

Contrail Service Orchestration Designer Tools User Guide

Published
2020-07-13

Release
5.1.2

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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.

Contrail Service Orchestration Designer Tools User Guide

5.1.2

Copyright © 2020 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 <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | vii

Documentation and Release Notes | vii

Documentation Conventions | vii

Documentation Feedback | x

Requesting Technical Support | x

Self-Help Online Tools and Resources | xi

Creating a Service Request with JTAC | xi

1

Designer Tools

Designer Tools Introduction | 2

Designer Tools Overview | 2

Access Designer Tools | 4

Change Your Designer Tools Password | 6

2

Configuration Designer

Configuration Designer Introduction | 9

Configuration Designer Overview | 9

Using the Configuration Designer | 10

Creating Configuration Templates | 12

About the Requests Page for the Configuration Designer | 12

Tasks You Can Perform | 12

Field Descriptions | 13

Creating Requests for Configuration Templates | 13

Designing Templates with a Configuration | 15

Designing Templates with a YANG Configuration | 20

Publishing Configuration Templates | 23

Managing Configuration Templates | 25

About the Designs Page for the Configuration Designer | 25

Tasks You Can Perform | 25

Field Descriptions | 26

Cloning Configuration Templates | 27

Deleting Configuration Template Designs | 28

Resource Designer

Resource Designer Introduction | 30

Resource Designer Overview | 30

Using the Resource Designer | 32

Creating VNF Packages | 34

About the Requests Page for the Resource Designer | 34

Tasks You Can Perform | 34

Field Descriptions | 34

VNF Overview | 35

Creating Requests for VNF Packages | 37

Designing VNF Packages | 39

Creating Basic VNF Information | 39

Adding Flavor Parameters | 42

Adding Standard and Custom Functions | 44

Designing a Supported Function Chain | 44

Viewing the Summary of VNF Packages | 46

Adding VNF Managers | 47

Publishing VNF Packages | 49

Managing VNF Packages | 50

About the Designs Page for the Resource Designer | 50

Tasks You Can Perform | 50

Field Descriptions | 51

Cloning VNF Packages | 52

Importing VNF Packages | 52

Exporting VNF Packages | 53

Deleting VNF Packages | 54

Network Service Designer

Network Service Designer Introduction | 56

Network Service Designer Overview | 56

Using the Network Service Designer | 57

Creating Requests for Network Services | 58

Network Services and Service Chains Overview | 58

Performance Overview | 59

About the Requests Page for the Network Service Designer | 60

Tasks You Can Perform | 61

Field Descriptions | 61

Creating Requests for Network Services | 62

Creating a Functional Service Chain | 64

Configuring Performance Goals | 65

Viewing Requests for Network Services | 67

Creating Network Services | 68

About the Build Page for the Network Service Designer | 68

Tasks You Can Perform | 69

Field Descriptions | 69

Viewing Information About VNFs | 70

Designing Network Services | 71

Designing a Network Service for a Centralized Deployment | 71

Designing a Network Service for a Distributed Deployment | 73

Connecting VNFs in a Service Chain | 74

Defining Ingress and Egress Points for a Service Chain | 75

Monitoring Performance Goals | 76

Configuring Network Services | 77

vSRX Configuration Settings | 78

LxCIPtable VNF Configuration Settings | 87

Cisco CSR-1000v VNF Configuration Settings | 90

Riverbed Steelhead VNF Configuration Settings | 92

Fortinet VNF Configuration Settings | 92

Ubuntu VNF Configuration Settings | 93

Managing Network Services | 94

About the Designs Page for the Network Service Designer | 94

Tasks You Can Perform | 94

Field Descriptions | 95

Publishing Network Service Designs | 96

Copying Network Service Designs | 96

Editing Network Service Designs | 97

Deleting Network Service Designs | 98

Viewing Network Service Designs | 99

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vii
- Documentation Conventions | vii
- Documentation Feedback | x
- Requesting Technical Support | x

Use this guide to plan, design, evaluate, and publish network services using the Designer Tools Portal (Configuration Designer, Resource Designer, and Network Service Designer). You can design the network service or service chain using the virtualized network functions (VNFs) from Juniper Networks or third-party companies. You can evaluate whether your network service meets the desired performance goals and publish the network services to the customers.

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 <https://www.juniper.net/documentation/>.

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 <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page viii 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page viii 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> RFC 1997, <i>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</i> <i>string2</i> <i>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

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

Convention	Description	Examples
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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Juniper Care or Partner Support Services 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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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 <https://support.juniper.net/support/requesting-support/>.

1

PART

Designer Tools

Designer Tools Introduction | 2

Designer Tools Introduction

IN THIS CHAPTER

- [Designer Tools Overview | 2](#)
- [Access Designer Tools | 4](#)
- [Change Your Designer Tools Password | 6](#)

Designer Tools Overview

NOTE:

- Designer Tools is available only for users with the Service Provider (SP) Administrator role.
- In the cloud-hosted version of Contrail Service Orchestration (CSO), which is managed by Juniper Networks, the SP Administrator role is available only for Juniper. Therefore, in the cloud-hosted version of CSO, Designer Tools is accessible only to Juniper.

Designer Tools are a suite of GUI-based tools that enable network designers to support virtualized network functions (VNFs) and network services in CSO. Designer Tools comprise the following:

- Configuration Designer, which is used to define and publish multivendor configuration templates.

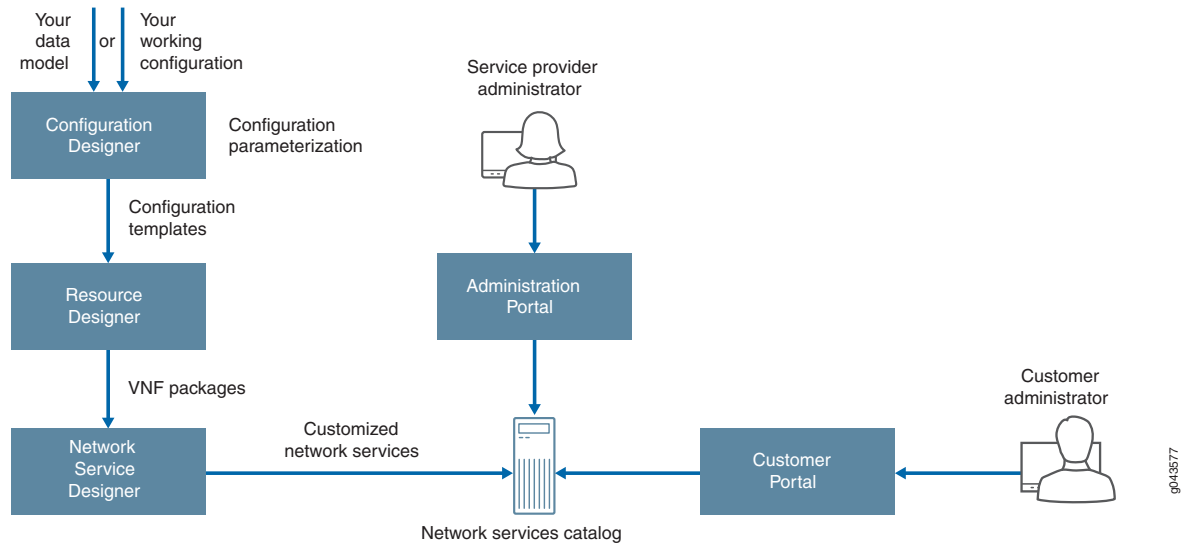
NOTE: The published configuration templates can be used in device templates in CSO (through the stage-2 configuration) or when building VNF packages using Resource Designer.

- Resource Designer, which is used to create, validate, and publish multivendor virtualized network function (VNF) packages.
- Network Services Designer (NSD), which is used to create and manage multivendor network services and service chains.

The workflow (see [Figure 1 on page 4](#)) to create a network service by using Designer Tools and use it in CSO is as follows:

1. Use Configuration Designer to:
 - a. Create a configuration design request.
 - b. Use Configuration Designer to publish the configuration templates.
2. Use Resource Designer to:
 - a. Create a VNF package request.
 - b. Validate, and publish VNF packages to NSD.
3. Use NSD to:
 - a. Create a network service design requests by using the VNFs from Resource Designer and (optionally) configuration templates.
 - b. Build and publish the network services to CSO
4. Service Provider administrators use Administration Portal to assign a set of network services to their customers.
5. Tenant administrators use Customer Portal to access the assigned network services to manage their sites and services.

Figure 1: Designer Tools Workflow



RELATED DOCUMENTATION

[Configuration Designer Overview | 9](#)

[Resource Designer Overview | 30](#)

[Network Service Designer Overview | 56](#)

Access Designer Tools

Users with the SP (Service Provider) Administrator role can access Designer Tools (Configuration Designer, Resource Designer, and Network Services Designer) by using a web browser.

NOTE: We recommend that you use Google Chrome Version 60 or later to access Designer Tools.

To access Designer Tools:

1. Open a browser window or tab and access the URL `https://central-IP-address:83`.

Where, *central-IP-address* is the IP address of the virtual machine (VM) that hosts the microservices for the central point of presence (POP). which is the same URL that you use to access Administration Portal. For example, `https://192.0.2.10:83`.

The Network Service Designer login page appears.

2. Enter the username and password in their respective fields.

NOTE: The username and password combination is the same one that you use to access Administration Portal.

3. Click **LOG IN**

The CSO Network Service Designer Home page appears.

4. (Optional) To access Configuration Designer or Resource Designer:

- a. Click the **Menu** icon in the top-left corner of the page.

The Designer Tools menu appears.

- b. Do one of the following:

- Click **Configuration Designer** to access Configuration Designer.

The CSO Configuration Designer Home page appears.

- Click **Resource Designer** to access Resource Designer.

The CSO Resource Designer Home page appears.

RELATED DOCUMENTATION

[Using the Configuration Designer | 10](#)

[Using the Resource Designer | 32](#)

[Network Service Designer Overview | 56](#)

Change Your Designer Tools Password



CAUTION: Do not change your password in Designer Tools. Instead, use Administration Portal to change your password.

Users with the SP (Service Provider) Administrator role can access Designer Tools by using the username and password that they use to log in to the Contrail Service Orchestration (CSO) Administration and Customer Portals. Therefore, if you change your password in Designer Tools, the password change is also applicable to the CSO Administration and Customer Portals.

To change your password:

1. Click the username on the right of the Designer Tools banner.

A drop-down list appears.

2. Click **Change Password**.

The Change Password page appears.

3. Change your password following the guidelines provided in [Table 3 on page 6](#).

4. Click **OK**.

You are logged out of the system. To log in to the GUI again, you must use your new password. Other sessions logged in with the same username are unaffected until the next login.

Table 3: Fields on the Change Password Page

Field	Description
Current Password	Enter your existing password.
New Password	Enter the new password, which must: <ul style="list-style-type: none"> • Contain at least one number, one special character, one uppercase, and one lowercase letter. • Be at least 6 characters long but not longer than 21 characters.
Confirm Password	Enter the new password for confirmation. NOTE: Select the Show Password check box to view the password and clear the check box to mask the password.

RELATED DOCUMENTATION

[Configuration Designer Overview | 9](#)

[Resource Designer Overview | 30](#)

[Network Service Designer Overview | 56](#)

2

PART

Configuration Designer

Configuration Designer Introduction | 9

Creating Configuration Templates | 12

Managing Configuration Templates | 25

Configuration Designer Introduction

IN THIS CHAPTER

- Configuration Designer Overview | 9
- Using the Configuration Designer | 10

Configuration Designer Overview

Configuration Designer, Resource Designer, and Network Services Designer (collectively known as Designer Tools) are a suite of GUI-based tools that enable network designers to support virtualized network functions (VNFs) and network services in Contrail Service Orchestration (CSO).

Configuration Designer provides an intuitive UI-based workflow for creating and managing configuration templates. The configuration templates that you create are rendered automatically in the UI. Resource Designer uses these templates to create VNF packages that are then published to Network Service Designer.

Network Service Designer uses the VNF packages to design customized network services that are published to the network services catalog. The network services catalog contains a list of usable network services.

Users with the Service Provider (SP) Administrator role access the network services catalog to assign a set of network services to their customers using Administration Portal. Finally, tenant users access the network services assigned to them using Customer Portal to manage their sites and services.

NOTE: In Administration and Customer Portals, you can create (add) configuration templates only for Juniper devices. In Configuration Designer, you can create configuration templates for both Juniper and non-Juniper devices.

A configuration template has prepopulated values for configuration settings associated with a virtualized network function (VNF). The configuration in the templates can be of the following types:

- Device-level base configurations, such as an interface configuration
- Service configurations, such as a firewall policy configuration
- Monitoring configurations, such as a CLI, SNMP, or other monitoring command configuration

In Configuration Designer, you can manually type a working configuration or copy and paste an existing golden configuration from your device. You can also use your own data model to configure your template. Once created, the templates are listed on a Design page, where you can review them at a glance. You can also modify the parameters and values of your templates as needed from the Design page.

The configuration templates can be used by:

- Network designers to create a day 0 configuration or default parameters in the Resource Designer. For example, they can enter interface information.
- Your customer administrators or end users (using the Customer Portal):
 - On Day 1 they can customize their services during VNF instantiation. For example, they can enter IP addresses for a given site.
 - On Day 2 they can update a configuration of Juniper Networks devices. For example, they can configure their network to block social media.

RELATED DOCUMENTATION

[Access Designer Tools | 4](#)

[Change Your Designer Tools Password | 6](#)

[Using the Configuration Designer | 10](#)

Using the Configuration Designer

Use the Configuration Designer to create a configuration template or modify an existing one. Follow these steps to get started with the Configuration Designer:

- Learn about the Configuration Designer. See [“Configuration Designer Overview” on page 9](#).
- Log into the Configuration Designer. See [“Access Designer Tools” on page 4](#).

To create a configuration template:

1. Create a request for a configuration template. See [“Creating Requests for Configuration Templates” on page 13](#).
2. Design a configuration template. You can design a configuration template using one of these methods:
 - Using a data model. Choose this method when you already have a data model for your configuration template. See [“Designing Templates with a YANG Configuration” on page 20](#).

- Using your working configuration. Choose this method when you have a Jinja template but want the Configuration Designer to generate a data model for your configuration template. See [“Designing Templates with a Configuration” on page 15](#).
3. Publish the configuration template to the Network Service Designer. See [“Publishing Configuration Templates” on page 23](#).

