This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
# Contents

About This Book 7

1 Overview of VMware vShield 9
   vShield Components 9
   vShield Manager 9
   vShield App 9
   vShield Edge 10
   vShield Endpoint 10

Ports Required for vShield 10

An Introduction to REST API for vShield Users 10
   How REST Works 10
   Using the vShield REST API 11
   RESTful Workflow Patterns 11
   For More Information About REST 12

2 vShield Manager Management 13
   Synchronize the vShield Manager with vCenter Server and DNS 13
   Retrieving Tech Support Logs 14
      Get the vShield Manager Technical Support Log File Path 14
      Get the vShield Edge Technical Support Log File Path 14

3 ESX Host Preparation for vShield App, Endpoint, and Isolation 15
   Install the Licenses for vShield Edge, vShield App, and vShield Endpoint 15
   Install vShield App, vShield Endpoint, and Port Group Isolation Services on an ESX Host 15
   Get the Installation Status of vShield Services on an ESX Host 17
   Uninstalling vShield Services from an ESX Host 18

4 vNetwork Preparation and vShield Edge Installation 19
   Enabling Port Group Isolation 19
      Enable Port Group Isolation on a vDS 20
      Get the Port Group Isolation Debug Statistics from an ESX Host 20
      Disable Port Group Isolation on a vDS 20
   Installing a vShield Edge 21
      Get the Install Parameters of a vShield Edge 22
      Uninstall a vShield Edge 22

5 vShield Edge Management 23
   Upgrading a vShield Edge 24
   Force a vShield Edge to Synchronize with the vShield Manager 24
   Manage CLI Credentials on a vShield Edge 25
   Managing DHCP 25
      Get the DHCP Server Status 25
      Start, Stop, or Restart the DHCP Service 25
      Post a DHCP Configuration 26
      Get the Configuration for All DHCP Hosts and Pools 26
      Get Timestamps of Last 10 DHCP Configurations 27
      Get a DHCP Configuration by Timestamp 27
Revert to a DHCP Configuration by Timestamp 27
Delete the DHCP Configuration on a vShield Edge 27
Managing NAT 28
Managing SNAT Rules 28
Managing DNAT Rules 30
Configuring the vShield Edge Firewall 33
Get the Firewall Rule Set for a vShield Edge 33
Post a Firewall Rule Set 34
Get the Status of the Default Policy for a vShield Edge 35
Change the Default Firewall Policy Action 35
Get Details of a Specific Firewall Rule 36
Get Timestamps of Last 10 Firewall Rule Sets for a vShield Edge 36
Get Firewall Rule Set by Timestamp 36
Revert to a Firewall Rule Set by Timestamp 36
Delete All Firewall Rules on a vShield Edge 36
Configuring VPNs 37
Get the Status of VPN Service 38
Start or Stop the VPN Service on a vShield Edge 38
Configure VPN Parameters on a vShield Edge 38
Add a Remote Site 39
Add Tunnels for a VPN Site 40
Get the Detailed IPSec Configurations for a Network 40
Get the Detailed Configuration for a VPN Site 41
Get the Detailed Tunnel Configuration 41
Delete a Tunnel for a VPN Site 41
Delete a Remote Site 41
Get the Current VPN Configuration on a vShield Edge 41
Get Timestamps of Last 10 VPN Configurations 42
Get a VPN Configuration by Timestamp 42
Revert to a VPN Configuration by Timestamp 42
Delete the VPN Configuration on a vShield Edge 42
Load Balancer 43
Get the Status of Load Balancer Service on a vShield Edge 43
Start or Stop the Load Balancer Service on a vShield Edge 44
Add a Listener for Load Balancing Service 44
Get the Current Load Balancer Configuration on a vShield Edge 45
Get the Configuration of a Specific Load Balancing Server 45
Get Timestamps of Last 10 Load Balancer Configurations 45
Get a Load Balancer Configuration by Timestamp 46
Revert to a Load Balancer Configuration by Timestamp 46
Delete the Load Balancer Configuration on a vShield Edge 46
Managing the MTU Threshold for a vShield Edge 46
View Traffic Statistics 47
Debug vShield Edge Services Using Service Statistics 47
Managing the Connection to a Syslog Server 48
Post a Syslog Server Configuration 48
Get the Current Syslog Server Configuration 48
Get Timestamps of Last 10 Syslog Server Configurations 48
Get a Syslog Server Configuration by Timestamp 49
Revert to a Syslog Server Configuration by Timestamp 49
Delete the Current Syslog Server Configuration 49

6 vShield App Management 51
Configuring Firewall Rules for a vCenter Container 51
View All Firewall Rules for a Container 51
Post an App Firewall Rule Set for a Container 52
View a List of Timestamps Identifying App Firewall Rule Set Changes 55
View a Previous Firewall Rule Set by Timestamp 55
Revert to a Previous Firewall Rule Set 55
Delete All Firewall Rules under a Container 55
Managing Security Groups 56
Add a Security Group 56
Add a Virtual Machine to a Security Group 57
Get the List of All Security Groups under a Base Node 57
Get the Details for a Single Security Group under a Base Node 58
Get IP Addresses for the Virtual Machines in a Security Group 58
Get the Properties from a Virtual Machine 58
Delete a Virtual Machine from a Security Group 58
Delete a Single Security Group 59
Delete All Security Groups under a Base Node 59
Configuring Syslog Service for a vShield App 59

7 vShield Endpoint Management 61
Register an SVM with the vShield Endpoint Service on an ESX Host 61
Retrieve SVM-Specific Network Information 62
Retrieve vShield Endpoint Service Status on an ESX Host 63
Uninstalling the vShield Endpoint Service from an ESX Host 63
Unregister an SVM from vShield Endpoint 63
Uninstall vShield Endpoint from the vShield Manager 64
Error Schema 64

Appendix 65
vShield Manager Schemas 65
vShield Manager to vCenter Server Synchronization Schema 65
DNS Service Schema 66
Virtual Machine Information Schema 66
Security Groups Schema 67
ESX Host Preparation and Uninstallation Schema 68
vShield App Schemas 69
vShield App Configuration Schema 69
vShield App Firewall Schema 69
Port Group Isolation Management Schema 71
Port Group Isolation Statistics Schema 71
vShield Edge Schemas 71
Base vShield Edge Configuration Schema 72
vShield Edge Installation and Upgrade Schema 72
vShield Edge Global Configuration Schema 73
vShield Edge CLI Login Credentials Schema 74
vShield Edge Firewall Schema 74
NAT Schema 77
DHCP Schema 79
VPN Schema 80
Load Balancer Schema 83
MTU Threshold Schema 84
Traffic Stats Schema 85
Syslog Schema 85
Error Message Schema 86

Index 87
About This Book

This manual, the vShield API Programming Guide, describes how to install, configure, monitor, and maintain the VMware® vShield™ system by using REST API requests. The information includes step-by-step configuration instructions and examples.

Intended Audience

This manual is intended for anyone who wants to use REST API to install or use vShield in a VMware vCenter™ environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with vShield.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to http://www.vmware.com/support/pubs.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

vShield Documentation

The following documents comprise the vShield documentation set:

- vShield Administration Guide
- vShield Quick Start Guide
- vShield API Programming Guide, this guide

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.
Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.
Overview of VMware vShield

VMware® vShield™ is a suite of network edge and application-aware firewalls built for VMware vCenter™ Server integration. vShield inspects client-server communications and inter-virtual-machine communication to provide detailed traffic analytics and application-aware firewall protection. vShield is a critical security component for protecting virtualized datacenters from attacks and misuse helping you achieve your compliance-mandated goals.

This guide assumes you have administrator access to the entire vShield system. If you are unable to access a screen or perform a particular task, consult your vShield administrator.

This chapter includes the following topics:

- “vShield Components” on page 9
- “Ports Required for vShield” on page 10
- “An Introduction to REST API for vShield Users” on page 10

vShield Components

vShield includes components and services essential for protecting virtual machines. vShield can be configured through a web-based user interface, a command line interface (CLI), and REST API.

To run vShield, you need one vShield Manager virtual machine and at least one vShield Zones, vShield App, or vShield Edge virtual machine.

vShield Manager

The vShield Manager is the centralized management component of vShield and is installed from OVA as a virtual machine by using the vSphere Client. Using the vShield Manager user interface or vSphere Client plug-in, administrators can install, configure, and maintain vShield components.

The vShield Manager virtual machine can run on a different ESX host from your vShield App and vShield Edge virtual machines.

The vShield Manager user interface leverages the VMware Infrastructure SDK to display a copy of the vSphere Client inventory panel.

For more on the using the vShield Manager user interface, see the vShield Administration Guide.

vShield App

A vShield App monitors all traffic into and out of an ESX host, and between virtual machines on the host. vShield App provides application-aware traffic analysis and stateful firewall protection. vShield App regulates traffic based on a set of rules, similar to an access control list (ACL).
As traffic passes through a vShield App, each session header is inspected to catalog the data. The vShield App creates a profile for each virtual machine detailing the operating system, applications, and ports used in network communication. Based on this information, the vShield App allows ephemeral port usage by permitting dynamic protocols such as FTP and RPC to pass through, while maintaining lockdown on ports 1024 and higher.

You cannot protect the Service Console or VMkernel with a vShield App because these components are not virtual machines.

**vShield Edge**

A vShield Edge provides network edge security to protect the virtual machines in a vCloud tenant's network from attacks originating from the public network. The vShield Edge connects the isolated, private networks of cloud tenants to the public side of the service provider network through common edge services such as DHCP, VPN, NAT, and load balancing.

You install a vShield Edge from the vShield Manager. You can install one vShield Edge instance per tenant port group on a vNetwork Distributed Switch (vDS).

You configure a vShield Edge by using REST API.

**vShield Endpoint**

vShield Endpoint delivers an introspection-based antivirus solution. vShield Endpoint uses the hypervisor to scan guest virtual machines from the outside without a bulky agent. vShield Endpoint is efficient in avoiding resource bottlenecks while optimizing memory use.

**Ports Required for vShield**

The vShield Manager requires ports 80/TCP and 443/TCP for REST API requests.

**An Introduction to REST API for vShield Users**

REST, an acronym for Representational State Transfer, is a term that has been widely employed to describe an architectural style characteristic of programs that rely on the inherent properties of hypermedia to create and modify the state of an object that is accessible at a URL.

**How REST Works**

Once a URL of such an object is known to a client, the client can use an HTTP GET request to discover the properties of the object. These properties are typically communicated in a structured document with an HTTP Content-Type of XML or JSON, that provides a representation of the state of the object. In a RESTful workflow, documents (representations of object state) are passed back and forth (transferred) between a client and a service with the explicit assumption that neither party need know anything about an entity other than what is presented in a single request or response. The URLs at which these documents are available are often “sticky,” in that they persist beyond the lifetime of the request or response that includes them. The other content of the documents is nominally valid until the expiration date noted in the HTTP Expires header.
Using the vShield REST API

**IMPORTANT** All vShield REST requests require authorization. You can use the following basic authorization:

```
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```

YWRtaW46ZGVmYXVsdA== represents the Base 64 encoding of the vShield Manager default login credentials (admin:default).

REST API uses HTTP requests (which are often executed by a script or other higher-level language) as a way of making what are essentially idempotent remote procedure calls that create, modify, or delete the objects defined by the API. This REST API (and others) is defined by a collection of XML documents that represent the objects on which the API operates. The operations themselves (HTTP requests) are generic to all HTTP clients.

To write a RESTful client, you need to understand only the HTTP protocol and the semantics of standard HTML markup. To use the vShield API effectively in such a client, you need to know three things:

- the set of objects that the API supports, and what they represent (What is a vDC? How does it relate to an Org?)
- how the API represents these objects (What does the XML schema for the vShield Edge firewall rule set look like? What do the individual elements and attributes represent?)
- how the client refers to an object on which it wants to operate

To answer these questions, you need to understand the vShield API resource schemas. These schemas define a number of XML types, many of which are extended by other types. The XML elements defined in these schemas, along with their attributes and composition rules (minimum and maximum number of elements or attributes, for example, or the prescribed hierarchy with which elements can be nested) represent the data structures of vShield objects. A client can “read” an object by making an HTTP GET request to the object’s resource URL. A client can “write” (create or modify) an object with an HTTP PUT or POST request that includes a new or changed XML body document for the object. And a client can usually delete an object with an HTTP DELETE request.

In this document, we present example requests and responses, and also provide reference information on the XML schemas that define the request and response bodies.

**RESTful Workflow Patterns**

All RESTful workflows fall into a pattern that includes only two fundamental operations:

- Make an HTTP request (typically GET, PUT, POST, or DELETE). The target of this request is either a well-known URL (such as the vShield Manager) or a link obtained from the response to a previous request. (For example, a GET request to an Org URL returns links to vDC objects contained by the Org.)
- Examine the response, which can be an XML document or an HTTP response code. If the response is an XML document, it may contain links or other information about the state of an object. If the response is an HTTP response code, it indicates whether the request succeeded or failed, and may be accompanied by a URL that points to a location from which additional information can be retrieved.

These two operations can repeat, in this order, for as long as necessary.
For More Information About REST

For a comprehensive discussion of REST from both the client and server perspectives, see:


There are also many sources of information about REST on the Web, including:

- http://www.infoq.com/articles/rest-introduction
The vShield Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

**IMPORTANT** All vShield REST requests require authorization. You can use the following basic authorization:

```
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```

YWRtaW46ZGVmYXVsdA== represents the Base 64 encoding of the vShield Manager default login credentials (admin:default).

The chapter includes the following topics:

- “Synchronize the vShield Manager with vCenter Server and DNS” on page 13
- “Retrieving Tech Support Logs” on page 14

**Synchronize the vShield Manager with vCenter Server and DNS**

You can use a single request to synchronize the vShield Manager with the vCenter Server and add DNS servers to the vShield Manager for IP address and hostname resolution. Synchronizing with vCenter Server enables the vShield Manager user interface to display your VMware Infrastructure inventory.

Synchronization with vCenter requires the vCenter URL and login credentials.

For the schema, see “vShield Manager to vCenter Server Synchronization Schema” on page 65.

For the DNS schema, see “DNS Service Schema” on page 66.

**Example 2-1.** Synchronizing the vShield Manager with vCenter Server and Identify DNS Services

Request:

```
POST <vshield_manager-uri>/api/1.0/global/config
```

You can also synchronize the vShield Manager with the vCenter Server without specifying DNS.

**Example 2-2.** Synchronizing the vShield Manager with vCenter Server without DNS

Request:

```
POST <vshield_manager-uri>/api/1.0/global/vcInfo
```
Retrieving Tech Support Logs

You can retrieve Technical Support logs from the vShield Manager and vShield Edge.

Get the vShield Manager Technical Support Log File Path

You can get the path to the diagnostic log file for the vShield Manager. You can then send the diagnostic log to technical support for assistance in troubleshooting an issue.

**Example 2-3. Getting the Tech Support Log File Path for a vShield Manager**

Request:

GET <vshield_manager-uri>/api/1.0/global/techSupportLogs

Get the vShield Edge Technical Support Log File Path

You can download the diagnostic log from a vShield Edge. You can then send the diagnostic log to technical support for assistance in troubleshooting an issue.

**Example 2-4. Getting the Tech Support Log File Path for a vShield Edge**

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/techSupportLogs
You can extend the capabilities of vShield by adding the following services: vShield App, vShield Endpoint, and vShield Edge. You must prepare each ESX host in your environment for these services. The vShield Manager OVA file contains the drivers and files necessary to install all additional services.

