



Firefly Suite

Getting Started Guide



Published: 2014-01-13

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2014, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Firefly Suite Getting Started Guide

Copyright © 2014, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Documentation Conventions	x
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xiii
Part 1	The Firefly Suite Solution	
Chapter 1	Introduction to the Firefly Suite Solution	3
	Understanding Firefly Suite	3
	Understanding Firefly Host for the Firefly Suite Solution	4
	Understanding Firefly Perimeter for the Firefly Suite Solution	6
	Understanding Junos Space Virtual Director for the Firefly Suite Solution	7
	Understanding the Firefly Suite Solution Use Cases	9
	Firefly Suite Solution Use Cases Structure	10
Part 2	Firefly Suite Solution Use Cases	
Chapter 2	Firefly Suite Solution Public Cloud Use Case	15
	Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology	15
	Public Cloud Tenant Customer Requirements	17
	Public Cloud Software and Hardware Requirements	17
	Understanding the Public Cloud Use Case Configurations Summary	19
	Using Firefly Suite Solution with Customer Portals	21
Chapter 3	Firefly Suite Solution Private Cloud Use Case	23
	Understanding the Firefly Suite Solution for the Private Cloud Use Case	23
	Understanding the Private Cloud Use Case Requirements, Topology, and Configuration	24
Chapter 4	Firefly Suite Solution Managed Security Services Use Case	27
	Understanding Firefly Suite and Managed Security Services	27
	Understanding the Managed Security Services Use Case Requirements, Topology, and Configuration	28

Chapter 5	Firefly Suite Solution Junos OS Out-of-the-Box Use Case	31
	Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case	31
	Understanding the Junos OS Out-of-the-Box Use Case Requirements, Topology, and Configuration	32
Part 3	Index	
	Index	37

List of Figures

Part 1	The Firefly Suite Solution	
Chapter 1	Introduction to the Firefly Suite Solution	3
	Figure 1: Firefly Host	5
	Figure 2: Junos Space Virtual Director	8
Part 2	Firefly Suite Solution Use Cases	
Chapter 2	Firefly Suite Solution Public Cloud Use Case	15
	Figure 3: Public Cloud Use Case Topology	16
Chapter 3	Firefly Suite Solution Private Cloud Use Case	23
	Figure 4: Private Cloud Use Case Topology	25
Chapter 4	Firefly Suite Solution Managed Security Services Use Case	27
	Figure 5: Managed Security Services Environment Using Juniper Networks Products	28
	Figure 6: Managed Security Services Use Case Topology	29
Chapter 5	Firefly Suite Solution Junos OS Out-of-the-Box Use Case	31
	Figure 7: Junos OS Out-of-the-Box Use Case Topology	32

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Part 1	The Firefly Suite Solution	
Chapter 1	Introduction to the Firefly Suite Solution	3
	Table 3: Firefly Perimeter Tools Used on VMware and KVM	7
Part 2	Firefly Suite Solution Use Cases	
Chapter 2	Firefly Suite Solution Public Cloud Use Case	15
	Table 4: Firefly Solution Public Cloud Use Case Software Requirements	18
	Table 5: Firefly Solution Hardware Requirements for the Public Cloud Use Case	18

About the Documentation

The *Firefly Suite Getting Started Guide* introduces Firefly Suite and the three products that it includes. This Getting Started Guide also provides common use case examples that explain how to use the Firefly products together to meet your virtualized environment security requirements. The use cases are focused on the VMware infrastructure and hypervisor platform. This guide does not include use cases for the KVM hypervisor platform.

Firefly Suite includes the following products:

- Firefly Host—For details on installing and configuring Firefly Host for VMware, see the *Firefly Host Getting Started Guide for VMware*, the *Firefly Host Installation and Upgrade Guide for VMware*, and the *Firefly Host Administration Guide for VMware*. For details on the Firefly Host SDK API, see the *Firefly Host Cloud Security SDK*.
- Firefly Perimeter—For details on installing and configuring Firefly Perimeter for VMware, see the *Firefly Perimeter Getting Started Guide for VMware*, the *Firefly Perimeter Installation and Upgrade Guide for VMware*, and the *Firefly Perimeter Administration Guide for VMware*. See the *Firefly Perimeter Getting Started Guide for KVM* for details on installing and configuring Firefly Perimeter for KVM.
- Junos Space Virtual Director—For details on provisioning, deploying, and configuring Firefly Perimeter for VMware using Virtual Director, see the *Junos Space Virtual Director Getting Started Guide*. For details on the Virtual Director SDK API, see the *Junos Space Virtual Director RESTful Web Services API Reference*.

Firefly Suite use cases also use Junos Space Security Director. For details on configuring Firefly Perimeter security using the Security Director GUI, see the *Junos Space Security Director User Guide*. For details on using the Security Director API, see the *Junos Space Security Director Restful Web Services API Reference*.

- [Documentation and Release Notes on page ix](#)
- [Documentation Conventions on page x](#)
- [Documentation Feedback on page xi](#)
- [Requesting Technical Support on page xii](#)

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons


Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> <i>RFC 1997, BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at

<https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

The Firefly Suite Solution

CHAPTER 1

Introduction to the Firefly Suite Solution

Firefly Suite allows you to secure your virtualized environment entirely both in the virtualized data center and at the tenant virtual network edge. Firefly Suite is composed of three products—Firefly Host, Firefly Perimeter, and Junos Space Virtual Director. The following topics introduce Firefly Suite and ways in which you can use it to create a security solution for your virtualized environment.

- [Understanding Firefly Suite on page 3](#)
- [Understanding Firefly Host for the Firefly Suite Solution on page 4](#)
- [Understanding Firefly Perimeter for the Firefly Suite Solution on page 6](#)
- [Understanding Junos Space Virtual Director for the Firefly Suite Solution on page 7](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Firefly Suite Solution Use Cases Structure on page 10](#)

Understanding Firefly Suite

Firefly Suite delivers security features that enable you to protect both inter-virtual machine (VM) traffic and traffic between VMs and external networks, including your physical network and the Internet. It is designed to address the need for robust security for diverse virtualized environments. It brings together the following products:

- Firefly Host

Firefly Host is the next rebranded evolution of vGW Series 5.5. It is a hypervisor-based security solution that is purpose-built for the virtualized environment. It protects VMs and their traffic in the virtualized data center.

- Firefly Perimeter

Firefly Perimeter delivers in a VM Junos OS and advanced security for branch SRX Series devices. It protects VM traffic and the virtualized network at the tenant virtual network edge.



NOTE: See the *Firefly Perimeter Getting Started Guide for VMware for Junos OS* features that are not supported by Firefly Perimeter.

- Junos Space Virtual Director

Junos Space Virtual Director allows you to rapidly provision and automatically deploy Firefly Perimeter instances into the VMware vCenter environment. After you deploy Firefly Perimeter, you can use Virtual Director to monitor them and efficiently manage their lifecycle.

Firefly Host and Firefly Perimeter provide proven and rigorous security when used alone for a dedicated purpose and enhanced security across entire virtualized environments when used together.

