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

第４版

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

更新履歴

更新日	更新内容	版数
2017/7/6	初版	1
2017/7/12	誤字修正/更新履歴追記/事前作業が可能な範囲を記載/M-FWのデフォルトゲートウェイ設定方法を記載/VRIDの制約を記載	2
2017/7/18	VPN-GW利用前提の構成へ変更/M-FW設定の説明追記	3
2017/8/1	vFWのインターフェース削除において、VRRP用通信設定の解除手順を追記。	4

前提条件

前提条件

■ファイアウォール(Brocade 5600 vRouter)(以下、vFW)からManaged Firewall(以下、M-FW)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。

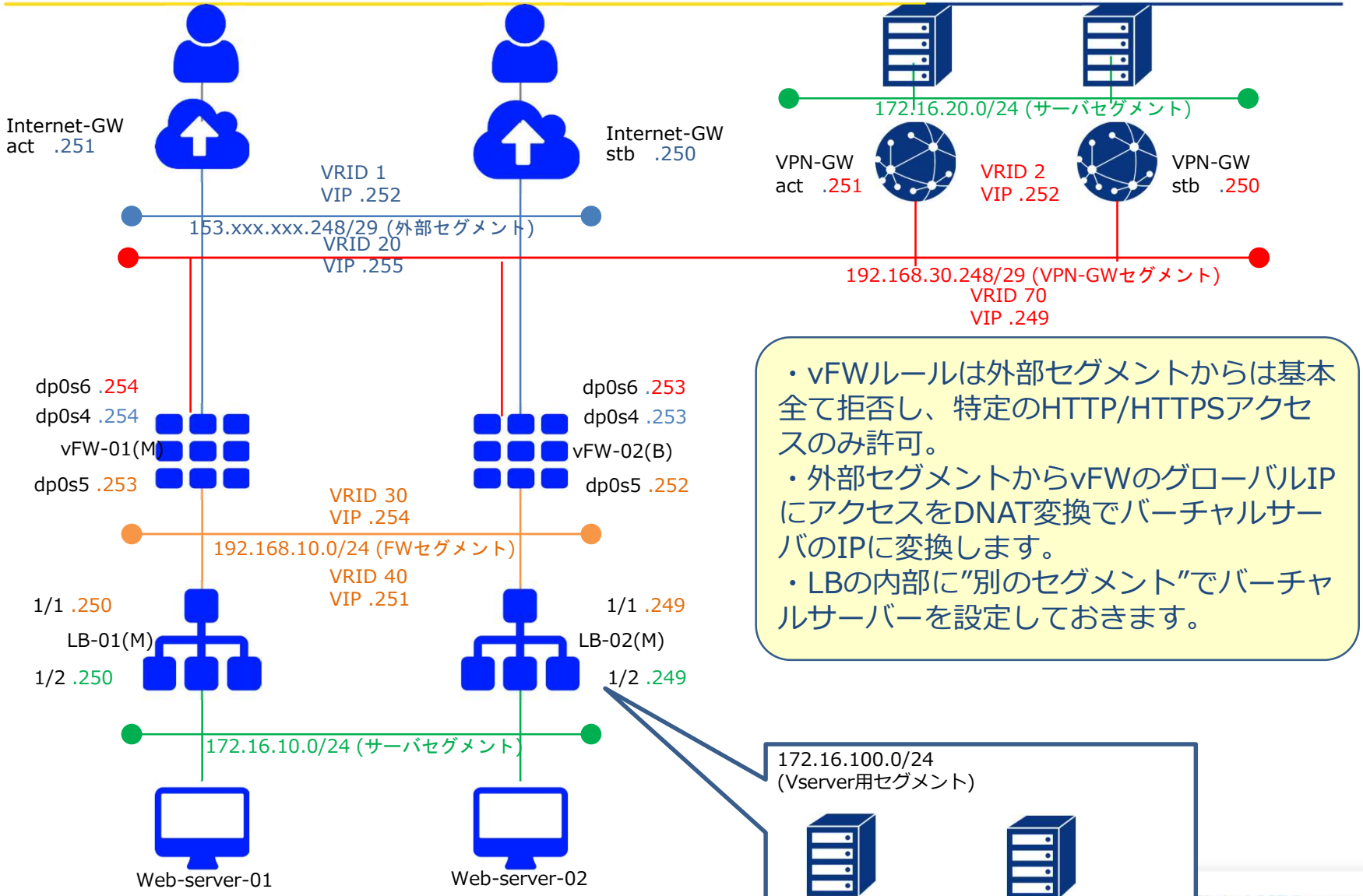
・ vFWで利用しているネットワークをM-FWへ付け替えます。

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

※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

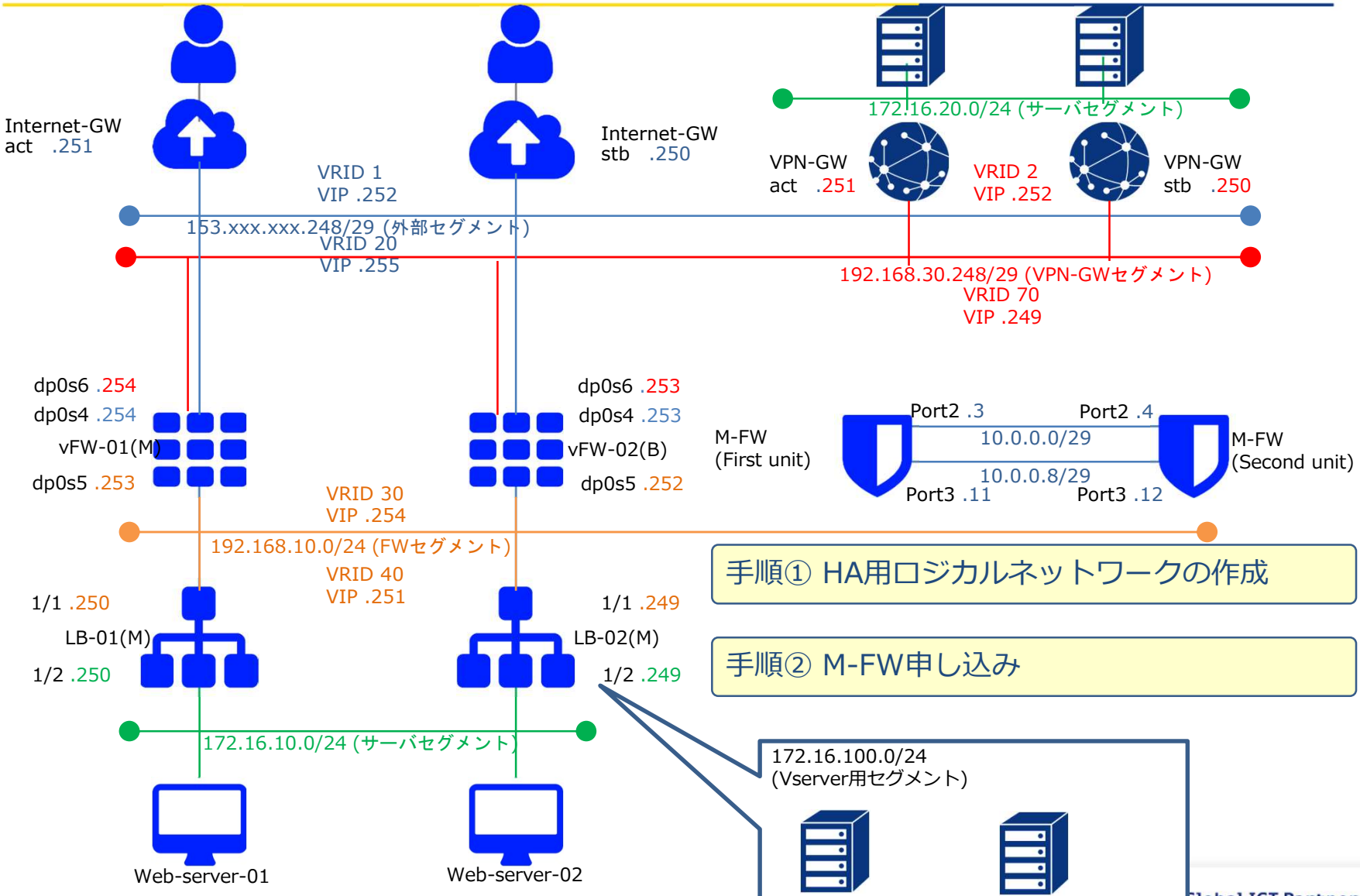
移行前構成（vFW構成）



・vFWルールは外部セグメントからは基本全て拒否し、特定のHTTP/HTTPSアクセスのみ許可。
・外部セグメントからvFWのグローバルIPにアクセスをDNAT変換でバーチャルサーバのIPに変換します。
・LBの内部に”別のセグメント”で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③まで事前作業が可能です。