**IMPORTANT** All vShield REST requests require authorization. You can use the following basic authorization:

```
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```

YWRtaW46ZGVmYXVsdA== represents the Base 64 encoding of the vShield Manager default login credentials (admin:default).

This chapter includes the following topics:

- “Install vShield App, vShield Endpoint, and Port Group Isolation Services on an ESX Host” on page 15
- “Get the Installation Status of vShield Services on an ESX Host” on page 17
- “Uninstalling vShield Services from an ESX Host” on page 18

**Install the Licenses for vShield Edge, vShield App, and vShield Endpoint**

You must install licenses for vShield Edge, vShield App, and vShield Endpoint before installing these components. You can install these licenses by using the vSphere Client.

1. From a vSphere Client host that is connected to a vCenter Server system, select **Home > Licensing**.
2. For the report view, select **Asset**.
3. Right-click a vShield asset and select **Change license key**.
4. Select **Assign a new license key** and click **Enter Key**.
5. Enter the license key, enter an optional label for the key, and click **OK**.
6. Click **OK**.
7. Repeat these steps for each vShield component for which you have a license.

**Install vShield App, vShield Endpoint, and Port Group Isolation Services on an ESX Host**

To shorten the time to deployment, you can install vShield App, vShield Endpoint, and Port Group Isolation services on an ESX host by using a single REST call. You can do this by including `VszInstallParams`, `PortgroupIsolationInstallParams`, and `EpsecInstallParams` in the POST body.
Port Group Isolation is a service used by a vShield Edge to isolate the virtual machines in a vDS port group from the external network. When Port Group Isolation is enabled, traffic is not allowed access to the virtual machines in the protected port group unless NAT rules or VLAN tags are configured.

NOTE Port Group Isolation is an optional feature that is not required for vShield Edge operation. Port Group Isolation is available for vDS-based vShield Edge installations only.

You must specify the host ID of the target ESX host to install all services.

See “ESX Host Preparation and Uninstallation Schema” on page 68.

Example 3-1. Installing a vShield App, vShield Endpoint, and Port Group Isolation on an ESX Host

Request:

POST <vshield_manager-uri>/api/1.0/vshield/<host-id>

Example:

POST /api/1.0/vshield/host-5450 HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 489

<VshieldConfiguration><VszInstallParams><DatastoreId>datastore-5035</DatastoreId><ManagementPortSwitchId>network-4485</ManagementPortSwitchId><MgmtInterface><IpAddress>10.112.196.245</IpAddress><NetworkMask>255.255.252.0</NetworkMask><DefaultGw>10.112.199.253</DefaultGw></MgmtInterface></VszInstallParams><PortgroupIsolationInstallParams><DatastoreId>datastore-5035</DatastoreId></PortgroupIsolationInstallParams><EpsecInstallParams>true</EpsecInstallParams><InstallAction>install</InstallAction></VshieldConfiguration>

ESX host preparation requires the following elements:

- **DatastoreId**: VC MOID of the datastore on which the vShield App and Port Group Isolation service virtual machine files will be stored.
- **ManagementPortSwitchId**: VC MOID of the port group that will host the management port of the vShield App.
- **MgmtInterface**
  - **IpAddress**: IP address to be assigned to the management port of the vShield App. This IP address must be able to communicate with the vShield Manager.
  - **NetworkMask**: Subnet mask associated with the IP address assigned to the management interface of the vShield App.
  - **DefaultGw**: IP address of the default gateway.

CAUTION Do not install vShield Zones/App on the ESX host where vCenter Server is running.

NOTE Port Group Isolation is an optional feature that is not required for vShield Edge operation. Port Group Isolation is available for vDS-based vShield Edge installations only.
After installation of all components is complete, do the following:

- **vShield App**: At this point, vShield App installation is complete. Each vShield App inherits global firewall rules set in the vShield Manager. The default firewall rule set allows all traffic to pass. You must configure blocking rules to explicitly block traffic. To configure App Firewall rules, see “Configuring Firewall Rules for a vCenter Container” on page 51.

- **Port Group Isolation**: You must enable the Port Group Isolation feature on each vDS. After enablement is complete, install a vShield Edge on each port group. See “vNetwork Preparation and vShield Edge Installation” on page 19.

- **vShield Endpoint**: To complete installation, see “vShield Endpoint Management” on page 61.

You can install a single service by identifying only that service in the POST body. In Example 3-2, only vShield App is installed, as identified by inclusion of the VszInstallParams element only.

**CAUTION** Do not install vShield Zones/App on the ESX host where vCenter Server is running.

### Example 3-2. Installing a vShield App Only

**Request:**

POST `<vshield_manager-uri>/api/1.0/vshield/<host-id>/vsz`

**Example:**

POST `/api/1.0/vshield/host-5126 HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 368

<VshieldConfiguration><VszInstallParams><DatastoreId>datastore-5131</DatastoreId><ManagementPortSwitchId>network-5134</ManagementPortSwitchId><MgmtInterface><IpAddress>10.112.196.245</IpAddress><NetworkMask>255.255.252.0</NetworkMask><DefaultGw>10.112.199.253</DefaultGw></MgmtInterface></VszInstallParams><InstallAction>install</InstallAction></VshieldConfiguration>

### Get the Installation Status of vShield Services on an ESX Host

You can retrieve the installation or uninstallation status of vShield services on an ESX host to track progress as complete or not initiated. If neither of these operations is in progress, the response includes the list of installed services on the ESX host.

### Example 3-3. Getting vShield Service Installation Status on an ESX Host

**Request:**

GET `<vshield_manager-uri>/api/1.0/vshield/<host-id>`
Uninstalling vShield Services from an ESX Host

You can uninstall vShield App, vShield Endpoint, and Port Group Isolation from an ESX host by using a single request.

Before uninstalling these services, complete the following tasks:

- **vShield Endpoint:** You must unregister SVMs before uninstalling vShield Endpoint from the ESX host. See “Unregister an SVM from vShield Endpoint” on page 63.
- **Port Group Isolation:** You must disable Port Group Isolation before uninstalling the service. See “Disable Port Group Isolation on a vDS” on page 20.

**CAUTION** Uninstalling any of these vShield services places the ESX host in maintenance mode. After uninstallation is complete, the ESX host reboots. If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue. If the vShield Manager is on the same ESX host, the vShield Manager must be migrated prior to uninstalling the vShield App.

Before uninstalling Port Group Isolation, disable the service on the host vDS. See “Disable Port Group Isolation on a vDS” on page 20.

**Example 3-4. Uninstalling All Three vShield Services from an ESX Host**

Request:

DELETE <vshield_manager-uri>/api/1.0/vshield/<host-id>

To uninstall two services at the same time, separate the services to be uninstalled with hyphens.

**Example 3-5. Uninstalling More than One Service**

Request:

DELETE <vshield_manager-uri>/api/1.0/vshield/<host-id>/<hyphen-separated-service-names>

Example:

This request uninstalls a vShield App (zones) and Port Group Isolation (pgi). The vShield Endpoint service is shortened to epsec.

DELETE /api/1.0/zones/vshield/<host-id>/vsz-pgi

You can uninstall a single service by specifying the service name.

**Example 3-6. Uninstall a vShield App Only**

Request:

DELETE <vshield_manager-uri>/api/1.0/vshield/<host-id>/vsz
After ESX host preparation is complete, you can secure internal networks by installing a vShield Edge. If you are installing vShield Edge instances on vDS port groups, you can isolate those port groups by enabling Port Group Isolation on each vDS.

**IMPORTANT** If you intend to use the Port Group Isolation feature, you should install Port Group Isolation on all ESX hosts in your vCenter environment before you install any vShield Edge virtual machines. If you do not install Port Group Isolation and attempt to enable the feature during vShield Edge installation, Port Group Isolation does not work. See “Install vShield App, vShield Endpoint, and Port Group Isolation Services on an ESX Host” on page 15.

**IMPORTANT** All vShield REST requests require authorization. You can use the following basic authorization:

```
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```

YWRtaW46ZGVmYXVsdA== represents the Base 64 encoding of the vShield Manager default login credentials (admin:default).

This chapter includes the following topics:

- “Enabling Port Group Isolation” on page 19
- “Installing a vShield Edge” on page 21

### Enabling Port Group Isolation

Port Group Isolation creates a barrier between the virtual machines protected by a vShield Edge and the external network. When you enable Port Group Isolation and install a vShield Edge on a vDS port group, you isolate each secured vDS port group from the external network. When Port Group Isolation is enabled, traffic is not allowed access to the virtual machines in the secured port group unless NAT rules or VLAN tags are configured.

**NOTE** Port Group Isolation is an optional feature that is not required for vShield Edge operation. Port Group Isolation is available for vDS-based vShield Edge installations only.

**To enable Port Group Isolation on a vDS**

1. Enable Port Group Isolation on each vDS.
2. Install a vShield Edge on each vDS port group you plan to secure.
3. Move the virtual machines to secured vDS port groups.
Enable Port Group Isolation on a vDS

After Port Group Isolation is installed on each ESX host, you must enable Port Group Isolation on each vDS where you will install a vShield Edge.

Example 4-1. Enabling Port Group Isolation on a vDS

Request:

PUT <vshield_manager-uri>/api/1.0/network/portgroupIsolation/dvs/<dvs-Moid>

Example:

PUT /api/1.0/portgroupIsolation/dvs/dvs-1069 HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
Connection: keep-alive

Get the Port Group Isolation Debug Statistics from an ESX Host

You can retrieve the statistics on Port Group Isolation activity from an ESX host for debug purposes.

The query returns XML with the path of the location of the statistics file on the vShield Manager. This path can be used to download the file over HTTP.

See “Port Group Isolation Statistics Schema” on page 71.

Example 4-2. Getting the Port Group Isolation Debug Statistics from an ESX Host

Request:

GET <vshield_manager-uri>/api/1.0/network/portgroupIsolation/<host-Id>/statsLocation

Disable Port Group Isolation on a vDS

Before uninstalling Port Group Isolation, disable the service on the host vDS.

Example 4-3. Disabling Port Group Isolation on a vDS

Request:

DELETE <vshield_manager-uri>/api/1.0/network/portgroupIsolation/dvs/<dvs-Moid>

Example:

DELETE /api/1.0/portgroupIsolation/dvs/dvs-1069 HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
Connection: keep-alive
Installing a vShield Edge

You can install one vShield Edge per port group, vDS port group, or Cisco® Nexus 1000V. A vShield Edge requires an external port group with a physical NIC and an internal port group that contains the virtual machines to be secured. The vShield Edge sits inline between these port groups. If an internal port group does not exist, you must create this port group before installing a vShield Edge.

The vShield Edge installation API copies the vShield Edge OVF from the vShield Manager to the specified datastore and deploys a vShield Edge on the given port group. After the vShield Edge is installed, the virtual machine powers on and initializes according to the given network configuration.

Installing a vShield Edge instance adds a virtual machine to the vCenter Server inventory, which is mirrored in the vShield Manager user interface. You must name the vShield Edge instance and specify an IP address for the management interface.

For the schema, see “vShield Edge Installation and Upgrade Schema” on page 72.

Example 4-4. Installing a vShield Edge

Request:

POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vshieldedge

<VShieldEdgeConfig>
  <InstallParams>
    <operationMode>routing</operationMode>
    <resourcePoolId>resource_pool_id_from_MOB</resourcePoolId>
    <hostId:host_id_from_MOB>hostId</hostId>
    <dataStoreId>datastore_id_from_MOB</dataStoreId>
    <InternalInterface>
      <networkId>interface_id_of_internal_interface_from_MOB</networkId>
      <networkAddress>ip_address_of_internal_interface</networkAddress>
      <subnetMask>subnetmask_for_internal_interface</subnetMask>
    </InternalInterface>
    <ExternalInterface>
      <networkId>interface_id_of_external_interface_from_MOB</networkId>
      <networkAddress>ip_address_of_external_interface</networkAddress>
      <defaultGw>default_gateway_for_external_interface</defaultGw>
    </ExternalInterface>
  </InstallParams>
</VShieldEdgeConfig>

Rules:

The installation schema requires the following values:

- operationMode: Enter routing as the value.
- resourcePoolId: Enter the VC MOID of the resource pool.
- hostId: Enter the VC MOID of the ESX Host to which the vShield Edge is to be cloned.
- dataStoreId: Enter the VC MOID of the Datastore to which the vShield Edge is to be cloned.
- InternalInterface: Enter the VC MOID for the internal port group.
- ExternalInterface: Enter the VC MOID for the external port group.

Example:

POST /api/1.0/network/network-244/vshieldedge HTTP/1.1
Content-Type: application/xml
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
Accept: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
Content-Length: 620
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><VShieldEdgeConfig><InstallParams><operationMode>routing</operationMode><resourcePoolId>network-244</resourcePoolId><hostId>host-28</hostId><dataStoreId>datastore-29</dataStoreId><InternalInterface><networkId>network-43</networkId><networkAddress>172.16.1.8</networkAddress><subnetMask>255.255.255.0</subnetMask></InternalInterface><ExternalInterface><networkId>network-39</networkId><networkAddress>10.112.196.218</networkAddress><subnetMask>255.255.252.0</subnetMask><defaultGw>10.112.199.253</defaultGw></ExternalInterface></InstallParams></VShieldEdgeConfig>

Get the Install Parameters of a vShield Edge

Example 4-5. Getting the Install Parameters of a vShield Edge

Request:
GET <vshield_manager-uri>/network/<internal-portgroup-vc-moref-id>/vshieldedge

Example:
GET /api/1.0/network/network-244/vshieldedge HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.169:9998

Uninstall a vShield Edge

CAUTION If you have enabled Port Group Isolation, you must migrate or power off the virtual machines on the ESX host from which you want to uninstall a vShield Edge. Uninstalling Port Group Isolation places the ESX host in maintenance mode. After uninstallation is complete, the ESX host reboots. If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue. If the vShield Manager is on the same ESX host, the vShield Manager must be migrated prior to uninstalling Port Group Isolation.

If you did not install and enable Port Group Isolation on an ESX host, you do not have to migrate virtual machines to uninstall a vShield Edge.

Example 4-6. Uninstalling a vShield Edge

Request:
DELETE <vshield_manager-uri>/network/<internal-portgroup-vc-moref-id>/vshieldedge

Example:
DELETE /api/1.0/network/network-244/vshieldedge HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
You can manage vShield Edge services and firewall policies by using REST API. By using REST call, you can start or stop services, post and delete configurations, and get service status.

For each service, you can enable logging to view debug and audit messages. You must identify a syslog server to receive the logs.

**IMPORTANT** All vShield REST requests require authorization. You can use the following basic authorization:

```
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```

YWRtaW46ZGVmYXVsdA== represents the Base 64 encoding of the vShield Manager default login credentials (admin:default).

This chapter includes the following topics:

- “Upgrading a vShield Edge” on page 24
- “Force a vShield Edge to Synchronize with the vShield Manager” on page 24
- “Manage CLI Credentials on a vShield Edge” on page 25
- “Managing DHCP” on page 25
- “Managing NAT” on page 28
- “Configuring the vShield Edge Firewall” on page 33
- “Configuring VPNs” on page 37
- “Load Balancer” on page 43
- “Managing the MTU Threshold for a vShield Edge” on page 46
- “View Traffic Statistics” on page 47
- “Debug vShield Edge Services Using Service Statistics” on page 47
- “Managing the Connection to a Syslog Server” on page 48
Upgrading a vShield Edge

You can upgrade a vShield Edge via REST API when a new software version is available.

For the schema, see “vShield Edge Installation and Upgrade Schema” on page 72.

**Example 5-1. Upgrading vShield Edge Software**

Request:

PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vshieldedge/update

Example:

PUT /api/1.0/network/network-598/vshieldedge/update HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: localhost
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

You can get the status of a vShield Edge upgrade by checking the status of a vShield Edge.

**Example 5-2. Getting the Status of a vShield Edge Upgrade**

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vshieldedge

Example:

GET /api/1.0/network/network-600/vshieldedge HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: localhost
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

Force a vShield Edge to Synchronize with the vShield Manager

If the configuration of a vShield Edge is out of sync with what shows in the vShield Manager user interface, you can force the vShield Manager to push the latest configuration to a vShield Edge.

**Example 5-3. Forcing a vShield Edge to Sync with the vShield Manager**

Request:

PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/action/forcesync

Example:

PUT /api/1.0/network/network-244/action/forcesync HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost
Manage CLI Credentials on a vShield Edge

You can set and change login credentials for the CLI on a vShield Edge virtual appliance via REST.

You can change the default CLI login credentials (username `admin` and password `default`) on a vShield Edge via REST.

You can use lower-case letters, numbers, and underscores in the CLI username. The username must start with a letter and be between 1 and 33 characters in length. The password cannot have spaces and must be at least 1 character in length.

For the schema, see “vShield Edge CLI Login Credentials Schema” on page 74.

**Example 5-4. Managing CLI Credentials on a vShield Edge**

Request:

```plaintext
PUT <vshield_manager-uri>/api/1.0/network/<vdc-moref-id>/cli/credentials
```

Managing DHCP

vShield Edge provides DHCP service to bind assigned IP addresses to MAC addresses, preventing MAC spoofing attacks. All virtual machines protected by a vShield Edge can obtain IP addresses dynamically from the vShield Edge DHCP service.

vShield Edge supports IP address pooling and one-to-one static IP address allocation based on the vCenter managed object ID (vmid) and interface ID (interfaceId) of the requesting client.

vShield Edge DHCP service adheres to the following rules:

- Listens on the vShield Edge internal interface (InternalInterface) for DHCP discovery.
- Uses the IP address of the internal interface on the vShield Edge as the default gateway address for all clients, and the broadcast and subnetMask values of the internal interface for the container network.

All DHCP settings configured by using REST requests appear under the vShield Edge > DHCP tab for the appropriate vShield Edge in the vShield Manager user interface and vSphere Client plug-in.

For the DHCP schema, see “DHCP Schema” on page 79.

Get the DHCP Server Status

**Example 5-5. Getting the Status of the DHCP Service on a vShield Edge**

Request:

```plaintext
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/service
```

Example:

```plaintext
GET /api/1.0/network/network-244/dhcp/service HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213
```

Start, Stop, or Restart the DHCP Service

**Example 5-6. Starting or Stopping the DHCP Service on a vShield Edge**

Request:

```plaintext
PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/action/
{start | stop | restart}
```
Example:

```
PUT /api/1.0/network/network-244/dhcp/action/start HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213
```

### Post a DHCP Configuration

You can add hosts and IP pools for DHCP service on a vShield Edge. The vShield Edge can allocate IP addresses to protected virtual machines from configured IP pools.

The vShield Manager processes the posted XML file as a complete configuration for the specific vShield Edge. The current configuration is replaced with this new configuration.

If you do not specify a value for the `<leaseTime/>` parameter, the default value of one day is used. A value of infinite is supported.

#### Example 5-7. Adding IP Pool Ranges to a vShield Edge

Request:

```
POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/config
```

Rules:

- DHCPConfigParams and its elements are optional
- leaseTime can be infinite or number of seconds. If not specified, the default lease time is 1 day.
- Logging is disabled by default. To enable logging, add a `<log/>` element within `<DHCPConfig/>`.

Example:

```
POST /api/1.0/network/network-244/dhcp/config HTTP/1.1
content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213
accept: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
content-length: 655

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VShieldEdgeConfig>
    <DHCPConfig>
        <DHCPBinding>
            <vmId>vm-70</vmId>
            <interfaceId>1</interfaceId>
            <hostName>vmware</hostName>
            <internalIPAddress>172.16.1.54</internalIPAddress>
        </DHCPBinding>
        <DHCPPool>
            <PoolRange>
                <rangeStart>172.16.1.50</rangeStart>
                <rangeEnd>172.16.1.53</rangeEnd>
            </PoolRange>
            <DHCPPoolParams>
                <leaseTime>infinite</leaseTime>
            </DHCPPoolParams>
        </DHCPPool>
    </DHCPConfig>
</VShieldEdgeConfig>
```

### Get the Configuration for All DHCP Hosts and Pools

You can retrieve the current DHCP configuration for a vShield Edge, including all configured hosts and IP pools.

#### Example 5-8. Getting the Configuration of All DHCP Hosts and Pools

Request:

```
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/config
```
Example:

GET /api/1.0/network/network-244/dhcp/config HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213

**Get Timestamps of Last 10 DHCP Configurations**

You can get a list of the last 10 DHCP configurations by timestamp.

**Example 5-9. Getting Last 10 DHCP Configurations**

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/snapshots

**Get a DHCP Configuration by Timestamp**

You can view the details of a past DHCP configuration by specifying the timestamp of the snapshot.

**Example 5-10. Getting a DHCP Configuration by Snapshot Timestamp**

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/snapshot/<snapshot-timestamp>

**Revert to a DHCP Configuration by Timestamp**

You can revert to a previous DHCP configuration by specifying the timestamp of the snapshot. The current configuration is saved for future reference.

**Example 5-11. Revert to an DHCP Configuration by Timestamp**

Request:

PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/snapshot/<snapshot-timestamp>

**Delete the DHCP Configuration on a vShield Edge**

You can delete the current DHCP configuration a vShield Edge.

**Example 5-12. Delete the DHCP Configuration on a vShield Edge**

Request:

DELETE <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dhcp/config

Example:

DELETE /api/1.0/network/network-244/dhcp/config HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213
Managing NAT

The vShield Edge provides network address translation (NAT) service to protect the IP addresses of internal, private networks from the public network. You can configure NAT rules to provide access to services running on privately addressed virtual machines. The NAT service configuration is separated into SNAT (Secure Network Address Translation) and DNAT (Destination Network Address Translation) rules.

All SNAT and DNAT rules configured by using REST requests appear under the vShield Edge > NAT tab for the appropriate vShield Edge in the vShield Manager user interface and vSphere Client plug-in.

For the NAT schema, see “NAT Schema” on page 77.

Managing SNAT Rules

The vShield Edge uses SNAT to map internal addresses to allocated public addresses. If you use Port Group Isolation, you must configure SNAT rules to allow traffic from the internal network to the external network.

Get the SNAT Rule Set

**Example 5-13. Get the SNAT rule set on a vShield Edge**

Request:
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/snat/rules

Example:
GET /api/1.0/network/network-244/snat/rules HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost

Post an SNAT Rule Set

You can post an SNAT rule set for a vShield Edge via REST. The vShield Manager processes the posted XML file as a complete rule set for the specific vShield Edge. The current rule set is replaced with this new set of rules.

**Example 5-14. Post an SNAT Rule Set on a vShield Edge**

Request:
POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/snat/rules

```
<VShieldEdgeConfig>
  <NATConfig>
    <NATRule>
      <externalIpAddress>
        <ipAddress>IpOrAny</ipAddress>
      </externalIpAddress>
      <internalIpAddress>
        <ipAddress>IpOrAny</ipAddress>
      </internalIpAddress>
    </NATRule>
    <IpRange>
      <rangeStart>ip_address</rangeStart>
      <rangeEnd>ip_address</rangeEnd>
    </IpRange>
  </NATConfig>
</VShieldEdgeConfig>
```

or

```
<VShieldEdgeConfig>
  <NATConfig>
    <IpRange>
      <rangeStart>ip_address</rangeStart>
      <rangeEnd>ip_address</rangeEnd>
    </IpRange>
  </NATConfig>
</VShieldEdgeConfig>
```
Rules:

- You can add multiple SNAT rules by entering multiple `<NATRule>` sections in the body.

  ```xml
  <VShieldEdgeConfig>
    <NATConfig>
      <NATRule>
        <internalIpAddress><ipAddress>172.17.1.11</ipAddress></internalIpAddress>
        <externalIpAddress><ipAddress>10.112.196.94</ipAddress></externalIpAddress>
      </NATRule>
      <NATRule>
        <internalIpAddress><ipAddress>172.17.1.12</ipAddress></internalIpAddress>
        <externalIpAddress><ipAddress>10.112.196.94</ipAddress></externalIpAddress>
      </NATRule>
    </NATConfig>
  </VShieldEdgeConfig>
  ```

- Logging is disabled by default. To enable logging, add a `<log />` element within `<NATRule>`.

- The `externalIpAddress` and `internalIpAddress` parameters can be entered in either of these methods.

  ```xml
  <ipAddress>IpOrAny</ipAddress>
  or
  <IpRange>
    <rangeStart>low_ip_address</rangeStart>
    <rangeEnd>high_ip_address</rangeEnd>
  </IpRange>
  ```

- SNAT does not support port and protocol parameters.

Example:

- **Multiple SNAT Rules**
  ```
  POST /api/1.0/network/network-244/snat/rules HTTP/1.1
  content-type: application/xml; charset=UTF-8
  Authorization: Basic YWRtaW46ZGVmYXVsdA==
  Host: 10.112.196.213
  accept: text/html, image/gif, image/jpeg, */*; q=.2, */*; q=.2
  content-length: 310
  
  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <VShieldEdgeConfig>
    <NATConfig>
      <NATRule>
        <internalIpAddress><ipAddress>172.17.1.11</ipAddress></internalIpAddress>
        <externalIpAddress><ipAddress>10.112.196.218</ipAddress></externalIpAddress>
      </NATRule>
      <NATRule>
        <internalIpAddress><ipAddress>172.17.1.54</ipAddress></internalIpAddress>
        <externalIpAddress><ipAddress>10.112.196.217</ipAddress></externalIpAddress>
      </NATRule>
    </NATConfig>
  </VShieldEdgeConfig>
  ```

- **SNAT Rule with IP Range**
  ```xml
  <VShieldEdgeConfig>
    <NATConfig>
      <NATRule>
        <internalIpAddress><IpRange><rangeStart>172.17.1.40</rangeStart><rangeEnd>172.17.1.45</rangeEnd></IpRange>
        <externalIpAddress><IpRange><rangeStart>10.112.196.218</rangeStart><rangeEnd>10.112.196.219</rangeEnd></IpRange>
      </NATRule>
    </NATConfig>
  </VShieldEdgeConfig>
  ```
Get Timestamps of Last 10 SNAT Rule Configurations for a vShield Edge

Example 5-15. Get Last 10 SNAT Rule Set Snapshots

Request:
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/snat/snapshots

Get SNAT Configuration by Snapshot Timestamp

Example 5-16. Get SNAT Configuration by Snapshot Timestamp

Request
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/snat/snapshot/<snapshot-timestamp>

Revert to an SNAT Configuration by Snapshot Timestamp

Example 5-17. Revert to an SNAT Configuration by Snapshot Timestamp

Request:
PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/snat/snapshot/<snapshot-timestamp>

Delete All SNAT Rules on a vShield Edge

Example 5-18. Delete All SNAT Rules on a vShield Edge

Request:
DELETE <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/snat/rules

Example:
DELETE /api/1.0/network/network-244/snat/rules HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host:sdfsdf

Managing DNAT Rules

DNAT maps public addresses to internal addresses. If you use Port Group Isolation, you must configure
DNAT rules to allow traffic from the external network to the internal network.

The vShield Edge supports two forms of DNAT:

- Traffic targeting a public address is forwarded to an internal host with the given internal IP address.
- Traffic targeting a specific port of a public address is forwarded to an internal host with the given internal
  IP address on the specified port.

Get the DNAT Rule Set

Example 5-19. Get the DNAT Rule Set on a vShield Edge

Request:
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dnat/rules
Example:
GET /api/1.0/network/network-244/dnat/rules HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost

Post a DNAT Rule Set

You can post a DNAT rule set for a vShield Edge.

The vShield Manager processes the posted XML file as a complete rule set for the specific vShield Edge. The current rule set is replaced with this new set of rules.

Example 5-20. Post a DNAT Rule Set on a vShield Edge

Request:
POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/dnat/rules

<VShieldEdgeConfig>
<NATConfig>
<NATRule>
<protocol>tcp|udp|icmp|any</protocol>
<internalIpAddress>see_below</internalIpAddress>
<internalPort>see_below</internalPort>
<externalIpAddress>see_below</externalIpAddress>
<externalPort>see_below</externalPort>
</NATRule>
</NATConfig>
</VShieldEdgeConfig>

Rules:

- You can add multiple DNAT rules by entering multiple <NATRule></NATRule> sections in the body.
- For <protocol /> options tcp and udp, you must specify internalPort and externalPort elements. For options icmp and any, the internalPort and externalPort elements are not expected.
- You must add <icmpType /> if you configure icmp as the protocol.
- Logging is disabled by default. To enable logging, add a <log /> element within <NATRule />.
- The externalIpAddress and internalIpAddress parameters can be entered in either of these formats.
  <ipAddress>IpOrAny</ipAddress>
  or
  <IpRange>
  <rangeStart>low_ip_address</rangeStart>
  <rangeEnd>high_ip_address</rangeEnd>
  </IpRange>
- The externalPort and internalPort parameters can be entered in either of these formats.
  <port>PortOrAny</port>
  or
  <PortRange>
  <rangeStart>low_port</rangeStart>
  <rangeEnd>high_port</rangeEnd>
  </PortRange>
Example:

- Multiple DNAT Rules
  
  POST /api/1.0/network/network-244/dnat/rules HTTP/1.1
  content-type: application/xml; charset=UTF-8
  Authorization: Basic YWRtaW46ZGVmYXVsdA==
  Host: 10.112.196.213
  accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
  content-length: 617

  <?xml version="1.0" encoding="UTF-8"
  standalone="yes"?>
  <VShieldEdgeConfig>
    <NATConfig>
      <NATRule>
        <protocol>tcp</protocol><internalIpAddress><ipAddress>172.16.1.11</ipAddress>
        <internalPort><port>any</port></internalPort><externalIpAddress><ipAddress>10.112.196.217</ipAddress>
        <externalPort><port>any</port></externalPort>
      </NATRule>
      <NATRule>
        <protocol>icmp</protocol><icmpType>any</icmpType><internalIpAddress><ipAddress>172.16.1.11</ipAddress>
        <externalIpAddress><ipAddress>10.112.196.218</ipAddress>
      </NATRule>
    </NATConfig>
  </VShieldEdgeConfig>

- DNAT Rule with IP Range

  content-length: 453

  <?xml version="1.0" encoding="UTF-8"
  standalone="yes"?>
  <VShieldEdgeConfig>
    <NATConfig>
      <NATRule>
        <protocol>tcp</protocol><internalIpAddress><IpRange><rangeStart>172.17.1.10</rangeStart>
        <rangeEnd>172.17.1.15</rangeEnd></IpRange></internalIpAddress>
        <internalPort><port>any</port></internalPort><externalIpAddress><ipAddress>10.112.196.219</ipAddress>
        <externalPort><port>any</port></externalPort>
      </NATRule>
    </NATConfig>
  </VShieldEdgeConfig>

- DNAT Rule with Port Range

  content-length: 518

  <?xml version="1.0" encoding="UTF-8"
  standalone="yes"?>
  <VShieldEdgeConfig>
    <NATConfig>
      <NATRule>
        <protocol>tcp</protocol><internalIpAddress><ipAddress>172.17.1.11</ipAddress>
        <internalPort><PortRange><rangeStart>15</rangeStart><rangeEnd>19</rangeEnd></PortRange>
        <externalIpAddress><ipAddress>10.112.196.219</ipAddress>
        <externalPort><PortRange><rangeStart>9915</rangeStart><rangeEnd>9919</rangeEnd></PortRange>
      </NATRule>
    </NATConfig>
  </VShieldEdgeConfig>

- DNAT Rule with IP and Port Range

  content-length: 627

  <?xml version="1.0" encoding="UTF-8"
  standalone="yes"?>
  <VShieldEdgeConfig>
    <NATConfig>
      <NATRule>
        <protocol>tcp</protocol><internalIpAddress><IpRange><rangeStart>172.17.1.15</rangeStart>
        <rangeEnd>172.17.1.19</rangeEnd></IpRange>
        <internalPort><PortRange><rangeStart>15</rangeStart><rangeEnd>19</rangeEnd></PortRange>
        <externalIpAddress><ipAddress>10.112.196.215</ipAddress>
        <externalPort><PortRange><rangeStart>9915</rangeStart><rangeEnd>9919</rangeEnd></PortRange>
      </NATRule>
    </NATConfig>
  </VShieldEdgeConfig>
Configuring the vShield Edge Firewall

The vShield Edge provides firewall protection for incoming and outgoing sessions. The default firewall policy allows all traffic to pass. In addition to the default firewall policy, you can configure a set of rules to allow or deny traffic sessions to and from specific sources and destinations. You manage the default firewall policy and firewall rule set separately for each vShield Edge agent.

All firewall rules for a vShield Edge configured by using REST requests appear under the vShield Edge > Firewall tab for the appropriate vShield Edge in the vShield Manager user interface and vSphere Client plug-in.

For the vShield Edge firewall schema, see “vShield Edge Firewall Schema” on page 74.

Get the Firewall Rule Set for a vShield Edge

Example 5-25. Get the Entire Firewall Rule Set on a vShield Edge

Request:
GET <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/rules
Example:
GET /api/1.0/network/network-244/firewall/rules HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213

**Post a Firewall Rule Set**

You add all firewall rules as a set for each vShield Edge. The vShield Manager processes the posted XML file as a complete rule set for the specified vShield Edge. The new rule set replaces the entire previous rule set.

**Example 5-26. Post the Firewall Rule Set on a vShield Edge**

Request:
POST <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/rules

```
<VShieldEdgeConfig>
  <FirewallConfig>
    <FirewallRule>
      <protocol>tcp|udp|icmp|any</protocol>
      <sourceIpAddress>see_below</sourceIpAddress>
      <sourcePort>see_below</sourcePort>
      <destinationIpAddress>see_below</destinationIpAddress>
      <destinationPort>see_below</destinationPort>
      <direction>in|out|both</direction>
      <action>allow|deny</action>
    </FirewallRule>
  </FirewallConfig>
</VShieldEdgeConfig>
```

Rules:
- You can add multiple firewall rules by entering multiple `<FirewallRule>` sections in the body.
- For `<protocol />` options tcp and udp, you must specify `<sourcePort>` and `<destinationPort>` elements. For options icmp and any, the `<sourcePort>` and `<destinationPort>` elements are not expected.
- You must add `<icmpType />` if you configure icmp as the protocol.
- Logging is disabled by default. To enable logging, add a `<log />` element within `<FirewallRule />`.
- The `<sourceIpAddress>` and `<destinationIpAddress>` parameters can be entered in either of these formats.
  - `<ipAddress>`IpOrAny</ipAddress>
  - `<IpRange>`<rangeStart>low_ip_address</rangeStart><rangeEnd>high_ip_address</rangeEnd></IpRange>`
- The `<sourcePort>` and `<destinationPort>` parameters can be entered in either of the following formats.
  - `<port>`PortOrAny</port>
  - `<PortRange>`<rangeStart>low_port</rangeStart><rangeEnd>high_port</rangeEnd></PortRange>`
Example:

- Allow any firewall rule set

