

ファイアウォール(Brocade 5600 vRouter)からvSRXへの交換によるマイグレ実施方法

第1版

更新履歴

更新日	更新内容	版数
2018/10/25	初版	1

前提条件

前提条件

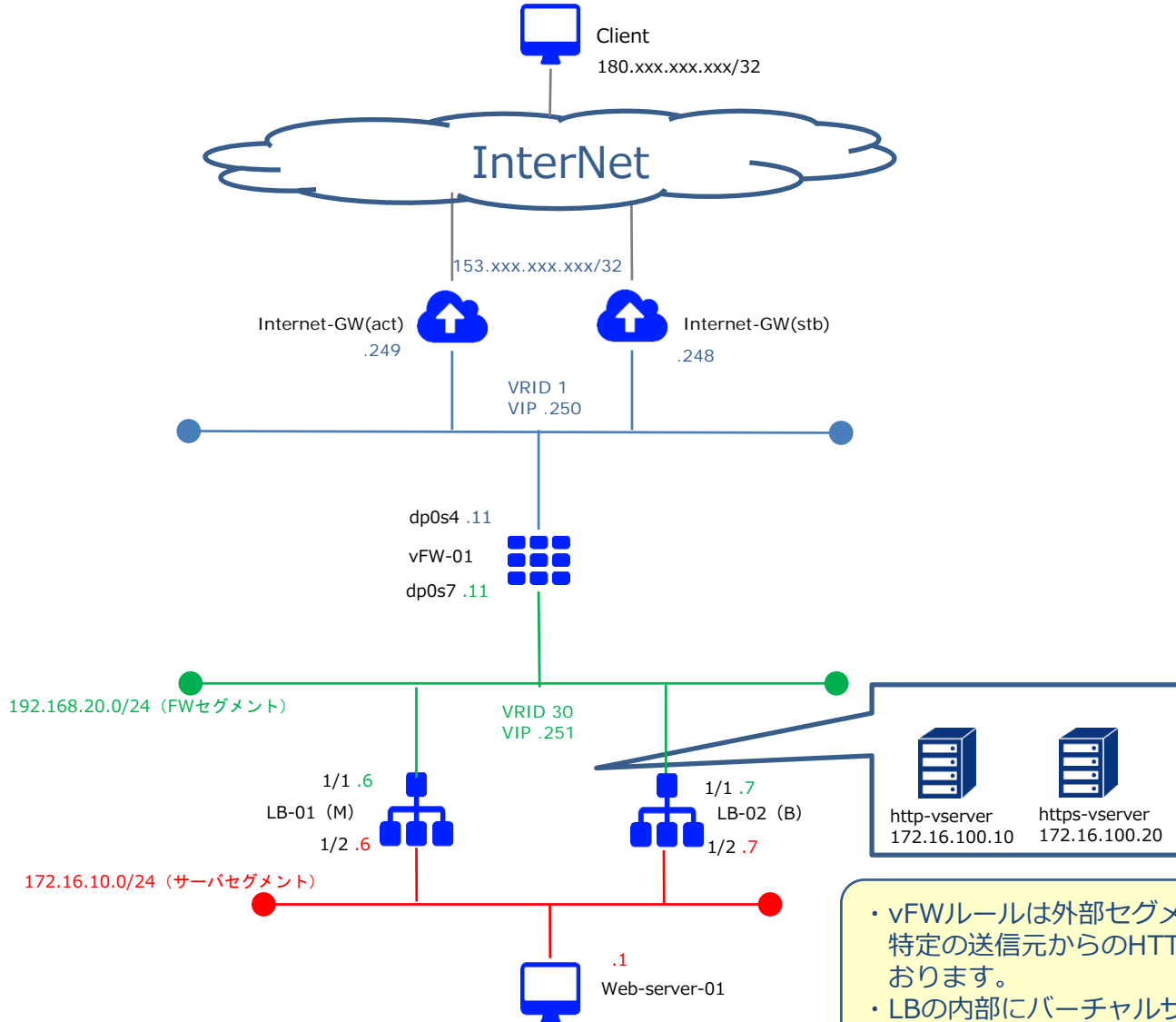
■ ファイアウォール(Brocade 5600 vRouter)(以下、vFW)からファイアウォール(vSRX)への並行運用によるマイグレ実施方法です。

- Internet-GW, ロードバランサー, Webサーバーの設定変更(Routing変更等)が発生するケースです。
- ロードバランサーは、ツーアーム構成のマイグレ実施方法です。ワンアーム構成をご利用の場合はお客様環境にそって、読み替えて頂きますようお願い致します。
- vFWで利用しているネットワークをvSRXへ接続します。
⇒ vFWからvSRXへ切り替える際、Internet-GW、ロードバランサーでルーティング設定変更が必要になります。また、通信断が発生致します。
- vSRXの基本設定は下記リンクを参照頂けますよう、よろしくお願いいたします。
<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/basic/basic.html>
- vSRXのルーティング設定はお客様構成に応じて設定をお願い致します。
- vSRX作成時、インターフェイス(ge-0/0/0.0)はTrustゾーンに設定されております。
⇒作成後、各インターフェイスはお客様環境にそって読み替えて設定頂きますようお願い致します。
- vFW/vSRX共に、ステートフルインスペクション機能を利用します。
⇒ ステートレスファイアウォールをご利用の場合、お客様環境にそって読み替えて頂きますようお願い致します。

※事前検証を行ってから移行を実施ください。

構成および移行フロー

移行前構成 (vFW構成)



