



SRX GUI設定ガイド

Version 11.2R2

Juniper Networks, K.K.
2011/10



Agenda

Chapter1. Basic Setup

Chapter2. Firewall Policy

Chapter3. NAT

Chapter4. VPN

Chapter5. PPPoE

はじめに

このガイドは、ローエンドのブランチSRX (SRX100~240) モデルを想定して、基本的な使用用途における初期のセットアップをGUIから簡単に行えることを主な目的として構成されております。

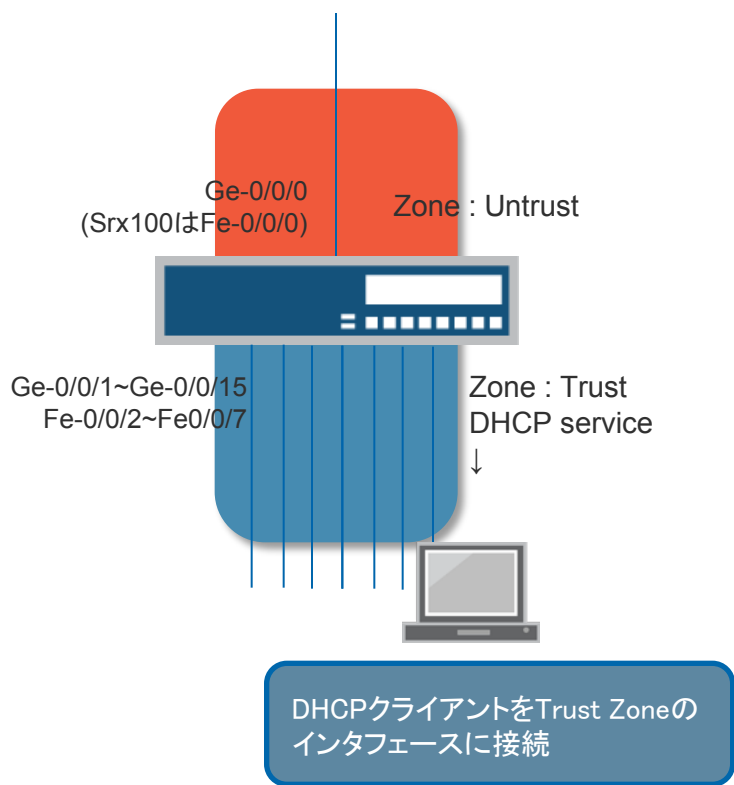
GUIにおける基本的な設定方法についてはミッドレンジ/ハイエンドSRX (SRX650~5800) とも共用となっておりますが、各モデルにおける物理インターフェースや構成要素の考え方などはHW Guideなどを参照してください。

また、各種ダイナミックルーティングプロトコル、Switching機能、HA、IDP、UTM、AppFW、などJUNOSがSRX上で提供することのできる様々な機能に関しては本書の取り扱い外となっております。必要に応じて別途CLIガイドなどを参照ください。

Chapter1. Basic Setup

工場出荷状態SRXの起動後デフォルト設定

工場出荷状態のSRXは以下のような設定になっており、Trust Zone(※Zoneについては後述)のポートに DHCPクライアント設定がなされたPCを接続することで自動的にGUIでの設定が開始できるようになっています。



```
管理: コマンドプロンプト
C:\Users¥juniper>
C:\Users¥juniper>ipconfig

Windows IP 構成

イーサネット アダプタ ローカル エリア接続 2:
   メディアの状態 . . . . . : メディア
   接続固有の DNS サフィックス . . . . . :

イーサネット アダプタ ローカル エリア接続:
   接続固有の DNS サフィックス . . . . . :
   IPv4 アドレス . . . . . : 192.168.1.2
   サブネット マスク . . . . . : 255.255.255.0
   デフォルト ゲートウェイ . . . . . : 192.168.1.1

イーサネット アダプタ ローカル エリア接続 3:
```

クライアントがSRXから払い出された IPを取得していることを確認

Step1 : SRXのGUI設定画面へのログイン

GUIのセットアップを開始するためには、`http://192.168.1/` へアクセスを行い(①)、`root / (passwordなし)` でログインを行います(②③)。

Juniper Web Device Manager - Windows Internet Explorer provided by Juniper Networks

ファイル(E) 編集(E) 表示(V) お気に入り(I) ツール(D) ヘルプ(H)

アドレス(D) `http://192.168.1/`

Juniper
Web Device
Manager

JUNIPER NETWORKS SRX210H

Username `root`

Password

Log In Reset

Copyright © 2011, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice](#). [Privacy](#).

Step2 : 初期セットアップウィザードの開始

Initial Setup

Host : NoName(srx210h) | Logged in as : root | Help | Logout

Setup Wizard

- Introduction
- System
 - Identification
 - Network
- Interfaces
- J-Web preferences
- Time Management
- Review & Commit

Introduction

Thank you for purchasing the srx210h Gateway.

As you use this wizard, refer to the upper left area of the page to see where you are in the setup process. Refer to the lower left area of the page for help related to the current page and its contents. When you click a link under the Resources heading, the document opens in your browser. If it is in a new tab, be sure to close only the tab (not the browser window) when you close the document.

About this page

This wizard leads you through the basic required steps to set up the SRX Series security device. To configure more detailed settings (for example, specific interface settings), use either the J-Web interface or the command-line interface (CLI).

Refer to this section of each page for information about the page and its contents.

Resources

- [JUNOS Software Security Configuration Guide](#)
- [SRX 210 Quickstart and Hardware Guides](#)

Initial Setupが開始されるので、「Start」ボタンを押す

Start

Step3 : Identificationの設定

Initial Setup

Host : NoName(srx210h) Logged in as : root Help Logout

JUNIPER NETWORKS

Setup Wizard

- Introduction
- System
- Identification
- Network
- Interfaces
- J-Web preferences
- Time Management
- Review & Commit

About this page

Complete this page to identify your device on the network and set a password for the root user. Click a field name to get information about the field.

[SRX 210 Quickstart and Hardware Guides](#)

Configure System: Identification * Required

Identification

Hostname * juniper.local

Domain name

Root password *

Verify root password *

Back Next

ホストネーム(①)とRootパスワード(②)を記載して、「Next」(③)へ

Step4 : Networkの設定

The screenshot displays the Juniper Networks Initial Setup wizard. The top navigation bar includes 'Initial Setup', 'Host : NoName(srx210h)', 'Logged in as : root', 'Help', and 'Logout'. The 'JUNIPER NETWORKS' logo is in the top right corner. The main content area is titled 'Setup Wizard' and 'Configure System: Network Settings'. A sidebar on the left lists navigation options: Introduction, System, Identification, Network (selected), Interfaces, J-Web preferences, Time Management, and Review & Commit. The main area contains a 'Network' section with 'Default Gateway' and 'DNS Name Servers' fields. The 'Default Gateway' field has an 'IP Address' input box with a red callout '1'. The 'DNS Name Servers' field has an 'IP Address' input box with a red callout '2' and an 'Add' button. Below the 'DNS Name Servers' field, there are two entries: '208.67.222.222' and '208.67.220.220', with 'Up', 'Down', and 'Remove' buttons. A blue callout box contains the text: 'デフォルトゲートウェイ(①)、DNSサーバー(②)の情報などを記入して、「Next」(③)へ (このステップはオプション)'. At the bottom right, there are 'Back' and 'Next' buttons, with a red callout '3' pointing to the 'Next' button.

Step5-1 : VLANの設定

Initial Setup

Host : NoName(srx210h) Logged in as : root Help Logout JUNIPER NETWORKS

Setup Wizard

- Introduction
- System
- Identification
- Network
- ⇒ Interfaces
- J-Web preferences
- Time Management
- Review & Commit

Interface Groups (VLANs)

THIS STEP IS OPTIONAL

Add Edit Delete

Name	Members	VLAN...
vlan-trust	ge-0/0/1.0 fe-0/0/2.0 fe-0/0/3.0 fe-0/0/4.0 fe-0/0...	3

About this page
The SRX Series security device supports integrated routing and bridging (IRB). The Junos operating system (OS) implements IRB with the help of VLANs combined with interfaces. A VLAN is a collection of interfaces that can be grouped together into a broadcast domain.
This page shows VLANs that act as the network interface for the device, and the page enables you to create new VLANs. Edit an existing VLAN by double-clicking the name or by selecting the row and clicking Edit. Create

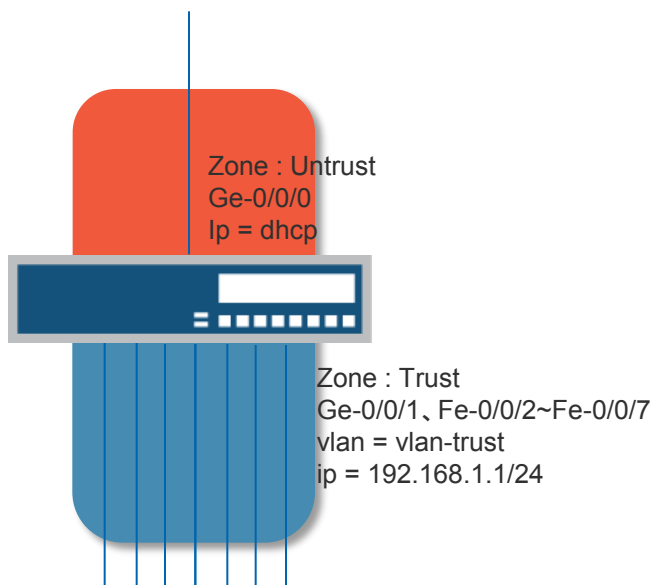
Back Next

デフォルトでは、vlan-trust (vlan-id=3)というVLANが作成されており、Untrust ZoneインタフェースのG(F)e-0/0/0以外のすべてのインタフェースがこのVlanに所属した設定となっている。

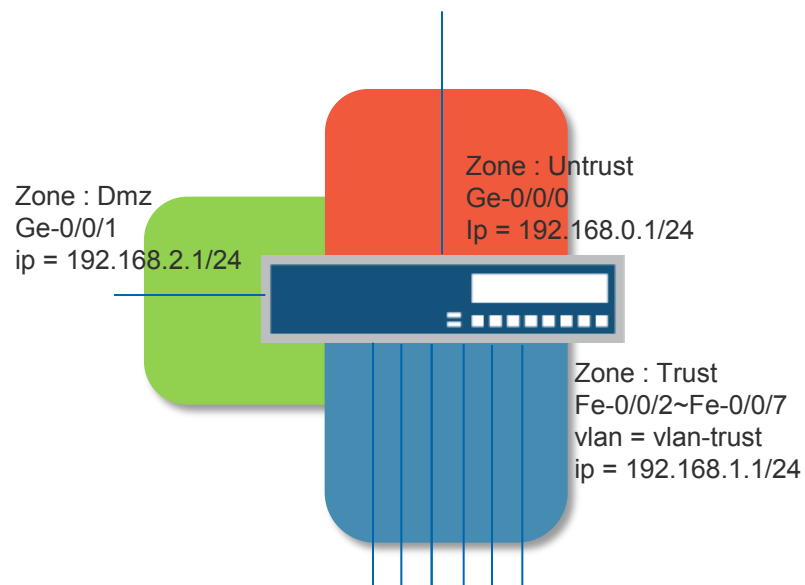
このままでよければ「Next」へ
本ガイドの例では次ページのようにインタフェース構成を変更するため、「Edit」へ

このガイドで構築する物理・論理構成

工場出荷時におけるデフォルト設定
(※このガイドではSRX210を使用)



このガイドで構成するサンプル設定構成



Step5-2 : VLANの設定

「Edit」を投下すると、vlan-trust に設定されているインターフェース一覧が表示される。
ここから設定を外したいインターフェースを選んで①、「<<」ボタンを投下し②、「Save」して「Next」へ

Setup Wizard

- Introduction
- System
 - Identification
 - Network
- Interfaces**
 - J-Web preferences
 - Time Management
 - Review & Commit

About this page
Group Gigabit Ethernet and Fast Ethernet interfaces to create VLANs. You may create up to four (4) VLAN groups during initial device setup. After you create a new VLAN, click Next to view it in the Interface Groups window.

Add/Edit Interface Group (VLAN)

Interface Group
VLAN id * 3

Available Interfaces

Interfaces In Group *

>>

<<

Select one or more interfaces in the Available Interfaces box, then click the ">>" button to add to group. You may also remove interfaces by selecting an interface in the right box and clicking the "<<" button.

Select one or more interfaces in the Available Interfaces box, then click the ">>" button to add to group. You may also remove interfaces by selecting an interface in the right box and clicking the "<<" button.

Step6-1 : Interfacesの設定 : アドレスの設定

Initial Setup
Host : NoName(srx210h) Logged in as : root Help Logout JUNIPER NETWORKS

Setup Wizard

- Introduction
- System
- Identification
- Network
- Interfaces
 - J-Web preferences
 - Time Management
 - Review & Commit

About this page
This page shows Gigabit Ethernet, Fast Ethernet, and VLAN interfaces. To edit an interface, double-click it, or select the row and click Edit. To add an interface, click Add. To delete an interface, select the row, and click the Delete button.

Note that you cannot use this page to delete a VLAN that was created in the current session. To delete such a VLAN, go back to the Interface Groups page.

Configure Interfaces
THIS STEP IS OPTIONAL

Add Edit Delete

Name	Address/Subnet	Security Zone	Services (Inbound)	Protocols (Inbound)
vlan.0	192.168.1.1/24	trust	all	all
ge-0/0/0.0	DHCP	untrust	dhcp,ftp	

Back Next

デフォルトでは、vlan.0 インタフェースに 192.168.1.1/24が、
Ge-0/0/0 インタフェースにdhcp クライアントの設定がなされている。

このままでよければ「Next」へ
本ガイドの例ではGe-0/0/0 に手動でアドレスを付与するため、
インタフェースをクリックしてハイライトし(①)、「Edit」(②)へ

Step6-2 : Interfacesの設定 : アドレスの設定

「Edit」を投下すると、address を設定する選択肢が3種類(DHCP、IP Address、PPPoE)表示されるので IP Addressを選択して(①)、アドレスとサブネットを記載して(②)、「Save」(③)へ

Setup Wizard

- Introduction
- System
- Identification
- Network
- **Interfaces**
- J-Web preferences
- Time Management
- Review & Commit

About this page
Edit the settings for an interface. After editing an interface, click Next to return to the Configure Interfaces page. Click a field name to get information about the field.

Add/Edit Interface * Required

Interface Settings

Interface: ①

Address * : DHCP IP Address PPPoe

IP address/subnet: ②

Security zone :

Services (Inbound)

<input type="checkbox"/> All	<input type="checkbox"/> HTTP
<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSH
<input type="checkbox"/> Ping	<input checked="" type="checkbox"/> DHCP

Protocols (Inbound)

<input type="checkbox"/> All	<input type="checkbox"/> OSPF
<input type="checkbox"/> BGP	<input type="checkbox"/> RIP
<input type="checkbox"/> PIM	<input type="checkbox"/> IGMP

Cancel Save ③

Step6 : Interfacesの設定 (PPPoEの場合: サンプル)

本ガイドでの構成例では説明しないが、PPPoE 接続の場合は、選択すると①設定項目が現れるのでProperties 設定を投入して②、「Save」へ

Add/Edit Interface * Required

Interface Settings

Interface:

Address * : DHCP Static IP address PPPoE

Security zone: ▼

PPPoE properties

Negotiate address:

User name: Password:

Access concentrator: Service name:

Services (Inbound)

All HTTP HTTPS SSH Ping DHCP

Protocols (Inbound)

All OSPF BGP RIP PIM IGMP

Step6-3 : Interfacesの設定 : インタフェースとZoneの追加

Initial Setup

Host : NoName(srx210h) Logged in as : root Help Logout

JUNIPER NETWORKS

Setup Wizard

- Introduction
- System
- Identification
- Network
- ➔ Interfaces
- J-Web preferences
- Time Management
- Review & Commit

About this page
This page shows Gigabit Ethernet, Fast Ethernet, and VLAN interfaces. To edit an interface, double-click it, or select the row and click Edit. To add an interface, click Add. To delete an interface, select the row, and click the Delete button.

Note that you cannot use this page to delete a VLAN that was created in the current session. To delete such a VLAN, go back to the Interface Groups page.

Configure Interfaces

THIS STEP IS OPTIONAL

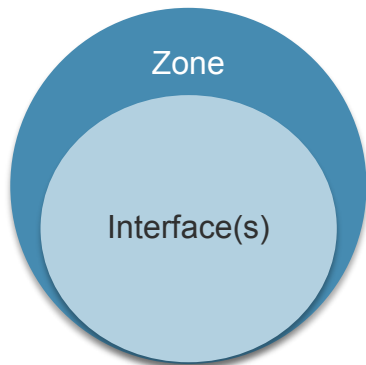
Add Edit Delete

Name	IP Address/Subnet	Security Zone	Services (Inbound)	Protocols (Inbound)
vlan.0	192.168.1.1/24	trust	all	all
ge-0/0/0.0	192.168.0.1/24	untrust	dhcp	

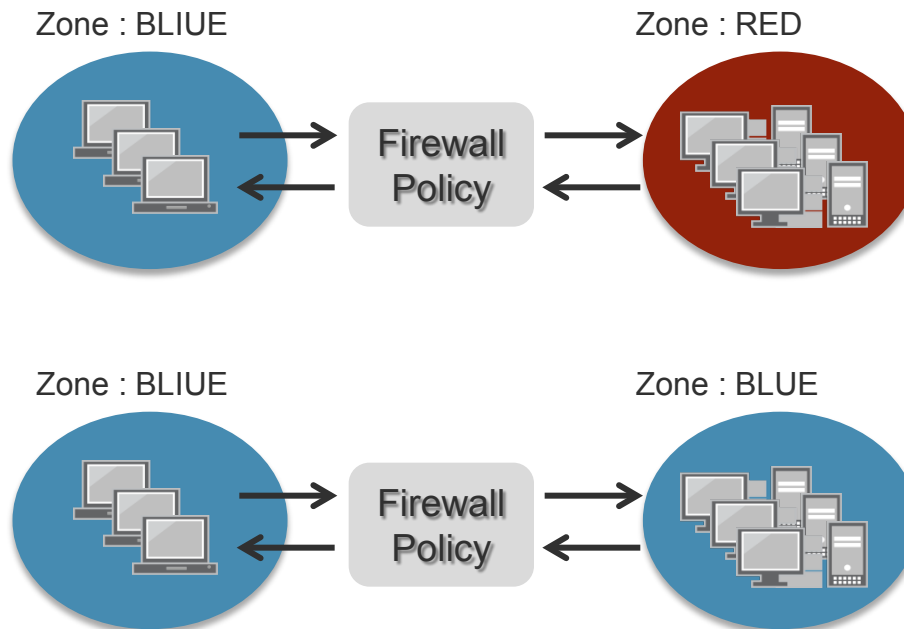
新しくインタフェース/Zoneを追加・設定するためには「Add」を押す。

Back Next

Security Zoneについて



セキュリティゾーンとは、インタフェース群に割り当てる仮想的なグループです。SRXではこのセキュリティゾーンを使用してトラフィックを制御します。異なるゾーン間で通信されるトラフィック、またはゾーン内の別インタフェース間で通信されるトラフィックがファイアウォールポリシーにて制御される通信対象となります。



Step6-4 : Interfacesの設定 : インタフェースとZoneの追加

インタフェースのプルダウンから追加したいインタフェースを指定して(①)、アドレスを設定する(②)、その際Zoneを新しく作成したい場合にはプルダウンから「Add new zone」を選択して(③)Zone名を記入し(④)、「Save」(⑤)

The screenshot shows the 'Add/Edit Interface' configuration page in the Juniper J-Web interface. The page is titled 'Setup Wizard' and has a sidebar with navigation options: Introduction, System, Identification, Network, Interfaces, J-Web preferences, Time Management, and Review & Commit. The main content area is divided into 'Interface Settings' and 'Services (Inbound)'. The 'Interface Settings' section includes fields for 'Interface *', 'Address *', 'IP address/subnet', and 'Security zone'. The 'Services (Inbound)' section has checkboxes for 'All', 'Untrust', 'Add new zone', and 'DHCP'. The 'Protocols (Inbound)' section has checkboxes for 'All', 'OSPF', 'BGP', 'RIP', 'PIM', and 'IGMP'. A blue callout box highlights the 'Add new zone' option in the 'Security zone' dropdown menu. A separate inset window shows the 'Add new zone' dialog with fields for 'IP address/subnet' and 'Zone name', and a 'Save' button. Green circles with numbers 1 through 5 indicate the steps: 1. Selecting the interface, 2. Setting the IP address, 3. Selecting 'Add new zone', 4. Entering the zone name, and 5. Clicking 'Save'.

Interface Settings

Interface * : ge-0/0/1.0

Address * : DHCP IP Address PPPoe

IP address/subnet: 192.168.2.1/24

Security zone : [dropdown menu]

Services (Inbound) trust

All Untrust Add new zone DHCP

Protocols (Inbound)

All OSPF BGP RIP PIM IGMP

Zone name: dmz

Services (Inbound)

All HTTPS Ping Untrust Add new zone DHCP

Protocols (Inbound)

All OSPF BGP RIP PIM IGMP

Cancel Save

Step6-5 : Interfacesの設定 : インタフェースとZoneの追加

Initial Setup

Host : NoName(srx210h) Logged in as : root

JUNIPER NETWORKS

Setup Wizard

- Introduction
- System
- Identification
- Network
- Interfaces
- J-Web preferences
- Time Management
- Review & Commit

Configure Interfaces

THIS STEP IS OPTIONAL

Add Edit Delete

Name	IP Address/Subnet	Security Zone	Services (Inbound)	Protocols (Inbound)
vlan.0	192.168.1.1/24	trust		all
ge-0/0/0.0	192.168.0.1/24	untrust		
ge-0/0/1.0	192.168.2.1/24	dmz		

Back Next

①

②

作成されたZoneとインタフェースを確認して(①)、「Next」(②)へ

Step7 : J-webの設定

Initial Setup

Host : NoName(srx210h) Logged in as : root Help Logout

JUNIPER NETWORKS

Setup Wizard

- Introduction
- System
- Identification
- Network
- Interfaces
- J-Web preferences**
- Time Management
- Review & Commit

About this page
J-Web is the Juniper Web Device Manager, which enables you to configure, monitor, and maintain the device by using an interface. This page enables you to select the way J-Web behaves when you start it. Click a heading to get information about the options.

Configure J-Web preferences: * Required

J-Web starting page options *

- Dashboard (expect 10-20 secs to load)
- Configure**
- Monitor
- Last accessed

J-Web commit options *

- Validate every time and explicit commit in the end**
- Commit every time

Back Next

J-webの基本設定、

- ・ ログイン後にデフォルトで表示されるタブ (①)
- ・ 設定変更後のCommit処理 (②) (※Commitのコンセプトについては後述) を選択し、「Next」(③)へ

Step8 : 時間・NTPの設定

Initial Setup
Host : NoName(srx210h) Logged in as : root

Setup Wizard

- Introduction
- System
 - Identification
 - Network
- Interfaces
- J-Web preferences
- Time Management
 - Review & Commit

Configure System: Time
THIS STEP IS OPTIONAL

Time

Current System Time 2011-10-03 14:51:00

Time Zone Asia/Tokyo

NTP Servers

192.168.1.100

Back Next

TimeZone (①)、時間 (②)、NTPサーバー (③) (オプション) の設定をして「Next」(④) へ

Step9 : 設定の確認、反映

セットアップウィザードで設定を行った項目について確認をし、修正箇所があれば「Back」へ、設定を反映させるためには「Commit」(①)へ

Commitを投下することでシステムに設定が反映される(②)
(Commitされるまでは設定変更はなされない)

2

1

Initial Setup
Host : NoName(srx210h)

Setup Wizard

- Introduction
- System
 - Identification
 - Network
- Interfaces
- J-Web preferences
- Time Management
- Review & Commit

About this page
When you edit a configuration, the changes you make do not take effect until you commit them. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file.
This page shows the information you have entered and any errors detected so you can review them and make changes, if necessary, before committing the configuration. Scroll down to see all the information.

Review & Commit
Review all System Settings and click Commit if OK. You may click headers to make changes.

System Configuration

Identity

Host name	juniper.local
Domain name	

Network

DNS name server	208.67.222.222 208.67.220.220
Domain search	
Default gateway	

Time

New date/time	
Time zone	Asia/Tokyo
NTP servers	192.168.1.100

Configuration Delivery

Configuration Delivery

OK

Details >>

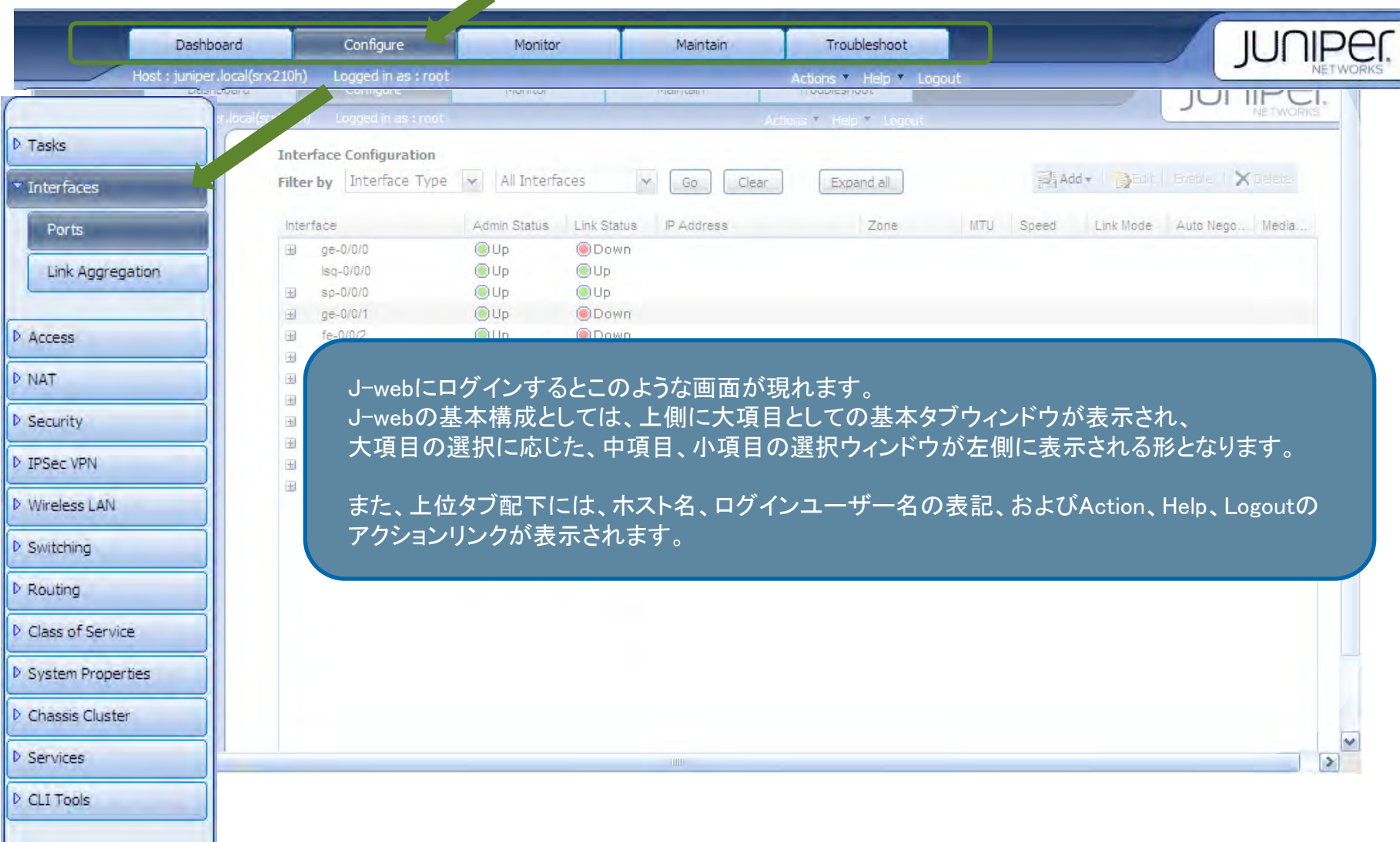
Back Commit

Step10 : J-webの確認 : ログイン

設定が完了するとログイン画面に戻るので、Step3で設定したパスワード(①)でログイン(②)



