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。

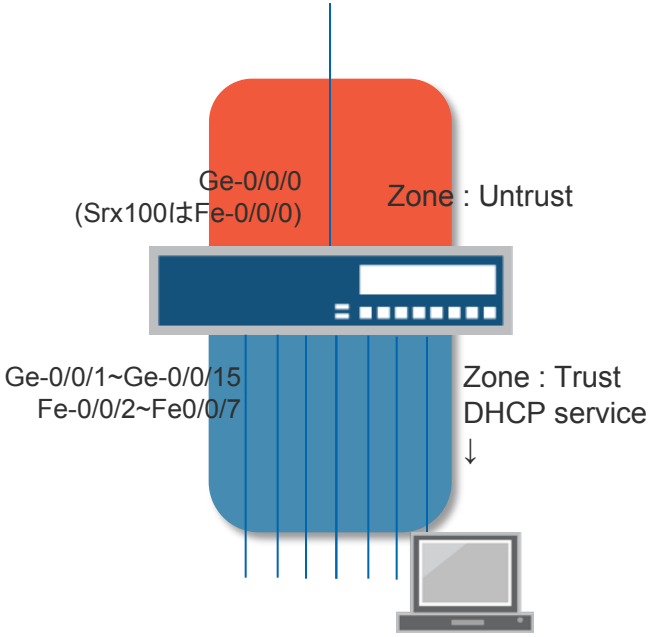
GUIにおける基本的な設定方法についてはミッドレンジ/ハイエンドSRX（SRX650~5800）とも共用となっておりますが、各モデルにおける物理インタフェースや構成要素の考え方などはHW Guideなどを参照してください。

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います。必要に応じて別途CLIガイドなどを参照ください。

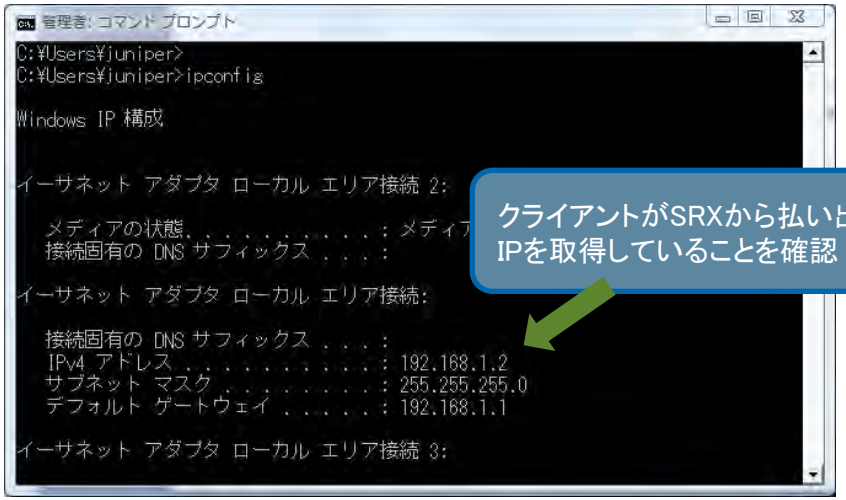
Chapter1. Basic Setup

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
DCHP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。



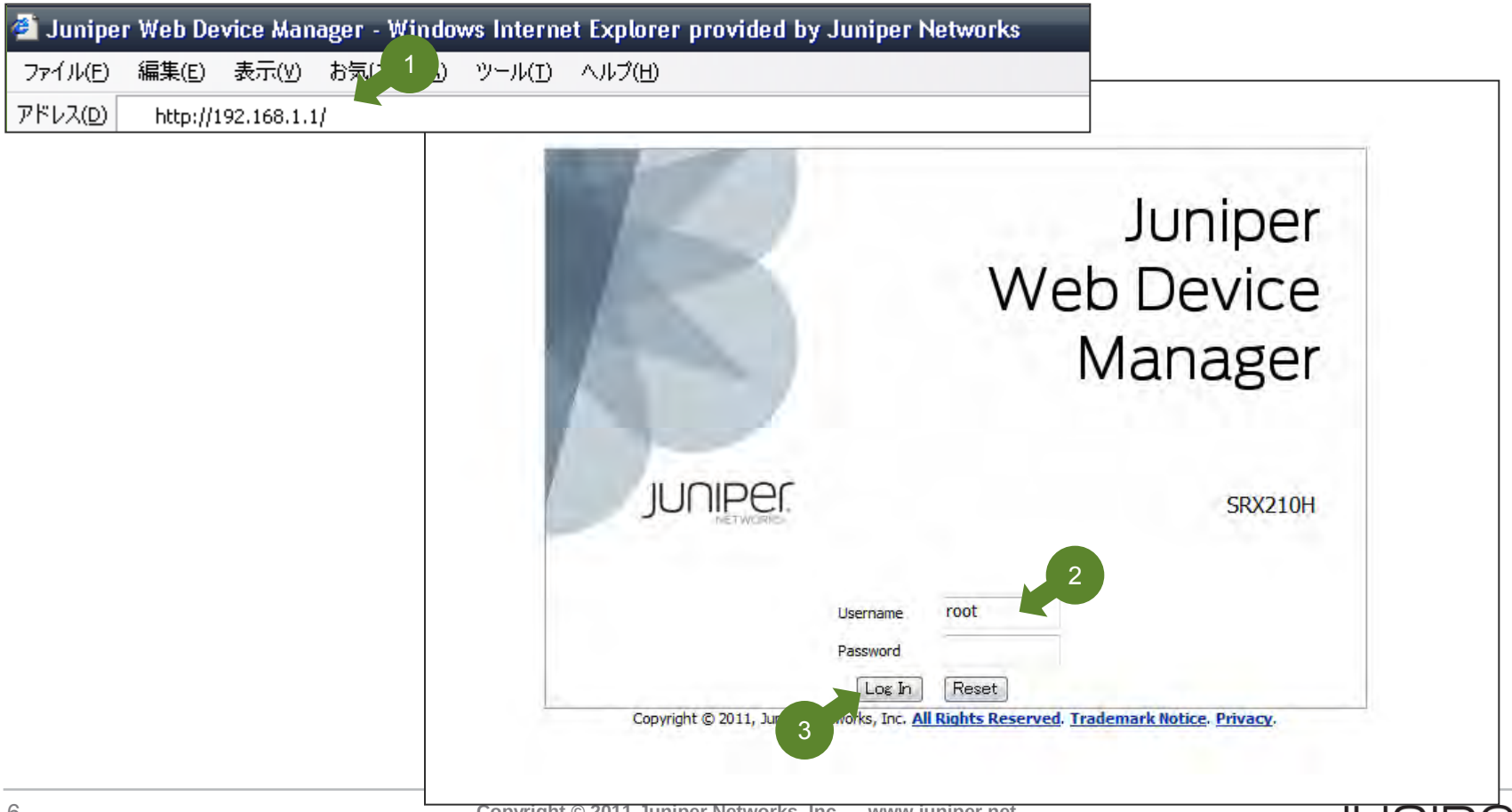
DHCPクライアントをTrust Zoneの
インタフェースに接続



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

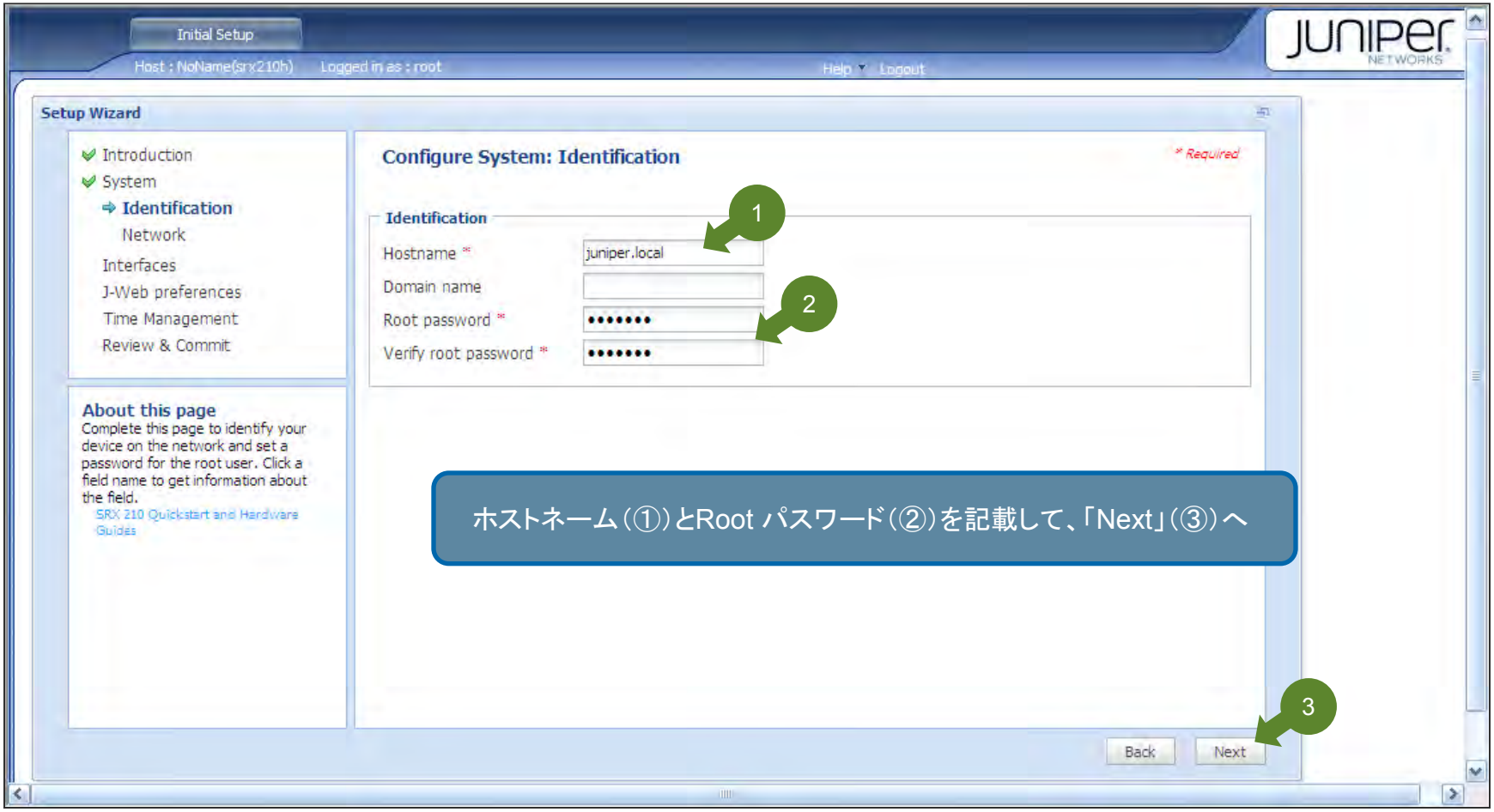
Step1：SRXのGUI設定画面へのログイン

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）。

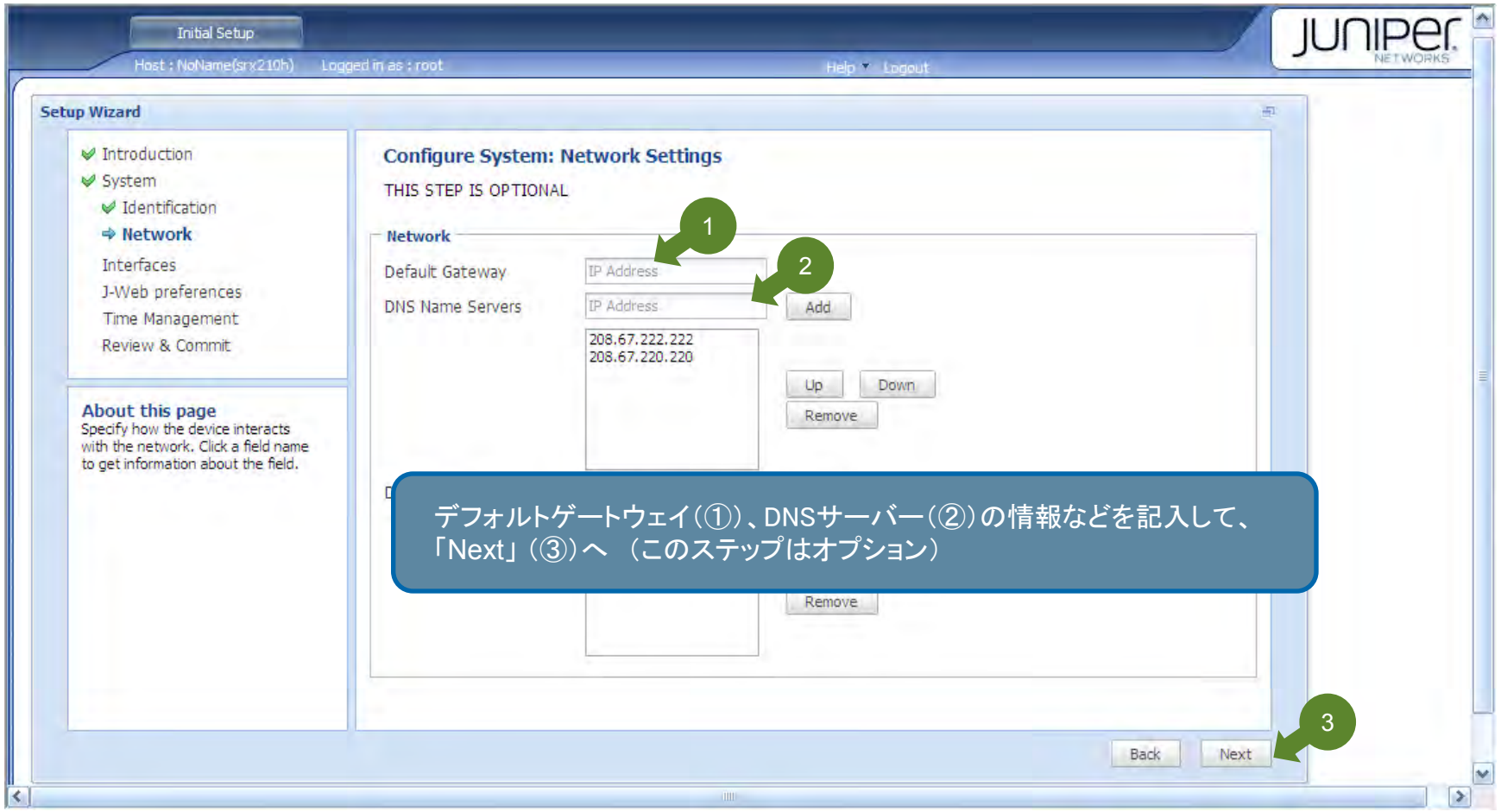


Step2：初期セットアップウィザードの開始

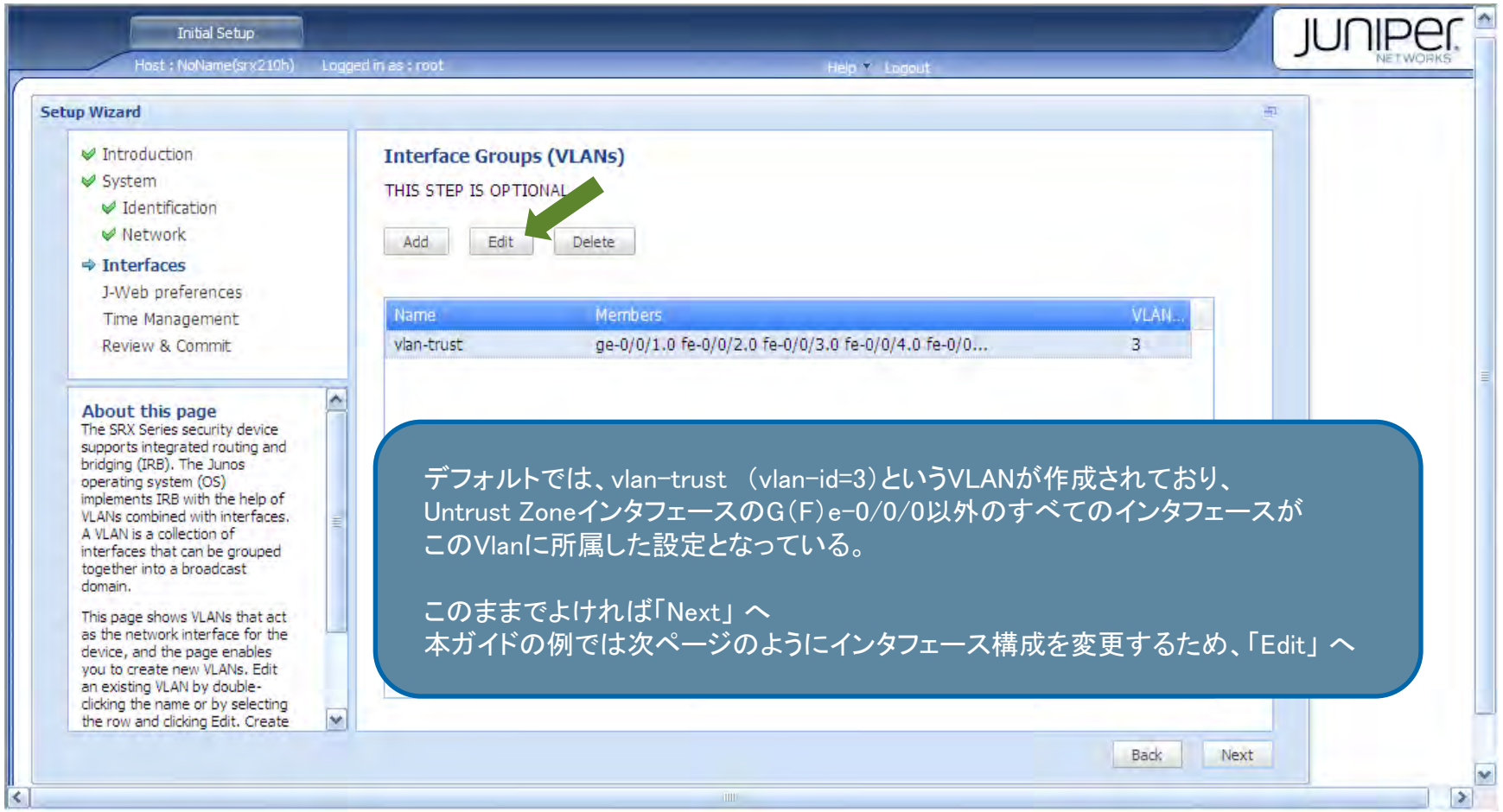
Step3：Identificationの設定



Step4 : Networkの設定



Step5-1：VLANの設定

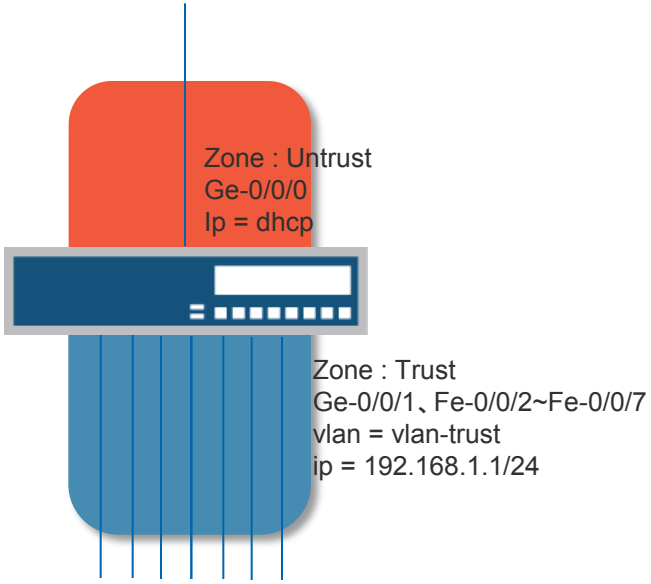


デフォルトでは、vlan-trust （vlan-id=3）というVLANが作成されており、
Untrust ZoneインタフェースのG（F）e-0/0/0以外のすべてのインタフェースが
このVlanに所属した設定となっている。

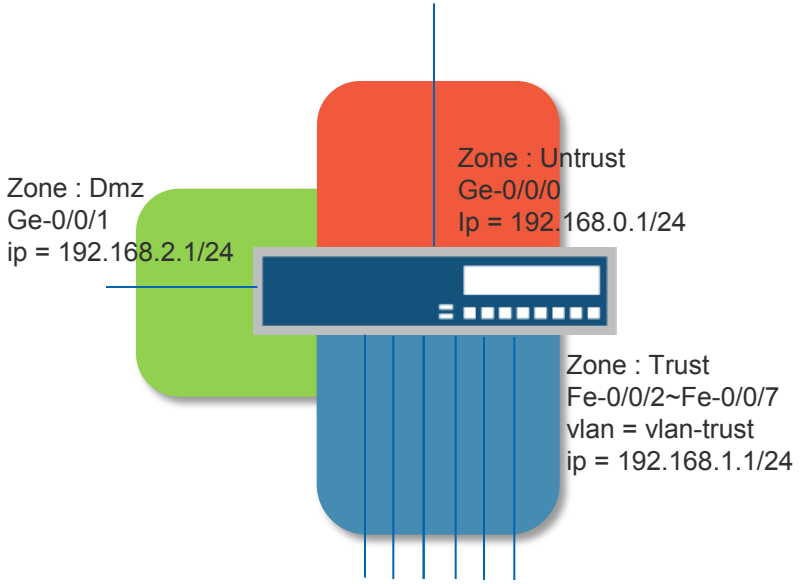
このままでよければ「Next」へ
本ガイドの例では次ページのようにインタフェース構成を変更するため、「Edit」へ

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）

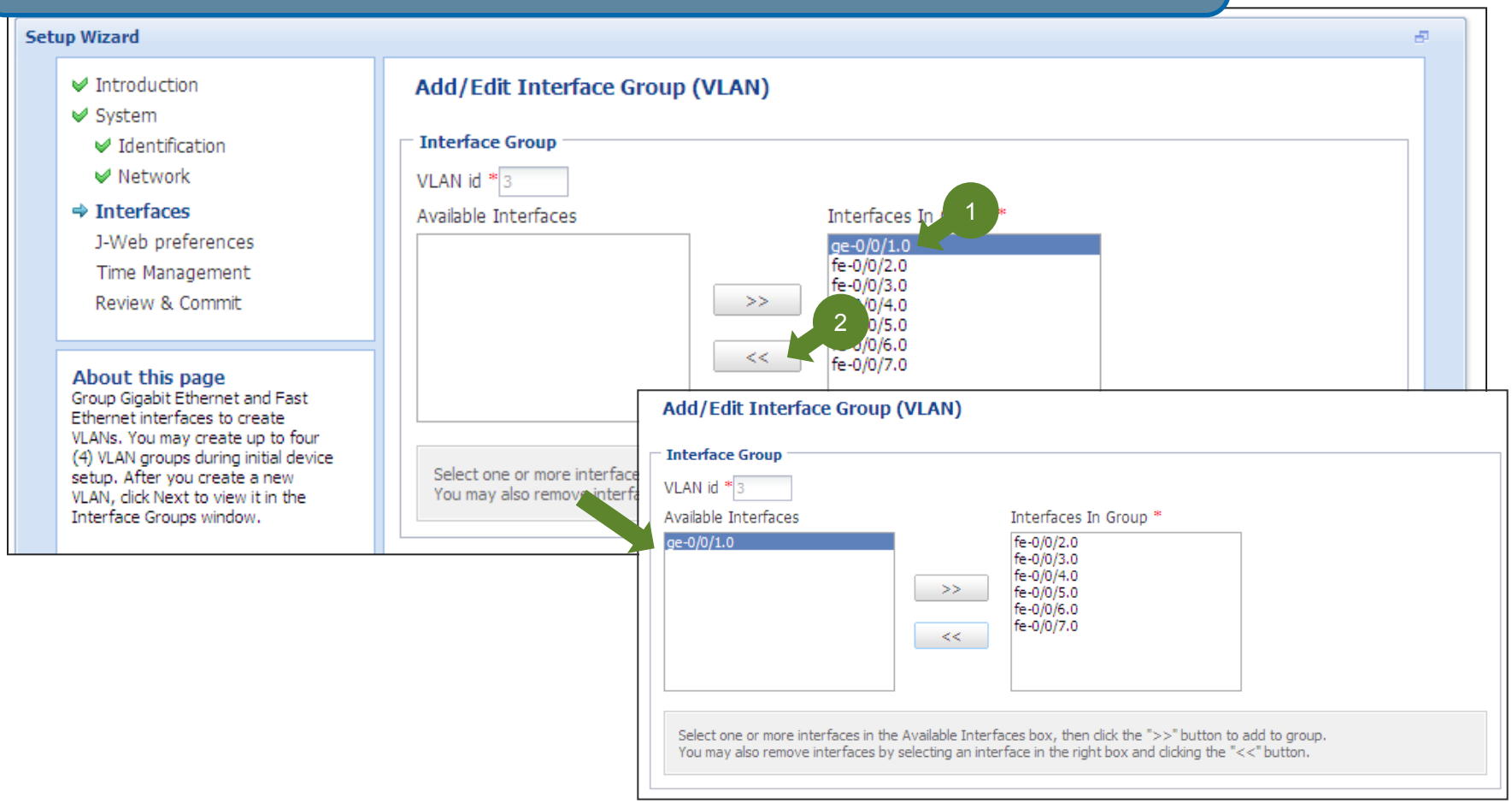


このガイドで構成するサンプル設定構成



Step5-2：VLANの設定

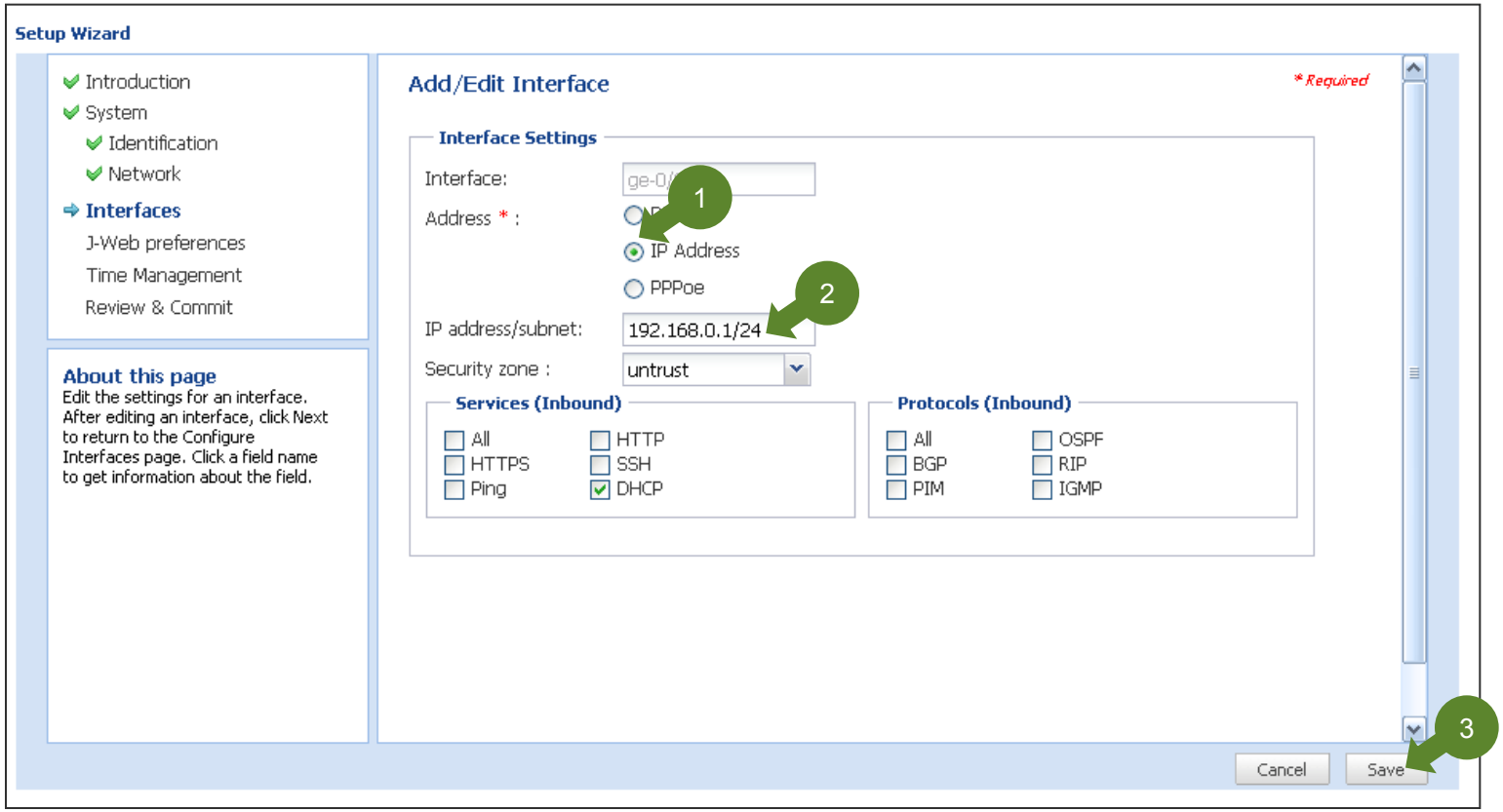
「Edit」を投下すると、vlan-trust　に設定されているインタフェース一覧が表示される。
ここから設定を外したいインタフェースを選んで（①）、「<<」ボタンを投下し（②）、「Save」して「Next」へ



Step6-1：Interfacesの設定：アドレスの設定

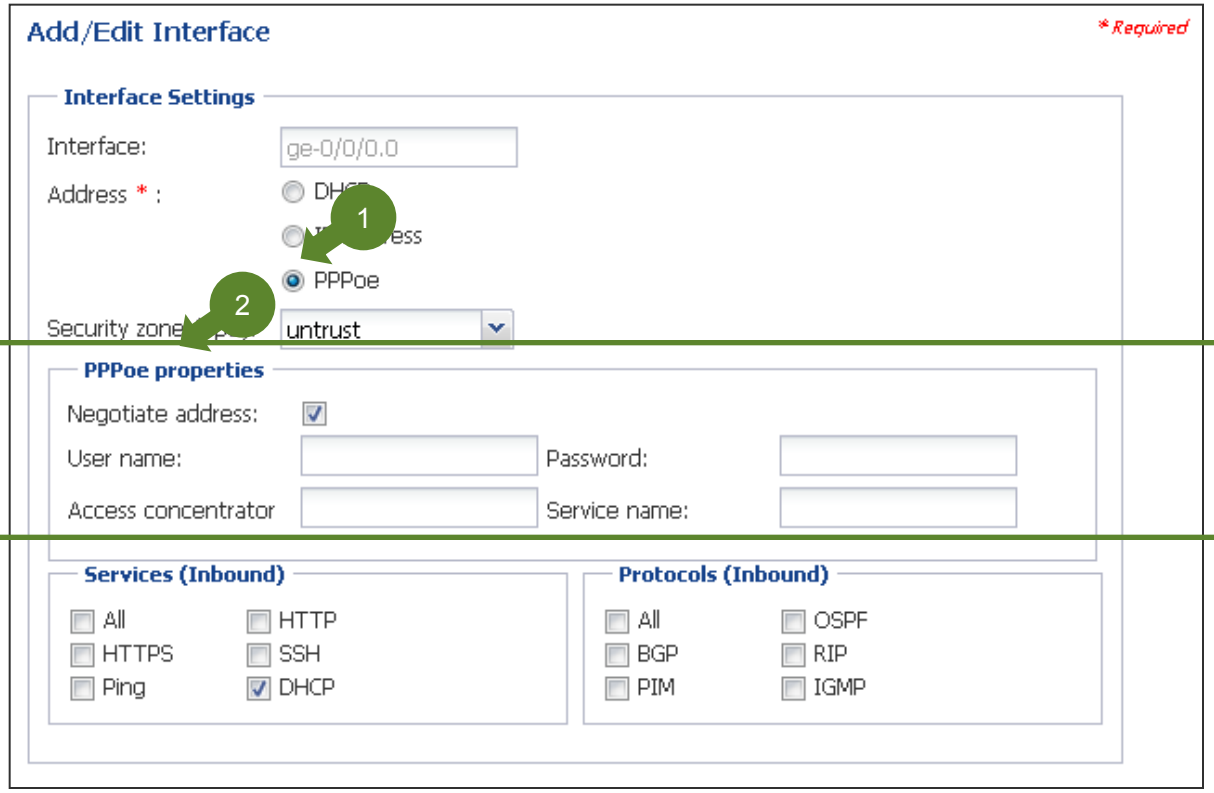
Step6-2：Interfacesの設定：アドレスの設定

「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

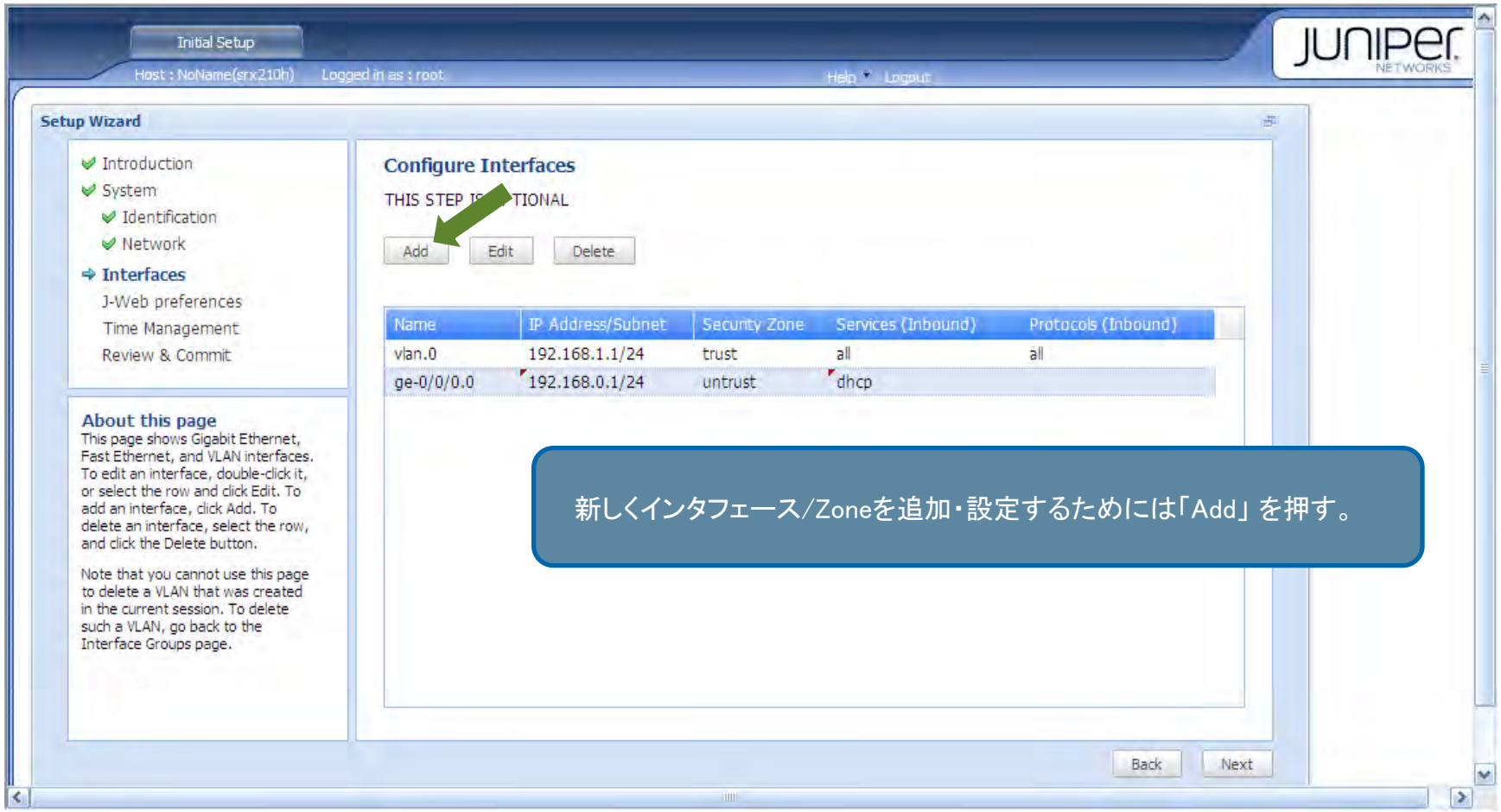


Step6：Interfacesの設定（PPPoEの場合：サンプル）

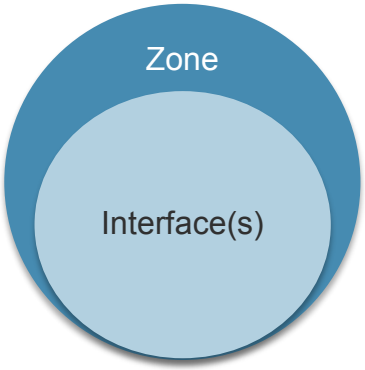
本ガイドでの構成例では説明しないが、PPPoE 接続の場合は、選択すると（①）設定項目が現れるのでProperties 設定を投入して（②）、「Save」へ



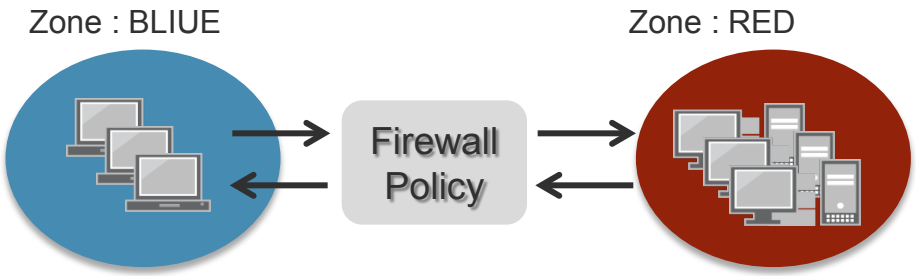
Step6-3：Interfacesの設定：インタフェースとZoneの追加

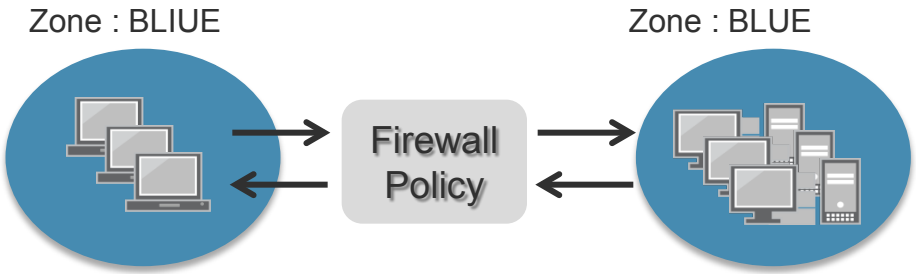


Security Zoneについて



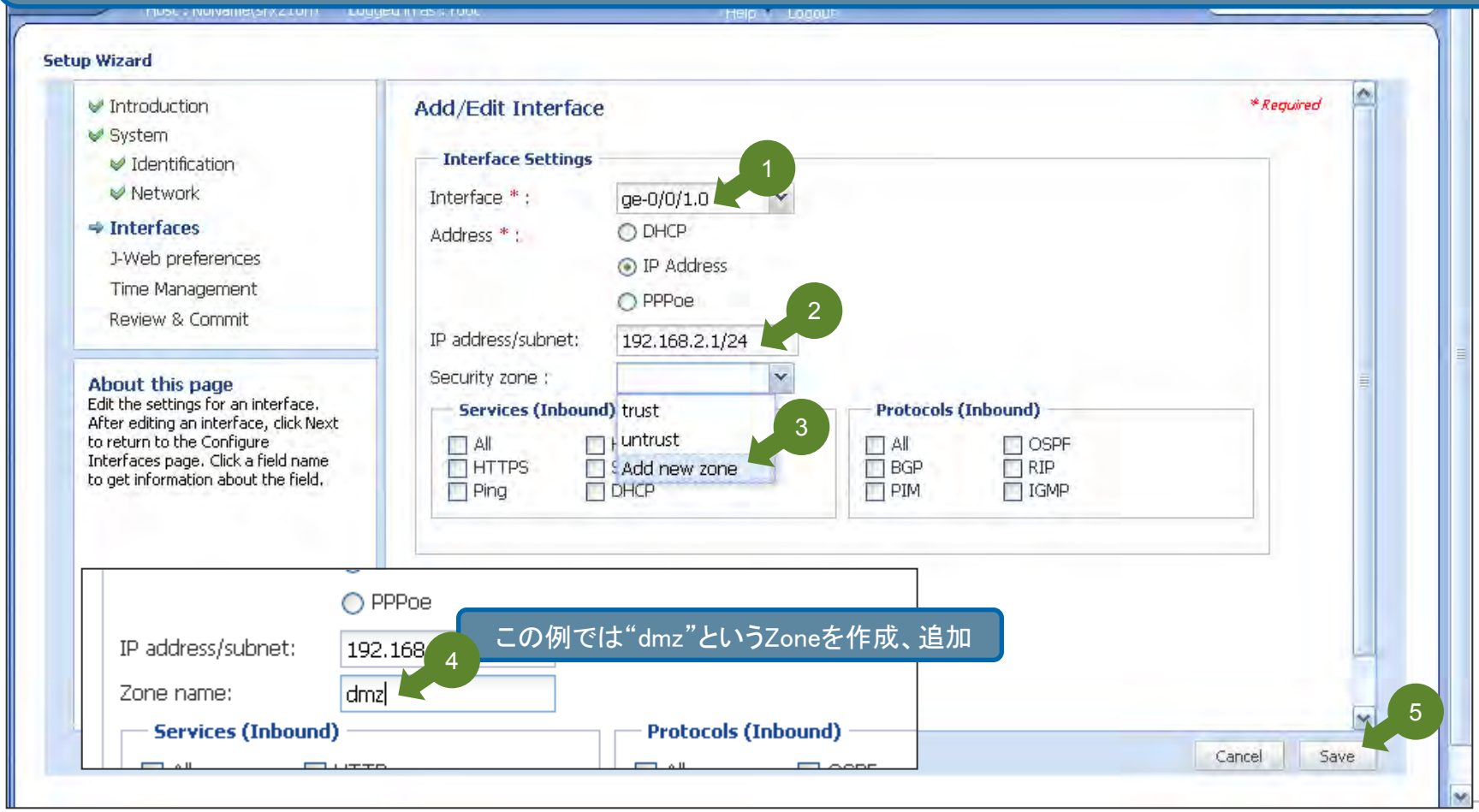
セキュリティゾーンとは、インタフェース群に割り当てる仮想的なグループです。
SRXではこのセキュリティゾーンを使用してトラフィックを制御します。
異なるゾーン間で通信されるトラフィック、またはゾーン内の別インタフェース間で
通信されるトラフィックがファイアウォールポリシーにて制御される通信対象となります。



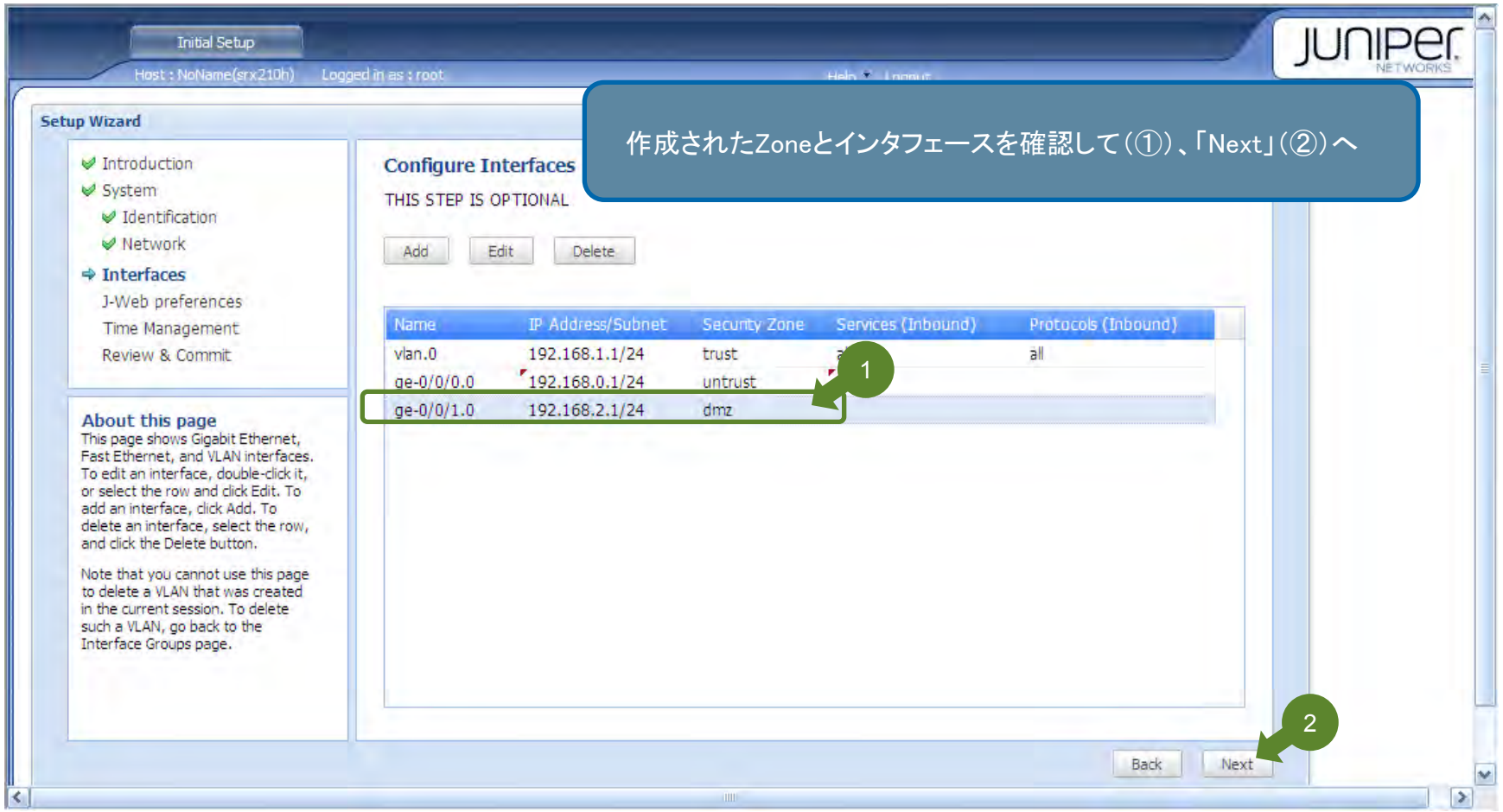


Step6-4：Interfacesの設定：インタフェースとZoneの追加

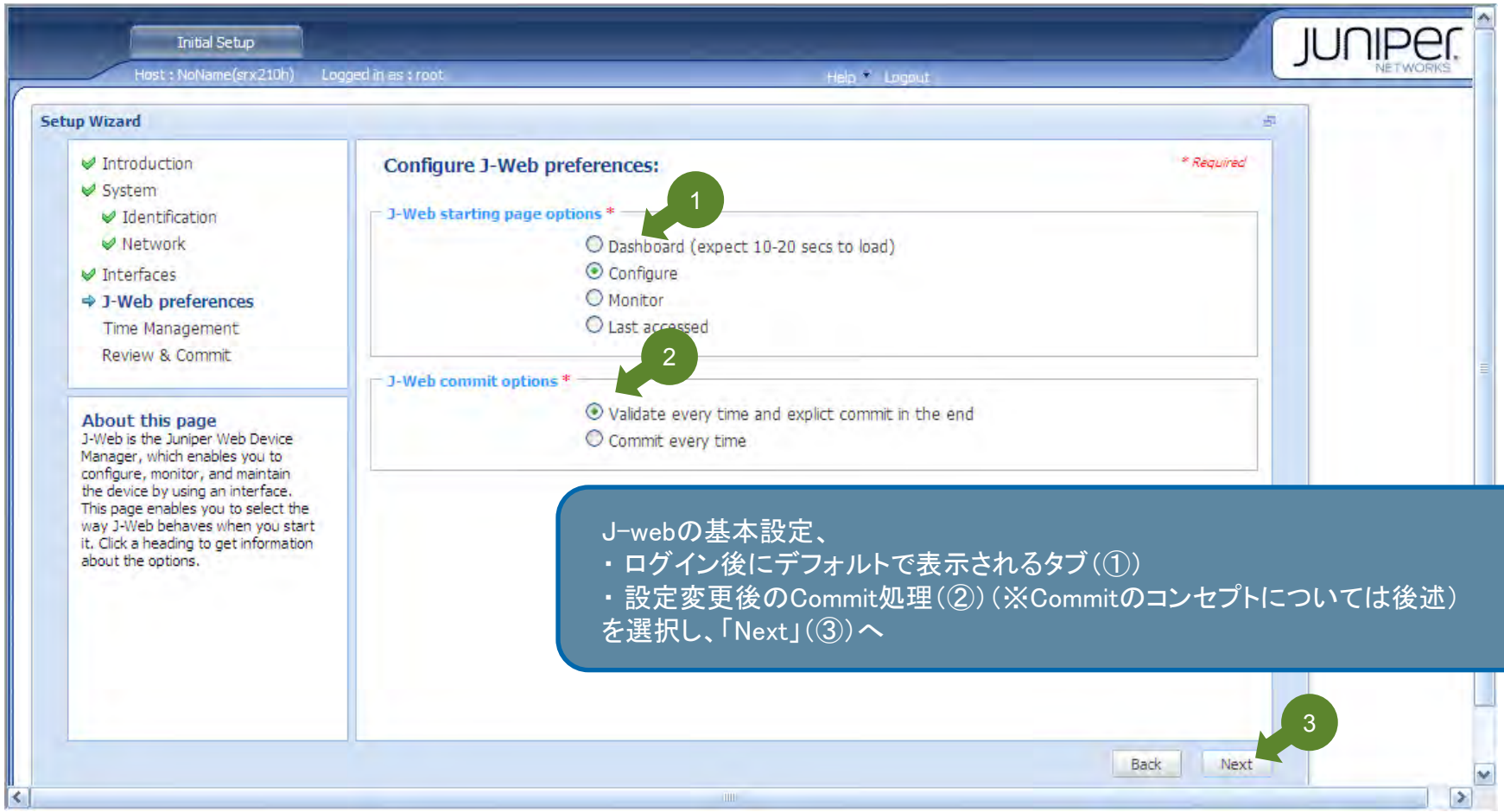
インタフェースのプルダウンから追加したいインタフェースを指定して（①）、アドレスを設定する（②）、
その際Zoneを新しく作成したい場合にはプルダウンから「Add new zone」を選択して（③）Zone名を記入し（④）、「Save」（⑤）