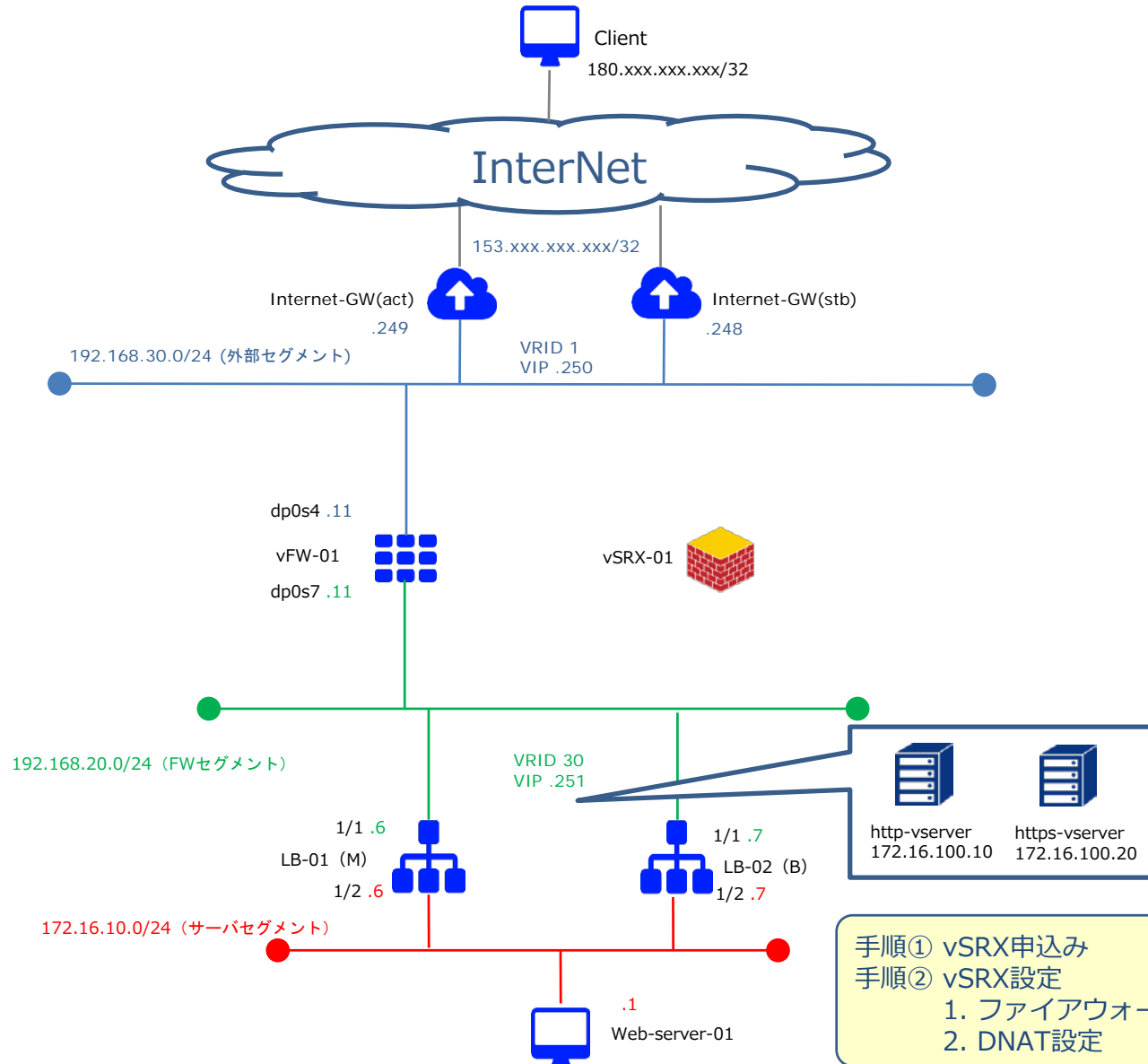
- vFWルールは外部セグメントからの通信は全て拒否し、特定の送信元からのHTTP/HTTPS通信のみ許可しております。
- LBの内部にバーチャルサーバーを設定しておきます。
- vFWの設定内容を次のページに記載致します。

移行前構成（vFW構成）設定値

vFW-01 Firewall Filterの設定

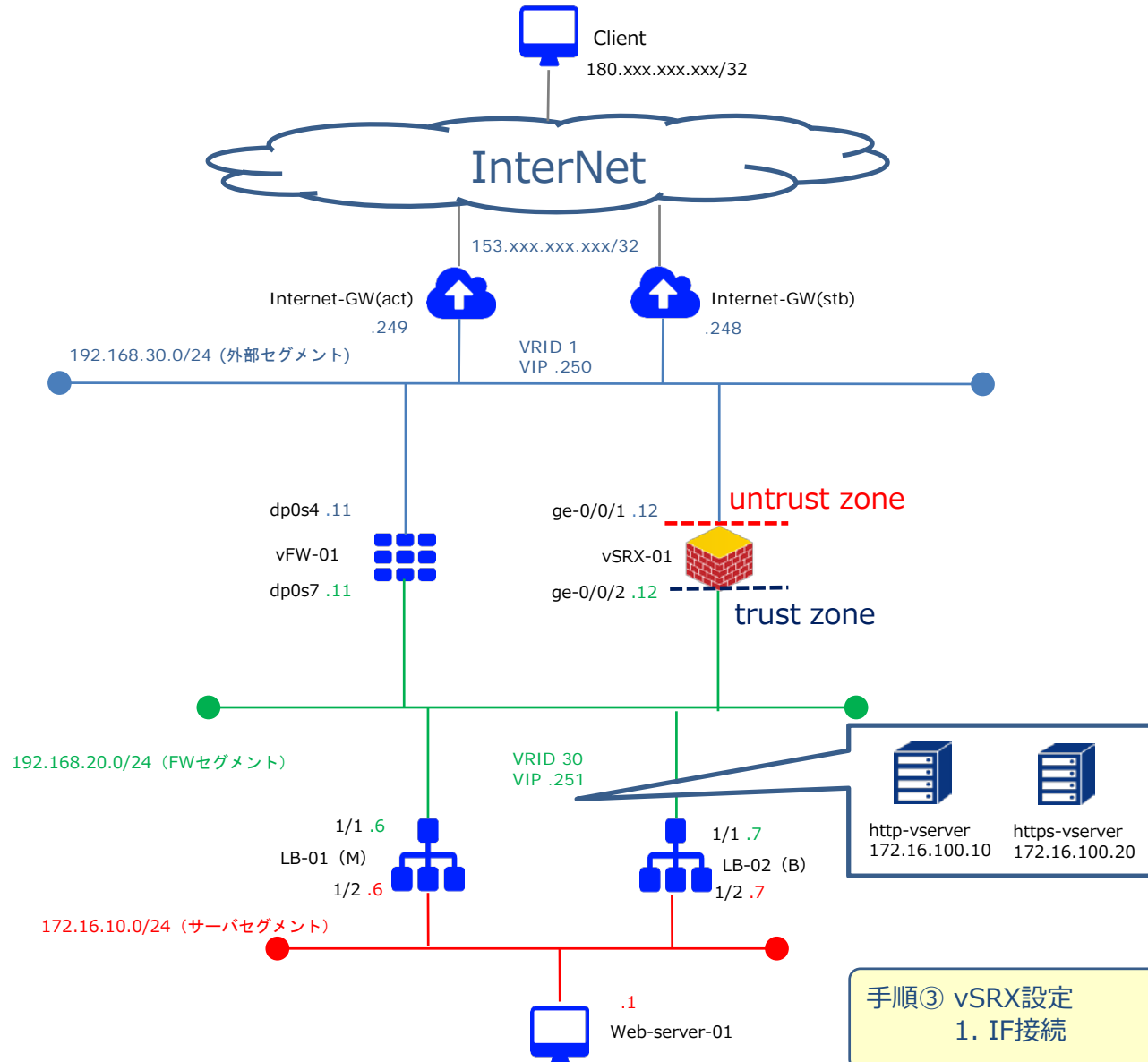
```
set security firewall name From-Internet default-action 'drop'  
set security firewall name From-Internet rule 10 action 'accept'  
set security firewall name From-Internet rule 10 protocol 'tcp'  
set security firewall name From-Internet rule 10 source address '180.xxx.xxx.xxx/32'  
set security firewall name From-Internet rule 10 destination port '80'  
set security firewall name From-Internet rule 10 state 'enable'  
set security firewall name From-Internet rule 20 action 'accept'  
set security firewall name From-Internet rule 20 protocol 'tcp'  
set security firewall name From-Internet rule 20 source address '180.xxx.xxx.xxx/32'  
set security firewall name From-Internet rule 20 destination port '443'  
set security firewall name From-Internet rule 20 state 'enable'  
set interface dataplane dp0s4 firewall in 'From-Internet'
```