Step10 : J-webの確認 : 基本ウィンドウ



Host : juniper.local(srx210h) Logged in as : root Actions Help Logout

Dashboard Configure Monitor Maintain Troubleshoot

Tasks

Interfaced

Ports

Link Aggregation

Access

NAT

Security

IPSec VPN

Wireless LAN

Switching

Routing

Class of Service

System Properties

Chassis Cluster

Services

CLI Tools

Interface Configuration

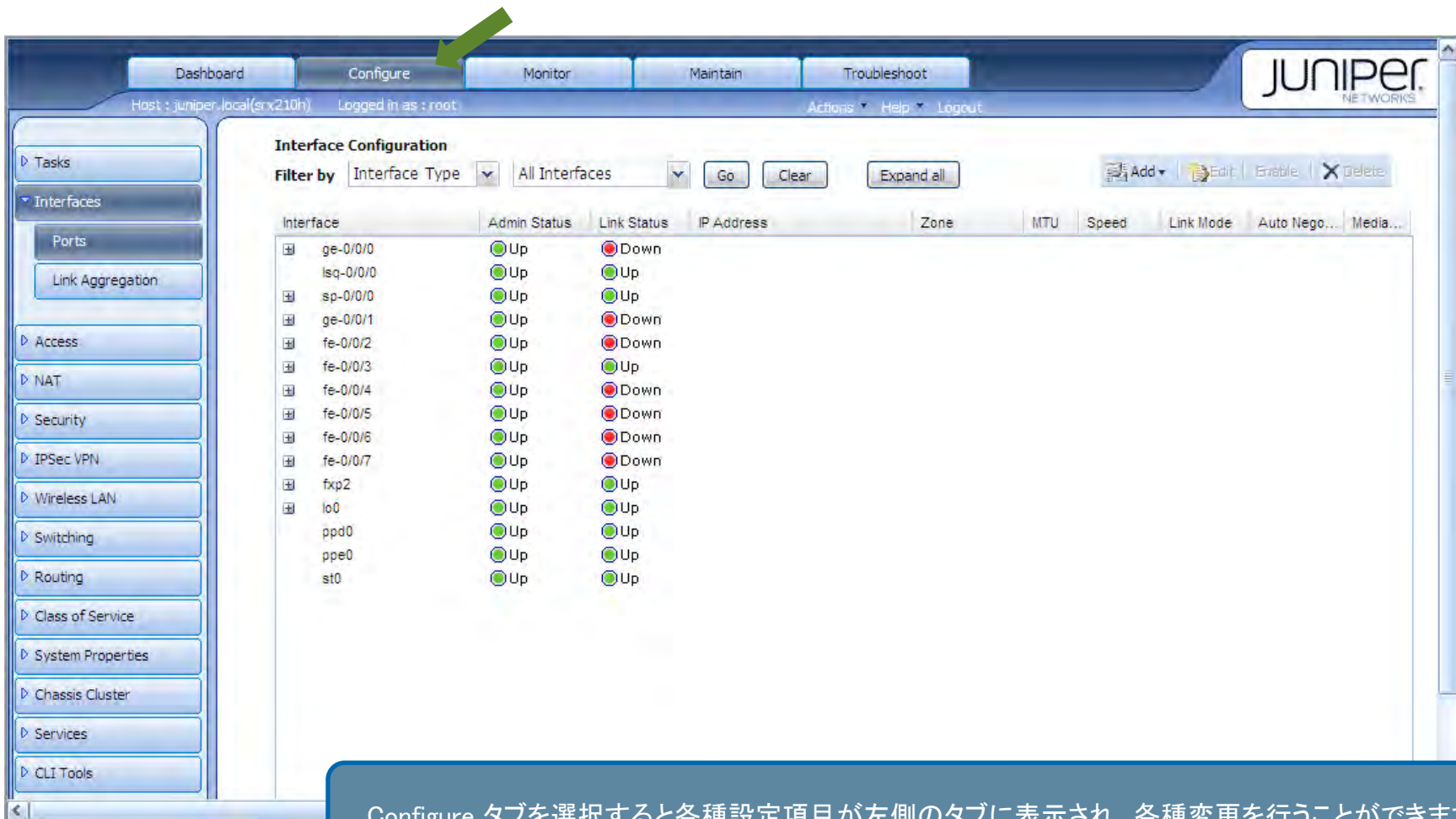
Filter by Interface Type All Interfaces Go Clear Expand all Add Edit Enable Delete

Interface	Admin Status	Link Status	IP Address	Zone	MTU	Speed	Link Mode	Auto Nego...	Media...
ge-0/0/0	Up	Down							
lsq-0/0/0	Up	Up							
sp-0/0/0	Up	Up							
ge-0/0/1	Up	Down							
fe-0/0/2	Up	Down							

J-webにログインするとこのような画面が現れます。
J-webの基本構成としては、上側に大項目としての基本タブウィンドウが表示され、大項目の選択に応じた、中項目、小項目の選択ウィンドウが左側に表示される形となります。

また、上位タブ配下には、ホスト名、ログインユーザー名の表記、およびAction、Help、Logoutのアクションリンクが表示されます。

Step10 : J-webの確認 : Congigure タブ



Host : juniper.local(srx210h) Logged in as : root Actions Help Logout

Interface Configuration

Filter by Interface Type All Interfaces Go Clear Expand all Add Edit Enable Delete

Interface	Admin Status	Link Status	IP Address	Zone	MTU	Speed	Link Mode	Auto Nego...	Media...
ge-0/0/0	Up	Down							
lsq-0/0/0	Up	Up							
sp-0/0/0	Up	Up							
ge-0/0/1	Up	Down							
fe-0/0/2	Up	Down							
fe-0/0/3	Up	Up							
fe-0/0/4	Up	Down							
fe-0/0/5	Up	Down							
fe-0/0/6	Up	Down							
fe-0/0/7	Up	Down							
fxp2	Up	Up							
lo0	Up	Up							
ppd0	Up	Up							
ppe0	Up	Up							
st0	Up	Up							

Configure タブを選択すると各種設定項目が左側のタブに表示され、各種変更を行うことができます。

Step10 : J-webの確認 : Dashboard タブ

The screenshot displays the Juniper J-web Dashboard. The top navigation bar includes tabs for Dashboard, Configure, Monitor, Maintain, and Troubleshoot. The Dashboard tab is selected, indicated by a green arrow. The main content area features a central image of a Juniper SRX210 device. Below this, there are several panels:

- System Identification:** Displays details such as Serial Number (AD2609AA0092), Host Name (juniper.local), Software Version (JUNOS Software Release [11.2R2.4]), Bios Version (1.7), System Up Time (00:23:15 since 2011-10-03 23:39:41 JST), and System Time (2011-10-04 00:02:56 JST).
- Resource Utilization:** A bar chart showing CPU (Control) at 32%, Memory (Control) at 64%, CPU (Data) at 45%, Memory (Data) at 23.24%, and Storage at 23.24%.
- System Alarms:** A table listing received alarms with their severity and descriptions.
- Security Resources:** A section showing Sessions (0%), FW policies (0.2%), and VPNs (0%).

A blue callout box at the bottom of the screenshot contains the text: "Dashboard タブを選択すると各種機器の情報や状態がグラフィカルに表示されます。"

Step10 : J-webの確認 : Monitor タブ



The screenshot shows the Juniper J-web interface with the 'Monitor' tab selected. A green arrow points to the 'Monitor' tab. The interface displays the following information:

- Port Monitoring:** A table showing the status of various ports. The 'ge-0/0/0' port is highlighted.
- Interface Statistics - ge-0/0/0:** Four sub-sections: Input Rate (0.000 Kbps), Output Rate (0.000 Kbps), Error Counters (Input/Output), and Packet Counters (Input/Output).

Port	Admin Status	Link Status	Address	Zone	Services	Protocols
ge-0/0/0	Up	Up				
ge-0/0/0.0	Up	Up	192.168.0.1/24	untrust	tftp,dhcp	
gr-0/0/0	Up	Up				
ip-0/0/0	Up	Up				
lsq-0/0/0	Up	Up				
lt-0/0/0	Up	Up				

Monitor タブを選択すると確認が可能な項目が左側のタブに表示され、選択することで各種状態の確認が可能です。

Step10 : J-webの確認 : Maintain タブ

Host : juniper.local(srx210h) Logged in as : root Actions Help Logout

Config Management

Upload

Type the name of a configuration file on the local hard drive. When you click "Upload and Commit", the configuration in the file replaces the existing configuration and takes effect. If any errors occur when the file is loading or committing, they are displayed and the previous configuration is restored.

* File to Upload ?

Maintain タブを選択すると設定やライセンス、ソフトウェアなどに関わる管理項目が左側のタブに表示され、各種管理を行うことができます。

Step10 : J-webの確認 : Troubleshoot タブ

Host : juniper.local(srx210h) Logged in as : root Actions Help Logout

Traceroute

Traceroute to Host

The traceroute diagnostic tool uses a series of packets crafted to elicit an ICMP "time exceeded" messages from intermediate points in the network between your device and the specified host.

The time-to-live for a packet is decremented each time the packet is routed, so traceroute generally receives at least one "time exceeded" response from each waypoint. Traceroute starts with a packet with a time-to-live value of one, and increments the time to live for subsequent packets, thereby constructing a rudimentary map of the path between hosts.

Entering a host below creates a traceroute task that will run until the traceroute is complete or until it fails due to time out.

* Remote Host ?

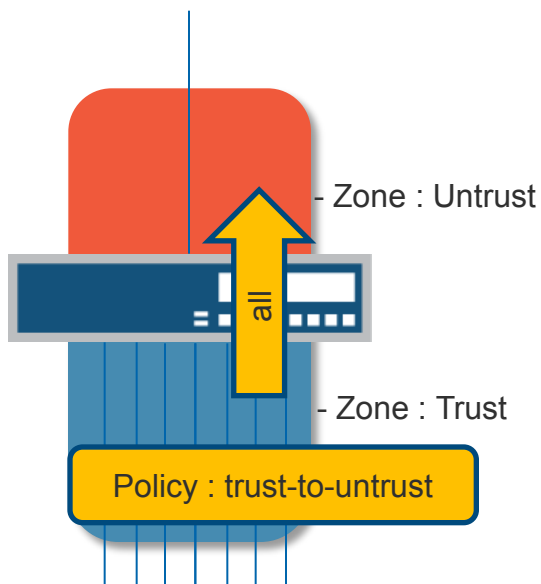
+ **Advanced options**

Troubleshoot タブを選択すると通信確認やパケットキャプチャに関する項目が左側のタブに表示され、障害時などにおける状況確認を行うことができます。

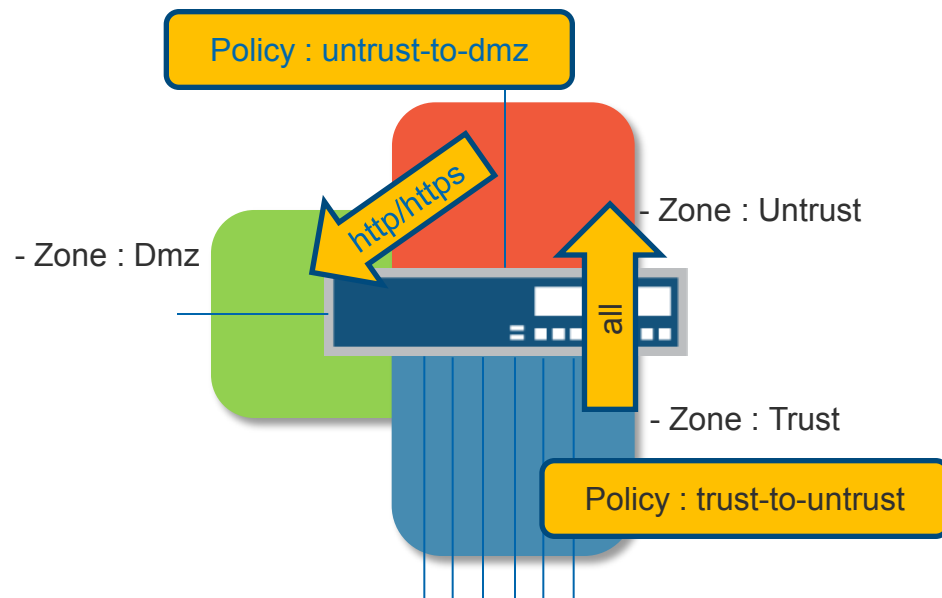
Chapter2. Firewall Policy

このガイドで構築するファイアウォールポリシー構成

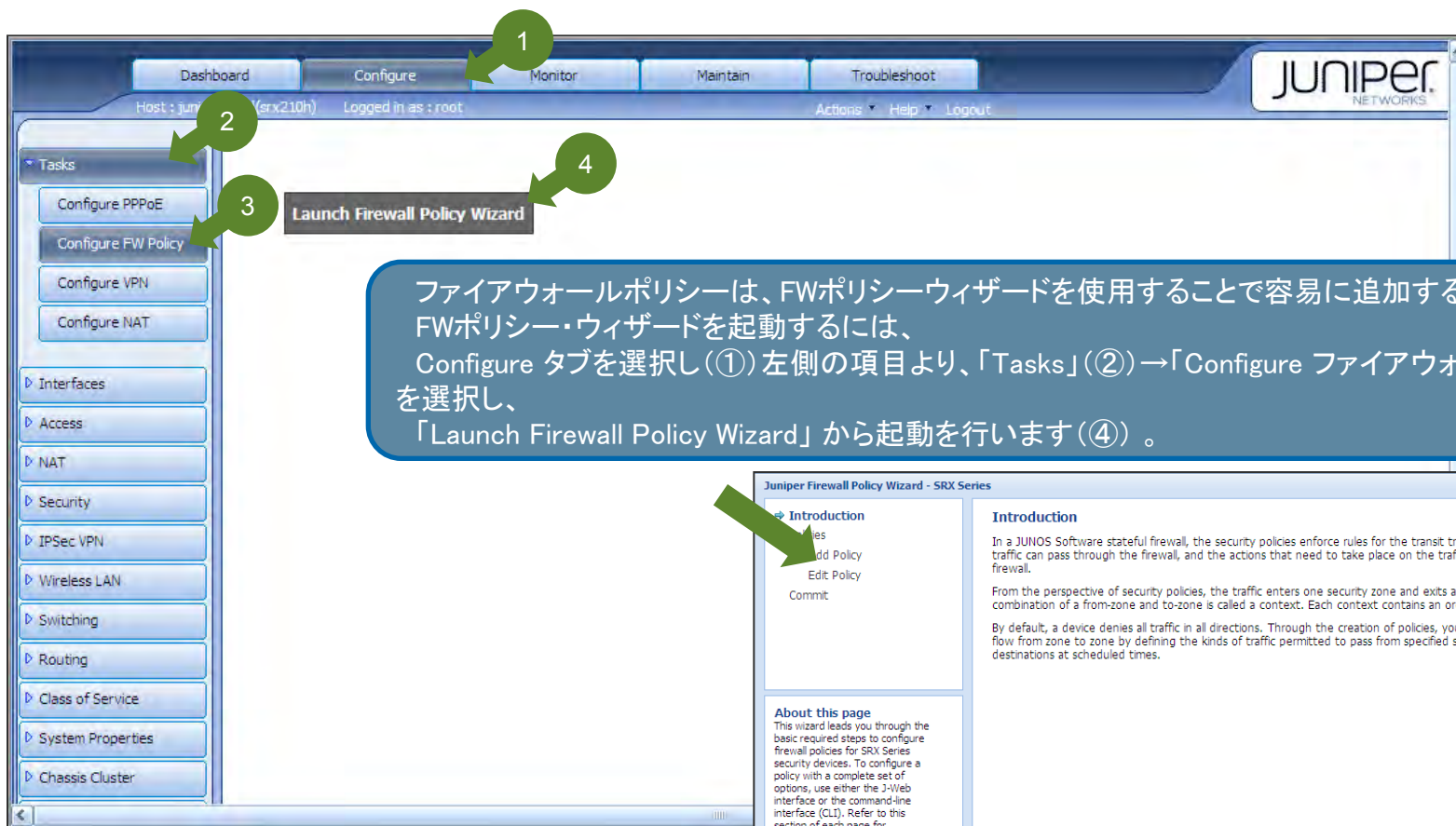
工場出荷時におけるファイアウォールのポリシー設定



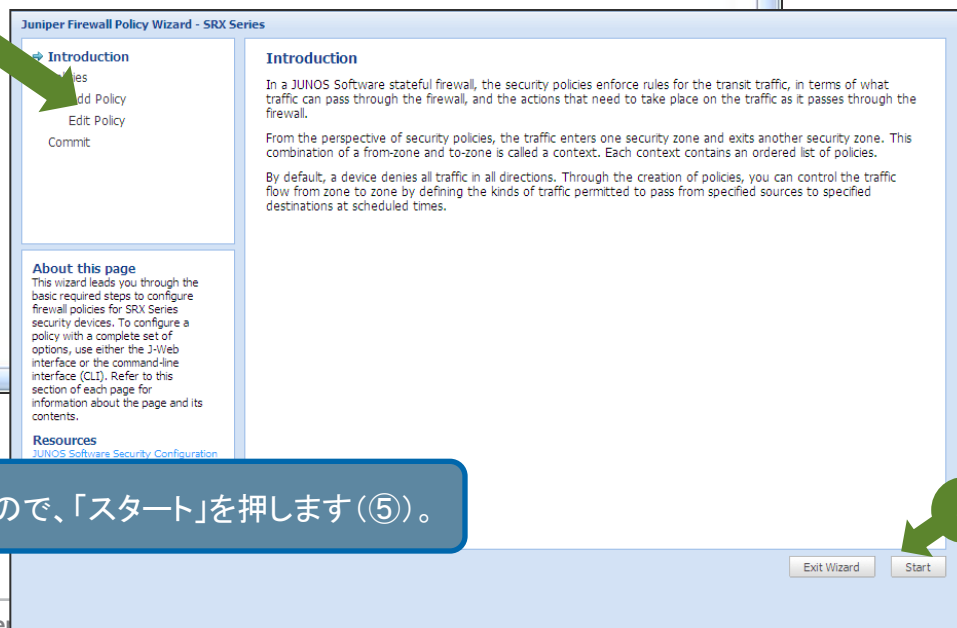
このガイドで構成するサンプル・ファイアウォールのポリシー設定



Step1 : ファイアウォールポリシー・ウィザードの起動



ファイアウォールポリシーは、FWポリシーウィザードを使用することで容易に追加することが可能です。FWポリシー・ウィザードを起動するには、Configure タブを選択し(①)左側の項目より、「Tasks」(②)→「Configure ファイアウォールポリシー」(③)を選択し、「Launch Firewall Policy Wizard」から起動を行います(④)。



別ウィンドウでウィザードが始まるので、「スタート」を押します(⑤)。

Step2 : ファイアウォールポリシーの追加



Juniper Firewall Policy Wizard - SRX Series

- Introduction
- ➔ Policies
 - Add Policy
 - Edit Policy
 - Commit

Configure Firewall Policies

Add Edit Delete

Reorder	Name	From Zone	To Zone	Application	Action
	trust-to-untrust	trust	untrust	any	✓

About this page
This page displays firewall policies that are already configured for the device. You can edit the displayed policies, create additional ones, or delete policies.

To make changes to a policy, double-click the row. To add policies, click Add. To delete a policy, select the row, and click Delete.

The rows sort alphabetically by From Zone. To reorder the rows so that the policy rules execute in a different sequence, use the arrows in the left column. We recommend placing more specific policies near the top of the list. The default policy is

Back

ウィザードが開始されたら、「Add」を押します(①)。

Step3-1 : ファイアウォールポリシー の追加 - アドレスブック の作成

The screenshot shows the Juniper Firewall Policy Wizard interface. On the left, a sidebar contains navigation options: Introduction, Policies, Add Policy (selected), Edit Policy, and Commit. The main area is titled 'Add/Edit Policy' and includes a 'Policy Name' field, a 'Source zone/address' section, and a 'Selected zone/address' section. Below these are two lists of 'Available zone/address' pairs. A blue callout box points to the 'Add Zone/Address Pair' link at the bottom of the page, stating: 'ファイアウォールポリシーで使用するアドレスオブジェクトをSRXではアドレスブックといいます。アドレスブックを作成するには、「Add Zone/Address Pair」のリンクをクリックします(①)。

A second blue callout box points to the 'Add Zone/Address Pair' dialog box, which is open in the foreground. It contains fields for 'Address name', 'Zone', and 'IP Address', along with 'Cancel' and 'Add' buttons. Green arrows with numbers 2 through 5 point to these elements: 2 points to the 'Address name' field (containing 'web-server'), 3 points to the 'Zone' field (containing 'dmz'), 4 points to the 'IP Address' field (containing '192.168.2.100'), and 5 points to the 'Add' button. The dialog box also has a 'Log (Optional)' checkbox and radio buttons for 'Permit' (selected) and 'Deny'.

Step3-2 : ファイアウォールポリシー の追加 - アドレスブック の作成

Juniper Firewall Policy Wizard - SRX Series

Introduction
Policies
➔ **Add Policy**
Edit Policy
Commit

About this page
Enter a policy name, and then complete the match criteria and action for that policy. The match criteria are the source zones and addresses, the destination zones and addresses, and the application that the traffic carries in its protocol headers. The action specifies how to handle the matching packets.
To add a new zone/address pair, click the link at the bottom of the page and fill in the dialog box that appears. When you create a new zone address pair, you cannot edit or delete it with this wizard. You must use the [Configure > Security > Policy Elements > Address Book](#) page.

Add/Edit Policy All fields are required

Policy Name:

Source zone/address	Destination zone/address	Application	Action
Selected zone/address	Selected zone/address	Selected applications	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="checkbox"/> Log (Optional)

Created Zone/Address Pairs:

Available zone/address	Available zone/address	Available applications
dmz/any	dmz/any	any
dmz/any-ipv4	dmz/any-ipv4	junos-aol
dmz/any-ipv6	dmz/any-ipv6	junos-bgp
dmz/web-server	dmz/web-server	junos-biff
trust/any	trust/any	junos-bootpc
trust/any-ipv4	trust/any-ipv4	

Add Zone/Address Pair

Cancel Save

作成したゾーンとアドレスブックのペアが作成されていることを確認します(①)。

Step4-1 : ファイアウォールポリシー の追加 — ファイアウォールポリシーの設定

ポリシー名を記入(①)し、「Source zone/address」(②)、「Destination zone/address」(③)、「Application」(④)、「Action」(⑤)、「Log (Option)」(⑥)からそれぞれ希望する選択肢を選び、「Save」(⑦)ボタンを押します。

Juniper Firewall Policy Wizard - SRX Series

Introduction
Policies
➔ **Add Policy**
Edit Policy
Commit

About this page
Enter a policy name, and then complete the match criteria and action for that policy. The match criteria are the source zones and addresses, the destination zones and addresses, and the application that the traffic carries in its protocol headers. The action specifies how to handle the matching packets.
To add a new zone/address pair, click the link at the bottom of the page and fill in the dialog box that appears. When you create a new zone address pair, you cannot edit or delete it with this wizard. You must use the [Configure > Security > Policy Elements > Address Book](#) page.

Add/Edit Policy All fields are required

Policy Name: untrust-to-dmz

Source zone/address	Destination zone/address	Application	Action
Selected zone/address untrust/any	Selected zone/address dmz/web-server	Selected applications junos-http	Action <input checked="" type="radio"/> Permit <input type="radio"/> Deny <input checked="" type="checkbox"/> Log (Optional)

Available zone/address: dmz/web-server, trust/any, trust/any-ipv4, trust/any-ipv6, untrust/any-ipv4, untrust/any-ipv6

Available zone/address: dmz/any, dmz/any-ipv4, dmz/any-ipv6, trust/any, trust/any-ipv4, trust/any-ipv6

Available applications: junos-http-ext, junos-https, junos-icmp-all, junos-icmp-ping, junos-icmp6-all

[Add Zone/Address Pair](#)

Cancel Save

Step4-2 : ファイアウォールポリシー の追加 — ファイアウォールポリシーの設定

意図したポリシーが作成されていることを確認したのち、「Commit」ボタンを押すと、設定が完了します。

Juniper Firewall Policy Wizard - SRX Series

Introduction
Policies
Add Policy
Edit Policy
Commit

Configure Firewall Policies

Add Edit Delete

Reorder	Name	From Zone	To Zone	Application	Action
	trust-to-untrust	trust	untrust	any	✓
	untrust-to-dmz	untrust	dmz	junos-http,junos-https	✓

About this page
This page displays firewall policies that are already configured for the device. You can edit the displayed policies, create additional ones, or delete policies.
To make changes to a policy, double-click the row. To add policies, click Add. To delete a policy, select the row, and click Delete.
The rows sort alphabetically by From Zone. To reorder the rows so that the policy rules execute in a different sequence, use the arrows in the left column. We recommend placing more specific policies near the top of the list. The default policy is

Configuration Delivery

Configuration Delivery OK Details >>

Back Commit

Step5-1 : ファイアウォールポリシー の追加 - ファイアウォールポリシーの順序設定

Juniper Firewall Policy Wizard - SRX Series

Introduction
Policies
Add Policy
Edit Policy
Commit

Configure Firewall Policies

Add Edit Delete

Reorder	Name	From Zone	To Zone	Application	Action
	trust-to-untrust	trust	untrust	any	✓
↕	untrust-to-dmz	untrust	dmz	junos-http,junos-https	✓
↕	untrust-to-dmz_2	untrust	dmz	junos-http	✓
↕	untrust-to-dmz_d...	untrust	dmz	any	✗

About this page
This page displays firewall policies that are already configured for the device. You can edit the displayed policies, create additional ones, or delete policies.
To make changes to a policy, double-click the row. To add policies, click Add. To delete a policy, select the row, and click

Back Commit

arrows in the left column. We recommend placing more specific policies near the top of the list. The default policy is

同じSource ZoneとDestination Zoneにおいて複数のFWポリシーを作成すると、「Reorder」の欄に矢印が表示されます。FWポリシーの順序を変更したい場合には、変更したいポリシーを変更したい順序に向けた矢印を選択します(①)。

Step5-2 : ファイアウォールポリシー の追加 — ファイアウォールポリシーの順序設定

Juniper Firewall Policy Wizard - SRX Series

Introduction
Policies
Add Policy
Edit Policy
Commit

Configure Firewall Policies

Add Edit Delete

Reorder	Name	From Zone	To Zone	Application	Action
	trust-to-untrust	trust	untrust	any	✓
▲ ▼	untrust-to-dmz	untrust	dmz	junos-http,junos-https	✓
▲ ▼	untrust-to-dmz_d...	untrust	dmz	any	✗
▲ ▼	untrust-to-dmz_2	untrust	dmz	junos-http	✓

About this page
This page displays firewall policies that are already configured for the device. You can edit the displayed policies, create additional ones, or delete policies.
To make changes to a policy, double-click the row. To add policies, click Add. To delete a policy, select the row, and click

arrows in the left column. We recommend placing more specific policies near the top of the list. The default policy is

Back Commit

①

②

FWポリシーが意図した順番に変更されていることを確認して(①)、「Commit」を押すことで(②)設定が反映されます。

Step6-1 : ファイアウォールポリシーの表示

①

②

③

④

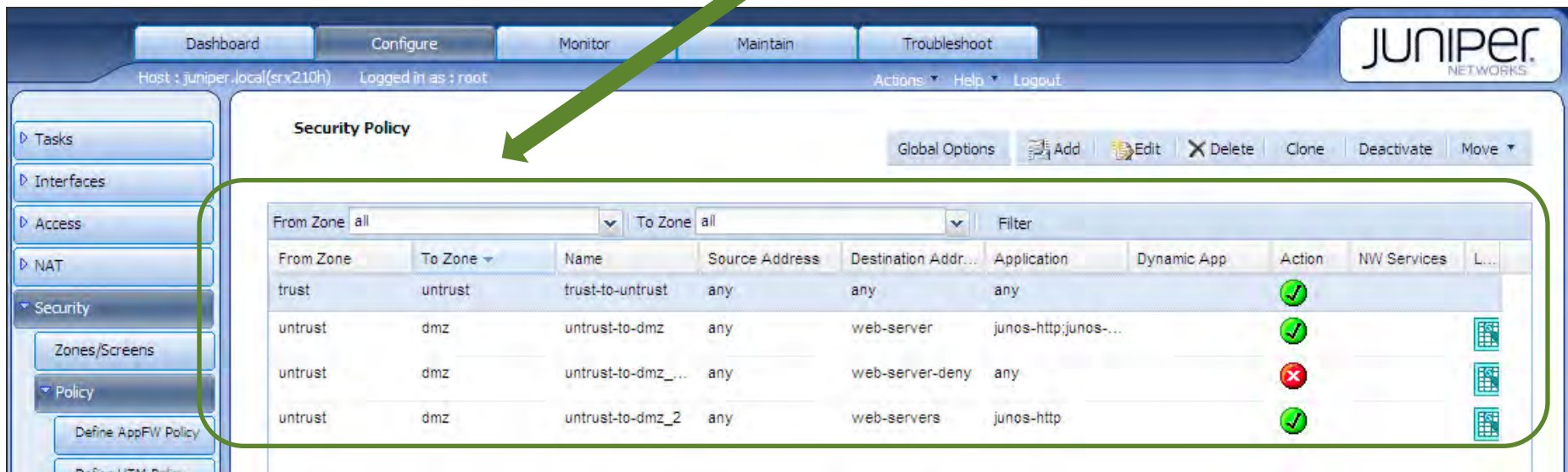
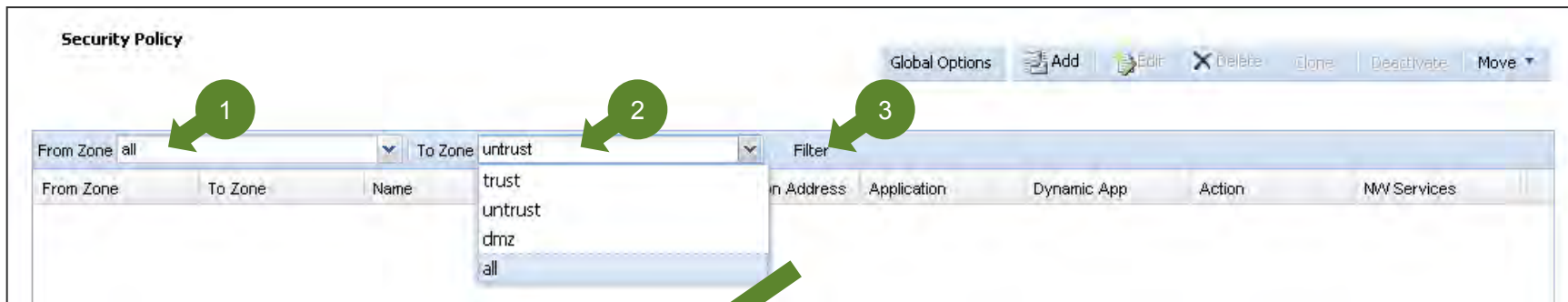
Security Policy

From Zone	To Zone	Name	Source Address	Destination Addr...	Application	Dynamic App	Action	NW Services	L...
trust	untrust	trust-to-untrust	any	any	any		✓		

ファイアウォールポリシーを表示するには、Configure タブを選択し(①)、左側の項目より、「Security」(②)→「Policy」(③)→「Apply Policy」(④)を選択することで表示させることが可能です。

Step6-2 : ファイアウォールポリシーの表示

作成したポリシーを表示、確認するためにはポリシー表示ウィンドウ上部にあるフィルターから表示させたいFrom/To Zoneを選択(①②)して「Filter」(③)を押します。



Step6-3 : ファイアウォールポリシーの表示

ファイアウォールポリシーの表示ルールは以下の配列になっています。

The screenshot shows the Juniper Networks configuration interface for a Security Policy. The table below represents the data shown in the interface:

From Zone	To Zone	Name	Source Address	Destination Address	Application	Dynamic App	Action	NW Services	Log/Count
untrust	dmz	untrust-to-dmz	any	dmz-servers	junos-https,junos-htt		Permit (Green checkmark)		
untrust	dmz	deny-all	any	any	any		Deny (Red X)		
untrust	dmz	untrust-to-dmz2	any	dmz-servers	junos-ftp		Permit (Green checkmark)		

Annotations in the diagram point to the following fields in the table:

- 送信元Zone** (Source Zone) points to the "From Zone" column.
- 送信先Zone** (Destination Zone) points to the "To Zone" column.
- ポリシー名** (Policy Name) points to the "Name" column.
- 送信元アドレス** (Source Address) points to the "Source Address" column.
- 送信先アドレス** (Destination Address) points to the "Destination Address" column.
- アプリケーション** (Application) points to the "Application" column.
- アクション** (Action) points to the "Action" column.
- FWログ** (FW Log) points to the "Log/Count" column.

