OVERVIEW OF VIRTUAL FIREWALLS ON VBLOCK™ INFRASTRUCTURE PLATFORMS

June 2012
Contents

Introduction ............................................................................................................................... 3
  Purpose ................................................................................................................................... 3
  Scope ...................................................................................................................................... 3
  Audience ................................................................................................................................. 3
  Feedback ................................................................................................................................ 3

Virtual and Physical Firewalls .................................................................................................. 4
  Physical Firewalls .................................................................................................................... 4
  Virtual Firewalls ....................................................................................................................... 5
  Key Benefits of Virtual Firewalls ............................................................................................... 5

Technology Overview ................................................................................................................. 8
  Vblock™ Infrastructure Platforms ............................................................................................. 8
  Cisco Virtual Firewall Products ................................................................................................ 9
  VMware Virtual Firewall Products .......................................................................................... 13
  Choosing a Virtual Firewall .................................................................................................... 16

Virtual Firewall Scenarios ......................................................................................................... 18
  Scenario 1: Three-Tiered Application ..................................................................................... 18
  Scenario 2: Virtual Desktops .................................................................................................. 22
  Scenario 3: Multi-Tenancy ..................................................................................................... 24
  Scenario 4: Demilitarized Zone .............................................................................................. 26

Conclusion .............................................................................................................................. 29
  Next Steps ............................................................................................................................. 29

References .............................................................................................................................. 30
Introduction

Network-based security has traditionally been implemented in data centers using various physical appliances placed in strategic locations on an infrequently changing network fabric. Zones of trust have been statically defined by IP addresses generally associated with specific locations.

Virtualization and the dynamic nature of a virtual environment change this paradigm. Now that workloads can be moved between locations, as well as instantiated or retired rapidly, the static, physical model falls short.

Static security is being replaced by, or augmented with, a more dynamic set of security products that operate without restrictions relating to physical location or boundaries. These virtual firewalls provide protection and benefits beyond the limitations of physical security.

Purpose

This paper provides an overview of virtual firewalls and explores the strategies of Cisco and VMware. It outlines when to use each type of firewall and discusses some common scenarios. After reading this paper, you should better understand how you can use Vblock™ Infrastructure Platforms and virtual firewalls together to address network access control requirements.

Use this paper as an introduction to virtualized firewalls. A thorough review of the Vblock platform requirements and your security requirements is recommended before selecting a virtualized firewall product.

Scope

This paper is a high-level overview of the virtual firewall offerings from Cisco and VMware. It is not an implementation guide, nor does it advocate the use of any particular products or security architectures or models. Issues relating to specific compliance objectives are also outside the scope of this document.

Audience

The primary audience for this paper is security administrators. The secondary audience is risk managers and auditors. Technical consultants, professional services personnel, IT managers, security architects, partner engineers, sales engineers, and customers architecting, implementing, managing, and auditing security controls on Vblock platforms may also find it useful.

Feedback

To suggest documentation changes and provide feedback on this paper, send email to docfeedback@vce.com. Include the title of this paper, the name of the topic to which your comment applies, and your feedback.
Virtual and Physical Firewalls

This section looks at some limitations of physical firewalls in a virtualized environment, as well as some of the concepts and benefits of virtual firewalls.

Physical Firewalls

Traditionally, network-based security has been implemented in data centers using various physical appliances placed in strategic locations on an infrequently changing network fabric. However, when this approach is used for a virtualized data center, it can lead to a number of problems, including:

- Bandwidth chokepoints
- Capacity sizing
- No intra-host virtual machine visibility
- Rigid physical topologies

Network Security Devices Become Bandwidth Chokepoints

Physical network security appliances require the virtual environment to be architected so that all network connections eventually pass through one of a small number of security appliances. This can splinter the virtual environment into isolated network-based silos, thus complicating administration and reducing the potential for sharing.

Capacity Sizing

Physical security devices are typically fixed-capacity; therefore, capacity is usually under- or over-provisioned. This is of particular concern in a virtual environment, which can change requirements rapidly.

No Intra-Host Virtual Machine Visibility

Traffic flowing between virtual machines on the same VMware vSphere host might never touch the physical network, and so it cannot be viewed, or even protected, by a physical firewall or security device. This requires virtual firewalls to apply network/security policies to locally switched virtual machine-to--virtual machine traffic or for all traffic to be sent inefficiently off-host.

Rigid Physical Topologies

Traditional firewall implementation security policies are directly tied to the physical topologies of the implementation rather than the workloads, which results in a rigid implementation that limits what can be done for and to the workloads. Virtual environments cater to the dynamic needs of an organization using autonomic and dynamic load balancing (Dynamic Resource Scheduling), rapid provisioning, and reconfiguration. Any solution based on a static network topology is simply not compatible with these capabilities.
Virtual Firewalls

Static security is being replaced by, or augmented with, a more dynamic set of security products. While some products in the virtual security space are simply repackaged static security solutions, some of the new offerings exemplify the new paradigm by operating without restrictions relating to physical location or boundaries. These offerings must also adapt to the elastic scaling of capacity in response to dynamic inventory and configuration changes.

