

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 (シングル構成版)

第3版

前提条件

前提条件

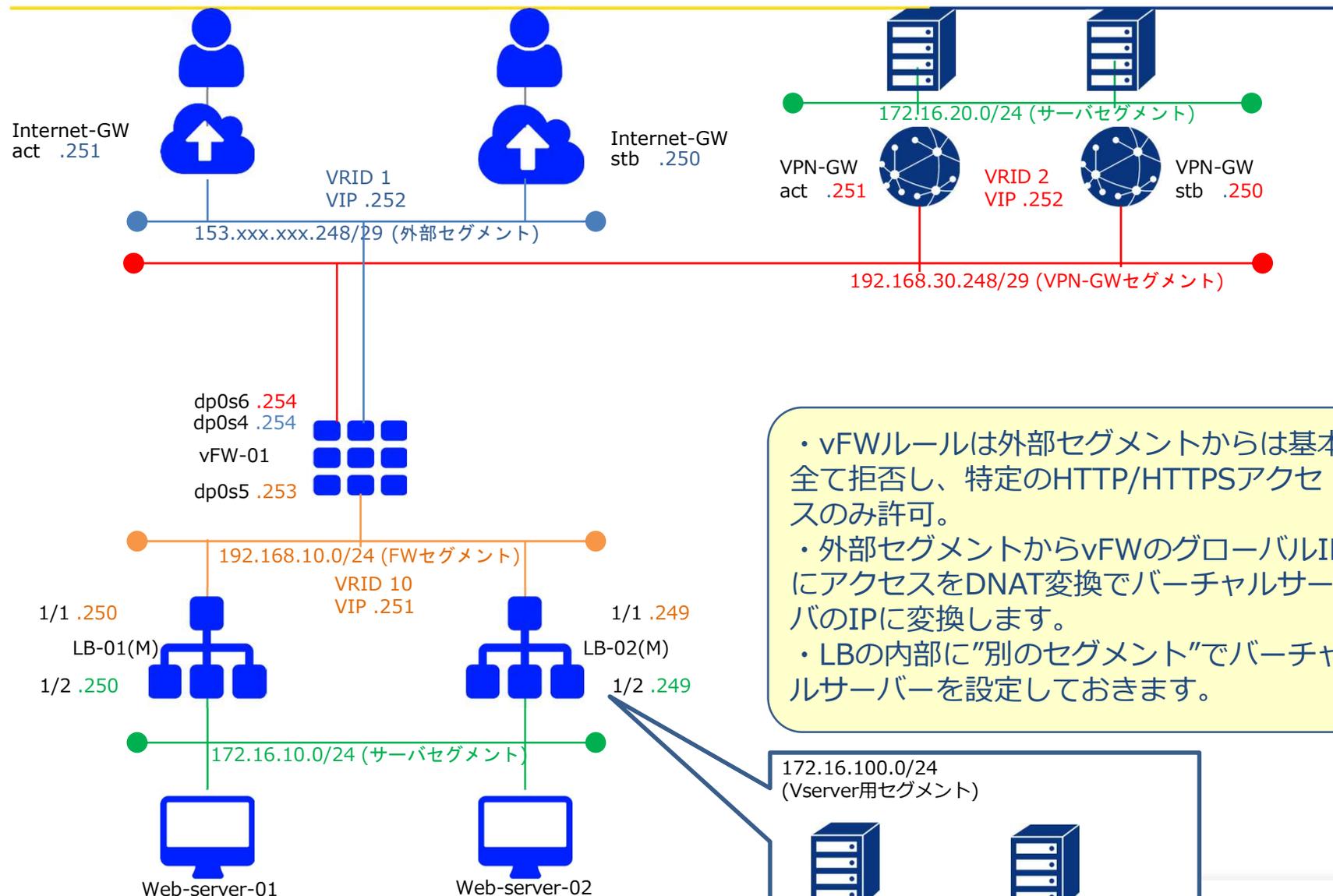
■ファイアウォール(vFW 5600 vRouter)(以下、vFW)からManaged Firewall(以下、M-FW)への交換によるマイグレ実施方法です。

- ・ Internet-GW, ロードバランサー, Webサーバーの設定変更(Routing変更等)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を設定しておきます。

172.16.100.0/24 (Vserver用セグメント)



