

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(外接 点設置構成)

第1版

前提条件

前提条件

■ ファイアウォール(Brocade 5600 vRouter)(以下、vFW)の外接点にManaged Firewall(以下、M-FW)が設置されている場合に、vFWから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。
- **M-FWでIPsecを確立後、vFWのIPsecを切断します。**
⇒ vFWのIPsec切断中、通信断が発生いたします。

※事前検証を行ってから移行を実施ください。

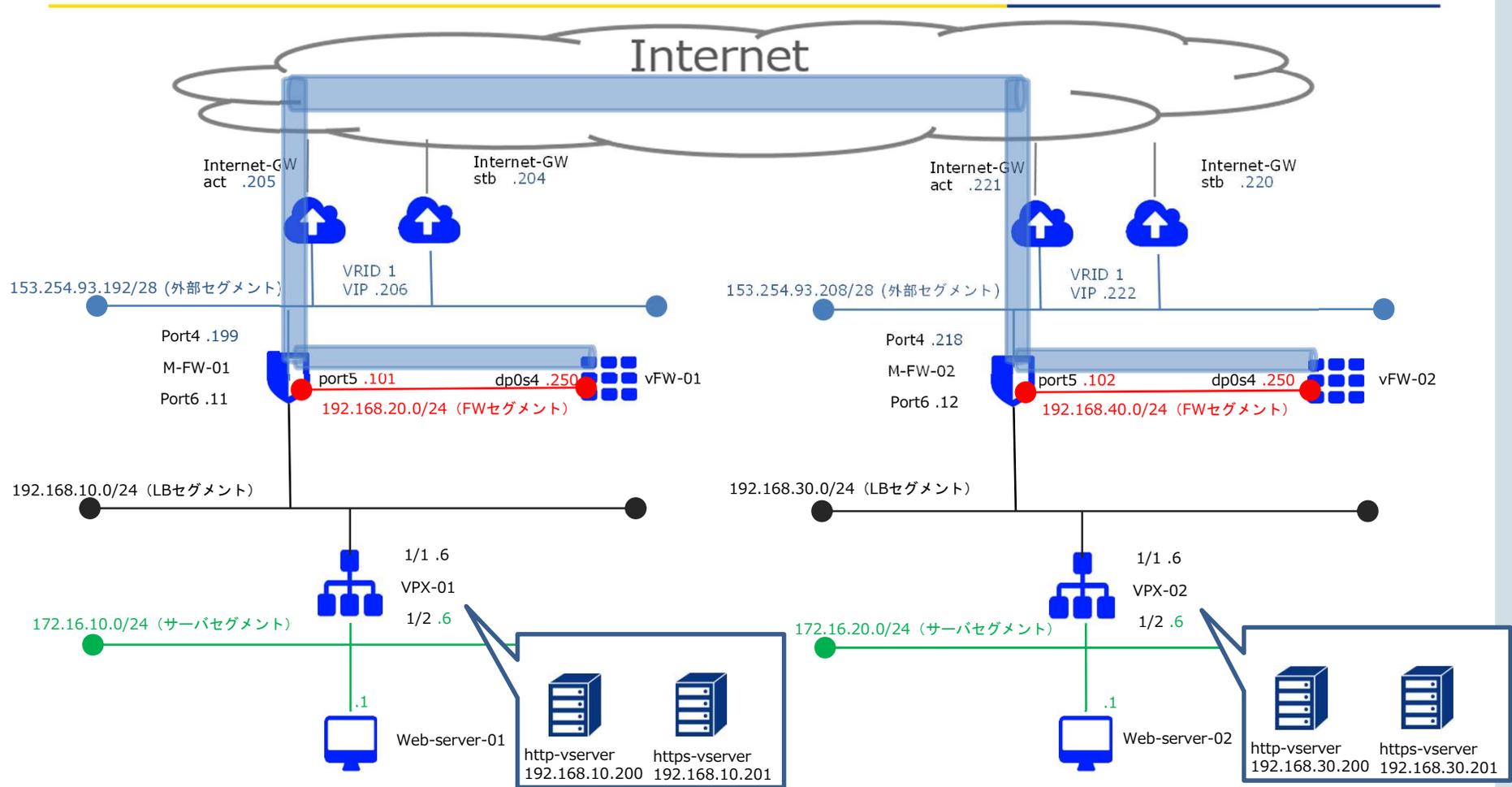
注意事項

- 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ございます。
また下記の要件を満たす必要がございます。
 - 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)



IPsecVPN

- 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 '10.1.1.2/30'  
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 '2'  
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 id '153.254.93.199'  
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 '192.168.20.101'  
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-02(IPsec)の設定

