

ファイアウォール(Brocade 5600 vRouter)とManaged Firewallから vSRXへの交換によるマイグレ実施方法 (シングル構成版)

第1版

更新履歴

更新日	更新内容	版数
2018/11/26	初版	1

前提条件

前提条件

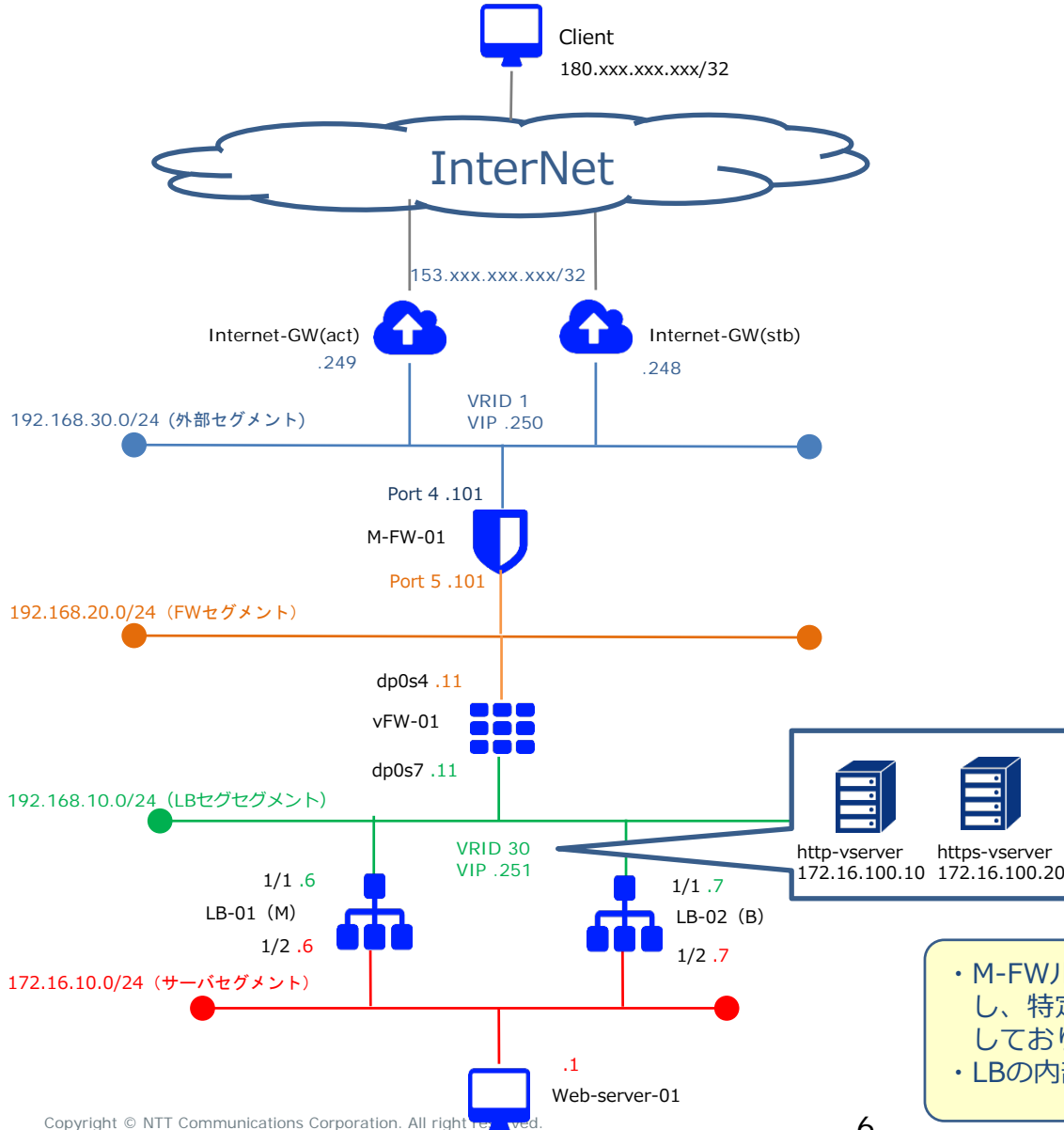
■ Managed Firewall(以下、M-FW)とファイアウォール(Brocade 5600 vRouter)(以下、vFW)からファイアウォール(vSRX)への交換によるマイグレ実施方法です。

- 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。
- M-FW、vFWで利用しているネットワークをvSRXへ接続します。
⇒ M-FW、vFWで利用しているネットワークの接続解除から、vSRXへの付け替え時、通信断の時間が発生いたします。
- 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。
- 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。
- 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。