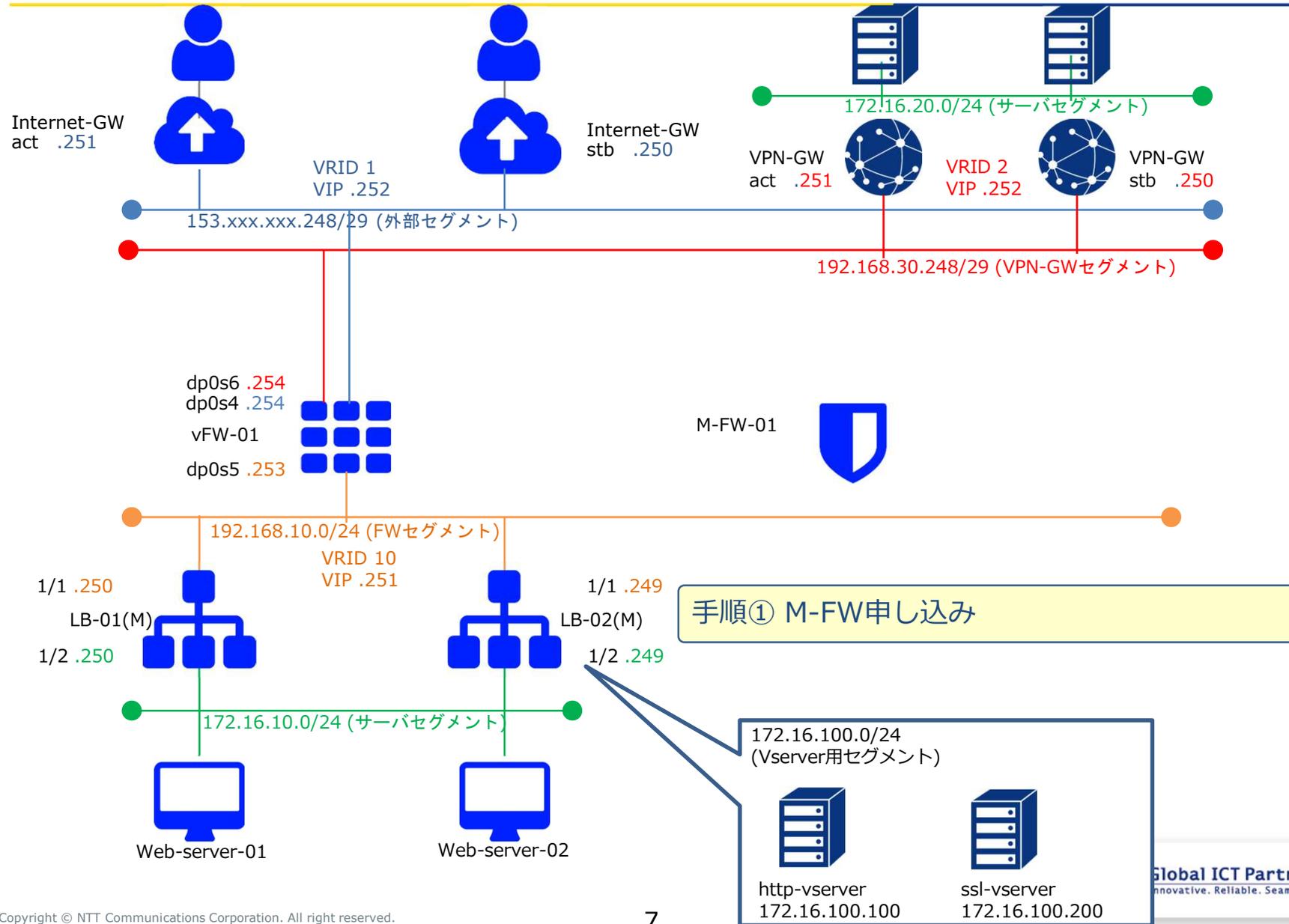
http-vserver
172.16.100.100



ssl-vserver
172.16.100.200

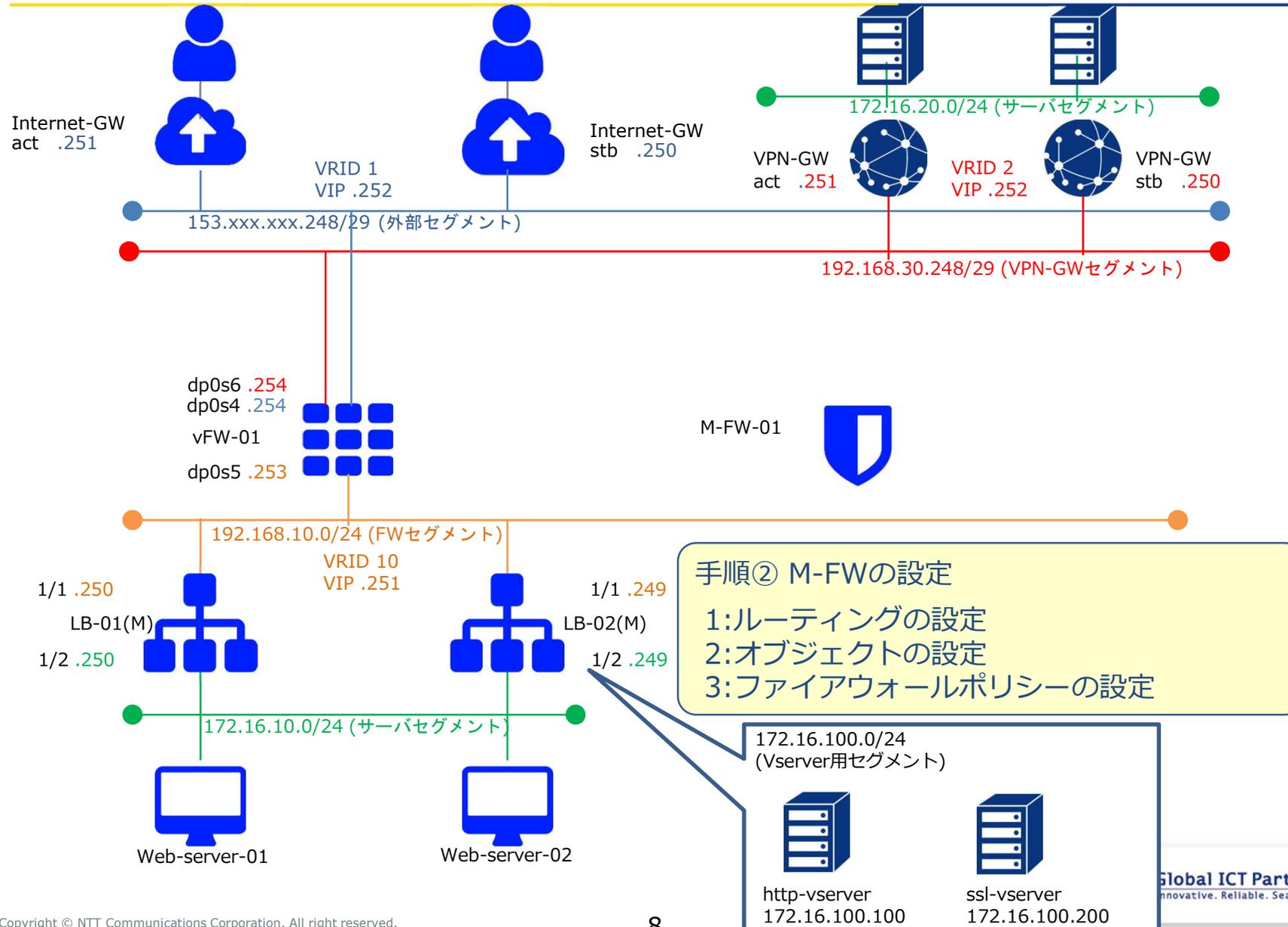