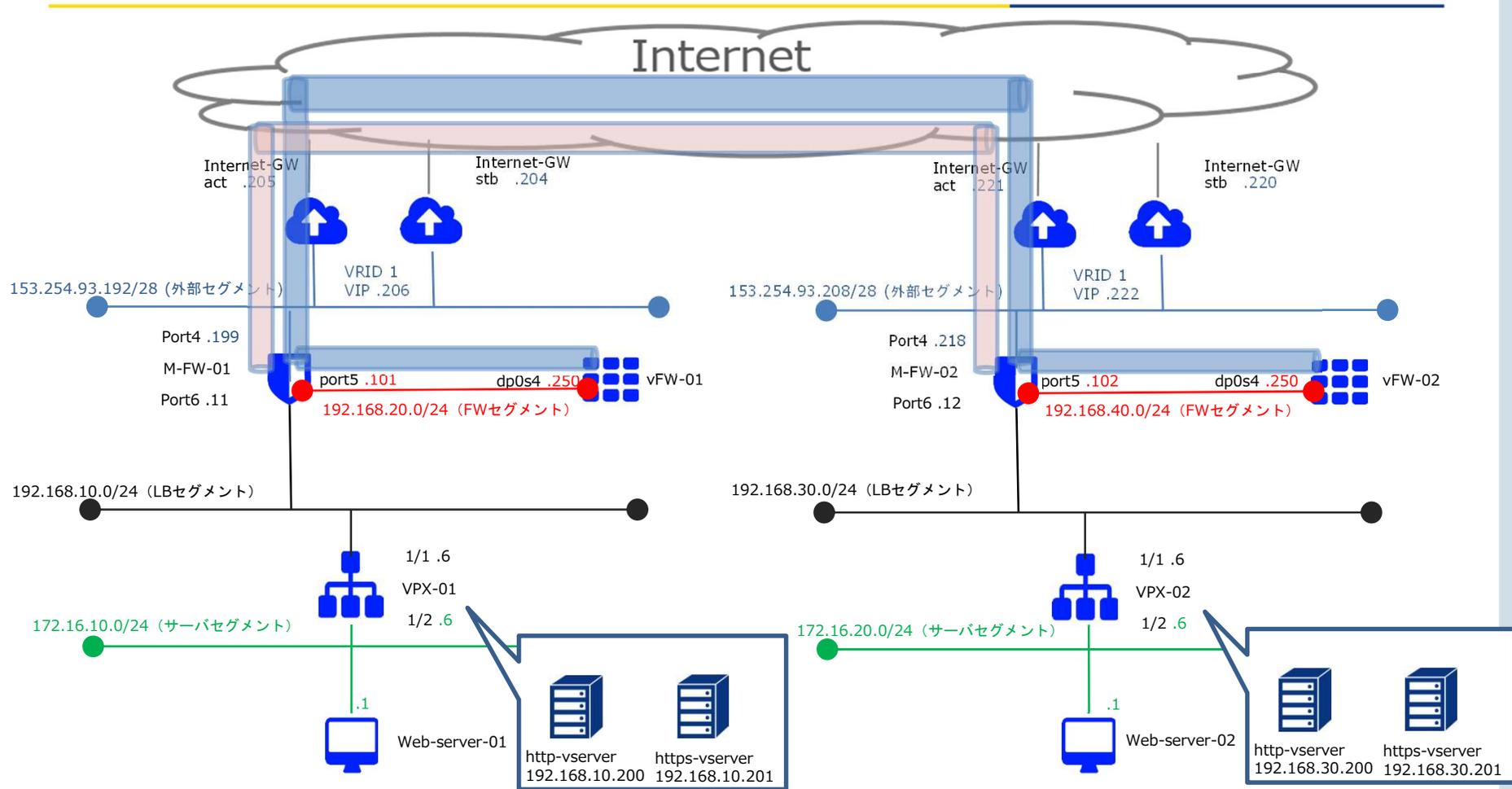
```
set interfaces vti vti0 address '10.1.1.1/30'  
set security vpn ipsec esp-group ESP-1W lifetime '3600'  
set security vpn ipsec esp-group ESP-1W proposal 1 encryption 'aes256'  
set security vpn ipsec esp-group ESP-1W proposal 1 hash 'sha2_256'  
set security vpn ipsec ike-group IKE-1W lifetime '28800'  
set security vpn ipsec ike-group IKE-1W proposal 1 dh-group '2'  
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 id '153.254.93.218'  
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 '192.168.40.102'  
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-02(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'
```