**Related
Documentation**

- [Understanding Firefly Host for the Firefly Suite Solution on page 4](#)
- [Understanding Firefly Perimeter for the Firefly Suite Solution on page 6](#)
- [Understanding Junos Space Virtual Director for the Firefly Suite Solution on page 7](#)

Understanding Firefly Host for the Firefly Suite Solution

Firefly Host is a comprehensive, hypervisor-based security solution. It is the rebranded evolution of vGW Series 5.5. When used together, Firefly Host and Firefly Perimeter allow you to secure your virtualized environment end-to-end.

- The Firefly Host Dashboard management center gives administrators full visibility into, and granular access control over, all traffic flowing between VMs in the virtualized data center and between VMs and external networks. It allows you to protect inter-VM traffic and restrict traffic flowing into VMs from sources outside the virtualized data center, both from physical devices in your organization and from the Internet. You can also govern traffic flowing from VMs to external destinations, both allowing and restricting it.

The Firefly Host Dashboard allows you to manage the range of features that Firefly Host provides. Firefly Host integrates intrusion detection service (IDS) and antivirus protection for the virtualized environment, and it provides compliance tools.

- Its integrated IDS engine inspects packets for malware and malicious traffic.
- Its antivirus protection provides on-demand and on-access scanning of VM disks and files, with full quarantine capability.
- The Firefly Host stateful firewall provides layers of defense and automated security. It provides access control over all traffic through security policies that define ports, protocols, destinations, and specified VMs to block.

Because virtualized environments can expand to include large numbers of VMs, Firefly Host allows you to define global security policies to apply automatically to all your VMs, group policies to apply to groups of them, and individual policies for individual VMs. Without diminishing your ability to distinguish security for a particular VM, the firewall policy feature allows for maximum flexibility.

- Firefly Host monitors the virtualized environment, sending alerts as appropriate.

You use an open virtual alliance (OVA) file to deploy Firefly Host into VMware. You can use either of the following methods to configure VM security:

- Firefly Host Dashboard—A central management, graphical user interface (GUI) that allows you to configure basic and advanced security features.
- Firefly Host programmatic interface— A set of XML-RPC APIs that implement the Firefly Host security features.

Figure 1 on page 5 shows at a high level the Firefly Host components.

Figure 1: Firefly Host

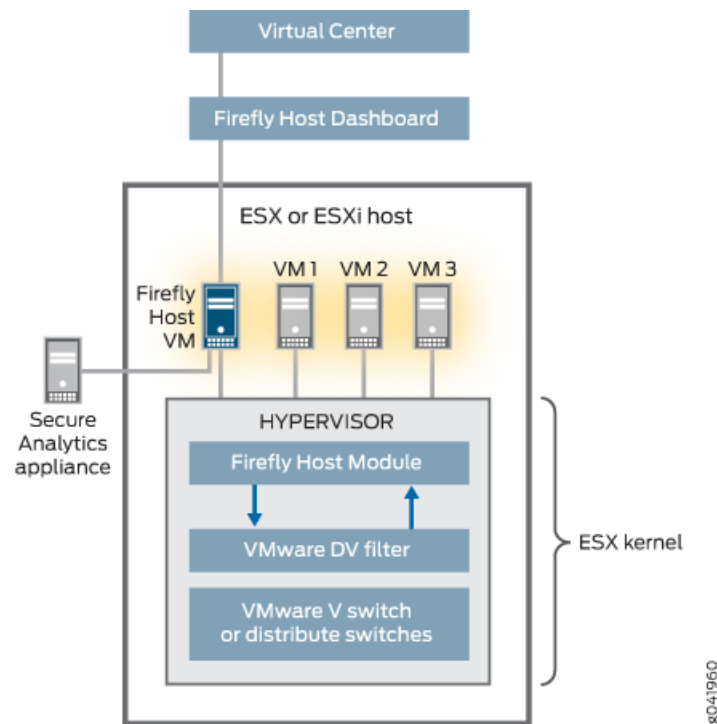


Figure 1 on page 5 illustrates the following Firefly Host components and their relationship to VMware and other devices.

- Firefly Host communicates with VMware to secure and manage the VMs that you create in your VMware virtualized data centers. You deploy a Firefly Host VM for each ESXi host whose VMs you want to secure. Using Firefly Host Dashboard, you can create policies for VMs on an ESXi host and push the policies to the Firefly Host VM installed on that host.

The Firefly Host VM inserts the Firefly Host Module into the hypervisor of an ESXi host that Firefly Host protects. The Firefly Host VM communicates security policies for VMs to the Firefly Host Module. All traffic is analyzed and secured by the Firefly Host Module.

- You can use Firefly Host Dashboard not only to create policies but also to configure many other Firefly Host features including:

- Integrating Firefly Host with Secure Analytics Appliance, formerly STRM, for defense-in-depth control such as centralized logging, event management, and network-wide threat detection.
- Creating SRX zone objects to retrieve a list of zones on an SRX device and select which zones to import into Firefly Host. You can configure zone synchronization to automatically poll an SRX device for zone updates.

Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding Firefly Perimeter for the Firefly Suite Solution on page 6](#)
- [Understanding Junos Space Virtual Director for the Firefly Suite Solution on page 7](#)

Understanding Firefly Perimeter for the Firefly Suite Solution

Firefly Perimeter delivers in a virtual machine (VM) Junos OS and SRX Series advanced security for branch SRX Series devices. It protects VM traffic and the virtualized network at the tenant virtual network edge. When used together, Firefly Perimeter and Firefly Host allow you to secure your virtualized environment from the virtualized data center to the tenant virtual network edge.

Firefly Perimeter runs as a VM on standard x86 servers. You can use Junos Space Virtual Director to configure and deploy Firefly Perimeter instances, unencumbered by the constraints of physical hardware deployment. You can also use the Firefly Perimeter Junos OS J-Web and CLI to deploy and configure Firefly Perimeter.

Some of the benefits that Firefly Perimeter provides for virtualized environments are:

- Stateful firewall protection at the tenant virtual network edge.

You can deploy a Firefly Perimeter instance for each of your tenants. You can configure firewalls that utilize 2-GB RAM, 2-GB disk space, and up to 8 vNICs each.

- Faster deployment of virtual firewalls than is possible with physical systems.

Because Firefly Perimeter is deployed as a VM, you can scale services up or down in public or private cloud environments as required.

- Routing and networking capabilities for virtualized environments.
- Centralized and local management capability.

You can deploy instances of Firefly Perimeter on VMware and KVM hypervisor platforms. This guide focuses on VMware.

[Table 3 on page 7](#) identifies the tools that you can use to deploy, configure, and manage Firefly Perimeter on VMware and on KVM.

