

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

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。

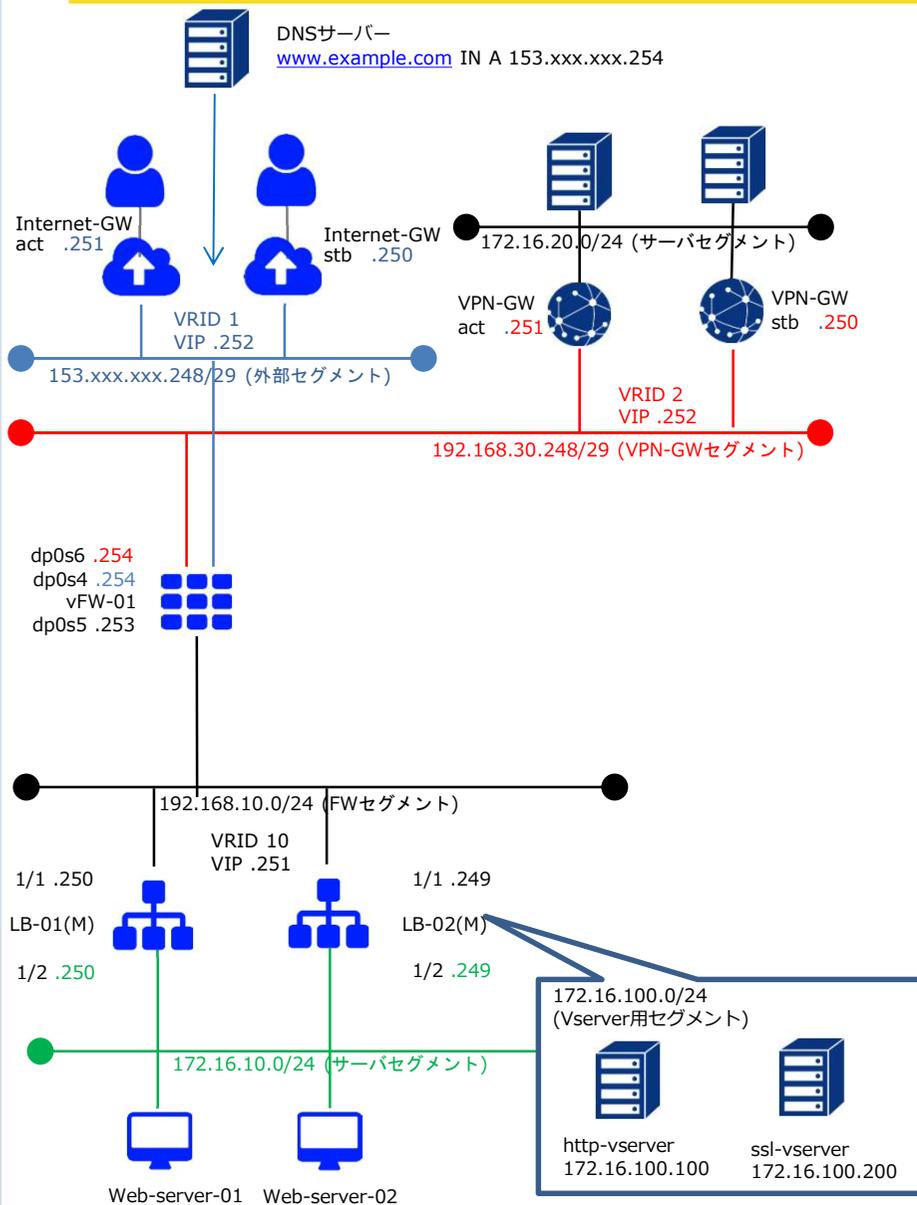
※事前検証を行ってから移行を実施ください。

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。

