Secure Segmentation of Tier 1 Applications in the DMZ

VMware® vShield™ App 5.0

TECHNICAL MARKETING DOCUMENTATION
V 1.0/ UPDATED JULY 2012
Table of Contents

Introduction ................................................................. 4
Virtualized DMZ Design .................................................. 4
  Fully Collapsed DMZ ................................................... 4
  Air Gap ................................................................ 5
vShield App Concepts .................................................... 5
  vShield App Containers ............................................... 5
    vSphere Resource Pools .............................................. 5
    Security Groups ......................................................... 5
  vApp ..................................................................... 5
    MAC Sets and IP Sets ............................................... 6
  Layer 2 and Layer 3 Rules ............................................. 6
Application Protocol Groupings ......................................... 6
DMZ Environment Example ............................................... 6
  DMZ Application Traffic ............................................... 6
    Application 1: Microsoft Exchange 2010 ....................... 7
    Application 2: IIS and MS-SQL .................................. 8
    Other Elements ......................................................... 8
  Use Policy Containers for Segmentation ......................... 8
    Security Group ......................................................... 8
    MAC Group ............................................................. 9
  Application Protocol Groups ....................................... 10
  Virtual Application (vApp) Containers ......................... 11
Creating Firewall Rules .................................................. 13
  Rule Set 1: Edge Transport Exchange Traffic .................. 13
  Rule Set 2: Allow Web Server DMZ Traffic .................... 14
  Rule Set 3: DMZ Management Traffic ............................ 14
  Rule Set 4: Edge Transport L2 Segmentation .................... 15
vShield SpoofGuard ......................................................... 15
DMZ Security Best Practices ........................................... 16
  Network Guidance ....................................................... 16
    Manage Network Bandwidth for the DMZ Tier ................ 16
    Enable vSphere Virtual Switch L2 Protections ................. 17
  Host Guidance .......................................................... 17
    Harden and Isolate Access to the vSphere Host ............... 17
    Use vSphere Host Resource Management Capabilities ......... 17
Table of Contents (continued)

VMware vCenter Server Guidance ........................................... 18
Operational Guidance .......................................................... 18
  Enforce Separation of Duties .............................................. 18
  Regularly Audit Virtualized DMZ Configuration ....................... 18
References ........................................................................ 19
About the Author ................................................................. 19
Acknowledgments ................................................................ 19
Secure Segmentation of Tier 1 Applications in the DMZ

Introduction

VMware® vShield™ App (vShield App) is a centrally managed, stateful, distributed virtual firewall. It protects virtual machines by placing a stateful firewall filter on every virtual network adaptor. vShield App enables simple-to-use, nondisruptive implementation of network security in VMware vSphere® (“vSphere”) environments.¹ This document focuses on the use of vShield App to secure applications in the DMZ.

Virtualized DMZ Design

There are two main ways to approach DMZ design with virtualization: fully collapsed and air gap. Because vShield App is transparent to network topology, the configuration of security groups and rules based on these groups remains the same between topologies.

Fully Collapsed DMZ

Taking full advantage of virtualization technology, this approach, shown in the following figure, virtualizes the entire DMZ—including all network and security devices. This design places virtual machines of different security levels on the same physical VMware® ESXi™ (ESXi) host and brings network security devices into the virtual infrastructure. The security of placing virtual machines of different trust levels on the same host has been assessed and ratified by third-party studies.² Sometimes described as a “DMZ in a box,” this configuration enables users to maximize server consolidation and realize significant cost reductions. This completely virtual infrastructure can fully enforce isolation and security for traffic entering, within, and leaving the DMZ.

¹ VMware vShield Edge, which provides edge firewall services, including stateful firewall, IPsec and SSL VPN, DHCP server, and load balancing, is not covered in this document.
The fully collapsed DMZ configuration completely leverages consolidation benefits. All servers and security devices are virtualized in this configuration, enabling users to isolate the virtual servers and the networks while managing communications between the zones with virtual security appliances. Because VMware® vShield™ (vShield) is designed from the ground up to work with vSphere capabilities such as VMware vSphere® High Availability (vSphere HA), VMware vSphere® vMotion® (vMotion), and VMware vSphere® Distributed Resource Scheduler™ (VMware DRS), this mitigates the impact of firewall security on operational, availability, and consolidation savings.

