

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

第1版

更新履歴

更新日	更新内容	版数
2018/07/23	初版	1



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)IPsec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への付け替え完了まで、通信断が発生いたします。
- vFWのVIPを、M-FWのインターフェースに引き継ぎます。

※事前検証を行ってから移行を実施ください。

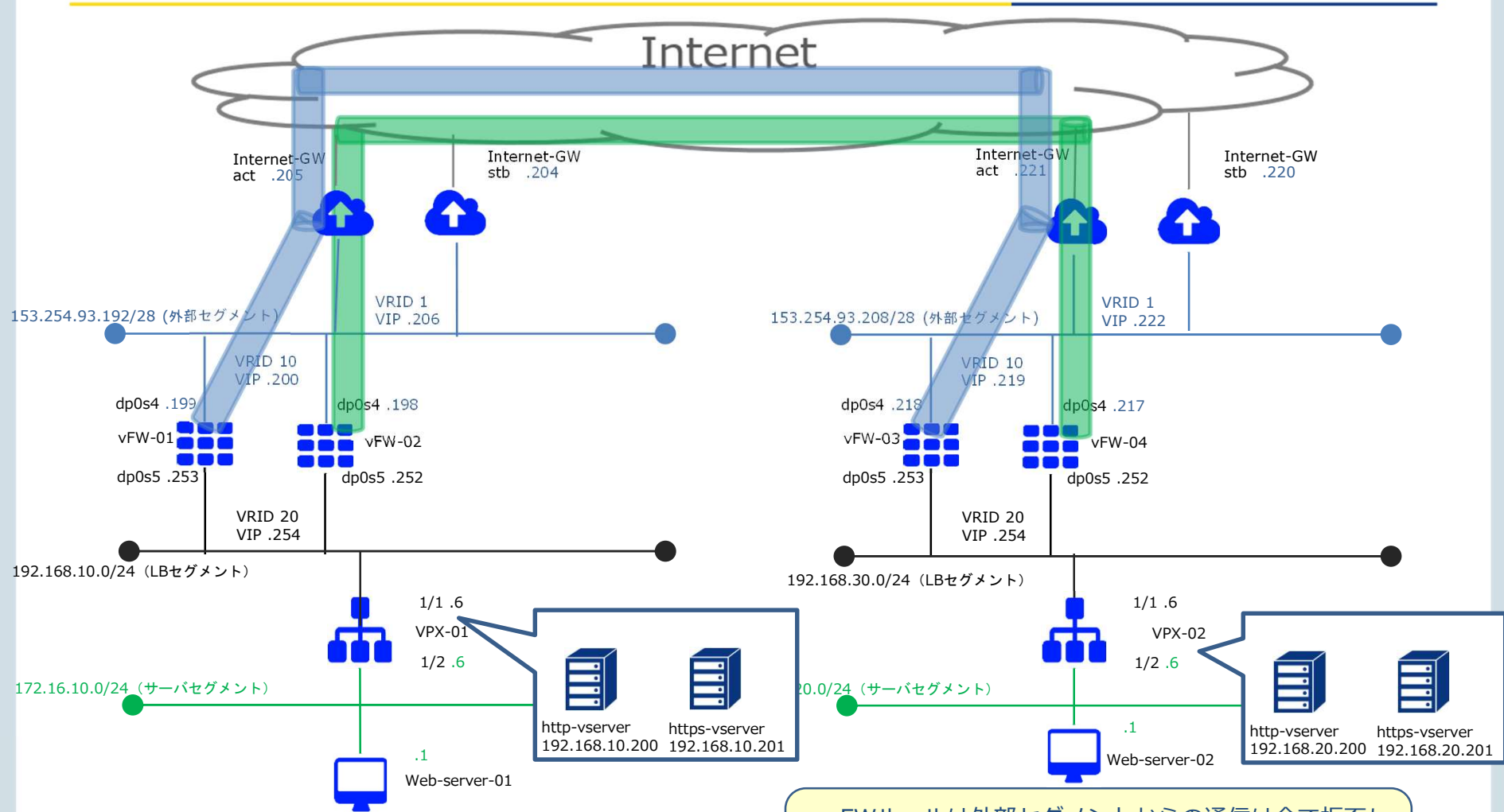
注意事項

- ・ HA構成ではIPsec機能は利用不可となります。本機能はシングル構成でのみ利用可能となります。
- ・ シングル構成2台で、M-FW IPsec機能の冗長化を図る場合、M-FW等の障害が発生した場合、手動にて各サーバーやネットワーク機器の経路を変更する必要があります。
- ・ Internet経由でIPsecをご利用される際、M-FWのInternet Gateway向きIFにプライベートIPアドレスを割り当てた場合、Internet GatewayとM-FWの間にNAT機器をご用意頂く必要があります。
また下記の要件を満たす必要があります。
 - ・ M-FW/UTM間でIPの接続性に問題ないこと
 - ・ InitiatorからResponder宛にUDP/ポート番号:500、UDP/ポート番号:4500、IP/プロトコル番号:50が通信許可されていること。

本条件で移行をされる場合、事前検証にて、Internet経由でIPsec通信が出来る事を確認した上で移行して下さい。

構成および移行フロー

移行前構成 (vFW構成)



IPsec

- vFWルールは外部セグメントからの通信は全て拒否し、Web-server-01/Web-server-02間のHTTP/HTTPS通信のみ許可しております。
- LBの内部にバーチャルサーバーを設定しておきます。
- vFWの設定内容を次のページに記載致します。

移行前構成 (vFW構成)

vFW-01(IPsec)の設定

```
set interfaces vti vti0 address '10.0.20.1/30'  
set security vpn ipsec esp-group ESP-1W lifetime '3600'  
set security vpn ipsec esp-group ESP-1W proposal 1 encryption 'aes256'  
set security vpn ipsec esp-group ESP-1W proposal 1 hash 'sha2_256'  
set security vpn ipsec ike-group IKE-1W lifetime '28800'  
set security vpn ipsec ike-group IKE-1W proposal 1 dh-group '14'  
set security vpn ipsec ike-group IKE-1W proposal 1 encryption 'aes256'  
set security vpn ipsec ike-group IKE-1W proposal 1 hash 'sha2_256'  
set security vpn ipsec site-to-site peer 153.254.93.218 authentication pre-shared-secret 'examplekey000'  
set security vpn ipsec site-to-site peer 153.254.93.218 ike-group 'IKE-1W'  
set security vpn ipsec site-to-site peer 153.254.93.218 local-address '153.254.93.199'  
set security vpn ipsec site-to-site peer 153.254.93.218 vti bind 'vti0'  
set security vpn ipsec site-to-site peer 153.254.93.218 vti esp-group 'ESP-1W'  
set protocols static interface-route 192.168.30.0/24 next-hop-interface 'vti0'
```

vFW-01(IPsecフィルター)の設定

```
set security firewall name From-Tunnel default-action 'drop'  
set security firewall name From-Tunnel rule 10 action 'accept'  
set security firewall name From-Tunnel rule 10 protocol 'tcp'  
set security firewall name From-Tunnel rule 10 source address '172.16.20.1'  
set security firewall name From-Tunnel rule 10 source port '80'  
set security firewall name From-Tunnel rule 20 action 'accept'  
set security firewall name From-Tunnel rule 20 protocol 'tcp'  
set security firewall name From-Tunnel rule 20 source address '172.16.20.1'  
set security firewall name From-Tunnel rule 20 source port '443'  
set security firewall name From-Tunnel rule 30 action 'accept'  
set security firewall name From-Tunnel rule 30 protocol 'tcp'  
set security firewall name From-Tunnel rule 30 source address '192.168.30.200'  
set security firewall name From-Tunnel rule 30 source port '80'  
set security firewall name From-Tunnel rule 40 action 'accept'  
set security firewall name From-Tunnel rule 40 protocol 'tcp'  
set security firewall name From-Tunnel rule 40 source address '192.168.30.201'  
set security firewall name From-Tunnel rule 40 source port '443'
```

```
set security firewall name To-Tunnel default-action 'drop'  
set security firewall name To-Tunnel rule 10 action 'accept'  
set security firewall name To-Tunnel rule 10 protocol 'tcp'  
set security firewall name To-Tunnel rule 10 source address '172.16.10.1'  
set security firewall name To-Tunnel rule 10 source port '80'  
set security firewall name To-Tunnel rule 20 action 'accept'  
set security firewall name To-Tunnel rule 20 protocol 'tcp'  
set security firewall name To-Tunnel rule 20 source address '172.16.10.1'  
set security firewall name To-Tunnel rule 20 source port '443'  
set security firewall name To-Tunnel rule 30 action 'accept'  
set security firewall name To-Tunnel rule 30 protocol 'tcp'  
set security firewall name To-Tunnel rule 30 source address '192.168.10.200'  
set security firewall name To-Tunnel rule 30 source port '80'  
set security firewall name To-Tunnel rule 40 action 'accept'  
set security firewall name To-Tunnel rule 40 protocol 'tcp'  
set security firewall name To-Tunnel rule 40 source address '192.168.10.201'  
set security firewall name To-Tunnel rule 40 source port '443'
```