  ```
  POST /api/1.0/network/network-244/firewall/rules HTTP/1.1
  content-type: application/xml; charset=UTF-8
  Authorization: Basic YWRtaW46ZGVmYXVsdA==
  Host: 10.112.196.213
  accept: text/html, image/gif, image/jpeg, *, q=0.2, */*; q=0.2
  content-length: 711
  
  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <VShieldEdgeConfig>
    <FirewallConfig>
      <FirewallRule>
        <protocol>any</protocol>
        <sourceIpAddress><ipAddress>any</ipAddress></sourceIpAddress>
        <sourcePort><port>any</port></sourcePort>
        <destinationIpAddress><ipAddress>any</ipAddress></destinationIpAddress>
        <destinationPort><port>any</port></destinationPort>
        <direction>out</direction>
        <action>allow</action>
      </FirewallRule>
      <FirewallRule>
        <protocol>icmp</protocol>
        <icmpType>any</icmpType>
        <sourceIpAddress><ipAddress>any</ipAddress></sourceIpAddress>
        <destinationIpAddress><ipAddress>any</ipAddress></destinationIpAddress>
        <direction>out</direction>
        <action>allow</action>
      </FirewallRule>
    </FirewallConfig>
  </VShieldEdgeConfig>
  ```

- Firewall rule set with deny action based on IP and port range

  ```
  content-length: 695
  
  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <VShieldEdgeConfig>
    <FirewallConfig>
      <FirewallRule>
        <protocol>tcp</protocol>
        <sourceIpAddress><IpRange><rangeStart>172.17.1.13</rangeStart><rangeEnd>172.17.1.16</rangeEnd></IpRange></sourceIpAddress>
        <sourcePort><PortRange><rangeStart>9922</rangeStart><rangeEnd>9925</rangeEnd></PortRange></sourcePort>
        <destinationIpAddress><IpRange><rangeStart>192.168.102.6</rangeStart><rangeEnd>192.168.102.9</rangeEnd></IpRange></destinationIpAddress>
        <destinationPort><PortRange><rangeStart>22</rangeStart><rangeEnd>25</rangeEnd></PortRange></destinationPort>
        <direction>in</direction>
        <action>deny</action>
      </FirewallRule>
    </FirewallConfig>
  </VShieldEdgeConfig>
  ```

Get the Status of the Default Policy for a vShield Edge

You can check the action—allow or deny—currently enforced for the default firewall policy.

Example 5-27. Get the Status of the Default Policy for a Specific Network

Request:

GET <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/default

Example:

GET /api/1.0/network/network-244/firewall/default HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213

Change the Default Firewall Policy Action

You can change the default firewall policy action to either allow all traffic or deny all traffic.

Example 5-28. Change the Action of the Default Firewall Policy on a vShield Edge

Request:

PUT <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/default/{allow|deny}
Example:

PUT /api/1.0/network/network-244/firewall/default/allow HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213

Get Details of a Specific Firewall Rule
You can view the details of a specific firewall rule applied on a vShield Edge.

Example 5-29. Get a Firewall Rule

Request:
GET <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/rules/<rule-id>

Get Timestamps of Last 10 Firewall Rule Sets for a vShield Edge

Example 5-30. Get Last 10 Firewall Rule Set by Timestamp

Request:
GET <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/snapshots

Get Firewall Rule Set by Timestamp

Example 5-31. Get Firewall Rule Set by Timestamp

Request:
GET <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/snapshot/<snapshot-timestamp>

Revert to a Firewall Rule Set by Timestamp

Example 5-32. Revert to an DNAT Configuration by Snapshot Timestamp

Request:
PUT <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/snapshot/<snapshot-timestamp>

Delete All Firewall Rules on a vShield Edge

If you delete all firewall rules on a vShield Edge agent, the agent enforces the default policy on all incoming and outgoing traffic sessions.

Example 5-33. Delete All Firewall Rules on a vShield Edge

Request:
DELETE <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/firewall/rules
Example:
DELETE /api/1.0/network/network-244/firewall/rules HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.213

Configuring VPNs

vShield Edge agents support site-to-site IPSec VPN between a vShield Edge appliance and remote sites. On both ends, static one-to-one NAT is required for the VPN address.

**Figure 5-1.** vShield Edge Providing VPN Access from a Remote Site to a Secured Port Group

At this time, vShield Edge agents support pre-shared key mode, IP unicast traffic, and no dynamic routing protocol between the vShield Edge and remote VPN routers. Behind each remote VPN router, you can configure multiple subnets to connect to the internal network behind a vShield Edge through IPSec tunnels. These subnets and the internal network behind a vShield Edge must have non-overlapping address ranges.

You can deploy a vShield Edge agent behind a NAT device. In this deployment, the NAT device translates the vShield Edge agent's VPN address into a public accessible address facing the Internet; remote VPN routers use this public address to access the vShield Edge.

Remote VPN routers can be located behind a NAT device as well. You must provide both the VPN native address and the NAT public address to set up the tunnel.

All VPN settings configured by using REST requests appear under the **vShield Edge > VPN** tab for the appropriate vShield Edge in the vShield Manager user interface and vSphere Client plug-in.

For the VPN schema, see “VPN Schema” on page 80.
Get the Status of VPN Service

You can determine if the VPN service on a vShield Edge is running or stopped by requesting the service status.

**Example 5-34. Getting the Status of VPN Service**

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/service

Example:

GET /api/1.0/network/network-244/vpn/ipsec/service HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998

Start or Stop the VPN Service on a vShield Edge

You enable or disable VPN service on a vShield Edge by updating the status to start or stop.

**Example 5-35. Starting or Stopping VPN Service on a vShield Edge**

Request:

PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/action/{start | stop}

Example:

PUT /api/1.0/network/network-244/vpn/ipsec/action/start HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998

PUT /api/1.0/network/network-244/vpn/ipsec/action/stop HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost

Configure VPN Parameters on a vShield Edge

You can provide configuration parameters on a vShield Edge agent to set a VPN tunnel to a remote VPN router. The first time you configure VPN service for a vShield Edge, the configuration must contain the server configuration and a minimum of one remote site with a tunnel. If these elements are not sent, the configuration is rejected.

The IPSec parameters must be compatible on all IPSec end points.

**Example 5-36. Configuring VPN Parameters**

Request:

POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/config

Rules:

- Logging is disabled by default. To enable logging, add a `<log />` element within `<VPNServerConfig>`.
- VPN service requires encryption. You must specify the `<encryptionAlgorithm />` element as either `3des` or `aes`.
- The `natedPublicIpAddress` element under `VPNServerConfig` is optional.
- The `siteName` and `tunnelName` can contain only alphanumeric characters.
Example:

POST /api/1.0/network/network-244/vpn/ipsec/config HTTP/1.1
Content-Type: application/xml
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 662

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VShieldEdgeConfig><VPNConfig><IpsecVPNConfig><SiteToSiteIpsec><VPNServerConfig><externalIpAddress>10.112.196.219</externalIpAddress></VPNServerConfig><VPNSite><Configuration><siteName>VSE1</siteName><remoteEndPointexternalIpAddress>10.112.196.99</remoteEndPointexternalIpAddress><sharedSecret>psk1</sharedSecret><mtu>1500</mtu></Configuration><VPNTunnel><Configuration><tunnelName>tunnelVSE</tunnelName><remoteSiteSubnet>172.15.1.0/24</remoteSiteSubnet><encryptionAlgorithm>3des</encryptionAlgorithm></Configuration></VPNTunnel></VPNSite><VPNSite><Configuration><siteName>VSE1</siteName><remoteEndPointexternalIpAddress>10.112.196.219</remoteEndPointexternalIpAddress><sharedSecret>psk1</sharedSecret><mtu>1500</mtu></Configuration><VPNTunnel><Configuration><tunnelName>tunnelVSE</tunnelName><remoteSiteSubnet>172.17.1.0/24</remoteSiteSubnet><encryptionAlgorithm>aes</encryptionAlgorithm></Configuration></VPNTunnel></VPNSite></SiteToSiteIpsec></IpsecVPNConfig></VPNConfig></VShieldEdgeConfig>
```

Add a Remote Site

You can add a remote VPN site to connect remote users to the virtual machines protected by a vShield Edge.

**Example 5-37. Adding a Remote VPN Site**

Request:

POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/sites

Example

POST /api/1.0/network/network-244/vpn/ipsec/sites
Content-Type: application/xml
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 576
Add Tunnels for a VPN Site

This call adds tunnels to the specified VPN site.

**Example 5-38. Adding Tunnels for a VPN Site**

Request:

```
POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/<site-name>/connections
```

Example

Where the remote site name is vsesite1.

```
POST /api/1.0/network/network-244/vpn/ipsec/vsesite1/connections
Content-Type: application/xml
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 391
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VShieldEdgeConfig><VPNConfig><IpsecVPNConfig><SiteToSiteIpsec><VPNSite><VPNTunnel><Configuration><tunnelName>tunnelVSE1</tunnelName><remoteSiteSubnet>172.19.1.0/24</remoteSiteSubnet><encryptionAlgorithm>3des</encryptionAlgorithm></Configuration></VPNTunnel></VPNSite></SiteToSiteIpsec></IpsecVPNConfig></VPNConfig></VShieldEdgeConfig>
```

Get the Detailed IPSec Configurations for a Network

You can retrieve a detailed VPN configuration for a network that contains the VPN server configurations, site configurations, tunnel configurations, and the detailed configuration of all tunnels in all sites.

**Example 5-39. Getting the Detailed VPN Configuration for a Network**

Request:

```
GET <vshield_manager-uri>/api/1.0/network/<vdc-moref-id>/vpn/ipsec/detailedconfig
```

Example:

```
GET /api/1.0/network/dvportgroup-1004/vpn/ipsec/detailedconfig HTTP/1.1
Host: localhost:9998
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```
Get the Detailed Configuration for a VPN Site

You can retrieve a detailed VPN configuration for a site that contains the VPN server configuration, site configuration, tunnel configuration, and the detailed configuration of all tunnels for the site.

**Example 5-40. Getting the Detailed Configuration for a VPN Site**

Request:

GET <vshield_manager-uri>/api/1.0/network/<vdc-moref-id>/vpn/ipsec/<site-name>/detailedconfig

Example:

GET /api/1.0/network/resgroup-v107/vpn/ipsec/site01/detailedconfig HTTP/1.1
Host: localhost:9998
authorization: Basic YWRtaW46ZGVmYXVsdA==

Get the Detailed Tunnel Configuration

You can request the list of tunnels configured for a VPN site.

**Example 5-41. Getting the Detailed Tunnel Configuration for a Site**

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/<site-name>/<connection-name>/detailedconfig

Delete a Tunnel for a VPN Site

This call deletes a tunnel from the specified site.

**Example 5-42. Deleting a Tunnel from a VPN Site**

Request:

DELETE <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/<site-name>/<connection-name>

Delete a Remote Site

You must specify the site name to delete a remote VPN site. The site and all associated tunnels are deleted.

**Example 5-43. Deleting a Remote VPN Site**

Request:

DELETE <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/site/<site-name>

Get the Current VPN Configuration on a vShield Edge

You can retrieve the current VPN configuration on a vShield Edge to view settings such as tunnels and sites, as well as entity naming and addressing.

**Example 5-44. Getting the Current VPN Configuration**

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/config
Example:

GET /api/1.0/network/network-244/vpn/ipsec/config HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998

Get Timestamps of Last 10 VPN Configurations

You can retrieve a list of the last 10 VPN configuration changes. You can use the returned timestamps to review the details of past configurations in a separate request.

Example 5-45. Getting Last 10 VPN Configurations by Timestamp

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/snapshots

Get a VPN Configuration by Timestamp

You can retrieve and view a specific historical VPN configuration by specifying the timestamp when the configuration was overwritten.

Example 5-46. Getting a VPN Configuration by Timestamp

Request

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/snapshot/<snapshot-timestamp>

Revert to a VPN Configuration by Timestamp

You can revert to a previous VPN configuration by specifying the timestamp of the previous configuration.

Example 5-47. Reverting to a VPN configuration by timestamp

Request:

PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/snapshot/<snapshot-timestamp>

Delete the VPN Configuration on a vShield Edge

You can delete the current VPN configuration to clear VPN settings from the vShield Edge running configuration. The vShield Edge saves the deleted configuration by marking it with a timestamp.

Example 5-48. Deleting the VPN Configuration on a vShield Edge

Request:

DELETE <vShield_Manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/vpn/ipsec/config

Example:

DELETE /api/1.0/network/network-244/vpn/ipsec/config HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
Load Balancer

The vShield Edge provides load balancing for HTTP traffic. Load balancing (up to Layer 7) enables Web application auto-scaling.

**Figure 5-2. vShield Edge Providing Load Balancing Service for Protected Virtual Machines**

You map an external (or public) IP address to a set of internal servers for load balancing. The load balancer accepts HTTP requests on the external IP address and decides which internal server to use. Port 80 is the default listening port for load balancer service.

All Load Balancer settings configured by using REST requests appear under the **vShield Edge > Load Balancer** tab for the appropriate vShield Edge in the vShield Manager user interface and vSphere Client plug-in.

For the load balancer schema, see “Load Balancer Schema” on page 83.

Get the Status of Load Balancer Service on a vShield Edge

**Example 5-49. Getting the Status of Load Balancer Service on a vShield Edge**

Request:

```
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer/service
```

Example:

```
GET /api/1.0/network/network-244/loadbalancer/service HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
```
Start or Stop the Load Balancer Service on a vShield Edge

Example 5-50. Starting or Stopping the Load Balancer Service on a vShield Edge

Request:

PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer/action/{start | stop}

Example:

PUT /api/1.0/network/network-244/loadbalancer/action/start HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998

Add a Listener for Load Balancing Service

You can map a global or public IP address with a set of internal servers for load balancing. The load balancer accepts HTTP requests on this IP address. The internalIPList is a comma-separated list of one or more IP:Port instances that represents servers that can be used for load balancing. If a port is not specified, port 80 is the default port. The vShield Manager processes the posted XML file as a complete set of load balancing servers for the specific network. The current set of load balancing servers for a network is replaced with this new set of servers.

You can add multiple servers as listeners by entering multiple <Listener /> sections in the body.

You can configure the algorithm that is used to determine load balancing. The optional <algorithm /> element can be set to round-robin or ip-hash. By default, the load balancer algorithm is set to round-robin.

Example 5-51. Adding a Load Balancer Listener on a vShield Edge

Request:

POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer/

Rules:

- Logging is disabled by default. To enable logging, add a <log /> element within <Listener />.
- The backendServers internalIPList element is a comma-separated IP list. Port 80 is used by default. You can specify custom IP:Port values in the internalIPList.

Example:

- Basic load balancer configuration

```xml
POST /api/1.0/network/network-244/loadbalancer HTTP/1.1
Content-Type: application/xml
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
Accept: text/html, image/gif, image/jpeg, *, q=0.2, */*; q=0.2
Content-Length: 490

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VShieldEdgeConfig>
<LoadBalancerConfig>
<Listener>
<externalIPAddress>10.112.196.95</externalIPAddress>
<BackEndServers>
<internalIPList>172.17.1.11,172.17.1.12</internalIPList>
</BackEndServers>
<algorithm>ip-hash</algorithm>
</Listener>
<Listener>
<externalIPAddress>10.112.196.96</externalIPAddress>
<BackEndServers>
<internalIPList>172.17.1.11,172.17.1.12</internalIPList>
</BackEndServers>
</Listener>
</LoadBalancerConfig>
</VShieldEdgeConfig>
```
Get the Current Load Balancer Configuration on a vShield Edge

You can retrieve the current Load Balancer configuration on a vShield Edge to view settings such as configured listeners.

Example 5-52. Getting All Load Balancer Servers on a vShield Edge

Request:
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer

Example:
GET /api/1.0/network/network-244/loadbalancer HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:80

Get the Configuration of a Specific Load Balancing Server

You can retrieve the current configuration of a single Load Balancer listener on a vShield Edge.

Example 5-53. Getting the Configuration of a Specific Load Balancing Server

Request:
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer/<loadbalancer-id>

Example:
GET /api/1.0/network/network-244/loadbalancer/3 HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:80

Get Timestamps of Last 10 Load Balancer Configurations

You can retrieve a list of the last 10 Load Balancer configuration changes. You can use the returned timestamps to review the details of past configurations in a separate request.

Example 5-54. Getting the Last 10 Load Balancer Configurations by Timestamp

Request:
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer/snapshots
Get a Load Balancer Configuration by Timestamp

You can retrieve and view a specific historical Load Balancer configuration by specifying the timestamp when the configuration was overwritten.

**Example 5-55. Getting Load Balancer Configuration by Timestamp**

**Request:**

