ファイアウォール(vFW 5600 vRouter)からManaged Firewallへの交換によるマイグレ実施方法(シングル構成,併用移行版)

第2版

更新履歴

更新日	更新内容	版数
2017/08/07	初版	1
2017/08/10	移行後VPN-GWセグメントのIPアドレス帯を修正。	2

前提条件

前提条件

■ファイアウォール(vFW 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)が発生するケースです。
・ vFWで利用しているネットワークとは別のネットワークをM-FWへ接続します。
⇒ vFWで利用しているネットワークから、M-FWで利用しているネットワークへ切り替える際、DNS設定変更が必要になります。

・Internet-GWおよびVPN-GW先のクライアントからWeb-serverへアクセスするケースを想定します。

・M-FWでSNATを利用しているため、Web-serverへアクセスする送信元IPアドレスがM-FWセグメントのIPアドレスとなります。Global IPを送信元にしたい場合、ロードバランサーのデフォルトルート変更後、SNAT設定を削除ください。

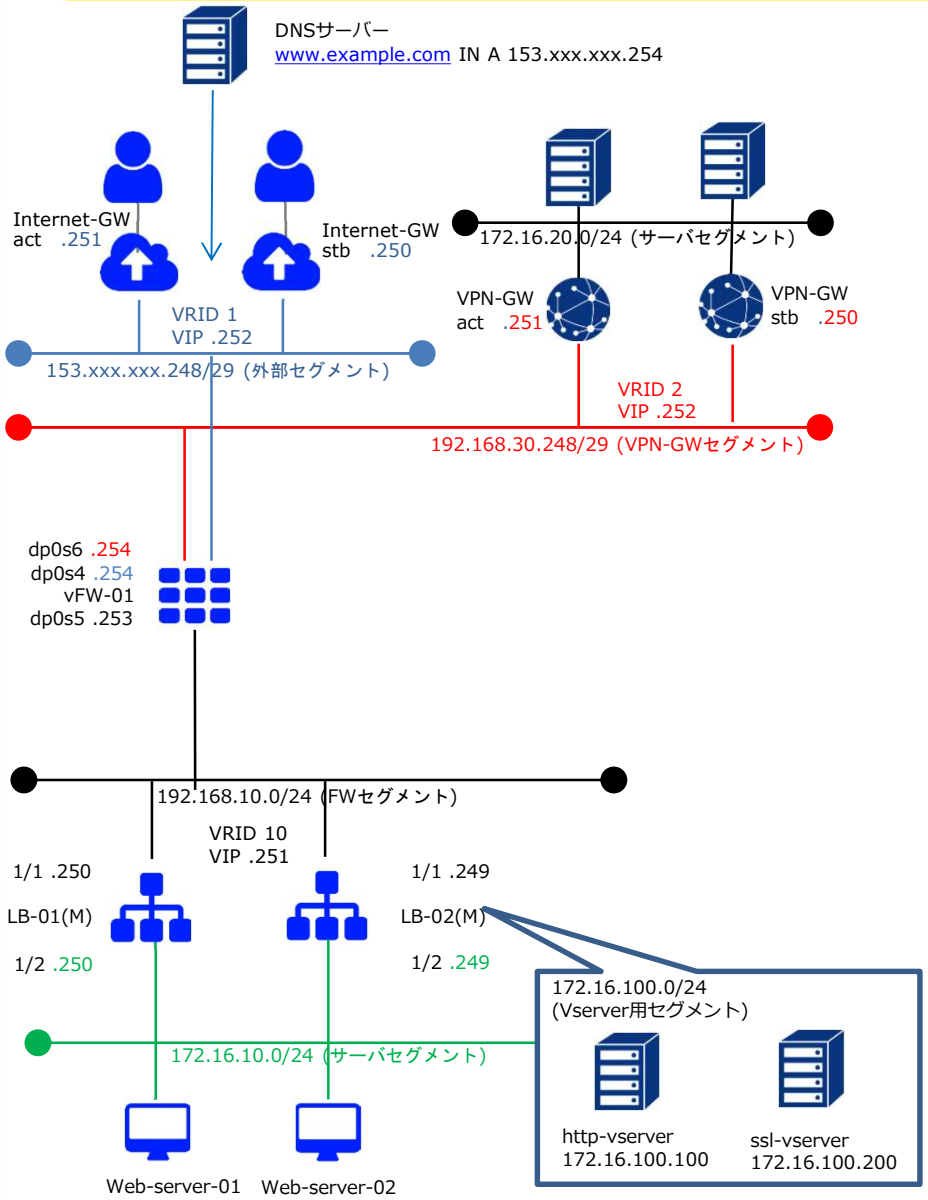
※事前検証を行ってから移行を実施ください。

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。

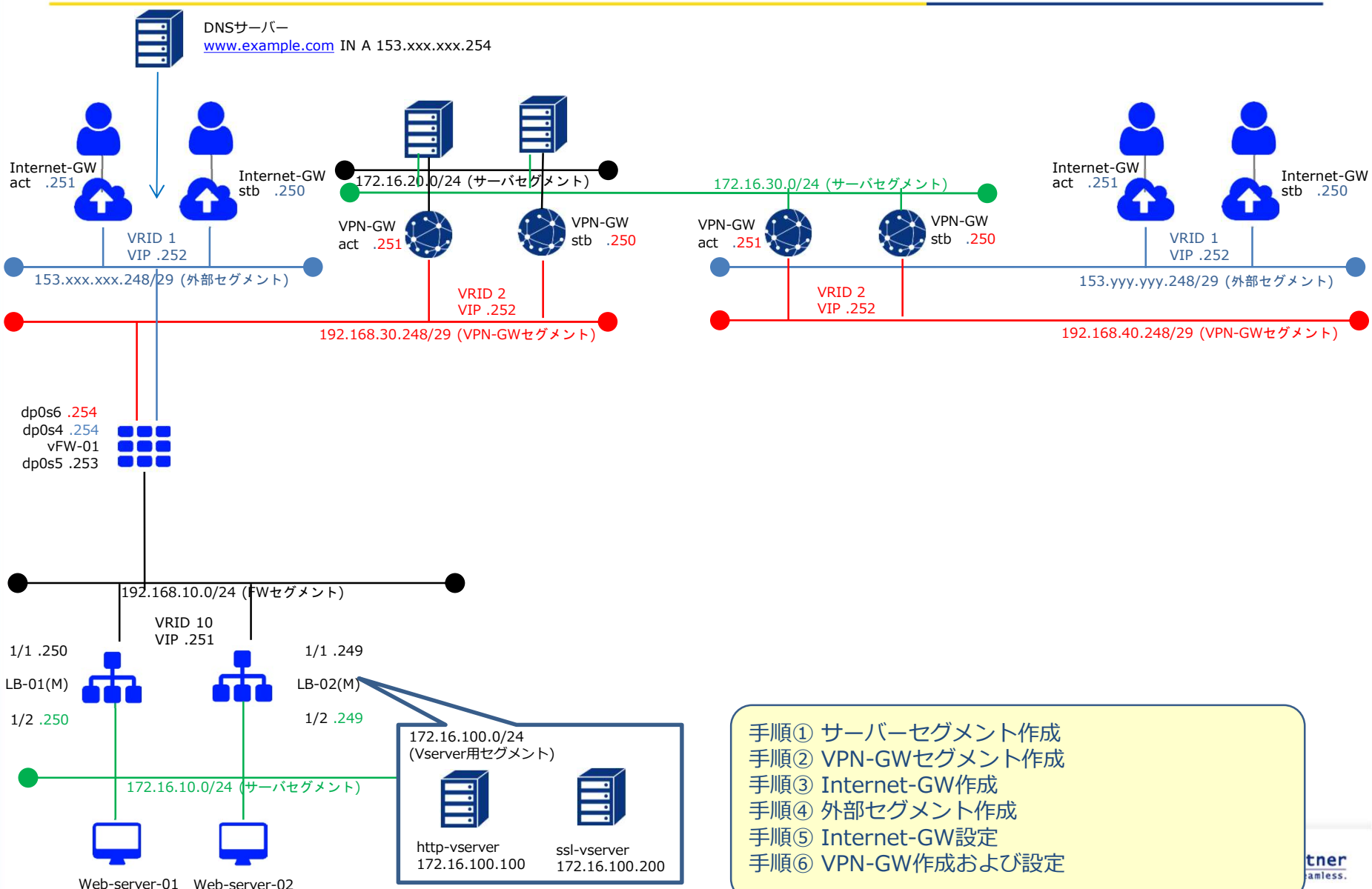
構成および移行フロー

移行前構成（vFW構成）



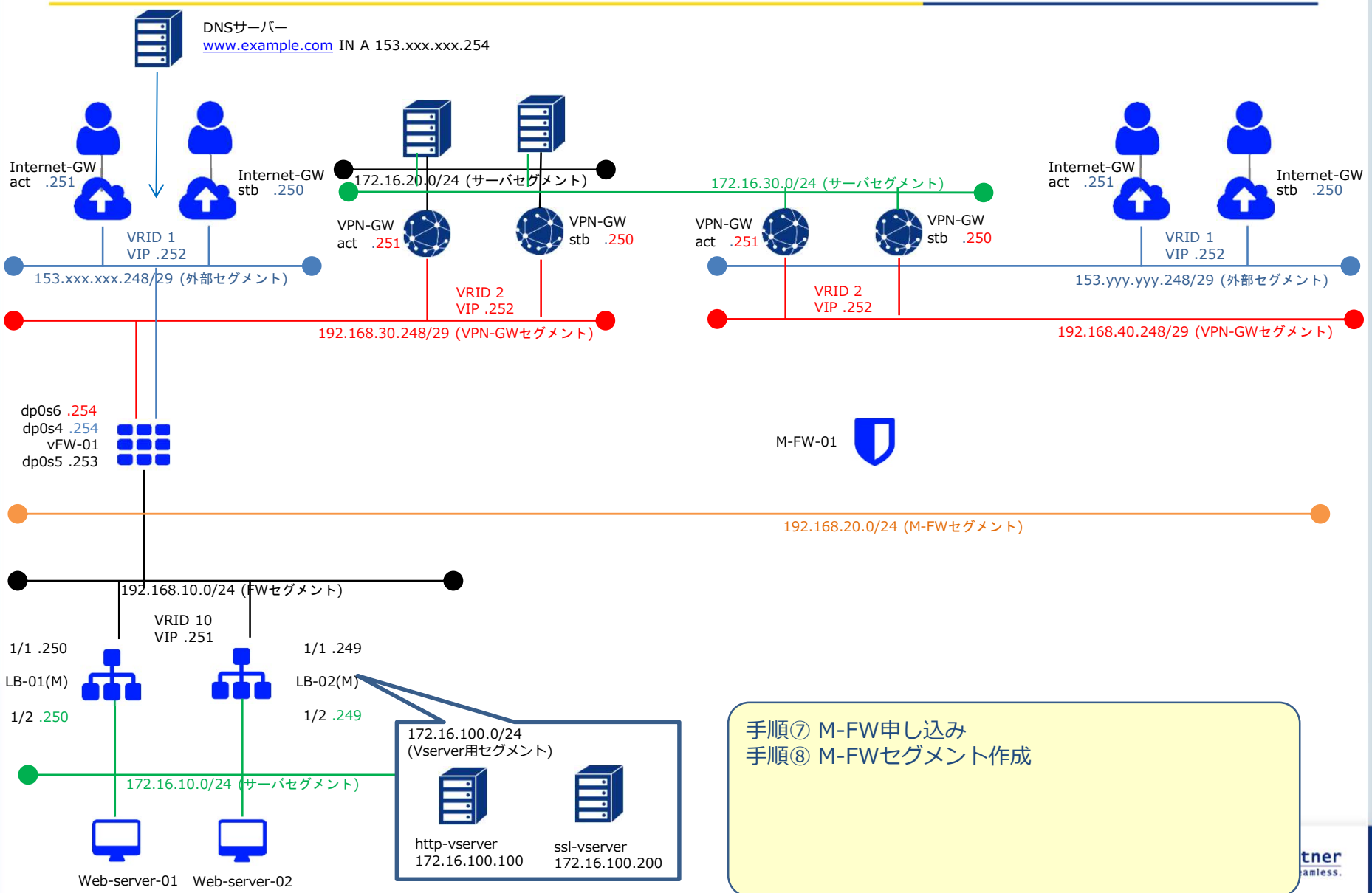
・vFWルールは外部セグメントからは基本全て拒否し、特定のHTTP/HTTPSアクセスのみ許可。
・外部セグメントからvFWのグローバルIPにアクセスをDNAT変換でバーチャルサーバのIPに変換します。
・LBの内部に”別のセグメント”でバーチャルサーバーを設定しておきます。

移行時構成①



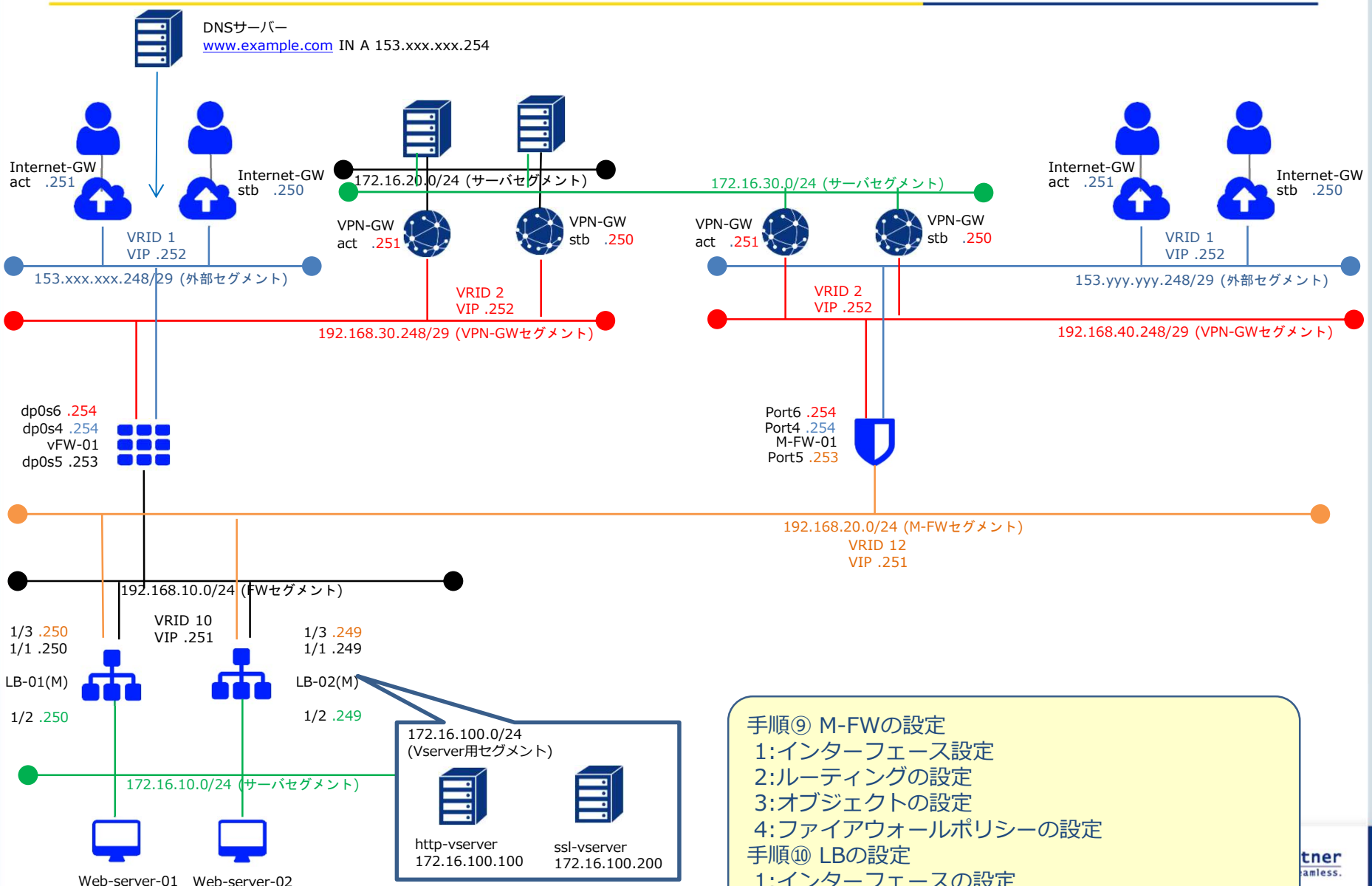
手順① サーバーセグメント作成
手順② VPN-GWセグメント作成
手順③ Internet-GW作成
手順④ 外部セグメント作成
手順⑤ Internet-GW設定
手順⑥ VPN-GW作成および設定