Virtual firewalls enable the use of network access controls between virtual machines (VMs) and other points in virtual and physical environments. Virtual firewalls are deployed within the fabric of the virtualization environment. The Cisco and VMware virtual firewall products outlined in this paper are deployed as either a hypervisor module and firewall service virtual appliance or as a virtual service blade on a distributed virtual switch.

Virtual firewalls operate using traditional IP address/protocol-based controls (“5-tuple”), but many can leverage other information like virtual machine attributes to enable higher-level policy-based management. Virtual firewalls have the following features:

- Integrate with the hypervisor, and, for the purposes of this discussion, interoperate with one or more types of distributed virtual switches
- Scale to effectively manage the policies of a large number of endpoints through integration with distributed virtual switch technologies and their centralized administration capabilities

Key Benefits of Virtual Firewalls

Virtual firewalls provide protection and benefits beyond the limitations of physical security in several significant ways:

- Dynamic (virtualization-aware) operations
- Ease of management
- Multi-tenant support
- Optimized operation model
- Cost-effectiveness

Dynamic (Virtualization-Aware) Operations

Virtualization can be highly dynamic with frequent add, delete, and change operations on virtual machines. Live migration of virtual machines occurs through manual or programmed events. The change awareness capability of virtual firewalls makes it possible to enforce stateful security policies that travel with virtual machines as they migrate from host to host or are freshly instantiated from templates. In addition, programmatic solutions can be implemented to automatically support and ensure compliance with business requirements.
Ease of Management

Virtual firewall technologies from Cisco and VMware connect to every virtual machine; therefore, policies can be applied to all traffic entering and exiting each system. This has two major benefits:

- It becomes practical to regulate all traffic, enabling control over both active and passive insider threats (for example, hackers and worms). This was not easy to do with physical firewalls.
- It enables a level of visibility into traffic that did not previously exist (for example, logging all traffic between two hosts within the same zone of trust).

The virtual firewall technologies make it possible to provide the same level of visibility to other tools, such as intrusion detection systems and intrusion prevention systems. This provides organizations more granular control and visibility into their systems and, with the enhanced support for automation (API’s and attribute-awareness, for example), more dynamic administration of the resources.

For example, a report of a blocked event on a perimeter firewall might trigger an attribute change on an internal host that causes comprehensive logging of all activity in which that particular host engages.

Multi-Tenant Support

Virtual firewalls support concurrent tenant-specific configurations and security policies. Logical security perimeters protect virtual data centers and enable safe sharing of network resources in multi-tenant infrastructures.

Optimized Operation Model

As organizations become more comfortable with combining roles where there is a platform or virtualization administrator, individual administrators can perform the responsibilities previously associated with legacy security, network, and server administrator roles. Administrators in a virtual environment are empowered to act in many facets of IT operations but they are still subject to the same checks and balances of organization policies and workflows.

However, if separation of duties is an important factor to your business, integration with distributed virtual switch technologies enables virtual firewalls to provide seamless integration with VMware vCenter while preserving traditional roles. This leaves the traditional IT operating model intact for:

- Security administrators to define security rules and policies
- Network administrators to manage those policies and associate them with a particular port profile
- Server administrators to select the appropriate port group; for example, Cisco Nexus 1000V-equivalent port profile for the particular virtual machine

This integration provides administrative separation between server, network, and security administrators, but effectively delegates aspects of security enforcement in ways that also increase efficiency compared with physical deployments.
A key decision to make is where to place your organization on a scale ranging from maximum efficiency to maximum separation of duties. Note that with the virtual firewall offerings discussed in this paper, for a sizable deployment any point on the scale is likely to be more efficient than a physical firewall.

Cost-Effectiveness

Virtual firewalls can be deployed as a virtual security appliance or a firewall service on a distributed virtual switch, such as Cisco Nexus 1000V on a Vblock platform. This enables effective allocation of capacity by tying security hardware and software expenditures to workload expansion. With the reduction in traditional physical components, the virtual firewall solution simplifies any physical complexity in deployments, resulting in lowered support costs. A single virtual appliance or framework with breadth of functionality provides comprehensive protection, eliminating the need for specialized hardware and multiple-point solutions specific to the Vblock platform and thus significantly reducing cost.
Technology Overview

This section looks at virtual firewall products from Cisco and VMware available for use with Vblock platforms.

Vblock™ Infrastructure Platforms

With Vblock platforms, VCE delivers the industry's first completely integrated IT offering that combines best-of-breed virtualization, networking, computing, storage, security, and management technologies with end-to-end vendor accountability. This converged infrastructure enables rapid virtualization deployment, so customers see an accelerated return on investment.

Vblock platforms are characterized by:

- Repeatable units of construction based on matched performance, operational characteristics, and discrete power, space, and cooling requirements
- Repeatable design patterns that facilitate rapid deployment, integration, and scalability
- An architecture that can be scaled for the highest efficiencies in virtualization
- An extensible management and orchestration model based on industry-standard tools, APIs, and methods
- A design that contains, manages, and mitigates failure scenarios in hardware and software environments

Vblock platforms provide pre-engineered, production-ready (fully tested) virtualized infrastructure components, including industry-leading technology from Cisco, EMC, and VMware. Vblock platforms are designed and built to satisfy a broad range of specific customer implementation requirements.