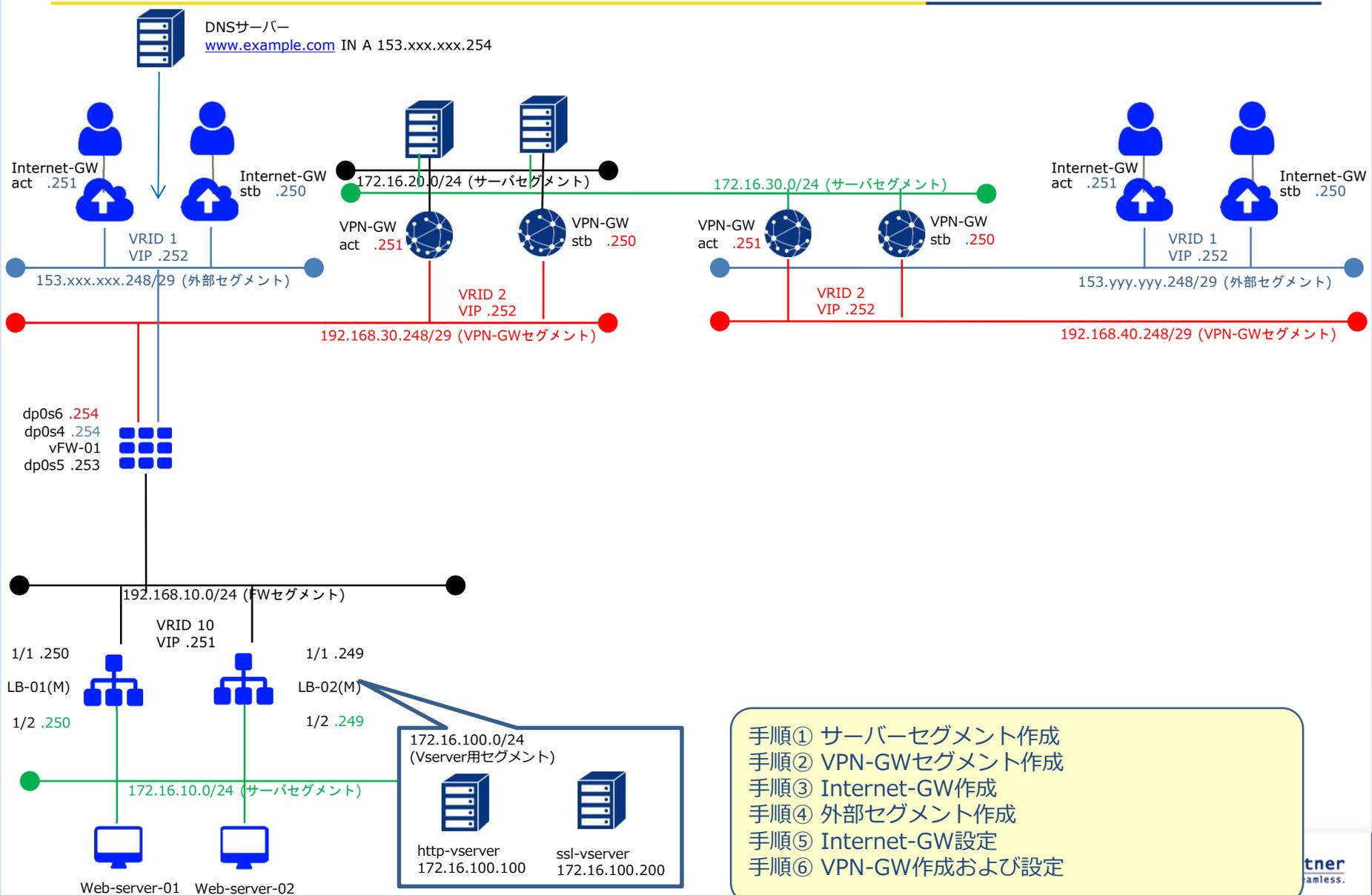
構成および移行フロー

移行前構成 (vFW構成)



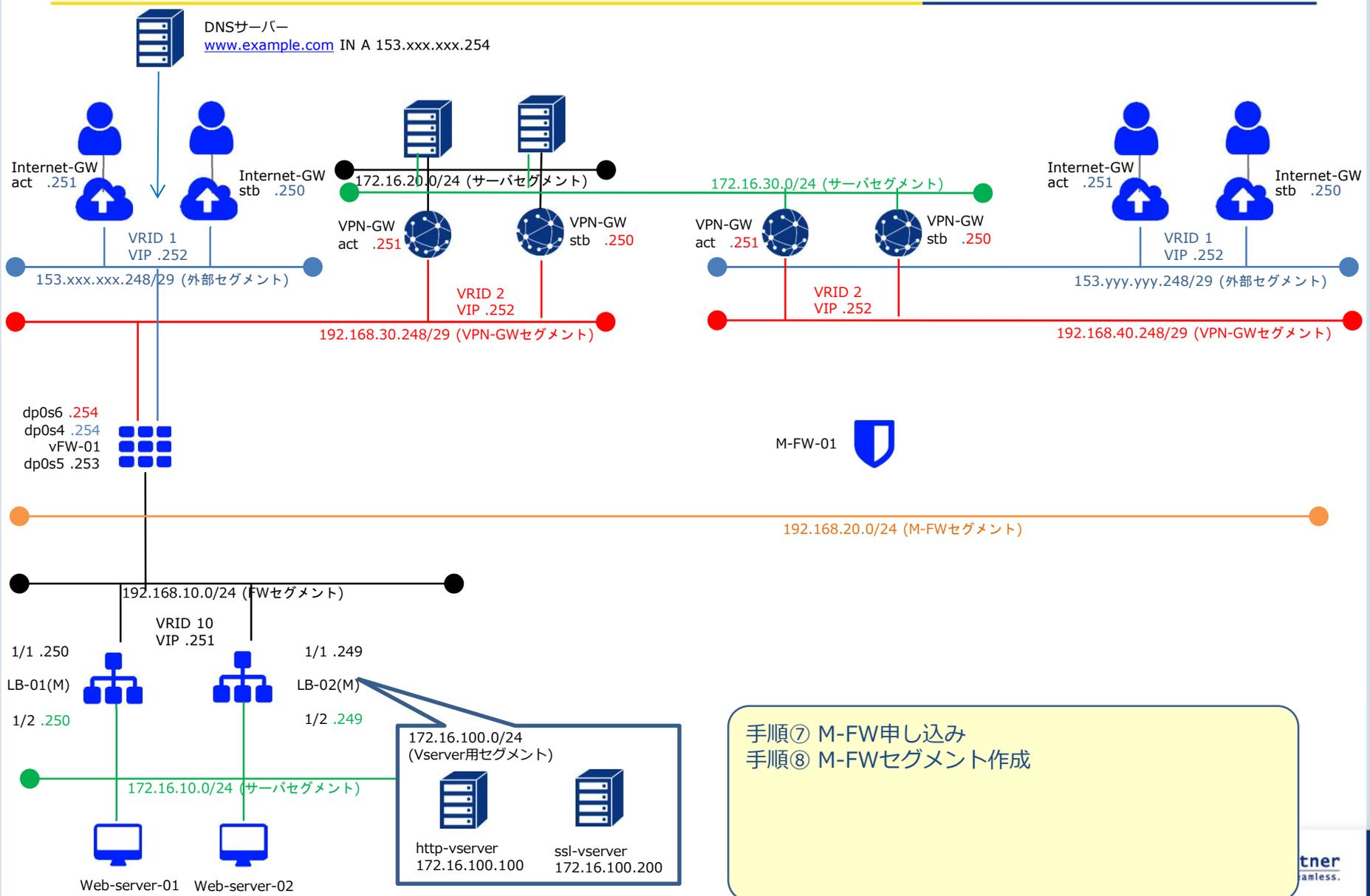
- vFWルールは外部セグメントからは基本全て拒否し、特定のHTTP/HTTPSアクセスのみ許可。
- 外部セグメントからvFWのグローバルIPにアクセスをDNAT変換でバーチャルサーバのIPに変換します。
- LBの内部に"別のセグメント"でバーチャルサーバを設定しておきます。