移行時構成②



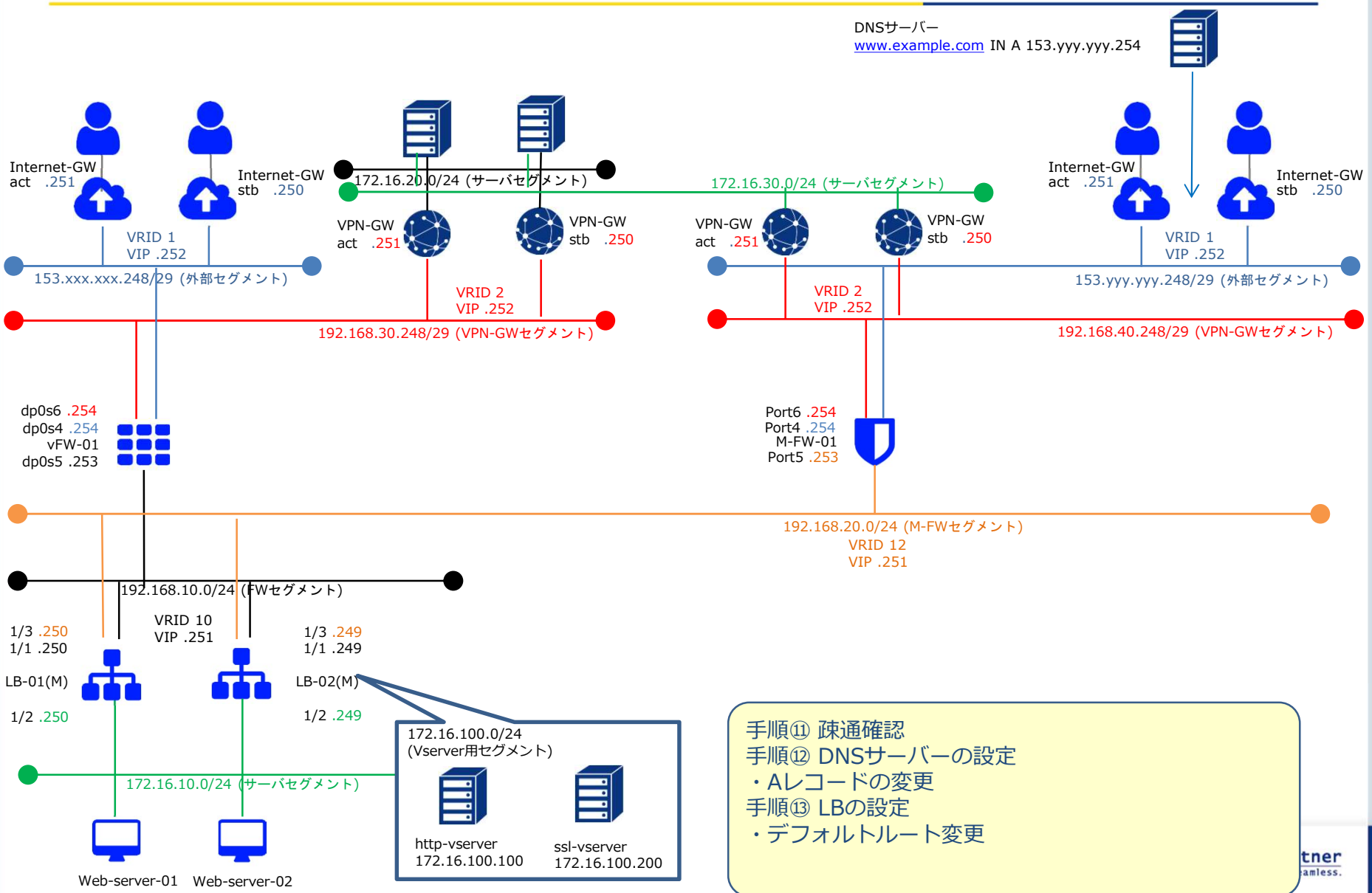
手順⑦ M-FW申し込み
手順⑧ M-FWセグメント作成

移行時構成③



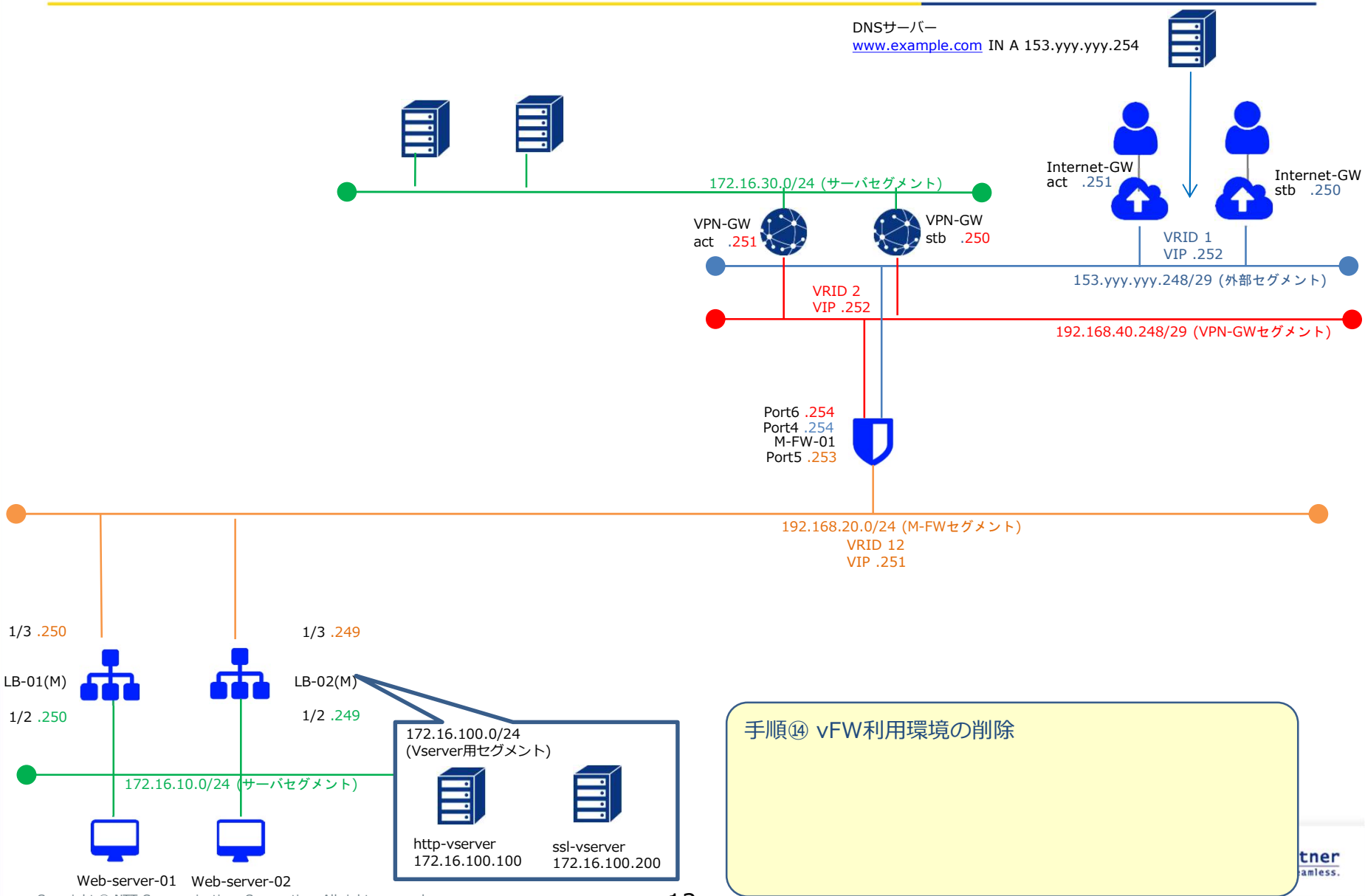
手順⑨ M-FWの設定
1:インターフェース設定
2:ルーティングの設定
3:オブジェクトの設定
4:ファイアウォールポリシーの設定
手順⑩ LBの設定
1:インターフェースの設定

移行時構成④



手順⑪ 疎通確認
手順⑫ DNSサーバーの設定
・Aレコードの変更
手順⑬ LBの設定
・デフォルトルート変更

移行完了構成（Managed Firewall構成）



手順⑭ vFW利用環境の削除

手順① サーバーセグメント作成

手順① サーバーセグメント作成

VPN-GW先のサーバーに新規サーバーセグメント172.16.30.0/24を作成ください。
また、Web-server宛ての通信に対し、本セグメント経由で接続ができるようVPN-GW先のクライアント側の設定をお願いいたします。

※セグメント作成および設定方法はクライアント環境により異なります。

手順② VPN-GWセグメント作成

手順② VPN-GWセグメント作成

1．ロジカルネットワークの作成ボタンを押下します。

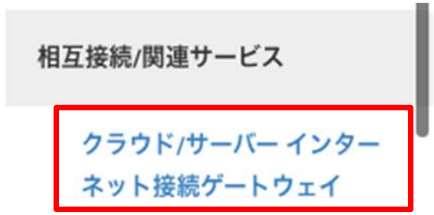
手順② VPN-GWセグメント作成

2-1.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、192.168.40.248/29を、ゲートウェイIPに192.168.40.252を記入)
・「DHCP 有効」にチェック
・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。

手順③ Internet-GW作成

手順③ Internet-GW作成

下記リンクを参照の上、インターネット接続のお申し込みをお願いいたします。
https://sdpf.ntt.com/services/docs/internet-gw/tutorials/internet-gw.html
コントロールパネルから「サーバーインスタンス」→相互接続/関連サービスから「クラウド/サバー インターネット接続ゲートウェイ」→「インターネットゲートウェイの作成」を選択

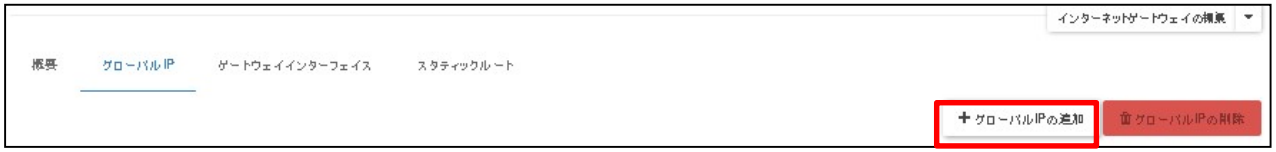


手順③ Internet-GW作成

下記リンクを参照の上、インターネット接続のお申し込みをお願いいたします。
https://sdpf.ntt.com/services/docs/internet-gw/tutorials/internet-gw.html
「インターネットゲートウェイの作成」をクリック。