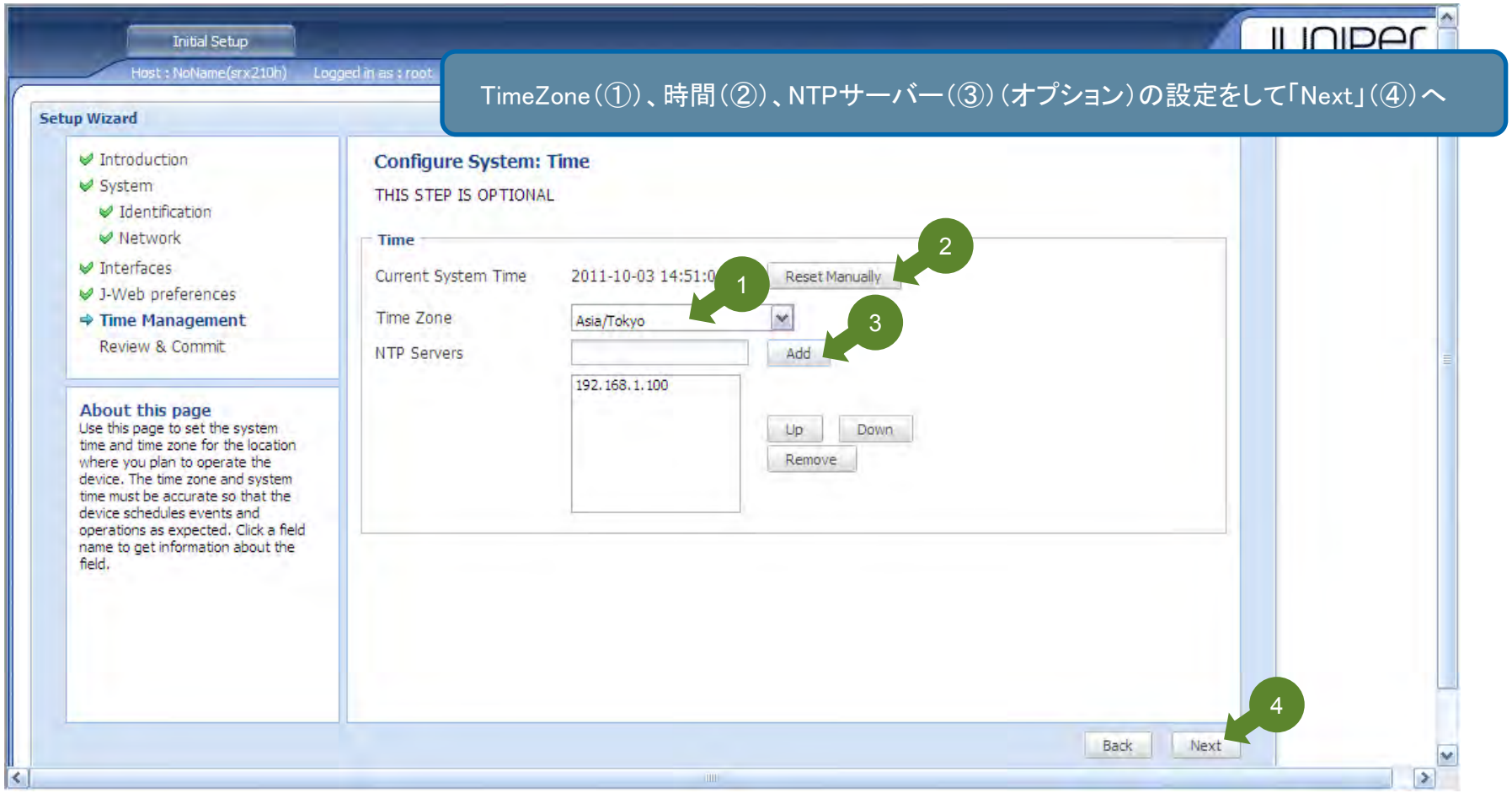
Step6-5：Interfacesの設定：インタフェースとZoneの追加



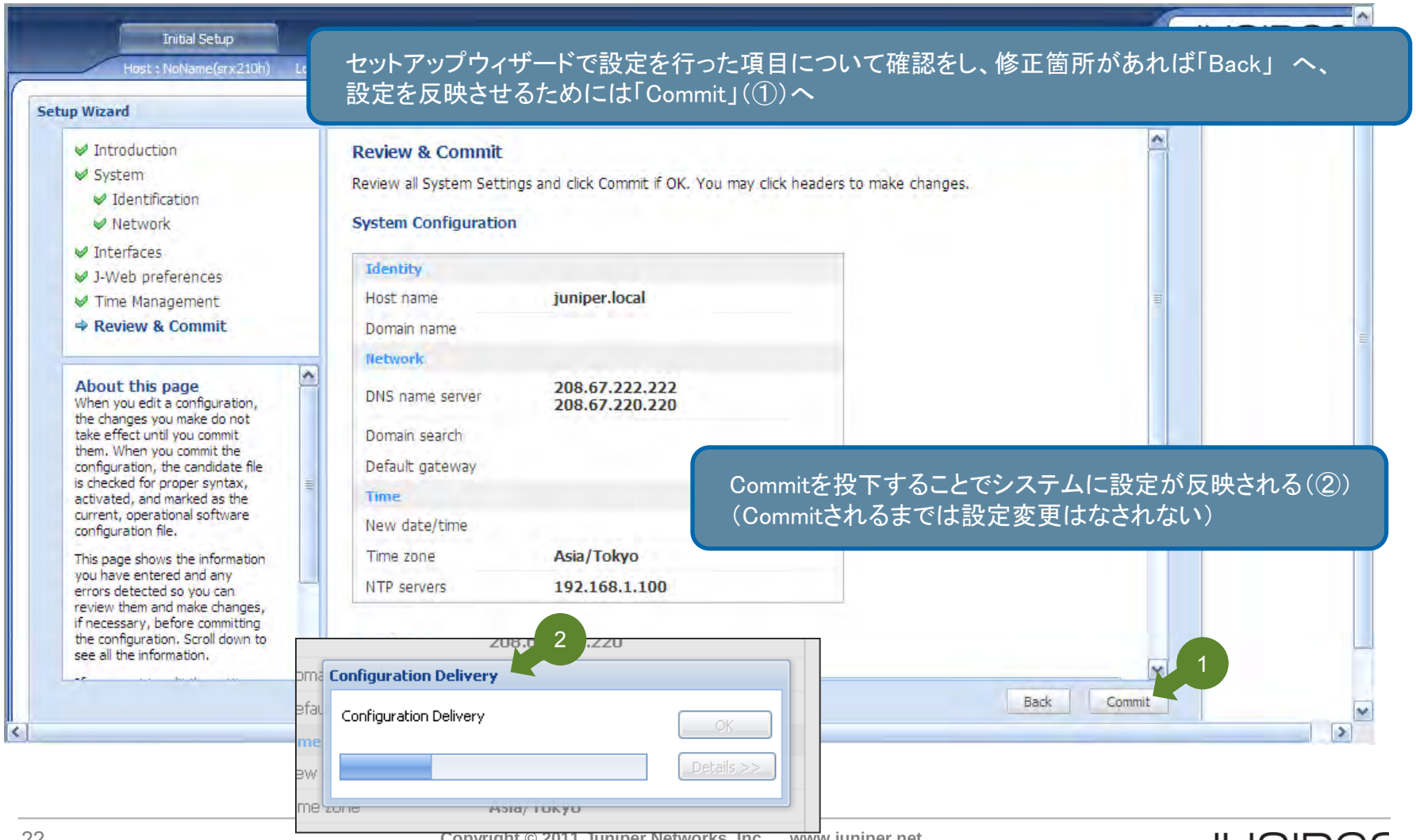
Step7：J-webの設定



Step8：時間・NTPの設定



Step9：設定の確認、反映



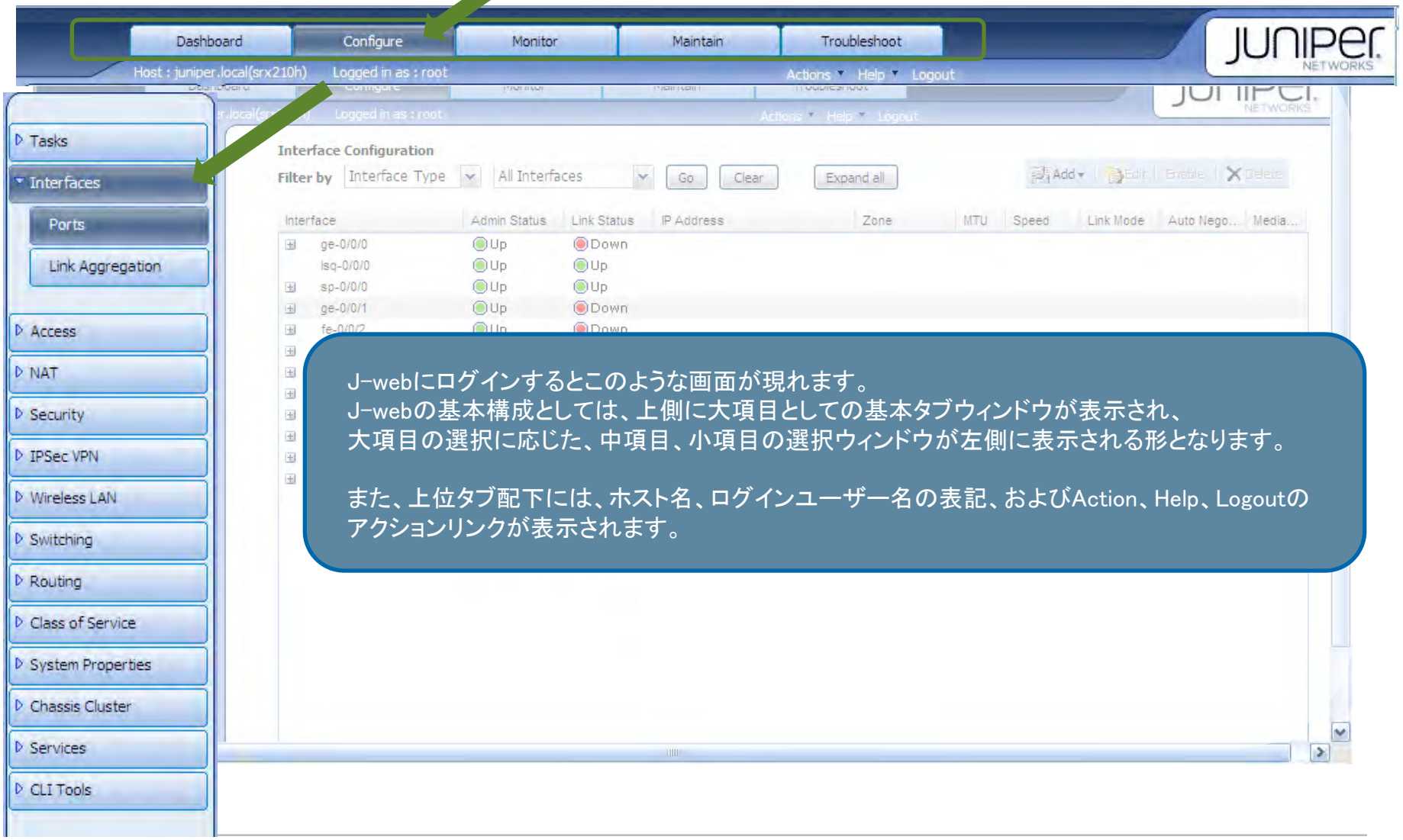
セットアップウィザードで設定を行った項目について確認をし、修正箇所があれば「Back」 へ、
設定を反映させるためには「Commit」（①）へ

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）

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）

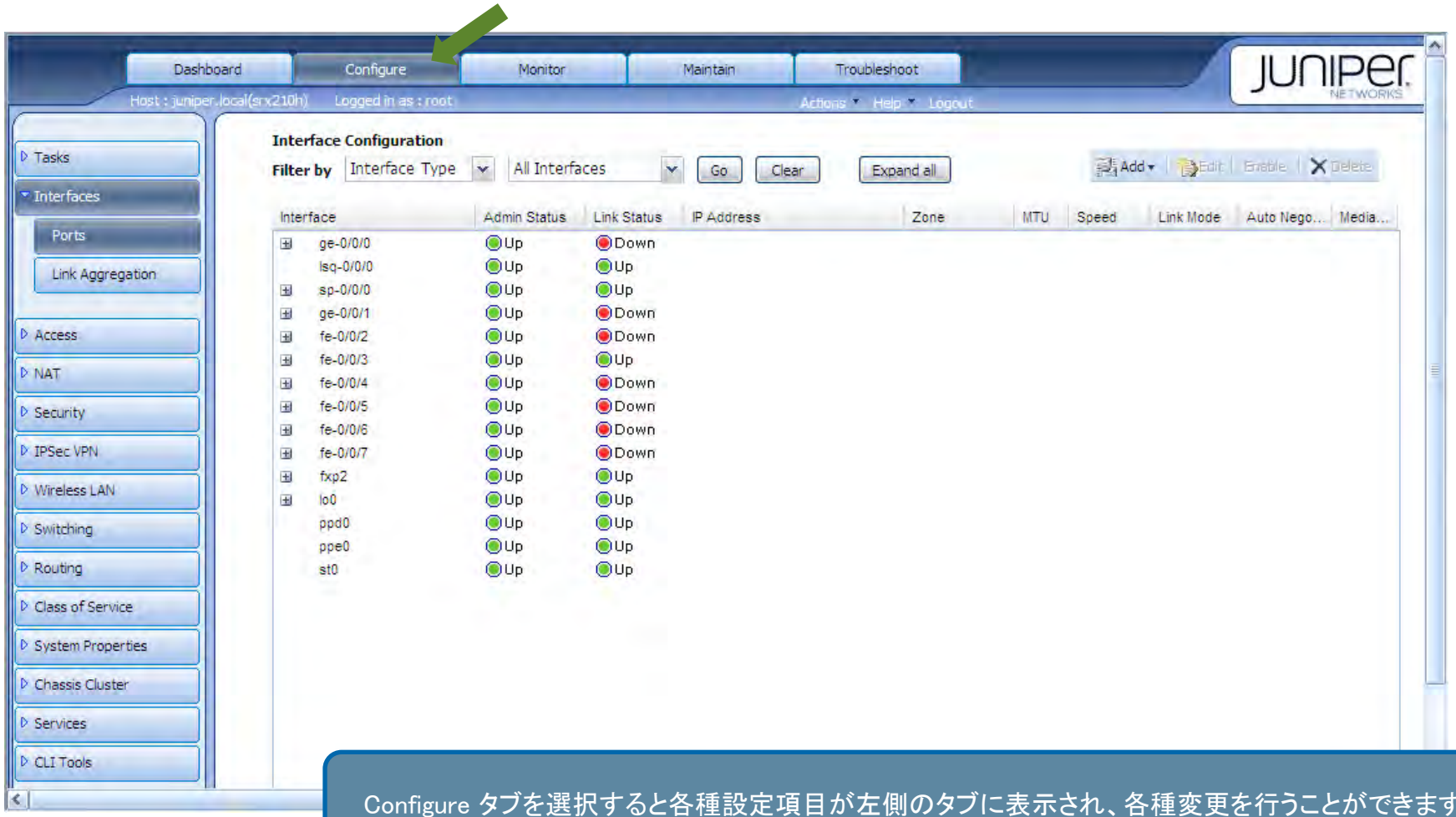
Step10：J-webの確認：基本ウィンドウ



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



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。

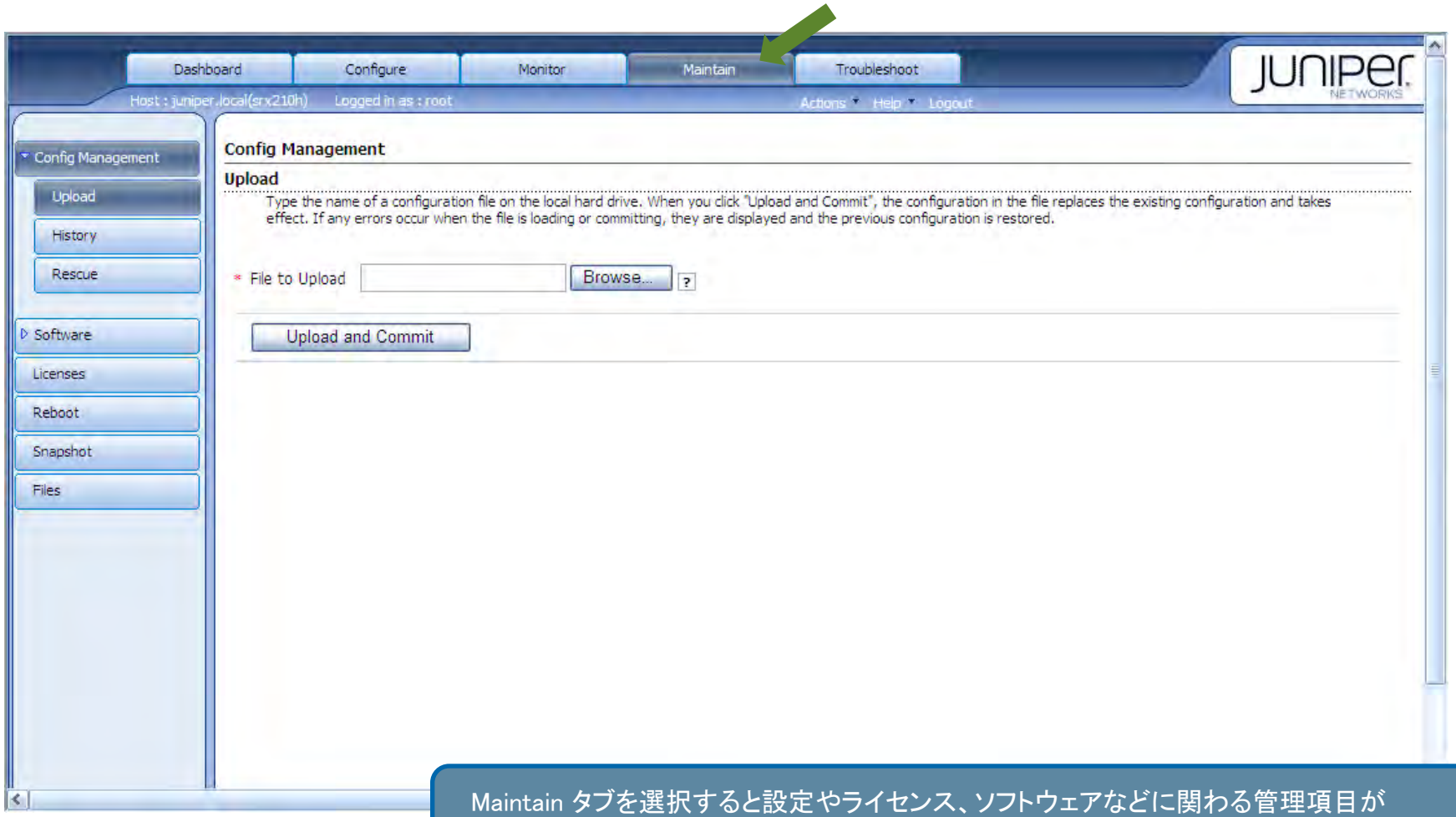
Step10：J-webの確認：Dashboard タブ

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

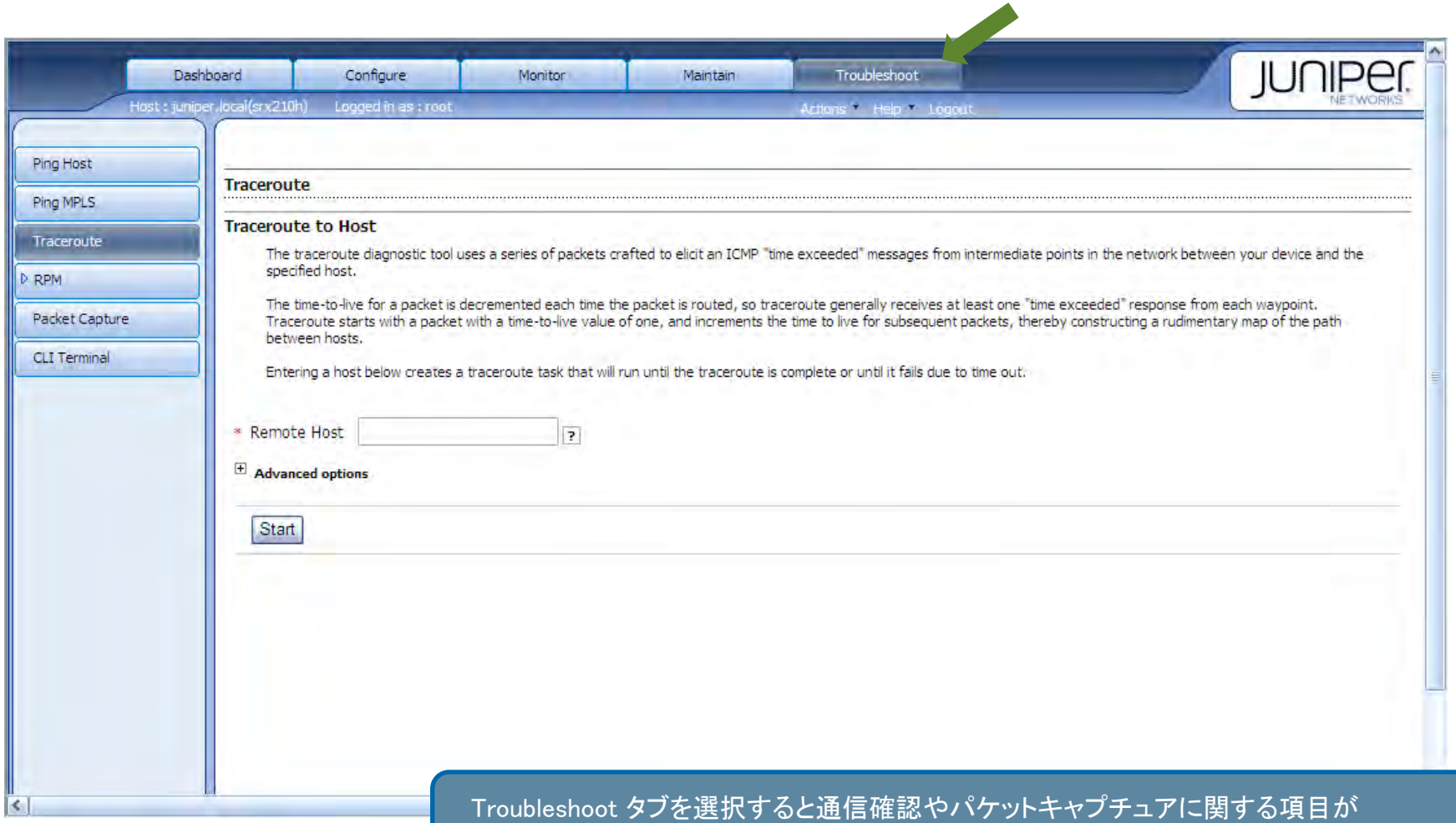
Monitor タブを選択すると確認が可能な項目が左側のタブに表示され、選択することで各種状態の確認が可能です。

Step10：J-webの確認：Maintain タブ



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

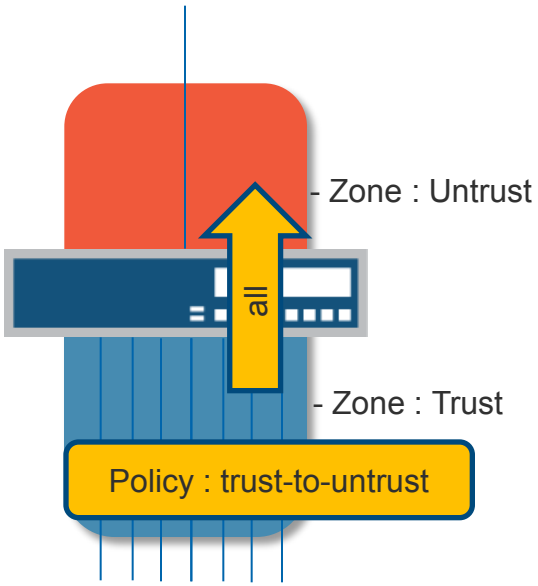


Troubleshoot タブを選択すると通信確認やパケットキャプチュアに関する項目が
左側のタブに表示され、障害時などにおける状況確認を行うことができます。

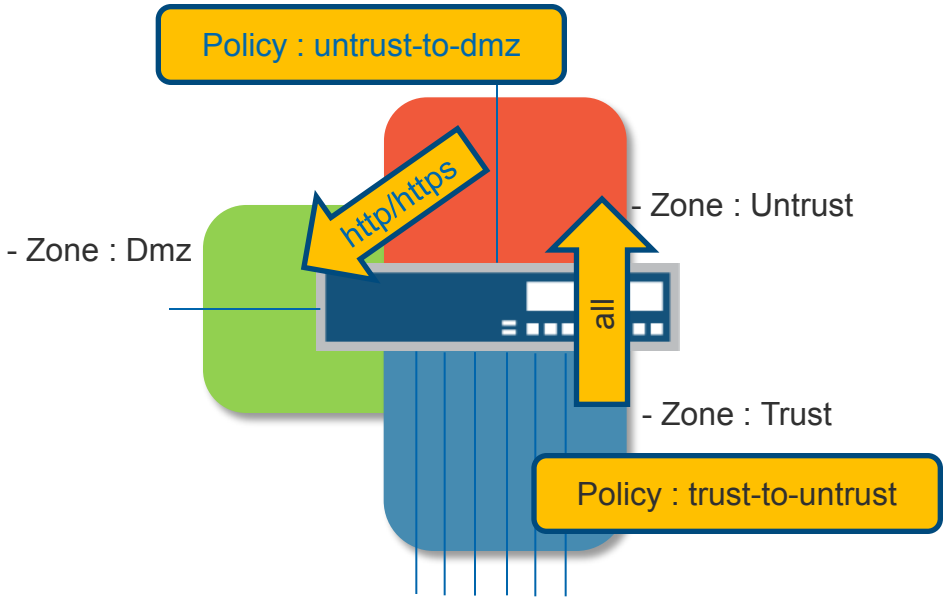
Chapter2. Firewall Policy

このガイドで構築するファイアウォールポリシー構成

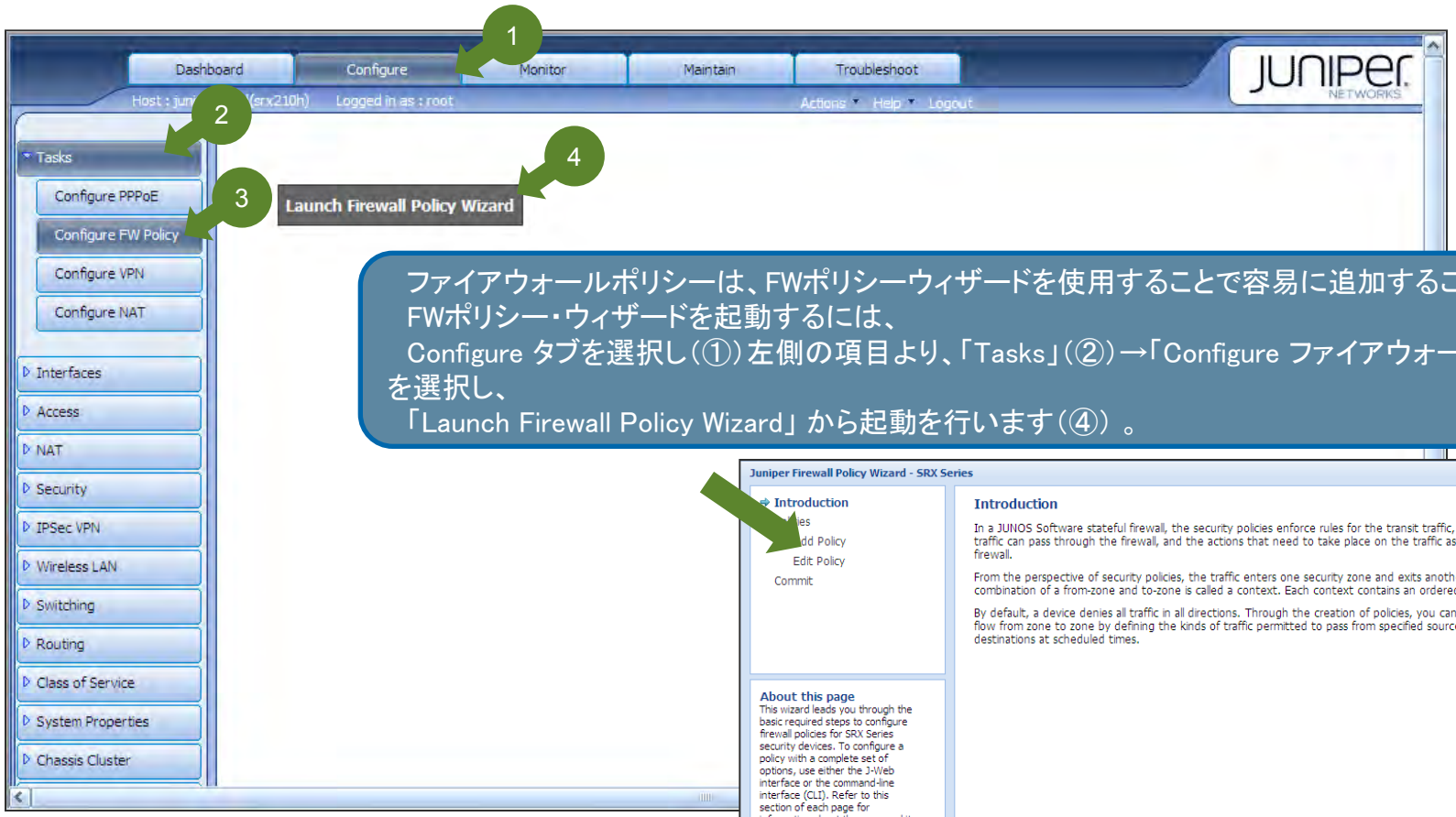
工場出荷時におけるファイアウォールのポリシー設定



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



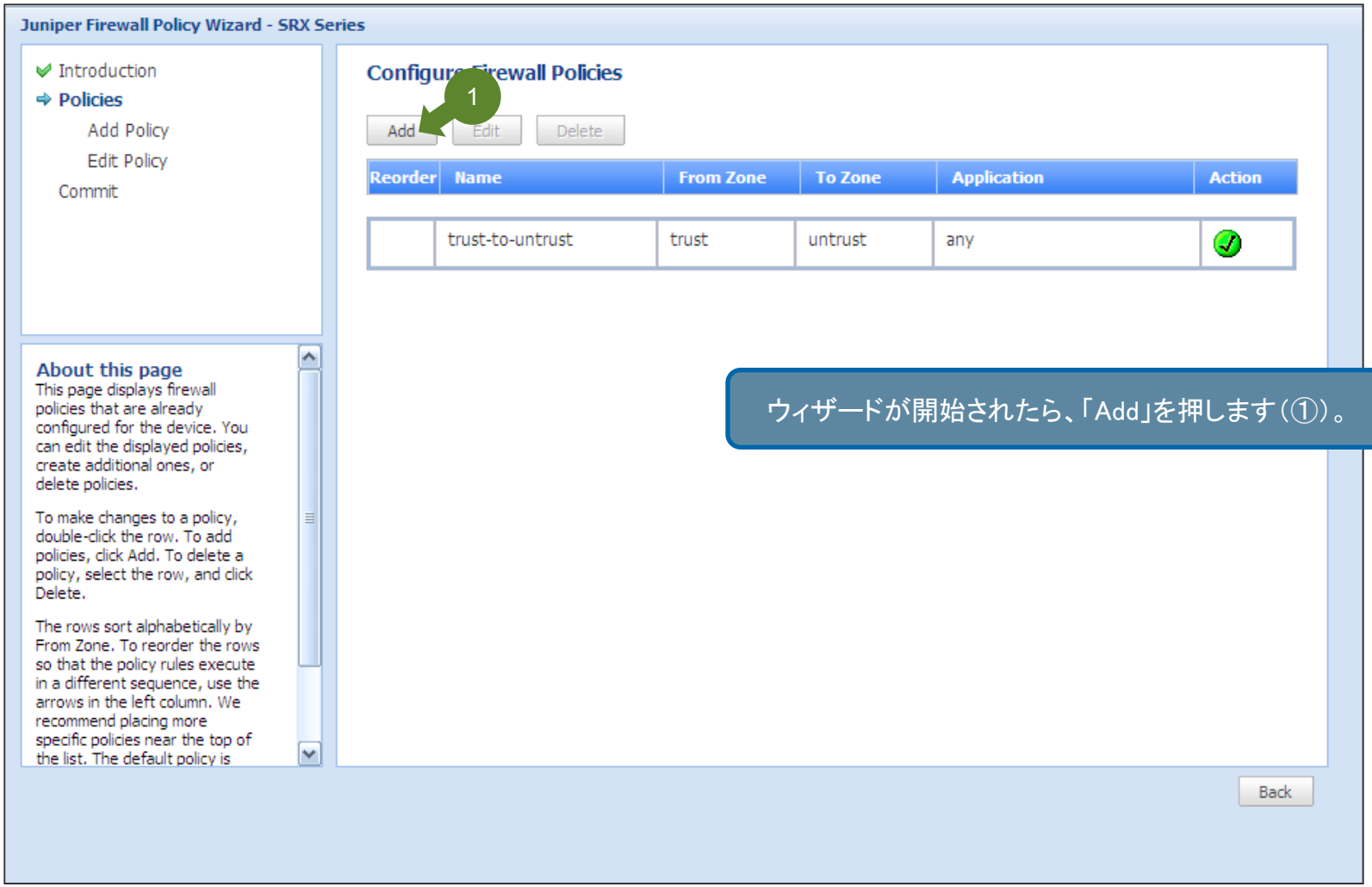
Step1：ファイアウォールポリシー・ウィザードの起動



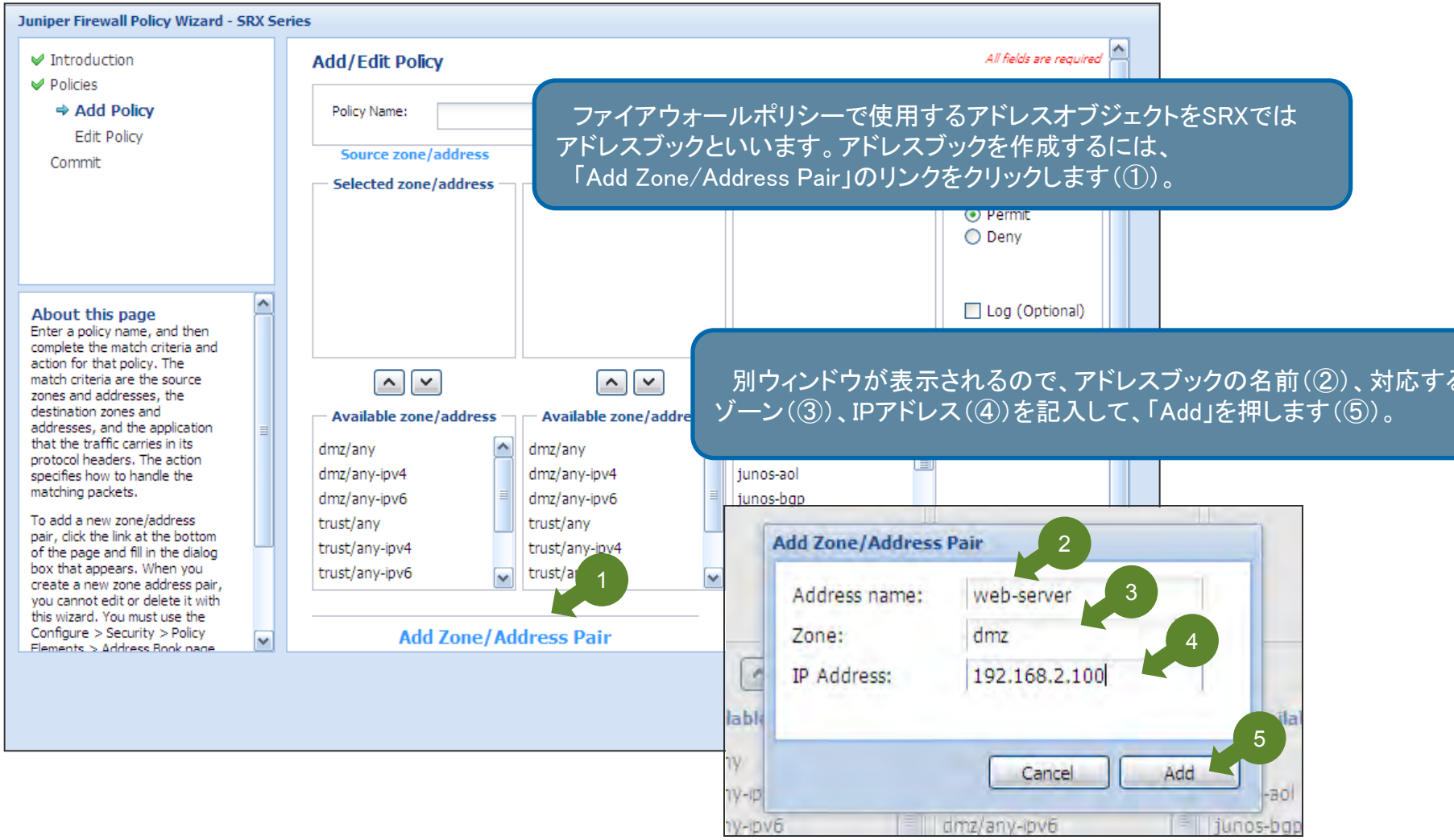
ファイアウォールポリシーは、FWポリシーウィザードを使用することで容易に追加することが可能です。
FWポリシー・ウィザードを起動するには、
Configure タブを選択し（①）左側の項目より、「Tasks」（②）→「Configure ファイアウォールポリシー」（③）を選択し、
「Launch Firewall Policy Wizard」から起動を行います（④）。

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）。

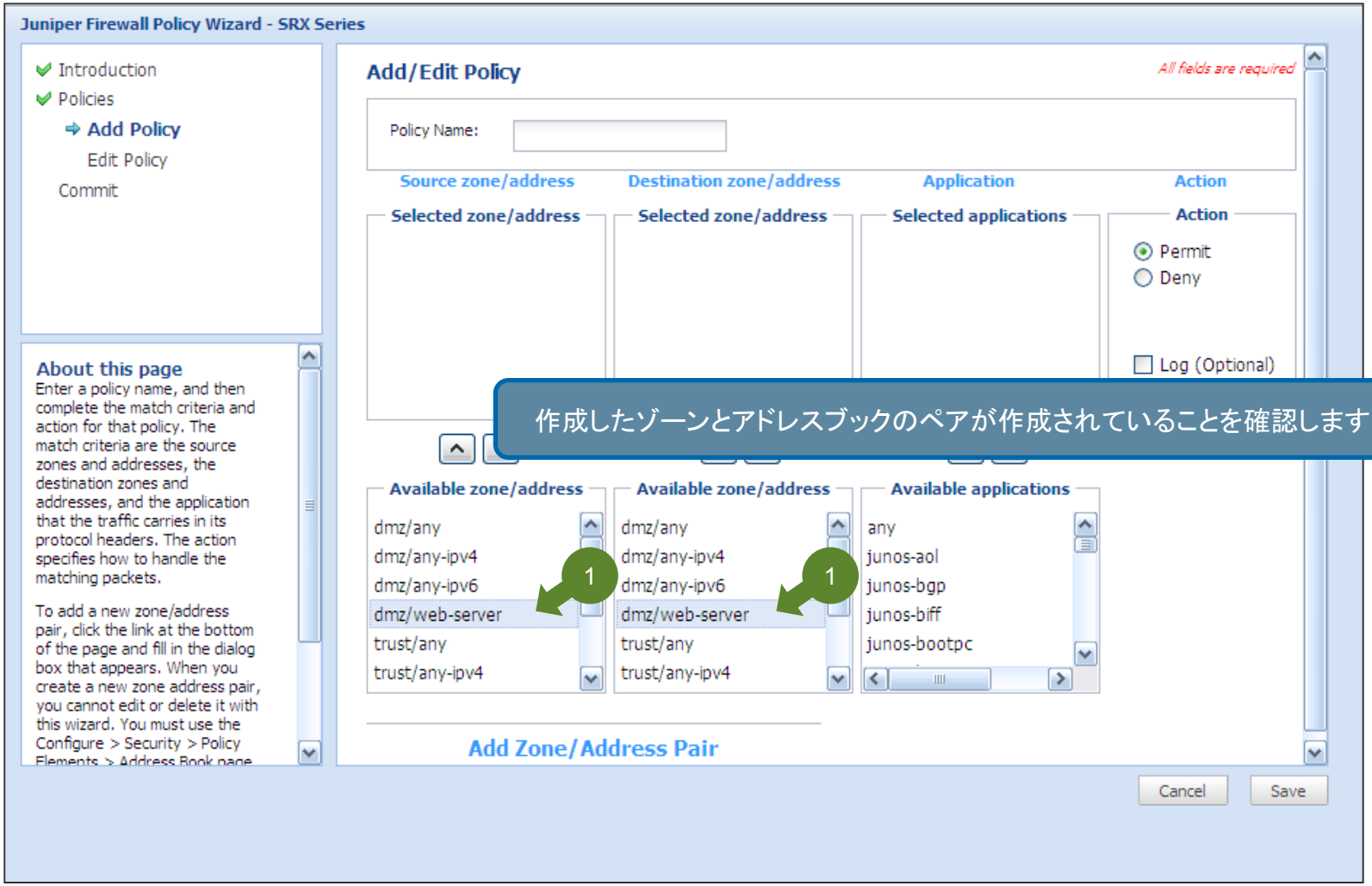
Step2：ファイアウォールポリシー の追加



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

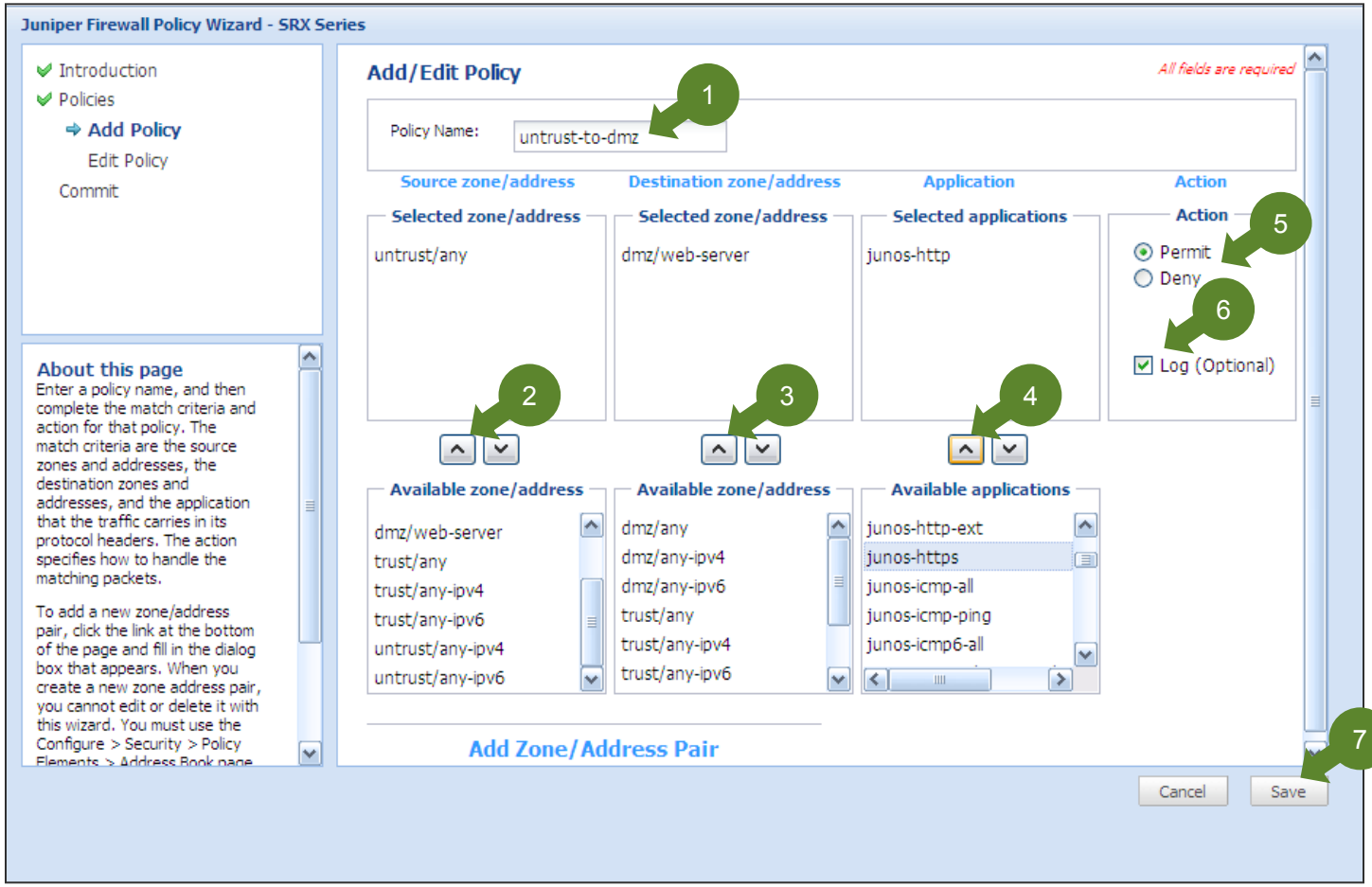


Step3-2：ファイアウォールポリシー の追加 ー アドレスブック の作成



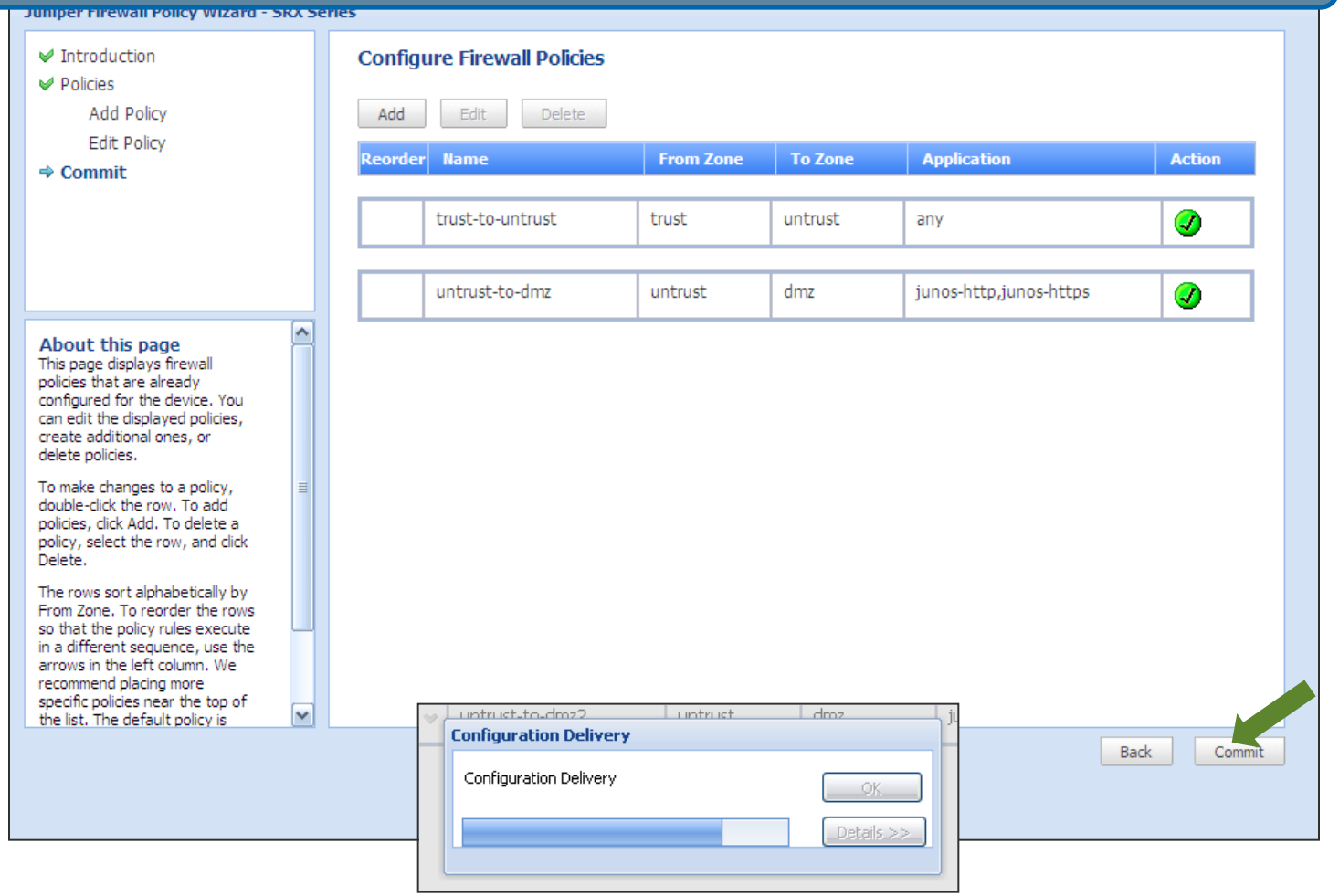
Step4-1：ファイアウォールポリシー の追加 ー ファイアウォールポリシーの設定

