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
2018/10/24	初版	1

Copyright © NTT Communications Corporation. All right reserved.

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)は発生しないケースです。

・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へ付け替えます。
⇒ vFWで利用しているネットワークの接続解除から、vSRXへの付け替え完了まで、通信断が発生いたします。

・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

・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。

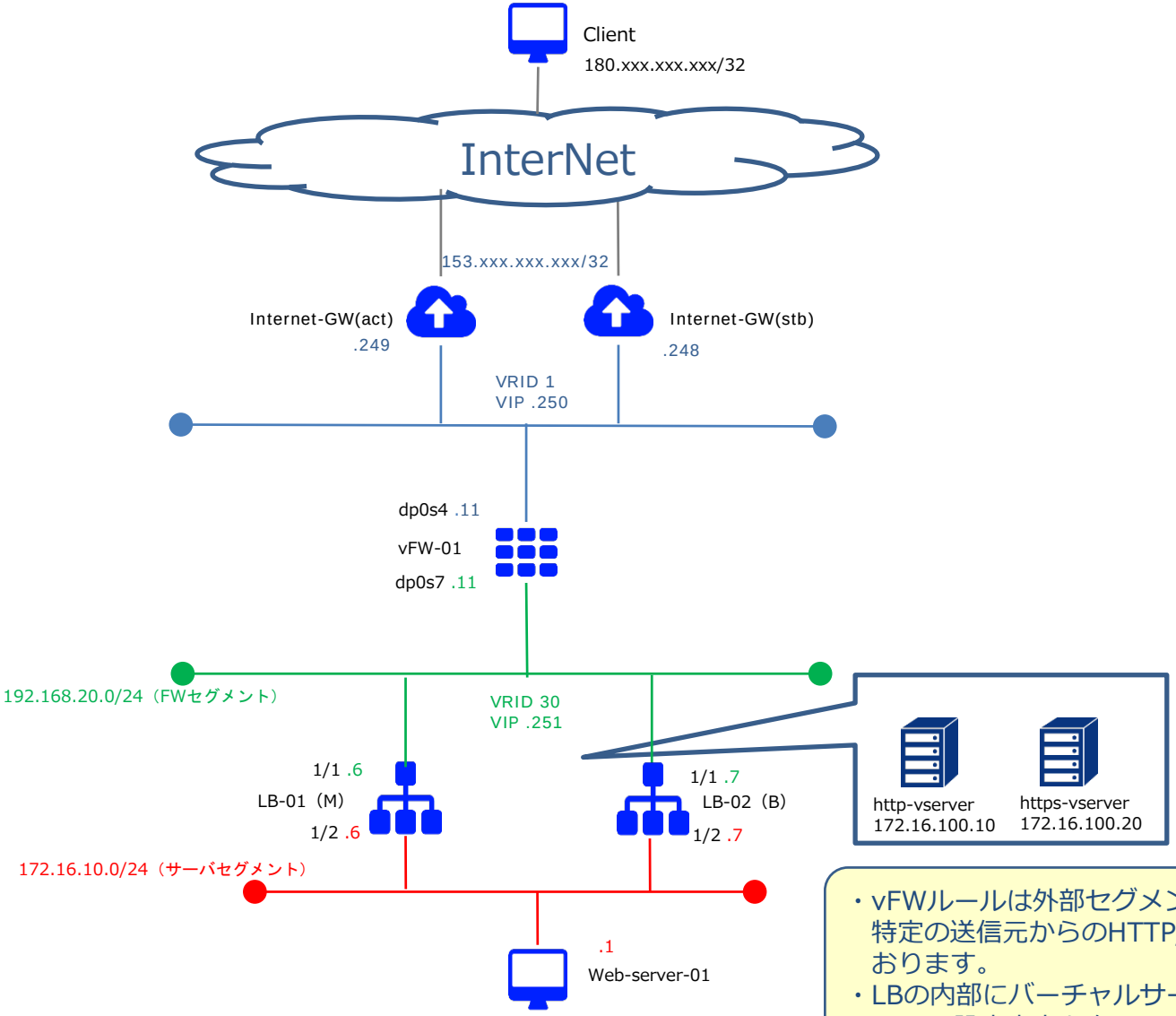
・vSRX作成時、インターフェイス(ge-0/0/0.0)はTrustゾーンに設定されております。
⇒作成後、各インターフェイスはお客様環境にそって読み替えて設定頂きますようお願い致します。