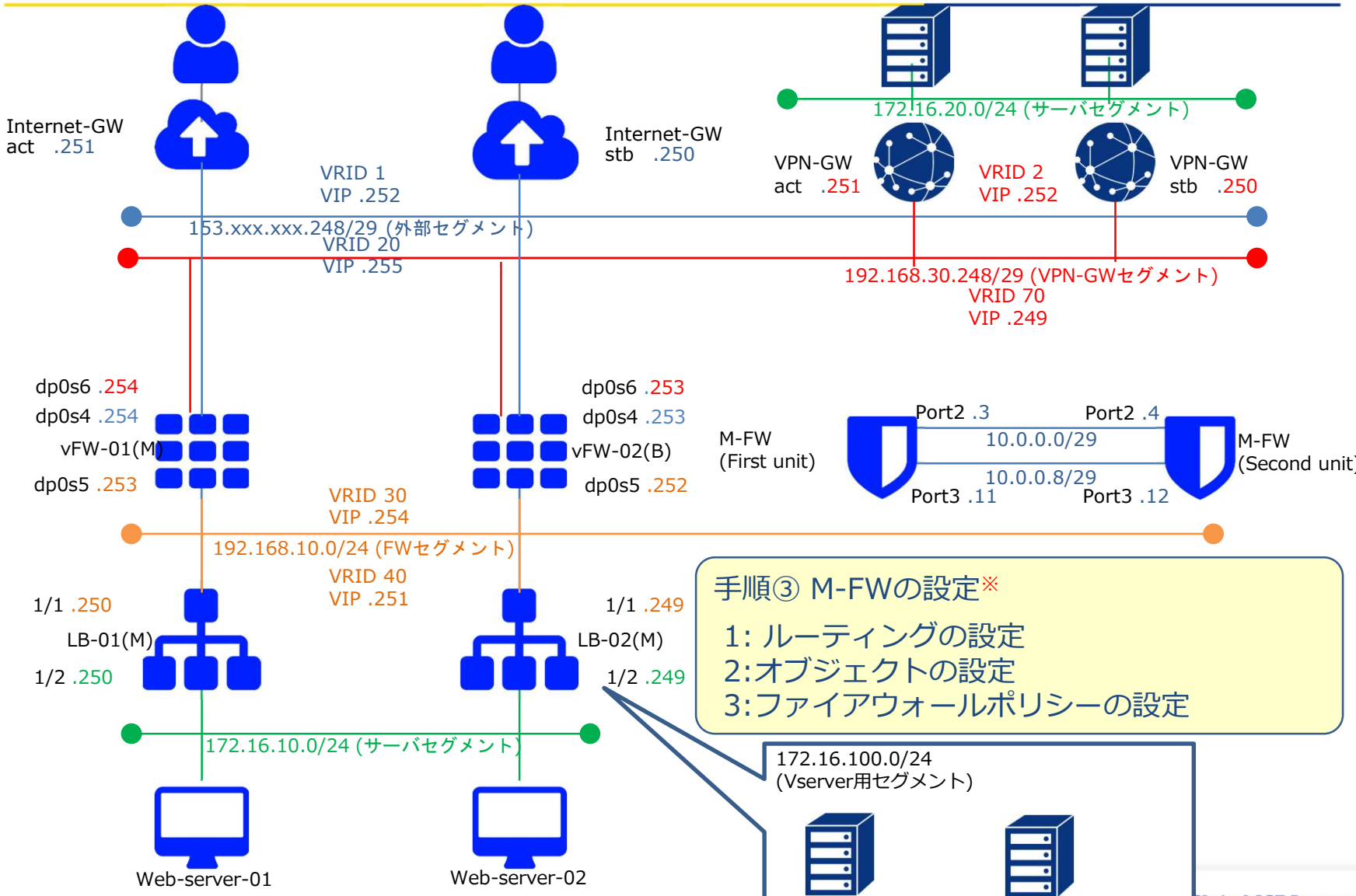


手順① HA用ロジカルネットワークの作成

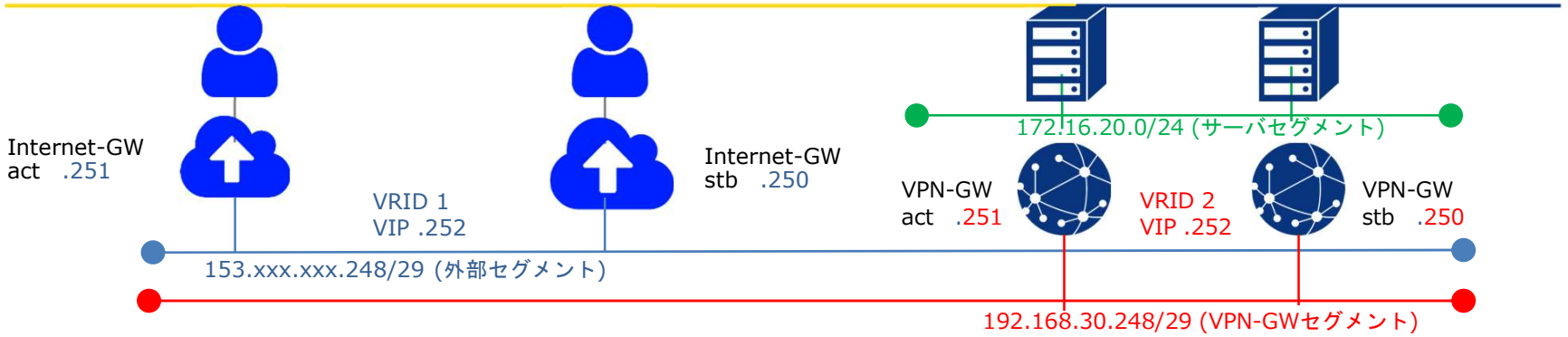
手順② M-FW申し込み

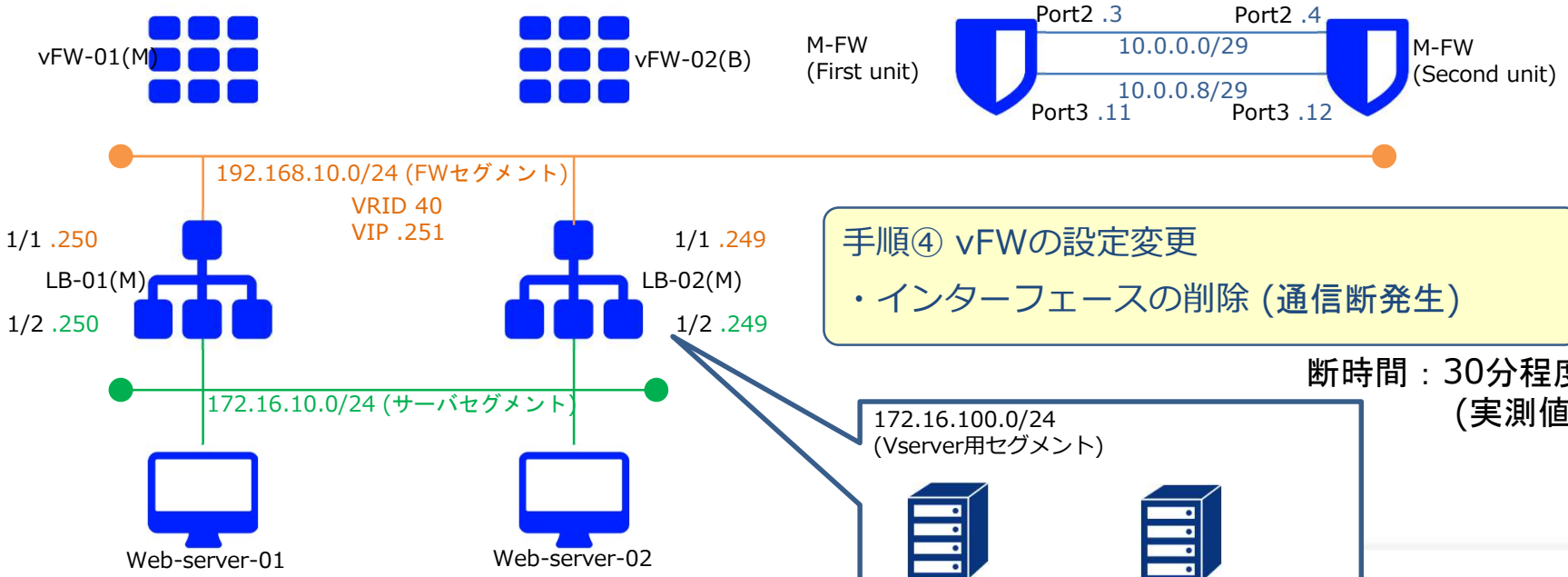
移行時構成②

※手順③まで事前作業が可能です。



移行時構成③



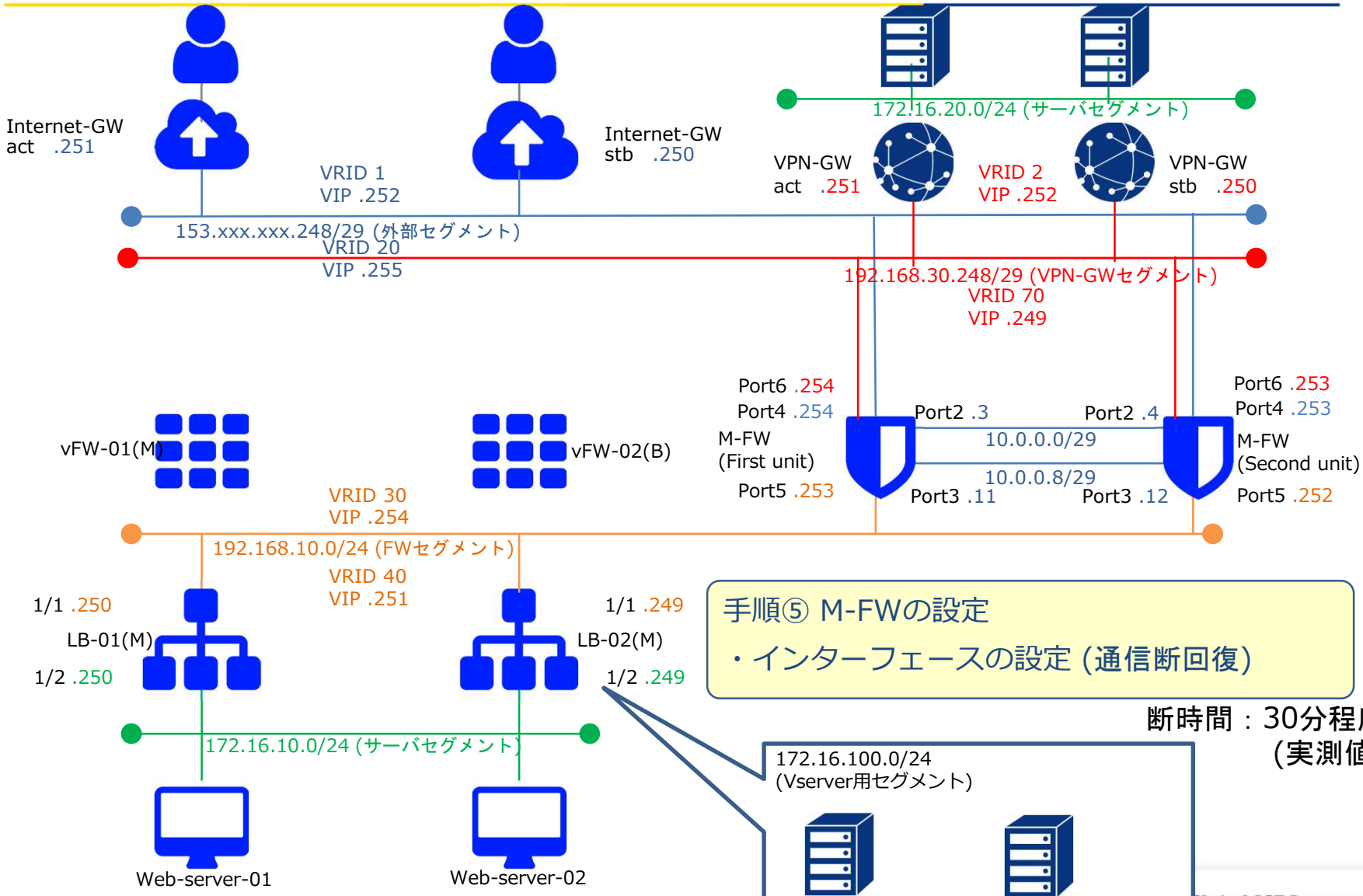


手順④ vFWの設定変更

・インターフェースの削除 (通信断発生)

断時間：30分程度
(実測値)

移行時構成④

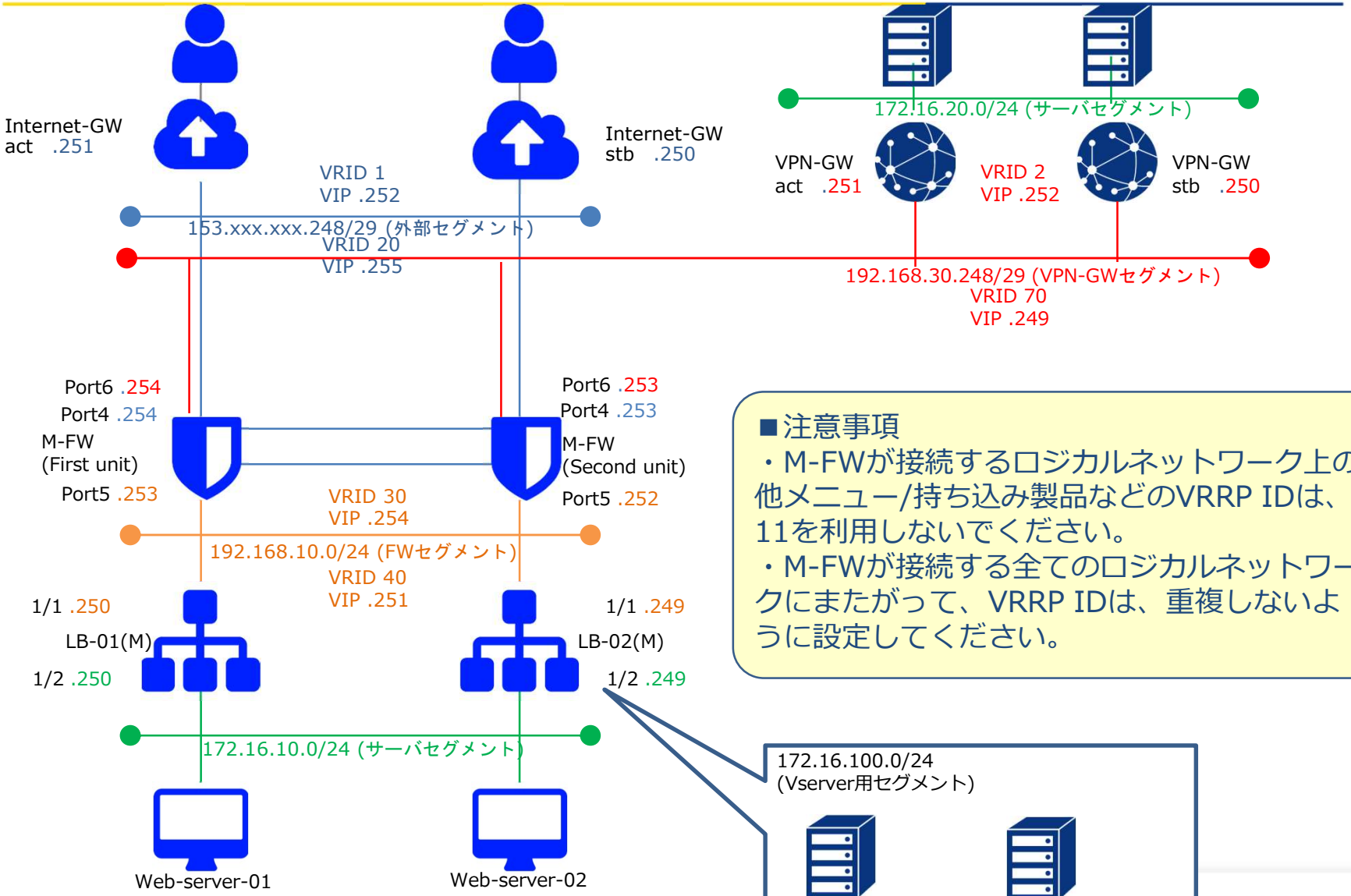


手順⑤ M-FWの設定

・インターフェースの設定 (通信断回復)

断時間：30分程度
(実測値)

移行完了構成（Managed Firewall構成）



■注意事項
・M-FWが接続するロジカルネットワーク上の他メニュー/持ち込み製品などのVRRP IDは、11を利用しないでください。
・M-FWが接続する全てのロジカルネットワークにまたがって、VRRP IDは、重複しないように設定してください。

手順① HA用ロジカルネットワークの作成

手順① HA用ロジカルネットワークの作成

下記リンクを参照の上、ロジカルネットワークのお申し込みをお願いいたします。
https://sdpf.ntt.com/services/docs/logical-network/tutorials/logicalnetwork.html

サービスメニューから「サーバーインスタンス」→クラウド/サーバー ローカルネットワークから「ロジカルネットワーク」をクリックください。

手順① HA用ロジカルネットワークの作成