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

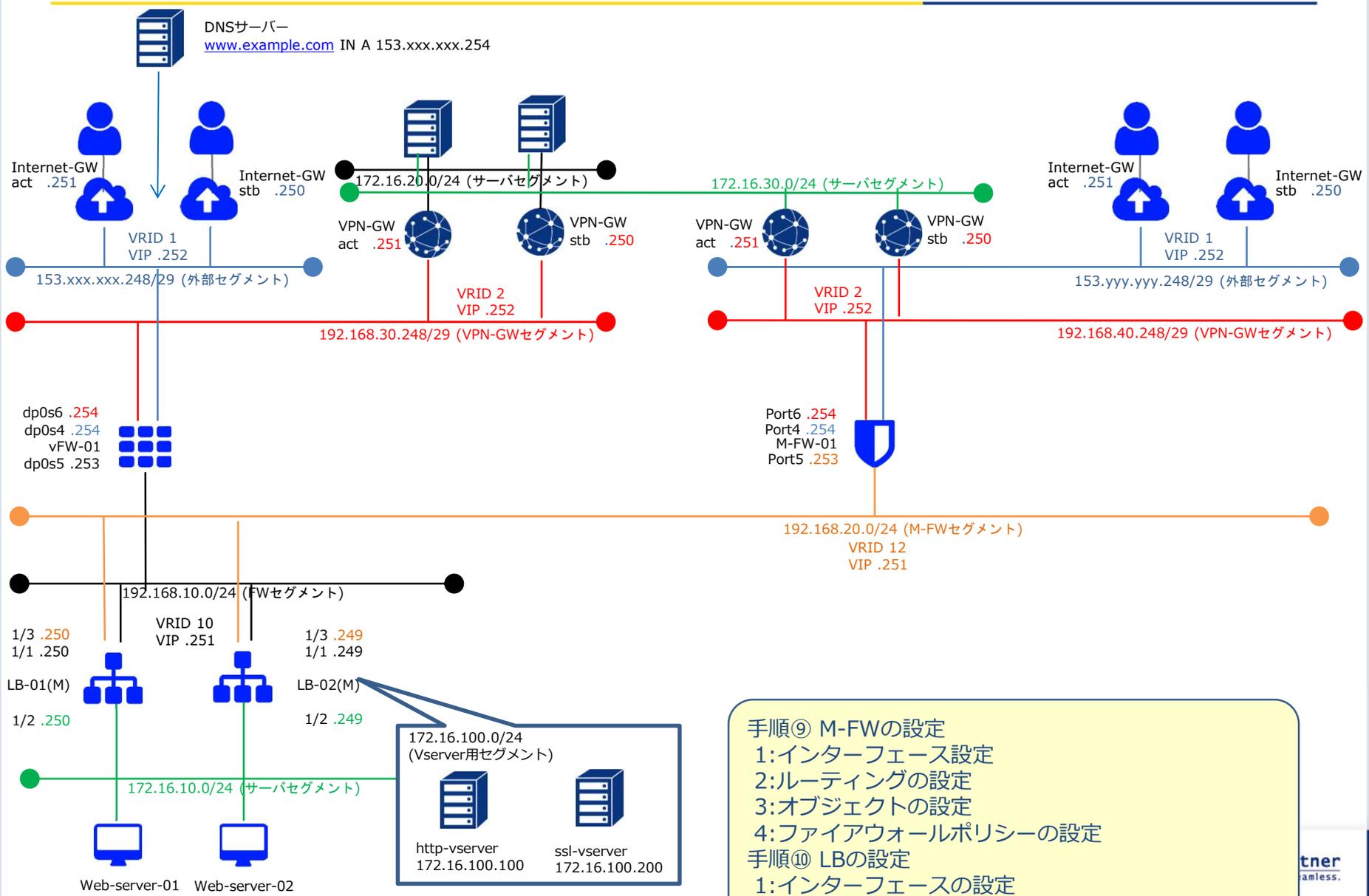
移行時構成②



手順⑦ M-FW申し込み
 手順⑧ M-FWセグメント作成

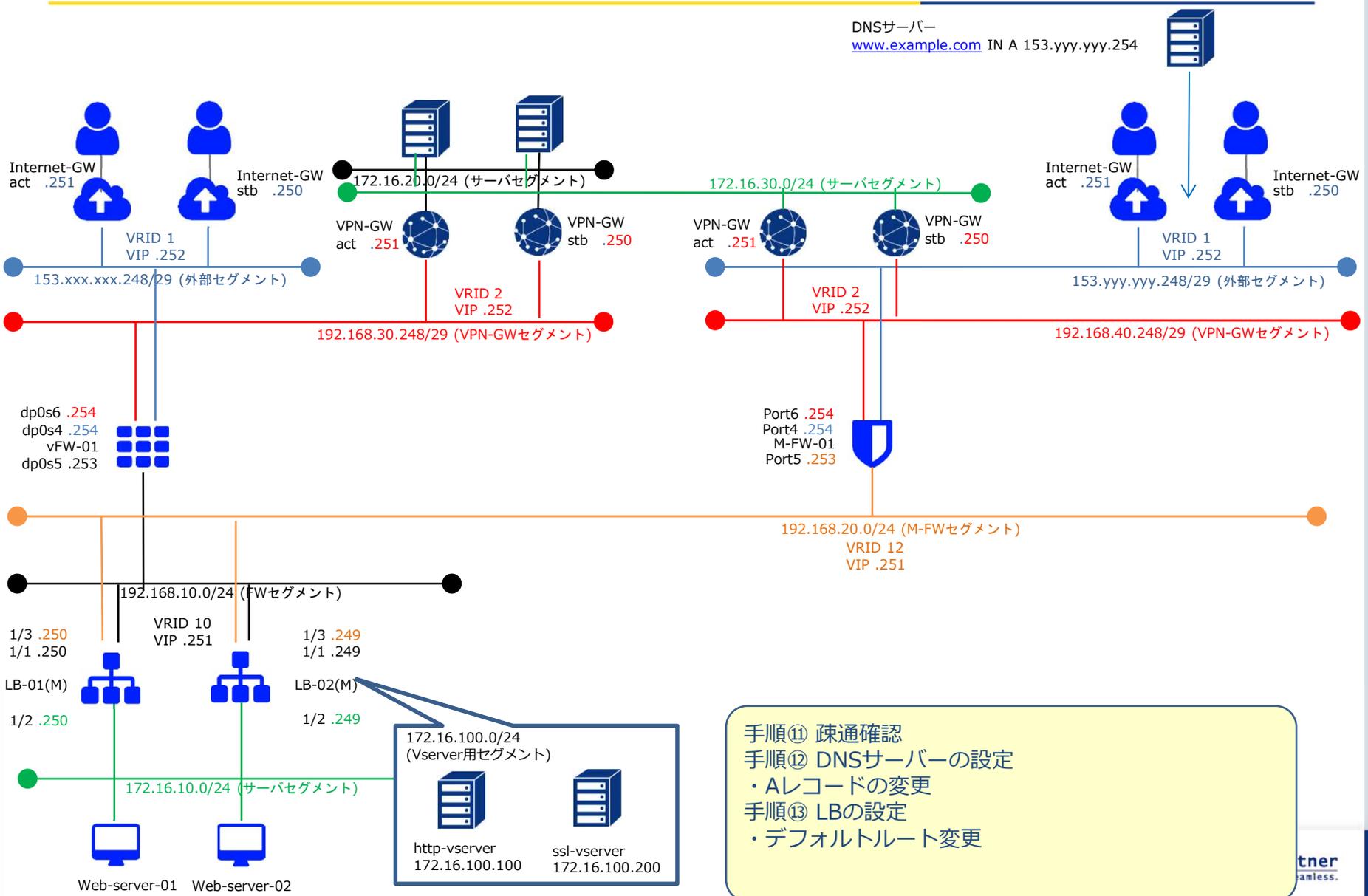


移行時構成③



- 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

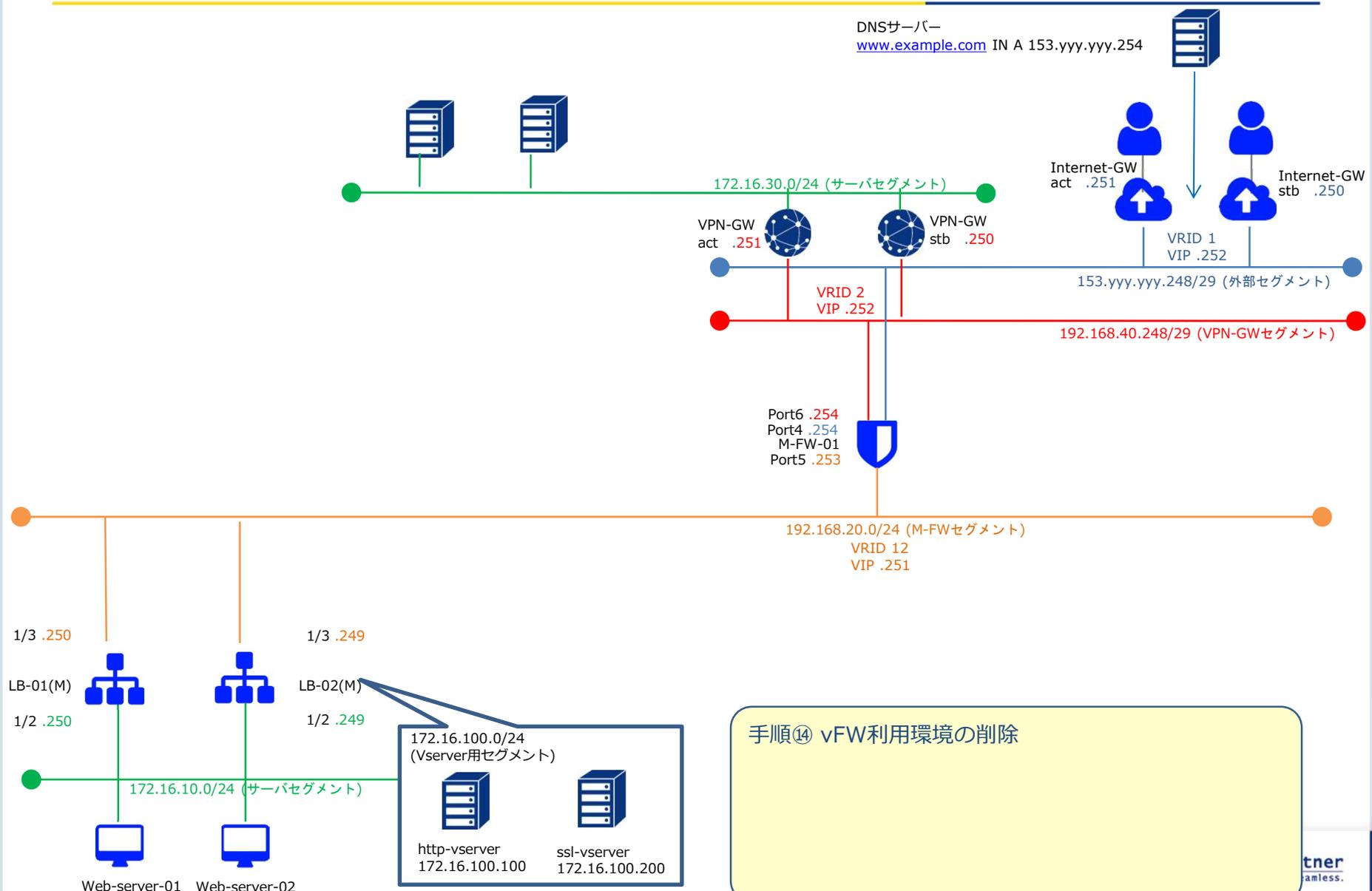
移行時構成④



- 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。

ロジカルネットワーク

		フィルター	+	ロジカルネットワークの作成	ロジカルネットワークの削除
<input type="checkbox"/> 名前	割当てサブネット	管理状態	プレーン	ステータス	アクション
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼

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。
- ・サブネットタブから、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。

ロジカルネットワークの作成

ロジカルネットワークの作成

ロジカルネットワーク名
vpn_seg

サブネット

サブネットの詳細

新しいロジカルネットワークを作成できます。合わせて、このロジカルネットワークに割り当てるサブネットを次のパネルで作成できます。

ブレン

データ用

ロジカルネットワークの説明

ロジカルネットワークのタグ

管理状態

UP

取り直し

戻る

次へ