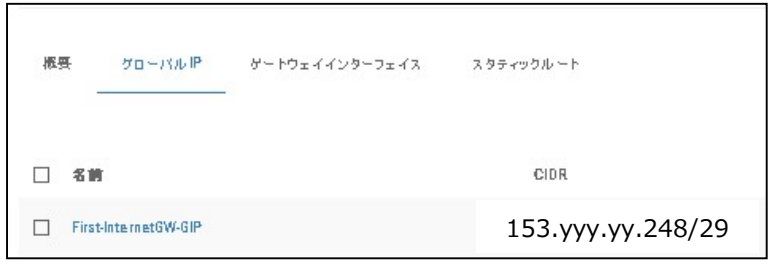
手順③ Internet-GW作成

作成したインターネットGWを選択し、「グローバルIP」タブから「グローバルIPの追加」をクリック。



グローバルIPネットマスクで”29”を選択し、「グローバルIPの追加」をクリック。

GIPが払い出されます。



手順④ 外部セグメント作成

手順④ 外部セグメント作成

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④ 外部セグメント作成

2-1.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、153.yyy.yy.248/29を、ゲートウェイIPに153.yyy.yyy.252を記入)
・「DHCP 有効」にチェック
・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。

手順⑤ Internet-GW設定

手順⑤ Internet-GW設定

作成したインターネットGWを選択し、「ゲートウェイインターフェース」タブから「ゲートウェイインターフェイスの追加」をクリック。

パラメータを入力し、
「ゲートウェイインターフェイスの追加」をクリック

手順⑤ Internet-GW設定

作成したインターネットGWを選択し、「スタティックルート」タブから「スタティックルートの追加」をクリック。

パラメータを入力し、
「スタティックルートの追加」をクリック

手順⑥ VPN-GW作成および設定

手順⑥ VPN-GW作成および設定

下記リンクを参照の上、VPN接続のお申し込みをお願いいたします。
https://ecl.ntt.com/documents/tutorials/rsts/Network/vpn.html

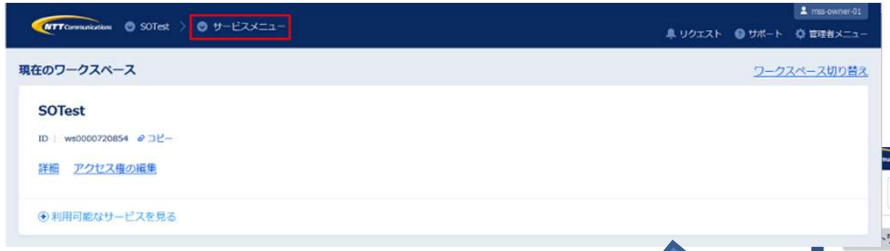
vFW利用中の設定を元に、Web-server宛ての通信を許可するよう、VPN-GWへ設定ください。

手順⑦ M-FW申し込み

手順⑦ M-FW申し込み

下記リンクを参照の上、シングル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_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⑦ 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」を選択ください。

セキュリティ

申込種別 デバイス追加

お申し込みの際の入力値は下記になります。

Device Information

メニュー	プラン	構成	ゾーン/グループ
Managed Firewall	2CPU-4GB	Single	zone1-groupa

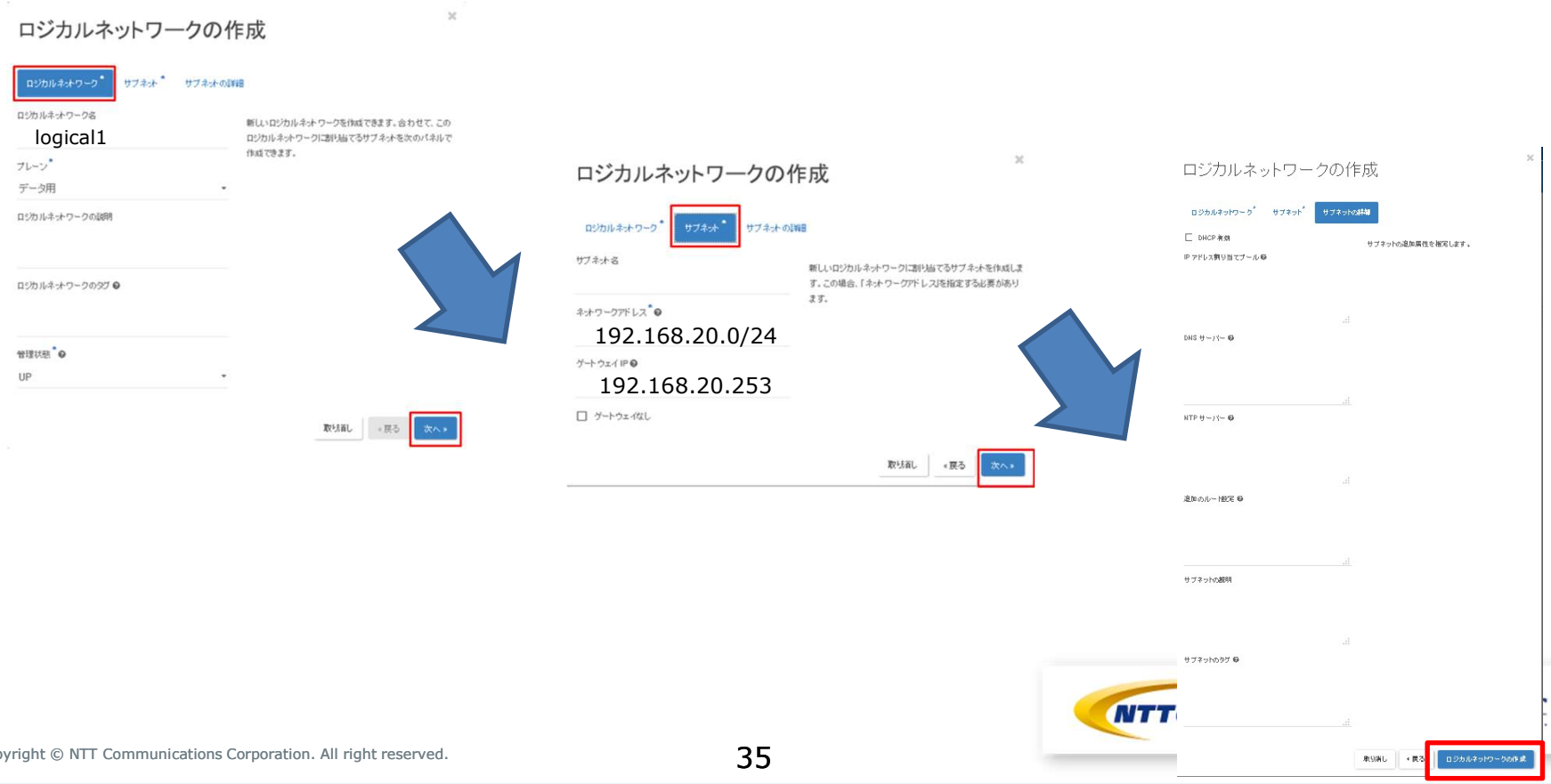
手順⑧ M-FWセグメント作成

手順⑧ M-FWセグメント作成

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⑧ M-FWセグメント作成

2-1. 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、192.168.20.0/24を、ゲートウェイIPに192.168.20.253を記入)
・「DHCP 有効」にチェックし、「IP アドレス割り当てプール」に192.168.20.1,192.168.20.100を設定。
・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。



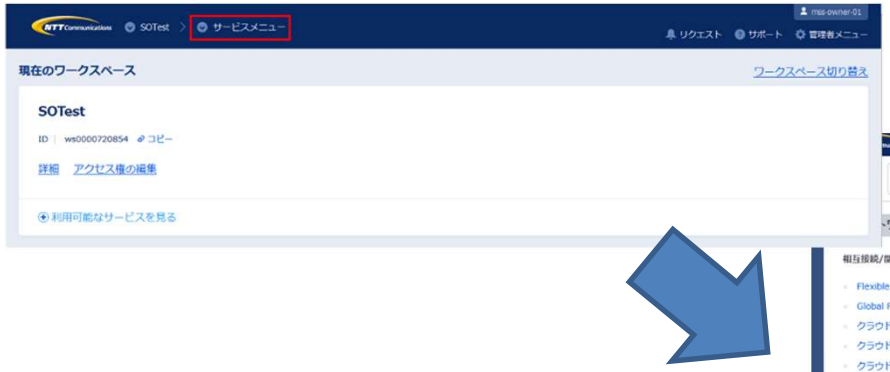
手順⑨-1 M-FWの設定
(インターフェース設定)

手順⑨-1 M-FWの設定
(インターフェース設定)

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⑨-1 M-FWの設定
(インターフェース設定)

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

Security Menu

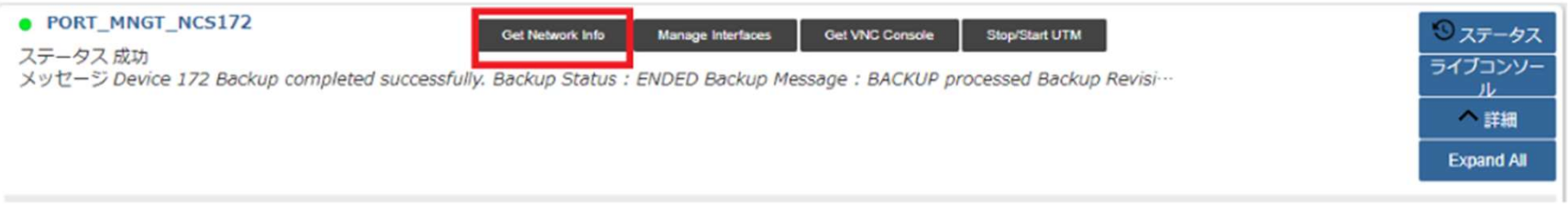
Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order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