Although users can employ 802.1Q VLANs with L3 routing in this configuration, they are not required. Because of virtualization awareness, DMZ application silos can be secured logically and simply. Like submarine compartments, DMZ applications can be sealed airtight with layer 2 and layer 3 rules, allowing just the needed communication channels. This new way of creating security policies closely ties to the VMware virtual machine objects. The rules can follow the virtual machines during the vMotion process, and are completely transparent to IP address changes and network renumbering.

Air Gap

The air gap model isolates virtual machines into separate host clusters based upon function, such as DMZ and non-DMZ. This has two disadvantages: It requires extra hardware and it does not allow sharing of resources between clusters. Nevertheless, the features of vShield App described in this paper will apply identically, regardless of whether the fully collapsed or air gap mode of deployment is used. The logical configuration used by vShield App is not affected by the physical topology.

**vShield App Concepts**

**vShield App Containers**

Policy enforcement in vShield App is agile, because it is based on logical constructs, such as VMware® vCenter™ (vCenter) containers and vShield security groups—not just physical constructs, such as IP addresses. This new way of creating security policies can follow virtual machines during the vMotion process, and are completely transparent to IP address changes and network renumbering.

After a container is defined and resources are placed in it, the group can be used as a source and/or destination in a firewall rule across the user’s virtual distributed firewall infrastructure. The following types of containers can be used to define vShield App policies for the DMZ.

**vSphere Resource Pools**

vSphere resource pools are containers designed to enable sharing of compute and memory resources within groups of virtual machines. Because resource pools are often used to group closely associated virtual machines, such as those belonging to a particular department in a company, leveraging this group for certain kinds of vShield App policies is a natural fit.

**Security Groups**

The vShield security group is the most flexible of the containers, because it can include other groupings, such as datacenter, cluster, vApp, and resource pools, as well as physical objects, such as virtual machines, virtual network adaptors, port groups, and IP/MAC address sets. This enables users to create groupings based on any number of factors, such as type of application, scope of compliance, and so on.

**vApp**

A VMware vSphere® vApp™ (vApp) is a vSphere container of virtual machines that also can be nested. In addition to segmentation, it provides resource allocation and start-up/shut-down order controls. A multilayer application in a DMZ usually requires unique protocol filtering for each application, as well as unique security hardening, depending on the tier. This easily can be handled by defining a multiple-level, nested vApp, and then defining policies per vApp at the different levels.
MAC Sets and IP Sets
MAC sets are groupings of MAC addresses and IP sets are groupings of IP addresses. These are used when the virtual DMZ is connected to physical network segments or physical devices. An example is when there is a physical Web proxy filter appliance in the DMZ subnet.

Layer 2 and Layer 3 Rules
vShield App rules for identifying traffic being controlled are organized into the following:

- **L2**: Layer 2 (data link layer) rules control traffic over protocols such as ARP, IPv6, and PPP.
- **L3**: Layer 3 (network layer) rules control protocols such as TCP and UDP, and therefore related higher-layer application traffic, such as DHCP, HTTP, and FTP.

vShield App can create and enforce logical (i.e., not just VLAN- or physical subnet–based) application boundaries all the way down to OSI layer 2, which is critical to security, because many hacking attacks work at layer 2. This accords with the positive security model, because we can seal DMZ applications airtight with L2 and L3 rules, allowing just the needed communication channels.

By assessing what communication is required between each tier of the application, L2 rules can be created that block all unnecessary traffic. For example, in a typical DMZ application, the DMZ tier is required to communicate only with the outside world, the next tier down in the application, and possibly another set of virtual machines for infrastructure services such as DNS, NTP, logging, and so on. L2 rules can be used to ensure that no other internal virtual machines can communicate with the DMZ. After having locked down unnecessary traffic, L3 rules can be used to restrict necessary traffic channels to required ports and protocols.

Application Protocol Groupings
Distinct from virtual machine containers, application protocol groups are custom groupings of application protocols defined by protocol and port information. This enables users to bundle all required ports between two tiers of a multitier app into a single logical group, which can then be used, along with security groups, to define firewall rules. For cases where application traffic between tiers involves different protocols in each direction, two application protocol groups can be created per pair of tiers, one for each direction of traffic.