```
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer/snapshot/<snapshot-timestamp>
```

Revert to a Load Balancer Configuration by Timestamp

You can revert to a previous Load Balancer configuration by specifying the timestamp of the previous configuration.

**Example 5-56. Reverting to a Previous Load Balancer Configuration by Timestamp**

**Request:**

```
PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer/snapshot/<snapshot-timestamp>
```

Delete the Load Balancer Configuration on a vShield Edge

**Example 5-57. Deleting the Load Balancer Configuration on a vShield Edge**

**Request:**

```
DELETE <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/loadbalancer
```

Example:

```
DELETE /api/1.0/network/network-244/loadbalancer HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
```

Managing the MTU Threshold for a vShield Edge

You can set a maximum transmission unit (MTU) threshold for traffic on the Internal and External interfaces of a vShield Edge.

For the MTU threshold schema, see “MTU Threshold Schema” on page 84.

**Example 5-58. Configuring the MTU Threshold for a vShield Edge**

**Request:**

```
PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/mtu
```

You can retrieve the current MTU threshold from a vShield Edge for reference.

**Example 5-59. Retrieving the MTU Threshold for a vShield Edge**

**Request:**

```
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/mtu
```
Example:

```
GET /api/1.0/network/network-244/mtu HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998

<?xml version="1.0" encoding="UTF-8" standalone="yes"?><VShieldEdgeConfig><MTU><internalInterfaceMTU>2000</internalInterfaceMTU><externalInterfaceMTU>2000</externalInterfaceMTU></MTU></VShieldEdgeConfig>
```

---

**View Traffic Statistics**

Each vShield Edge agent offers a collection service for traffic statistics. Traffic statistics provide information on the sessions in and out of your network.

For the traffic statistics schema, see “Traffic Stats Schema” on page 85.

**Example 5-60. Getting Traffic Statistics for a vShield Edge**

Request:

```
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/trafficstats/all
```

Example:

```
GET /api/1.0/network/network-244/trafficstats/all HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost
```

---

**Debug vShield Edge Services Using Service Statistics**

You can retrieve the path to the service statistics file of a vShield Edge and use the statistics to debug service issues.

**Example 5-61. Debugging a vShield Edge by Using Service Statistics**

Request:

```
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/serviceStats
```

Response:

XML with path of vShield Edge service statistics file which can be downloaded over http
Managing the Connection to a Syslog Server

You can connect a vShield Edge to a syslog server for vShield Edge log management.

For the traffic statistics schema, see “Syslog Schema” on page 85.

Post a Syslog Server Configuration

Example 5-62. Posting a Syslog Server Configuration

Request:

POST <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/syslog/config

<VShieldEdgeConfig>
   <SyslogServerConfig>
      <ipAddress>A.B.C.D</ipAddress>
      .....  
      .....  
   </SyslogServerConfig>
</VShieldEdgeConfig>

Rules:

You can add up to two syslog servers.

Example:

POST /api/1.0/network/network-244/syslog/config
Content-Type: application/xml
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: localhost:9998
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 173

<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><VShieldEdgeConfig><SyslogServerConfig><ipAddress>10.112.196.123</ipAddress></SyslogServerConfig></VShieldEdgeConfig>

Get the Current Syslog Server Configuration

Example 5-63. Getting the Running Syslog Server Configuration

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/syslog/config

Get Timestamps of Last 10 Syslog Server Configurations

Example 5-64. Getting Last 10 Syslog Server Configurations by Timestamp

Request:

GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/syslog/snapshots
Get a Syslog Server Configuration by Timestamp

Example 5-65. Getting a Syslog Server Configuration by Timestamp

Request:
GET <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/syslog/snapshot/<snapshot-timestamp>

Revert to a Syslog Server Configuration by Timestamp

Example 5-66. Reverting to a Syslog Server Configuration by Timestamp

Request:
PUT <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/syslog/snapshot/<snapshot-timestamp>

Delete the Current Syslog Server Configuration

Example 5-67. Deleting a Syslog Server Configuration

Request:
DELETE <vshield_manager-uri>/api/1.0/network/<internal-portgroup-vc-moref-id>/syslog/config
You can configure vShield App firewall rules and syslog service by using REST API calls.

**IMPORTANT**  All vShield REST requests require authorization. You can use the following basic authorization:

```
Authorization: Basic YmRtOW46ZGVeYXVsdA==
```

YmRtOW46ZGVeYXVsdA== represents the Base 64 encoding of the vShield Manager default login credentials (admin:default).

This chapter includes the following topics:

- “Configuring Firewall Rules for a vCenter Container” on page 51
- “Managing Security Groups” on page 56
- “Configuring Syslog Service for a vShield App” on page 59

### Configuring Firewall Rules for a vCenter Container

The primary function of a vShield App is to provide firewall protection on an ESX host by inspecting each session and returning details to the vShield Manager. Traffic details include sources, destinations, direction of sessions, applications, and ports being used. Traffic details can be used to create firewall allow or deny rules.

In the vShield Manager user interface or vSphere Client plug-in, the **App Firewall** tab contains the firewall rules enforced by vShield App instances. You can manage App Firewall rules at the datacenter, cluster, and port group levels to provide a consistent set of rules across multiple vShield App instances under these containers. As membership in these containers can change dynamically, App Firewall maintains the state of existing sessions without requiring reconfiguration of firewall rules. In this way, App Firewall effectively has a continuous footprint on each ESX host under the managed containers.

When creating App Firewall rules, you can create general rules based on incoming or outgoing traffic at the container level. For example, you can create a rule to deny any traffic from outside of a datacenter that targets a destination within the datacenter. You can create a rule to deny any incoming traffic that is not tagged with a VLAN ID.

All firewall rules configured by using REST requests appear under the **App Firewall** tab for the appropriate container in the vShield Manager user interface and vSphere Client plug-in.

For the complete firewall XML schema, see “vShield App Firewall Schema” on page 69.

### View All Firewall Rules for a Container

You can view all of the firewall rules for a specific container—datacenter, cluster, or port group—and any child containers by identifying the MOREF ID (container-moref-id) of the container. For example, if you request the rule set at the datacenter level, the response includes the rules for the clusters and port groups within that datacenter.

It is good practice to view the current firewall rule set before posting new or updated rules.
Viewing the Firewall Rule Set for a Container

Example 6-1.

Request:
GET <vshield_manager-uri>/api/1.0/zones/<container-moref-id>/firewall/rules

Example:
GET /api/1.0/zones/datacenter-4361/firewall/rules HTTP/1.1
Host: localhost
Authorization: Basic YWRtaW46ZGVmYXVsdA==

Post an App Firewall Rule Set for a Container

You can add an App Firewall rule set via REST for a datacenter, cluster, or port group container.

The vShield Manager processes the posted XML file as a complete rule set for the specified container. The current container rule set is replaced with this new set of rules.

If you add a new rule to an existing rule set, the new rule must be identified as Rule ID 0:

Example 6-2.

Post a Firewall Rule Set at the Datacenter Level

Request:
POST <vshield_manager-uri>/api/1.0/zones/<container-moref-id>/firewall/rules

Example:
POST /api/1.0/zones/datacenter-7/firewall/rules
content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 192.168.102.134
content-length: 655

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<vshieldZonesFirewallConfiguration><ContainerAssociation><Container id="vShield">
  <InstanceId>datacenter-7</InstanceId></Container><Container id="ANY">
    <Name>ANY</Name></Container><RuleSet><Rule><ID>0</ID><Precedence>High</Precedence><Position>1</Position><Source ref="vShield" exclude="false"/>
    <Destination ref="vShield" exclude="true"/>
    <SourcePorts>ANY</SourcePorts><Application type="UNICAST">FTP</Application><DestinationPorts>21</DestinationPorts><Protocol>TCP</Protocol><Action>ALLOW</Action><Log>false</Log><Notes></Notes></Rule><Rule><ID>58024</ID><Precedence>High</Precedence><Position>1</Position><Source ref="vShield" exclude="true"/>
    <Destination ref="vShield" exclude="false"/>
    <SourcePorts>ANY</SourcePorts><Application type="UNICAST">MS-DS</Application><DestinationPorts>445</DestinationPorts><Protocol>TCP</Protocol><Action>DENY</Action><Log>false</Log><Notes></Notes></Rule><Rule><ID>1001</ID><Precedence>Default</Precedence><Position>1</Position><Source ref="ANY" exclude="false"/>
    <Destination ref="ANY" exclude="false"/>
    <SourcePorts>68</SourcePorts><Application type="UNICAST">DHCP-Server</Application><DestinationPorts>67</DestinationPorts><Protocol>UDP</Protocol><Action>ALLOW</Action><Log>false</Log><Notes></Notes></Rule><Rule><ID>1002</ID><Precedence>Default</Precedence><Position>2</Position><Source ref="ANY" exclude="false"/>
    <Destination ref="ANY" exclude="false"/>
    <SourcePorts>67</SourcePorts><Application type="UNICAST">DHCP-Client</Application><DestinationPorts>68</DestinationPorts><Protocol>UDP</Protocol><Action>ALLOW</Action><Log>false</Log><Notes></Notes></Rule><Rule><ID>1003</ID><Precedence>Default</Precedence><Position>3</Position><Source ref="ANY" exclude="false"/>
    <Destination ref="ANY" exclude="false"/>
    <SourcePorts>68</SourcePorts><Application type="UNICAST">ANY</Application><DestinationPorts>67</DestinationPorts><Protocol>UDP</Protocol><Action>ALLOW</Action><Log>false</Log><Notes></Notes></Rule><Rule><ID>1004</ID><Precedence>Default</Precedence><Position>4</Position><Source ref="ANY" exclude="false"/>
    <Destination ref="ANY" exclude="false"/>
    <SourcePorts>ANY</SourcePorts><Application type="UNICAST">ANY</Application><DestinationPorts>67</DestinationPorts><Protocol>UDP</Protocol><Action>ALLOW</Action><Log>false</Log><Notes></Notes></Rule>
Chapter 6 vShield App Management

Example 6-3. Posting a Firewall Rule Set at the Datacenter Level with Destination IP as a VLAN Container

Example:

POST /api/1.0/zones/datacenter-7/firewall/rules
content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 192.168.102.134
content-length: 655

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<vshieldZonesFirewallConfiguration><ContainerAssociation><Container id="No Vlan (0)"><Name>No Vlan (0)</Name><Container id="vShield"><InstanceId>
Example 6-4. Posting a Firewall Rule Set at the Cluster Level

Example:

POST /api/1.0/zones/domain-c14/firewall/rules
content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 192.168.102.134
content-length: 655

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<vshieldZonesFirewallConfiguration><ContainerAssociation><Container id="CL2"><InstanceId>domain-c14</InstanceId></Container></ContainerAssociation>
<RuleSet><Rule><ID>0</ID><Precedence>High</Precedence><Position>1</Position>
<source ref="CL2" exclude="false"/><destination ref="CL2" exclude="true"/>
<sourcePorts>ANY</sourcePorts><application type="UNICAST">FTP</application>
<destinationPorts>21</destinationPorts><protocol>TCP</protocol><action>ALLOW</action><log>false</log><notes></notes></rule><rule><ID>58012</ID><Precedence>High</Precedence><Position>2</Position>
<source ref="CL2" exclude="false"/><destination ref="CL2" exclude="true"/>
<sourcePorts>ANY</sourcePorts><application type="UNICAST">ORACLE-HTTP</application>
<destinationPorts>7777</destinationPorts><protocol>TCP</protocol><action>DENY</action><log>false</log><notes></notes></rule></ruleSet>
</vshieldZonesFirewallConfiguration>

Example 6-5. Posting a Firewall Rule Set at the Port Group Level

Example:

POST /api/1.0/zones/portgroup-512/firewall/rules
content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 192.168.102.134
content-length: 655

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<vshieldZonesFirewallConfiguration><ContainerAssociation><Container id="zone-1"><InstanceId>udz-6</InstanceId></Container></ContainerAssociation>
<RuleSet><Rule><ID>0</ID><Precedence>High</Precedence><Position>2</Position>
<source ref="zone-1" exclude="true"/><destination ref="zone-1" exclude="false"/>
<sourcePorts>ANY</sourcePorts><application type="UNICAST">FTP</application>
<destinationPorts>21</destinationPorts><protocol>TCP</protocol><action>ALLOW</action><log>false</log><notes></notes></rule><rule><ID>58013</ID><Precedence>High</Precedence><Position>1</Position>
<source ref="zone-1" exclude="true"/><destination ref="zone-1" exclude="false"/>
<sourcePorts>ANY</sourcePorts><application type="UNICAST">SSH</application>
<destinationPorts>22</destinationPorts><protocol>TCP</protocol><action>DENY</action><log>false</log><notes></notes></rule></ruleSet>
</vshieldZonesFirewallConfiguration>
**View a List of Timestamps Identifying App Firewall Rule Set Changes**

You can view a list of timestamps marking firewall rule set changes for a specific container. To view the rule set according to a specific timestamp, see “View a Previous Firewall Rule Set by Timestamp” on page 55.

**Example 6-6. View a List of Firewall Rule Sets by Timestamps**

Request:

GET <vshield_manager-uri>/api/1.0/zones/<container-moref-id>/firewall/snapshots

Example:

GET /api/1.0/zones/datacenter-4361/firewall/snapshots HTTP/1.1
Host: localhost
Authorization: Basic YWRtaW46ZGVmYXVsdA==

**View a Previous Firewall Rule Set by Timestamp**

You can view a historical rule set by its timestamp. To view the list of timestamps, see “View a List of Timestamps Identifying App Firewall Rule Set Changes” on page 55.

**Example 6-7. View a Firewall Rule Set by Timestamp**

Request:

GET <vshield_manager-uri>/api/1.0/zones/<container-moref-id>/firewall/snapshot/<snapshot-timestamp>

Example:

GET /api/1.0/zones/datacenter-4361/firewall/snapshot/1274872770000 HTTP/1.1
Host: localhost
Authorization: Basic YWRtaW46ZGVmYXVsdA==

**Revert to a Previous Firewall Rule Set**

You can revert to a previous firewall rule set by specifying the appropriate container and timestamp.

**Example 6-8. Revert to a Previous Firewall Rule Set**

Request:

PUT <vshield_manager-uri>/api/1.0/zones/<container-moref-id>/firewall/snapshot/<timestamp>

Example:

PUT /api/1.0/zones/datacenter-4361/firewall/snapshot/1274872770000 HTTP/1.1
Host: localhost
Authorization: Basic YWRtaW46ZGVmYXVsdA==

**Delete All Firewall Rules under a Container**

You can delete the entire rule set for a datacenter, cluster, or port group container. When you delete the firewall rule set at the datacenter or cluster level, the system reverts to the default rules for that container and all child containers. If you delete rules at the cluster or port group level, any rules set at the datacenter remain enforced.

**Example 6-9. Delete a Firewall Rule Set for a Container**

Request:

DELETE <vshield_manager-uri>/api/1.0/zones/<container-moref-id>/firewall/rules
Managing Security Groups

A security group is a trust zone that you create and assign resources to for vShield App firewall protection. Security groups are containers, like a vApp or a cluster. Typically, containers are created in the vCenter and viewed in the vShield Manager user interface.

Security groups enables you to create custom containers from within vShield. You arbitrarily assign resources, such as virtual machines and network adapters, to a security group. After the group is defined, you add the group to an vShield App firewall rule for protection. See “Configuring Firewall Rules for a vCenter Container” on page 51.

All security groups configured by using REST requests appear under the Security Groups tab for the appropriate node in the vShield Manager user interface and vSphere Client plug-in.

For the security groups schema, see “Security Groups Schema” on page 67.

Add a Security Group

Example 6-10. Adding a Security Group

Request:

POST <vshield_manager-uri>/api/1.0/global/securityGroups/<base-node-moref-id>/groups

Example:

- Adding a single security group

  POST /api/1.0/global/securityGroups/datacenter-7/groups/ HTTP/1.1
  authorization: Basic YWRtaW46ZGVmYXVsdA==
  host: 10.112.196.127
  Content-Type: application/xml
  Content-Length: 474


- Adding a single security group with no network adapters

  POST /api/1.0/global/securityGroups/datacenter-7/groups/ HTTP/1.1
  authorization: Basic YWRtaW46ZGVmYXVsdA==
  host: 10.112.196.127
  Content-Type: application/xml
  Content-Length: 299

You can add multiple security groups in one request.

**Example 6-11. Adding Multiple Security Groups**

Example:

```plaintext
POST /api/1.0/global/securityGroups/datacenter-7/groups/ HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127
Content-Type: application/xml
Content-Length: 815

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

---

### Add a Virtual Machine to a Security Group

You can add a virtual machine to a Security Group by specifying the node in which the Security Group resides. You use the vNIC identifier to identify the virtual machine. To get the `<NIC-ID>` parameter, see “Get the Properties from a Virtual Machine” on page 58.