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。

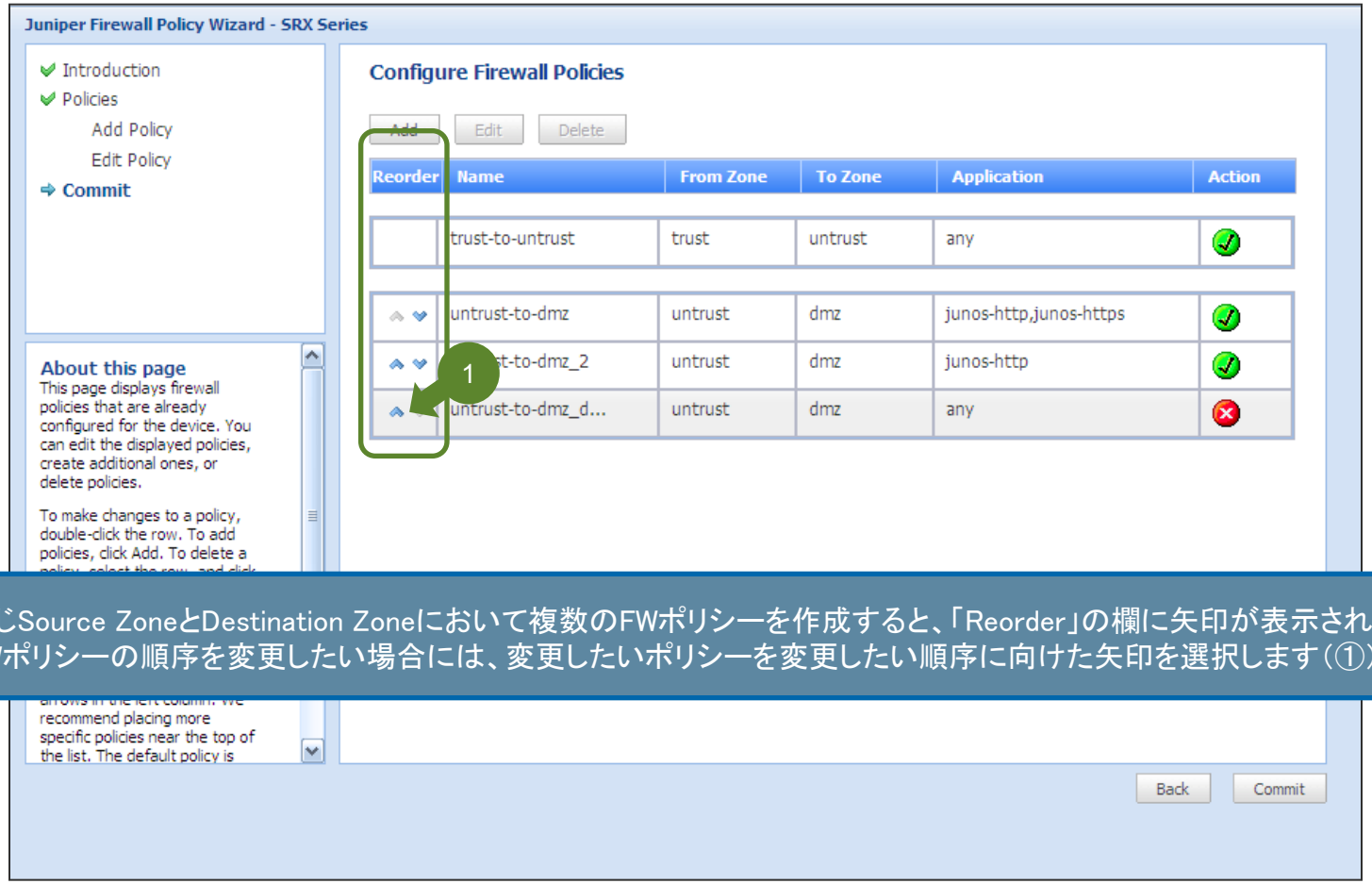


Step4-2：ファイアウォールポリシー の追加 ー ファイアウォールポリシーの設定

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。

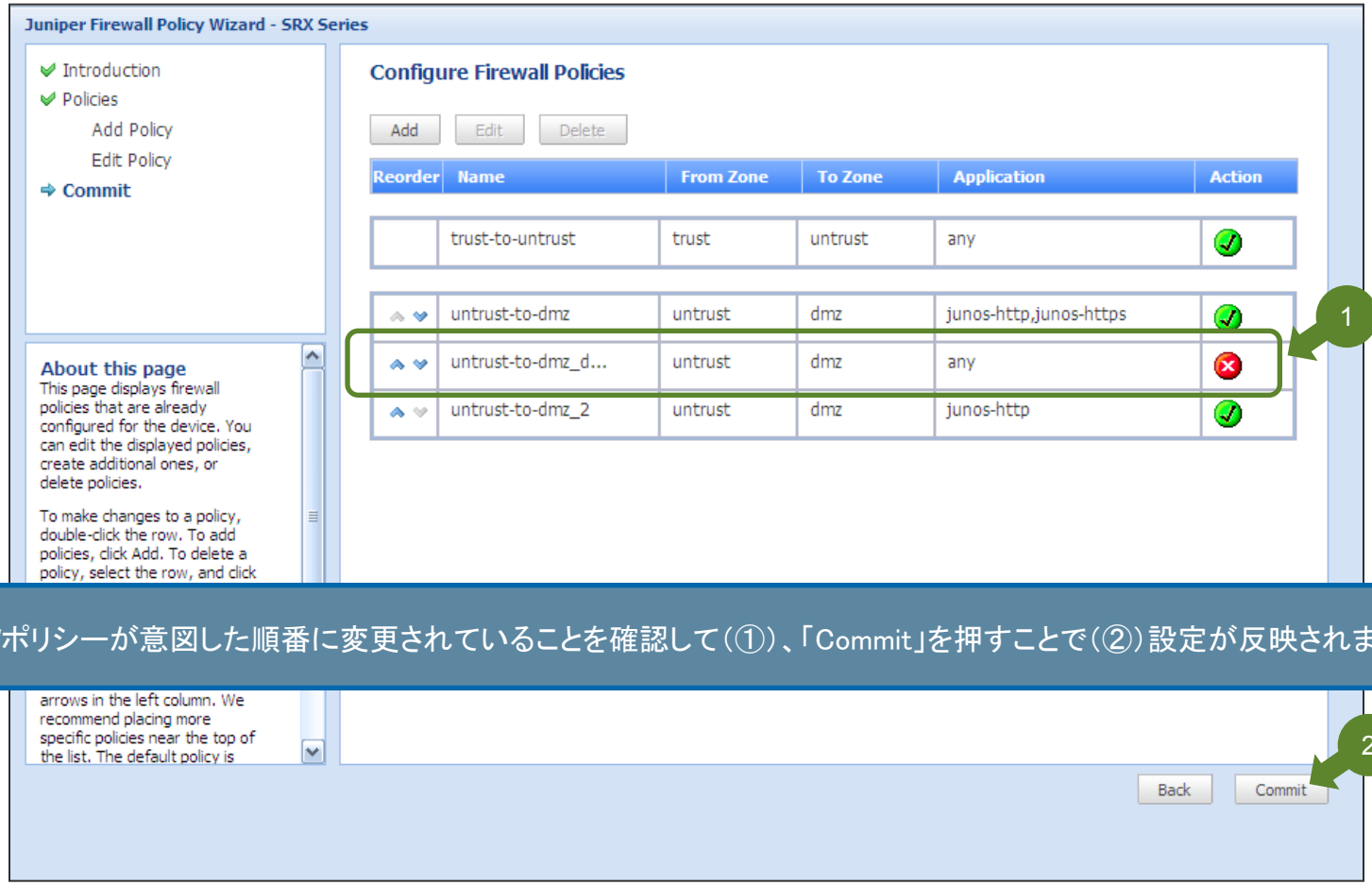


Step5-1：ファイアウォールポリシー の追加
ー ファイアウォールポリシーの順序設定



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
ー ファイアウォールポリシーの順序設定

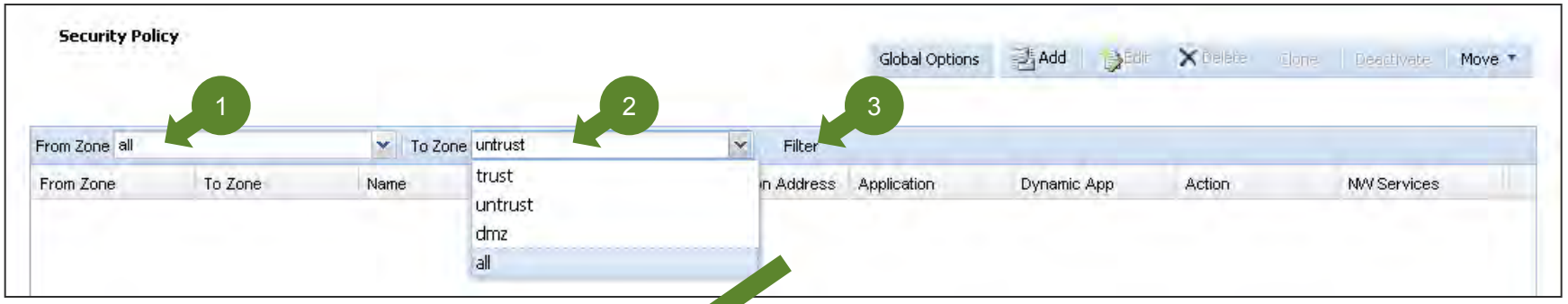


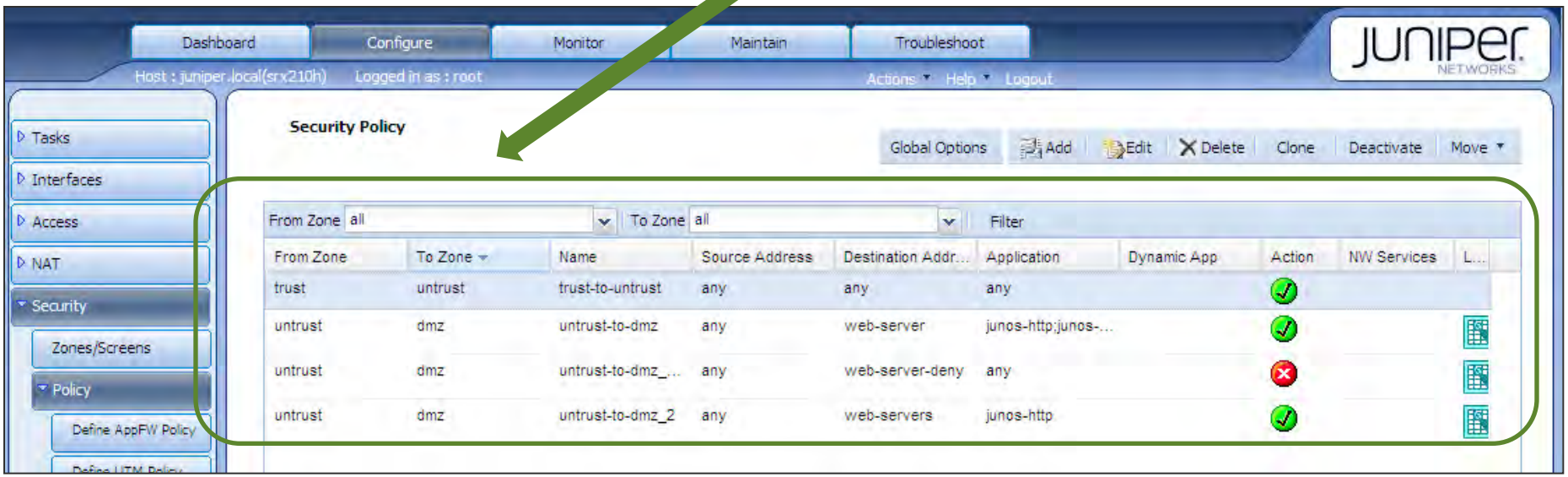
FWポリシーが意図した順番に変更されていることを確認して（①）、「Commit」を押すことで（②）設定が反映されます。

Step6-1：ファイアウォールポリシーの表示

Step6-2：ファイアウォールポリシーの表示

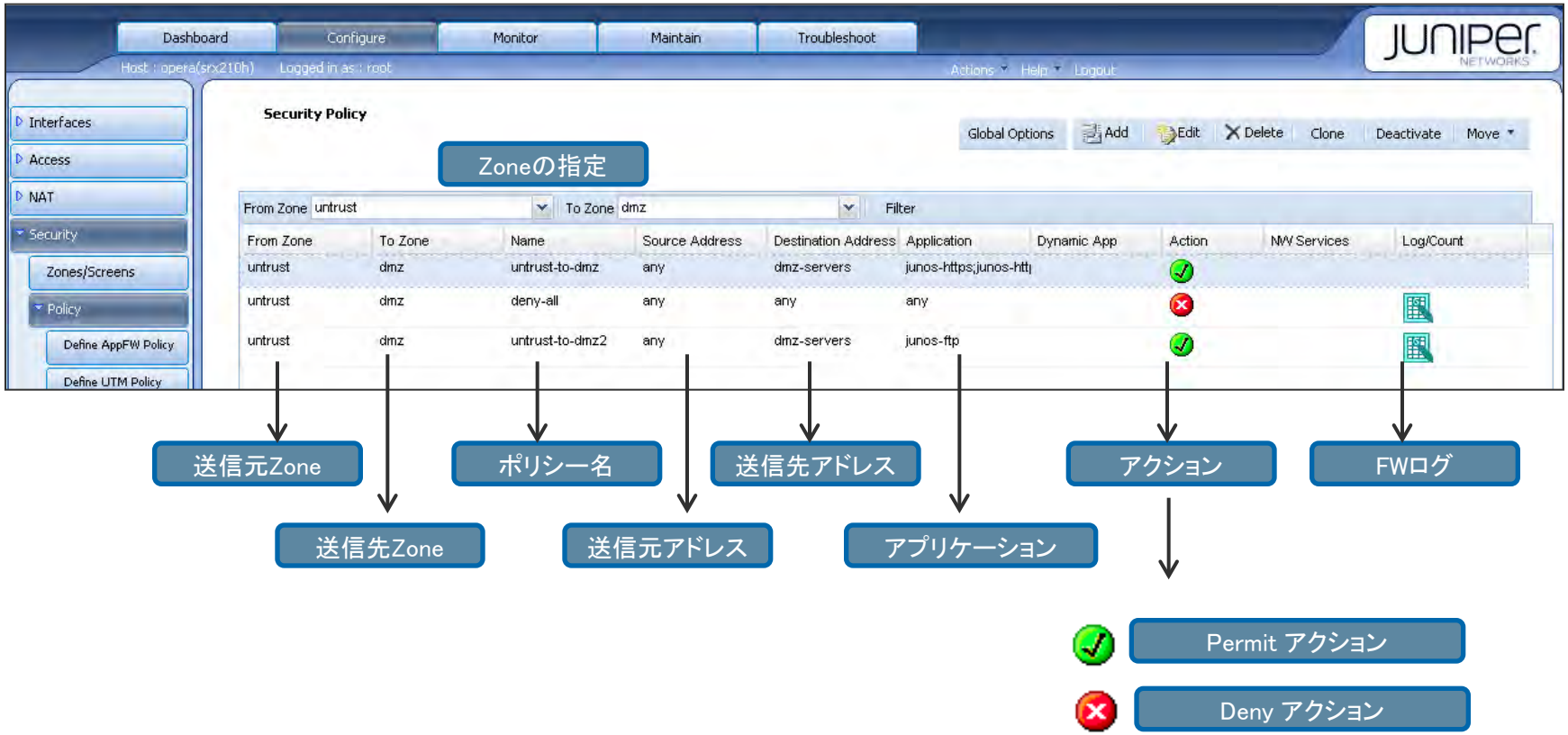
作成したポリシーを表示、確認するためにはポリシー表示ウィンドウ上部にあるフィルターから
表示させたいFrom/To Zoneを選択（①②）して「Filter」（③）を押します。





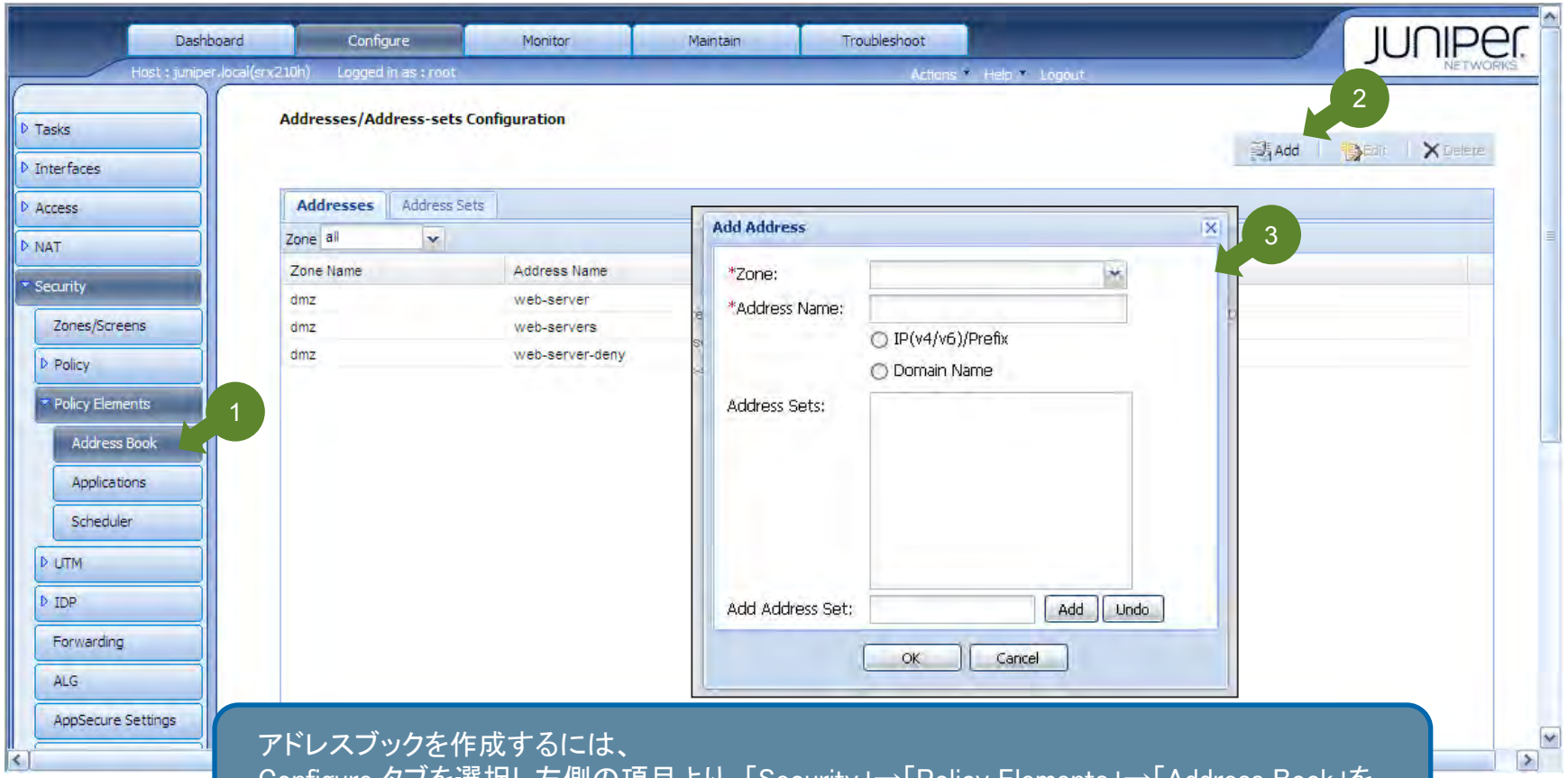
Step6-3：ファイアウォールポリシーの表示

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。



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

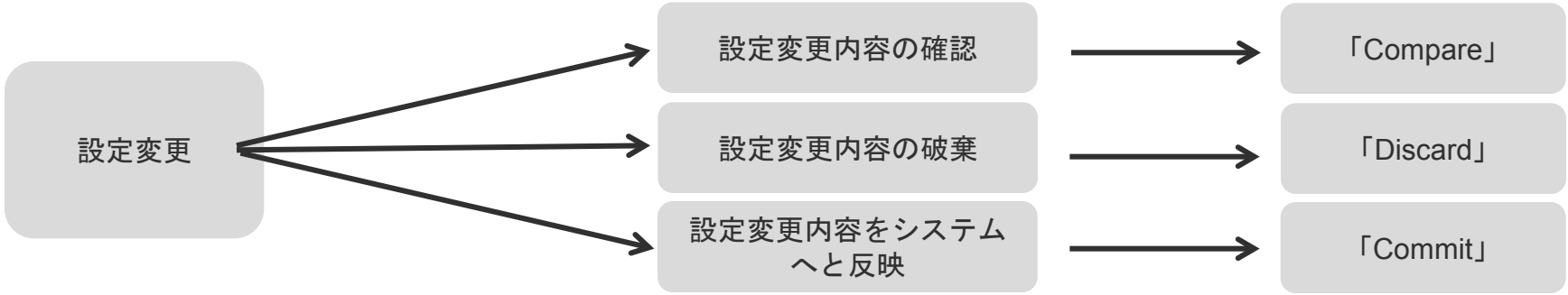
ファイアウォールポリシーはセットアップウィザードからではなく、個別に設定を行うことも可能です。



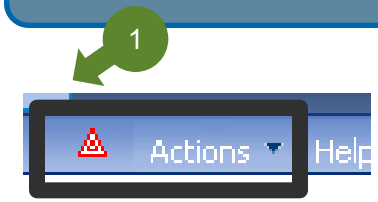
アドレスブックを作成するには、
Configure タブを選択し左側の項目より、「Security」→「Policy Elements」→「Address Book」を選択して（①）「Add」（②）でアドレスブック設定ウィンドウを表示させます（③）。

Step8：GUI設定と「Commit」について

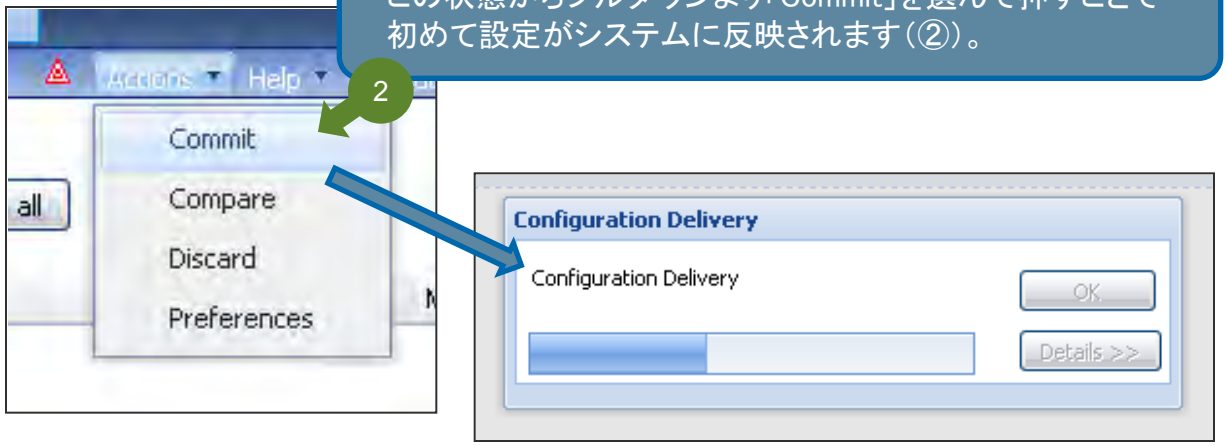
GUIでの設定変更はJUNOS CLIと同様に、即時反映されることなく「Commit」を経てシステムに反映される仕組みになっています。



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）

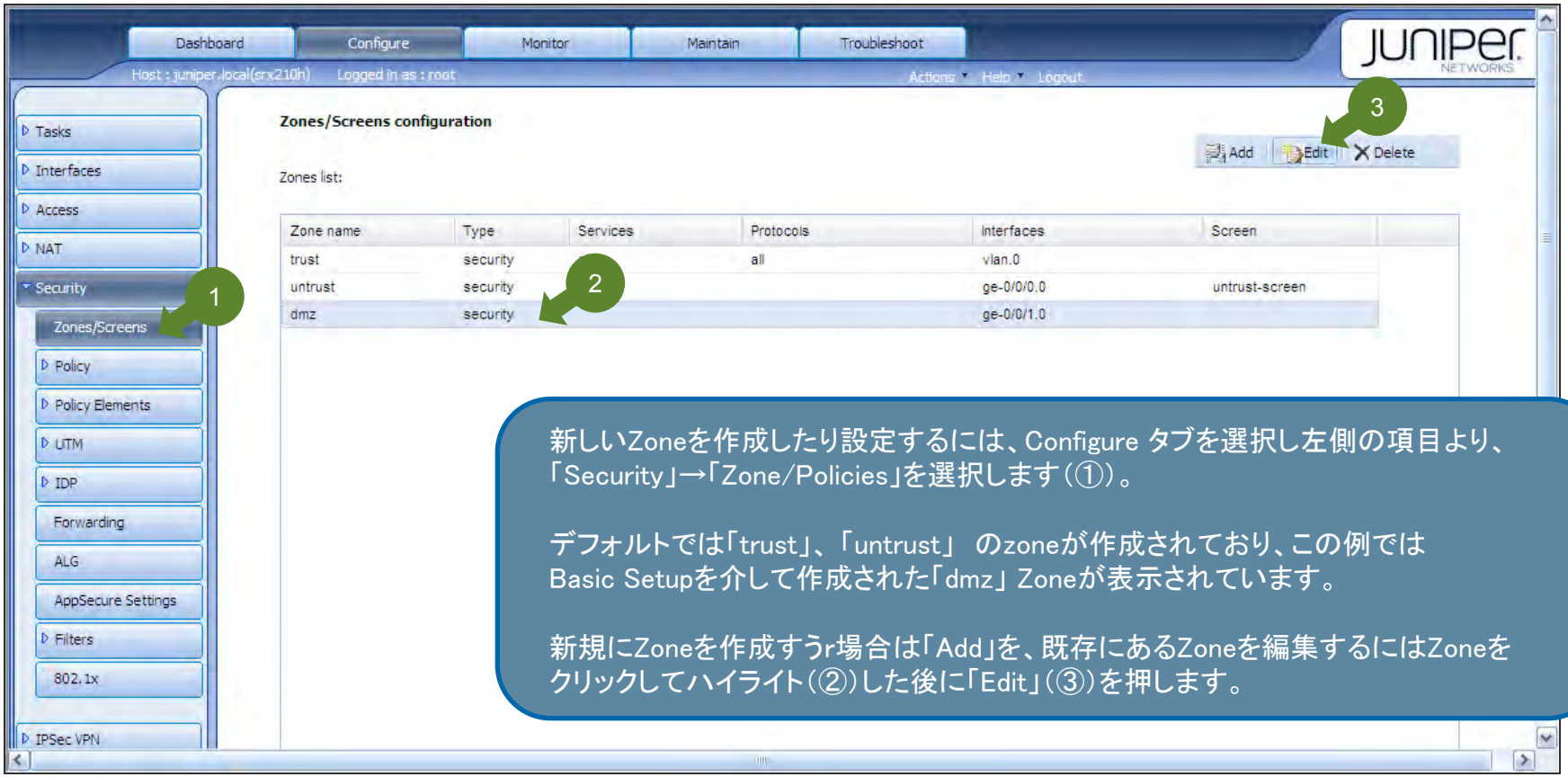


この状態からプルダウンより「Commit」を選んで押すことで初めて設定がシステムに反映されます（②）。



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。

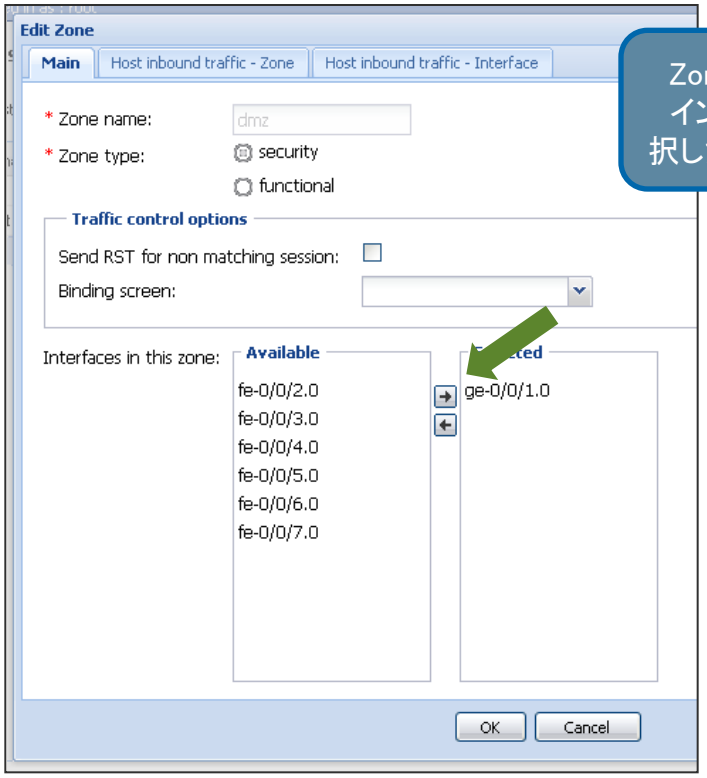


新しいZoneを作成したり設定するには、Configure タブを選択し左側の項目より、「Security」→「Zone/Policies」を選択します（①）。

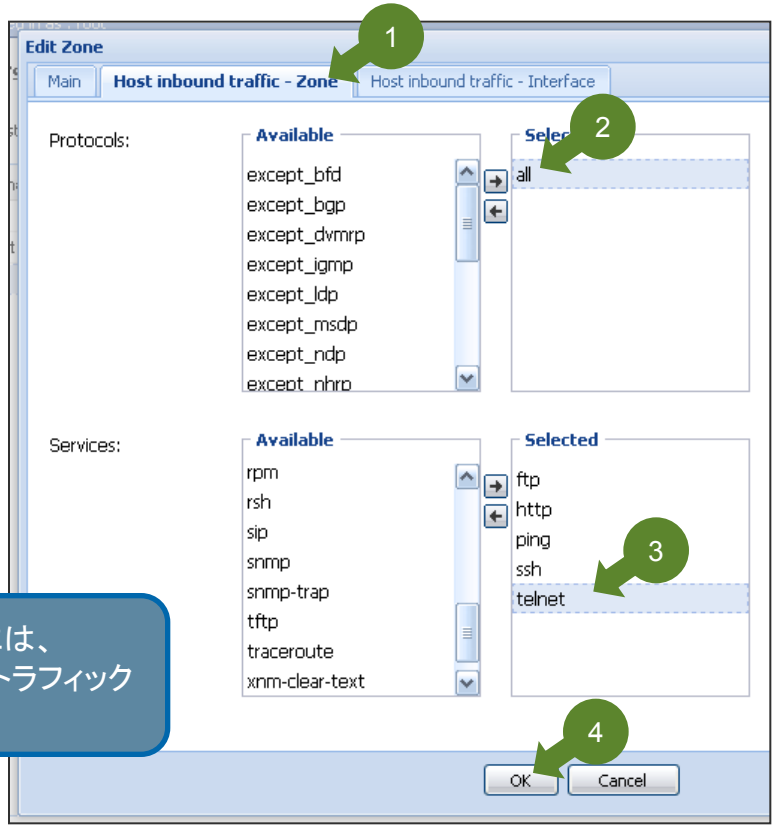
デフォルトでは「trust」、「untrust」 のzoneが作成されており、この例では
Basic Setupを介して作成された「dmz」 Zoneが表示されています。

新規にZoneを作成すうr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

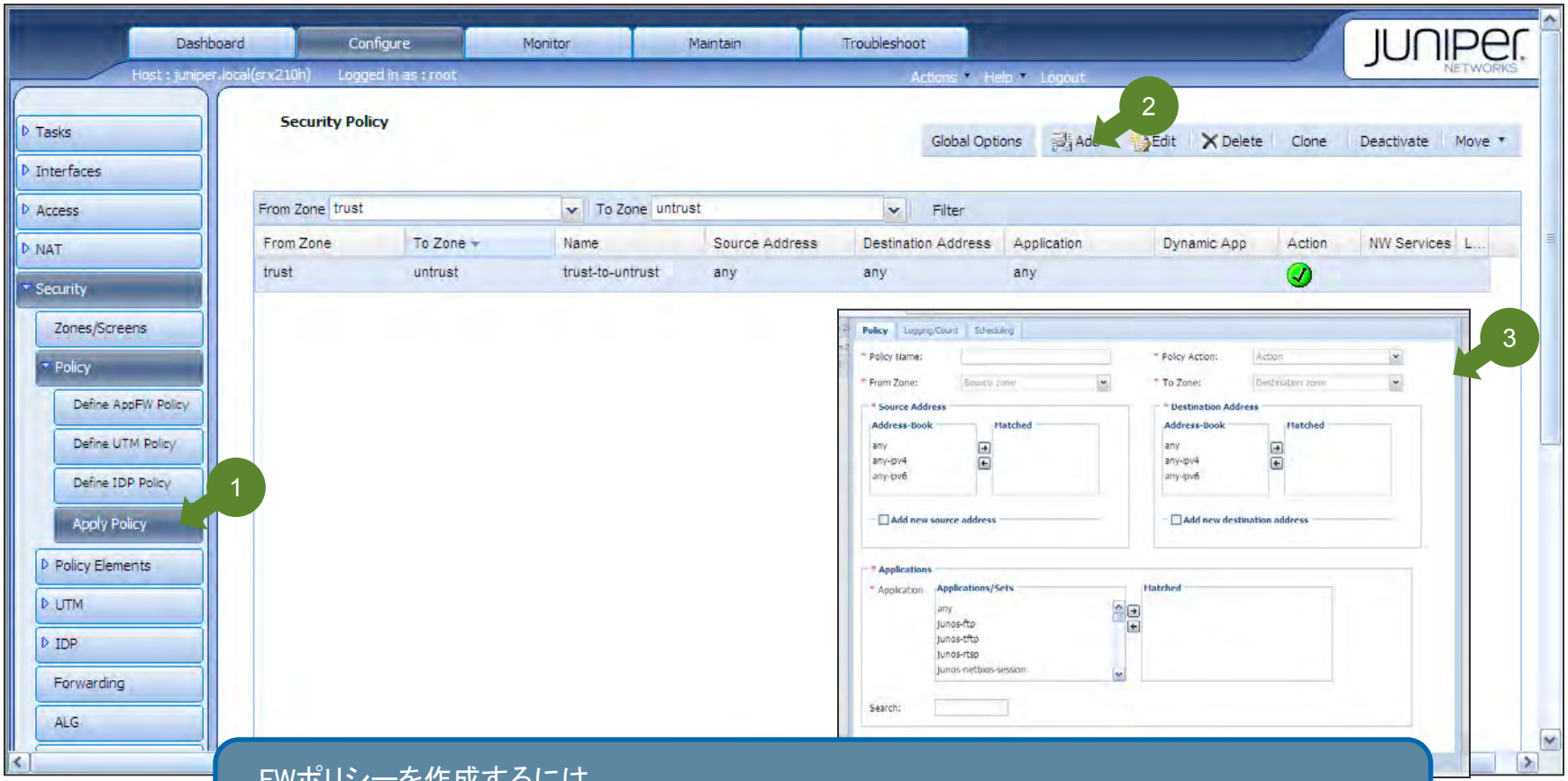


Zoneの設定ウィンドウが表示されるので、
インタフェースの増減を行う場合は、「→」「←」で選択したインタフェースを動かします。



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。

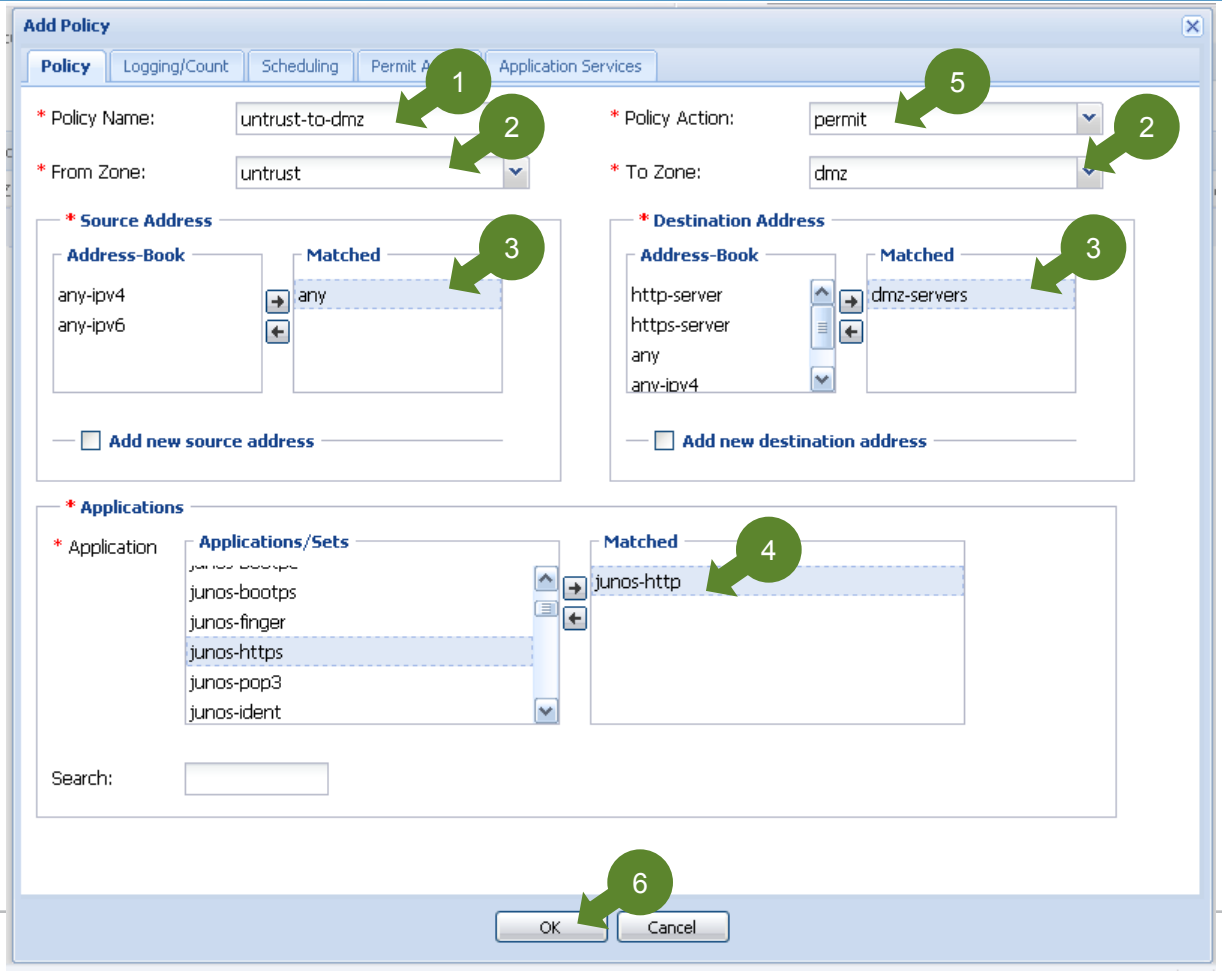
Step9-3：ファイアウォールポリシーの設定
FWポリシーの設定



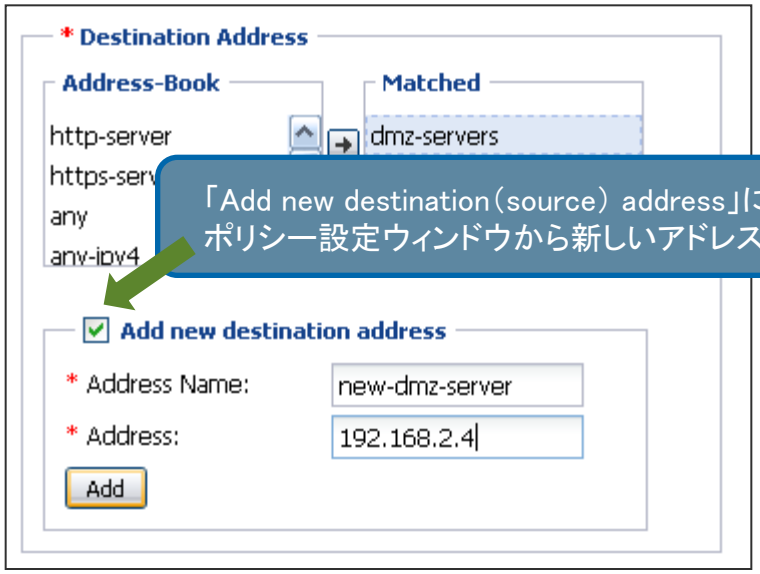
FWポリシーを作成するには、
Configure タブを選択し左側の項目より、「Security」→「Policy」→「Apply Policy」を選択して（①）
「Add」（②）でポリシー設定ウィンドウを表示させます（③）。

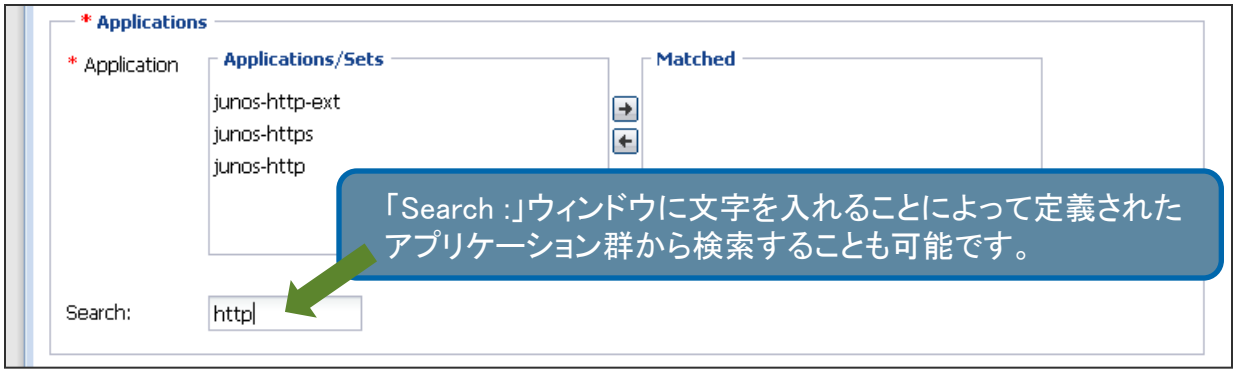
Step9-4：ファイアウォールポリシーの設定
FWポリシーの設定

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。



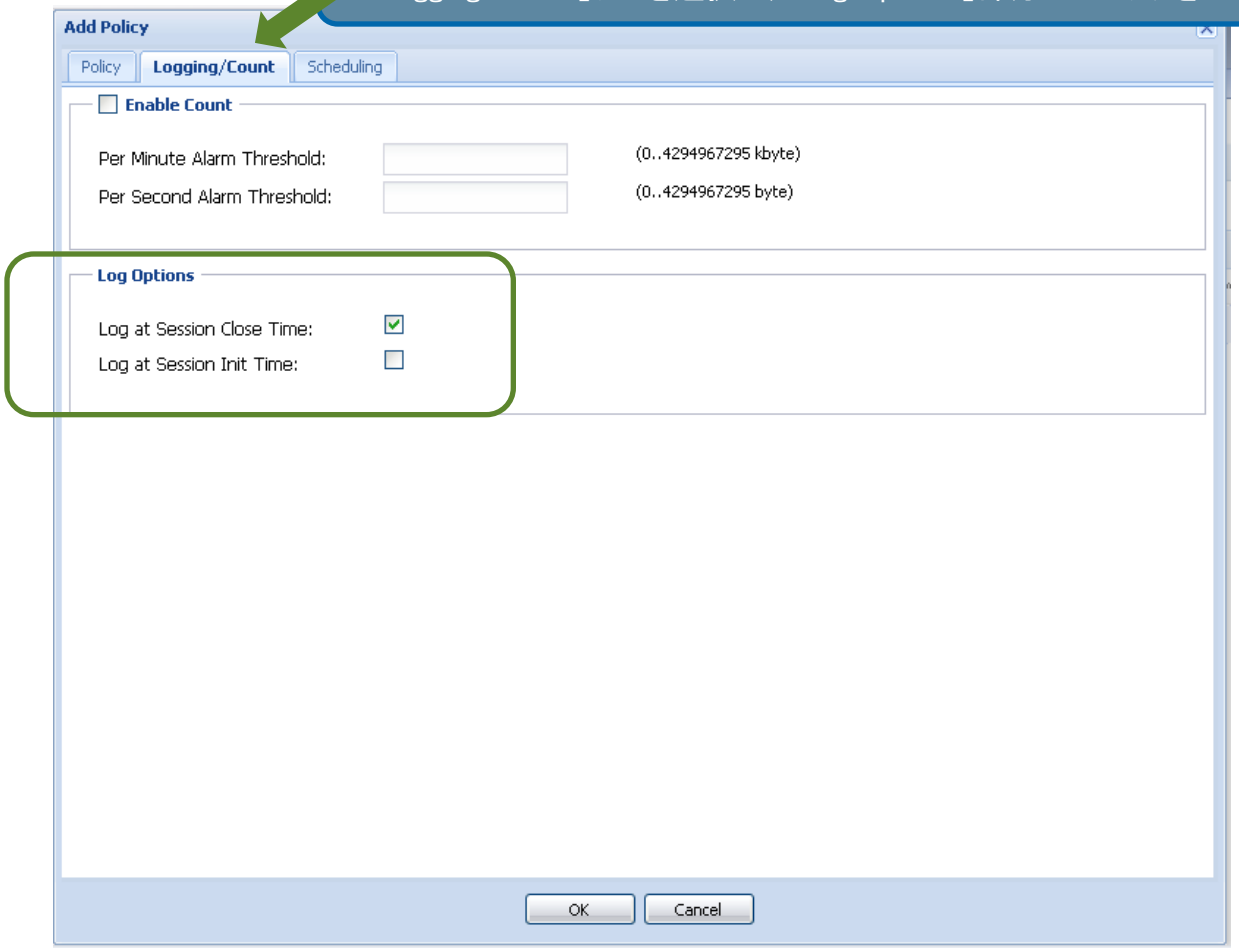
Step9-5：ファイアウォールポリシーの設定
FWポリシーの設定





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ギングを追加するには、
「Logging/Count」タブを選択し、「Log Options」部分にチェックをいれます。

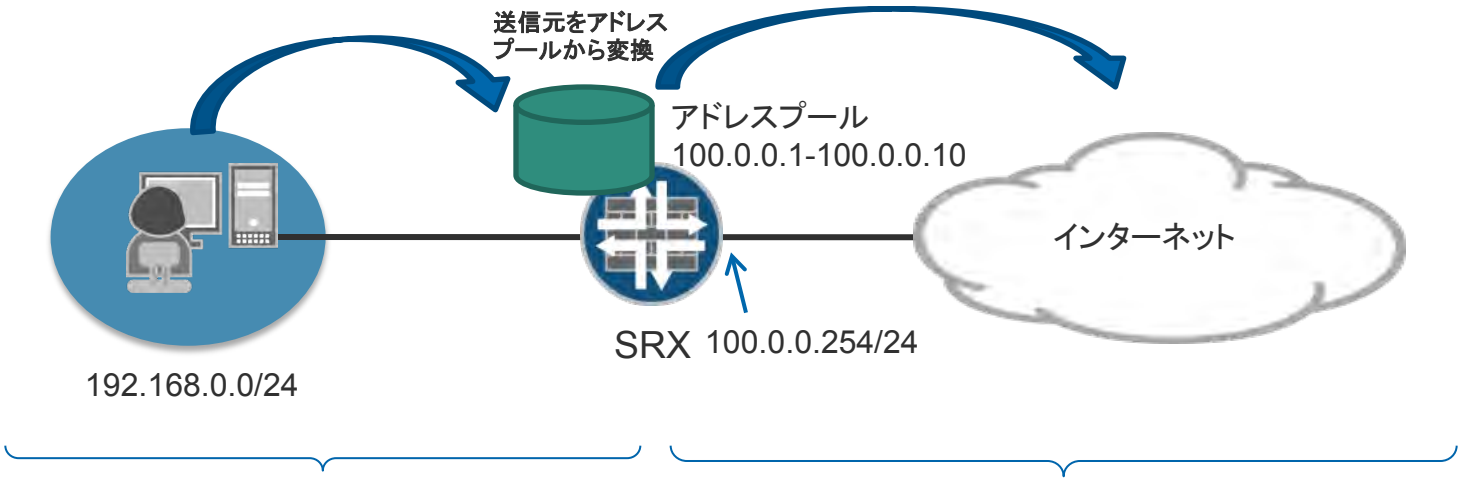


Chapter3. NAT

- Source NAT
- Static NAT

Source NAT ー このガイドで構築する物理・論理構成

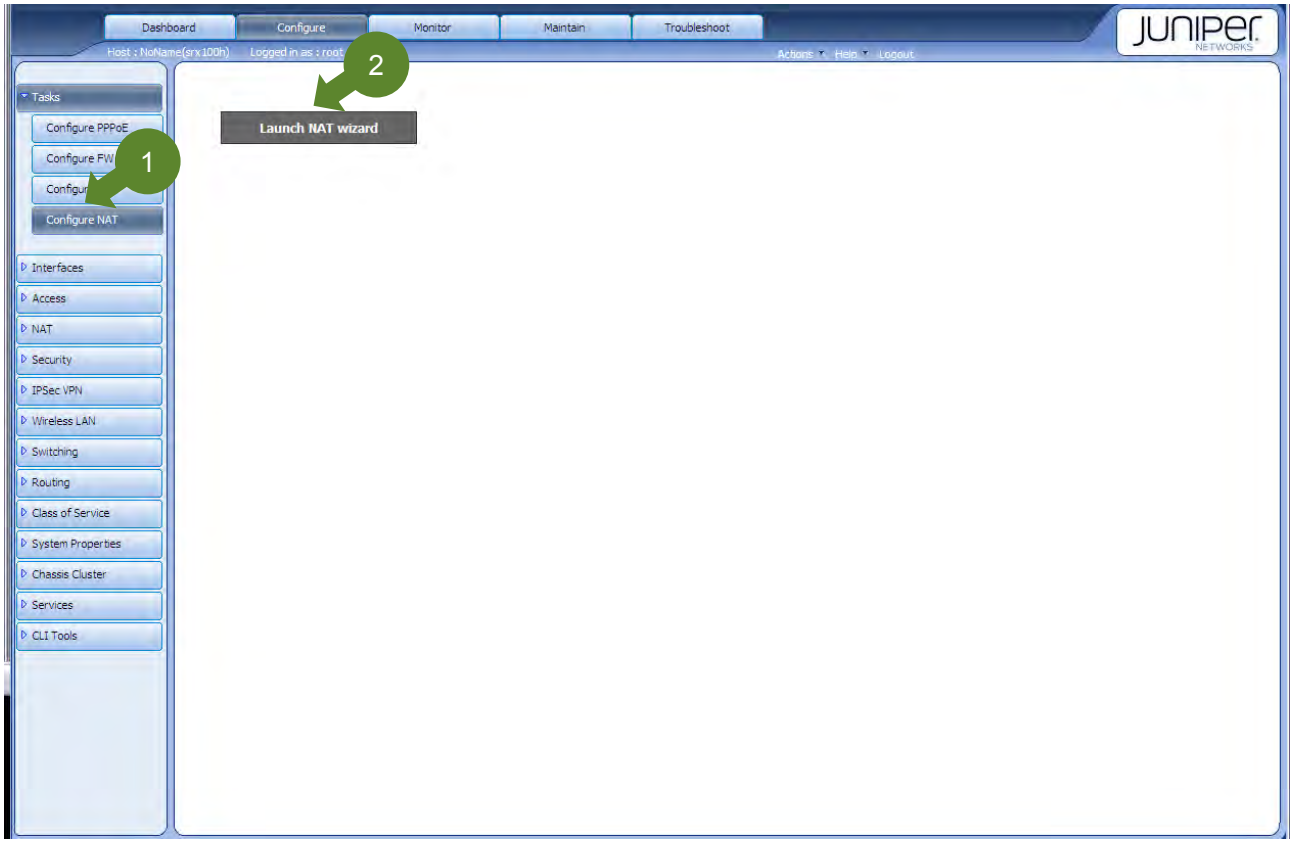
Trust zone(192.168.0.0/24)から、Untrust Zone(インターネット)
へ抜ける通信に関しては、アドレスプール(100.0.0.1-100.0.0.10)
を利用し、Source NATにて、通信をする。



Source NAT設定 (1/12)

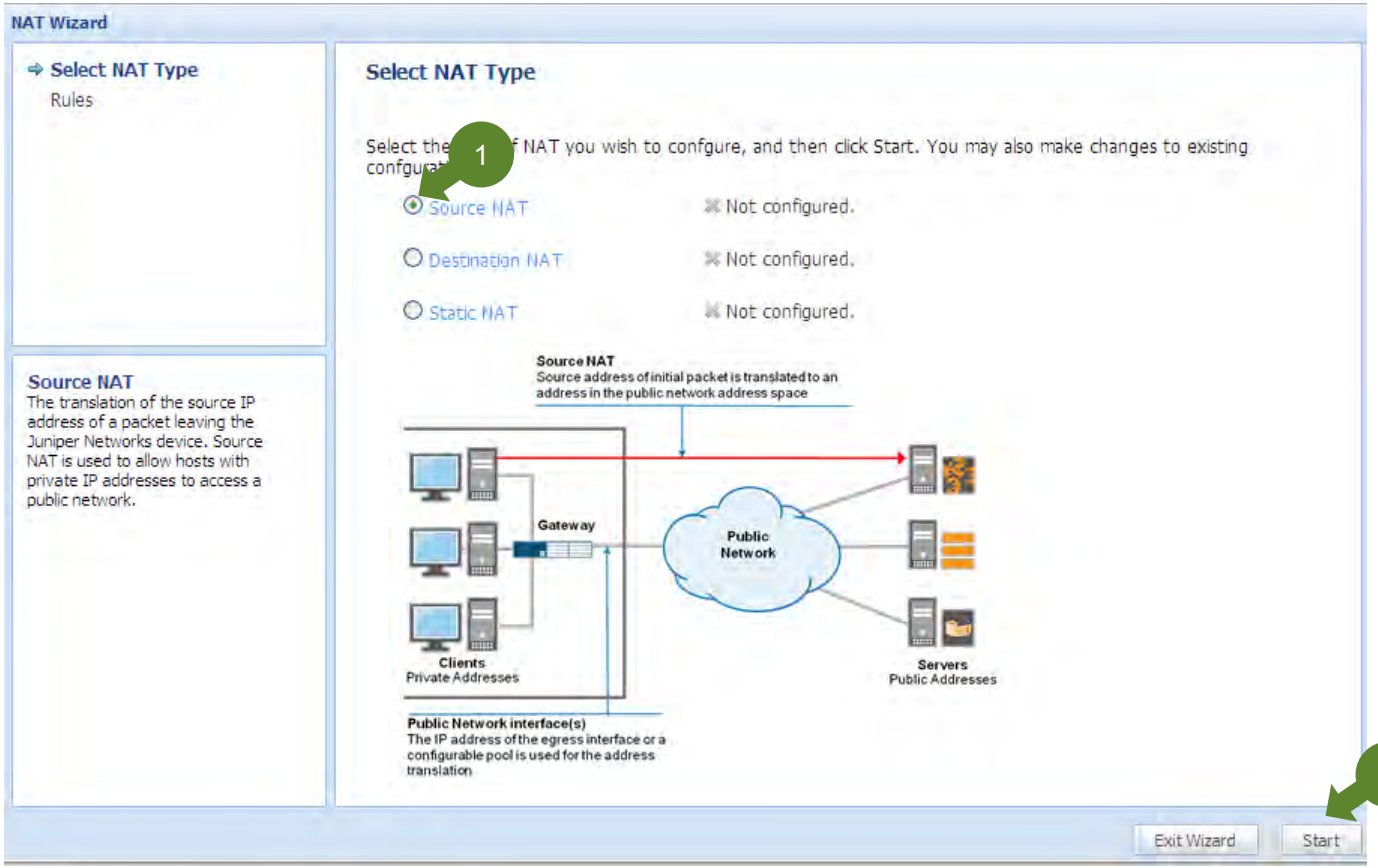
NATの設定は、「NAT Wizard」を使用して簡単に作成することが可能です。