※事前検証を行ってから移行を実施ください。

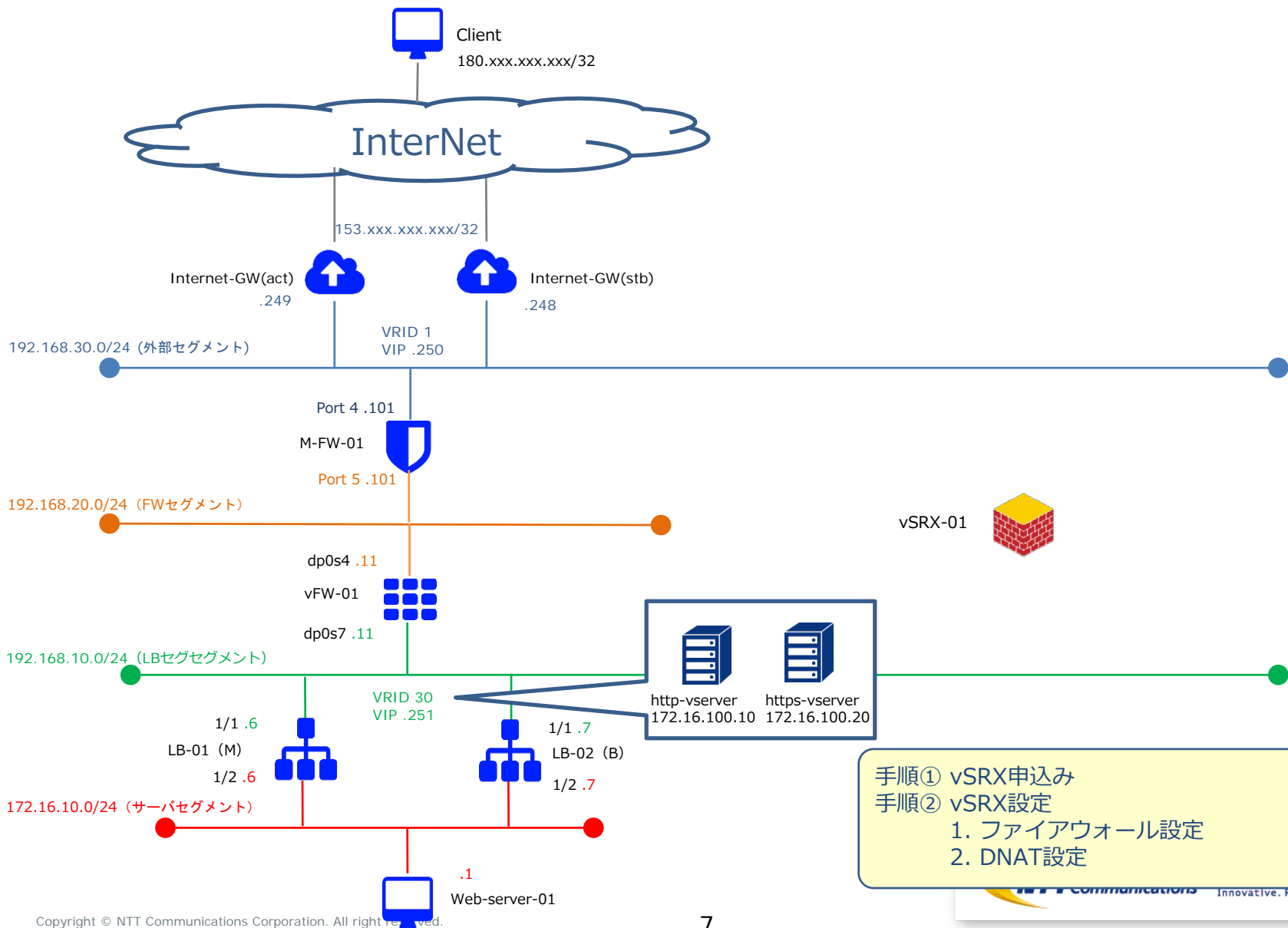
構成および移行フロー

移行前構成 (M-FW, vFW構成)



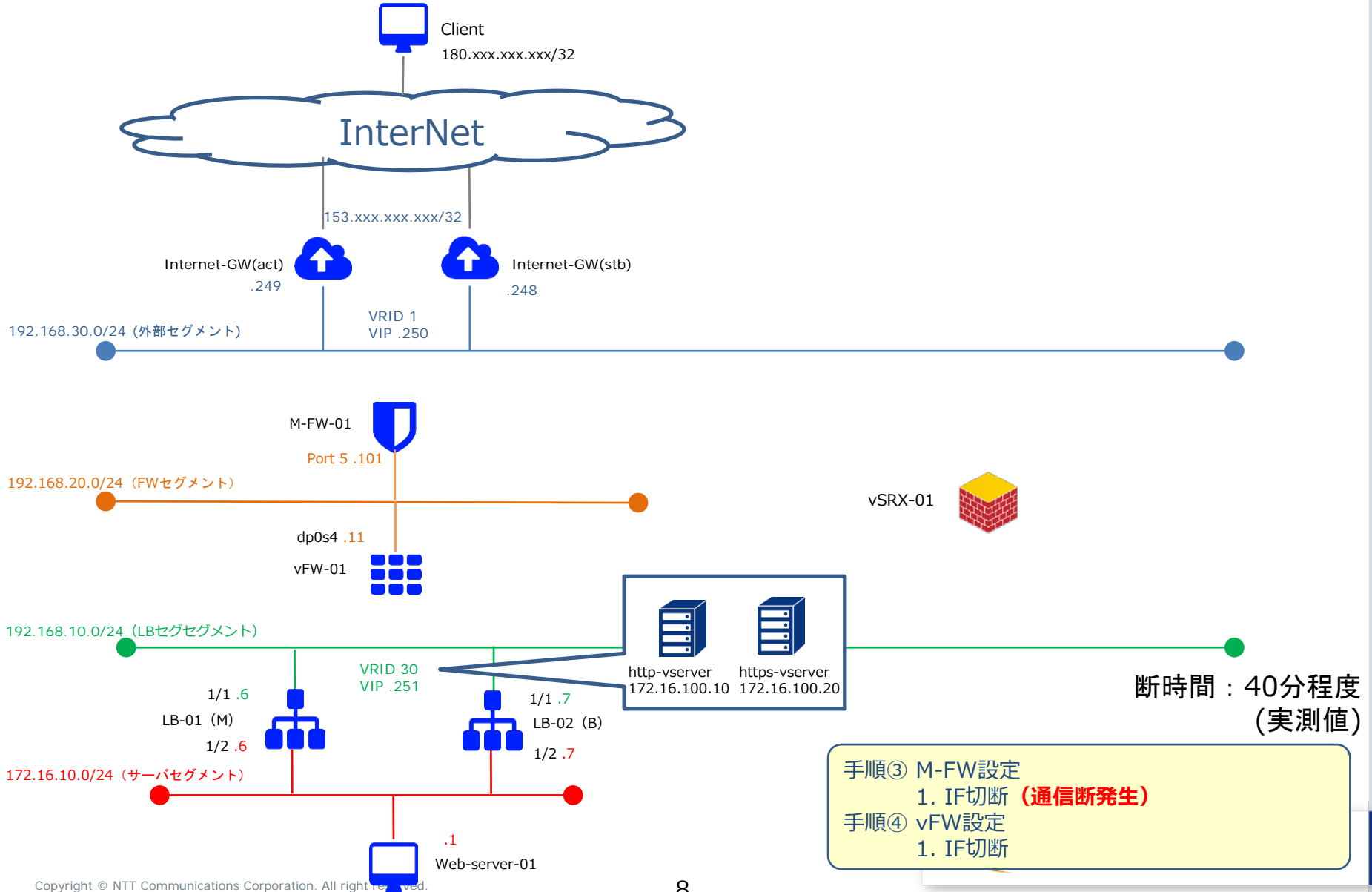
- M-FWルールは外部セグメントからの通信は全て拒否し、特定の送信元からのHTTP/HTTPS通信のみ許可しております。
- LBの内部にバーチャルサーバーを設定しておきます。