移行前構成 (vFW構成)

vFW-01 ファイアウォールフィルターの設定

```
set security firewall name From-Internet default-action 'drop'  
set security firewall name From-Internet rule 10 action 'accept'  
set security firewall name From-Internet rule 10 protocol 'esp'  
set security firewall name From-Internet rule 10 source address '153.254.93.218'  
set security firewall name From-Internet rule 20 action 'accept'  
set security firewall name From-Internet rule 20 protocol 'udp'  
set security firewall name From-Internet rule 20 source address '153.254.93.218'  
set security firewall name From-Internet rule 20 source port '500'  
set security firewall name From-Internet rule 30 action 'accept'  
set security firewall name From-Internet rule 30 protocol 'tcp'  
set security firewall name From-Internet rule 30 source address '153.254.93.218'  
set security firewall name From-Internet rule 30 source port '1293'  
set security firewall name From-Internet rule 40 action 'accept'  
set security firewall name From-Internet rule 40 protocol 'udp'  
set security firewall name From-Internet rule 40 source address '153.254.93.218'  
set security firewall name From-Internet rule 40 source port '1293'  
set security firewall name From-Internet rule 50 action 'accept'  
set security firewall name From-Internet rule 50 protocol 'udp'  
set security firewall name From-Internet rule 50 source address '153.254.93.218'  
set security firewall name From-Internet rule 50 source port '50'  
set security firewall name From-Internet rule 60 action 'accept'  
set security firewall name From-Internet rule 60 protocol 'tcp'  
set security firewall name From-Internet rule 60 source address '153.254.93.218'  
set security firewall name From-Internet rule 60 source port '50'
```

```
set security firewall name To-Internet default-action 'drop'  
set security firewall name To-Internet rule 10 action 'accept'  
set security firewall name To-Internet rule 10 protocol 'esp'  
set security firewall name To-Internet rule 10 source address '153.254.93.199'  
set security firewall name To-Internet rule 20 action 'accept'  
set security firewall name To-Internet rule 20 protocol 'udp'  
set security firewall name To-Internet rule 20 source address '153.254.93.199'  
set security firewall name To-Internet rule 20 source port '500'  
set security firewall name To-Internet rule 30 action 'accept'  
set security firewall name To-Internet rule 30 protocol 'tcp'  
set security firewall name To-Internet rule 30 source address '153.254.93.199'  
set security firewall name To-Internet rule 30 source port '1293'  
set security firewall name To-Internet rule 40 action 'accept'  
set security firewall name To-Internet rule 40 protocol 'udp'  
set security firewall name To-Internet rule 40 source address '153.254.93.199'  
set security firewall name To-Internet rule 40 source port '1293'  
set security firewall name To-Internet rule 50 action 'accept'  
set security firewall name To-Internet rule 50 protocol 'udp'  
set security firewall name To-Internet rule 50 source address '153.254.93.199'  
set security firewall name To-Internet rule 50 source port '50'  
set security firewall name To-Internet rule 60 action 'accept'  
set security firewall name To-Internet rule 60 protocol 'tcp'  
set security firewall name To-Internet rule 60 source address '153.254.93.199'  
set security firewall name To-Internet rule 60 source port '50'
```

移行前構成 (vFW構成)

vFW-03(IPsec)の設定

```
Set interfaces vti vti0 address '10.0.20.2/30'  
set security vpn ipsec esp-group ESP-1W lifetime '3600'  
set security vpn ipsec esp-group ESP-1W proposal 1 encryption 'aes256'  
set security vpn ipsec esp-group ESP-1W proposal 1 hash 'sha2_256'  
set security vpn ipsec ike-group IKE-1W lifetime '28800'  
set security vpn ipsec ike-group IKE-1W proposal 1 dh-group '14'  
set security vpn ipsec ike-group IKE-1W proposal 1 encryption 'aes256'  
set security vpn ipsec ike-group IKE-1W proposal 1 hash 'sha2_256'  
set security vpn ipsec site-to-site peer 153.254.93.199 authentication pre-shared-secret 'examplekey000'  
set security vpn ipsec site-to-site peer 153.254.93.199 ike-group 'IKE-1W'  
set security vpn ipsec site-to-site peer 153.254.93.199 local-address '153.254.93.218'  
set security vpn ipsec site-to-site peer 153.254.93.199 vti bind 'vti0'  
set security vpn ipsec site-to-site peer 153.254.93.199 vti esp-group 'ESP-1W'  
set protocols static interface-route 192.168.10.0/24 next-hop-interface 'vti0'
```

vFW-03(IPsecフィルター)の設定

```
set security firewall name From-Tunnel default-action 'drop'  
set security firewall name From-Tunnel rule 10 action 'accept'  
set security firewall name From-Tunnel rule 10 protocol 'tcp'  
set security firewall name From-Tunnel rule 10 source address '172.16.10.1'  
set security firewall name From-Tunnel rule 10 source port '80'  
set security firewall name From-Tunnel rule 20 action 'accept'  
set security firewall name From-Tunnel rule 20 protocol 'tcp'  
set security firewall name From-Tunnel rule 20 source address '172.16.10.1'  
set security firewall name From-Tunnel rule 20 source port '443'  
set security firewall name From-Tunnel rule 30 action 'accept'  
set security firewall name From-Tunnel rule 30 protocol 'tcp'  
set security firewall name From-Tunnel rule 30 source address '192.168.10.200'  
set security firewall name From-Tunnel rule 30 source port '80'  
set security firewall name From-Tunnel rule 40 action 'accept'  
set security firewall name From-Tunnel rule 40 protocol 'tcp'  
set security firewall name From-Tunnel rule 40 source address '192.168.10.201'  
set security firewall name From-Tunnel rule 40 source port '443'
```

```
set security firewall name To-Tunnel default-action 'drop'  
set security firewall name To-Tunnel rule 10 action 'accept'  
set security firewall name To-Tunnel rule 10 protocol 'tcp'  
set security firewall name To-Tunnel rule 10 source address '172.16.30.1'  
set security firewall name To-Tunnel rule 10 source port '80'  
set security firewall name To-Tunnel rule 20 action 'accept'  
set security firewall name To-Tunnel rule 20 protocol 'tcp'  
set security firewall name To-Tunnel rule 20 source address '172.16.30.1'  
set security firewall name To-Tunnel rule 20 source port '443'  
set security firewall name To-Tunnel rule 30 action 'accept'  
set security firewall name To-Tunnel rule 30 protocol 'tcp'  
set security firewall name To-Tunnel rule 30 source address '192.168.30.200'  
set security firewall name To-Tunnel rule 30 source port '80'  
set security firewall name To-Tunnel rule 40 action 'accept'  
set security firewall name To-Tunnel rule 40 protocol 'tcp'  
set security firewall name To-Tunnel rule 40 source address '192.168.30.201'  
set security firewall name To-Tunnel rule 40 source port '443'
```