RELATED DOCUMENTATION

| [Configuration Designer Overview](#) | 9.

Creating Configuration Templates

IN THIS CHAPTER

- [About the Requests Page for the Configuration Designer | 12](#)
- [Creating Requests for Configuration Templates | 13](#)
- [Designing Templates with a Configuration | 15](#)
- [Designing Templates with a YANG Configuration | 20](#)
- [Publishing Configuration Templates | 23](#)

About the Requests Page for the Configuration Designer

To access this page, click **Home> Requests**.

You can use the Requests page to request a new configuration template. A configuration template has prepopulated values for configuration settings associated with a virtualized network function (VNF). By using a configuration template for a network service, you can avoid having to manually configure settings for each service.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a request for a configuration template. See [“Creating Requests for Configuration Templates” on page 13](#).
- Design a new configuration template using a predefined working configuration. In this method, the Configuration Designer generates the data model. See [“Designing Templates with a Configuration” on page 15](#).
- Design a new configuration template using the YANG model. See [“Designing Templates with a YANG Configuration” on page 20](#).

Field Descriptions

Table 4 on page 13 provides guidelines on using the fields on the Requests page for the Configuration Designer.

Table 4: Fields on the Requests Page for the Configuration Designer

Field	Description
Requests Page	
New Template	<p>Click to request a new configuration template.</p> <p>The New Template page allows you to define the requirements for your configuration template.</p>
Configuration Template Request	
Begin with config	<p>Click to design a new configuration template using a predefined working configuration.</p> <p>Select this method if you have the Jinja2 configuration but need the Configuration Designer to generate a data model for your configuration template.</p>
Begin with YANG	<p>Click to design a configuration template using an existing data model.</p> <p>Select this method if you already have the Jinja2 (a template engine for Python) configuration and the data model for your configuration template.</p>
Delete	<p>Click to delete a configuration template request.</p>

RELATED DOCUMENTATION

Configuration Designer Overview	9
Using the Configuration Designer	10

Creating Requests for Configuration Templates

You can create a configuration template by first making a request for it. A request allows you to define the requirements for the configuration template, including the template format, vendor, and the supported device family.

To create a request for a configuration template:

1. Click **Home > Requests > New Template**.
2. Complete the configuration according to the guidelines provided in [Table 5 on page 14](#).
3. Click **Create**.

A new template request is created.

Table 5: Fields on the New Template Page

Field	Description
Name	<p>Specify a name for your configuration template. Only a string of alphanumeric characters, dashes, and spaces are accepted.</p> <p>Example: ucpe-SRX DPI config</p>
Description	<p>Enter a description for your configuration template. Make this description as clear and useful as possible for all administrators.</p> <p>Example: NFX JCP configuration to restore default route from LAN to WAN. This configuration is pushed to JCP after the service chain is deleted.</p>
Output config format	<p>Select a format for your configuration template:</p> <ul style="list-style-type: none"> • CLI (Command-line interface) • XML (Extensible Markup Language) • Native—Default file format of the application that we use to create and save files. We use CLI plug-in and it is used for cms_plug-in.
Category	<p>Specify the category for the configuration template. Categories allow you to group your templates and filter and search them easily.</p> <ul style="list-style-type: none"> • VNF—Select this option when you create a configuration template for the virtualized network function. • Device Template—Select this option when you create a device template for a network device, such as a customer premises equipment (CPE) device. • Other—Select this option when you create a configuration template for a network function other than VNF or device template.
Vendor	<p>Specify the vendor that you want the configuration template to support.</p> <p>Example: Juniper Networks</p>

Table 5: Fields on the New Template Page (*continued*)

Field	Description
Device family	Specify the device family that you want the configuration template to support. Example: juniper-srx

RELATED DOCUMENTATION

[Configuration Designer Overview](#) | 9

[Designing Templates with a YANG Configuration](#) | 20

[Designing Templates with a Configuration](#) | 15

Designing Templates with a Configuration

You can design a configuration template either by using your own data model or by using the data model generated by the Configuration Designer. The Configuration Designer provides a configuration template wizard that takes you through a step-by-step procedure to create your configuration template. You can design multiple templates by creating requests and launching respective wizards from them.

To design a template using the data model generated by the Configuration Designer, you provide your Jinja configuration and the wizard automatically parses its parameters and generates the data model for your template. See <http://jinja.pocoo.org/docs/2.10/templates/> for documenting the configuration templates of the jinja2 Python module.

Before you begin, create a configuration template request. See [“Creating Requests for Configuration Templates” on page 13](#).

To design a template with your configuration:

1. From the Configuration Template Request drop-down list, select **Begin with config**.

The Templatize Config page appears.

2. Enter or copy and paste your Jinja configuration in the space provided for it.

The wizard parses the parameters in your configuration and generates a variables tree in the Detected Variables panel.

NOTE: You can also download a sample template from this page.

NOTE: When you paste the Jinja template, the Configuration Designer detects the keywords **post_config**, **pre_config**, and **diff_config**, automatically. If the configuration template contains any one of these three keywords, the template will enable the **Diff Config** feature.

3. Review your configuration and edit it as needed. The wizard accordingly updates the variables in the Detected Variables panel. Click **Next**.

The Customize Variables page appears.

4. Select any variable to update. You can update different attributes of your template, such as the Yang and data types. You can also add default values and descriptions. See [Table 6 on page 17](#) for sample fields and their descriptions.

5. After completing your configuration, click **Next**.

The Generate UI page appears and generates the data model according to your values and displays as read-only. You can drag and drop the field labels to reorder the UI.

NOTE: If you edit an existing template and change its data model, then you can generate a new UI for it by clicking **Re-generate ui**. If you do not want a new UI, skip to the next step.

6. Click **Next**.

The Validate Template page appears.

7. Enter values that you want to validate, and ensure that the configuration template is displayed with the correct values.

8. Click **Validate**.

The Rendered Config page appears and the configuration template is generated using the values that you entered.

9. Make sure your data in the configuration template is complete and correct.

10. Click **Yes, it looks good** to close the page. If any parameter value in the configuration template needs to be changed, click **No, it needs change** to return to the previous page.

11. Click **Next**.

The Review Template page is displayed. It contains three tabs—Jinja Template, Data Model, and View Def. You can click through the tabs to view and update your Jinja template, data model, and the view definition.

12. Click **Done** to save your configuration template.

The Designs page is updated with the new configuration template and its status shows as **Validated**. You can monitor and manage the new configuration template from the Configuration Design page.

NOTE: You must publish the configuration template for it to be available for the Resource Designer to create virtualized network function (VNF) packages. See [“Publishing Configuration Templates” on page 23](#).

Table 6: Sample Fields on the Customize Variables Page

Field	Description
Detected Variables	<p>Edit the variable name. A configuration template contains variables that get replaced with values when a template is rendered. The Configuration Designer automatically generates these variables from your Jinja configuration.</p> <p>You can edit the variable name.</p> <p>Example: left_interface</p>

Table 6: Sample Fields on the Customize Variables Page (*continued*)

Field	Description
Yang Type	<p>Select an appropriate Yang type from the drop-down list. A Yang module defines a data model through its data, and through the hierarchical organization and constraints on that data. It uses a hierarchical, tree-based structure with the following nodes:</p> <ul style="list-style-type: none"> • leaf node—Contains a single value of a specific type • leaf-list node—Contains a sequence of leaf nodes • container node—Contains a grouping of related nodes containing only child nodes, which can be any of the six node types • list node—Contains a sequence of list entries, each of which is uniquely identified by one or more key leafs • choice node—Contains a set of alternatives, only one of which may exist at any one time • case node—Contains branches of the choice node
Data Type	<p>Select an appropriate data type based on your variable. In Yang, each leaf and leaf-list node includes the type statement to identify the data type for valid data for that node. Yang defines a set of built-in types and also provides the typedef statement for defining a derived type from a base type, which can be either a built-in type or another derived type.</p> <ul style="list-style-type: none"> • String—Human-readable string • Boolean—True or false • Init8—8-bit signed integer • Init16—16-bit signed integer • Init32—32-bit signed integer • Init64—64-bit signed integer • Uint8—8-bit unsigned integer • Uint16—16-bit unsigned integer • Uint32—32-bit unsigned integer • Uint64—64-bit unsigned integer • Enumeration—Enumerated strings with associated numeric values • Inet: ip-address—192.0.2.101 • Inet: ip-prefix—192.0.2.0/24 • Empty—A leaf that does not have any value
Display Name	Specify the name of the variable as you want it to display.

Table 6: Sample Fields on the Customize Variables Page (*continued*)

Field	Description
Key	Specify the key to be associated with the variable. Keys are identifiers used in defining list entries in the Yang data hierarchy. They help distinguish one list entry from another.
Required	Specify if the variable is mandatory.
Default Value	Specify the default value for the variable.
Pattern	Specify the regular expression (regex pattern) if the data type of the variable is string. Example: <code>^[a-z][A-Z]</code>
Information	This field displays values only if the data type of the variable is enumeration. When you select the data type as enumeration, you need to specify the values for the enumeration list and these values are displayed in the Information column. You can also edit the enumeration list. Example: <code>["abc","def"]</code>
Description	Enter a meaningful description for the variable. Example: Firewall policy information

To create an actual configuration for a device, you must log in to Administration Portal or Customer Portal. You must enter the actual values for the configuration in the configuration template. The configuration template then renders the actual values. You can click on stage2 configuration to view the actual configuration.

To delete an actual configuration for a device, you must login to Administration Portal or Customer Portal and execute the delete command, remove command or an alternate command for the configuration. The command to delete a configuration depends on the existing configuration on the device.

RELATED DOCUMENTATION

[Configuration Designer Overview | 9](#)

[Designing Templates with a YANG Configuration | 20](#)

Designing Templates with a YANG Configuration

You can design a configuration template either by using your own YANG model or by using the YANG model generated by the Configuration Designer. The Configuration Designer provides a wizard that takes you through a step-by-step procedure to create a configuration template. You can design multiple templates by creating requests and launching respective wizards from them.

To design a template using your own data model, make sure to have your data model schema and Jinja (a template engine for Python) template content ready.

Before you begin, create a configuration template request. See [“Creating Requests for Configuration Templates” on page 13](#).

To design a configuration template with your own YANG model:

1. From the Configuration Template Request drop-down list, select **Begin with YANG**.

The Enter YANG Schema page appears.

2. Enter or copy and paste your YANG schema in the space provided for it. Click **Next**.

The Enter Jinja Template page is displayed.

3. Enter or copy and paste your Jinja template content in the space provided for it. Click **Next**.

NOTE: You can also download a sample template from this page.

NOTE: When you paste the Jinja template, the Configuration Designer detects the keywords **post_config**, **pre_config**, and **diff_config** automatically. If the configuration template contains any one of these three keywords, the template will enable the **Diff Config** feature.

4. Click **Next**.

The Generate UI page appears and generates a UI page based on your YANG schema and displays a read-only view. The fields on this page map to the parameters in the configuration template. You can drag and drop the field labels to reorder the UI.

NOTE: If you edit an existing template and change its data model, then you can generate a new UI for it by clicking **Re-generate ui**. If you do not want a new UI, skip to the next step.

5. Click **Next**.

The Validate Template page appears.

6. Enter values that you want to validate. See [Table 7 on page 21](#) for sample fields and their descriptions. Click **Validate**.

A configuration template is generated using the values that you entered.

7. In the Validate Template page, make sure your data in the template is complete and correct.
8. Click **Yes, it looks good** to close the page. If any parameter value in the configuration template needs to be changed, click **No, it needs change** to return to the previous page.
9. Click **Next**.

The Review Template page is displayed. It contains three tabs—Jinja Template, Data Model, and View Def. You can click through the tabs to view and update your Jinja template, data model, and view definition.

10. Click **Done** to save your configuration template.

The Designs page is updated with the new configuration template and its status shows as **Validated**. You can monitor and manage the new configuration template from the Configuration Design page.

NOTE: You need to publish the configuration template for it to be available for the Resource Designer to create virtualized network function (VNF) packages. See [“Publishing Configuration Templates” on page 23](#).

Table 7: Sample Fields on the Validate Template Page

Field	Description
Name Servers	Specify the fully qualified domain names (FQDNs) or IP addresses of one or more DNS name servers. Example: 10.0.2.15
NTP Servers	Specify the FQDNs or IP addresses of one or more NTP servers. Example: ntp.example.net

Table 7: Sample Fields on the Validate Template Page (*continued*)

Field	Description
Time Zone	Specify the time zone for your virtual machine. Example: UTC
Enable Default Screens	For a centralized deployment, select True to enable the default screens security profile for the destination zone or False to disable default screening. Example: False NOTE: You cannot configure this setting for a distributed deployment.
Enable Re-filter	Select True to enable a stateless firewall filter that protects the Routing Engine from denial-of-service (DoS) attacks or False to allow DoS attacks. Example: True
Loopback Addr	Specify an IPv4 or IPv6 loopback address for the management interface of your virtual machine. Example: 192.0.2.25
Hostname	For a centralized deployment, specify the hostname of your virtual machine that contains the vSRX VNF. The hostname has no limit on the number of characters and accepts letters, numbers, and symbols. Example: vm-vsrx NOTE: For a distributed deployment, the vSRX application resides on the NFX250 device, and you cannot configure this setting.
Syslog Servers	Specify the FQDNs or IP addresses of one or more system log servers. Example: 192.0.2.55
Right Interface	Specify the identifier of the interface receiving data transmitted by the host. Example: GigabitEthernet3
Left Interface	Specify the identifier of the interface that transmits data to the host. Example: GigabitEthernet2
Allowed Prefix List	

Table 7: Sample Fields on the Validate Template Page (*continued*)

Field	Description
Ping Prefix List	<p>If you set the Enable Re-filter field to True, specify the routes that the Junos Space Virtual Appliance uses for ping operations when it discovers the vSRX VNF.</p> <p>Example: 10.0.2.1/24</p>
SNMP Prefix list	<p>If you set the Enable Re-filter field to True, specify the routes that the Junos Space Virtual Appliance uses for SNMP operations when it discovers the vSRX VNF.</p> <p>Example: 10.0.2.0/24</p>
Space Servers	<p>If you set the Enable Re-filter field to True, specify the IP addresses of the virtual machines that contain the Junos Space Virtual Appliances.</p> <p>Example: 10.0.2.50</p>

RELATED DOCUMENTATION

[Configuration Designer Overview](#) | 9

[Designing Templates with a Configuration](#) | 15

Publishing Configuration Templates

After you have designed a configuration template, you need to publish it. Only published configuration templates are available to the Resource Designer for creating virtualized network function (VNF) packages.