移行時構成①



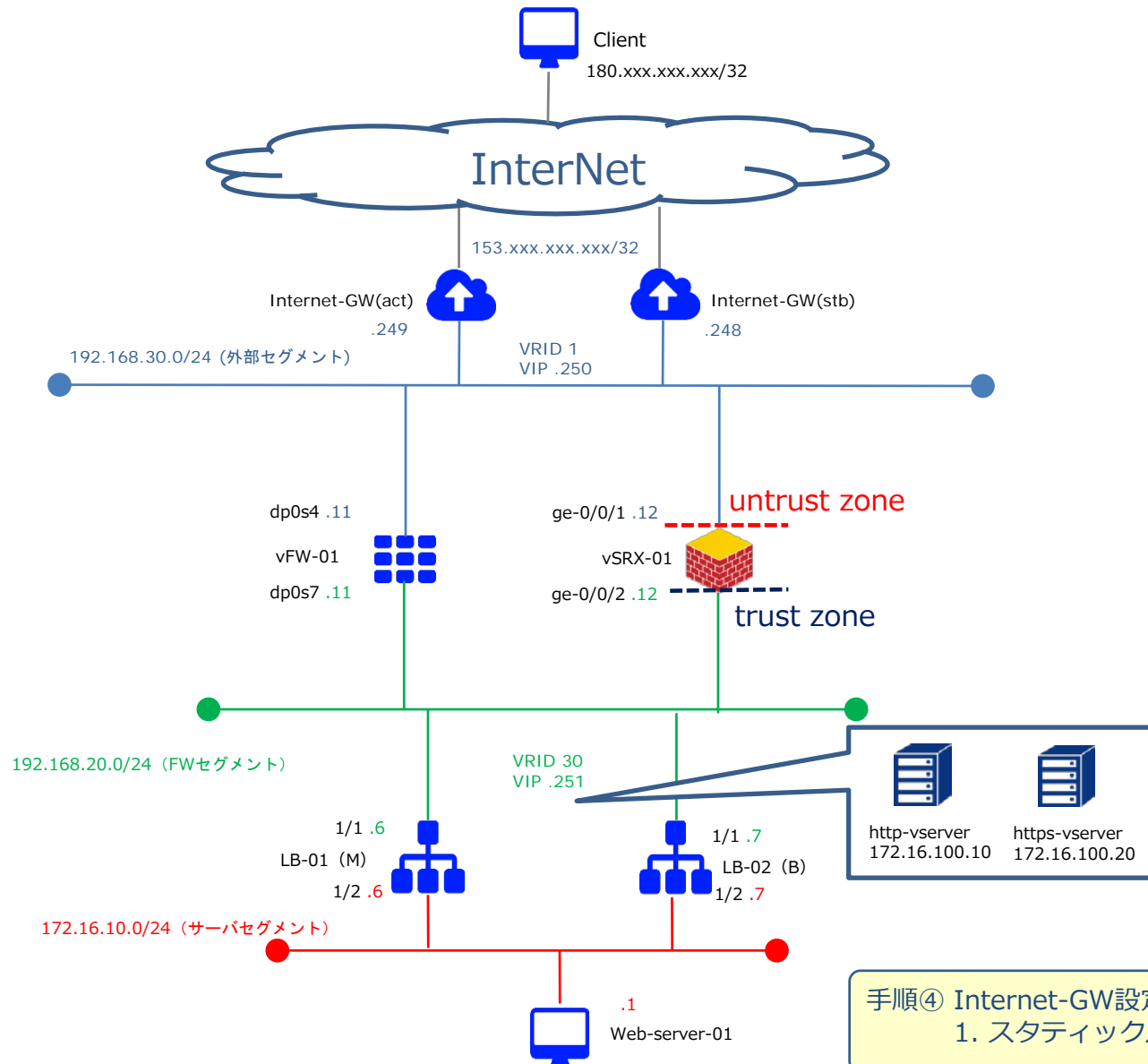
- 手順① vSRX申込み
- 手順② vSRX設定
 - 1. ファイアウォール設定
 - 2. DNAT設定