移行時構成①

※手順②まで事前作業が可能です。

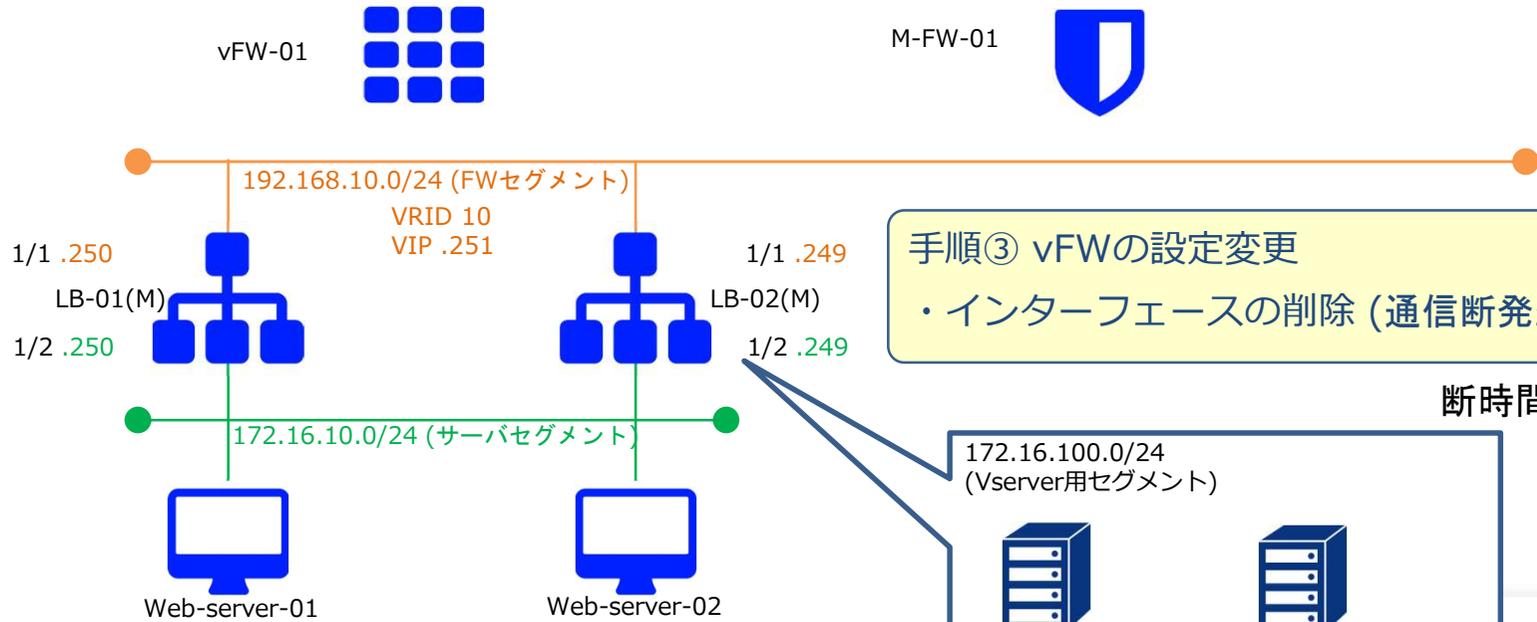
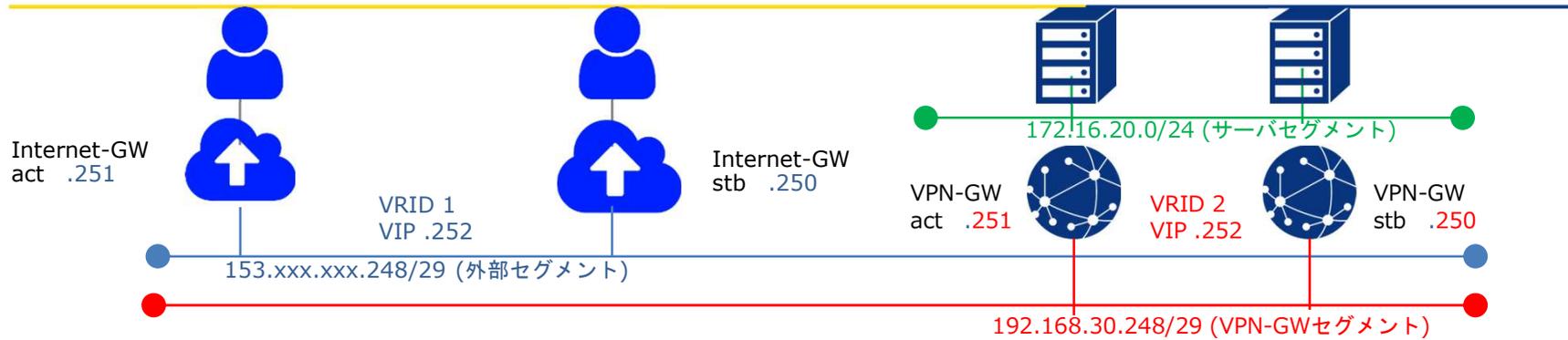