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）



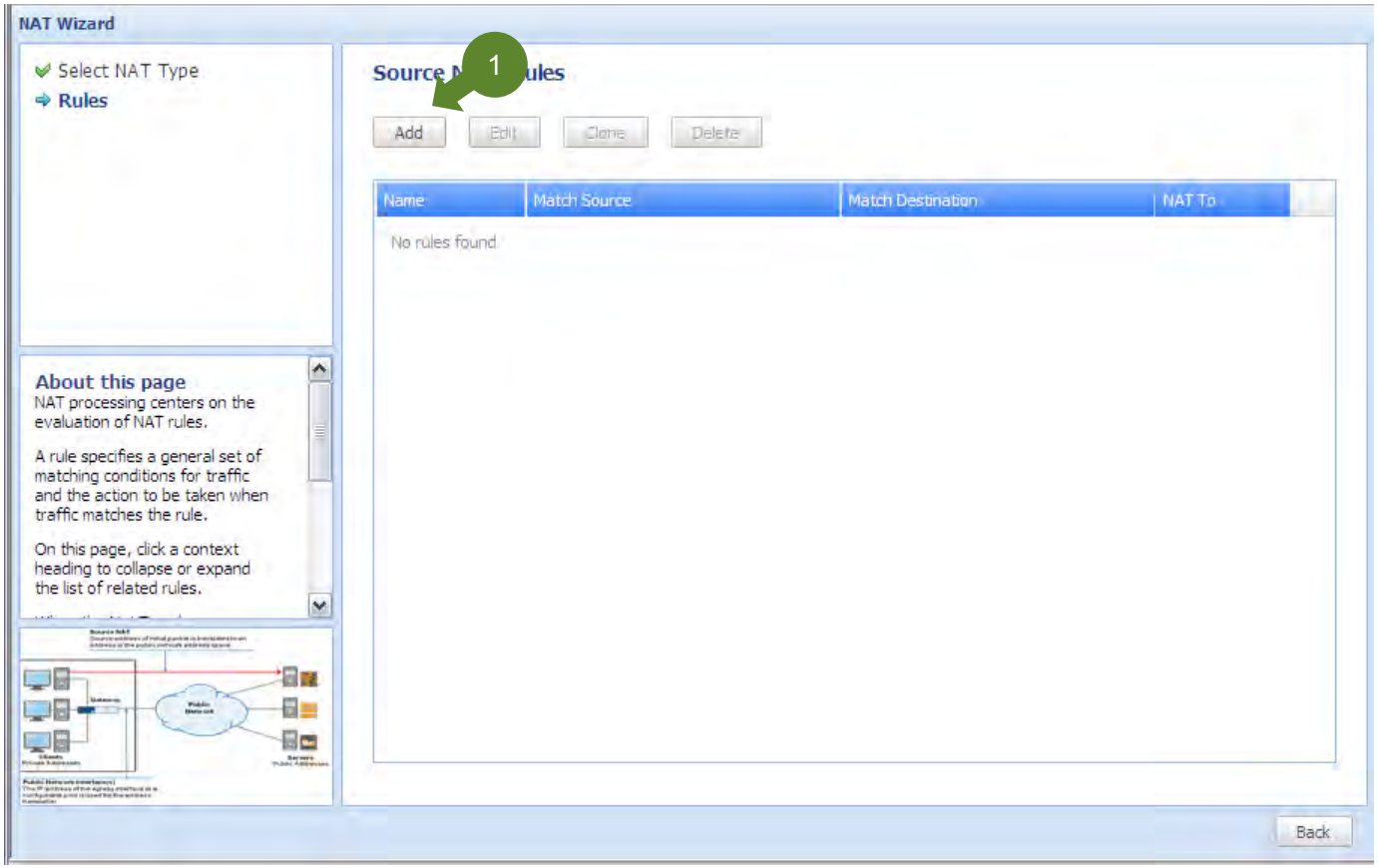
Source NAT設定 (2/12)

「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。



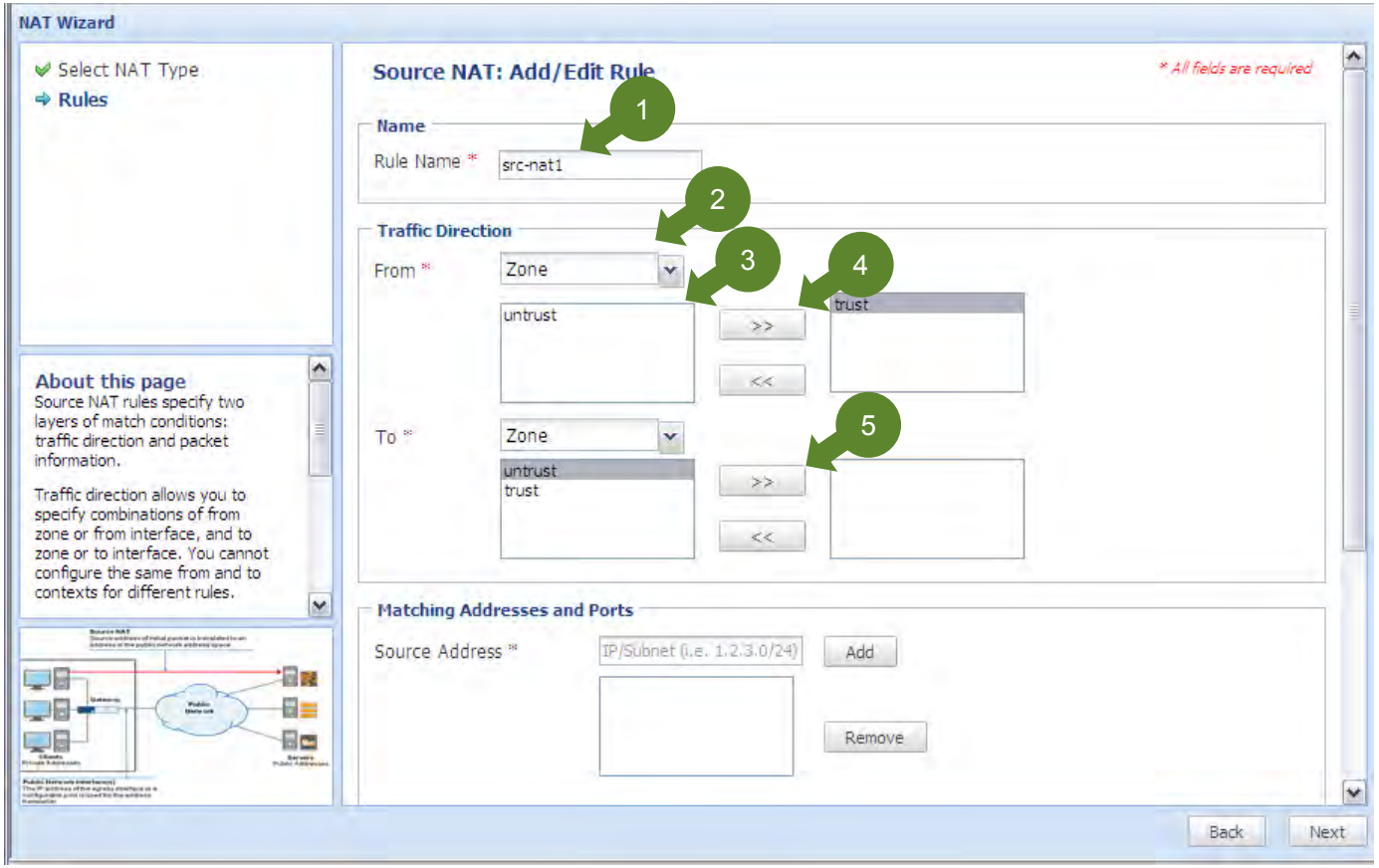
Source NAT設定 (3/12)

「Add」ボタン(①)を押し、Source NATを新規作成します。



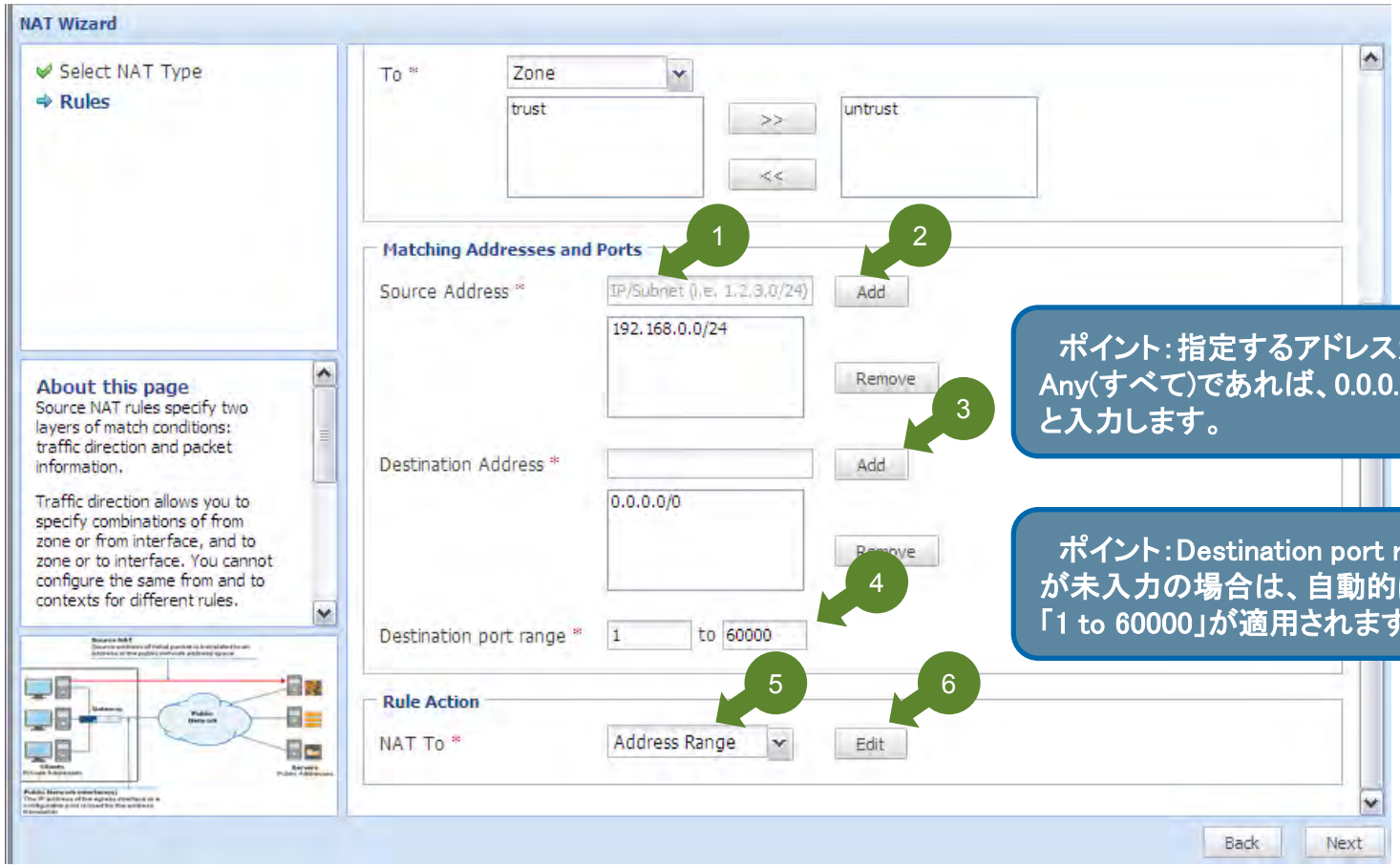
Source NAT設定 (4/12)

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。



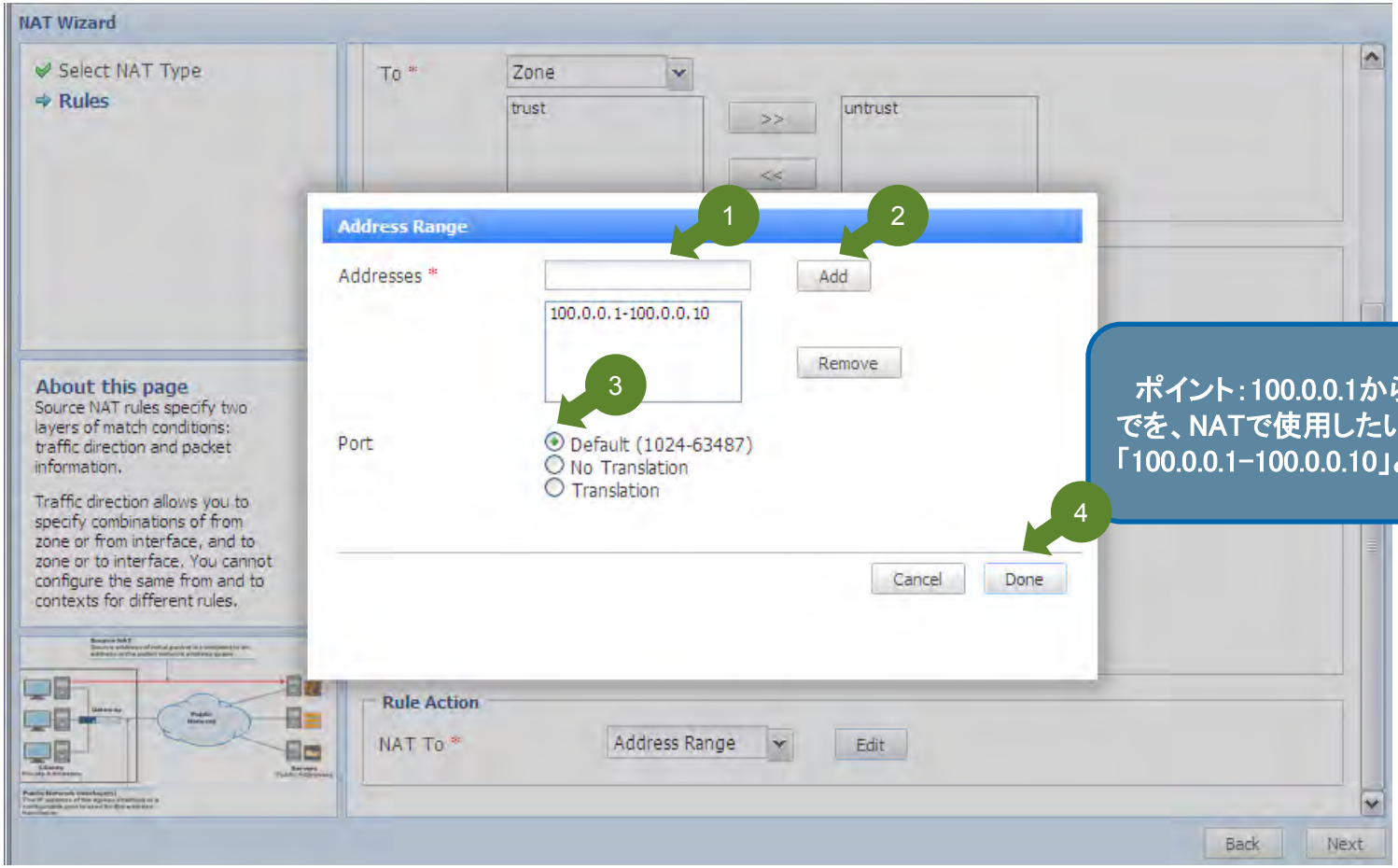
Source NAT設定 (5/12)

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ルールの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。



Source NAT設定 (6/12)

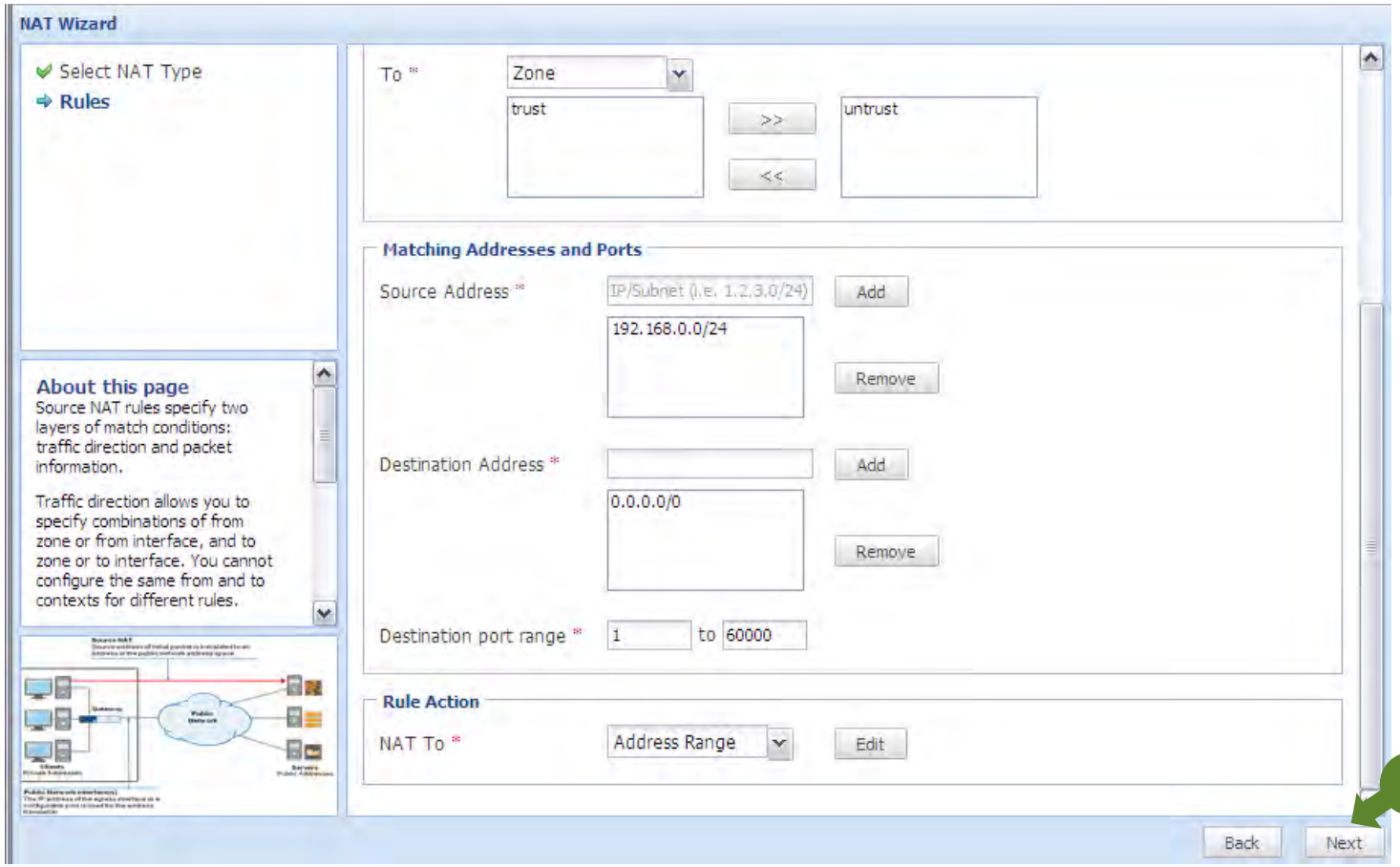
アドレスプールで使用するアドレス①を入力し、「Add」ボタン②で決定します。設定したアドレスレンジを用いて、ポートトランスレーションのオプション③を選択します。「Done」ボタン（④）を押します。



ポイント：100.0.0.1から100.0.0.10までを、NATで使用したい場合には、「100.0.0.1−100.0.0.10」と入力します。

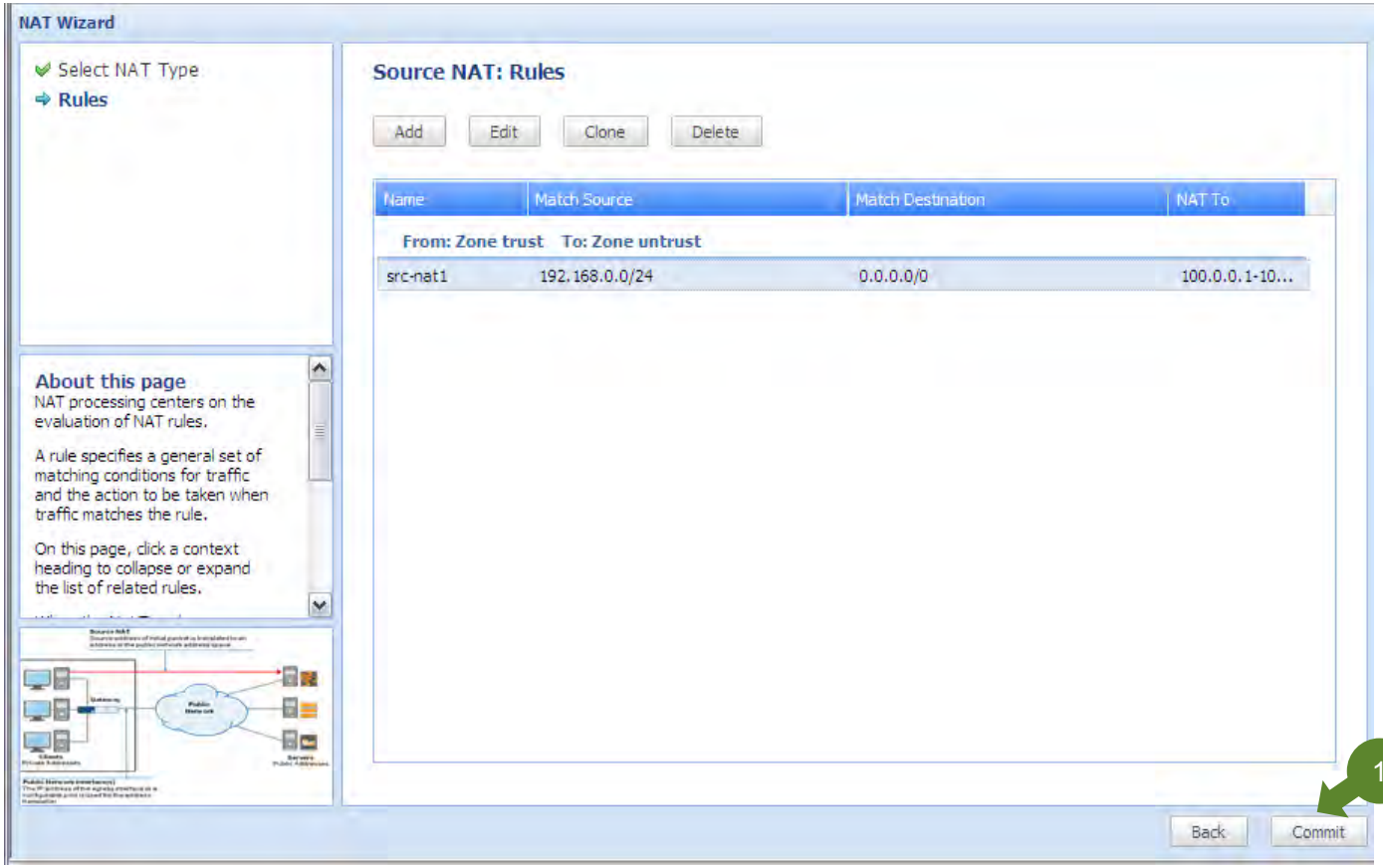
Source NAT設定 (7/12)

アドレスプールの設定を終えたら、「Next」ボタン（①）を押します。



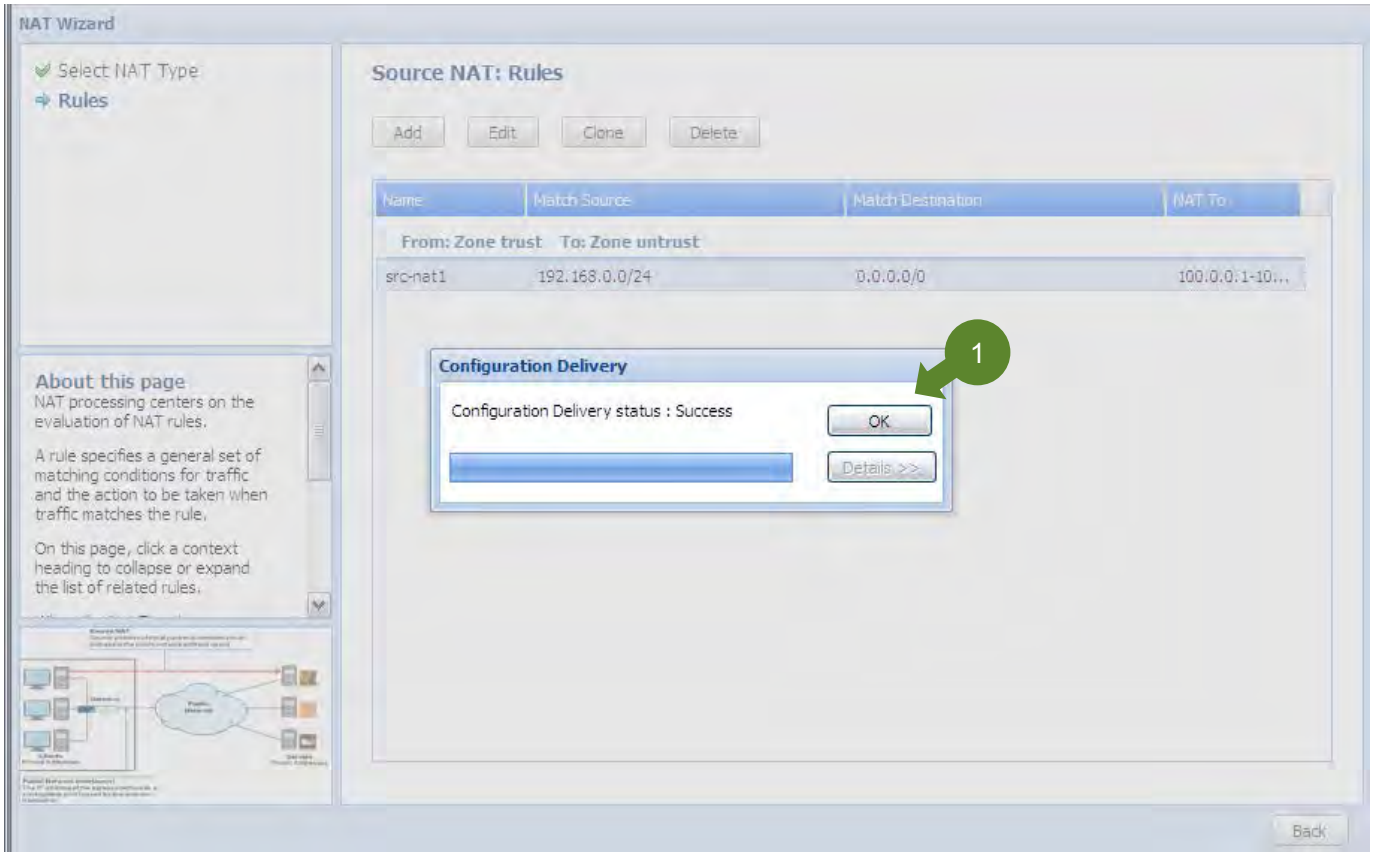
Source NAT設定 (8/12)

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。



Source NAT設定 (9/12)

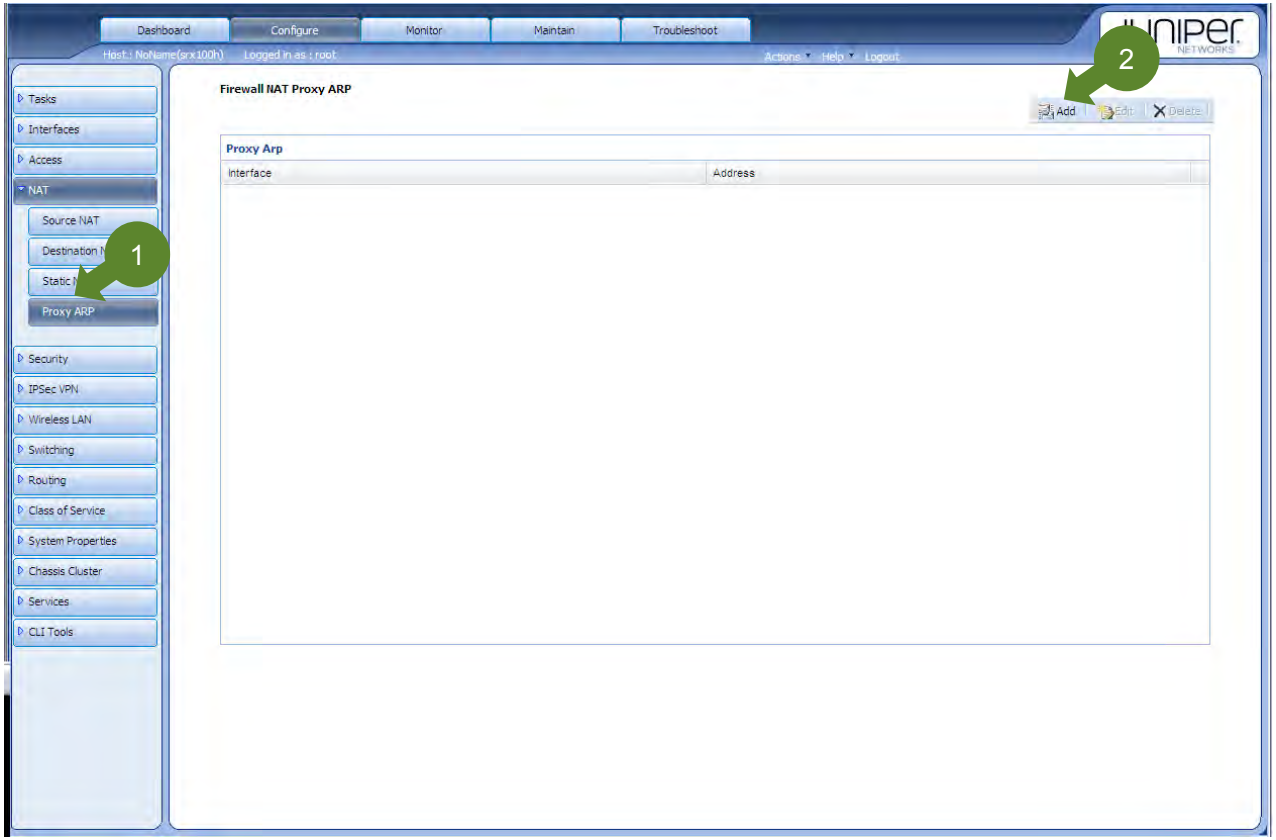
Commitプロセスが行われます。問題が無ければ、「OK」ボタン①をクリックして、Wizardを終了します。



Source NAT設定 (10/12)

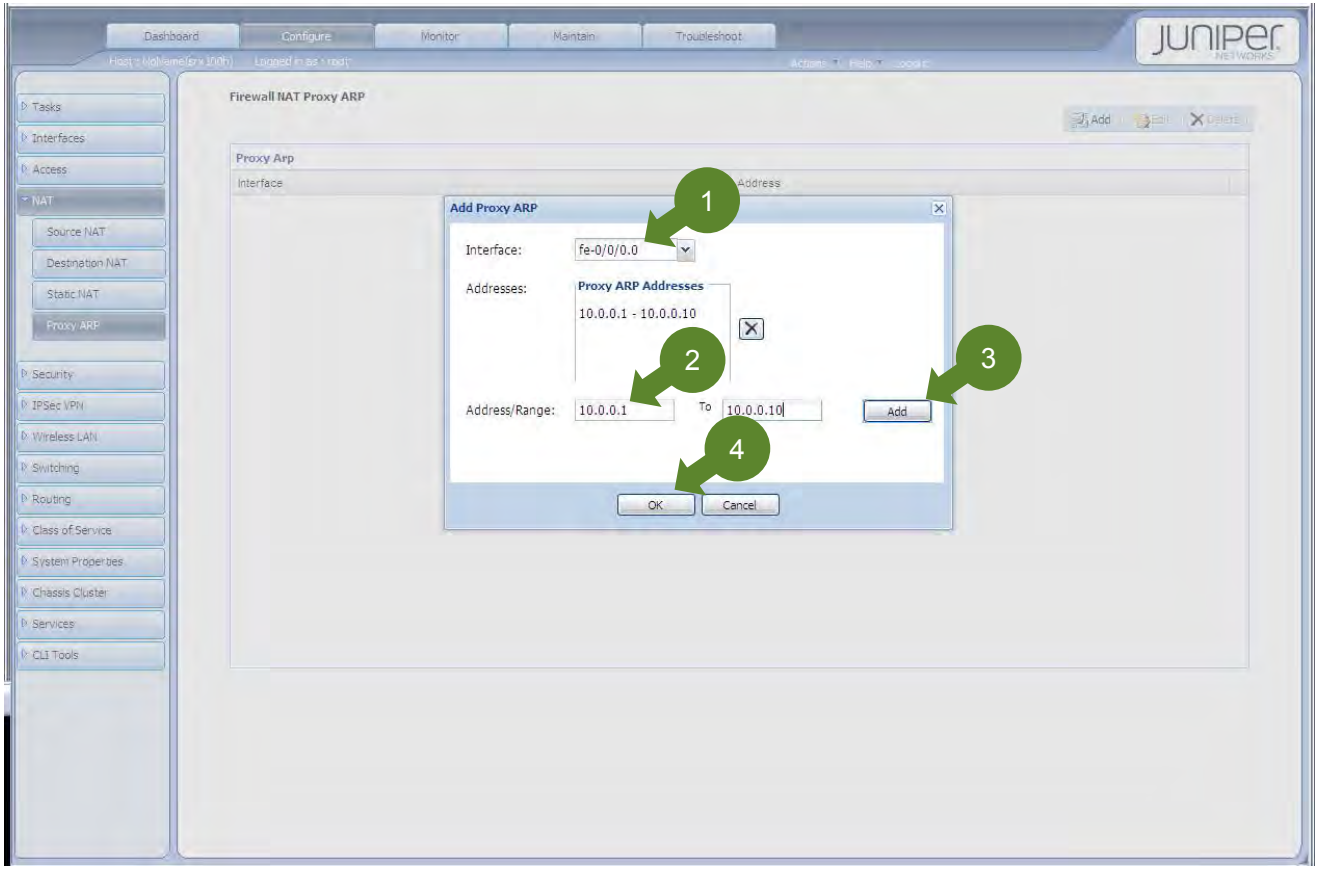
アドレスプールは、実在しないアドレスのため、Proxy ARPの設定が必要になります。

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）



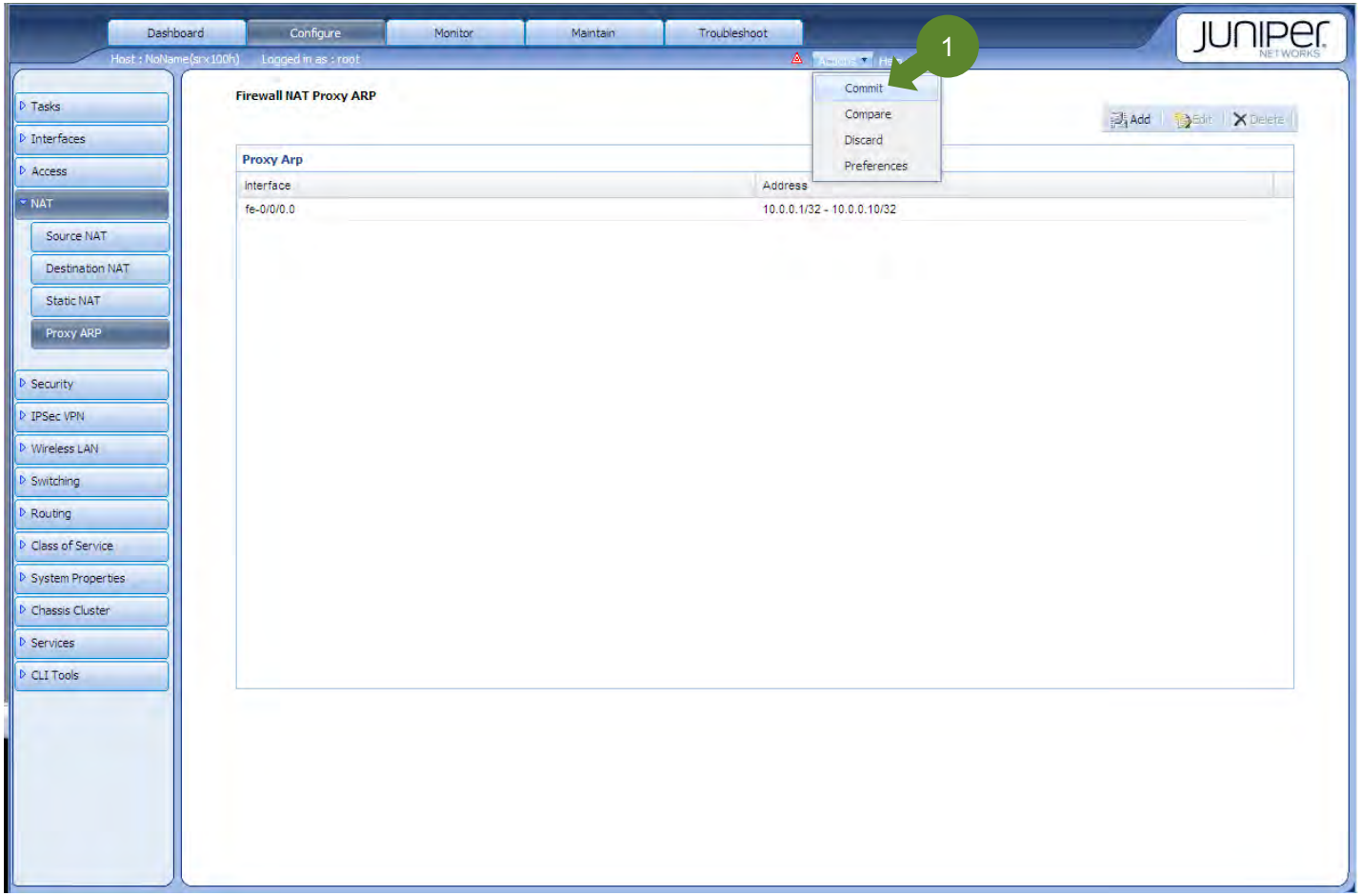
Source NAT設定 (11/12)

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。



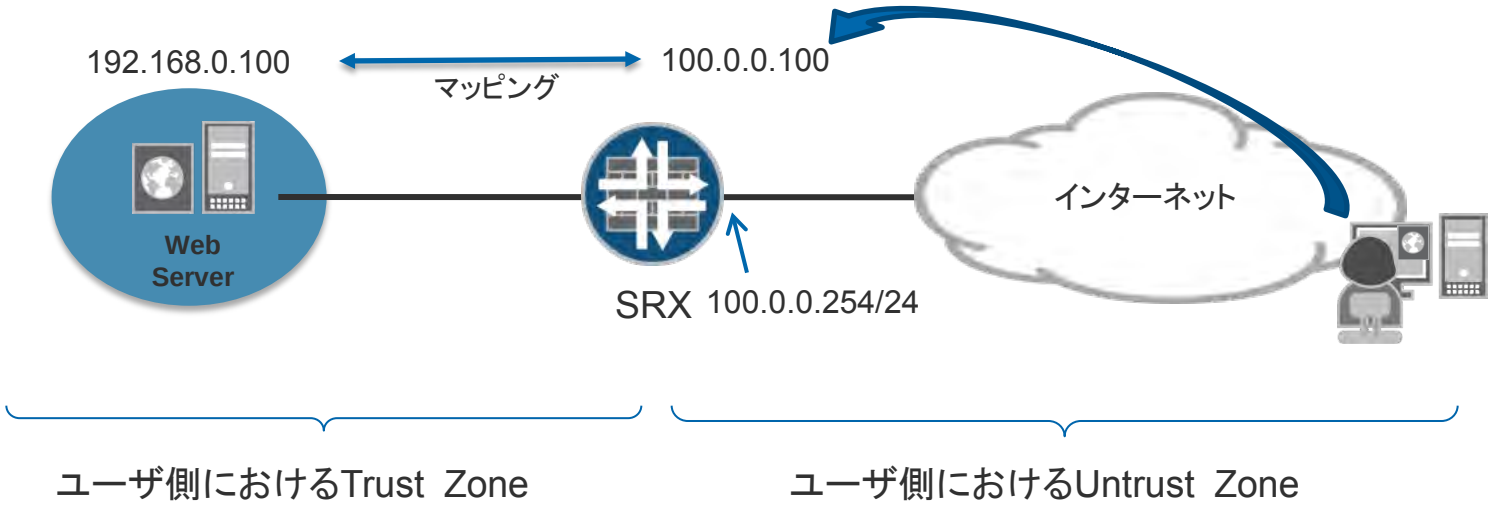
Source NAT設定 (12/12)

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。



Static NAT ー このガイドで構築する物理・論理構成

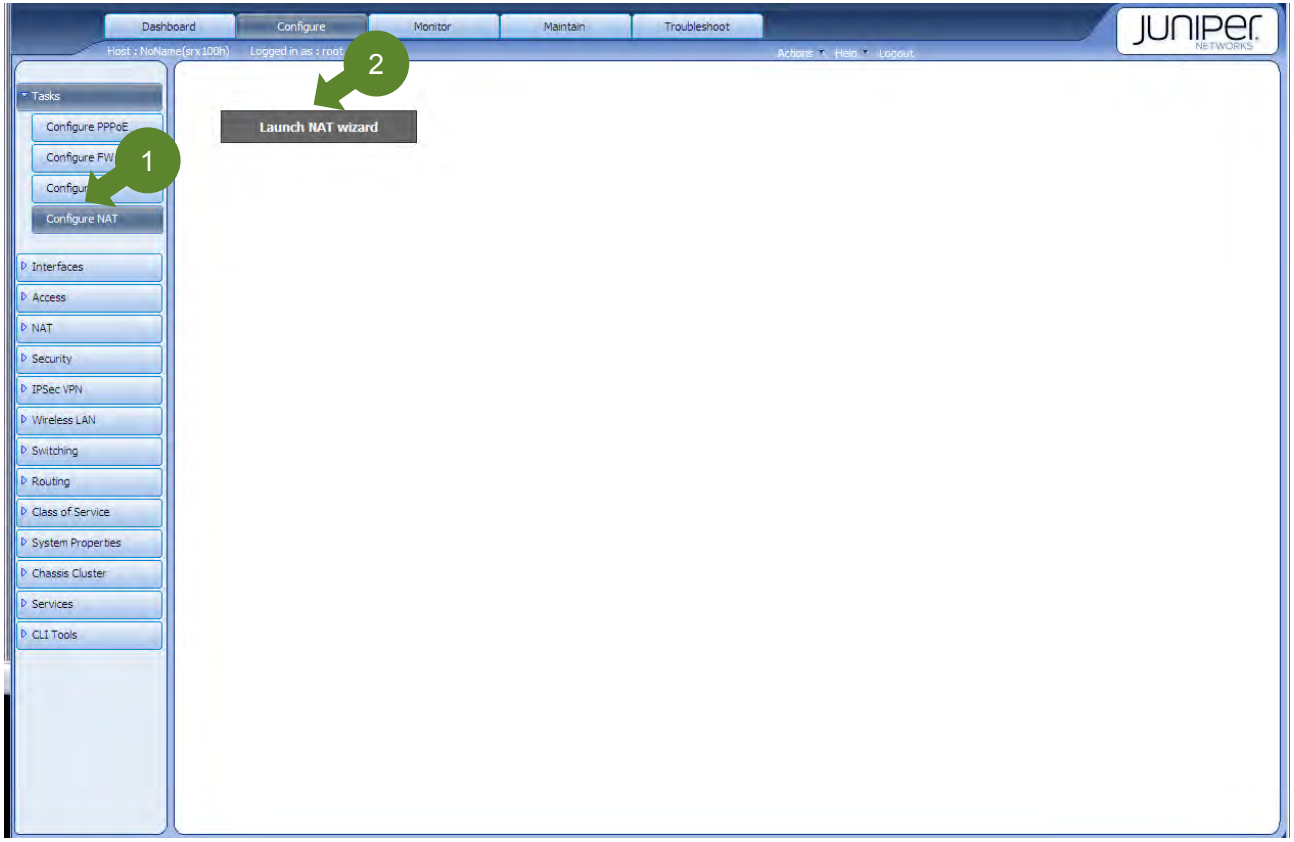
Untrust Zone(インターネット)から、Trust Zoneにあるサーバ(192.168.0.100)に対して、グローバルアドレス(100.0.0.100)を利用し、Static NATにて、通信できるようにする。



Static NAT設定 (1/9)

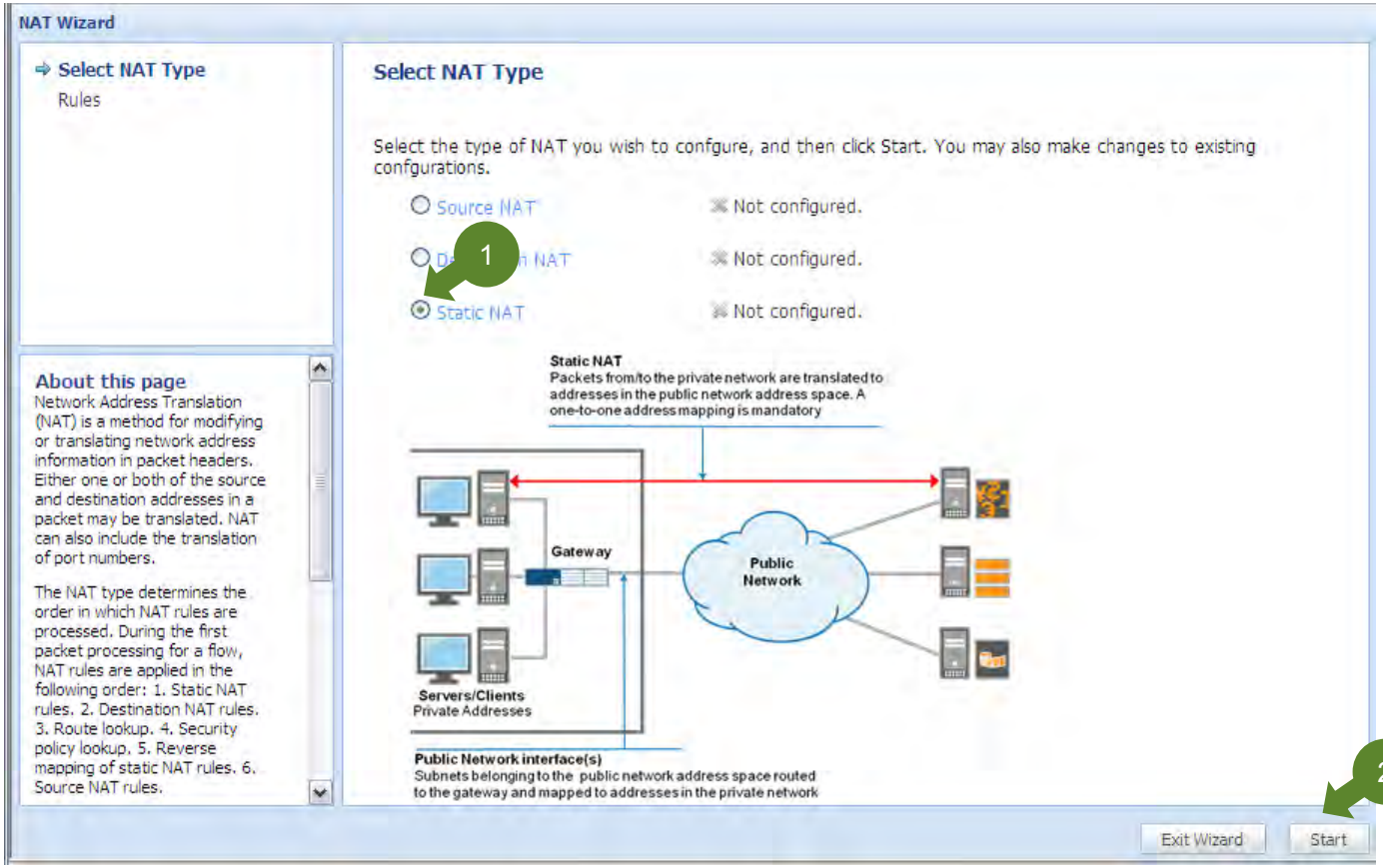
NATの設定は、「NAT Wizard」を使用して簡単に作成することが可能です。

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）



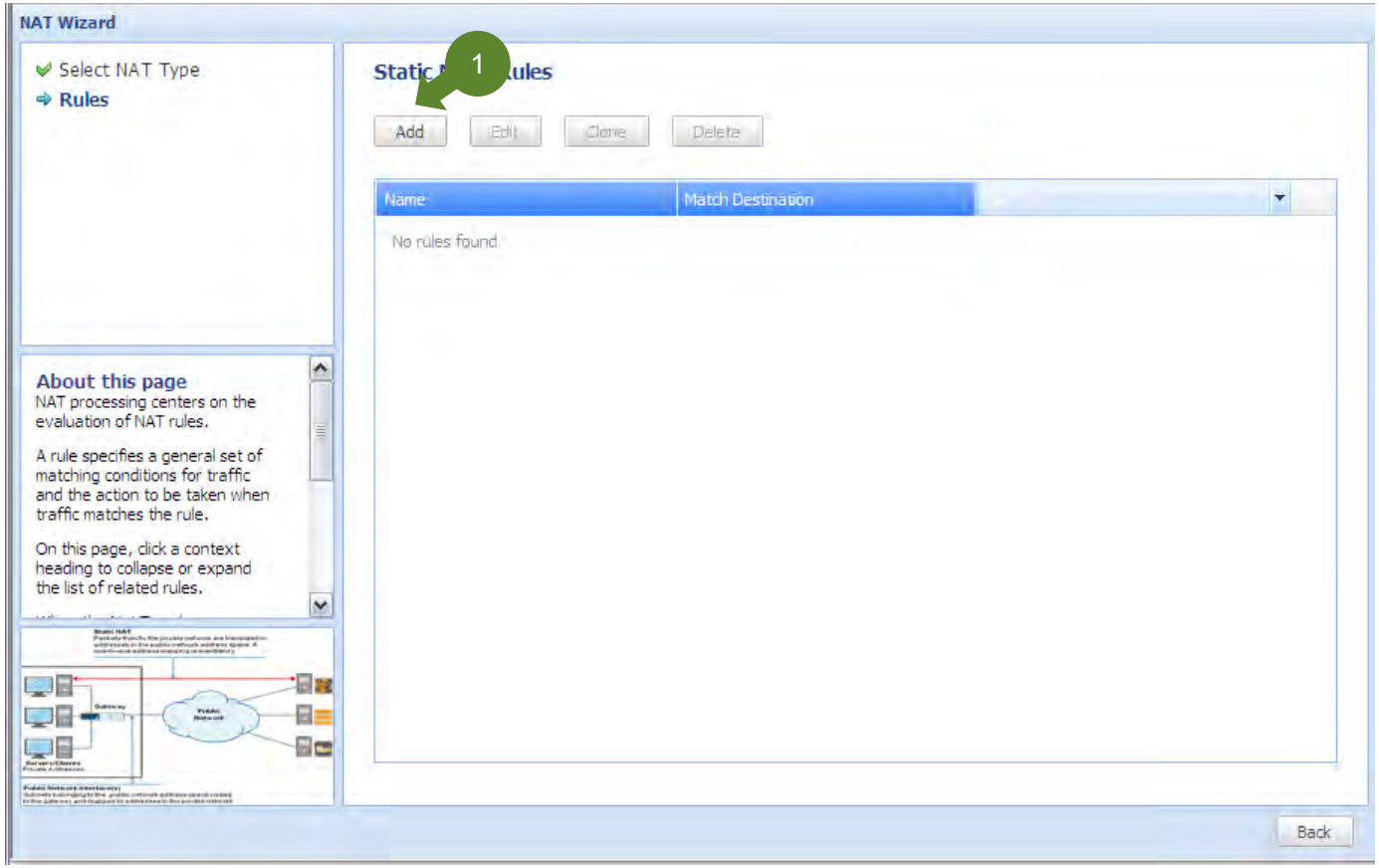
Static NAT設定 (2/9)