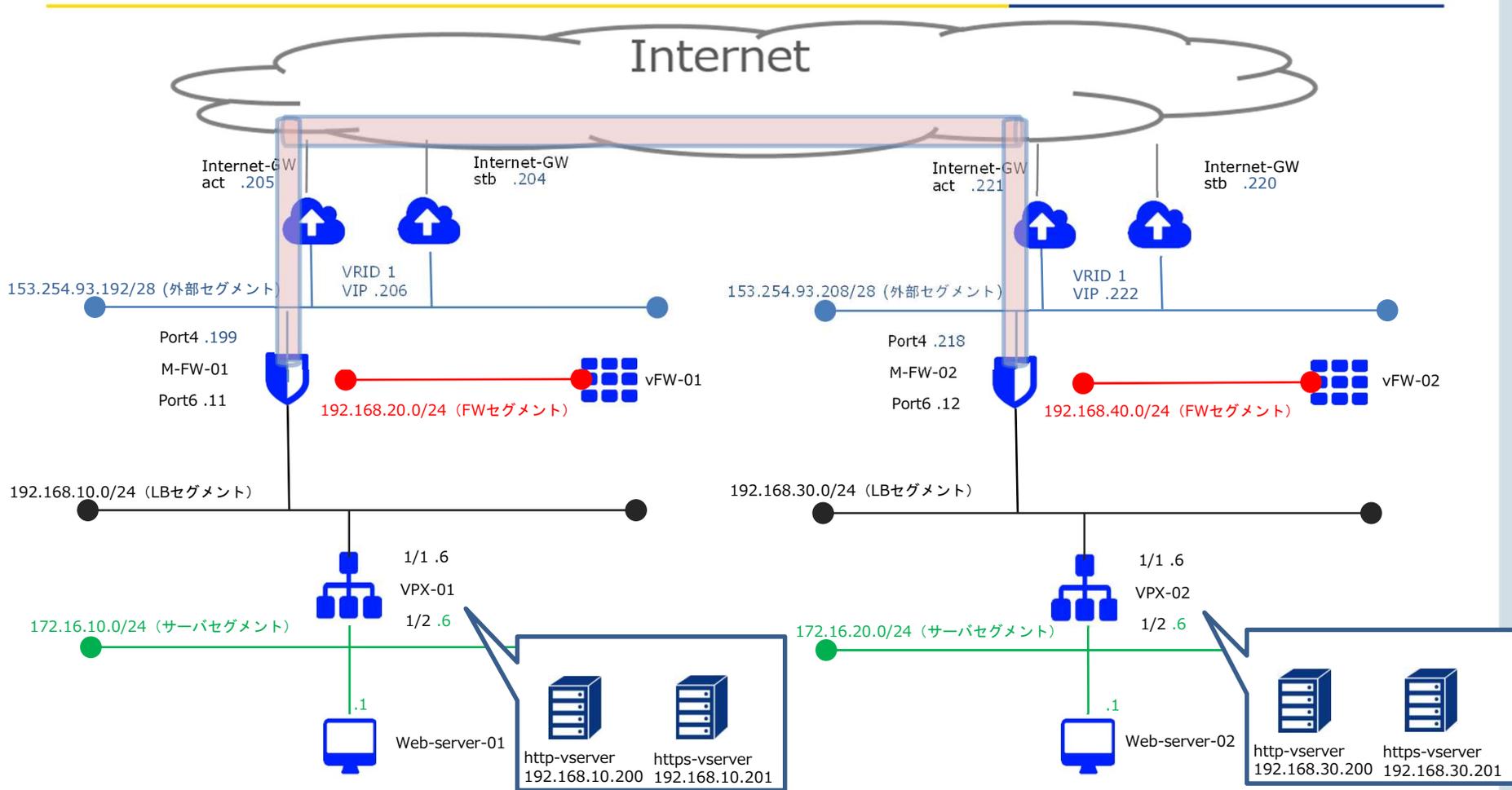
移行時構成①



手順① M-FW設定

1. IPsec設定
2. IPsecルーティング設定
3. IPsecポリシー設定
4. IPsecVPN状態確認

移行時構成②

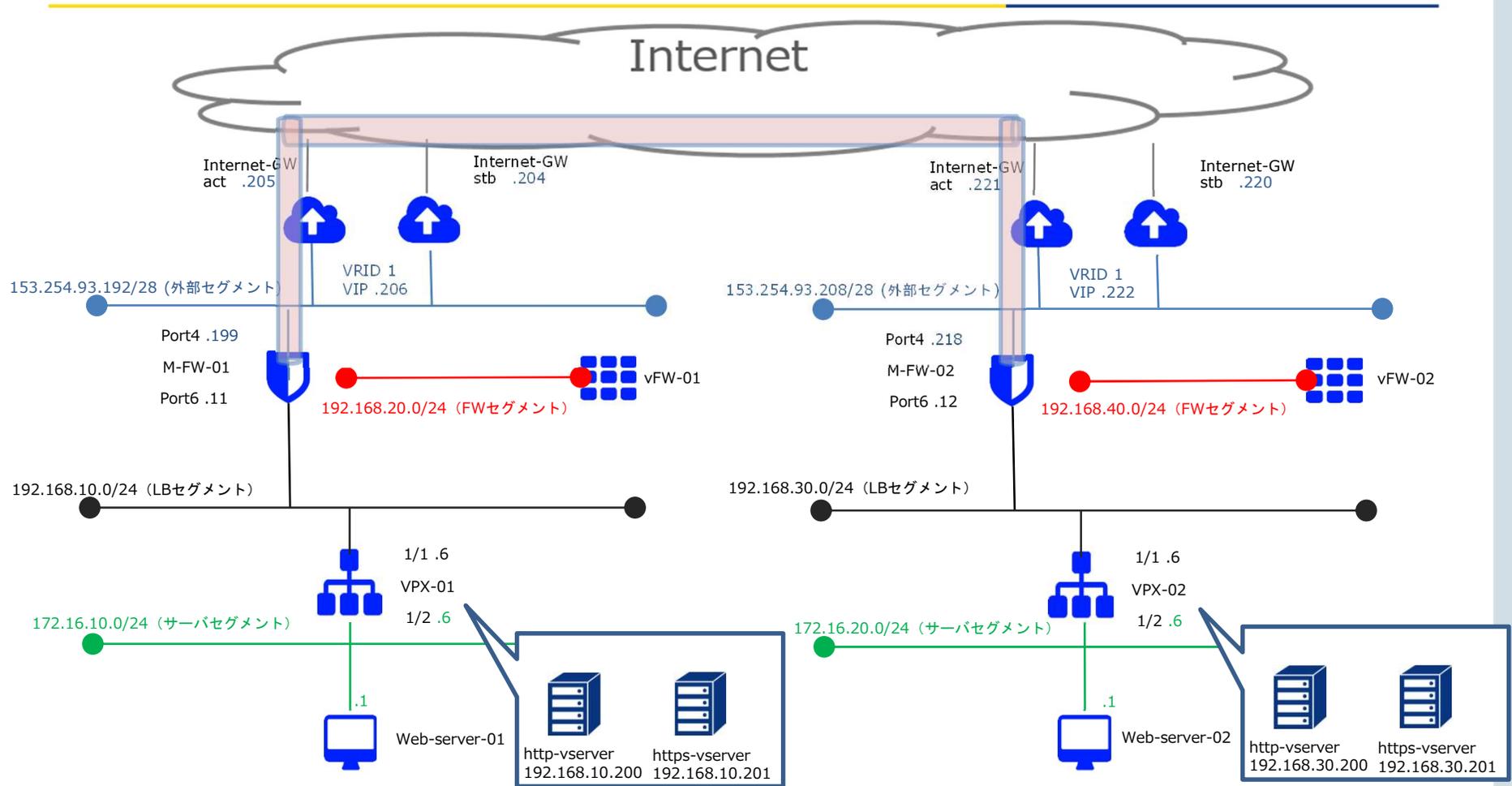


IPsecVPN

断時間：10分程度
(実測値)