移行時構成②



手順③ vSRX設定
1. IF接続

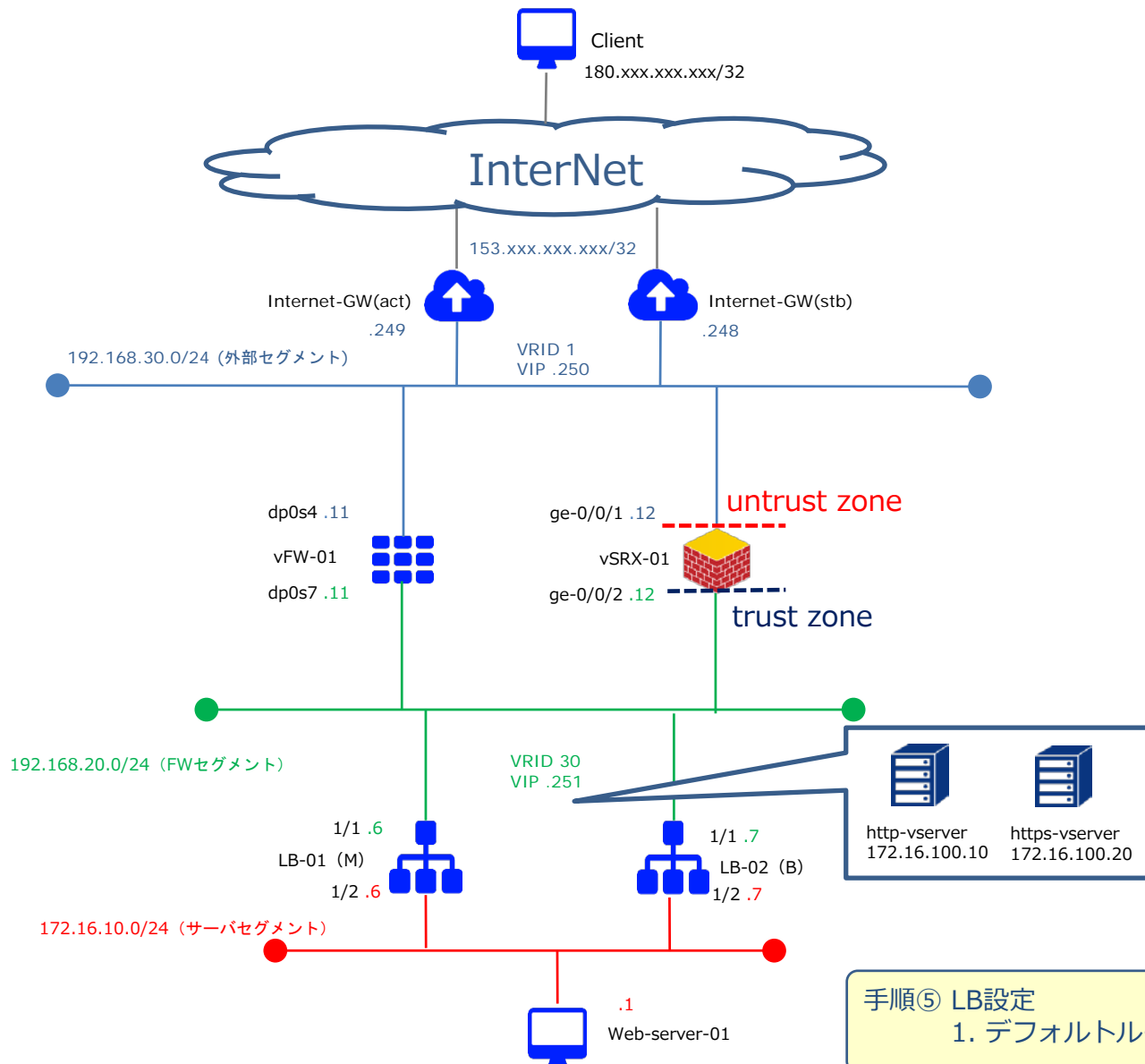
移行時構成③



断時間：5分程度
(実測値)

手順④ Internet-GW設定
1. スタティックルート変更(通信断発生)

