vmware SOLUTION READINESS

VMware vShield™ App
Protecting Virtual SAP Deployments

August 2011

VMware, Inc
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

List of Figures

List of Tables

1. Executive Summary

VMware vShield™ App is one of the VMware vShield family of virtualization security products. vShield App is a virtual appliance that provides visibility and enforcement of network activity within a VMware vSphere® deployment to comply with corporate security policies and industry regulations. For example, SAP ERP systems cover a wide variety of business processes that must comply with Sarbanes-Oxley, and it is common for SAP business functions to include credit card processing, which must conform to PCI Security Council standards. For organizations running SAP applications, compliance with these industry regulations is extremely important.

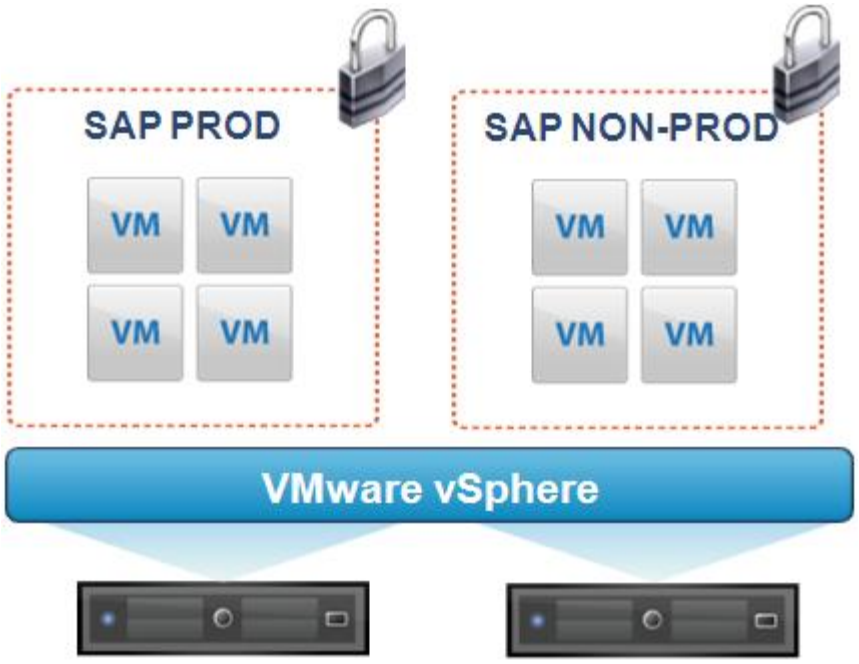
This document describes an example deployment of vShield App 5.0 with SAP on Oracle and SAP on SQL Server. The architecture and configuration are discussed, and sample workloads are executed with some basic firewall configurations.

2. Introduction

VMware vShield App is a hypervisor-level firewall and is one of the VMware security products that protects applications and resource pools in a virtual datacenter from internal and external network-based threats. This paper describes an example configuration of vShield App with SAP. For more background information on vShield, see Reference Documents on page 19.

vShield App enables customers to support applications belonging to different trust levels on the same virtual datacenter (for example, production and non-production). It enforces proper segmentation for all applications based on firewall rules. Figure 1 shows an example deployment of SAP applications with vShield App.

Figure 1. Isolating Applications into Zones with vShield App



The example above depicts two separate environments/zones in the SAP landscape that need to be isolated. Each zone can include multiple virtual machines running several database and application servers. The isolated zones represent the following potential use cases:

- Two different SAP production applications that must be isolated in a production ESX cluster.
- A sandbox and a test environment that must be isolated in a non-production ESX cluster.
- A production and non-production environment that must be isolated in a consolidated ESX cluster.

2.1 Benefits of vShield App

Table 1 summarizes the features and benefits of vShield App.

Table 1. vShield App Features and Benefits

Benefits	Features
Improved visibility	• Hypervisor-based, vNIC level technology inspects *all* traffic leaving and entering a virtual machine and the virtual environment in general. • Flow monitoring decodes this traffic into identifiable protocols and applications. This feature provides the ability to observe network activity between virtual machines to define and refine firewall policies.
Improved control	• Application-layer firewall can deny or allow traffic to/from virtual machines, virtual environment. • Intelligence from flow monitoring can be used to define firewall rules, based on actual traffic, not just defined policy. • Flexible groupings, built-in to VMware vCenter™ or custom-defined using security groups, to provide necessary segmentation for security enclaves. • Layer 2 isolation.
Audit proof	• Logging of security events, such as creation/deletion of rules, trigger firewall rules.
Cost-effective	• Reduce dependence on physical firewalls and VLAN-enabled switches.
Adaptive	• Implement security that follows virtual machines throughout their dynamic lifecycle. • Firewall policies are enforced throughout the ESXi cluster so rules are maintained as virtual machines are live migrated between ESXi hosts. • Integrate security workflows into existing VMware Infrastructure™ administration workflows using vCenter.
Simple	• Implement fewer rules less often without compromising security