ロジカルネットワークの作成

ロジカルネットワークの作成

サブネット

サブネットの詳細

サブネット名

新しいロジカルネットワークに割り当てるサブネットを作成します。この場合、「ネットワークアドレス」を指定する必要があります。

ネットワークアドレス

192.168.40.248/29

ゲートウェイIP

192.168.40.252

ゲートウェイなし

取り直し

戻る

次へ

ロジカルネットワークの作成

ロジカルネットワークの作成

サブネット

サブネットの詳細

DHCP 有効

サブネットの追加属性を指定します。

IP アドレス割り当てルール

DNS サーバー

NTP サーバー

追加のルーティング

サブネットの説明

サブネットのタグ

取り直し

戻る

ロジカルネットワークの作成



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/サーバー 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



インターネット接続ゲートウェイ



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。

インターネットゲートウェイの作成

名前

説明

説明:
インターネットゲートウェイを作成するためのパラメータを指定します。

インターネットサービス*

Internet-Service-01

QoSオプション*

10Mbps-BestEffort:(type=best effort, bandw

取り消し

インターネットゲートウェイの作成

手順③ Internet-GW作成

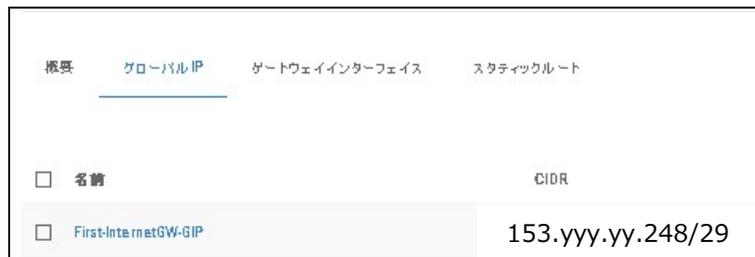
作成したインターネットGWを選択し、「グローバルIP」タブから「グローバルIPの追加」をクリック。



