

IPsec(サイト間トンネル) 機能 利用時の移行②

第1版

前提条件

前提条件

■ IPsecをファイアウォール(vFW 5600 vRouter)(以下、vFW)でご利用されている場合に、**外接点にManaged Firewall(以下、M-FW)を設置する実施方法です。**

- ・ vFWで利用しているネットワークの外側にM-FWを設置します。
⇒ vFWで利用しているネットワークの接続解除から、vFWおよびM-FWの設定変更完了まで、通信断の時間が発生いたします。

■ MFWでIPsec対応後にMFWでIPsecをご利用予定の方はIPsec移行構成-サイト間トンネル利用時②.pptxの資料による移行方法も合わせてご検討ください。

■参考 ①と② (本資料) の比較

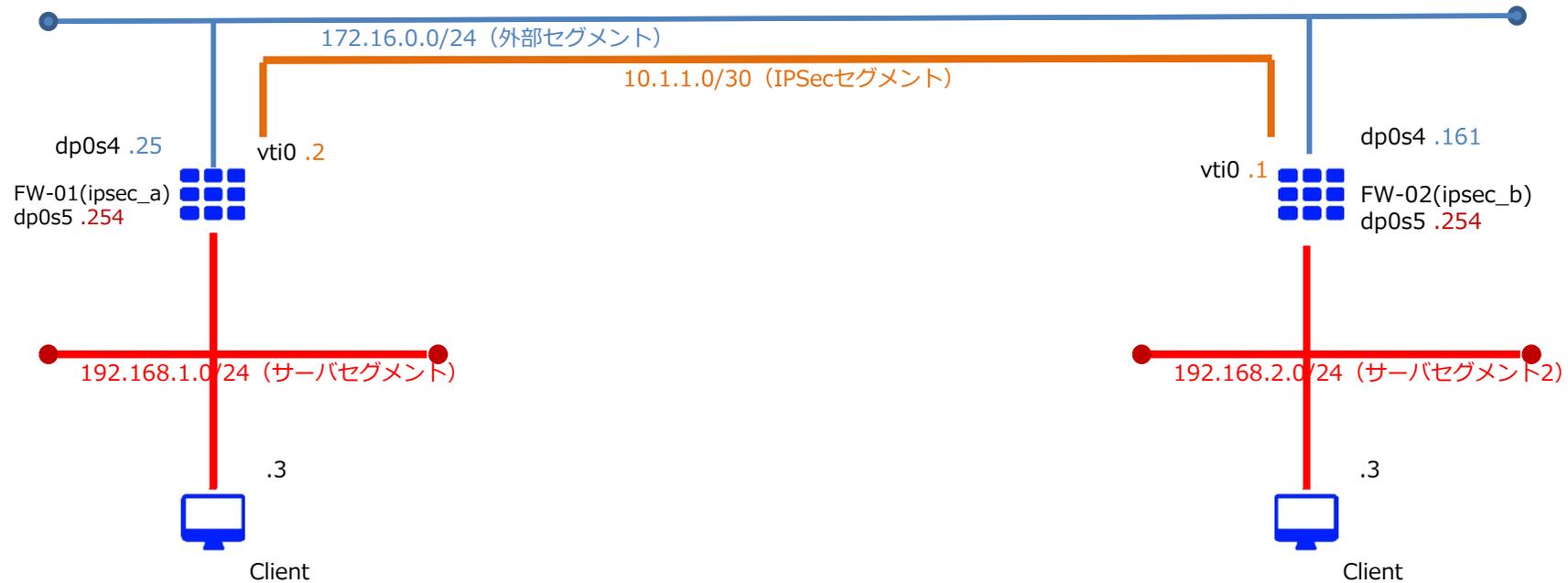
	設定項目	①資料	②資料 (本資料)
初期導入時	vFWのネットワーク設定	1回	3回
	ルーティングの追加	無	有
MFWでのIPsec対応後の移行	vFWのLNW切断回数	2回	0回
	MFWのネットワーク設定	1回	0回

※移行必要な動作は上記以外にもありますが、①資料と②資料の差のみ記載してあります。

※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

検証環境構成図 Managed FW差し込みパターン①



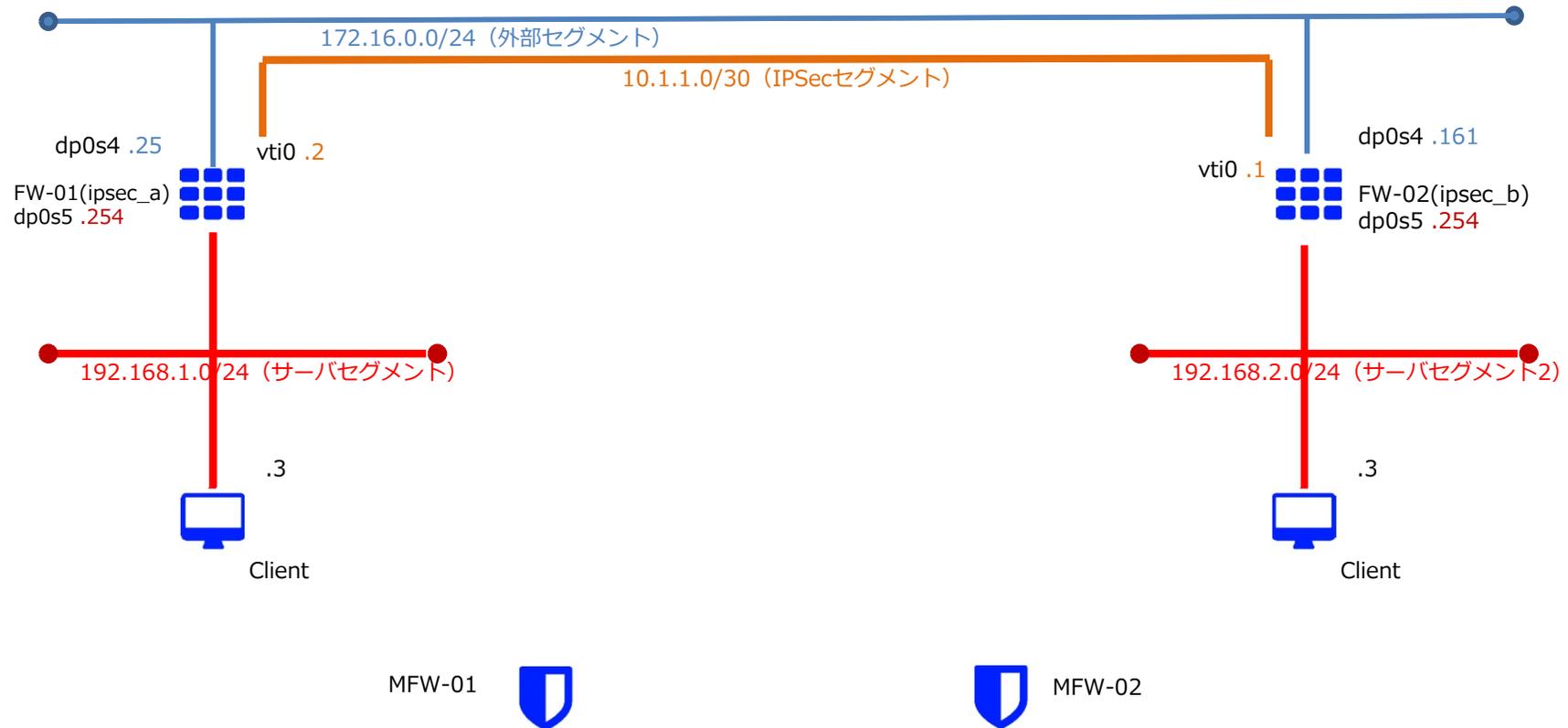
FW-01(ipsec_a)の設定

```
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 'sha1'
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 'sha1'
set security vpn ipsec site-to-site peer 172.16.0.161 authentication pre-shared-secret 'test_key_1'
set security vpn ipsec site-to-site peer 172.16.0.161 ike-group 'IKE-1W'
set security vpn ipsec site-to-site peer 172.16.0.161 local-address ' 172.16.0.25 '
set security vpn ipsec site-to-site peer 172.16.0.161 vti bind 'vti0'
set security vpn ipsec site-to-site peer 172.16.0.161 vti esp-group 'ESP-1W'
set protocols static interface-route 192.168.2.0/24 next-hop-interface 'vti0'
```