1．ロジカルネットワークの作成ボタンを押下します。

手順① HA用ロジカルネットワークの作成

2-1. 1本目のロジカルネットワークを作成します。
- ・ロジカルネットワークタブから、必要項目を設定し、「次へ」を選択。
- ・サブネットタグから、必要項目を設定し、「次へ」を選択。
  (ネットワークアドレスに、10.0.0.0/29を、ゲートウェイなしにチェックを付けます。)
- ・サブネットの詳細タブから、必要項目を設定し、「ロジカルネットワークの作成」を選択。
  (DHCP有効にチェックを付けます。)

手順① HA用ロジカルネットワークの作成

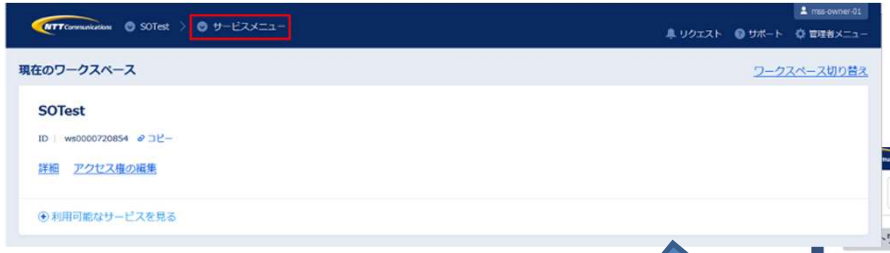
2-2. 2本目のロジカルネットワークを作成します。
- ・ロジカルネットワークタブから、必要項目を設定し、「次へ」を選択。
- ・サブネットタグから、必要項目を設定し、「次へ」を選択。
  (ネットワークアドレスに、10.0.0.8/29を、ゲートウェイなしにチェックを付けます。)
- ・サブネットの詳細タブから、必要項目を設定し、「ロジカルネットワークの作成」を選択。
  (DHCP有効にチェックを付けます。)

手順② M-FW申し込み

手順② M-FW申し込み

下記リンクを参照の上、HA構成のお申し込みをお願いいたします。
https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/order/managed_firewall_utm_v2/order_new_ha.html

SDPFポータルからアクセス
ワークスペースを選択後、Smart Data Platform ポータルのダッシュボード画面、またはダッシュボード⇒ワークスペース一覧画面の『サービスメニュー』をクリックします。