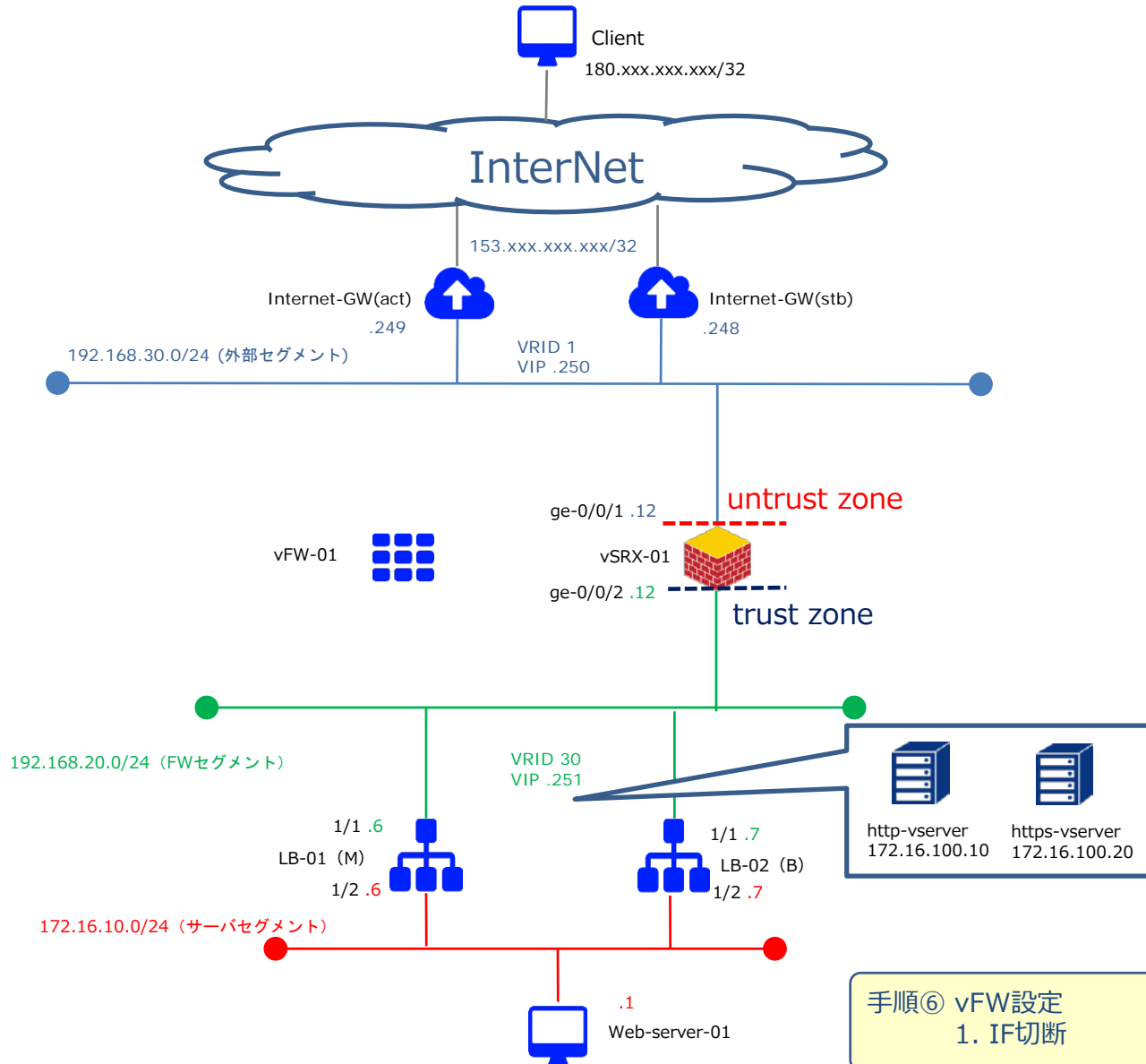
移行時構成④



断時間：5分程度
(実測値)

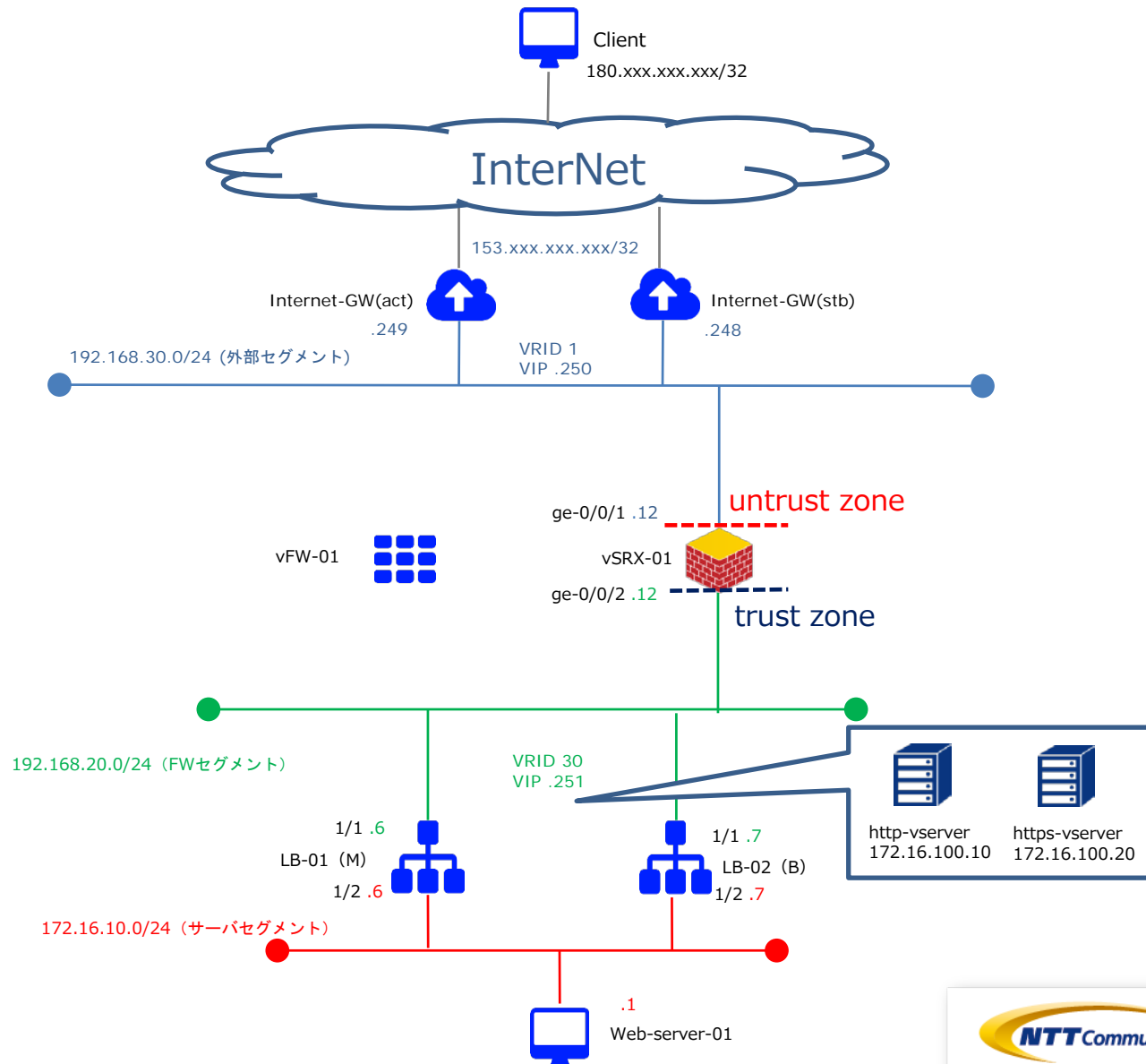
手順⑤ LB設定
1. デフォルトルート変更(通信断回復)