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

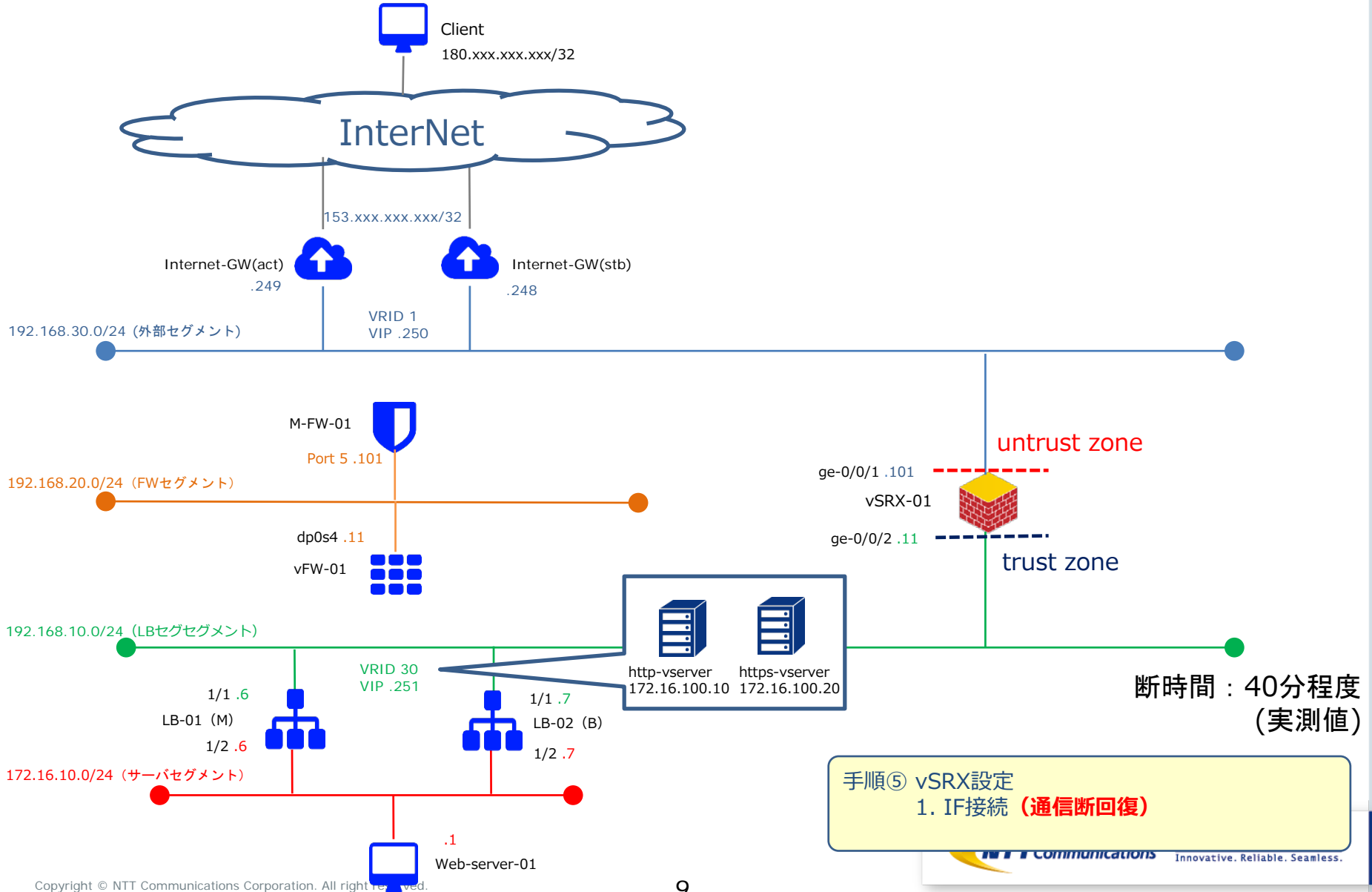
移行時構成②



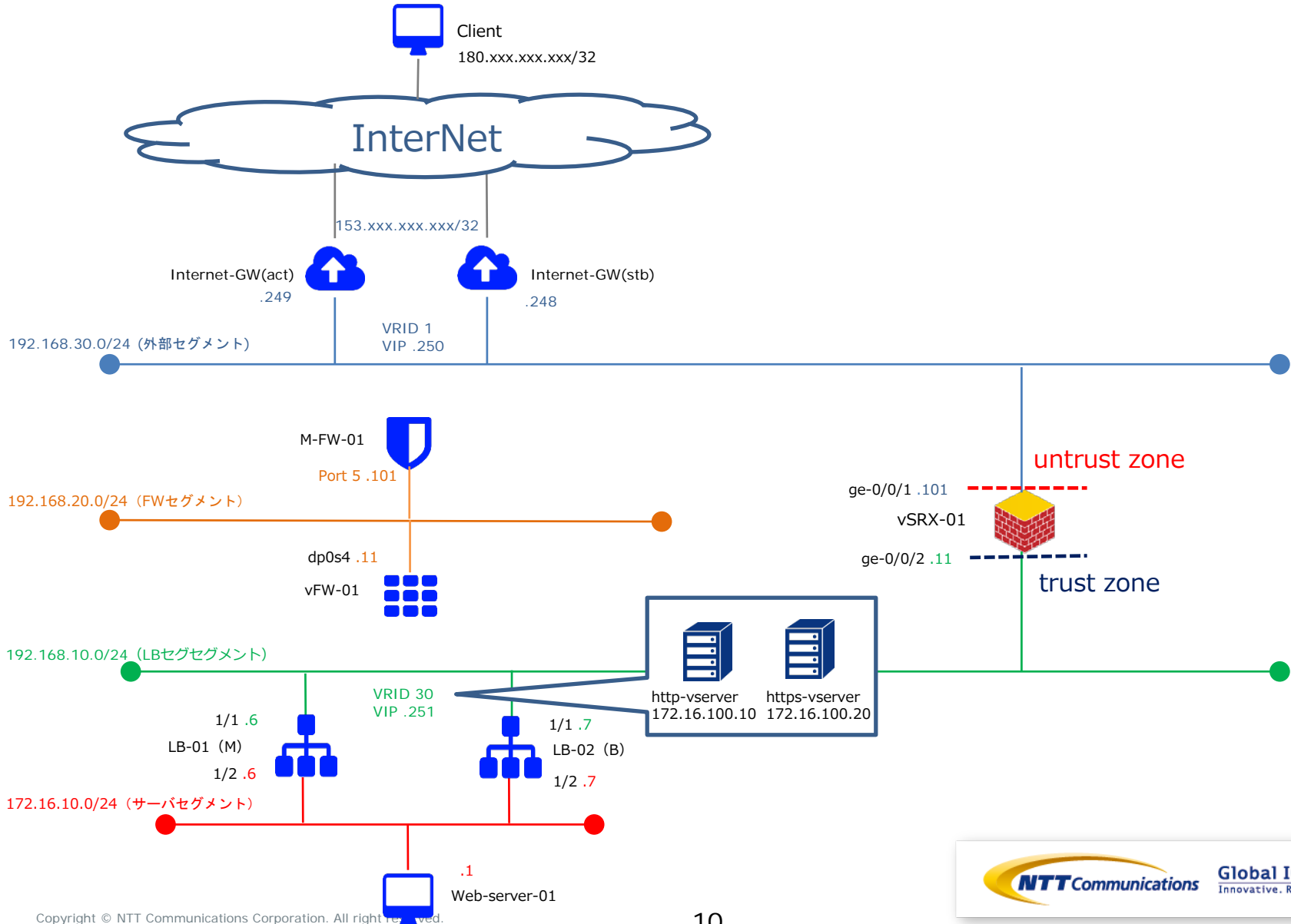
断時間：40分程度
(実測値)

- 手順③ M-FW設定
1. IF切断 (通信断発生)
- 手順④ vFW設定
1. IF切断

移行時構成③



移行完了構成



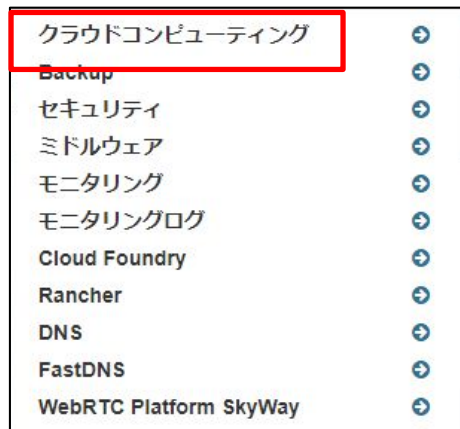
手順① vSRX申し込み

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

ソーン/グループ

ソーン/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

× 取り消し

ファイアウォールの作成

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

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 M-FWの設定変更 (インターフェースの切断)

手順③ M-FWの設定 (インターフェースの切断)

M-FWのインターフェースの設定が可能です。

https://ecl.ntt.com/documents/tutorials/security/rsts/security/operation/managed_firewall_utm/3110_interface_single.html