Administrators can define security rules based on containers which can be any of the following VMware vSphere® objects:

- Datacenter
- Cluster
- Resource pool
- vApp
- Port group
- VLAN

A rule that is created for a container applies to all resources in that container. For example, a rule that denies any traffic from inside a vApp to a specific destination outside that vApp applies to all the virtual machines in that vApp. In this document, a vApp container is used as an example. A vApp is a resource container for multiple virtual machines that work together as part of a multitier application. In Figure 1, each zone can also be viewed as a vApp comprising all the associated virtual machines for that application.

SAP administrators can benefit from vShield App in the following ways:

- Organizing applications into vApps and setting policies against these vApps allows administrators to focus on the application architecture and remove themselves from details such as IP addresses.

  For SAP, an IP address change does not typically involve any change to the application configuration files—the same can be said of the firewall rules.

- In non-production environments, administrators can easily test the impact of firewall settings to their application.
- Non-production landscapes can be very dynamic in SAP environments, for example, creation of sandbox and training systems for new project personnel and end users. These systems can be rapidly provisioned in virtual machines and quickly isolated with vShield App.
  - End users with access to training systems can be protected from accessing the QA systems.
  - New developers and project consultants who are coming up to speed in sandbox systems can be isolated from core development environments.
- In cases of high consolidation, administrators need not have security concerns about how their applications are co-existing with other applications on the same ESXi host or cluster:
  - Different applications are isolated in their own vApps.
  - Production and non-production vApps are isolated and protected from each other.
- vShield firewall policies apply to all ESXi hosts in the cluster so they are still enforced when a virtual machine is live migrated between hosts or a to a new host in the cluster (assuming that all hosts are protected by running the vShield App appliance and hypervisor module.

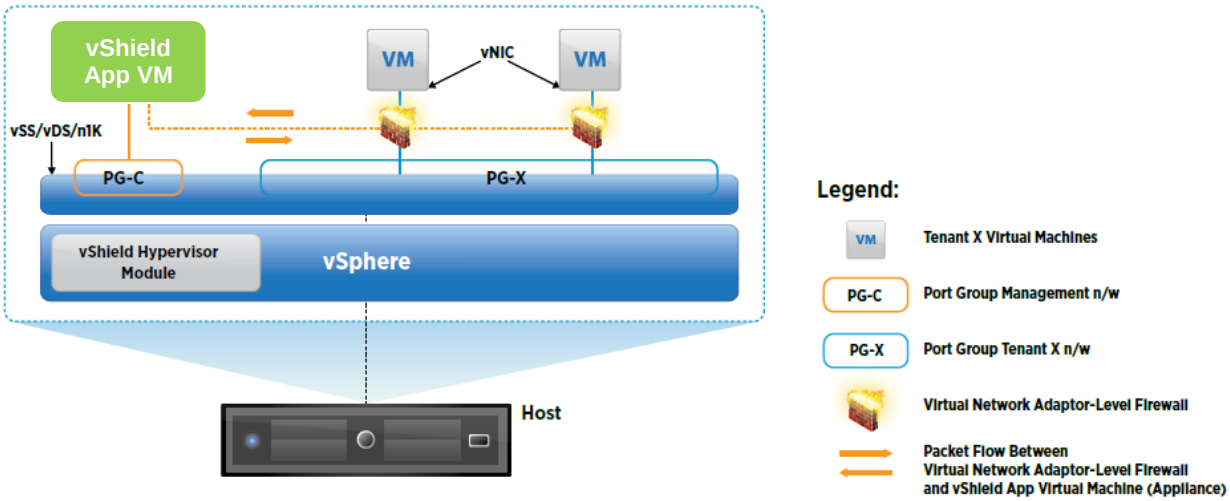
2.2 Architecture

VMware vShield App includes the following components:

- VMware vShield Manager™ – The centralized network management component of vShield. It is installed as a virtual appliance on any ESXi host in the vCenter environment. It centrally manages the firewall rules and distributes them to vShield App appliances across the environment.
- vShield App - Installs as a hypervisor module and firewall service virtual appliance on each ESXi host. vShield App provides firewalls between virtual machines by placing a firewall filter on every virtual network adapter. By default, a vShield App virtual appliance is 2 x vCPU and cannot be migrated using VMware vSphere® vMotion®.
- A vSphere plug-in option that can register vShield Manager as a VMware vSphere® Client™ plug-in, after which, you can configure most vShield options from the vSphere Client.