FW-02(ipsec_a)の設定

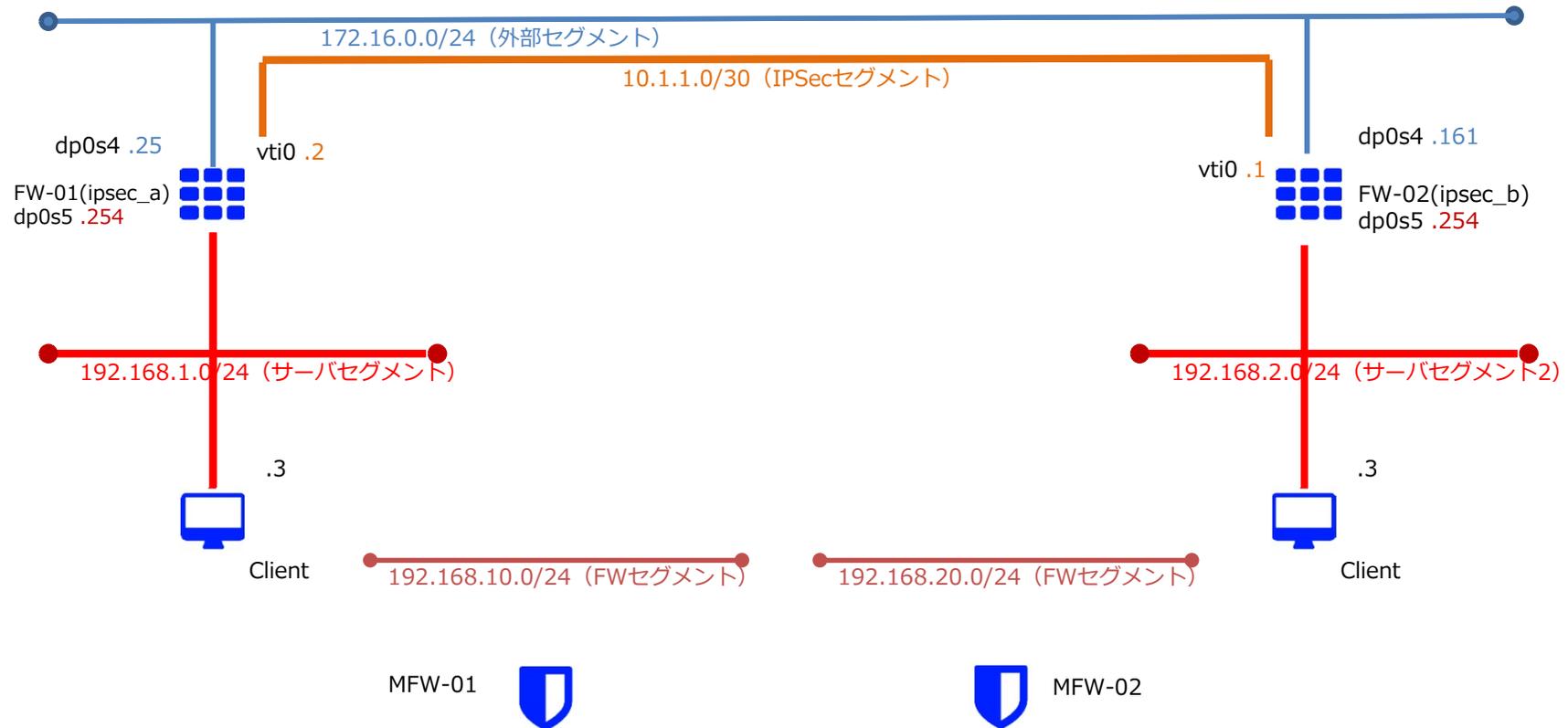
```
set interfaces vti vti0 address '10.1.1.1/30'
set security vpn ipsec esp-group ESP-1W lifetime '3600'
set security vpn ipsec esp-group ESP-1W proposal 1 encryption 'aes256'
set security vpn ipsec esp-group ESP-1W proposal 1 hash 'sha1'
set security vpn ipsec ike-group IKE-1W lifetime '28800'
set 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 'sha1'
set security vpn ipsec site-to-site peer 172.16.0.25 authentication pre-shared-secret 'test_key_1'
set security vpn ipsec site-to-site peer 172.16.0.25 ike-group 'IKE-1W'
set security vpn ipsec site-to-site peer 172.16.0.25 local-address ' 172.16.0.161 '
set security vpn ipsec site-to-site peer 172.16.0.25 vti bind 'vti0'
set security vpn ipsec site-to-site peer 172.16.0.25 vti esp-group 'ESP-1W'
set protocols static interface-route 192.168.1.0/24 next-hop-interface 'vti0'
```