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。

ロジカルネットワーク

<input type="checkbox"/> 名前	割当てサブネット	管理状態	プレーン	ステータス	アクション
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼

フィルター

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。
- ・サブネットタブから、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。

ロジカルネットワークの作成

ロジカルネットワーク

inet_seg

次へ

ロジカルネットワークの作成

サブネット

153.yyy.yyy.248/29

153.yyy.yyy.252

次へ

ロジカルネットワークの作成

サブネットの詳細

DHCP 有効

ロジカルネットワークの作成

次へ



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ースの追加」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ースの追加」をクリック

ゲートウェイインターフェースの追加

名前

説明

説明:
ゲートウェイインターフェース追加のためのパラメータを指定します。

接続ロジカルネットワーク*

inet_seg_3 (153.153.140.80/29)

ゲートウェイIPv4アドレス*

153.yyy.yyy.252

プライマリデバイスIPv4アドレス*

153.yyy.yyy.251

セカンダリデバイスIPv4アドレス*

153.yyy.yyy.250

VRRPグループID*

1

取り消し

ゲートウェイインターフェースの追加

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

The 'Add Static Route' dialog box is shown. It has a title bar with a close button. The form contains the following fields and buttons:

- 名前** (Name): An empty text input field.
- 説明** (Description): An empty text input field.
- 宛先** (Destination): A text input field containing '153.yyy.yyy.248/29'.
- ネクストホップ** (Next Hop): A text input field containing '153.yyy.yyy.254'.
- 説明:** (Description): A text area containing the text: 'インターネットゲートウェイに対するスタティックルート追加のためのパラメータを指定します。' (Specify parameters for adding a static route to the Internet gateway.)
- 取り消し** (Cancel): A button.
- スタティックルートの追加** (Add Static Route): A button, highlighted with a red box.

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

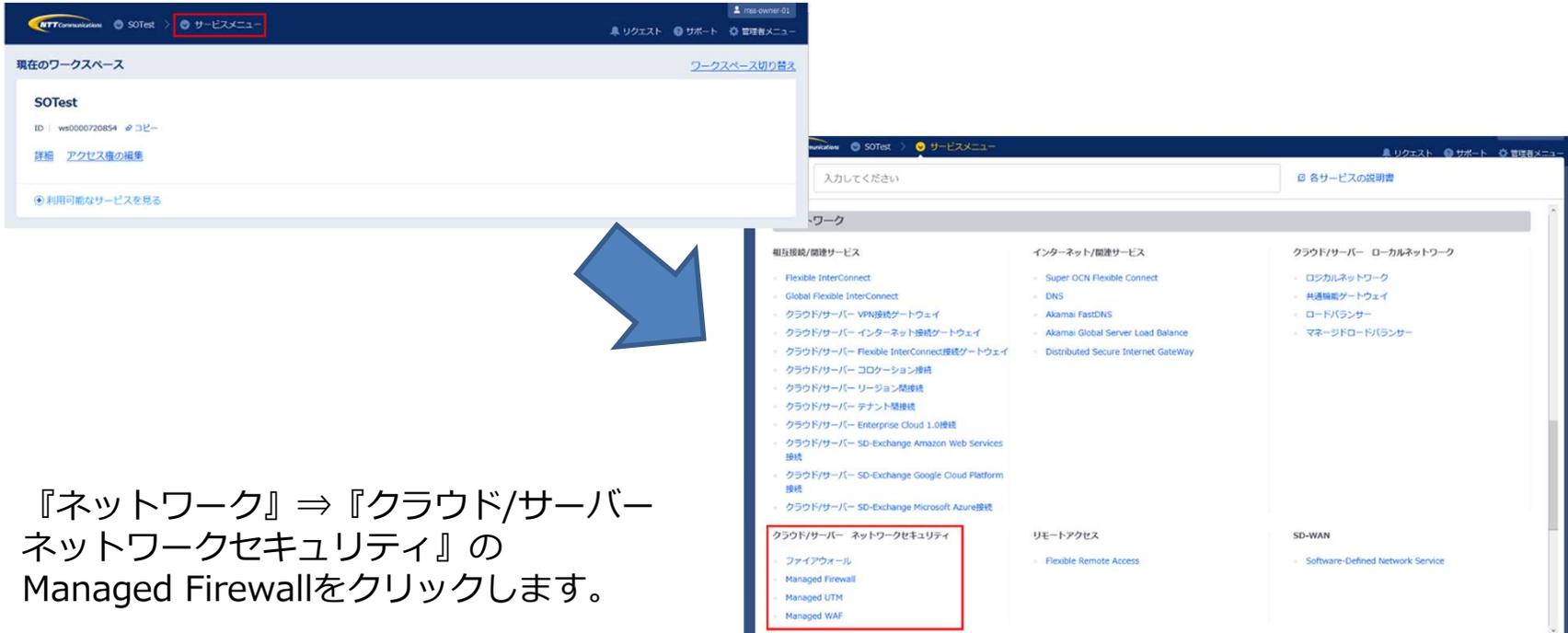
手順⑦ M-FW申し込み

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。



現在のワークスペース

SOTest

ID : ws0000720854 @ コピー

詳細 アクセス権の編集

利用可能なサービスを見る

サービスメニュー

入力してください

各サービスの説明書

ワーク

- 相互接続/関連サービス
 - Flexible InterConnect
 - Global Flexible InterConnect
 - クラウド/サーバー VPN接続ゲートウェイ
 - クラウド/サーバー インターネット接続ゲートウェイ
 - クラウド/サーバー Flexible InterConnect接続ゲートウェイ
 - クラウド/サーバー コロケーション接続
 - クラウド/サーバー リージョン間接続
 - クラウド/サーバー テナント間接続
 - クラウド/サーバー Enterprise Cloud 1.0接続
 - クラウド/サーバー SD-Exchange Amazon Web Services 接続
 - クラウド/サーバー SD-Exchange Google Cloud Platform 接続
 - クラウド/サーバー SD-Exchange Microsoft Azure接続
- クラウド/サーバー ネットワークセキュリティ
 - ファイアウォール
 - Managed Firewall
 - Managed UTM
 - Managed WAF
- インターネット/関連サービス
 - Super OCN Flexible Connect
 - DNS
 - Akamai FastDNS
 - Akamai Global Server Load Balance
 - Distributed Secure Internet GateWay
- リモートアクセス
 - Flexible Remote Access
- クラウド/サーバー ローカルネットワーク
 - ロジカルネットワーク
 - 共通機能ゲートウェイ
 - ロードバランサー
 - マネージドロードバランサー
- SD-WAN
 - Software-Defined Network Service