「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。



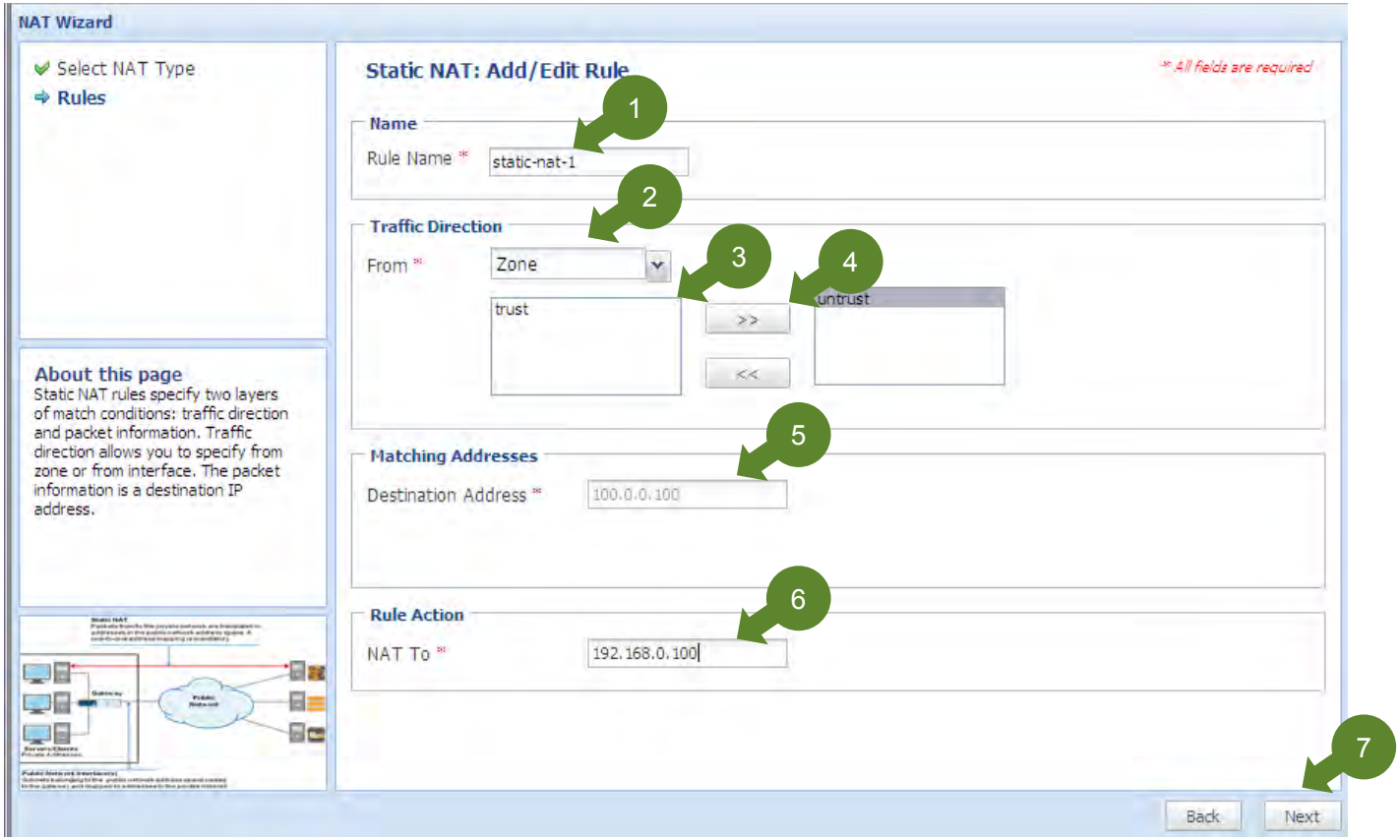
Static NAT設定 (3/9)

「Add」ボタン(①)を押し、Static NATを新規作成します。



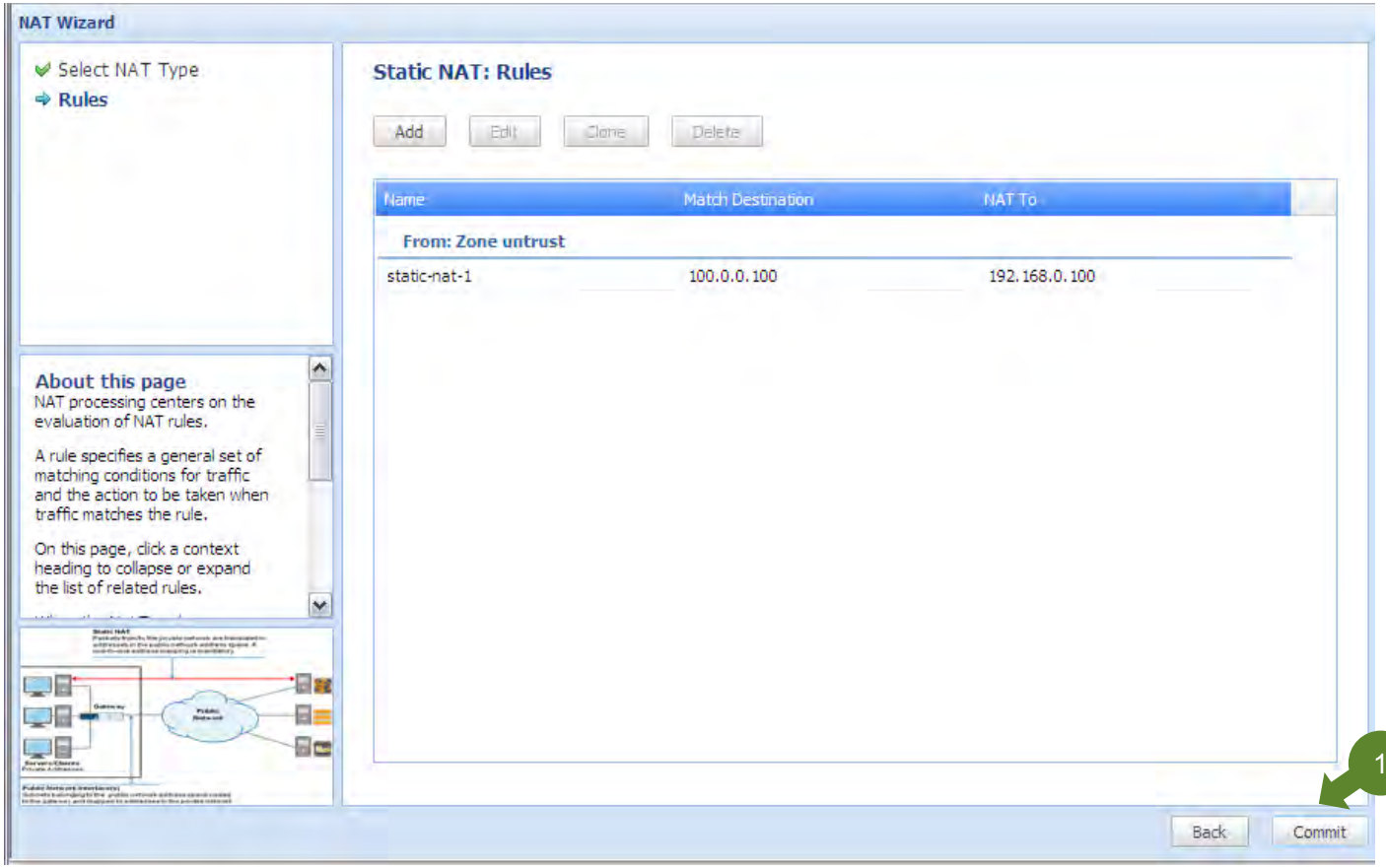
Static NAT設定 (4/9)

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。



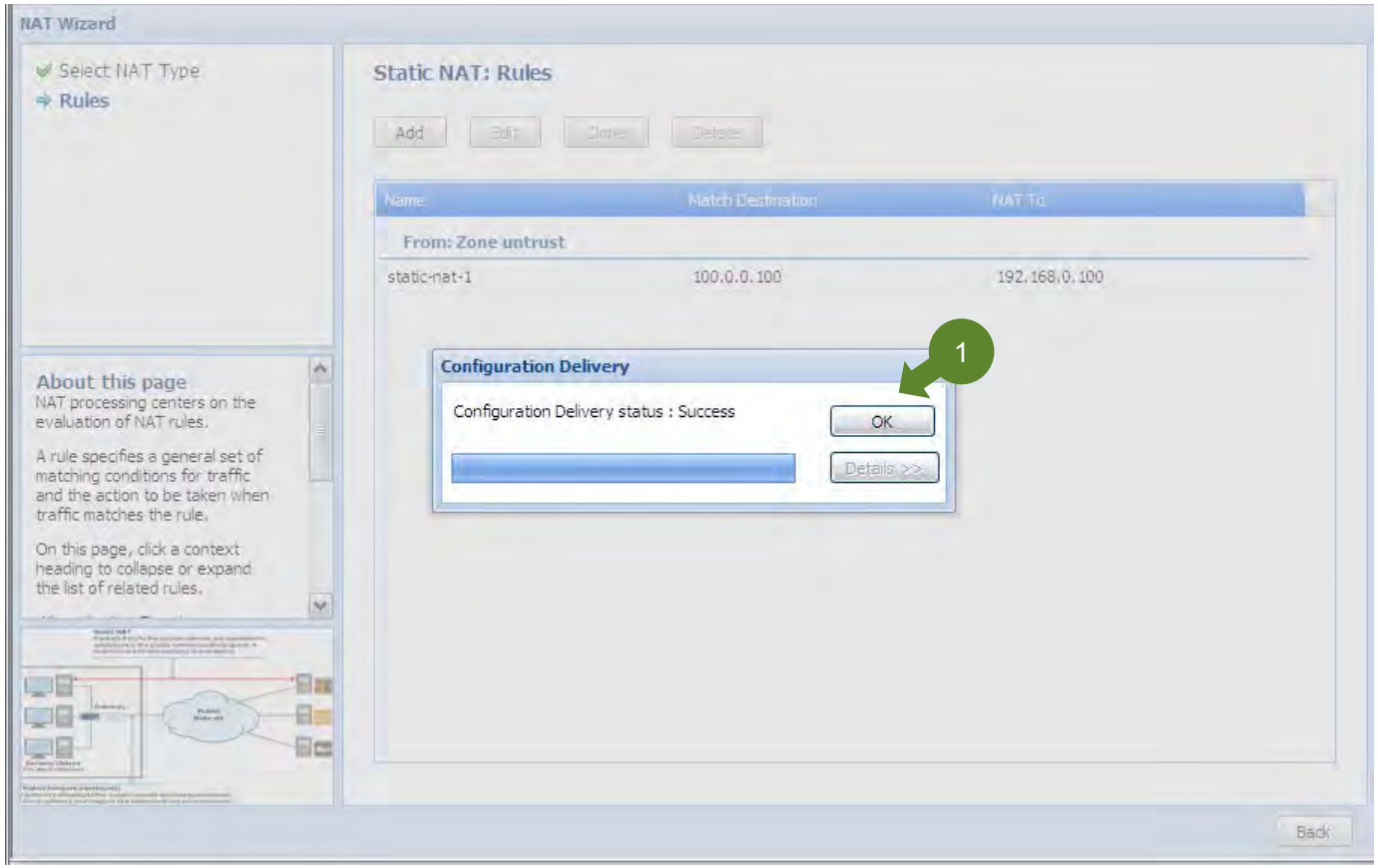
Static NAT設定 (5/9)

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。



Static NAT設定 (6/9)

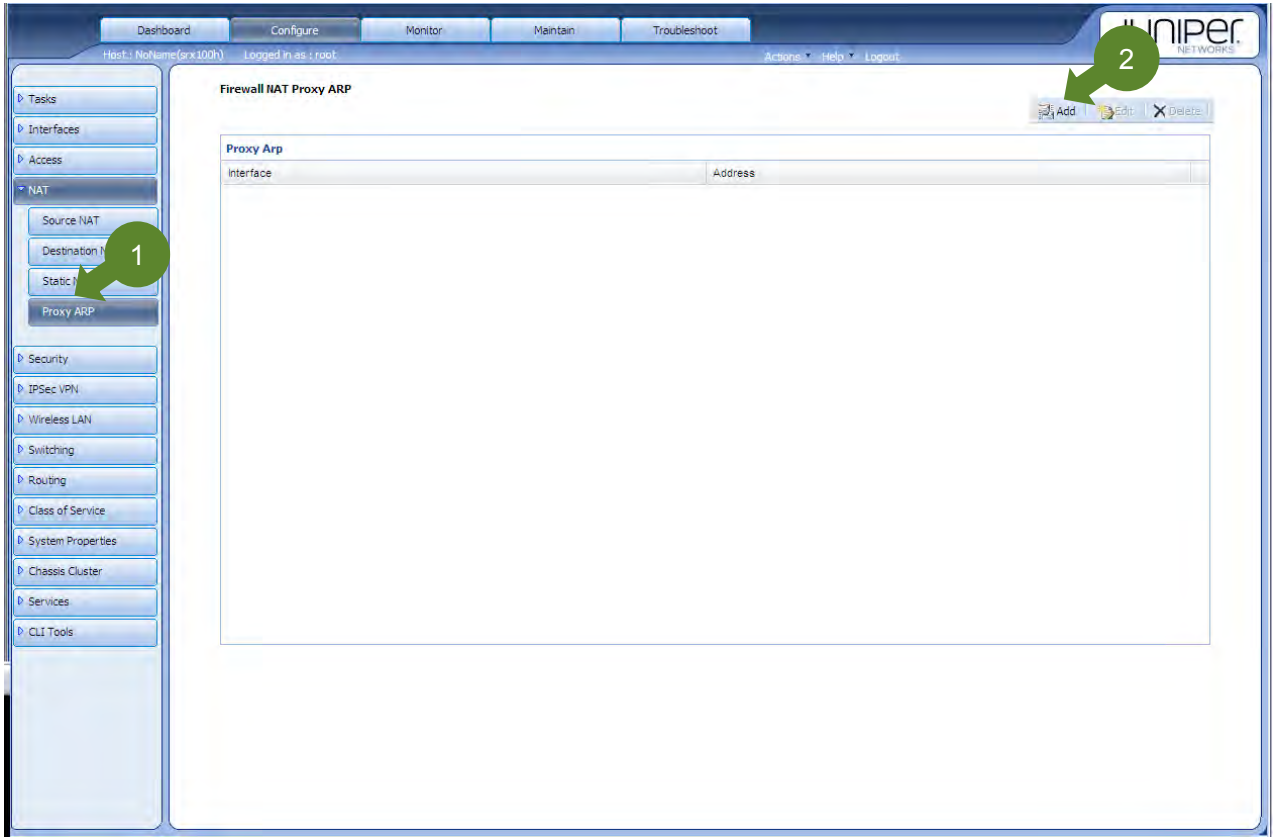
Commitプロセスが行われます。問題が無ければ、「OK」ボタン①をクリックして、Wizardを終了します。



Static NAT設定 (7/9)

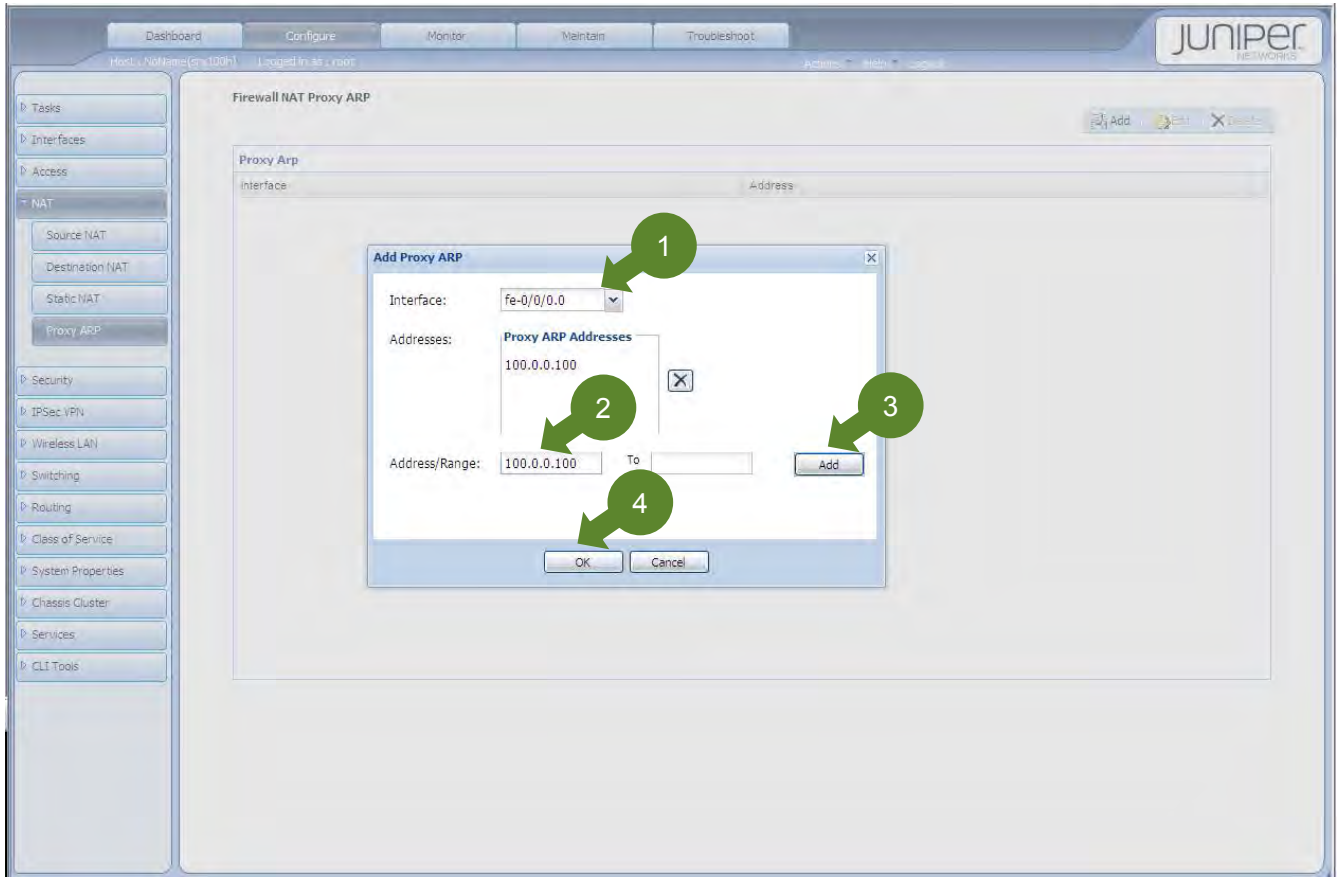
アドレスプールは、実在しないアドレスのため、Proxy ARPの設定が必要になります。

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）



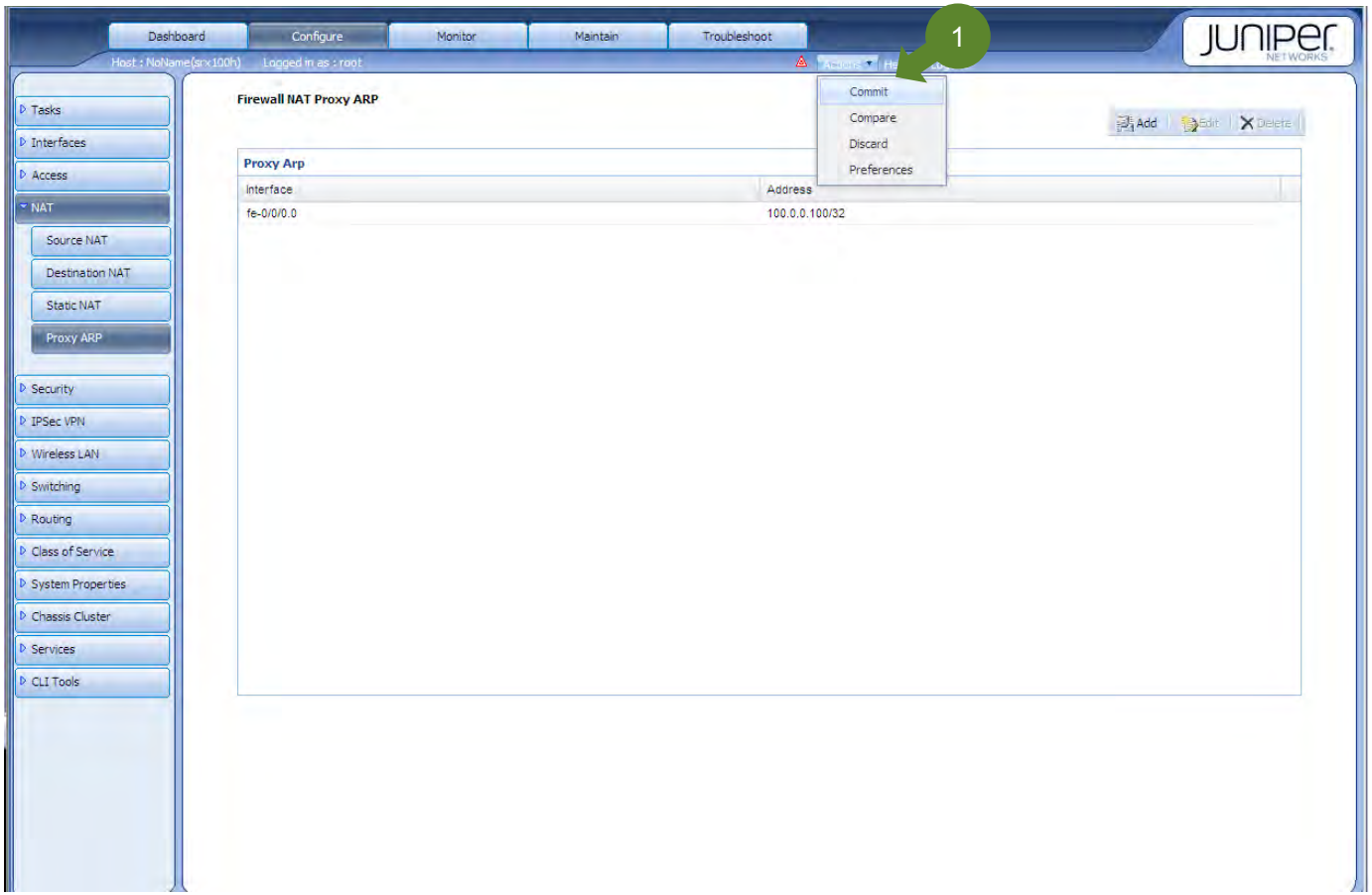
Static NAT設定 (8/9)

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)

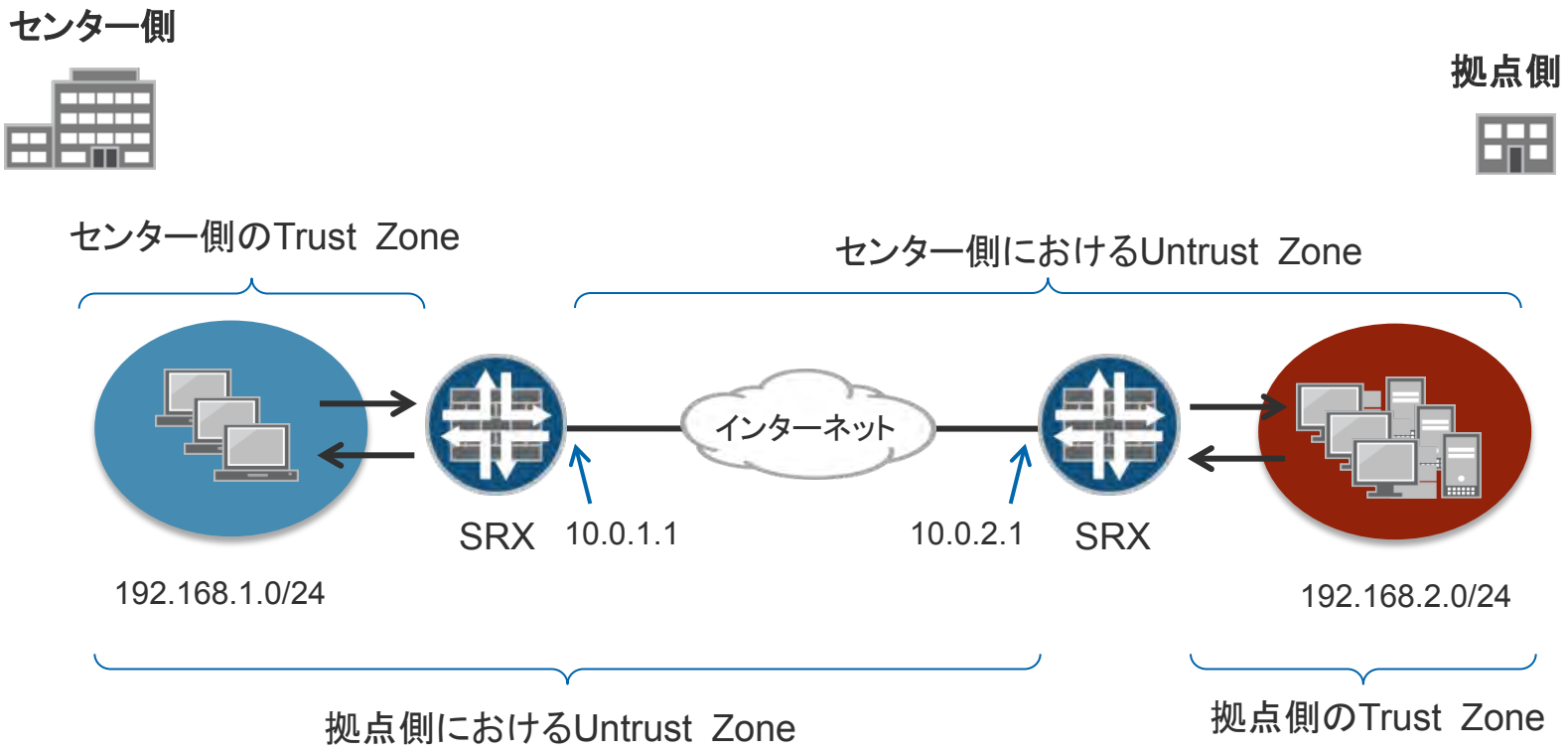
Proxy ARPの設定を終えたら、「Commit」ボタン①をクリックして終了です。



Chapter4. VPN

- Site-to-Site VPN
- リモートアクセスVPN

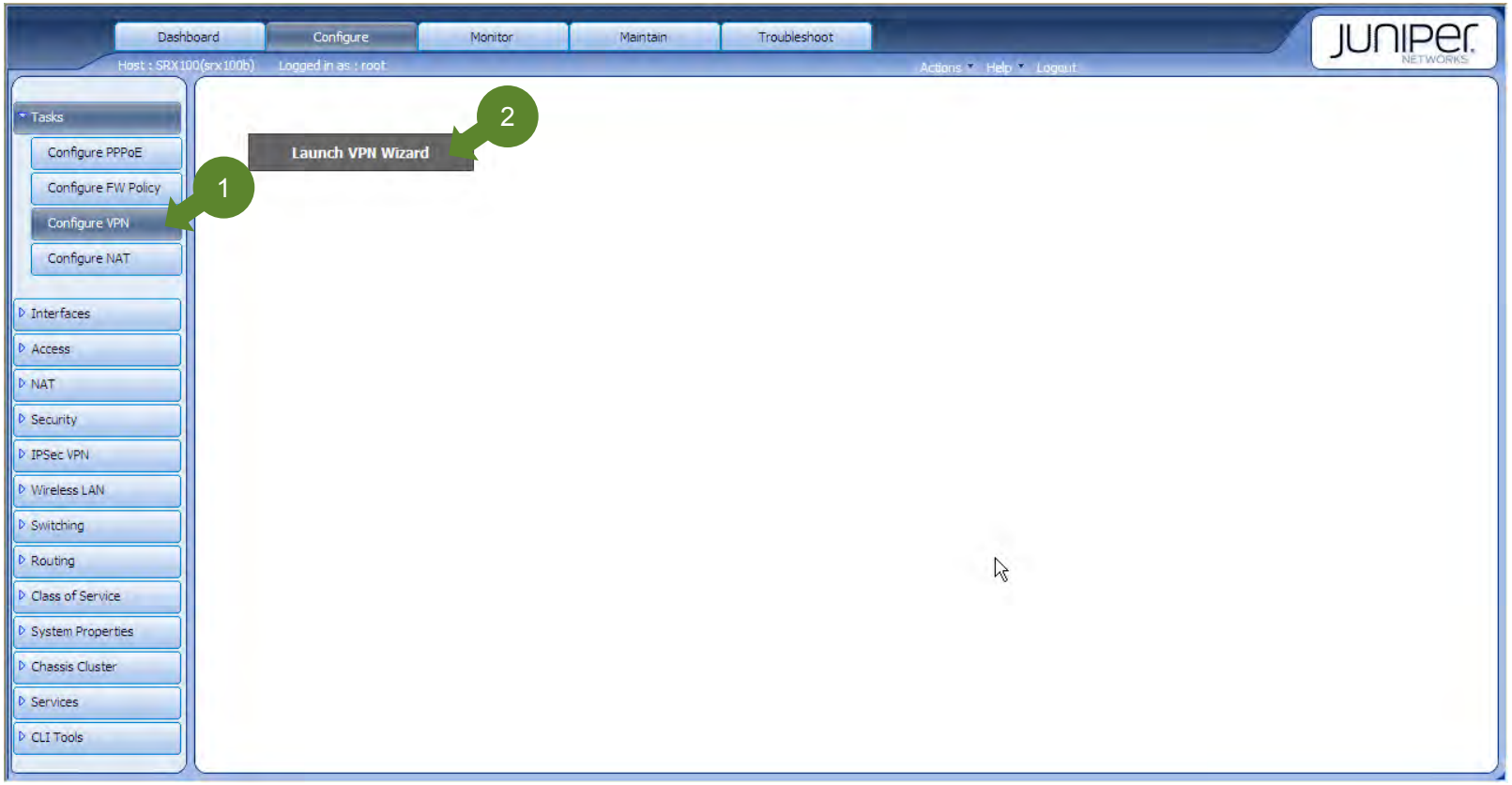
Site-to-Site VPN ー このガイドで構築する物理・論理構成



Site-to-Site VPN設定 (1/9)

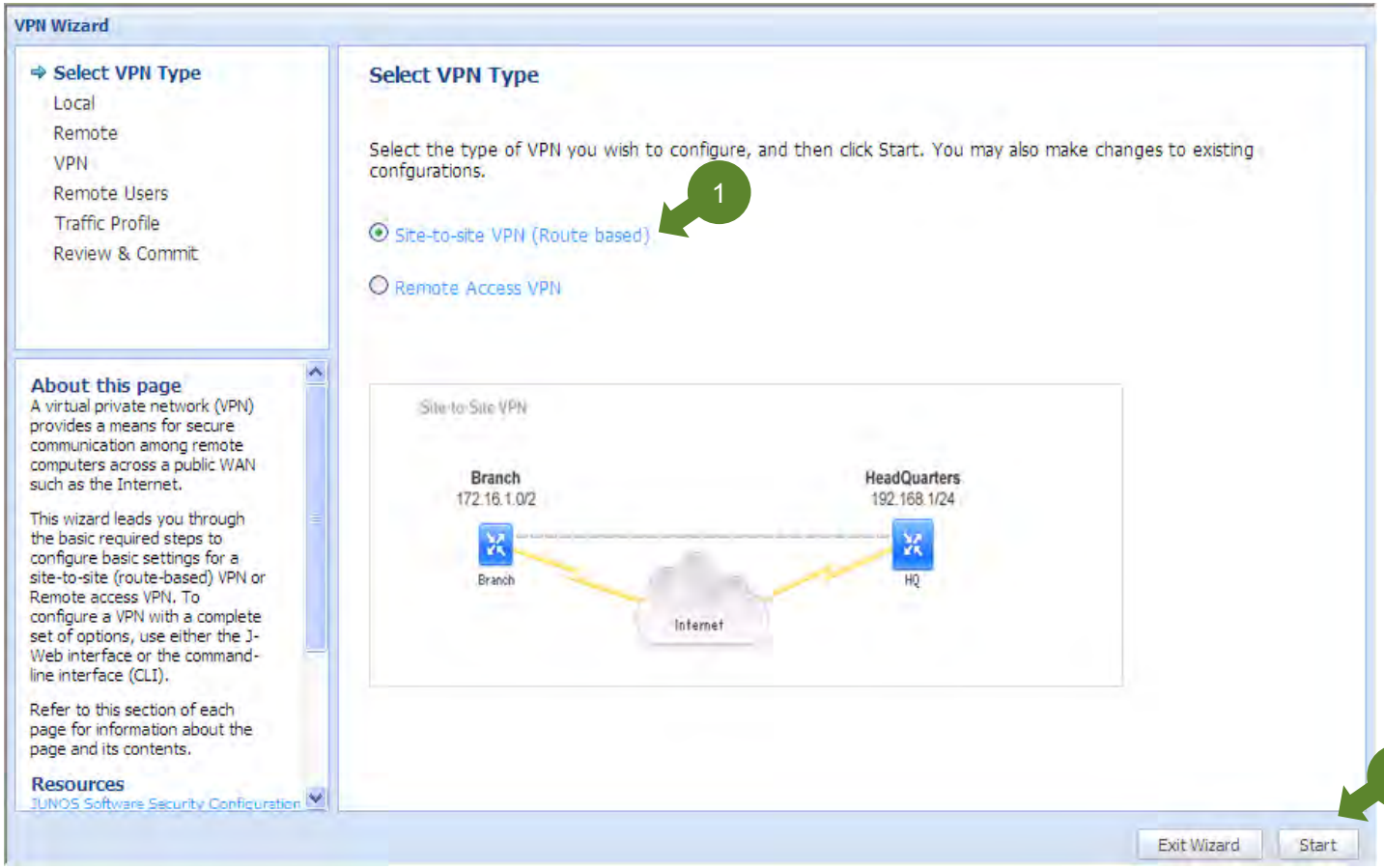
VPNの設定は、「VPN Wizard」を使用して簡単に作成することが可能です。

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。



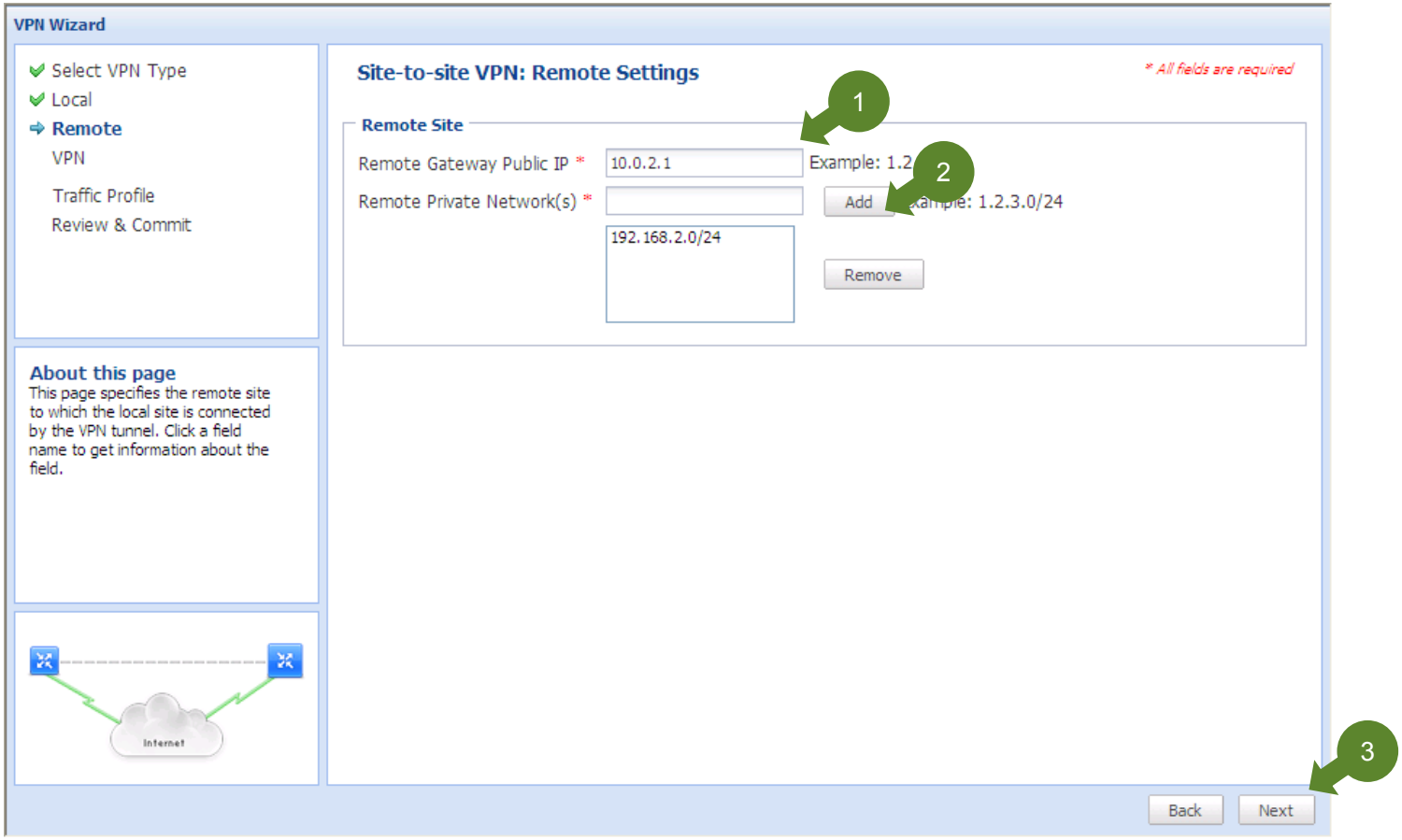
Site-to-Site VPN設定 (3/9)

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。

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。

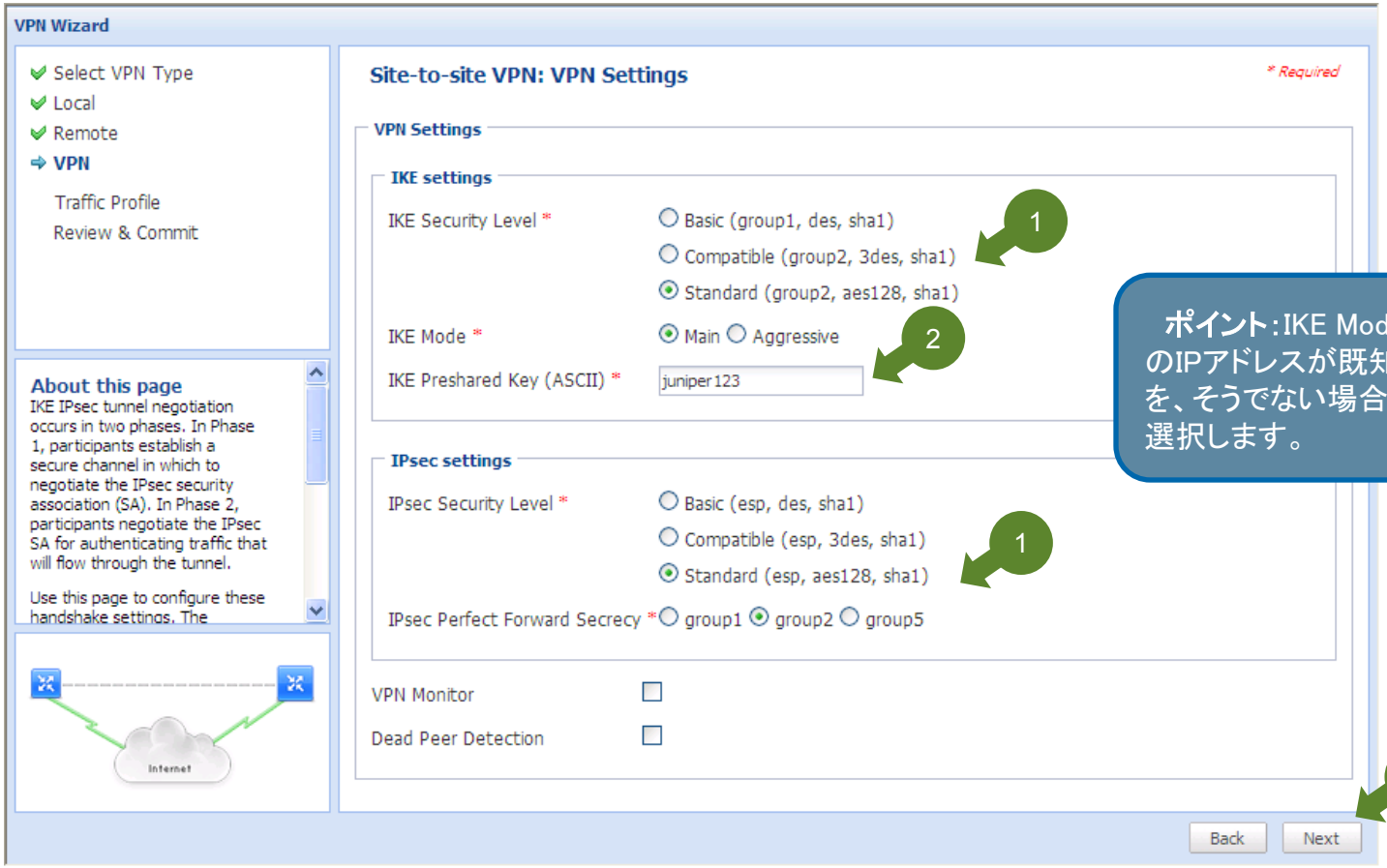
Site-to-Site VPN設定 (4/9)

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。



Site-to-Site VPN設定 (5/9)

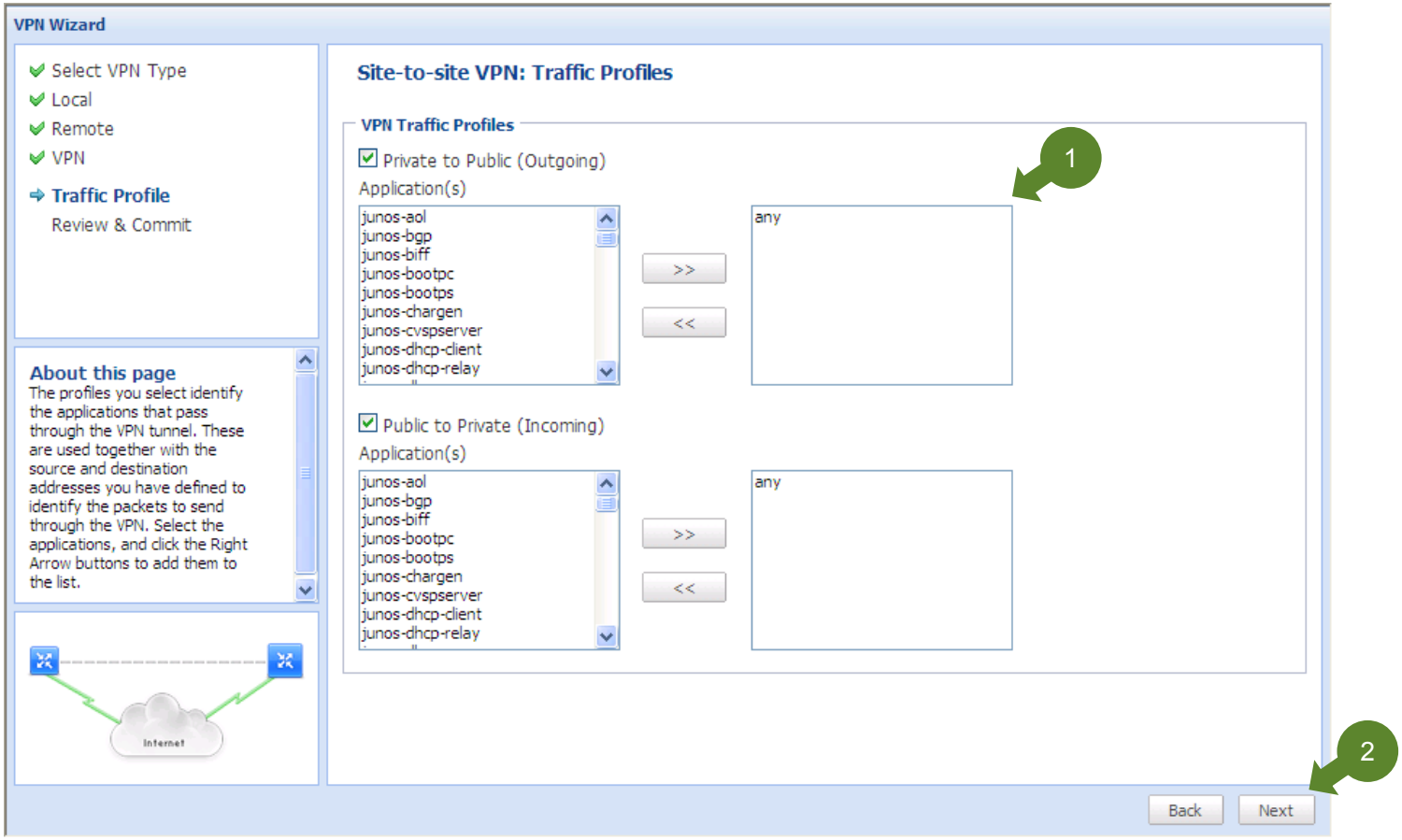
暗号化トンネルのセキュリティ強度を選択(①)し、事前共有鍵を設定し(②)、「Next」(③)を押します。



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。

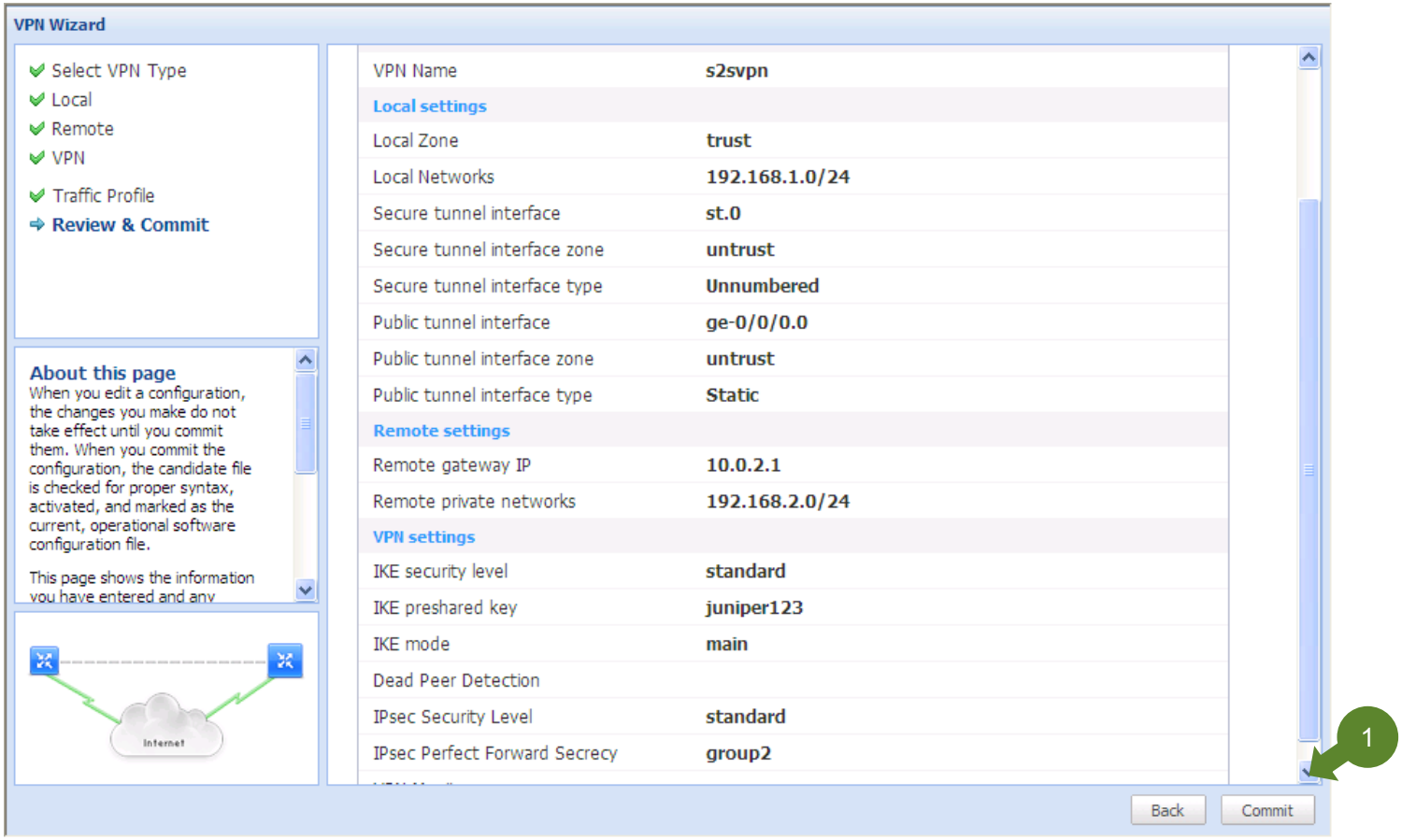
Site-to-Site VPN設定 (6/9)

暗号化対象となる通信を　指定（①）し、「Next」（②）を押します。



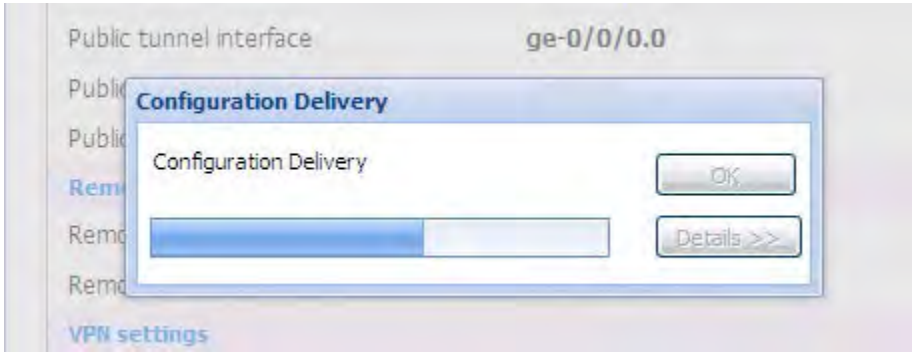
Site-to-Site VPN設定 (7/9)

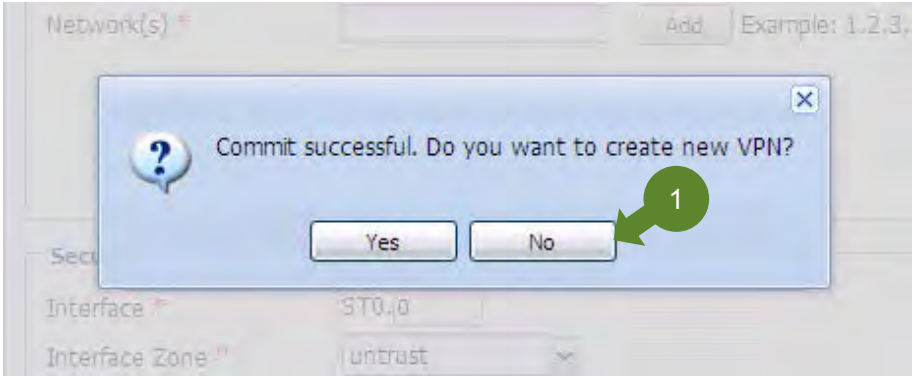
設定内容を確認し、問題が無ければ、「Commit」ボタン（①）をクリックします。



Site-to-Site VPN設定 (8/9)

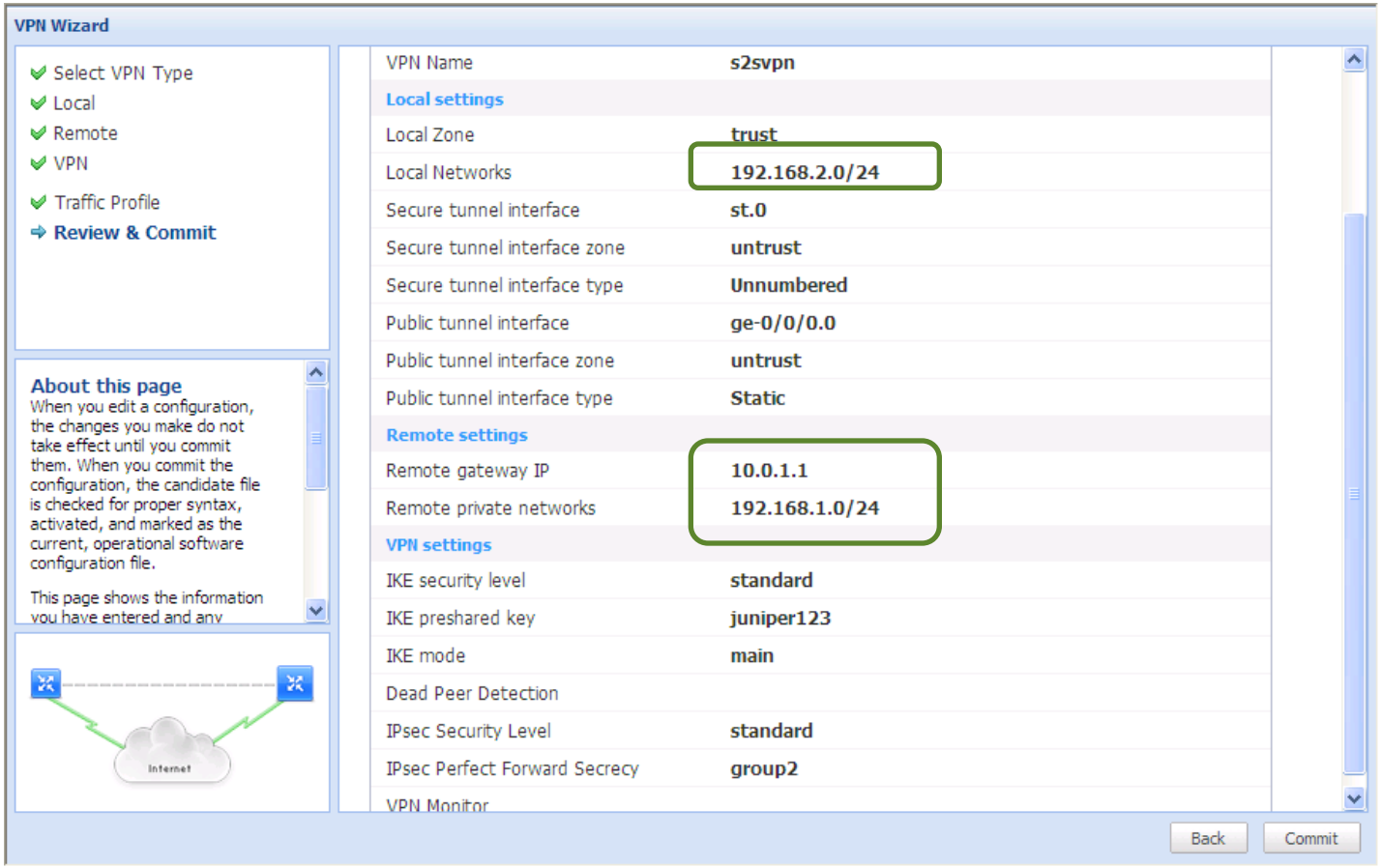
Commitプロセスが行われます。問題が無ければ、続けてVPNを設定するかどうかの確認画面が表示されますので、「No」をクリックして、Wizardを終了します。