Legend for Action:

- Permit アクション (Green checkmark icon)
- Deny アクション (Red X icon)

Step7 : ファイアウォールポリシーの設定 アドレスブックの設定

ファイアウォールポリシーはセットアップウィザードからではなく、個別に設定を行うことも可能です。

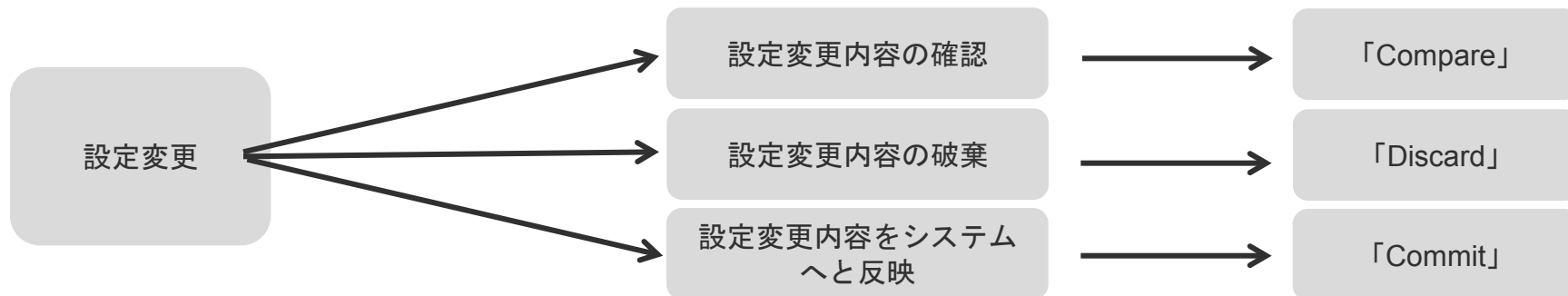
The screenshot shows the Juniper Networks configuration interface. The main window is titled "Addresses/Address-sets Configuration". On the left sidebar, the "Security" menu is expanded, and "Address Book" is selected, indicated by a green callout with the number 1. In the top right corner of the main window, there are "Add", "Edit", and "Delete" buttons, with a green callout with the number 2 pointing to the "Add" button. An "Add Address" dialog box is open in the center, with a green callout with the number 3 pointing to it. The dialog box contains fields for "Zone", "Address Name", and "Address Sets", along with radio buttons for "IP(v4/v6)/Prefix" and "Domain Name".

Zone Name	Address Name
dmz	web-server
dmz	web-servers
dmz	web-server-deny

アドレスブックを作成するには、Configure タブを選択し左側の項目より、「Security」→「Policy Elements」→「Address Book」を選択して①「Add」②でアドレスブック設定ウィンドウを表示させます③。

Step8 : GUI設定と「Commit」について

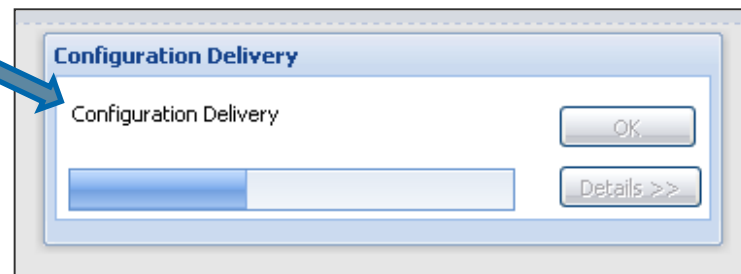
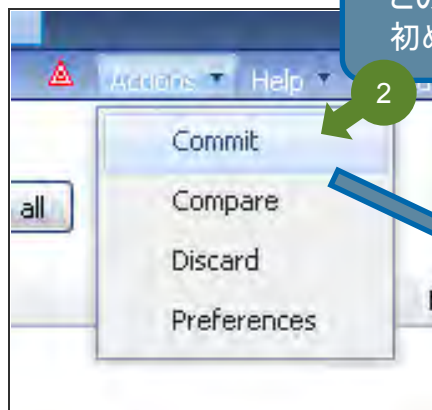
GUIでの設定変更はJUNOS CLIと同様に、即時反映されることなく「Commit」を経てシステムに反映される仕組みになっています。



GUI設定が完了すると「Action」タブに赤い印が表示され、ハイライトされる(①)



この状態からプルダウンより「Commit」を選んで押すことで初めて設定がシステムに反映されます(②)。



Step9-1 : ファイアウォールポリシーの設定 Zoneの設定

ファイアウォールポリシーを適用するZone を作成・設定変更するには、
Configure タブを選択し左側の項目より、「Security」→「Zone/Screens」から行います。

Zones/Screens configuration

Zones list:

Zone name	Type	Services	Protocols	Interfaces	Screen
trust	security		all	vlan.0	
untrust	security			ge-0/0/0.0	untrust-screen
dmz	security			ge-0/0/1.0	

① ② ③

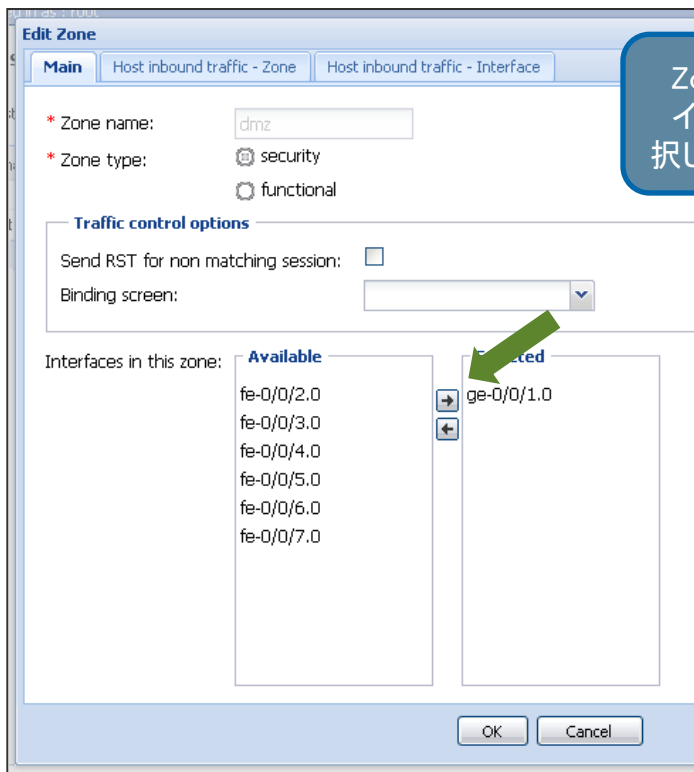
新しいZoneを作成したり設定するには、Configure タブを選択し左側の項目より、「Security」→「Zone/Policies」を選択します(①)。

デフォルトでは「trust」、「untrust」のzoneが作成されており、この例ではBasic Setupを介して作成された「dmz」Zoneが表示されています。

新規にZoneを作成する場合は「Add」を、既存にあるZoneを編集するにはZoneをクリックしてハイライト(②)した後に「Edit」(③)を押します。

Step9-2 : ファイアウォールポリシーの設定

Zoneの設定



Zoneの設定ウィンドウが表示されるので、
インタフェースの増減を行う場合は、「→」「←」で選
択したインタフェースを動かします。



Zoneに対して許可するInboundトラフィックを設定する場合には、
「Host inbound traffic -Zone」タブを選択し(①)、許可したいトラフィック
やプロトコルを追加し(②③)、「OK」(④)を押します。

Step9-3 : ファイアウォールポリシーの設定

FWポリシーの設定

Dashboard Configure Monitor Maintain Troubleshoot

Host : juniper.local(eri210h) Logged in as : root Actions Help Logout

JUNIPER NETWORKS

Security Policy

Global Options Add Edit Delete Clone Deactivate Move

From Zone trust To Zone untrust Filter

From Zone	To Zone	Name	Source Address	Destination Address	Application	Dynamic App	Action	NW Services	L...
trust	untrust	trust-to-untrust	any	any	any		✓		

Policy Logging/Count Scheduling

Policy Name: * Policy Action: Action

From Zone: Source zone To Zone: Destination zone

Source Address Address-book: Matched

any any-ipv4 any-ipv6

Destination Address Address-book: Matched

any any-ipv4 any-ipv6

Applications Application: Applications/Sets: Matched

any junos-ftp junos-ftp junos-rsp junos-netbios-session

Search:

FWポリシーを作成するには、
Configure タブを選択し左側の項目より、「Security」→「Policy」→「Apply Policy」を選択して(①)
「Add」(②)でポリシー設定ウインドウを表示させます(③)。

Step9-4 : ファイアウォールポリシーの設定

FWポリシーの設定

ポリシー設定ウィンドウが表示されたら、ポリシー名(①)、From/To Zone(②)、送信元/送信先 アドレス(③)、対象アプリケーション(④)、及びポリシーアクション(⑤)を記載、選択し、「OK」(⑥)を押します。

Add Policy

Policy | Logging/Count | Scheduling | Permit Action | Application Services

* Policy Name: untrust-to-dmz

* From Zone: untrust

* To Zone: dmz

* Policy Action: permit

* Source Address

Address-Book: any-ipv4, any-ipv6

Matched: any

* Destination Address

Address-Book: http-server, https-server, any, any-ipv4

Matched: dmz-servers

* Applications

* Application: junos-ftp, junos-bootps, junos-finger, junos-https, junos-pop3, junos-ident

Matched: junos-http

Search:

OK Cancel

Step9-5 : ファイアウォールポリシーの設定 FWポリシーの設定

*** Destination Address**

Address-Book

http-server
https-server
any
any-ipv4

Matched

dmz-servers

Add new destination address

* Address Name:

* Address:

*** Applications**

* Application

Applications/Sets

junos-http-ext
junos-https
junos-http

Matched

Search:

Step9-6 : ファイアウォールポリシーの設定 FWポリシーの設定

作成したファイアウォールポリシーにファイアウォールログを追加するには、「Logging/Count」タブを選択し、「Log Options」部分にチェックをいれます。

Add Policy

Policy **Logging/Count** Scheduling

Enable Count

Per Minute Alarm Threshold: (0..4294967295 kbyte)

Per Second Alarm Threshold: (0..4294967295 byte)

Log Options

Log at Session Close Time:

Log at Session Init Time:

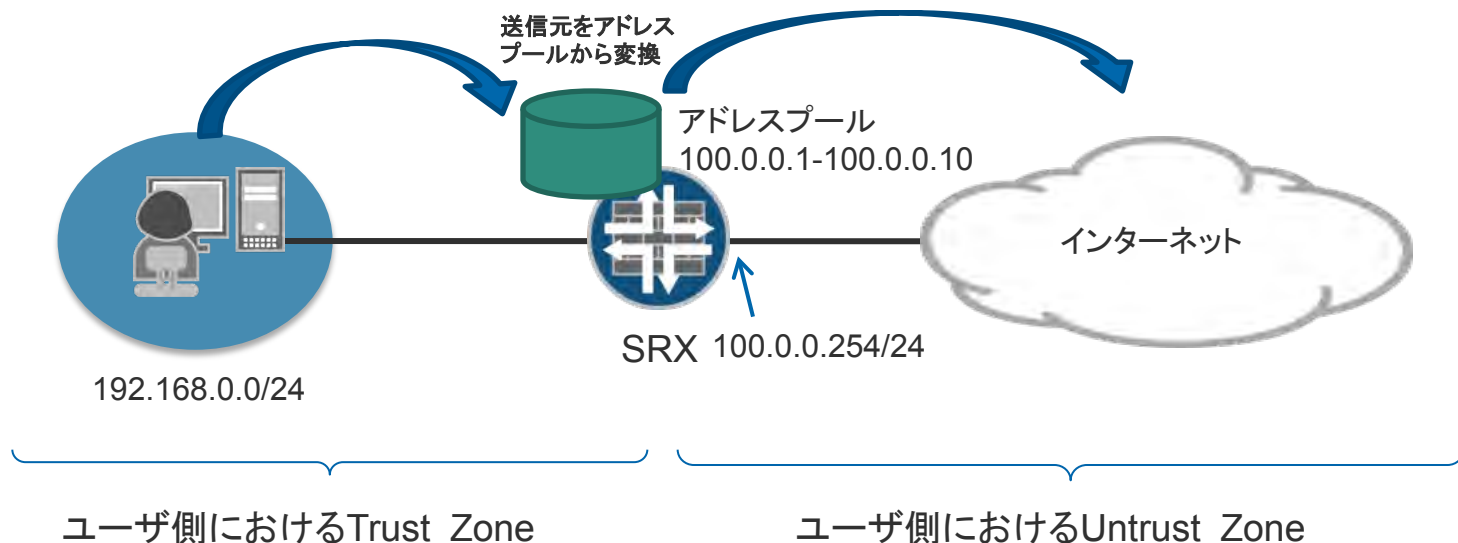
OK Cancel

Chapter3. NAT

- Source NAT
- Static NAT

Source NAT – このガイドで構築する物理・論理構成

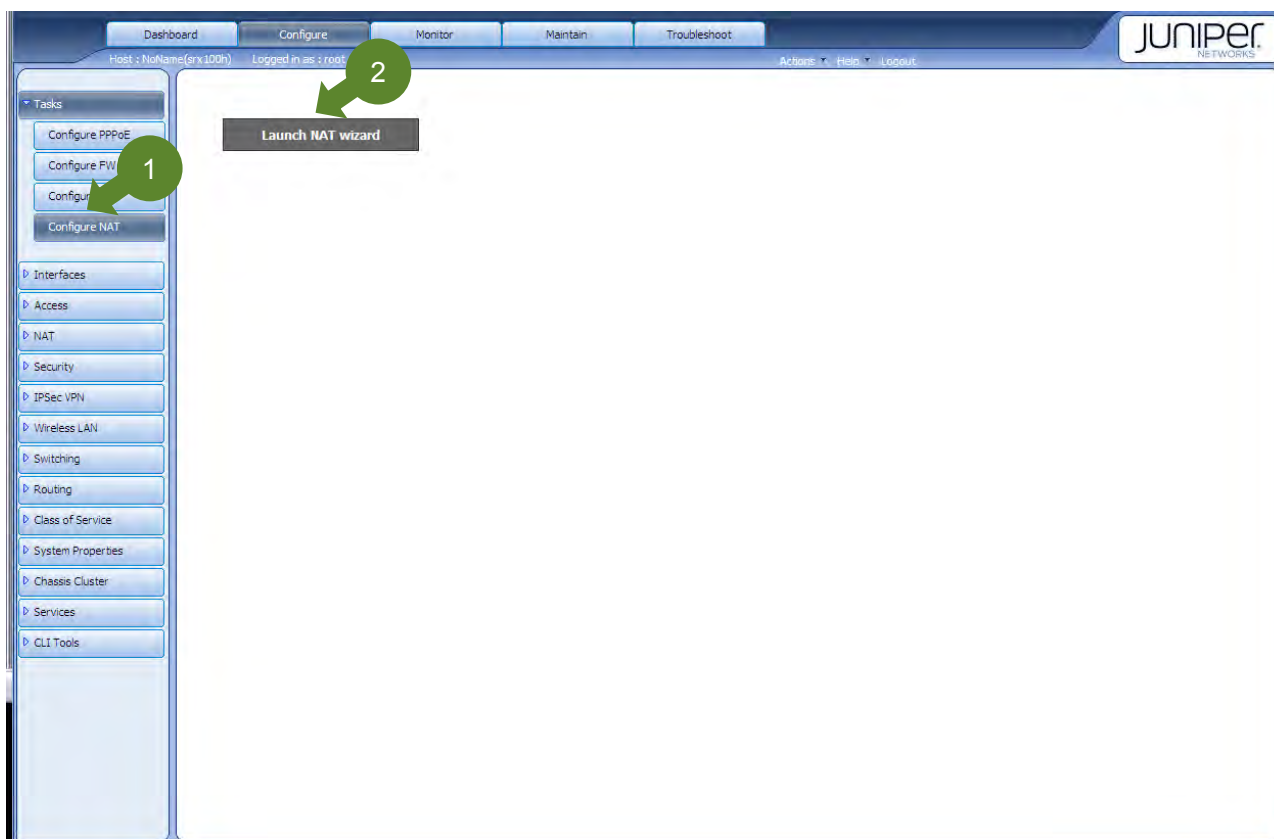
Trust zone(192.168.0.0/24)から、Untrust Zone(インターネット)へ抜ける通信に関しては、アドレスプール(100.0.0.1-100.0.0.10)を利用し、Source NATにて、通信をする。



Source NAT設定 (1/12)

NATの設定は、「NAT Wizard」を使用して簡単に作成することが可能です。

ウィザードは、Configure タブを選択し左側の項目より、「Wizards」→「NAT Wizard」から行います(①)。「Launch NAT Wizard」のリンクをクリック(②)することでウィザードが別ウィンドウで表示されます(次ページ)



Source NAT設定 (2/12)

「Source NAT」を選択し(①)、「Start」(②)からセットアップウィザードを開始します。

The screenshot shows the 'NAT Wizard' configuration window. On the left, a sidebar contains a 'Select NAT Type' section with a 'Rules' sub-section. Below this, the 'Source NAT' section is expanded, providing a description: 'The translation of the source IP address of a packet leaving the Juniper Networks device. Source NAT is used to allow hosts with private IP addresses to access a public network.' The main area, titled 'Select NAT Type', contains three radio button options: 'Source NAT' (selected), 'Destination NAT', and 'Static NAT'. Each option has a status indicator: 'Not configured.' for Source and Destination NAT, and 'Not configured.' for Static NAT. A green callout bubble with the number '1' points to the 'Source NAT' radio button. Below the options is a diagram illustrating Source NAT. It shows a 'Clients' network with 'Private Addresses' connected to a 'Gateway'. The Gateway is connected to a 'Public Network' cloud, which contains 'Servers' with 'Public Addresses'. A red arrow shows a packet originating from a client, passing through the gateway, and being translated to a public address before reaching a server. A green callout bubble with the number '2' points to the 'Start' button at the bottom right of the wizard. The 'Exit Wizard' button is also visible.

Source NAT設定 (3/12)

「Add」ボタン(①)を押し、Source NATを新規作成します。

The screenshot shows the 'NAT Wizard' interface. On the left, there is a sidebar with a 'Rules' link and an 'About this page' section. The main area is titled 'Source NAT Rules' and contains an 'Add' button, 'Edit', 'Clone', and 'Delete' buttons. Below these buttons is a table with columns for 'Name', 'Match Source', 'Match Destination', and 'NAT To'. The table currently displays 'No rules found.' A green circle with the number '1' and an arrow points to the 'Add' button. At the bottom right of the main area is a 'Back' button.

About this page
NAT processing centers on the evaluation of NAT rules.
A rule specifies a general set of matching conditions for traffic and the action to be taken when traffic matches the rule.
On this page, click a context heading to collapse or expand the list of related rules.

Source NAT
One-to-one translation of internal private IP addresses to the public IP address of the public interface (WAN).

Public Network (Internet)
The IP address of the public interface is a single public IP address that the network administrator

Source NAT設定 (4/12)

Source NATのルール名①を入力します。Source NATを適用するゾーン②を指定します。すでに設定されているゾーンの中から送信元ゾーン③を選択し、「>>」ボタン④にて決定します。同様に、送信先ゾーンを選択し、「>>」ボタン⑤にて決定します。

NAT Wizard

✓ Select NAT Type
➔ Rules

Source NAT: Add/Edit Rule * All fields are required

Name

Rule Name ¹

Traffic Direction

From ²

To ³

Matching Addresses and Ports

Source Address ⁴

Back Next

Source NAT設定 (5/12)

Source NATを適用させる送信元アドレス①を入力し、「Add」ボタン②にて決定します。同様に、送信先アドレスを入力し、「Add」ボタン③にて決定します。送信先ポート④を入力します。NATルールアクションにアドレスプール(Address Range)⑤を選択します。アドレスプールを使用する場合には、使うアドレスプールを設定するため、「Edit」ボタン⑥を押します。

NAT Wizard

✔ Select NAT Type
➔ Rules

To **
Zone [v]
trust [] >> untrust []
<< []

Matching Addresses and Ports

Source Address **
IP/Subnet (i.e. 1.2.3.0/24) [Add] ①
192.168.0.0/24 [Remove] ②

Destination Address **
[Add] ③
0.0.0.0/0 [Remove]

Destination port range **
1 [] to 60000 [] ④

Rule Action

NAT To **
Address Range [v] ⑤ [Edit] ⑥

Back Next

About this page
Source NAT rules specify two layers of match conditions: traffic direction and packet information.
Traffic direction allows you to specify combinations of from zone or from interface, and to zone or to interface. You cannot configure the same from and to contexts for different rules.

Publicly Externally (external)
The IP addresses of the agents attached to it should only be used for the external connectivity.

① ポイント: 指定するアドレスが、Any(すべて)であれば、0.0.0.0/0と入力します。

② ポイント: Destination port rangeが未入力の場合は、自動的に、「1 to 60000」が適用されます。

Source NAT設定 (6/12)

アドレスプールで使用するアドレス①を入力し、「Add」ボタン②で決定します。設定したアドレスレンジを用いて、ポートトランスレーションのオプション③を選択します。「Done」ボタン④を押します。

The screenshot shows the NAT Wizard configuration interface. A dialog box titled "Address Range" is open in the foreground. The dialog has a blue header with the title. Below the header, there is a text input field labeled "Addresses *" containing the range "100.0.0.1-100.0.0.10". To the right of this field are two buttons: "Add" and "Remove". Below the "Addresses" field, there is a "Port" section with three radio button options: "Default (1024-63487)", "No Translation", and "Translation". The "Default" option is selected. At the bottom of the dialog are "Cancel" and "Done" buttons. Green callout circles with numbers 1 through 4 point to the "Addresses" input field, the "Add" button, the "Default" radio button, and the "Done" button respectively. In the background, the NAT Wizard interface is visible, showing a "To" field with a "Zone" dropdown menu set to "trust", and a "Rule Action" section with a dropdown menu set to "Address Range".

ポイント: 100.0.0.1から100.0.0.10までを、NATで使いたい場合には、「100.0.0.1-100.0.0.10」と入力します。

Source NAT設定 (7/12)

アドレスプールを設定したら、「Next」ボタン(①)を押します。

NAT Wizard

✔ Select NAT Type
➔ Rules

About this page
Source NAT rules specify two layers of match conditions: traffic direction and packet information.
Traffic direction allows you to specify combinations of from zone or from interface, and to zone or to interface. You cannot configure the same from and to contexts for different rules.

To *
Zone: untrust

Matching Addresses and Ports

Source Address **
IP/Subnet (i.e. 1.2.3.0/24)
192.168.0.0/24

Destination Address **
0.0.0.0/0

Destination port range **
1 to 60000

Rule Action

NAT To **
Address Range

Back Next

Source NAT設定 (8/12)

設定内容を確認し、問題が無ければ、「Commit」ボタン(①)をクリックします。

The screenshot displays the 'NAT Wizard' interface. On the left, a sidebar shows 'Select NAT Type' with a checkmark and 'Rules' with a right-pointing arrow. Below this is an 'About this page' section with explanatory text and a diagram of Source NAT. The main area is titled 'Source NAT: Rules' and contains buttons for 'Add', 'Edit', 'Clone', and 'Delete'. A table lists the configured rule:

Name	Match Source	Match Destination	NAT To
From: Zone trust To: Zone untrust			
src-nat1	192.168.0.0/24	0.0.0.0/0	100.0.0.1-10...

At the bottom right, there are 'Back' and 'Commit' buttons. A green circle with the number '1' and an arrow points to the 'Commit' button.

Source NAT設定 (9/12)

Commitプロセスが行われます。問題が無ければ、「OK」ボタン①をクリックして、Wizardを終了します。

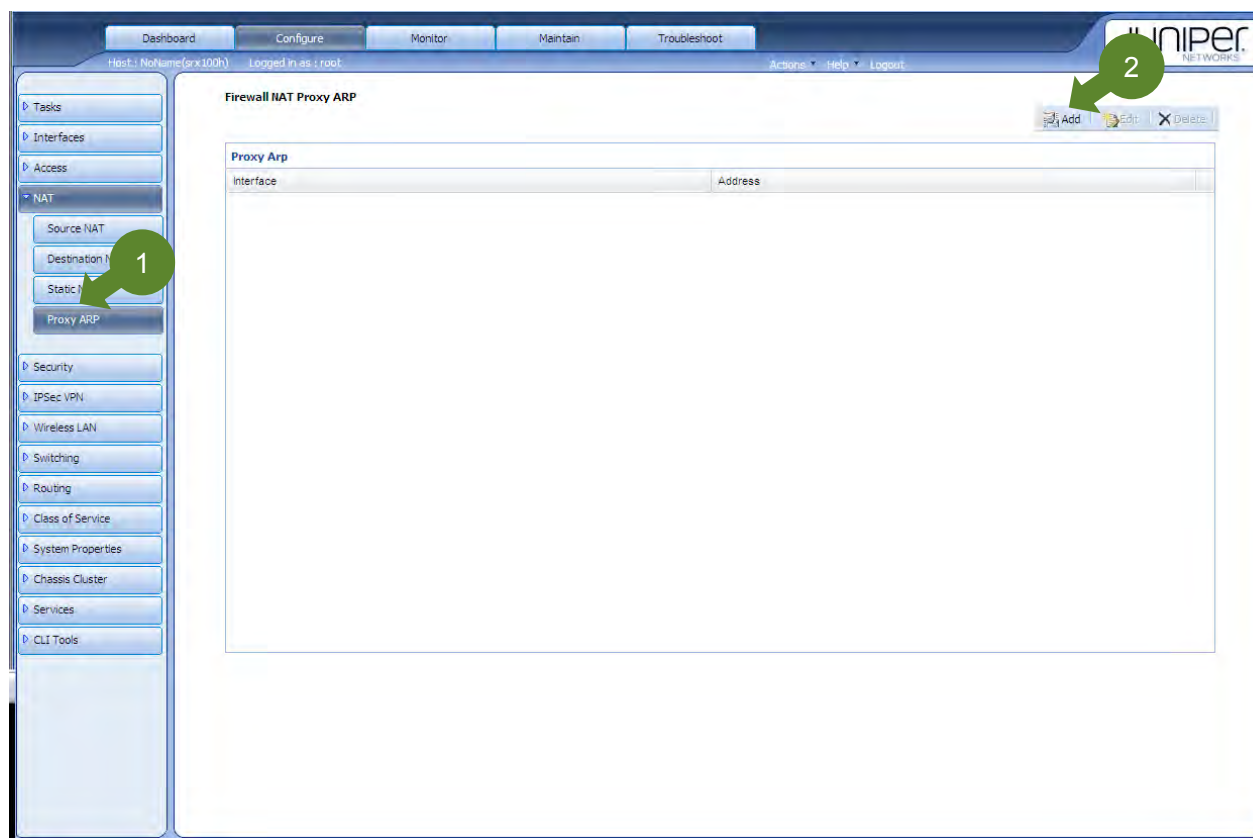
The screenshot shows the NAT Wizard interface. On the left, there is a sidebar with 'Select NAT Type' and 'Rules' options. The main area is titled 'Source NAT: Rules' and contains a table with columns: Name, Match Source, Match Destination, and NAT To. A row is visible with Name 'src-nat1', Match Source '192.168.0.0/24', Match Destination '0.0.0.0/0', and NAT To '100.0.0.1-10...'. Below the table, a 'Configuration Delivery' dialog box is open, displaying 'Configuration Delivery status : Success' and buttons for 'OK' and 'Details >>'. A green circle with the number '1' points to the 'OK' button. A 'Back' button is located at the bottom right of the wizard window.