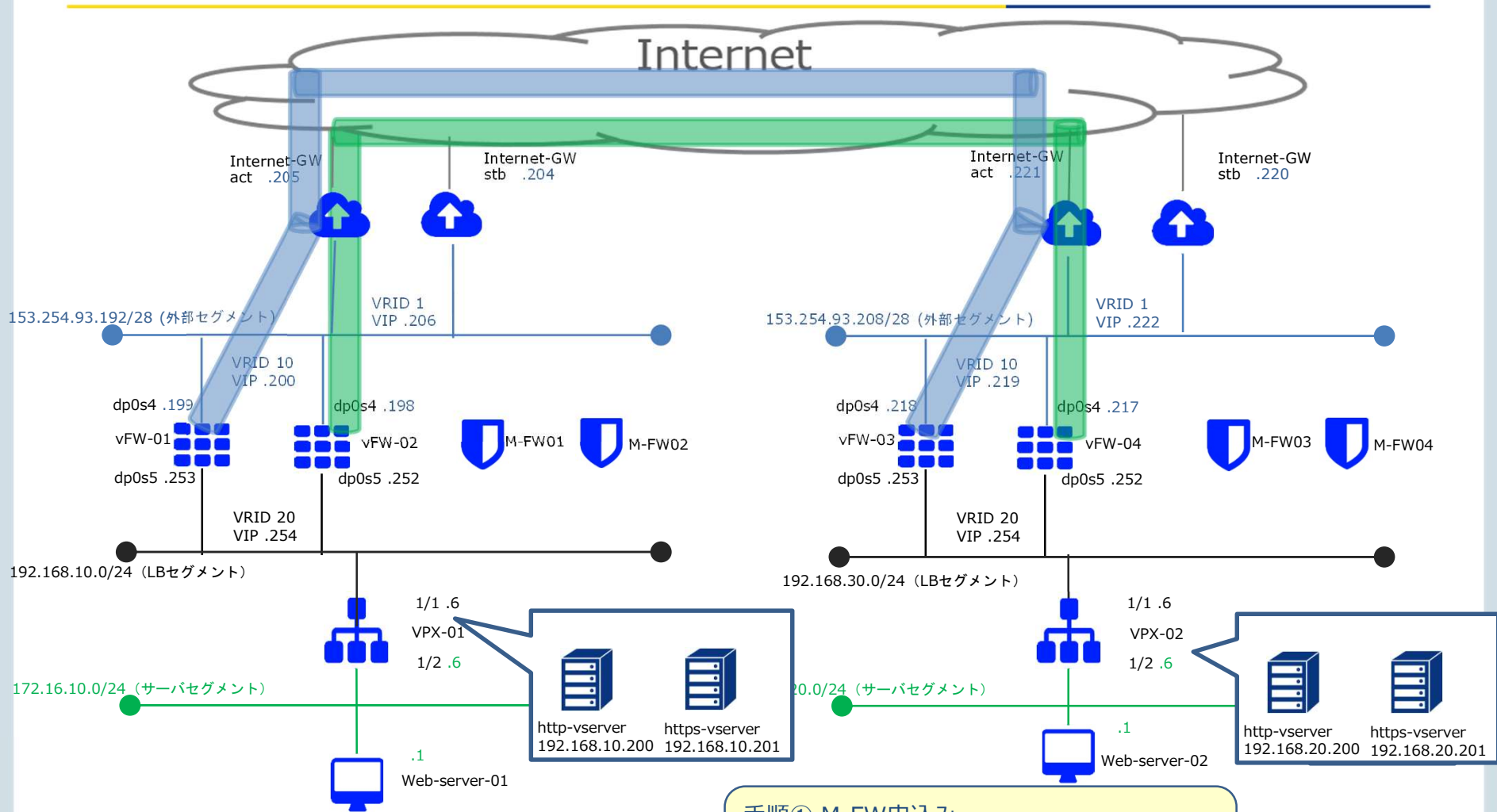
移行前構成 (vFW構成)

vFW-03 ファイアウォールフィルターの設定

```
set security firewall name From-Internet default-action 'drop'  
set security firewall name From-Internet rule 10 action 'accept'  
set security firewall name From-Internet rule 10 protocol 'esp'  
set security firewall name From-Internet rule 10 source address '153.254.93.199'  
set security firewall name From-Internet rule 20 action 'accept'  
set security firewall name From-Internet rule 20 protocol 'udp'  
set security firewall name From-Internet rule 20 source address '153.254.93.199'  
set security firewall name From-Internet rule 20 source port '500'  
set security firewall name From-Internet rule 30 action 'accept'  
set security firewall name From-Internet rule 30 protocol 'tcp'  
set security firewall name From-Internet rule 30 source address '153.254.93.199'  
set security firewall name From-Internet rule 30 source port '1293'  
set security firewall name From-Internet rule 40 action 'accept'  
set security firewall name From-Internet rule 40 protocol 'udp'  
set security firewall name From-Internet rule 40 source address '153.254.93.199'  
set security firewall name From-Internet rule 40 source port '1293'  
set security firewall name From-Internet rule 50 action 'accept'  
set security firewall name From-Internet rule 50 protocol 'udp'  
set security firewall name From-Internet rule 50 source address '153.254.93.199'  
set security firewall name From-Internet rule 50 source port '50'  
set security firewall name From-Internet rule 60 action 'accept'  
set security firewall name From-Internet rule 60 protocol 'tcp'  
set security firewall name From-Internet rule 60 source address '153.254.93.199'  
set security firewall name From-Internet rule 60 source port '50'
```

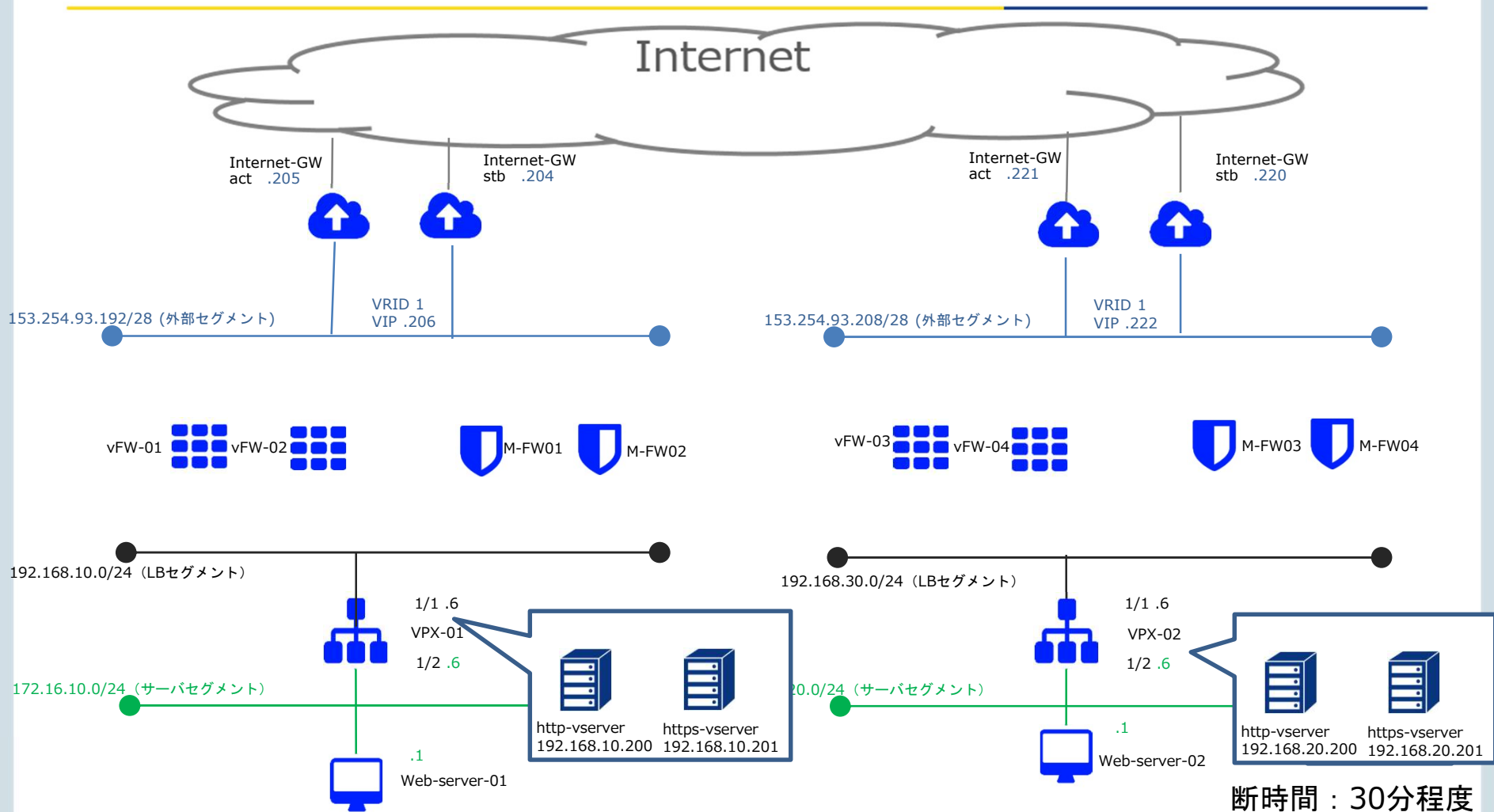
```
set security firewall name To-Internet default-action 'drop'  
set security firewall name To-Internet rule 10 action 'accept'  
set security firewall name To-Internet rule 10 protocol 'esp'  
set security firewall name To-Internet rule 10 source address '153.254.93.218'  
set security firewall name To-Internet rule 20 action 'accept'  
set security firewall name To-Internet rule 20 protocol 'udp'  
set security firewall name To-Internet rule 20 source address '153.254.93.218'  
set security firewall name To-Internet rule 20 source port '500'  
set security firewall name To-Internet rule 30 action 'accept'  
set security firewall name To-Internet rule 30 protocol 'tcp'  
set security firewall name To-Internet rule 30 source address '153.254.93.218'  
set security firewall name To-Internet rule 30 source port '1293'  
set security firewall name To-Internet rule 40 action 'accept'  
set security firewall name To-Internet rule 40 protocol 'udp'  
set security firewall name To-Internet rule 40 source address '153.254.93.218'  
set security firewall name To-Internet rule 40 source port '1293'  
set security firewall name To-Internet rule 50 action 'accept'  
set security firewall name To-Internet rule 50 protocol 'udp'  
set security firewall name To-Internet rule 50 source address '153.254.93.218'  
set security firewall name To-Internet rule 50 source port '50'  
set security firewall name To-Internet rule 60 action 'accept'  
set security firewall name To-Internet rule 60 protocol 'tcp'  
set security firewall name To-Internet rule 60 source address '153.254.93.218'  
set security firewall name To-Internet rule 60 source port '50'
```

