

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

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

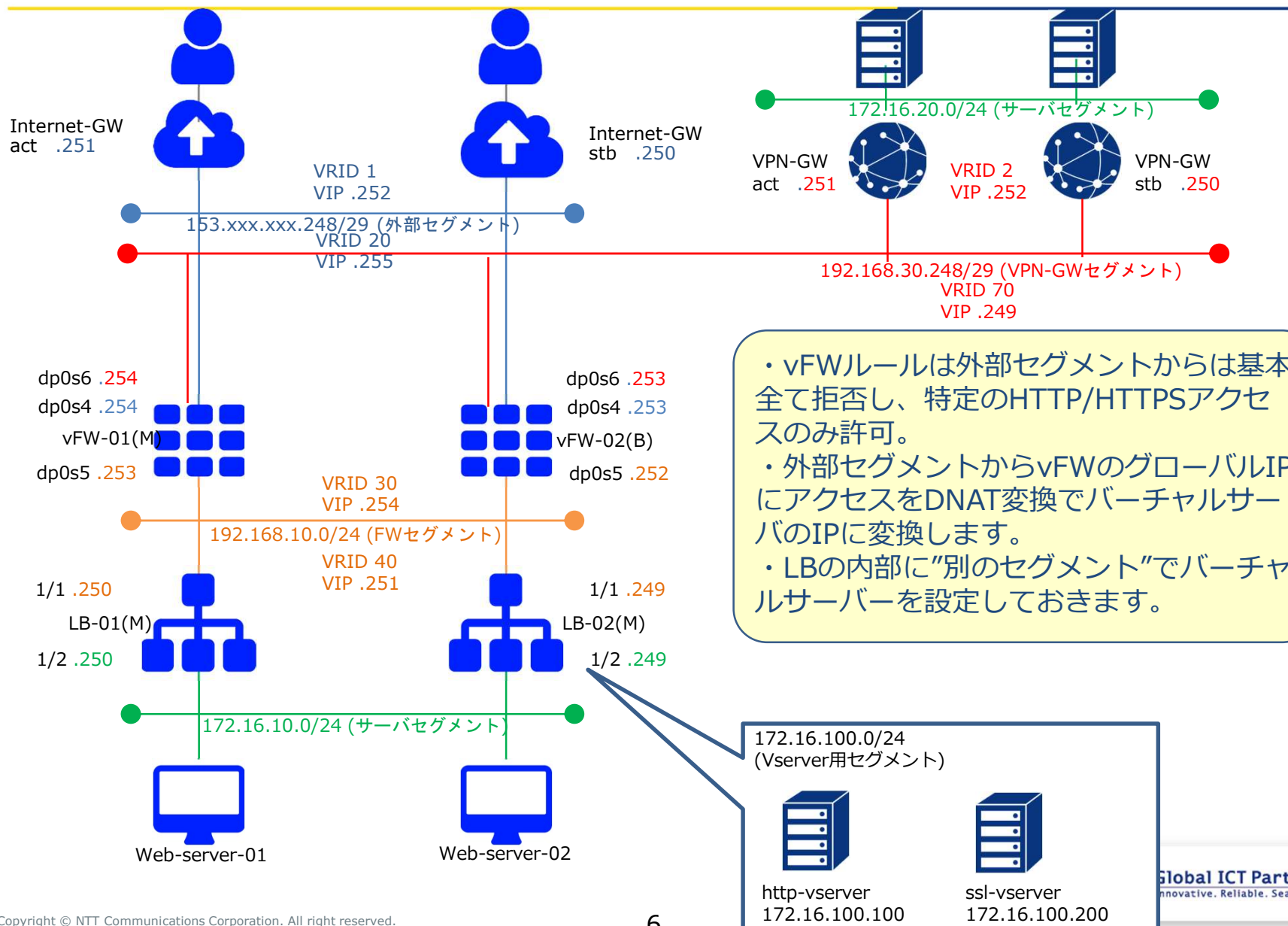
■ファイアウォール(Brocade 5600 vRouter)(以下、vFW)からManaged Firewall(以下、M-FW)への交換によるマイグレ実施方法です。