Table 3: Firefly Perimeter Tools Used on VMware and KVM

Firefly Perimeter on VMware	Firefly Perimeter on KVM
<p>To deploy Firefly Perimeter on VMware and provision it, you can use the following tools:</p> <ul style="list-style-type: none"> • Junos Space Virtual Director GUI and API • OVA/OVF (open virtualization application/open virtualization format) 	<p>To deploy Firefly Perimeter on KVM, you use a self-extracting Juniper Virtual Appliance (JVA) package.</p> <p>JVA is similar to a VMware OVA file. It runs as a Bash script on Linux systems. It extracts the Firefly Perimeter image and creates a VM for it.</p> <p>NOTE: There are no tools to provision Firefly Perimeter on KVM. Junos Space Virtual Director is not available for Firefly Perimeter at this time.</p>
<p>To secure Firefly Perimeter instances on VMware, you can use the following tools:</p> <ul style="list-style-type: none"> • Junos OS CLI • Junos OS J-Web • Junos Space Security Director GUI and API <p>To manage the lifecycle of Perimeter instances on VMware, you can use the following tool.</p> <ul style="list-style-type: none"> • Junos Space Virtual Director GUI and API 	<p>To secure Firefly Perimeter on KVM, you can use the following tools:</p> <ul style="list-style-type: none"> • Junos OS CLI • Junos OS J-Web • Junos Space Security Director GUI and API
<p>For device management access to Firefly Perimeter on VMware, you can use the following tools:</p> <ul style="list-style-type: none"> • Junos OS CLI for local management • NetConf APIs from an external VM or Junos Space Security Director 	<p>For device management access of Firefly Perimeter on KVM, you can use the following tools:</p> <ul style="list-style-type: none"> • Junos OS CLI for local management • NetConf APIs from an external VM

Firefly Perimeter is used in all use cases covered in this document. Refer to the following figures for examples of where it is deployed: [Figure 3 on page 16](#), [Figure 4 on page 25](#), and [Figure 6 on page 29](#).

Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding Firefly Host for the Firefly Suite Solution on page 4](#)
- [Understanding Junos Space Virtual Director for the Firefly Suite Solution on page 7](#)

Understanding Junos Space Virtual Director for the Firefly Suite Solution

Junos Space Virtual Director allows administrators to automatically provision and deploy Firefly Perimeter instances into the VMware environment. It allow you to monitor the deployed Firefly Perimeter VMs and efficiently manage their lifecycles.

Using Virtual Director, you can create templates that define the parameters and characteristics that a VM requires to execute a Firefly Perimeter instance. The provisioning template also specifies where the Firefly Perimeter VM will reside in the ESXi host's hierarchy. You can use the same template to provision and deploy one or more Firefly

Perimeter instances. You can create multiple templates to launch Firefly Perimeter instances with different characteristics.

You can use Virtual Director to deploy and manage Firefly Perimeter instances in either of the following ways:

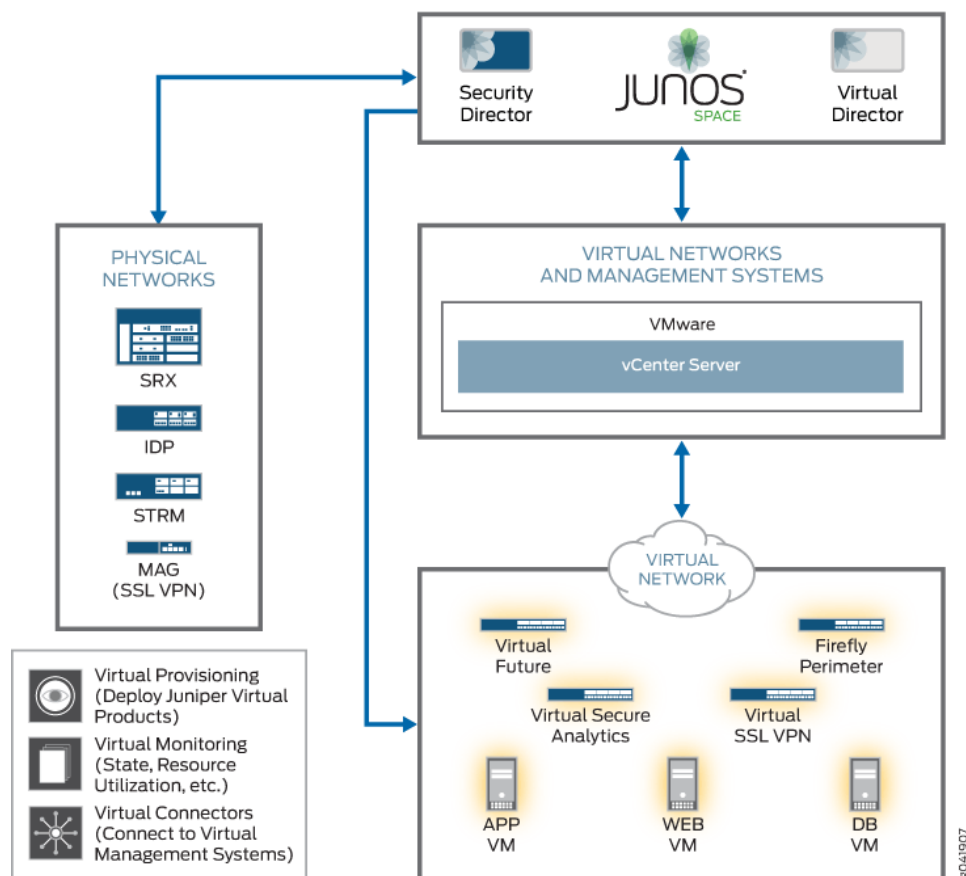
- Junos Space Virtual Director graphical user interface (GUI)
- Junos Space Virtual Director programmatic interface, which provides a set of Web REST services APIs



NOTE: For this Firefly release, Virtual Director supports Firefly Perimeter on VMware only.

Figure 2 on page 8 shows Virtual Director and its relationship to other virtualized products and physical Juniper security systems.

Figure 2: Junos Space Virtual Director



- Both Virtual Director and Security Director are Junos Space applications. Virtual Director registers Firefly Perimeter instances with the Junos Space Platform to allow Security Director to configure policies for them.

- Virtual Director allows you to select a virtualization provider. Presently VMware is the only supported virtualization provider. You can use Virtual Director with VMware to manage one or more vCenter ESXi hosts and virtual devices.

Firefly Perimeter runs in a virtual machine (VM). Virtual Director synchronizes Firefly Perimeter VM instances with VMware to allow you to use Security Director to configure Firefly Perimeter security and for other related functions such as logging. Synchronizing Firefly Perimeter instances with VMware allows Virtual Director to display current machine characteristics for these Firefly Perimeter VMs.

- In the future other virtualized applications and appliances communicating with the same virtualization provider will be able to take advantage of Virtual Director.

Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding Firefly Host for the Firefly Suite Solution on page 4](#)
- [Understanding Firefly Perimeter for the Firefly Suite Solution on page 6](#)

Understanding the Firefly Suite Solution Use Cases

Firefly Suite which is composed of three products—Firefly Host, Firefly Perimeter, and Junos Space Virtual Director—allows you to secure your virtualized environment. Because it brings together these three products, Firefly Suite allows for extensive application flexibility. The *Firefly Suite Getting Started Guide* covers at a conceptual level common use cases that entail use of these products. The use cases that it presents are for specific virtualized environments. They can also serve as guidelines for how to deploy Firefly Suite security for similar environments using features covered in the use case or other applicable Firefly Suite features.



NOTE: All of the Firefly Suite solution use cases use the VMware vCenter infrastructure and its ESXi hypervisor platform.