手順⑨-1 M-FWの設定
(インターフェース設定)

［サービス] -> [ワークフロー] -> ［UTM 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。
シングル構成の場合、［Cluster Port Management］及び［Cluster Route Management］は使用しません 。

手順⑨-1 M-FWの設定
(インターフェース設定)

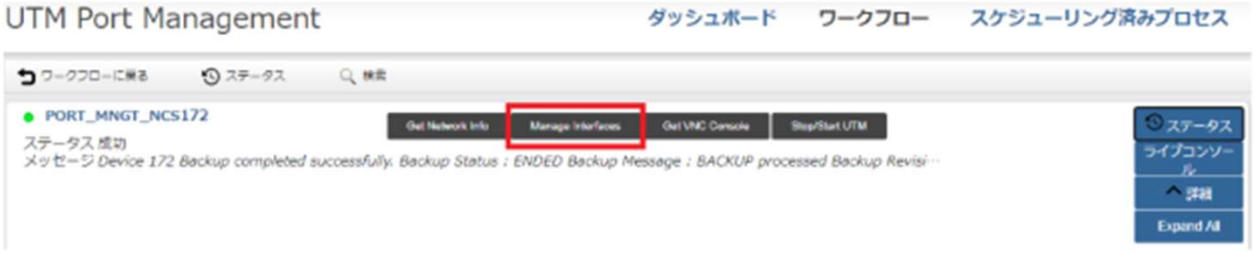
最新のお客さまネットワーク情報を参照可能にするため、設定対象のデバイスをクリックで選択して［Get Network Info］をクリックします。



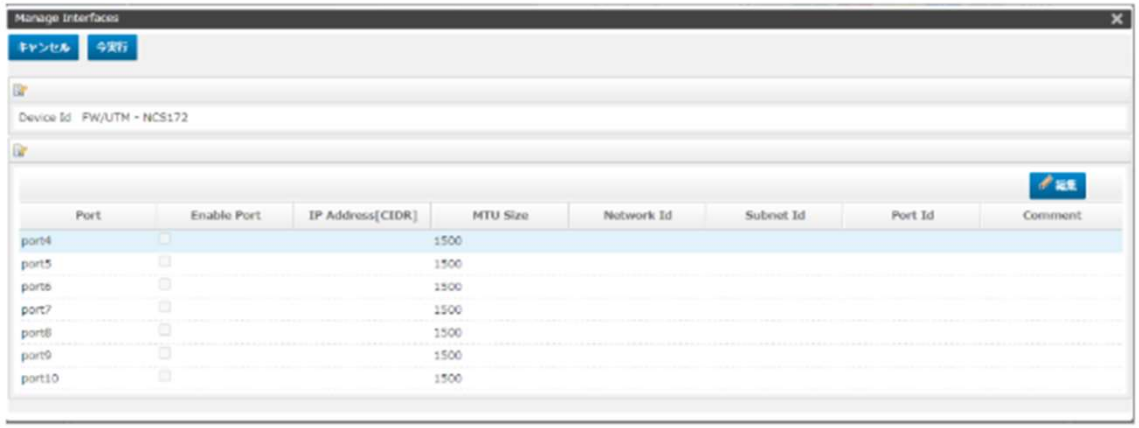
［タスク ステータス］が表示されます。Get Network Infoのタスクが「緑色」になれば正常終了です。[クローズ]で閉じてください。

手順⑨-1 M-FWの設定
(インターフェース設定)

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⑨-1 M-FWの設定
(インターフェース設定)

［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⑨-1 M-FWの設定 (インターフェース設定)

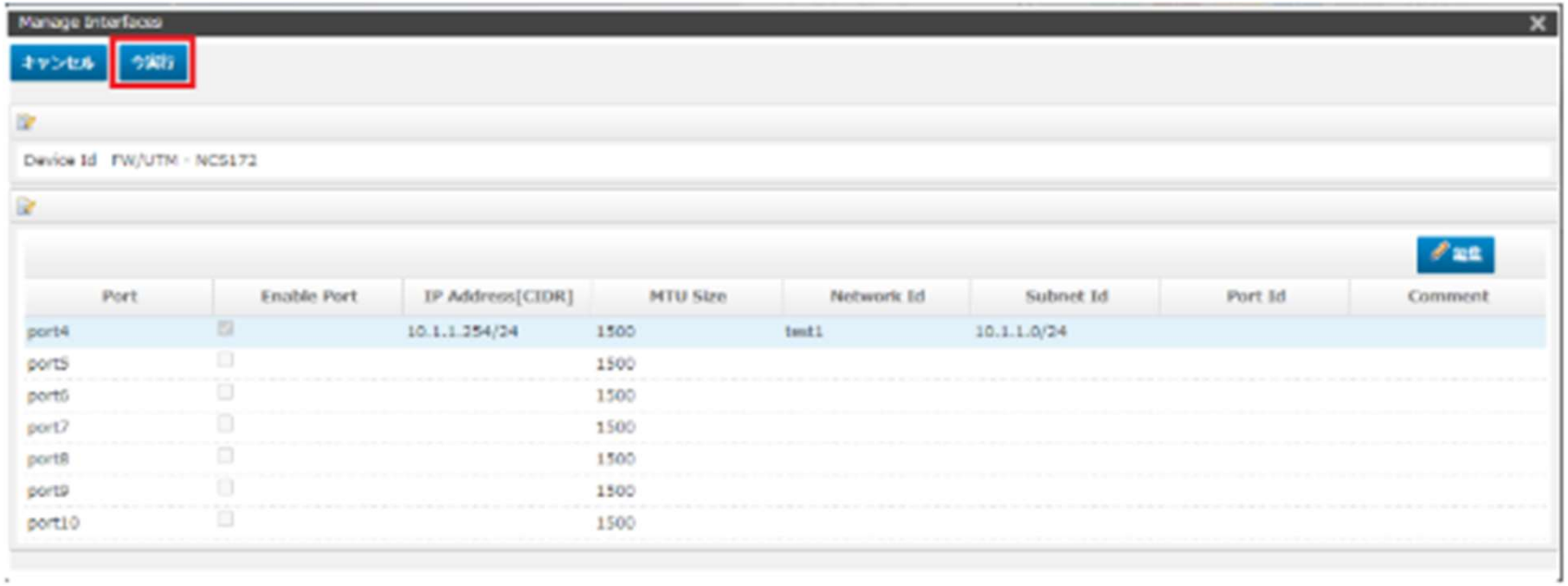
［Enable Port］をチェックすると設定値を入力できます。
FWセグメント(Port5) の入力値は下記になります。
［保存］をクリックします。この画面で保存しただけではデバイスに適用されません。

手順⑨-1 M-FWの設定
(インターフェース設定)

［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⑨-1 M-FWの設定
(インターフェース設定)

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。

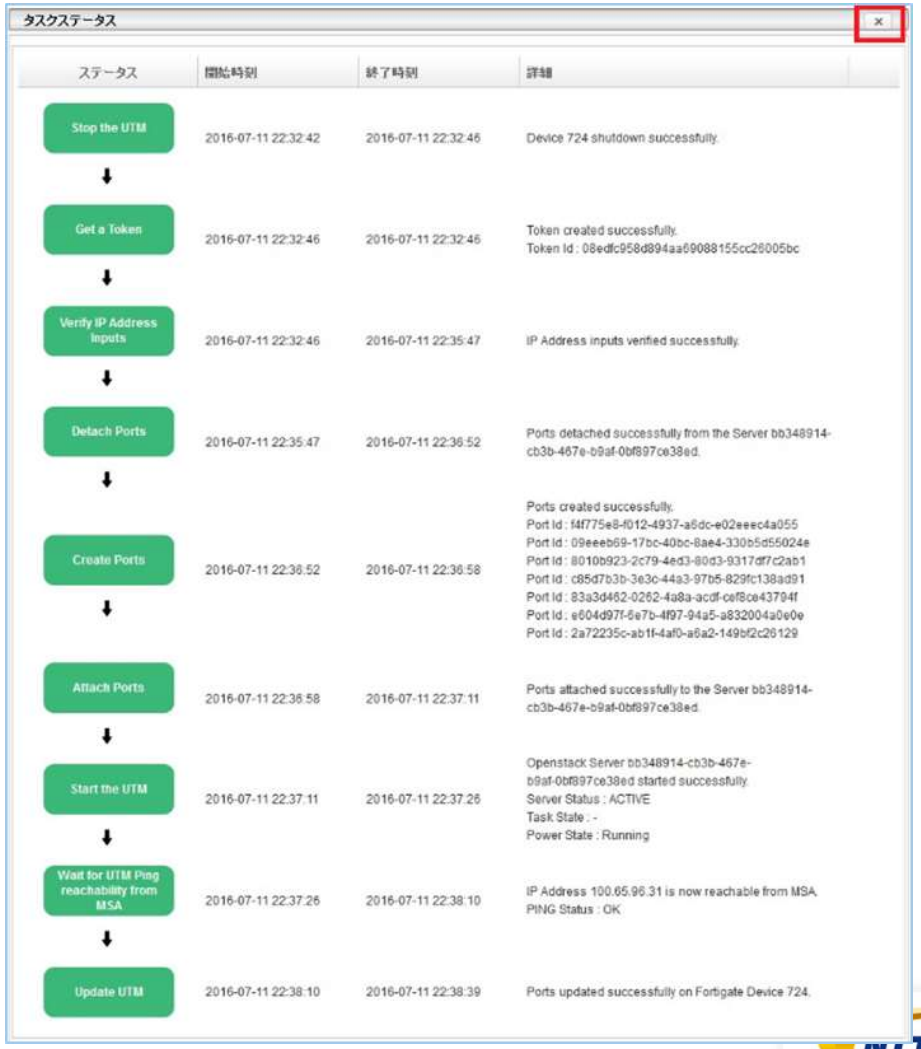


手順⑨-1 M-FWの設定
(インターフェース設定)