Use one of the following methods to design a configuration template:

- Using a data model. Choose this method when you already have a data model for your configuration template. See [“Designing Templates with a YANG Configuration” on page 20](#).
- Using your working configuration. Choose this method when you have a Jinja template but want the Configuration Designer to generate a data model for your configuration template. See [“Designing Templates with a Configuration” on page 15](#).

To publish a configuration template:

1. Select **Home> Designs**.

The Configuration Template Designs page appears. All the configuration templates are displayed in a table.

2. Select the configuration template (with the status as Validated) that you want to publish to the Resource Designer.
3. Select **Publish** from the Edit drop-down list.

Your configuration template is published and available to be used by the Resource Designer. Its status changes from **Validated** to **Published**.

RELATED DOCUMENTATION

| [Configuration Designer Overview](#) | 9

Managing Configuration Templates

IN THIS CHAPTER

- [About the Designs Page for the Configuration Designer | 25](#)
- [Cloning Configuration Templates | 27](#)
- [Deleting Configuration Template Designs | 28](#)

About the Designs Page for the Configuration Designer

To access this page, click **Home > Designs**.

Use the Designs page to manage configuration template designs that you have saved or published.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the configuration template designs. [Table 8 on page 26](#) describes the fields on the Configuration Template Designs page.
- Modify a configuration template design that you published or saved using the configuration. Click **Edit** from the drop-down list at the end of the appropriate row and make your updates. See [“Designing Templates with a Configuration” on page 15](#).
- Modify a configuration template design that you published or saved using the YANG model. Click **Edit** from the drop-down list at the end of the appropriate row and make your updates. See [“Designing Templates with a YANG Configuration” on page 20](#).
- Publish a configuration template. See [“Publishing Configuration Templates” on page 23](#).
- Clone a configuration template. See [“Cloning Configuration Templates” on page 27](#).
- Delete a configuration template. See [“Deleting Configuration Template Designs” on page 28](#).

Field Descriptions

Table 8 on page 26 provides guidelines on using the fields on the Designs page for the Configuration Designer.

Table 8: Fields on the Configuration Template Designs Page

Field	Description
Template	View the configuration template name. The name can be a string of alphanumeric characters, dashes, and spaces. Example: srx-lan-to-wan-config
Family	View the device family supported by the configuration template. Example: juniper-srx
Vendor	View the vendor that the configuration template supports. Example: Juniper Networks
Output Format	View the format used by the configuration template. It can be one of the following: <ul style="list-style-type: none"> • CLI (Command-line interface) • XML (Extensible Markup Language) • Native - Default file format of the application that we use to create and save files. We use CLI plug-in and it is used for cms_plug-in.
Category	View the category for the configuration template. <ul style="list-style-type: none"> • VNF—A configuration template for the virtualized network function. • Device Template—A device template for the network function and this cannot be published to the Resource Designer. • Other—A configuration template for the network function other than VNF or device template.
Diff-Config	Use to compare configuration difference between the two configuration files. <ul style="list-style-type: none"> • Yes—Diff.Config feature is enabled for the template. • No—Diff.Config feature is disabled for the template.

Table 8: Fields on the Configuration Template Designs Page (*continued*)

Field	Description
Status	<p>View the configuration template status:</p> <ul style="list-style-type: none"> • In-Progress—Configuration template request was created but the template hasn't been validated. • Validated—Configuration Designer validated the configuration template and it is ready to be published. • Published—Configuration Designer published the configuration template and it is available to the Resource Designer for use.
Description	<p>View the configuration template description.</p> <p>Example: NFX Stage-1 configuration</p>

RELATED DOCUMENTATION

[Configuration Designer Overview | 9](#)

[About the Requests Page for the Configuration Designer | 12](#)

Cloning Configuration Templates

Cloning a template is useful when you want to create a configuration template that is similar to an existing one but with small differences. You can easily clone an existing template from the Designs page and customize it as needed.

To clone a configuration template design:

1. Select **Home>Designs**.

The Designs page appears.

2. Select the configuration template design that you want to clone, and click the clone icon at the top of the Designs page.

The Clone Template page appears.

3. Specify an appropriate name for your new configuration template. For example, uCPE-SRX NAT config.

4. Click **Save**.

A message is displayed indicating that the template was cloned successfully. The cloned configuration template appears on the Designs page.

If you want to edit the cloned configuration template, select the template and click **Edit** from the drop-down list at the end of the row.

RELATED DOCUMENTATION

[About the Designs Page for the Configuration Designer | 25](#)

[Designing Templates with a Configuration | 15](#)

[Designing Templates with a YANG Configuration | 20](#)

Deleting Configuration Template Designs

You can easily delete a configuration template design from the Designs page.

To delete a configuration template design:

1. Select **Home>Designs**.

The Designs page appears.

2. Select the configuration template design that you want to delete.

3. Click **Delete** from the drop-down list at the end of the row.

A page requesting confirmation for the deletion appears.

4. Click **Yes** to confirm that you want to delete the design.

The configuration template design is deleted.

RELATED DOCUMENTATION

[About the Designs Page for the Configuration Designer | 25](#)

3

PART

Resource Designer

Resource Designer Introduction | **30**

Creating VNF Packages | **34**

Managing VNF Packages | **50**

Resource Designer Introduction

IN THIS CHAPTER

- Resource Designer Overview | 30
- Using the Resource Designer | 32

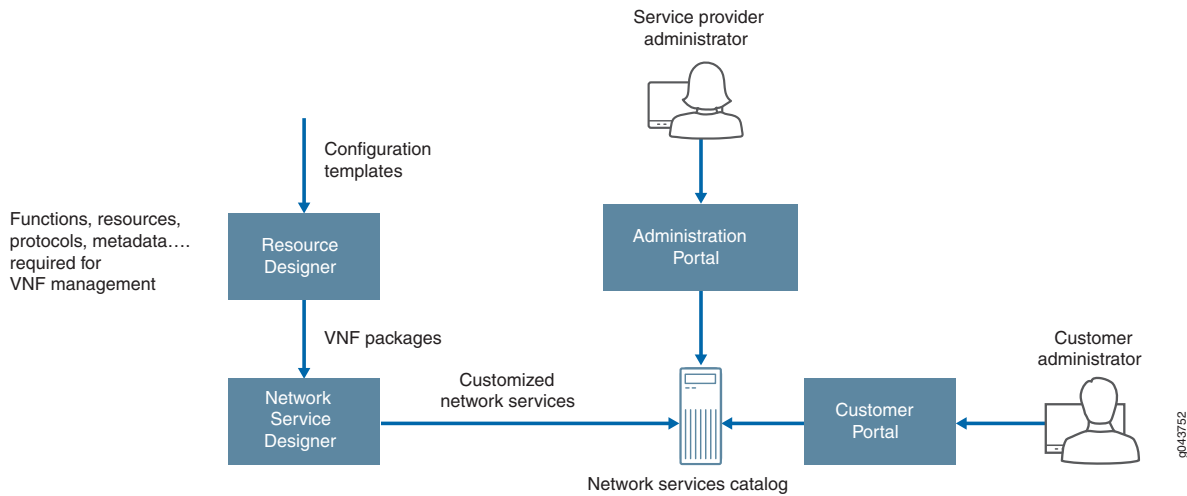
Resource Designer Overview

Configuration Designer, Resource Designer, and Network Services Designer (collectively known as Designer Tools) are a suite of GUI-based tools that enable network designers to support virtualized network functions (VNFs) and network services in Contrail Service Orchestration (CSO).

Resource Designer provides an intuitive GUI-based workflow that guides users with the Service Provider (SP) Administrator role as they provide the required information to create a VNF package. Resource Designer also validates the VNF package before it is published to Network Service Designer. Network Service Designer uses VNF packages to design customized network services that are published to the network services catalog, which contains a list of usable network services.

Service provider administrators access the network services catalog to assign a set of network services to their customers using Administration Portal. Finally, tenant users access the network services assigned to them using Customer Portal to manage their sites and services. [Figure 2 on page 31](#) shows the Resource Designer workflow.

Figure 2: Resource Designer Workflow



Users with the SP Administrator role can use Resource Designer to create and onboard a VNF package that can be used for defining network services. A VNF package is a set of metadata or templates designed for a specific vendor's VNF. Each VNF has its own combination of resources and performance characteristics. Having access to different levels of VNF packages can help you to design specific service-level agreements (SLAs) for your services. You can assign resources to VNFs using the vendor's data sheets as a basis.

A typical VNF package might include:

- **VNF base configuration template**, which is a configuration template that can be created in Configuration Designer:
 - To ensure correct startup and ongoing manageability of the VNF
 - For management IP address, SNMP, and system log configuration of the VNF
- **VNF descriptor (VNFD)**, which is a deployment template that describes a VNF in terms of its deployment and operational behavior requirements. VNFD is mainly used during the instantiation of a VNF and for lifecycle management of the VNF instance, and it includes the following properties:
 - **Connection points**—Represents the management interface, left interface, and right interface. Connections points are used to connect the virtual links.
 - **Virtual links**—Represents the management network link, left network link, and right network. Virtual links provide connectivity between VDUs.
 - **Virtual deployment units (VDUs)** and a topology showing how the VDUs are connected.
VDUs are basic part of VNFs and are used to host the network function.
 - **Allocated CPU and memory**
 - **Required storage**
 - **Names and types of VNF images**

- Deployment flavors—A differentiated option such as Gold, Silver, or Bronze with an appropriate SLA metric.
- VNF auto-scale policies
- **VNF Manager plug-in**, which is a plug-in type and name. For example, a VNF Manager for VNF lifecycle management.
- **Supported function chains**, which are sequences of network functions, such as firewall, NAT, or WAN optimization, that the VNF packages offers.

Some VNFs, like vSRX, support multiple functions and service chains. For example, vSRX can be deployed in the context of multiple functions such as firewalls, carrier-grade NAT, IDP, UTM, malware, and others.

RELATED DOCUMENTATION

[Access Designer Tools | 4](#)

[Change Your Designer Tools Password | 6](#)

[Using the Resource Designer | 32](#)

Using the Resource Designer

Use the Resource Designer to create a VNF package or modify an existing one. Follow these steps to get started with the Resource Designer:

- Learn about the Resource Designer. See [“Resource Designer Overview” on page 30](#).
- Log into the Resource Designer. See [“Access Designer Tools” on page 4](#).

To create a VNF package:

1. Create a request for a VNF package. See [“Creating Requests for VNF Packages” on page 37](#).
2. Design a VNF package. See [“Designing VNF Packages” on page 39](#).
3. Publish the VNF package to the Network Service Designer. See [“Publishing VNF Packages” on page 49](#).

You can also perform the following tasks using the Resource Designer:

- Clone a VNF package. See [“Cloning VNF Packages” on page 52](#).
- Import a VNF package. See [“Importing VNF Packages” on page 52](#).
- Export a VNF package. See [“Exporting VNF Packages” on page 53](#).

RELATED DOCUMENTATION

| [Resource Designer Overview](#) | 30

Creating VNF Packages

IN THIS CHAPTER

- [About the Requests Page for the Resource Designer | 34](#)
- [VNF Overview | 35](#)
- [Creating Requests for VNF Packages | 37](#)
- [Designing VNF Packages | 39](#)
- [Adding VNF Managers | 47](#)
- [Publishing VNF Packages | 49](#)

About the Requests Page for the Resource Designer

To access this page, click **Home > Requests**.

Use the Requests page to request a new VNF package. A VNF package is a package of device metadata or templates for a specific vendor VNF. You can also view the open VNF package requests with the request name, date, and time.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a request to design a VNF package. See [“Creating Requests for VNF Packages” on page 37](#).
- Design a new VNF package. See [“Designing VNF Packages” on page 39](#).

Field Descriptions

[Table 9 on page 35](#) provides guidelines on using the fields on the Requests page for the Resource Designer.

Table 9: Fields on the Requests Page for the Resource Designer

Field	Description
Requests Page	
New Request	<p>Click to request a new VNF package.</p> <p>The New Request page allows you to define the requirements for your VNF package.</p>
VNF Package Request	
Begin	<p>Hover over the bottom right of the package and click to design a VNF package.</p> <p>The Basic VNF Information page appears. You can specify the basic information for the VNF package, supported VNF, and function chains.</p>
Delete	<p>Hover over the bottom right of the package and click to delete a VNF package request.</p> <p>The VNF package request is deleted.</p>

RELATED DOCUMENTATION

[Resource Designer Overview](#) | 30

[Using the Resource Designer](#) | 32

VNF Overview

A virtualized network function (VNF) is a software application used in a Network Functions Virtualization (NFV) implementation that has well defined interfaces, and provides one or more component networking functions in a defined way. For example, a security VNF provides Network Address Translation (NAT) and firewall component functions.

For Contrail Service Orchestration (CSO) in a centralized deployment model, you design network services for customers based on VNFs. Each VNF used in the network service is deployed in its own virtual machine (VM). The connections between VNFs depend on how VIMs define them over the NFV Infrastructure (NFVI).

For CSO in distributed deployment model, the Open vSwitch (OVS) bridges are used within the NFX hypervisor.

You can specify the following required resources for a VNF package when you create it in Resource Designer.

- Number of virtual CPUs
- Virtual memory (MB)
- Virtual disk capacity (MB)
- License cost

CSO supports a range of Juniper Networks and third-party VNFs. Vendors can provide multiple versions of a VNF that offer differentiated performance. You can see available VNFs and their specifications and resource requirements in the VNF catalog of the Network Service Designer tool. [Table 10 on page 36](#) lists the VNFs that are currently supported by CSO.