- ・ 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。

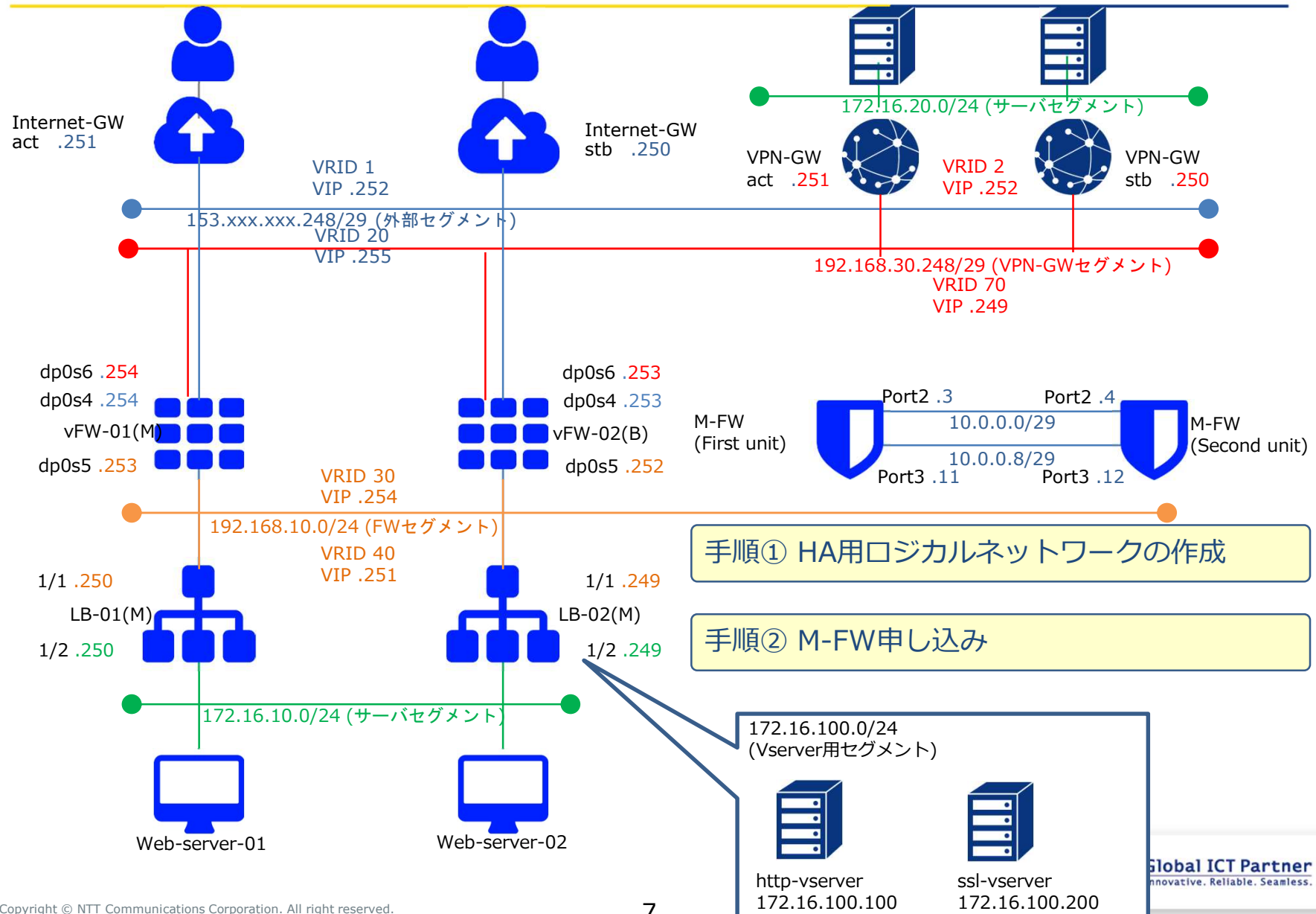
172.16.100.0/24 (Vserver用セグメント)