The Firefly Suite solution use cases are:

- Firefly Suite solution for the public cloud—This use case applies to the public cloud and its service provider's requirements to provide security for their tenant customers whose VMs they host and for whom they provide secure connectivity.
- Firefly Suite solution for the private cloud—This use case applies to virtualized environments in which the cloud and the equipment that it runs on are internal to an organization, whether that organization is a large enterprise, a university, or another type of organization whose environment is virtualized. Private cloud administrators want to provide their employees with VMs and segment and secure them within groups such as departments or organizations.
- Firefly Suite solution for managed security services providers—Among the services that these providers offer are clouds with tenant VMs and management of dedicated firewalls and secure VPNs.

This use case addresses managed security services providers who manage physical firewalls for their customers and who want to simplify that process using Firefly Perimeter. For example, a managed security services provider might use Firefly Perimeter to provide virtual firewalls and secure VPNs for customers whose companies have many local sites. This approach would allow a company's local sites to securely connect to the organization's headquarters, eliminating the need for each local site to manage its own firewall and the equipment that it runs on.

- Junos OS out-of-the-box Firefly Suite solution—Junos OS out-of-the-box is a Firefly Suite solution for system integrators, Juniper Networks partners, and other organizations who provide their customers with custom x86 systems specialized for the customer's company or organization. The custom x86 appliances typically host many applications that run in separate VMs. These appliances typically include a VPN that provides connectivity to the central office. Systems integrators and other custom system providers can leverage Firefly Perimeter to provide a firewall offering on their appliances to secure the appliance and its communication to and from the central office.

**Related
Documentation**

- [Understanding Firefly Suite on page 3](#)
- [Firefly Suite Solution Use Cases Structure on page 10](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)
- [Understanding the Firefly Suite Solution for the Private Cloud Use Case on page 23](#)
- [Understanding Firefly Suite and Managed Security Services on page 27](#)
- [Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case on page 31](#)

Firefly Suite Solution Use Cases Structure

Firefly Suite includes three products—Firefly Host, Firefly Perimeter, and Junos Space Virtual Director—that allow you to secure your virtualized environment entirely. The *Firefly Suite Getting Started Guide* covers four use cases that use these products.

The Firefly Suite solution for the public cloud uses all three products. Some configurations that it uses are also required for the other three use cases.

This guide provides complete information for the public cloud use case. Each of the other three use cases includes the following:

- A description of the use case.
- A reference to the public cloud software and hardware requirements for the use case, calling out any differences.
- A topology that is specific to the use case.

The four Firefly Suite solution use cases use the VMware ESXi hypervisor and vSphere virtualized infrastructure.

**Related
Documentation**

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)
- [Understanding the Firefly Suite Solution for the Private Cloud Use Case on page 23](#)
- [Understanding Firefly Suite and Managed Security Services on page 27](#)
- [Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case on page 31](#)

PART 2

Firefly Suite Solution Use Cases

- [Firefly Suite Solution Public Cloud Use Case on page 15](#)
- [Firefly Suite Solution Private Cloud Use Case on page 23](#)
- [Firefly Suite Solution Managed Security Services Use Case on page 27](#)
- [Firefly Suite Solution Junos OS Out-of-the-Box Use Case on page 31](#)

CHAPTER 2

Firefly Suite Solution Public Cloud Use Case

- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)
- [Public Cloud Tenant Customer Requirements on page 17](#)
- [Public Cloud Software and Hardware Requirements on page 17](#)
- [Understanding the Public Cloud Use Case Configurations Summary on page 19](#)
- [Using Firefly Suite Solution with Customer Portals on page 21](#)

Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology

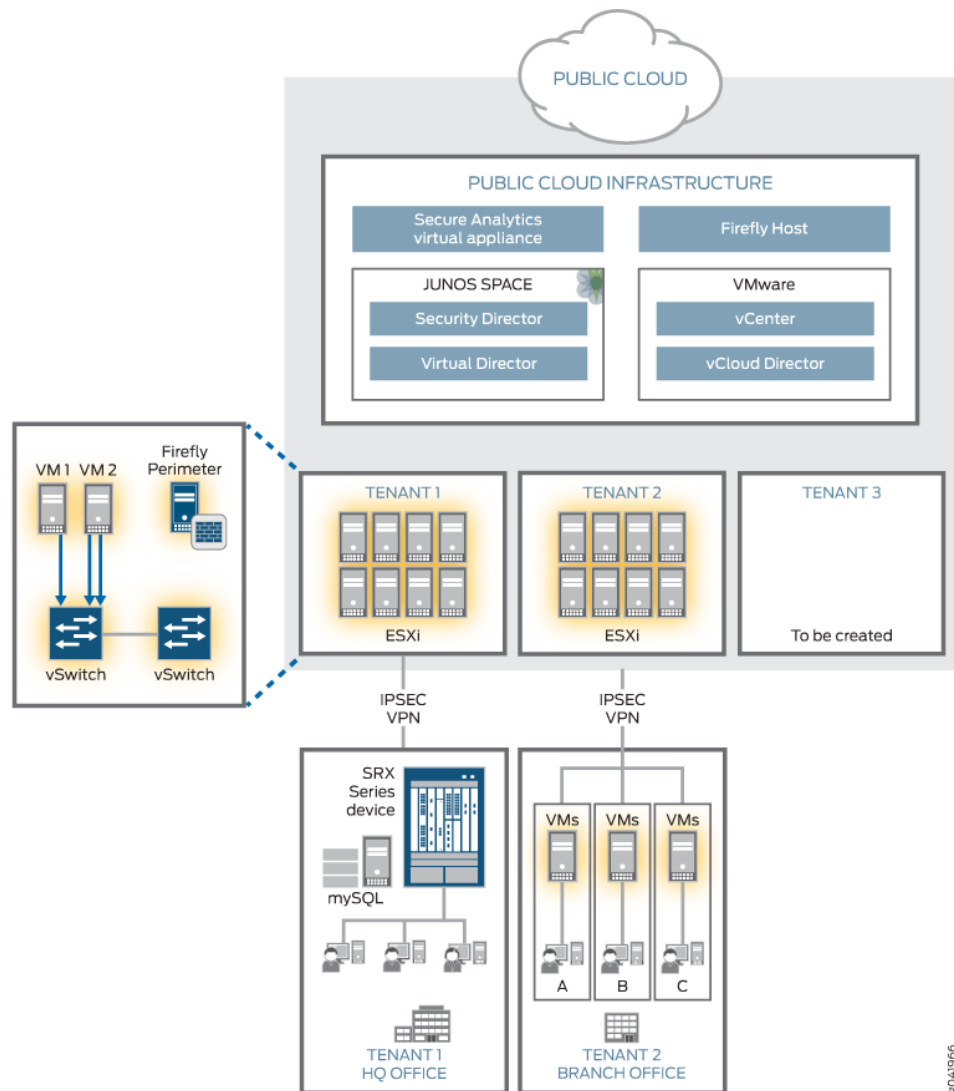
The Firefly Suite public cloud use case addresses public cloud service providers who host large numbers of VMs for their tenant customers, which in some cases can exceed 50,000 VMs. Firefly Suite offers you the opportunity to provide your customers with the security that they require both inside their virtualized data centers and at the tenant virtual network edge.

[Figure 3 on page 16](#) shows the Firefly Suite public cloud use case solution topology, including the Firefly Suite products, Junos Space products, Juniper Networks Secure Analytics virtual appliance, and the VMware products that are deployed in the cloud infrastructure. All of these products are used to carry out the use case configurations.