Refer to the Vblock Infrastructure Platforms Technical Overview for detailed information on the Vblock platform architecture.
Cisco Virtual Firewall Products

Cisco offers two virtual firewall products along with a management console to provide enterprise-class security for virtualized environments:

- Cisco Virtual Security Gateway (VSG)
- Cisco ASA 1000V Cloud Firewall
- Cisco Virtual Network Management Center (VNMC)

Implementing Cisco Virtual Security Gateway with Cisco ASA 1000V in a virtual multi-tenant data center security solution provides tenant edge, intra-tenant, and inter-tenant virtual and cloud security. Cisco Virtual Security Gateway and the Cisco ASA 1000V Cloud Firewall provide complementary functionalities:

- Cisco Virtual Security Gateway provides virtual machine context-aware and zone-based security capabilities
- Cisco ASA 1000V Cloud Firewall enables multi-tenant edge security, default gateway functionality, and protection against network-based attacks

Together, they provide a trusted and comprehensive virtual firewall solution. The Cisco virtual security solution requires integration with the Cisco Nexus 1000V distributed virtual switch.

Note: This particular switch is part of the standard configuration on some Vblock platforms, which allows for a Cisco solution for virtual security on a Vblock platform.

Cisco Virtual Security Gateway

The Cisco Virtual Security Gateway enables a broad set of multi-tenant workloads that have varied security profiles to share a common compute infrastructure. By associating one or more virtual machines into distinct zones of trust defined under tenant policy, Cisco Virtual Security Gateway ensures that access to zones of trust is controlled and monitored through established security policies. It uses virtual network service data path (vPath) technology embedded in the Cisco Nexus 1000V Series Virtual Ethernet Module (VEM), offering transparent insertion and efficient deployment.
Cisco Virtual Security Gateway is deployed as a virtual appliance on VMware (deployed from an Open Virtualization Format (OVF) template) or as a virtual service blade on the Cisco Nexus 1010 Virtual Services Appliance. Figure 1 shows the overall architecture of the Cisco Virtual Security Gateway solution and how the required components of the solution are integrated.

Cisco Virtual Security Gateway operates with the Cisco Nexus 1000V Series distributed switch in the VMware vSphere hypervisor and it uses the Cisco vPath technology, which is embedded inside the Cisco Nexus 1000V Virtual Ethernet Module. It intercepts traffic at the hypervisor layer and directs it to the appropriate networking service. Cisco vPath also provides policy-enforcement offload capabilities from the networking services to the vPath. This enables fast-path capabilities for the networking services at the hypervisor layer. The Cisco Virtual Network Management Center virtual appliance provides centralized device and security policy management of Cisco Virtual Security Gateway. Cisco Virtual Network Management Center registers to VMware vCenter to have visibility into the VMware environment.

**Figure 1. Cisco Virtual Security Gateway solution architecture**
The key components of the Cisco Virtual Security Gateway solution are listed below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Virtual Network Management Center</td>
<td>A virtual appliance that provides centralized device and security policy management of Cisco Virtual Security Gateway. Supports multi-tenant environments.</td>
</tr>
<tr>
<td>Cisco Virtual Security Gateway</td>
<td>Operates with the Cisco Nexus 1000V Distributed Virtual Switch (DVS) in the VMware vSphere hypervisor; uses the vPath embedded in the Cisco Nexus 1000V Series Virtual Ethernet Module.</td>
</tr>
<tr>
<td>Cisco Nexus 1000V Series Switches</td>
<td>Virtual machine access switches that are an intelligent switch implementation for VMware vSphere environments running the Cisco NX-OS software operating system.</td>
</tr>
<tr>
<td>VMware vCenter Server</td>
<td>Manages the vSphere environment and provides unified management of all the hosts and virtual machines in the data center from a single console.</td>
</tr>
</tbody>
</table>


**Cisco ASA 1000V Cloud Firewall**

The Cisco ASA 1000V Cloud Firewall is a virtual security appliance that extends the Adaptive Security Appliance (ASA) security platform to provide enterprise-class security for virtual and cloud infrastructures. Complementing the zone-based security capabilities of Cisco Virtual Security Gateway, Cisco ASA 1000V is optimized to provide multi-tenant edge security, default gateway capability, and protection against network-based attacks. It can also serve as a VXLAN gateway. It integrates with Cisco Nexus 1000V, which enables a multi-hypervisor capable solution and allows a single Cisco ASA 1000V instance to secure multiple ESXi hosts.

In addition to its integration with the Cisco Nexus 1000V, Virtual Security Gateway, and Virtual Network Management Center components, Cisco ASA 1000V extends the ASA product line to provide end-to-end security for hybrid infrastructures (physical-virtual-cloud).

Figure 2 illustrates the integration of the Cisco ASA 1000V solution components.
Cisco ASA 1000V acts as the edge firewall while Cisco Virtual Security Gateway controls the virtual machine–to–virtual machine traffic. Similar to Cisco Virtual Security Gateway, Cisco ASA 1000V integrates with the Cisco Nexus 1000V switch and uses its Virtual Ethernet Module-embedded vPath technology. Cisco Virtual Network Management Center acts as the primary management console for creating security policies for the Cisco ASA 1000V firewall.

