

# 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2版

# 更新履歴

更新日	更新内容	版数
2018/10/03	初版	1
2018/10/17	NATで、グローバルIPアドレスを変換する前提で各種修正	2

# 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VRRPプライオリティ変更によるマイグレ実施方法です。

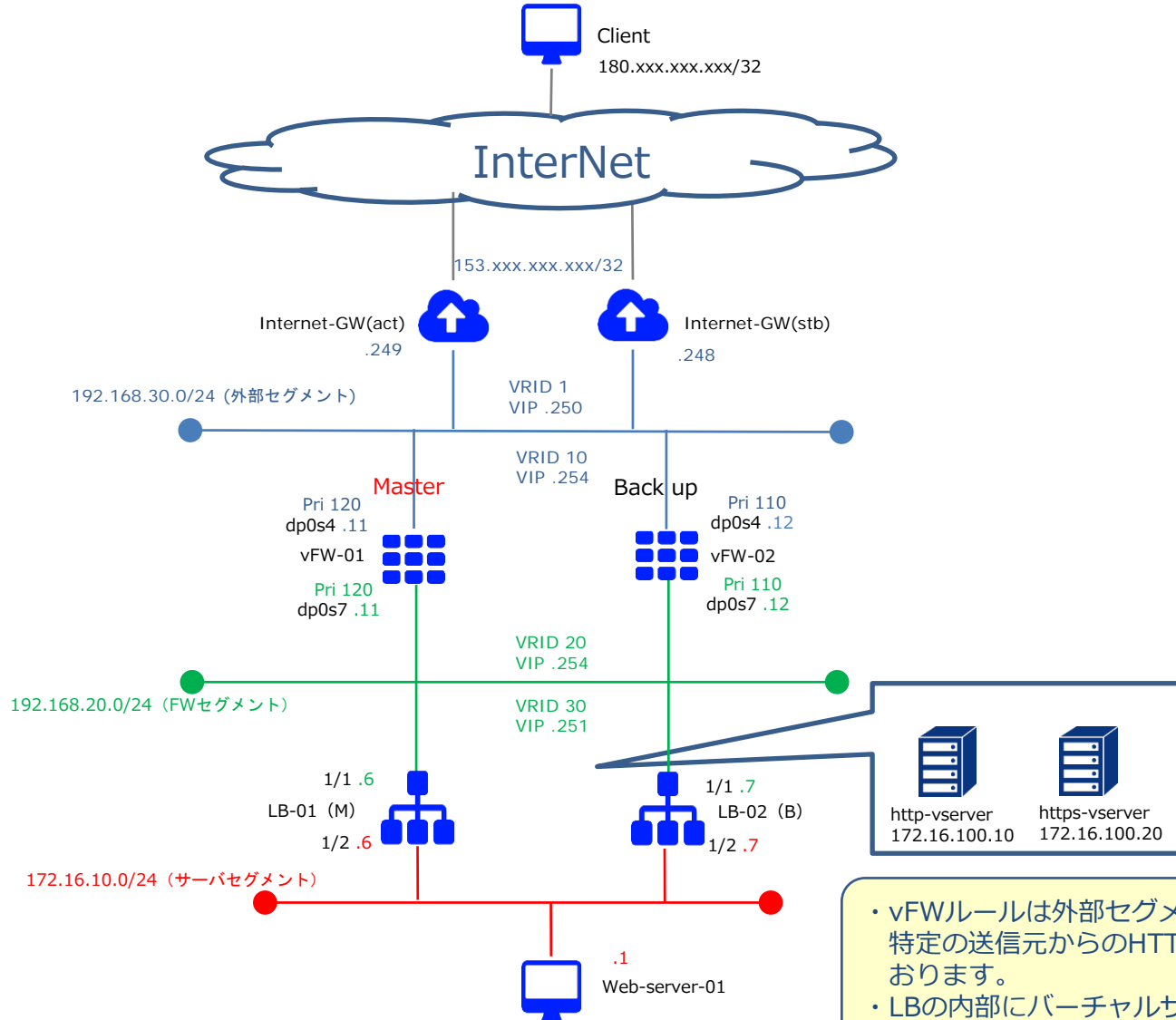
- Internet-GW, ロードバランサー, Webサーバーの設定変更(Routing変更等)は発生しないケースです。
- ロードバランサーは、ツーアーム構成のマイグレ実施方法です。ワンアーム構成をご利用の場合はお客様環境にそって、読み替えて頂きますようお願い致します。
- vFW(×2台)で利用しているVRRPグループにvSRX(×2台)を追加致します。  
⇒ 本手順検証において、VRRPグループ追加時、及びvSRXのプライオリティ値変更による移行時通信断は確認できませんでした。ただし、お客様のご利用アプリケーションに影響なく移行出来る事を保証するわけではございませんので、事前検証の上、切替に伴う通信影響をご確認頂けますようお願い致します。
- 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のVRRP advertise-intervalの値は、vFWと同等の値を設定して下さい。
- 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'
```

## vFW-01 VRRPの設定

```
set interfaces dataplane dp0s4 vrrp vrrp-group 10 advertise-interval '[任意の値]'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 preempt 'true'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 priority '120'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 'rfc-compatibility'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 virtual-address '192.168.30.254'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 sync-group 'test'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 advertise-interval '[任意の値]'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 preempt 'true'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 priority '120'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 'rfc-compatibility'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 virtual-address '192.168.20.254'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 sync-group 'test'
```

## vFW-01 VRRPの状態