[タスク ステータス]が表示されます。

手順⑨-1 M-FWの設定
(インターフェース設定)

すべてのステータスが「緑色」になれば正常終了です。

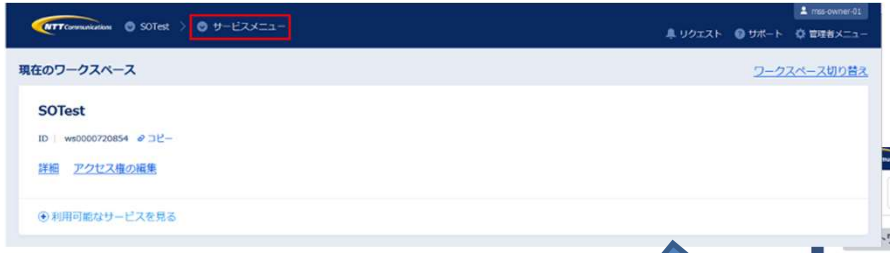


手順⑨-2 M-FWの設定
(ルーティングの設定)

手順⑨-2 M-FWの設定
(ルーティングの設定)

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_v2/4210_routing_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⑨-2 M-FWの設定
(ルーティングの設定)

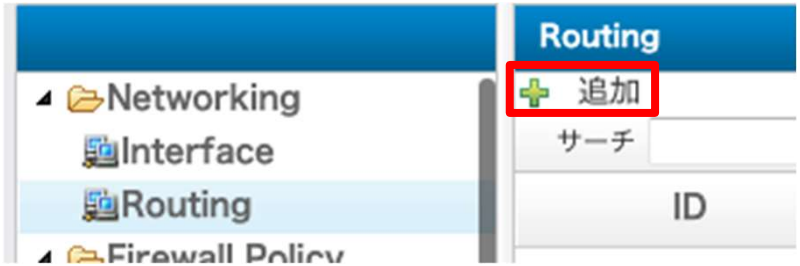
Managed Firewall(Version2)の「Operation」をクリックしてください。

手順⑨-2 M-FWの設定
(ルーティングの設定)

「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 Routing をクリックします。
オブジェクト ‣ Networking ‣ Routing



手順⑨-2 M-FWの設定
(ルーティングの設定)

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⑨-2 M-FWの設定
(ルーティングの設定)

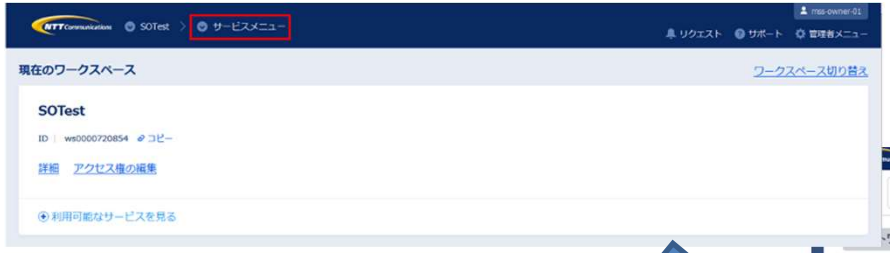
設定値を入力して、［保存］をクリックします
VPN-GW先サーバーセグメント宛て通信の入力値は下記になります。

手順⑨-3 M-FWの設定
(オブジェクトの設定)

手順⑨-3 M-FWの設定
(オブジェクトの設定)

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⑨-3 M-FWの設定
(オブジェクトの設定)

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

手順⑨-3 M-FWの設定
(オブジェクトの設定)

「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⑨-3 M-FWの設定
(オブジェクトの設定)

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⑨-3 M-FWの設定
(オブジェクトの設定)

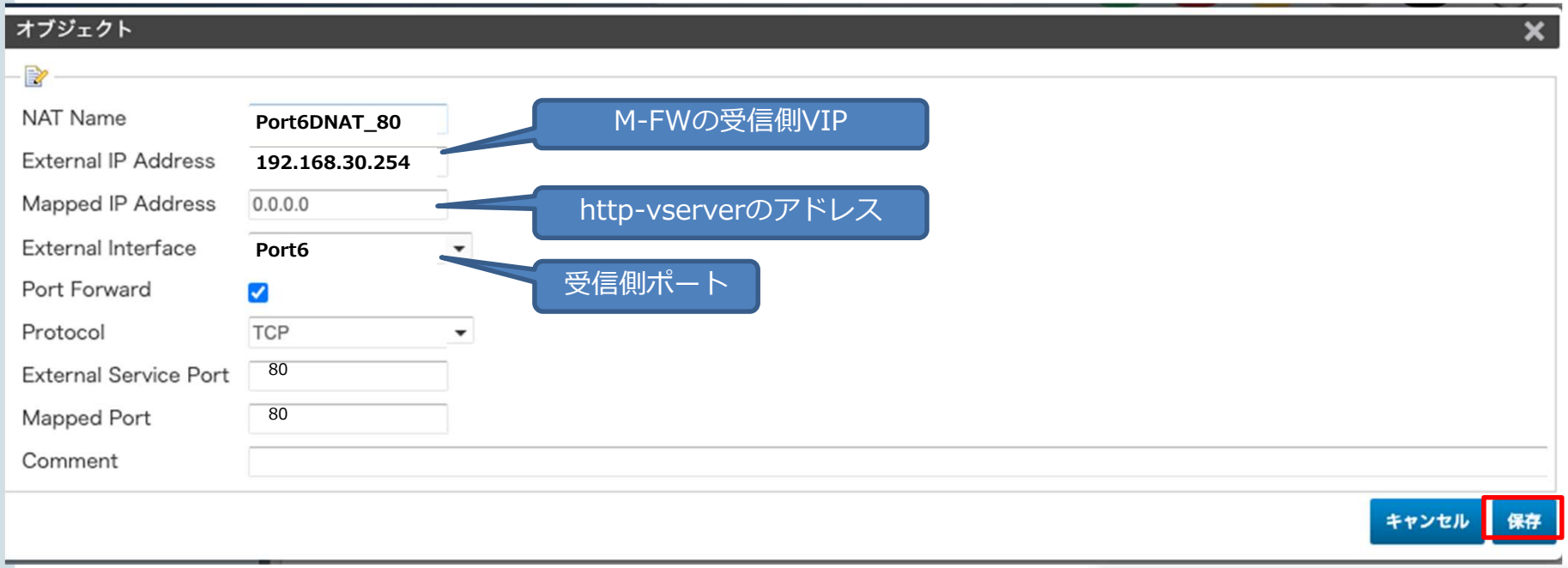
設定値を入力して、［保存］をクリックします。

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⑨-3 M-FWの設定
(オブジェクトの設定)

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⑨-3 M-FWの設定
(オブジェクトの設定)

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。

「変更の保存」をクリックして、設定をデバイスへ適用します。

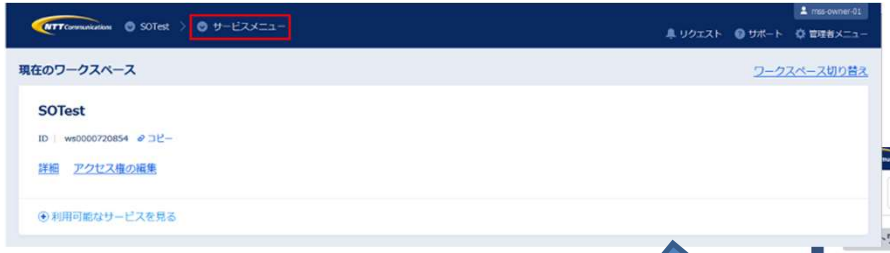
手順⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

手順⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

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⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

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⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