検証環境構成図 Managed FW差し込みパターン①



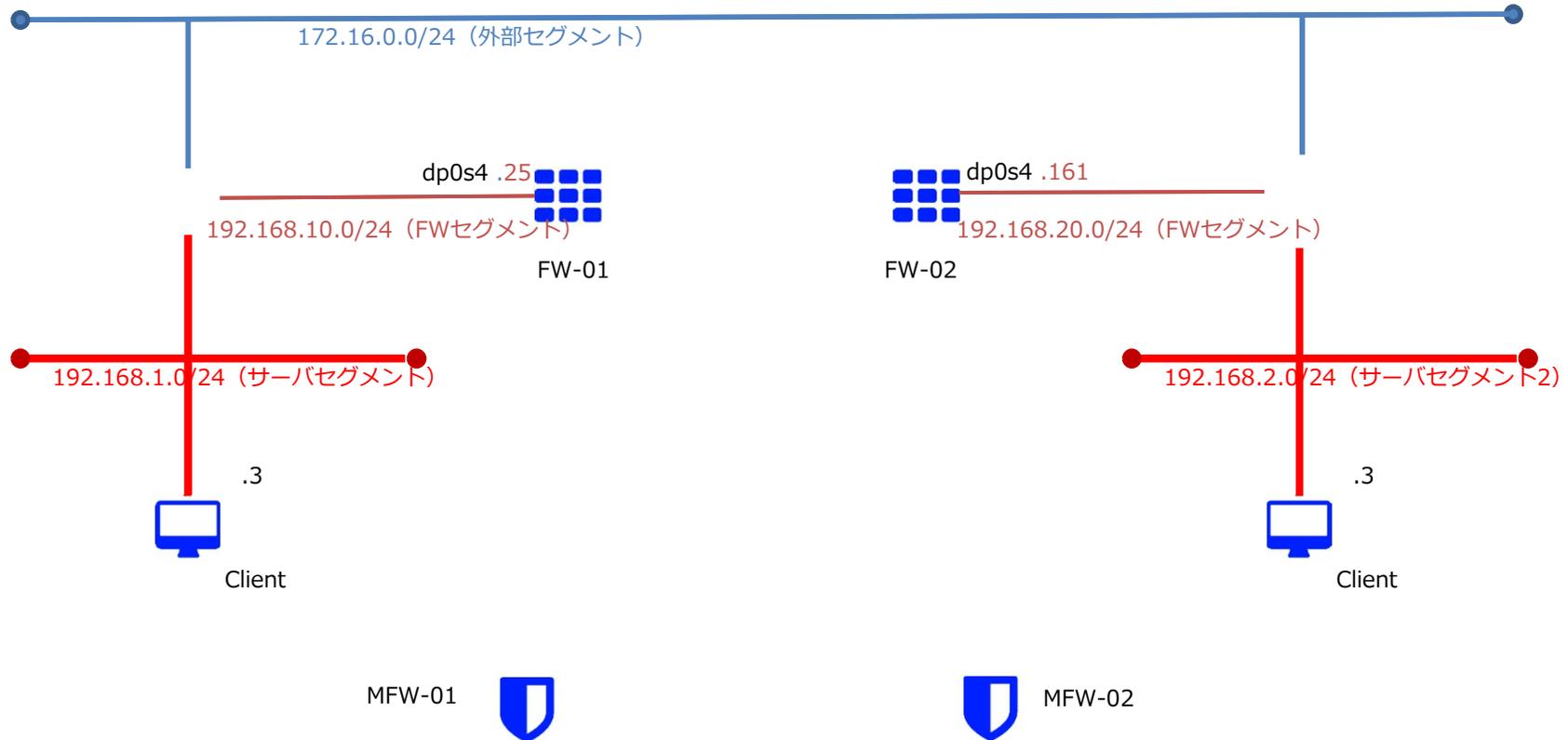
手順① : Managed FWの申込み

検証環境構成図 Managed FW差し込みパターン①



- 手順② FWセグメントの作成
- 手順③ M-FWの設定
- 1:SNATオブジェクトの設定
- 2:DNAT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
- 4:ルーティングの設定