『ネットワーク』⇒『クラウド/サーバーネットワークセキュリティ』の
Managed Firewallをクリックします。

手順② M-FW申し込み

Managed Firewall(Version2)の「Order」をクリックしてください。

Security Menu

Network-based Security	Managed Firewall Managed UTM	Order
	Managed WAF	Order
	Managed Firewall(Version2) Managed UTM(Version2)	Order
	Managed WAF(Version2)	Order
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order

申込種別に「デバイス追加(HA)」を選択ください。

セキュリティ

申込種別 デバイス追加(HA)

お申し込みの際の入力値は下記になります。

Device Information

No	構成	メニュー	プラン	ゾーン/グループ	HA リンク1			HA リンク2		
					ネットワークID01	サブネットID01	IPアドレス01	ネットワークID02	サブネットID 02	IPアドレス02
1	High Availability	Managed Firewall	2CPU-4GB	zone1-groupa	6d777f11-951b-4b10-9899-58663a576594/HA-seg1	10.0.0.2 ～ 10.0.0.6	10.0.0.3	0d6af951-44c0-4f86-b551-6bb564469987/HA-seg2	10.0.0.10 ～ 10.0.0.14	10.0.0.11
2	High Availability	Managed Firewall	2CPU-4GB	zone1-groupb	6d777f11-951b-4b10-9899-58663a576594/HA-seg1	10.0.0.2 ～ 10.0.0.6	10.0.0.4	0d6af951-44c0-4f86-b551-6bb564469987/HA-seg2	10.0.0.10 ～ 10.0.0.14	10.0.0.12

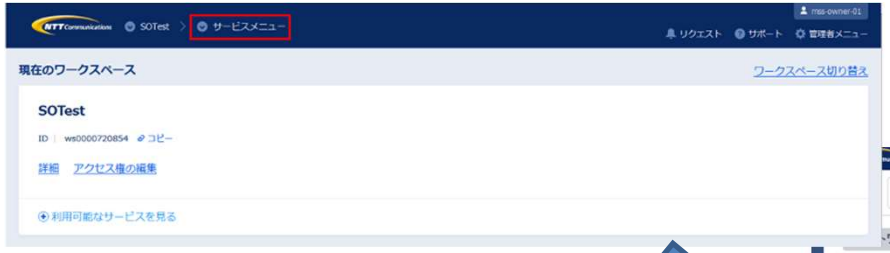
手順③ M-FWの設定

手順③-1 M-FWの設定
(ルーティングの設定)

手順③-1 M-FWの設定

ルーティングの設定は下記をご覧ください。
https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/operation/managed_firewall_utm_v2/4220_routing_ha.html

SDPFポータルからアクセス
ワークスペースを選択後、Smart Data Platform ポータルのダッシュボード画面、またはダッシュボード⇒ワークスペース一覧画面の『サービスメニュー』をクリックします。



『ネットワーク』⇒『クラウド/サーバーネットワークセキュリティ』の
Managed Firewallをクリックします。

手順③-1 M-FWの設定

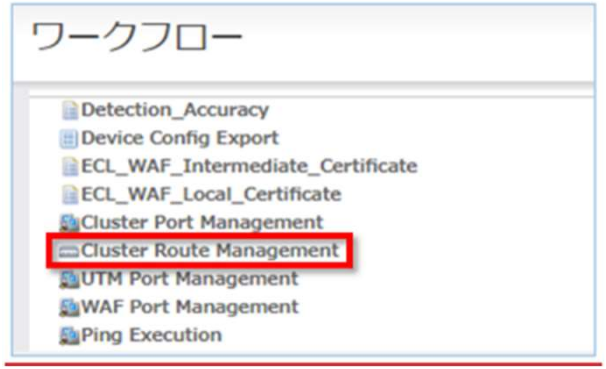
Managed Firewall(Version2)の「Operation」をクリックしてください。

Security Menu

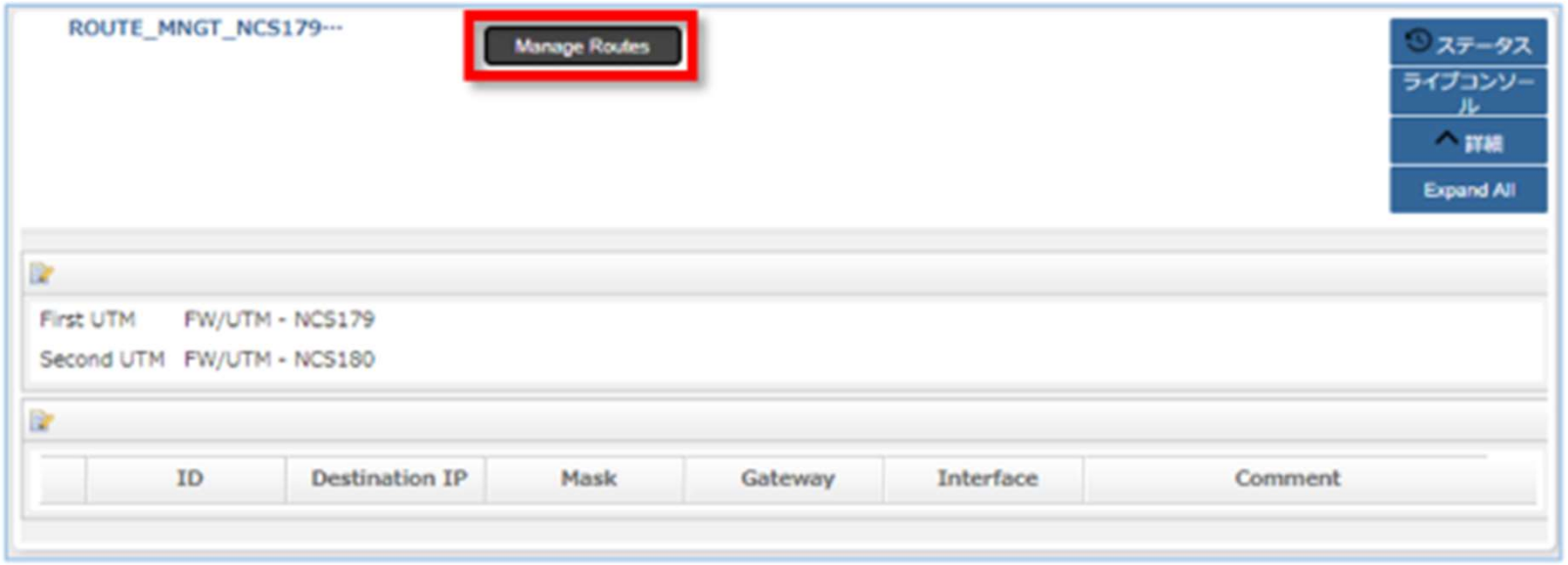
Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order	Operation

手順③-1 M-FWの設定

HA構成の場合、ルーティングは［ワークフロー］で設定します。
[サービス] - [ワークフロー] - ［Cluster Route Management］をクリックしてください。



［ネットワーク管理］に表示されている［Cluster Route Management］の［Manage Routes］をクリックします。



手順③-1 M-FWの設定

設定値を入力して、［保存］をクリックします
WebServer宛て通信の入力値は下記になります。

Internet GW(デフォルトゲートウェイ)宛て通信の入力値は、下記になります。

手順③-1 M-FWの設定

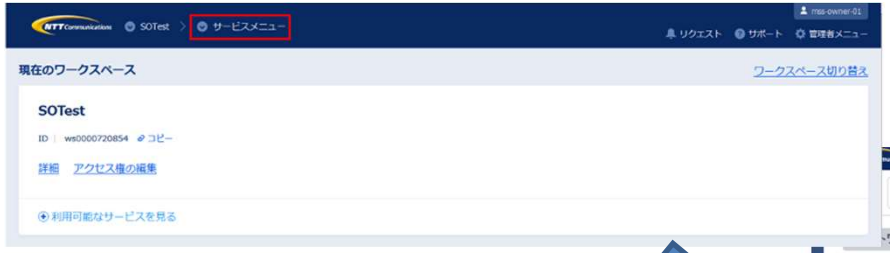
設定値を入力して、［保存］をクリックします
VPN-GW先サーバーセグメント宛て通信の入力値は下記になります。

手順③-2 M-FWの設定
(Destination NATの設定)

手順③-2 M-FWの設定

Destination NATの設定は下記をご覧ください。。
https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/operation/managed_firewall_utm_v2/4330_destination_nat.html

SDPFポータルからアクセス
ワークスペースを選択後、Smart Data Platform ポータルのダッシュボード画面、またはダッシュボード⇒ワークスペース一覧画面の『サービスメニュー』をクリックします。



『ネットワーク』⇒『クラウド/サーバーネットワークセキュリティ』の
Managed Firewallをクリックします。

手順③-2 M-FWの設定

Managed Firewall(Version2)の「Operation」をクリックしてください。

Security Menu

Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order	Operation

手順③-2 M-FWの設定

「デバイス」からいずれかのデバイスを右クリックします。

画面右側の「コンフィグ」をクリックします。

画面左側のオブジェクト画面から Destination NAT をクリックします。
オブジェクト ‣ NAT Object ‣ Destination NAT
画面右側の Destination NAT 画面で［追加］をクリックします。