Name	Match Source	Match Destination	NAT To
src-nat1	192.168.0.0/24	0.0.0.0/0	100.0.0.1-10...

Source NAT設定 (10/12)

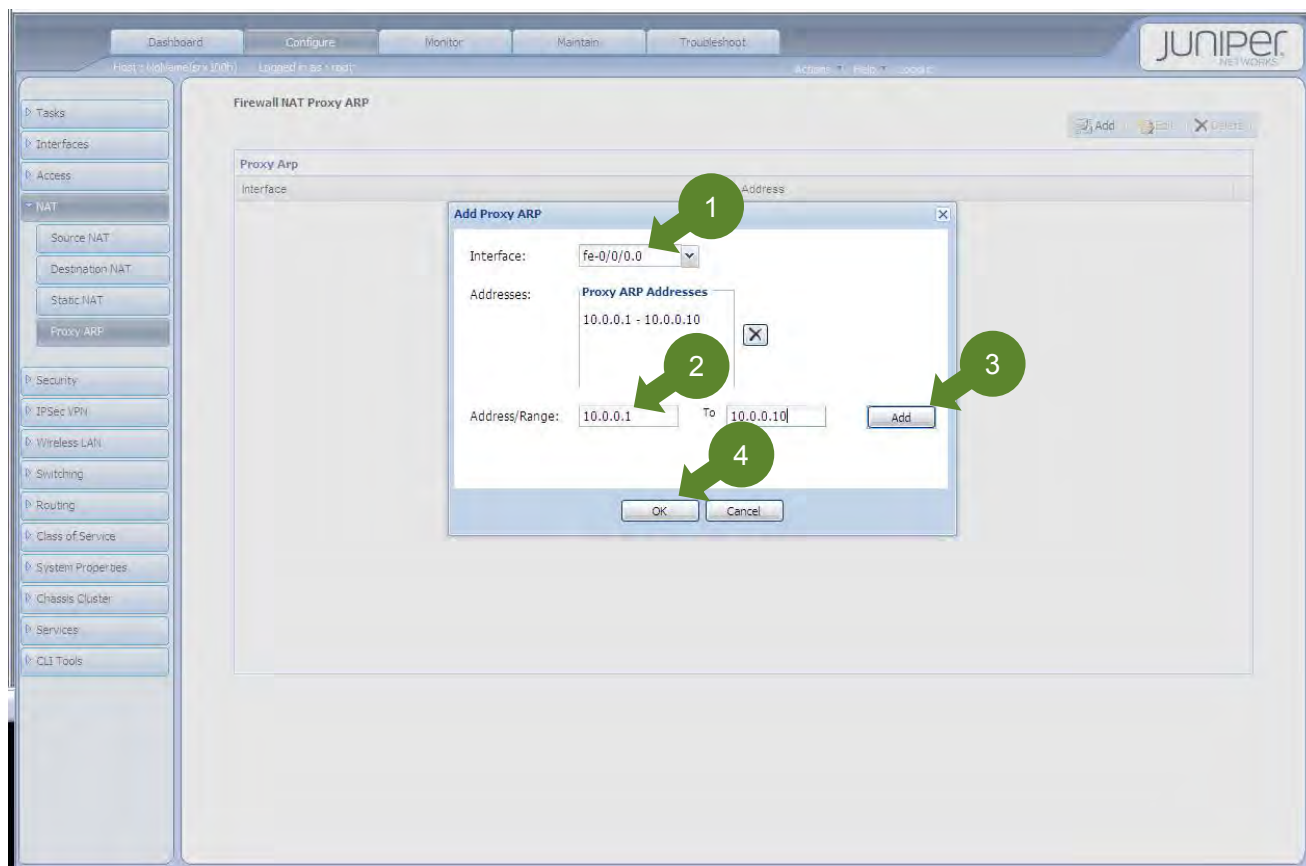
アドレスプールは、実在しないアドレスのため、Proxy ARPの設定が必要になります。

Configure タブを選択し左側の項目より、「NAT」→「Proxy Arp」から行います(①)。
「Add」ボタン②を押し、Proxy ARPの新規作成を行います。(次ページ)



Source NAT設定 (11/12)

Proxy ARPを、送出するインターフェース①を選択します。 Proxy ARPを適用するアドレス②を入力します。入力後、「Add」ボタン③を押します。設定を終えたら、「OK」ボタン④を押します。



Source NAT設定 (12/12)

Proxy ARPの設定を終えたら、「Commit」ボタン①をクリックして終了です。

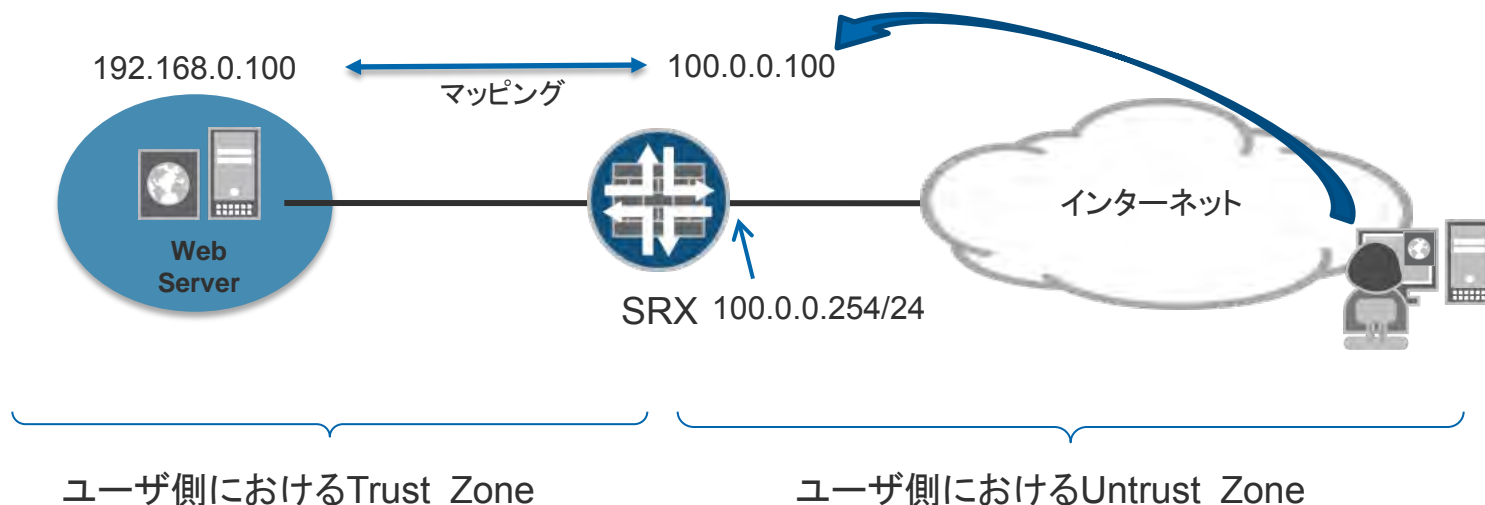
The screenshot shows the Juniper Networks configuration interface. The top navigation bar includes 'Dashboard', 'Configure', 'Monitor', 'Maintain', and 'Troubleshoot'. The user is logged in as 'root' on a host named 'srv100h'. The left sidebar shows a tree view with categories like 'Tasks', 'Interfaces', 'Access', 'NAT', 'Security', 'IPSec VPN', 'Wireless LAN', 'Switching', 'Routing', 'Class of Service', 'System Properties', 'Chassis Cluster', 'Services', and 'CLI Tools'. The 'NAT' category is expanded, showing 'Source NAT', 'Destination NAT', 'Static NAT', and 'Proxy ARP'. The 'Proxy ARP' option is selected. The main content area is titled 'Firewall NAT Proxy ARP' and contains a table with the following data:

Interface	Address
fe-0/0/0.0	10.0.0.1/32 - 10.0.0.10/32

Below the table are 'Add', 'Edit', and 'Delete' buttons. A context menu is open over the 'Commit' button, with options: 'Commit', 'Compare', 'Discard', and 'Preferences'. A green circle with the number '1' points to the 'Commit' button.

Static NAT – このガイドで構築する物理・論理構成

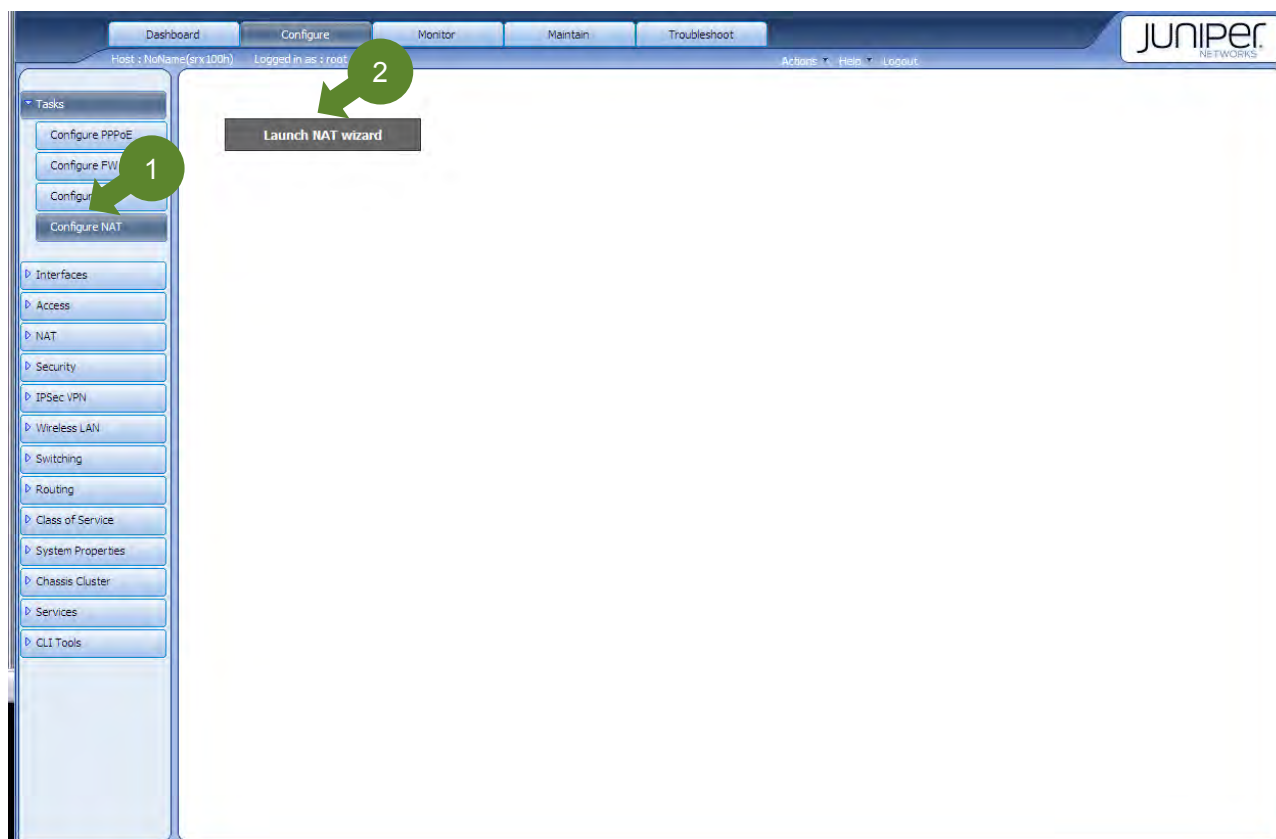
Untrust Zone(インターネット)から、Trust Zoneにあるサーバ(192.168.0.100)に対して、グローバルアドレス(100.0.0.100)を利用し、Static NATにて、通信できるようにする。



Static NAT設定 (1/9)

NATの設定は、「NAT Wizard」を使用して簡単に作成することが可能です。

ウィザードは、Configure タブを選択し左側の項目より、「Wizards」→「NAT Wizard」から行います(①)。「Launch NAT Wizard」のリンクをクリック(②)することでウィザードが別ウィンドウで表示されます(次ページ)



Static NAT設定 (2/9)

「Static NAT」を選択し(①)、「Start」(②)からセットアップウィザードを開始します。

NAT Wizard

➔ Select NAT Type
Rules

Select NAT Type

Select the type of NAT you wish to configure, and then click Start. You may also make changes to existing configurations.

- Source NAT Not configured.
- Destination NAT Not configured.
- Static NAT** Not configured.

Static NAT
Packets from/to the private network are translated to addresses in the public network address space. A one-to-one address mapping is mandatory.

Public Network interface(s)
Subnets belonging to the public network address space routed to the gateway and mapped to addresses in the private network

Exit Wizard **Start**

About this page
Network Address Translation (NAT) is a method for modifying or translating network address information in packet headers. Either one or both of the source and destination addresses in a packet may be translated. NAT can also include the translation of port numbers.

The NAT type determines the order in which NAT rules are processed. During the first packet processing for a flow, NAT rules are applied in the following order: 1. Static NAT rules. 2. Destination NAT rules. 3. Route lookup. 4. Security policy lookup. 5. Reverse mapping of static NAT rules. 6. Source NAT rules.

Static NAT設定 (3/9)

「Add」ボタン(①)を押し、Static NATを新規作成します。

The screenshot shows the 'NAT Wizard' interface. On the left, there is a sidebar with 'Select NAT Type' (checked) and 'Rules'. Below this is an 'About this page' section explaining NAT processing and rule specifications. At the bottom left is a diagram of a network topology with a 'Public Network' cloud and a 'Gateway' device. The main area is titled 'Static NAT Rules' and contains buttons for 'Add', 'Edit', 'Clone', and 'Delete'. A green circle with the number '1' is placed over the 'Add' button. Below the buttons is a table with columns 'Name' and 'Match Destination', currently displaying 'No rules found'. A 'Back' button is located at the bottom right of the main area.

Static NAT設定 (4/9)

Static NATのルール名①を入力します。Static NATを適用するゾーン②を指定します。すでに設定されているゾーンの中から送信元ゾーン③を選択し、「>>」ボタン④にて決定します。送信先アドレス(マッピングさせたいグローバルアドレス)⑤を入力し、Rule Actionに、グローバルアドレスにマッピングさせたいホストのアドレス⑥を入力し、「Next」ボタン⑦を押します。

NAT Wizard

✓ Select NAT Type
⇒ Rules

Static NAT: Add/Edit Rule * All fields are required

Name

Rule Name ^{**}: static-nat-1

Traffic Direction

From ^{**}: Zone

trust >> untrust <<

Matching Addresses

Destination Address ^{**}: 100.0.0.100

Rule Action

NAT To ^{**}: 192.168.0.100

Back Next

About this page
Static NAT rules specify two layers of match conditions: traffic direction and packet information. Traffic direction allows you to specify from zone or from interface. The packet information is a destination IP address.

Static NAT
Provides specific flow control and security implementation to addresses in the public network address space. A conventional static NAT maps a 1:1 relationship.

Public Address only - Internet Access
Customer's originating for the public network address space created by the address and mapped to a connection to the public network.

Static NAT設定 (5/9)

設定内容を確認し、問題が無ければ、「Commit」ボタン(①)をクリックします。

The screenshot shows the 'NAT Wizard' interface. On the left, a sidebar indicates the current step is 'Rules' (marked with a green arrow) under 'Select NAT Type'. Below this is an 'About this page' section explaining NAT processing and rule evaluation. At the bottom left is a network diagram showing traffic flow through a gateway to a public network.

The main area is titled 'Static NAT: Rules' and contains a table of rules. The table has columns for 'Name', 'Match Destination', and 'NAT To'. A rule named 'static-nat-1' is shown with a match destination of '100.0.0.100' and a NAT to address of '192.168.0.100'. The rule is associated with the 'From: Zone untrust' zone. Buttons for 'Add', 'Edit', 'Clone', and 'Delete' are located above the table.

At the bottom right of the interface, there are 'Back' and 'Commit' buttons. A green circle with the number '1' and an arrow points to the 'Commit' button, indicating the final step of the configuration process.

Name	Match Destination	NAT To
From: Zone untrust		
static-nat-1	100.0.0.100	192.168.0.100

Static NAT設定 (6/9)

Commitプロセスが行われます。問題が無ければ、「OK」ボタン①をクリックして、Wizardを終了します。

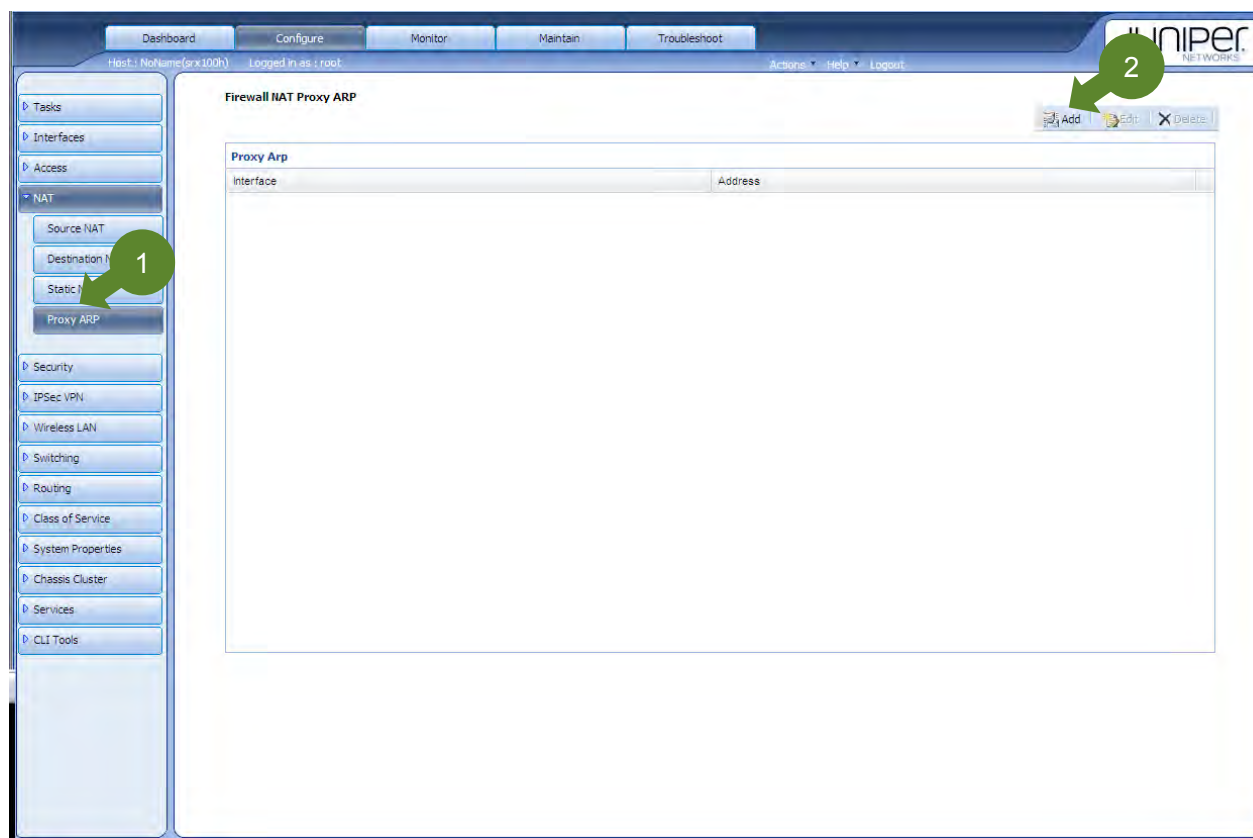
The screenshot shows the 'NAT Wizard' interface. On the left, there are navigation options: 'Select NAT Type' and 'Rules'. Below this is an 'About this page' section with explanatory text and a network diagram. The main area is titled 'Static NAT: Rules' and contains a table with columns for 'Name', 'Match Destination', and 'NAT To'. A single rule is listed: 'static-nat-1' with 'Match Destination' '100.0.0.100' and 'NAT To' '192.168.0.100'. A 'Configuration Delivery' dialog box is open in the foreground, showing a success message and an 'OK' button. A green circle with the number '1' points to the 'OK' button. A 'Back' button is visible at the bottom right of the wizard window.

Name	Match Destination	NAT To
static-nat-1	100.0.0.100	192.168.0.100

Static NAT設定 (7/9)

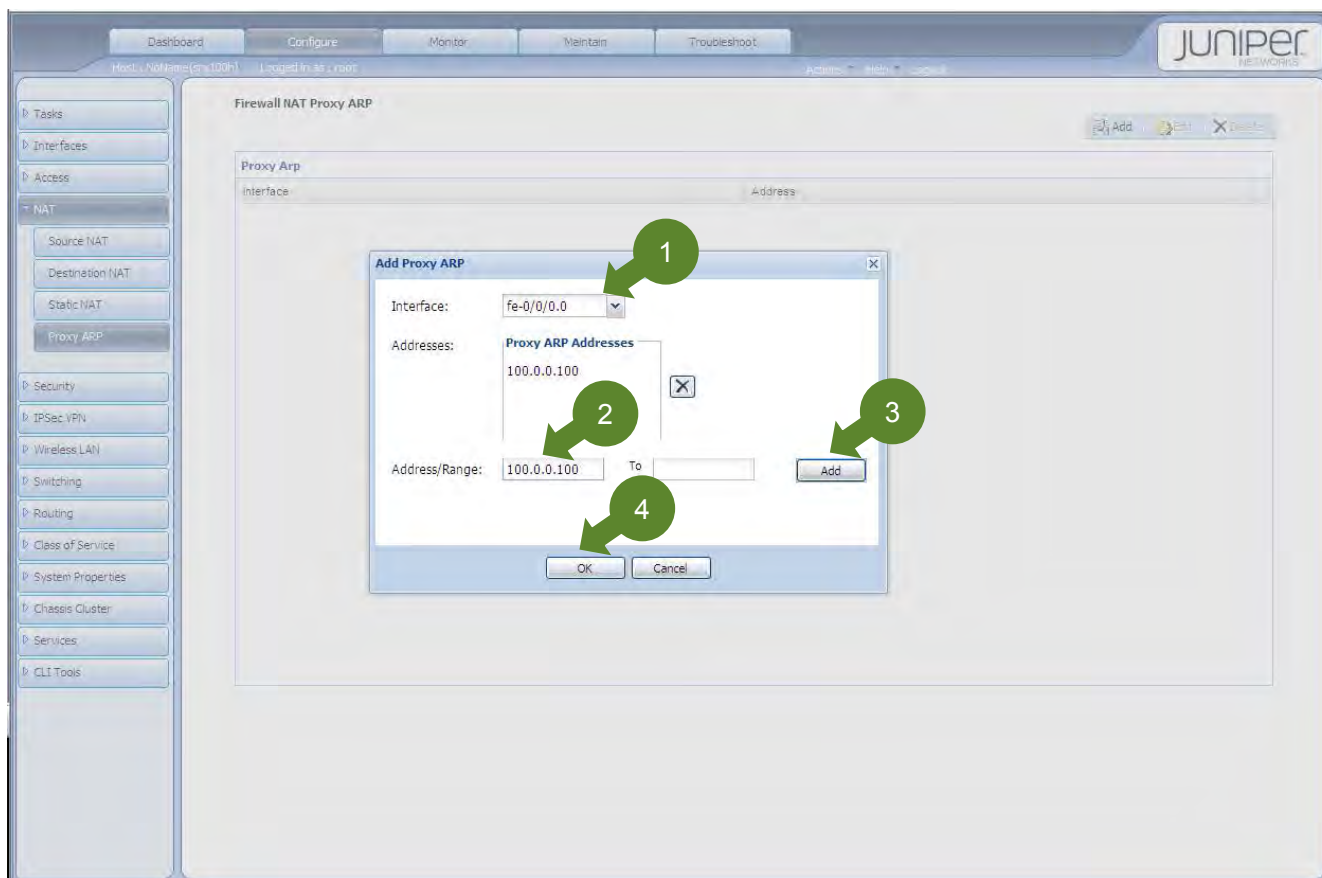
アドレスプールは、実在しないアドレスのため、Proxy ARPの設定が必要になります。

Configure タブを選択し左側の項目より、「NAT」→「Proxy ARP」から行います(①)。
「Add」ボタン②を押し、Proxy ARPの新規作成を行います。(次ページ)



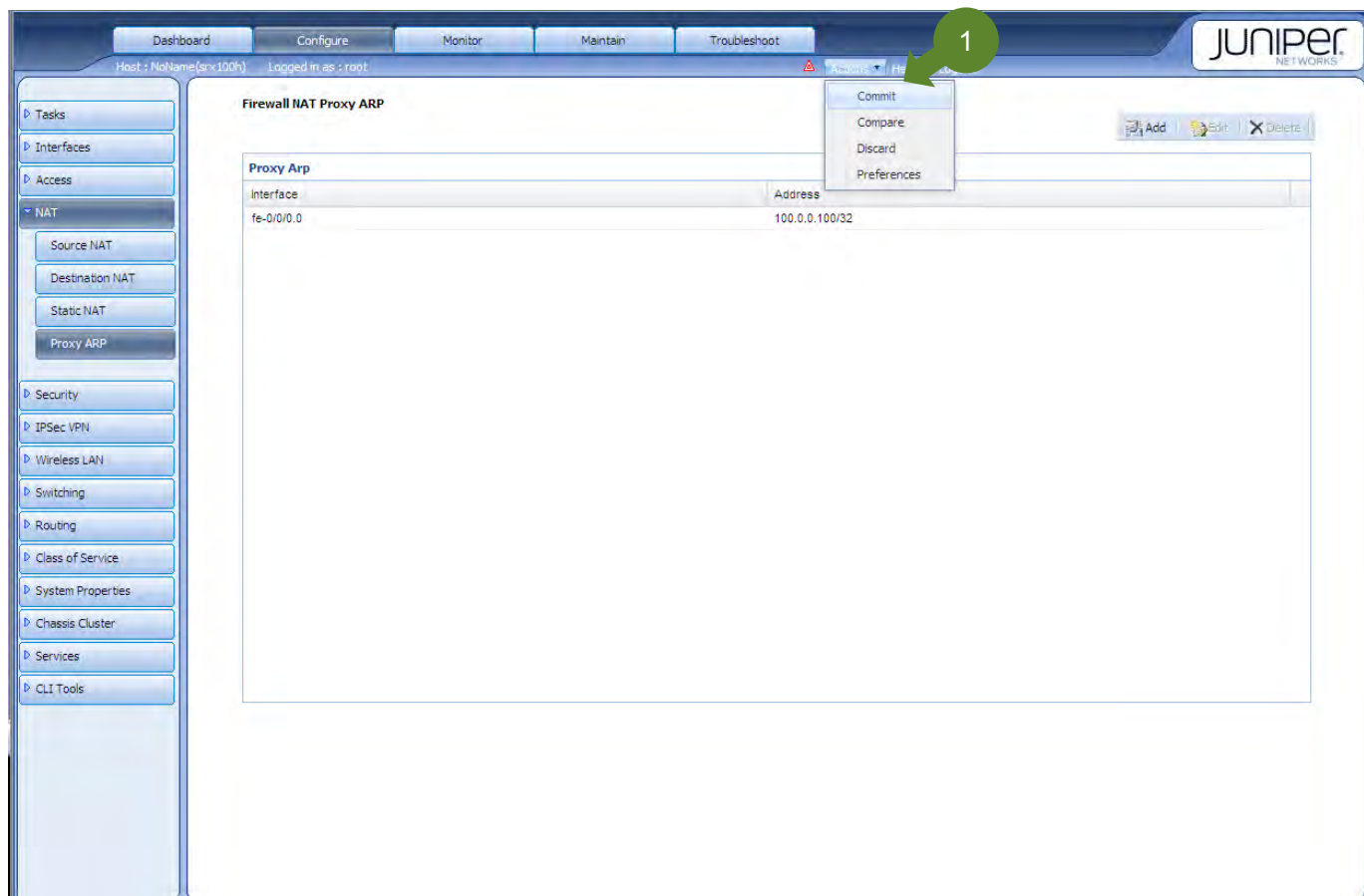
Static NAT設定 (8/9)