The architecture of vShield App is described in *The Technology Foundations of VMware vShield* available at http://www.vmware.com/files/pdf/techpaper/vShield-Tech-Foundations-WP.pdf. Figure 2 repeats that content.

Figure 2. vShield App Architecture



The vShield App virtual machine is deployed with a vShield hypervisor module on each host. The vShield App virtual machine is a preinstalled, preconfigured virtual machine with a hardened operating system specialized for handling firewall operations. The hypervisor module effectively places a network packet filter between the virtual network adaptor and the virtual switch, referred to as a virtual network adaptor-level firewall. It allows the traffic coming in and out of virtual network adaptors to be efficiently inspected and, if required, directed to the vShield App virtual machine for further processing, as depicted by the dotted line in 2.

3. Example SAP Deployment

This section describes the technical deployment of the use case shown in Figure 1, where two zones exist that need to be isolated from each other. Each zone is configured as a vApp, so there are two vApps with SAP on Oracle/Linux in one and SAP on MSSQL/Windows in the other. Table 2 describes the technical environment. The sizes of the virtual machines are not based on any specific business requirements.

Table 2. Technical Environment

Component	Description
Hypervisor	vSphere 4.1 U 1
vShield product	vShield App 5.0 Beta

ESXi cluster	• Cluster name = “VSHIELD TEST”
	• 2 x ESXi hosts
	  ○ ESXi host 1 - 16-core (“tsa-bl465-1”)
	  ○ ESXi host 2 - 48-core (“tsa-bl685-1”)

vApp	SAP_MSSQL • Netweaver 7.0 ABAP stack, MSSQL 2005 , Windows 2003 • Virtual machine SAP_app_windows (8 vCPU) : application server • Virtual machine SAP_dbci_windows (6 vCPU): database and Central Instance

vApp	SAP_ORACLE
	• Netweaver 7.0 ABAP stack, Oracle 10.2, Red Hat 5.6
	• Virtual machine SAP_app_linux (8 vCPU): application server
	• Virtual machine SAP_dbci_linux (4 vCPU): database and Central Instance
	• Two sub vApps
	  ○ app tier
	  ○ db tier

Each SAP system is considered a three-tier deployment because the application and database servers reside in separate virtual machines (the third tier is the client/front end). Note that the central instance inside the database virtual machine can also be used to run application workloads (this will be used in one of the workload scenarios).

Figure 3 describes the security zone configuration for the SAP on Oracle environment. Two “sub” vApps exist within the main vApp that isolates the application from the database tier. This addresses situations where database administrators require firewall protection between the databases and the application servers.