A complete list of solution deployment considerations and requirements for Cisco ASA 1000V along with product literature is available at http://www.cisco.com/go/asa1000v.
Cisco Virtual Network Management Center

Cisco Virtual Network Management Center is a transparent, scalable, multi-tenant capable, policy-driven management solution for the Cisco virtual security appliances such as Cisco ASA 1000V and Cisco Virtual Security Gateway that provides end-to-end security of virtualized infrastructures. Key benefits of Cisco Virtual Network Management Console include:

- Rapid, scalable deployment through dynamic, template-driven policy management based on security profiles
- Management flexibility through an XML API that helps enable programmatic integration with third-party management and orchestration tools
- Collaborative governance with role-relevant management interfaces for network, server, and security administrators

Cisco Virtual Network Management Center acts as the primary GUI-based manager for both Cisco ASA 1000V and Cisco Virtual Security Gateway. In addition, Cisco Adaptive Security Device Manager (ASDM) can manage Cisco ASA 1000V. Cisco Virtual Security Gateway deployments on the Cisco Nexus 1010 appliance are managed entirely through the command-line interface (CLI).

VMware Virtual Firewall Products

VMware vShield products offer security services within a single management framework for securing virtual data centers and cloud environments at all levels—host, network, application, data, and endpoint.

The VMware vShield products include:

- VMware vShield App
- VMware vShield Edge
- VMware vShield Endpoint
- VMware vShield Zones
- VMware vShield Manager

VMware vShield leverages the unique advantages virtualization brings to security—such as introspection, hardware independence, and change awareness—and integrates with VMware vCenter Server to give a single framework for security hosts, networks, applications, data and endpoints against internal and external threats. For further information about VMware vShield products go to http://www.vmware.com/products/vshield/overview.html.
VMware vShield App

VMware vShield App protects applications from network-based threats in the virtual data center with a hypervisor-level application firewall and administrator-defined containers called security groups to enforce granular segmentation between applications. It provides firewalling between virtual machines by placing a firewall filter on every virtual network adapter and implements an IP-based stateful firewall and application layer gateway for a broad range of protocols including Oracle, FTP, Sun/Linux/Microsoft remote procedure call (RPC). This firewall filter operates transparently and does not require network changes or modifications of IP addresses.

VMware vShield App installs as a hypervisor module and firewall service virtual appliance on each ESXi host in the cluster hosting the protected virtual machines. The hypervisor module places a vNIC-level firewall enforcement point for the traffic to and from the virtual machines. VMware vShield App is tightly integrated with VMware vSphere, and therefore works with vSphere features such as Distributed Resource Scheduler (DRS), vMotion, Distributed Power Management (DPM), and Maintenance mode.

In addition to the hypervisor-level firewalling, policy management, logging, and auditing features, VMware vShield App extends into Sensitive Data Discovery (available in vShield App with Data Security). VMware vShield App with Data Security enables IT organizations to quickly assess the state of compliance with regulations from across the world. It also provides a management console for selecting regulations to be used in compliance scans, and includes templates of regulations including PCI-DSS (Payment Card Industry–Data Security Standard), Private Health Information (PHI), and so forth. Additional discussion related to DLP and vShield App with Data Security are outside the scope of this document.

VMware vShield Edge

VMware vShield Edge secures the edge, or perimeter, of a virtual data center with firewalling, VPN, NAT, DHCP, and Web load-balancing capabilities that enable rapid, secure scaling of virtualized infrastructures. Along with network isolation, these services create logical security perimeters around virtual data centers and enable secure multi-tenancy. VMware vShield Edge is compatible with port groups on the vNetwork Standard Switch (VSS), vNetwork Distributed Switch (vDS), and the Cisco Nexus 1000V switch. VMware vShield Edge management is supported through the VMware vShield Manager Web interface and the VMware vShield Manager plug-in to VMware vCenter Server.

The VMware vShield Edge virtual appliance has external and internal network interfaces. The internal interface connects to the secured inside port group and is the gateway for all protected virtual machines in this port group. The external interface connects to an uplink port group that has access to a shared corporate network or a service provider access-layer network.

VMware vShield Edge deployments use one of the following methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Group Isolation</td>
<td>Creates a secure, isolated network without VLANs or PVLANs; once Port Group Isolation is enabled, virtual machines can communicate only within the port group and use vShield Edge as the gateway. Installs as a hypervisor module and service virtual appliance on each VMware ESXi host and is only available on a vNetwork Distributed Switch.</td>
</tr>
<tr>
<td>Method</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standard VLAN configuration</td>
<td>Isolation of virtual machines is provided exclusively by the VLAN, and VMware vShield Edge is used as the gateway to communicate with the external network. Supported on a VSS, vDS, and Cisco Nexus 1000V.</td>
</tr>
</tbody>
</table>

**VMware vShield Endpoint**

VMware vShield Endpoint optimizes antivirus and other host and endpoint security for use in VMware vSphere environments. VMware vShield Endpoint offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. It enables users to manage antivirus and anti-malware policies for virtualized environments with the same management interfaces used to secure physical environments. It enforces remediation using predefined policies that dictate whether a malicious file should be deleted, quarantined, or otherwise handled. The VMware vShield Endpoint driver manages file remediation activity within the virtual machine. It also helps satisfy compliance and audit requirements through logging of antivirus and anti-malware activities.

