the data packets that are intended specifically for it, but in promiscuous mode a NIC will accept all data packets flowing through the switch.

Figure 3 shows a VMware ESX environment that includes a packet capture appliance to monitor the virtual network.

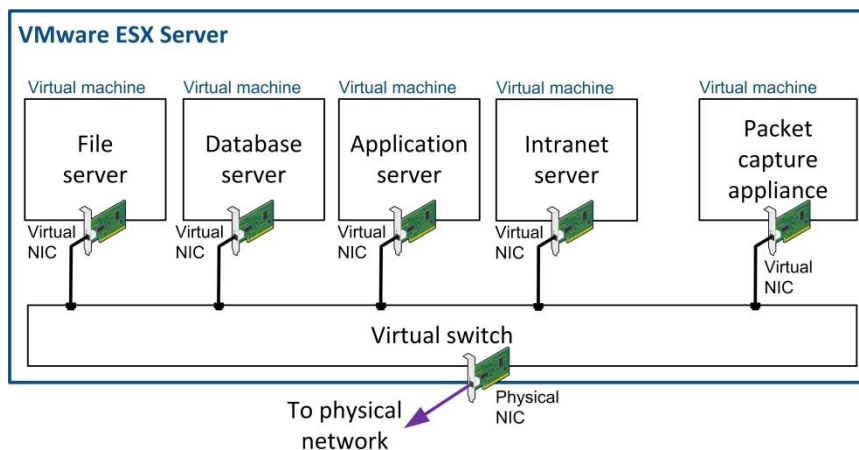


Figure 3 VMware ESX environment with packet capture appliance

The steps involved in setting up a traffic-based monitoring environment for the virtual network are:

1. Configure your VMware ESX server to allow promiscuous mode networking.
2. Ensure that the virtual NIC on the packet capture appliance is configured to operate in promiscuous mode (many appliances will do this by default).

Unified monitoring of the physical and VMware environment

You can combine the above approaches to implement unified monitoring of your entire network from one place. There are two approaches to doing this:

- Install the packet capture software as a virtual appliance in the VMware environment and configure it to capture data from the physical network.
- Install the packet capture software on a physical PC or server, and capture data from the virtual network.

Unified monitoring to packet capture virtual appliance

With this approach, you would associate two virtual NICs with the packet capture appliance, as shown in Figure 4. One of these NICs is connected to the same virtual as the other virtual machines hosted on the VMware ESX server switch (virtual switch 1). The second virtual NIC on the packet capture appliance is connected to a dedicated virtual switch (virtual switch 2), which in turn is associated with a dedicated physical NIC that is connected to the monitoring port on the physical switch.

Because the virtual NICs associated with the packet capture appliance are operating in promiscuous mode, they can see all traffic flowing through virtual switch 1 **and** virtual switch 2.

Figure 4 shows this setup:

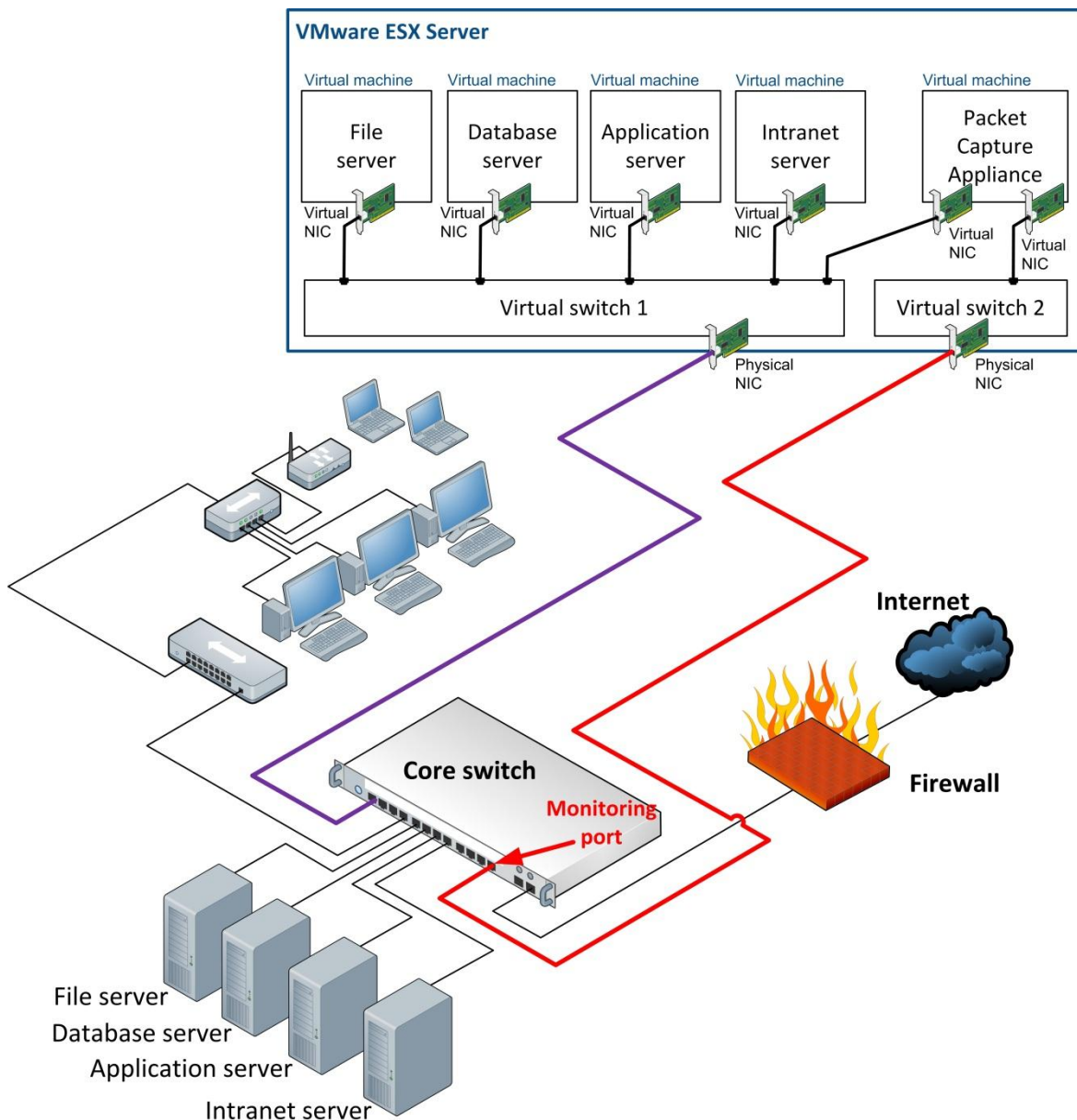


Figure 4 Unified monitoring of VMware and physical network to packet capture appliance

Unified monitoring to physical packet capture device

With this approach, a packet capture appliance in the VMware ESX environment captures data from the virtual network switch. The VMware ESX server is connected to the core switch on the physical network, and the port to which it is connected is a monitored port. The packet capture appliance on the physical network, which is connected to the monitoring port, is therefore able to capture and store the traffic data from the virtual network.

Figure 5 shows this setup:

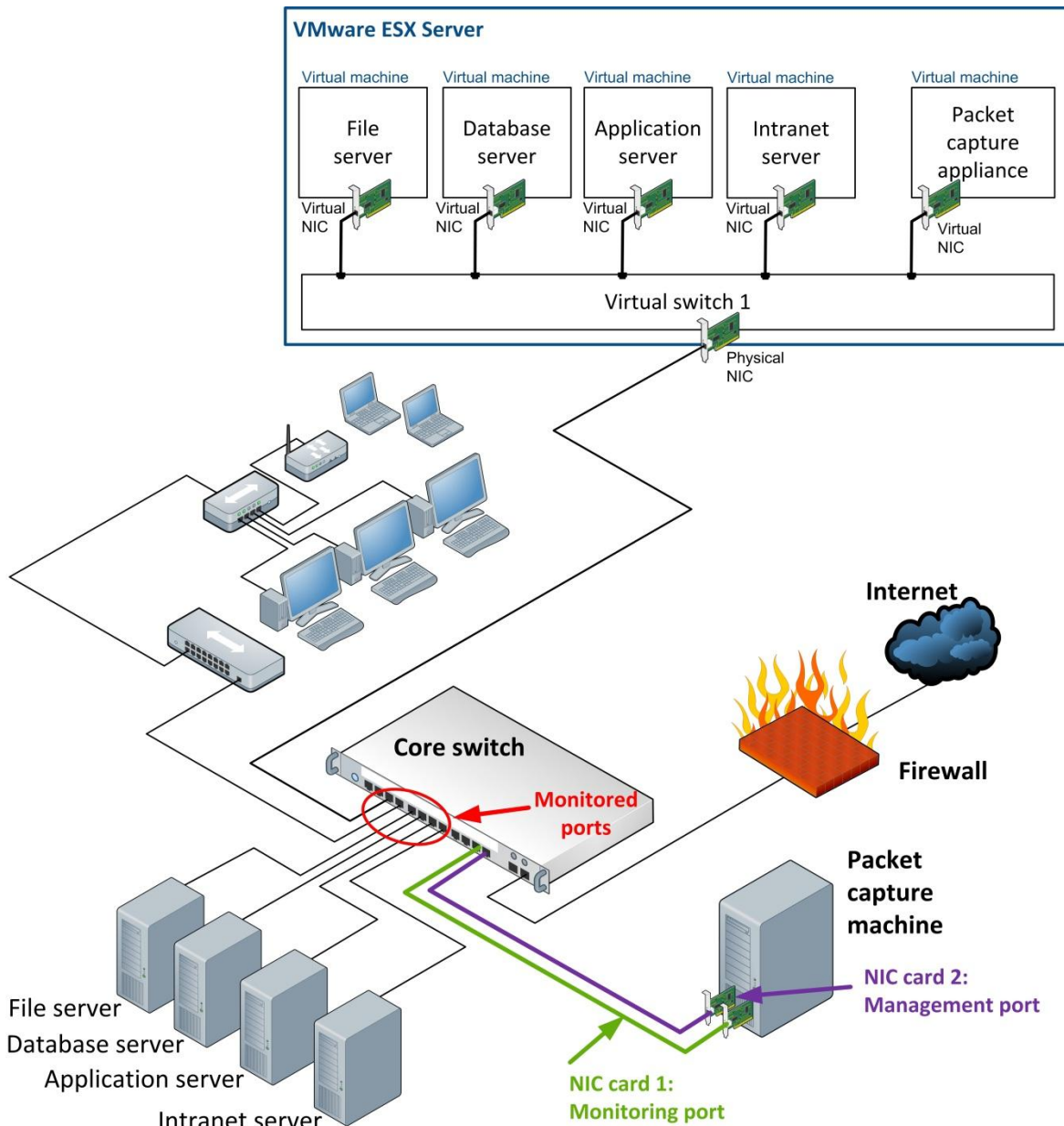


Figure 5 Unified monitoring of VMware and physical network to packet capture machine

Recommended approach

There are advantages and disadvantages to both approaches, so ultimately how you implement a unified network monitoring environment will depend on the needs of your own organization and network. On balance, we believe storing traffic data in the physical environment is the preferred approach. If the virtual environment is

unavailable for any reason, the physical data capture server will still be available, whereas if you store the captured data in the virtual environment it goes down with the ship.

NetFort LANguardian

NetFort LANGuardian is software that analyzes network traffic and provides a unique level of visibility into everything that is happening on the network, including user activity, file and database monitoring, intrusion detection, bandwidth usage, and Internet access. LANGuardian is primarily a full packet capture product, although it can also accept flow data. You can implement all of the monitoring scenarios described in this white paper with LANGuardian:

- Deploy on a standalone PC or server to monitor physical network traffic, and to capture traffic from a VMware environment.
- Deploy as a VMware virtual appliance to monitor traffic in your VMware environment, and to capture traffic from your physical environment.

Unlike most other full packet capture appliances, LANGuardian is a software-only product that runs on industry standard PCs and servers. No bespoke hardware is required.

For more information and to download a free trial, please visit www.netfort.com or contact us directly by phone or e-mail.

About NetFort

NetFort provides a range of software products to monitor activity on virtual and physical networks. Headquartered in Galway, Ireland, NetFort was established in 2002 and has built up a global customer base in the enterprise, education, and government sectors.

North America Sales Office

280 Madison Avenue,
#912 - 9th Floor,
New York,
NY 10016
USA

Phone: +1 (646) 452 9485

UK Sales Office

27 Old Gloucester Street
London
WC1N 3XX

Phone: +44 (207) 060 2850

Asia-Pacific Sales Office

c/o Innovation Centre,
90 Sippy Downs Drive,
Sippy Downs,
Queensland 4556
Australia

Phone: +61 (7) 5450 2769

Head Office

Unit 7
IDA Innovation Centre
Upper Newcastle
Galway
Ireland

Phone: +353 (91) 520 501

Email: sales@netfort.com