移行時構成①



- 手順① M-FW申込み
 手順② M-FW設定投入
 1:ルーティング設定
 2:IPSecセッティング設定
 3:IPSecルーティング設定
 4:IPSecポリシー設定

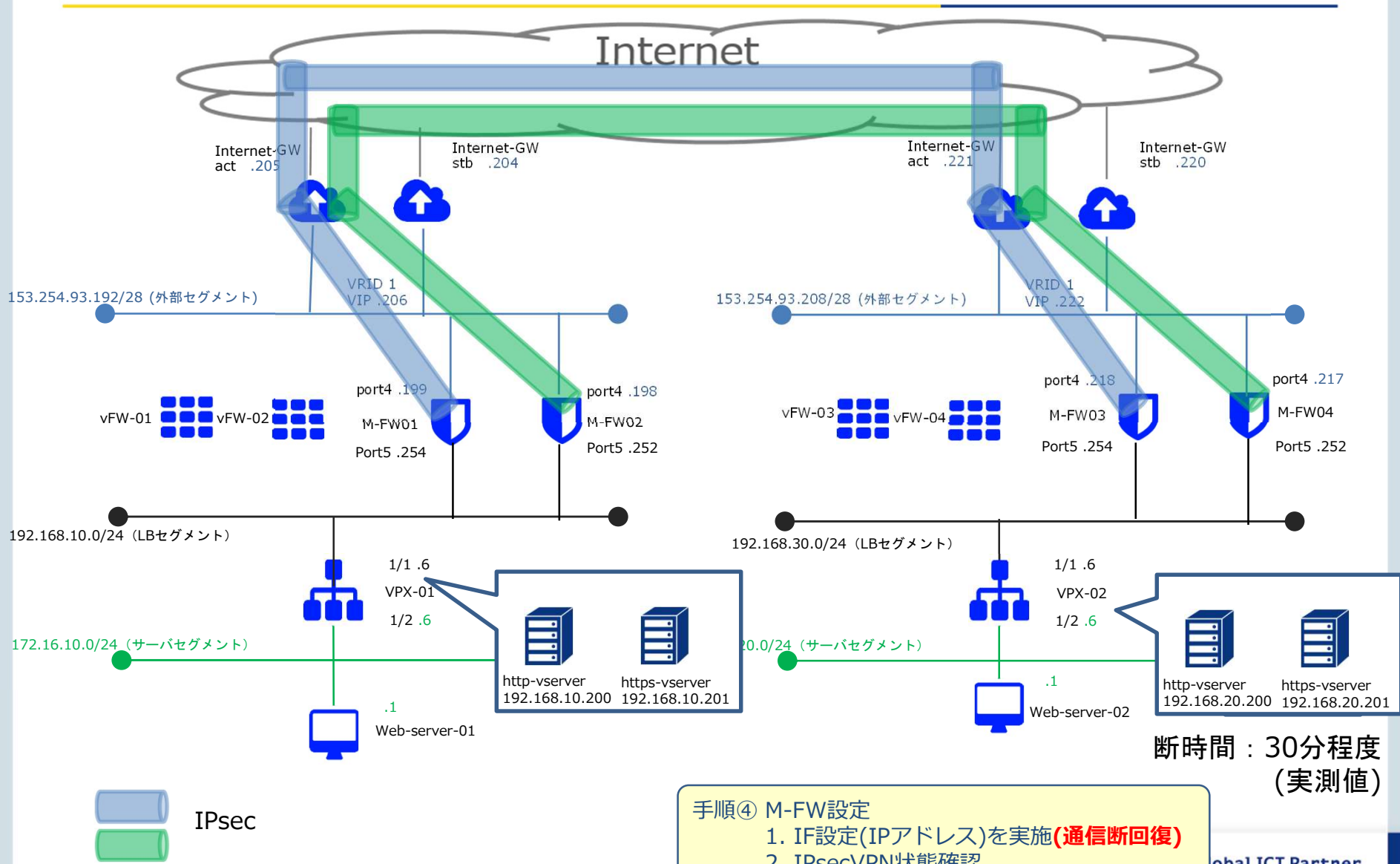
移行時構成②



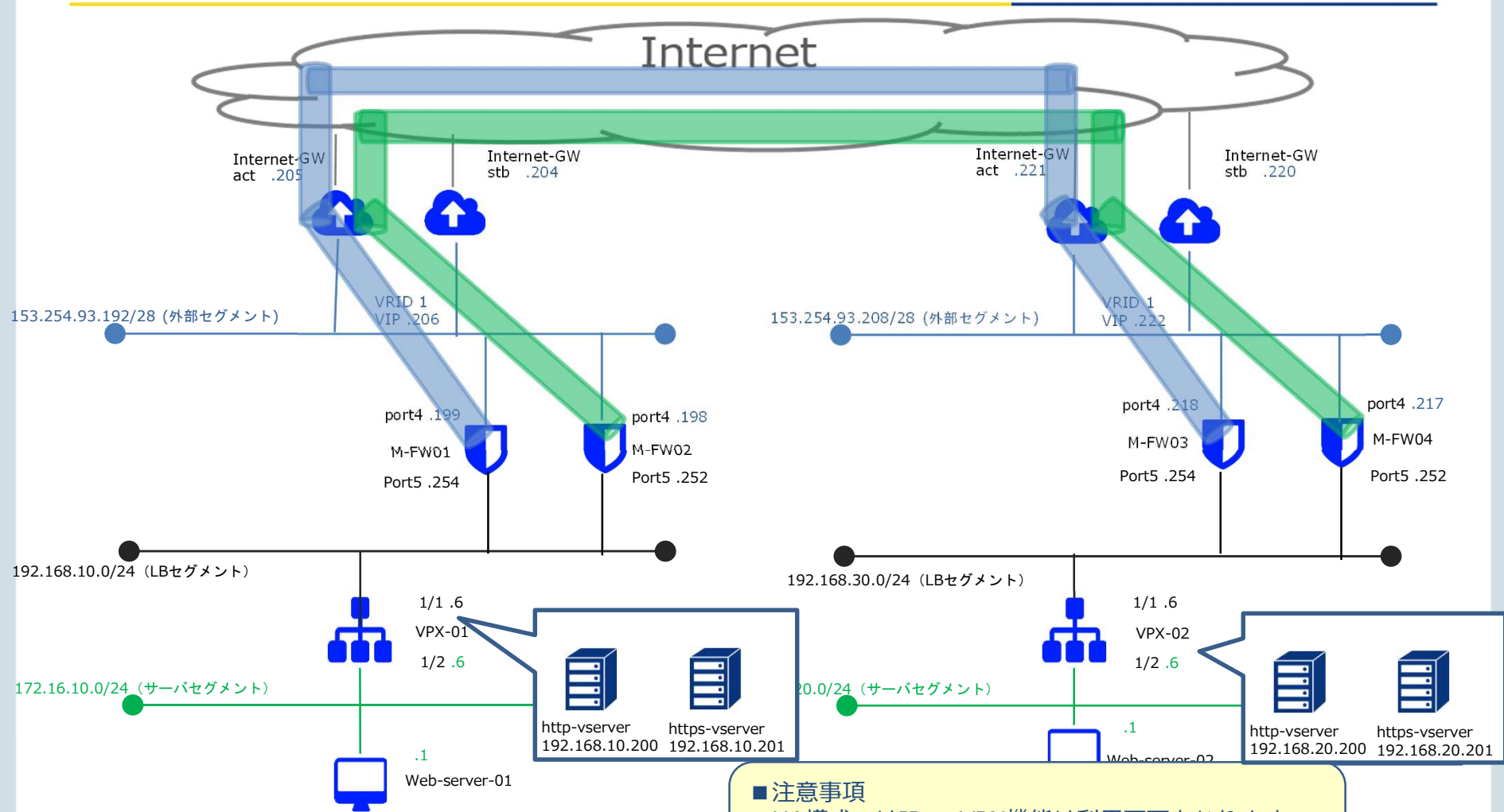
断時間：30分程度
(実測値)