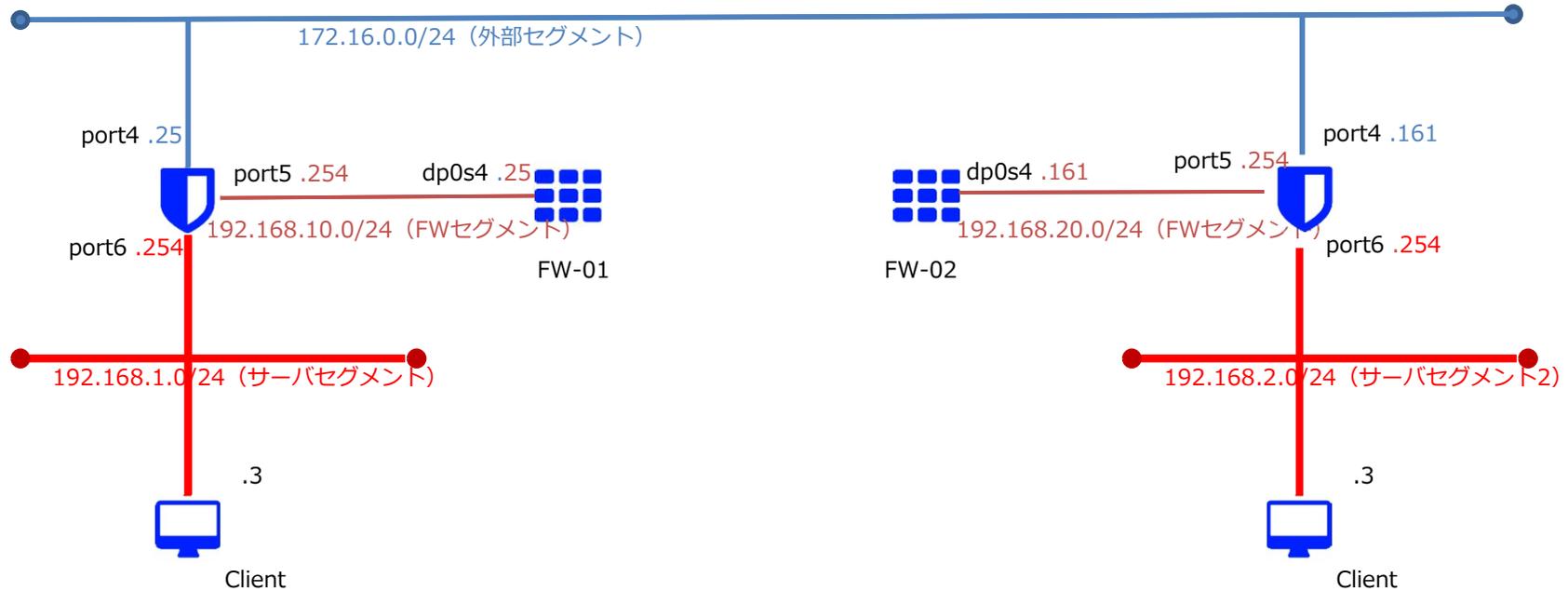
検証環境構成図 Managed FW差し込みパターン①



手順④ vFWの設定変更

- 1:ロジカルネットワークの切断(外部セグメント)
(通信断発生)
- 2:ロジカルネットワークの接続(FWセグメント)
- 3:vFWの設定変更

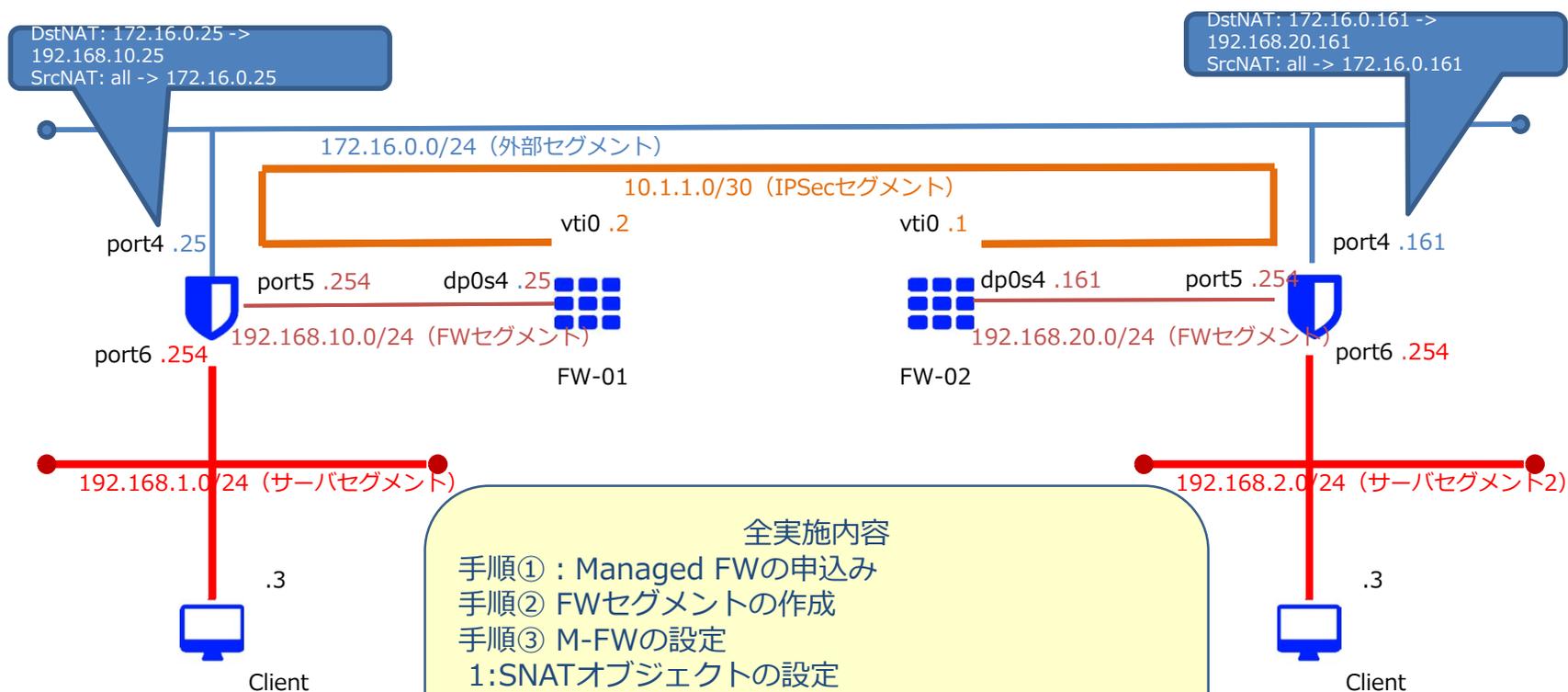
検証環境構成図 Managed FW差し込みパターン①



手順⑤ M-FWの設定

- ・ロジカルネットワークの接続 (通信断回復)

検証環境構成図 Managed FW差し込みパターン②完成図



- 全実施内容**
- 手順① : Managed FWの申込み
 - 手順② FWセグメントの作成
 - 手順③ M-FWの設定
 - 1:SNATオブジェクトの設定
 - 2:DNAT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
 - 4:ルーティングの設定
 - 手順④ vFWの設定変更
 - 1:ロジカルネットワークの切断(外部セグメント)
(通信断発生)
 - 2:ロジカルネットワークの接続(FWセグメント)
 - 3:vFWの設定変更
 - 手順⑤ M-FWの設定
 - ・ロジカルネットワークの接続 (通信断回復)

手順① M-FW申し込み

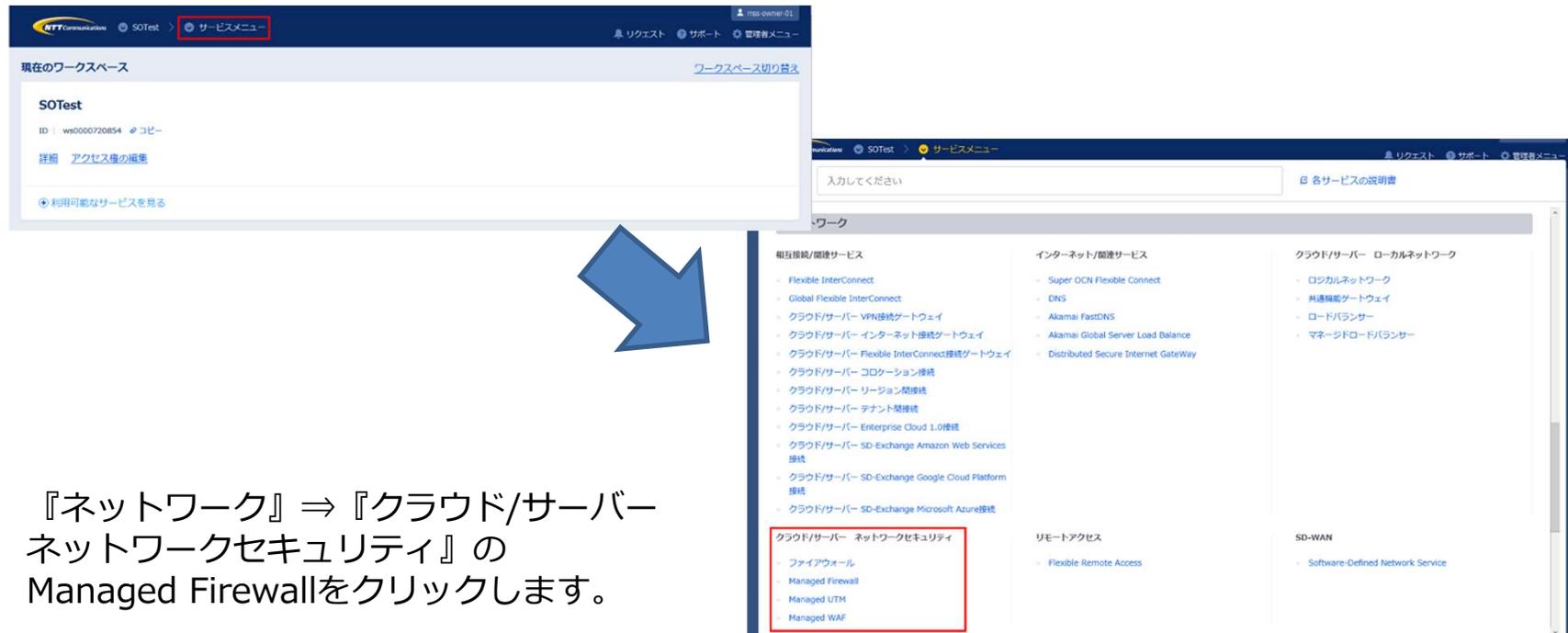
手順① M-FW申し込み

下記リンクを参照の上、シングル構成のお申し込みをお願いいたします。

https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/order/managed_firewall_utm_v2/order_new_single.html