http-vserver 172.16.100.100

ssl-vserver 172.16.100.200

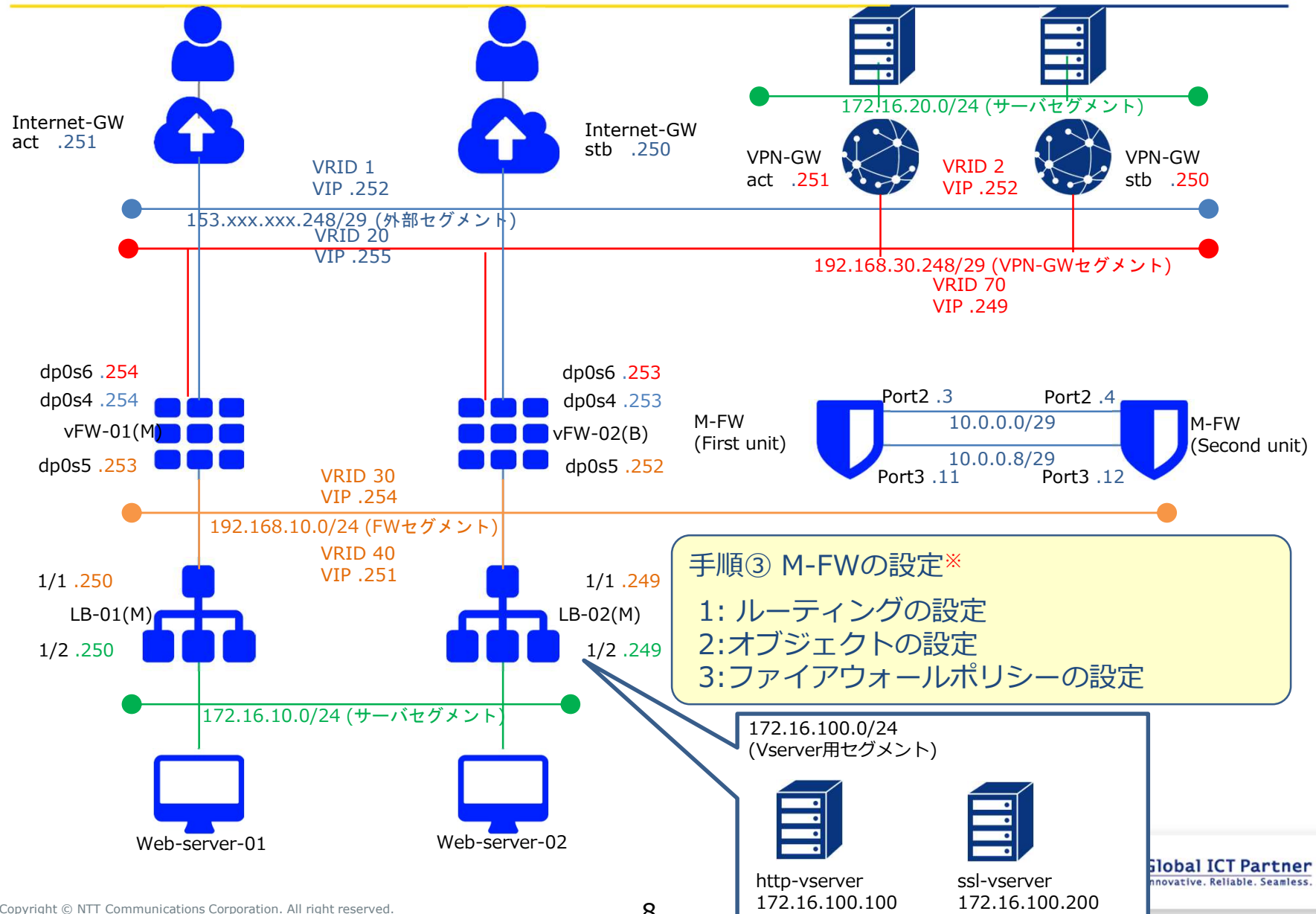
移行時構成①

※手順③まで事前作業が可能です。



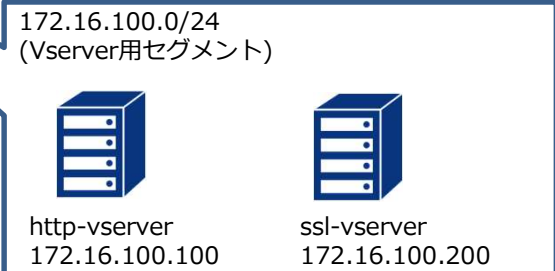
移行時構成②

※手順③まで事前作業が可能です。

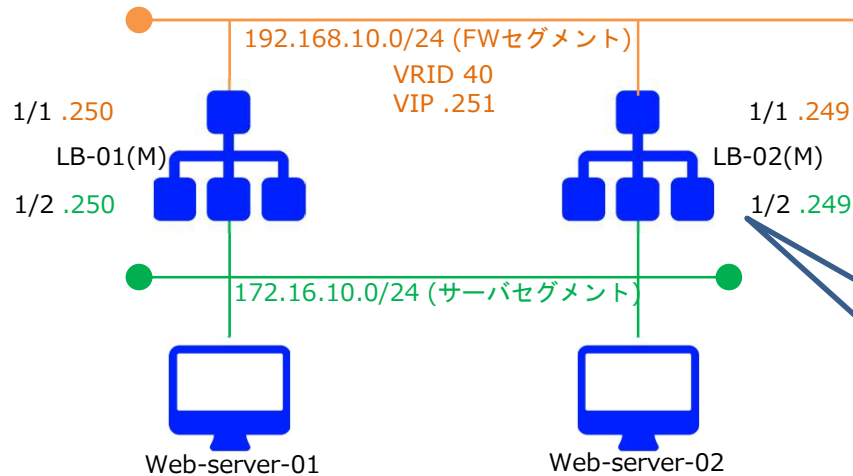
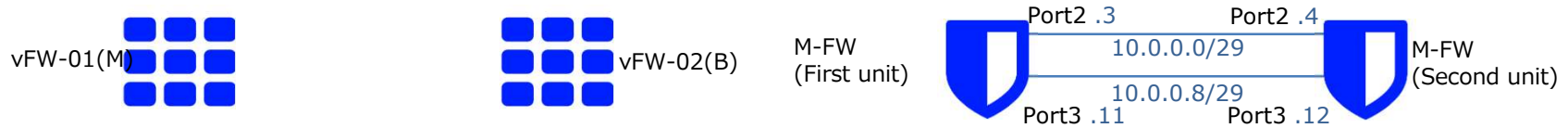
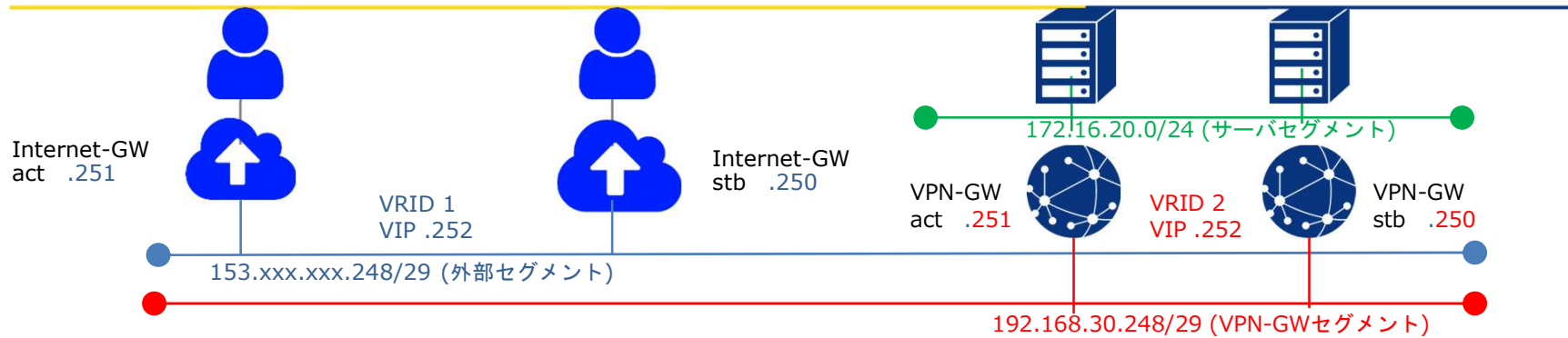


手順③ M-FWの設定※

- 1: ルーティングの設定
- 2: オブジェクトの設定
- 3: ファイアウォールポリシーの設定



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)

172.16.100.0/24
(Vserver用セグメント)