**Example 6-12. Adding a Virtual Machine to a Security Group**

Request:

```plaintext
POST <vshield_manager-uri>/api/1.0/global/securityGroups/<base-node-moref-id>/nodes/<nic-id>
```

Example:

```plaintext
POST /api/1.0/global/securityGroups/dvportgroup-343/nodes/502a7702-8936-be93-ec75-1f8d00b6efb.000 HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127
Content-Type: application/xml
Content-Length: 207

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VsmGlobalConfig><SecurityGroups><SecurityGroupIdList><SecurityGroupId>udz-1</SecurityGroupId></SecurityGroupIdList></SecurityGroups></VsmGlobalConfig>
```

---

### Get the List of All Security Groups under a Base Node

**Example 6-13. Getting the List of All Security Groups under a Base Node**

Request:

```plaintext
GET <vshield_manager-uri>/api/1.0/global/securityGroups/<base-node-moref-id>/groups
```

Example:

```plaintext
GET /api/1.0/global/securityGroups/datacenter-7/groups HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127
```
Get the Details for a Single Security Group under a Base Node

Example 6-14. Getting the Details of a Single Security Group

Request:
GET <vshield_manager-uri>/api/1.0/global/securityGroups/<BASE-NODE-MOREF-ID>/groups/<securityGroupId>

Example:
GET /api/1.0/global/securityGroups/datacenter-2/groups/secgroup-6 HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127

Get IP Addresses for the Virtual Machines in a Security Group

You can get the IP addresses for the virtual machines within a Security Group.

Example 6-15. Getting the IP Addresses of Virtual Machines in a Security Group

Request:
GET <vshield_manager-uri>/api/1.0/global/securityGroups/<base-node-moref-id>/groups/<securityGroupId>/ipList

Get the Properties from a Virtual Machine

You can get the properties of a virtual machine so that you can use the NIC-ID to add the virtual machine to a Security Group. See “Add a Virtual Machine to a Security Group” on page 57.

See “Virtual Machine Information Schema” on page 66.

Example 6-16. Getting the Properties of a Virtual Machine

Request:
GET <vshield_manager-uri>/api/1.0/global/vmInfo/<vm-moref-id>

Example:
GET /api/1.0/global/vmInfo/vm-570 HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127

Delete a Virtual Machine from a Security Group

You can delete a virtual machine from a Security Group by specifying the node in which it resides.

Example 6-17. Deleting a Virtual Machine from a Security Group

Request:
DELETE <vshield_manager-uri>/api/1.0/global/securityGroups/<base-node-moref-id>/nodes/<nic-id>

Example:
DELETE /api/1.0/global//securityGroups/datacenter-2/groups/secgroup-6/nodes/590e17ca-58bc-25d3-f001-9cf6515d6466.003 HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127
Delete a Single Security Group

You can delete a single Security Group under a base node by specifying the Security Group ID.

**Example 6-18. Deleting a Single Security Group**

Request:

```
DELETE <vshield_manager-uri>/api/1.0/global/securityGroups/<base-node-moref-id>/
       groups/<securityGroupId>
```

Example:

```
DELETE /api/1.0/global/securityGroups/datacenter-2/groups/secgroup-1 HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127
```

Delete All Security Groups under a Base Node

You can delete all security groups under a base node. Firewall rules related to deleted security groups are also deleted.

**Example 6-19. Deleting All Security Groups under a Base Node**

Request:

```
DELETE <vshield_manager-uri>/api/1.0/global/securityGroups/<base-node-moref-id>/groups
```

Example:

```
DELETE /api/1.0/global/securityGroups/datacenter-2/groups/ HTTP/1.1
authorization: Basic YWRtaW46ZGVmYXVsdA==
host: 10.112.196.127
```

Configuring Syslog Service for a vShield App

You can configure all vShield App instances to send system events to up to two syslog servers. All vShield App instances share the same syslog server configuration.

This request returns the list of syslog servers configured on the first vShield App instance that responds.

**Example 6-20. Get the Syslog Server Configuration for All vShield App Instances**

Request:

```
GET <vshield_manager-uri>/api/1.0/zones/syslogServers
```

This request configures all vShield App instances connected to the vShield Manager to send events to the specified syslog servers.

**Example 6-21. Post the Syslog Server Configuration across All vShield App Instances**

Request:

```
POST <vshield_manager-uri>/api/1.0/zones/syslogServers
```
This request deletes the syslog server configuration across all vShield App instances connected to the vShield Manager.

**Example 6-22. Delete the Syslog Server Configuration across all vShield App Instances**

Request:
DELETE <vshield_manager-uri>/api/1.0/zones/syslogServers

This request deletes a single syslog server by IP address across all vShield App instances connected to the vShield Manager.

**Example 6-23. Delete a Single Syslog Server by IP Address from All vShield App Instances**

Request:
DELETE <vshield_manager-uri>/api/1.0/zones/syslogServers/<ip_of_syslogServer>
The VMware Endpoint system delivers an introspection-based antivirus solution that uses the hypervisor to scan guest virtual machines from the outside with only a thin agent on each guest virtual machine.

You installed the vShield Endpoint service as part of ESX host preparation. You must perform the following tasks in sequence to complete EPSec installation.

**IMPORTANT** All vShield REST requests require authorization. You can use the following basic authorization:

```
Authorization: Basic YWRtaW46ZGVmYXVsdA==
```

`YWRtaW46ZGVmYXVsdA==` represents the Base 64 encoding of the vShield Manager default login credentials (admin:default).

### Register an SVM with the vShield Endpoint Service on an ESX Host

You can register and unregister a third-party antivirus security virtual machine (SVM) with vShield Endpoint.

In the POST request, `vmId` is the 0-based index of the vNIC that the SVM uses to communicate with the vShield Endpoint service. The vShield Manager connects the vNIC to the correct port group to enable communication between the SVM and the vShield Endpoint service.

To register SVMs on multiple ESX hosts in a single REST call, include multiple `<SvmRegister />` sections in the request body.

**Example 7-1. Registering an SVM with vShield Endpoint Service**

Request:

```
POST <vshieldmanager-uri>/api/1.0/endpointsecurity/svm

<VShieldEndpointSecurity>
  <SvmRegister>
    <vmId>vmid_of_svm_vm</vmId>
    <ipAddress>ipaddress_of_svm_vnic</ipAddress>
    <port>port_for_communication</port>
    <vendorId>partner_identification_string</vendorId>
  </SvmRegister>
</VShieldEndpointSecurity>
```

Where:

- `vmId` is the SVM managed object ID in vCenter.
- `ipAddress` is the IP address of the SVM's vNIC that is connected to the vmkernel port group.
- `port` is the port on which the SVM listens to connection from the EPSec vmkernel module.
- `vendorId` is the string that is used as an identifier of the partner who owns the SVM.
Example:

POST /api/1.0/endpointsecurity/svm HTTP/1.1
accept: application/xml
content-type: application/xml
host: 10.112.199.123:80
Authorization: Basic YWRtaW46ZGVmYXVsdA==
content-length: 204

<VShieldEndpointSecurity><SvmRegister><vmId>vm-3983</vmId><ipAddress>192.168.0.1</ipAddress>
<port>6666</port><vendorId>SomeVendor</vendorId></SvmRegister>
</VShieldEndpointSecurity>

Response:

HTTP 204 No Content: The Endpoint Security VM is successfully registered.
HTTP 401 Unauthorized: The username or password sent in Authorization header is wrong.
HTTP 400 Bad Request
  40002=Acquiring data from VC failed for <>
  40005=SVM with moid: <> failed to register
  40006=SVM with moid: <> already registered
  40009=Invalid SVM details
  40010=Endpoint LKM not installed
  40012=Endpoint LKM not installed due to bad ESX version
  40015=vmId is malformatted or of incorrect length : <>
  40020=Invalid vendorId for {0}
  40022=Host: <> has a registered SVM with moid: <>

Retrieve SVM-Specific Network Information

You must specify the virtual machine ID of the SVM to view network information.

Example 7-2. Retrieve SVM-Specific vShield Endpoint Network Information

Request:

GET <vshieldmanager-uri>/api/1.0/endpointsecurity/svm/<vmId>/<vendorId>/connInfo

Example:

GET /api/1.0/endpointsecurity/svm/vm-1234/JohnDoe/connInfo HTTP/1.1
host: 10.112.199.123:80
Authorization: Basic YWRtaW46ZGVmYXVsdA==

Response:

HTTP 200 OK
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VShieldEndpointSecurity>
  <HostToSvmConnectionInfo>
    <ipAddress>ip_address</ipAddress>
    <port>port</port>
  </HostToSvmConnectionInfo>
</VShieldEndpointSecurity>

HTTP 401 Unauthorized : The username or password sent in Authorization header is wrong.
HTTP 405 Method Not Allowed : If the vmId is missed in the URI.
HTTP 400 Bad Request : Internal error codes. Please refer the Error Schema for more details.
  40002=Acquiring 1. data from VC failed for <>
  40007=SVM with moid: <> not registered
  40015=vmId is malformatted or of incorrect length : <>
Retrieve vShield Endpoint Service Status on an ESX Host

You must specify the host ID of the ESX host.

Example 7-3. Retrieving vShield Endpoint Service Status from an ESX Host

Request:
GET <vshieldmanager-uri>/api/1.0/endpointsecurity/host/<hostId>

Example:
GET /api/1.0/endpointsecurity/host/host-1234 HTTP/1.1
host: 10.112.199.123:80
Authorization: Basic YWRtaW46ZGVmYXVsdA==

Response:
HTTP 200 OK
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VShieldEndpointSecurity>
  <lkmStatus>installed|notInstalled|badEsxVersion</lkmStatus>
</VShieldEndpointSecurity>

HTTP 401 Unauthorized : The username or password sent in Authorization header is wrong.
HTTP 404 Not Found : If the hostId is missing in the URI.
HTTP 400 Bad Request : Internal error codes. Please refer the Error Schema for more details.
  40002=Acquiring 1. data from VC failed for <>
  40017=hostId is malformatted or of incorrect length : <>

Uninstalling the vShield Endpoint Service from an ESX Host

Before you uninstall the vShield Endpoint from the vShield Manager and ESX host, you must unregister the SVM from the vShield Endpoint service.

CAUTION If any of the virtual machines that are running on the target ESX host cannot be migrated to another ESX host, these virtual machines must be powered off or migrated manually before the uninstallation can continue.

Unregister an SVM from vShield Endpoint

You must specify the virtual machine ID of the SVM to unregister the SVM from the vShield Endpoint service.

Example 7-4. Unregistering an SVM from vShield Endpoint

Request:
DELETE <vshieldmanager-uri>/endpointsecurity/svm/<vmId>

Example:
DELETE /api/1.0/endpointsecurity/svm/vm-1234 HTTP/1.1
host: 10.112.199.123:80
Authorization: Basic YWRtaW46ZGVmYXVsdA==

Response:
HTTP 204 No Content: The Endpoint Security VM is successfully unregistered.
HTTP 401 Unauthorized: The username or password sent in Authorized header is wrong.
HTTP 405 Method Not Allowed: If the vmId is missed in the URI.
HTTP 400 Bad Request: Internal error codes. Please refer the Error Schema for more details.
  40002=Acquiring data from VC failed for <>
  40015=vmId is malformatted or of incorrect length : <>
Uninstall vShield Endpoint from the vShield Manager

After the SVM is unregistered, you can uninstall the vShield Endpoint from the vShield Manager. See “Uninstalling vShield Services from an ESX Host” on page 18.

Error Schema

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
   elementFormDefault="qualified">
  <xs:element name="Errors">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="unbounded" name="Error" type="ErrorType"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="ErrorType">
    <xs:sequence>
      <xs:element name="code" type="xs:unsignedInt"/>
      <xs:element name="description" type="xs:string"/>
      <xs:element minOccurs="0" name="index" type="xs:int"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```
Appendix

The REST API configuration of the vShield Edge and vShield App virtual machines supports schemas for installation and service management.

This appendix covers the following topics:
- “vShield Manager Schemas” on page 65
- “ESX Host Preparation and Uninstallation Schema” on page 68
- “vShield App Schemas” on page 69
- “vShield Edge Schemas” on page 71
- “Error Message Schema” on page 86

vShield Manager Schemas

The following schemas detail vShield Manager configuration via REST API.

vShield Manager to vCenter Server Synchronization Schema

This schema synchronizes the vShield Manager with the vCenter Server inventory by leveraging the vCenter Server SDK.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VsmGlobalConfig">
    <xs:complexType>
      <xs:all>
        <xs:element minOccurs="0" name="VcInfo" type="VcInfoType" />
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="VcInfoType">
    <xs:sequence>
      <xs:element name="ipAddress">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="userName">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```
DNS Service Schema

This schema can be used to identify DNS services for the vShield Manager.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VsmGlobalConfig">
    <xs:complexType>
      <xs:all>
        <xs:element minOccurs="0" name="VcInfo" type="VcInfoType" />
        <xs:element minOccurs="0" name="DnsInfo" type="DnsInfoType" />
      </xs:all>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="DnsInfoType">
    <xs:sequence>
      <xs:element name="PrimaryDNS" type="xs:string" />
      <xs:element minOccurs="0" name="SecondaryDNS" type="xs:string" />
      <xs:element minOccurs="0" name="TertiaryDNS" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Virtual Machine Information Schema

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VsmGlobalConfig">
    <xs:complexType>
      <xs:all>
        <xs:element minOccurs="0" name="VMInfo" type="VMInfoType" />
      </xs:all>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="VMInfoType">
    <xs:sequence>
      <xs:element name="VNICS" type="VNICSType" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="VNICSType">
    <xs:sequence>
      <xs:element name="VNIC" type="VNICType" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="VNICType">
    <xs:sequence>
      <xs:element name="Id" type="xs:string" />
      <xs:element name="Name" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```
Security Groups Schema

This schema details Security Group configuration and management via REST API.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

<xs:element name="VsmGlobalConfig">
    <xs:complexType>
        <xs:all>
            <xs:element minOccurs="0" name="SecurityGroups" type="SecurityGroups" />
        </xs:all>
    </xs:complexType>
</xs:element>

<xs:complexType name="SecurityGroups">
    <xs:choice>
        <xs:element name="SecurityGroup" type="SecurityGroup" maxOccurs="unbounded" />
        <xs:element name="SecurityGroupIdList" type="SecurityGroupIdList" />
    </xs:choice>
</xs:complexType>

<xs:complexType name="SecurityGroup">
    <xs:sequence>
        <xs:element name="SecurityGroupBaseNode" type="xs:string" />
        <xs:element name="SecurityGroupName" type="xs:string" />
        <xs:element name="SecurityGroupId" type="xs:string" minOccurs="0" />  
        <xs:element name="SecurityGroupNodeList" type="NodeList" />  
        <xs:element name="SecurityGroupIPList" type="IPList" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="SecurityGroupIdList">
    <xs:sequence>
        <xs:element name="SecurityGroupId" type="xs:string" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="IPList">
    <xs:sequence>
        <xs:element name="IP" type="xs:string" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="NodeList">
    <xs:sequence>
        <xs:element name="Node" type="SecurityGroupNode" maxOccurs="unbounded" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="SecurityGroupNode">
    <xs:sequence>
        <xs:element name="Id" type="xs:string" />
        <xs:element name="Name" type="xs:string" minOccurs="0" />
        <xs:element name="IPList" type="IPList" minOccurs="0" />
    </xs:sequence>
</xs:complexType>

</xs:schema>
```
ESX Host Preparation and Uninstallation Schema

This schema can be used to install or uninstall vShield App, Port Group Isolation, and vShield Endpoint services on an ESX host.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="VshieldConfiguration">
    <xs:complexType>
      <xs:all>
        <xs:element minOccurs="0" name="VszInstallParams" type="VszInstallParams"/>
        <xs:element minOccurs="0" name="PortgroupIsolationInstallParams" type="PortgroupIsolationInstallParams"/>
        <xs:element minOccurs="0" name="EpsecInstallParams" type="xs:boolean"/>
        <xs:element name="InstallAction" type="InstallAction"/>
          <!-- InstallAction to be taken on appliance - install/upgrade -->
        <xs:element name="InstallStatus" type="InstallStatus"/>
          <!-- only in response -->
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="InstallStatus">
    <xs:sequence>
      <xs:element minOccurs="0" name="ProgressState" type="xs:string"/>
      <xs:element minOccurs="0" name="ProgressSubState" type="xs:string"/>
      <xs:element minOccurs="0" name="InstalledServices" type="InstalledServices"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="InstalledServices">
    <xs:sequence>
      <xs:element name="VszInstalled" type="xs:boolean"/>
      <xs:element name="PortgroupIsolationInstalled" type="xs:boolean"/>
      <xs:element name="EpsecInstalled" type="xs:boolean"/>
    </xs:sequence>
  </xs:complexType>

  <!-- Install parameters -->
  <xs:complexType name="VszInstallParams">
    <xs:sequence>
      <xs:element name="DatastoreId" type="Moid"/>
      <xs:element name="ManagementPortSwitchId" type="xs:string"/>
        <!-- contains the networkId of the mgmt portgroup -->
      <xs:element name="MgmtInterface" type="MgmtInterfaceType"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="MgmtInterfaceType">
    <xs:sequence>
      <xs:element name="IpAddress" type="IP"/>
      <xs:element name="NetworkMask" type="IP"/>
      <xs:element name="DefaultGw" type="IP"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="PortgroupIsolationInstallParams">
    <xs:sequence>
      <xs:element minOccurs="0" name="ResourcePoolId" type="Moid"/>
      <xs:element name="DatastoreId" type="Moid"/>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="InstallAction">
    <xs:restriction base="xs:string">
      <xs:enumeration value="install"/>
      <xs:enumeration value="upgrade"/>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```
vShield App Schemas

The following schemas detail vShield App configuration via REST API.

vShield App Configuration Schema

This schema configures a vShield App after installation.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="ZonesConfiguration">
    <xs:complexType>
      <xs:all>
        <xs:element name="VszInstallParams" type="VszInstallParams" minOccurs="0"/>
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="VszInstallParamsType">
    <xs:sequence>
      <xs:element name="NodeId" type="xs:string"/>
      <xs:element name="DatacenterId" type="xs:string"/>
      <xs:element name="DatastoreId" type="xs:string"/>
      <xs:element name="NameForZones" type="xs:string"/>
      <xs:element name="VswitchForMgmt" type="xs:string"/>
      <xs:element name="MgmtInterface" type="InterfaceType"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="InterfaceType">
    <xs:sequence>
      <xs:element name="IpAddress" type="xs:NMTOKEN"/>
      <xs:element name="NetworkMask" type="xs:NMTOKEN"/>
      <xs:element name="DefaultGw" type="xs:NMTOKEN"/>
      <xs:element minOccurs="0" name="VlanTag" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

vShield App Firewall Schema

This schema configures the firewall rules enforced by a vShield App.