SDPFポータルからアクセス

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



The screenshot shows the SDPF portal interface. In the top navigation bar, the 'Service Menu' (サービスメニュー) is highlighted with a red box. Below it, the 'Current Workspace' (現在のワークスペース) section shows 'SOTest' with ID 'ws0000720854'. A blue arrow points from this section to the 'Service Menu' (サービスメニュー) page. The 'Service Menu' page displays a search bar and a list of services. Under the 'Cloud/Server Network Security' (クラウド/サーバー ネットワークセキュリティ) category, 'Managed Firewall' (ファイアウォール) is highlighted with a red box. Other services listed include 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① M-FW申し込み

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

Security Menu

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



申込種別に「デバイス追加」を選択ください。

セキュリティ

申込種別



お申し込みの際の入力値は下記になります。

Device Information			
メニュー	プラン	構成	ゾーングループ
Managed Firewall	2CPU-4GB	Single	zone1-groupa

手順② FWセグメントの作成

手順② FWセグメントの作成

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② FWセグメントの作成

2-1.ロジカルネットワークを作成します。

- ・ロジカルネットワークタブから、必要項目を設定し、「次へ」を選択。
- ・サブネットタブから、必要項目を設定し、「次へ」を選択。

(ネットワークアドレスに、192.168.10.0/24を、ゲートウェイIPに192.168.10.254を記入)

- ・「DHCP 有効」にチェックし、「IP アドレス割り当てプール」に192.168.10.1,192.168.10.200を設定。
- ・サブネットの詳細タブから、必要項目を設定し、「ロジカルネットワークの作成」を選択。

ロジカルネットワークの作成

ロジカルネットワーク

ロジカルネットワーク名

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

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

管理役割

UP

取り直し 戻る 次へ

ロジカルネットワークの作成

ロジカルネットワーク

サブネット

サブネットの詳細

サブネット名

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

ネットワークアドレス

192.168.10.0/24

ゲートウェイIP

192.168.10.254

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 アドレス割り当てプール

DNS サーバー

NTP サーバー

追加のルーティング

サブネットの説明

サブネットのタグ

取り直し 戻る 次へ



手順② FWセグメントの作成

2-1.ロジカルネットワークを作成します。

- ・ロジカルネットワークタブから、必要項目を設定し、「次へ」を選択。
- ・サブネットタブから、必要項目を設定し、「次へ」を選択。

(ネットワークアドレスに、192.168.20.0/24を、ゲートウェイIPに192.168.20.254を記入)

- ・「DHCP 有効」にチェックし、「IP アドレス割り当てプール」に192.168.20.1,192.168.20.200を設定。
- ・サブネットの詳細タブから、必要項目を設定し、「ロジカルネットワークの作成」を選択。

ロジカルネットワークの作成

ロジカルネットワーク

サブネット

サブネットの詳細

ロジカルネットワーク名

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

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

管理役割

UP

取り直し

戻る

次へ

ロジカルネットワークの作成

ロジカルネットワーク

サブネット

サブネットの詳細

サブネット名

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

ネットワークアドレス

192.168.20.0/24

ゲートウェイIP

192.168.20.254

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 アドレス割り当てプール

DNS サーバー

NTP サーバー

追加のルータ設定

サブネットの説明

サブネットのタグ

取り直し

戻る

ロジカルネットワークの作成

手順③ M-FWの設定

手順③-1 M-FWの設定 (Destination NATの設定)

手順③-1 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③-1 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	Operation

手順③-1 M-FWの設定

「デバイス」からいずれかのデバイスを右クリックします。



画面右側の「コンフィグ」をクリックします。



画面左側のオブジェクト画面から 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③-1 M-FWの設定

設定値を入力して、[保存] をクリックします。

MFW-01

オブジェクト

NAT Name	Port4_DNAT
External IP Address	172.16.0.25
Mapped IP Address	192.168.10.25
External Interface	port4
Port Forward	<input type="checkbox"/>
Comment	

キャンセル 保存

MFW-02

オブジェクト

NAT Name	Port4DNAT
External IP Address	172.16.0.161
Mapped IP Address	192.168.20.161
External Interface	port4
Port Forward	<input type="checkbox"/>
Comment	

キャンセル 保存

手順③-2 M-FWの設定(SNATの設定)

手順③-2 M-FWの設定(SNATの設定)

Source 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_v2/4340_source_nat.html

SDPFポータルからアクセス

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

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

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

手順③-2 M-FWの設定(SNAT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(SNATの設定)

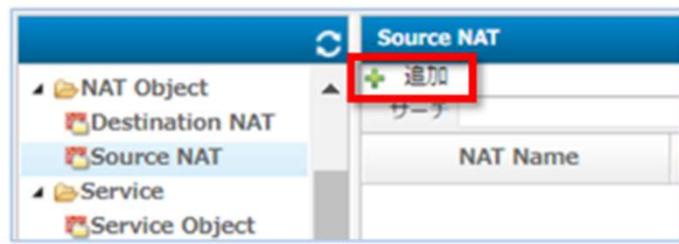
「デバイス」からいずれかのデバイスを右クリックします。



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 Source NAT をクリックします。
オブジェクト ▶ NAT Object ▶ Source NAT
画面右側の Source NAT 画面で [追加] をクリックします。



手順③-2 M-FWの設定(SNATの設定)

設定値を入力して、[保存] をクリックします。

MFW-01

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

- NAT Name: Port5_SNAT
- Start IP Address: 172.16.0.25
- End IP Address: 172.16.0.25
- Comment: (empty)

A blue callout bubble points to the End IP Address field with the text "SNAT後のアドレスを StartとEndに入力" (Enter the address after SNAT in Start and End). At the bottom right, there are two buttons: "キャンセル" (Cancel) and "保存" (Save), with the "保存" button highlighted by a red rectangle.

MFW-02

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

- NAT Name: Port5_SNAT
- Start IP Address: 172.16.0.161
- End IP Address: 172.16.0.161
- Comment: (empty)

A blue callout bubble points to the End IP Address field with the text "SNAT後のアドレスを StartとEndに入力" (Enter the address after SNAT in Start and End). At the bottom right, there are two buttons: "キャンセル" (Cancel) and "保存" (Save), with the "保存" button highlighted by a red rectangle.