- 手順③ vFWの設定変更
1. VRRP設定解除(通信断発生)
 2. IF切断

移行時構成③



移行完了構成 (Managed Firewall構成)



■ 注意事項

- ・ HA構成ではIPsecVPN機能は利用不可となります。
- ・ シングル構成2台で、Managed Firewall IPsecVPN機能の冗長化を図る場合、Managed Firewall等の障害が発生した場合、手動にて各サーバやネットワーク機器の経路を変更する必要があります。



手順① Managed Firewall申込み

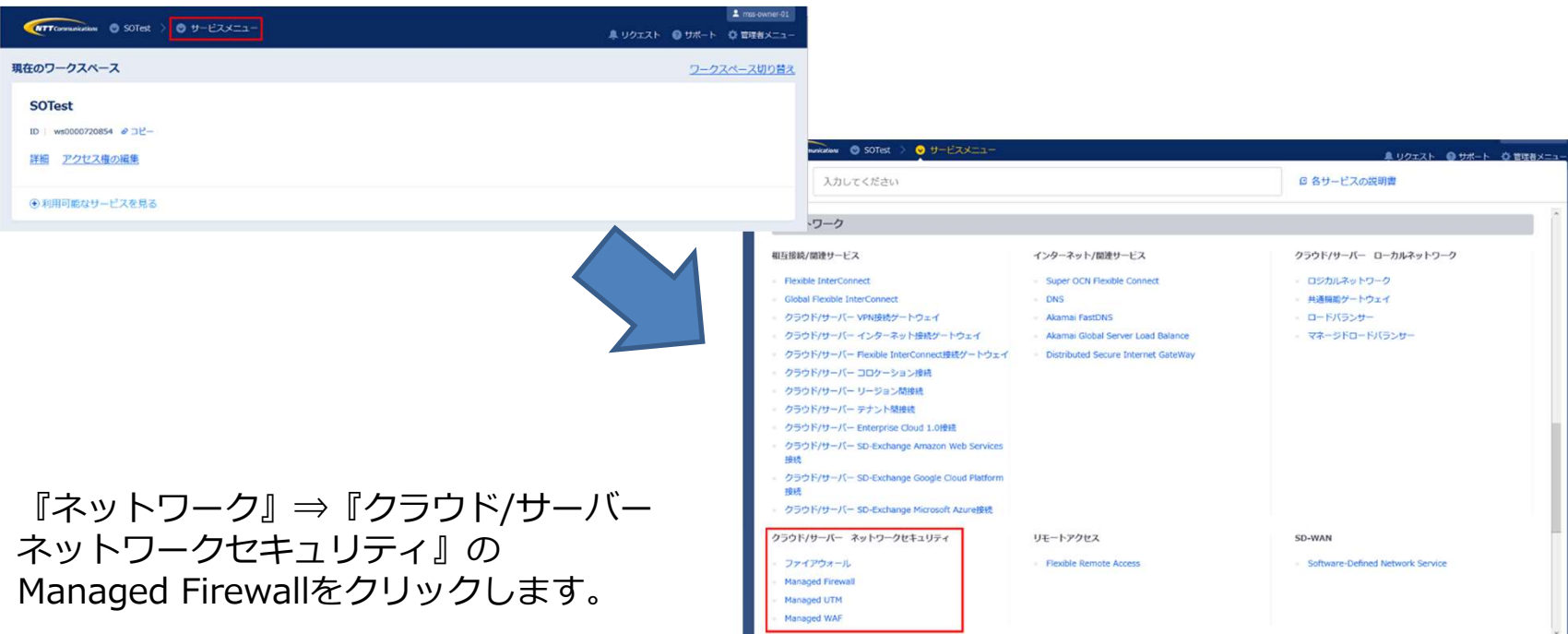
手順① M-FW申し込み

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. The top navigation bar includes 'NTT Communications', 'SOTest', and 'サービスメニュー' (Service Menu), which is highlighted with a red box. Below the navigation bar, the current workspace is identified as 'SOTest'. A large blue arrow points from the 'サービスメニュー' link in the top bar to the 'サービスメニュー' section in the main content area. This section contains a search bar and a list of services categorized into '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', and 'リモートアクセス'. Under the 'クラウド/サーバー ネットワークセキュリティ' category, 'ファイアウォール', 'Managed Firewall', 'Managed UTM', and 'Managed WAF' are listed, with 'Managed Firewall' highlighted by 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://ecl.ntt.com/documents/tutorials/security/rsts/security/order/managed_firewall_u
tm/order_new_single.html](https://ecl.ntt.com/documents/tutorials/security/rsts/security/order/managed_firewall_u
tm/order_new_single.html)

コントロールパネル画面にログイン後、
セキュリティをクリックし、M-FWのOrderをクリックください。

- クラウドコンピューティング
- Backup
- セキュリティ**
- ミドルウェア
- モニタリング
- Cloud Foundry
- DNS
- HC with Microsoft Azure



Security Menu

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

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)

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) highlighted in a red box. The bottom screenshot shows the 'Network Security' (ネットワークセキュリティ) section, 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②-1 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②-1 M-FWの設定 (ルーティングの設定)

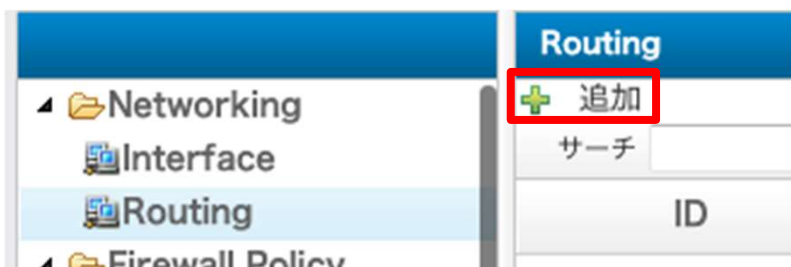
「デバイス」からいずれかのデバイスを右クリックします。



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②-1 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
参考までに、M-FW01の設定値を記載します。

Internet GWをデフォルトゲートウェイとして設定するための入力値は、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	153.254.93.206
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 (ルーティングの設定)

「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②-2 M-FWの設定 (IPsecセッティングの設定)

手順②-2 M-FWの設定 (IPsecセッティングの設定)

IPsecセッ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_v2/4901_ipsec_configuration.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), which 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 ID 'ws0000720854' and a 'サービスメニュー' (Service Menu) link. A blue arrow points from this link to the main 'サービスメニュー' page. This page features a search bar and a grid of service categories. 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 it contains sub-items: 'ファイアウォール' (Firewall), 'Managed Firewall', 'Managed UTM', and 'Managed WAF'.