Table 10: VNFs Supported by CSO

Vendor Name	VNF Name	Network Functions Supported	Deployment Model Support	Element Management System Support
Juniper Networks	<ul style="list-style-type: none"> • vSRX • vSRX managed by Junos Space • vSRX on uCPE 	<ul style="list-style-type: none"> • Network Address Translation • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified Threat Management (UTM) 	<ul style="list-style-type: none"> • Centralized deployment • Distributed deployment 	EMS microservice
Linux	IP Table	<ul style="list-style-type: none"> • NAT • Firewall 	Centralized deployment	EMS microservice
Linux	HAProxy	Load Balancer	Centralized deployment	EMS microservice
Cisco	Cisco1000v	Firewall	Centralized deployment	Junos Space Network Management Platform
Riverbed	<ul style="list-style-type: none"> • Riverbed • Riverbed-NFX150 	WAN optimization	Distributed deployment NOTE: Supported on NFX150 and NFX250 platforms only	EMS microservice

Table 10: VNFs Supported by CSO (continued)

Vendor Name	VNF Name	Network Functions Supported	Deployment Model Support	Element Management System Support
Fortinet	<ul style="list-style-type: none"> Fortinet-no-oam Fortinet-oam 	Firewall without WAN optimization	<ul style="list-style-type: none"> SD-WAN deployment Distributed deployment <p>NOTE: Supported on NFX150 and NFX250 platforms only</p>	EMS microservice
Ubuntu	<ul style="list-style-type: none"> Ubuntu-fw Ubuntu-fw-NFX150 	Firewall without WAN optimization	<ul style="list-style-type: none"> SD-WAN deployment Distributed deployment <p>NOTE: Supported on NFX150 and NFX250 platforms only</p>	EMS microservice

RELATED DOCUMENTATION

[Creating Requests for VNF Packages](#) | 37

Creating Requests for VNF Packages

You can create a configuration template by making a request. A request allows you to define the basic requirements for the VNF package, including the vendor and the supported device family.

1. Click **Home > Requests > New Requests**.
2. Complete the configuration according to the guidelines provided in [Table 11 on page 38](#).
3. Click **Create**.

A new VNF package request is created. If you want to discard your changes, click **Cancel** instead.

Table 11: Fields on the New Request Page

Field	Description
Name	Specify a unique name for your VNF package using a string of alphanumeric characters, dashes, and spaces. Example: vSRX
Description	Enter a description for your VNF package. Make this description as clear and useful as possible for all administrators.
Vendor	Select the vendor for the VNF package. Example: Juniper Networks
Target family	This field is auto-populated with the device family supported by the vendor. Example: juniper-nfx
VNF Package Capability Version	Select the version of VNF package. The available options are: <ul style="list-style-type: none"> • 1.0—Does not support NFX150 device. • 1.1—Supports NFX150 device.
Vendor Logo	This field is auto-populated with the vendor logo for the selected vendor. You can also click Select files to upload logos for any new vendor that you add to the vendor list through an API.

RELATED DOCUMENTATION

[Resource Designer Overview | 30](#)
[About the Requests Page for the Resource Designer | 34](#)
[Designing VNF Packages | 39](#)

Designing VNF Packages

IN THIS SECTION

- [Creating Basic VNF Information | 39](#)
- [Adding Flavor Parameters | 42](#)
- [Adding Standard and Custom Functions | 44](#)
- [Designing a Supported Function Chain | 44](#)
- [Viewing the Summary of VNF Packages | 46](#)

You can design a VNF package using the Resource Designer. The Resource Designer provides a VNF package wizard that takes you through a step-by-step procedure to create your VNF package. You can design multiple VNF packages by creating requests and launching respective wizards from them.

Before You Begin

Create a request to design a VNF package. See [“Creating Requests for VNF Packages” on page 37](#).

To design a VNF package, you need to perform the following:

Creating Basic VNF Information

You can click through each tab on this page to specify basic VNF information, flavor parameters, standard functions, custom functions, and supported function chains for the VNF package.

To create basic VNF information:

1. Click **Home > Requests**. You see the Requests page and can view the number of open requests that you created to design a VNF package.
2. Select **Begin** from the appropriate open VNF request wizard.

You are directed to the **Configure** page. It contains three tabs—Enter Basic Information, Select Functions, and Design Function Chains. You can click through the tabs to specify basic VNF information, flavor parameters, standard functions, custom functions, and supported function chains that are required for the VNF package.

3. Complete the configuration according to the guidelines provided in [Table 12 on page 40](#).

Table 12: Fields on the VNF Information Page

Field	Description
VNFD Name	<p>Displays the VNF Package request name that you provided. A VNFD is a deployment template that describes the deployment and operational behavior of the VNF. Some of the VNFs are listed below:</p> <ul style="list-style-type: none"> • Juniper Networks vSRX—Supports both centralized and distributed deployments. • LxCIPtable—A free, third-party VNF based on Linux IP tables; supports only centralized deployments. • CSR-1000V—Cisco Cloud Services Router 1000V Series; supports only for centralized deployments. • HAProxy—An open source, reliable solution that offers high availability and proxy service for TCP applications.
VNF Package Capability Version	<p>Displays the VNF package capability version.</p> <p>Example: 1.1</p>
VNF Manager	<p>Select the VNF configuration manager. A VNF manager represents plug-in information, which includes plug-in type and name and is extracted from an existing VNF. The VNF manager manages the life cycle management of VNFs including third-party VNFs. Some of the VNF managers are listed below:</p> <ul style="list-style-type: none"> • Viptables • viptables_v2 • generic_v2 • JunosSpace • riverbed_v2 • Space_14_2 • Space_DMS_CMS_2_0
Deployment Type	<p>Select the deployment type.</p> <ul style="list-style-type: none"> • uCPE only—Select this option for a distributed deployment. • vCPE only—Select this option for a centralized deployment.
Basic Configuration	<p>Select the basic configuration template. A basic configuration template ensures correct startup and ongoing manageability, management IP address, SNMP, and system logs and is created by using the Configuration Designer.</p> <p>Example: vSRX Space firewall config</p>

Table 12: Fields on the VNF Information Page (*continued*)

Field	Description
BootStrap Configuration	<p>Select the bootstrap configuration as a reference to the configuration template for the bootstrap configuration to be used when the VNF is spawned. Bootstrap configuration template is created using the Configuration Designer.</p> <p>Example: default-domain</p>
Network Configuration	<p>Select the network configuration as a reference to the configuration template for the networking configuration to be staged on the VNF. Network configuration template is created using the Configuration Designer.</p> <p>Example: default-domain</p>
OAM Ports	Enter one or more OAM port names for the distributed deployment VNF package.
VNF Capability	<p>Select one or more capabilities supported for the software release of the VNF.</p> <ul style="list-style-type: none"> • SRIOV-DATA—Supports SRIOV and its data interfaces • SRIOV-MGMT—Supports SRIOV and its management interfaces • CDROM-Bootstrapping—Supports bootstrap configuration through CDROM ISO • UserData-Bootstrapping—Supports bootstrap configuration using CloudInit • MGMT-VLAN-Tagged-Traffic—Supports VLAN tagged traffic and its management interfaces • DATA-VLAN-Tagged-Traffic—Supports VLAN tagged traffic and its data interfaces • Transparent-mode—Supports insertion in transparent mode • L3-mode—Supports Layer 3 mode • Direct-OAM-Reachability—Enables service chaining of a third-party VNF. This option is supported only for centralized deployments(vCPE-Only).
Connection Points	<p>Specify the connection points for the VNF package. You can also specify whether to enable or disable the TCP offloads for the VNF connection points. This option is supported only for distributed deployments(uCPE-Only).</p> <ul style="list-style-type: none"> • internal—For internal management network. • oob—For out-of-band (OOB) management network. • mgmt-interface—For Operation, Administration, and Maintenance (OAM) network. • left-interface—For incoming traffic to the VNF. • right-interface—For outgoing traffic from the VNF. <p>NOTE:</p> <ul style="list-style-type: none"> • You can configure only left interface and right interface for centralized deployment model. • You can re-order the connection points as per the port index(0-4).

Table 12: Fields on the VNF Information Page (continued)

Field	Description
Package Flavors	Click Add icon. The New Flavor Parameters window appears. Add the flavor parameters to the VNF package.

Adding Flavor Parameters

You can create a package flavor (for example, Gold, Silver, or Bronze) and assign the flavor to the VNF. Flavor parameters are computational properties of virtual deployable units (VDUs) and each package flavor supports only one virtual deployable unit (VDU). You can specify different resources for each VDU such as number of CPUs, allocated memory size, and allocated disk size. You can also specify a VNF image for VDU for vCPE devices and specify the bootstrap script for uCPE devices.

To add flavor parameters:

1. From the Package Flavors field on the Basic VNF Information page, click **Add**.

The New Flavor Parameters wizard appears.

2. Complete the configuration according to the guidelines provided in [Table 13 on page 42](#).

3. Click **Save**. If you want to discard your changes, click **Cancel** instead.

A graphical representation of the wizard is displayed and shows the VNF flavor name and the required virtual resources.

4. Click the edit icon at the top of the wizard to modify the flavor parameters. If you want to close the wizard, click the **X** icon.

5. Click **Next**.

The Select Functions page appears with the standard and custom functions.

Table 13: New Flavor Parameters

Field	Description
Flavor Name	Specify the name of the package flavor for the VNF. Example: Gold, Silver, or Bronze

Table 13: New Flavor Parameters (*continued*)

Field	Description
Image Name	<p>Select the VNF image file.</p> <p>Click Upload Image to upload VNF images for the centralized deployment through Administration Portal. See <i>Uploading a Device Image</i>.</p> <p>Example: csr1000v-img</p>
CPU	<p>Specify the number of virtual CPUs required for the VNF using a numeric value without a fractional component.</p> <p>Example: 4 CPU cores</p>
Memory	<p>Specify the virtual memory size required for the VNF in megabytes (MB) using a numeric value without a fractional component.</p> <p>Example: 4096 MB</p>
Disk	<p>Specify the virtual disk capacity required for the VNF in gigabytes (GB) using a numeric value without a fractional component.</p> <p>Example: 128 GB</p>
Bootstrap Script	<p>Bootstrap script is supported only for the uCPE deployment. You can add a bootstrap script to support a third-party VNF for the uCPE devices.</p> <p>Click Add.</p> <p>The Edit Bootstrap Script wizard appears.</p>
Edit Bootstrap Script	<p>Edit and save the script. If you want to discard your changes, click Cancel instead.</p>
Script Type	<p>Select the supported bootstrap script for the third-party VNF. Supported bootstrap script types are:</p> <ul style="list-style-type: none"> • bash • sh • python • perl <p>The default script type is bash.</p>

Adding Standard and Custom Functions

To add standard and custom functions:

1. On the Select Functions page, from the Standard Functions wizard, select the function category from the Category drop-down list. To select all function categories, click **All**.
 - There are four function categories: Security, Switching, Networking, and Routing.
 - When you select a function category, a list of network functions that belong to the function category is displayed in the wizard. For example, NAT, Firewall, Anitspam, and Antivirus are displayed when you select **Security**.
2. Select the network function that you want to add to the VNF package individually. If you want to select all network functions, click **Select All**.
3. Click **Add Custom Function** to add a custom function if the predefined category does not have the network function the user wants to use.

The Edit Custom Function wizard appears.

- a. Specify the name of the custom function.
 - b. Select the function category.
 - c. Click **Save**. If you want to discard your changes, click **Cancel** instead.
4. Click **Next**.

The Design Function Chains page appears.

Designing a Supported Function Chain

To design a supported function chain:

1. On the Design Function Chains page, a list of standard and custom functions are displayed in the Function Palette wizard at the bottom of the page.
2. Drag any standard or custom function from the Function Palette wizard at the bottom of the page and drop it on the Supported Function Chains workspace at the top of the page in the order that they should appear. If you drop two or more functions to the workspace, the functions will automatically connect with a connection arrow to form a service chain.
3. Click the edit icon on the network function to add a configuration template for the network function.

The Config Template wizard appears.

4. From the Template Name drop-down list, select the network configuration template to be staged on the VNF. Some configuration templates are listed as follows:
 - **IPTable NAT config** —Configuration template designed for NAT.
 - **IPTable Firewall config** —Configuration template designed for firewall.
 - **FireFly UTM config**—Configuration template designed for firefly UTM.
 5. Click **Save**. If you want to discard your changes, click **Cancel** instead.
 6. Using the guidelines in [Table 14 on page 46](#), specify assurance parameters for the VNF on the left panel of the page. Assurance parameters are used to provide SLA performance and scale indicators from the data sheet for the VNF. Each VNF flavor can achieve the SLA performance and scale indicators. When you design a network service in Network Service Designer, these values are used to determine how well your design meets your target performance for the network service.
 7. Click **Next**.
- The service chain is created and displayed in the same page. For example, Antispam-UTM-NAT-Antivirus.
8. If you use more than one network function in the VNF package, click **Service Chain** to create the next combination of services.
 9. Repeat steps 4 through 6 to create the service chain.
 10. Repeat steps 6 through 9 until you have covered all possible combinations of the network functions including each function on its own.
 11. Click **Next**.

The Review VNF Package page appears.

Table 14: Assurance Parameters of the Network Function

Field	Description
Service Mode	<p>Select the mode of network service that can be configured for the VNF.</p> <ul style="list-style-type: none"> • Transparent—Used for services that do not modify the packet. Also known as <i>bump-in-the-wire</i> or <i>Layer 2 mode</i>. Example: Firewall, IDP, and so on. • In-Network—Provides a gateway service where packets are routed between the service instance interfaces. Example: NAT, Layer 3 firewall, load balancer, HTTP proxy, and so on. • In-Network-NaT—Similar to in-network mode, but return traffic does not need to be routed to the source network. In-network-nat mode is particularly useful for NAT service. <p>The default service mode is In-Network.</p>
Bandwidth	<p>Specify the data rate for the virtualized network function in megabytes per second (Mbps) or gigabytes per second (Gbps).</p> <p>Example: 185</p>
Latency	<p>Specify the time a packet takes to traverse the virtualized network function in milliseconds (ms).</p> <p>Example: 5.8</p>
Sessions	<p>Specify the maximum number of sessions concurrently supported for the VNF.</p> <p>Example: 25,000</p>
License cost	<p>Specify the license cost for the virtualized network function in USD.</p>

Viewing the Summary of VNF Packages

To view the summary of a VNF package:

1. On the Review VNF package page, you can view the VNF basic information, number of standard and custom network functions available, number of standard and custom network functions selected, and the number of service chains created for the VNF package.
2. Click the edit icon on top corner of each wizard to edit the individual fields of VNF basic information, functions, and service chains.
3. Click **Done**.

A success message is displayed.

The VNF package is added in the Designs page and the status of the package changes to **Validated**.

RELATED DOCUMENTATION

Resource Designer Overview	 30
Creating Requests for VNF Packages	 37
Adding VNF Managers	 47
Publishing VNF Packages	 49

Adding VNF Managers

Resource Designer allows a service provider to add a new VNF manager, including third-party VNF manager plug-in information, from the Designs page.