Proxy ARPを、送出するインターフェース①を選択します。 Proxy ARPを適用するアドレス②を入力します。入力後、「Add」ボタン③を押します。設定を終えたら、「OK」ボタン④を押します。



Source NAT設定 (9/9)

Proxy ARPの設定を終えたら、「Commit」ボタン①をクリックして終了です。



Chapter4. VPN

- Site-to-Site VPN
- リモートアクセスVPN

Site-to-Site VPN – このガイドで構築する物理・論理構成

センター側

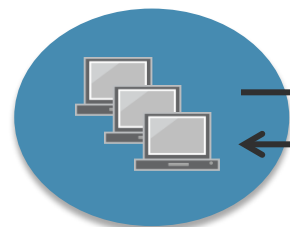


拠点側



センター側のTrust Zone

センター側におけるUntrust Zone



192.168.1.0/24



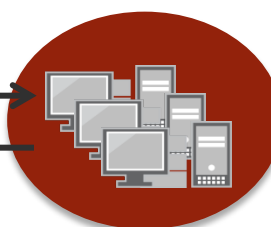
SRX 10.0.1.1



インターネット



10.0.2.1 SRX



192.168.2.0/24

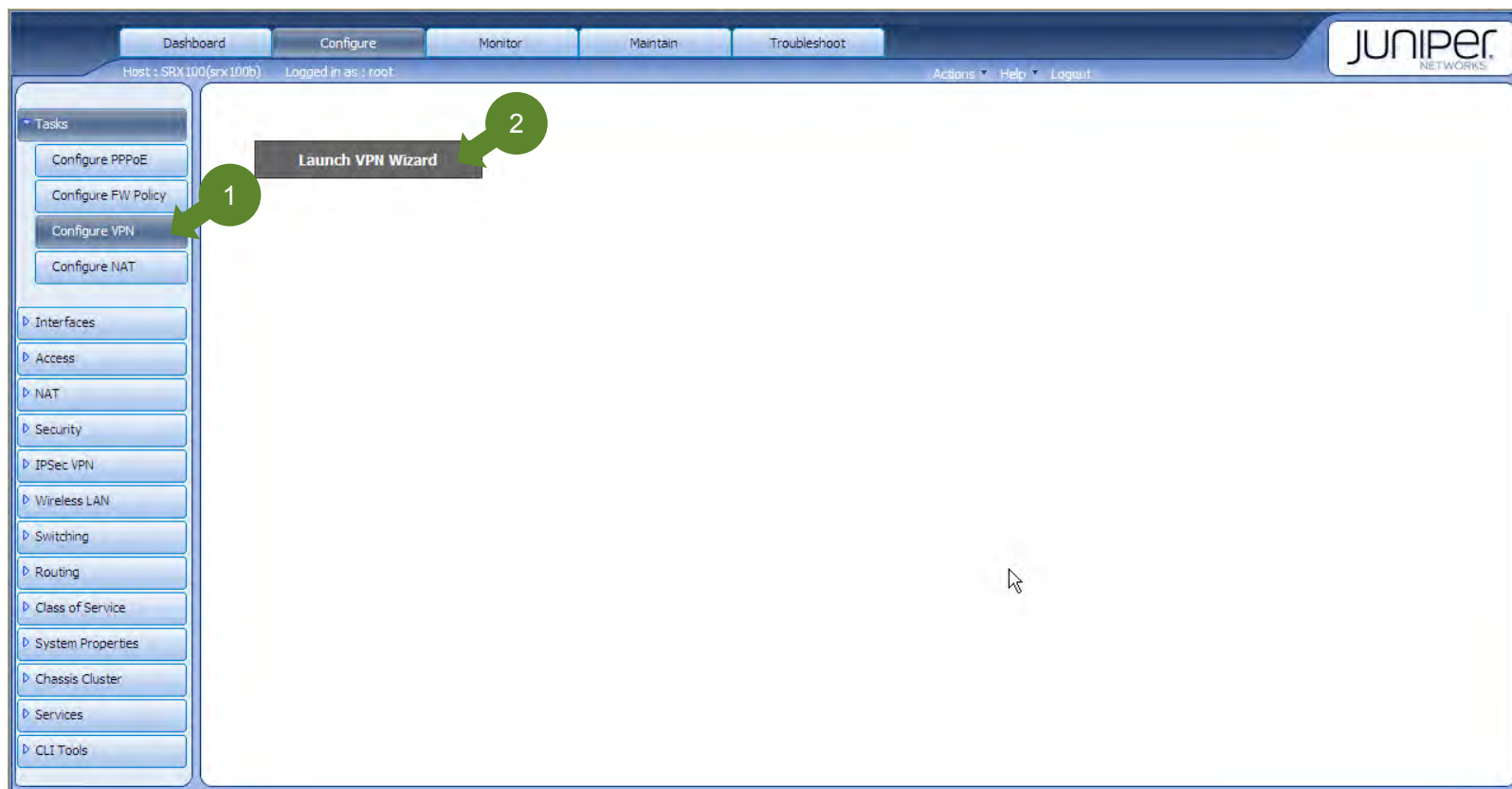
拠点側におけるUntrust Zone

拠点側のTrust Zone

Site-to-Site VPN設定 (1/9)

VPNの設定は、「VPN Wizard」を使用して簡単に作成することが可能です。

ウィザードは、Configure タブを選択し左側の項目より、「Tasks」→「Configure VPN」から行います(①)。「Launch VPN Wizard」のリンクをクリック(②)することでウィザードが別ウィンドウで表示されます(次ページ)



Site-to-Site VPN設定 (2/9)

「Site-to-site VPN (Route based)」を選択し(①)、「Start」(②)からセットアップウィザードを開始します。

VPN Wizard

→ **Select VPN Type**

- Local
- Remote
- VPN
- Remote Users
- Traffic Profile
- Review & Commit

About this page

A virtual private network (VPN) provides a means for secure communication among remote computers across a public WAN such as the Internet.

This wizard leads you through the basic required steps to configure basic settings for a site-to-site (route-based) VPN or Remote access VPN. To configure a VPN with a complete set of options, use either the J-Web interface or the command-line interface (CLI).

Refer to this section of each page for information about the page and its contents.

Resources

[JUNOS Software Security Configuration](#)

Select VPN Type

Select the type of VPN you wish to configure, and then click Start. You may also make changes to existing configurations.

Site-to-site VPN (Route based) ①

Remote Access VPN

Site-to-Site VPN

Branch 172.16.1.0/2

HeadQuarters 192.168.1/24

Branch

HQ

Internet

Exit Wizard Start ②

Site-to-Site VPN設定 (3/9)

VPNポリシー名(①)、ローカル拠点の暗号化対象とするネットワークゾーン(②)とアドレス(③)、暗号化トンネルインタフェースの論理番号(④)、所属ゾーン(⑤)、Interface type(⑥)、および外部ネットワークと接続しているInterface(⑦)とタイプ(⑧)を指定し、「Next」(⑨)を押します。

VPN Wizard

✓ Select VPN Type
➔ Local
Remote
VPN
Traffic Profile
Review & Commit

About this page
This page identifies the outgoing interface for a site-to-site VPN. On this page you specify the local private network, the secure tunnel interface, and the public network through which the tunnel passes. On the next page you specify the remote site private network.
Click a field name to get information about the field.

Site-to-site VPN: Local Settings * All fields are required

Name
VPN Name * s2svpn ①

Local Private Network
Zone * trust ②
Network(s) * 192.168.1.0/24 ③
Add Example: 1.2.3.0/24
Remove

Secure Tunnel Interface
Interface * ST0.0 ④
Interface Zone * untrust ⑤
Interface type * Unnumbered ⑥ Numbered

Public Network
Interface * ge-0/0/0.0 ⑦
Interface Zone * untrust
Interface type * Static ⑧ Dynamic (DHCP)

Back Next ⑨

ポイント: 暗号化トンネルの論理番号(④)は、機器内で重複していない番号を、所属ゾーン(⑤)は外部ネットワークのインタフェース(⑦)と同じゾーンを選択します。


Site-to-Site VPN設定 (4/9)

VPN対向拠点機器のグローバルIPアドレス(①)、暗号化通信を行う対向拠点のネットワークアドレス(②)を指定し、「Next」(③)を押します。

VPN Wizard

- ✓ Select VPN Type
- ✓ Local
- ➔ **Remote**
- VPN
- Traffic Profile
- Review & Commit

About this page
This page specifies the remote site to which the local site is connected by the VPN tunnel. Click a field name to get information about the field.



Site-to-site VPN: Remote Settings ** All fields are required*

Remote Site

Remote Gateway Public IP * Example: 1.2.3.4 (①)

Remote Private Network(s) * Add (②) Remove

Back Next (③)

Site-to-Site VPN設定 (5/9)

暗号化トンネルのセキュリティ強度を選択(①)、事前共有鍵を設定し(②)、「Next」(③)を押します。

VPN Wizard

- ✔ Select VPN Type
- ✔ Local
- ✔ Remote
- ➔ **VPN**
 - Traffic Profile
 - Review & Commit

About this page
IKE IPsec tunnel negotiation occurs in two phases. In Phase 1, participants establish a secure channel in which to negotiate the IPsec security association (SA). In Phase 2, participants negotiate the IPsec SA for authenticating traffic that will flow through the tunnel.
Use this page to configure these handshake settings. The

Site-to-site VPN: VPN Settings * Required

VPN Settings

IKE settings

IKE Security Level * Basic (group1, des, sha1) Compatible (group2, 3des, sha1) Standard (group2, aes128, sha1)

IKE Mode * Main Aggressive

IKE Preshared Key (ASCII) *

IPsec settings

IPsec Security Level * Basic (esp, des, sha1) Compatible (esp, 3des, sha1) Standard (esp, aes128, sha1)

IPsec Perfect Forward Secrecy * group1 group2 group5

VPN Monitor

Dead Peer Detection

Back Next

ポイント: IKE Modeは、対向機器のIPアドレスが既知の場合はMainを、そうでない場合はAggressiveを選択します。

Site-to-Site VPN設定 (6/9)

暗号化対象となる通信を 指定(①)し、「Next」(②)を押します。

The screenshot shows the 'VPN Wizard' interface. On the left, a sidebar contains a progress list: 'Select VPN Type' (checked), 'Local' (checked), 'Remote' (checked), and 'VPN' (checked). Below this is the 'Traffic Profile' section, which is currently selected and includes a 'Review & Commit' link. An 'About this page' section explains that profiles identify applications passing through the VPN tunnel. At the bottom left, a diagram shows two VPN endpoints connected to an 'Internet' cloud. The main area is titled 'Site-to-site VPN: Traffic Profiles' and contains two sections: 'VPN Traffic Profiles' and 'Public to Private (Incoming)'. Both sections have a checked checkbox and an 'Application(s)' list. The 'Private to Public (Outgoing)' section has a green arrow labeled '1' pointing to its 'Application(s)' list, which contains 'any'. The 'Public to Private (Incoming)' section also has a 'Public to Private (Incoming)' checkbox checked and an 'Application(s)' list containing 'any'. At the bottom right, there are 'Back' and 'Next' buttons, with a green arrow labeled '2' pointing to the 'Next' button.

Site-to-Site VPN設定 (7/9)

設定内容を確認し、問題が無ければ、「Commit」ボタン(①)をクリックします。

VPN Wizard

- ✔ Select VPN Type
- ✔ Local
- ✔ Remote
- ✔ VPN
- ✔ Traffic Profile
- ➔ **Review & Commit**

About this page
When you edit a configuration, the changes you make do not take effect until you commit them. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file.
This page shows the information you have entered and any

VPN Name s2svpn

Local settings

Local Zone	trust
Local Networks	192.168.1.0/24
Secure tunnel interface	st.0
Secure tunnel interface zone	untrust
Secure tunnel interface type	Unnumbered
Public tunnel interface	ge-0/0/0.0
Public tunnel interface zone	untrust
Public tunnel interface type	Static

Remote settings

Remote gateway IP	10.0.2.1
Remote private networks	192.168.2.0/24

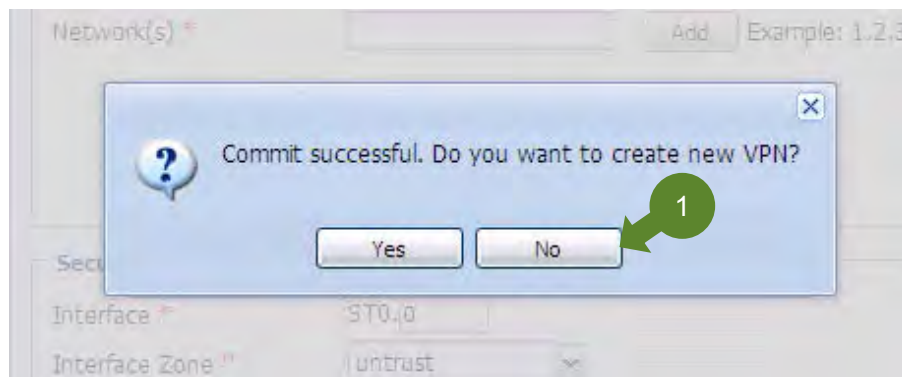
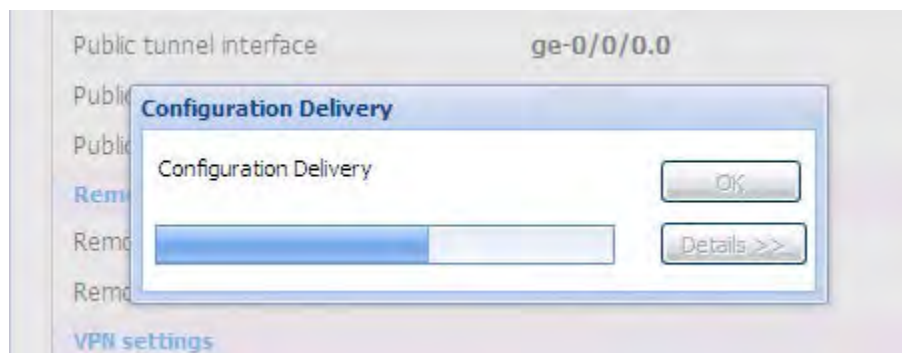
VPN settings

IKE security level	standard
IKE preshared key	juniper123
IKE mode	main
Dead Peer Detection	
IPsec Security Level	standard
IPsec Perfect Forward Secrecy	group2

Back Commit

Site-to-Site VPN設定 (8/9)

Commitプロセスが行われます。問題が無ければ、続けてVPNを設定するかどうかの確認画面が表示されますので、「No」をクリックして、Wizardを終了します。



Site-to-Site VPN設定 (9/9)

対向拠点側の暗号化対象ネットワークアドレス設定は、ローカル拠点の機器で設定したアドレスと対称となるようにします。

The screenshot shows the 'VPN Wizard' configuration interface. On the left, a sidebar contains a progress list with 'Review & Commit' selected, and a diagram of two sites connected via the Internet. The main area displays configuration fields for 'Local settings', 'Remote settings', and 'VPN settings'. The 'Local Networks' field is set to '192.168.2.0/24' and the 'Remote private networks' field is set to '192.168.1.0/24', both highlighted with green boxes. The 'Remote gateway IP' is set to '10.0.1.1'. At the bottom right, there are 'Back' and 'Commit' buttons.

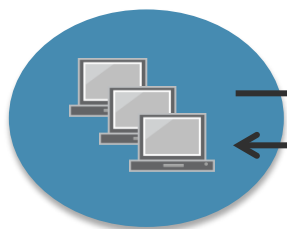
Field	Value
VPN Name	s2svpn
Local settings	
Local Zone	trust
Local Networks	192.168.2.0/24
Secure tunnel interface	st.0
Secure tunnel interface zone	untrust
Secure tunnel interface type	Unnumbered
Public tunnel interface	ge-0/0/0.0
Public tunnel interface zone	untrust
Public tunnel interface type	Static
Remote settings	
Remote gateway IP	10.0.1.1
Remote private networks	192.168.1.0/24
VPN settings	
IKE security level	standard
IKE preshared key	juniper123
IKE mode	main
Dead Peer Detection	
IPsec Security Level	standard
IPsec Perfect Forward Secrecy	group2
VPN Monitor	

リモートアクセスVPN – ネットワーク概要

センター側



Trust Zone



192.168.1.0/24

SRX



ge-0/0/0



IPプール

192.168.200.0/24

インターネット



モバイルユーザ



自宅からのアクセス

リモートアクセスVPN設定 (1/13)

「Remote Access VPN」を選択し(①)、「Start」(②)からセットアップウィザードを開始します。

VPN Wizard

→ **Select VPN Type**

- Local
- Remote
- VPN
- Remote Users
- Traffic Profile
- Review & Commit

Select VPN Type

Select the type of VPN you wish to configure, and then click Start. You may also make changes to existing configurations.

Site-to-site VPN (Route based)

Remote Access VPN

Dynamic VPN

Branch 172.16.1.0/24

Remote User

Branch

Internet

Exit Wizard Start


リモートアクセスVPN設定 (2/13)

ローカル拠点の暗号化対象とするネットワークゾーン(①)とアドレス(②)、外部ネットワークと接続しているInterface(③)を指定し、「Next」(④)を押します。

VPN Wizard

- Select VPN Type
- ➔ Local
- VPN
- Remote Users
- Review & Commit

About this page
On this page you specify the local private network and the public network through which the tunnel passes. The name of the remote access VPN is preset.
If you have previously configured a remote access VPN, you can use this page to edit the existing remote access VPN or click the button at the



Remote Access VPN: Local Settings * All fields are required

Name
VPN Name * wizard_dyn_vpn

Protected Networks

Zone * trust ①

Network(s) * ②
Add example: 1.2.3.0/24
192.168.1.0/24
Remove

Public Network

Interface * ge-0/0/0.0 ③
Interface Zone * untrust

Back Next ④

リモートアクセスVPN設定 (3/13)

暗号化トンネルのセキュリティ強度を選択(①)し、事前共有鍵(②)およびRemote Identity(③)を設定し、「Next」(④)を押します。

VPN Wizard

- ✓ Select VPN Type
- ✓ Local
- ➔ **VPN**
- Remote Users
- Review & Commit

About this page
IKE IPsec tunnel negotiation occurs in two phases. In Phase 1, participants establish a secure channel in which to negotiate the IPsec security association (SA). In Phase 2, participants negotiate the IPsec SA for authenticating traffic that will flow through the tunnel.
Use this page to configure these handshake settings. The

Remote Access VPN: VPN Settings * Required

VPN Settings

IKE Security Level *
 Basic (group1, des, sha1) ①
 Compatible (group2, 3des, sha1)
 Standard (group2, aes128, sha1) ②

IKE Preshared Key (ASCII) *
 ③

Remote Identity *
 ③

Dead Peer Detection

IPsec Security Level *
 Basic (esp, des, sha1)
 Compatible (esp, 3des, sha1)
 Standard (esp, aes128, sha1) ①

IPsec Perfect Forward Secrecy * group1 group2 group5

Back Next ④

リモートアクセスVPN設定 (4/13)

リモートアクセスを行うユーザ名・パスワードを登録(①)します。また内部ルーティングのために、リモートアクセスクライアントに割り当てるプールアドレス(②)、DNSサーバ(③)、WINSサーバアドレス(④)を指定します。最後に「Next」(⑤)を押します。

VPN Wizard

- ✔ Select VPN Type
- ✔ Local
- ✔ VPN
- ➔ Remote Users
- Review & Commit

About this page
Describe the settings for the remote user of the remote access VPN. Click a field name to get information about the field.

Remote Access VPN: Remote User Settings * Required

Authentication
Same credentials used for Xauth and authentication for client download.
At least one user must be created.

User Name	Password
user1	●●●●●●
user2	●●●●●●
user3	●●●●●●
user4	●●●●●●

▼ Add More...

IP Settings

IP Pool (for Config Mode) * 192.168.200.1/24 IP pool settings are shared by multiple VPN's

DNS Server 192.168.1.10

WINS Server 192.168.1.10

Poolアドレスの最初と最後のアドレスを指定したい場合、およびセカンダリーのDNS/Winsサーバアドレス指定は、後から別メニューで行います。(後述のオプション参照)

Back Next

リモートアクセスVPN設定 (5/13)

設定内容を確認し、問題が無ければ、「Commit」ボタン(①)をクリックします。

VPN Wizard

- ✔ Select VPN Type
- ✔ Local
- ✔ VPN
- ✔ Remote Users
- ➔ Review & Commit

About this page
When you edit a configuration, the changes you make do not take effect until you commit them. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file.
This page shows the information you have entered and any

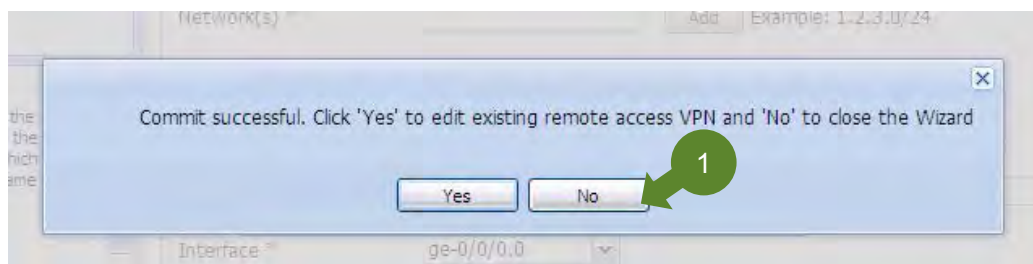
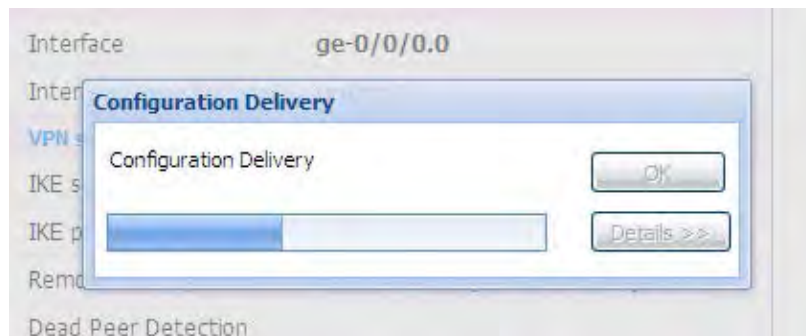
Remote Access VPN Configuration

VPN Name	
VPN Name	wizard_dyn_vpn
Protected Networks	
Zone	trust
Networks	192.168.1.0/24
Public Network	
Interface	ge-0/0/0.0
Interface zone	untrust
VPN settings	
IKE security level	standard
IKE preshared key	juniper123
Remote identity	Host name: vpnuser@example.com
Dead Peer Detection	
IPsec Security Level	standard
IPsec Perfect Forward Secrecy	group2
Remote user IP settings	
IP pool range/IP	192.168.200.1/24
DNS server	192.168.1.10
WINS server	192.168.1.10

Back Commit

リモートアクセスVPN設定 (6/13)

Commitプロセスが行われます。問題が無ければ、続けてVPNを設定するかどうかの確認画面が表示されますので、「No」をクリックして、Wizardを終了します。



リモートアクセスVPN設定 (7/13)

外部からHTTPSでアクセスできるように設定を追加します。「System Properties」->「Management Access」をクリック(①)し、「Edit」ボタンをクリック(②)します。

Host : SRX100(srx100b) Logged in as : root

Actions Help Logout

Management Access Configuration

Name	Value
Management access	
Loopback address	-
HTTP enabled	true
Telnet enabled	true
JUNOScript over clear text enabled	true
Secure access	
HTTPS enabled	true
HTTPS certificate	system-generated-certificate
SSH enabled	true
JUNOScript over SSL enabled	false
JUNOScript over SSL certificate	
Certificates	

1

2

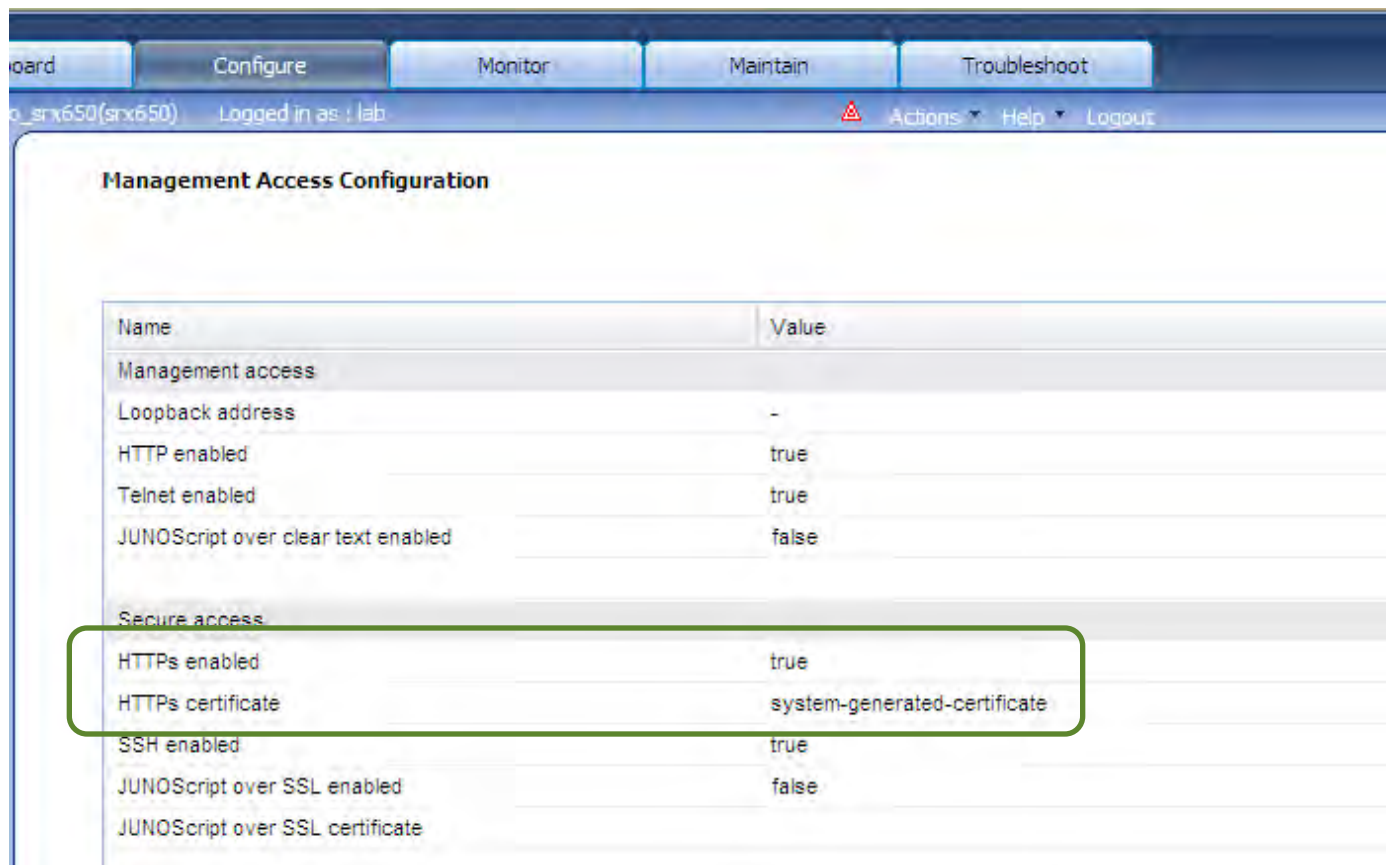
リモートアクセスVPN設定 (8/13)

「Services」タブを選択(①)します。HTTPSを有効化(②)し、証明書(③)とUntrust側のInterface(④)を指定した後、「OK」ボタンをクリック(⑤)します。

The screenshot shows the 'Edit Management Access' configuration window. The 'Services' tab is selected, indicated by a green callout box with the number 1. The 'Enable HTTP' section is expanded, showing 'Enable HTTP' checked (callout 2) and 'ge-0/0/1.0' selected in the 'Selected interfaces' list. The 'Enable HTTPS' section is also expanded, showing 'Enable HTTPS' checked (callout 3), 'system-generated-certificate' selected in the 'HTTPS certificate' dropdown (callout 3), and 'ge-0/0/0.0' selected in the 'Selected interfaces' list (callout 4). The 'OK' button is highlighted with a green callout box with the number 5.