・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）



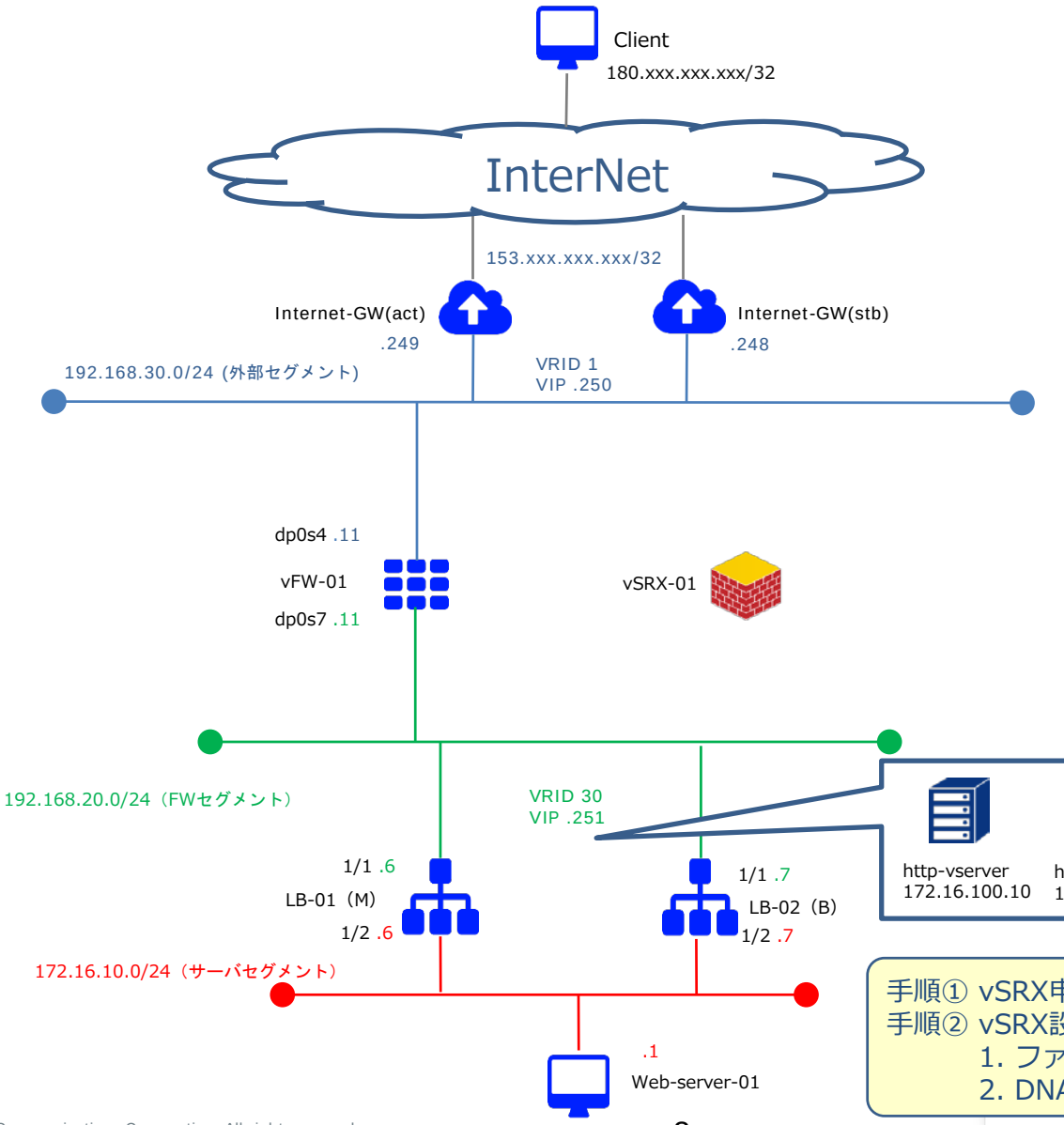
- vFWルールは外部セグメントからの通信は全て拒否し、特定の送信元からのHTTP/HTTPS通信のみ許可しております。
- LBの内部にバーチャルサーバーを設定しておきます。
- vFWの設定内容を次のページに記載致します。