The following assumptions are made for the public cloud use case:

- Two tenants, tenant-1 and tenant-2, are preconfigured and the cloud administrator has already provisioned them with Firefly Perimeter instances.
- A new tenant called tenant-3 is introduced to the cloud and the cloud administrator will provision it with a Firefly Perimeter instance.
- IPSec VPNs are used to connect the VMs in the two preconfigured tenants to their company premises.
 - The IPSec VPN connects tenant-1 to corporate headquarters.
 - The IPSec VPN connects tenant-2 to a branch office. The company has virtualized its own data center and provided its branch office users with virtual machines (VMs).

Figure 3: Public Cloud Use Case Topology



8041966

Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Public Cloud Tenant Customer Requirements on page 17](#)
- [Public Cloud Software and Hardware Requirements on page 17](#)
- [Understanding the Public Cloud Use Case Configurations Summary on page 19](#)
- [Using Firefly Suite Solution with Customer Portals on page 21](#)
- [Understanding the Firefly Suite Solution for the Private Cloud Use Case on page 23](#)
- [Understanding Firefly Suite and Managed Security Services on page 27](#)
- [Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case on page 31](#)

Public Cloud Tenant Customer Requirements

Public cloud tenant customers generally express the following requirements:

- They want to know that their VMs are securely segmented from those of other tenants.

Because public clouds are multitenant environments in which customers who belong to different companies share the same hosts and pooled resources, service providers must make available to every tenant security protection to ensure the privacy and integrity of their VMs and environments.

- They want to control access to their VMs.

The service provider's customers want to ensure that their VMs are open only to Internet requests that they deem appropriate. They also want their hosted Web server VMs to allow Web requests from the Internet but not allow SSH access.

- They require that one or more of their hosted VMs can communicate with a physical server at the customer premise.

For this example one of the customers requires that their tenant hosted Web server must be able to query a database on the physical server at corporate headquarters over an IPsec VPN.

Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)
- [Public Cloud Software and Hardware Requirements on page 17](#)
- [Understanding the Public Cloud Use Case Configurations Summary on page 19](#)
- [Using Firefly Suite Solution with Customer Portals on page 21](#)
- [Understanding the Firefly Suite Solution for the Private Cloud Use Case on page 23](#)
- [Understanding Firefly Suite and Managed Security Services on page 27](#)
- [Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case on page 31](#)

Public Cloud Software and Hardware Requirements

[Table 4 on page 18](#) shows the software products and appliances that are configured for the Firefly Series public cloud use case solution.

These virtual resources are part of the public cloud infrastructure. The public cloud administrator uses them to configure tenants, deploy Firefly Perimeter instances for them, deploy and secure tenant VMs, and configure IPsec VPNs for tenants.

Table 4: Firefly Solution Public Cloud Use Case Software Requirements

Software Requirements for the Public Cloud Use Case
Junos Space server
<p>All of the Firefly products are required.</p> <ul style="list-style-type: none"> • Firefly Perimeter You can configure firewalls that utilize 2-GB RAM, 2 GB disk space, and up to 8 vNICs each. Firefly Perimeter API functions are enabled and preconfigured to allow access from an external management VM. • Firefly Host Firefly Host API functions are enabled and preconfigured to allow access from an external management server. The API functions are also used to configure Firefly Host smart groups. • Junos Space Virtual Director Virtual Director API functions are enabled. Virtual Director runs in a VM on the Junos Space server. <p>Junos Space Security Director. Security Director API functions are enabled. Security Director runs in a VM on the Space server.</p>
Secure Analytics virtual appliance
<p>VMware products</p> <ul style="list-style-type: none"> • VMware vCenter 5.0 and 5.1 • VMware ESXi 5.0 and 5.1 hosts software with 8 CPUs • VMware vSphere 5.0 and 5.1 <p>NOTE: vSphere 5.5 is not supported because of a Firefly Host incompatibility issue.</p>

[Table 5 on page 18](#) shows the public cloud use case hardware requirements.

Table 5: Firefly Solution Hardware Requirements for the Public Cloud Use Case

Firefly Solution Hardware Requirements for the Public Cloud Use Case
1 TB space of network-attached storage (NAS)
Physical SRX Series devices deployed at customer branch offices
A database server deployed at one of the customer branch offices
A physical Secure Analytics appliance deployed at customer branch offices

- Related Documentation**
- [Understanding Firefly Suite on page 3](#)
 - [Understanding the Firefly Suite Solution Use Cases on page 9](#)
 - [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)
 - [Public Cloud Tenant Customer Requirements on page 17](#)
 - [Understanding the Public Cloud Use Case Configurations Summary on page 19](#)

- [Using Firefly Suite Solution with Customer Portals on page 21](#)

Understanding the Public Cloud Use Case Configurations Summary

The public cloud use case includes configuration overviews for three tenants. It assumes that two tenants, tenant-1 and tenant-2, are preconfigured and that the cloud administrator has already provisioned them with Firefly Perimeter instances. A new tenant called tenant-3 is introduced to the cloud and the cloud administrator provisions it with a Firefly Perimeter instance.

Product APIs are used for tenant-1 configurations. Product GUIs are used for tenant-2 configurations. For tenant-3, two ways are identified: using product APIs and using product GUIs.

Here is a summary of the public cloud use case configurations required for the three tenants.

- For tenant-1, the cloud administrator:
 - Generates a new VM using the VMware API.
 - Adds firewall policy rules for the new VM using the Junos Space Security Director RESTful Web services API.
 - Creates a smart group using the Firefly Host XML-RPC API. The smart group is defined to include the VM and automatically secure it by pushing policy to it. The policy allows the new VM to communicate with other VMs in tenant-1.
 - Adds the VM to the tenant-1 Firefly Perimeter instance address book using the Junos Space Security Director RESTful Web services API.
 - Configures an IPsec VPN for the tenant using the Junos Space Security Director RESTful Web services API.

The VPN local endpoint gateway is on the tenant's Firefly Perimeter instance. The VPN peer endpoint is configured on the SRX Series device at the customer premises.

- For tenant-2, the cloud administrator:
 - Generates a VM by cloning an existing tenant-2 VM using the VMware vCenter GUI.
 - Creates a smart group using the Firefly Host Dashboard GUI. The smart group is defined to include the VM and automatically secure it by pushing policy to it. The policy allows the new VM to communicate with other VMs in tenant-2.
 - Adds firewall policy rules to the tenant-2 Firefly Perimeter instance using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.
 - Configures an IPsec VPN for tenant-2 using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.

The VPN local endpoint gateway is on the tenant's Firefly Perimeter instance. The VPN peer endpoint is configured on the SRX Series device at the customer premises.

- Adds the new VM to the tenant-2 Firefly Perimeter instance address book using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.
- For tenant-3, the cloud administrator configures and introduces the new tenant to the cloud. The administrator can use either APIs or GUIs for this configuration. Both approaches are covered.

To configure tenant-3 using APIs, the cloud administrator:

- Provisions and deploys a Firefly Perimeter instance using the Junos Space Virtual Director API.
- Generates a new VM using the VMware vCenter API.
- Creates a smart group using the Firefly Host XML-RPC API. The smart group is defined to include the VM and automatically secure it by pushing policy to it. The policy allows the new VM to communicate with other VMs in tenant-3.
- Adds firewall rules for the new VM using the Junos Space Security Director RESTful Web services API.
- Adds the VM to the Firefly Perimeter address book using the Junos Space Security Director RESTful Web services API.