手順③-3 M-FWの設定(ファイアウォールポリシーの設定)

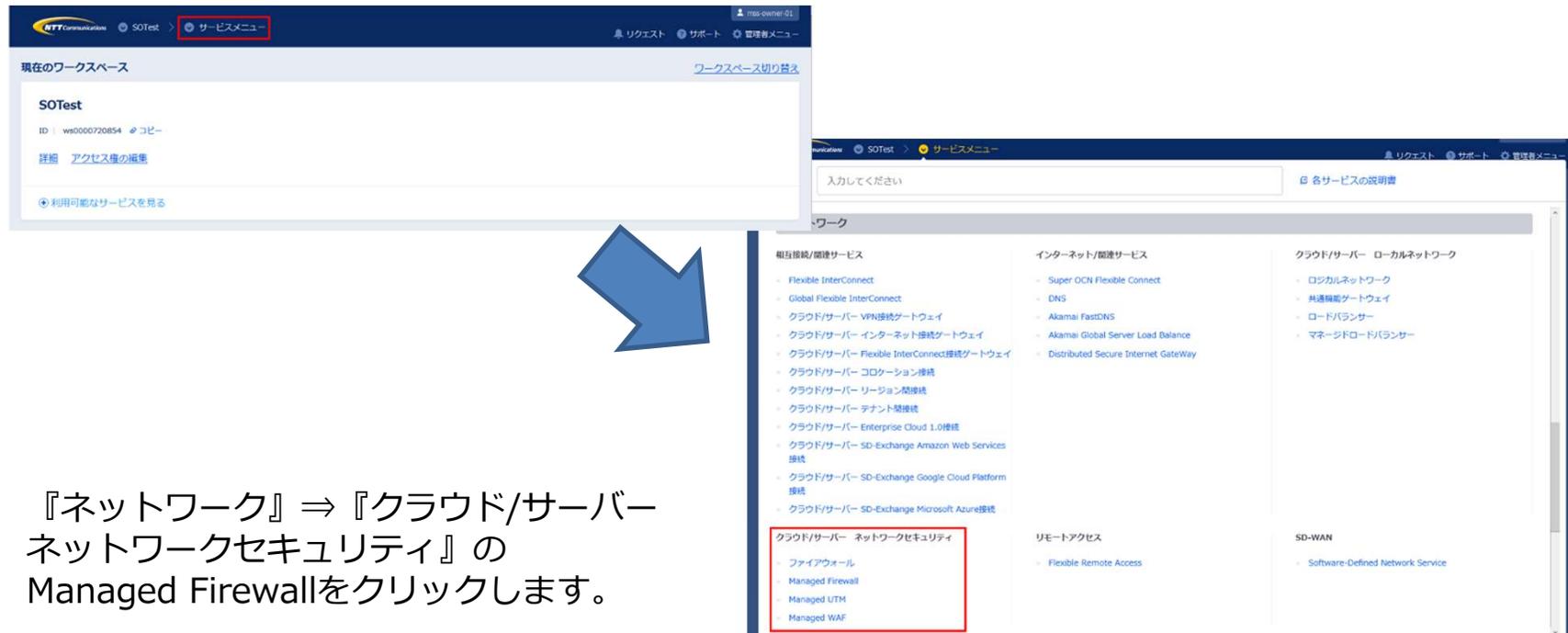
手順③-3 M-FWの設定

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 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。



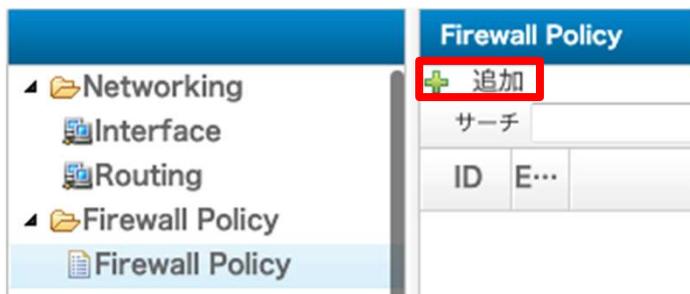
画面右側の「コンフィグ」をクリックします。



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。

MFW-01 & MFW-02

オブジェクト

ID 1

Move rule No Move Move before Move after

Enable

Source

Incoming Interface Port4 **受信側ポート**

Source Address all **送信元アドレス**

Destination

Outgoing Interface Port5 **送信側ポート**

Destination Address Type Address Object NAT Object

Destination NAT Port4_DNAT **DNAT用に作成したオブジェクト**

Service ALL

Action ACCEPT

NAT

Log Disable

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の設定)

設定値を入力して、[保存] をクリックします。

MFW-01 & MFW-02

オブジェクト

ID 4

Move rule No Move Move before Move after

Enable

Source

Incoming Interface Port5

Source Address all

Destination

Outgoing Interface Port6

Destination Address Type Address Object NAT Object

Destination Address all

Service ALL

Action ACCEPT

NAT

Log Disable

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の設定)

設定値を入力して、[保存] をクリックします。

MFW-01 & MFW-02

オブジェクト

ID 4

Move rule No Move Move before Move after

Enable

Source

Incoming Interface Port6 受信側ポート

Source Address all

Destination

Outgoing Interface Port5 送信側ポート

Destination Address Type Address Object NAT Object

Destination Address all

Service ALL

Action ACCEPT

NAT

Log Disable

UTM Function

Comment

キャンセル 保存

手順③-4 M-FWの設定(ルーティングの設定)

手順③-4 M-FWの設定

ルーティングの設定は下記をご覧ください。

https://sdpf.ntt.com/services/docs/network-based-security/tutorials/rsts/security/operation/managed_firewall_utm_v2/4210_routing_single.html

SDPFポータルからアクセス

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

The 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 a larger screenshot of the 'サービスメニュー' page. In this larger screenshot, the 'サービスメニュー' (Service Menu) is visible, and the 'ネットワークセキュリティ' (Network Security) section is highlighted with a red box. This section includes 'ファイアウォール' (Firewall), 'Managed Firewall', 'Managed UTM', and 'Managed WAF'. Other sections include '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'.

『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③-4 M-FWの設定

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

Security Menu

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

手順③-4 M-FWの設定

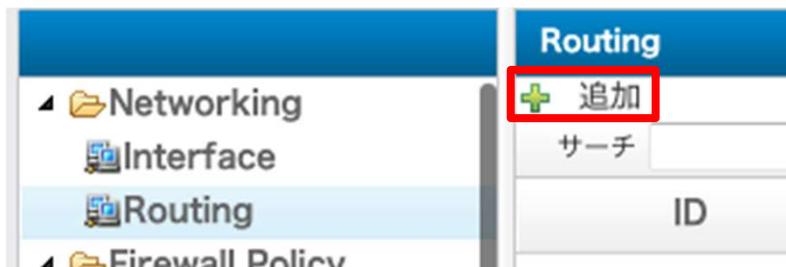
「デバイス」からいずれかのデバイスを右クリックします。



画面右側の「コンフィグ」をクリックします。



画面左側のオブジェクト画面から Routing をクリックします。
オブジェクト ▶ Networking ▶ Routing



手順③-4 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

MFW-01

オブジェクト	
ID	1
Destination IP	192.168.2.0
Subnet Mask	255.255.255.0
Gateway	192.168.10.25
Interface	Port5
Comment	

サーバセグメント2宛の通信

送信先Gateway address(FW-01)

送信先Port

キャンセル 保存

MFW-02

オブジェクト	
ID	1
Destination IP	192.168.1.0
Subnet Mask	255.255.255.0
Gateway	192.168.20.161
Interface	Port5
Comment	