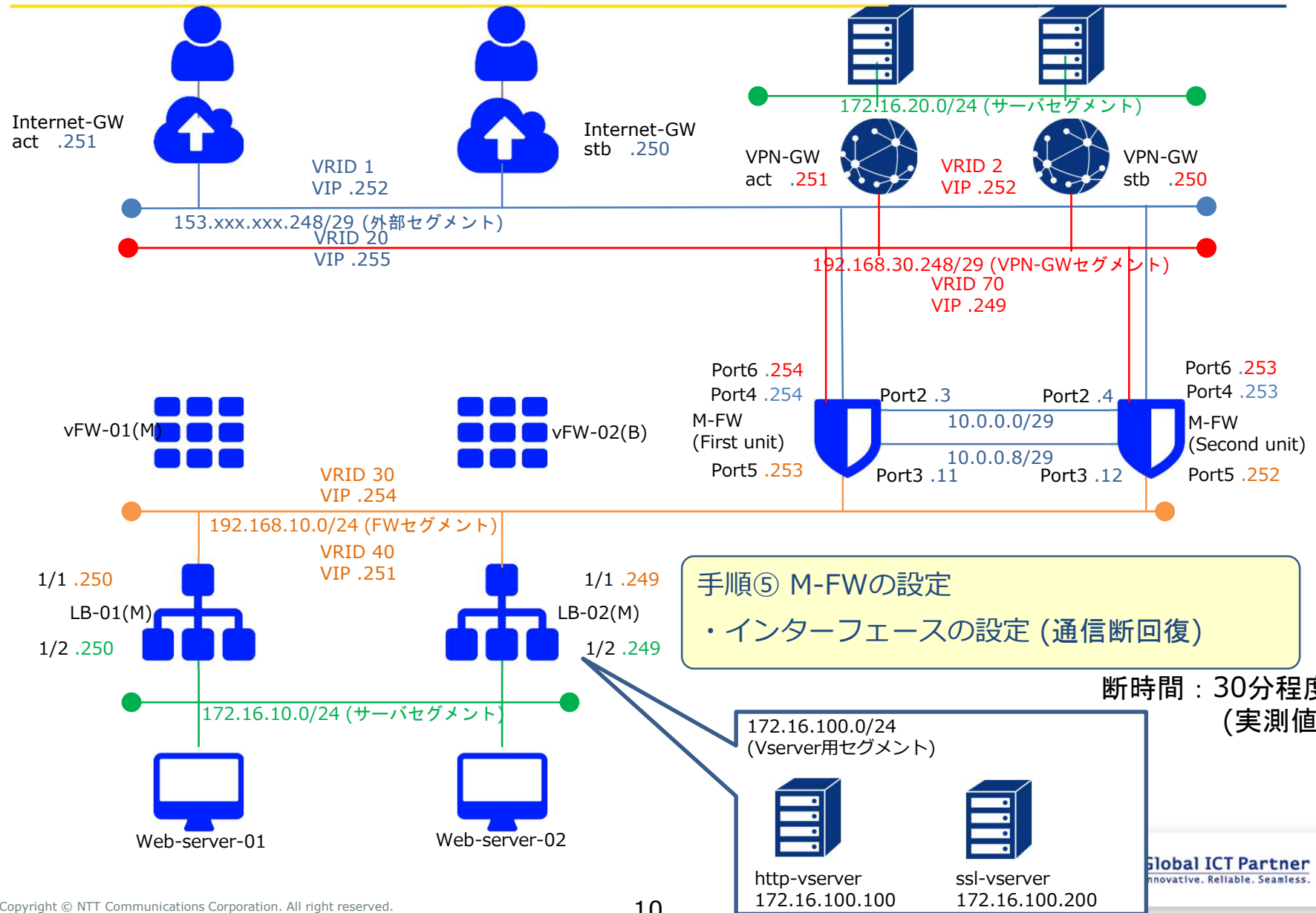


http-vserver
172.16.100.100



ssl-vserver
172.16.100.200

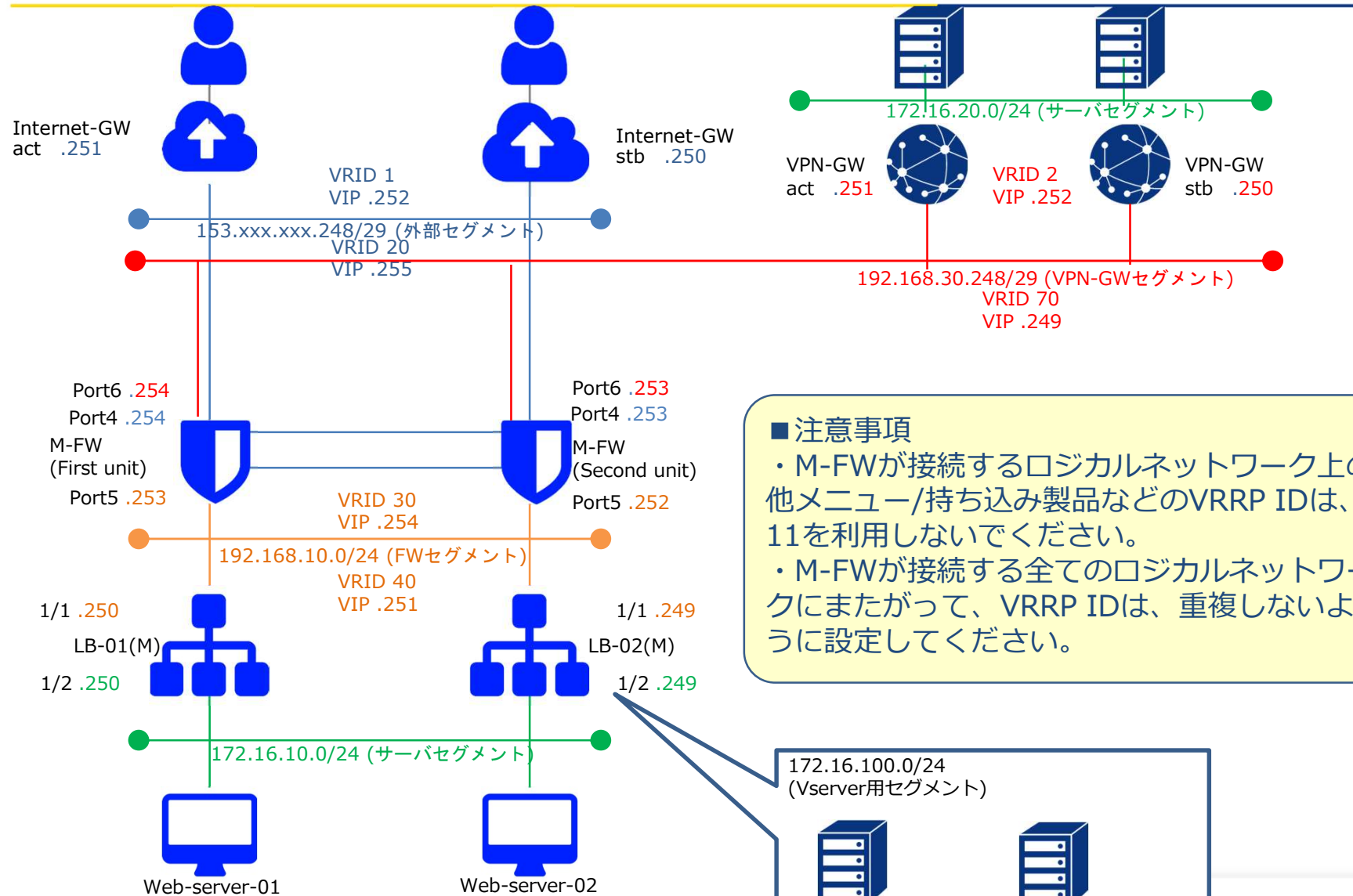
移行時構成④



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。

172.16.100.0/24
(Vserver用セグメント)



http-vserver
172.16.100.100



ssl-vserver
172.16.100.200

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。



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

ロードバランサー

Managed Load Balancer

共通機能ゲートウェイ

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。

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。)