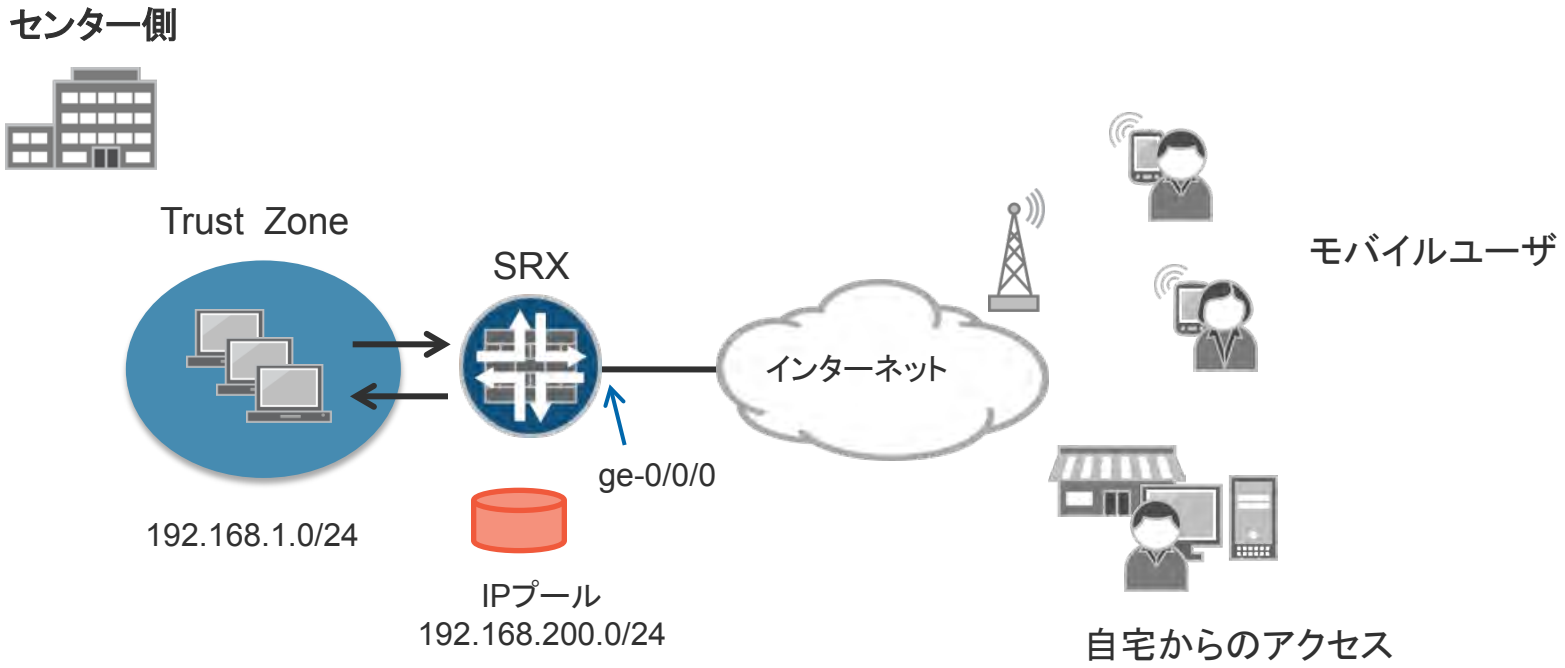


Site-to-Site VPN設定 (9/9)

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。

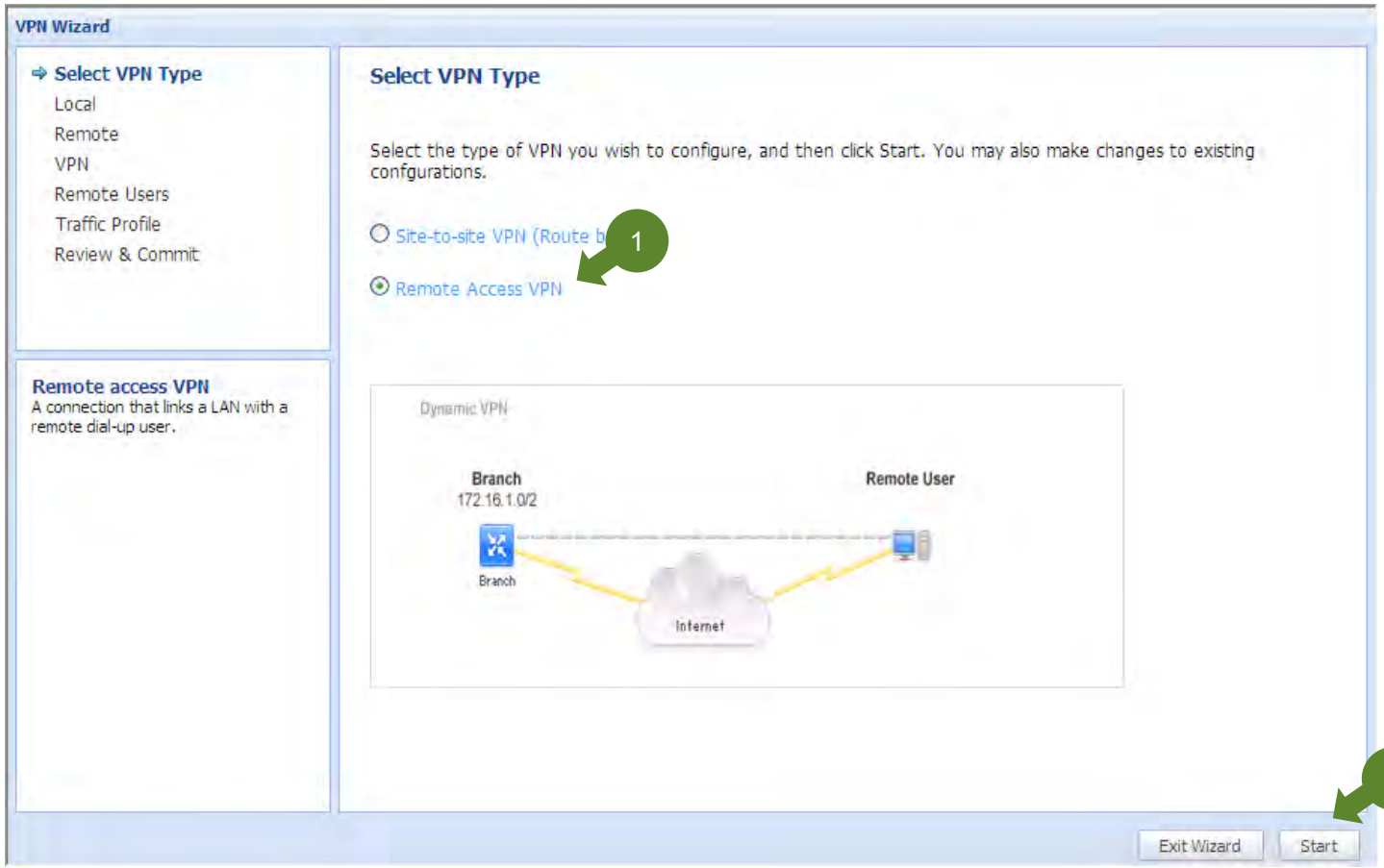


リモートアクセスVPN ー ネットワーク概要



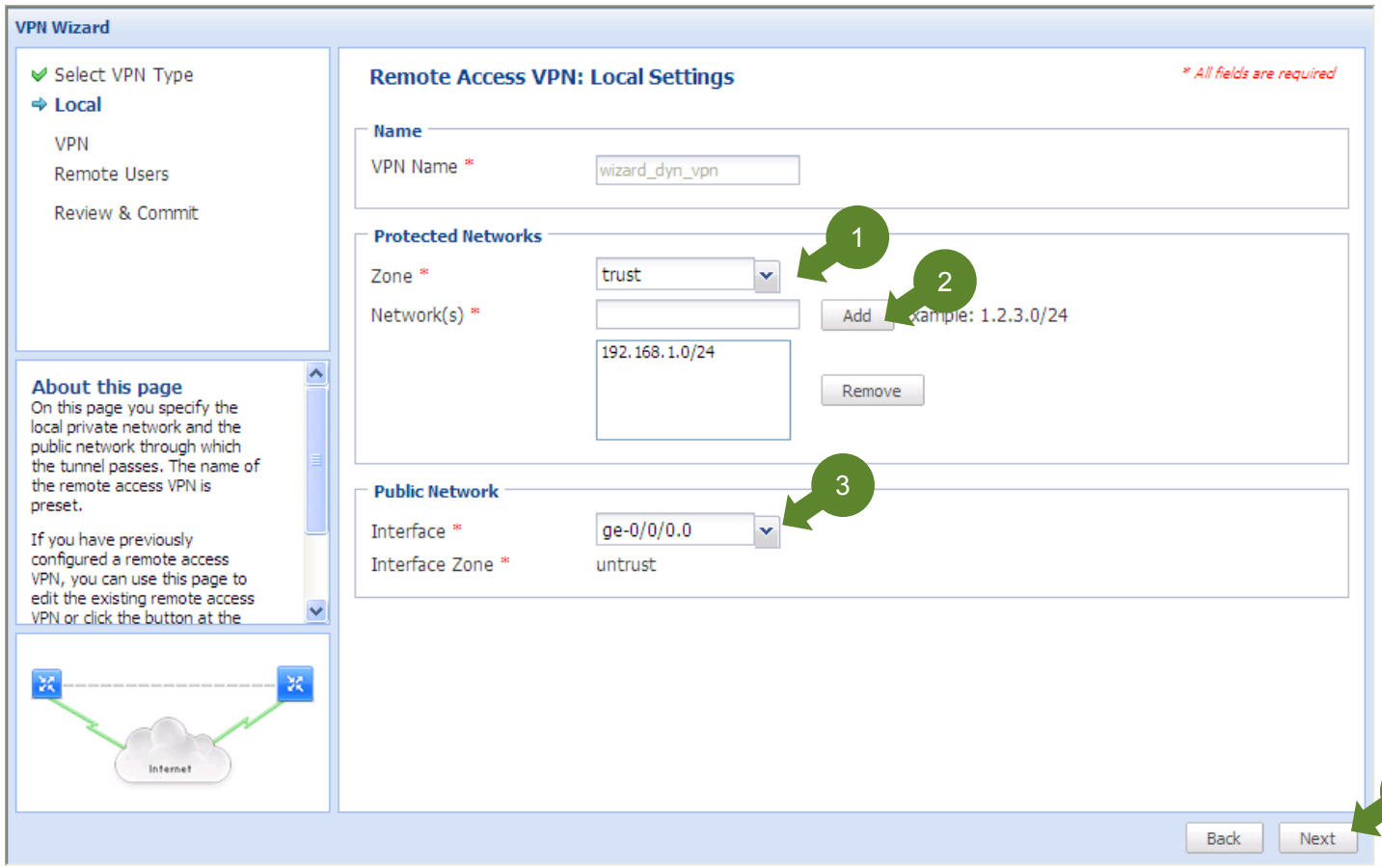
リモートアクセスVPN設定 (1/13)

「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。



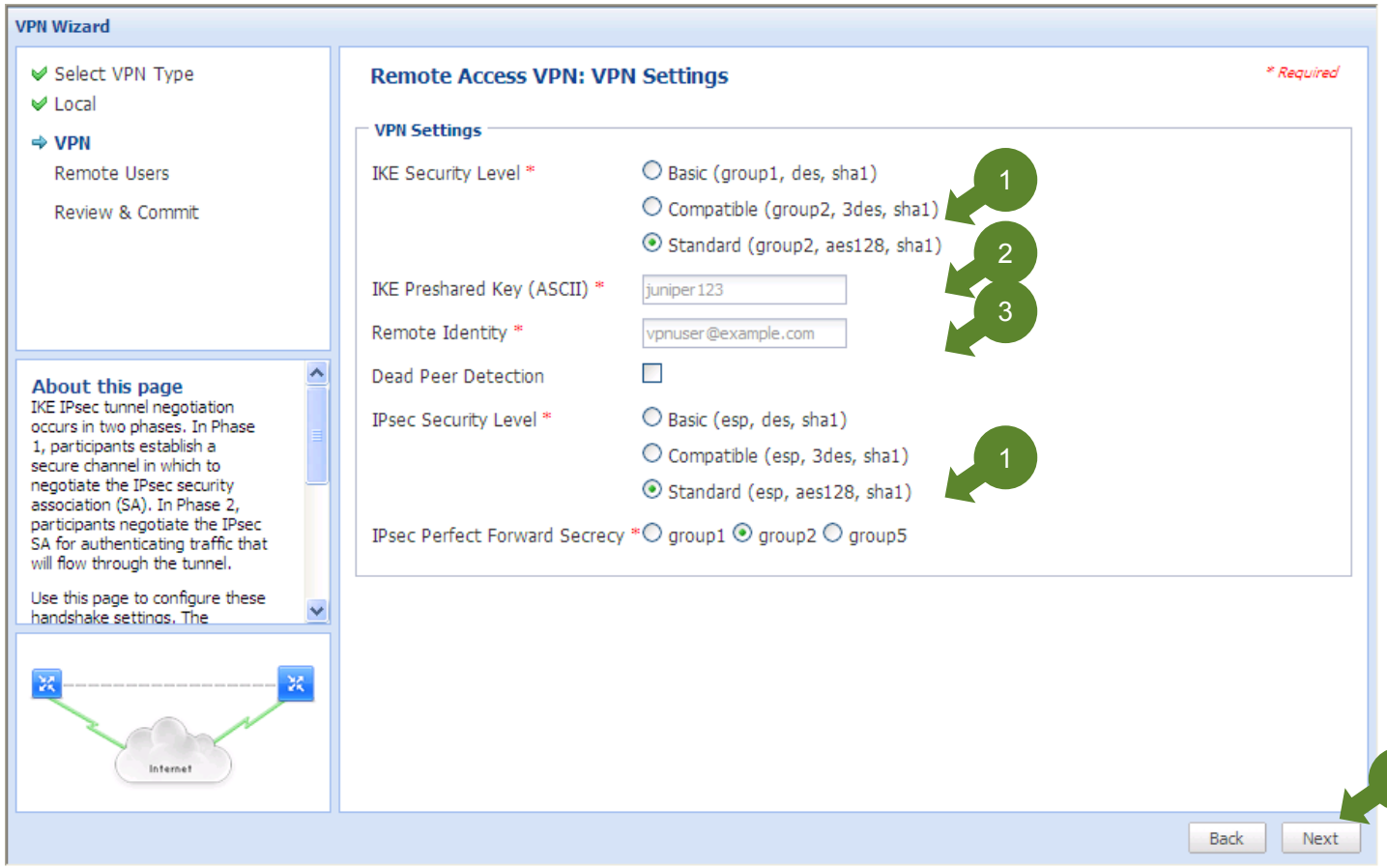
リモートアクセスVPN設定 (2/13)

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。



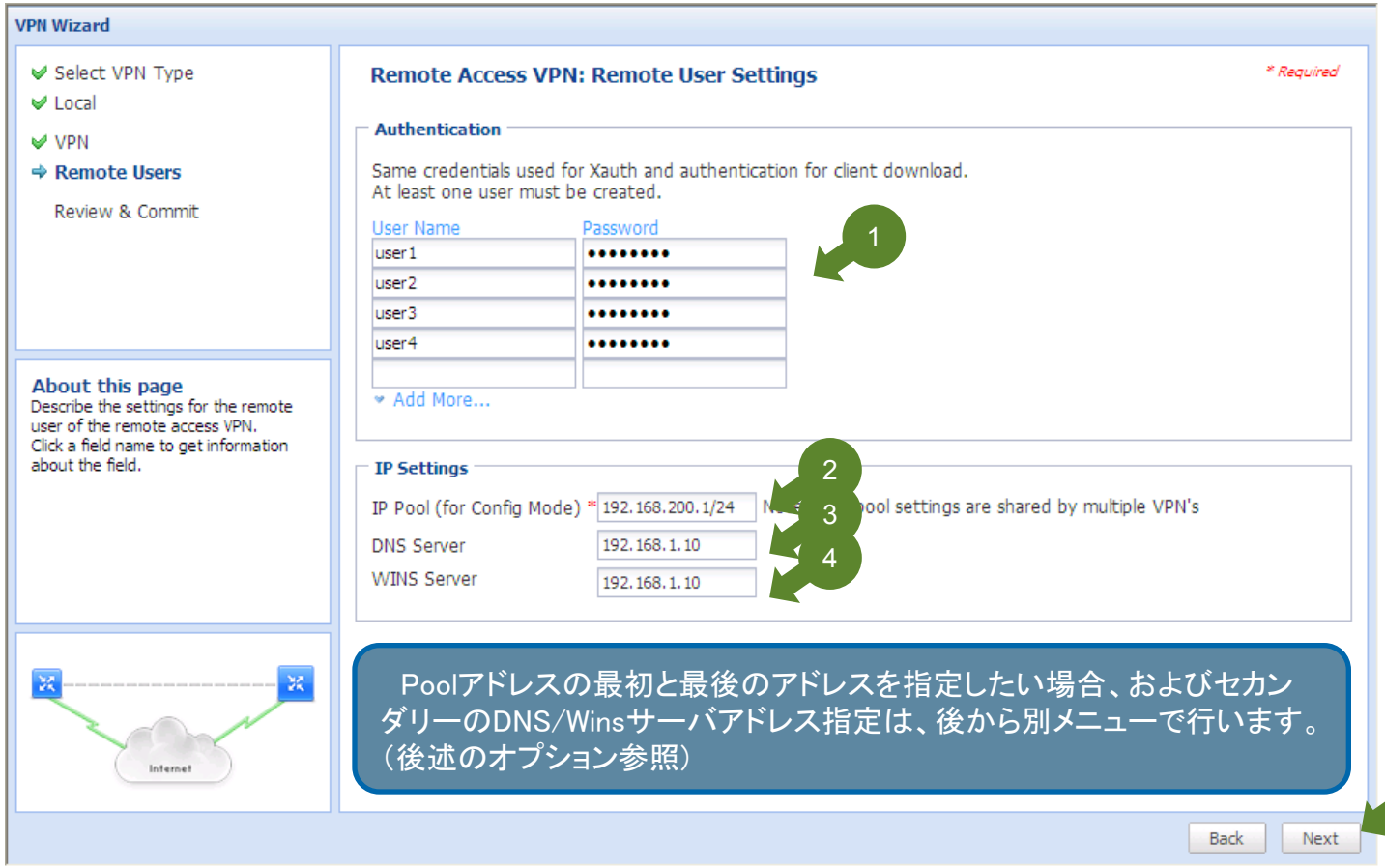
リモートアクセスVPN設定 (3/13)

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。



リモートアクセスVPN設定 (4/13)

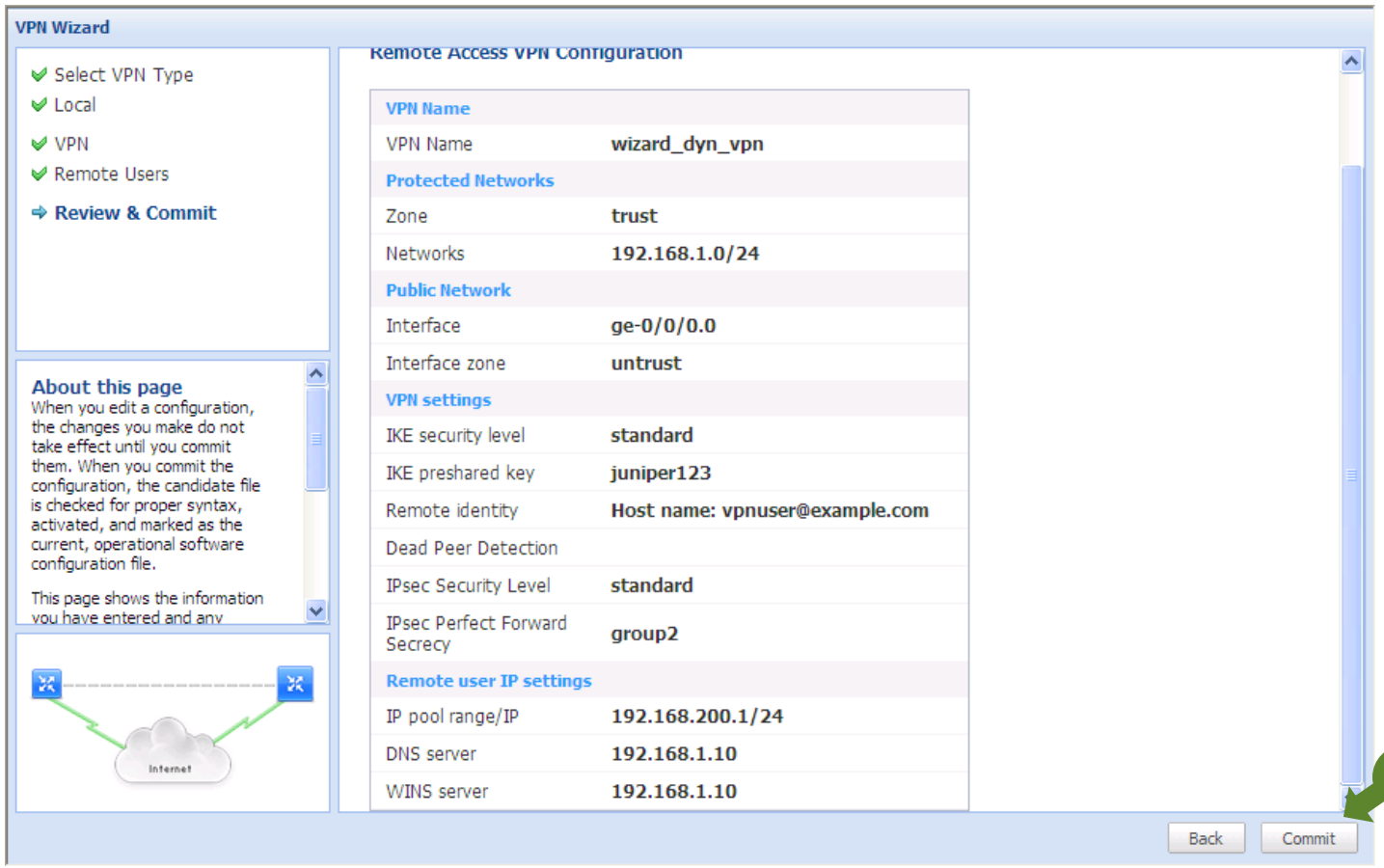
リモートアクセスを行うユーザ名・パスワードを登録（①）します。また内部ルーティングのために、リモートアクセスクライアントに割り当てるプールアドレス（②）、DNSサーバ（③）、WINSサーバアドレス（④）を指定します。最後に「Next」（⑤）を押します。



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）

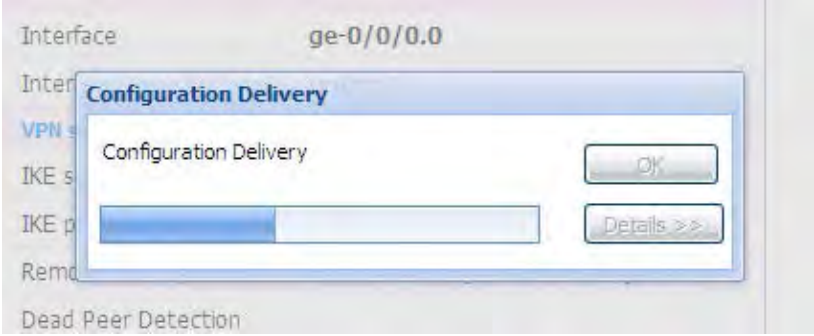
リモートアクセスVPN設定 (5/13)

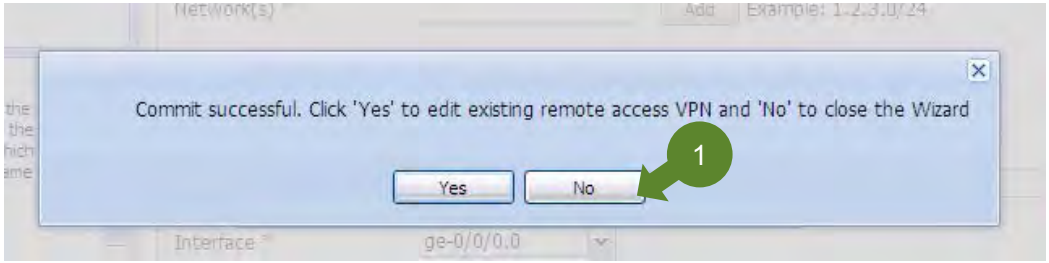
設定内容を確認し、問題が無ければ、「Commit」ボタン（①）をクリックします。



リモートアクセスVPN設定 (6/13)

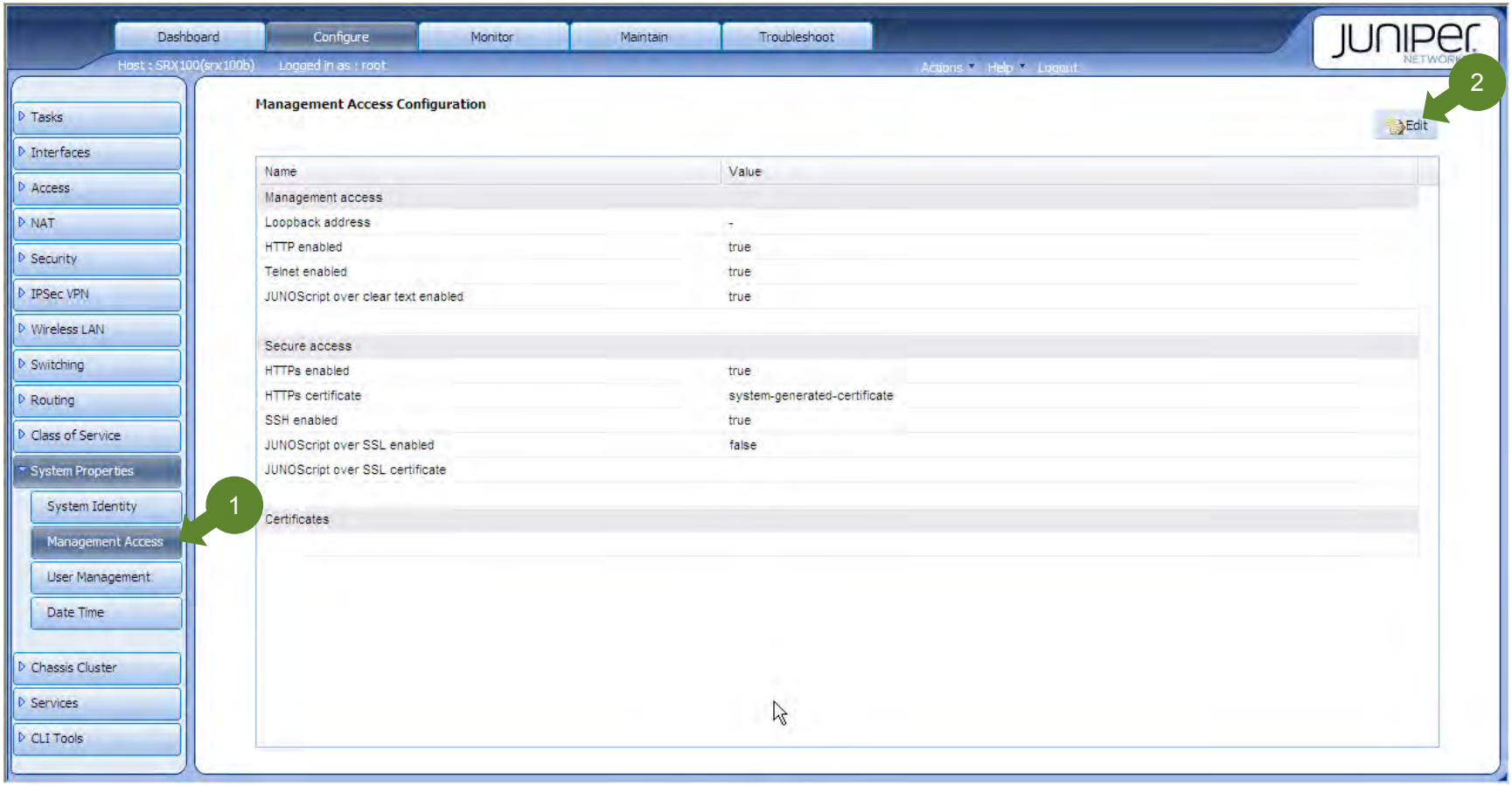
Commitプロセスが行われます。問題が無ければ、続けてVPNを設定するかどうかの確認画面が表示されますので、「No」をクリックして、Wizardを終了します。





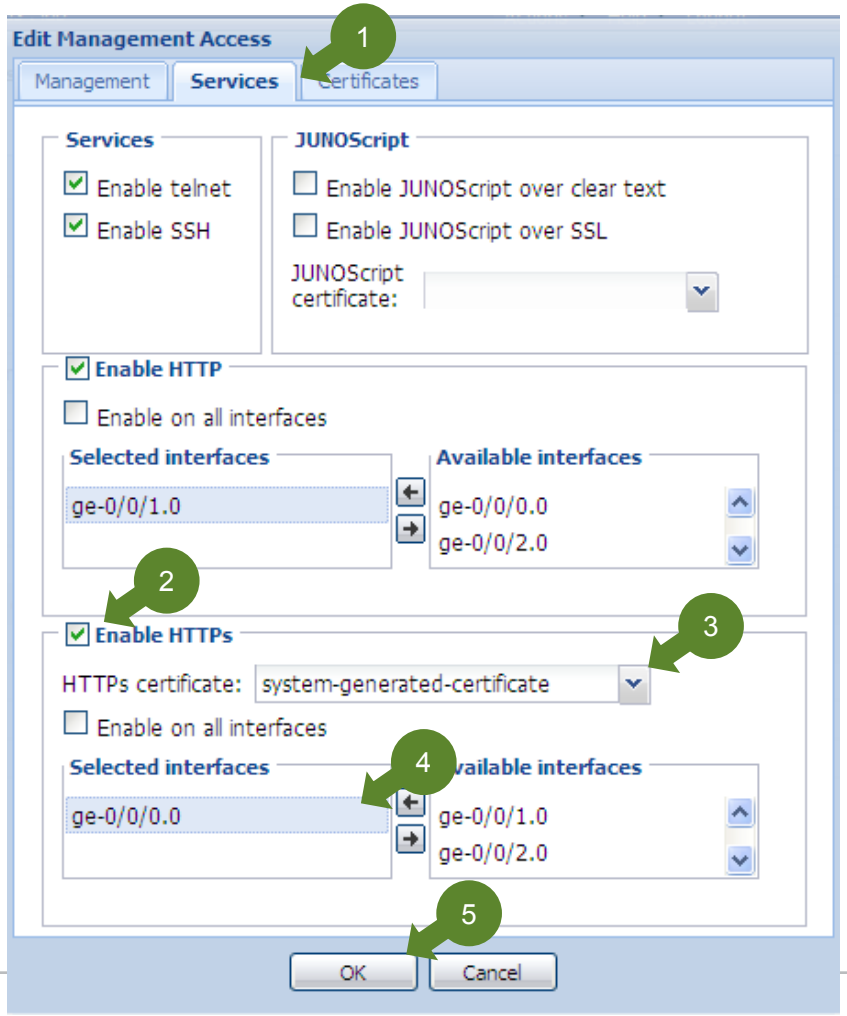
リモートアクセスVPN設定 (7/13)

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。



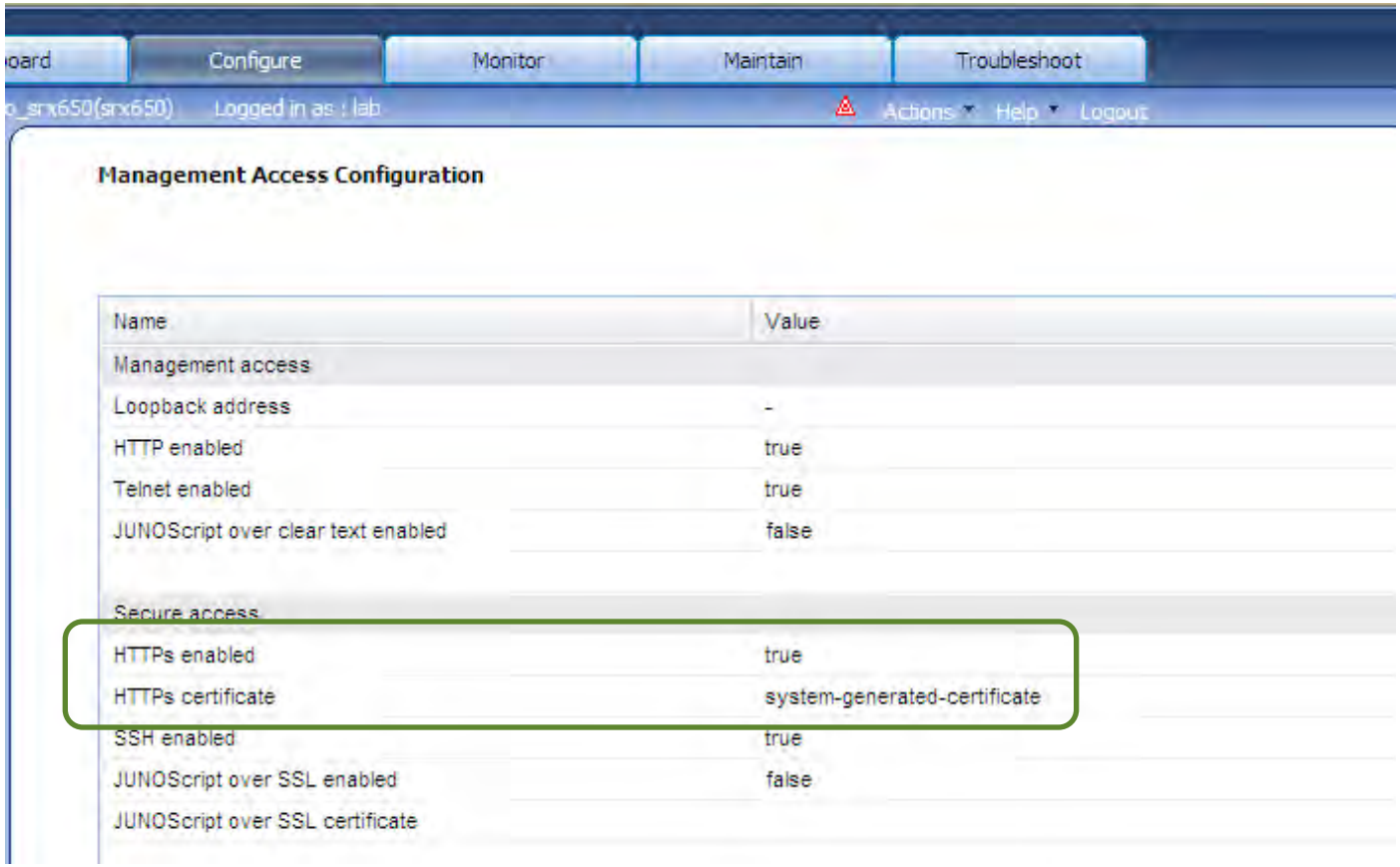
リモートアクセスVPN設定 (8/13)

「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。



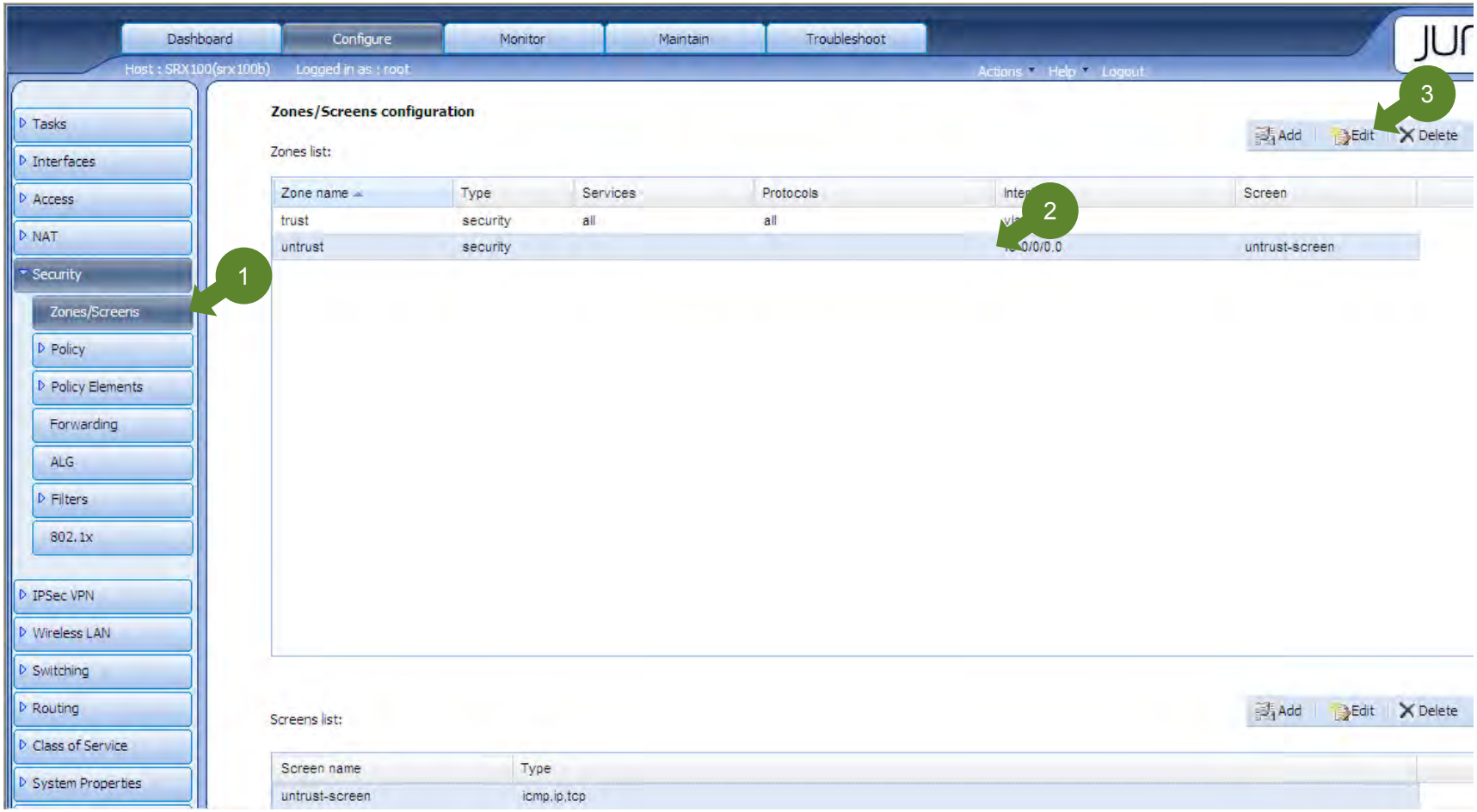
リモートアクセスVPN設定 (9/13)

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。



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。

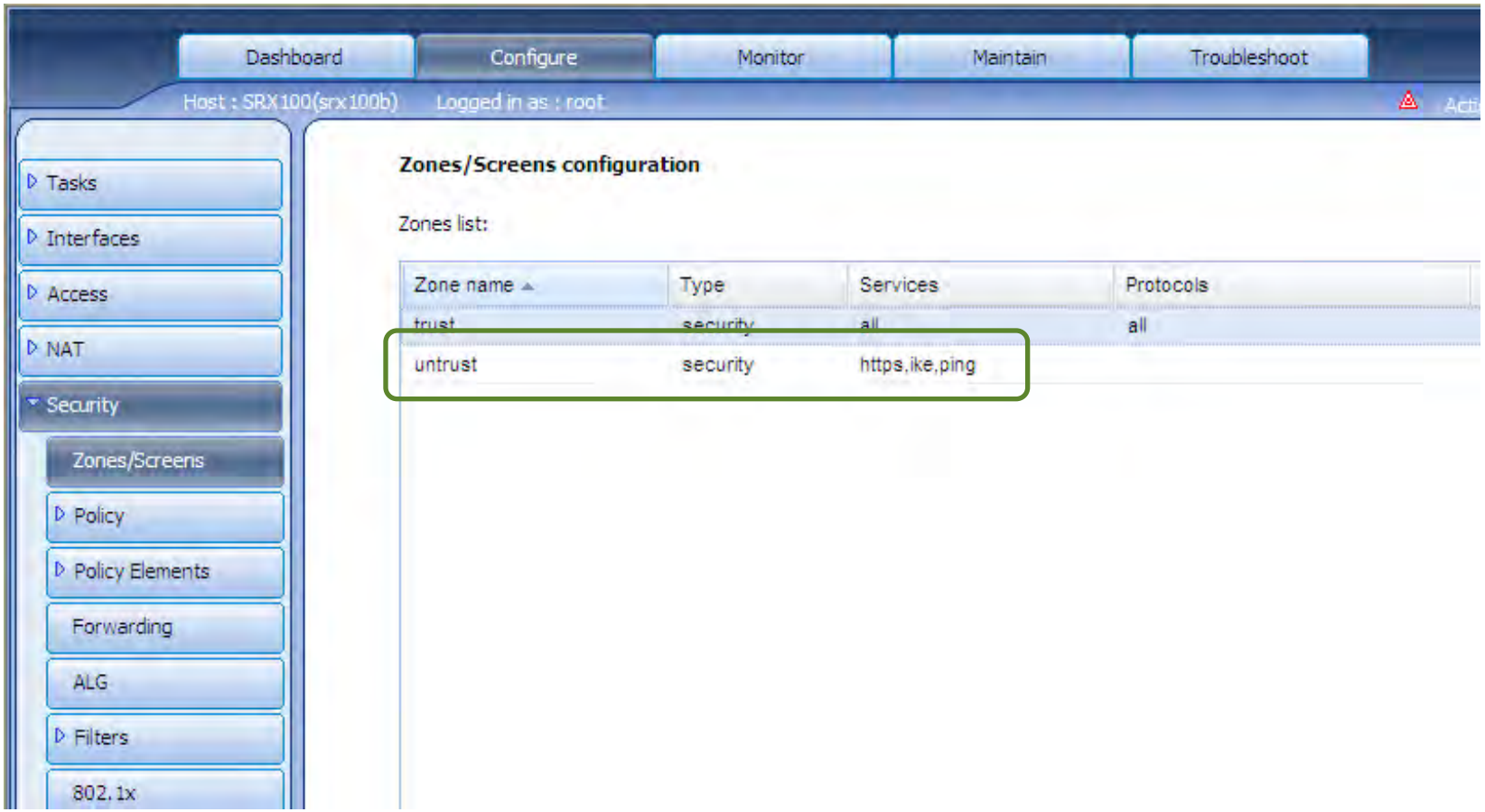


リモートアクセスVPN設定 (11/13)

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。

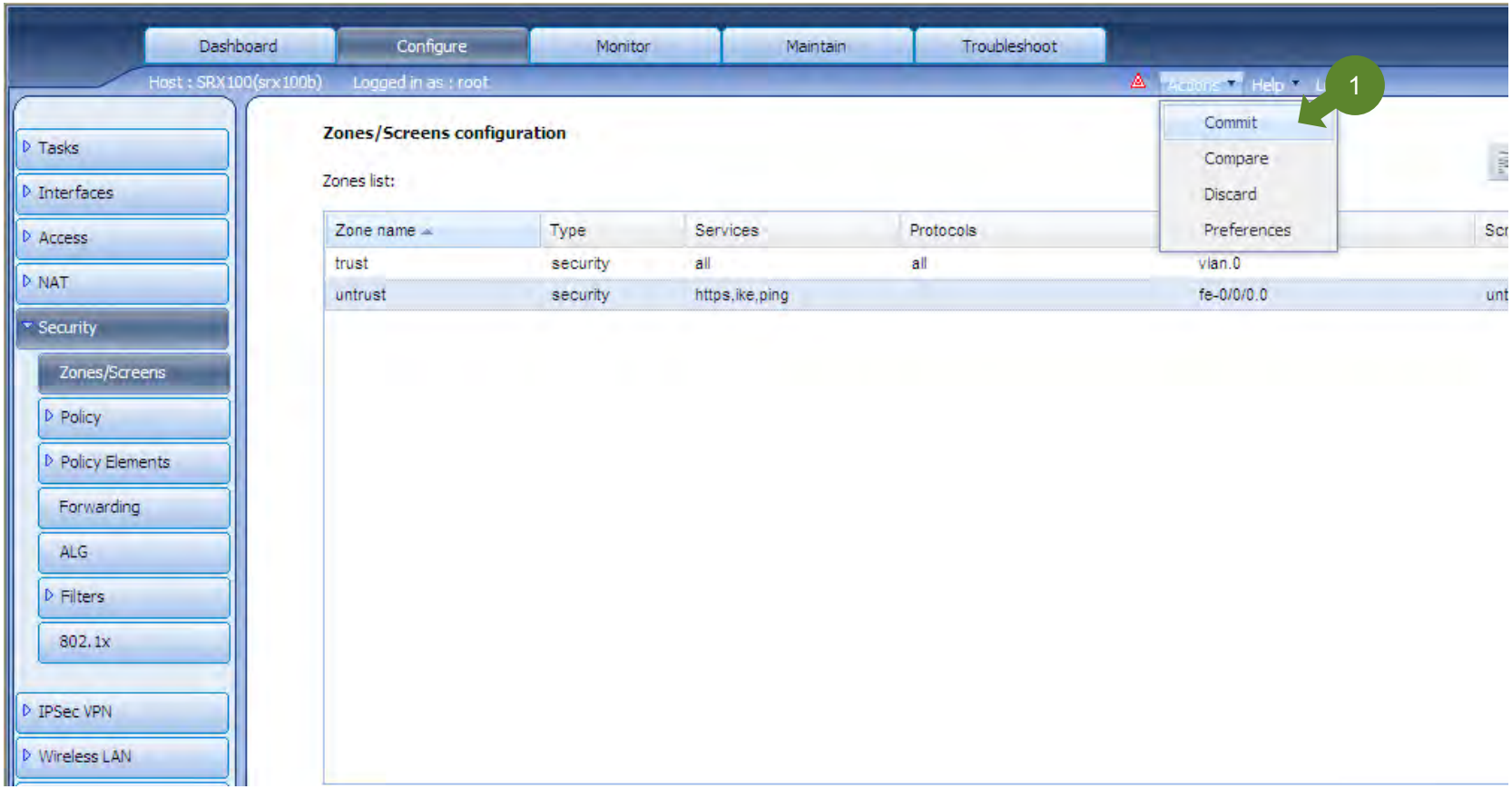
リモートアクセスVPN設定 (12/13)

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。



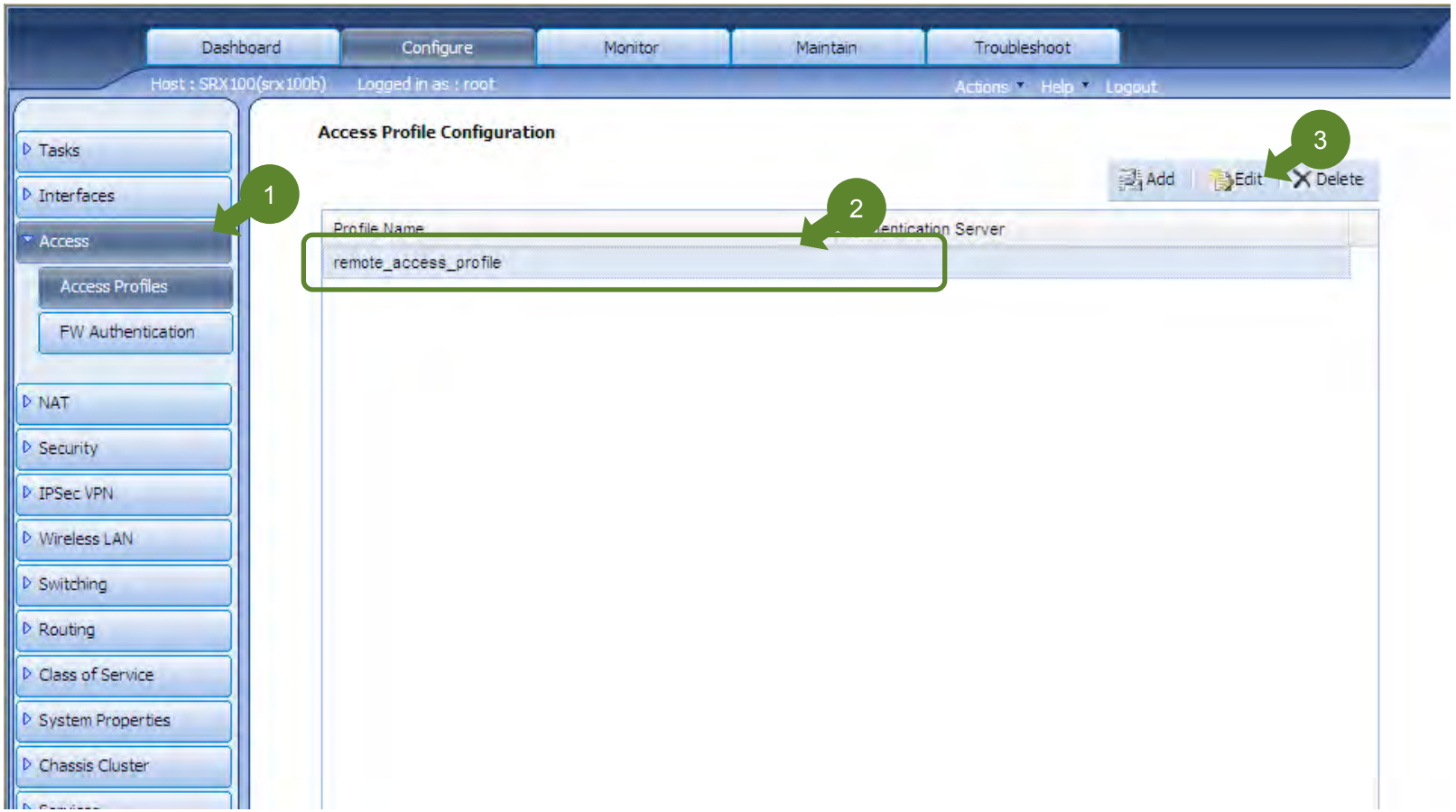
リモートアクセスVPN設定 (13/13)