```xml
<?xml version="1.0" encoding="UTF-8"?>
```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
  <xs:element name="vshieldZonesFirewallConfiguration">
    <xs:complexType>
      <xs:choice>
        <xs:element name="ContainerAssociation" type="vmw:ContainerAssociation"/>
        <xs:element name="RuleSet" type="vmw:RuleSet"/>
      </xs:choice>
      <xs:element name="SnapshotTimeStamps" type="TimeStamps"/>
      <xs:element name="StatusMessage" type="xs:string" minOccurs="1"/>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="ContainerAssociation">
    <xs:sequence>
      <xs:element maxOccurs="unbounded" name="Container" type="vmw:Container"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="Container">
    <xs:sequence>
      <xs:element name="InstanceId" type="xs:string"/>
      <xs:element name="Name" type="xs:string"/>
      <xs:element name="IPAddress" type="xs:string"/>
    </xs:sequence>
    <xs:attribute name="id" use="required" type="xs:string"/>
  </xs:complexType>
  <xs:complexType name="RuleSet">
    <xs:sequence>
      <xs:element maxOccurs="unbounded" ref="vmw:Rule"/>
    </xs:sequence>
  </xs:complexType>
  <xs:element name="Rule">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="ID" type="xs:integer"/>
        <xs:element name="Precedence" type="xs:string"/>
        <xs:element name="Position" type="xs:integer"/>
        <xs:element ref="Source"/>
        <xs:element ref="Destination"/>
        <xs:element name="SourcePorts" type="xs:NMTOKEN"/>
        <xs:element ref="Application"/>
        <xs:element name="DestinationPorts" type="xs:NMTOKEN"/>
        <xs:element name="Protocol" type="xs:string"/>
        <xs:element name="Action" type="xs:string"/>
        <xs:element name="Log" type="xs:boolean"/>
        <xs:element name="Notes" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="Source">
    <xs:complexType>
      <xs:attribute name="exclude" use="required" type="xs:boolean"/>
      <xs:attribute name="ref" use="required" type="xs:string"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="Destination">
    <xs:complexType>
      <xs:attribute name="exclude" use="required" type="xs:boolean"/>
      <xs:attribute name="ref" use="required" type="xs:string"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
Port Group Isolation Management Schema

The following schema details Port Group Isolation management via REST API.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VShieldPortgroupIsolationConfig">
    <xs:complexType>
      <xs:choice>
        <xs:element name="PortgroupIsolation" type="PortgroupIsolationType" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="PortgroupIsolationType">
    <xs:sequence>
      <xs:element name="resourcePoolId" type="xs:string" />
      <xs:element name="dataStoreId" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Port Group Isolation Statistics Schema

This schema can be used to retrieve the Port Group Isolation statistics from an ESX host.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VShieldPortgroupIsolationConfig">
    <xs:complexType>
      <xs:choice>
        <xs:element name="StatsLocation" type="xs:string" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

vShield Edge Schemas

The following schemas detail vShield Edge installation and configuration.
Base vShield Edge Configuration Schema

This schema represents the base of the entire vShield Edge schema. The sections that follow detail each element from this schema.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VShieldEdgeConfig">
    <xs:complexType>
      <xs:all>
        <xs:element minOccurs="0" name="GlobalConfig" type="GlobalConfig"/>
        <xs:element minOccurs="0" name="DHCPConfig" type="DHCPConfig"/>
        <xs:element minOccurs="0" name="NATConfig" type="NATConfig"/>
        <xs:element minOccurs="0" name="LoadBalancerConfig" type="LoadBalancerConfig"/>
        <xs:element minOccurs="0" name="FirewallConfig" type="FirewallConfig"/>
        <xs:element minOccurs="0" name="InstallParams" type="InstallParams"/>
        <xs:element minOccurs="0" name="VPNConfig" type="VPNConfig"/>
        <xs:element minOccurs="0" name="TrafficStats" type="TrafficStats"/>
        <xs:element minOccurs="0" name="TechSupportLogsLocation" type="TechSupportLogsLocation"/>
      </xs:all>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

vShield Edge Installation and Upgrade Schema

This schema installs or upgrades a vShield Edge in a port group on an ESX host. You can install one vShield Edge per port group with an attached NIC.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VShieldEdgeConfig">
    <xs:complexType>
      <xs:all minOccurs="0">
        <xs:element name="InstallParams" type="InstallParams"/>
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="InstallParams">
    <xs:sequence>
      <xs:element name="operationMode">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:pattern value="routing"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="resourcePoolId" type="Moid"/>
      <xs:element name="hostId" type="Moid"/>
      <xs:element name="dataStoreId" type="Moid"/>
      <xs:element name="InternalInterface" type="Interface"/>
      <xs:element name="ExternalInterface" type="Interface"/>
      <xs:element name="enablePortgroupIsolation" type="xs:boolean" minOccurs="0"/>
      <xs:element name="InstallStatus" type="xs:string" minOccurs="0"/> <!-- Only in response -->
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="Interface">
    <xs:sequence>
      <xs:element name="networkId" type="Moid"/>
      <xs:element name="networkAddress" type="IP"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```
vShield Edge Global Configuration Schema

This schema represents the global configuration of a vShield Edge instance.

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

<xs:element name="VShieldEdgeConfig">
  <xs:complexType>
    <xs:choice>
      <xs:element ref="GlobalConfig" />
    </xs:choice>
  </xs:complexType>
</xs:element>

<!-- In Response from server for querying config on Edge -->
<xs:complexType name="GlobalConfig">
  <xs:sequence>
    <xs:element name="operationMode" type="OpMode" />
    <xs:element name="InternalInterface" type="Interface" />
    <xs:element name="ExternalInterface" type="Interface" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="Interface">
  <xs:sequence>
    <xs:element name="networkId" type="Moid" />
    <xs:element name="networkAddress" type="IP" />
    <xs:element name="subnetMask" type="IP" />
    <xs:element minOccurs="0" name="defaultGw" type="NMTOKEN" /> <!--Used only for External Interface -->
  </xs:sequence>
</xs:complexType>

<xs:simpleType name="OpMode">
  <xs:restriction base="xs:string">
    <xs:pattern value="routing|bridging"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IP">
  <xs:restriction base="xs:string">
    <xs:pattern value="((25[0-5]|2[0-4]\d|1\d\d|\d)\.){3}(25[0-5]|2[0-4]\d|1\d\d|\d)"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="Moid">
  <xs:restriction base="xs:string">
    <xs:pattern value="[a-zA-Z0-9\-]+"/>
  </xs:restriction>
</xs:simpleType>
vShield Edge CLI Login Credentials Schema

This schema manages the login credentials for the CLI on a vShield Edge.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VShieldEdgeConfig">
    <xs:complexType>
      <xs:all minOccurs="0">
        <xs:element name="CLILoginCredentials" type="CLILoginCredentials"/>
      </xs:all>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="CLILoginCredentials">
    <xs:sequence>
      <xs:element name="username">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="33" />
            <xs:pattern value="[a-z][a-z0-9_]*"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="password">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:pattern value="[^\s]+"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

vShield Edge Firewall Schema

This schema configures the firewall rules for a node.

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <xs:element name="VShieldEdgeConfig">
    <xs:complexType>
      <xs:element name="FirewallConfig" type="FirewallConfig"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```
<xs:choice>
  <xs:element name="defaultPolicy">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:pattern value="allow|deny"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element> <!-- Request/Response for -->
  <xs:element maxOccurs="unbounded" name="FirewallRule" type="FirewallRule" />
  <!-- Request/Response from Client -->
  <xs:element maxOccurs="unbounded" name="FirewallRuleStats" type="FirewallRuleStats" /> <!-- Response from Client -->
  <xs:element name="Snapshots" type="Snapshots" />
  <!-- Only in Response from Server -->
</xs:choice>
</xs:complexType>

<xs:complexType name="FirewallRule">
  <xs:sequence>
    <xs:element name="protocol" type="PROTOCOL" />
    <xs:element minOccurs="0" name="icmpType" type="IcmpType" />
    <!-- Mandatory only when protocol=icmp -->
    <xs:element name="sourceIpAddress" type="IpInfo" />
    <xs:element minOccurs="0" name="sourcePort" type="PortInfo" />
    <xs:element name="destinationIpAddress" type="IpInfo" />
    <xs:element minOccurs="0" name="destinationPort" type="PortInfo" />
    <xs:element name="direction">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value="in|out|both"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="action">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value="allow|deny"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element minOccurs="0" name="log" type="xs:boolean" />
    <xs:element minOccurs="0" name="ruleId" type="xs:unsignedInt" />
    <!-- only in Response from REST server -->
  </xs:sequence>
</xs:complexType>

<xs:complexType name="FirewallRuleStats">
  <xs:sequence>
    <xs:element name="FirewallRule" type="FirewallRule" />
    <xs:element name="packetCount" type="xs:unsignedInt" />
    <xs:element name="byteCount" type="xs:unsignedInt" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="IpInfo">
  <xs:choice>
    <xs:element name="ipAddress" type="IpOrAny" />
    <xs:element name="IpRange" type="IpRange" />
  </xs:choice>
</xs:complexType>

<xs:complexType name="IpRange">
  <xs:sequence>
    <xs:element name="rangeStart" type="IP" />
    <xs:element name="rangeEnd" type="IP" />
  </xs:sequence>
</xs:complexType>
<xs:complexType name="PortInfo">
  <xs:choice>
    <xs:element name="port" type="PortOrAny" />
    <xs:element name="PortRange" type="PortRange" />
  </xs:choice>
</xs:complexType>

<xs:complexType name="PortRange">
  <xs:sequence>
    <xs:element name="rangeStart" type="PORT" />
    <xs:element name="rangeEnd" type="PORT" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="Snapshots">
  <xs:sequence>
    <xs:element maxOccurs="unbounded" name="timestamp" type="xs:unsignedInt" />
  </xs:sequence>
</xs:complexType>

<xs:simpleType name="IP">
  <xs:restriction base="xs:string">
    <xs:pattern value="((25\[0-5]\|2[0-4][0-9]\|1[0-9][0-9]\|1[0-9]?)\(0-9\))\.
[3](25\[0-5]\|2[0-4][0-9]\|1[0-9][0-9]\|0-9))]" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IpOrAny">
  <xs:restriction base="xs:string">
    <xs:pattern value="(((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|1[0-9])\(0-9\))\.
[3](25[0-5]|2[0-4][0-9]|1[0-9][0-9]|1-9])?0-9))\(any\)" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PORT">
  <xs:restriction base="xs:string">
    <xs:pattern value="((6[0-5]|6-3][0-9]\|0-9)|[0-9][0-9]|0-9)\(0-9]](0-9)]" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PortOrAny">
  <xs:restriction base="xs:string">
    <xs:pattern value="((6[0-5][0-5]|6-3][0-9]|0-9)\|0-9)](0-9)](0-9)](0-9)](0-9)](any)" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PROTOCOL">
  <xs:restriction base="xs:string">
    <xs:pattern value="tcp|udp|icmp|any" />
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IcmpType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="echo-reply"/>
    <xs:enumeration value="destination-unreachable"/>
    <xs:enumeration value="source-quench"/>
    <xs:enumeration value="redirect"/>
    <xs:enumeration value="echo-request"/>
    <xs:enumeration value="router-advertisement"/>
    <xs:enumeration value="router-solicitation"/>
    <xs:enumeration value="time-exceeded"/>
    <xs:enumeration value="parameter-problem"/>
    <xs:enumeration value="timestamp-request"/>
    <xs:enumeration value="timestamp-reply"/>
    <xs:enumeration value="address-mask-request"/>
  </xs:restriction>
</xs:simpleType>
NAT Schema

This schema configures SNAT and DNAT rules for a node.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VShieldEdgeConfig">
    <xs:complexType>
      <xs:all minOccurs="0">
        <xs:element name="NATConfig" type="NATConfig"/>
      </xs:all>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="NATConfig">
    <xs:choice>
      <xs:element maxOccurs="unbounded" name="NATRule" type="NATRule"/>
      <xs:element maxOccurs="unbounded" name="NATRuleStats" type="NATRuleStats"/>
      <xs:element name="Snapshots" type="Snapshots"/>
    </xs:choice>
  </xs:complexType>
  <xs:complexType name="NATRule">
    <xs:sequence>
      <xs:element minOccurs="0" name="protocol" type="PROTOCOL"/>
      <xs:element minOccurs="0" name="icmpType" type="IcmpType"/>
      <xs:element name="internalIpAddress" type="IpInfo"/>
      <xs:element minOccurs="0" name="internalPort" type="PortInfo"/>
      <xs:element name="externalIpAddress" type="IpInfo"/>
      <xs:element minOccurs="0" name="externalPort" type="PortInfo"/>
      <xs:element minOccurs="0" name="log" type="xs:boolean"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="NATRuleStats">
    <xs:sequence>
      <xs:element name="NATRule" type="NATRule"/>
      <xs:element name="packetCount" type="xs:unsignedInt"/>
      <xs:element name="byteCount" type="xs:unsignedInt"/>
      <xs:element name="ingressInterface" type="xs:string"/>
      <xs:element name="egressInterface" type="xs:string"/>
      <xs:element minOccurs="0" name="srcIpForRule" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="IpInfo">
    <xs:choice>
      <xs:element name="ipAddress" type="IpOrAny"/>
      <xs:element name="IpRange" type="IpRange"/>
    </xs:choice>
  </xs:complexType>
  <xs:complexType name="IpRange">
    <xs:sequence>
      <xs:element name="rangeStart" type="IP"/>
      <xs:element name="rangeEnd" type="IP"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```
DHCP Schema

This schema defines the structure of DHCP.

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

<xs:element name="VShieldEdgeConfig">
  <xs:complexType>
    <xs:element name="DHCPConfig" type="DHCPConfig"/>
  </xs:complexType>
</xs:element>

<xs:complexType name="DHCPConfig">
  <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" name="DHCPBinding" type="DHCPBinding"/>
    <xs:element minOccurs="0" maxOccurs="unbounded" name="DHCPPool" type="DHCPPool"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="DHCPBinding">
  <xs:sequence>
    <xs:element name="vmId" type="Moid"/>
    <xs:element name="interfaceId">
      <xs:simpleType>
        <xs:restriction base="xs:unsignedInt">
          <xs:minInclusive value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="hostName">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value="((\[A-Za-z0-9\]-\[A-Za-z0-9\]-\[A-Za-z0-9\]\-\-\[A-Za-z0-9\]+)\*\(\.)\{0,1\})*\[A-Za-z0-9\]+"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="internalIPAddress" type="IP"/>
    <xs:element minOccurs="0" name="DHCPConfigParams" type="DHCPConfigParams"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="DHCPPool">
  <xs:sequence>
    <xs:element name="PoolRange" type="IpRange"/>
    <xs:element minOccurs="0" name="DHCPConfigParams" type="DHCPConfigParams"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="DHCPConfigParams">
  <xs:sequence>
    <xs:element minOccurs="0" name="domainName">
      <xs:simpleType>
        <xs:restriction value="any"/>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
</xs:schema>
VPN Schema

This schema configures VPN parameters for a node.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="VShieldEdgeConfig">
    <xs:complexType>
      <xs:all minOccurs="0">
        <xs:element name="VPNConfig" type="VPNConfig"/>
      </xs:all>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="VPNConfig">
    <xs:choice>
      <xs:element name="IpsecVPNConfig" type="IpsecVPNConfig"/>
      <xs:element minOccurs="0" name="Snapshots" type="Snapshots"/>
    </xs:choice>
  </xs:complexType>
</xs:schema>
```
<xs:complexType name="IpsecVPNConfig">
  <xs:choice>
    <xs:element minOccurs="0" name="SiteToSiteIpsec" type="SiteToSiteIpsec" />
    <xs:element minOccurs="0" name="IpsecService" type="xs:string" />
  </xs:choice>
</xs:complexType>