サーバセグメント宛での通信

送信先Gateway address(FW-02)

送信先Port

キャンセル 保存

手順④-1 vFWの設定変更 (インターフェースの削除(外部 セグメント))

手順④-1 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④-1 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

概要

ファイアウォールインタフェース

名前	説明	スロット番号	ロジカルネットワーク	IPアドレス	仮想IPアドレス	Enterprise Cloud 2.0接続	ステータス	アクション
dp0s4		1			-	-	稼働中	ファイアウォールインタフェースの編集 ▼ ロジカルネットワークの接続
dp0s5	-	2			-	-	稼働中	ファイアウォールインタフェースの編集 ▼ ロジカルネットワークの切断

手順④-2 vFWの設定変更 (インターフェースの追加(FWセグメント))

手順④-2 vFWのインターフェース追加

下記リンクを参考の上、vFWのインターフェース追加をお願いいたします。

<https://ecl.ntt.com/documents/tutorials/rsts/Firewall/instance/setting.html>

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 (highlighted with a red box)

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④-2 vFWのインターフェース追加

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接続」を選択

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
dp0s5	-	2			-	-	稼働中	ファイアウォール ロジカルネットワークの切断

手順④-3 vFWの設定変更 (IPSecの設定追加)

手順④-3 vFWの設定変更(IPSecの設定追加)

Local IDと対向Peer IDを一致させるために下記を設定

FW-01

```
set security vpn ipsec site-to-site peer 172.16.0.161 authentication id '172.16.0.25'
```

FW-02

```
set security vpn ipsec site-to-site peer 172.16.0.25 authentication id 172.16.0.161
```

手順⑤M-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. 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 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' (Service Menu) 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 its sub-items include '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

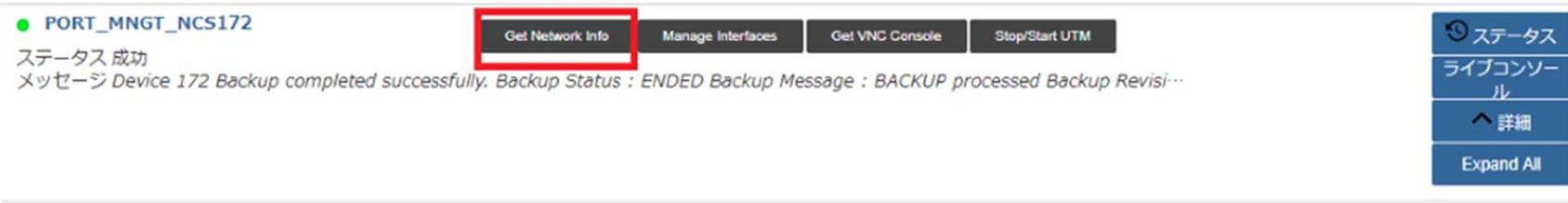
手順⑤ M-FWの設定

[サービス] -> [ワークフロー] -> [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。



● PORT_MNGT_NCS172

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

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...

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

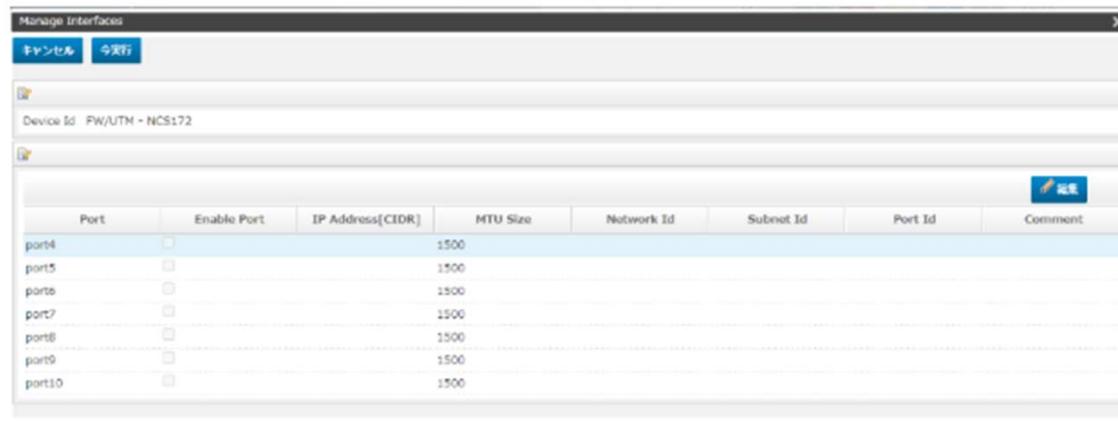
クローズ

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。



[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。

MFW-01

キャンセル 保存

Port port4

Enable Port

IP Address[CIDR] 172.16.0.25/24

MTU Size 1500

Network Id external_segment

Subnet Id 172.16.0.0/24

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

MFW-02

キャンセル 保存

Port port4

Enable Port

IP Address[CIDR] 172.16.0.161/24

MTU Size 1500

Network Id external_segment

Subnet Id 172.16.0.0/24

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(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。

MFW-01

キャンセル 保存

Port port5

Enable Port

IP Address[CIDR] 192.168.10.254/24

MTU Size 1500

Network Id net_seg_a

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

MFW-02

キャンセル 保存

Port port5

Enable Port

IP Address[CIDR] 192.168.20.254/24

MTU Size 1500

Network Id net_seg_b

Subnet Id 192.168.20.0/24

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(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。