To clone a VNF package design:

1. Click **Home > Requests**. You see the Requests page and can view the number of open requests that you created to design a VNF package.
2. Select **Begin** from the appropriate open VNF request wizard.
The Basic VNF Information page appears.
3. Click **Add VNF Manager**.
The New VNF Manager wizard appears.
4. Complete the configuration according to the guidelines provided in [Table 15 on page 47](#).
5. Click **Save**. If you want to discard your changes, click **Cancel** instead.

Table 15: Add VNF Manager

Field	Description
VNF Manager Name	Select the VNF configuration manager. A VNF manager represents plug-in information, which includes plug-in type and name. Example: JunosSpace

Table 15: Add VNF Manager (*continued*)

Field	Description
Username	Specify the username that you configured for the VNF manager.
Password	<p>Specify the password that you configured for the VNF manager.</p> <p>You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters.</p>
Plug In	<p>Select the plug-in type.</p> <ul style="list-style-type: none"> • Built-In—Built-in plug-in name. • External Plugin—Python plug-in package name.
Built-In	<p>PlugIn Name—Specify the built-in plug-in name.</p> <p>Example: viptables</p>
External Plugin	<ul style="list-style-type: none"> • PlugIn Name—Specify the python VNF manager plug-in name, which is used to provide additional features on top of the existing built-in VNF manager. The naming convention of the package name is <Vendor><VNFM Name><Version>, and this can be installed through the PIP tool. • Display Name—Specify the display name for the VNF manager. • Description—Enter a description for your VNF manager. Make this description as clear and useful as possible for all administrators. • Vendor—Specify the vendor name that you want the external plug-in to support. • EMS Name—Specify an EMS name for the EMS instance that manages the VNF instances instantiated from the VNF package. Each POP is associated with an EMS instance to manage instances instantiated in the POP. The same EMS instance is shared by multiple POPs or dedicated EMS instances for each POP, and the EMS name is used to find the right EMS instance to manage the VNF instances in a specific POP. <p>Example: Junos Space 15.1 and Versa Director 1.1.</p>

RELATED DOCUMENTATION

[About the Designs Page for the Resource Designer | 50](#)
[Designing VNF Packages | 39](#)

Publishing VNF Packages

After you have designed a VNF package, you need to publish the designed VNF package to the Network Service Designer. Only published VNF packages are available from the Network Service Designer.

To publish a VNF package to the Network Service Designer:

1. Select **Home > Designs**.

The VNF Package Designs page appears. All of the VNF packages are displayed in a table.

2. Select the VNF package (with the status as Validated) that you want to publish to the Network Service Designer.

3. Select **Publish to NSD** from the drop-down list at the end of the row.

Your VNF package is published and available to be used by the Network Service Designer. The status of the package changes from **Validated** to **Published**.

RELATED DOCUMENTATION

[Resource Designer Overview](#) | 30

[Creating Requests for VNF Packages](#) | 37

[About the Designs Page for the Resource Designer](#) | 50

Managing VNF Packages

IN THIS CHAPTER

- [About the Designs Page for the Resource Designer | 50](#)
- [Cloning VNF Packages | 52](#)
- [Importing VNF Packages | 52](#)
- [Exporting VNF Packages | 53](#)
- [Deleting VNF Packages | 54](#)

About the Designs Page for the Resource Designer

To access this page, click **Home > Designs**.

Use the Designs page to manage VNF packages that you have saved or published. You can also view the information about each VNF package.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the VNF package information. See [Table 16 on page 51](#) for field descriptions of the Designs page.
- Export a VNF package from the Resource Designer. See [“Exporting VNF Packages” on page 53](#).
- Import a VNF package to the Resource Designer. See [“Importing VNF Packages” on page 52](#).
- Clone a VNF Package. See [“Cloning VNF Packages” on page 52](#).
- Modify the VNF package that you saved or published using the **Edit** option from the drop-down list. See [“Designing VNF Packages” on page 39](#).
- Publish a VNF package. See [“Publishing VNF Packages” on page 49](#).
- Delete a VNF package. See [“Deleting VNF Packages” on page 54](#).

Field Descriptions

Table 16 on page 51 provides guidelines on using the fields on the Designs page for the Resource Designer.

Table 16: Fields on the Designs Page for the Resource Designer

Field	Description
VNF Name	View the VNF package name. The name can be a string of alphanumeric characters, dashes, and spaces. Example: ucpe-vSRX
Vendor	View the vendor that the VNF package supports. Example: Juniper Networks
Family	View the device family supported by the VNF package. Example: juniper-srx
Date	View the data and time when the VNF design package was created. Example: 01/24/2017 12:01
Status	View the VNF package status. <ul style="list-style-type: none"> • Started —An empty VNF package was created and the components need to be added. • In-Progress — A VNF package was created but the package is not validated. • Validated— Resource Designer validated the VNF package and it is ready to be published. • Published—Resource Designer published the VNF package and it is available from the Network Service Designer.

RELATED DOCUMENTATION

[Resource Designer Overview](#) | 30

[About the Requests Page for the Resource Designer](#) | 34

Cloning VNF Packages

You can clone a VNF package from the Designs page when you want to quickly create a copy of an existing VNF package and modify its parameters including the name of the VNF.

To clone a VNF package design:

1. Select **Home > Designs**.

The Designs page appears.

2. Select the VNF package design that you want to clone, and click the clone icon at the top of the Designs page.

The Clone VNF Package wizard appears.

3. Specify an appropriate name for your new VNF package.

4. Click **Save**.

A success message is displayed. The cloned VNF package appears on the Designs page.

If you want to edit the cloned VNF package, select the VNF package and click **Edit** from the drop-down list at the end of the row.

RELATED DOCUMENTATION

[About the Designs Page for the Resource Designer | 50](#)

[Designing VNF Packages | 39](#)

Importing VNF Packages

You can import a VNF package design to the Designs page from third-party applications and VNF packages from another Resource Designer. A VNF package design retains its state when it is imported.

To import a VNF package design:

1. Select **Home > Designs**.

The Designs page appears.

2. Click the Import VNF package icon at the top of the Designs page.

The Import VNF wizard appears.

3. Click **Select files** to select the VNF JSON data file.

NOTE: You need to retain the file format as .json to successfully import the VNF package design to the Resource Designer.

4. Click **Import**. If you want to discard the import process, click **Cancel** instead.

A success message is displayed indicating that the VNF is imported. The imported VNF package appears on the Designs page.

RELATED DOCUMENTATION

[About the Designs Page for the Resource Designer | 50](#)

[Designing VNF Packages | 39](#)

Exporting VNF Packages

You can export a VNF package design from the Designs page when you want to use this VNF package in another Resource Designer that is running in another customer's server. A VNF package design retains its state when it is exported.

To export a VNF package design:

1. Select **Home > Designs**.

The Designs page appears with a list of VNF packages.

2. Select the VNF package design that you want to export.

3. Select **Export** from the drop-down list at the end of the row.

The VNF package JSON file opens at the bottom of the page.

4. Save the file to your computer.

You can modify the parameters and rename the JSON filename if required.

RELATED DOCUMENTATION

[About the Designs Page for the Resource Designer | 50](#)

[Designing VNF Packages | 39](#)

[Importing VNF Packages | 52](#)

Deleting VNF Packages

To delete a VNF package design:

1. Select **Home > Designs**.

The Designs page appears with a list of VNF packages.

2. Select the VNF package design that you want to delete.

3. Select **Delete** from the drop-down list at the end of the row.

A page requesting confirmation for the deletion appears.

4. Click **Yes** to confirm.

The VNF package design is deleted.

RELATED DOCUMENTATION

[Resource Designer Overview | 30](#)

[About the Designs Page for the Resource Designer | 50](#)

4

PART

Network Service Designer

Network Service Designer Introduction | 56

Creating Requests for Network Services | 58

Creating Network Services | 68

Managing Network Services | 94

Network Service Designer Introduction

IN THIS CHAPTER

- [Network Service Designer Overview | 56](#)
- [Using the Network Service Designer | 57](#)

Network Service Designer Overview

Configuration Designer, Resource Designer, and Network Services Designer (collectively known as Designer Tools) are a suite of GUI-based tools that enable network designers to support virtualized network functions (VNFs) and network services in Contrail Service Orchestration (CSO). Network Service Designer uses the VNF packages (created and published by Resource Designer) to design customized network services and then publish the services to the network services catalog. Users in CSO can then use the network services and service chains that are part of the network services catalog.

NOTE: A network service can be a single VNF providing a single service (for example, firewall or NAT), a single VNF providing two or more services (for example, firewall and UTM) or a chain of VNFs providing two or more services (for example, VNF1 provides NAT service, VNF2 provides firewall service, and so on)

With Network Service Designer you can:

- Create requests for new network services.
- Design customized network services for your customers.
- Design new standard network services that you can offer to all your customers.
- Update existing network services.
- Publish services to the network service catalog.
- Manage network services that you are designing or have published to the network catalog.
- Configure some basic parameters for the VNFs used in a network service and the virtual containers in which the VNFs reside.

After the service is published, SP Administrators can assign the service to tenants by using the CSO Administration Portal.

RELATED DOCUMENTATION

[Network Services and Service Chains Overview](#) | 58

[Access Designer Tools](#) | 4

Using the Network Service Designer

When you log in to Network Service Designer, the Requests page displays open requests for new network services. Use this page to start designs for those open requests and to create new requests for network services.

Before You Begin

- Learn about the Network Service Designer. See [“Network Service Designer Overview”](#) on page 56.
- Log into the Network Service Designer. See [“Access Designer Tools”](#) on page 4.

Creating a Network Service

You create a network service as follows:

1. Create a request for a network service. See [“Creating Requests for Network Services”](#) on page 62.
2. Design a service chain—a structure that details specific VNFs, a performance specification, and defined ingress and egress points for the network service. See [“Designing Network Services”](#) on page 71.
3. Publish the final design—the network service—to the network service catalog. See [“Publishing Network Service Designs”](#) on page 96.

RELATED DOCUMENTATION

[Network Services and Service Chains Overview](#) | 58

[Creating Requests for Network Services](#) | 62

[Designing Network Services](#) | 71

Creating Requests for Network Services

IN THIS CHAPTER

- [Network Services and Service Chains Overview | 58](#)
- [Performance Overview | 59](#)
- [About the Requests Page for the Network Service Designer | 60](#)
- [Creating Requests for Network Services | 62](#)
- [Creating a Functional Service Chain | 64](#)
- [Configuring Performance Goals | 65](#)
- [Viewing Requests for Network Services | 67](#)

Network Services and Service Chains Overview

The terms *network service* and *service chain* are sometimes used interchangeably, but they are not the same; you need to understand the difference between them:

- A *network service* is a final product offered to end users with a full description of its functionality and specified performance.

Administrators deploy network services between two locations in a virtual network, so that traffic traveling in a specific direction on that link is subject to action from that service. This term is defined in the ETSI Network Functions Virtualization (NFV) standard.

- A *service chain* refers to the structure of a network service, and consists of a set of linked network functions, which are provided by specific virtualized network functions (VNFs), with a defined direction for traffic flow and defined ingress and egress points. Although not defined in the ETSI NFV standard, this term is regularly used in NFV and software-defined networking (SDN).

You can create a service chain in the Network Service Designer by using:

- One VNF instance that provides one or more functions. See [Figure 3 on page 59](#).

Using one VNF instance instead of multiple instances increases performance.

- Multiple instances of the same VNF, each providing certain functions. See [Figure 4 on page 59](#).

- Using multiple instances of the same VNF lowers performance, such as when you want to create differentiated services.
- Instances of different VNFs, each providing certain functions. See [Figure 4 on page 59](#).
- You might need to use different VNFs if one VNF cannot fulfill all network functions or if a particular VNF offers an advantage for a network function.

Figure 3: Service Chain with One VNF Instance That Provides All Functions

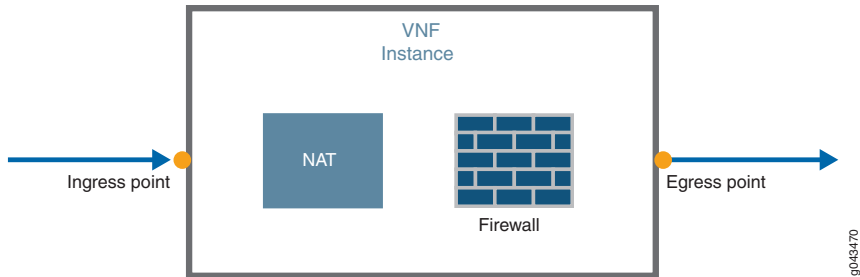
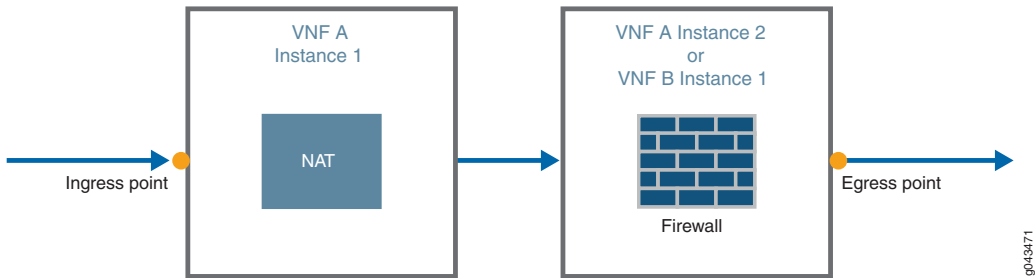


Figure 4: Service Chain with Either Multiple Instances of the Same VNF or Multiple VNFs



RELATED DOCUMENTATION

Performance Overview 59
Designing Network Services 71
Defining Ingress and Egress Points for a Service Chain 75

Performance Overview

The following parameters define the performance of a network service, a virtualized network function (VNF), and the component functions of a VNF:

- Sessions—Maximum number of sessions allowed for one instance of the service.
- Bandwidth (Mbps or Gbps)—Data rate for the function or service.
- Latency (ms or ns)—Time taken by a packet to traverse the function or service.
- Licence cost (USD)—Cost of the function or service.

Vendors provide specified values for these parameters for a VNF and for each allowed combination of components in the VNF (internal service chain). You can view the specified values in the Vendor catalog.