Figure 3. SAP on Oracle vApp Security Architecture

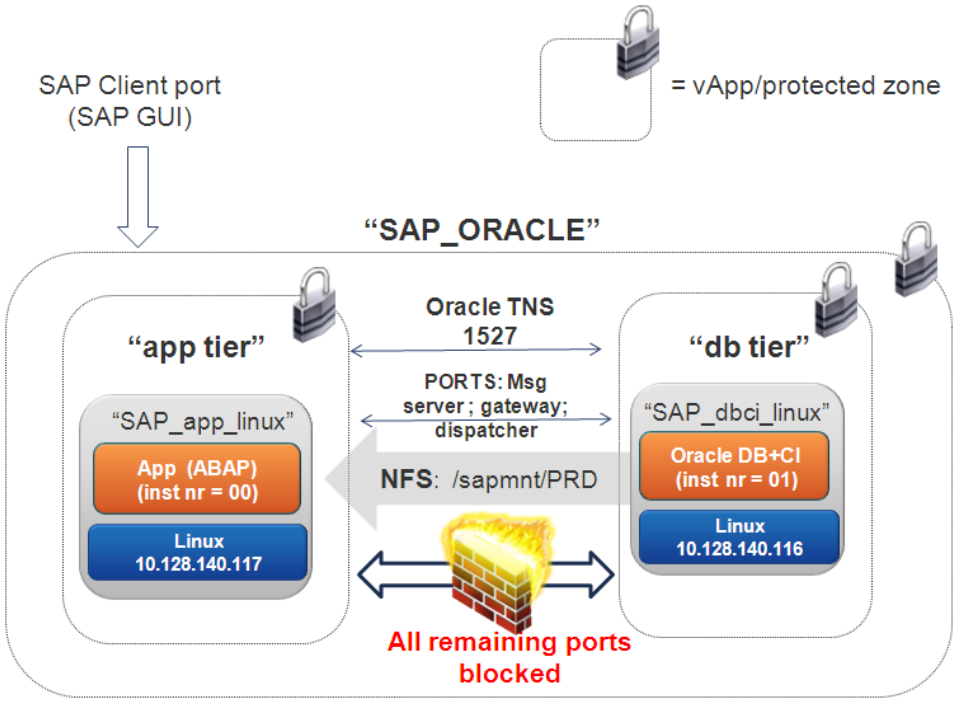


Figure 4 shows the security zone configuration for the SAP on MSSQL environment.

Figure 4. SAP on MSSQL vApp Security Architecture

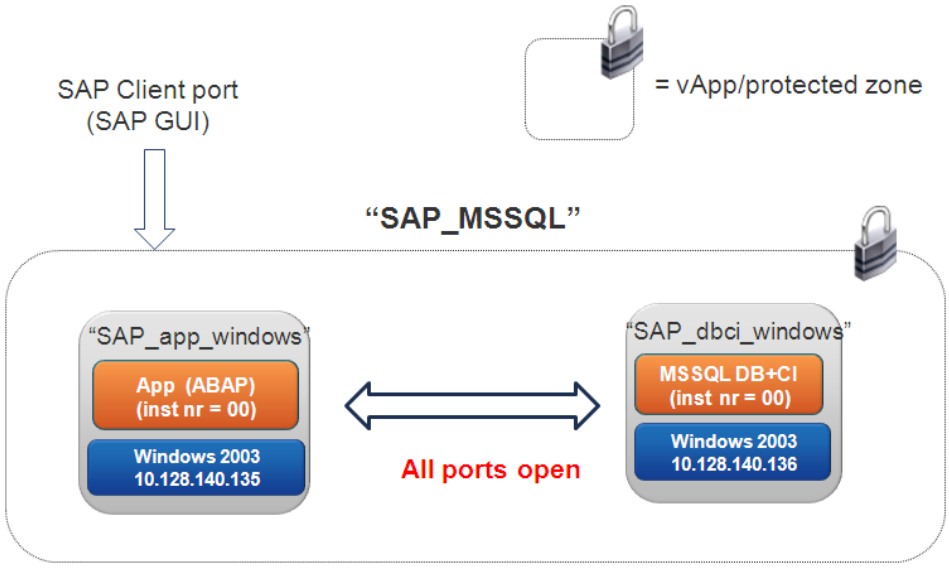
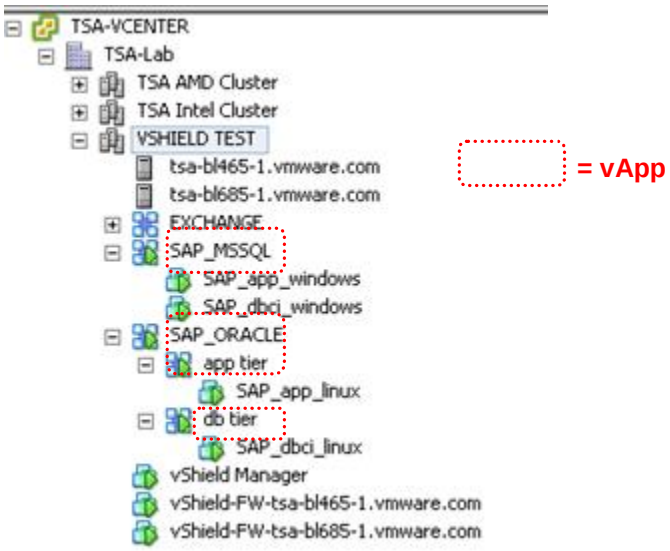


Figure 5 shows the vApp configuration in vCenter.

Figure 5. vApp Configuration in vCenter



See Appendix A for the vShield App configuration for the above security zones. Firewall setup can be entered in the intuitive GUI which is available as separate tab in vCenter (after installing the plug-in). The configuration steps involve the following:

- Configure *L3 High Precedence* rules – Here all outside access to the vApps is blocked. This secures the SAP environment.

  No IP addresses need to be entered here, simply reference the name of the vApp.

- Identify and set up application specific ports – The SAP-specific ports that must be opened to allow access for certain protocols are identified and saved as a logical entity. This includes:
  - SAP GUI port to enable client access to the vApp
  - Ports to enable communication between the SAP application and database server
- Under *Application High Precedence* – The ports identified in the previous step are opened to allow the required access in and out of the vApps.