移行前構成（vFW構成）設定値

vFW-01 Firewall Filterの設定

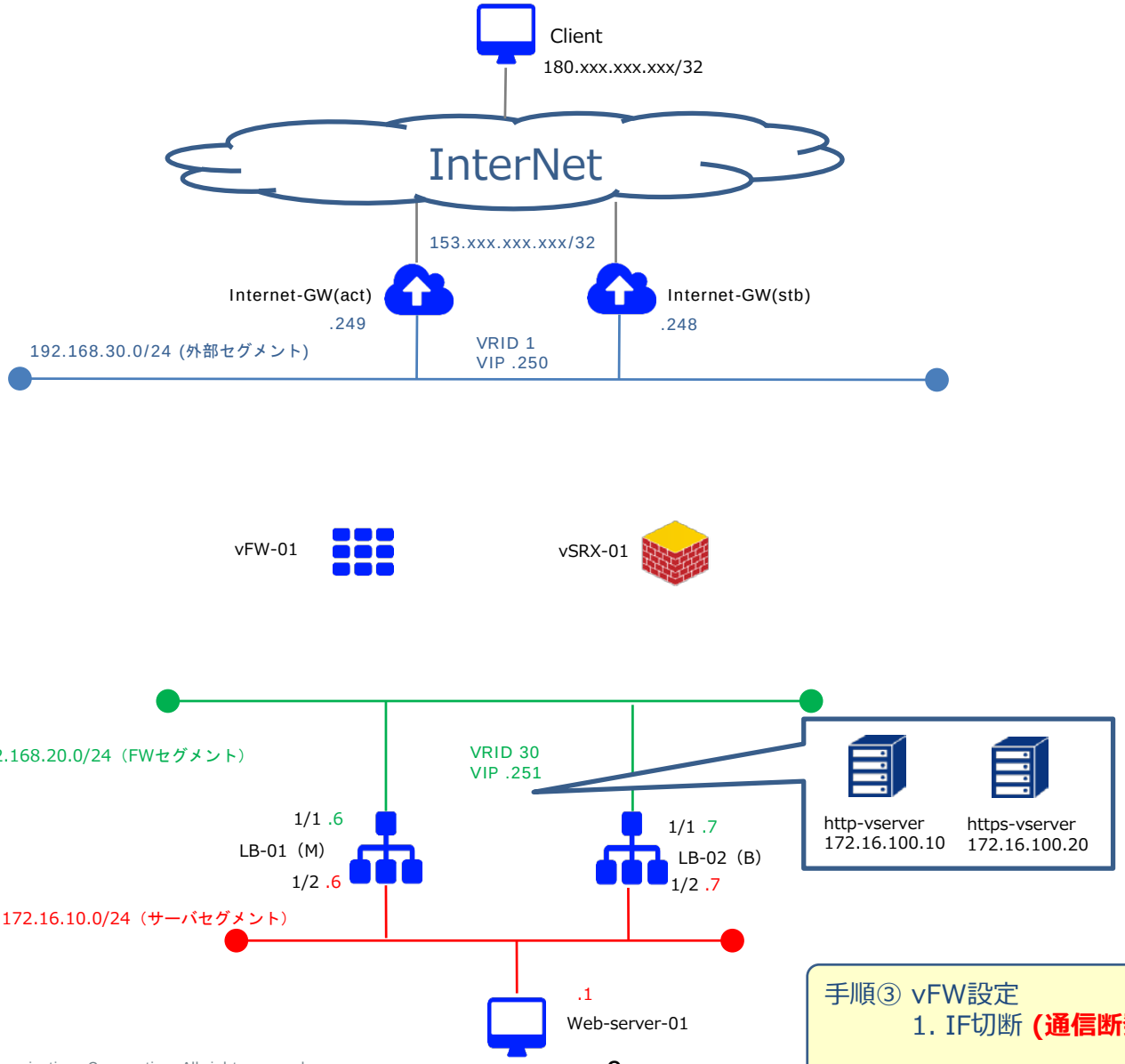
```
set security firewall name From-Internet default-action 'drop'
set security firewall name From-Internet rule 10 action 'accept'
set security firewall name From-Internet rule 10 protocol 'tcp'
set security firewall name From-Internet rule 10 source address ‘180.xxx.xxx.xxx/32’
Set security firewall 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 security firewall name From-Internet rule 30 action 'accept'
set security firewall name From-Internet rule 30 protocol 'vrrp'
set security firewall name From-Internet rule 30 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

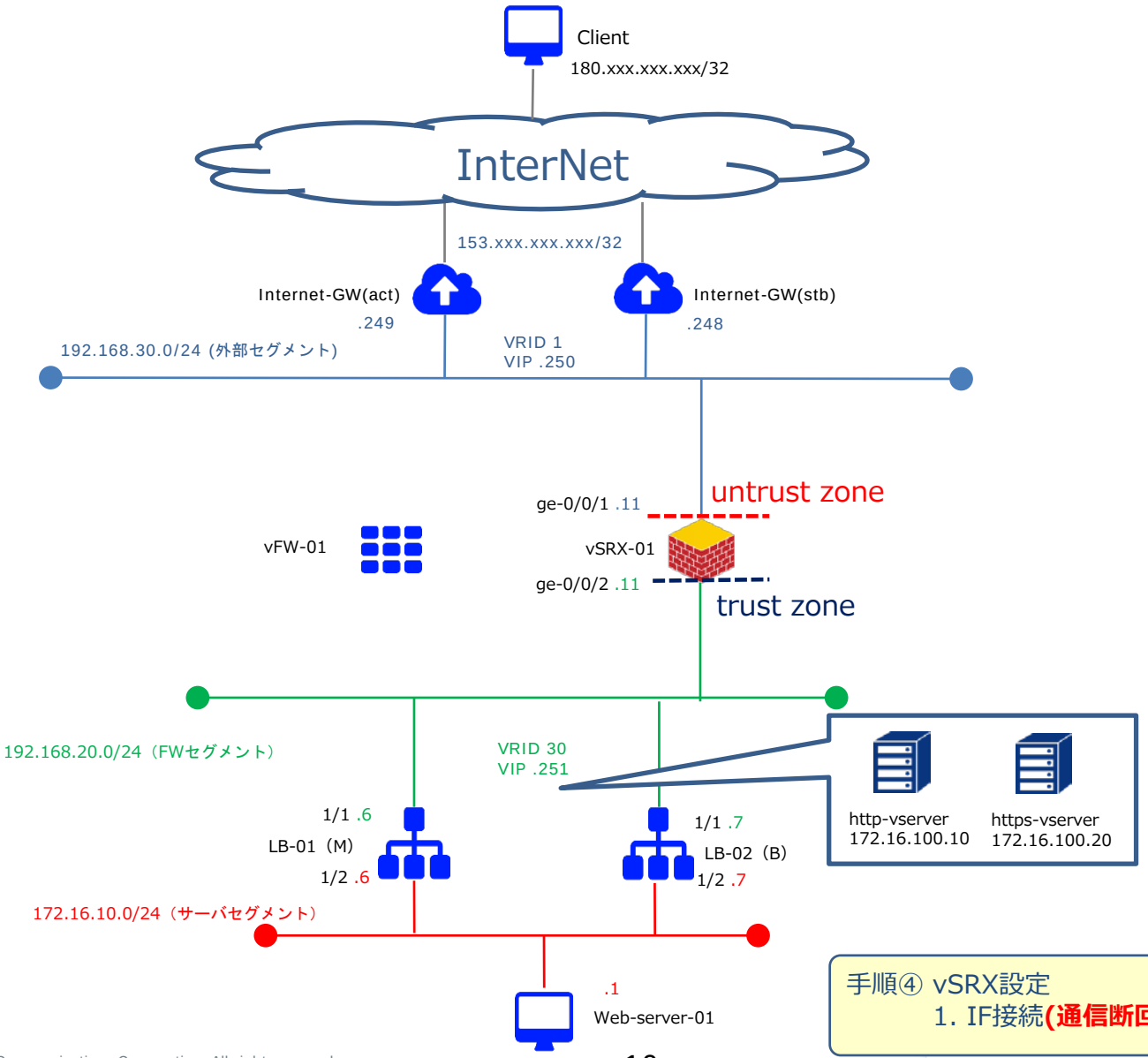
移行時構成②



断時間：50分程度
（実測値）

手順③ vFW設定
1. IF切断 **(通信断発生)**