手順③-2 M-FWの設定

設定値を入力して、［保存］をクリックします。

外部セグメント(Port4)の80番ポートのDNATの入力値は下記になります。

手順③-2 M-FWの設定

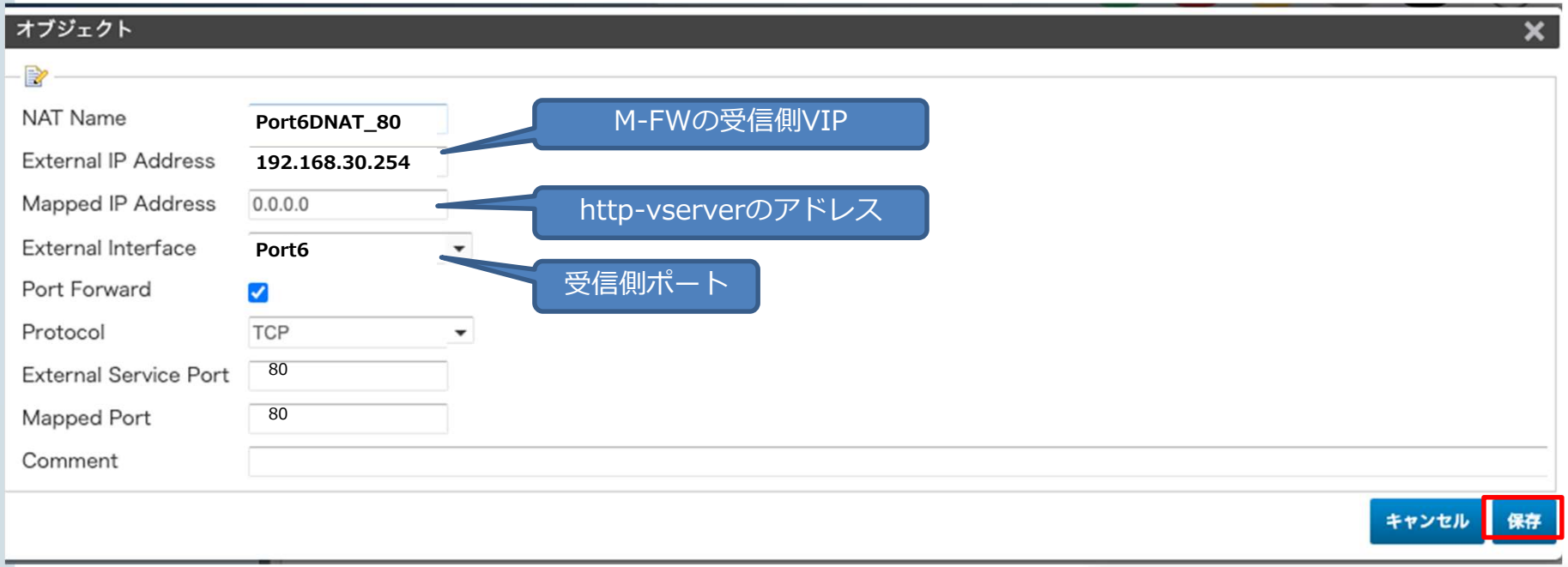
設定値を入力して、［保存］をクリックします。

外部セグメント(Port4)の443番ポートのDNATの入力値は下記になります。

手順③-2 M-FWの設定

設定値を入力して、［保存］をクリックします。

VPN-GWセグメント(Port6)の80番ポートのDNATの入力値は下記になります。



手順③-2 M-FWの設定

設定値を入力して、［保存］をクリックします。

VPN-GWセグメント(Port6)の443番ポートのDNATの入力値は下記になります。

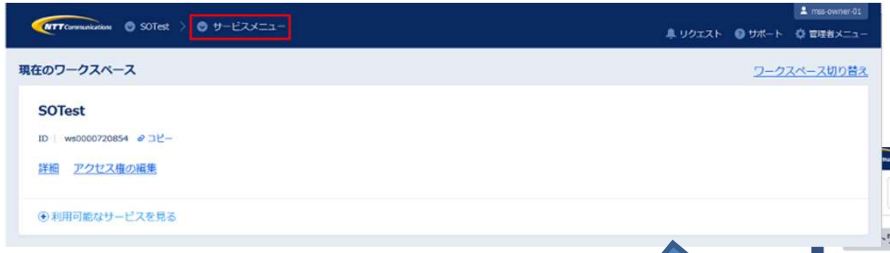
手順③-3 M-FWの設定
(ファイアウォールポリシー設定)

手順③-3 M-FWの設定

ファイアウォールポリシーの設定は下記をご覧ください。
https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/operation/managed_firewall_utm_v2/4500_firewall_policy.html

SDPFポータルからアクセス

ワークスペースを選択後、Smart Data Platform ポータルのダッシュボード画面、またはダッシュボード⇒ワークスペース一覧画面の『サービスメニュー』をクリックします。



『ネットワーク』⇒『クラウド/サーバーネットワークセキュリティ』の
Managed Firewallをクリックします。

手順③-3 M-FWの設定

Managed Firewall(Version2)の「Operation」をクリックしてください。

Security Menu

Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order	Operation

手順③-3 M-FWの設定

「デバイス」からいずれかのデバイスを右クリックします。

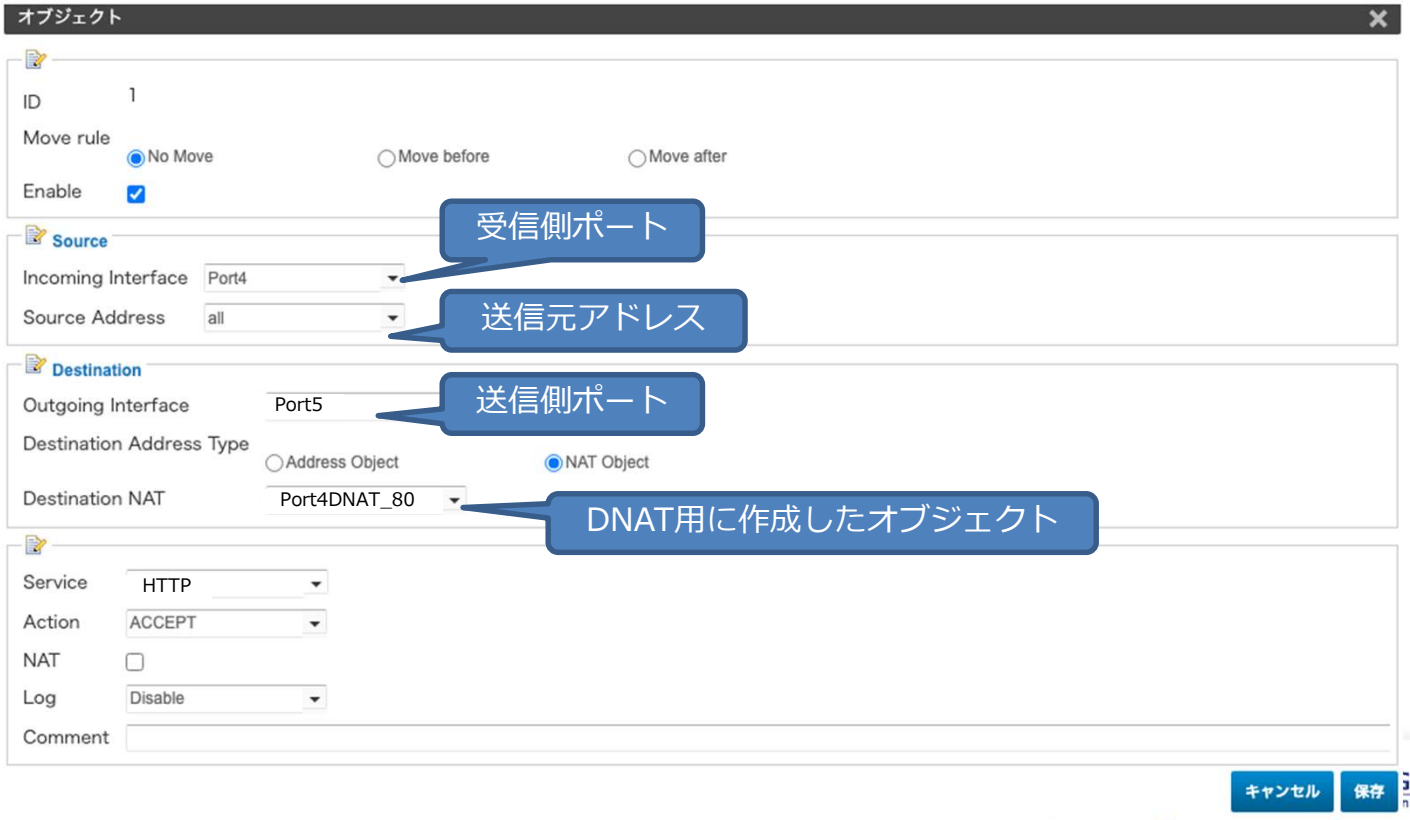
画面右側の「コンフィグ」をクリックします。

画面左側のオブジェクト画面から Firewall Policy をクリックします。
オブジェクト ‣ Firewall Policy ‣ Firewall Policy
画面右側の Firewall Policy 画面で［追加］をクリックします。