To configure tenant-3 using GUIs, the cloud administrator:

- Provisions and deploys a Firefly Perimeter instance using the Junos Space Virtual Director GUI.
- Generates a VM by cloning an existing tenant-3 VM using the VMware vCenter GUI.
- Creates a smart group using the Firefly Host Dashboard GUI. The smart group is defined to include the VM and automatically secure it by pushing policy to it. The policy allows the new VM to communicate with other VMs in tenant-3.
- Adds firewall policy rules to the tenant-3 Firefly Perimeter instance using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.
- Configures an IPsec VPN for tenant-3 using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.

The VPN local endpoint gateway is on the tenant's Firefly Perimeter instance. The VPN peer endpoint is configured on the SRX Series device at the customer premises.

- Adds the new VM to the tenant-3 Firefly Perimeter instance address book using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.

**Related
Documentation**

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)

- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)
- [Public Cloud Tenant Customer Requirements on page 17](#)
- [Using Firefly Suite Solution with Customer Portals on page 21](#)

Using Firefly Suite Solution with Customer Portals

A public cloud service provider *could* manage the security for a large number of VMs that they host, but carrying this out becomes untenable when their cloud expands to include thousands of VMs. Moreover, in most cases tenant administrators want to be able to define *and* manipulate security policy for their VMs directly.

Products such as OpenStack and Cloud Stack allow service providers to make available to tenant administrators front-end custom portals that allow the administrators to do just that. When portals are used, VM management is largely driven through use of APIs.

The Firefly Suite solution lends itself to this kind of application. For example, a portal implementation might use the Firefly Host, Firefly Perimeter, and Junos Space Security Director APIs on the back end to change the behavior of the firewall used to secure each VM based on what the tenant administrator specifies.

Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)
- [Public Cloud Tenant Customer Requirements on page 17](#)

CHAPTER 3

Firefly Suite Solution Private Cloud Use Case

- [Understanding the Firefly Suite Solution for the Private Cloud Use Case on page 23](#)
- [Understanding the Private Cloud Use Case Requirements, Topology, and Configuration on page 24](#)

Understanding the Firefly Suite Solution for the Private Cloud Use Case

Many large enterprises, financial institutions, universities, and other organizations have virtualized their data centers to implement private clouds that they manage. A private cloud is internal to the company or organization and used exclusively for it. Private clouds allow companies to maximize resources by pooling and sharing them. Use of virtualized, pooled resources in a private cloud can challenge privacy requirements unless security for the virtualized environment is implemented. To keep data private and protect it, a company can segment their virtualized environment into groups such as business units or departments and secure those groups differently based on requirements. For example, a company might want to ensure that their human resources department is kept separate from that of other groups such as their marketing and accounting departments. Private clouds are similar to public clouds in regard to segmentation, but with private clouds segmented groups are internal to the company. In a public cloud, segmented groups, or tenants, belong to different companies.

Private cloud administrators typically have a number of requirements in common, chief of which are the following concerns:

- They want to provide their employees with secure VMs, virtual servers, and other resources appropriately.
- They want to securely segment virtual machines (VMs) and data for their internal organizations.
- They want applications and tools that allow them to easily deploy security for their virtualized environments, including the ability to institute and apply compliance rules to VMs. They want to deploy these security measures without having to create custom implementations using APIs.

As a private cloud administrator, you can deploy Firefly Suite to secure your virtualized environment and its organizations entirely, including at the VM level and the network

edge of each segmented group. Firefly Suite is designed for the virtualized environment to facilitate security deployment. You can use its product GUIs to easily provision and deploy security to protect VMs and their traffic in many ways and to create firewalls to protect overall segmented groups, business units, and departments.

**Related
Documentation**

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Private Cloud Use Case Requirements, Topology, and Configuration on page 24](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)

Understanding the Private Cloud Use Case Requirements, Topology, and Configuration

The private cloud software requirements are the same as those for the public cloud. Their hardware requirements are also the same as those for the public cloud with the exception that a physical SRX Series device is not required.

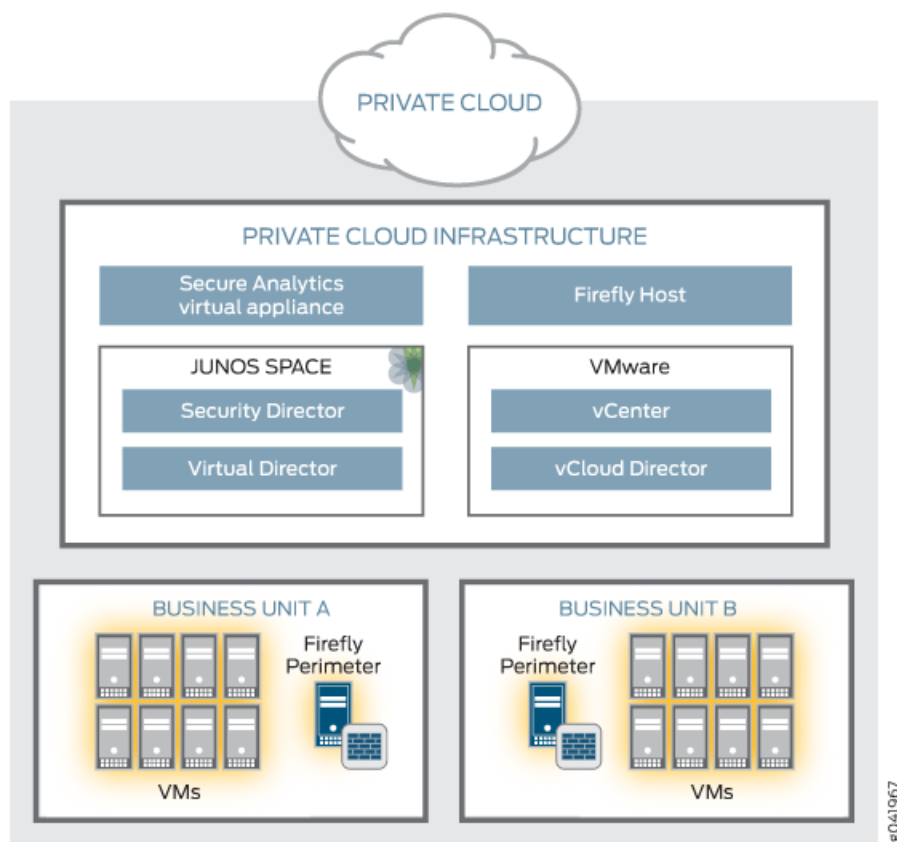
To configure the private cloud for this use case the administrator uses application GUIs.

The private cloud administrator:

- Provisions and deploys a Firefly Perimeter instance for each segmented group using the Junos Space Virtual Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.
- Creates a smart group for segmented groups using the Firefly Host Dashboard management center GUI. For each group, the smart group is defined to include the group's VMs and automatically secure them by pushing policy to them. The policy allows existing and new VMs to communicate with other VMs in their group and with other VMs in the private cloud.
- Adds firewall rules to the segmented group's Firefly Perimeter instance for the VMs in that group using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.
- For each segmented group, creates a new VM and adds it to the group's Firefly Perimeter instance address book using the Junos Space Security Director GUI. Alternatively you could use the Firefly Perimeter Junos OS J-Web.