```
user@vFW-01:~$ show vrrp
```

Interface	Group	RFC State	Addr Compliant	Last Owner	Sync Transition	Group
dp0s4	10	MASTER	dp0vrrp1	no	2d18h25m44s	<none>
dp0s7	20	MASTER	dp0vrrp2	no	2d18h25m44s	<none>

```
user@vFW-01:~$
```

# 移行前構成 (vFW構成) 設定値

## vFW-02 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'
```

## vFW-02 VRRPの設定

```
set interfaces dataplane dp0s4 vrrp vrrp-group 10 advertise-interval '[任意の値]'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 preempt 'true'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 priority '110'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 'rfc-compatibility'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 virtual-address '192.168.30.254'
set interfaces dataplane dp0s4 vrrp vrrp-group 10 sync-group 'test'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 advertise-interval '[任意の値]'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 preempt 'true'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 priority '110'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 'rfc-compatibility'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 virtual-address '192.168.20.254'
set interfaces dataplane dp0s7 vrrp vrrp-group 20 sync-group 'test'
```

## vFW-02 VRRPの状態

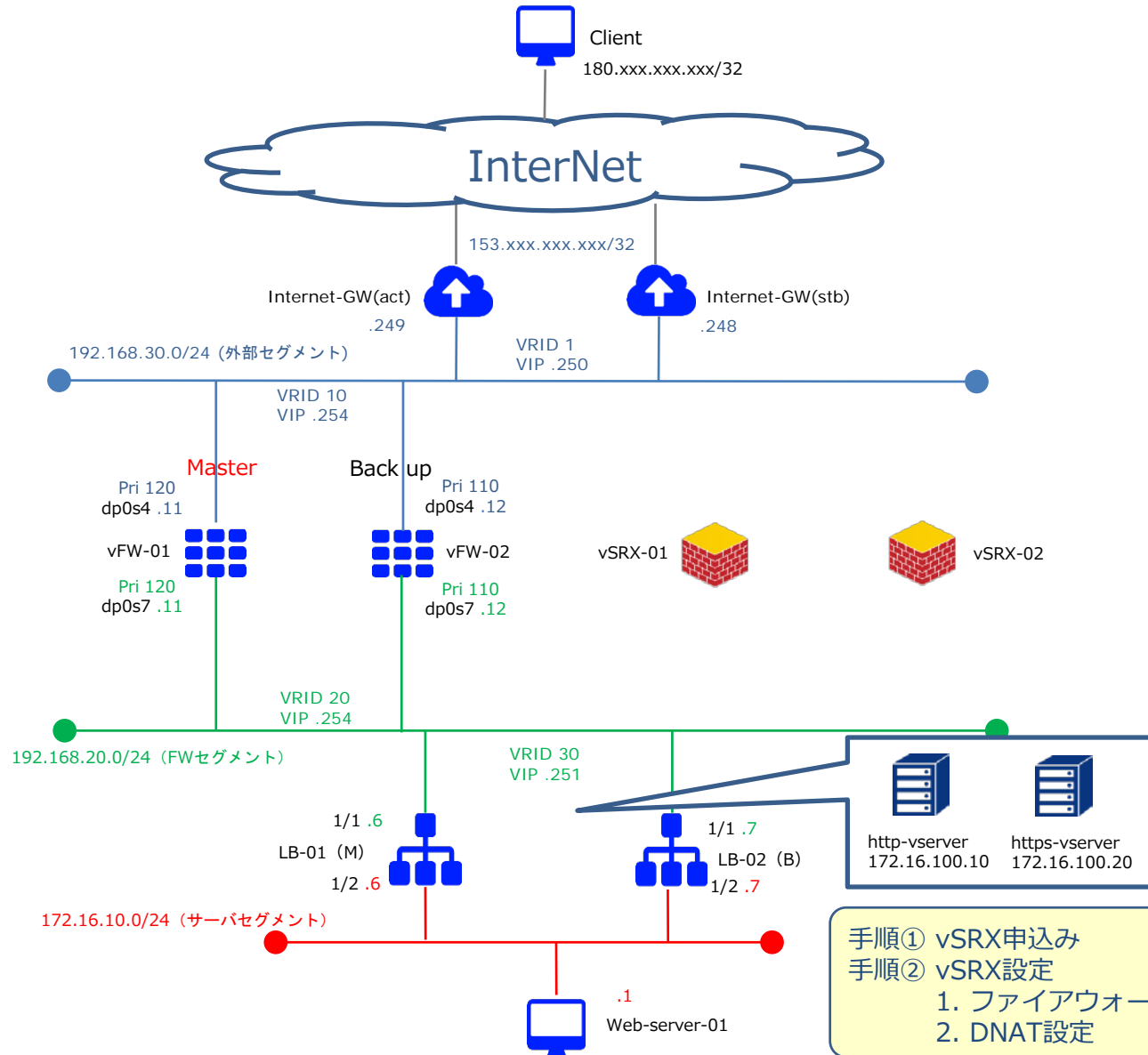
```
user@vFW-02:~$ show vrrp
```

Interface	Group	RFC State	Addr Compliant	Last Owner	Sync Transition	Group
dp0s4	10	BACKUP	dp0vrrp2	no	2d18h27m0s	<none>
dp0s7	20	BACKUP	dp0vrrp1	no	2d18h26m56s	<none>

```
user@vFW-02:~$
```