『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 (IPsecセッティングの設定)

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	Operation

手順②-2 M-FWの設定 (IPsecセッティングの設定)

「デバイス」からいずれかのデバイスを右クリックします。

The screenshot shows a management console with a navigation menu at the top containing 'デバイス', 'ログ&レポート', 'サービス', 'カスタマープロフィール', and 'チケット管理'. Below the menu, the 'デバイス' section is active, displaying a table of devices. The table has columns for 'ステータス', 'デバイス名', 'HAペア', 'HAステータス', and '領域'. Two devices are listed: 'FW/UTM-NCS677' and 'openstack-NCS676'. The 'FW/UTM-NCS677' entry is highlighted with a red box. Below the table, it says 'Showing 1 - 2 of 2 entries'.

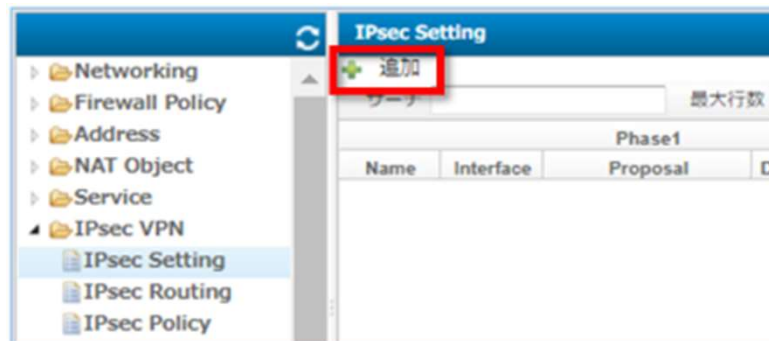
ステータス	デバイス名	HAペア	HAステータス	領域
●	FW/UTM-NCS677			jp3_zone1-groupa
●	openstack-NCS676			jp3_zone1-groupa

画面右側の「コンフィグ」をクリックします。

The screenshot shows the configuration page for the 'FW/UTM' device. The navigation menu at the top is the same as in the previous screenshot. Below the menu, the 'FW/UTM' device is selected, and there are four tabs: '概説', '詳細', 'コンフィグ', and 'ログ'. The 'コンフィグ' tab is highlighted with a red box. Below the tabs, the breadcrumb 'デバイス / FW/UTM' is visible, followed by the title 'SNMP設定'.

手順②-2 M-FWの設定 (IPsecセッティングの設定)

画面左側のオブジェクト画面から IPsec VPN をクリックします。
オブジェクト ▶ IPsec VPN ▶ IPsec Setting
画面右側の IPsec Setting 画面で [追加] をクリックします。



手順②-2 M-FWの設定 (IPsecセッティングの設定)

画面右側の [追加] をクリックし、IPsec機能で使用するパラメータを定義します。
対向機器との間でVPNトンネルを作成する為の暗号化・認証の方式を選択します。
Pre-Shared Keyは初回投入後、暗号化されます。
参考までに、M-FW01の設定値を記載します。

The screenshot shows the configuration window for IPsec phases. It is divided into sections for Phase 1 and Phase 2. Blue callout boxes point to specific fields:

- Tunnelに紐付けるIF**: Points to the 'Interface' field in the Phase 1 Tunnel section, which is set to 'port4'.
- Phase1で使用するProposal**: Points to the 'Proposal' dropdown in the Phase 1 section, set to 'aes126-sha256'.
- Phase1で使用するDHグループ**: Points to the 'DH Group' dropdown in the Phase 1 section, set to '14'.
- 対向機器のIPアドレス**: Points to the 'Remote Gateway' field in the Phase 1 Tunnel section, set to '153.254.93.218'.
- 対向機器と共通のキー**: Points to the 'Pre-Shared Key' field in the Phase 1 Tunnel section, set to 'examplekey000'.
- Phase2で使用するProposal**: Points to the 'Proposal' dropdown in the Phase 2 section, set to 'aes128-sha256'.
- Phase2で使用するProposal**: Points to the 'DH Group' dropdown in the Phase 2 section, set to '14'.

At the bottom of the window, there are 'キャンセル' (Cancel) and '保存' (Save) buttons.

手順②-2 M-FWの設定 (IPsecセッティングの設定)

「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②-3 M-FWの設定 (IPSecルーティングの設定)

手順②-3 M-FWの設定 (IPsecルーティングの設定)

IPsec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_v2/4902_ipsec_routing.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②-3 M-FWの設定 (IPsec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	Operation

手順②-3 M-FWの設定 (IPsec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。

The screenshot shows a management console with a navigation menu at the top containing 'デバイス', 'ログ&レポート', 'サービス', 'カスタマープロフィール', and 'チケット管理'. Below the menu, the 'デバイス' section is active, displaying a table of devices. The table has columns for 'ステータス', 'デバイス名', 'HAペア', 'HAステータス', and '領域'. Two devices are listed: 'FW/UTM-NCS677' and 'openstack-NCS676'. The 'FW/UTM-NCS677' device name is highlighted with a red box. Below the table, it says 'Showing 1 - 2 of 2 entries'.

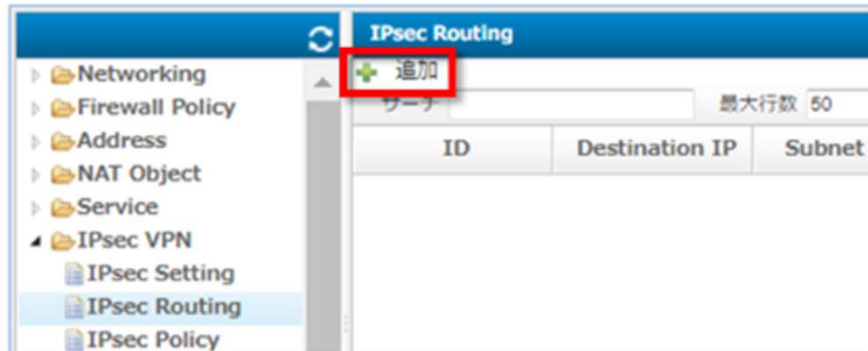
ステータス	デバイス名	HAペア	HAステータス	領域
●	FW/UTM-NCS677			jp3_zone1-groupa
●	openstack-NCS676			jp3_zone1-groupa

画面右側の「コンフィグ」をクリックします。

The screenshot shows the configuration page for the 'FW/UTM' device. The navigation menu at the top is the same as in the previous screenshot. Below the menu, the 'FW/UTM' device is selected, and there are four tabs: '概説', '詳細', 'コンフィグ', and 'ログ'. The 'コンフィグ' tab is highlighted with a red box. Below the tabs, the breadcrumb 'デバイス / FW/UTM' is visible, followed by the title 'SNMP設定'.

手順②-3 M-FWの設定 (IPsecルーティングの設定)

画面左側のオブジェクト画面から IPsec VPN をクリックします。
オブジェクト ▶ IPsec VPN ▶ IPsec Routing
画面右側の IPsec Routing画面で [追加] をクリックします。



手順②-3 M-FWの設定 (IPsecルーティングの設定)

IPsec Setting (IPsec設定) で作成したVPNトンネル宛にスタティック ルートを設定します。
設定後 [保存] をクリックしてください。

Black hole Routingが「Disable」の時は、このルーティングを設定するトンネル インターフェイスを選択してください。Black hole Routingが「Enable」のときはInterfaceは表示されません。
参考までに、M-FW01の設定値を記載します。

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

ID	5001
Destination IP	192.168.30.0
Subnet Mask	255.255.255.0
Blackhole Routing	Disable
Interface	Tunnel1
Comment	

Callouts point to the following fields:

- 送信先IPアドレス (Destination IP)
- サブネットマスク (Subnet Mask)
- Blackhole Routing 無効 (Blackhole Routing Disabled)
- Tunnel インターフェース (Tunnel Interface)

Buttons at the bottom right: キャンセル (Cancel) and 保存 (Save).