4. Workload Characterizations

This section describes workload tests executed against the SAP environments defined previously. The following tests were conducted:

- Workload test 1 – Run single SAP vApp; all virtual machines resided on the same ESXi host
- Workload test 2 – Run two SAP vApps; virtual machines were spread across two ESXi hosts
- Workload was based on the SAP batch job "SGEN"

4.1 Workload Test 1 – Single SAP vApp

Table 3 shows some workload statistics gathered from running a SAP batch job in the SAP_ORACLE vApp. All virtual machines of the vApp reside on one ESXi host. The batch job was executed three times with different degrees of parallelism which resulted in varying network traffic between the application and database server.

Table 3. Workload Results from running SAP Batch Workload (1 x vApp on 1 x ESXi host)

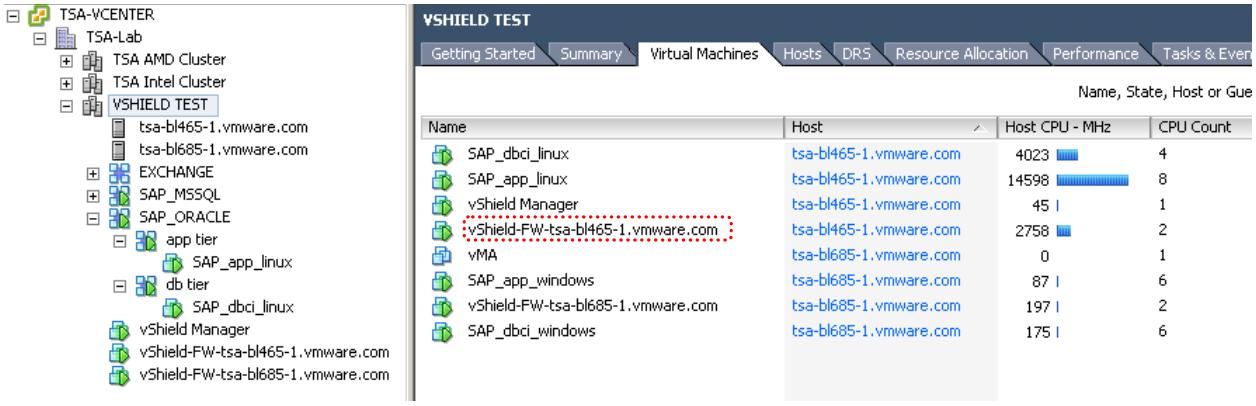
Kbps	Total Packets per 20s Sampling Period	FW VM (2 x vCPU) CPU Util (on ESXi host 1)
50128	216097	1714 MHz
90896	396101	2077 MHz
137496	601933	2758 MHz

Source: *approximate* averages from vCenter performance charts. 1 CPU/core = 2.299 GHz.

As expected with increasing batch workload, there is more network traffic between the virtual machines, which is driving up the utilization of the firewall appliance.

Figure 6 is a vCenter screen capture showing the performance of the virtual machines during one of the runs (the impacted vShield firewall appliance is highlighted by the dotted square).

Figure 6. Batch Workload running in vApp SAP_ORACLE



4.2 Workload Test 2 – Multiple SAP vApps

SAP batch jobs were executed simultaneously in both vApps SAP_ORACLE and SAP_MSSQL. The following runs were executed:

- Run 1 – Each vApp (and associated virtual machines) resided on their own ESXi host.
- Run 2 – Both vApps resided on one ESXi host.
- Run 3 – Run SAP batch load on the database server virtual machines only (that is, do not use application server virtual machines).

Table 4 shows the results of the run.

Table 4. Workload Results from running SAP Batch Workload (2 x vApps)

vApp	Kbps	Total Packets per 20s Sampling Period	FW VM (2 x vCPU) CPU Util
Run 1 – vApps on separate ESXi hosts			
SAP_ORACLE (on ESXi host 1)	104488	453396	2367 MHz (on ESXi host 1)
SAP_MSSQL (on ESXi host 2)	34784	184653	1847 MHz (on ESXi host 2)
Run 2 – vApps on one ESXi host			
SAP_ORACLE SAP_MSSQL (on ESXi host 2)	153208	690550	3276 MHz (on ESXi host 2)
Run 3 – Run workload on application instances inside database virtual machine.			
SAP_ORACLE SAP_MSSQL (on ESXi host 2)	n/a	n/a	219 MHz (on ESXi host 2)

Source: *approximate* averages from vCenter performance charts. 1 CPU/core = 2.299 GHz.