Network Service Designer evaluates the aggregate performance of the design against the goals in the request and displays the information in the Goals pane.

RELATED DOCUMENTATION

Configuring Performance Goals 65
Monitoring Performance Goals 76
VNF Overview 35
Viewing Information About VNFs 70
Designing Network Services 71

About the Requests Page for the Network Service Designer

To access this page, click **Home> Requests**.

Use the Requests page to create and manage requests for new network services. You must create a request before you can design a network service.

A request contains information about the required service, such as:

- The customer’s name.
- The requested functions in the network service. For example, NAT, UTM, and firewall.
- The performance goals for the service.

As soon as you start to design the network service, the request becomes a design, which you track on the Designs page. See [“About the Designs Page for the Network Service Designer” on page 94](#).

Tasks You Can Perform

You can perform the following tasks from this page:

- Create requests for new network services. See [“Creating Requests for Network Services” on page 62](#).
- Specify a sequence of network functions that you want in the network service. See [“Creating a Functional Service Chain” on page 64](#).
- View open requests for network services. See [“Viewing Requests for Network Services” on page 67](#).

Field Descriptions

[Table 17 on page 61](#) provides guidelines on using the fields on the Requests page for the Network Service Designer.

Table 17: Fields on the Requests Page for the Network Service Designer

Field	Description
New Request	Click to request a new network service design. The New Request page allows you to define the requirements for your network service design.
Begin	Hover over a saved request and click Begin to design a network service. The Build page appears. You can specify the virtual network function, update the function configuration, and specify the performance goals.
Edit	Click to edit the network service design request details.
Delete	Click to delete a network service design request.

RELATED DOCUMENTATION

Network Service Designer Overview	56
About the Designs Page for the Network Service Designer	94

Creating Requests for Network Services

You must create a request before you can design a network service. When you create a request for a network service, you define the requirements for the service, including the required network functions and the performance goals.

To create a request for a network service:

1. Click **Home** in the toolbar and **Requests** in the left navigation bar.
2. Click **New Request**.

The Request Information page in which you specify information about the request appears.

3. Configure the request information according to the guidelines provided in [Table 18 on page 62](#).
4. Click **Next**.

The Service Chain and Design Goals page appears, displaying the Goals pane, the Functional Service Design area, and the Function Palette.

5. Configure the goals and service chain according to the guidelines provided in [Table 18 on page 62](#).
6. Click **Next**.

The Summary page appears that displays the details you entered for the request.

7. Review the details and make corrections if necessary, using the **Previous** and **Next** options to navigate through the pages.
8. After updating the information, click **Create**.

The request for the network service design appears on the Requests page.

Table 18: Fields on the New Request Page

Field	Description
<i>Request Information</i>	
Name	Specify the name for the request. The Name field accepts up to 60 characters, including letters, numbers, and symbols.
Priority Request	(Optional) If the request is urgent, select the Priority Request check box.

Table 18: Fields on the New Request Page (continued)

Field	Description
Customer Name	<p>(Optional) Specify a customer name.</p> <p>The Customer Name field accepts up to 60 characters, including letters, numbers, and symbols.</p>
Description	<p>(Optional) Specify a description for the service.</p> <p>The Description field accepts up to 500 characters, including letters, numbers, and symbols.</p>
Requirements	<p>(Optional) Specify the requirements for the request.</p> <p>The Requirements field accepts up to 1000 characters, including letters, numbers, and symbols.</p>
Deployment Type	<p>(Optional) Select a Deployment Type from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • vCPE-Only • uCPE-Only <p>The default option is vCPE-Only.</p>
Attachments	<p>(Optional) Click Select Files, navigate to the file you want to attach, and click Open.</p> <p>The file is uploaded to the Attachments (Optional) field.</p>
<i>Service Chain and Design Goals</i>	
Function Palette	View the list of supported network functions in the Function Palette. You can drag the network function from the Function Palette and drop it to the Functional Service Design area.
Functional Service Design	Create a functional service chain by placing the required network functions in the required order. See “Creating a Functional Service Chain” on page 64 .
Goals	Configure the performance goals for a network service. You can define goals for the number of sessions, bandwidth, latency, and license cost. See “Configuring Performance Goals” on page 65 .
Summary	Review the details and make corrections if necessary, using the Previous and Next options to navigate through the pages.

RELATED DOCUMENTATION

[Network Services and Service Chains Overview | 58](#)

[Performance Overview | 59](#)

[Designing Network Services | 71](#)

[Configuring Performance Goals | 65](#)

[Creating a Functional Service Chain | 64](#)

Creating a Functional Service Chain

Network Service Designer automatically connects the network functions in the order that you place them in the design area. You can insert a function between two functions already on the design pane. If you make an error, you can use the delete icon or you can right-click a component in the design area and delete the component.

NOTE: The WAN links that are supported are WAN0, WAN1, and WAN2.

To create a functional service chain:

- For a centralized deployment model, drag and drop the network functions in the required order from the Function Palette to the Functional Service Design area.
- For a distributed deployment model, drag the network function from the Function Palette and drop it to the Functional Service Design area in the following order:
 - Between the ingress point and AppRouting function
 - Between the AppRouting function and WAN links
 - Between WAN Links and the egress point

RELATED DOCUMENTATION

[Creating Requests for Network Services | 62](#)

Configuring Performance Goals

To configure the performance goals of a network service:

1. Click **Home > Requests > New Request**.
2. Enter the request information and click **Next**.
3. In the Goals pane, click **Add Goal**.

The New Goal window is displayed.

4. Configure the goals according to the guidelines provided in [Table 19 on page 65](#).

BEST PRACTICE: Adding one or more goals to the request enables you to track performance of those parameters when you design a network service for the request. Although adding goals is not mandatory, we recommend that you do so.

5. Click **Save**.

Table 19: Fields on the Performance Goal Page

Field	Description
<i>Session</i>	
Goal Value	<p>Specify the target value for the goal. When you design a network service, the goal value is used by the Network Service Designer to evaluate how your design meets the goal. There is no upper limit. As a guideline, typical achievable values for a firewall are as follows:</p> <ul style="list-style-type: none"> • Session: 25,000–60,000 Min. of path • Bandwidth: 185–240 Mbps • Latency: 2–6 ms • License Cost: 100 USD

Table 19: Fields on the Performance Goal Page (*continued*)

Field	Description
Acceptable Value	<p>Specify a value that is lower than the target and acceptable for the network service. When you design a network service, the acceptable value is used by the Network Service Designer to evaluate how your design meets the goal.</p> <p>Example:</p> <ul style="list-style-type: none"> • Session: 20,000 Min. of path • Bandwidth: 150 Mbps • Latency: 5 ms • License Cost: 99 USD
Must Value	<p>Specify the minimum value for the goal. The minimum value should be lower than the acceptable value. When you design a network service, the must value is used by the Network Service Designer to evaluate how your design meets the goal.</p> <p>Example:</p> <ul style="list-style-type: none"> • Session: 15,000 Min. of path • Bandwidth: 100 Mbps • Latency: 4 ms • License Cost: 95 USD
Based on	<p>View the method that is used by the Network Service Designer to evaluate how your design meets the goal. You cannot edit this field.</p> <p>Example:</p> <ul style="list-style-type: none"> • Session: Min. of path If there are multiple VNFs in the service chain, then the VNF with the smallest bandwidth is chosen. • Bandwidth: Min. of path • Latency: Cumulative • License Cost: Cumulative
Unit	<p>Specify the measurement unit of the goal.</p> <p>Example:</p> <ul style="list-style-type: none"> • Bandwidth: Mbps, Gbps • Latency: ns, ms • License Cost: USD

RELATED DOCUMENTATION

[Performance Overview | 59](#)

[Monitoring Performance Goals | 76](#)

Viewing Requests for Network Services

You can view the requests for a network service in a hierarchical grid view and tree view. The grid view is the default option.

To view the requests for a network service in the tree view:

1. Select **Home > Requests**.

The Request page appears. All requests for a network service are displayed in the grid view.

2. Click **Show Details** (hierarchy icon at the top left of the page).

The requests for the network service are listed in the Home page.

3. Select a request to view the detailed information about the customer, supported function requirements, and design goals.

RELATED DOCUMENTATION

[About the Requests Page for the Network Service Designer | 60](#)

Creating Network Services

IN THIS CHAPTER

- About the Build Page for the Network Service Designer | 68
- Viewing Information About VNFs | 70
- Designing Network Services | 71
- Connecting VNFs in a Service Chain | 74
- Defining Ingress and Egress Points for a Service Chain | 75
- Monitoring Performance Goals | 76
- Configuring Network Services | 77
- vSRX Configuration Settings | 78
- LxCIPtable VNF Configuration Settings | 87
- Cisco CSR-1000v VNF Configuration Settings | 90
- Riverbed Steelhead VNF Configuration Settings | 92
- Fortinet VNF Configuration Settings | 92
- Ubuntu VNF Configuration Settings | 93

About the Build Page for the Network Service Designer

To access this page click **Home** > **Designs** > *Design Name* > **Edit**.

You can also view the Build page by following these steps:

1. Click **Home** in the toolbar and **Requests** in the left navigation bar.
2. Hover over an existing request.

A menu appears at the bottom right of the request that you are hovering over.

3. Click **Begin**.

The Build page appears.

Use the Build page to design, configure, save, and publish a network service. You can also view VNFs to use in your design and monitor how the design performs against your target goals.

Tasks You Can Perform

You can perform the following tasks from this page:

- View performance specifications, required resources, and component network functions for each VNF. See [“Viewing Information About VNFs” on page 70](#).
- Design a service chain for both distributed and centralized deployment models. See [“Designing Network Services” on page 71](#).
- Define the ingress and egress point for a service chain. See [“Defining Ingress and Egress Points for a Service Chain” on page 75](#).
- Connect VNFs in a service chain. See [“Connecting VNFs in a Service Chain” on page 74](#).
- Configure the performance goals of a network service. See [“Configuring Performance Goals” on page 65](#).
- Monitor the performance of a service. See [“Monitoring Performance Goals” on page 76](#).

Field Descriptions

[Table 20 on page 69](#) provides guidelines on using the fields on the Build page for the Network Service Designer.

Table 20: Fields on the Network Service Build Page

Field	Description
Functional Service Design	View the functions in the network service.
Network Service Design	Drag and drop the VNFs from the VNF category, add ingress and egress points, and connect the VNFs.
Goals	Click to monitor the performance goals for the network service.
Info	Click to add the information about the Network Service Design that you want to track.
Docs	Click to upload documents about the Network Service Design, such as specifications, or requirement documents.
VNF Category	Choose the VNFs from the VNF category.
Functional Configuration	Click to configure the VNF settings.

Table 20: Fields on the Network Service Build Page (*continued*)

Field	Description
Save NSD	Click to save the network service design template.
Publish NSD	Click to publish the network service design template to the network service catalog.
Delete NSD	Click to delete multiple NSD templates together.

RELATED DOCUMENTATION

[About the Designs Page for the Network Service Designer](#) | 94

Viewing Information About VNFs

You can view performance specifications, required resources, and component network functions for each VNF, which you created in the Resource Designer, in the VNF catalog. Reviewing this information can help you to determine which VNF to use when you are designing a network service.

To view information about a specific VNF:

1. Click the network function in the Vendor catalog.

The information window for the network function appears, displaying the following information in the Details tab:

- A graphical representation of the complete network function with ingress and egress points.
- A list of resources required for the network function.

2. Click **Functions**.

You see the category of the network function, such as security, and the component functions, such as NAT and firewall.

3. Click **Service Chains** to display:

- A list of the potential internal service chains (allowed combinations of component functions) for this network function.

Lines without arrows connecting component functions in an internal service chain indicate that the order of the functions does not matter.

- The performance specification for each internal service chain.
4. Click anywhere outside the window to close the VNF information window.

RELATED DOCUMENTATION

[VNF Overview | 35](#)

[Performance Overview | 59](#)

Designing Network Services

IN THIS SECTION

- [Designing a Network Service for a Centralized Deployment | 71](#)
- [Designing a Network Service for a Distributed Deployment | 73](#)

When you save a request it appears on the Requests page. You can then design a service chain to fulfill the request, using VNFs in the Vendor catalog to provide the requested network functions.

You can design the service chains for the following deployment models:

Designing a Network Service for a Centralized Deployment

To design a service chain for a centralized deployment model:

1. Click **Home** in the toolbar and **Requests** in the left navigation bar.

The Requests page appears, displaying the open requests.

2. Click **Begin**.

The Build page displays the requested network functions and the goals.

3. Click the first function in the chain.

The VNF catalog at the bottom right of the page is refreshed to show the VNFs that provide this function.

4. Drag and drop a VNF from the catalog to the Network Service Design workspace.

The function appears inside the VNF image.

5. Add an ingress point to the first VNF in the chain.

The Performance Goals pane is refreshed to indicate how the network service design meets the defined goals.

6. Click the next function in the chain.

The VNF catalog is refreshed to show only the VNFs that provide this function. If a VNF in the Network Service Design workspace supports this function, a faded image of the function appears inside the VNF image.

7. Choose a VNF for this function:

- To implement this function with the same VNF, click the faded image in the VNF image.
- To implement this function with a different VNF, drag the VNF from the Vendor catalog to the Network Service Design workspace.

8. Repeat Step 6 and Step 7 until you have assigned a VNF to each required network function. If you make an error in the design area, you can right-click and delete the component.

9. If you have used multiple VNFs in your design, connect them by packet flow.

10. Add an egress point to the last VNF in the chain.

The Performance Goals pane is refreshed again to indicate how the network service design meets the customer goals.

11. Click **Save NSD** to save the design.

12. (Optional) Configure the Network Service.

13. Click **Publish NSD** to add the service to the catalog.

The Publish NSD page appears.

- a. Specify a name (that customers see) for this network service.

The field accepts up to 60 characters, including letters, numbers, and symbols.

- b. Specify a description of the service.

The field accepts up to 500 characters, including letters, numbers, and symbols.

- c. Select the type of service from the menu.
- d. Click **Publish**.

Designing a Network Service for a Distributed Deployment

To design a service chain for a distributed deployment model:

1. Click **Home** in the toolbar and **Requests** in the left navigation bar.

The Requests page appears, displaying the open requests.

2. Click **Begin**.

The Build page displays the requested network functions and the goals.

3. Click the first function in the chain.

The Vendor catalog is refreshed to show only the VNFs that provide this function.