DMZ Environment Example
In this environment, we will show vShield App securing DMZ implementations of Microsoft Exchange and a custom Web application using an IIS Web server and MS-SQL database. We will follow the positive security model, which means a “default deny” follows after all other firewall rules. The reader should refer to the VMware vShield Administration Guide for installation and basic configuration steps.³

DMZ Application Traffic
The following diagram shows how virtual machines in the environment will be secured using these application groups and containers: Exchange Edge Transport, IIS Web server traffic,⁴ and management consoles.

---

Each application is described in detail in the next few sections.

**Application 1: Microsoft Exchange 2010**

For this example, we are using a vShield App 5.0 firewall to secure the Microsoft Exchange Server 2010 Edge Transport server role in the DMZ. Because the vShield App rules use containers and application protocol groupings, we can create firewall rules for each functional server type. The defined server types are as follows:

1. **Client access server**
   This provides mailbox server protocol access for OWA, POP3/IMAP4, and ActiveSync (mobile-device) clients.

2. **Mailbox server**
   This hosts the mailbox and public folder data. It also provides MAPI access for Outlook clients. The Mailbox servers can be deployed in a cluster for availability in a database availability group (DAG).³

3. **Edge Transport server**
   The final hop of outgoing mail and initial hop of incoming mail, it is designed to be placed in the perimeter/DMZ. It does not need to belong to the domain or send DNS queries to the DNS server. It also provides mail quarantine and SMTP service to enhance security.

4. **Hub Transport server**
   This routes mail to the next hop, which can be a Hub Transport, Edge Transport, or Mailbox server. It uses AD site information to determine the mail flow.

5. **Unified Messaging**
   This enables end users to access their mailbox, address book, and calendar using a telephone and voice. It requires a PBX or VoIP gateway.

---

This example uses firewall rules for vShield App to provide security segmentation for the Edge Transport server. According to Exchange 2010 best practices, only the Edge Transport server should be in the DMZ. The Edge Transport server role is deployed outside the Exchange organization as a standalone server in the perimeter network or as a member of a perimeter network Microsoft Active Directory domain.

Application 2: IIS and MS-SQL
This example secures the Web server (Rx-Tracker-Web) of a healthcare application in the DMZ. The Web server uses IIS and the database is MS-SQL. vShield App will be used to perform the following:
1. It will allow only needed protocols in and out of the DMZ.
2. It will isolate the servers in the DMZ completely from each other’s traffic.

Other Elements
In addition to the two applications, this example will control traffic related to two other elements in the environment:
1. A management resource pool, which contains the virtual machines running management consoles for the IT administrators.
2. Reverse Web proxies, running on physical devices.

Use Policy Containers for Segmentation
Security Group
First, we create a Security Group container for the servers in the DMZ, called “DMZ.”

<table>
<thead>
<tr>
<th>CORP</th>
<th>General</th>
<th>Flow Monitoring</th>
<th>App Firewall</th>
<th>Endpoint</th>
<th>SpooGuard</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hosts</td>
<td>Port Groups</td>
<td>Grouping</td>
<td>Applications</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ</td>
<td>Security Group</td>
<td>[EDGE], [Rx-Tracker-Web]</td>
</tr>
</tbody>
</table>

MAC Group

We then create a MAC group of the MAC addresses of the network interfaces of the physical Web reverse proxies connected to the DMZ, called “Web Proxy.”
Secure Segmentation of Tier 1 Applications in the DMZ

Application Protocol Groups

We start by creating an application protocol group for external Web traffic to/from the Rx-Tracker-Web server. Using the VMware vSphere® Client™ (vSphere Client), go to the Home > Inventory > Hosts and Clusters view. At the CORP datacenter level, navigate to General > Applications > Add. Name the new application protocol group “Web.” Click **Ok** to save.

The completed application group looks like the following:

![Application Protocol Group](image)

In the same way, we create an application protocol group for SMTP (TCP 25) and SMTP antirelay (TCP 587) called “SMTP 25, 587” at the CORP level. We also will use the default rule “SMTP” for internal Exchange communication between the Edge Transport and the Hub Transport servers.