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



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。

ロジカルネットワーク

		フィルター	+	ロジカルネットワークの作成	ロジカルネットワークの削除
<input type="checkbox"/> 名前	割当てサブネット	管理状態	プレーン	ステータス	アクション
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼
<input type="checkbox"/>		UP	データ用	稼働中	ロジカルネットワークの編集 ▼

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。
- ・サブネットタブから、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。

ロジカルネットワークの作成

ロジカルネットワークの作成

ロジカルネットワーク名
logical1

サブネット

サブネットの詳細

新しいロジカルネットワークを作成できます。合わせて、このロジカルネットワークに割り当てるサブネットを次のパネルで作成できます。

ブレン

データ用

ロジカルネットワークの説明

ロジカルネットワークのタブ

管理状態

UP

取り直し

戻る

次へ

ロジカルネットワークの作成

ロジカルネットワーク

サブネット

サブネットの詳細

サブネット名

新しいロジカルネットワークに割り当てるサブネットを作成します。この場合、「ネットワークアドレス」を指定する必要があります。

ネットワークアドレス

192.168.20.0/24

ゲートウェイIP

192.168.20.253

ゲートウェイなし

取り直し

戻る

次へ

ロジカルネットワークの作成

ロジカルネットワーク

サブネット

サブネットの詳細

DHCP 有効

サブネットの追加属性を設定します。

IP アドレス割り当てプール

192.168.20.1,192.168.20.100

DNS サーバー

NTP サーバー

追加のルーティング

サブネットの説明

サブネットのタブ

取り直し

戻る

ロジカルネットワークの作成



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。

The screenshot shows the SDPF portal interface. In the top navigation bar, the 'サービスメニュー' (Service Menu) tab is highlighted with a red box. A blue arrow points from this tab to a larger view of the 'サービスメニュー' page. In this view, the 'ネットワーク' (Network) section is expanded, and the 'クラウド/サーバー ネットワークセキュリティ' (Cloud/Server Network Security) sub-section is highlighted with a red box. Under this sub-section, the following options are listed: 'ファイアウォール' (Firewall), 'Managed Firewall', 'Managed UTM', and 'Managed WAF'. The 'Managed Firewall' option is the target of the instruction.

『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。

● PORT_MNGT_NCS172
ステータス 成功
メッセージ Device 172 Backup completed successfully. Backup Status : ENDED Backup Message : BACKUP processed Backup Revisi...

Get Network Info Manage Interfaces Get VNC Console Stop/Start UTM

ステータス
ライブコンソール
↑ 詳細
Expand All

[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。

タスクステータス

ステータス	開始時刻	終了時刻	詳細
Get Network Info	2020-08-25 05:30:09	2020-08-25 05:30:11	Get Network Info successful

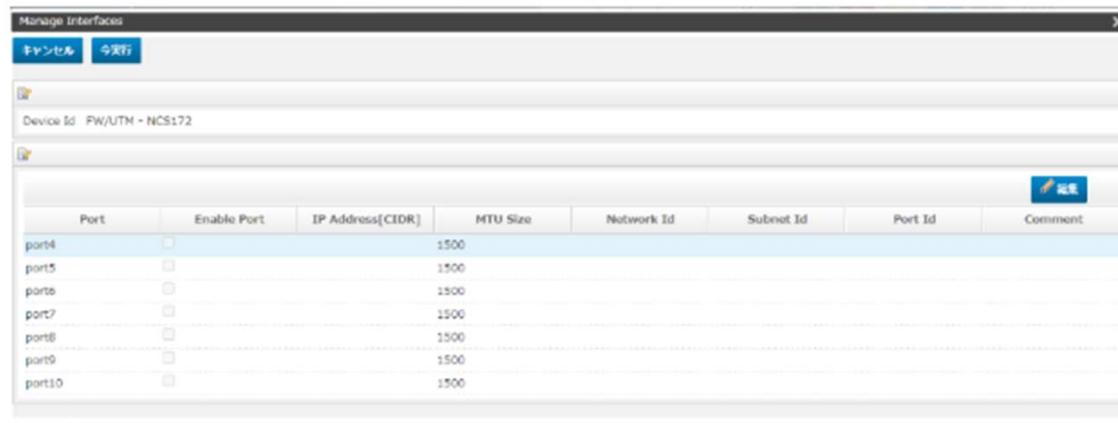
クローズ

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。

キャンセル	保存
	
Port	port4
Enable Port	<input checked="" type="checkbox"/>
IP Address[<small>CIDR</small>]	153.XXX.XXX.254/29 Port4に付与するIPアドレス
MTU Size	1500
Network Id	<input type="text"/>
Subnet Id	153.XXX.XXX.248/29 Port4に接続するネットワークアドレス
Port Id	<input type="text"/>
Comment	<input type="text"/>

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。

キャンセル 保存

📄

Port	Port5
Enable Port	<input checked="" type="checkbox"/>
IP Address[<small>CIDR</small>]	<input type="text" value="192.168.10.253/24"/>
MTU Size	<input type="text" value="1500"/>
Network Id	<input type="text" value="logical1"/>
Subnet Id	<input type="text" value="192.168.10.0/24"/>
Port Id	<input type="text"/>
Comment	<input type="text"/>

Port4に付与するIPアドレス

Port4に接続するネットワークアドレス

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。

キャンセル 保存

📄

Port	port6
Enable Port	<input checked="" type="checkbox"/>
IP Address[<small>CIDR</small>]	192.168.30.254/29
MTU Size	1500
Network Id	vpn_seg
Subnet Id	192.168.30.248/29
Port Id	
Comment	

Port6に付与するIPアドレス

Port6に接続するネットワークアドレス

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。

Manage Interfaces

キャンセル 今実行

Device Id FW/UTM - NCS172

編集

Port	Enable Port	IP Address[CIDR]	MTU Size	Network Id	Subnet Id	Port Id	Comment
port4	<input checked="" type="checkbox"/>	10.1.1.254/24	1500	test1	10.1.1.0/24		
port5	<input type="checkbox"/>		1500				
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。

タスクステータス	開始時刻	終了時刻	詳細
Verify IP Address, MTU inputs ↓	2020-08-24 05:49:23	2020-08-24 05:49:26	IP Address inputs verified successfully.