The following figures show the workloads of the different virtual machines in vCenter for the different runs.

Figure 7. Run1: Batch Workload Running in vApp SAP_ORACLE and SAP_MSSQL – Separate ESXi Hosts

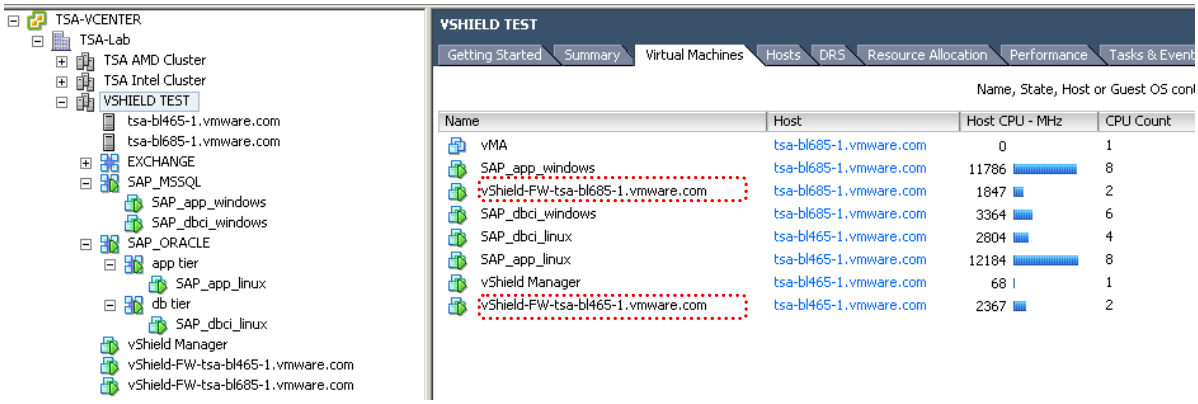


Figure 8. Run 2: Batch Workload Running in vApp SAP_ORACLE and SAP_MSSQL – One ESXi Host

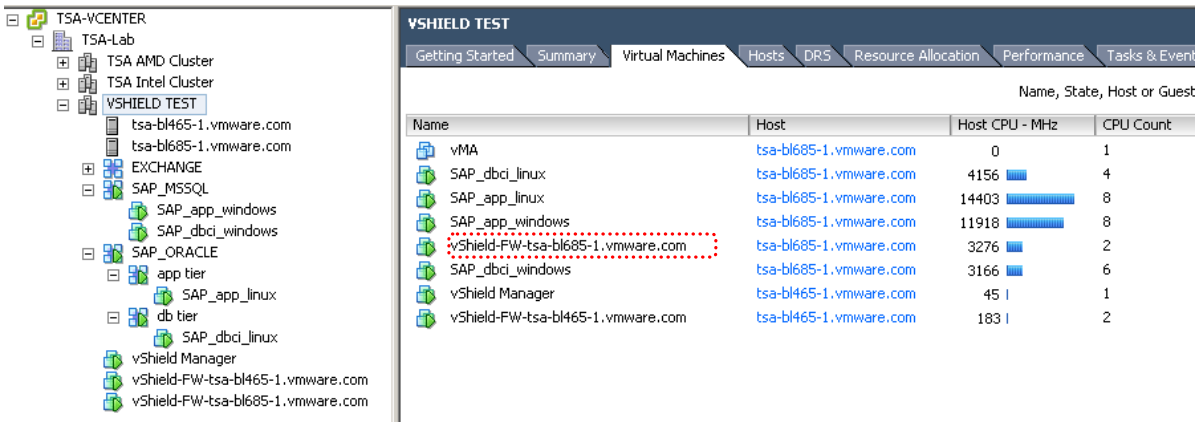
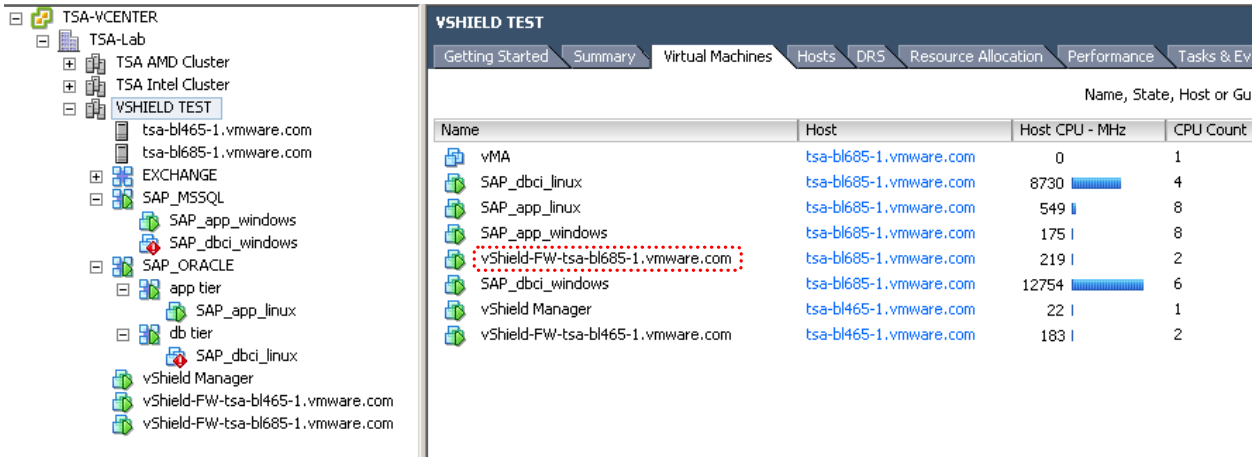