![Application Protocol Group](image)

Finally, we must create an application protocol group for the management traffic types (in this case, RDP and SSH) allowed into the DMZ.
Secure Segmentation of Tier 1 Applications in the DMZ

Virtual Application (vApp) Containers

Next, we create virtual application (vApp) containers for Exchange servers. “Exchange” is the parent vApp, and each type of Exchange role has a child vApp containing the actual virtual machines. For example, the Edge Transport role is contained in a child vApp named “EDGE,” and the virtual machines are EDGE01 and EDGE02. All of these vApp or virtual machine names can be used as source of destination in vShield firewall rules.

Right-click the newly created Exchange vApp icon in the inventory panel of the vSphere Client. Select Add New vApp, type in the name of the Exchange role, EDGE, and save.
Repeat for CAS, Mailbox, and HUB. The created nested vApp looks like the following:

We will do the same for the Web and database (DB) servers of the healthcare application.
Creating Firewall Rules

Now that all the containers have been defined for this example, rules can be created using the easily understandable container names.

Rule Set 1: Edge Transport Exchange Traffic

These rules allow for all recommended ports in the Microsoft Exchange 2010 Edge Transport–required ports document.\(^7\)

<table>
<thead>
<tr>
<th>SOURCE IP</th>
<th>SOURCE PORT</th>
<th>DEST. IP</th>
<th>TRANSPORT PROTOCOL</th>
<th>DEST. PORT</th>
<th>APPLICATION PROTOCOL</th>
<th>COMMENT</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>ANY</td>
<td>Edge</td>
<td>TCP</td>
<td>25, 587</td>
<td>SMTP</td>
<td>ALLOW</td>
<td></td>
</tr>
<tr>
<td>Edge</td>
<td>ANY</td>
<td>ANY</td>
<td>TCP</td>
<td>25, 587</td>
<td>SMTP</td>
<td>ALLOW</td>
<td></td>
</tr>
<tr>
<td>Hub</td>
<td>ANY</td>
<td>Edge</td>
<td>TCP</td>
<td>25</td>
<td>SMTP</td>
<td>ALLOW</td>
<td></td>
</tr>
<tr>
<td>Hub</td>
<td>ANY</td>
<td>Edge</td>
<td>TCP</td>
<td>50636</td>
<td>EdgeSync</td>
<td>ALLOW</td>
<td></td>
</tr>
<tr>
<td>Edge</td>
<td>ANY</td>
<td>Hub</td>
<td>TCP</td>
<td>25</td>
<td>SMTP</td>
<td>ALLOW</td>
<td></td>
</tr>
</tbody>
</table>

The completed rule set will look like the following:

![Image of vSphere Client UI with App Firewall tab]

NOTE: The default deny rule at the bottom of the list is in accordance with the positive security model, which dictates that all communications should be denied unless explicitly required. The default deny at the end of the preceding table should be created in the “System Defined” section of L3 rules in the Home > Inventory > Hosts and Clusters > CORP > vShield > App Firewall tab of the vSphere Client UI, because it must operate after all other L2 and L3 rules.

Rule Set 2: Allow Web Server DMZ Traffic
This rule allows common Web client port access to the Web server.

<table>
<thead>
<tr>
<th>SOURCE IP</th>
<th>SOURCE PORT</th>
<th>DEST. IP</th>
<th>TRANSPORT PROTOCOL</th>
<th>DEST. PORT</th>
<th>APPLICATION PROTOCOL</th>
<th>COMMENT</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Proxy</td>
<td>ANY</td>
<td>Rx-Tracker-Web</td>
<td>TCP</td>
<td>80, 443</td>
<td>Web</td>
<td>ALLOW</td>
<td></td>
</tr>
<tr>
<td>ANY</td>
<td>ANY</td>
<td>Rx-Tracker-Web</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>DENY</td>
<td></td>
</tr>
</tbody>
</table>

Create a rule to allow the Web traffic requests to be forwarded from the corporate perimeter Web proxy/filter to Rx-Tracker-Web. The completed rule in the vSphere Client is as follows:

NOTE: The default deny rule is the same one we set earlier—that is, the “System Defined” row automatically operates after all other L3 rules.

Rule Set 3: DMZ Management Traffic
This rule allows RDP and SSH sessions to be initiated from the Management resource pool to the DMZ.