手順③-3 M-FWの設定

設定値を入力して、［保存］をクリックします。

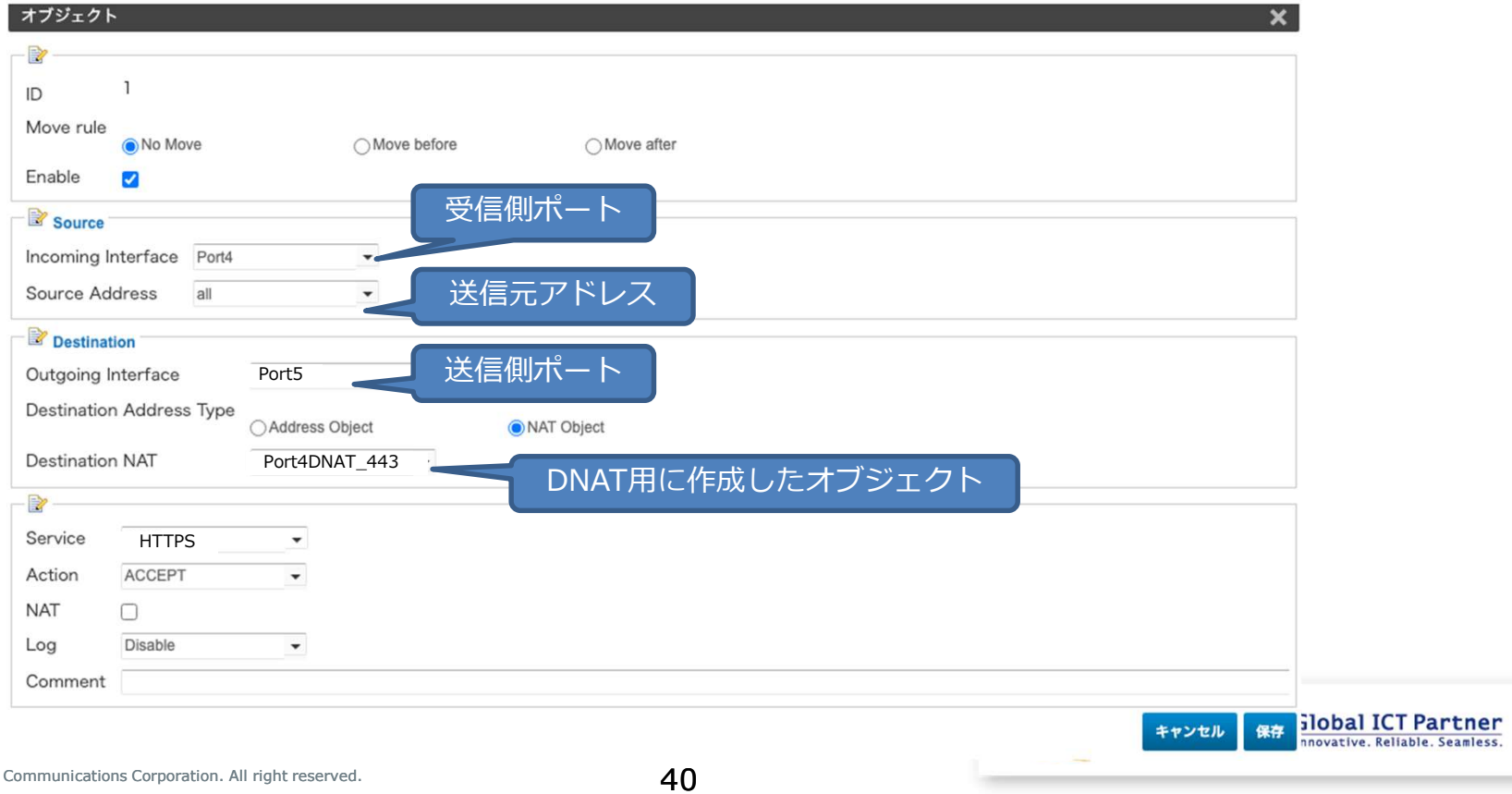
外部セグメント(Port4)の入力値は下記になります。
153.xx.xx.254の80番ポートへのアクセスの場合、172.16.100.100にDestination NATおよびACL設定するポリシー



手順③-3 M-FWの設定

設定値を入力して、［保存］をクリックします。

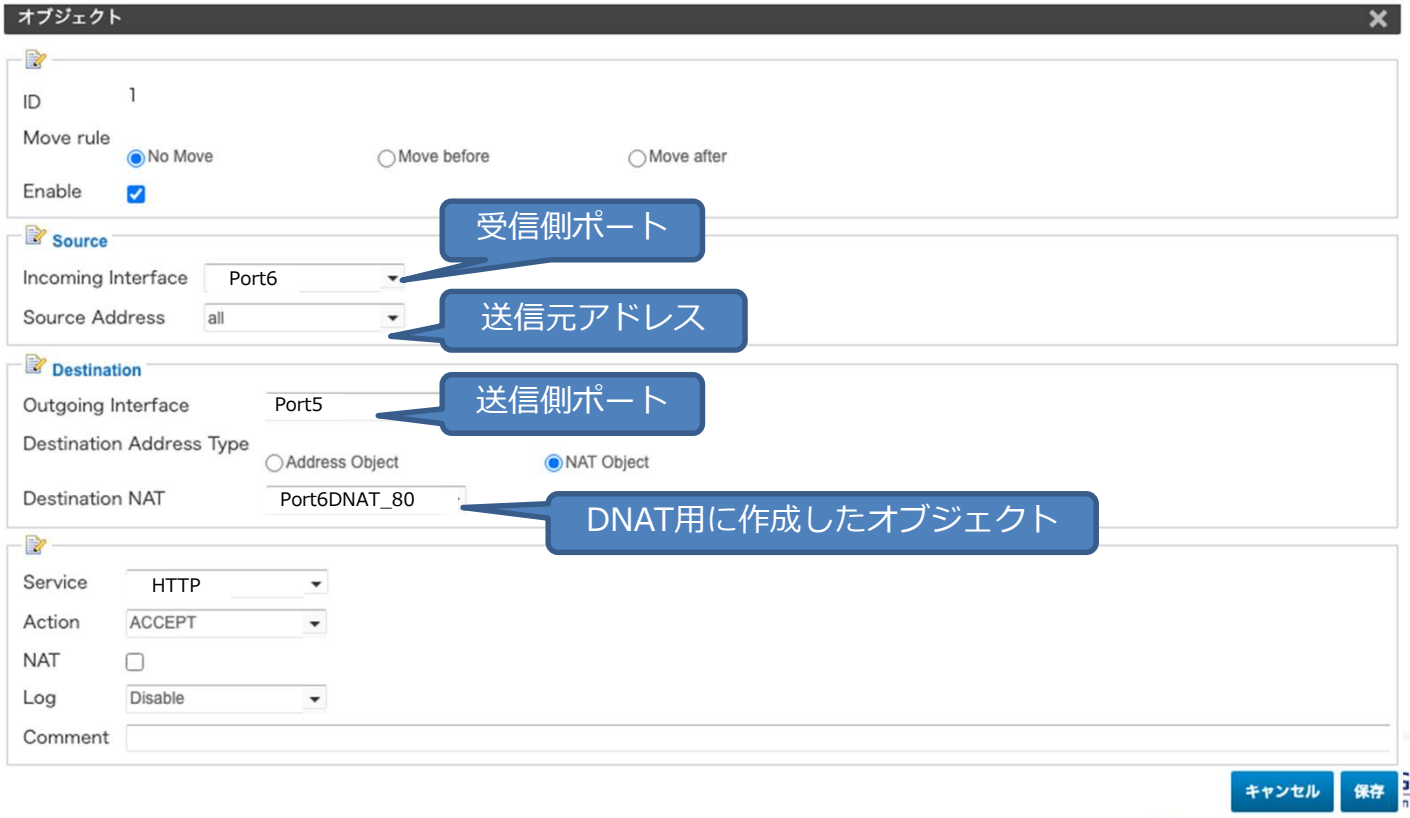
外部セグメント(Port4)の入力値は下記になります。
153.xx.xx.254の443番ポートへのアクセスの場合、172.16.100.200にDestination NATおよびACL設定するポリシー



手順③-3 M-FWの設定

設定値を入力して、［保存］をクリックします。

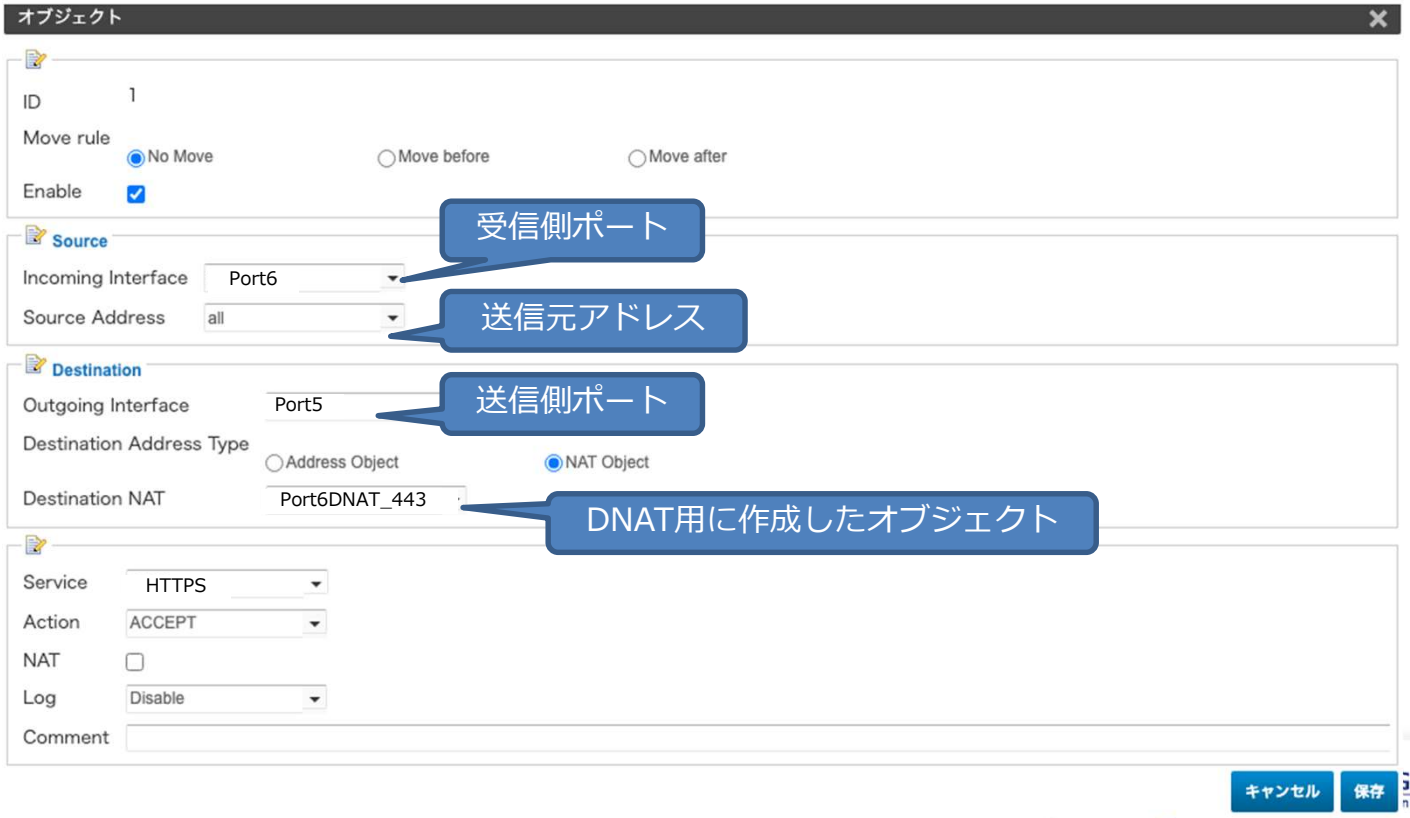
VPN-GWセグメント(Port6)の入力値は下記になります。
192.168.30.254の80番ポートへのアクセスの場合、172.16.100.100にDestination NATおよびACL設定するポリシー