Figure 9. Run 3: Execute Workloads on the Database Server Virtual Machines – One ESXi host



The results show the following:

- Consolidating three-tier SAP applications onto the same ESXi host drives up the firewall appliance utilization as it increases the network traffic.
- Two-tier systems (that is, systems where the database and application instances reside in the same virtual machine) produce no network traffic between virtual machines so do not generate load on the vShield App appliance (in SAP deployments, depending on sizing and scaling requirements, some customers may chose to deploy two-tier systems).

Note that SAP client traffic from end-user desktops to the application servers was not tested here. To get an idea of how much network traffic client interaction may generate, we can use the, the certified 16,000 user three-tier OLTP benchmark on VMware documented at http://www.sap.com/solutions/benchmark/pdf/BM-NewsJuly2010.pdf. 16000 concurrent users generated 27,000 packets per second between the benchmark driver and application servers.

5. Deployment Considerations

The following are some guidelines and considerations to observe when deploying vShield App.

- Deploying SAP instances in separate virtual machines allows the instances to have the same instance number, for example, 00. The instance numbers determine the port numbers required for SAP communication protocols. A reduced set of instance numbers makes firewall configuration easier as administrators can work with a reduced set of port numbers.
- Virtual machines that are protected by vShield App should exist in clusters in which all the ESXi hosts are prepared – preparation means the vShield App appliance has been installed on the ESXi host. This way firewall rules are enforced when the virtual machine is live migrated between hosts (note: a virtual machine on a prepared ESXi host has the following vmx configuration parameter: `ethernet0.filter0.name = vshield-dvfilter-module`).
- When live-migrating a virtual machine that is part of a vApp, specify the correct target vApp. If a virtual machine is moved out of the vApp, firewall rules (configured against the vApp) no longer apply.
- For high availability considerations for the vShield App appliances, see the section on High Availability in *The Technology Foundations of VMware vShield.*

6. Summary

This paper describes some use cases of deploying SAP with vShield App. vShield App provides microsegmentation / zoning of different landscapes which enables a secure SAP deployment. The configurations covered here are examples only, but provide a starting point from which to plan for a security architecture to cover a SAP installation on VMware in production and non-production environments.

Workload characterizations conducted against SAP show that CPU resources are required by vShield firewall virtual machines, the extent of which is dependent on the network traffic generated by the application. When there is a need for additional firewall capacity, administrators can add CPU or memory resources to the vShield App appliance. If the cluster is resource limited, administrators can add another host to the cluster along with the vShield App appliance and the hypervisor module.

Customer workloads will differ from those tested here which will result in different utilizations of the vShield App firewall appliance. Situations where systems are designed as two-tier instead of three-tier would reduce network traffic between virtual machines and lower firewall appliance utilization. For example, some SAP customers may deploy database and application instances in a single large virtual machine.

Categorizing applications into a container such as vApp greatly simplifies management of firewall policies with vShield App. Application and security administrators can respond rapidly to specific demands in a dynamic landscape, and while virtual machine templates enable quick deployment of systems, vShield App facilitates speedy security compliance.