リモートアクセスVPN設定 (9/13)

HTTPS が有効となっており、証明書が指定されていることを確認します。



The screenshot shows the Juniper configuration interface for 'Management Access Configuration'. The 'Secure access' section is highlighted with a green box, indicating that HTTPS is enabled and a system-generated certificate is used.

Name	Value
Management access	
Loopback address	-
HTTP enabled	true
Telnet enabled	true
JUNOScript over clear text enabled	false
Secure access	
HTTPs enabled	true
HTTPs certificate	system-generated-certificate
SSH enabled	true
JUNOScript over SSL enabled	false
JUNOScript over SSL certificate	

リモートアクセスVPN設定 (10/13)

Untrustゾーンに対して、HTTPSアクセスが可能となるよう設定を行います。「Security」→「Zones/Screens」をクリック(①)します。Untrustゾーンを選択(②)し、「Edit」ボタンをクリック(③)します。

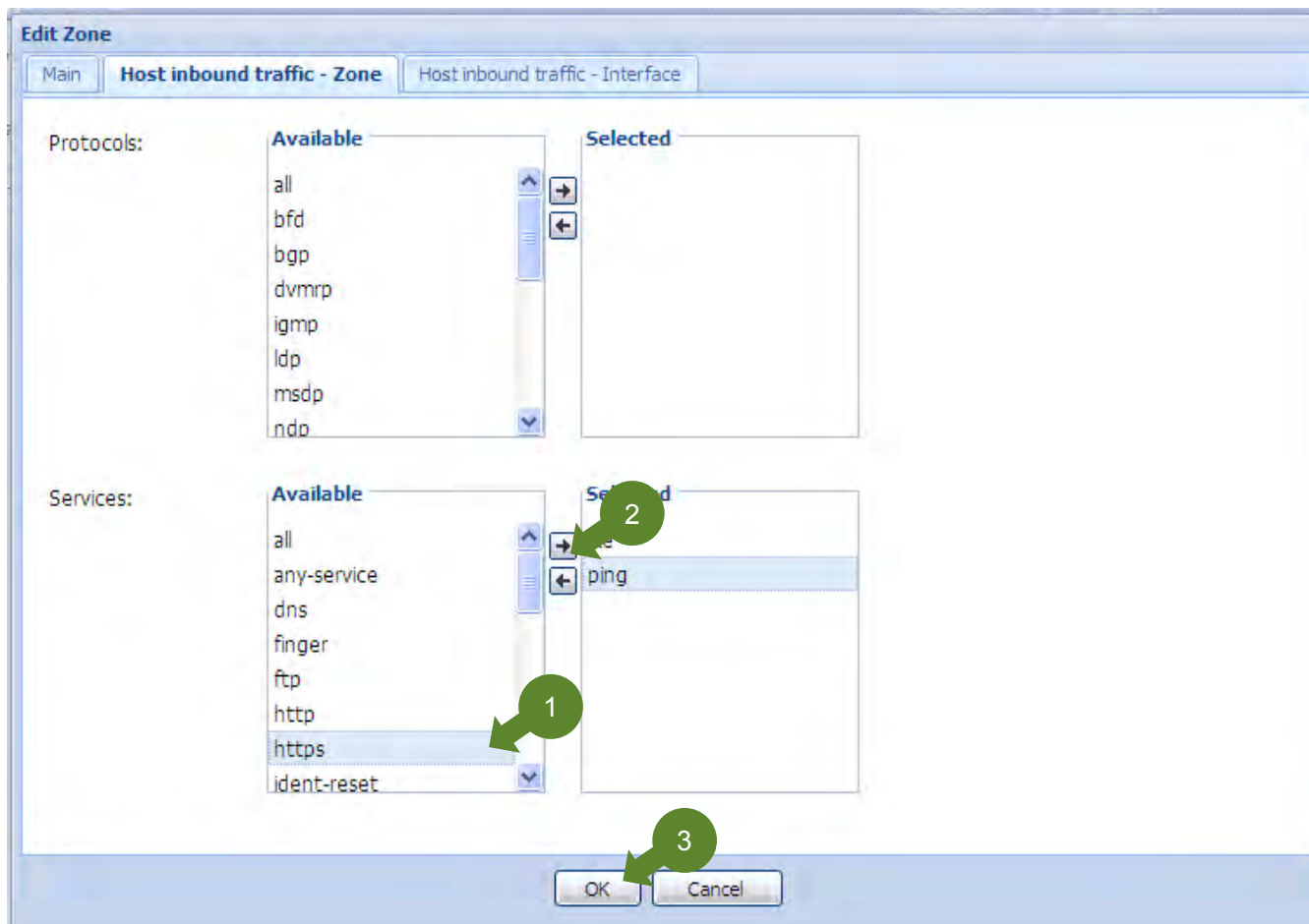
The screenshot shows the Juniper SRX100 configuration interface. The left sidebar has 'Security' expanded, with 'Zones/Screens' selected (1). The main area shows 'Zones/Screens configuration' with a table of zones. The 'untrust' zone is selected (2). The 'Edit' button is highlighted (3).

Zone name	Type	Services	Protocols	Interfaces	Screen
trust	security	all	all	...	
untrust	security			...	untrust-screen

Screen name	Type
untrust-screen	icmp,ip,tcp

リモートアクセスVPN設定 (11/13)

httpsサービスを選択(①)し、AvailableからSelectedへ移動させて(②)、OKボタンをクリック(③)します。



リモートアクセスVPN設定 (12/13)

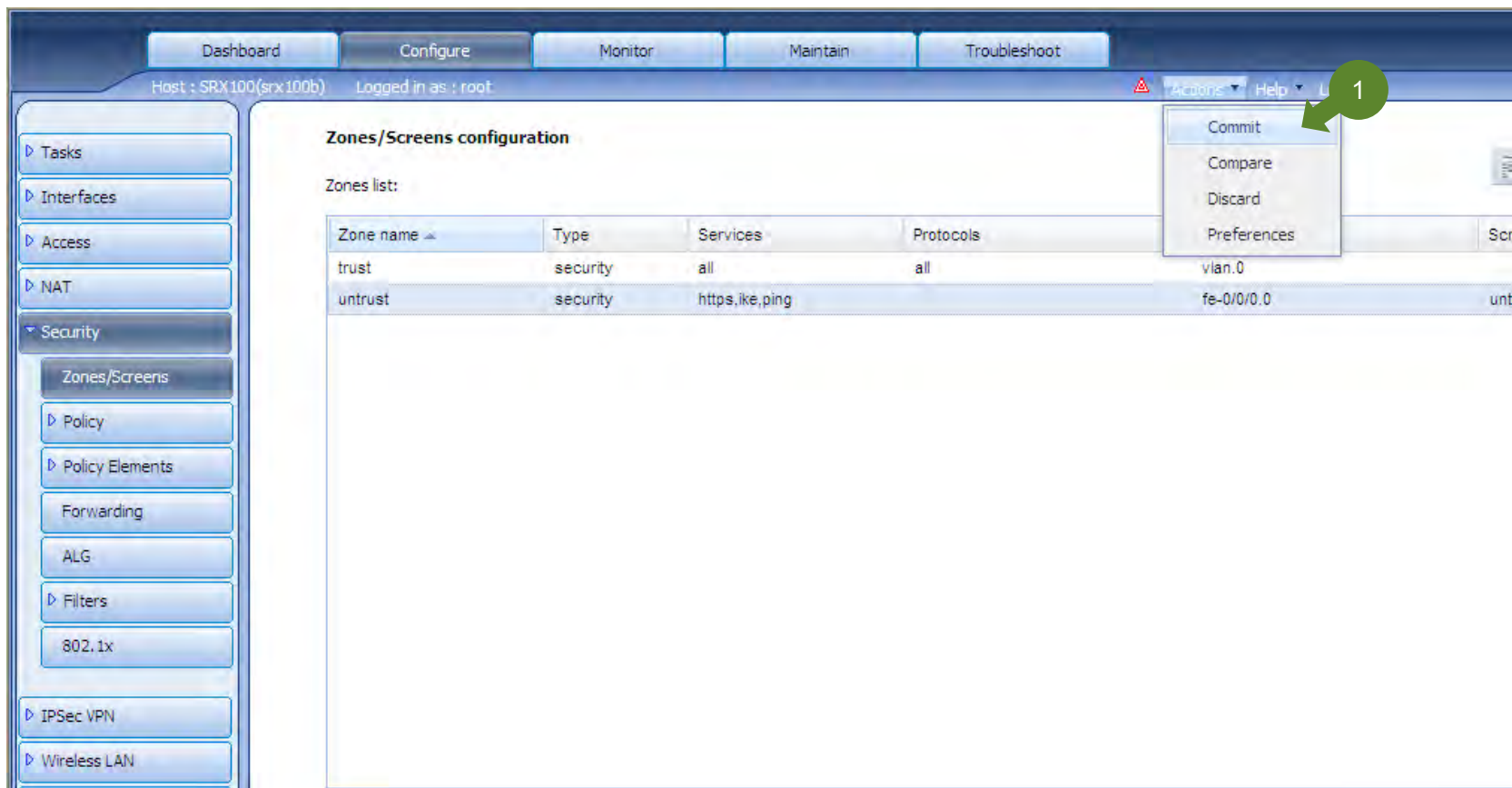
UntrustゾーンのServicesにhttps(およびVPN用のIKE)が含まれていることを確認します。

The screenshot shows the Juniper SRX100 configuration interface. The top navigation bar includes Dashboard, Configure, Monitor, Maintain, and Troubleshoot. The host is identified as SRX100(srx100b) and the user is logged in as root. The left sidebar shows a navigation menu with categories like Tasks, Interfaces, Access, NAT, Security, and 802.1x. The main content area is titled 'Zones/Screens configuration' and displays a 'Zones list' table. The table has four columns: Zone name, Type, Services, and Protocols. The 'untrust' zone is highlighted with a green box, indicating its configuration: Type is 'security' and Services are 'https,ike,ping'.

Zone name ▲	Type	Services	Protocols
trust	security	all	all
untrust	security	https,ike,ping	

リモートアクセスVPN設定 (13/13)

「Actions」→「Commit」を選択(①)し、設定を反映させます。



The screenshot shows the Juniper Networks configuration interface for a Juniper SRX100. The main content area displays the 'Zones/Screens configuration' page. The 'Zones list' table is visible, showing two zones: 'trust' and 'untrust'. The 'trust' zone is of type 'security', has 'all' services, and 'all' protocols. The 'untrust' zone is also of type 'security', has 'https,ike,ping' services, and 'fe-0/0/0.0' protocols. The 'Actions' menu is open, and the 'Commit' option is highlighted with a green circle and arrow labeled '1'.

Zone name	Type	Services	Protocols	Screen
trust	security	all	all	vlan.0
untrust	security	https,ike,ping	fe-0/0/0.0	unt

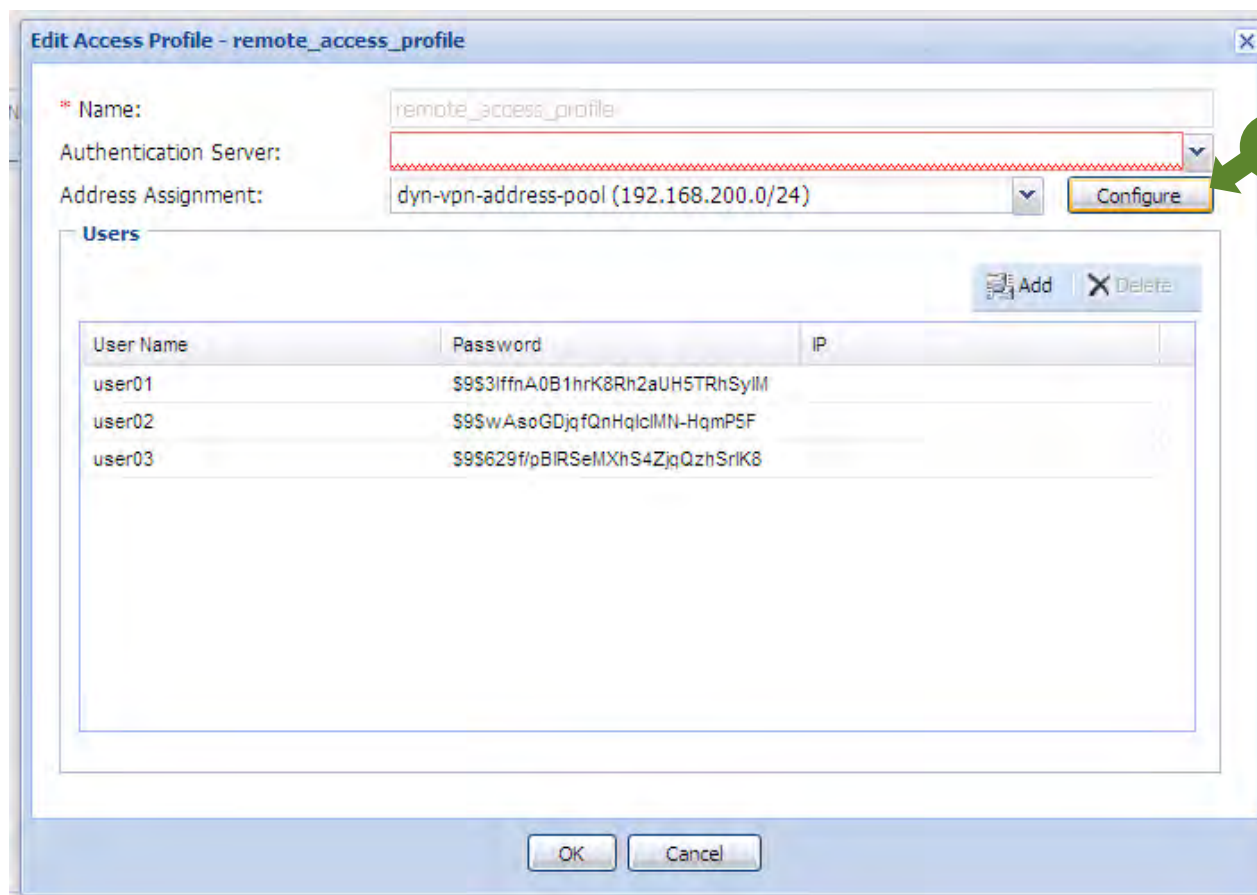
リモートアクセスVPN設定 – オプション(1/6)

プールアドレスの範囲、セカンダリDNS/WINSサーバの指定を行うには、Access Profileの設定を変更します。「Configure」→「Access」→「Access Profiles」をクリック(①)します。Wizardによって作成された「remote_access_profile」を選択(②)し、Editボタンをクリック(③)します。

The screenshot displays the Juniper SRX100 configuration interface. The top navigation bar includes tabs for Dashboard, Configure, Monitor, Maintain, and Troubleshoot. The status bar indicates the host is SRX100(srx100b) and the user is logged in as root. The left sidebar contains a navigation menu with categories like Tasks, Interfaces, Access, NAT, Security, IPSec VPN, Wireless LAN, Switching, Routing, Class of Service, System Properties, and Chassis Cluster. The 'Access' category is expanded, and 'Access Profiles' is selected, marked with a green circle 1. The main content area is titled 'Access Profile Configuration' and shows a table with one entry: 'remote_access_profile', marked with a green circle 2. To the right of the table are buttons for Add, Edit, and Delete, with the 'Edit' button highlighted, marked with a green circle 3.

リモートアクセスVPN設定 – オプション(2/6)

「Configure」ボタンをクリック(①)します。



Edit Access Profile - remote_access_profile

* Name: remote_access_profile

Authentication Server: [Redacted]

Address Assignment: dyn-vpn-address-pool (192.168.200.0/24) **Configure**

Users

Add X Delete

User Name	Password	IP
user01	\$9\$3iffnA0B1hrK8Rh2aUH5TRhSylM	
user02	\$9\$wAsoGDjqfQnHqlcIMN-HqmP5F	
user03	\$9\$629fpBIRSeMXhS4ZjqQzhSrlK8	

OK Cancel

リモートアクセスVPN設定 – オプション(3/6)

「dyn-vpn-address-pool」をクリック(①)すると、下の「Properties of selected address pool」で編集できるようになります。「Add」ボタンをクリック(②)します。

Address Pool Configuration

Address Pools

Address Pool Name	Network Address
dyn-vpn-address-pool	192.168.200.0/24

Properties of selected address pool

* Name: dyn-vpn-address-pool

* Network Address: 192.168.200.0/24

Address Ranges XAUTH Attributes

Address Range Name	Lower Limit	High Limit
--------------------	-------------	------------

OK Reset

リモートアクセスVPN設定 – オプション(4/6)

レンジ名、レンジの最初と最後のIPアドレスを指定します(①)。

Address Pools

Address Pool Name	Network Address
dyn-vpn-address-pool	192.168.200.0/24

Properties of selected address pool

* Name: dyn-vpn-address-pool

* Network Address: 192.168.200.0/24

Address Ranges

Address Range Name	Lower Limit	High Limit
pool-range	192.168.200.11	192.168.200.20

OK Reset

リモートアクセスVPN設定 – オプション(5/6)

「XAUTH Attributes」をクリック(①)し、セカンダリDNS/WINSサーバのアドレスを指定(②)します。
設定に間違いが無いことを確認し、「OK」ボタンをクリック(③)します。

The screenshot shows the 'Address Pool Configuration' dialog box. It contains a table of address pools and a section for the properties of the selected pool. The 'XAUTH Attributes' section is expanded, showing fields for Primary and Secondary DNS and WINS Servers. Green arrows and numbers 1, 2, and 3 indicate the steps to be followed.

Address Pool Name	Network Address
dyn-vpn-address-pool	192.168.200.0/24

Properties of selected address pool:

* Name: dyn-vpn-address-pool

* Network Address: 192.168.200.0/24

Address Ranges: XAUTH Attributes

Primary DNS Server: 192.168.1.10/32

Secondary DNS Server: 192.168.1.11/32

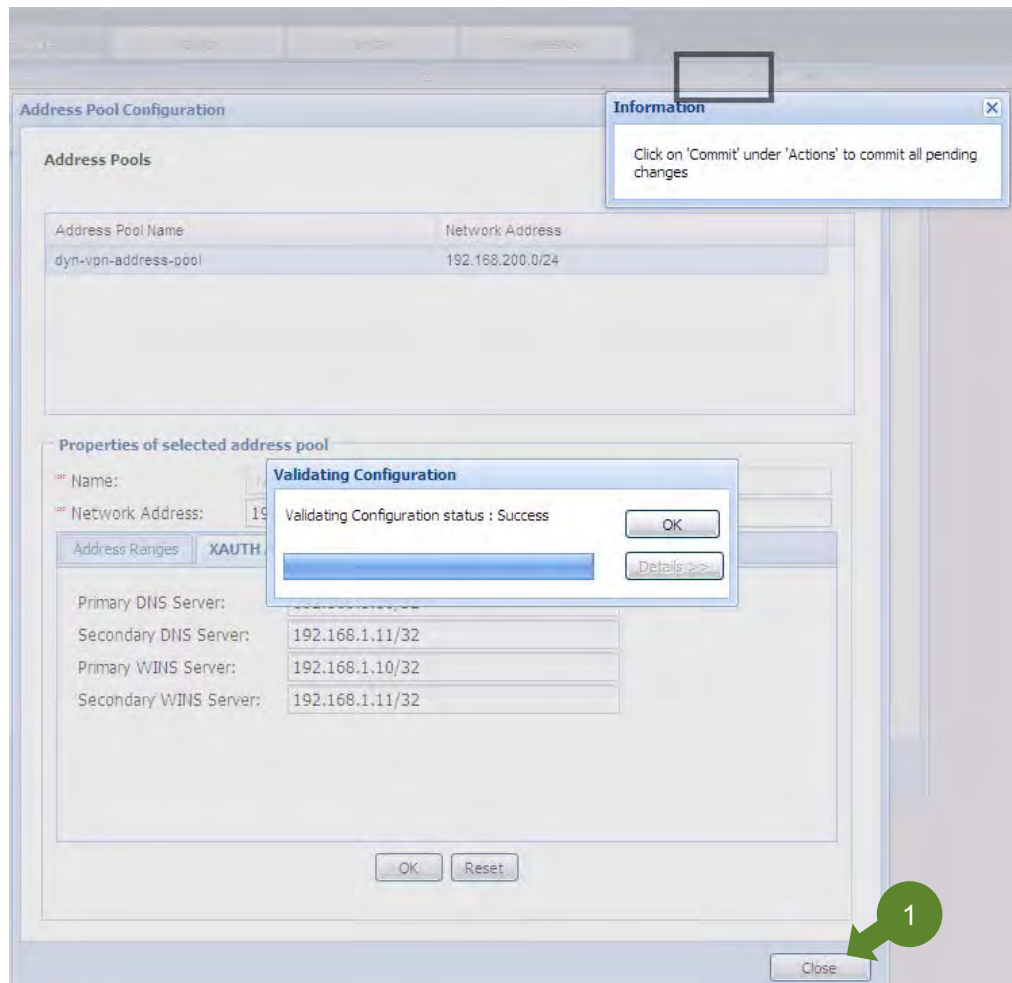
Primary WINS Server: 192.168.1.10/32

Secondary WINS Server: 192.168.1.11/32

Buttons: OK, Reset

リモートアクセスVPN設定 – オプション(6/6)

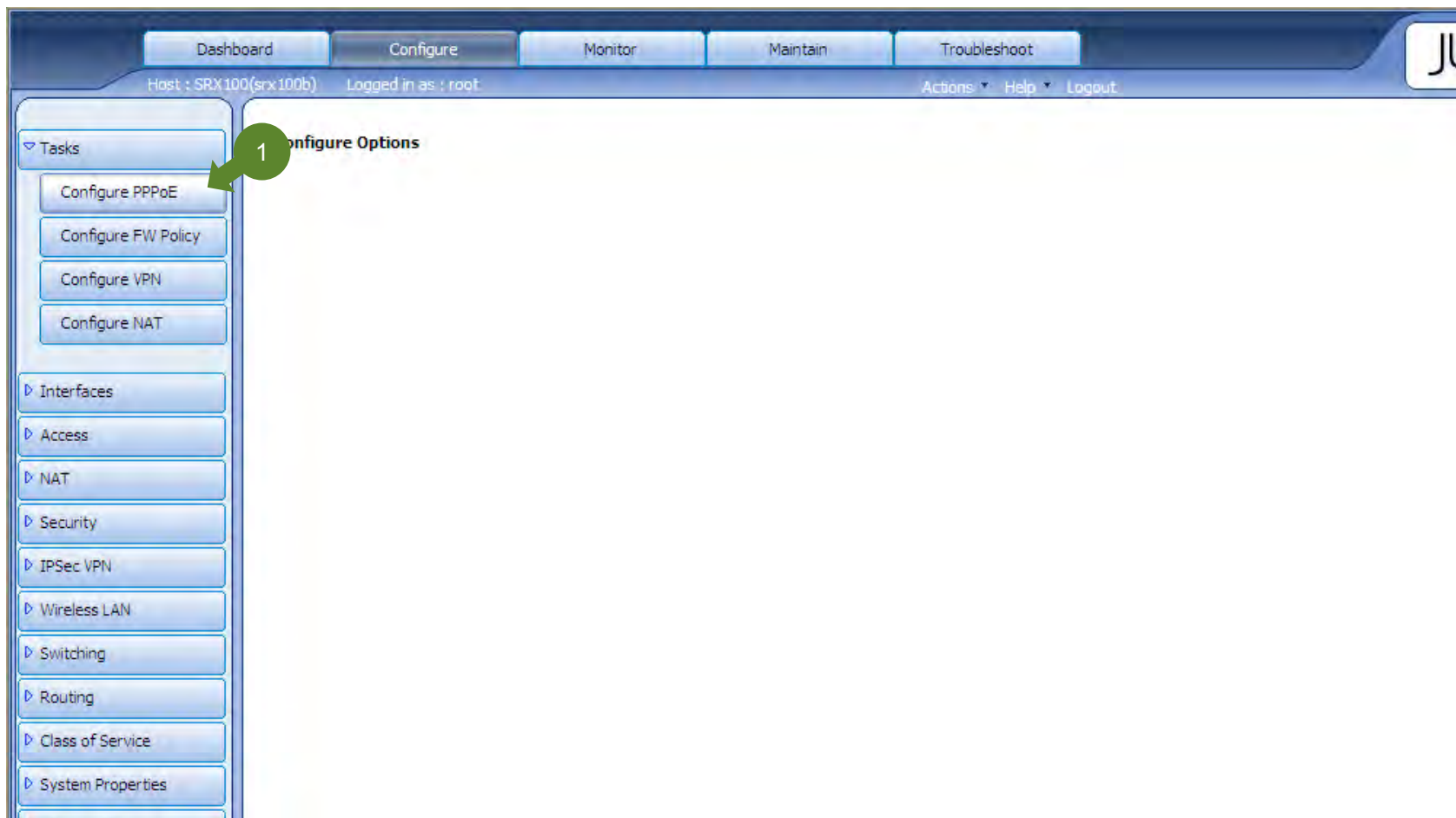
「Close」ボタンをクリック(①)後、Commitボタンをクリックし、設定を反映させます。



Chapter5. PPPoE

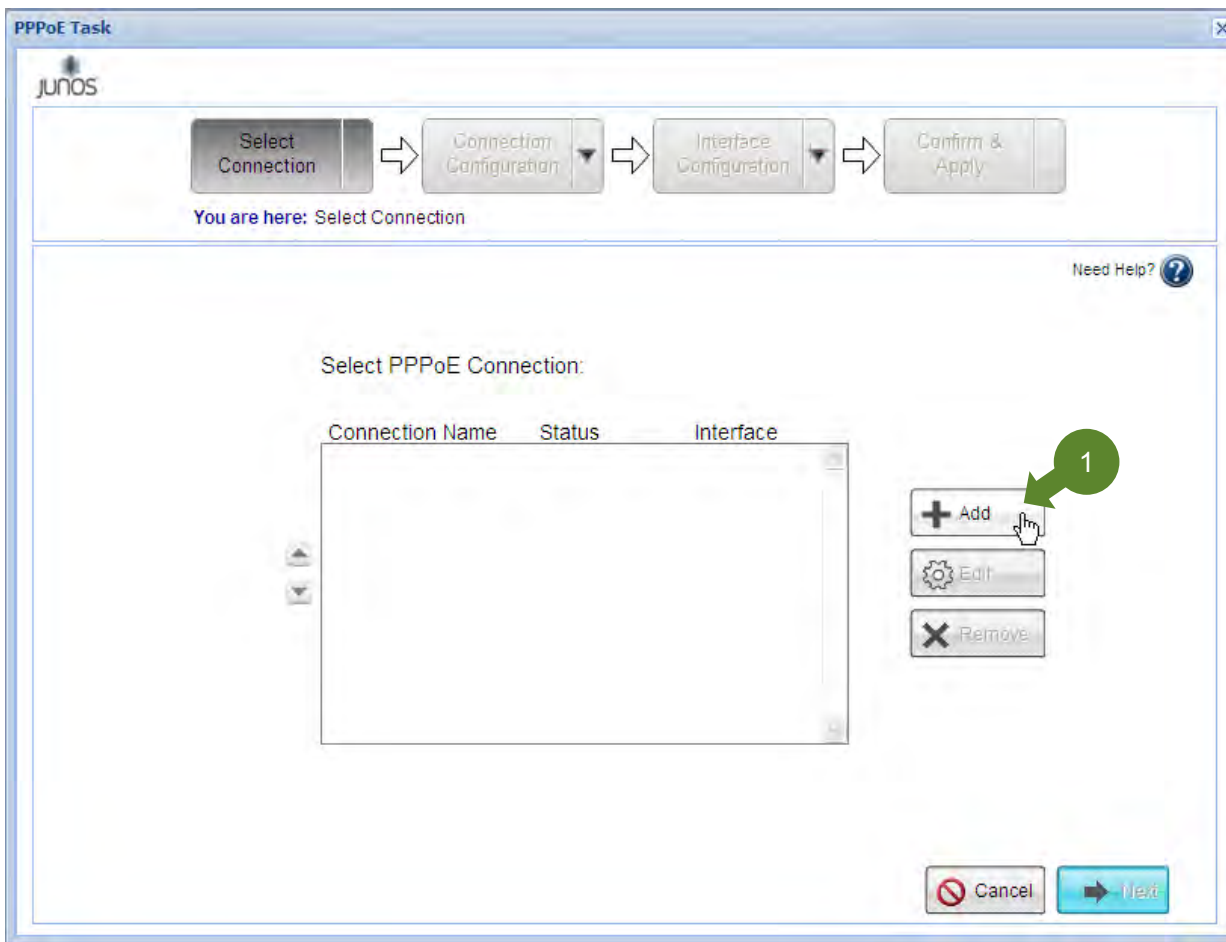
PPPoE設定(1/22)

PPPoEの設定は、ウィザードを使用して簡単に設定することが可能です。ウィザードは、Configure タブを選択し左側の項目より、「Tasks」→「Configure PPPoE」をクリックする(①)と表示されます。(次ページ)



PPPoE設定(2/22)

「Add」ボタンをクリックします。(①)



PPPoE設定(3/22)

「Connection Name」の入力欄にPPPoE接続設定名 (ISP名など)を入力し①、「Next」ボタンをクリックします②。

PPPoE Task

junos

Select Connection → Connection Configuration → Interface Configuration → Confirm & Apply

You are here: Connection Configuration > Basic Settings

Need Help? ?