[Figure 4 on page 25](#) shows the topology for a private cloud, including all of the products that its administrator might use. The Firefly Suite private cloud use case solution does not use vCloud Director to deploy VMs for groups, but other private cloud deployments might use it.

Figure 4: Private Cloud Use Case Topology



Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Firefly Suite Solution for the Private Cloud Use Case on page 23](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)

CHAPTER 4

Firefly Suite Solution Managed Security Services Use Case

- [Understanding Firefly Suite and Managed Security Services on page 27](#)
- [Understanding the Managed Security Services Use Case Requirements, Topology, and Configuration on page 28](#)

Understanding Firefly Suite and Managed Security Services

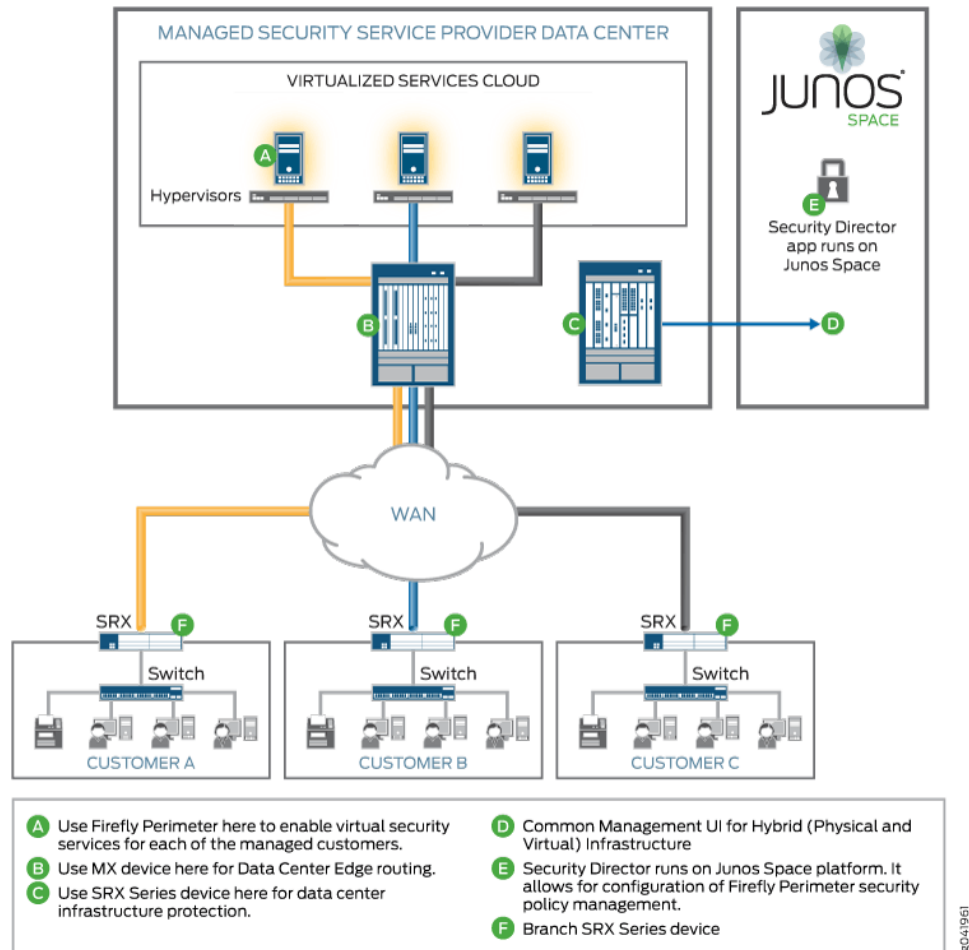
Large telecom service providers and managed security services providers offer various managed security services to their customers, including dedicated firewalls and IPsec VPNs. Virtual managed services can be deployed in a number of ways. For virtual firewalls, typically the service provider consolidates services on virtual hardware at their site and offers the virtual firewall as a fully managed service.

In the past managed security services providers might have offered their customers physical firewalls. However, provisioning physical firewalls is a tedious and slow process that often takes from thirty to sixty days resulting in delayed setup for new tenant customers. By contrast, virtual firewalls can be deployed and scaled quickly, and they offer lower capital expenditures (CapEx) and operating cost expense (OpEx) investment.

Managed security services providers can use Firefly Perimeter to provide their customers with virtual firewalls. A single Firefly Perimeter instance can be used for a customer with remote locations. For example, the customer's company might have remote retail stores or coffee shops. The Firefly Perimeter instance resides on the service provider's virtual hardware and physical infrastructure instead of at every remote store branch or coffee shop site. The service provider hosts and manages the Firefly Perimeter solution, which also offers secure connectivity. This *clean pipe* solution requires minimum gear and limited configuration complexity at the remote customer site.

[Figure 5 on page 28](#) shows software and hardware products that an extensive managed security services data center might contain, including appropriate Juniper Networks products.

Figure 5: Managed Security Services Environment Using Juniper Networks Products



Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Managed Security Services Use Case Requirements, Topology, and Configuration on page 28](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)

Understanding the Managed Security Services Use Case Requirements, Topology, and Configuration

The Firefly Suite managed security services use case requires Firefly Perimeter and the VMware products, which are described in the public cloud use case. You can deploy Firefly Perimeter instances using only these products. However, you could use the Junos Space Virtual Director GUI or API and the Junos Space Security Director GUI or its RESTful

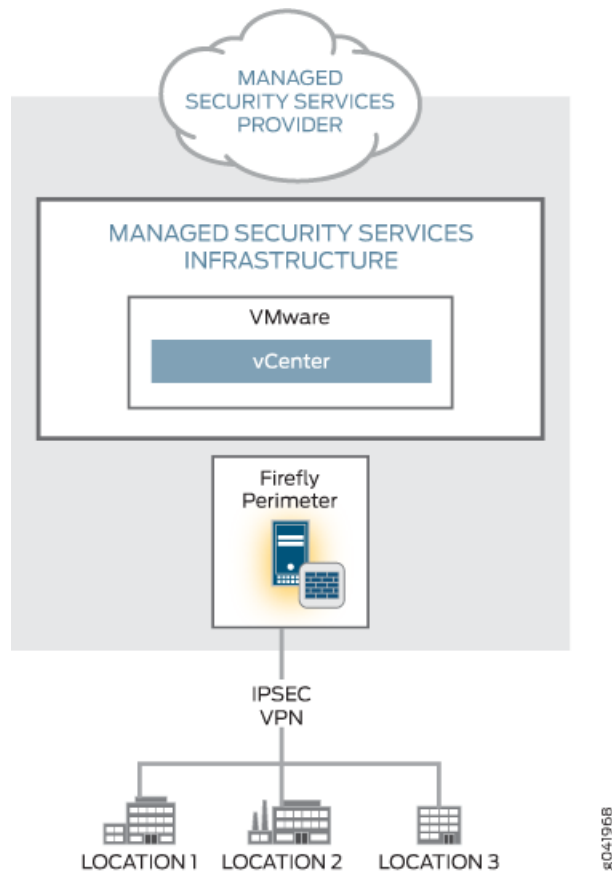
Web services API to provision, deploy, and secure Firefly Perimeter, but these products are not required.