Although VMware vShield Endpoint is part of the VMware vShield family, detailed technical discussions related to it are outside the scope of this document. Refer to [http://www.vmware.com/products/vshield-endpoint/overview.html](http://www.vmware.com/products/vshield-endpoint/overview.html) for additional information on VMware vShield Endpoint.

**VMware vShield Zones**

VMware vShield Zones enable basic segmentation of traffic between virtual machines allowing for connections to be packet filtered and grouped based on the 5-tuple—source IP address, destination IP address, source port, destination port, and protocol. VMware vShield Zones are deployed per VMware vSphere host and serves as an application-aware firewall for the virtual data center. Depending on how services are virtualized, this may be sufficient for security policies that do not require much granularity.

**VMware vShield Manager**

VMware vShield Manager is the central point of control for all vShield solutions and integrates seamlessly with VMware vCenter to offer role-based access control and administrative delegation in a unified framework for managing virtualization security. It promotes IT compliance with centralized logging and reporting and supports integration of VMware vShield with third-party solutions using the REST APIs.

VMware vShield Manager is deployed in a security virtual machine and is designed to install, configure, and manage all vShield products. The user interface offers configuration and data-viewing options for vShield Edge and vShield App. Tight integration with vCenter Manager allows users to display all underlying vSphere resource pools.
Choosing a Virtual Firewall

Cisco and VMware provide virtual firewall products that are suited for virtual machine–to–virtual machine and for virtual machine-to-outside traffic. Within each category, Cisco and VMware emphasize different roles for their products. VMware emphasizes integration, ease of use, and efficiency. Cisco emphasizes the forms of specialization that were developed to support the security principles of separation of duties and least privilege. Therefore, they designed the deployment and management model for their virtual firewalls to maintain the traditional operational model.

Choosing a firewall product is based on several factors, including:

- Management and administration
- Deployment models
- Feature requirements
- Licensing model

Management and Administration

The VMware vShield line of products aligns well with organizations rapidly adapting from traditional physical security models to new virtualization technologies and strategies and exploring new avenues of unified administration. These products also work well with brand new virtual data center deployments without any restrictions on existing physical/legacy security administration models. VMware firewalls provide an integrated approach by optimizing administration and enabling tighter integration with other VMware products used in virtual environments. The firewalls use a single management framework for securing virtual data centers and cloud environments at all levels.

Cisco firewalls are a good choice for organizations that place high importance on separation of duties and environments that have existing traditional firewall deployments. The Cisco firewalls offer an organizationally non-disruptive operation model with management tasks split into categories, and present a common operational model for supporting virtual and physical security deployments. This provides an administrative segregation between server, network, and security administrators, while preserving existing administrative structures with minimal impact on people or processes. The approach outlined in Scenario 1 is powerful and scalable, but differs from the traditional firewall "grid" management model.

A key manifestation of disruptive/non-disruptive strategies is how security rules are constructed. While the actual capabilities map closely to the products discussed here, the Cisco products tend to downplay the application of security controls as a consequence of business policy, in favor of more traditional, IP/networking-centric controls. VMware products portray a shift from legacy operation models, setting up a policy-driven access control by collapsing the traditional IT roles into a central point of administration.
Deployment Models

Deployment models for both VMware and Cisco firewalls require some level of integration with virtual distributed switches. VMware vShield Edge is compatible with port groups on the vNetwork Standard Switch, vNetwork Distributed Switch, and the Cisco Nexus 1000V switch. The Cisco virtual security solution is only designed for the Cisco Nexus 1000V distributed virtual switch. However, since Cisco Nexus 1000V is part of the standard configuration on some Vblock platforms, either solution offers compatibility with the Vblock platform.

Feature Requirements

Choice can also be scenario-driven and it depends on what features the firewall offers. The Virtual Firewall Scenarios section provides examples of the types of firewall that can be used, based on their intra- or inter-tenant capabilities, context-awareness, and other features.

Licensing Model

Another factor to consider when choosing a firewall is its licensing model. VMware vShield is tightly coupled with vSphere and licenses vShield firewalls by virtual machine (workload count). Cisco aligns their Virtual Security Gateway licenses with Cisco Nexus 1000V, effectively licensing per CPU socket. Note that licensing and related costs are significantly dependent on business needs such as workload count and density, policy structure, and other factors as discussed above.

Summary

Deployment designs can include a single virtual firewall or combinations of Cisco and VMware inter- and intra-tenant firewalls. Both Cisco and VMware provide great options for intra-tenant as well as inter-tenant and edge security. Implementation details, such as vPath and vNIC expectations and supported switches, and administration mechanics differ, but their effective capabilities align tightly, enabling each vendor to offer a well-rounded stable of virtual firewalls.
Virtual Firewall Scenarios

This section explores several common virtual firewall scenarios. The treatment of the individual scenarios is not meant to be exhaustive but rather to give you ideas. The scenarios include:

- Three-tiered application
- Virtual desktop
- Multi-tenancy
- Demilitarized zone (DMZ)

For the purposes of this paper, we have selected a particular firewall product for each scenario; however, firewalls from either Cisco or VMware can be used to demonstrate any of the scenarios below. The discussion addresses the roles of virtual firewalls in the primary scenario, but note that real-world deployments are likely to benefit from both zone and edge firewalls.