移行時構成⑤



手順⑥ vFW設定
1. IF切断

移行完了構成



手順① vSRX申し込み

手順① vSRX申込み

下記リンクを参照の上、vSRXのお申し込みをお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/instance/create.html>

コントロールパネル画面にログイン後、クラウドコンピューティングをクリックし、「ネットワーク」、「ファイアウォール」、「vSRX」をクリックしてください。



手順① vSRX申込み

ファイアウォール作成ボタンをクリックし、「詳細」と「インターフェイス」で必要な設定値を入力してください。

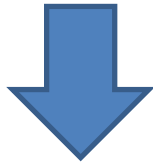
インターフェイス設定では管理用IPアドレスを入力してください。
設定を入力後、「ファイアウォールの作成」をクリックしてください。



ファイアウォール (vSRX)

フィルター +ファイアウォールの作成 ファイアウォールの削除

名前 説明 ブラン ソーン/グループ ステータス 最終オペレーション状態 最終オペレーション詳細 アクション



ファイアウォールの作成

詳細 インターフェイス

名前 ファイアウォールを作成するための詳細情報を指定します。

説明

ファイアウォールプラン*
ファイアウォールプランを選択してください

ゾーン/グループ
ゾーン/グループを選択する前に、ファイアウォールプランを選択する必要があります。



ファイアウォールの作成

詳細 インターフェイス

インターフェイス名 ファイアウォールを作成するためのインターフェイス情報を指定します。

ロジカルネットワーク*
ロジカルネットワークを選択してください

IPアドレス*

デフォルトゲートウェイ

手順②-1 vSRX設定 (ファイアーウォール設定)

手順②-1 vSRX設定 (ファイアウォール設定)

ゾーンベースファイアウォールの設定は下記をご覧ください。

https://ecl.ntt.com/documents/tutorials/rsts/vSRX/fwfunction/zonebase/vsrx_zonebase.html

ファイアウォールに論理的に「ゾーン」と呼ばれる領域を作成し、インターフェイスをゾーンに所属させます。

受信パケットに必要なポリシーをゾーンごとに設定するため、ゾーンに属するインターフェイスに対して同一のポリシーを適用させることが可能になります。

ゾーンベースファイアウォールを設定には、「アドレスグループの設定」、「アプリケーションセットの設定」が必要になります。

手順②-1 vSRX設定 (ファイアウォール設定)

下記URLを参考にアドレスグループの設定をお願い致します。

https://ecl.ntt.com/documents/tutorials/rsts/vSRX/fwfunction/zonebase/vsrx_address-set.html

パケットフィルタリングを設定する時にIPアドレスを条件にしたルールを設定することができ、IPアドレスに簡易的な名称をつけてパケットフィルタリングの条件にすることが可能です。
複数のIPアドレスをグループ化する場合、それぞれのIPアドレスに対してアドレスブックを作成し、複数のアドレスブックを含んだアドレスセットを作成して下さい。

参考までに、vSRX-01の設定値は以下の通りです。

```
user@vSRX-01# set security address-book global address CLIENT_01 180.xxx.xxx.xxx/32
user@vSRX-01# set security address-book global address-set CLIENT_GROUP address
CLIENT_01
user@vSRX-01# commit
```

手順②-1 vSRX設定 (ファイアウォール設定)

下記URLを参考にアプリケーションセットの設定をお願い致します。

https://ecl.ntt.com/documents/tutorials/rsts/vSRX/fwfunction/zonebase/vsrx_application-set.html

vSRXにあらかじめ登録されているアプリケーションもしくは任意の名称をつけてアプリケーションを定義しパケットフィルタリングの条件にすることが可能です。

参考までに、vSRX-01の設定値は以下の通りです。

```
user@vSRX-01# set applications application HTTP_DEF protocol tcp destination-port 80
user@vSRX-01# set applications application HTTPS_DEF protocol tcp destination-port 443
user@vSRX-01# set applications application-set HTTP_HTTPS_DEF application HTTP_DEF
user@vSRX-01# set applications application-set HTTP_HTTPS_DEF application HTTPS_DEF
user@vSRX-01# commit
```

手順②-1 vSRX設定 (ファイアウォール設定)

作成したアドレスセットとアプリケーションセットを送信元とする通信(パケット)に関して許可して、それ以外の通信(パケット)はゾーンベースファイアウォールで遮断する設定を行います。

外部セグメントからの通信は全て拒否し、特定の送信元(180.xxx.xxx.xxx/32)からのHTTP/HTTPS通信のみ許可する設定は、下記になります。

```
user@vSRX-01# set security policies from-zone untrust to-zone trust policy PERMIT_GROUP match source-address CLIENT_GROUP
user@vSRX-01# set security policies from-zone untrust to-zone trust policy PERMIT_GROUP match destination-address any
user@vSRX-01# set security policies from-zone untrust to-zone trust policy PERMIT_GROUP match application HTTP_HTTPS_DEF
user@vSRX-01# set security policies from-zone untrust to-zone trust policy PERMIT_GROUP then permit
user@vSRX-01# commit
```

手順②-2 vSRX設定 (DNAT設定)

手順②-2 vSRX設定 (DNAT設定)

Destination NATの設定は下記をご覧ください。

<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/network/nat/nat.html>

CLIでログイン後、

シェルコマンドモード > オペレーションモード > コンフィグレーションモードへ移行します。

宛先が153.xxx.xxx.xxx/32のHTTP/HTTPS通信をロードバランサーのVirtual Serverに変換致します。

参考までに、vSRX-01の設定値を次ページに記載します。

手順②-2 vSRX設定 (DNAT設定)