To provide their customers with Firefly Perimeter instances, the service provider:

- Deploys Firefly Perimeter using an OVA file to boot Firefly Perimeter and the Firefly Perimeter CLI. Alternatively, you could use the Device Management Interface (DMI)/NetConf.
- Configures firewall security using the Firefly Perimeter CLI or J-Web.
- Configures an IPsec VPN for the customer using the Firefly Perimeter CLI or J-Web.

Figure 6 on page 29 shows the topology for the Firefly Suite managed security services use case solution.

Figure 6: Managed Security Services Use Case Topology



Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding Firefly Suite and Managed Security Services on page 27](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)
- [Understanding the Firefly Suite Solution Public Cloud Use Case and Its Topology on page 15](#)

CHAPTER 5

Firefly Suite Solution Junos OS Out-of-the-Box Use Case

- Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case on page 31
- Understanding the Junos OS Out-of-the-Box Use Case Requirements, Topology, and Configuration on page 32

Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case

System integrators, Juniper Networks partners, and other organizations who offer custom virtualized x86 appliances could integrate Firefly Perimeter on their appliances to provide their customers with data and traffic firewall security.

Custom appliances host many applications that are specific to a customer's business or industry. Typically the applications run in separate VMs. These appliances also commonly incorporate VPN connectivity from the appliance back to a central location. Firefly Perimeter integration could be used to secure traffic to and from the central location.

Many businesses use these custom appliances geared for their industry. For example, large banks and investment firms for whom security is a concern take advantage of customized appliances that are loaded with software applications for financial information services. Military organizations might also use custom appliances that are hardened servers deployed in tanks to allow communication to central command posts over VPNs. Firefly Perimeter could be used to further protect their hardened systems and secure their communication.

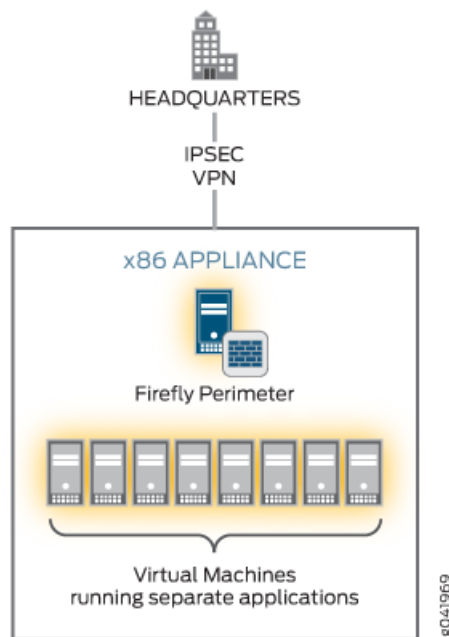
If you deliver Firefly Perimeter on your custom appliances, you might need to build a custom manageability solution. To build a solution that installs and manages single instances of Firefly Perimeter, you can use an OVA file to boot Firefly Perimeter and the Firefly Perimeter CLI or DMI/Net to further provision it.



NOTE: You can use Junos Space Virtual Director and Junos Space Security Director in this use case scenario, although it is not a requirement.

Figure 7 on page 32 shows the topology for the Firefly Suite Junos OS out-of-the-box use case solution.

Figure 7: Junos OS Out-of-the-Box Use Case Topology



Related Documentation

- [Understanding Firefly Suite on page 3](#)
- [Understanding the Junos OS Out-of-the-Box Use Case Requirements, Topology, and Configuration on page 32](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)

Understanding the Junos OS Out-of-the-Box Use Case Requirements, Topology, and Configuration

The Junos OS out-of-the-box use case requires Firefly Perimeter and the VMware products, used for and described in the public cloud use case. You can deploy Firefly Perimeter instances using only these products. However, you could use the Junos Space Virtual Director GUI or API and the Junos Space Security Director GUI or RESTful Web services API to deploy and secure Firefly Perimeter, but these products are not required.

To provide their customers with a firewall on their customized x86 systems, the custom appliance provider:

- Provisions and deploys Firefly Perimeter using an OVA file to boot Firefly Perimeter and the Firefly Perimeter Junos OS CLI or Device Management Interface/NetConf
- Configures firewall security using the Firefly Perimeter Junos OS CLI or J-Web.
- configures an IPsec VPN for the customer using the Firefly Perimeter Junos OS CLI or J-Web.

Related Documentation

- [Understanding Firefly Suite on page 3](#)

- [Understanding the Firefly Suite Solution for the Junos OS Out-of-the-Box Use Case on page 31](#)
- [Understanding the Firefly Suite Solution Use Cases on page 9](#)

PART 3

Index

- [Index on page 37](#)

Index

Symbols

#, comments in configuration statements.....	xi
(), in syntax descriptions.....	xi
< >, in syntax descriptions.....	xi
[], in configuration statements.....	xi
{ }, in configuration statements.....	xi
(pipe), in syntax descriptions.....	xi

B

braces, in configuration statements.....	xi
brackets	
angle, in syntax descriptions.....	xi
square, in configuration statements.....	xi

C

comments, in configuration statements.....	xi
conventions	
text and syntax.....	x
curly braces, in configuration statements.....	xi
customer support.....	xii
contacting JTAC.....	xii

D

documentation	
comments on.....	xi

F

Firefly Host.....	3
benefits.....	4
Firefly Host Dashboard.....	4
stateful firewall.....	4
Firefly Perimeter.....	3
benefits.....	6
Virtual Director.....	6
VMware and KVM tools.....	6
Firefly Suite	
definition.....	3
Firefly Host.....	3, 4
Firefly Perimeter.....	3, 6
solution use cases.....	10
Virtual Director.....	3, 7

Firefly Suite solution for custom appliances.....	31
Firefly Suite solution for portals.....	21
Firefly Suite solution use cases	
Junos OS out-of-the-box.....	31, 32
managed security services.....	27
private cloud.....	23, 24
public cloud.....	15, 17, 19
font conventions.....	x

J

Junos OS out-of-the-box use case.....	9
configuration summary.....	32
custom appliance provider.....	31, 32
software and hardware requirements.....	32
system integrators.....	31
topology.....	31, 32

M

managed security services providers.....	27
managed security services use case.....	9
configuration summary.....	28
service providers.....	27, 28
software and hardware requirements.....	28
topology.....	28
manuals	
comments on.....	xi

P

parentheses, in syntax descriptions.....	xi
private cloud use case.....	9
configuration summary.....	24
customer requirements.....	23
software and hardware requirements.....	24
topology.....	24
public cloud use case.....	9
configurations summary.....	19
service providers.....	15
software and hardware requirements.....	17
tenant customer requirements.....	17
topology.....	15

S

support, technical See technical support	
syntax conventions.....	x

T

technical support	
contacting JTAC.....	xii
tenant virtual network edge.....	6

U

use cases

components.....	10
Junos OS out-of-the-box.....	9
managed security services.....	9
overview.....	9
private cloud.....	9
public cloud.....	9
VMware.....	9

V

Virtual Director.....	3
benefits.....	7
Firefly Perimeter.....	7