移行時構成②

※手順②まで事前作業が可能です。

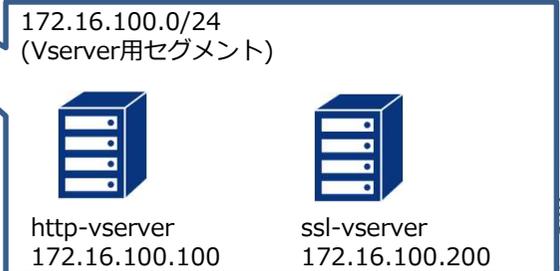


移行時構成③

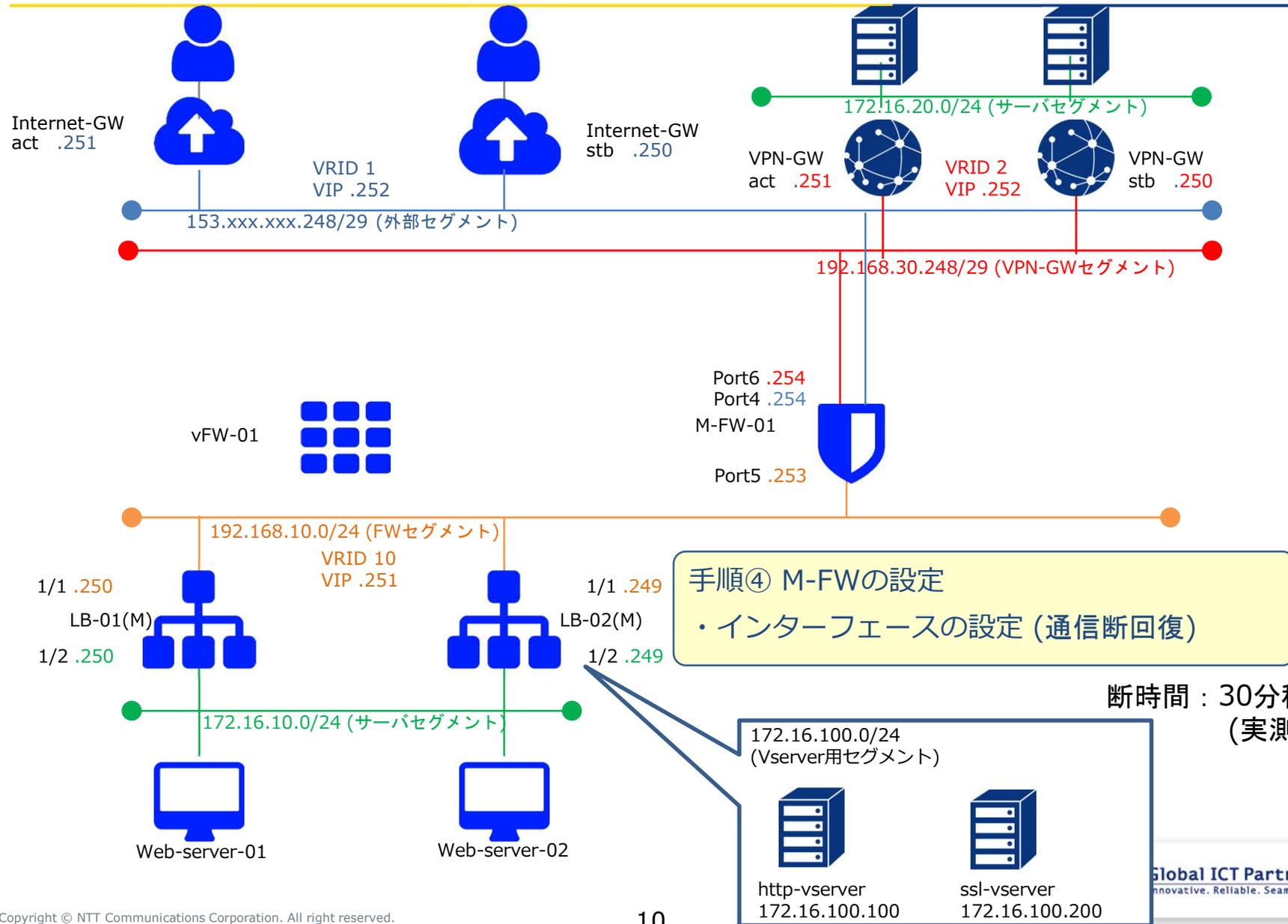