コントロールパネル画面にログイン後、
セキュリティをクリックし、Managed FirewallのOperationをクリックください。

- クラウドコンピューティング
- Backup
- セキュリティ
- ミドルウェア
- モニタリング
- Cloud Foundry
- DNS
- HC with Microsoft Azure



Security Menu

Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
Host-based Security	Managed Anti-Virus	Order	Operation
	Managed Virtual Patch		
	Managed Host-based Security Package		

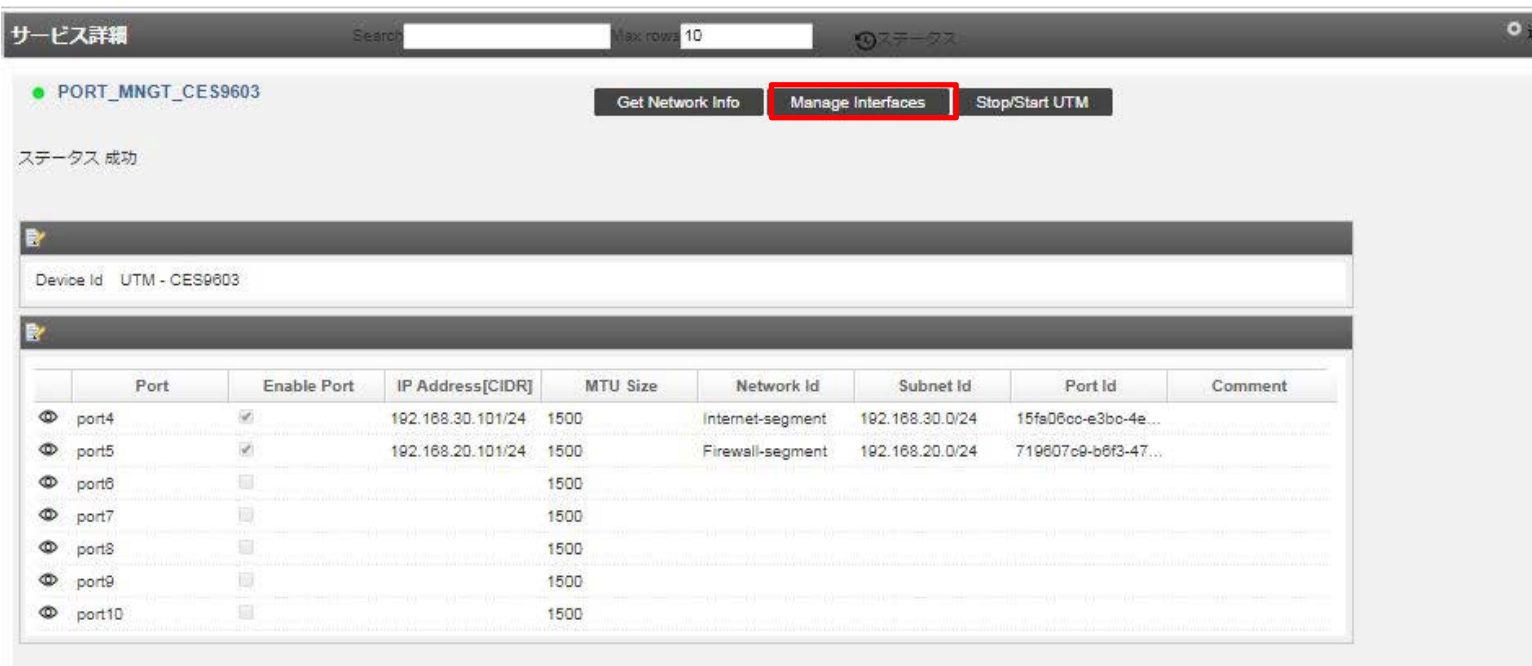
手順③ M-FWの設定 (インターフェースの切断)

[UTM Port Management] をクリックしてください。



手順③ M-FWの設定 (インターフェースの切断)