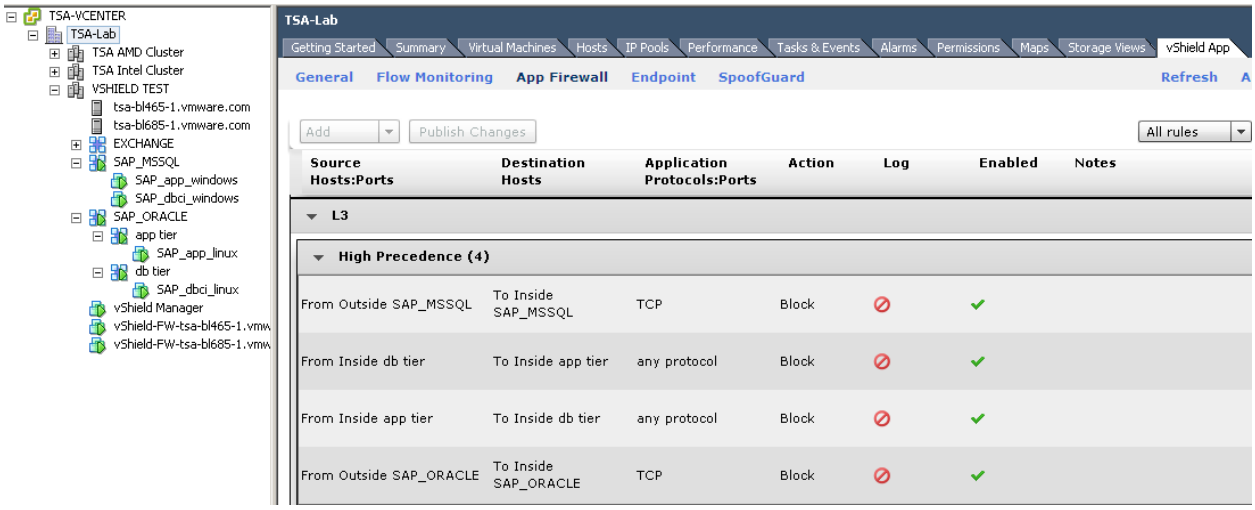
7. Reference Documents

- VMware vShield App product page
  http://www.vmware.com/products/vshield-app/overview.html
- *The Technology Foundations of VMware vShield*
  http://www.vmware.com/files/pdf/techpaper/vShield-Tech-Foundations-WP.pdf
- *VMware vShield App Design Guide*
  http://www.vmware.com/files/pdf/techpaper/vShield-App-Design-Guide.pdf
- *Virtualized 3-Tier Environment Supports 16,000 SAP SD Benchmark Users*
  http://www.sap.com/solutions/benchmark/pdf/BM-NewsJuly2010.pdf

Appendix A – vShield App Configuration

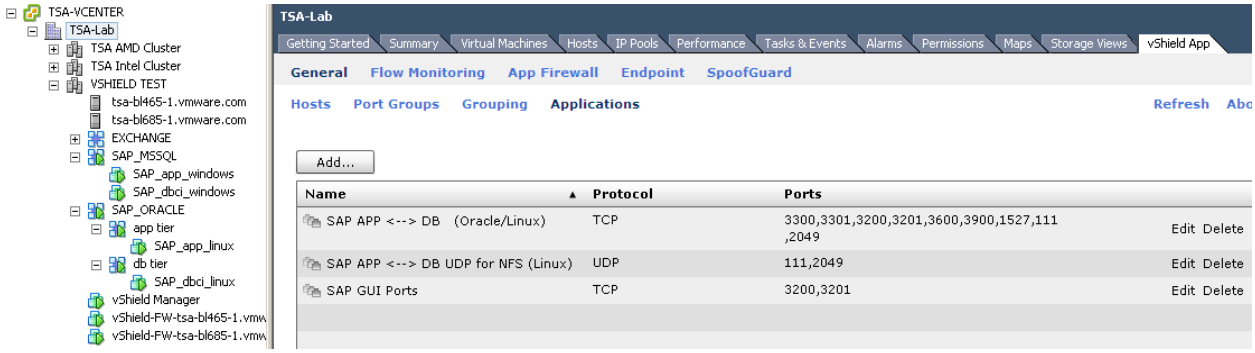
Figure 10 shows the vShield App configuration for this example. First, each vApp is protected by blocking external access to the virtual machines inside the vApp. This blocks all ports and protocols in and out of the vApp.

Figure 10. vShield App Configuration "L3 High Precedence" Rules – blocks access to vApps



Specific ports are identified and created as **Applications** in vShield App – this is shown in Figure 11. These are SAP-specific ports that must be unblocked to and from the vApps to allow for basic operations—client access from the SAP client (SAP GUI) and communication between the application and database server.

Figure 11. vShield App Configuration – Identify Application Specific Ports



The ports/protocols identified must be assigned to the appropriate vApps and unblocked – this is shown in Figure 12.

Figure 12. vShield App Configuration - Unblock Application Specific Ports for vApps