<table>
<thead>
<tr>
<th>SOURCE IP</th>
<th>SOURCE PORT</th>
<th>DEST. IP</th>
<th>TRANSPORT PROTOCOL</th>
<th>DEST. PORT</th>
<th>APPLICATION PROTOCOL</th>
<th>COMMENT</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>ANY</td>
<td>DMZ</td>
<td>TCP</td>
<td>22, 3389</td>
<td>Management Applications</td>
<td>ALLOW</td>
<td></td>
</tr>
</tbody>
</table>

The completed rule in the vSphere Client is as follows:
Rule Set 4: Edge Transport L2 Segmentation

This rule set provides a complete layer 2 and higher block to any traffic between the Rx-Tracker-Web and Exchange Edge Transport servers. This is recommended, because the two DMZ servers should never communicate directly with each other. If one of the servers is compromised, it cannot be used to directly attack the other server. Even ARP and RARP will be denied.

<table>
<thead>
<tr>
<th>SOURCE IP</th>
<th>SOURCE PORT</th>
<th>DEST. IP</th>
<th>TRANSPORT PROTOCOL</th>
<th>DEST. PORT</th>
<th>APPLICATION PROTOCOL</th>
<th>COMMENT</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDGE</td>
<td>ANY</td>
<td>Rx-Tracker-Web</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>DENY</td>
<td></td>
</tr>
<tr>
<td>Rx-Tracker-Web</td>
<td>ANY</td>
<td>EDGE</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>DENY</td>
<td></td>
</tr>
<tr>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>ALLOW</td>
<td></td>
</tr>
</tbody>
</table>

The completed rule in the vSphere Client is as follows:

**NOTE:** We have a default allow rule in the L2 System Defined row. This is because L2 rules operate before L3 rules, and a default deny L2 would not allow any traffic flow out of any virtual machine unless an explicit L2 allow rule applied to it. Instead, we construct L3 rules to selectively control virtual machine traffic and then use explicit L2 deny rules for those channels that we want to block completely. In this case, we are using L2 rules between the Edge and Rx-Tracker-Web virtual servers in the DMZ, because there is no need for the two to communicate with each other.

**vShield SpoofGuard**

SpoofGuard is an advanced protection against man-in-the-middle (MITM) attacks that is available with vShield App. It is a layer 2 security feature that enables the administrator to verify IP/MAC pairs for every virtual network adaptor. By using SpoofGuard, an administrator can manually or automatically inspect and reject new MAC/IP pairs. Crafted packets from a compromised virtual machine in the DMZ, with altered IP or MAC addresses, will be dropped right at the virtual network interface.

SpoofGuard is enabled in the vSphere datacenter context. There are the two following options:

1. Automatically trust IP assignments on first use.
2. Manually approve all assignments.
Secure Segmentation of Tier 1 Applications in the DMZ

In the SpoofGuard tab, the user can verify the MAC address, IP address, virtual machine name, and approver/date approved.

DMZ Security Best Practices

Regardless of the application being secured in the DMZ, there are a number of best practices for vShield App configuration that should be employed. The following section discusses these generic best practices, and then shows how they can be applied to a specific real-world application.

This is a summary of DMZ profile hardening guide recommendations for vSphere 5 environments. For complete documentation, including the security guide for vSphere 5, check here.

Network Guidance

Manage Network Bandwidth for the DMZ Tier

One key capability available with the VMware vSphere® Distributed Switch (VDS) is network I/O control (NIOC), which enables the control of bandwidth using the concept of groups and shares. By managing the traffic in the DMZ tier, users can protect other tiers from denial of service on the network, due either to DMZ virtual machine compromise, unexpected demand, or configuration error.

The NIOC shares are configured on the dvportgroups of the VDS, so to take advantage of this feature, DMZ-tier virtual machines must be placed on a separate dedicated dvportgroup. This dvportgroup does not need to have a unique VLAN. By fixing the shares for the DMZ dvportgroup, the user can be assured that traffic flowing in and out of the DMZ will never overwhelm the other virtual machines on that host.

For more details on VDS concepts, see VMware vSphere Distributed Switch Best Practices.
Secure Segmentation of Tier 1 Applications in the DMZ

Enable vSphere Virtual Switch L2 Protections
This protects against MITM attacks if a virtual machine in the DMZ is compromised. Another virtual machine in the DMZ cannot falsely advertise itself as the gateway for that subnet.