ロジカルネットワークの作成

ロジカルネットワーク名

プラン*

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*

サブネット*

サブネットの詳細

サブネット名

ネットワークアドレス*

10.0.0.0/29

ゲートウェイ IP

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

IPアドレスの割り当てポリシー

DNS サーバー

NTP サーバー

連絡先 Eメール

サブネットの説明

サブネットの分類

取り直し <戻る 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

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。)

ロジカルネットワークの作成

ロジカルネットワーク名

プラン*

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*

サブネット*

サブネットの詳細

サブネット名

ネットワークアドレス*

10.0.0.8/29

ゲートウェイ IP

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

IPアドレス割当て方法

DNS サーバ

NTP サーバ

既定のルートを指定

サブネットの説明

サブネットの優先度

取り直し

戻る

ロジカルネットワークの作成

手順② M-FW申し込み

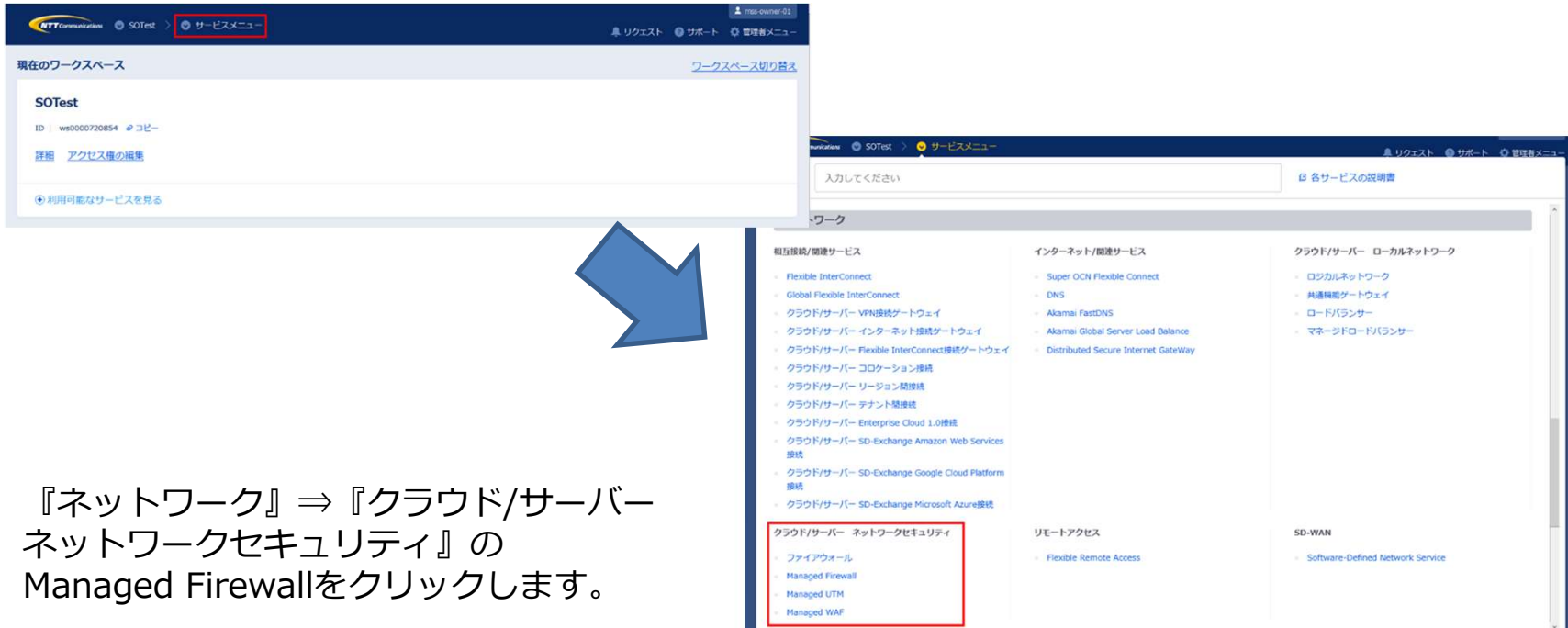
手順② M-FW申し込み

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。



The screenshot shows the SDPF portal interface. The top navigation bar includes 'NTT Communications', 'SOTest', and 'サービスメニュー' (Service Menu). The main content area displays the '現在のワークスペース' (Current Workspace) as 'SOTest' with ID 'ws0000720854'. Below this, there is a search bar and a list of services categorized into '相互接続/関連サービス' (Interconnection/Related Services), 'インターネット/関連サービス' (Internet/Related Services), 'クラウド/サーバー ローカルネットワーク' (Cloud/Server Local Network), 'リモートアクセス' (Remote Access), and 'SD-WAN'. A red box highlights 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, which includes 'ファイアウォール' (Firewall), 'Managed Firewall', 'Managed UTM', and 'Managed WAF'. A blue arrow points from the 'サービスメニュー' link in the top navigation bar to the 'Managed Firewall' item in the service list.

『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	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(HA)」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				HA リンク1		HA リンク2				
No	構成	メニュー	プラン	ゾーン/グループ	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



Global ICT Partner
Innovative. Reliable. Seamless.