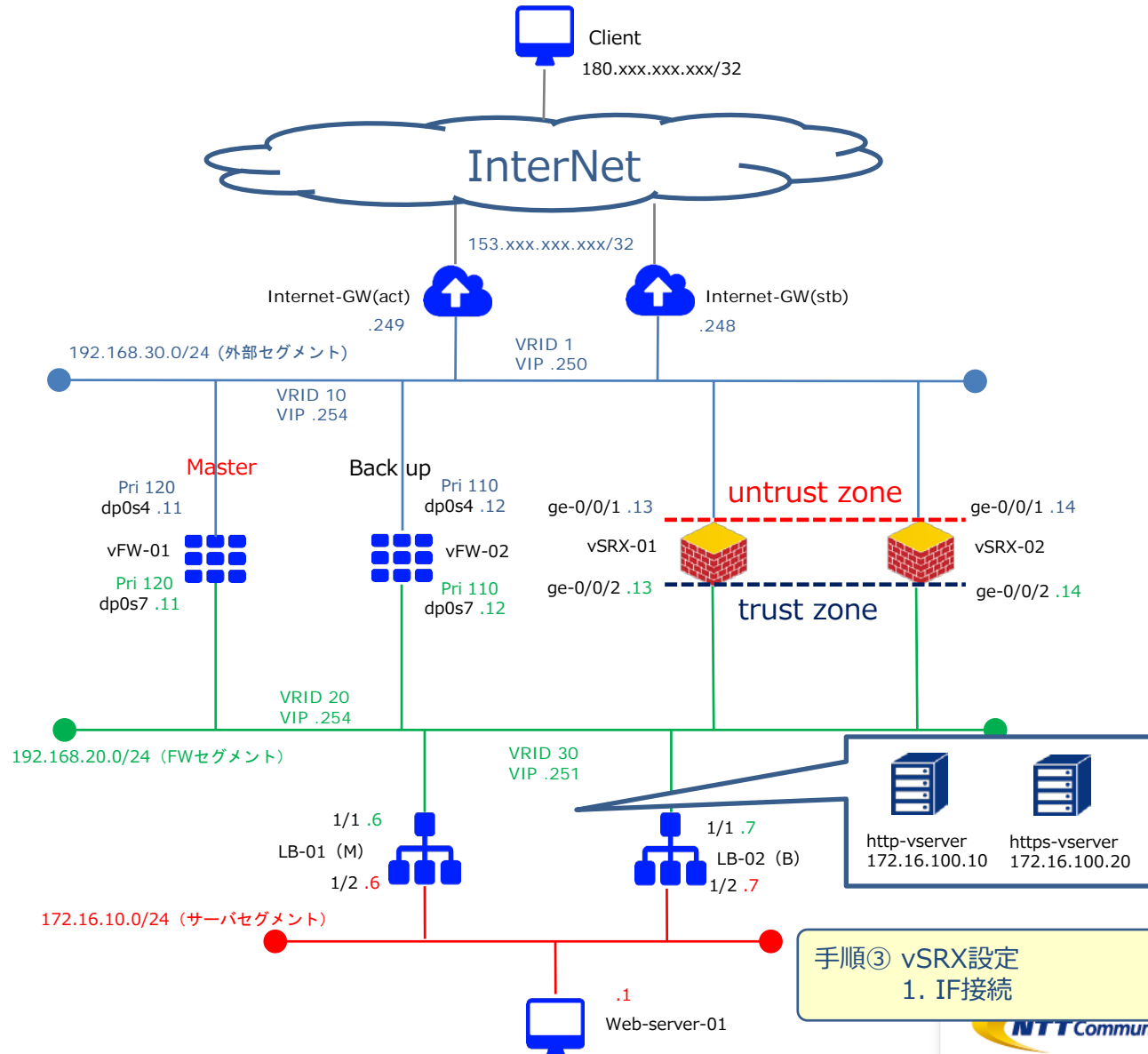


# 移行時構成①

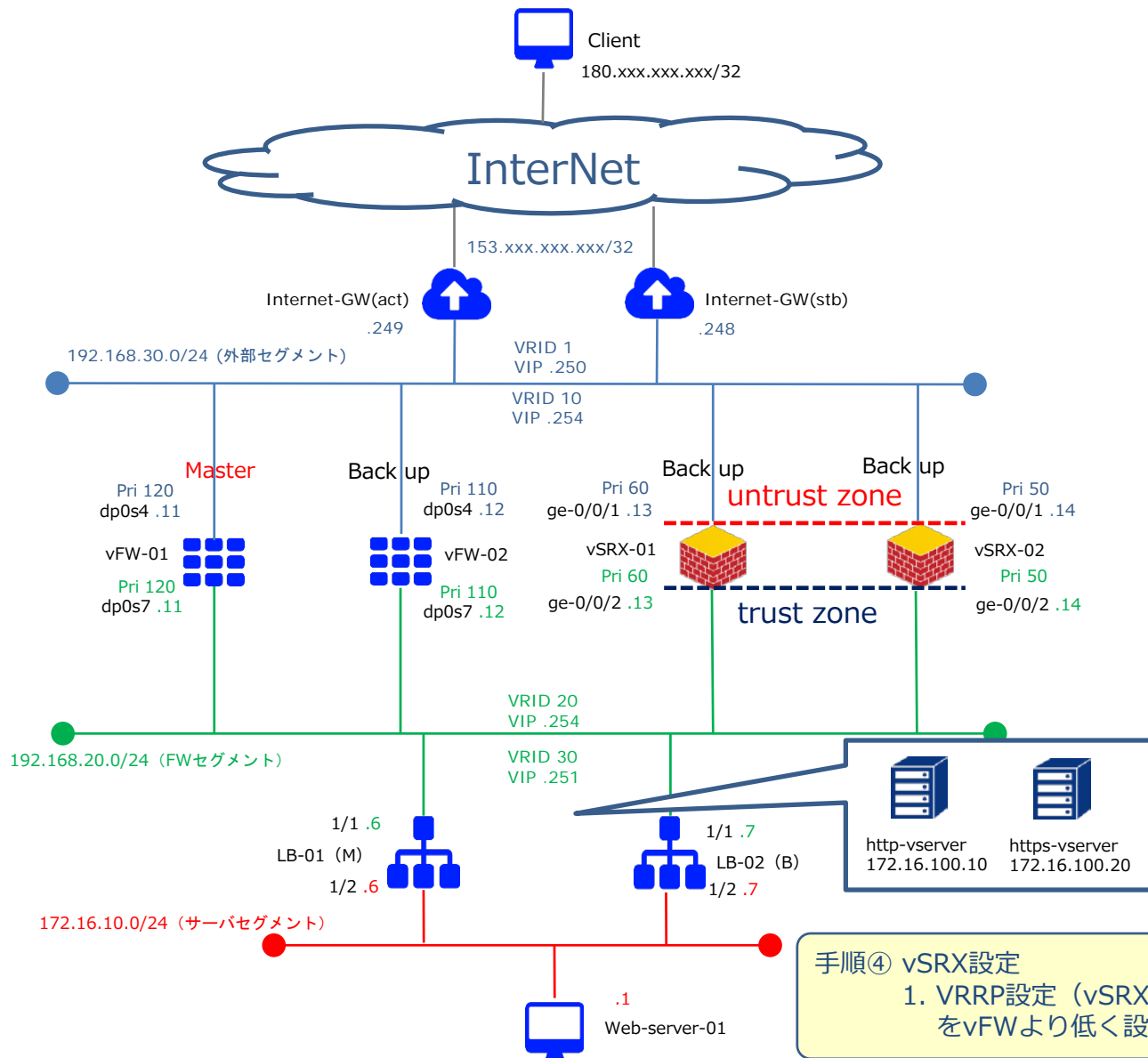


- 手順① vSRX申込み