After initial setup is completed or a new virtual machine is added to the virtual switch or port group, users lock down layer 2 changes by disabling Promiscuous Mode, MAC Address Changes, and Forged Transmissions. This helps protect against attacks such as data snooping, sniffing, and MAC spoofing.

Host Guidance

Harden and Isolate Access to the vSphere Host
- Use the vSphere (ESXi) host firewall to limit the IPs allowed to access the management IP. This stops any hacker from trying to connect to the DMZ ESXi hosts using an IP different from the vi-admin designated system IPs.
- Make sure that the host management interface and IP is accessible only to authorized administrators. This can be achieved in the following ways:
  - Use a VPN to restrict access to the management network.
  - Limit the permitted systems on the management network.
  - Use a JumpBox.
  - An example of this is a hardened Windows or Linux host, which allows connections only on limited management traffic ports, such as HTTP/S, RDP, or SSH. The firewall on the ESXi host would be set to allow connections only from this JumpBox IP to the management interface IP.

Use vSphere Host Resource Management Capabilities
Denial of service within a virtual environment can occur if an individual virtual machine is allowed to use a disproportionate share of vSphere host resources. In so doing, it starves other virtual machines running on the same vSphere host. One instance of this in the DMZ is when a virtual machine in the DMZ is compromised.

The following actions can guard against this possibility:
- Set resource reservations and limits for virtual machines using VMware vCenter Server™ (vCenter Server). These controls are in the Resources tab of the individual Virtual Machine Properties menu.
- Use VMware DRS. Using vShield App within VMware DRS clusters ensures secure compute load-balancing operations without performance compromise, because the security policy follows the virtual machine.
VMware vCenter Server Guidance

The following guidelines should be observed when configuring the VMware vCenter Server system being used to manage the DMZ hosts.

- Least Privilege roles and permissions assigned to administrators
- Default Administrators group removed as a VMware vCenter administrator and disabled in Windows
- Special-purpose local vSphere administrators’ account created on vCenter Server
- Separation of duties between network, server, and virtual machine administrators
- Lockdown mode enabled on hosts, DCUI left enabled
- Hosts access integrated with AD
- All certificates changed from defaults to CA signed certificates to prevent MITM attacks
- Remote logging to centralized syslog servers, logs mirrored across sites
- NTP used to maintain consistent time
- Nonservice account access attempts to vCenter Server certificate directory monitored and alert sent to administrators via enterprise monitoring system
- All access to managed object browser disabled
- Access to management network restricted to a limited subset of administrator desktops
- Database privileges locked down to minimum
- Patching using VMware vSphere® Update Manager™ via VUMDS

Operational Guidance

Enforce Separation of Duties

Mitigate configuration mistakes by using VMware vCenter Server to define roles and responsibilities for each administrator of the vSphere environment. By distributing rights based on skills and responsibilities, users can significantly reduce the chance of misconfiguration. Because the DMZ tends to have very specific and well-known applications and user roles, restricting rights to an as-needed basis follows Least Privilege. As an added benefit, this method also limits the amount of authority any one administrator has over the system as a whole. One specific user might be an information security officer with permissions to audit the DMZ configuration. A read-only role can be created for this purpose in the VMware vCenter Server and VMware vShield Manager.

Regularly Audit Virtualized DMZ Configuration

Regular audit of configurations is essential in both physical and virtual environments. When virtualizing a DMZ or any part of the infrastructure, it is important for users to regularly audit the configurations of all of the components—including vShield, vCenter Server, and virtual switches. Users must conduct these audits to make sure that changes to configurations can be controlled and that the changes do not cause a security hole in the configuration.
References

vShield documentation  
https://www.vmware.com/support/pubs/vshield_pubs.html  

VMware vSphere 5.0 Hardening Guide  
http://vmware.com/go/securityguides  

CESG and VMware Deliver Trusted Platform for Hosting Multi-Level Environments  

VMware vSphere Distributed Switch Best Practices  

What’s New in VMware vSphere 5.0 Networking  

About the Author

Grant Suzuki is part of the Networking and Security Technical Marketing team. He has secured infrastructures working at Symantec, Blue Coat, McAfee, and many government organizations.

Acknowledgments

The author would like to thank the following individuals for their valuable contribution to this paper:

• Rob Randall, VMware Principal Security and Compliance Solutions Architect
• Jeff Szastak, VMware Staff Systems Engineer – CoE Solutions Specialist