手順② M-FWの設定変更(通信断発生/IF切断完了後回復)
1. Vyatta向けIFの切断

移行時構成③

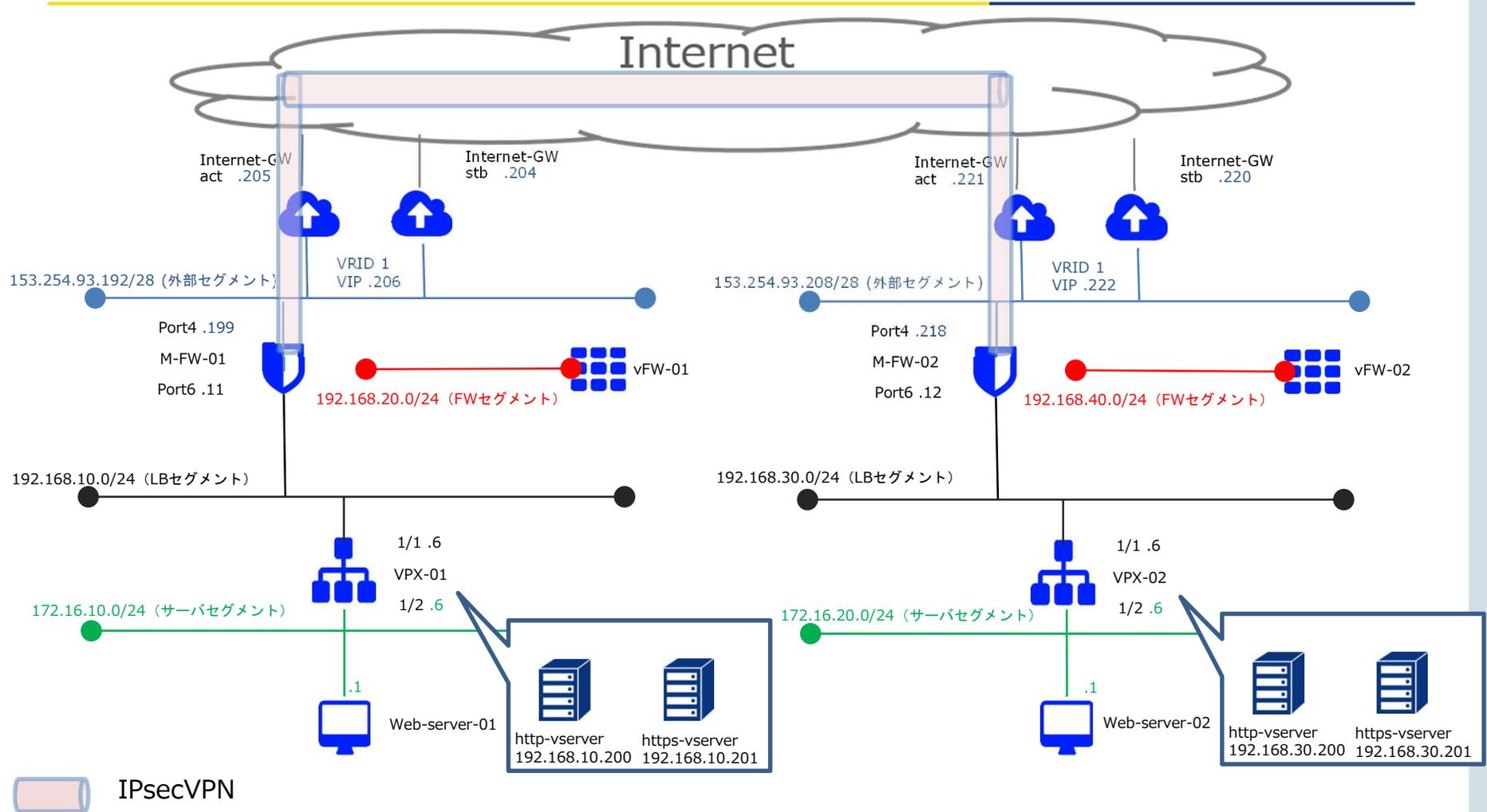


IPsecVPN

手順③ M-FW設定変更

1. vFW 向けルーティングの削除
2. vFW IPsec用DstNATポリシーの削除
3. vFW IPsec用DstNATオブジェクトの削除

移行完了構成 (Managed Firewall構成)



手順①-1 M-FWの設定 (IPsecセッティングの設定)

手順①-1 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 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①-1 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①-1 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 web interface with a navigation bar at the top containing tabs for 'デバイス' (Devices), 'ログ&レポート' (Logs & Reports), 'サービス' (Services), 'カスタマープロフィール' (Customer Profiles), and 'チケット管理' (Ticket Management). Below the navigation bar, the 'デバイス' section is active, displaying a table of devices. The table has columns for 'ステータス' (Status), 'デバイス名' (Device Name), 'HAペア' (HA Pair), 'HAステータス' (HA Status), and '領域' (Area). 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