<xs:complexType name="SiteToSiteIpsec">
  <xs:choice>
    <xs:element name="VPNServerConfig" type="VPNServerConfig" />
    <xs:element maxOccurs="unbounded" name="VPNSite" type="VPNSite" />
  </xs:choice>
</xs:complexType>

<xs:complexType name="VPNServerConfig">
  <xs:sequence>
    <xs:element name="externalIpAddress" type="IP" />
    <xs:element minOccurs="0" name="natedPublicIpAddress" type="IP" />
    <xs:element minOccurs="0" name="log" type="xs:boolean" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="VPNSite">
  <xs:sequence>
    <xs:element minOccurs="0" name="Configuration" type="VPNSiteConfig" />
    <xs:element minOccurs="0" maxOccurs="unbounded" name="VPNTunnel" type="VPNTunnel" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="VPNSiteConfig">
  <xs:sequence>
    <xs:element name="siteName">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value="[a-zA-Z0-9_]*"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="remoteEndPointexternalIpAddress" type="IP" />
    <xs:element name="sharedSecret">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="mtu">
      <xs:simpleType>
        <xs:restriction base="xs:unsignedInt">
          <xs:minInclusive value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="VPNTunnel">
  <xs:sequence>
    <xs:element minOccurs="0" name="Configuration" type="VPNTunnelConfig" />
    <xs:element minOccurs="0" name="DetailedConfiguration" type="VPNTunnelDetailedConfig"/>
  </xs:sequence>
</xs:complexType>
<xs:element minOccurs="0" name="Status" type="VPNTunnelStatus"/>
<!-- Response from REST server for Query Connection Status -->
</xs:sequence>
</xs:complexType>

<xs:complexType name="VPNTunnelConfig">
<xs:sequence>
<xs:element name="tunnelName">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:pattern value="[a-zA-Z0-9_]+"/> <!-- tunnelName should contain only alphanumeric characters -->
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="remoteSiteSubnet" type="CIDR"/>
<xs:element name="encryptionAlgorithm">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:pattern value="aes|3des"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>

<xs:complexType name="VPNTunnelDetailedConfig">
<xs:sequence>
<xs:element name="mode" type="xs:string"/>
<xs:element name="auto" type="xs:string"/>
<xs:element name="authby" type="xs:string"/>
<xs:element name="aggremode" type="xs:string"/>
<xs:element name="ikeLifeTime" type="xs:unsignedInt"/>
<xs:element name="ike" type="xs:string"/>
<xs:element name="keyexchange" type="xs:string"/>
<xs:element name="pfs" type="xs:string"/>
<xs:element name="esp" type="xs:string"/>
<xs:element name="saLifeTime" type="xs:unsignedInt"/>
<xs:element name="dpddelay" type="xs:unsignedInt"/>
<xs:element name="dpdtimeout" type="xs:unsignedInt"/>
<xs:element name="dpdaction" type="xs:string"/>
<xs:element name="NetworkEndpointsConfig" type="NetworkEndpointsConfig"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="VPNTunnelStatus">
<xs:sequence>
<xs:element name="policy" type="xs:string"/>
<xs:element name="mode" type="xs:string"/>
<xs:element name="ikeLife" type="xs:unsignedInt"/>
<xs:element name="ipsecLife" type="xs:unsignedInt"/>
<xs:element name="NetworkEndpointsConfig" type="NetworkEndpointsConfig"/>
<xs:element name="VseToRemoteSiteStats" type="VPNStats"/>
<xs:element name="RemoteSiteToVseStats" type="VPNStats"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="VPNStats">
<xs:sequence>
<xs:element name="fromPort" type="xs:unsignedInt"/>
<xs:element name="toPort" type="xs:unsignedInt"/>
<xs:element name="protocol" type="xs:string"/>
<xs:element name="spi" type="xs:string"/>
<xs:element name="reqid" type="xs:string"/>
<xs:element name="encryption" type="xs:string"/>
<xs:element name="authentication" type="xs:string"/>
<xs:element name="packets" type="xs:unsignedInt"/>
<xs:element name="bytes" type="xs:unsignedInt"/>
</xs:sequence>
</xs:complexType>
Load Balancer Schema

This schema configures load balancer parameters for a node. You can configure load balancer listeners and the load balancing algorithm.

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

<x:schema name="VShieldEdgeConfig">
  <xs:complexType>
    <xs:element ref="LoadBalancerConfig" />
  </xs:complexType>
</xs:schema>

<x:schema name="LoadBalancerConfig">
  <xs:choice>
    <xs:element name="LoadBalancerService" type="xs:string" />
    <xs:element maxOccurs="unbounded" name="Listener" type="Listener" />
  </xs:choice>
</xs:schema>

<x:schema name="Listener">
  <xs:sequence>
    <xs:element name="externalIPAddress" type="IP" />
    <xs:element name="BackEndServers" type="BackEndServers" />
  </xs:sequence>
</xs:schema>
MTU Threshold Schema

This schema configures the MTU threshold for the External and Internal interfaces of a vShield Edge.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xs:element name="VShieldEdgeConfig">
        <xs:complexType>
            <xs:all minOccurs="0">
                <xs:element name="MTU" type="MTU"/>
            </xs:all>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="MTU">
        <xs:sequence>
            <xs:element minOccurs="0" maxOccurs="1" name="internalInterfaceMTU" type="xs:unsignedInt"/>
            <xs:element minOccurs="0" maxOccurs="1" name="externalInterfaceMTU" type="xs:unsignedInt"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```
Traffic Stats Schema

This schema configures the Traffic Stats collection service for a node.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xs:element name="VShieldEdgeConfig">
        <xs:complexType>
            <xs:all minOccurs="0">
                <xs:element name="TrafficStats" type="TrafficStats"/>
            </xs:all>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="TrafficStats">
        <xs:sequence>
            <xs:element maxOccurs="unbounded" name="StatsRecord" type="StatsRecord"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="StatsRecord">
        <xs:sequence>
            <xs:element name="ipAddress" type="xs:NMTOKEN"/>
            <xs:element minOccurs="0" name="timeStamp" type="xs:unsignedInt"/>
            <xs:element minOccurs="0" name="txPacketCount" type="xs:unsignedInt"/>
            <xs:element minOccurs="0" name="rxPacketCount" type="xs:unsignedInt"/>
            <xs:element minOccurs="0" name="txByteCount" type="xs:unsignedInt"/>
            <xs:element minOccurs="0" name="rxByteCount" type="xs:unsignedInt"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

Syslog Schema

This schema enables connection from a vShield Edge to a syslog server.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xs:element name="VShieldEdgeConfig">
        <xs:complexType>
            <xs:all minOccurs="0">
                <xs:element name="SyslogServerConfig" type="SyslogServerConfig"/>
            </xs:all>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="SyslogServerConfig">
        <xs:choice>
            <xs:element minOccurs="1" maxOccurs="2" name="ipAddress" type="IP"/>
            <xs:element name="Snapshots" type="Snapshots"/>
        </xs:choice>
    </xs:complexType>

    <xs:simpleType name="IP">
        <xs:restriction base="xs:string">
            <xs:pattern value="((25[0-5]|2[0-4]\d|1\d{2}|[1-9]\d|\d)\.(25[0-5]|2[0-4]\d|1\d{2}|[1-9]\d|\d)){3}(25[0-5]|2[0-4]\d|1\d{2}|[1-9]\d|\d)"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="Snapshots">
        <xs:sequence>
            <xs:element maxOccurs="unbounded" name="timestamp" type="xs:unsignedInt"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```
Error Message Schema

This schema details error messages.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="Errors">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="unbounded" name="Error" type="ErrorType"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

If a REST API call results in an error, the HTTP reply contains the following information.

- An XML error document as the response body
- Content-Type: application/xml
- An appropriate 2xx, 4xx, or 5xx HTTP status code

Table 8-1. Error Message Status Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>The request was valid and has been completed. Generally, this response is accompanied by a body document (XML).</td>
</tr>
<tr>
<td>204 No Content</td>
<td>Same as 200 OK, but the response body is empty (No XML).</td>
</tr>
<tr>
<td>400 Bad Request</td>
<td>The request body contains an invalid representation or the representation of the entity is missing information. The response is accompanied by Error Object (XML).</td>
</tr>
<tr>
<td>401 Unauthorized</td>
<td>An authorization header was expected. Request with invalid or no vShield Manager Token.</td>
</tr>
<tr>
<td>403 Forbidden</td>
<td>The user does not have enough privileges to access the resource.</td>
</tr>
<tr>
<td>404 Not Found</td>
<td>The resource was not found. The response is accompanied by Error Object (XML).</td>
</tr>
<tr>
<td>500 Internal Server Error</td>
<td>Unexpected error with the server. The response is accompanied by Error Object (XML).</td>
</tr>
<tr>
<td>503 Service Unavailable</td>
<td>Cannot proceed with the request, because some of the services are unavailable. Example: vShield Edge is Unreachable. The response is accompanied by Error Object (XML).</td>
</tr>
</tbody>
</table>
Index

C
CLI, manage vShield Edge credentials 25

D
debug, Port Group Isolation 20
debugging a vShield Edge 47
DHCP
    about 25
    configuring 26
    delete configuration 27
    get configuration by timestamp 27
    hosts and pools 26
    last 10 configurations 27
    revert to configuration by timestamp 27
    server status 25
    start, stop, or restart service 25
disabling Port Group Isolation 20
DNAT
    about 30
    delete configuration 33
    get configuration by timestamp 33
    get rule set 30
    last 10 configurations 33
    post rule set 31
    revert to configuration by timestamp 33

E
enabling Port Group Isolation 19
ESX host preparation 15

F
firewall
vShield App
    about 51
    delete configuration 55
    get configuration by timestamp 55
    last 10 configurations 55
    post rule set 52
    revert to configuration by timestamp 55
    view rule set 51
vShield Edge
    about 33
    change the default policy action 35
    default policy status 35
    delete configuration 36
    get configuration by timestamp 36
    get rule set 33
    last 10 configurations 36
post rule set 34
revert to configuration by timestamp 36
view a specific rule 36
forced synchronization 24

I
installation
    Port Group Isolation 15
    status 17
    vShield App 15
    vShield Edge 21
    vShield Endpoint 15
installation parameters of vShield Edge 22

L
Load Balancer
    about 43
    add a listener 44
    delete configuration 46
    get configuration by timestamp 46
    get current configuration 45
    get current configuration of single server 45
    last 10 configurations 45
    revert to configuration by timestamp 46
    server status 43
    start or stop service 44
logs, tech support 14

M
MTU threshold 46

N
NAT
DNAT
    about 30
    delete configuration 33
    get configuration by timestamp 33
    get rule set 30
    last 10 configurations 33
    post rule set 31
    revert to configuration by timestamp 33
SNAT
    about 28
    delete configuration 30
    get configuration by timestamp 30
    get rule set 28
    last 10 configurations 30
    post rule set 28
    revert to configuration by timestamp 30
### Port Group Isolation
- **debug statistics**: 20
- **disable**: 20
- **enable**: 19
- **install**: 15
- **uninstall**: 18
- **preparing the ESX host**: 15

### Security Groups
- **about**: 56
- **adding**: 56
  - adding a virtual machine: 57
  - deleting a security group: 59
  - deleting a VM from a group: 58
- **deleting all security group**: 59
- **get details**: 58
- **get IP address details**: 58
- **get list of**: 57
- **get properties of a VM**: 58

### SNAT
- **about**: 28
  - delete configuration: 30
  - get configuration by timestamp: 30
  - get rule set: 28
  - last 10 configurations: 30
  - post rule set: 28
  - revert to configuration by timestamp: 30

### Port Group Isolation installation: 17
- **vShield App installation**: 17
- **vShield Endpoint installation**: 17

### SVM
- **get network info**: 62
- **registering with vShield Endpoint**: 61
- **retrieve status**: 63
- **unregistering**: 63

### Syslog
- **about**: 48
- **vShield App**: 59
- **vShield Edge**: 49
  - delete configuration: 49
  - get configuration by timestamp: 49
  - get current configuration: 48
  - last 10 configurations: 48
  - post a configuration: 48
  - revert to configuration by timestamp: 49

### tech support logs: 14

### traffic statistics for a vShield Edge: 47

### Uninstall vShield: 17
- **uninstallation**: 17
- **uninstalling a vShield**: 17
- **unregistering a vShield Endpoint SVM**: 63
- **upgrading a vShield Edge**: 24

### VPN
- **about**: 37
  - add a site: 39
  - add tunnels for a site: 40
  - delete a site: 41
  - delete a tunnel for a site: 41
  - delete configuration: 42
  - get configuration by timestamp: 42
  - get current configuration: 41
  - get the detailed configuration: 40
get the detailed configuration for a site 41
get the detailed configuration for a tunnel 41
last 10 configurations 42
post configuration 38
revert to configuration by timestamp 42
server status 38
start or stop service 38

vShield
about 9
uninstalling 17

vShield App
about 9

firewall
about 51
delete configuration 55
get configuration by timestamp 55
last 10 configurations 55
post rule set 52
revert to configuration by timestamp 55
view rule set 51

install 15

Security Groups
about 56
adding 56
adding a virtual machine 57
deleting a security group 59
deleting a VM from a group 58
deleting all security group 59
get details 58
get IP address details 58
get list of 57
get properties of a VM 58

Syslog 59
uninstall 18

vShield Edge
about 10

CLI credentials 25
debugging 47

DHCP
about 25
configuring 26
delete configuration 27
get all hosts and pools 26
get configuration by timestamp 27
last 10 configurations 27
revert to configuration by timestamp 27
start, stop, or restart 25
status 25

DNAT
about 30
delete configuration 33
get configuration by timestamp 33
get rule set 30
last 10 configurations 33
post rule set 31
revert to configuration by timestamp 33

firewall
about 33
change the default policy action 35
default policy status 35
delete configuration 36
get configuration by timestamp 36
get rule set 33
last 10 configurations 36
post rule set 34
revert to configuration by timestamp 36
view a specific rule 36

force sync with vShield Manager 24
get traffic statistics 47
installation 21
installation parameters 22

Load Balancer
about 43
add a listener 44
delete configuration 46
get configuration by timestamp 46
get current configuration 45
get current configuration of single server 45
last 10 configurations 45
revert to configuration by timestamp 46
start or stop service 44
status 43

MTU threshold 46

NAT
about 28

SNAT
about 28
delete configuration 30
get configuration by timestamp 30
get rule set 28
last 10 configurations 30
post rule set 28
revert to configuration by timestamp 30

Syslog
about 48
delete configuration 49
get configuration by timestamp 49
get current configuration 48
last 10 configurations 48
post a configuration 48
revert to configuration by timestamp 49

tech support log 14
uninstallation 22
upgrading 24

VPN
about 37
add a site 39
add tunnels for a site 40
delete a site 41
delete a tunnel for a site 41
delete configuration 42
get configuration by timestamp 42
generate current configuration 41
get the detailed configuration 40
get the detailed configuration for a site 41
get the detailed configuration for a tunnel 41
last 10 configurations 42
post configuration 38
revert to configuration by timestamp 42
start or stop service 38
status 38

vShield Endpoint
  about 10
  error schema 64
  get SVM network info 62
  install 15
  managing 61
  registering an SVM 61
  retrieve SVM status 63
  uninstall 18
  uninstalling 63
  unregistering an SVM 63

vShield Manager
  about 9
  configure DNS 13
  force sync with vShield Edge 24
  sync with vCenter 13
  tech support log 14

vShield Zones
  vShield 9
  vShield Manager 9