手順③-3 M-FWの設定

設定値を入力して、［保存］をクリックします。

VPN-GWセグメント(Port6)の入力値は下記になります。
192.168.30.254の443番ポートへのアクセスの場合、172.16.100.200にDestination NATおよびACL設定するポリシー

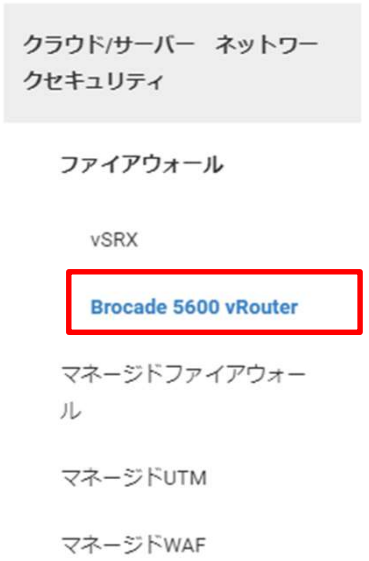


手順④ vFWのインターフェース削除

手順④ vFWのインターフェース削除

下記リンクを参考の上、vFWのインターフェース削除をお願いいたします。

サービスメニューから『サーバーインスタンス』をクリックし、
『クラウド/サーバー　ネットワークセキュリティ』→『ファイアーウォール』→『Brocade 5600 vRouter』をクリックください。



手順④ vFWのインターフェース削除

1．ファイアウォール一覧から対象vFWを選択
2．ファイアウォールインタフェースタブから、対象のインタフェースの右側「▼」を
　　クリックして「VRRP通信設定の解除」を選択
3．　VRRP用通信設定の解除(ポップアップ画面)において「VRRP用通信設定の解除」を選択

※dp0s4, dp0s5,dp0s6で実施。

手順④ vFWのインターフェース削除

1．ファイアウォール一覧から対象vFWを選択
2．ファイアウォールインタフェースタブから、対象のインタフェースの右側「▼」を
　　クリックして「ロジカルネットワークの切断」を選択

※dp0s4, dp0s5,dp0s6で実施。

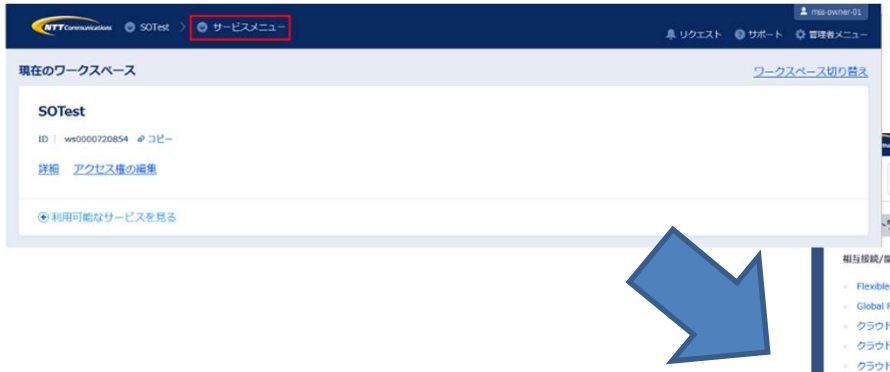
手順⑤ M-FWの設定
(インターフェースの設定)

手順⑤ M-FWの設定

M-FWのインターフェースの設定が可能です。
https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/operation/managed_firewall_utm_v2/3110_interface_single.html

SDPFポータルからアクセス

ワークスペースを選択後、Smart Data Platform ポータルのダッシュボード画面、またはダッシュボード⇒ワークスペース一覧画面の『サービスメニュー』をクリックします。



『ネットワーク』⇒『クラウド/サーバーネットワークセキュリティ』の
Managed Firewallをクリックします。

手順⑤ M-FWの設定

Managed Firewall(Version2)の「Operation」をクリックしてください。

Security Menu

Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order	Operation

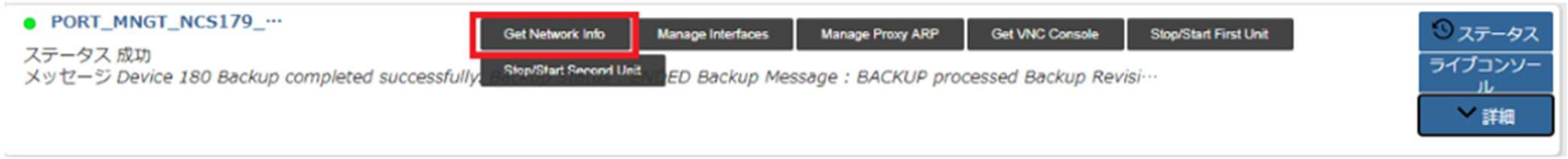
手順⑤ M-FWの設定

[サービス] -［ワークフロー］-［Cluster Port Management］をクリックすると、インターフェース設定の詳細画面が開きます。
HA構成の場合、［UTM Port Management］は使用しません。

20

手順⑤ M-FWの設定

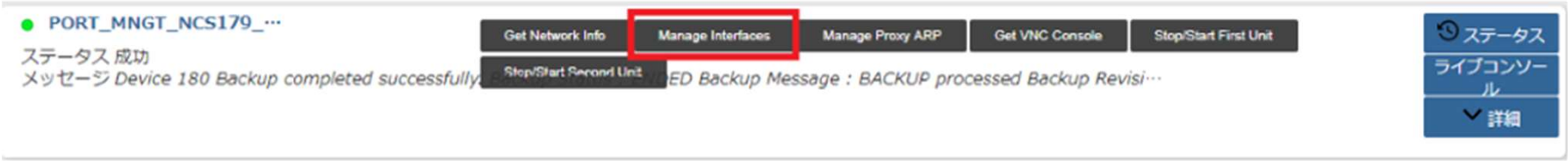
最新のお客さまネットワーク情報を参照可能にするため、設定対象のデバイスをクリックで選択して［Get Network Info］をクリックします。



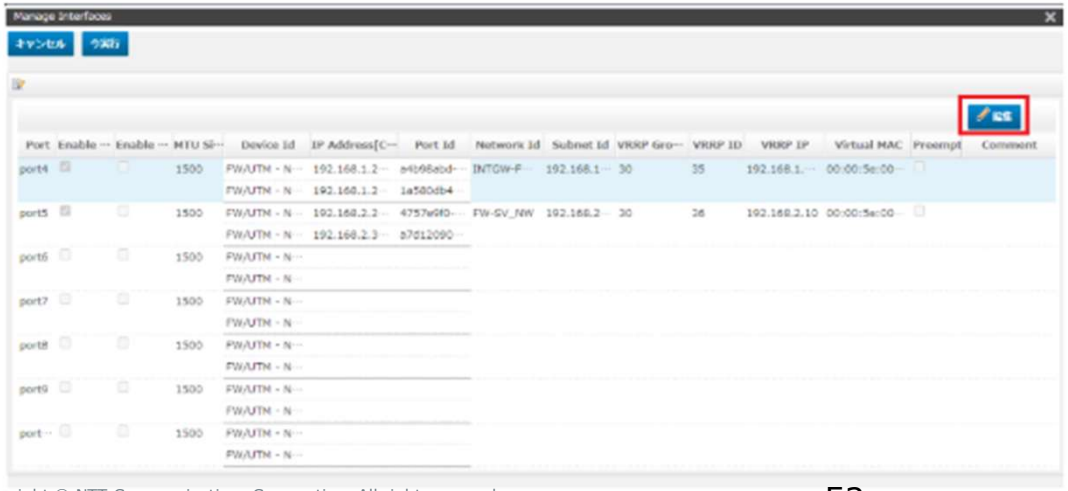
［タスク ステータス］が表示されます。Get Network Infoのタスクが「緑色」になれば正常終了です。[クローズ]で閉じてください。