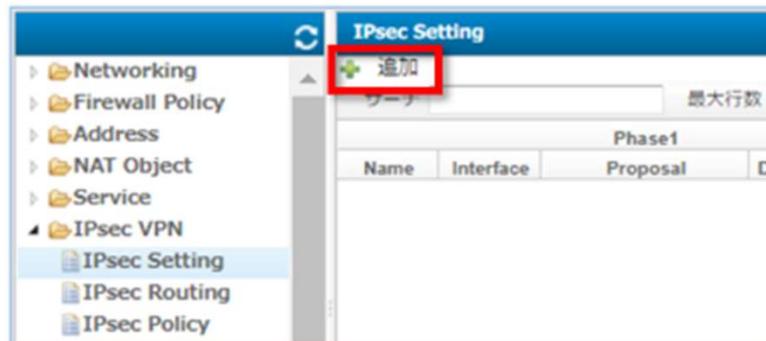
画面右側の「コンフィグ」をクリックします。



The screenshot shows the configuration page for the 'FW/UTM' device. The navigation bar at the top is the same as in the previous screenshot. Below it, the 'FW/UTM' device is selected, and there are four tabs: '概説' (Overview), '詳細' (Details), 'コンフィグ' (Configuration), and 'ログ' (Logs). 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①-1 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①-1 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 an IPsec tunnel. It is divided into two phases, Phase 1 and Phase 2. Blue callout boxes point to specific fields with the following labels:

- 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 menu in the Phase 1 section, which is set to 'aes126-sha256'.
- Phase1で使用するDHグループ**: Points to the 'DH Group' dropdown menu in the Phase 1 section, which is 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, which is 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, which is set to 'examplekey000'.
- Phase2で使用するProposal**: Points to the 'Proposal' dropdown menu in the Phase 2 section, which is set to 'aes128-sha256'.
- Phase2で使用するProposal**: Points to the 'DH Group' dropdown menu in the Phase 2 section, which is set to '14'.

At the bottom of the window, there are 'キャンセル' (Cancel) and '保存' (Save) buttons. A 'Comments' field is also visible at the bottom left.

手順①-1 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①-2 M-FWの設定 (IPsecルーティングの設定)

手順①-2 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 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①-2 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①-2 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 bar 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 navigation bar, 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'.

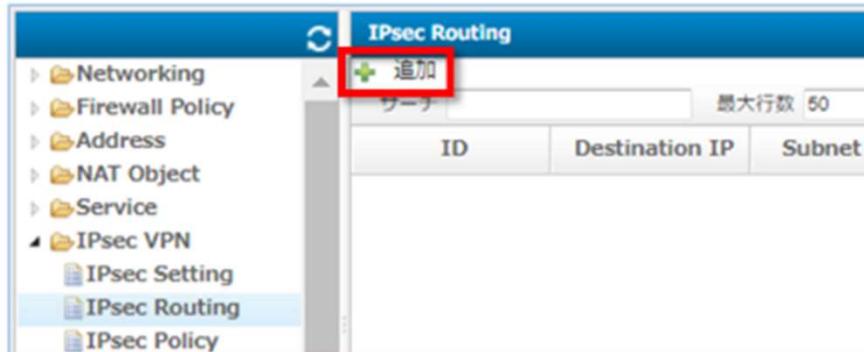
ステータス	デバイス名	HAペア	HAステータス	領域
●	FW/UTM-NCS677			jp3_zone1-groupa
●	openstack-NCS676			jp3_zone1-groupa

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 bar at the top is the same as in the previous screenshot. Below the navigation bar, the device name 'FW/UTM' is displayed with a green status indicator. To the right of the device name, there are four buttons: '概説', '詳細', 'コンフィグ', and 'ログ'. The 'コンフィグ' button is highlighted with a red box. Below the device name, there is a breadcrumb trail 'デバイス / FW/UTM' and a sub-section header 'SNMP設定'.

手順①-2 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①-2 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。

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

送信先IPアドレス

サブネットマスク

Blackhole Routing 無効

Tunnel インターフェース

キャンセル 保存

手順①-2 M-FWの設定 (IPsec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①-3 M-FWの設定 (IPSecポリシーの設定)