- 手順② vSRX設定
  - 1. ファイアウォール設定
  - 2. DNAT設定

# 移行時構成②

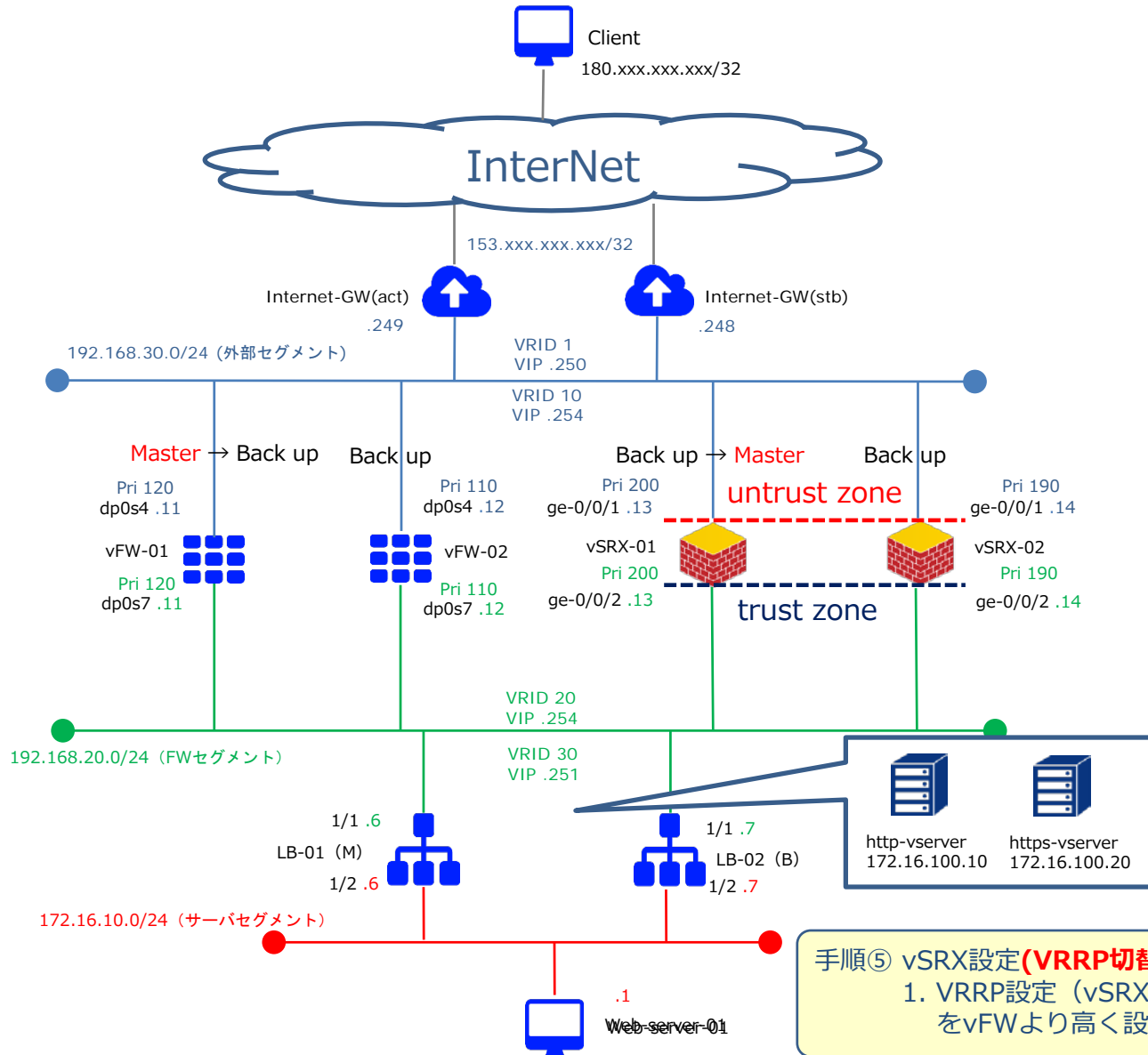