4. Drag the VNF from the Vendor catalog and drop the network functions at the appropriate points in the network chain to meet the requirements of your network.

The Performance Goals pane is refreshed to indicate how the network service design meets the customer goals.

NOTE: The ingress point, egress points, and gateway router are automatically updated for the distributed deployment model.

5. Click the next function in the chain.

The Vendor catalog updates to show only the VNFs that provide this function. If a VNF in the Network Service Design workspace supports this function, a faded image of the function appears inside the VNF image.

6. If you have used multiple VNFs in your design, then drag and drop the network functions at the appropriate points in the network chain.

The Performance Goals pane again updates to indicate how the network service design meets the customer goals.

7. Repeat Step 4 and Step 5 until you have assigned a VNF to the required network function. If you make an error, you can right-click a component in the network service design area and delete the component.

8. (Optional) Click **Function Configuration** and configure the network service.

9. Click **Save NSD** to save the design.

10. Click **Publish NSD** to add the service to the catalog.

The Publish NSD page appears.

a. Specify an official name (that customers see) for this network service.

The field accepts up to 60 characters, including letters, numbers, and symbols.

b. Specify a description of the service for customers to read.

The field accepts up to 500 characters, including letters, numbers, and symbols.

c. Select the type of service from the menu.

d. Click **Publish**.

RELATED DOCUMENTATION

[Network Services and Service Chains Overview | 58](#)

[Performance Overview | 59](#)

[Defining Ingress and Egress Points for a Service Chain | 75](#)

[Connecting VNFs in a Service Chain | 74](#)

[Configuring Network Services | 77](#)

Connecting VNFs in a Service Chain

To connect VNFs in a service chain:

1. Click **Connect**, then click **ELAN**.

The dots that represent potential ingress and egress points on the VNFs enlarge.

2. Hover over the egress point of the first VNF until a green circle appears.

3. Click and hold the green circle, then drag the cursor to the green circle that appears around the ingress point for the next VNF, and release the mouse button.

A one-way arrow indicating the flow of traffic in the service chain appears.

4. Repeat Step 1 through Step 3 until you have connected all VNFs in the service chain.

RELATED DOCUMENTATION

[Network Services and Service Chains Overview | 58](#)

[Designing Network Services | 71](#)

Defining Ingress and Egress Points for a Service Chain

To define the ingress point and the egress point for a service chain that you are designing:

1. Click **Ingress**.

The dots that represent potential ingress and egress points on VNFs enlarge.

2. Click the dot that represents the ingress point for the service chain.

An arrow indicating the direction of traffic flow with the label I appears.

3. Click **Egress**.

4. Click the dot that represents the egress point for the service chain.

An arrow indicating the direction of traffic flow with the label E appears.

5. Click the egress point of the last VNF to define the egress point.

RELATED DOCUMENTATION

[Network Services and Service Chains Overview | 58](#)

[Designing Network Services | 71](#)

[Monitoring Performance Goals | 76](#)

Monitoring Performance Goals

Network Service Designer provides comprehensive information about the performance of VNFs and their component network functions in the VNF catalog. Network Service Designer also tracks the aggregate performance of a network service that you are designing and saves the information to the network service catalog.

Minimizing the number of VNFs and VNF instances in a service chain optimizes the performance of a network service. For example, using one VNF instance for both NAT and firewall functions provides higher performance than using either separate instances of the same VNF or different VNFs to provide the functions.

You specify performance goals for the service when you create a request for a network service. When you are designing a service chain, you evaluate the performance of your design against the requested goals.

To monitor the performance of a service that you are designing:

1. Click the right arrow in the Goals pane to view the performance goals.
2. Add an ingress point to the first VNF in the service chain immediately after you assign that VNF to the first network function.
3. Monitor the values in the Goals pane as you design your service chain.

RELATED DOCUMENTATION

[Network Services and Service Chains Overview | 58](#)

[Performance Overview | 59](#)

[Designing Network Services | 71](#)

[Defining Ingress and Egress Points for a Service Chain | 75](#)

Configuring Network Services

When you are designing a service chain or after you have designed a service chain, you can configure settings for the VNFs in the chain. The configuration settings you can configure are specified in Configuration Designer and the values for the settings are specified in Resource Designer. The settings that you configure are:

- The virtual container in which the VNF resides.
- The network functions, such as NAT or firewall.

The settings that you can configure depend on the actual VNF. Manual configurations are optional and override automatic configurations specified by the Contrail Service Orchestration (CSO) deployment script, other CSO components, or default settings that you configured with Resource Designer.

To configure the network service:

1. View the service chain design on the Build page.

If the design is not currently visible on the Build page:

- a. Click **Home** in the toolbar and **Designs** in the left navigation bar.

The list of saved and published designs appears.

- b. Click **Edit** for the network service you want to configure.

The Build page appears, displaying the service chain design.

2. Click **Function Configuration**.

The Service page appears, displaying the VNFs in the service chain and the Base Configure tab for the first VNF in the Functional Service Design workspace.

3. Specify the settings on the Base Configure tab.

This action configures the virtual machine in which the VNF resides.

BEST PRACTICE:

- Complete all the settings in the Base Configure tab to optimize your deployment. End users can see these settings in Customer Portal or custom access software and should not override them.
- Configure few example settings for the service. These example settings must be generic and not network-specific. End users can configure service settings specific to their networks in Customer Portal.

4. (Optional) Specify settings on the other tabs for this VNF to customize a particular function such as NAT.

End users can customize their own services with these settings in Customer Portal. Settings that end users specify in Customer Portal override conflicting settings that you specify in Network Service Designer.

5. Click the next VNF icon in the Configuration page.
6. Repeat Step 3 and Step 4.
7. Repeat Steps 5 through 7 for each VNF in the chain.
8. Click **OK**.

The Service page closes.

RELATED DOCUMENTATION

[vSRX Configuration Settings | 78](#)

[LxCIPtable VNF Configuration Settings | 87](#)

[Cisco CSR-1000v VNF Configuration Settings | 90](#)

[Riverbed Steelhead VNF Configuration Settings | 92](#)

vSRX Configuration Settings

BEST PRACTICE: Service providers configure base settings for a VNF. Customers should not change these values unless directed to do so by their service provider. Service providers may provide some generic examples of service configurations for their customers. Customers can configure services—for example, by creating policies—appropriate to their networks in Customer Portal.

Use the information in the following tables to provide values for the available settings:

- [Table 21 on page 79](#) shows the settings you can configure for the virtual machine (VM) that contains the VNF.
- [Table 22 on page 81](#) shows the firewall settings you can configure.

NOTE: Firewall is supported on both centralized deployment model and distributed deployment model.

- [Table 23 on page 83](#) shows the Network Address Translation (NAT) settings you can configure.

NOTE: NAT is supported in distributed deployment model only.

- [Table 24 on page 84](#) shows the unified threat management (UTM) settings you can configure.

NOTE: UTM is supported on both centralized deployment model and distributed deployment model.

Table 21: Fields for the vSRX Base Settings

Field	Description
Host Name	<p>For a cloud site, specify the hostname of the VM that contains the vSRX VNF. The field has no limit on the number of characters and accepts letters, numbers, and symbols.</p> <p>Example: vm-vsrx</p> <p>For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.</p>
Loopback Address	<p>Specify an IPv4 loopback address for the management interface of the VM.</p> <p>Example: 192.0.2.25</p>
DNS Servers	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more DNS name servers.</p> <p>Example: 192.0.2.35</p>
NTP Servers	<p>Specify the FQDNs or IP addresses of one or more NTP servers.</p> <p>Example: 192.0.2.45</p>
Syslog Servers	<p>Specify the FQDNs or IP addresses of one or more system log servers.</p> <p>Example: 192.0.2.55</p>

Table 21: Fields for the vSRX Base Settings (*continued*)

Field	Description
Enable Re-filter	<p>Select True to enable a stateless firewall filter that protects the Routing Engine from denial-of-service (DoS) attacks or False to allow DoS attacks.</p> <p>Example: True</p>
Enable Default Screens	<p>For a cloud site, select True to enable the default screens security profile for the destination zone or False to disable default screening.</p> <p>Example: False</p> <p>You cannot configure this setting for an on-premise site.</p>
Time Zone	<p>Specify the time zone for the VM.</p> <p>Example: UTC</p>
Right Interface	<p>Specify the identifier of the VM interface that transmits data.</p> <p>Example: ge-0/0/1</p> <p>For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.</p>
Left Interface	<p>Specify the identifier of the VM interface that receives data.</p> <p>Example: ge-0/0/0</p> <p>For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.</p>
SNMP Prefix List	<p>If you set the Enable Re-filter field to True, specify the routes that the Junos Space Virtual Appliance uses for SNMP operations when it discovers the vSRX VNF.</p> <p>Example: 10.0.2.0/24</p>
Ping Prefix List	<p>If you set the Enable Re-filter field to True, specify the routes that the Junos Space Virtual Appliance uses for ping operations when it discovers the vSRX VNF.</p> <p>Example: 10.0.2.1/24</p>
Space Servers	<p>If you set the Enable Re-filter field to True, specify the IP addresses of the VMs that contain the Junos Space Virtual Appliances.</p> <p>Example: 10.0.2.50</p>

Table 22: Fields for the vSRX Firewall Settings

Field	Description
Policy Name	<p>Specify the name of the rule. The field has no limit on the number of characters and accepts letters, numbers, and symbols.</p> <p>Example: policy-1</p>
Source Zone	<p>Select the security zone from which packets originate.</p> <ul style="list-style-type: none"> • left—Interface that transmits data to the host • right—Interface that receives data transmitted from the host <p>Zone policies are applied to traffic traveling from one security zone (source zone) to another security zone (destination zone). This combination of a source zone and a destination zone is called a <i>context</i>.</p> <p>Example: left</p>
Destination Zone	<p>Select the security zone to which packets are delivered.</p> <ul style="list-style-type: none"> • left—Interface that transmits data to the host • right—Interface that receives data transmitted from the host <p>Zone policies are applied to traffic traveling from one security zone (source zone) to another security zone (destination zone). This combination of a source zone and a destination zone is called a <i>context</i>.</p> <p>Example: right</p>
Source Address	<p>Specify the source IP address prefixes that the network service uses as match criteria for incoming traffic.</p> <p>To add source addresses:</p> <ol style="list-style-type: none"> 1. Click the Source Address column. The source-address page appears. 2. Select any to match any source IP address of packets or ipp to match a specific prefix in the source IP address for which the application enforces the policy. 3. If you select ipp, specify a prefix. 4. Click OK. <p>Example: 10.0.2.30</p>

Table 22: Fields for the vSRX Firewall Settings (*continued*)

Field	Description
Destination Address	<p>Specify the destination IP address prefixes that the network service uses as match criteria for outgoing traffic.</p> <p>To add a destination address:</p> <ol style="list-style-type: none"> 1. Click the Destination Address column. The destination-address page appears. 2. Select any to match any source IP address of packets or ipp to match a specific prefix in the source IP address for which the application enforces the policy. 3. If you select ipp, specify a prefix. 4. Click OK. <p>Example: 192.0.2.0/24</p>
Action	<p>Select permit to transmit packets that match the rule or deny to drop packets that match the rule.</p> <p>Example: permit</p>

Table 22: Fields for the vSRX Firewall Settings (*continued*)

Field	Description
Application	<p>Specify the applications to which the policy applies. The applications are based on protocols and ports.</p> <p>To specify applications:</p> <ol style="list-style-type: none"> Click the Application column. The application page appears. In the allowed_apps field, select any to match any application or app to choose specific applications. If you select app, press and hold the Ctrl key and click the required applications from the drop-down list. <ul style="list-style-type: none"> • junos-tcp-any • junos-udp-any • junos-ftp • junos-http • junos-https • junos-icmp-all • junos-icmp-ping • junos-telnet • junos-tftp Click OK. <p>Example:</p> <ul style="list-style-type: none"> • junos-tcp-any • junos-udp-any

Table 23: Fields for the vSRX NAT Settings

Field	Guidelines
NAT Source Name	<p>Specify the source IP address of packets that the policy rules match.</p> <p>Example: 10.0.2.2/24</p>
NAT Destination Name	<p>Specify the destination IP address of packets that the policy rules match.</p> <p>Example: 10.0.2.3/24</p>

Table 23: Fields for the vSRX NAT Settings (*continued*)

Field	Guidelines
NAT policy settings—For information about the following policy settings, see the firewall policy settings in Table 2.	
<ul style="list-style-type: none"> • Policy Name • Source Zone • Destination Zone • Source Address • Destination Address • Action • Application 	

Table 24: Fields for the vSRX UTM Settings

Field	Description
Antivirus	<p>Select True to check for viruses in application layer traffic against a virus signature database. Select False to disable checking for viruses.</p> <p>Example: True</p>
Antispam	<p>Select True to block spam e-mails or False to allow spam e-mails.</p> <p>Example: True</p>
Antispam Black List	<p>Specify an address blacklist for local spam filtering.</p> <p>Blacklists contain e-mail addresses from which you do not want to receive messages.</p> <p>NOTE: When both the whitelist and blacklist are in use, the whitelist is checked first. If there is no match, then the blacklist is checked.</p> <p>Example: john@example.net</p>
Antispam White List	<p>Specify an address whitelist for local spam filtering.</p> <p>Whitelists contain e-mail addresses from which you want to receive messages.</p> <p>NOTE: When both the whitelist and blacklist are in use, the whitelist is checked first. If there is no match, then the blacklist is checked.</p> <p>Example: user@example.net</p>

Table 24: Fields for the vSRX UTM Settings (*continued*)

Field	Description
Antispam Action	<p>Select the antispam action that you want the device to take when it detects spam:</p> <ul style="list-style-type: none"> • block—Blocks the message • tag-subject—Tags the subject field with a preprogrammed string • tag-header—Tags the message header with a preprogrammed string <p>Example: block</p>
Content Filter	<p>Select True to block different types of traffic based on the MIME type, file extension, protocol command, and embedded object type or False to permit these types of traffic.</p> <p>Example: True</p>
Content Filter Extensions	<p>Specify one or more file extensions to block over HTTP, FTP, SMTP, IMAP, and POP3 connections.</p> <p>Example: exe, pdf, js</p>
Content Filter Mime	<p>Specify the MIME types to be blocked or permitted over HTTP, FTP, SMTP, IMAP, and POP3 connections.</p> <p>Example: application, exe</p>
Content Filter Protocol Commands	<p>Specify commands for HTTP, FTP, SMTP, IMAP, and POP3 protocols to block traffic based on these commands.</p> <p>Example: put, mput</p>
Content Filter Content Type	<p>Press and hold the Ctrl key and click one or more of the following types of content to specify filtering of traffic that is supported only for HTTP and is not covered by file extensions or MIME types:</p> <ul style="list-style-type: none"> • Active X • Windows executable files (.exe) • HTTP cookie • Java applet • Zip files <p>Example: activex, exe</p>