ロードバランサーのVirtual Serverへアクセスする為のIPアドレス変換設定は、下記になります。

```
user@vSRX-01# set security nat destination pool POOL1 address 172.16.100.10/24 port 80
user@vSRX-01# set security nat destination pool POOL2 address 172.16.100.20/24 port 443
user@vSRX-01# set security nat destination rule-set RULE1 from zone untrust
user@vSRX-01# set security nat destination rule-set RULE1 rule RULE1-1 match destination-address
153.xxx.xxx.xxx/32
user@vSRX-01# set security nat destination rule-set RULE1 rule RULE1-1 match destination-port 80
user@vSRX-01# set security nat destination rule-set RULE1 rule RULE1-1 then destination-nat pool POOL1
user@vSRX-01# set security nat destination rule-set RULE1 rule RULE1-2 match destination-address
153.xxx.xxx.xxx/32
user@vSRX-01# set security nat destination rule-set RULE1 rule RULE1-2 match destination-port 443
user@vSRX-01# set security nat destination rule-set RULE1 rule RULE1-2 then destination-nat pool POOL2
user@vSRX-01# commit
```


手順③ vSRX設定 (インターフェース設定)

手順③ vSRX設定 (インターフェース設定)

vSRXに設定するインターフェースに対してIPアドレスを設定し通信可能にするためには、ECL2.0のカスタマポータル上でインターフェースとIPアドレスの設定を実行する必要があります。

vSRXのインターフェースはge-0/0/0を除き初期状態でゾーンに所属させる設定がされておられません。通信するためには必ずゾーンベースファイアウォールのいずれかのゾーンに所属させる必要があります。

インターフェースのIPアドレスに着信する通信を許可するためにはhost-inbound-traffic配下で該当の通信を許可する設定が必要になります。

手順③ vSRX設定 (インターフェース設定)

下記リンクを参照の上、ECL2.0のカスタマポータル上でvSRXのインターフェース設定をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/instance/update.html>

コントロールパネル画面にログイン後、クラウドコンピューティングをクリックし、「ネットワーク」、「ファイアウォール」、「vSRX」をクリックしてください。



手順③ vSRX設定 (インターフェース設定)

対象のvSRXで「ファイアウォールインターフェースの編集」をクリックして下さい。

The screenshot displays a configuration page for vSRX instances. A table lists several instances, with the first one selected. A dropdown menu is open for the selected instance, showing various management options. The option 'ファイアウォールインターフェースの編集' (Edit Firewall Interface) is highlighted with a red box.

vSRX ID	Configuration	Group	Monitoring Status	Login Status	Completion	UUID	Action
<input type="checkbox"/> vSRX-01	vSRX_15.1X49-D105.1_2CPU_4GB_8IF_STD	zone1_groupb	モニタリングステータス: ACTIVE	ログインステータス: ACTIVE	完了	5b599e78-51f9-4187-8ef1-4473edc5b4e9	ファイアウォールの編集

- ファイアウォールインターフェースの編集
- 許可されたアドレスペアの編集
- パスワードのリセット
- ファイアウォールの起動
- ファイアウォールの停止
- ファイアウォールの再起動
- コンソール
- ファイアウォールの削除

2件表示

NTT Communications All Rights Reserved.

手順③ vSRX設定 (インターフェース設定)

編集したいインターフェースタブを開き、「このインターフェースを編集する」にチェックを入れ、接続先ロジカルネットワークと固定IPアドレスを指定して下さい。
設定値を入力後、「ファイアウォールインターフェースの編集」をクリックして下さい。

「このインターフェースを編集する」に必ずチェックを入れてください。チェックを入れない場合、編集は反映されません。

参考までに、以下はvSRX-01の設定値となります。

ファイアウォールインターフェースの編集

インターフェース1 インターフェース2 インターフェース3 インターフェース4
インターフェース5 インターフェース6 インターフェース7 インターフェース8

このインターフェースを編集する
ロジカルネットワーク*

Internet-segment:(192.168.30.0/24)

固定IPアドレス*

192.168.30.12

ファイアウォールのインターフェースを編集するための情報を指定します。この画面では、接続ロジカルネットワークおよび固定IPアドレスの編集が可能です。

× 取り消し ファイアウォールインターフェースの編集

ファイアウォールインターフェースの編集

インターフェース1 インターフェース2 インターフェース3 インターフェース4
インターフェース5 インターフェース6 インターフェース7 インターフェース8

このインターフェースを編集する
ロジカルネットワーク*

Firewall-segment:(192.168.20.0/24)

固定IPアドレス*

192.168.20.12

ファイアウォールのインターフェースを編集するための情報を指定します。この画面では、接続ロジカルネットワークおよび固定IPアドレスの編集が可能です。

× 取り消し ファイアウォールインターフェースの編集

手順③ vSRX設定 (インターフェース設定)

下記リンクを参照の上、CLIでvSRXのインターフェース設定をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/basic/basic.html#vsrx-cli-ssh>

CLIでログイン後、

シェルコマンドモード > オペレーションモード > コンフィグレーションモードへ移行して下さい。

参考までに、CLIにて入力するコマンドは下記となります。

※ 本検証では、host-inbound-traffic 設定にて ping を許可しております。

追加で許可するサービスやプロトコルがある場合は、下記リンクを参照の上、ご利用の環境で必要に応じて設定をお願い致します。

https://ecl.ntt.com/documents/tutorials/rsts/vSRX/fwfunction/zonebase/vsrx_zoneconfig.html

```
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.12/24
user@vSRX-01# set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services ping
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.12/24
user@vSRX-01# set security zones security-zone trust interfaces ge-0/0/2.0 host-inbound-traffic system-services ping
user@vSRX-01# commit
```

手順④ Internet-GW設定 (スタティックルート変更)

手順④ Internet-GW設定 (スタティックルート変更)

下記リンクを参照の上、ECL2.0のカスタマポータル上でインターネットゲートウェイのスタティックルートの設定変更をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/Network/internet.html>

コントロールパネル画面にログイン後、クラウドコンピューティングをクリックし、「ネットワーク」、「インターネット接続」をクリックしてください。



手順④ Internet-GW設定 (スタティックルート変更)

対象のインターネットゲートウェイをクリックし、「スタティックルート」をクリック。
対象のスタティックルートをチェックし、「スタティックルートの削除」をクリックして下さい。
通信断が発生します。



インターネットゲートウェイの編集 ▼

概要 グローバルIP ゲートウェイインターフェイス スタティックルート

+ スタティックルートの追加 **■ スタティックルートの削除**

<input checked="" type="checkbox"/>	名前	説明	宛先	ネクストホップ	ステータス	アクション
<input checked="" type="checkbox"/>	(d5cab8df-8e05)		153.138.234.67/32	192.168.30.11	稼働中	スタティックルートの編集 ▼



×

スタティックルートの削除の確認

"(d5cab8df-8e05)" を選択しました。選択内容を確認してください。この操作は取り消せません。

取り消し **■ スタティックルートの削除**

手順④ Internet-GW設定 (スタティックルート変更)

対象のインターネットゲートウェイをクリックし、「スタティックルート」から「スタティックルートの追加」をクリック。



The screenshot shows the configuration page for an Internet Gateway. The 'Static Routes' tab is selected. A red box highlights the '+ スタティックルートの追加' button. Below the buttons is a table with columns: 名前, 説明, 宛先, ネクストホップ, ステータス, アクション. The table is currently empty, with the text '表示する項目がありません' (No items to display) below it.