# 移行時構成③



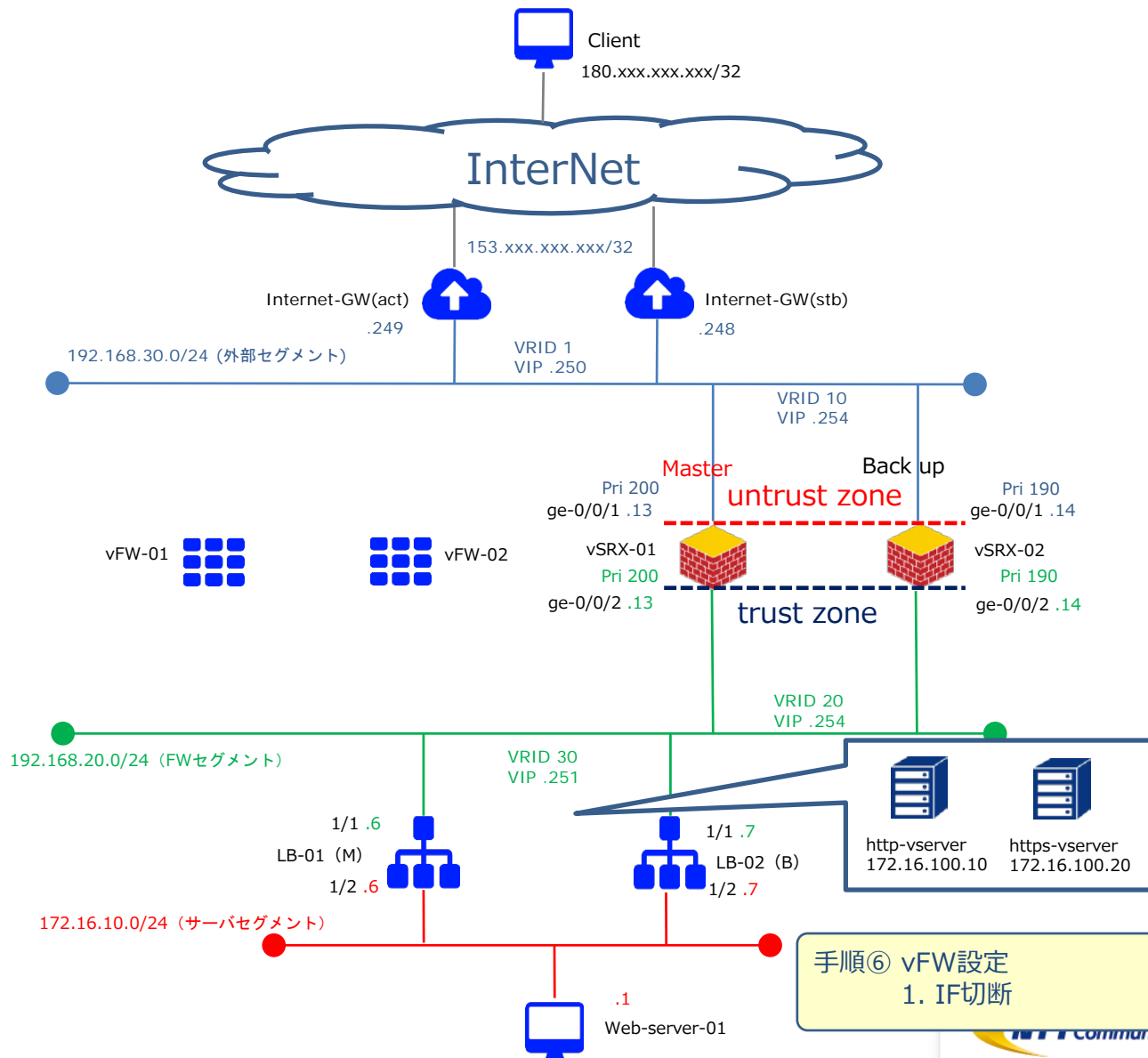
手順④ vSRX設定  
 1. VRRP設定 (vSRX2台のプライオリティをvFWより低く設定)