Scenario 1: Three-Tiered Application

We used the Cisco Virtual Security Gateway to demonstrate securing the deployment of a three-tiered application. Cisco Virtual Security Gateway provides the standard 5-tuple network attributes that can be used in the security policies. Below is a sample security policy for a multi-tier content hosting application deployment:

- Permit only port 80 (HTTP) for virtual machines in the web zone.
- Permit port 22 (SSH) for virtual machines that belong to the database zone.
- Allow communication only between web servers and database servers.
- Allow communication only between application servers and database servers.
- Explicitly deny all traffic to the zones.

**Note:** This example works for a single or multi-tenant environment.

Tasks are split into three sections—security, network, and server administrators.
Tasks for Security Administrators

The security administrator performs the following tasks on the Cisco Virtual Network Management Center to create a policy using the conditions based upon network attributes. These tasks create a policy for the same three-tier scenario.

1. Define tenants by logging in to Cisco Virtual Network Management Center and choosing the Tenant Management section. Right-click the root and select **Create Tenant**, as shown in the following screenshot:

![Creating a tenant](image)

2. Define zones by going to the Policy Management section to define the security policy. Select **Policy Management > Security Policies > Firewall Policy > Tenant A > Zones**. Here security administrators can add three zones (WebZone, AppZone, and DBZone). After defining the zone, choose the **Conditions** tabs to classify the zone. For this case, we are using network attributes to classify the zones. In addition to network attributes, Cisco Virtual Security Gateway also supports policies based on virtual machine attributes such as the virtual machine name, cluster name, port profiles, and guest operating system. Policies can also be defined based on user-defined custom attributes.

3. Use the predefined zones to define the security policy. Select **Policy Management > Security Policies > Firewall Policy > Tenant A > Policies**. Add a new policy.

4. Implement the specifications outlined above by adding rules to the policy, as shown in the following screenshot:
Adding rules to the policy

5. Define a policy set and add the policy to the set. This provides the flexibility to add new policies in the future without changing existing policy.

6. Bind the policy set to the security profile by building a security profile and assigning the policy set to it.

7. In order to push policies to a Virtual Security Gateway, assign the Virtual Security Gateway to a tenant. Once assigned, all the policies—security profiles—are pushed to that Virtual Security Gateway.

8. Log in to Cisco Virtual Security Gateway CLI and verify the policy being pushed successfully by Cisco Virtual Network Management Center, as shown in the following screenshot:

Verifying the security policy using Cisco Virtual Security Gateway CLI
Tasks for Network Administrators

Next, the network administrator creates a port profile and can bind the security policy to this port profile. Since the definition of the security policy does not require a separate port profile, a single port profile can be used for all the virtual machines. The following screenshot shows this binding:

![Binding a security profile to the port profile](image)

Tasks for Server Administrators

The server administrator needs to open the network settings of the virtual machine and select the port profile that the network administrator created with the security profile. The network profile and the security profiles are dynamically instantiated when the virtual machine associates this network port profile. The following screenshot shows selecting a firewall-enabled port group for the virtual machine:

![Selecting a firewall-enabled port group for the virtual machine](image)

This three-tiered access control can also be achieved using virtual machine attributes such as the virtual machine name, cluster name, port-profiles, guest operating system, and so forth. Cisco Virtual Security Gateway also supports custom attributes-based policies.
Scenario 2: Virtual Desktops

This scenario involves imposing better network security controls on an existing environment. The scenario attempts to provide added security against internal and external threats, and better satisfy compliance requirements. The specific technical requirements include:

- Impose finer-grain controls on virtual desktop networking. This allows extending virtual desktops beyond task workers working in tightly locked-down environments to knowledge workers who require greater flexibility.
- Create network zones of trust while maintaining the existing network configuration, such as topology and LAN segments.
- Impose data center–wide policies that are absolute, while allowing individual zones or clusters to have additional independent policies.
- Create optional data center–wide network policies so that security best practices are implemented but can be overridden as needed for specific business purposes.
- Monitor and audit network traffic, particularly for virtual desktops.

In this case, virtual desktops and business applications are already running and located on the internal corporate network. The existing networking setup should be maintained, with security controls layered on to meet business needs and technical objectives. VMware vShield App is used to demonstrate this solution.

VMware vShield App configuration includes the following three tasks:

- Create logical groupings.
- Create data center policies.
- Create virtual desktop policies.

Creating Logical Groupings

Provide logical groupings by creating custom security groups. You can do this by creating vSphere containers for the logical groupings. This example uses resource pools to group virtual desktops and business services, as well as vApps, to contain all virtual machines belonging to the same application. The following screenshot shows the resource pools and vApps in use.

[Image: Nested resource pools]
Creating Data Center–Wide Policies

VMware vShield App allows for the creation of high- and low-precedence data center policies. Based on the specifications outlined above, the following high-precedence policies need to be created:

- Web browsing to public Internet by all desktops is permitted.
- All other traffic to public Internet from desktops is denied.

These rules are written in terms of the virtual desktop infrastructure (VDI) resource pool, which means they apply to every virtual desktop that is created.

In addition, create a low-precedence rule to block NetBIOS traffic from any virtual machine to any other virtual machine. This rule provides a method to implement a security best practice but can be overridden for specific virtual machines or groups at a later time.

Finally, set default rules to deny-all.