手順②-4 M-FWの設定 (IPSecポリシーの設定)

手順②-4 M-FWの設定 (IPsecポリシーの設定)

IPsec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_v2/4903_ipsec_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. A blue arrow points from this tab 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) services, 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②-4 M-FWの設定 (IPsec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②-4 M-FWの設定 (IPsec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。

The screenshot shows a management console with a navigation menu at the top containing 'デバイス', 'ログ&レポート', 'サービス', 'カスタマープロフィール', and 'チケット管理'. Below the menu, the 'デバイス' section is active, displaying a table of devices. The table has columns for 'ステータス', 'デバイス名', 'HAペア', 'HAステータス', and '領域'. Two devices are listed: 'FW/UTM-NCS677' and 'openstack-NCS676'. The 'FW/UTM-NCS677' entry is highlighted with a red box. Below the table, it says 'Showing 1 - 2 of 2 entries'.

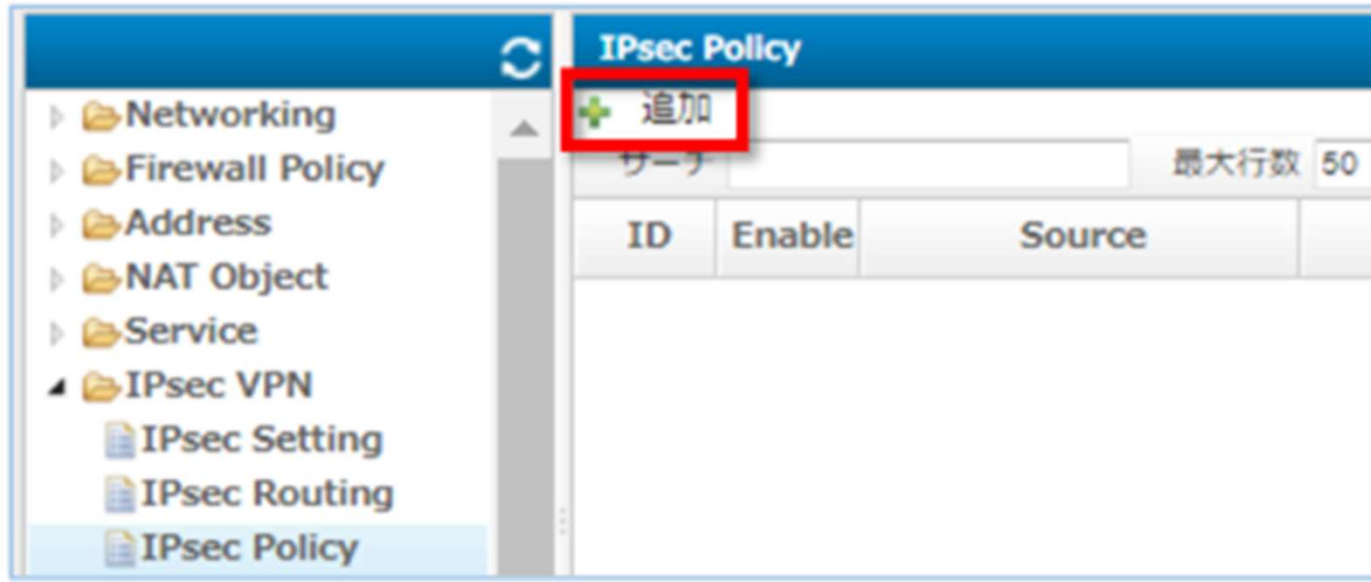
ステータス	デバイス名	HAペア	HAステータス	領域
●	FW/UTM-NCS677			jp3_zone1-groupa
●	openstack-NCS676			jp3_zone1-groupa

画面右側の「コンフィグ」をクリックします。

The screenshot shows the configuration page for the 'FW/UTM' device. The navigation menu at the top is the same as in the previous screenshot. Below the menu, the 'FW/UTM' device is selected, and there are four tabs: '概説', '詳細', 'コンフィグ', and 'ログ'. The 'コンフィグ' tab is highlighted with a red box. Below the tabs, the breadcrumb 'デバイス / FW/UTM' is visible, followed by the title 'SNMP設定'.

手順②-4 M-FWの設定 (IPsecポリシーの設定)

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



手順②-4 M-FWの設定 (IPsec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。

IPsec VPNトンネルを経由した通信についてのポリシー制御を設定します。

参考までに、M-FW01で、IPsec VPNトンネルを経由したHTTP通信を受信した場合に許可するポリシーを以下に記載します。

オブジェクト

ID 5001

Move rule No Move Move before Move after

Enable

Source

Incoming Interface Tunnel1

Source Address all

Destination

Outgoing Interface port4

Destination Address Type Address Object NAT Object

Destination Address all

Service HTTP

Action ACCEPT

NAT

Log Disable

Comments

キャンセル 保存

手順②-4 M-FWの設定 (IPsec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。

IPsec VPNトンネルを経由した通信についてのポリシー制御を設定します。

参考までに、M-FW01で、IPsec VPNトンネルを経由したHTTPS通信を受信した場合に許可するポリシーを以下に記載します。

オブジェクト

ID 5001

Move rule No Move Move before Move after

Enable

Source

Incoming Interface Tunnel1

Source Address all

Destination

Outgoing Interface port4

Destination Address Type Address Object NAT Object

Destination Address all

Service HTTPS

Action ACCEPT

NAT

Log Disable

Comments

キャンセル 保存

手順② M-FWの設定

全てのM-FWにて同様の手順でルーティング設定、IPsecセッティング設定、IPsecルーティング設定、IPsecポリシー設定をお願いいたします。

手順③-1 vFWの設定変更 (VRRP設定解除)

手順③-1 vFWの設定変更 (VRRP設定解除)

ファイアウォールのVRRP設定の解除をお願いいたします。
コントロールパネル画面にログイン後、「ネットワーク」、「ファイアウォール」をクリックし、対象のファイアウォールを選択ください。

The screenshot shows a web interface for managing vFW. On the left is a navigation menu with the following items: テナント情報, サーバー, 専用ハイパーバイザー, ストレージ, ネットワーク, インターネット接続, VPN接続, ロジカルネットワーク, マネージドファイアウォール, **ファイアウォール** (highlighted with a red box), ロードバランサー, and 共通機能ゲートウェイ. The main content area is titled 'ファイアウォール' and contains a table with the following data:

<input type="checkbox"/>	名前	説明	
<input type="checkbox"/>	FW-01	mFW IPsec test	B
<input type="checkbox"/>	FW-02	mFW IPsec test	B
<input type="checkbox"/>	FW-03	mFW IPsec test	B
<input type="checkbox"/>	FW-04	mFW IPsec test	B

Below the table, it says '4 件表示'.

手順③-1 vFWの設定変更 (VRRP設定解除)

「ファイアウォールインターフェース」タブを選択ください。
対象のインターフェースから、「VRRP用通信設定の解除」をクリック。

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	ef8dbe1a-1784-4caa-9d80-8b7fde723519	153.254.93.199	153.254.93.200	-	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	14a88507-ba81-4157-a379-694c32dd65e0	192.168.10.253	192.168.10.254	-	稼働中	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	71fb9534-9def-46cd-b0a7-8e4a4a6a55df	10.0.10.101	-	-	稼働中	ファイアウォールインターフェイスの編集

「VRRP用通信設定の解除」をクリック。**通信断が発生します。**

VRRP用通信設定の解除

仮想IPアドレス
153.254.93.200

VRID
10

説明:
本設定により、VRRP用通信設定を解除します。
本設定は、VRRPを構成するそれぞれのファイアウォールに対して必要となります。
本設定に加え、ファイアウォールのCLI/API/GUIにてVRRP設定を解除する必要があります。

取り消し **VRRP用通信設定の解除**

手順③-1 vFWの設定変更 (VRRP設定解除)

全てのvFWにて同様の手順でVRRP設定解除をお願いいたします。

手順③-2 vFWの設定変更 (インターフェースの切断)

手順③-2 vFWの設定変更 (インターフェースの切断)

vFWのインターフェースの切断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③-2 vFWの設定変更 (インターフェースの切断)