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)

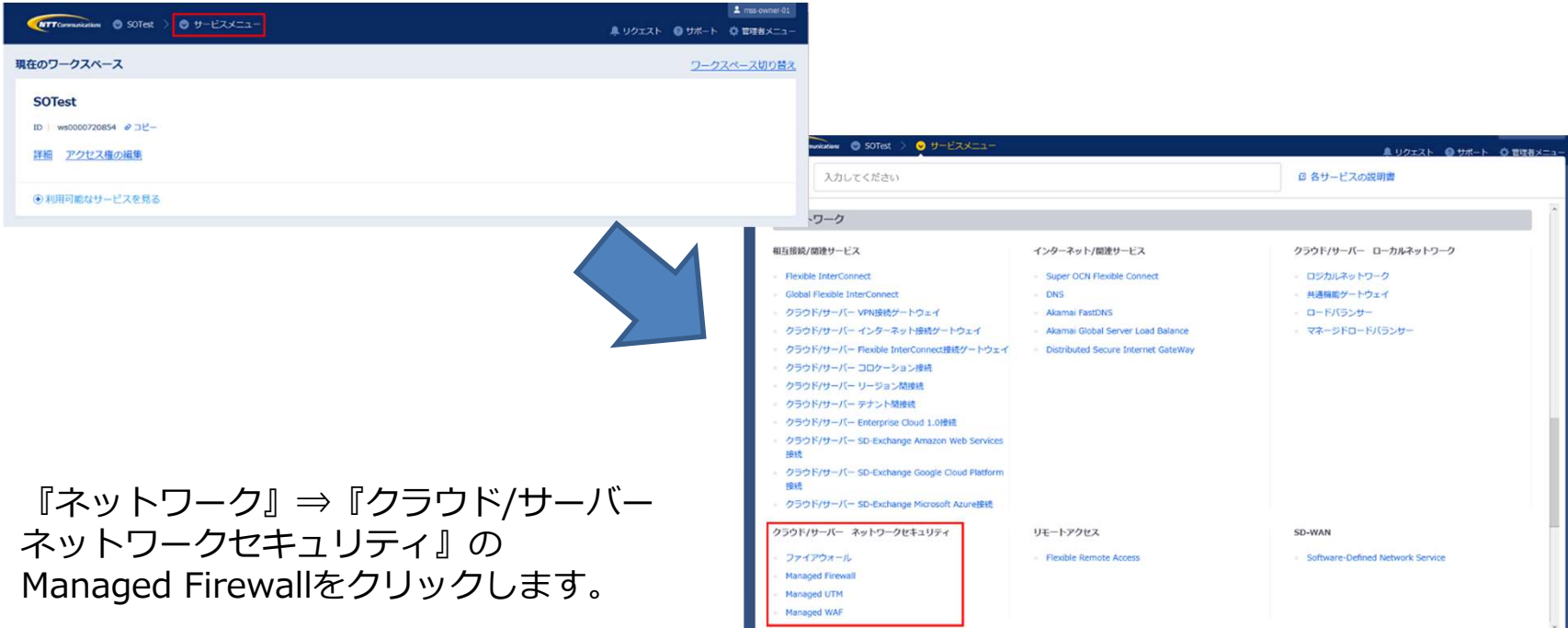
手順③-1 M-FWの設定

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。



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

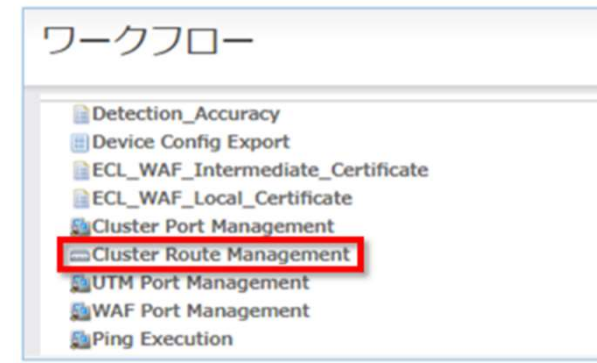
Managed Firewall(Version2)の「Operation」をクリックしてください。

Security Menu

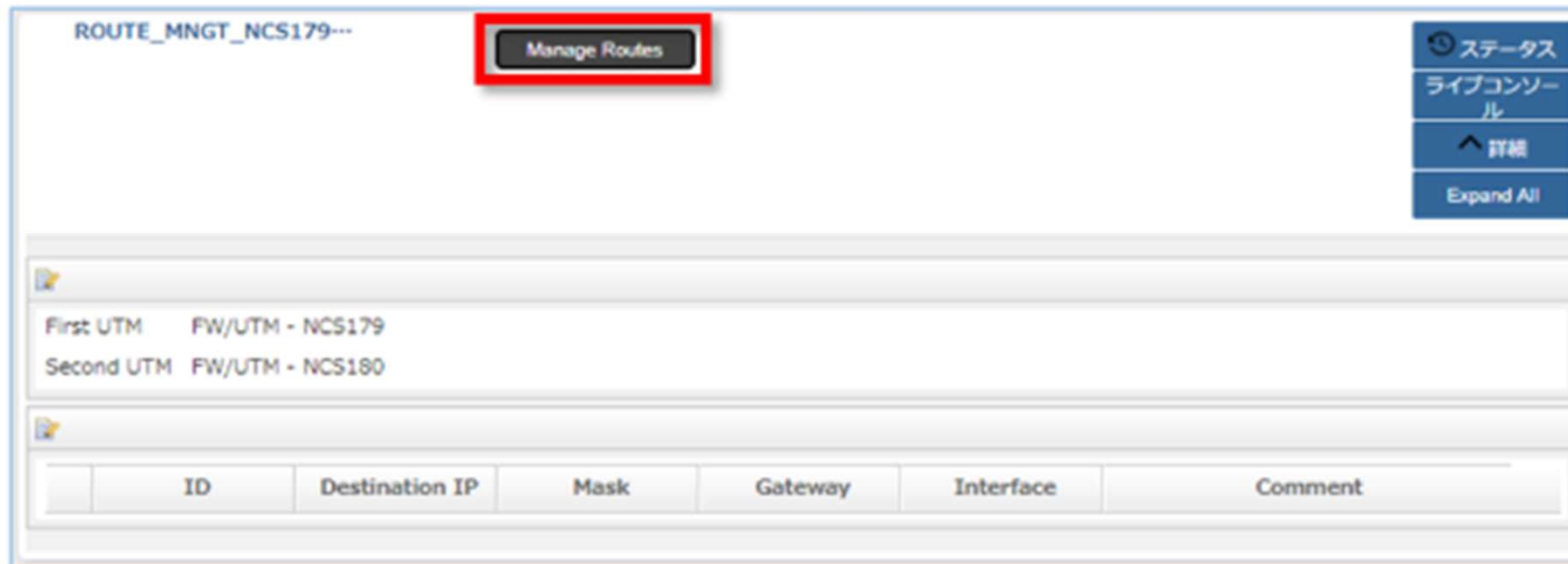
Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
	Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order