設定対象のM-FWをクリックで選択し、[Manage Interfaces] をクリックします。
どのポート番号でクリックしても同じ画面が開きます。

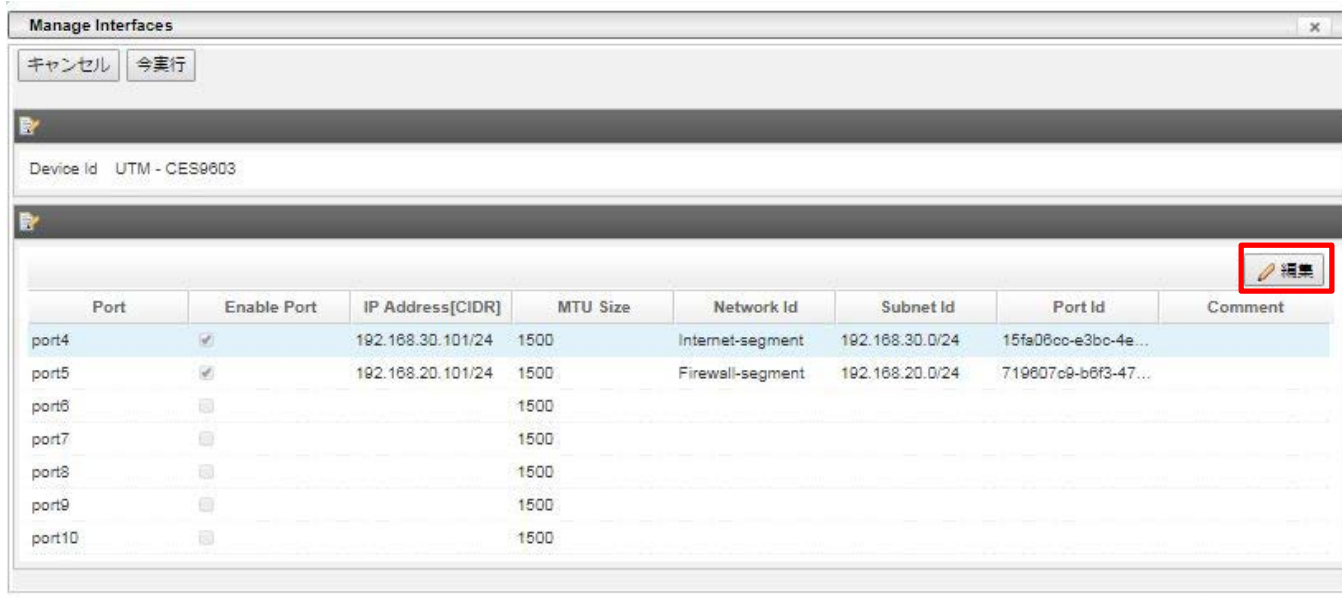


The screenshot shows a web interface for managing network services. At the top, there is a search bar and a 'max rows' dropdown set to 10. Below this, the service name 'PORT_MNGT_CES9603' is displayed. Three buttons are visible: 'Get Network Info', 'Manage Interfaces' (highlighted with a red box), and 'Stop/Start UTM'. The status is 'ステータス 成功'. Below the buttons, the device ID is 'UTM - CES9603'. A table lists the network interfaces with columns for Port, Enable Port, IP Address, MTU Size, Network Id, Subnet Id, Port Id, and Comment.

Port	Enable Port	IP Address[CIDR]	MTU Size	Network Id	Subnet Id	Port Id	Comment
port4	<input checked="" type="checkbox"/>	192.168.30.101/24	1500	Internet-segment	192.168.30.0/24	15fa06cc-e3bc-4e...	
port5	<input checked="" type="checkbox"/>	192.168.20.101/24	1500	Firewall-segment	192.168.20.0/24	719607c9-b6f3-47...	
port6	<input type="checkbox"/>		1500				
port7	<input type="checkbox"/>		1500				
port8	<input type="checkbox"/>		1500				
port9	<input type="checkbox"/>		1500				
port10	<input type="checkbox"/>		1500				

手順③ M-FWの設定 (インターフェースの切断)

[Manage Interfaces] の画面が開きます。Port 2,3は [Manage Interfaces] の画面には表示されません。設定対象のポートをクリックで選択して、[編集] をクリックします。



The screenshot shows the 'Manage Interfaces' window for device 'UTM - CES9603'. It contains a table with the following data:

Port	Enable Port	IP Address[CIDR]	MTU Size	Network Id	Subnet Id	Port Id	Comment
port4	<input checked="" type="checkbox"/>	192.168.30.101/24	1500	Internet-segment	192.168.30.0/24	15fa06cc-e3bc-4e...	
port5	<input checked="" type="checkbox"/>	192.168.20.101/24	1500	Firewall-segment	192.168.20.0/24	719607c9-b6f3-47...	
port6	<input type="checkbox"/>		1500				
port7	<input type="checkbox"/>		1500				
port8	<input type="checkbox"/>		1500				
port9	<input type="checkbox"/>		1500				
port10	<input type="checkbox"/>		1500				

The 'Edit' button (represented by a pencil icon) is highlighted with a red box in the top right corner of the table area.

手順③ M-FWの設定 (インターフェースの切断)