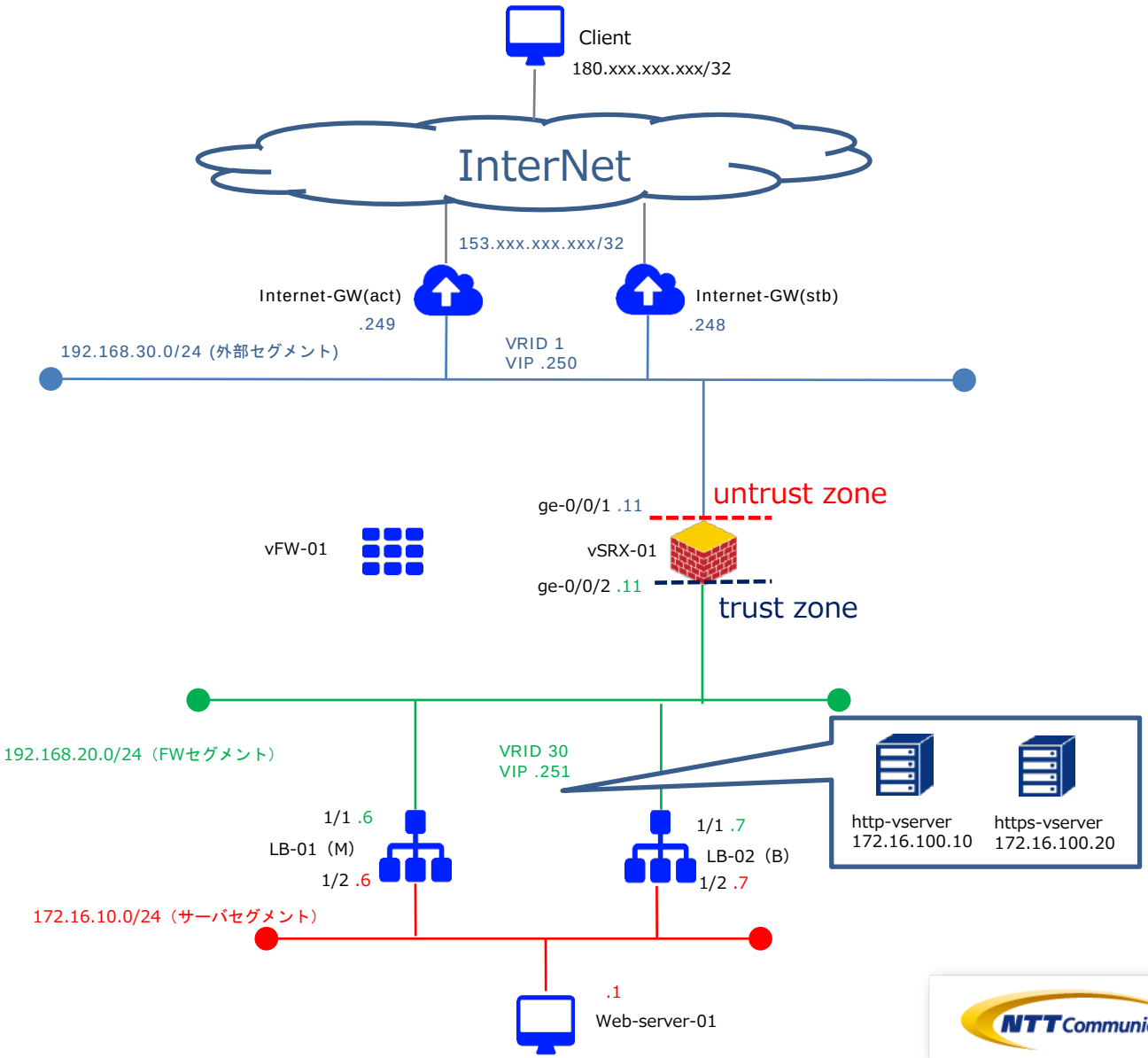
移行時構成③



断時間：50分程度
（実測値）

手順④ vSRX設定
1. IF接続**(通信断回復)**

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

ファイアーウォール作成ボタンをクリックし、「詳細」と「インターフェース」で必要な設定値を入力してください。
インターフェース設定では管理用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。

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ー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 vFW設定
(インターフェースの切断)

手順③ 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。

手順③ 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。

「ロジカルネットワークの切断」をクリック。**通信断が発生します。**

手順④ vSRX設定
(インターフェース設定)

手順④ 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イスに対して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イスとIPアドレスの設定を実行する必要があります。

vSRXに設定するIPアドレスはvFWで使用していたIPアドレスを設定して下さい。

vSRXのインターフェイスは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りません。
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。

インターフェイスの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④ 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④ 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イスの編集」をクリックして下さい。

手順④ vSRX設定
(インターフェース設定)

編集したいインターフェイスタブを開き、「このインターフェイスを編集する」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イスの編集」をクリックして下さい。

「このインターフェイスを編集する」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。

手順④ 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 192.168.30.11/24
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 192.168.20.11/24
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
```

インターフェース設定が完了すると、**通信が回復します。**