# 移行時構成④

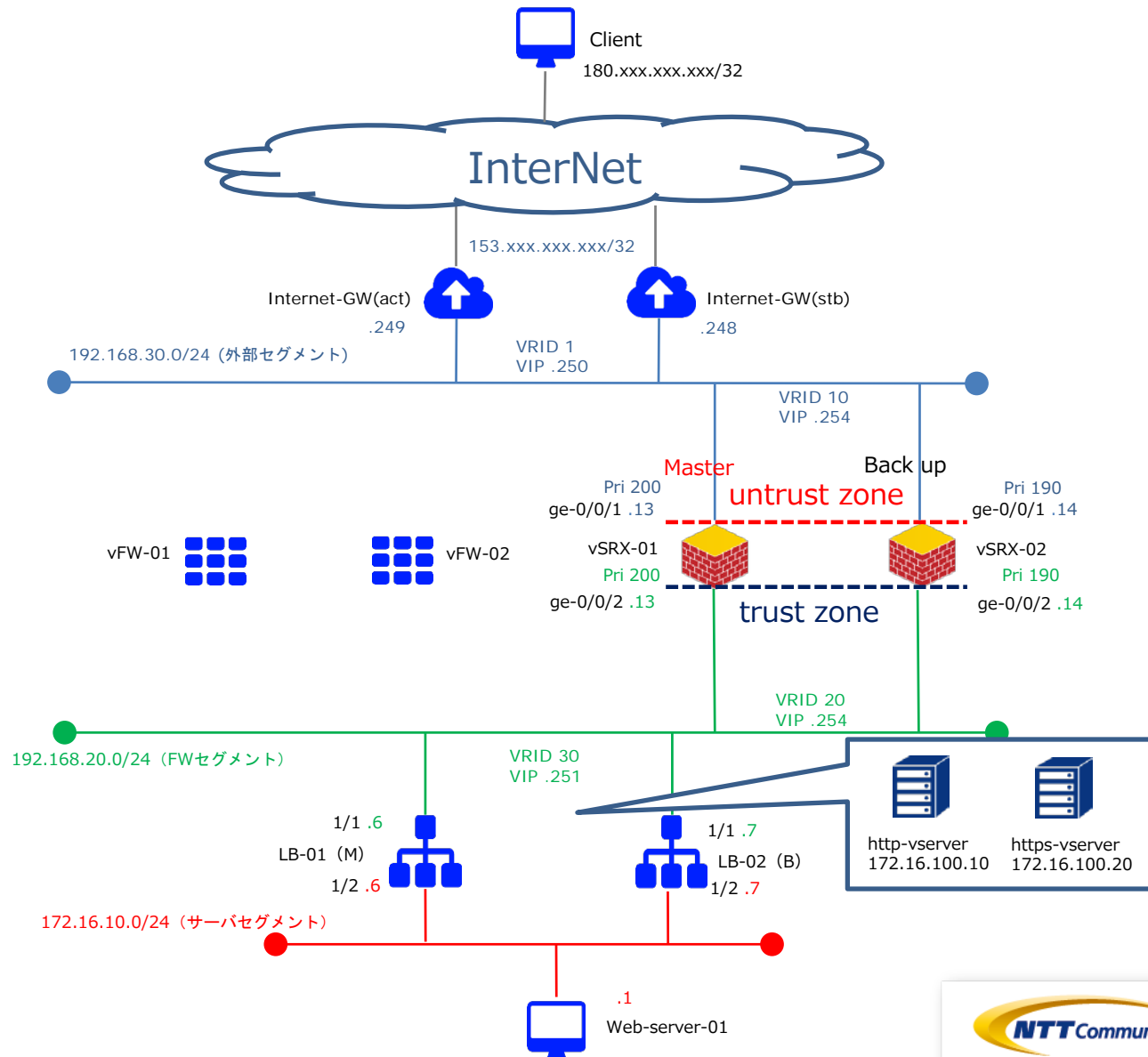


手順⑤ vSRX設定 (**VRRP切替わりが発生**)  
 1. VRRP設定 (vSRX2台のプライオリティをvFWより高く設定)

# 移行時構成⑤



# 移行完了構成



# 手順①vSRX申し込み

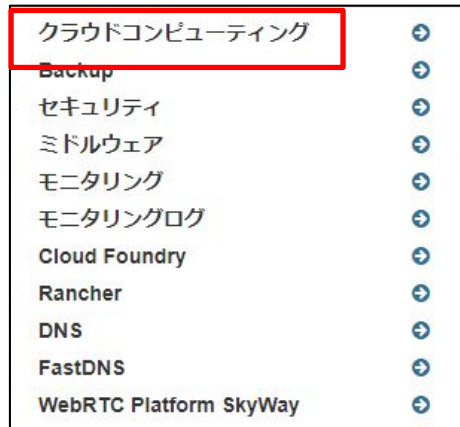
---

# 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。

× 取り消し    ファイアウォールの作成

### 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

× 取り消し    **ファイアウォールの作成**

# 手順① vSRX申込み

---

同様の手順でvSRX-02のお申込みをお願いいたします。

# 手順②-1 vSRX設定 (ファイアウォール設定)

---

## 手順②-1 vSRX設定 (ファイアウォール設定)

ファイアウォールフィルター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](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](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](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②-1 vSRX設定 (ファイアウォール設定)