Table 24: Fields for the vSRX UTM Settings (*continued*)

Field	Description
Content Filter Apply To	<p>Press and hold the Ctrl key and click one or more of the following protocols in the drop-down list to specify filtering of traffic associated with these protocols:</p> <ul style="list-style-type: none"> • HTTP • FTP • POP3 • IMAP • SMTP <p>Example: http, ftp</p>
Web filter	<p>Select True to prevent access to specific websites and embedded object types or False to permit access to all websites.</p> <p>Example: True</p>
Web Filter Black List	<p>Specify URLs to create a blacklist of websites to block.</p> <p>NOTE: A Web filtering profile can contain one whitelist or one blacklist with multiple user-defined categories, each with a permit or block action.</p> <p>Example:</p> <ul style="list-style-type: none"> • www.example1.com • www.example2.com
Web Filter White List	<p>Specify URLs to create a whitelist of websites that users can always access.</p> <p>With local Web filtering, the firewall intercepts every HTTP request in a TCP connection and extracts the URL. The network service then looks up the URL to determine whether it is in the whitelist or blacklist based on its user-defined category.</p> <p>NOTE: A Web filtering profile can contain one whitelist or one blacklist with multiple user-defined categories, each with a permit or block action.</p> <p>Example: www.example3.net</p>

Table 24: Fields for the vSRX UTM Settings (continued)

Field	Description
Policy settings—For information about the following policy settings, see the firewall policy settings in Table 2.	
<ul style="list-style-type: none">• Source Zone• Destination Zone• Source Address• Destination Address• Action• Application	

RELATED DOCUMENTATION

| [Configuring Network Services](#) | 77

LxCIPtable VNF Configuration Settings

BEST PRACTICE: Service providers configure base settings for a VNF. Customers should not change these values unless directed to do so by their service provider. Service providers may provide some generic examples of service configurations for their customers. Customers can configure services—for example, by creating policies—appropriate to their networks in Customer Portal.

Use the information in the following tables to provide values for the available settings:

NOTE: The tables are applicable for centralized deployment model only.

- [Table 25 on page 88](#) shows the base settings you can configure for the Linux container.
- [Table 26 on page 88](#) shows the firewall settings you can configure.
- [Table 27 on page 90](#) shows the Network Address Translation (NAT) settings you can configure.

Table 25: Fields for the LxCIP Base Settings

Field	Description
Loopback Address	Specify a loopback IP address. Example: 192.0.2.10
Operation	Select add to apply the policies to a specific route or del to prevent use of the policies on specific routes. Example: add
Route	Specify the IP prefix of the route to which the policies should apply. Example: 192.0.2.20/24
Next Hop	Specify the IP address of a Contrail gateway network to which the VM connects. Example: 192.0.2.20

Table 26: Fields for the LxCIP Firewall Policy Settings

Field	Description
<i>Firewall Policies</i>	
Prevent SSH Brute	Select True to prevent SSH brute attacks or False to allow SSH brute attacks. Example: False
Prevent Ping Flood	Select True to prevent ping flood attacks or False to allow ping flood attacks. Example: False
<i>Forwarding Rule Settings</i>	
Destination Address	Specify the destination IP address prefix that the network service uses as a match criterion for outgoing traffic. Example: 192.0.2.25/24

Table 26: Fields for the LxCIP Firewall Policy Settings (*continued*)

Field	Description
Operation	<p>Select the operation, which applies to a chain of rules of the same type, from the drop-down list. The following options are available:</p> <ul style="list-style-type: none"> • append—Append the rule to a rule chain. • insert-before—Insert the rule before a rule with the same name. • delete—Replace an existing rule with this name. <p>Example: append</p>
Source Address	<p>Specify the source IP address prefix that the network service uses as a match criterion for outgoing traffic.</p> <p>Example: 192.0.2.20/24</p>
Name	<p>Specify the name for the rule. The field has no limit on the number of characters and accepts letters, numbers, and symbols.</p> <p>Example: vsrx-fw-policy</p>
Action	<p>Select the action for the rule, which applies to all traffic that matches the specified criteria.</p> <ul style="list-style-type: none"> • accept—Transmit packets that match the policy parameters. • drop—Drop packets that match the policy parameters. • reject—Reject packets that match the policy parameters. <p>Example: accept</p>
Service	<p>Specify the service that you want the rule to match.</p> <p>Example:</p> <ul style="list-style-type: none"> • http • smtp
Type	<p>Select the type of packet that the rule matches.</p> <ul style="list-style-type: none"> • input—Packets that the network service receives that are addressed to this VM • forward—Packets that the network service receives that are addressed to other VMs • output—Packets that the network service transmits <p>The application creates a chain of all rules with a particular type.</p> <p>Example: input</p>

Table 27: Fields for the LxCIP NAT Policy Settings

Field	Description
Left Interface	<p>Specify the name of the interface on which the network service enforces NAT for incoming traffic.</p> <p>Example: Eth1</p>
Right Interface	<p>Specify the name of the interface on which the network service enforces NAT for outgoing traffic.</p> <p>Example: Eth2</p>

RELATED DOCUMENTATION

| [Configuring Network Services](#) | 77

Cisco CSR-1000v VNF Configuration Settings

BEST PRACTICE: Service providers configure base settings for a VNF. Customers should not change these values unless directed to do so by their service provider. Service providers may provide some generic examples of service configurations for their customers. Customers can configure services—for example, by creating policies—appropriate to their networks in Customer Portal.

Use the information in the following tables to provide values for the available settings:

NOTE: The tables are applicable for centralized deployment model only.

- [Table 28 on page 91](#) shows the base settings you can configure for the virtual machine (VM) that contains the VNF.
- [Table 29 on page 91](#) shows the firewall settings you can configure.

Table 28: Fields for the CSR-1000v Base Settings

Field	Description
Host Name	Specify the hostname of the VM. Example: host1
Loopback Address	Specify the IPv4 loopback IP address. Example: 10.0.2.50
Name Servers	Specify the fully qualified domain names (FQDNs) or IP addresses of one or more DNS name servers. Example: 10.0.2.15
NTP Servers	Specify the FQDNs or IP addresses of one or more NTP servers. Example: ntp.example.net

Table 29: Fields for the CSR-1000v Firewall Settings

Field	Description
Left Interface	Specify the identifier of the interface that transmits data to the host. Example: GigabitEthernet2
Right Interface	Specify the identifier of the interface receiving data transmitted by the host. Example: GigabitEthernet3
Left to Right Allowed Apps	Select the applications from the drop-down list for which the policy is enforced in outgoing packets. The following applications are available: <ul style="list-style-type: none"> • http • https • telnet • ftp • tcp • udp • icmp Example: http, https

Table 29: Fields for the CSR-1000v Firewall Settings (*continued*)

Field	Description
Right to Left Allowed Apps	<p>Select the application from the drop-down list for which the policy is enforced for incoming packets. The following applications are available:</p> <ul style="list-style-type: none"> • http • https • telnet • ftp • tcp • udp • icmp <p>Example: ftp, udp</p>

RELATED DOCUMENTATION

| [Configuring Network Services](#) | 77

Riverbed Steelhead VNF Configuration Settings

You configure the Riverbed Steelhead VNF through its own software. See the Riverbed Steelhead documentation for information about how to configure the VNF settings.

RELATED DOCUMENTATION

| [Configuring Network Services](#) | 77

Fortinet VNF Configuration Settings

You can configure the Fortinet VNF by logging in to the Fortinet UI. The URL for accessing the Fortinet UI is `https://loopback-IP-Address-of-spoke: 49155`, where the loopback IP address is the IP address that you provided to Contrail Service Orchestration (CSO) while configuring the spoke site.

For information about configuring the VNF, see the Fortinet documentation.

RELATED DOCUMENTATION

| [Configuring Network Services](#) | 77

Ubuntu VNF Configuration Settings

You can configure the Ubuntu VNF by logging in to the regional microservices virtual machine (VM) and establishing an outbound SSH connection to the loopback IP address of the spoke. The CLI command to access the Ubuntu VNF is as follows:

```
root@regionalmsvm:~#ssh -p 49153 admin@loopback-IP-Address
```

For information about configuring the VNF settings, see the Ubuntu documentation.

RELATED DOCUMENTATION

| [Configuring Network Services](#) | 77

Managing Network Services

IN THIS CHAPTER

- [About the Designs Page for the Network Service Designer | 94](#)
- [Publishing Network Service Designs | 96](#)
- [Copying Network Service Designs | 96](#)
- [Editing Network Service Designs | 97](#)
- [Deleting Network Service Designs | 98](#)
- [Viewing Network Service Designs | 99](#)

About the Designs Page for the Network Service Designer

To access this page, click **Home> Designs**.

Use the Designs page to view and manage the network service design templates that you have saved or published.

Tasks You Can Perform

You can perform the following tasks from this page:

- Publish a network service design template to the network service catalog. See [“Publishing Network Service Designs” on page 96](#)
- Editing a network service design template. See [“Editing Network Service Designs” on page 97](#)
- Delete one or more network service designs. See [“Deleting Network Service Designs” on page 98](#)
- Copy one or more network service designs. See [“Copying Network Service Designs” on page 96](#)
- View complete details of a network service design. See [“Viewing Network Service Designs” on page 99](#)

Field Descriptions

Table 30 on page 95 provides guidelines on using the fields on the Designs page for the Network Service Designer.

Table 30: Fields on the Designs Page for the Network Service Designer

Field	Description
Priority	View the priority of the network service design.
Customer Name	View the customer name. The name can be a string of alphanumeric characters, dashes, and spaces. Example: Juniper Networks
Network Design	View the network service design name. The name can be a string of alphanumeric characters, dashes, and spaces. Example: nsd-firewall-nat-test
Functional Design	View the name of the functional design, which is obtained from the tenant requirement. The name can be a string of alphanumeric characters, dashes, and spaces. Example: nsd-fd-test
Date	View the date and time when the network service design template was created. Example: 02/06/2017 11:01
Status	View the network service design status: <ul style="list-style-type: none"> • Started—Network Service Design template is created and the components need to be added. • In-Progress—Network Service Design template is created but the template has not been validated. • Validated—Network Service Design template is validated and it is ready to be published. • Published—Network Service Designer published the network service design template and it is available to the Customer Portal for use.

RELATED DOCUMENTATION

Publishing Network Service Designs

After you have designed a network service design template, you need to publish the design to the network service catalog. Only published designs are available from the network service Catalog.

To publish a completed design to the network service catalog:

1. Select **Home> Designs**.

The Network Service Designs page appears. All the network service designs are displayed in a table.

2. Select the network service design that you want to publish.

The status of the template is **Validated**. For published designs, the status is **Published**.

3. Select **Publish** from the Edit drop-down list.

Your network service design is published and available to be used by the network service catalog. Its status changes from **Validated** to **Published**.

RELATED DOCUMENTATION

Copying Network Service Designs

You can create a new network service design template by copying an existing design template and editing it.

To copy one or more designs that you have saved or published:

1. Select **Home> Designs**.

The Network Service Designs page appears. All the network service designs are displayed in a table.

2. Select the network service design that you want to copy and click **Copy NSD**.

A page requesting confirmation for the copying appears.

3. Click **Yes** to confirm that you want to copy the designs.

The additional services appear in the table with the status as **Validated**.

RELATED DOCUMENTATION

| [About the Designs Page for the Network Service Designer](#) | 94

Editing Network Service Designs

To edit a network service design that you have saved or published:

1. View the network service design on the Build page.

If the design is not currently visible on the Build page:

- a. Click **Home** in the toolbar and **Designs** in the left navigation bar.

The list of saved and published designs appears.

- b. Click **Edit** for the network service you want to configure.

The Build page appears, displaying the network service design.

2. Click **Function Configuration** at the right of the Build page.

The Service page appears, displaying the VNFs in the service chain and the Base Configure tab for the first VNF in the Functional Service Design workspace.

3. Specify the settings on the Base Configure tab.

This action configures the VM in which the VNF resides.

BEST PRACTICE: Complete all the settings on the Base Configure tab to optimize the Contrail Service Orchestration (CSO). End users can see these settings in Customer Portal and should not override them.

4. (Optional) Specify settings on the other tabs for this VNF to customize a particular function such as Network Address Translation (NAT).

End users can customize their own services with these settings in Customer Portal. Settings that end users specify in Customer Portal override conflicting settings that you specify in Network Service Designer.

5. Click the next VNF icon in the Configuration page.
6. Repeat Step 3 and Step 4.
7. Repeat Steps 5 through 7 for each VNF in the chain.
8. Click **OK**.

The Service page closes.

RELATED DOCUMENTATION

[About the Designs Page for the Network Service Designer](#) | 94

Deleting Network Service Designs

To delete a network service design:

1. Select **Home>Designs**.

The Designs page appears.

2. Select the network service design that you want to delete.

3. Click **Delete**.

A page requesting confirmation for the deletion appears.

4. Click **Yes** to confirm that you want to delete the design.

The network service design is deleted.

To delete multiple designs that you have saved or published:

1. From the list of designs, select the designs that you want to delete.
2. Click **Delete NSD**.

A page requesting confirmation for the deletion appears.

3. Click **Yes** to confirm that you want to delete the designs.

The designs are deleted and are then displayed on the Requests Page.

RELATED DOCUMENTATION

| [About the Designs Page for the Network Service Designer](#) | 94

Viewing Network Service Designs

You can view the network service design in grid view and tree view. The default option is grid view.

To view the network service designs that you have saved or published:

1. Select **Home> Designs**.

The Network Service Designs page appears. All the network service designs are displayed in a table.

2. Click **Show Details**.

The network service designs are categorized according to their status and listed in the Home page.

3. Select a network service design template to view the detailed information about the design template, such as customer information, resource requirements, network design, and functional design.

You can edit, publish, or delete a network service design from this view.

RELATED DOCUMENTATION

| [About the Designs Page for the Network Service Designer](#) | 94