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。

ステータス	開始時刻	終了時刻	詳細
Stop the UTM	2016-07-11 22:32:42	2016-07-11 22:32:46	Device 724 shutdown successfully.
↓			
Get a Token	2016-07-11 22:32:46	2016-07-11 22:32:46	Token created successfully. Token Id : 08edfc958d894aa69088155cc26005bc
↓			
Verify IP Address inputs	2016-07-11 22:32:46	2016-07-11 22:35:47	IP Address inputs verified successfully.
↓			
Detach Ports	2016-07-11 22:35:47	2016-07-11 22:36:52	Ports detached successfully from the Server bb348914-cb3b-467e-b9af-0bf897ce38ed.
↓			
Create Ports	2016-07-11 22:36:52	2016-07-11 22:36:58	Ports created successfully. Port Id : f4f775e8-1012-4937-a5dc-e02eeec4a055 Port Id : 09eeeb69-17bc-40bc-8ae4-330b5d55024e Port Id : 8010b923-2c79-4ed3-80d3-9317d7c2ab1 Port Id : c85d7b3b-3e3c-44a3-97b5-829fc138ad91 Port Id : 83a3d462-0262-4a8a-3cdf-cef8ce43794f Port Id : e604d97f-6e7b-4f97-94a5-a832004a0e0e Port Id : 2a72235c-ab1f-4af0-a6a2-149bf2c26129
↓			
Attach Ports	2016-07-11 22:36:58	2016-07-11 22:37:11	Ports attached successfully to the Server bb348914-cb3b-467e-b9af-0bf897ce38ed.
↓			
Start the UTM	2016-07-11 22:37:11	2016-07-11 22:37:26	Openstack Server bb348914-cb3b-467e-b9af-0bf897ce38ed started successfully. Server Status : ACTIVE Task State : - Power State : Running
↓			
Wait for UTM Ping reachability from MSA	2016-07-11 22:37:26	2016-07-11 22:38:10	IP Address 100.65.96.31 is now reachable from MSA. PING Status : OK
↓			
Update UTM	2016-07-11 22:38:10	2016-07-11 22:38:39	Ports updated successfully on Fortigate Device 724.

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。

The image shows two screenshots of the SDPF portal. The top screenshot shows the 'Service Menu' (サービスメニュー) selected in the navigation bar. A blue arrow points from this menu to the bottom screenshot. The bottom screenshot shows the 'Network Security' (ネットワークセキュリティ) section under 'Cloud/Server' (クラウド/サーバー), with 'Managed Firewall' (Managed Firewall) highlighted in a red box.

『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。

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

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。

オブジェクト

ID	1
Destination IP	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	192.168.10.251
Interface	port4
Comment	

WebServer宛の通信

送信先Gateway address(LBの上側VIP)

送信先Port

キャンセル 保存

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。

オブジェクト

ID	1
Destination IP	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	153.xxx.xxx.252
Interface	Port4
Comment	

Internet GW(デフォルトゲートウェイ)のVIP

送信先Port

キャンセル 保存

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。

オブジェクト ✕

ID	1	VPN-GW先サーバーセグメント宛の通信
Destination IP	172.16.20.0	
Subnet Mask	0.0.0.0	
Gateway	192.168.30.252	送信先アドレス(VPN-GWのVIP)
Interface	Port6	送信先Port
Comment		

キャンセル 保存

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。

The image shows two screenshots of the SDPF portal. The top screenshot shows the 'Service Menu' (サービスメニュー) tab selected in the navigation bar. The bottom screenshot shows the 'Network Security' (ネットワークセキュリティ) section under 'Cloud/Server' (クラウド/サーバー), with 'Managed Firewall' (Managed Firewall) highlighted in a red box. A blue arrow points from the 'Service Menu' tab in the top screenshot to the 'Network Security' section in the bottom screenshot.

『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。

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⑨-3 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。

オブジェクト

NAT Name	<input type="text"/>
External IP Address	153.xx.xx.254
Mapped IP Address	0.0.0.0
External Interface	Port4
Port Forward	<input checked="" type="checkbox"/>
Protocol	TCP
External Service Port	80
Mapped Port	80
Comment	<input type="text"/>

キャンセル 保存

M-FWの受信側VIP

http-vserverのアドレス

受信側ポート

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。

オブジェクト

NAT Name	<input type="text"/>	
External IP Address	153.xx.xx.254	M-FWの受信側VIP
Mapped IP Address	0.0.0.0	ssl-vserverのアドレス
External Interface	Port4	
Port Forward	<input checked="" type="checkbox"/>	受信側ポート
Protocol	TCP	
External Service Port	443	
Mapped Port	443	
Comment	<input type="text"/>	

キャンセル 保存

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。

オブジェクト

NAT Name	Port6DNAT_80	M-FWの受信側VIP
External IP Address	192.168.30.254	
Mapped IP Address	0.0.0.0	http-vserverのアドレス
External Interface	Port6	
Port Forward	<input checked="" type="checkbox"/>	受信側ポート
Protocol	TCP	
External Service Port	80	
Mapped Port	80	
Comment		

キャンセル 保存

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。

The screenshot shows a configuration window titled "オブジェクト" (Object). The fields are as follows:

NAT Name	Port6DNAT_443	M-FWの受信側VIP
External IP Address	192.168.30.254	ssl-vserverのアドレス
Mapped IP Address	0.0.0.0	
External Interface	Port6	受信側ポート
Port Forward	<input checked="" type="checkbox"/>	
Protocol	TCP	
External Service Port	443	
Mapped Port	443	
Comment		

At the bottom right, there are two buttons: "キャンセル" (Cancel) and "保存" (Save). The "保存" button is highlighted with a red box.

「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。

デバイスからの同期 **変更の保存** 変更の破棄

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。

The image shows two screenshots of the SDPF portal. The top screenshot shows the 'Service Menu' (サービスメニュー) tab selected in the navigation bar. The bottom screenshot shows the 'Network Security' (ネットワークセキュリティ) section under the 'Cloud/Server' (クラウド/サーバー) category, with 'Managed Firewall' (ファイアウォール) highlighted by a red box. A blue arrow points from the 'Service Menu' tab in the top screenshot to the 'Network Security' section in the bottom screenshot.