---

同様の手順でvSRX-02のファイアウォール設定をお願いいたします。



# 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②-2 vSRX設定 (DNAT設定)

---

同様の手順でvSRX-02のDNAT設定をお願いいたします。

# 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 the instances with their names, configurations, and monitoring status. A dropdown menu is open for the selected instance, showing options for firewall management. 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-	vSRX_15.1X49-	zone1_groupb	モニタリングステータス:	完了	5b599e78-51f9-4187-8ef1-4473edc5b4e9	ファイアウォールの編集
<input type="checkbox"/> 01	D105.1_2CPU_4GB_8IF_STD		ログインステータス: ACTIVE			
			仮想サーバステータス: ACTIVE			

- 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  
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。

Internet-seg:(192.168.30.0/24)

固定IPアドレス  
192.168.30.13

× 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  
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。

FW-seg:(192.168.20.0/24)

固定IPアドレス  
192.168.20.13

× 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](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 192.168.30.13/24
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 192.168.20.13/24
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③ vSRX設定 (インターフェース設定)

---

同様の手順でvSRX-02のインターフェース設定をお願いいたします。

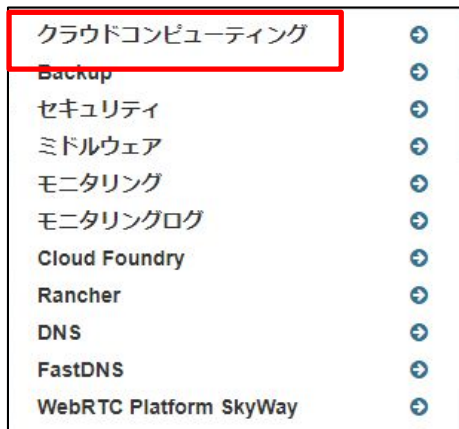
# 手順④ vSRX設定 (VRRP設定)

---

## 手順④ vSRX設定 (VRRP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VRRP設定をお願いいたします。  
<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/network/vrrp.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 (VRRP設定)

対象のvSRXの「許可されたアドレスペアの編集」をクリックしてください。

The screenshot displays a configuration page for vSRX instances. A table lists the instances with their respective details. A context menu is open for the selected instance, highlighting the option to edit allowed address pairs.

vSRX ID	Configuration	Zone	Monitoring Status	Login Status	Completion	IP Address	Actions
<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イスの編集 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

Communications All Rights Reserved.

## 手順④ vSRX設定 (VRRP設定)

編集したいインターフェイスタブを開き、「アドレスペアの追加」をクリックして下さい。  
外部セグメントとFWセグメントのインターフェースでアドレスペアの設定をお願いいたします。  
設定値を入力後、「許可されたアドレスペアの更新」をクリックして下さい。

参考までに、以下はvSRX-01の設定値となります。

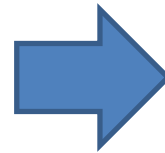
許可されたアドレスペアの更新

インターフェイス1 インターフェイス2 インターフェイス3 インターフェイス4  
インターフェイス5 インターフェイス6 インターフェイス7 インターフェイス8

+ アドレスペアの追加

ファイアウォールの許可されたアドレスペアを更新します。

× 取り消し 許可されたアドレスペアの更新



許可されたアドレスペアの更新

インターフェイス1 インターフェイス2 インターフェイス3 インターフェイス4  
インターフェイス5 インターフェイス6 インターフェイス7 インターフェイス8

アドレスペア1

IPアドレス\*  
192.168.30.254

種別  
VRRP

MACアドレス

VRID  
10

+ アドレスペアの追加

ファイアウォールの許可されたアドレスペアを更新します。

× 取り消し 許可されたアドレスペアの更新

## 手順④ vSRX設定 (VRRP設定)

下記リンクを参照の上、CLIでvSRXのVRRP設定をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/network/vrrp.html#vrrp-vrrp>

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。

対象である全てのインターフェースに対してVRRP設定を行った後、commitを入力してください。  
VRRPプライオリティはvFWより低い値を設定いたします。

VRRP advertise-intervalは、**vFWのadvertise-intervalの値と揃えて下さい。**

下記のように、VRRPグループIDはvFWと合わせて下さい。

### 【vFW設定】

```
set interfaces dataplane dp0s4 vrrp vrrp-group 10  
set interfaces dataplane dp0s7 vrrp vrrp-group 20
```

### 【vSRX設定】

```
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.13/24 vrrp-group 10  
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.13/24 vrrp-group 20
```



## 手順④ vSRX設定 (VRRP設定)

参考までに、vSRX-01の設定値を下記に記載します。

```
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.13/24 vrrp-group 10 virtual-address 192.168.30.254
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.13/24 vrrp-group 10 priority 60
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.13/24 vrrp-group 10 preempt
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.13/24 vrrp-group 10 accept-data
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.13/24 vrrp-group 10 advertise-interval [任意の値]
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.13/24 vrrp-group 20 virtual-address 192.168.20.254
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.13/24 vrrp-group 20 priority 60
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.13/24 vrrp-group 20 preempt
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.13/24 vrrp-group 20 accept-data
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.13/24 vrrp-group 20 advertise-interval [任意の値]
user@vSRX-01# commit
```