Virtual Desktop Policies

Nested resource pools are used to provide greater control over virtual desktops. Inside the top-level VDI pool, there is a resource pool for knowledge workers and another for task workers. Resource pools are used to control server resource utilization; for example, using requiring use of shares or setting limits on CPU and memory usage. Resource pools are purposed to provide finer-grained control on network policies.

Create the following rules at the cluster level:

- DNS access from the VDI resource pools to a physical DNS server located at a specific IP address is allowed.
- Active Directory access from the VDI resource pool to a virtual Active Directory vApp is allowed.
- All attempts by any desktop to directly communicate with any other desktop are denied and logged.
- Desktops in the knowledge worker resource pool are allowed to communicate with the virtual SharePoint vApp; this is not permitted for the task worker resource pools.
The following screenshot shows the entire set of VMware vShield App rules for the above example:

<table>
<thead>
<tr>
<th>Summary</th>
<th>Rules</th>
<th>Security Groups</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source (A.B.C.D/m)</td>
<td>Source Port</td>
<td>Destination (A.B.C.D/m)</td>
<td>Destination Port</td>
</tr>
<tr>
<td>VDI</td>
<td>ANY</td>
<td>Outside Data Center 01</td>
<td>HTTP</td>
</tr>
<tr>
<td>VDI</td>
<td>ANY</td>
<td>Outside Data Center 01</td>
<td>-</td>
</tr>
<tr>
<td>VDI</td>
<td>ANY</td>
<td>Outside Data Center 01</td>
<td>-</td>
</tr>
</tbody>
</table>

Cluster Level Rules

| Source (A.B.C.D/m) | Source Port | Destination (A.B.C.D/m) | Destination Port |
| VDI | ANY | VDI: 192.168.129.32 | DNS | 53 | UDP | ALLOW |
| VDI | ActiveDirectory | Kerberos | 88 | TCP | ALLOW |
| VDI | ActiveDirectory | LDAP | 389 | TCP | ALLOW |
| VDI | ActiveDirectory | MS-DNS | 135 | TCP | ALLOW |

Knowledge Worker: ANY | Sharepoint | HTTP | 80 | TCP | ALLOW |

Data Center Low Precedence Rules

| Source (A.B.C.D/m) | Source Port | Destination (A.B.C.D/m) | Destination Port |
| ANY | DHCP-Server | ANY | DHCP-Server | 67 | UDP | ALLOW |
| ANY | DHCP-Client | ANY | DHCP-Client | 68 | UDP | ALLOW |

VMware vShield App rules for virtual desktops

In this way a layer of security is added on top of an existing VDI network, and different kinds of policies are applied to meet technical and business goals.

Scenario 3: Multi-Tenancy

You can use a combination of the firewalls discussed in this paper to manage security policies in multi-tenant environments. Use firewalls such as VMware vShield Zones, VMware vShield App, and Cisco Virtual Security Gateway individually to achieve intra-tenant security virtual machine-to-virtual machine traffic control or use them with edge firewalls such as VMware vShield Edge or Cisco ASA 1000V to enable inter-tenant access control.

Use the management solutions for these firewalls such as the VMware vShield Manager for VMware firewalls or Cisco Virtual Network Management Center to set up security policies in a dense multi-tenant environment so that administrators can rapidly add and delete tenants and update tenant-specific configurations and security policies. Figure 3 displays a multi-tenant environment that uses the various virtual firewalls discussed in this paper.
Figure 3. Multi-tenant deployment on Vblock platform

In the architecture shown, Tenant A has its own Virtual Security Gateway and vShield Zone, vShield App, or both—acting as firewalls to provide security policies for its virtual machines. Tenant B has its own separate set of firewalls to manage security policies for its virtual machines.
The following is a set of requirements in a multi-tenant deployment that hosts potentially up to thousands of tenants in a shared infrastructure:

- Traffic isolation between the tenants
- Complete protection and confidentiality of tenant applications and data
- Integration with enterprise directory services (for example, Active Directory)
- Compliance with various audit requirements

Using a combination of the virtual firewalls discussed in the previous sections, a solution can be implemented to help achieve the following:

- Full confidentiality and protection of tenant applications and data with built-in firewall and VPN
- Enterprise directory services for security policies
- Compliance by logging all traffic information on a per-tenant basis
- Lower cost of security by eliminating purpose-built appliances and by increasing utilization and virtual machine density

For additional information on multi-tenancy solution for Vblock platforms, refer to the Vblock Solution for Trusted Multi-tenancy Design Guide. This paper provides detailed information about the foundational elements of multi-tenancy, including secure separation, service assurance, security and compliance, availability and data protection, tenant management and control, and service provider management and control. It also demonstrates processes for designing and managing Vblock platforms to deliver infrastructure and service multi-tenancy.

Scenario 4: Demilitarized Zone

This scenario requires meeting a list of requirements for a DMZ used for hosting a range of functions, including a public-facing Web application and some collaboration applications that need to be accessed by trusted third parties such as external partners and remote office sites. Traditionally, these resources might reside in several different networks arranged behind a range of firewalls. For this scenario, a VMware vShield deployment solution satisfies these requirements. VMware vShield App and VMware vShield Edge are used to build the DMZ.