MFW-01

キャンセル 保存

Port port6

Enable Port

IP Address[CIDR] 192.168.1.254/24

MTU Size 1500

Network Id server_segment_a

Subnet Id 192.168.1.0/24

Port Id

Comment

Port6に付与するIPアドレス

Port6に接続するネットワークアドレス

MFW-02

キャンセル 保存

Port port6

Enable Port

IP Address[CIDR] 192.168.2.254/24

MTU Size 1500

Network Id server_segment_b

Subnet Id 192.168.2.0/24

Port Id

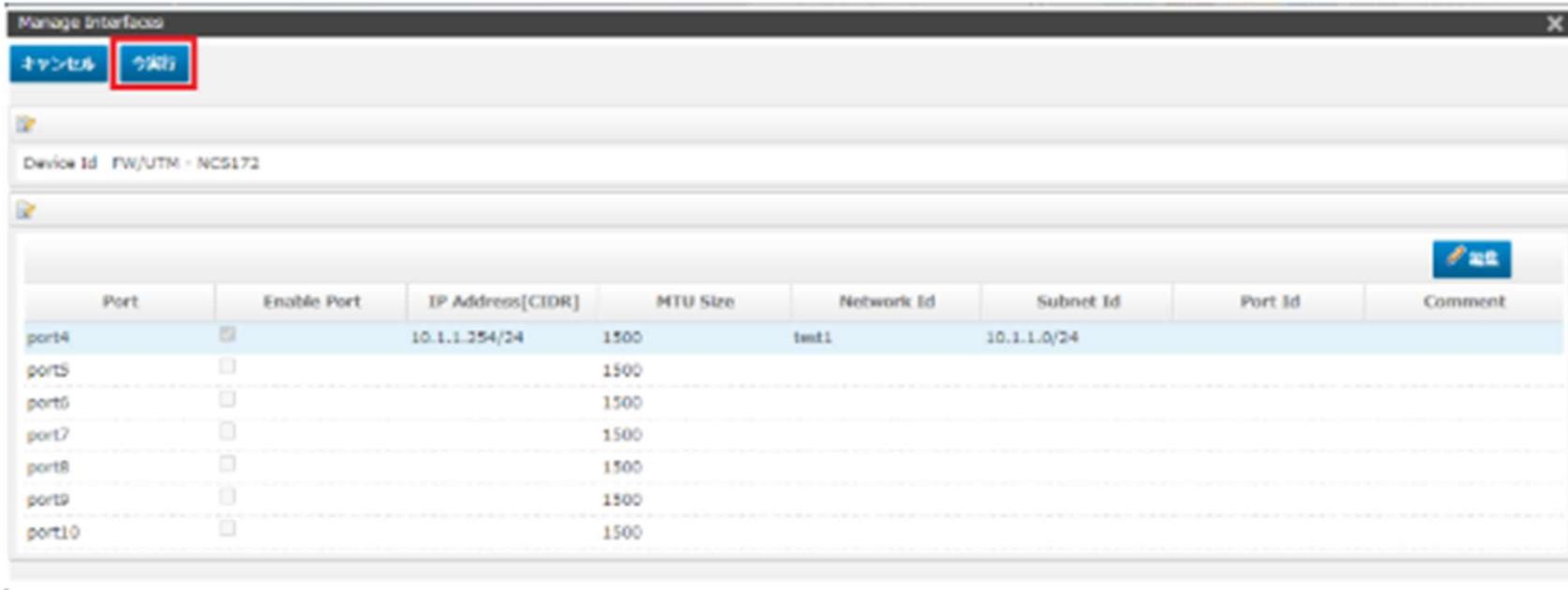
Comment

Port6に付与するIPアドレス

Port6に接続するネットワークアドレス

手順④ M-FWの設定

使用するポート設定が準備できたら、Manage Interfaces画面で「今実行」をクリックします。



The screenshot shows the 'Manage Interfaces' window for device 'FW/UTM - NCS172'. It contains a table with the following data:

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 : 08edfc958d894aa60088155cc26005bc
↓			
Verify IP Address inputs	2016-07-11 22:32:46	2016-07-11 22:35:47	IP Address inputs verified successfully.
↓			
Detach Ports	2016-07-11 22:35:47	2016-07-11 22:36:52	Ports detached successfully from the Server bb348914-cb3b-467e-b9af-0b897ce38ed.
↓			
Create Ports	2016-07-11 22:36:52	2016-07-11 22:36:58	Ports created successfully. Port Id : f4f775e8-012-4937-a5dc-e02eeec4a055 Port Id : 09eeeb69-17bc-40bc-8ae4-330b5d55024e Port Id : 8010b923-2c79-4ed3-80d3-9317d7c2ab1 Port Id : c85d7b3b-3e3c-44a3-97b5-829fc138ad91 Port Id : 83a3d462-0262-4a8a-3cdf-cef8ce43794f Port Id : e604d97f-6e7b-4f97-94a5-a832004a0e0e Port Id : 2a72235c-ab1f-4af0-a6a2-149b2c26129
↓			
Attach Ports	2016-07-11 22:36:58	2016-07-11 22:37:11	Ports attached successfully to the Server bb348914-cb3b-467e-b9af-0b897ce38ed.
↓			
Start the UTM	2016-07-11 22:37:11	2016-07-11 22:37:26	Openstack Server bb348914-cb3b-467e-b9af-0b897ce38ed 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.

動作確認

ファイアウォールのトンネル状態確認

FW01(ipsec_a)

```
user-admin@vyatta:~$ show vpn ipsec sa
```

Peer ID / IP	Local ID / IP	Tunnel	State	Bytes Out/In	Encrypt	Hash	A-Time	L-Time	Proto
172.16.0.161	192.168.10.25	vti	up	0.0/0.0	aes256	sha1	2361	3600	all

FW02 (ipsec_b)

```
user-admin@vyatta:~$ show vpn ipsec sa
```

Peer ID / IP	Local ID / IP	Tunnel	State	Bytes Out/In	Encrypt	Hash	A-Time	L-Time	Proto
172.16.0.25	192.168.20.161	vti	up	0.0/0.0	aes256	sha1	2446	3600	all

動作確認

ファイアウォールのvti0インタフェース状態

FW01(IPsec-a)

```
user-admin@vyatta:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface    IP Address          S/L Description
-----
dp0s4        192.168.10.25/24    u/u
vti0         10.1.1.2/30         u/u
```

FW-02(IPsec-b)

```
user-admin@vyatta:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface    IP Address          S/L Description
-----
dp0s4        192.168.20.161/24  u/u
vti0         10.1.1.1/30        u/u
```

動作確認

仮想サーバ(192.168.1.3)から対向の仮想サーバ(192.168.2.3)に対しての通信確認を実行しました。

ping

```
[test-user@ipsec-test-a ~]$ ping 192.168.2.3
[test-user@ipsec-test-a masuyamag]$ ping 192.168.2.3
PING 192.168.2.3 (192.168.2.3) 56(84) bytes of data.
64 bytes from 192.168.2.3: icmp_seq=1 ttl=60 time=7.26 ms
64 bytes from 192.168.2.3: icmp_seq=2 ttl=60 time=3.95 ms
64 bytes from 192.168.2.3: icmp_seq=3 ttl=60 time=3.65 ms
64 bytes from 192.168.2.3: icmp_seq=4 ttl=60 time=15.0 ms
64 bytes from 192.168.2.3: icmp_seq=5 ttl=60 time=3.50 ms
^C
--- 192.168.2.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 3.504/6.690/15.074/4.416 ms
[test-user@ipsec-test-a ~]$
```

動作確認

仮想サーバ(192.168.1.3)から対向の仮想サーバ(192.168.2.3)に対しての通信確認を実行しました。

ftp

```
[test-user@ipsec-test-a ~]$ ftp 192.168.2.3
Connected to 192.168.2.3 (192.168.2.3).
220 (vsFTPD 3.0.2)
Name (192.168.2.3:test-user):
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> dir
227 Entering Passive Mode (192,168,2,3,39,81).
150 Here comes the directory listing.
226 Directory send OK.
ftp>
ftp> put test_file
local: test_file remote: test_file
227 Entering Passive Mode (192,168,2,3,177,254).
150 Ok to send data.
226 Transfer complete.
ftp>
ftp> dir
227 Entering Passive Mode (192,168,2,3,131,59).
150 Here comes the directory listing.
-rw-r--r--  1 1001  1001    19 Jul 17 15:20 test_file
226 Directory send OK.
ftp>
ftp> bye
221 Goodbye.
```