## 手順④ vSRX設定 (VRRP設定)

VRRP機能を利用するためには、ゾーンベースファイアウォール設定でVRRPを設定したゾーンもしくはインターフェイスで、VRRPパケットを許可しておく必要があります。

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。  
VRRP設定をしている全てのインターフェイスに対して、ゾーン設定を行います。

参考までに、vSRX-01の設定値を下記に記載します。

```
user@vSRX-01# set security zones security-zone untrust interfaces ge-0/0/1 host-inbound-traffic protocols vrrp
user@vSRX-01# set security zones security-zone trust interfaces ge-0/0/2 host-inbound-traffic protocols vrrp
user@vSRX-01# commit
```

## 手順④ vSRX設定 (VRRP設定)

下記リンクを参照の上、CLIでvSRXのVRRP設定をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/network/vrrp.html#vrrp-vrrp>

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。

下記コマンドで、vFW-01が「master」、vSRX-01が「backup」状態になっていることが確認してください。

VRRP設定をしている全てのインターフェースでVRRP状態が「backup」になっていることを確認してください。

本検証では、vFW-01のIPアドレスは 192.168.30.11、192.168.20.11 です。

【show vrrp】

```
user@vSRX-01> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	10	backup	Active	D 3.588	lcl	192.168.30.13
					vip		192.168.30.254
					mas		192.168.30.11
ge-0/0/2.0	up	20	backup	Active	D 3.587	lcl	192.168.20.13
					vip		192.168.20.254
					mas		192.168.20.11

## 手順④ vSRX設定 (VRRP設定)

---

同様の手順でvSRX-02のVRRP設定をお願いいたします。

# 手順⑤ vSRX設定変更 (VRRPプライオリティ切替)

---

## 手順⑤ vSRX設定変更 (VRRPプライオリティ切替)

下記リンクを参照の上、vSRXのVRRP設定変更をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/vSRX/network/vrrp.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。

vSRX-01をVRRPのマスタールーターに設定いたします。  
お客様環境に合わせてVRRPプライオリティ値の変更をお願いいたします。

参考までに、vSRX-01の設定値を次のページに記載致します。

## 手順⑤ vSRX設定変更 (VRRPプライオリティ切替)

vSRX-01ではVRRPプライオリティを「60」から「200」に変更致します。

**非対称ルーティングを防ぐため**、VRRP設定をしている全てのインターフェースで同時にVRRPプライオリティ変更をお願い致します。

```
user@vSRX-01# set interfaces ge-0/0/1 unit 0 family inet address 192.168.30.13/24 vrrp-group 10 priority 200
user@vSRX-01# set interfaces ge-0/0/2 unit 0 family inet address 192.168.20.13/24 vrrp-group 20 priority 200
user@vSRX-01# commit
```

下記コマンドで、**vSRX01が「master」状態**になっていることが確認できます。

VRRP設定をしている全てのインターフェースでVRRP状態が「master」になっていることを確認してください。

【show vrrp】

```
user@vSRX-01> show vrrp
```

Interface	State	Group	VR state	VR Mode	Timer	Type	Address
ge-0/0/1.0	up	10	master	Active	A 0.489	lcl	192.168.30.13 vip 192.168.30.254
ge-0/0/2.0	up	20	master	Active	A 0.684	lcl	192.168.20.13 vip 192.168.20.254

## 手順⑤ vSRX設定変更 (VRRPプライオリティ切替)

同様の手順でvSRX-02のVRRP設定をお願いいたします。

vSRXのプライオリティ変更による移行後、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の設定変更 (インターフェースの切断)

---

## 手順⑥ vFWの設定変更 (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 the management interface for a Brocade 5600 vRouter. On the left is a navigation menu with categories: 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, マネージドファイアウォール, and ロードバランサー. The 'ファイアウォール' (Firewall) category is selected, and 'Brocade 5600 vRouter' is highlighted with a red box. The main content area is titled 'ファイアウォール' and displays a table of firewall instances:

<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 indicates '3 件表示' (3 items displayed).

# 手順⑥ vFWの設定変更 (インターフェースの切断)

対象のインターフェースから、「VRRP用通信設定の解除」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	192.168.30.254	-	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-da13-44b7-9358-2cfb335afe02	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	192.168.20.254	-	稼働中	ファイアウォールインターフェイスの編集 ▼

「VRRP用通信設定の解除」をクリック。

### VRRP用通信設定の解除

仮想IPアドレス  
192.168.30.254

VRID  
10

**説明:**  
本設定により、VRRP用通信設定を解除します。  
本設定は、VRRPを構成するそれぞれのファイアウォールに対して必要となります。  
本設定に加え、ファイアウォールのCLI/API/GUIにてVRRP設定を解除する必要があります。

取り消し **VRRP用通信設定の解除**

# 手順⑥ vFWの設定変更 (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 <b>ロジカルネットワークの切断</b> VRRP用通信設定の登録 VRRP用通信設定の解除
dp0s5	-	2	07295beb-da13-44b7-9358-2cfb335afe02	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。

## 手順⑥ vFWの設定変更 (インターフェースの切断)

---

同様の手順でvFW-02の外部セグメントとFWセグメントのインターフェースの切断をお願いいたします。