[Enable Port] のチェックを外してください。

[保存] をクリックします。この画面で保存しただけではデバイスに適用されません。



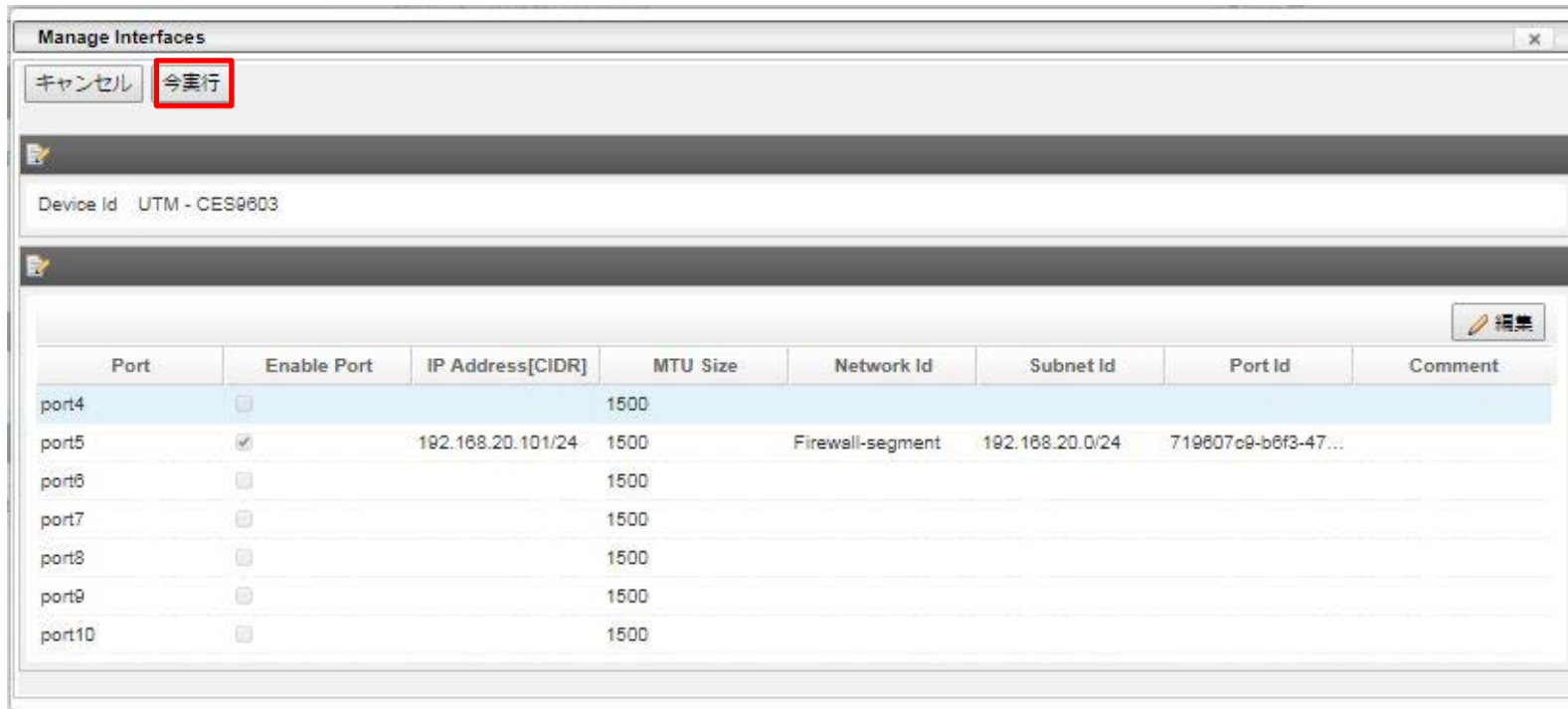
The screenshot shows a configuration window for an M-FW interface. At the top left, there are two buttons: 'キャンセル' (Cancel) and '保存' (Save), with '保存' highlighted by a red box. Below the buttons, the interface displays the following fields:

- Port: port4
- Enable Port: (unchecked, highlighted by a red box)
- MTU Size: 1500
- Comment: (empty text box)

手順③ M-FWの設定 (インターフェースの切断)

Manage Interfaces画面で [今実行] をクリックします。

通信断が発生します。

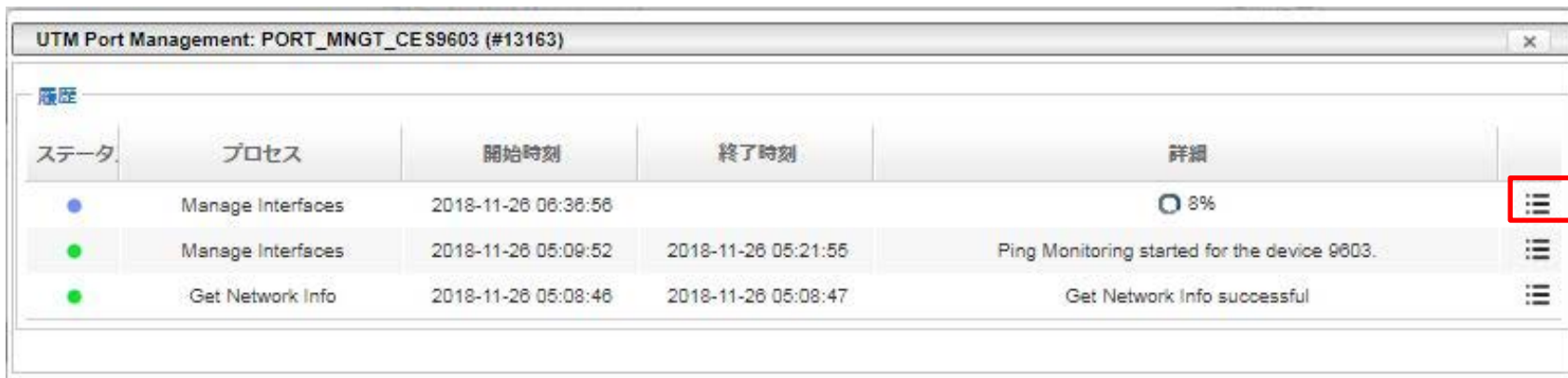


The screenshot shows the 'Manage Interfaces' window for device 'UTM - CES9603'. At the top, there are two buttons: 'キャンセル' and '今実行', with '今実行' highlighted by a red box. Below the buttons, the device ID is displayed as 'UTM - CES9603'. A table lists the network interfaces with columns for Port, Enable Port, IP Address[CIDR], MTU Size, Network Id, Subnet Id, Port Id, and Comment. The 'port5' row is highlighted in blue, indicating it is selected.