手順③ vFWの設定変更
 ・インターフェースの削除 (通信断発生)

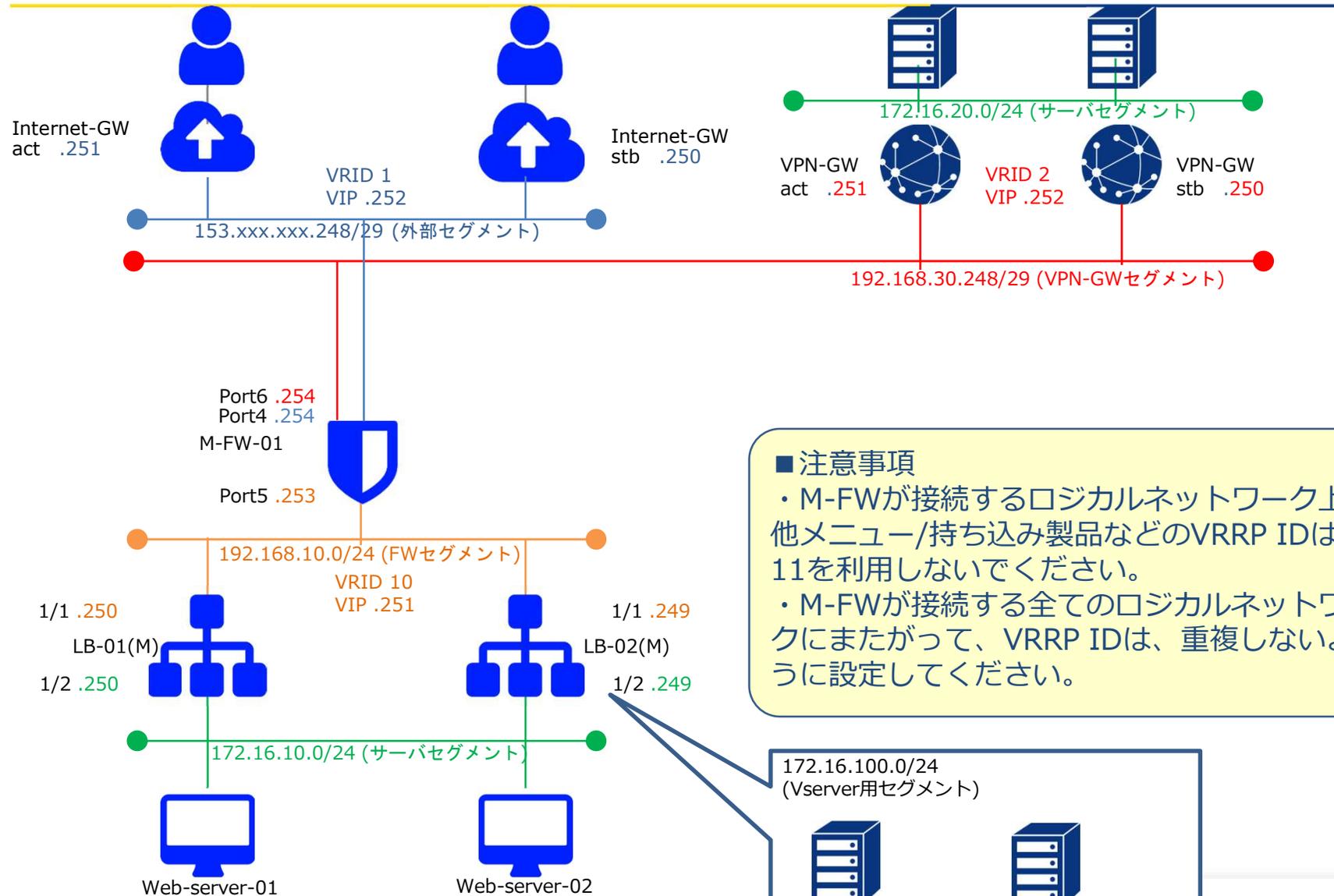
断時間：30分程度
 (実測値)