Connection Name:

Select PPPoE Service Provider:

Auto Discover
 Specify Manually

Address Concentrator Name:

Service Name:

Advanced Options

Select Authentication Type:

Auto Negotiate PAP CHAP

← Back Cancel **Next** →

PPPoE設定(4/22)

PPPoE接続用のユーザID(①)とパスワード(②)を入力し、「Next」ボタンをクリック(③)します。

PPPoE Task

Junos

Select Connection → Connection Configuration → Interface Configuration → Confirm & Apply

You are here: Connection Configuration > Auto Negotiate Authentication

Need Help? ?

Account Credential:

User Name:

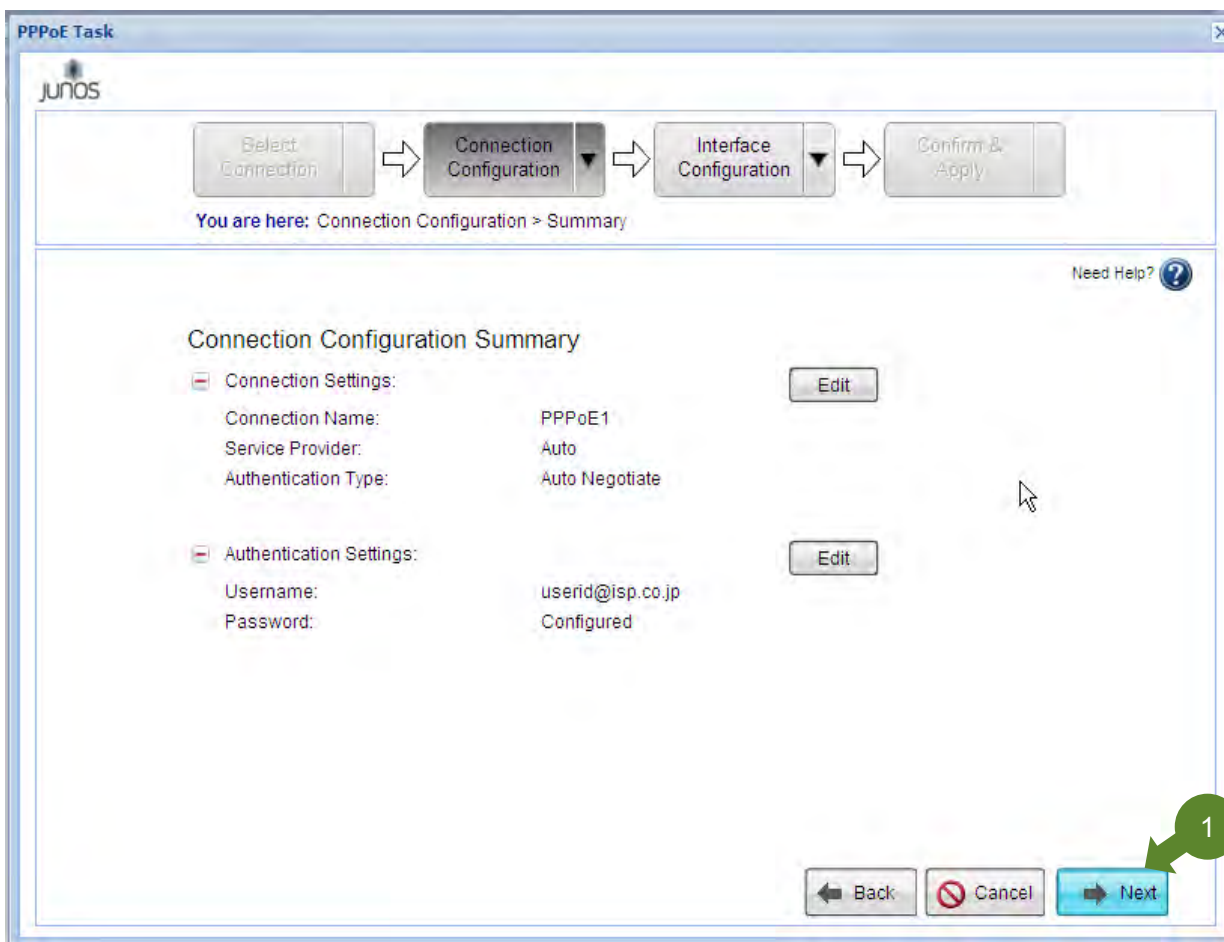
Password:

Confirm Password:

Back Cancel Next

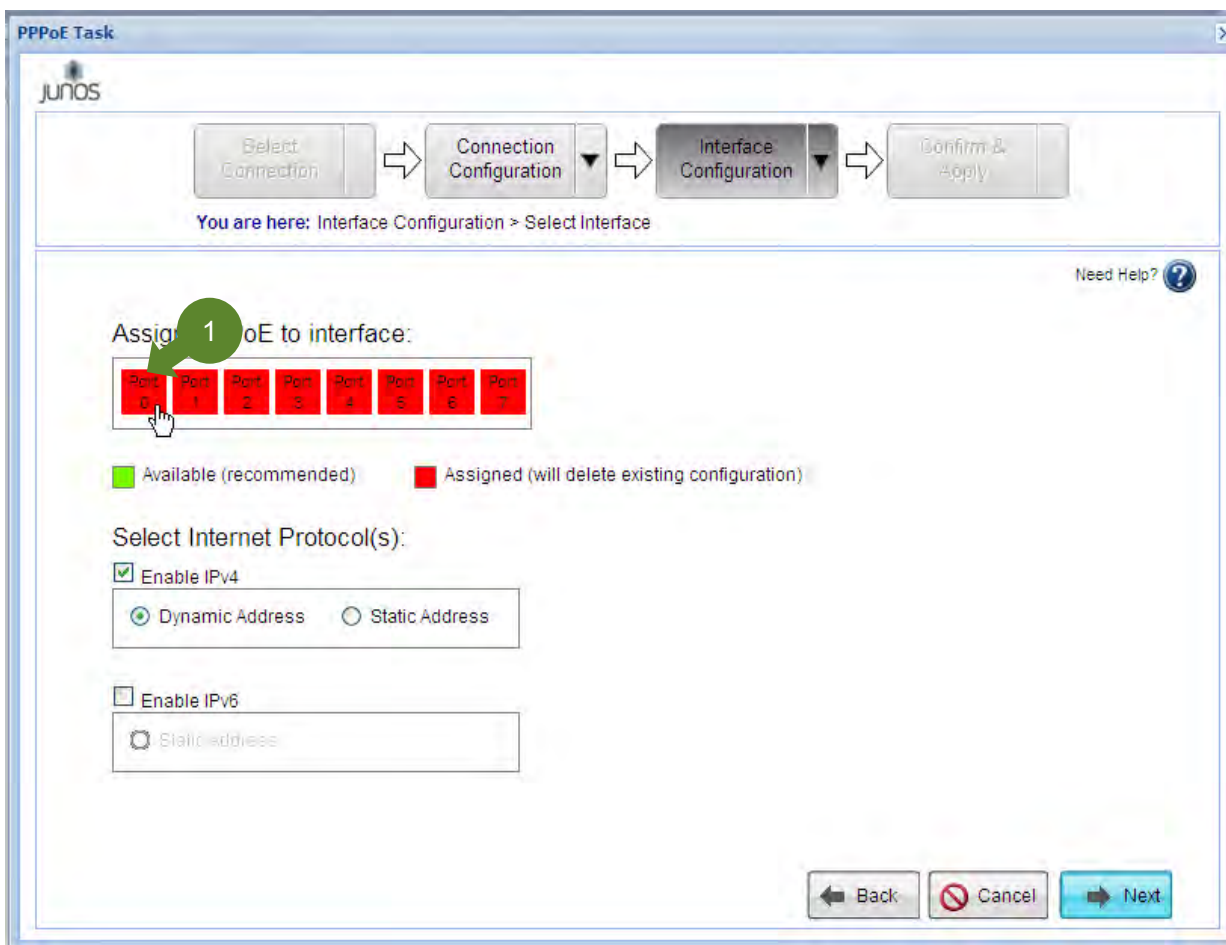
PPPoE設定(5/22)

入力した設定が表示されていることを確認し、正しければ「Next」ボタンをクリック(①)します。



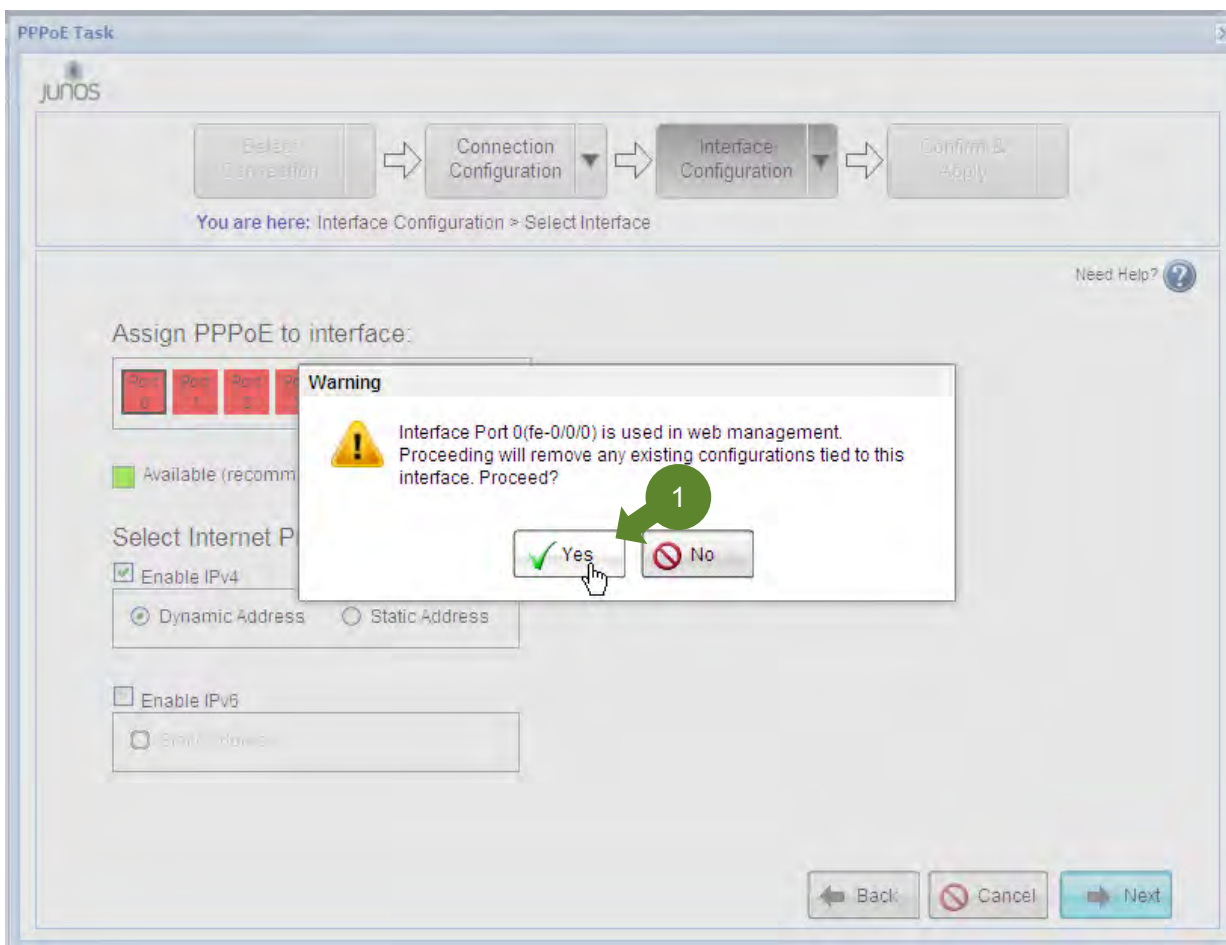
PPPoE設定(6/22)

PPPoE回線を接続するインタフェースをクリック(①)します。



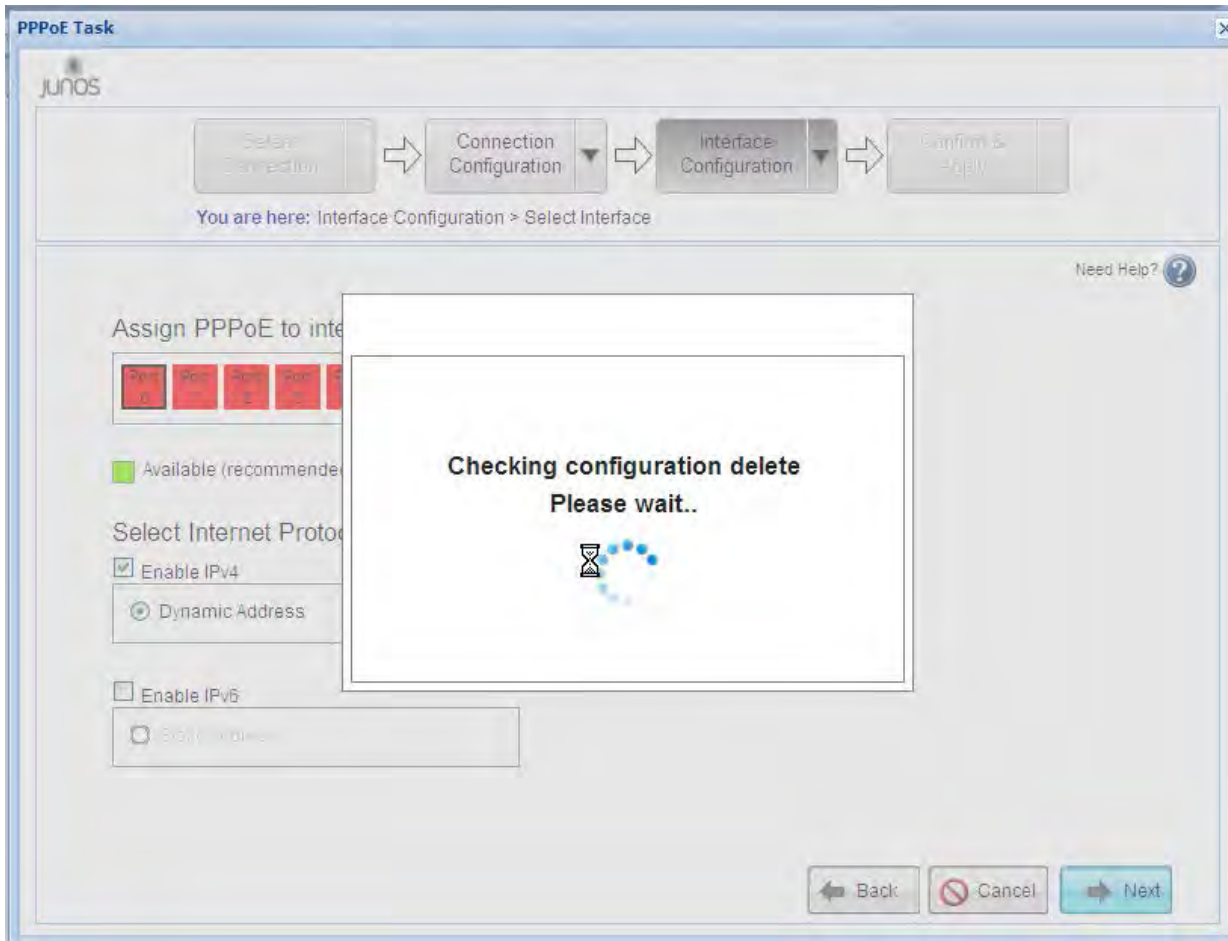
PPPoE設定(7/22)

PPPoE回線を接続するインタフェース上の既存設定を削除しても良いか？という内容のメッセージが表示されます。正しいインタフェースを選択しているのであれば、「Yes」ボタンをクリック①します



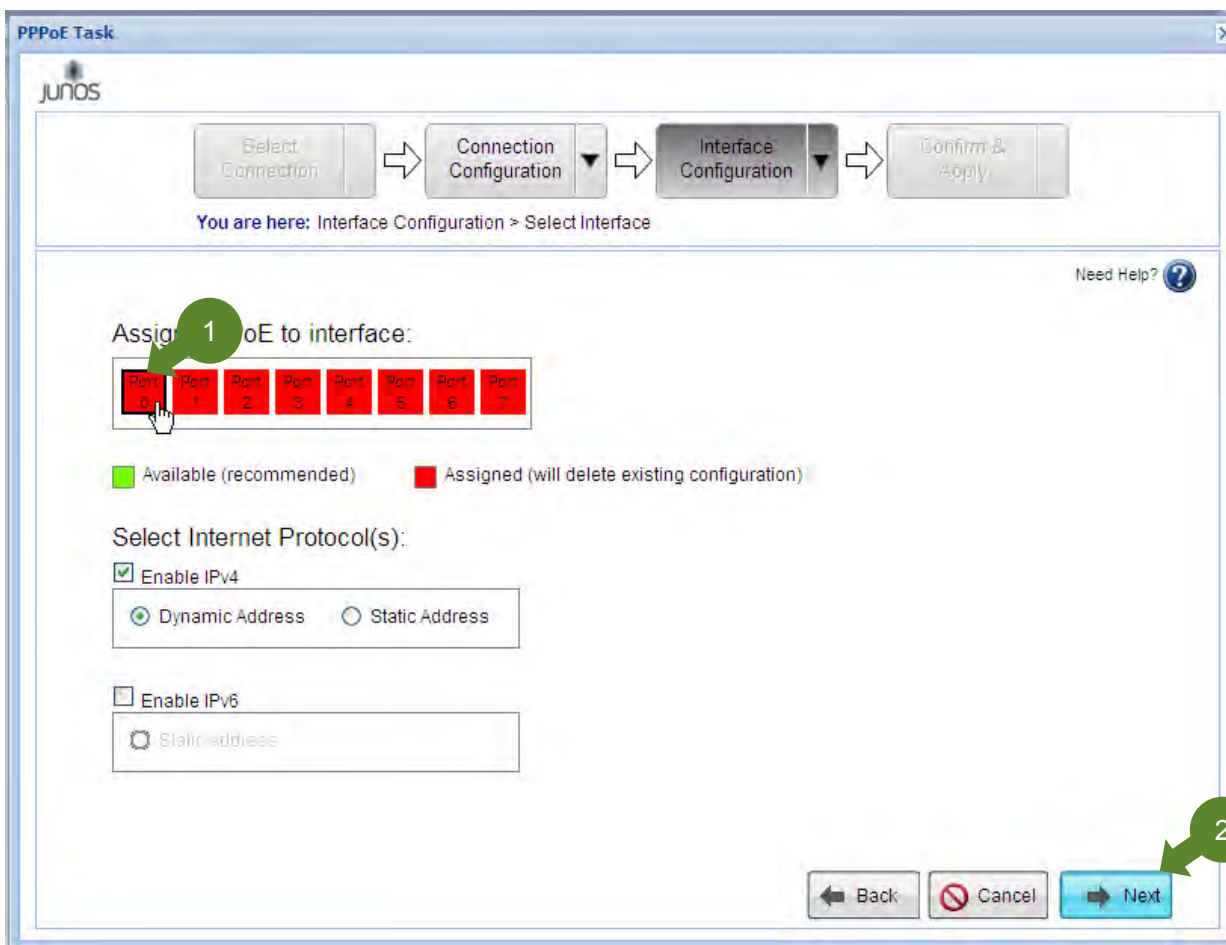
PPPoE設定(8/22)

PPPoE回線を接続するインタフェース上の既存設定を削除していますので、しばらく待ちます。



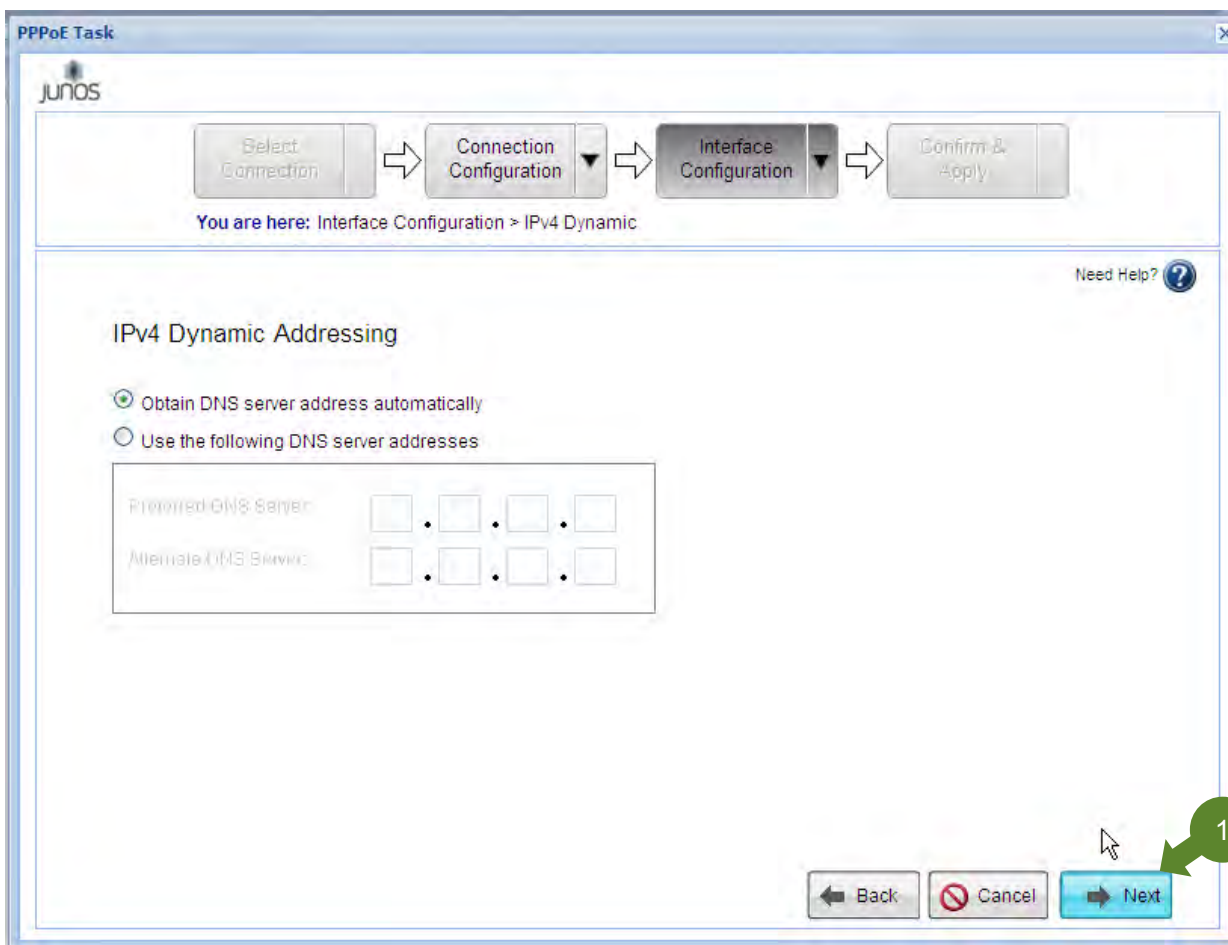
PPPoE設定(9/22)

選択したインターフェースに太い黒枠が付いていることを確認します(①)。ISPから付与されるグローバルアドレスが動的であれば、このまま「Next」ボタン(②)をクリックします。



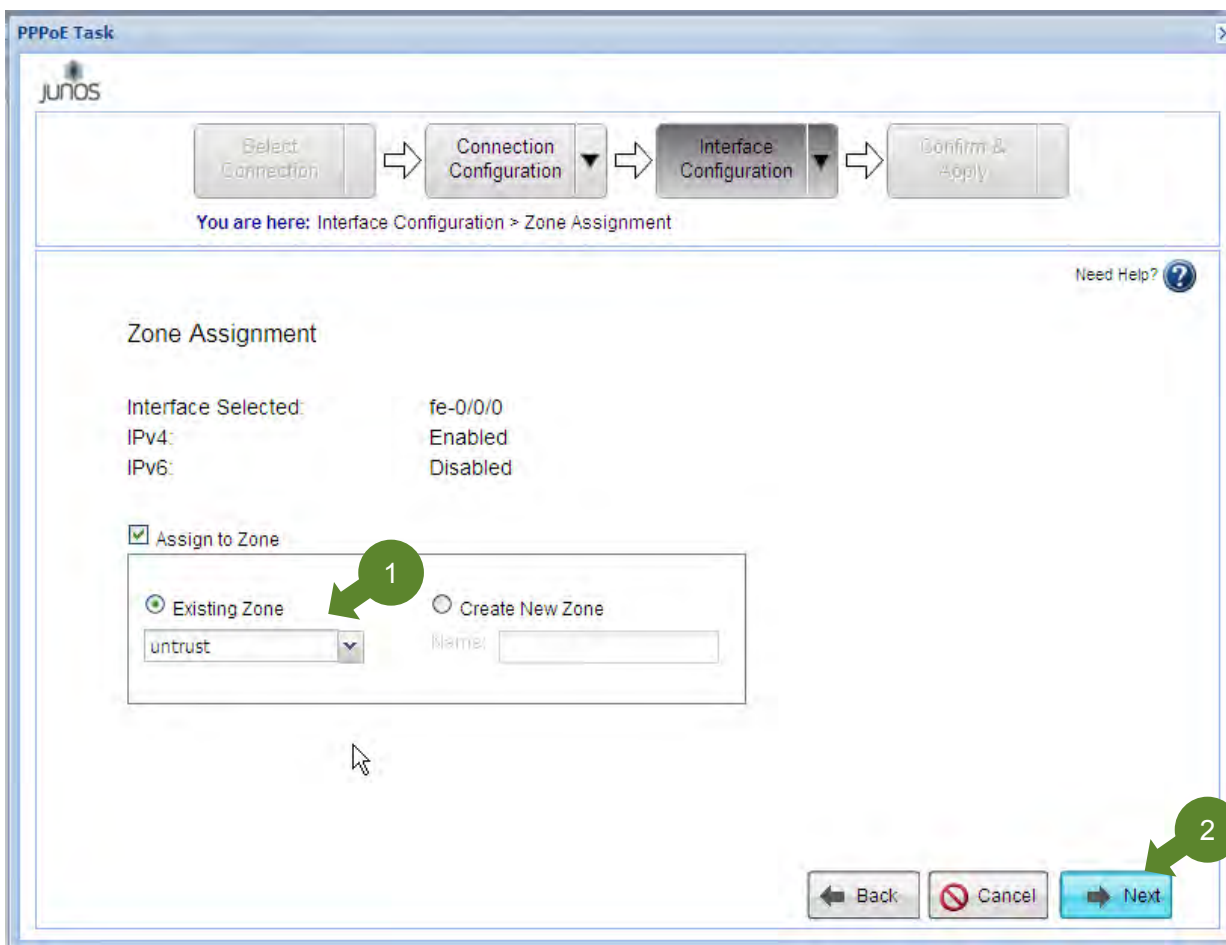
PPPoE設定(10/22)