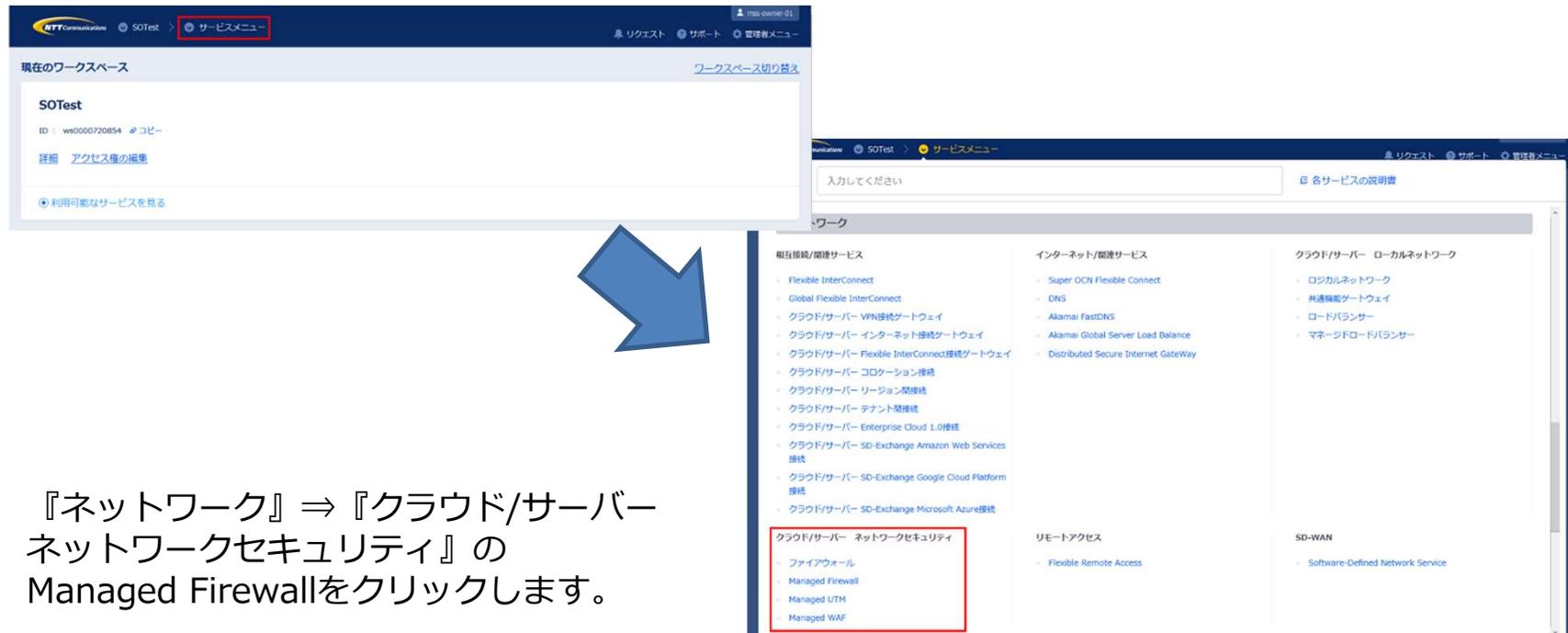
手順①-3 M-FWの設定 (IPsecポリシーの設定)

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) highlighted in a red box. A blue arrow points from this box 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①-3 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①-3 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'.

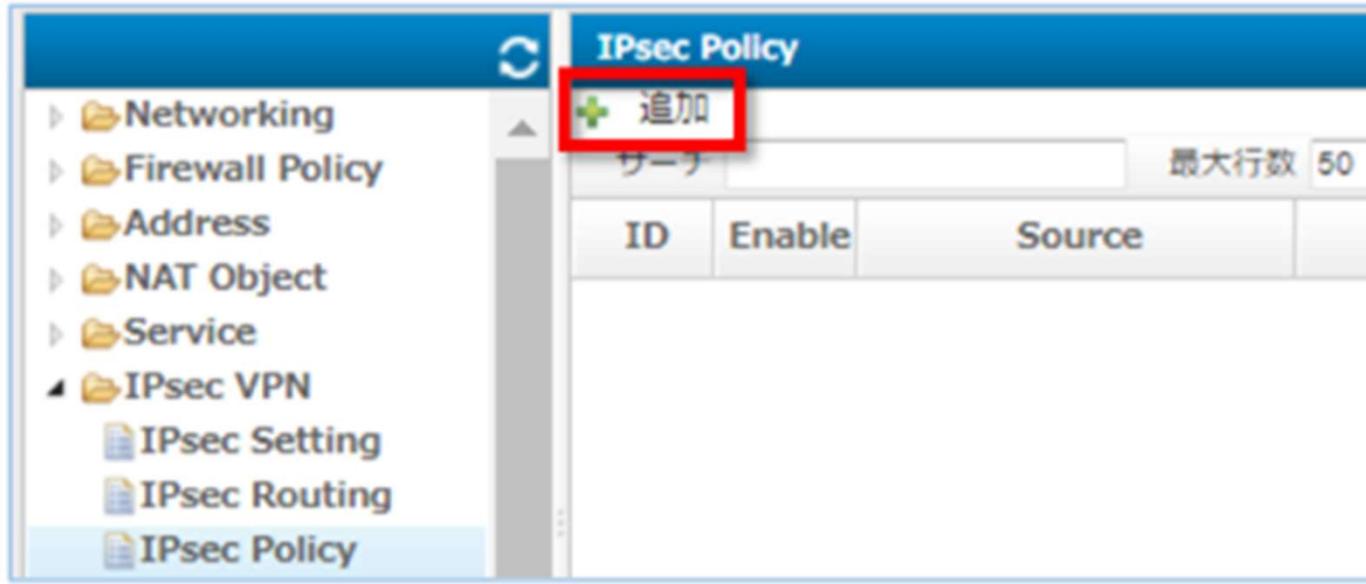
ステータス	デバイス名	HAペア	HAステータス	領域
●	FW/UTM-NCS677			jp3_zone1-groupa
●	openstack-NCS676			jp3_zone1-groupa

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 the 'コンフィグ' button is highlighted with a red box. Other buttons visible are '概説', '詳細', and 'ログ'. Below the buttons, the breadcrumb 'デバイス / FW/UTM' and the title 'SNMP設定' are visible.