「Actions」->「Commit」を選択（①）し、設定を反映させます。



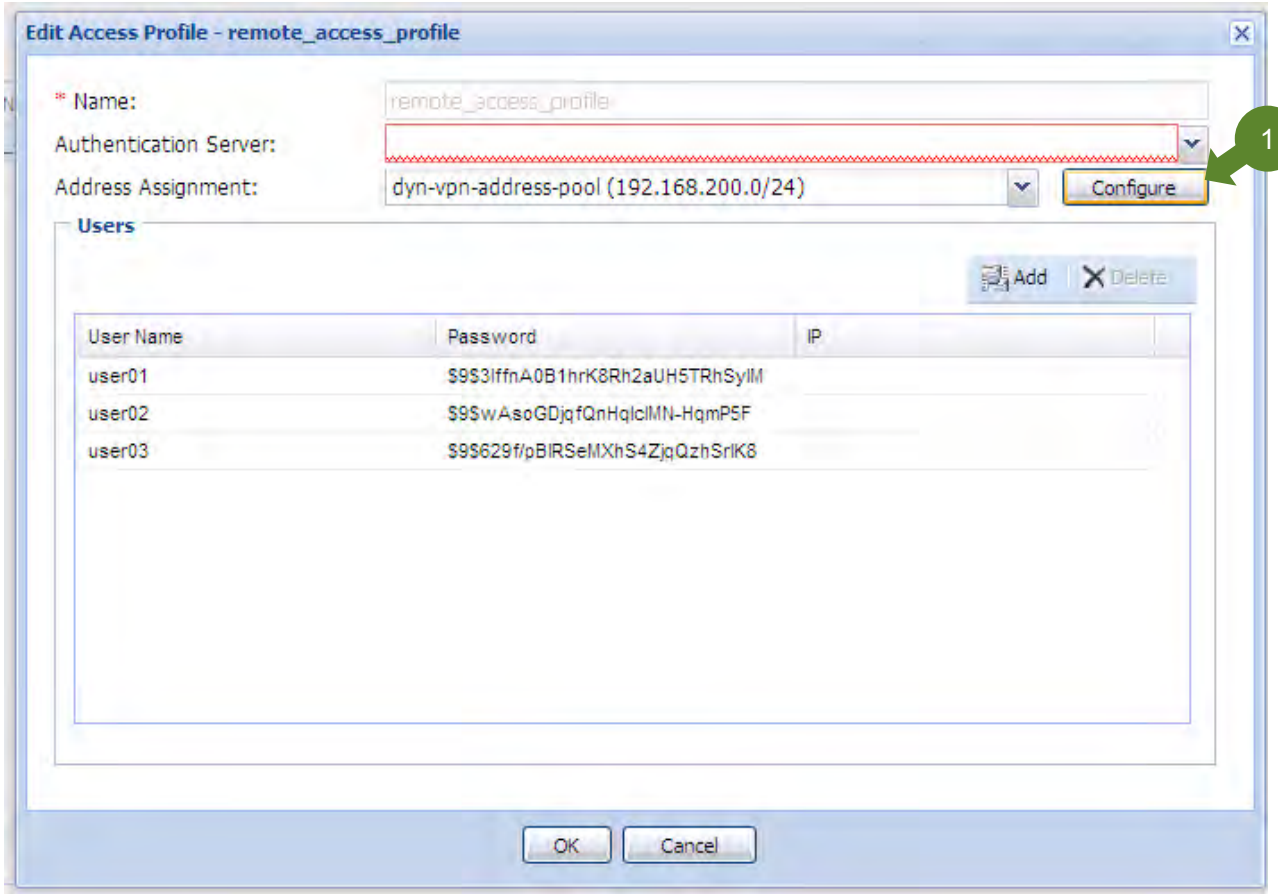
リモートアクセスVPN設定 – オプション(1/6)

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。



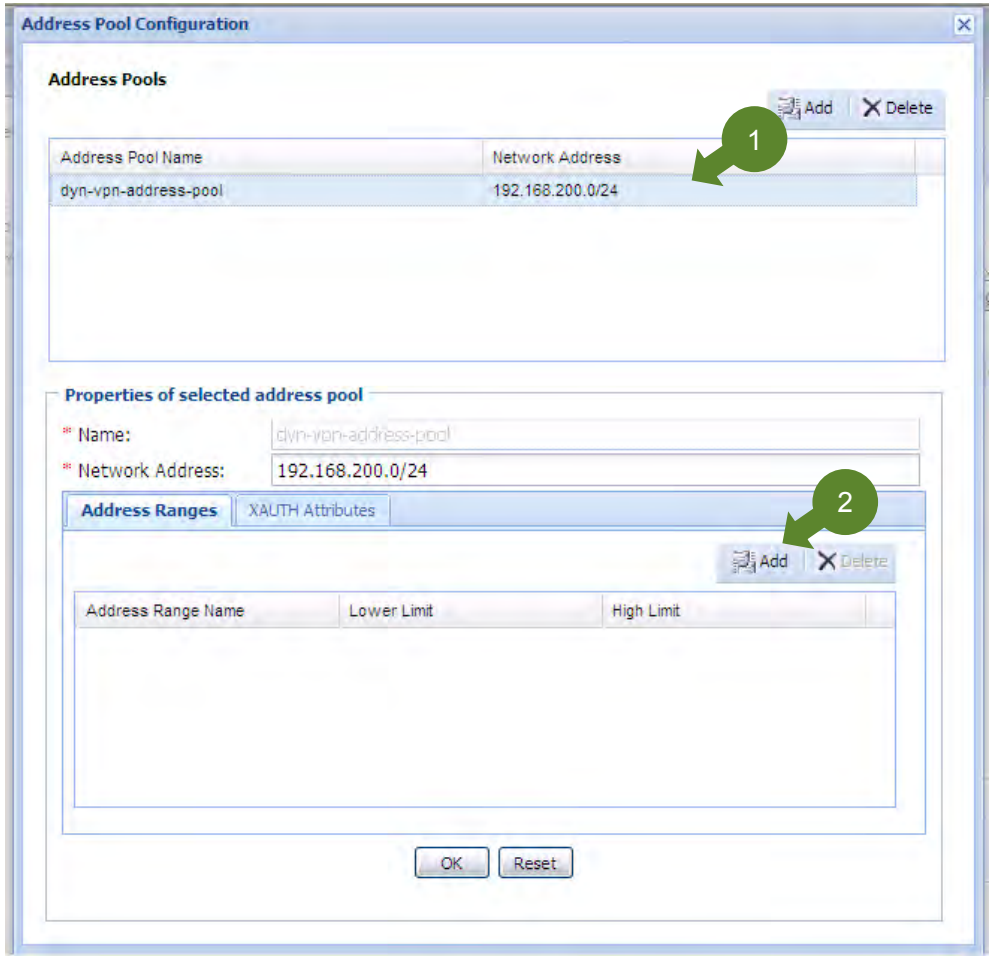
リモートアクセスVPN設定 – オプション(2/6)

「Configure」ボタンをクリック(①)します。



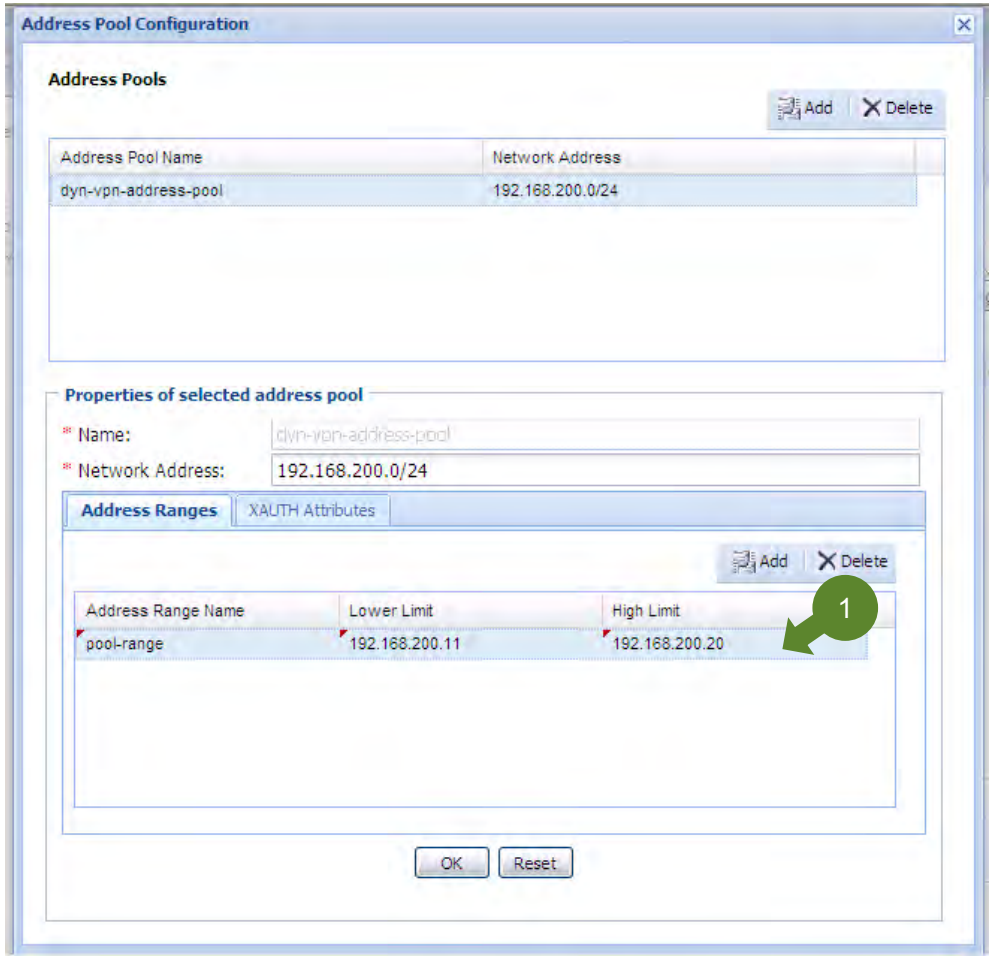
リモートアクセスVPN設定 – オプション(3/6)

「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。



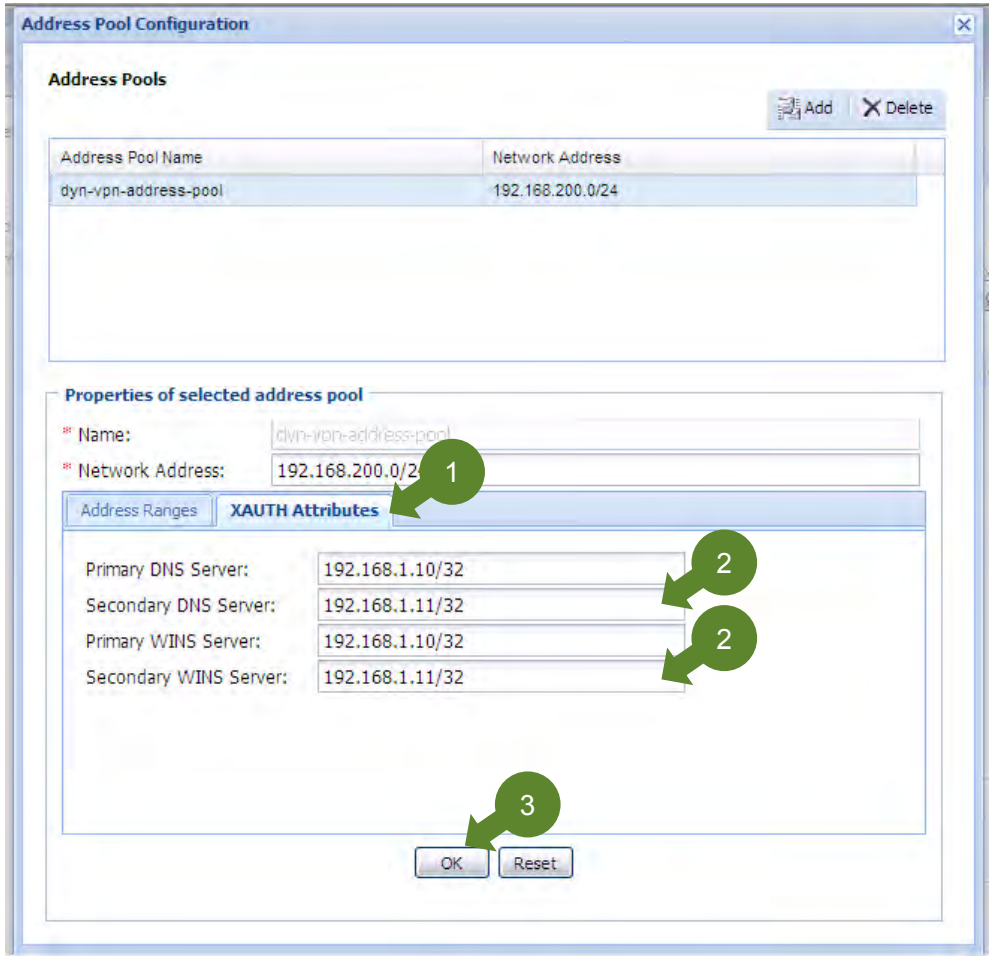
リモートアクセスVPN設定 – オプション(4/6)

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）。



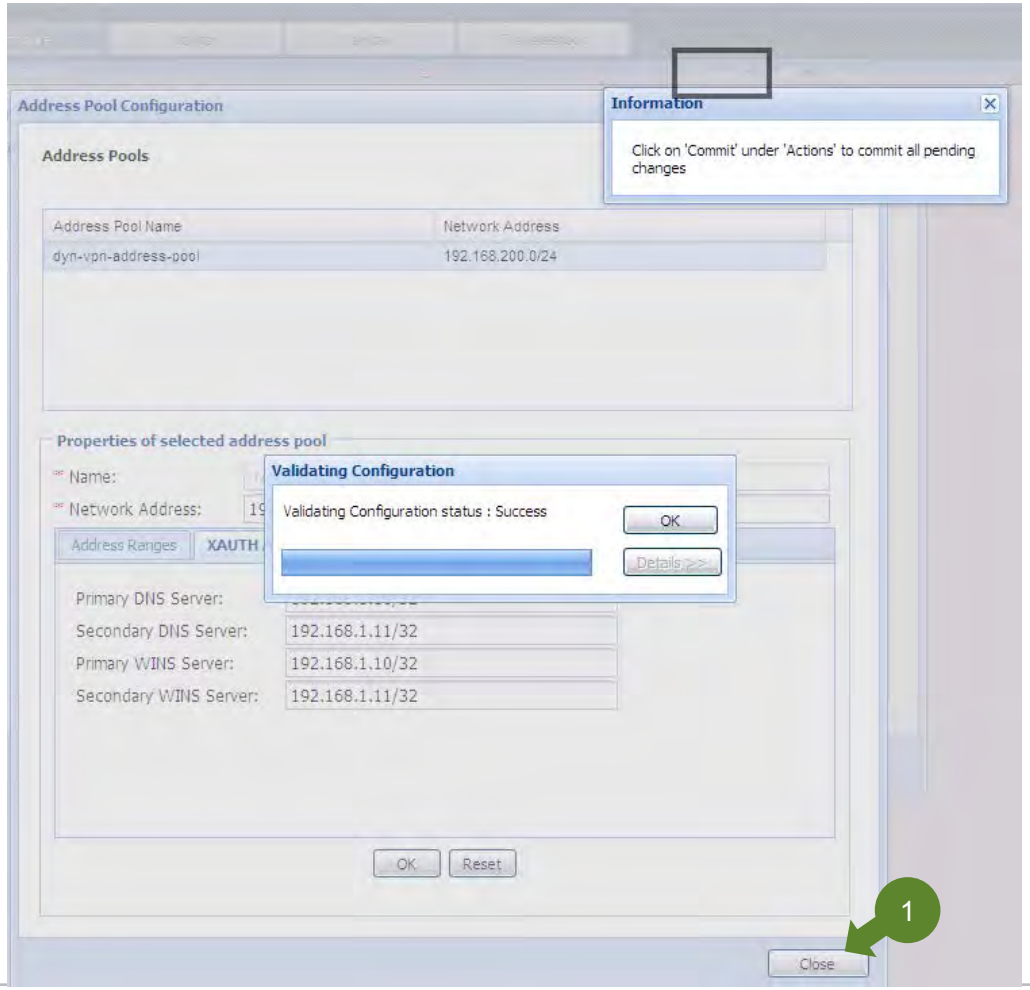
リモートアクセスVPN設定 – オプション(5/6)

「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。



リモートアクセスVPN設定 – オプション(6/6)

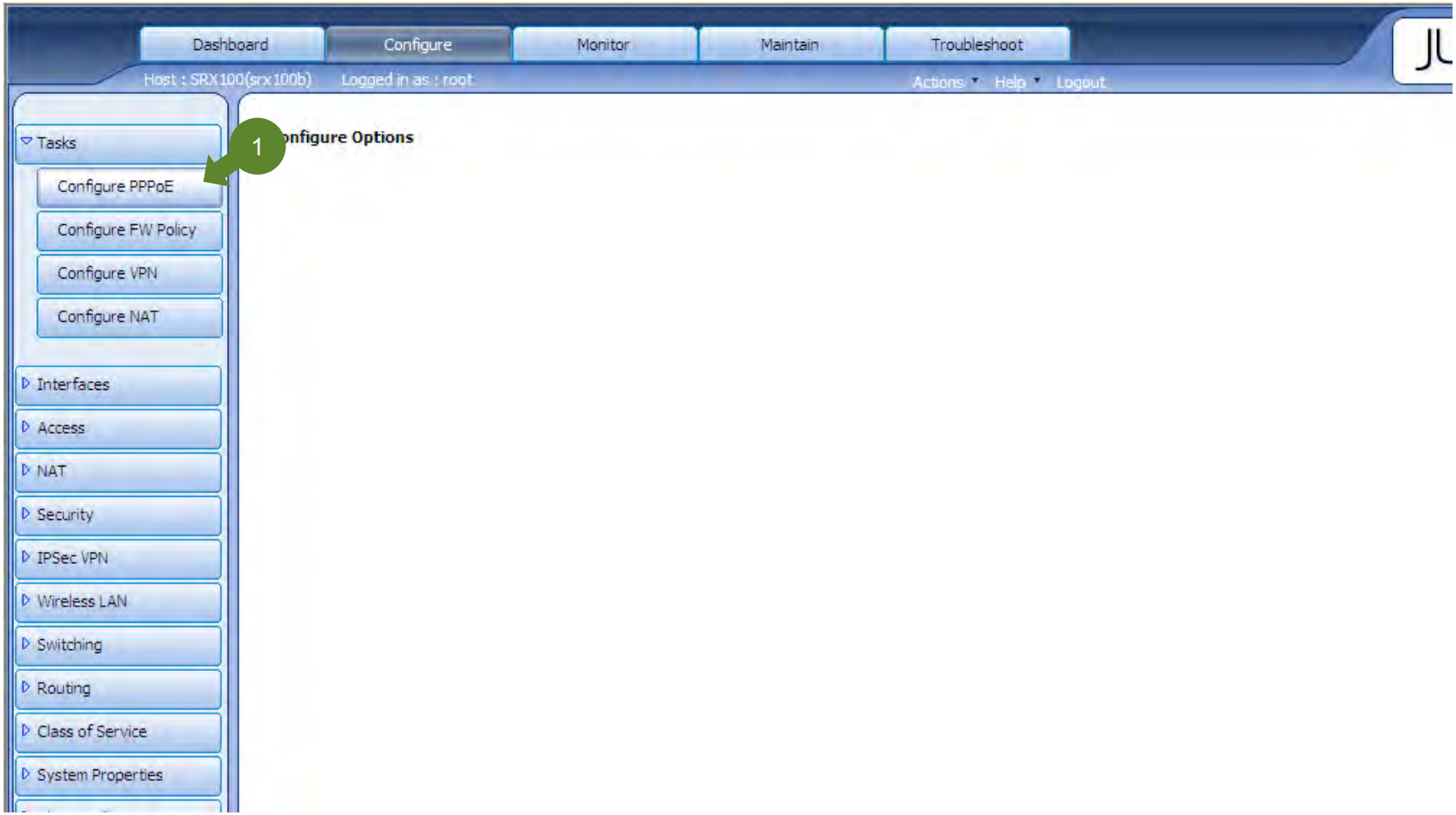
「Close」ボタンをクリック(①)後、Commitボタンをクリックし、設定を反映させます。



Chapter5. PPPoE

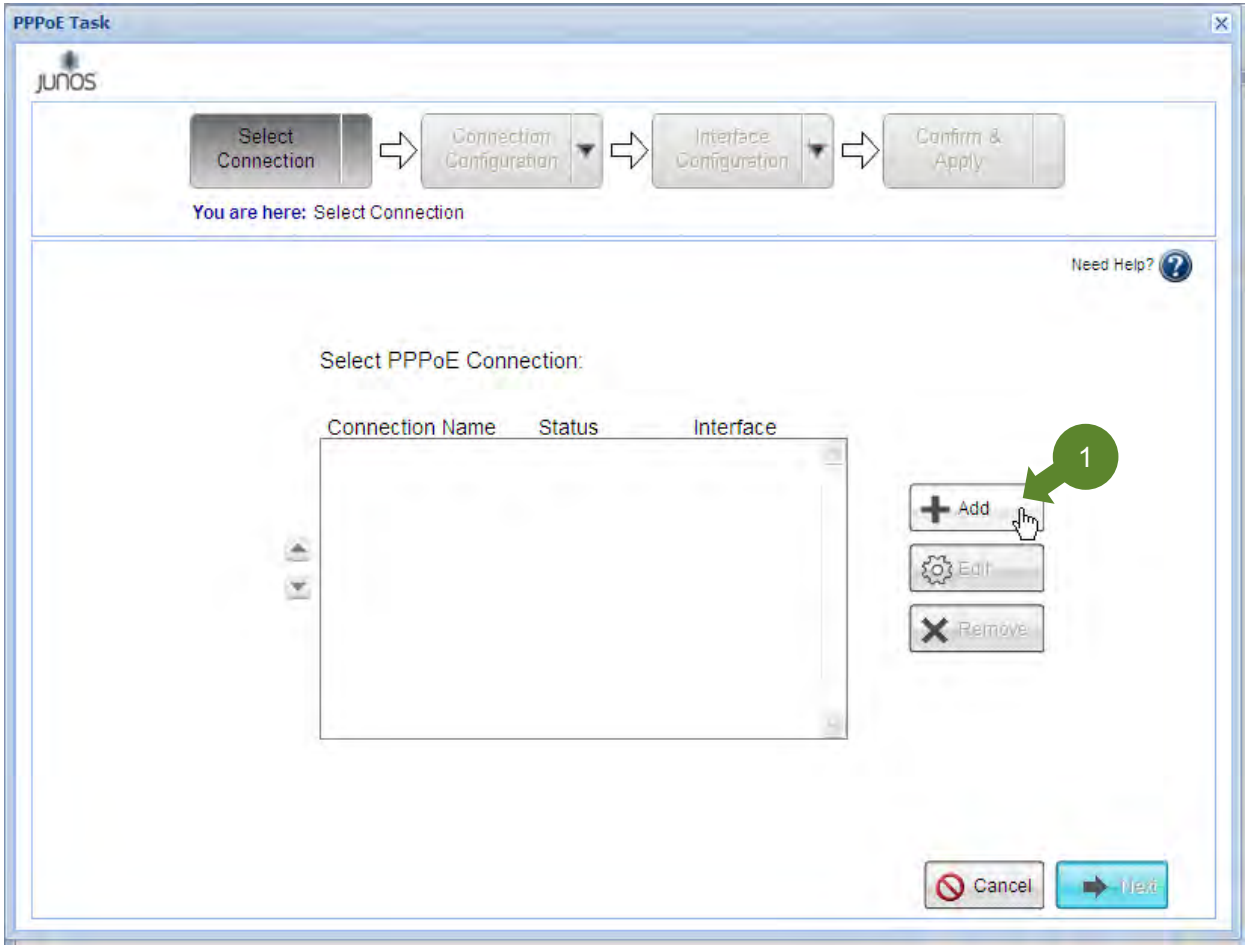
PPPoE設定(1/22)

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）



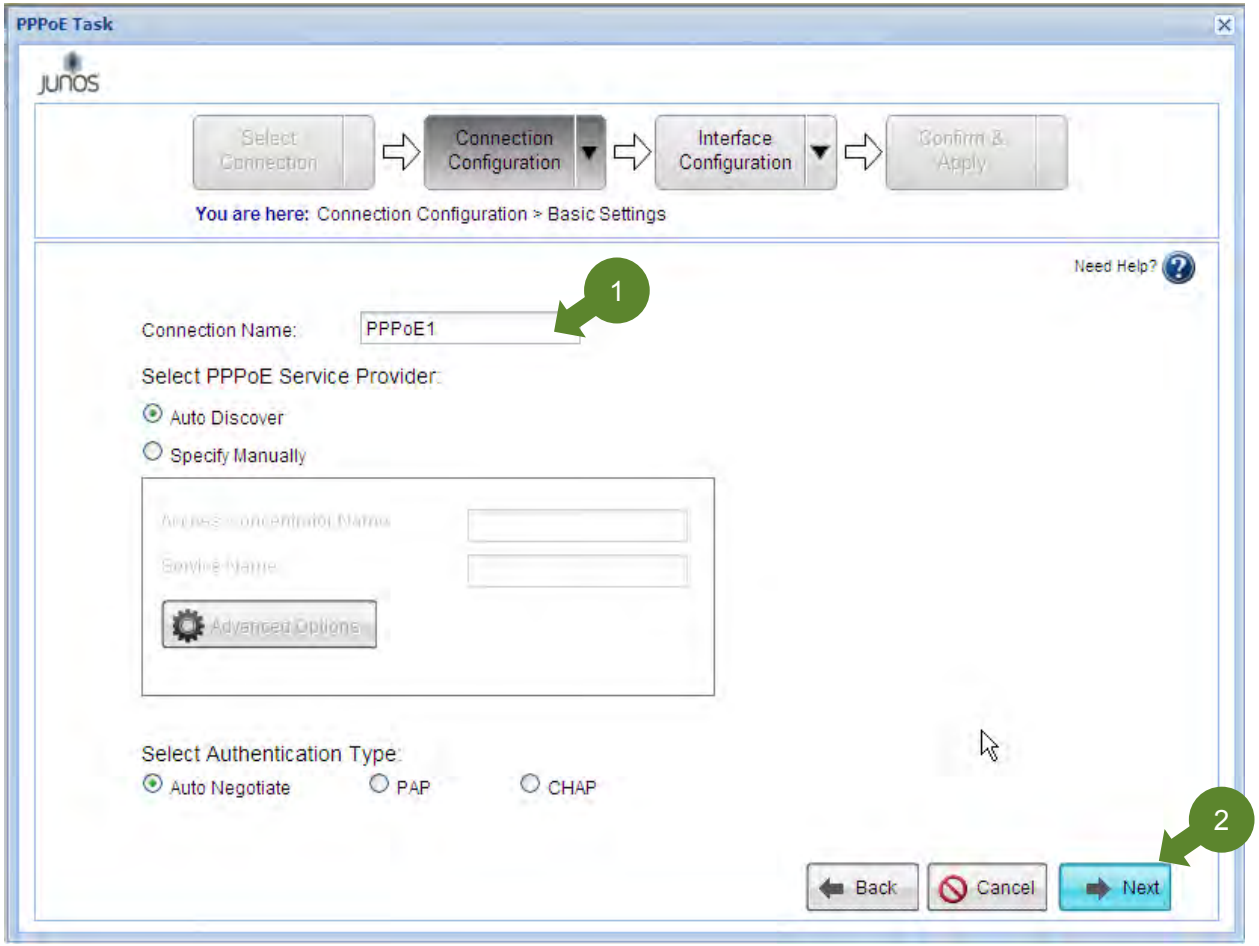
PPPoE設定(2/22)

「Add」ボタンをクリックします。(①)



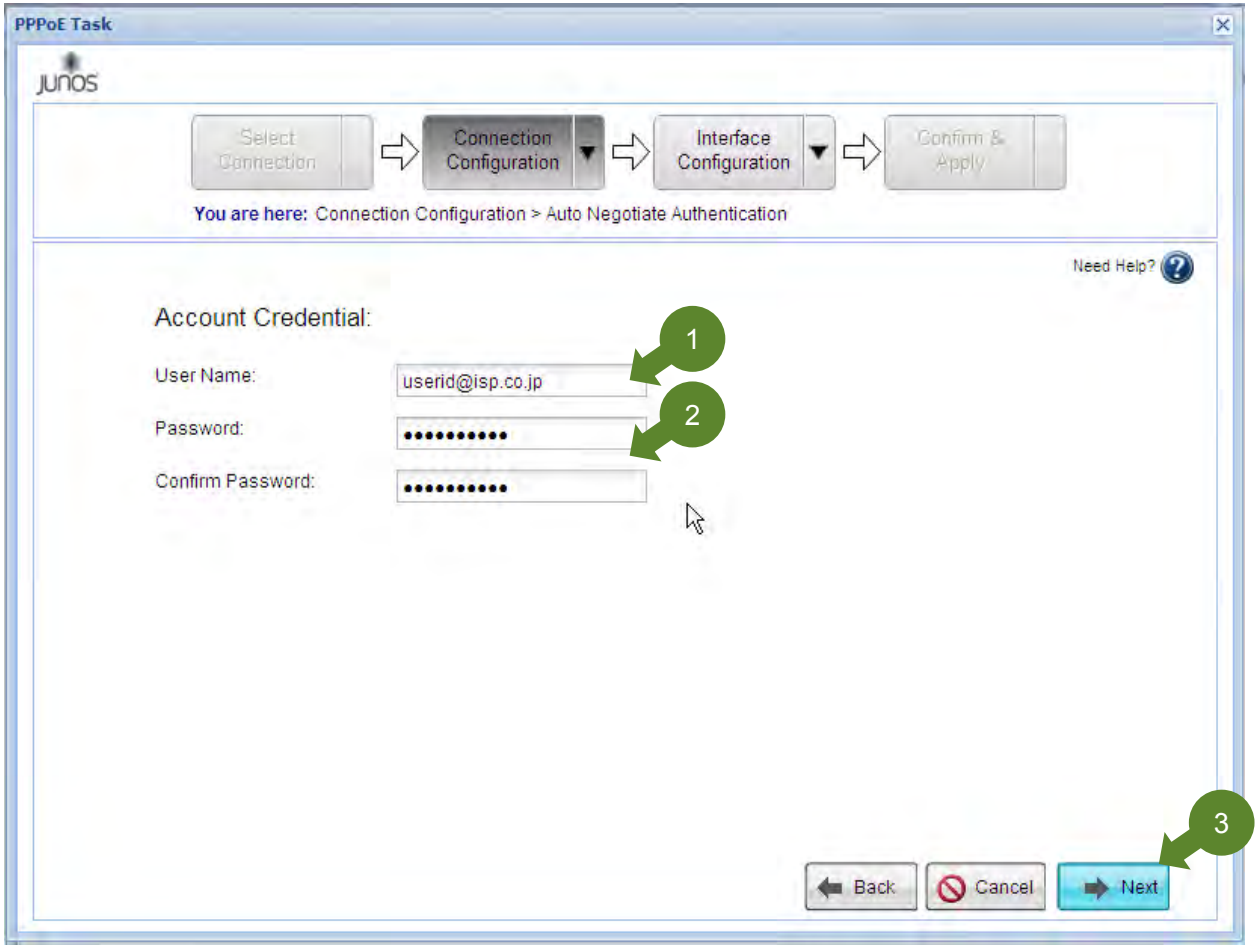
PPPoE設定(3/22)

「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）。



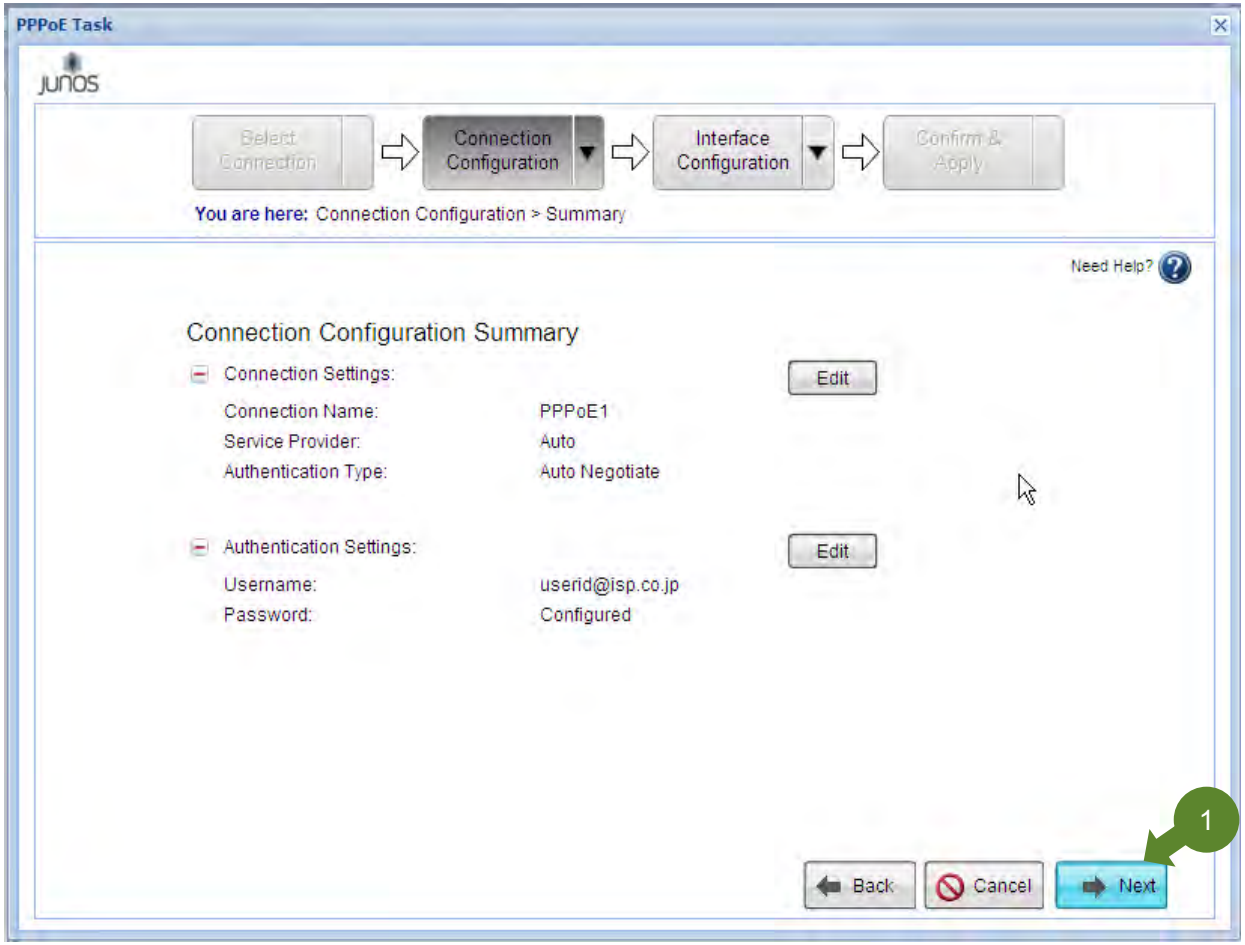
PPPoE設定(4/22)

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。



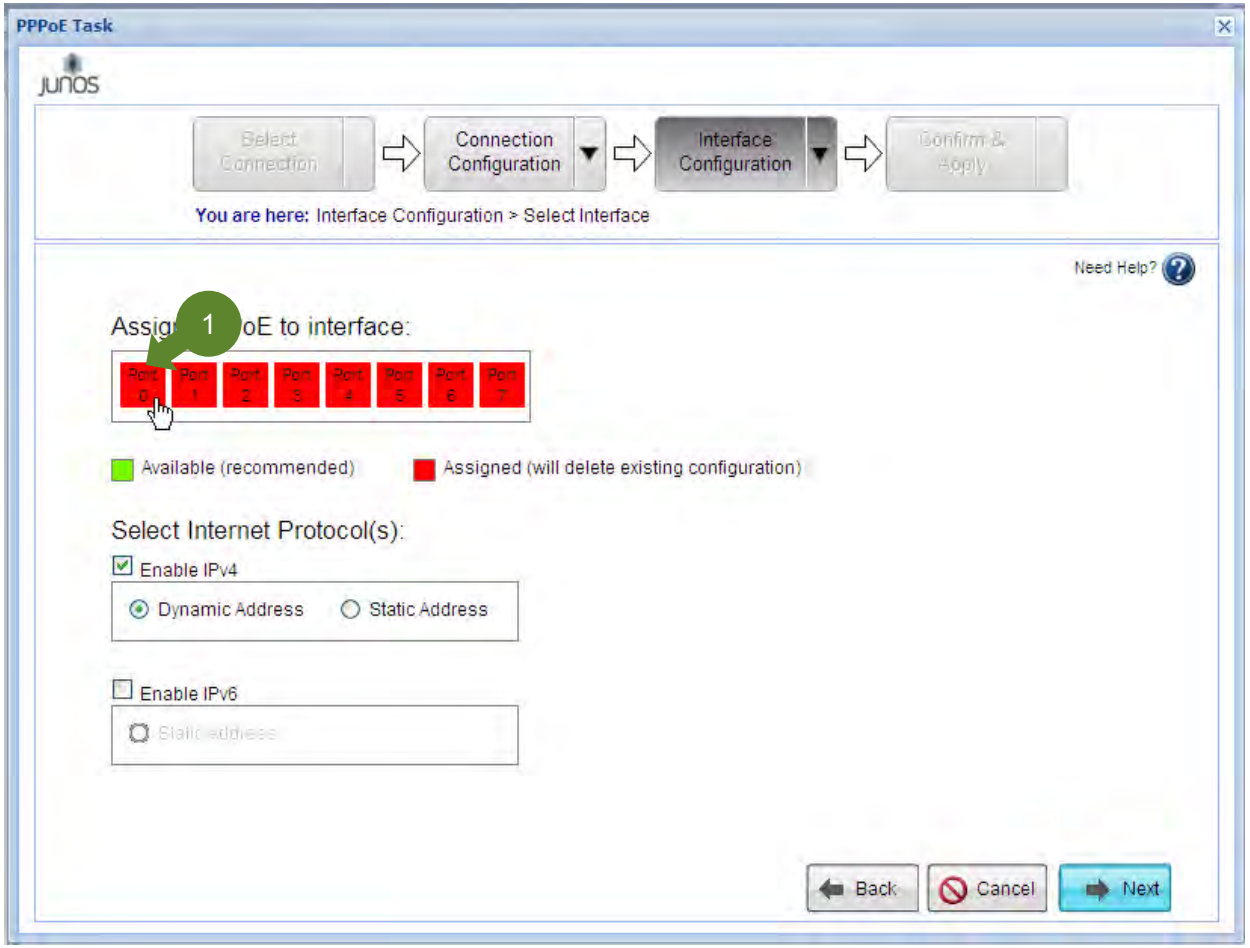
PPPoE設定(5/22)

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。



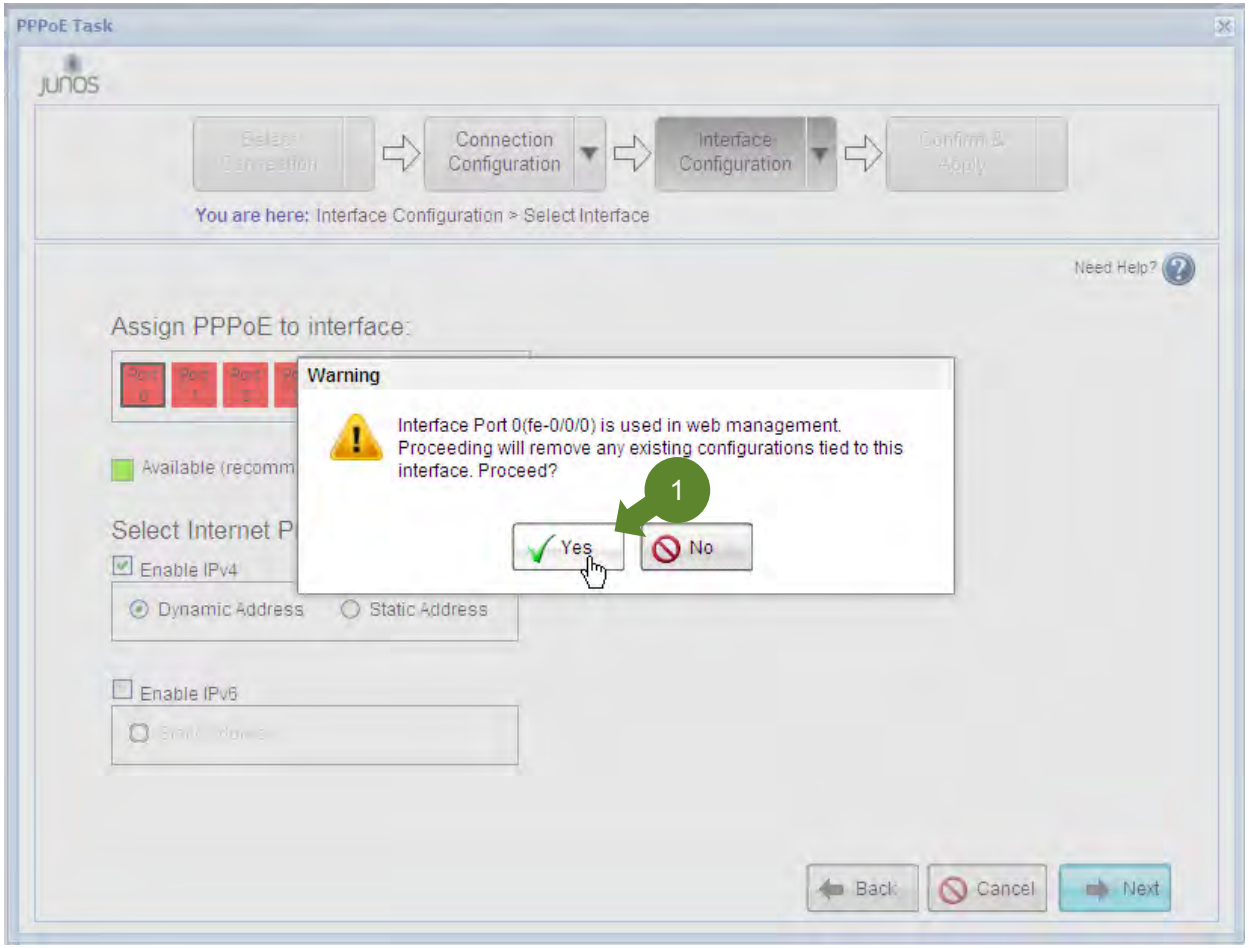
PPPoE設定(6/22)

PPPoE回線を接続するインタフェースをクリック(①)します。



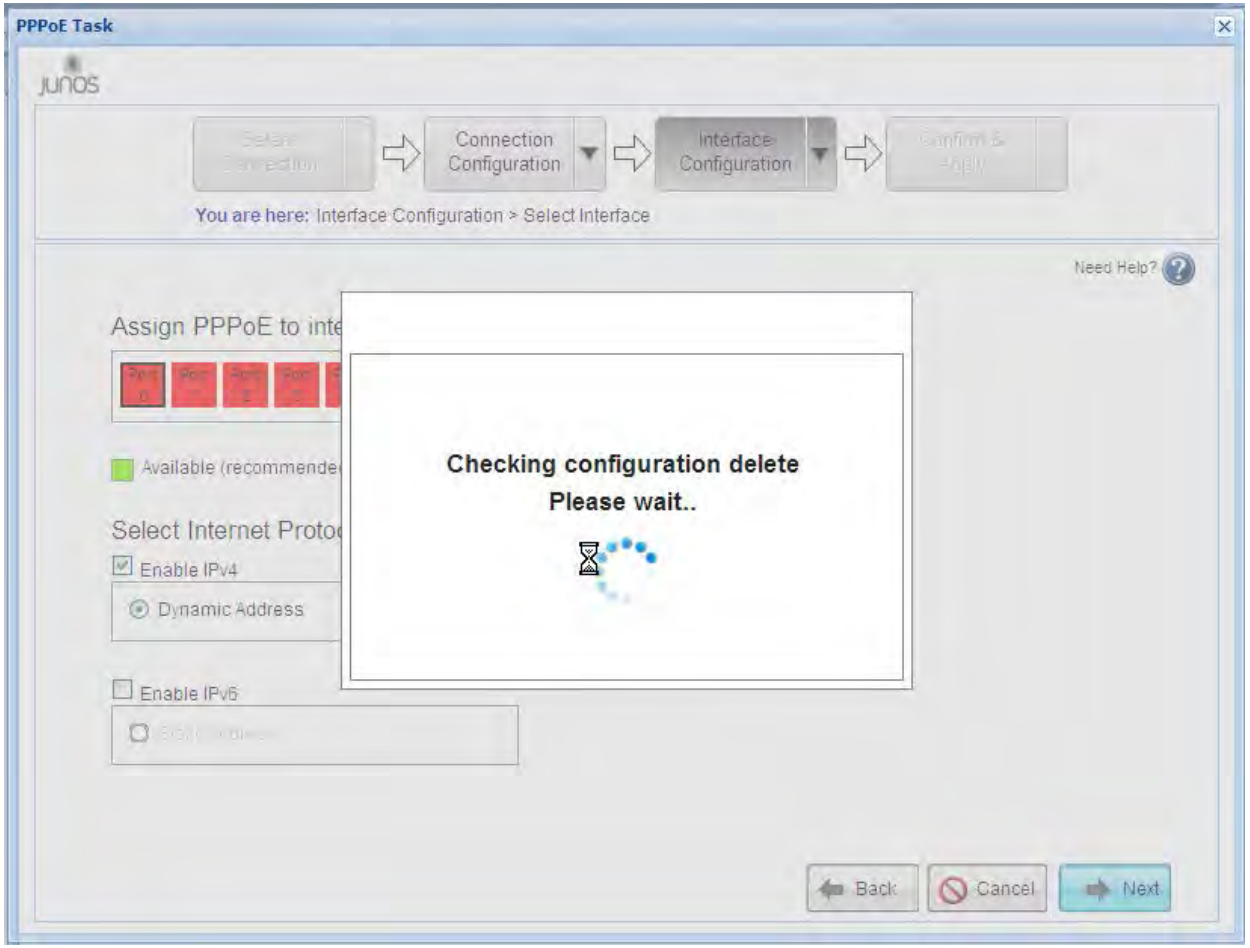
PPPoE設定(7/22)

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



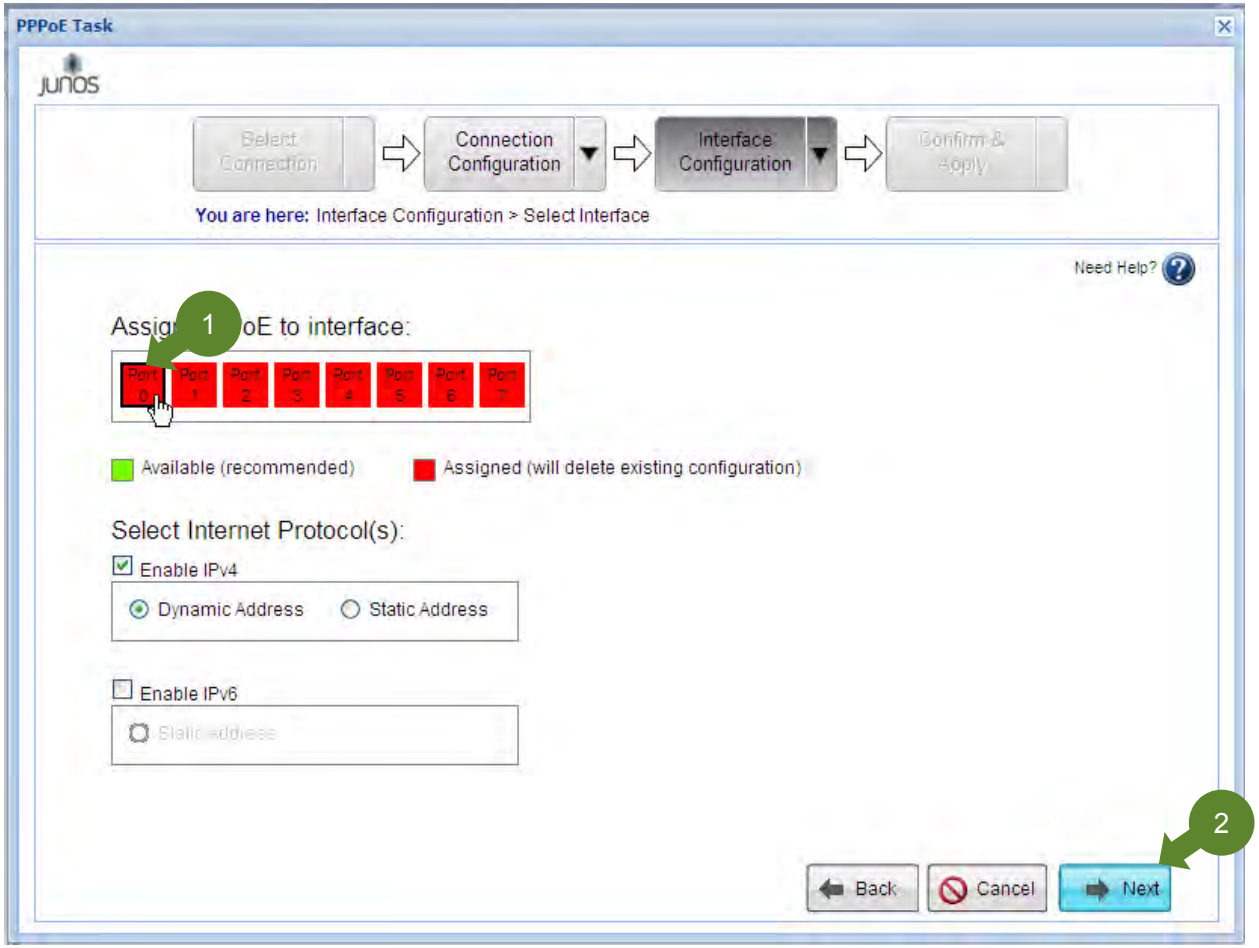
PPPoE設定(8/22)

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。



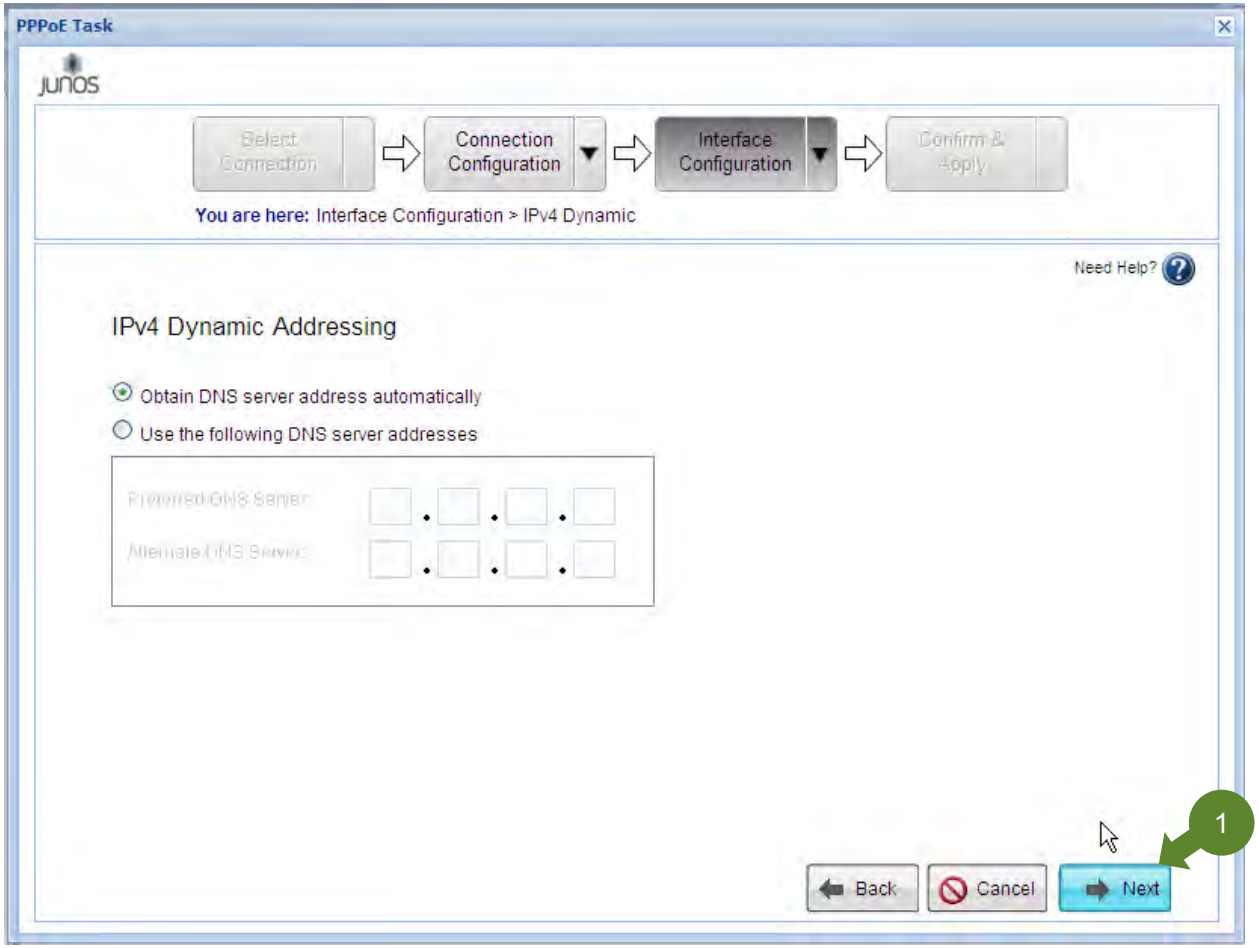
PPPoE設定(9/22)