スタティックルートのネクストホップにvSRX-01のIPアドレスを入力してください。設定を入力後、「スタティックルートの追加」をクリックしてください。



The screenshot shows the 'Add Static Route' dialog box. The 'Next Hop' field is filled with '192.168.30.12'. The 'Add Static Route' button is highlighted with a red box.

名前	説明:
	インターネットゲートウェイに対するスタティックルート追加のためのパラメータを指定します。

宛先 *
153.138.234.67/32

ネクストホップ *
192.168.30.12

取り消し **スタティックルートの追加**

手順⑤ LB設定 (デフォルトルート変更)

手順⑤ LB設定 (デフォルトルート変更)

下記リンクを参照の上、ECL2.0のカスタマポータル上でロードバランサーのデフォルトゲートウェイの設定変更をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/LoadBalancer/instance/operations.html>

コントロールパネル画面にログイン後、クラウドコンピューティングをクリックし、「ネットワーク」、「ロードバランサー」をクリックしてください。



手順⑤ LB設定 (デフォルトルート変更)

対象のロードバランサーから、「ロードバランサーの編集」をクリック。

		フィルター	+	ロードバランサーの作成	ロードバランサーの削除
<input type="checkbox"/> 名前	説明	ロードバランサープラン	ゾーン/グループ	ステータス	アクション
<input type="checkbox"/> VPX-01		Citrix_NetScaler_VPX_12.0-53.13_Standard_Edition_50Mbps_2CPU-8GB-4IF	zone1-groupa	稼働中	ロードバランサーの編集
<input type="checkbox"/> VPX-02		Citrix_NetScaler_VPX_12.0-53.13_Standard_Edition_50Mbps_2CPU-8GB-4IF	zone1-groupa	稼働中	ロードバランサーの編集

2 件表示

「デフォルトゲートウェイ」をvSRX-01のIPアドレスに変更し、「ロードバランサーの編集」をクリック。
通信が回復します。

ロードバランサーの編集

名前
VPX-01

説明
ロードバランサーの基本情報を指定します。

ロードバランサープラン
元のプランを変更しない

利用可能なサブネット
(e58413f4-296d) (192.168.10.0/24)

デフォルトゲートウェイ
192.168.20.12

各リソースに対する料金は、作成/変更操作が完了した時点で発生します。
作成前にこちらの注意事項をご確認ください。

取り消し **ロードバランサーの編集**

手順⑤ LB設定 (デフォルトルート変更)

同様の手順でLB-02のデフォルトルートの設定変更をお願いいたします。

vSRXへの移行後、お客様環境に応じて通信確認をお願い致します。

正常に通信が出来ている事を確認した後、次のページ

「手順⑥ vFWの設定変更（インターフェースの切断）」に進んで下さい。

手順⑥ vFW設定 (インターフェースの切断)

手順⑥ vFWの設定 (インターフェースの切断)

ファイアウォールのロジカルネットワーク切断をお願いいたします。
コントロールパネル画面にログイン後、「ネットワーク」、「Brocade 5600 vRouter」をクリックし、対象のファイアウォールを選択ください。

The screenshot shows a web-based network management interface. On the left is a sidebar menu with the following items: ネットワーク, インターネット接続, VPN接続, ロジカルネットワーク, **ファイアウォール**, vSRX, **Brocade 5600 vRouter** (highlighted with a red box), マネージドファイアウォール, and ロードバランサー. The main content area is titled 'ファイアウォール' and displays a table of firewall configurations:

<input type="checkbox"/>	名前	説明	ファイ
<input type="checkbox"/>	MGMT-FW		Broca
<input type="checkbox"/>	vFW-01		Broca
<input type="checkbox"/>	vFW-02		Broca

At the bottom of the table, it says '3 件表示' (Display 3 items).

手順⑥ vFWの設定 (インターフェースの切断)

対象のインターフェースから、「ロジカルネットワークの切断」をクリック。

概要		ファイアウォールインターフェイス						
名前	説明	スロット番号	ロジカルネットワーク	IP アドレス	仮想IPアドレス	Enterprise Cloud 2.0 接続	ステータス	アクション
dp0s4	-	1	69093a73-1386-41df-acff-792d102ed9b8	192.168.30.11	-	-	稼働中	ファイアウォールインターフェイスの編集 ロジカルネットワークの接続 ロジカルネットワークの切断 VRRP用通信設定の登録 VRRP用通信設定の解除
dp0s5	-	2	07295beb-da13-44b7-9358-2cfb3335afe02	10.0.0.11	-	-	稼働中	ファイアウォールインターフェイスの編集
dp0s6	-	3	-	-	-	-	停止中	ファイアウォールインターフェイスの編集
dp0s7	-	4	6200b5fb-0391-4263-86e8-5bb0bda7f0c3	192.168.20.11	-	-	稼働中	ファイアウォールインターフェイスの編集

「ロジカルネットワークの切断」をクリック。

ロジカルネットワークの切断

ロジカルネットワーク*

Internet-seg (192.168.30.0/24)

IP アドレス

192.168.30.11

説明:

ファイアウォールからロジカルネットワークを切断します。

ロジカルネットワークの切断には、再起動が実施されますので、処理が完了するまで10分程度かかる場合がございます。