「デバイス」からいずれかのデバイスを右クリックします。

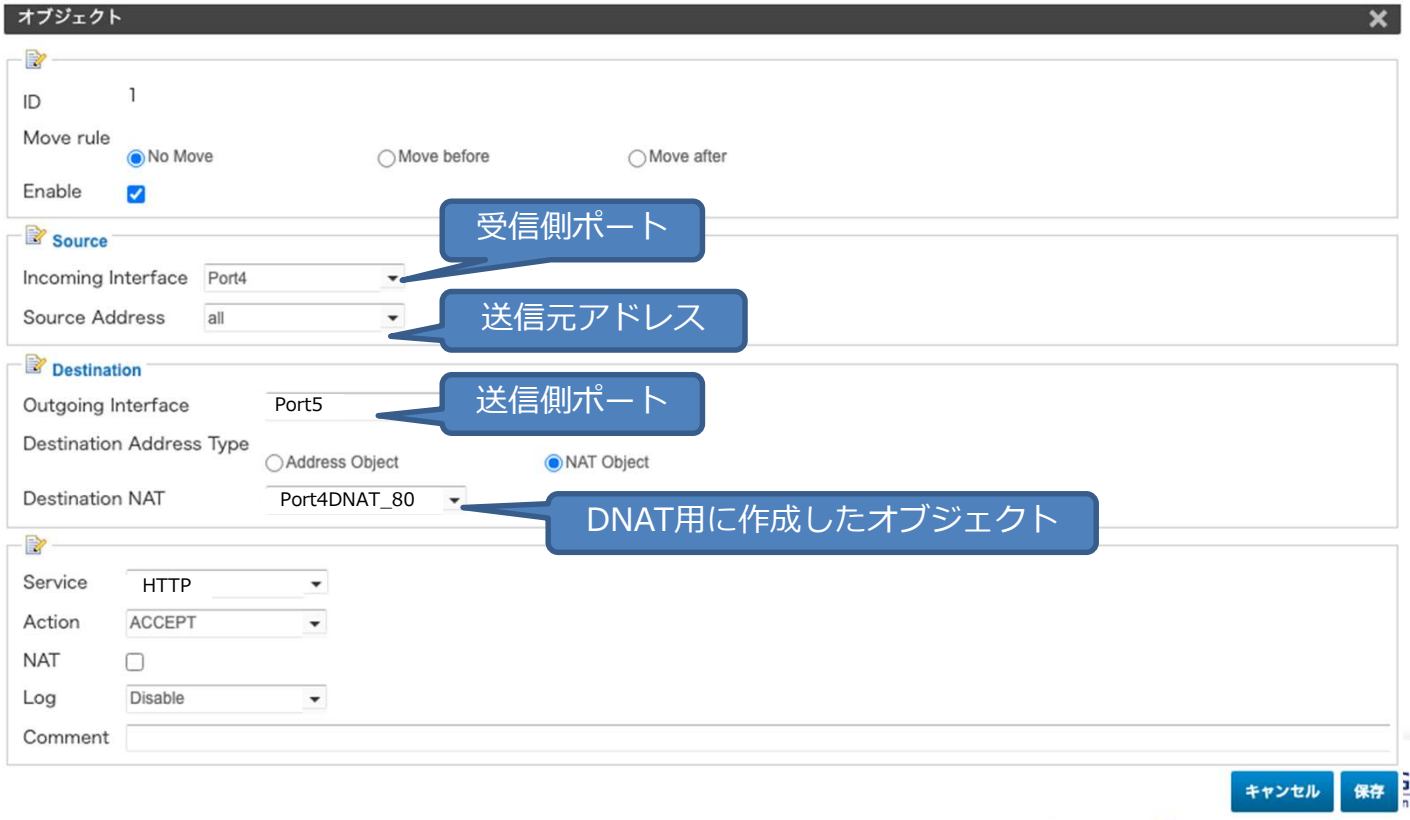
画面右側の「コンフィグ」をクリックします。

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⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

設定値を入力して、［保存］をクリックします。

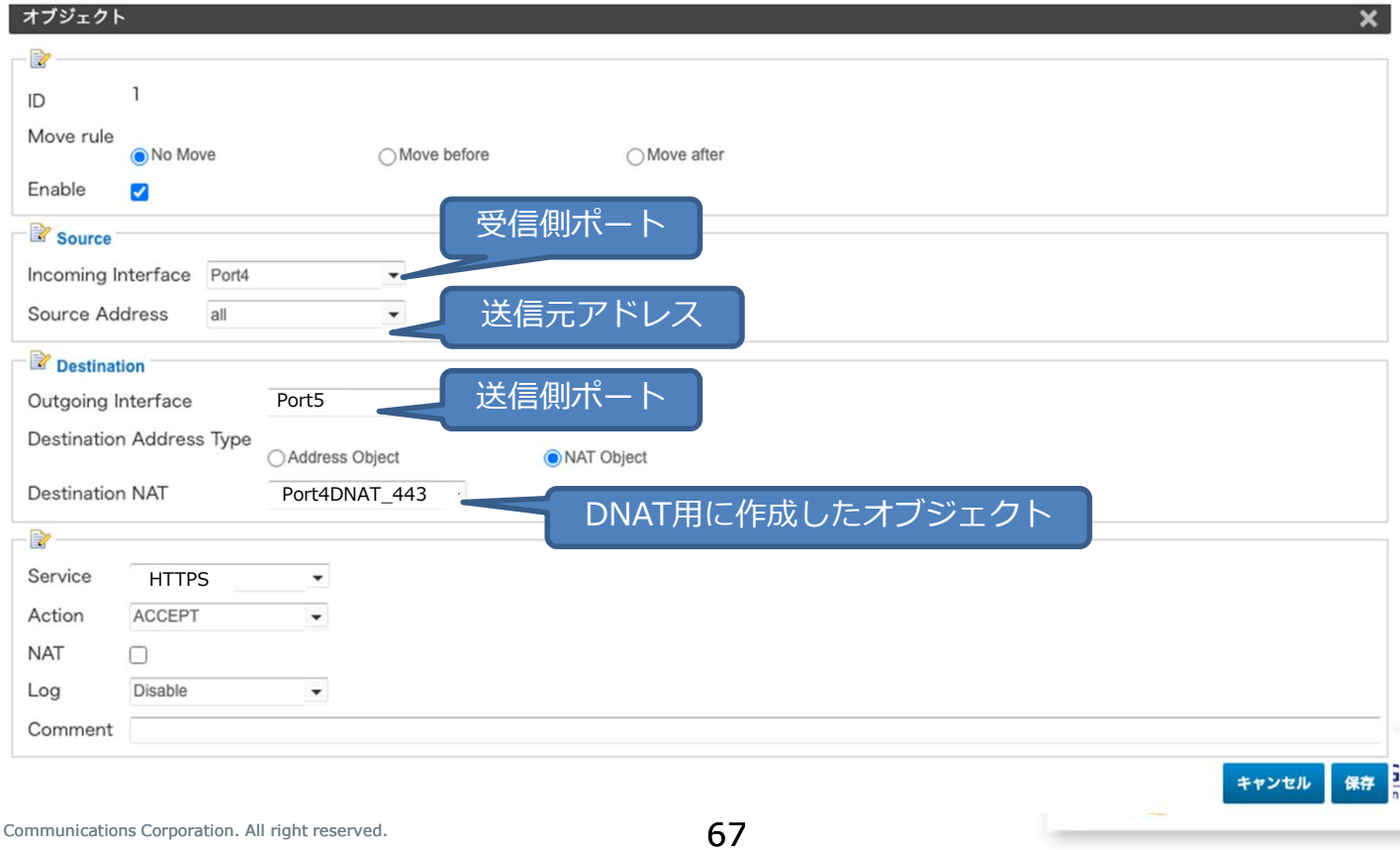
外部セグメント(Port4)の入力値は下記になります。
153.xx.xx.254の80番ポートへのアクセスの場合、172.16.100.100にDestination NATおよびACL設定するポリシー