移行時構成④

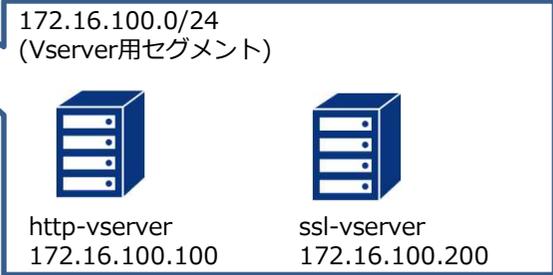


移行完了構成 (Managed Firewall構成)



■ 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 M-FW申し込み

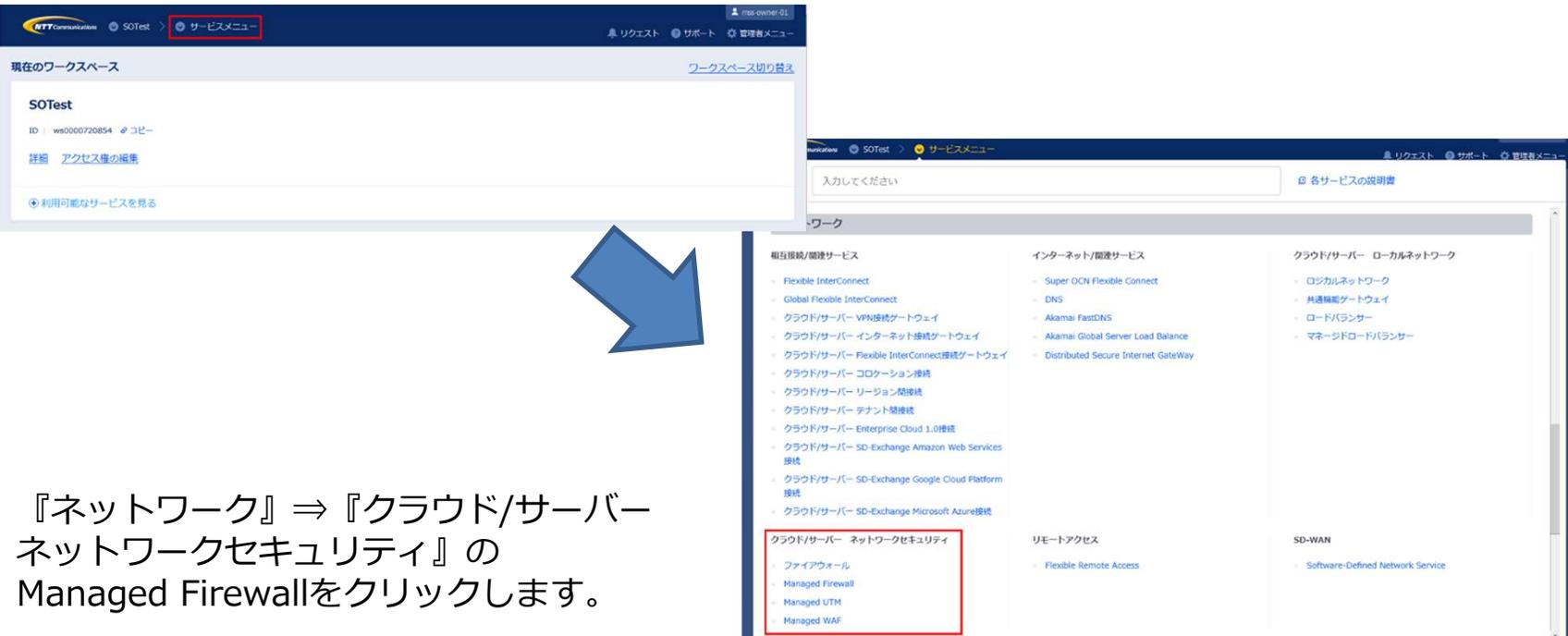
手順① M-FW申し込み

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。



The screenshot shows the SDPF portal interface. In the top navigation bar, the 'Service Menu' (サービスメニュー) is highlighted with a red box. Below, the 'Current Workspace' (現在のワークスペース) section shows 'SOTest' with ID 'ws0000720854'. A blue arrow points from this section to the 'Service Menu' (サービスメニュー) page. The 'Service Menu' page displays a search bar and a list of services categorized into 'Interconnect/Cloud Services', 'Internet/Cloud Services', 'Cloud/Server Local Network', 'Remote Access', and 'SD-WAN'. Under the 'Cloud/Server Network Security' category, 'Managed Firewall' is highlighted with 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① 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② M-FWの設定

手順②-1 M-FWの設定 (ルーティングの設定)

手順②-1 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_v2/4210_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) tab selected in the navigation bar. The bottom screenshot shows the 'Network' (ネットワーク) section, where the 'Network Security' (ネットワークセキュリティ) category is expanded, and 'Managed Firewall' (Managed Firewall) is highlighted with a red box. A blue arrow points from the 'Service Menu' tab in the top screenshot to the 'Managed Firewall' item 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②-1 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