The hypothetical DMZ needs to provide the following:

- Web access for DMZ Web servers, so they can download patches
- Remote SSH into the Web servers, for remote maintenance
- ICMP ping traffic permitted to the Web servers to allow third-party uptime monitoring
- Automatic IP address assignment within the DMZ, including fixed IPs for specific virtual machines like the Web servers
- Network load balancing for the Web servers
- Multiple VPN tunnels for secure connection by outside partners as well as remote offices
- Firewall rules to lock down traffic to and from the DMZ and minimize inter-virtual machine traffic within it
Various tasks must be performed in order to achieve the following:

- IP address management
- NAT and load balancing
- VPN configuration
- Firewall policy creation

### IP Address Management

Use the DHCP feature of VMware vShield Edge to automatically assign IP addresses. Static assignments are used for the Web servers as well as an associated database. All IP assignments are logged for audit purposes.

### NAT and Load Balancing

Use the Source NAT feature of VMware vShield Edge to allow systems in the DMZ with a router to connect to the outside network. PAT (port address translation) is used for all outgoing connections.

Use the VMware vShield Edge load balancer feature for users to browse the Web applications. The load balancer is configured to listen on the external interface address of the VMware vShield Edge for Web requests, and route them accordingly. Configure both Web servers to participate, using a round robin algorithm. Configure Destination NAT so that an ICMP ping to the VMware vShield Edge external IP address is forwarded to one of the Web servers, allowing uptime monitoring by a third-party.

### VPN Configuration

Configure a VPN tunnel for external partners to connect to collaboration services running in the DMZ. Configure a remote site, and then create a specific tunnel. The tunnel is encrypted using AES, and the remote site can use any IPSEC Site-to-Site VPN product on their side. Use the VMware vShield Edge external IP address to create the tunnel, avoiding the use of any additional IP addresses on the corporate network.
Firewall Rules

Configure firewall rules in two separate places:

- VMware vShield Edge provides perimeter security for traffic going in and out of the DMZ by monitoring it at the vShield Edge internal interface.
- VMware vShield App restricts traffic within the DMZ, both destined to and originating from individual virtual machines.

At the VMware vShield Edge internal interface, the default policy is to deny all traffic. Based on the outlined requirements, add permit rules to allow Web servers to contact the outside network to download patches and to allow all remote sites to connect to the Web servers via SSH for remote maintenance. The firewall rules are applied after the incoming traffic is translated by the destination NAT mappings. The following screenshot shows the VMware vShield Edge firewall rules configuration.

**Firewall rules on VMware vShield Edge**

In order to control traffic within the DMZ, use VMware vShield App with the security groups feature. Define security groups for the Web servers and the associated database, and assign membership by virtual machine vNIC.

Use these groups to create VMware vShield App firewall rules. The point of policy definition is the DMZ Port Group, and this is the context in the vSphere client UI where the rules are created.

Using the features of both VMware vShield App and VMware vShield Edge, the DMZ requirements for this scenario are met without purchasing numerous hardware devices like firewalls, VPN terminators, and load balancers.
Conclusion

Security solutions based on a static physical model are not sufficient to meet the needs of dynamic virtual data centers. Traditional physical firewalls

- Have fixed capacity levels and corresponding cost inefficiencies since they are usually oversized to accommodate peak usage levels.
- Face challenges with workloads that migrate between physical locations or that are dynamically scaled.
- Require artificial network constructs (VLANs and locality-driven topologies) that can be complicated to maintain, and are chokepoints in the network that generally see some, but not all, of the network traffic.
- Are expensive and inflexible, and require clumsy, expensive, infrastructure but still deliver incomplete network control.

Virtual firewall products, such as those from Cisco and VMware, can mirror the functionality of traditional firewalls while enabling simplified administration and preserving secure administrative practices. Virtual firewalls also make it simpler to monitor and control traffic between any two systems, even systems in the same zone of trust that would not have had a firewall between them in a traditional deployment.

VCE can provide industry-leading virtual firewalls solutions on Vblock platforms by leveraging Cisco and VMware for enterprise customers and service providers.

Next Steps

To learn more about VCE and Vblock platforms, contact a VCE representative or visit www.vce.com.
References

Refer to the following for more information about virtual firewalls running on Vblock platforms:

- Vblock Solution for Trusted Multi-Tenancy: Design Guide
- Cloud Service Assurance: Cisco Virtual Security Gateway (VSG) and Cisco Virtual Wide Area Application Services (VWAAS) on Vblock Infrastructure Platforms

Obtain additional information on VMware firewall products using the following links:


Obtain additional information on Cisco firewall products using the following links:

- http://www.cisco.com/go/vsg
- http://www.cisco.com/go/asa1000v
ABOUT VCE
VCE, the Virtual Computing Environment Company formed by Cisco and EMC with investments from VMware and Intel, accelerates the adoption of converged infrastructure and cloud-based computing models that dramatically reduce the cost of IT while improving time to market for our customers. VCE, through the Vblock platform, delivers the industry's first completely integrated IT offering with end-to-end vendor accountability. VCE's prepackaged solutions are available through an extensive partner network, and cover horizontal applications, vertical industry offerings, and application development environments, allowing customers to focus on business innovation instead of integrating, validating and managing IT infrastructure.
For more information, go to www.vce.com.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." VCE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.