手順⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

設定値を入力して、［保存］をクリックします。

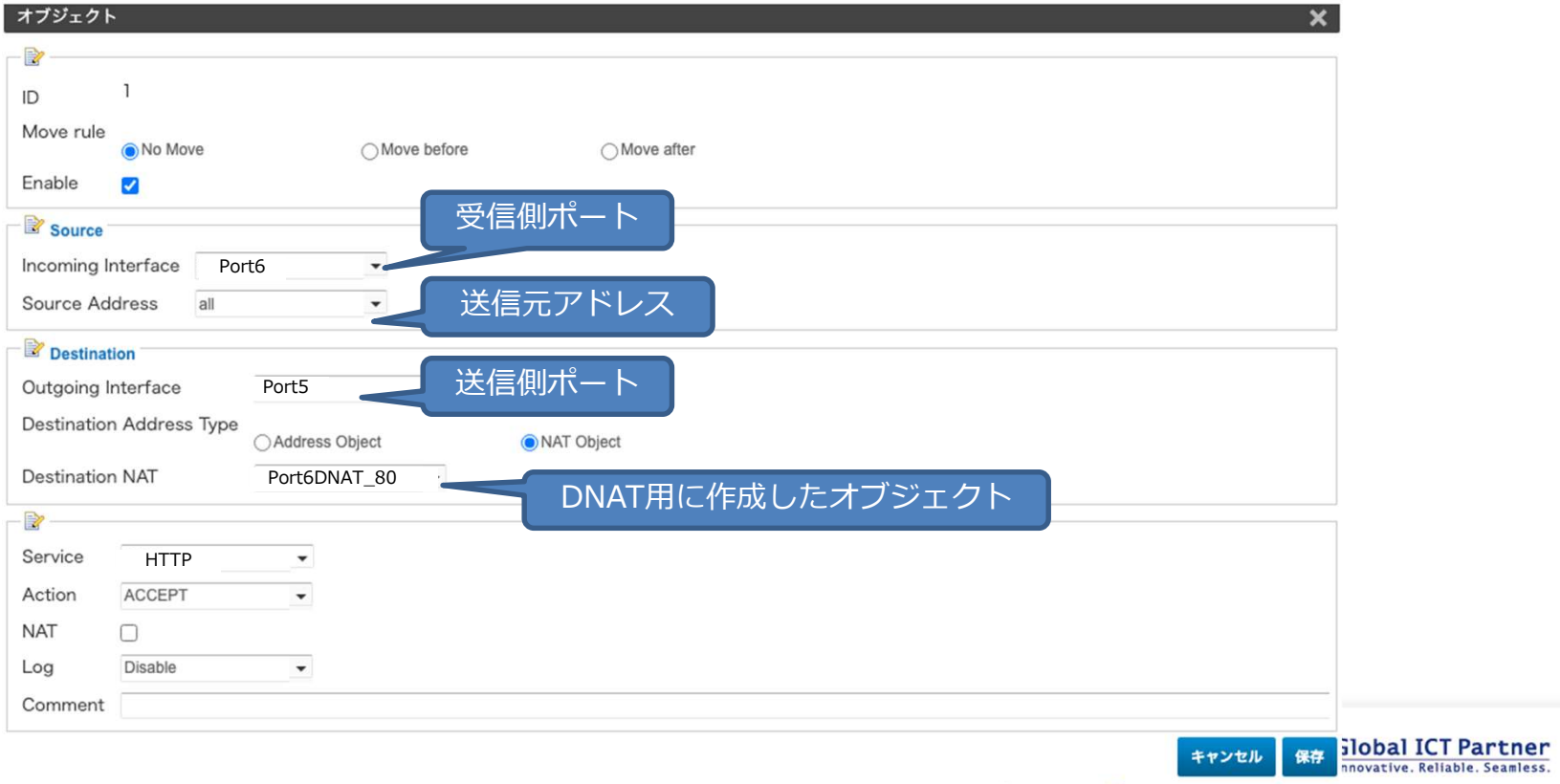
外部セグメント(Port4)の入力値は下記になります。
153.xx.xx.254の443番ポートへのアクセスの場合、172.16.100.200にDestination NATおよびACL設定するポリシー



手順⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

設定値を入力して、［保存］をクリックします。

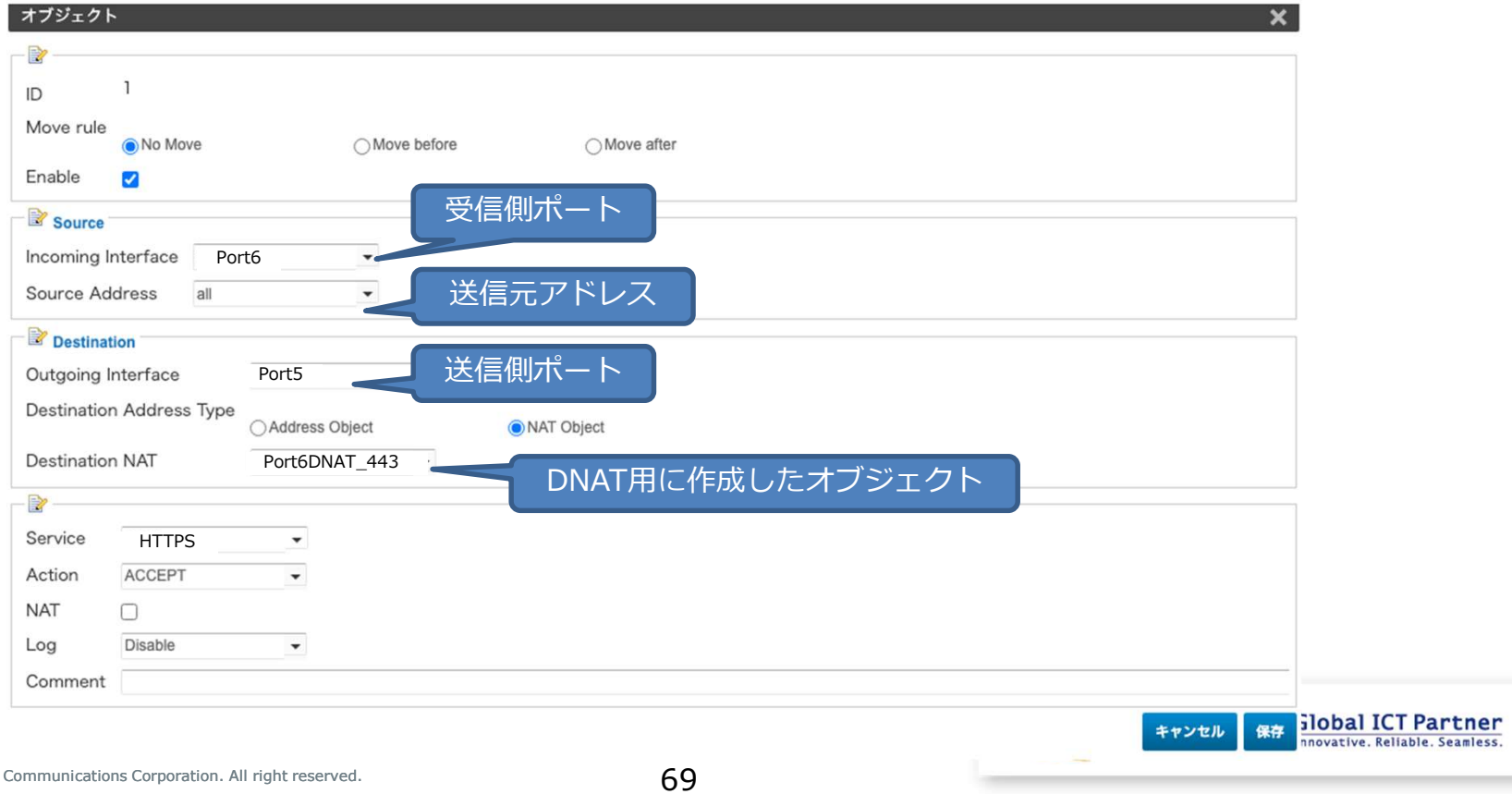
VPN-GWセグメント(Port6)の入力値は下記になります。
192.168.30.254の80番ポートへのアクセスの場合、172.16.100.100にDestination NATおよびACL設定するポリシー



手順⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

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⑨-4 M-FWの設定
(ファイアウォールポリシーの設定)

「変更の保存」をクリックして、設定をデバイスへ適用します。

手順⑩-1 LBの設定
(インターフェースの設定)

手順⑩-1 LBの設定
(インターフェースの設定)

下記リンクを参照の上、LBへロジカルネットワークの接続をお願いいたします。
https://ecl.ntt.com/documents/tutorials/rsts/LoadBalancer/instance/setting.html
コントロールパネル画面にログイン後、「ネットワーク」、「ロードバランサー」をクリックし、
対象のロードバランサーを選択ください。
その後「ロードバランサーインターフェース」タブを選択ください。

手順⑩-1 LBの設定
(インターフェースの設定)

対象のインターフェースから、「ロジカルネットワークの接続」をクリック。

「ロジカルネットワーク」にM-WFセグメントを選択、「IPアドレス」にインターフェースIPアドレスを入力。「ロジカルネットワークの接続」をクリック。(両方のLBに設定ください)

手順⑩-1 LBの設定
(インターフェースの設定)

VRRPの設定を行い、VRID(12)およびVIP(192.168.20.251)を設定ください。

手順⑪ 疎通確認

手順⑪ 疎通確認

お客様端末からhostsファイルを書き換え、M-FW経由の疎通確認を実施します。

Windowsの場合
C:¥Windows¥System32¥drivers¥etc¥hostsファイルを開き、以下を記載。

```
153.yyy.yyy.254        www.example.com
```

ブラウザから”WebサーバーのFQDN”へアクセスし、疎通に問題がないことを確認。
hostsファイルを再度開きコメントアウト。

```
#153.yyy.yyy.254       www.example.com
```

※社内網など、プロキシサーバーを経由した場合は正常に疎通確認ができない場合があります。
　疎通確認はInternet環境に直接つながる端末でご確認ください。

手順⑫ DNSサーバーの設定

手順⑫ DNSサーバーの設定

お客様管理のDNSサーバーのAレコードを、新しく用意したグローバルIPアドレスに書き換えください。

変更前

www.example.com 300 IN A 153.xxx.xxx.254

変更後

www.example.com 300 IN A 153.yyy.yyy.254

※DNS TTLの設定値により、伝搬に時間を要する場合がございます。
事前にTTLの値を小さく(300s)設定ください。

手順⑬ LBの設定
(デフォルトルート変更)

手順⑬ LBの設定
(デフォルトルート変更)

ロードバランサーから該当ロードバランサーを選択し、「ロードバランサーの編集」を選択。

デフォルトゲートウェイをM-FW(Port5)のアドレスに変更し、「ロードバランサーの編集」を選択

手順⑭ vFW利用環境の削除

手順⑭ vFW利用環境の削除

vFWが利用しているロジカルネットーワーク、VPN-GW、Internet-GWおよびvFWを削除ください。