『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)

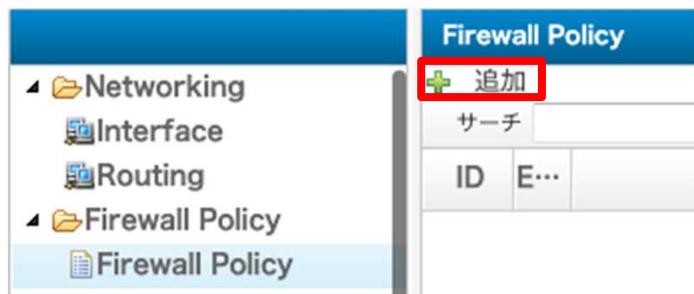
「デバイス」からいずれかのデバイスを右クリックします。



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

オブジェクト

ID 1

Move rule No Move Move before Move after

Enable

Source

Incoming Interface Port4

Source Address all

Destination

Outgoing Interface Port5

Destination Address Type Address Object NAT Object

Destination NAT Port4DNAT_80

Service

Service HTTP

Action ACCEPT

NAT

Log Disable

Comment

キャンセル 保存

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

The screenshot shows a configuration window titled "オブジェクト" (Object) with the following fields and callouts:

- ID:** 1
- Move rule:** No Move, Move before, Move after
- Enable:**
- Source:**
 - Incoming Interface:** Port4 (Callout: 受信側ポート)
 - Source Address:** all (Callout: 送信元アドレス)
- Destination:**
 - Outgoing Interface:** Port5 (Callout: 送信側ポート)
 - Destination Address Type:** Address Object, NAT Object
 - Destination NAT:** Port4DNAT_443 (Callout: DNAT用に作成したオブジェクト)
- Service:** HTTPS
- Action:** ACCEPT
- NAT:**
- Log:** Disable
- Comment:** (empty)

キャンセル

保存

Global ICT Partner
innovative. Reliable. Seamless.

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

オブジェクト

ID 1

Move rule No Move Move before Move after

Enable

Source

Incoming Interface Port6

Source Address all

Destination

Outgoing Interface Port5

Destination Address Type Address Object NAT Object

Destination NAT Port6DNAT_80

Service HTTP

Action ACCEPT

NAT

Log Disable

Comment

キャンセル 保存

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

The screenshot shows the 'オブジェクト' (Object) configuration window for a firewall policy. The configuration is as follows:

- ID:** 1
- Move rule:** No Move, Move before, Move after
- Enable:**
- Source:**
 - Incoming Interface:** Port6 (Callout: 受信側ポート)
 - Source Address:** all (Callout: 送信元アドレス)
- Destination:**
 - Outgoing Interface:** Port5 (Callout: 送信側ポート)
 - Destination Address Type:** Address Object, NAT Object
 - Destination NAT:** Port6DNAT_443 (Callout: DNAT用に作成したオブジェクト)
- Service:** HTTPS
- Action:** ACCEPT
- NAT:**
- Log:** Disable
- Comment:** (empty)

キャンセル

保存

Global ICT Partner
innovative. Reliable. Seamless.

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。

デバイスからの同期

変更の保存

変更の破棄

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。

名前	説明	スロット番号
Interface 1/1	-	1
Interface 1/2	-	2
Interface 1/3	-	3
Interface 1/4	-	4

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。

Interface 1/1	-	1	b7D2caDf-ec95-4fd1-862c-b3984b9398a5	192.168.11.249	-	稼働中	ロード バランサー インターフェイスの編集 ▼
Interface 1/2	-	2	4121D765-7f18-456d-a1De-Dd1D7a2Dd1c2	172.16.10.249	-	稼働中	ロード バランサー インターフェイスの編集 ▼
Interface 1/3	-	3	-	-	-	停止中	ロード バランサー インターフェイスの編集 ▼
Interface 1/4	-	4	-	-	-	停止中	ロード バランサー インターフェイスの編集 ▼ ロジカルネットワークの接続

4 件表示

「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)

ロジカルネットワークの接続

ロジカルネットワーク*

logical_M-fw-seg-50(1) 192.168.20.0/24

IPアドレス

192.168.20.249

説明:

ロード バランサー にロジカルネットワークを接続します。

ロード バランサー に既に接続されているロジカルネットワークは選択できません。

ロジカルネットワークの接続には、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。

ロジカルネットワークの接続時に指定するIPアドレス帯は、ロード バランサー 内部 で利用しているIPアドレス帯と重複しない値を指定してください。

重複した値の場合、操作がエラーとなり再作成が必要となる場合があります。

取り直し

ロジカルネットワークの接続

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。

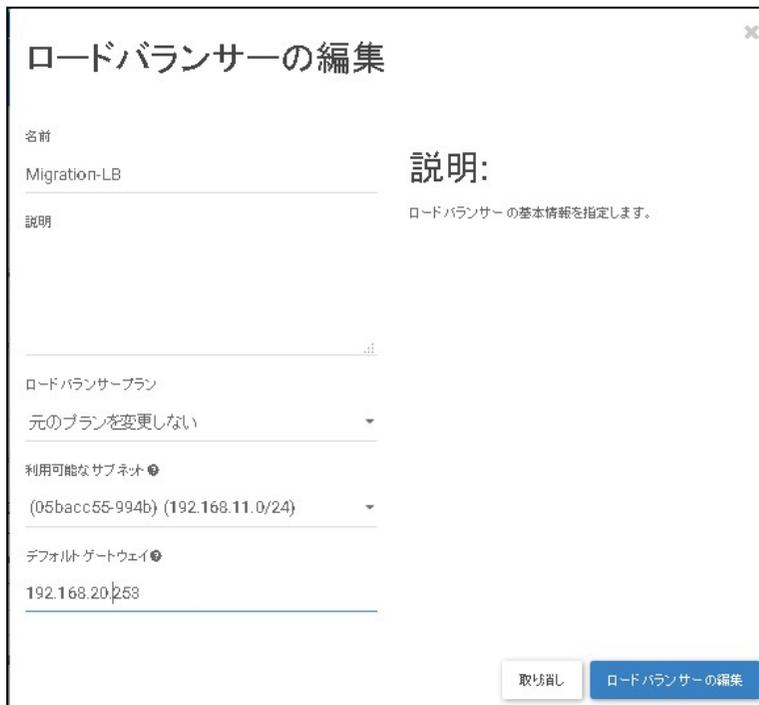
手順⑬ LBの設定 (デフォルトルート変更)

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

A screenshot of a dialog box titled 'ロードバランサーの編集' (Edit Load Balancer). The dialog contains the following fields and controls:

- 名前** (Name): Migration-LB
- 説明** (Description): 説明: ロードバランサーの基本情報を指定します。
- ロードバランサープラン** (Load Balancer Plan): 元のプランを変更しない
- 利用可能なサブネット** (Available Subnet): (05bacc55-994b) (192.168.11.0/24)
- デフォルトゲートウェイ** (Default Gateway): 192.168.20.253

At the bottom right of the dialog, there are two buttons: '取り消し' (Cancel) and 'ロードバランサーの編集' (Edit Load Balancer).

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ワーク、VPN-GW、Internet-GWおよびvFWを削除ください。