手順①-3 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①-3 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①-3 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①-3 M-FWの設定 (IPSec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① M-FWの設定

対向のM-FWにて同様の手順でオブジェクト設定、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。

対向のM-FWにて各種設定が完了後、IPSec接続が確立されます。

手順①-4 M-FWの設定 (IPsec状態確認)

手順①-4 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) highlighted with a red box. Below it, the '現在のワークスペース' (Current Workspace) section shows 'SOTest' with a red box around the 'サービスメニュー' link. A blue arrow points from this link to the main 'サービスメニュー' page. The main page displays a search bar and a grid of service categories. Under 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, 'Managed Firewall' is 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①-4 M-FWの設定 (IPsec状態確認)

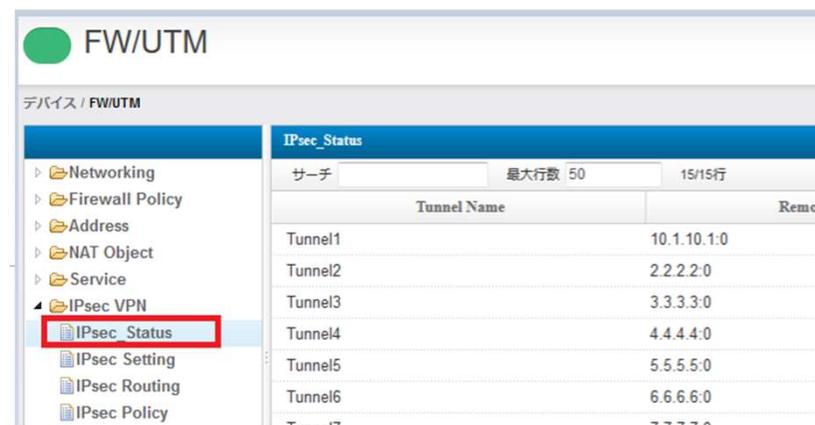
Managed Firewall(Version2)の「Operation」をクリックしてください。

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

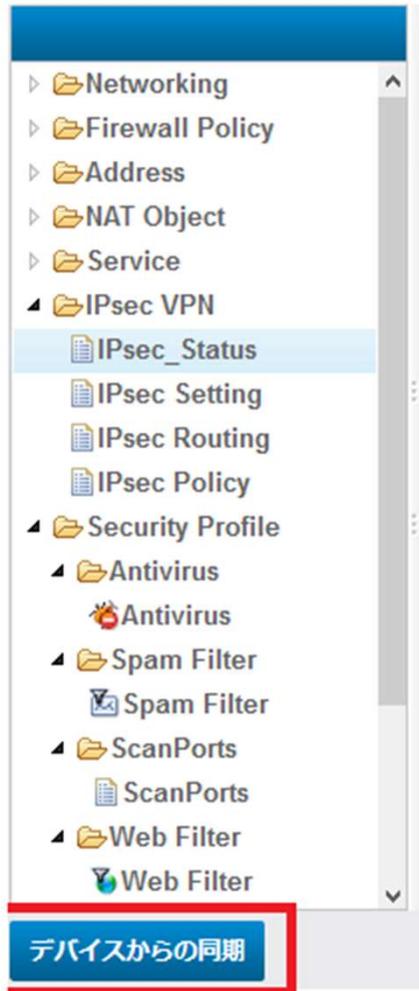
手順①-4 M-FWの設定 (IPsec状態確認)

[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①-4 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。



手順② M-FWの設定変更 (Vyatta向けIFの切断)

手順② M-FWの設定変更 (Vyatta向けIFの切断)

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. The top navigation bar includes 'サービスメニュー' (Service Menu) and 'サポート' (Support). 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 'サービスメニュー' (Service Menu) which is expanded to show various services. A blue arrow points from the 'サービスメニュー' link in the top navigation to the 'サービスメニュー' section in the main content. Within the 'サービスメニュー' 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.

『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の設定変更 (Vyatta向けIFの切断)

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 M-FWの設定変更 (Vyatta向けIFの切断)

[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。

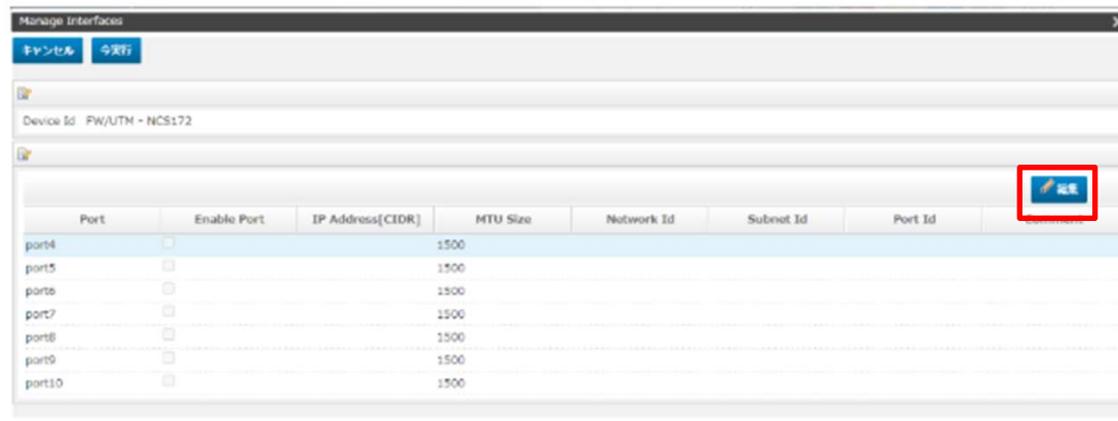


手順② M-FWの設定変更 (Vyatta向けIFの切断)

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② M-FWの設定変更 (Vyatta向けIFの切断)

[Enable Port] のチェックを外すと該当Portが無効になります。
[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 port5

Enable Port

MTU Size 1500

Comment

Portを無効

手順② M-FWの設定変更 (Vyatta向けIFの切断)