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。

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。

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。

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。

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	0.0.0.0	http-vserverのアドレス
External Interface	Port4	受信側ポート
Port Forward	<input checked="" type="checkbox"/>	
Protocol	TCP	
External Service Port	80	
Mapped Port	80	
Comment		

キャンセル 保存

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。

オブジェクト

NAT Name	Port4DNAT_443	M-FWの受信側VIP
External IP Address	153.xx.xx.254	ssl-vserverのアドレス
Mapped IP Address	0.0.0.0	
External Interface	Port4	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。

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 values:

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		

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 border.

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。

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	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		

キャンセル 保存

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。

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 top 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' 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。



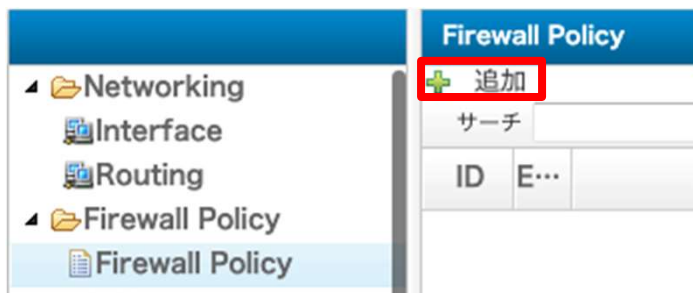
画面右側の「コンフィグ」をクリックします。



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

The screenshot shows the configuration window for a firewall rule. The settings are as follows:

- 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_80 (Callout: DNAT用に作成したオブジェクト)
- Service:** HTTP
- Action:** ACCEPT
- NAT:**
- Log:** Disable
- Comment:** (empty)

キャンセル

保存

Global ICT Partner
innovative. Reliable. Seamless.

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

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

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

Action

Service HTTP

Action ACCEPT

NAT

Log Disable

Comment

キャンセル 保存

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

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

キャンセル 保存

Global ICT Partner
innovative. Reliable. Seamless.

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。

概要 ファイアウォールインターフェイス

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 インターフェイスの編集 ▼ ロジカルネットワークの接続 ロジカルネットワークの切断 VRRP用通信設定の登録 VRRP用通信設定の解除
dp0s5	-	2				-	停止中	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	-	-	-	-	停止中	ファイアウォール インターフェイスの編集 ▼

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。

概要 **ファイアウォールインターフェイス**

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				-	停止中	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接続 ロジカルネットワークの切断 VRRP用通信設定の登録 VRRP用通信設定の解除
dp0s5	-	2				-	停止中	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	-	-	-	-	停止中	ファイアウォール インターフェイスの編集 ▼

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。

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 large 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 'ネットワーク' (Network) category. 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-category is highlighted with a red box, and it contains the following items: 'ファイアウォール' (Firewall), 'Managed Firewall', 'Managed UTM', and 'Managed WAF'. Other categories like 'インターネット/関連サービス' and 'クラウド/サーバー ローカルネットワーク' are also visible.

『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。

-  Detection_Accuracy
-  Device Config Export
-  ECL_WAF_Intermediate_Certificate
-  ECL_WAF_Local_Certificate
-  Cluster Port Management
-  Cluster Route Management
-  UTM Port Management
-  WAF Port Management
-  Ping Execution

HA構成用

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。

The screenshot shows a device management interface for a device named "PORT_MNGT_NCS179_...". The status is "成功" (Success). A message indicates "Device 180 Backup completed successfully". A red box highlights the "Get Network Info" button. Other buttons include "Manage Interfaces", "Manage Proxy ARP", "Get VNC Console", and "Stop/Start First Unit". On the right, there are buttons for "ステータス" (Status), "ライブコンソール" (Live Console), and "詳細" (Details).

[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。

The screenshot shows a "タスクステータス" (Task Status) window. It contains a table with the following data:

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

A red box highlights the "クローズ" (Close) button at the bottom right of the window.

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。

The screenshot shows a management interface for a device named 'PORT_MNGT_NCS179...'. The status is 'ステータス 成功' (Status Success) with a message: 'メッセージ Device 180 Backup completed successfully'. A row of buttons includes 'Get Network Info', 'Manage Interfaces' (highlighted with a red box), 'Manage Proxy ARP', 'Get VNC Console', and 'Stop/Start First Unit'. Below these are 'Stop/Start Second Unit' and a message: 'ED Backup Message : BACKUP processed Backup Revisi...'. On the right, there are buttons for 'ステータス' (Status), 'ライブコンソール' (Live Console), and '詳細' (Details).

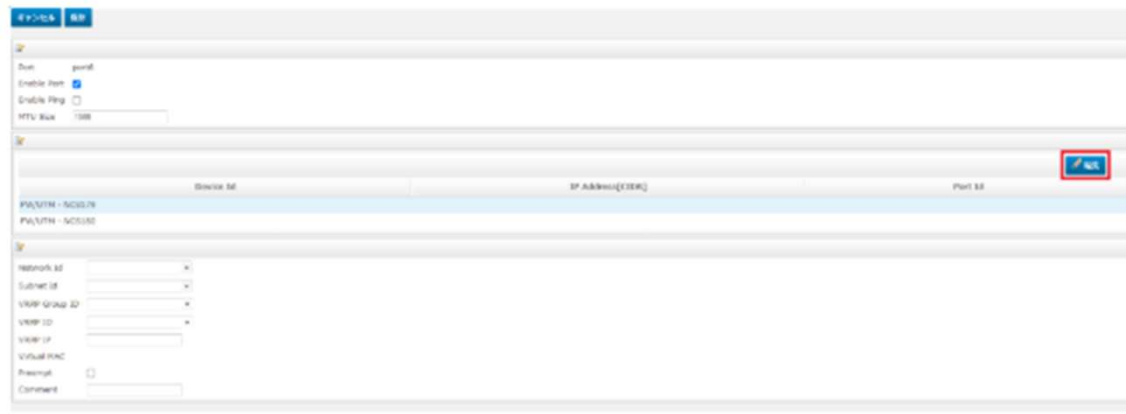
[Manage Interfaces] の画面が開きます。Port 2,3は [Manage Interfaces] の画面には表示されません。設定対象のポートをクリックで選択して、[編集] をクリックします。