手順②-1 M-FWの設定

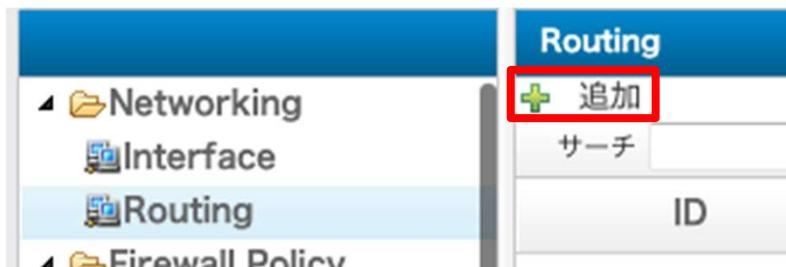
「デバイス」からいずれかのデバイスを右クリックします。



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



手順②-1 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。

オブジェクト

ID	1
Destination IP	172.16.100.0
Subnet Mask	255.255.255.255
Gateway	192.168.10.251
Interface	port5
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②-1 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。

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	送信先アドレス(VPN-GWのVIP)
Gateway	192.168.30.252	
Interface	Port6	送信先Port
Comment		

キャンセル **保存**

手順②-2 M-FWの設定 (Destination NATの設定)

手順②-2 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。

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, where 'Managed Firewall' (Managed Firewall) is highlighted with 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②-2 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②-2 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②-2 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。

オブジェクト

NAT Name	Port4DNAT_80	M-FWの受信側VIP
External IP Address	153.xx.xx.254	
Mapped IP Address	172.16.100.100	http-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	80	
Mapped Port	80	
Comment		

キャンセル 保存

手順②-2 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。

The screenshot shows a configuration window titled "オブジェクト" (Object) with a close button (X) in the top right corner. The window contains the following fields and callouts:

- NAT Name:** Port4DNAT_443
- External IP Address:** 153.xx.xx.254 (Callout: M-FWの受信側VIP)
- Mapped IP Address:** 172.16.100.200 (Callout: ssl-vserverのアドレス)
- External Interface:** Port4 (Callout: 受信側ポート)
- Port Forward:**
- Protocol:** TCP
- External Service Port:** 443
- Mapped Port:** 443
- Comment:** (empty text box)

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

手順②-2 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。

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	172.16.100.100	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②-2 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。

オブジェクト

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	172.16.100.200	
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		

キャンセル 保存

手順②-3 M-FWの設定 (ファイアウォールポリシー設定)

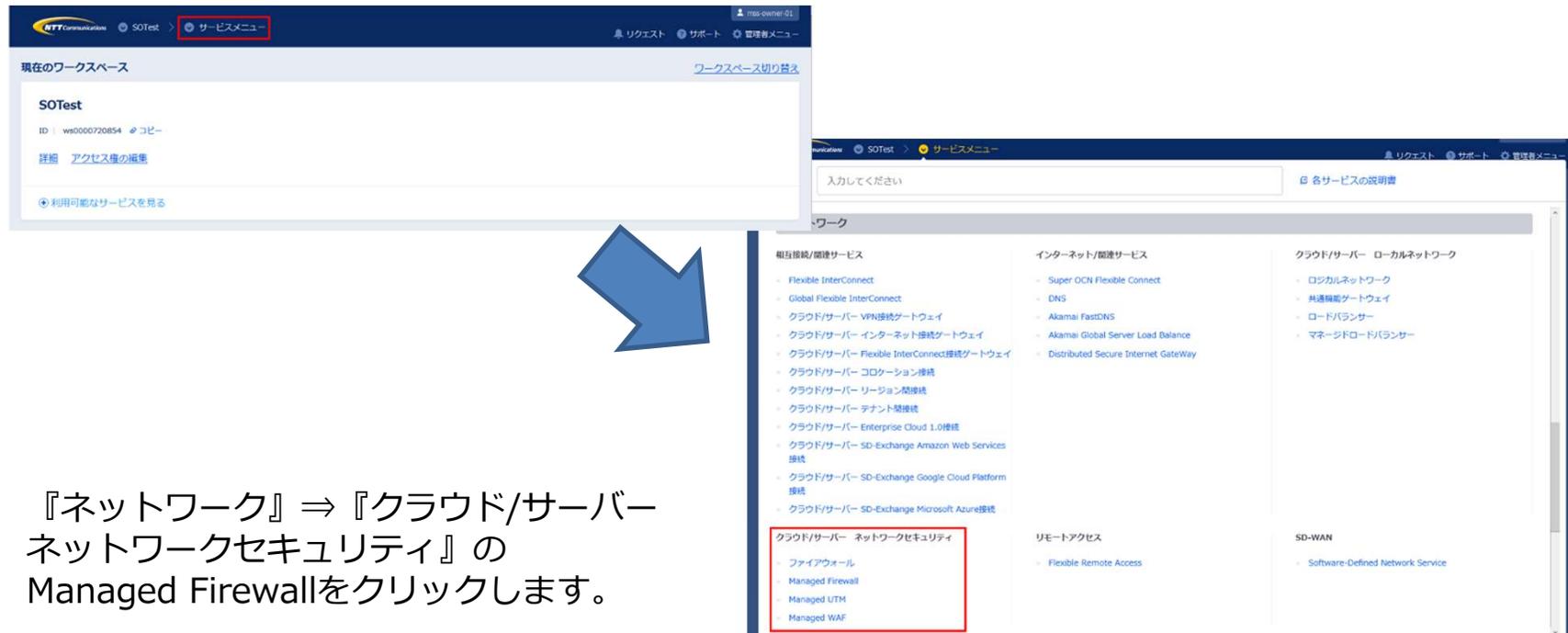
手順②-3 M-FWの設定

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②-3 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②-3 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。