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。
通信断が発生します。

Manage Interfaces

キャンセル 今実行

Device Id FW/UTM - NCS172

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	int1	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② M-FWの設定変更 (Vyatta向けIFの切断)

[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② M-FWの設定変更 (Vyatta向けIFの切断)

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② M-FWの設定変更 (Vyatta向けIFの切断)

対向のM-FWにて同様の手順でFW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。

対向のM-FWにてFWセグメント向けインターフェースを切断後、**通信が回復いたします。**

手順③-1 M-FWの設定変更 (vFW 向けルーティングの削除)

手順③-1 M-FWの設定変更 (vFW 向けルーティングの削除)

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 screenshot shows the SDPF portal interface. At the top, the 'サービスメニュー' (Service Menu) button is highlighted with a red box. Below it, 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 'サービスメニュー' page. On the main page, the 'ワーク' (Work) 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) category is highlighted with a red box. Under this category, 'Managed Firewall' is listed.

『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の設定変更 (vFW 向けルーティングの削除)

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②-1 M-FWの設定 (ルーティングの設定)

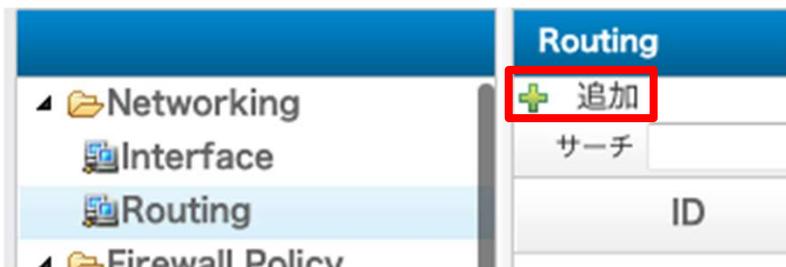
「デバイス」からいずれかのデバイスを右クリックします。



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③-1 M-FWの設定変更 (vFW 向けルーティングの削除)

デバイス管理から該当デバイスの"UTM"を右クリックし、[デバイス管理] をクリックしてください。



手順③-1 M-FWの設定変更 (vFW 向けルーティングの削除)

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

GatewayがVyatta IF向けのルーティングを選択し [削除] をクリックします。

Routing

検索 [] 最大行数 50 4/4行

ID	Destination IP	Subnet Mask	Gateway	Interface	Comment
1	0.0.0.0	0.0.0.0	153.254.93.205	port4	
➔ 2	172.16.20.0	255.255.255.0	192.168.20.101	port5	
3	192.168.30.0	255.255.255.0	192.168.20.101	port5	
4	172.16.10.0	255.255.255.0	192.168.10.6	port5	

[OK] をクリックし、削除してください。

確認 ✕

オブジェクトを削除しますか？

キャンセル OK

手順③-1 M-FWの設定変更 (vFW 向けルーティングの削除)

「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③-2 M-FWの設定変更 (vFW IPsec用DstNATの削除)

手順③-2 M-FWの設定変更 (vFW IPsec用DstNATの削除)

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の設定変更 (vFW IPsec用DstNATの削除)

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の設定変更 (vFW IPsec用DstNATの削除)

「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 the 'Devices' page with a table of devices. The first row is highlighted with a red box.

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

Showing 1 - 2 of 2 entries

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 'コンフィグ' button is highlighted with a red box.

FW/UTM

概説 詳細 **コンフィグ** ログ

デバイス / FW/UTM

SNMP設定

手順③-2 M-FWの設定変更 (vFW IPsec用DstNATの削除)

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
対象のファイアウォールポリシーを選択し [削除] をクリックします。

Firewall Policy

+ 追加 編集 上へ移動 下へ移動 複製 **削除**

サーチ 最大行数 50 3/3行

ID	Enable	Source	Destination	Service	Action
➔ 1	<input checked="" type="checkbox"/>	Port4-all	Port4-Port4DNAT	HTTPS	ACCEPT
2	<input checked="" type="checkbox"/>	Port5-all	Port4-all	SSH	ACCEPT
3	<input checked="" type="checkbox"/>	Port5-all	Port6-all	SSH	ACCEPT

[OK] をクリックし、削除してください。

確認

オブジェクトを削除しますか？

キャンセル OK

手順③-2 M-FWの設定変更 (vFW IPsec用DstNATの削除)

「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③-3 M-FWの設定変更 (vFW IPsec用DstNATオブジェクト の削除)

手順③-3 M-FWの設定変更 (vFW IPsec用DstNATオブジェクトの削除)

Destination NATの設定は下記をご覧ください。。

https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/operation/managed_firewall_utm_v2/4330_destination_nat.html

SDPFポータルからアクセス

ワークスペースを選択後、Smart Data Platform ポータルのダッシュボード画面、またはダッシュボード⇒ワークスペース一覧画面の『サービスメニュー』をクリックします。

『ネットワーク』⇒『クラウド/サーバー ネットワークセキュリティ』の Managed Firewallをクリックします。

手順③-3 M-FWの設定変更 (vFW IPsec用DstNATオブジェクトの削除)

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の設定変更 (vFW IPsec用DstNATオブジェクトの削除)

「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。



手順③-3 M-FWの設定変更 (vFW IPsec用DstNATオブジェクトの削除)

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
対象の NAT Object を選択し [削除] をクリックします。



[OK] をクリックし削除します。



手順③-3 M-FWの設定変更 (vFW IPsec用DstNATオブジェクトの削除)

「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③ M-FWの設定変更

対向のM-FWにて同様の手順でルーティング設定、ファイアウォールポリシー設定、Destination NAT設定の変更をお願いいたします。