DNSサーバアドレス情報を指定します。通常はISPから自動的に配信されたものを利用しますので、設定は特に変更せず、「Next」ボタン(①)をクリックします。



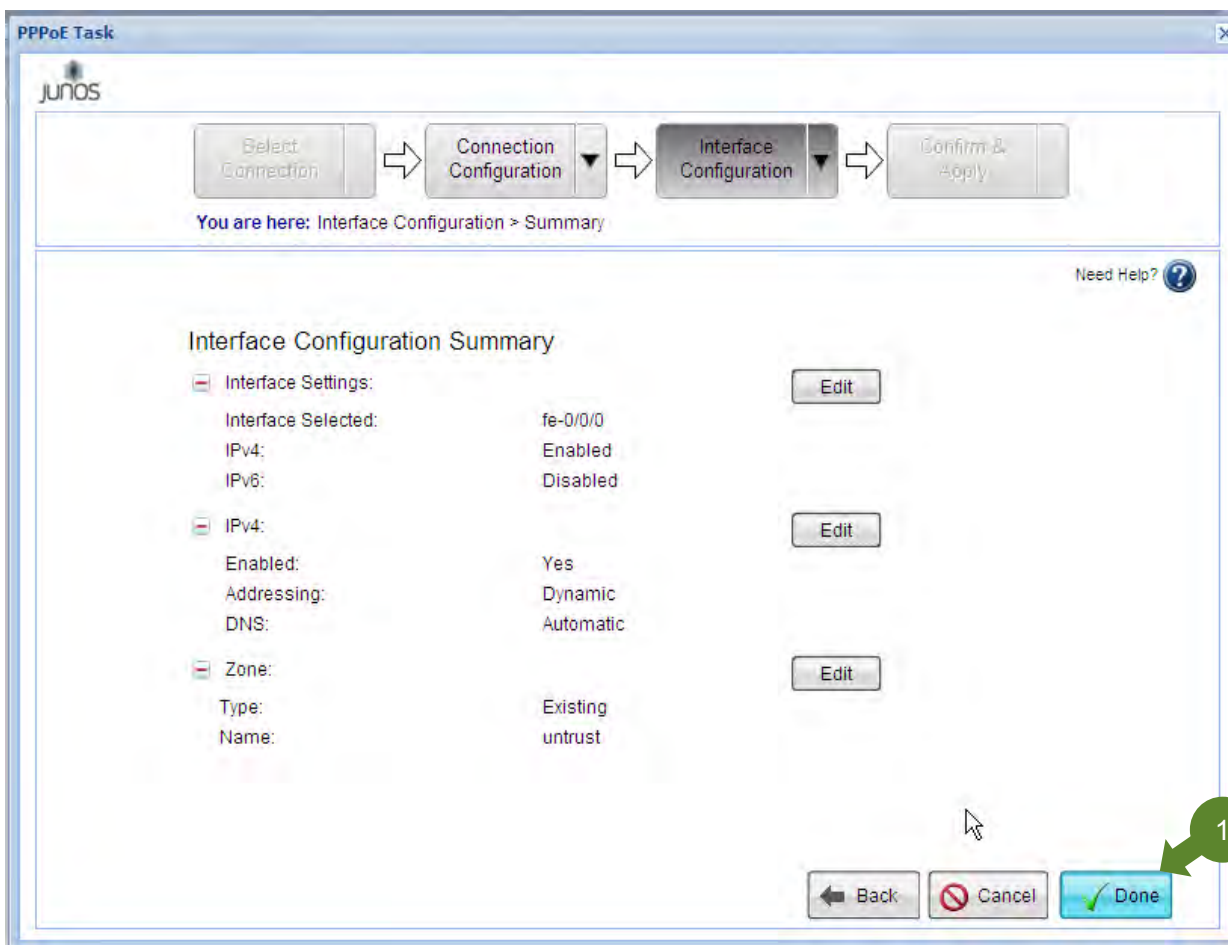
PPPoE設定(11/22)

PPPoE回線を接続するインタフェースのZoneを指定します(①)。通常はuntrustを指定します。よろしければ「Next」ボタン(②)をクリックします。



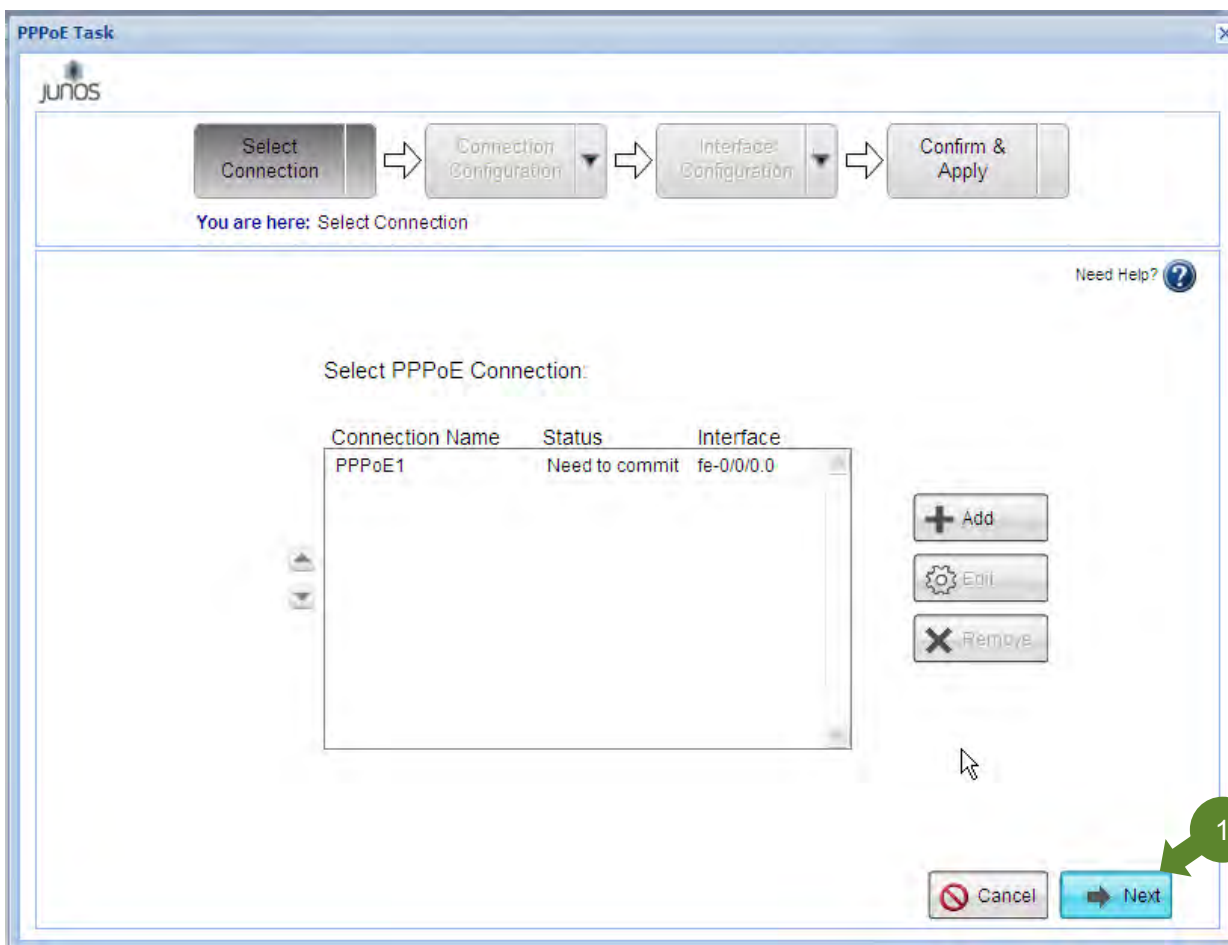
PPPoE設定(12/22)

入力した設定が表示されていることを確認し、正しければ「Next」ボタンをクリック(①)します。



PPPoE設定(13/22)

「Next」ボタンをクリック(①)します。



PPPoE設定(14/22)

これまでの設定が表示されますので、「+」ボタンをクリックし①、内容を確認してください。正しければ「Next」ボタンをクリックします②。

PPPoE Task

junos

Select Connection → Connection Configuration → Interface Configuration → Confirm & Apply

You are here: Confirm & Apply > Summary

Need Help? ?

Congratulations

PPPoE Configuration **steps completed successfully**. Please review your configuration below. To make additional changes or corrections click on Edit to navigate to the corresponding area.

Summary:

Connection: PPPoE1

Connection Configuration Summary:

- + Connection Settings: Edit
- + Authentication Settings: Edit

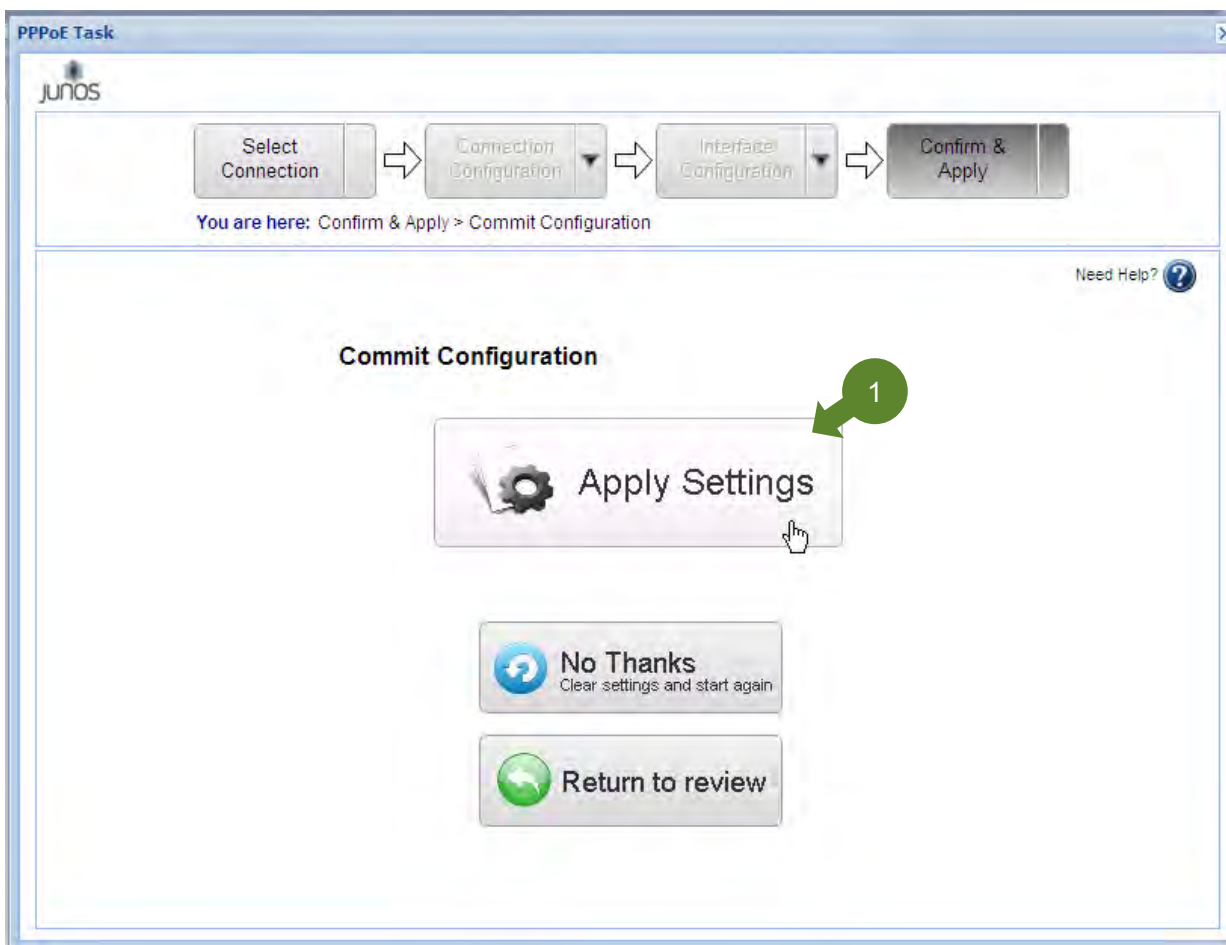
Interface Configuration Summary:

- + Interface Settings: Edit

Back Next

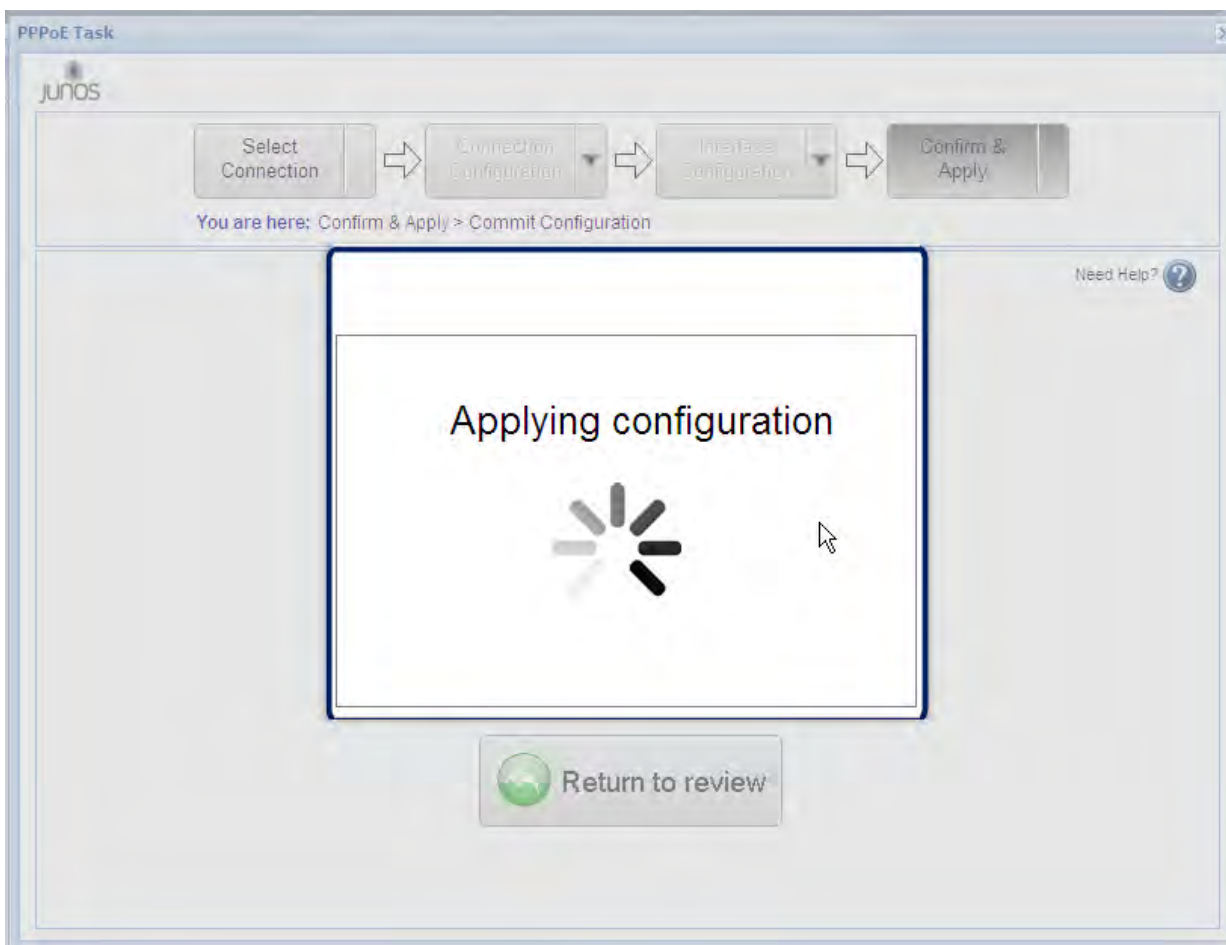
PPPoE設定(15/22)

「Apply Settings」ボタンをクリックします(①)。



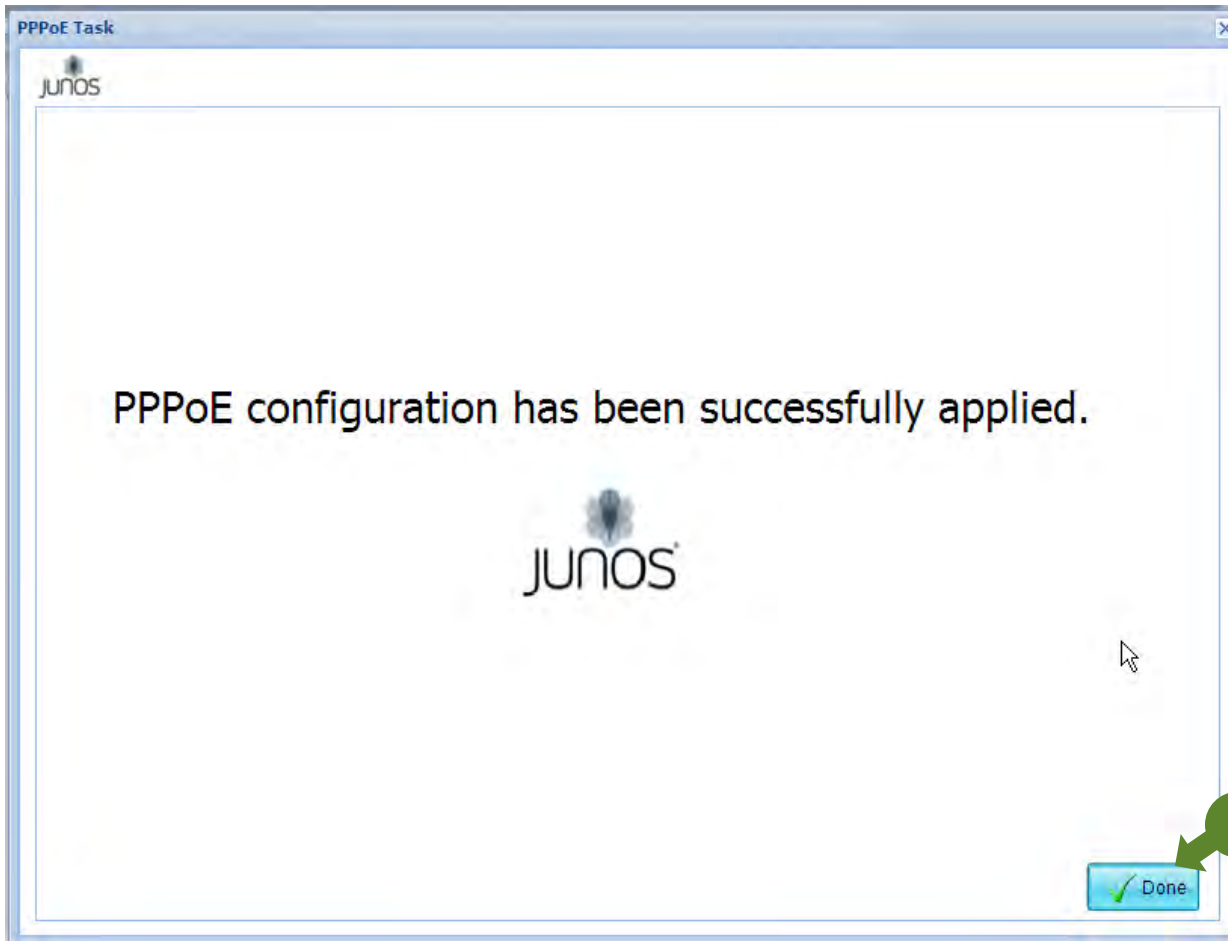
PPPoE設定(16/22)

設定反映中となりますので、しばらく待ちます。



PPPoE設定(17/22)

設定が設定された旨のメッセージが表示されます。「Done」ボタンをクリックし(②)、ウィザードを終了します。



PPPoE設定(18/22)

PPPoEセッションが切断された場合に、自動的に再接続させるための設定を追加します。「CLI Tools」→「Point and Click CLI」をクリックします。次に画面中ほどの設定ツリーにて「groups」→「wiz-PPPoE-0」→「interfaces」→「interface」→「pp0」→「unit」→「0」→「pppoe-options」をクリックします。「Auto reconnect」設定項目に対し、30くらいの値(単位は秒)を入力し、「Commi...」ボタンをクリックします。

The screenshot displays the Juniper NCA interface for configuring PPPoE options. The left sidebar shows the navigation menu with 'Point and Click CLI' selected (1). The configuration tree on the left shows the path: groups > wiz-PPPoE-0 > interfaces > interface > pp0 > unit > 0 > pppoe-opt (2). The main configuration area shows the 'Pppoe options' section with the following fields:

- Access concentrator: []
- Auto reconnect: 30 (3) [?] M
- Idle timeout: [] [?]
- Pppoe mode: []
- Service name: [] [?]
- Underlying interface: fe-0/0/0.0 [?] *

The 'Auto reconnect' field is highlighted in yellow, indicating it has been modified. The 'Commit...' button is highlighted (4). The legend at the bottom explains the icons: Comment (C), Inactive (I), and Modified (M).

PPPoE設定(19/22)

設定を反映させるため、「OK」ボタンをクリックします(①)。

The screenshot displays the Juniper configuration web interface. The top navigation bar includes tabs for Dashboard, Configure, Monitor, Maintain, and Troubleshoot. Below the navigation bar, the host information is SRX100(srx100h) and the user is logged in as root. The left sidebar contains a tree view of configuration categories, with 'CLI Tools' expanded to show 'CLI Viewer', 'CLI Editor', and 'Point and Click CLI'. The main content area is titled 'Summary of Changes' and shows a list of configuration changes. The first change is 'set group wiz_PPPoE_0 interfaces interface pp0 unit 0 pppoe-options auto-reconnect 30'. Below the list, there are 'OK' and 'Cancel' buttons. A green circle with the number '1' and an arrow points to the 'OK' button, indicating the step to click to apply the changes.

PPPoE設定(20/22)

正常に設定反映が行われると、Successと表示されます(①)。

The screenshot displays the Juniper configuration web interface. At the top, there are navigation tabs: Dashboard, Configure, **M**, Maintain, and Troubleshoot. The 'M' tab is selected and highlighted with a green circle containing the number '1', with an arrow pointing to it. Below the tabs, the status bar shows 'Host : SRX100(srx100h)' and 'Logged in as : root'. On the right side of the status bar, there are links for 'Actions', 'Help', and 'Logout'. On the left side, there is a vertical menu with various configuration categories like Tasks, Interfaces, Access, NAT, Security, etc. The main content area is divided into two sections. The left section is titled 'Configuration' and shows a tree view of the configuration hierarchy, including 'groups', 'wiz-PPPoE-0', 'system', 'interfaces', 'interface', 'pp0', 'unit', '0', 'ppp-option', 'pppoe-opti', 'family', 'fe-0/0/0', 'routing-options', 'security', 'system', 'interfaces', 'protocols', 'security', and 'vlans'. The right section displays a 'Success' message with an 'OK' button below it. A mouse cursor is visible in the lower right area of the main content.

PPPoE設定(21/22)

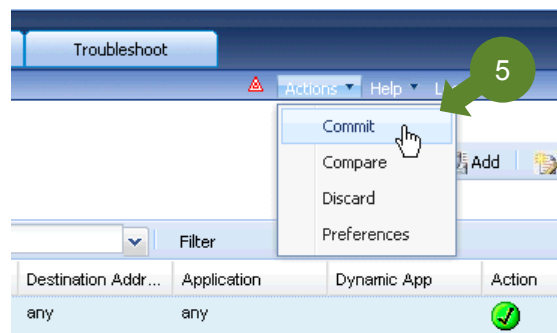
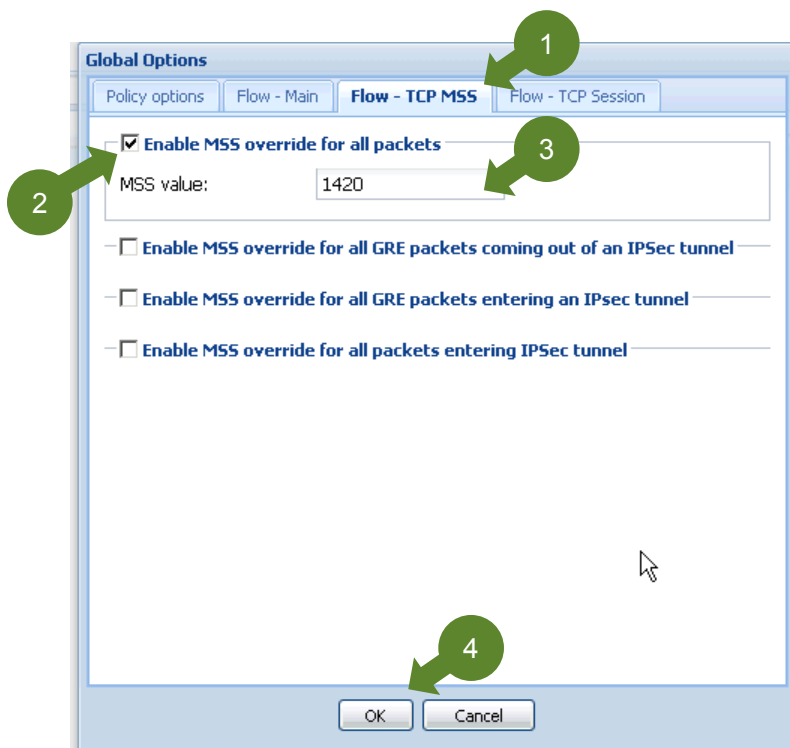
TCP MSSの設定を追加します。「Security」→「Policy」→「Apply Policy」をクリック(①)します。次に「Global Options」ボタンをクリックします(②)。

The screenshot displays the Juniper SRX100 configuration interface. The top navigation bar includes 'Dashboard', 'Configure', 'Monitor', 'Maintain', and 'Troubleshoot'. The main content area is titled 'Security Policy'. On the left sidebar, the 'Security' menu is expanded, and 'Apply Policy' is highlighted with a green circle and the number 1. In the top right of the policy configuration area, the 'Global Options' button is highlighted with a green circle and the number 2. Below this, a table shows the policy configuration:

From Zone	To Zone	Name	Source Address	Destination Addr...	Application	Dynamic App	Action	NW Service
trust	untrust	trust-to-untrust	any	any	any		✓	

PPPoE設定(22/22)

「Flow - TCP」タブをクリックし(①)、「Enable MSS override for all packets」チェックボックスを有効にします(②)。次にMSS value値として数値(ここでは1420)(③)を入力し、「OK」ボタンをクリックします(④)。最後に設定を反映させるため、「Actions」->「Commit」ボタンをクリックします(⑤)。



PPPoE接続確認(1/2)

Monitor タブ (①) から「PPPoE」(②)をクリックし、PPPoE InterfaceのState(③)が「Session Up」になっていれば、PPPoEが正常に接続できていることになります。

The screenshot shows the Juniper Network OS Monitor interface. The 'Monitor' tab is selected, indicated by a green circle with the number 1. In the left-hand navigation menu, the 'PPPoE' option is highlighted, indicated by a green circle with the number 2. The main content area displays the 'PPPoE Interfaces' table, where the 'State' column for the 'pp0.0' interface is 'Session up', indicated by a green circle with the number 3. Below this, the 'PPPoE Statistics' section shows 'Active PPPoE Sessions' as 1. A table lists various packet types and their counts for sent and received packets. Another table shows timeout statistics for PADI, PADO, and PADR.

Interface	Underlying Interface	State	Service	Session ID	AC	AC MAC Address
pp0.0	fe-0/0/0.0	Session up	None	3461	BAS	

Packet Type	Sent	Received
PADI	1	0
PADO	0	1
PADR	1	0
PADS	0	1
PADT	0	0
Service Name Error	0	0
AC System Error	0	0
Generic Error	0	0
Malformed Packet		0
Unknown Packet		0

Timeout	Sent
PADI	0
PADO	0
PADR	0

PPPoE接続確認(2/2)

Monitor タブのInterfaces (①)をクリックした後、Ports for FPC(②) から「All」を選択すると、PPPoE接続インタフェースの情報(グローバルIPアドレスなど)が確認できます(④)。

Host : SRX100F (100h) Logged in as : root Actions Help Logout

Dashboard Configure Monitor Maintain Troubleshoot

Port Monitoring

Ports for FPC: All Show Graph Details Refresh interval (sec): 30

Port	Admin Status	Link Status	Address	Zone	Services	Protocols
pine	Up	Up				
pp0	Up	Up				
pp0.0	Up	Up	1.3.17	untrust		
ppd0	Up	Up				
ppe0	Up	Up				
st0	Up	Up				
tap	Up	Up				

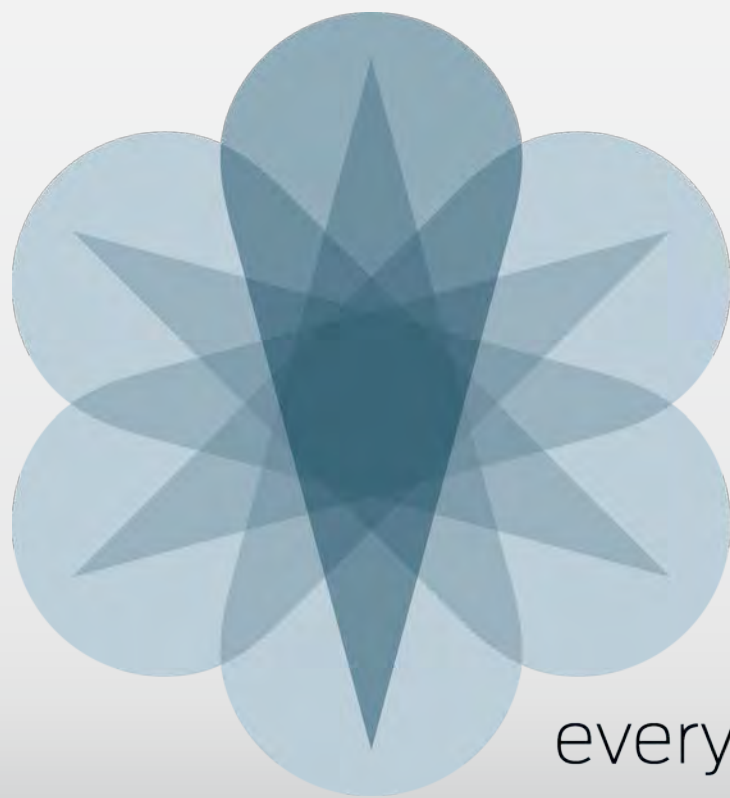
Interface Statistics - fe-0/0/0

Input Rate: 0.000 Kbps

Output Rate: 0.000 Kbps

Error Counters: Input Output

Packet Counters: Input Output



everywhere