Port	Enable Port	IP Address[CIDR]	MTU Size	Network Id	Subnet Id	Port Id	Comment
port4	<input type="checkbox"/>		1500				
port5	<input checked="" type="checkbox"/>	192.168.20.101/24	1500	Firewall-segment	192.168.20.0/24	719607c9-b6f3-47...	
port6	<input type="checkbox"/>		1500				
port7	<input type="checkbox"/>		1500				
port8	<input type="checkbox"/>		1500				
port9	<input type="checkbox"/>		1500				
port10	<input type="checkbox"/>		1500				

手順③ M-FWの設定 (インターフェースの切断)

[ステータス] や [メッセージ] が表示されている領域をクリックすると、履歴が表示され [Manage Interfaces] プロセスの開始時刻、進捗が表示されます。



ステータス	プロセス	開始時刻	終了時刻	詳細	
●	Manage Interfaces	2018-11-28 06:36:56		○ 8%	☰
●	Manage Interfaces	2018-11-28 05:09:52	2018-11-28 05:21:55	Ping Monitoring started for the device 9603.	☰
●	Get Network Info	2018-11-28 05:08:46	2018-11-28 05:08:47	Get Network Info successful	☰

手順③ M-FWの設定 (インターフェースの切断)

すべてのステータスが「緑色」になれば正常終了になります。

ステータス	開始時刻	終了時刻	詳細
Set Context for First UTM	2018-11-01 07:03:52	2018-11-01 07:03:53	Context set for the First Unit : OPENSTACK SETUP : jp2_zone1-groupd
↓			
Verify IP Address Inputs	2018-11-01 07:03:53	2018-11-01 07:03:58	IP Address inputs verified successfully.
↓			
Verify VRRP, MTU Inputs	2018-11-01 07:03:58	2018-11-01 07:03:59	VRRP and MTU inputs verified successfully.
↓			
Import Ports	2018-11-01 07:03:59	2018-11-01 07:04:02	Import Ports successful
↓			
Stop Ping Monitoring	2018-11-01 07:04:02	2018-11-01 07:07:07	Ping Monitoring stopped for the HA devices.
↓			
Stop the UTM	2018-11-01 07:07:07	2018-11-01 07:07:21	Openstack Server 8dd08056-5dda-4fa3- bc10-8633724a83d6 stopped successfully. Server Status : SHUTOFF Task State :- Power State : Shutdown
↓			
Wait for UTM Ping unreachability from MSA	2018-11-01 07:07:21	2018-11-01 07:07:31	IP Address 100.69.07.125 is now unreachable from MSA. PING Status : Destination Host Unreachable
↓			

手順④ vFWの設定変更 (インターフェースの切断)

手順④ 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。

<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

3 件表示

手順④ 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。



The screenshot shows the 'ファイアウォールインターフェイス' (Firewall Interface) configuration page. It contains a table with the following columns: 名前 (Name), 説明 (Description), スロット番号 (Slot Number), ロジカルネットワーク (Logical Network), IP アドレス (IP Address), 仮想IPアドレス (Virtual IP Address), Enterprise Cloud 2.0 接続 (Enterprise Cloud 2.0 Connection), ステータス (Status), and アクション (Action). The table lists four interfaces: dp0s4, dp0s5, dp0s6, and dp0s7. The 'アクション' column for each interface has a dropdown menu. The dropdown menu for dp0s4 is open, showing options: 'ロジカルネットワークの切断' (Disconnect Logical Network), 'VRRP用通信設定の登録' (Register VRRP Communication Settings), and 'VRRP用通信設定の解除' (Deregister VRRP Communication Settings). The 'ロジカルネットワークの切断' option is highlighted with a red box.

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	6916c6fe-7185-4bd5-8d27-d6cce58a7df4	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
dp0s5	-	2	53f003e5-3ccd-4b95-a46c-445a6756fc6b	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	5a826d1d-28f7-4549-a609-03a066d9e781	192.168.10.11	-	-	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。



The dialog box titled 'ロジカルネットワークの切断' (Disconnect Logical Network) contains the following information:

- ロジカルネットワーク*: LB-segment (192.168.10.0/24)
- IP アドレス: 192.168.10.11
- 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。

At the bottom, there are two buttons: '取り消し' (Cancel) and 'ロジカルネットワークの切断' (Disconnect Logical Network), with the latter highlighted by a red box.

手順⑤-1 vSRX設定 (インターフェース接続)

手順⑤-1 vSRX設定 (インターフェース接続)

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。

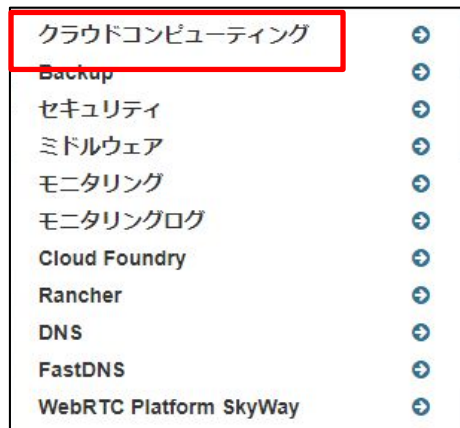
インターフェースのIPアドレスに着信する通信を許可するためにはhost-inbound-traffic配下で該当の通信を許可する設定が必要になります。

手順⑤-1 vSRX設定 (インターフェース接続)

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⑤-1 vSRX設定 (インターフェース接続)

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。

The screenshot displays a configuration page for vSRX instances. A table lists the instances, and a dropdown menu is open for the selected instance, showing various configuration options. The option 'ファイアウォールインターフェイスの編集' (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

NTT Communications All Rights Reserved.

手順⑤-1 vSRX設定 (インターフェース接続)

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*

192.168.30.101

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*

LB-segment:(192.168.10.0/24)

固定IPアドレス*

192.168.10.11

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⑤-1 vSRX設定 (インターフェース接続)

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 192.168.30.101/24
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 192.168.10.11/24
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
```

インターフェース接続設定が完了すると、**通信が回復します。**