The screenshot shows the 'Manage Interfaces' configuration window. It contains a table with columns: Port, Enable, MTU, Device Id, IP Address, Port Id, Network Id, Subnet Id, VRRP Group, VRRP ID, VRRP IP, Virtual MAC, Preempt, and Comment. The table lists several ports (port4, port5, port6, port7, port8, port9, port...) with their respective configurations. A red box highlights the '編集' (Edit) button in the top right corner of the table.

Port	Enable	MTU	Device Id	IP Address	Port Id	Network Id	Subnet Id	VRRP Group	VRRP ID	VRRP IP	Virtual MAC	Preempt	Comment
port4	<input type="checkbox"/>	1500	FW/UTM - N	192.168.1.2	a4096e0d	INTGW-F	192.168.1	30	35	192.168.1	00:00:5e:00	<input type="checkbox"/>	
			FW/UTM - N	192.168.1.2	1a500db4								
port5	<input type="checkbox"/>	1500	FW/UTM - N	192.168.2.2	4757a9d0	FW-GV_NW	192.168.2	30	26	192.168.2.10	00:00:5e:00	<input type="checkbox"/>	
			FW/UTM - N	192.168.2.3	a7012090								
port6	<input type="checkbox"/>	1500	FW/UTM - N										
			FW/UTM - N										
port7	<input type="checkbox"/>	1500	FW/UTM - N										
			FW/UTM - N										
port8	<input type="checkbox"/>	1500	FW/UTM - N										
			FW/UTM - N										
port9	<input type="checkbox"/>	1500	FW/UTM - N										
			FW/UTM - N										
port...	<input type="checkbox"/>	1500	FW/UTM - N										
			FW/UTM - N										

手順⑤ M-FWの設定

各デバイスを選択し、編集を押します。



The screenshot shows a configuration page for M-FW. At the top, there are tabs for 'キャンセル' and '保存'. Below, there are checkboxes for 'Enable Port' and 'Enable Ping', and a text field for 'MTV Size'. A table lists devices with columns for 'Device ID', 'IP Address[CIDR]', and 'Port ID'. The first two rows are highlighted in blue. A red box highlights the '保存' button in the top right corner of the table area. Below the table, there are several dropdown menus for 'Network ID', 'Subnet ID', 'VLAN Group ID', and 'VLAN ID', along with a 'VLAN MAC' field and a 'Comment' field.

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。



The screenshot shows a close-up of the configuration page. At the top, there are buttons for 'キャンセル' and '保存', with the '保存' button highlighted by a red box. Below, there is a 'Device Id' field with the value 'FW/UTM - NCS179'. The 'IP Address[CIDR]' field is empty and highlighted by a red box. The 'Port ID' field is also visible.

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。

キャンセル 保存

Port port4
Enable Port
Enable Ping
MTU Size 1500

Device Id	IP Address[CIDR]	Port Id
FW/UTM - NCS1621	192.168.10.253/24	
FW/UTM - NCS1622	192.168.10.252/24	

Network Id inet-seg
Subnet Id 153.xx.xx.248/29
VRRP Group ID 20
VRRP ID 153.xx.xx.255
VRRP IP
Virtual MAC
Preempt
Comment

Port4に接続するセグメント
Internet GWやVPN GWなど、他のVRRP IDと重複しない値
Port4にアサインするVIP

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。

キャンセル 保存

Port Port5
Enable Port
Enable Ping
MTU Size 1500

Device Id	IP Address[CIDR]	Port Id
FW/UTM - NCS1621	192.168.10.253/24	
FW/UTM - NCS1622	192.168.10.252/24	

Network Id logical20
Subnet Id 192.168.10.0/24
VRRP Group ID 1
VRRP ID 30
VRRP IP 192.168.10.254
Virtual MAC
Preempt
Comment

Port5に接続するセグメント
Internet GWやVPN GWなど、他のVRRP IDと重複しない値
Port5にアサインするVIP

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。

キャンセル 保存

Port Port6
Enable Port
Enable Ping
MTU Size 1500

Device Id	IP Address[CIDR]	Port Id
FW/UTM - NCS1621	192.168.30.253	
FW/UTM - NCS1622	192.168.30.254	

Network Id vpn-seg
Subnet Id 192.168.30.248/29
VRRP Group ID 1
VRRP ID 70
VRRP IP 192.168.30.249
Virtual MAC
Preempt
Comment

Port6に接続するセグメント
Internet GWやVPN GWなど、他のVRRP IDと重複しない値
Port6にアサインするVIP

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。

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⑤ 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。

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 : 08edfc95d894aa69088155cc26005bc
↓			
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. Ports created successfully. Port Id : 14f775e8-012-4937-a6dc-e02eeca4055 Port Id : 09eeeb59-17bc-40bc-8ae4-330b5d55024e Port Id : 8010b923-2c79-4ed3-80d3-9317dfc2ab1 Port Id : c85d7b3b-3e3c-44a3-97b5-829fc138ad91 Port Id : 83a34462-0262-4a8a-acdf-caf8ce43794f Port Id : e604d97f-5e7b-4f97-94a5-a832004a0e0e Port Id : 2a72235c-ab1f-4af0-a6a2-149b12c29129
↓			
Create Ports	2016-07-11 22:36:52	2016-07-11 22:36:58	
↓			
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 100.85.96.31 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.