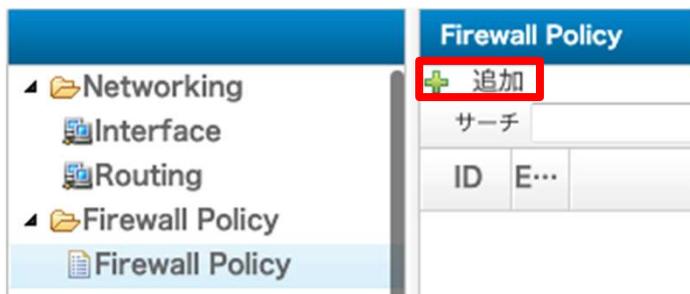
画面右側の「コンフィグ」をクリックします。



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②-3 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

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②-3 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

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_443

Action

Service HTTPS

Action ACCEPT

NAT

Log Disable

Comment

キャンセル 保存

手順②-3 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

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

Global ICT Partner
innovative. Reliable. Seamless.

手順②-3 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

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_443

Service HTTPS

Action ACCEPT

NAT

Log Disable

Comment

キャンセル 保存

手順③ vFWのインターフェース 削除

手順③ vFWのインターフェース削除

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』 → 『ファイアウォール』 → 『Brocade 5600 vRouter』 をクリックください。



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

vSRX

Brocade 5600 vRouter

マネージドファイアウォール

マネージドUTM

マネージドWAF

手順③ 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で実施。

概要

ファイアウォールインタフェース

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		-	-		稼働中	ファイアウォールインタフェースの編集 ▼ ロジカルネットワークの接続
dp0s5	-	2		-	-		稼働中	ファイアウォールインタフェースの編集 ▼ ロジカルネットワークの切断

手順④ M-FWの設定 (インターフェースの設定)

手順④ 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。

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. Below the navigation bar, the '現在のワークスペース' (Current Workspace) section shows 'SOTest' with its ID and a '利用可能なサービスを見る' (View available services) link. A blue arrow points from this link to the 'サービスメニュー' page. The 'サービスメニュー' page displays a search bar and a list of services under the 'ワーク' (Work) section. 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) category is highlighted with a red box, and the 'Managed Firewall' service is also highlighted with a red box. Other categories include '相互接続/関連サービス', 'インターネット/関連サービス', 'クラウド/サーバー ローカルネットワーク', 'リモートアクセス', and 'SD-WAN'.

『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④ 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④ M-FWの設定

[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④ 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。

● 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

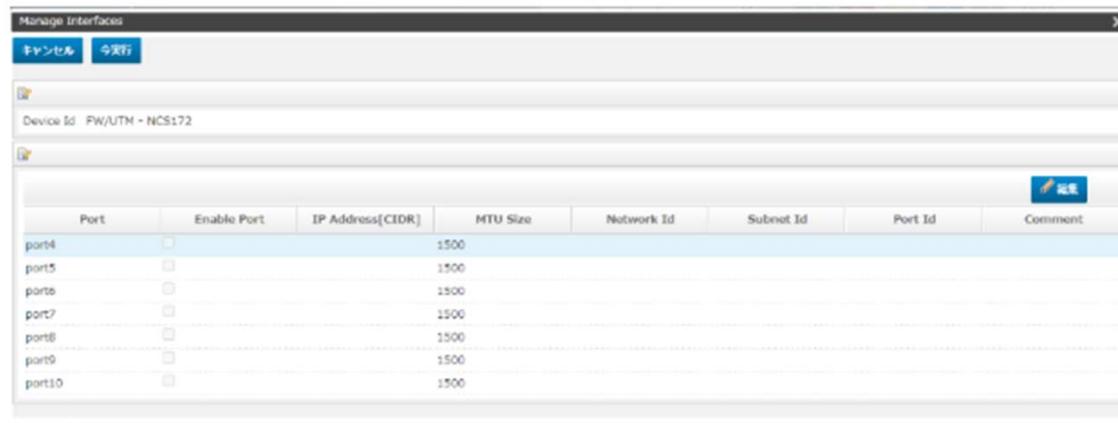
クローズ

手順④ 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④ 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。

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④ 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。

キャンセル 保存

Port Port5

Enable Port

IP Address[CIDR] 192.168.10.253/24 Port4に付与するIPアドレス

MTU Size 1500

Network Id logical1

Subnet Id 192.168.10.0/24 Port4に接続するネットワークアドレス

Port Id

Comment

手順④ 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。

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④ 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。

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④ M-FWの設定

[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④ 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。

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 : 08edfc958d894aa60088155cc26005bc
↓			
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 : f4f775e8-012-4937-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-a6a2-149b2c26129
↓			
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.