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。



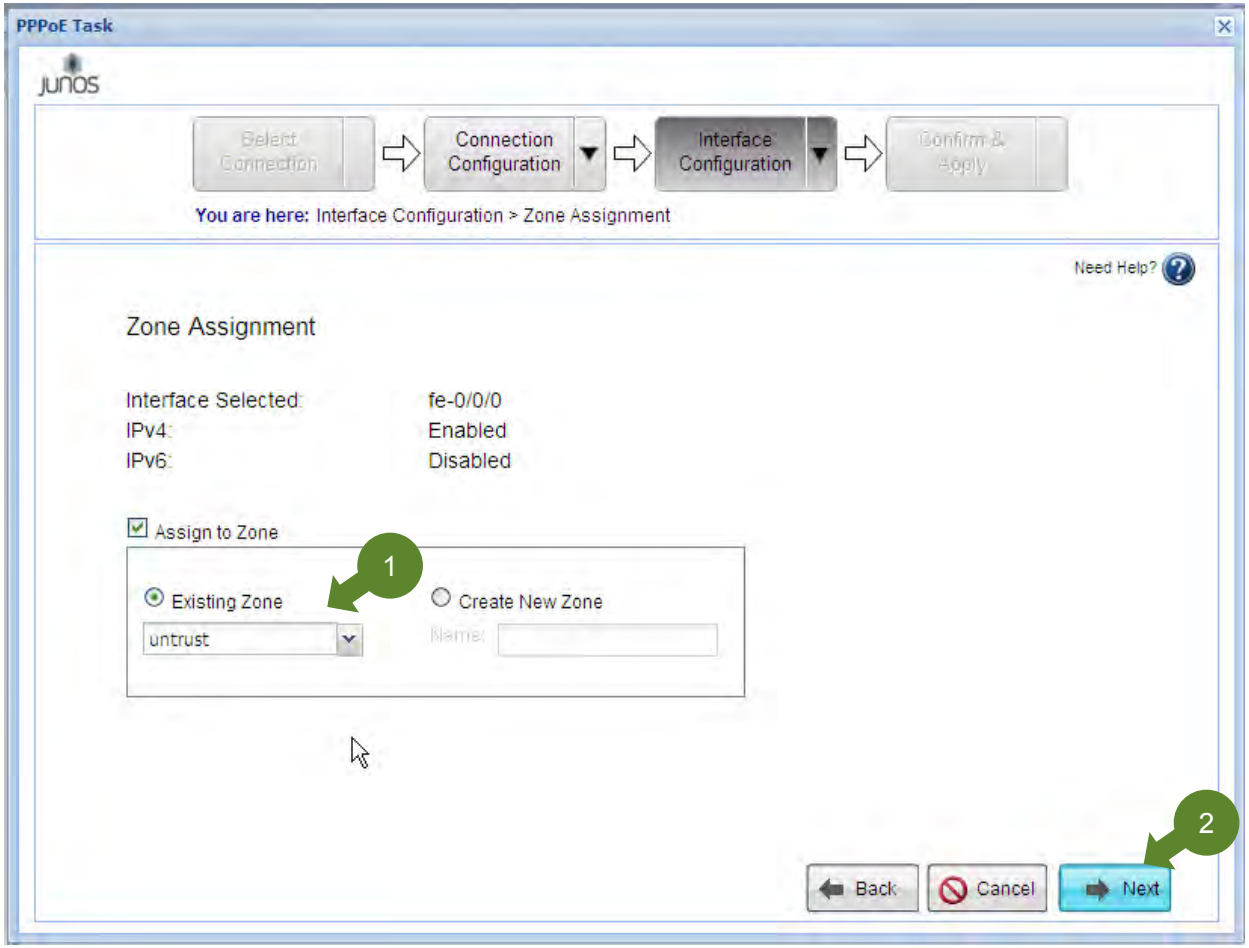
PPPoE設定(10/22)

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。



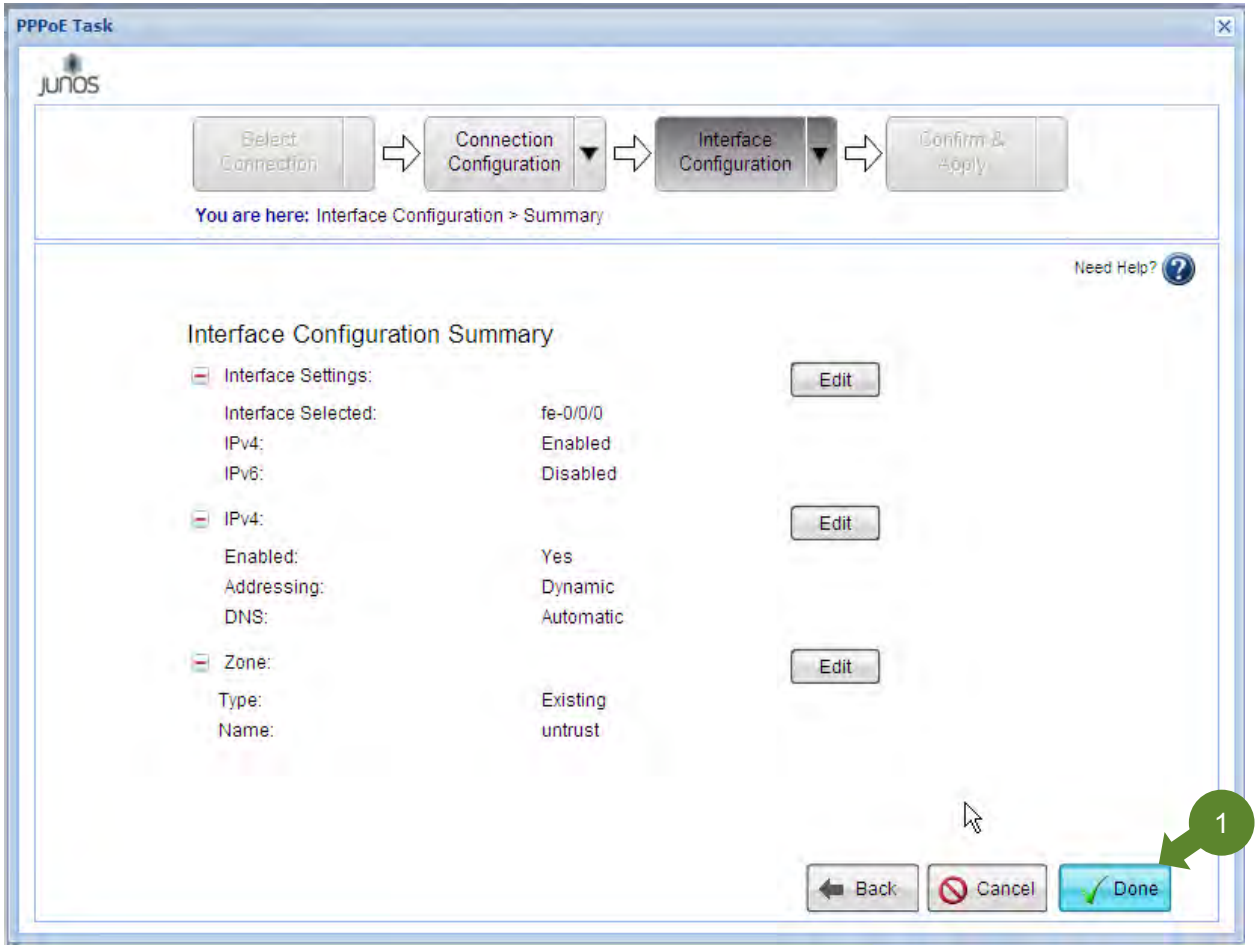
PPPoE設定(11/22)

PPPoE回線を接続するインタフェーズの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。



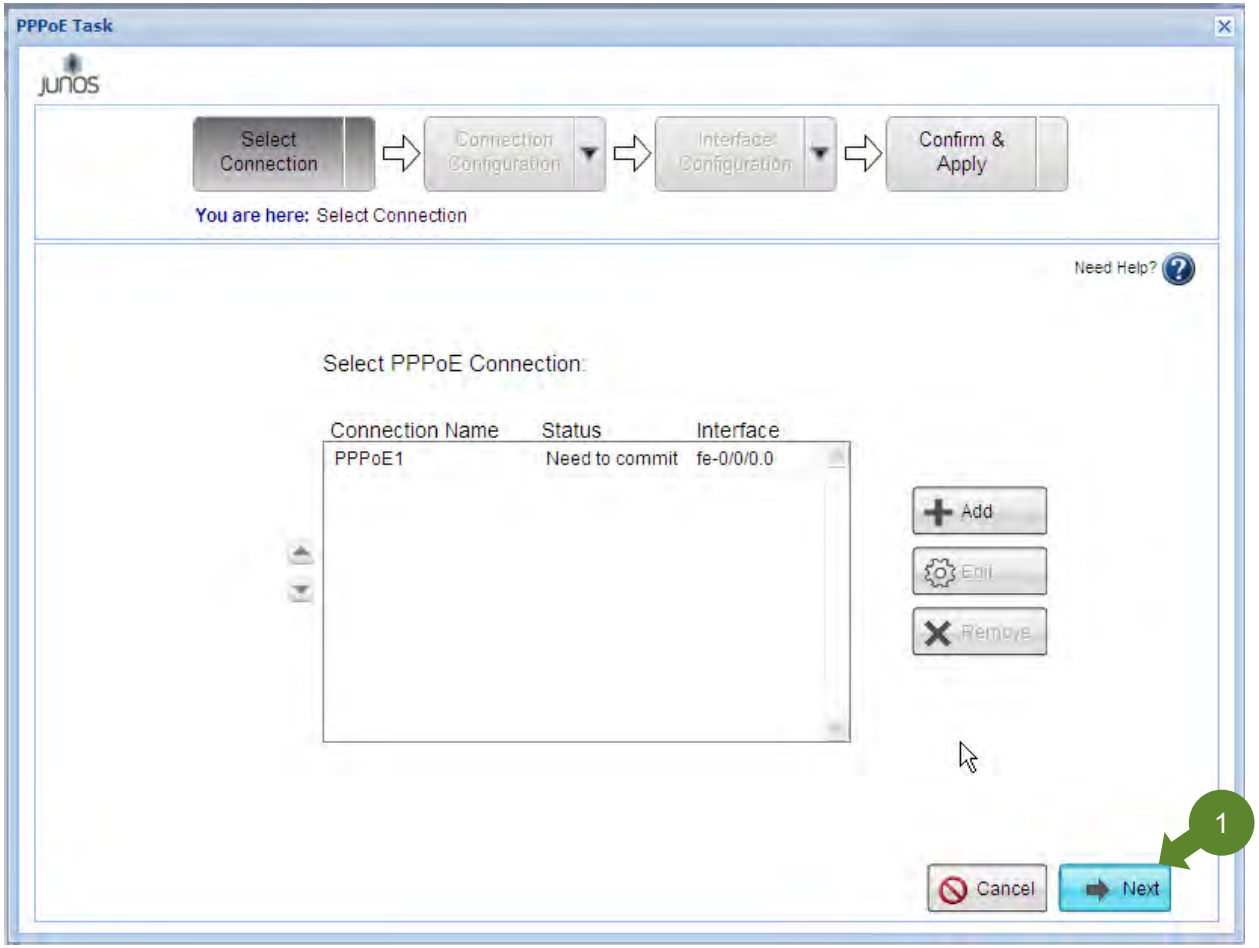
PPPoE設定(12/22)

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。



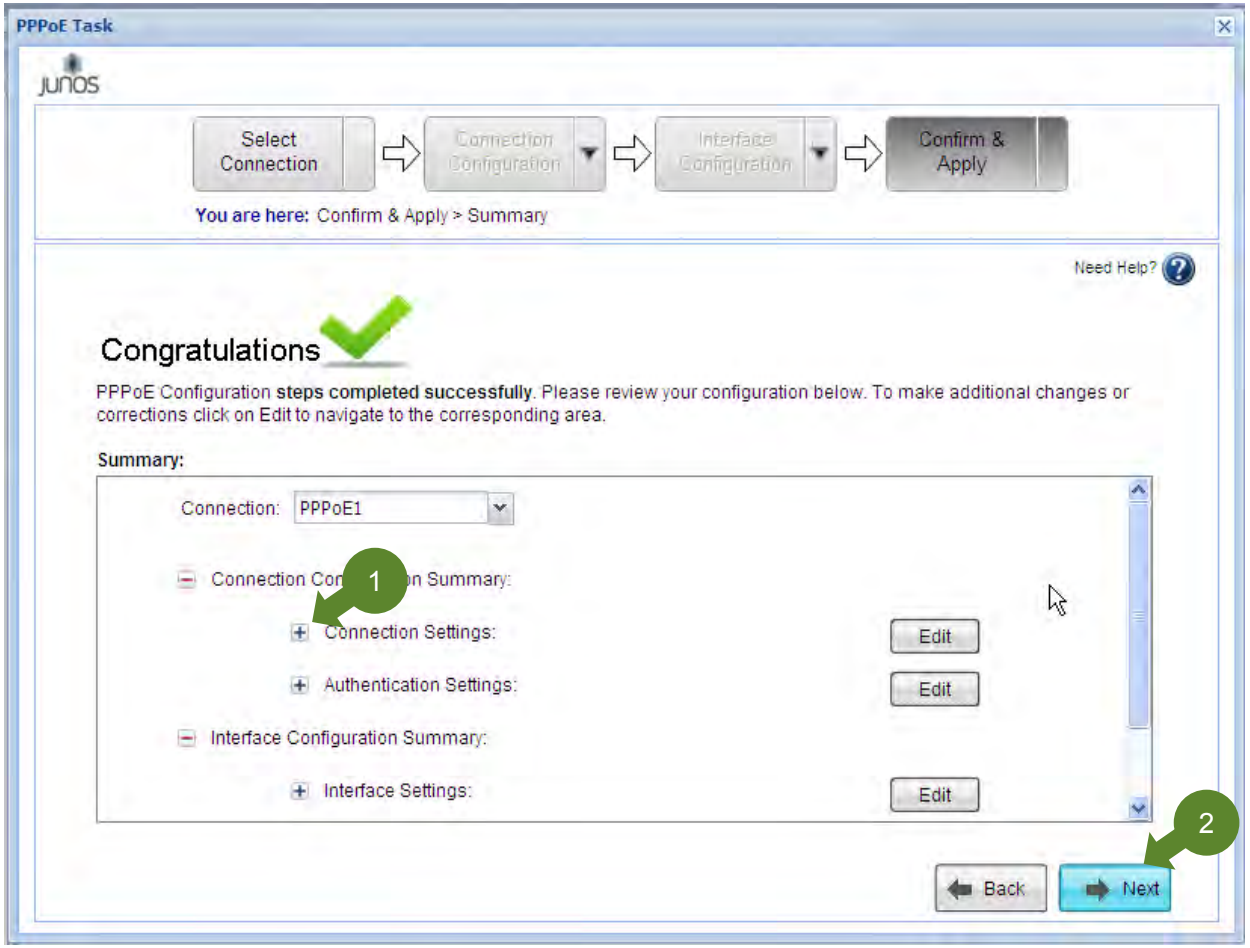
PPPoE設定(13/22)

「Next」ボタンをクリック(①)します。



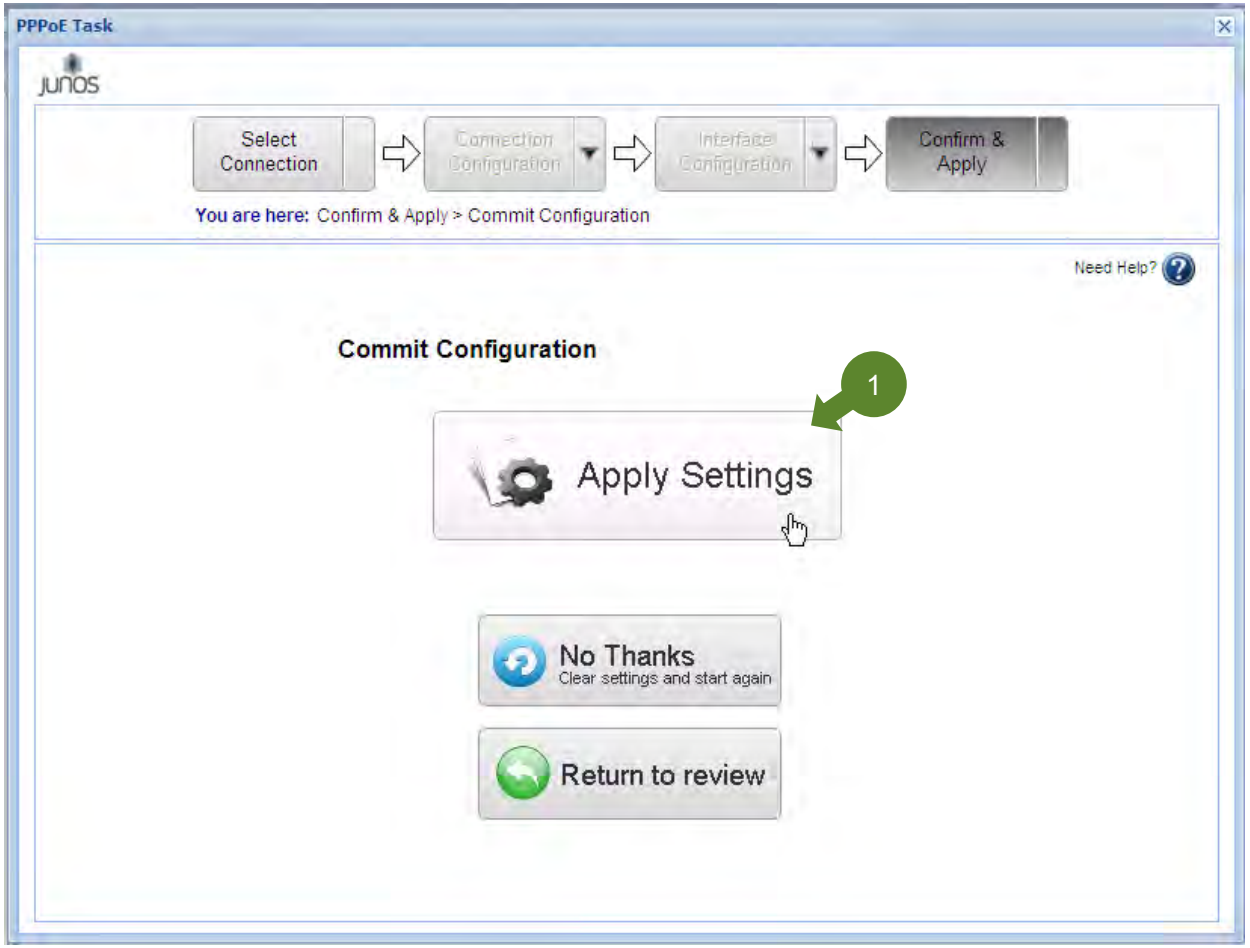
PPPoE設定(14/22)

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）。



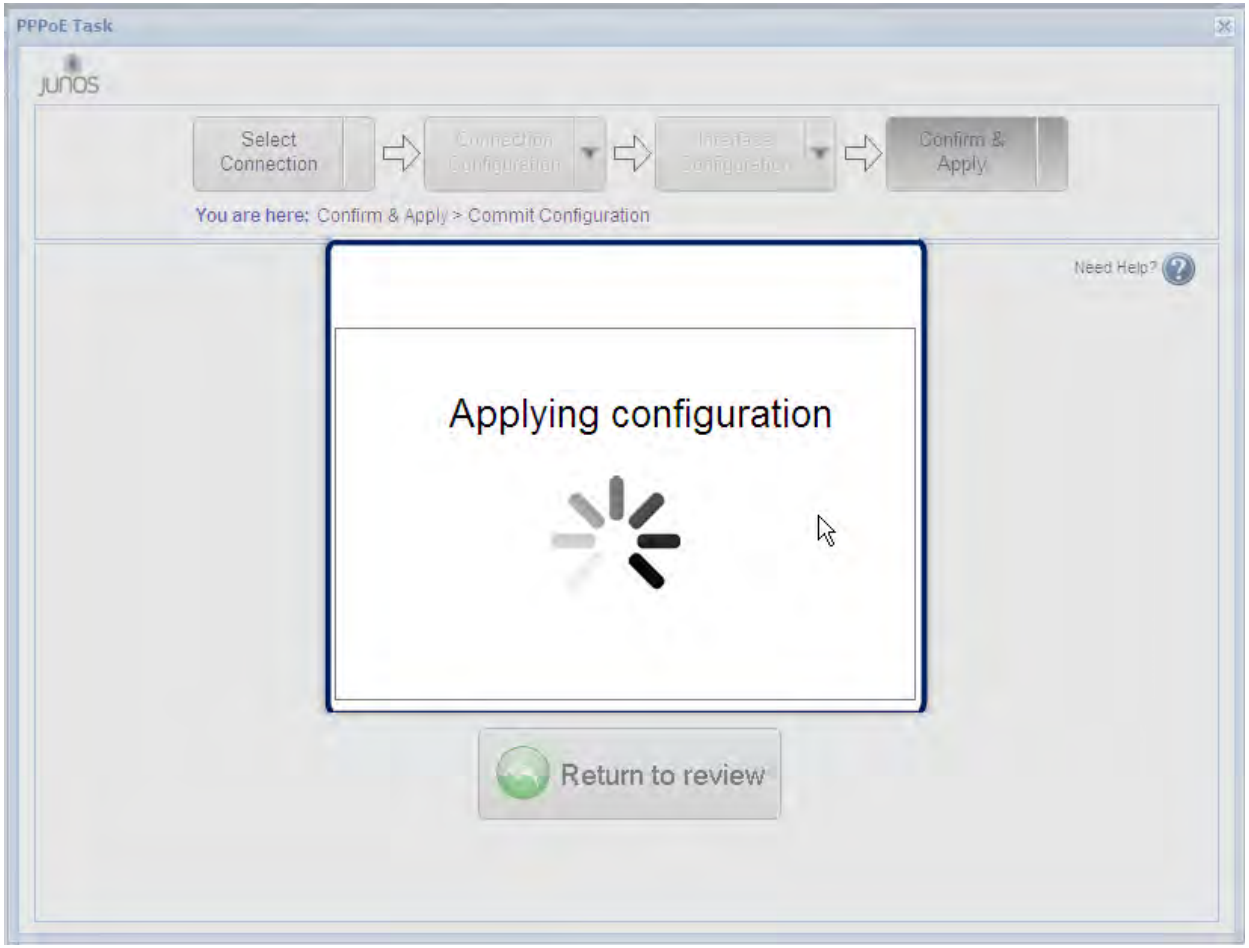
PPPoE設定(15/22)

「Apply Settings」ボタンをクリックします（①）。



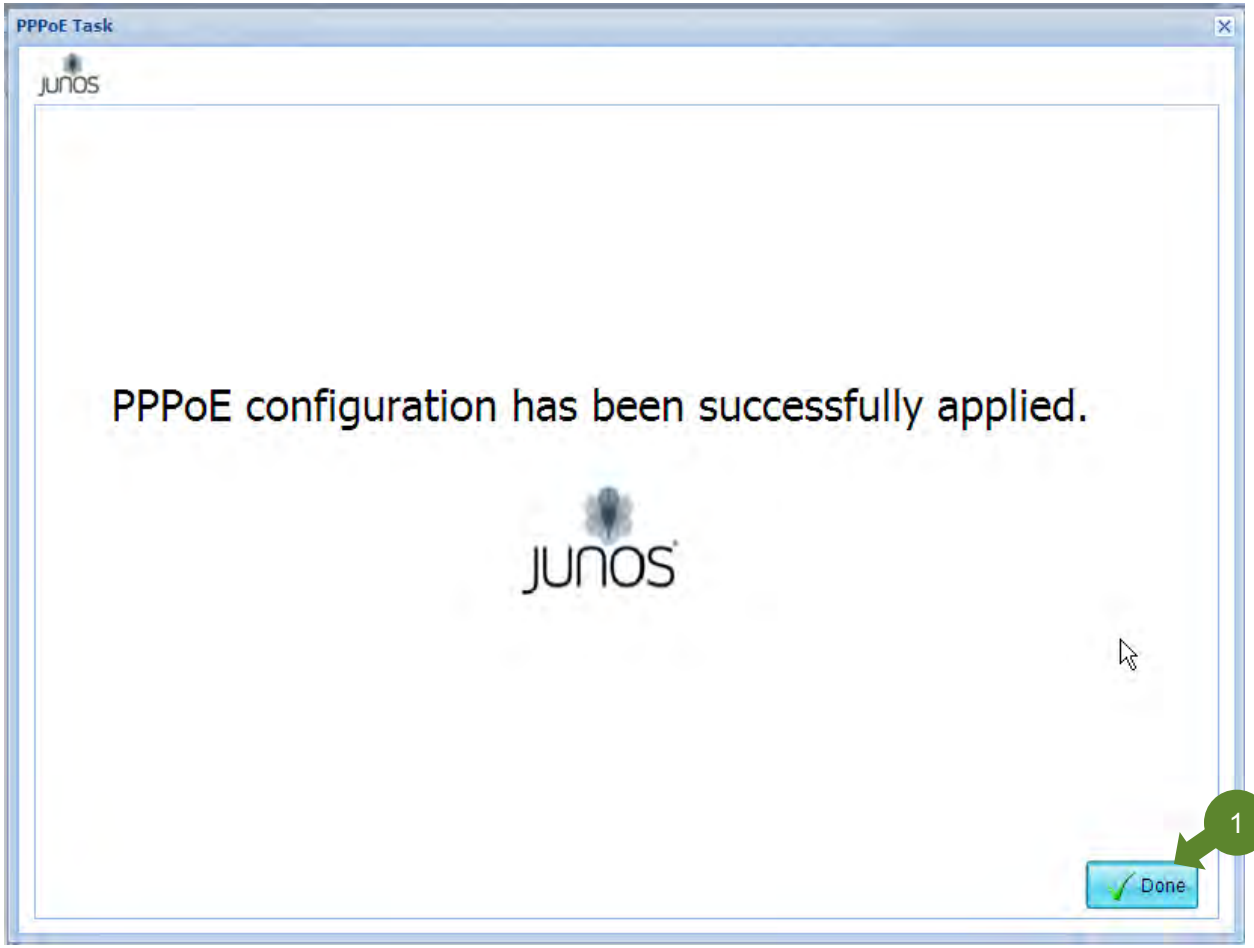
PPPoE設定(16/22)

設定反映中となりますので、しばらく待ちます。



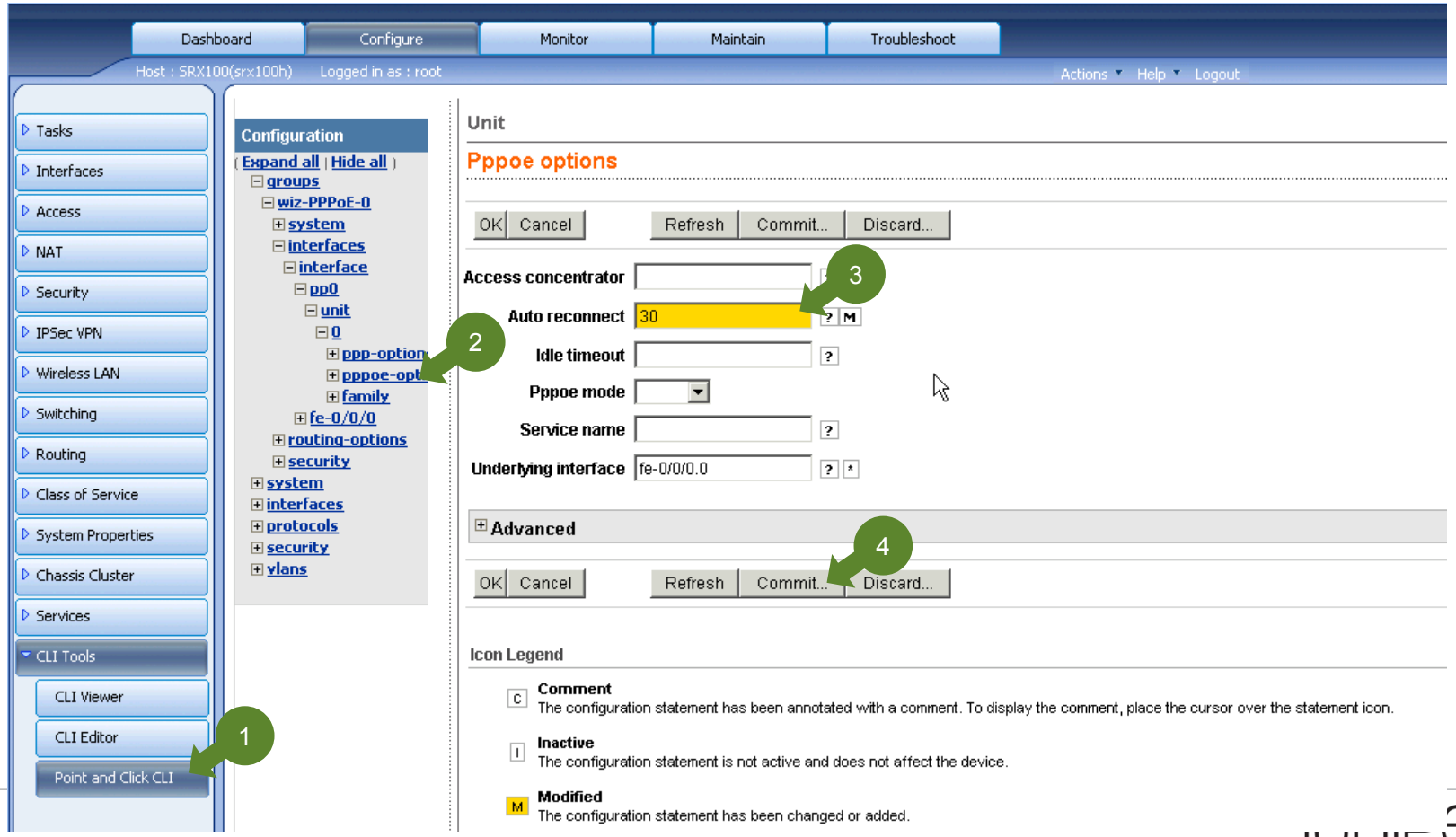
PPPoE設定(17/22)

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。



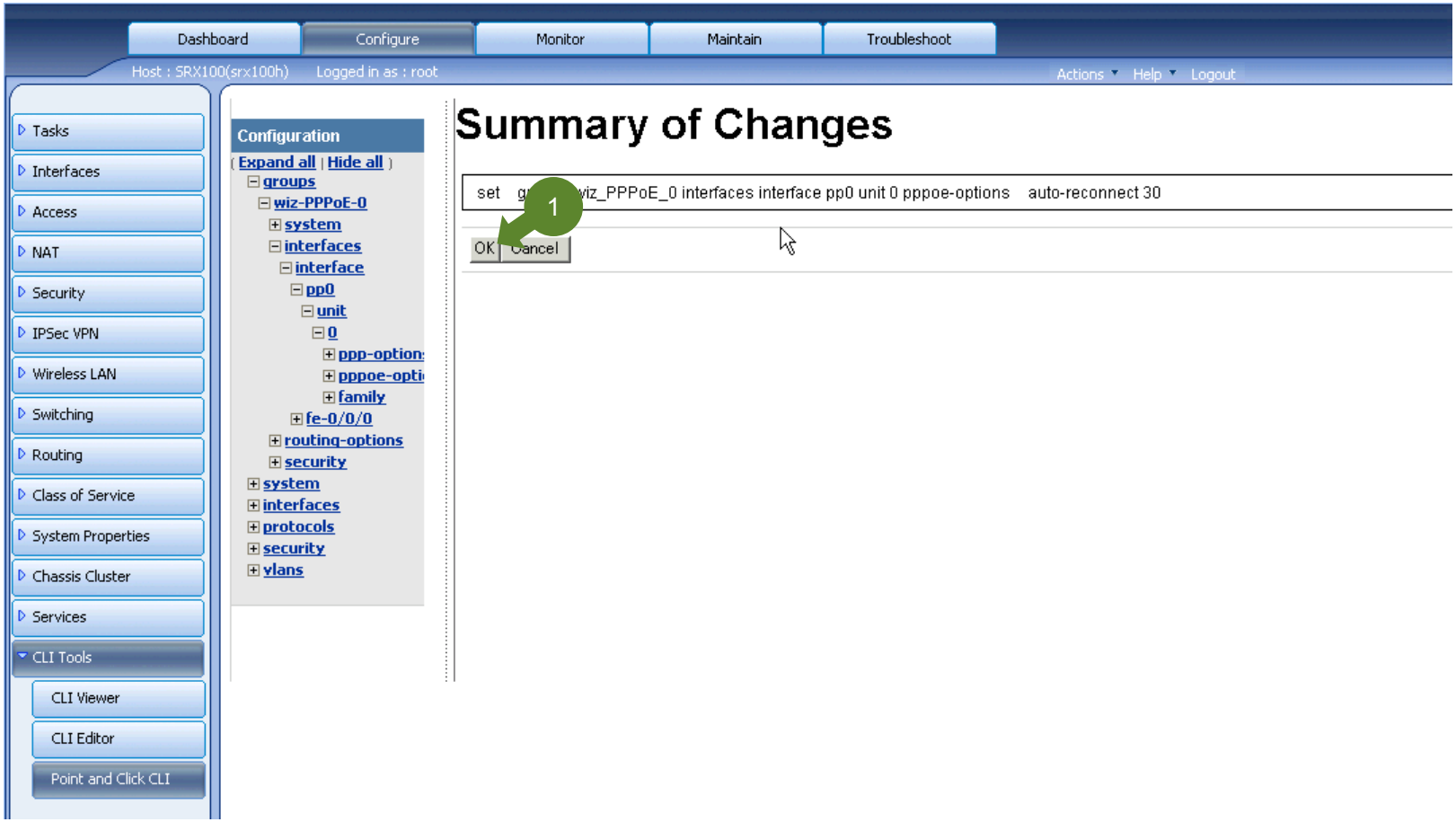
PPPoE設定(18/22)

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。



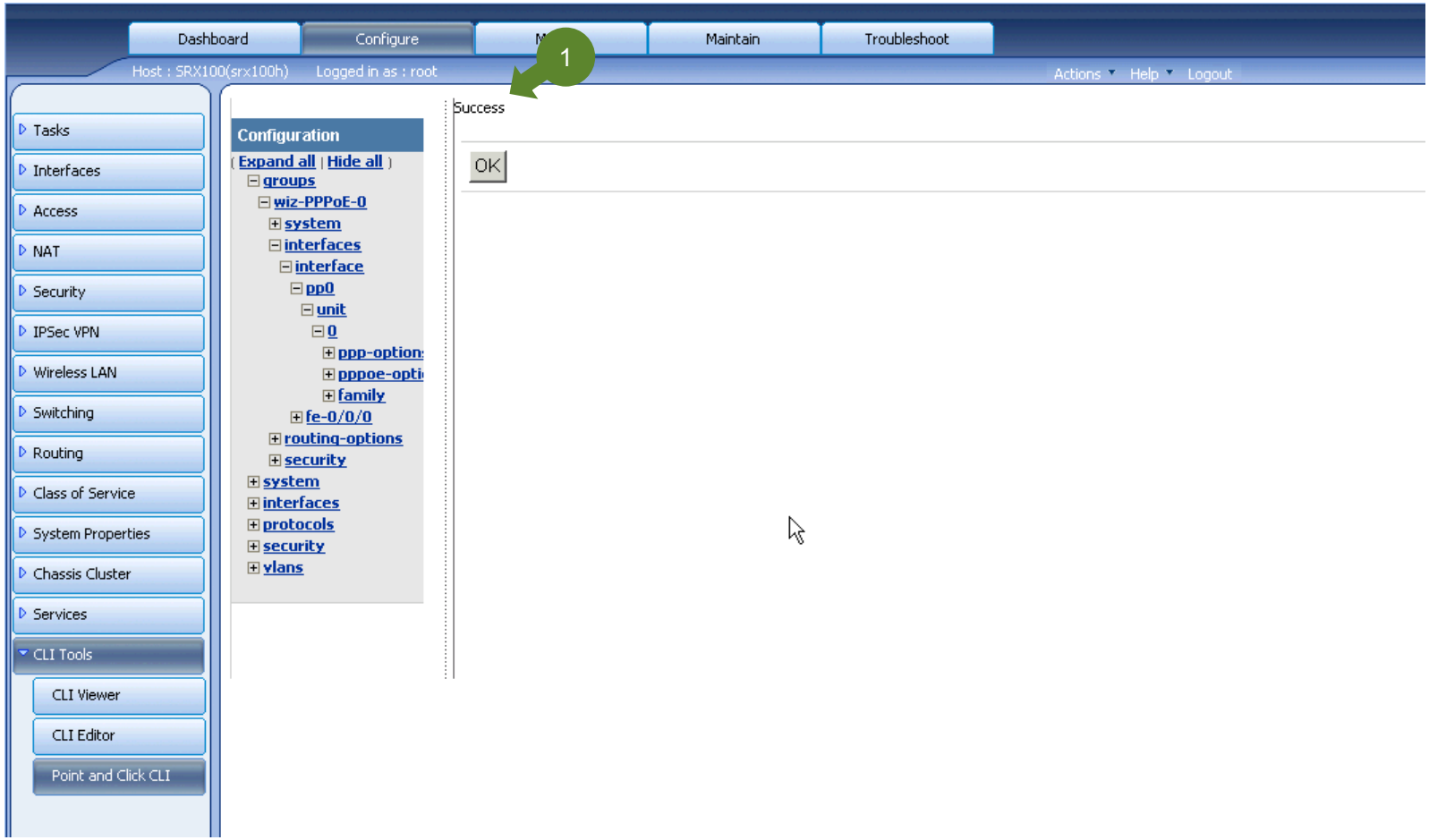
PPPoE設定(19/22)

設定を反映させるため、「OK」ボタンをクリックします（①）。



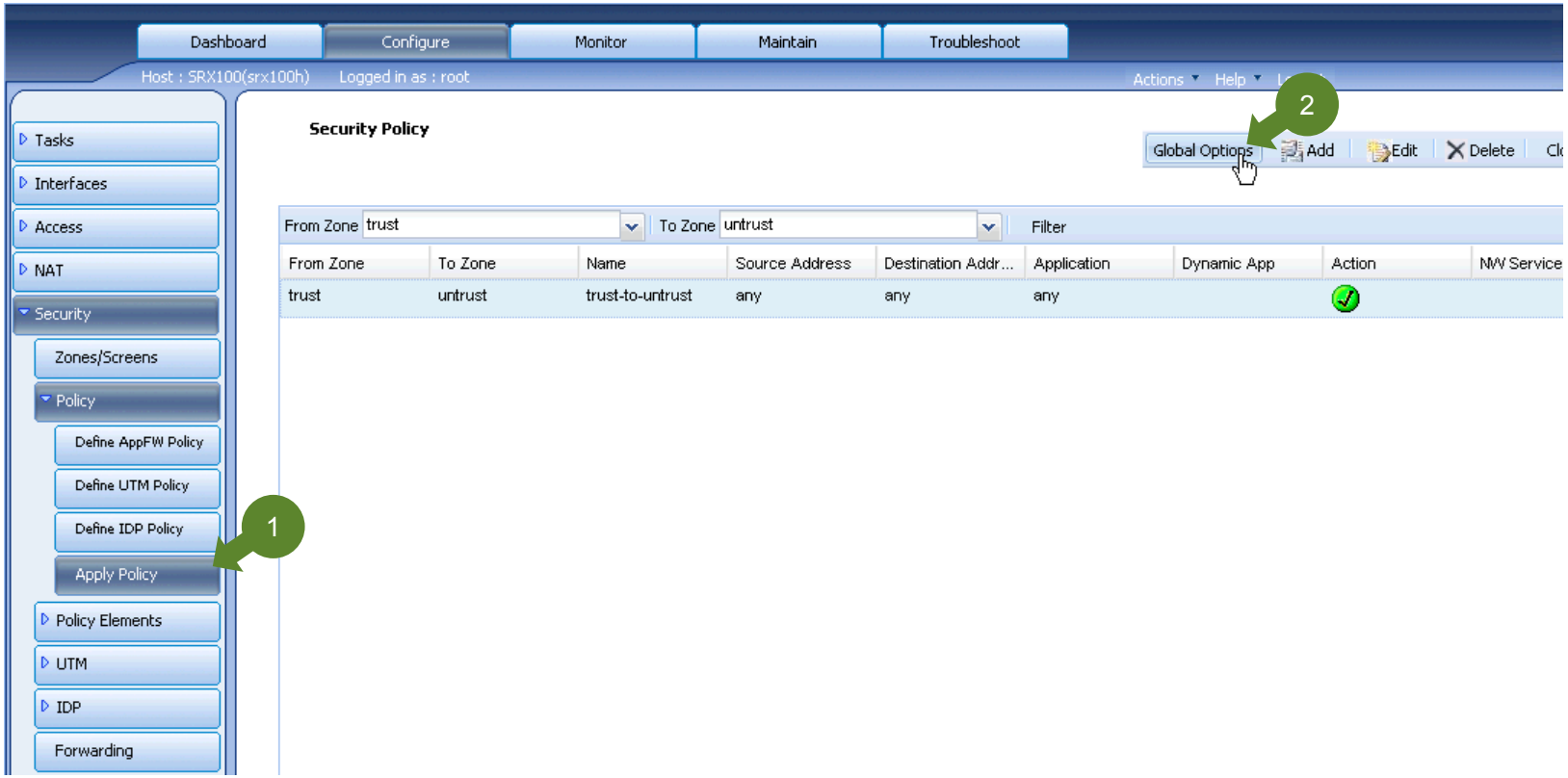
PPPoE設定(20/22)

正常に設定反映が行われると、Successと表示されます（①）。



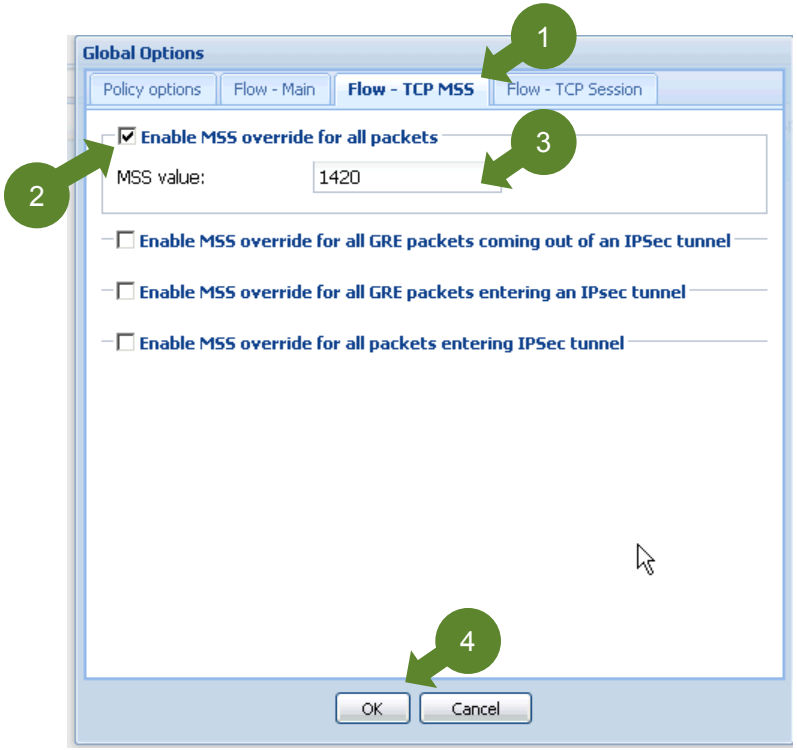
PPPoE設定(21/22)

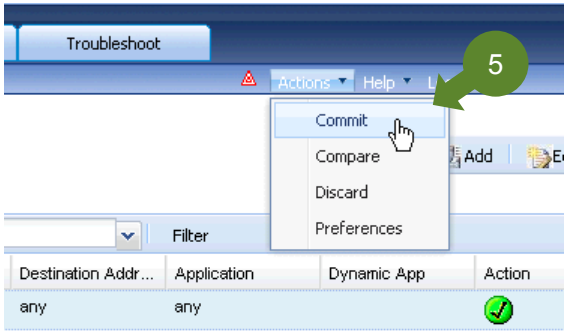
TCP MSSの設定を追加します。「Security」 -> 「Policy」 -> 「Apply Policy」 をクリック(①)します。次に「Global Options」ボタンをクリックします(②)。



PPPoE設定(22/22)

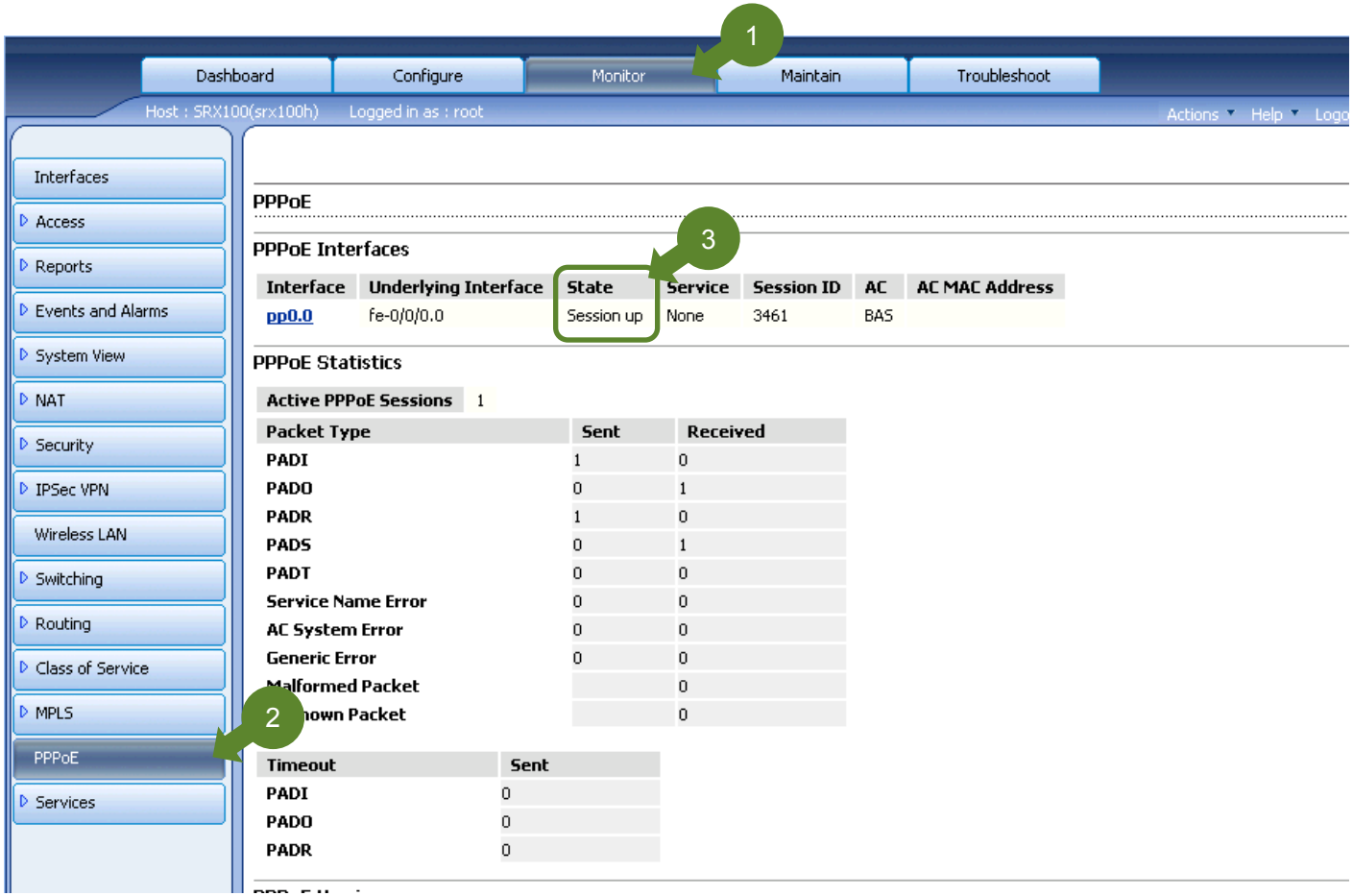
「Flow –TCP」タブをクリックし(①)、「Enable MSS override for all packets」チェックボックスを有効にします(②)。
次にMSS value値として数値(ここでは1420)(③)を入力し、「OK」ボタンをクリックします(④)。
最後に設定を反映させるため、「Actions」->「Commit」ボタンをクリックします(⑤)。





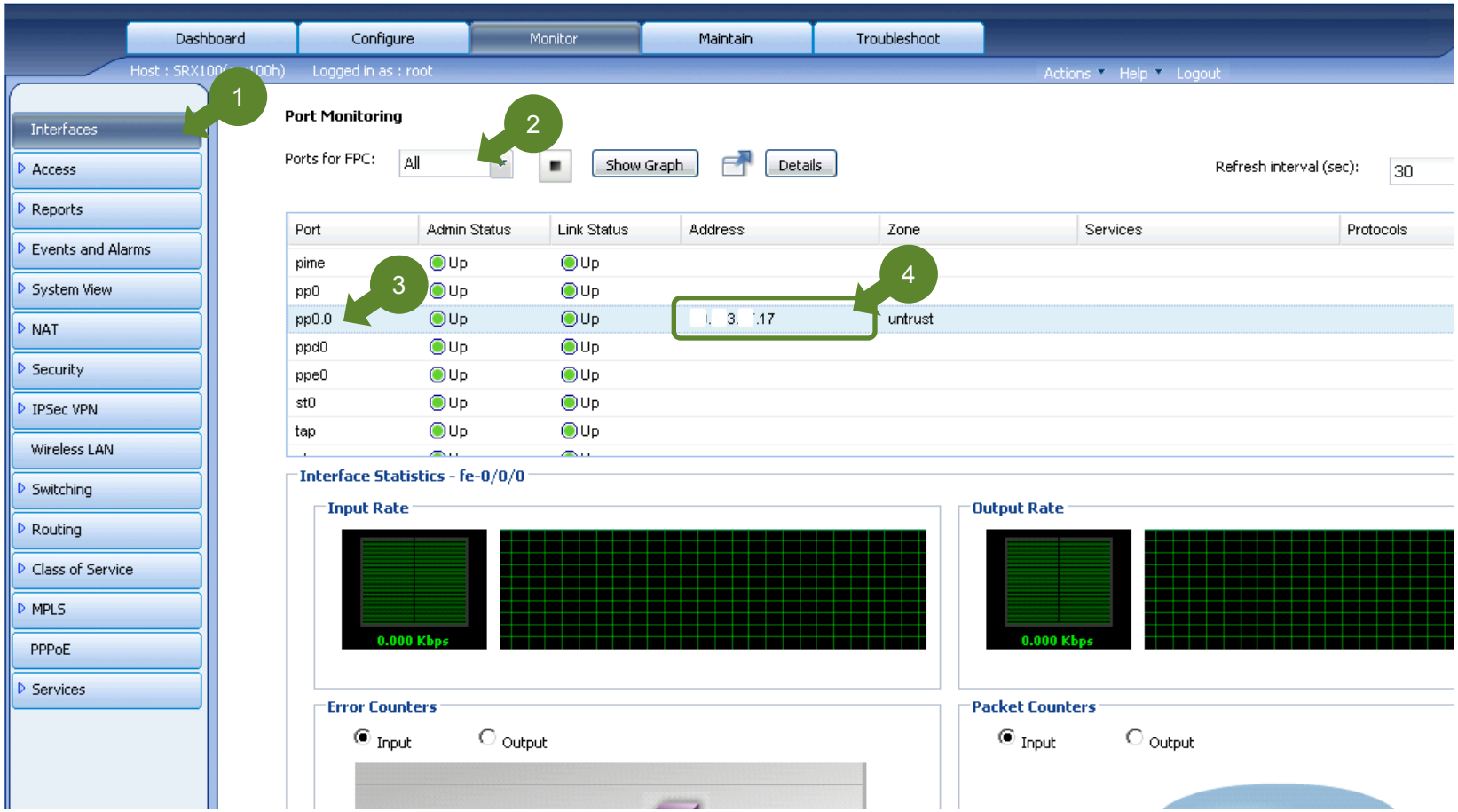
PPPoE接続確認(1/2)

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。



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)。



everywhere