手順⑤ M-FWの設定

設定対象のデバイスをクリックで選択し、［Manage Interfaces］をクリックします。

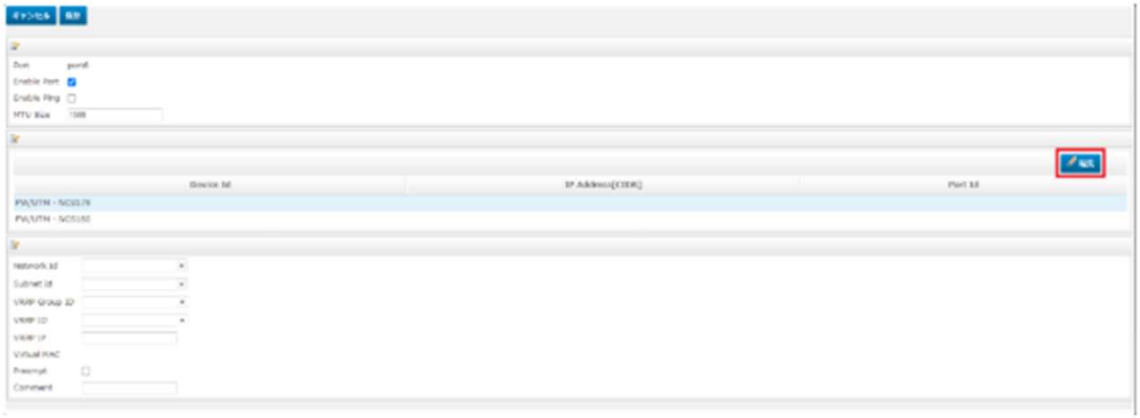


［Manage Interfaces］の画面が開きます。Port 2,3は［Manage Interfaces］の画面には表示されません。設定対象のポートをクリックで選択して、［編集］をクリックします。



手順⑤ M-FWの設定

各デバイスを選択し、編集を押します。



各デバイスに設定する実IPアドレスを入力し、[保存]をクリックします。

手順⑤ M-FWの設定

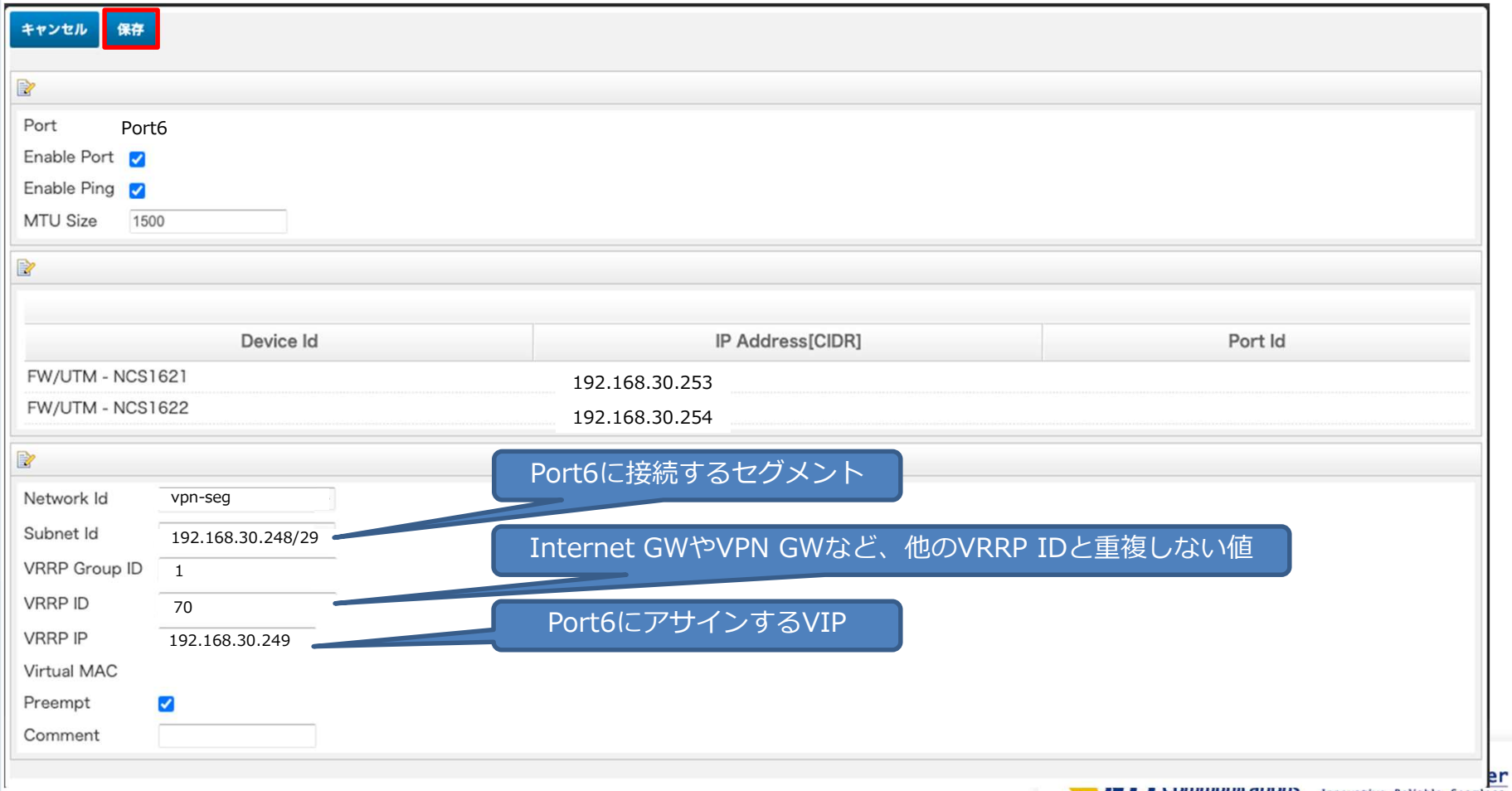
［Enable Port］をチェックすると設定値を入力できます。
外部セグメント(Port4)の入力値は下記になります。
［保存］をクリックします。この画面で保存しただけではデバイスに適用されません。

手順⑤ M-FWの設定

［Enable Port］をチェックすると設定値を入力できます。
FWセグメント(Port5) の入力値は下記になります。
［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。

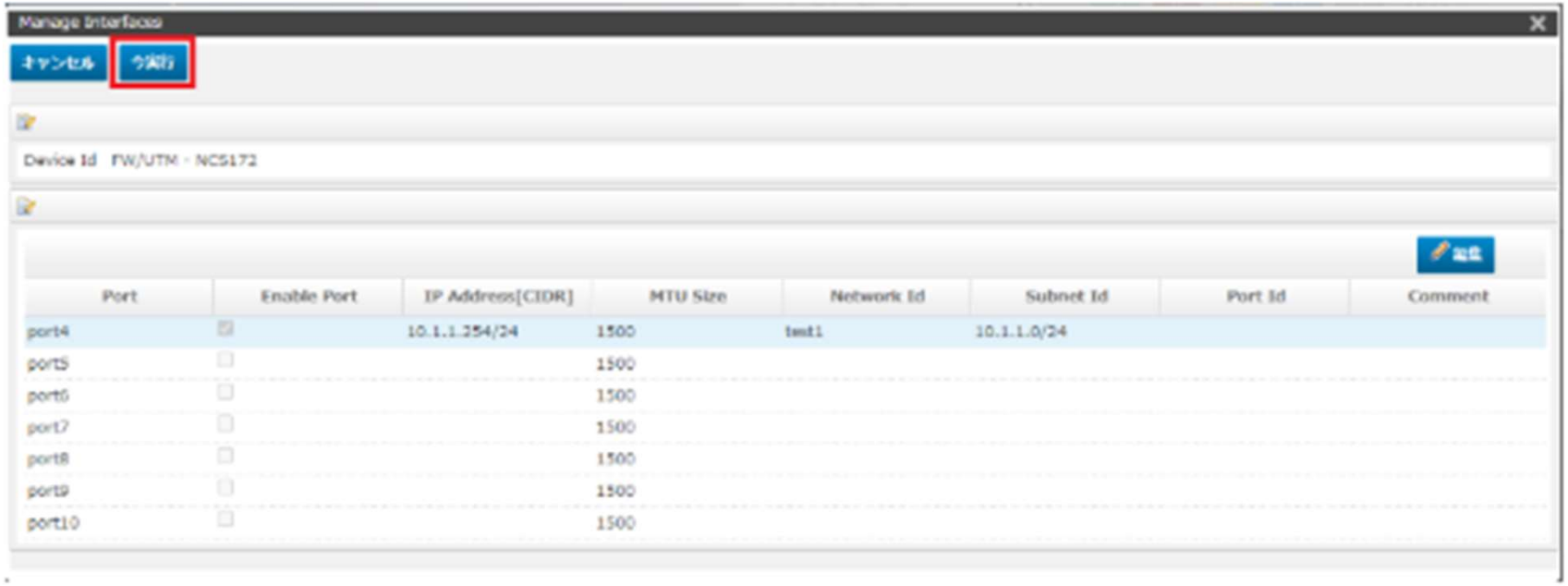
手順⑥ M-FWの設定

［Enable Port］をチェックすると設定値を入力できます。
VPN-GWセグメント(Port6)の入力値は下記になります。
［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。



手順⑤ M-FWの設定

使用するポート設定が準備できたら、Manage Interfaces画面で［今実行］をクリックします。



手順⑤ M-FWの設定

[タスク ステータス]が表示されます。

手順⑤ M-FWの設定

すべてのステータスが「緑色」になれば正常終了です。