対象のインターフェースから、「ロジカルネットワークの切断」をクリック。

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	ef8dbe1a-1784-4caa-9d80-8b7fde723519	153.254.93.199	-	-	稼働中	ファイアウォールインターフェースの編集 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	14a88507-ba81-4157-a379-694c32dd65e0	192.168.10.253	-	-	稼働中	ファイアウォールインターフェースの編集
dp0s6	-	3	-	-	-	-	停止中	ファイアウォールインターフェースの編集
dp0s7	-	4	71fb9534-9def-46cd-b0a7-8e4a4a6a55df	10.0.10.101	-	-	稼働中	ファイアウォールインターフェースの編集

「ロジカルネットワークの切断」をクリック

ロジカルネットワークの切断

ロジカルネットワーク*

Internet-Segment-01 (153.254.93.192/28)

IP アドレス

153.254.93.199

説明:

ファイアウォールからロジカルネットワークを切断します。

ロジカルネットワークの切断には、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。

手順③-2 vFWの設定変更 (インターフェースの切断)

全てのvFWにて同様の手順で外部セグメントとLBセグメントのインターフェースの切断をお願いいたします。

手順④-1 M-FWの設定 (インターフェースの設定)

手順④-1 M-FWの設定 (インターフェースの設定)

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 'サービスメニュー' (Service Menu) link. A blue arrow points from this link to the main content area. The main content area 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' option 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④-1 M-FWの設定 (インターフェースの設定)

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④-1 M-FWの設定 (インターフェースの設定)

[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④-1 M-FWの設定 (インターフェースの設定)

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。

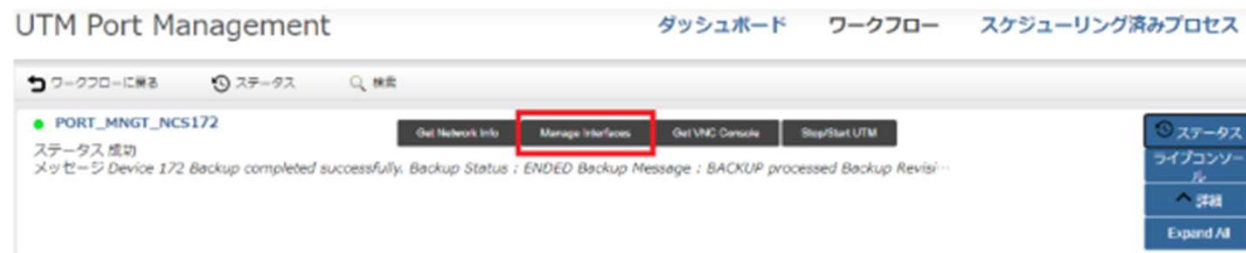
タスクステータス

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

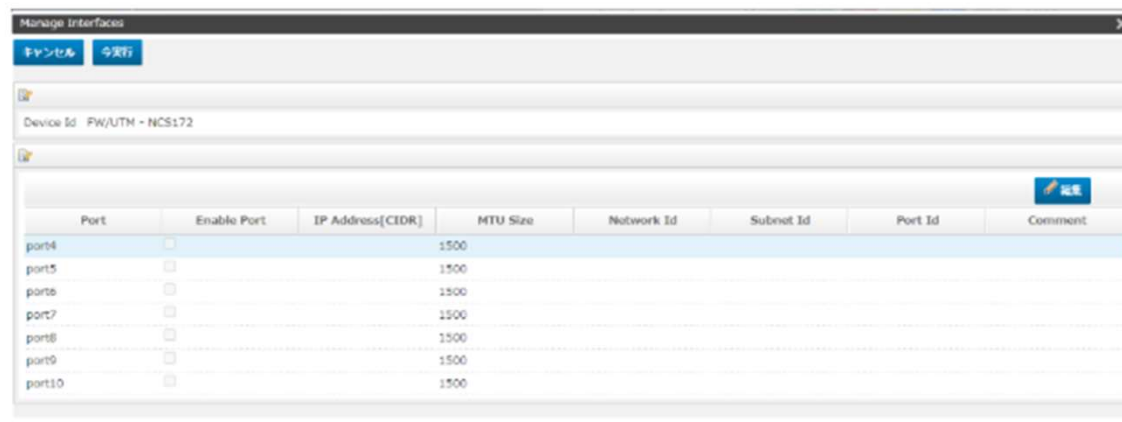
クローズ

手順④-1 M-FWの設定 (インターフェースの設定)

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④-1 M-FWの設定 (インターフェースの設定)

[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。
参考までに、M-FW01の設定値を記載します。

キャンセル	保存
-------	----

Port	port4
Enable Port	<input checked="" type="checkbox"/>
IP Address[<small>CIDR</small>]	153.254.93.199/28
MTU Size	1500
Network Id	Internet-Segment-01
Subnet Id	153.254.93.192/28
Port Id	
Comment	

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④-1 M-FWの設定 (インターフェースの設定)

[Enable Port] をチェックすると設定値を入力できます。

LB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。

参考までに、M-FW01の設定値を記載します。

<input type="button" value="キャンセル"/> <input type="button" value="保存"/>	
	
Port	port4
Enable Port	<input checked="" type="checkbox"/>
IP Address[<small>CIDR</small>]	192.168.10.254/24
MTU Size	1500
Network Id	LB-Segment-01
Subnet Id	192.168.10.0/24
Port Id	
Comment	

Port5に付与するIPアドレス

Port5に接続するネットワークアドレス

手順④-1 M-FWの設定 (インターフェースの設定)

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④-1 M-FWの設定 (インターフェースの設定)

[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④-1 M-FWの設定 (インターフェースの設定)

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 : 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 : f4f775e8-012-4937-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-a6a2-149bf2c26129
↓			
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④-1 M-FWの設定 (インターフェースの設定)

全てのM-FWにて同様の手順でインターフェースの設定をお願いいたします。
1台目のM-FW (M-FW01, M-FW03) のLAN側のIPアドレスに、vFWのVIPを割り当てているため
2台目のM-FW (M-FW02, M-FW04) のLAN側のIPアドレスに、vFWのVIP 以外を割り当てて
下さい。

手順④-2 M-FW状態確認 IPsec状態確認

手順④-2 M-FWの設定 (IPsec状態確認)

M-FWのIPsec状態の確認が可能です。

https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/operation/managed_firewall_utm_v2/4007_ipsec_status_via_w.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 'サービスメニュー' (Service Menu) and '管理メニュー' (Management Menu). The main content area is divided into sections: '現在のワークスペース' (Current Workspace) showing 'SOTest' with ID 'ws0000720854', and 'ワーク' (Work) which contains a grid of service categories. A blue arrow points from the 'サービスメニュー' link in the top bar to the 'サービスメニュー' section in the main content. Within the 'ワーク' 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 its sub-items, including 'Managed Firewall', are also 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④-2 M-FWの設定 (IPsec状態確認)

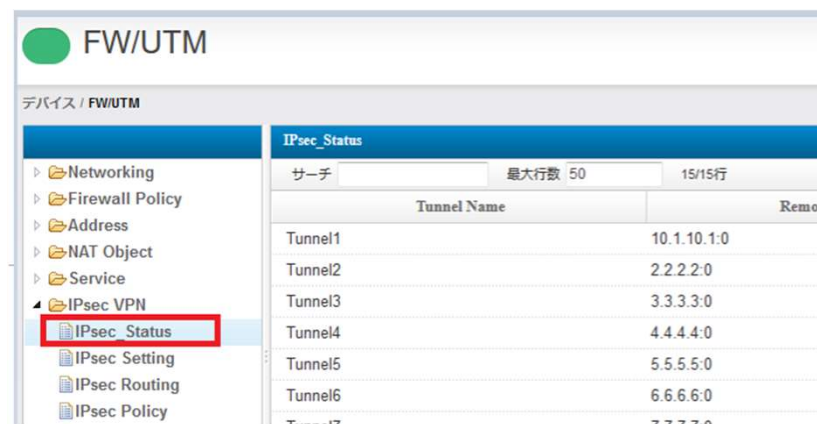
Managed Firewall(Version2)の「Operation」をクリックしてください。

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④-2 M-FWの設定 (IPsec状態確認)

[デバイス管理]に表示されるUTMデバイスをクリック後、コンフィグを選択肢、[IPsec Status] をクリックすると、IPsec セットィング で設定したIPsecのステータスを確認できる画面が開きます。



手順④-2 M-FWの設定 (IPsec状態確認)

最新の情報を取得するためには[デバイスからの同期]を押してください。

