IPsec(サイト間トンネル）機能利用時の移行②

第1版

更新履歴

更新日	更新内容	版数
2017/12/11	初版	1

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

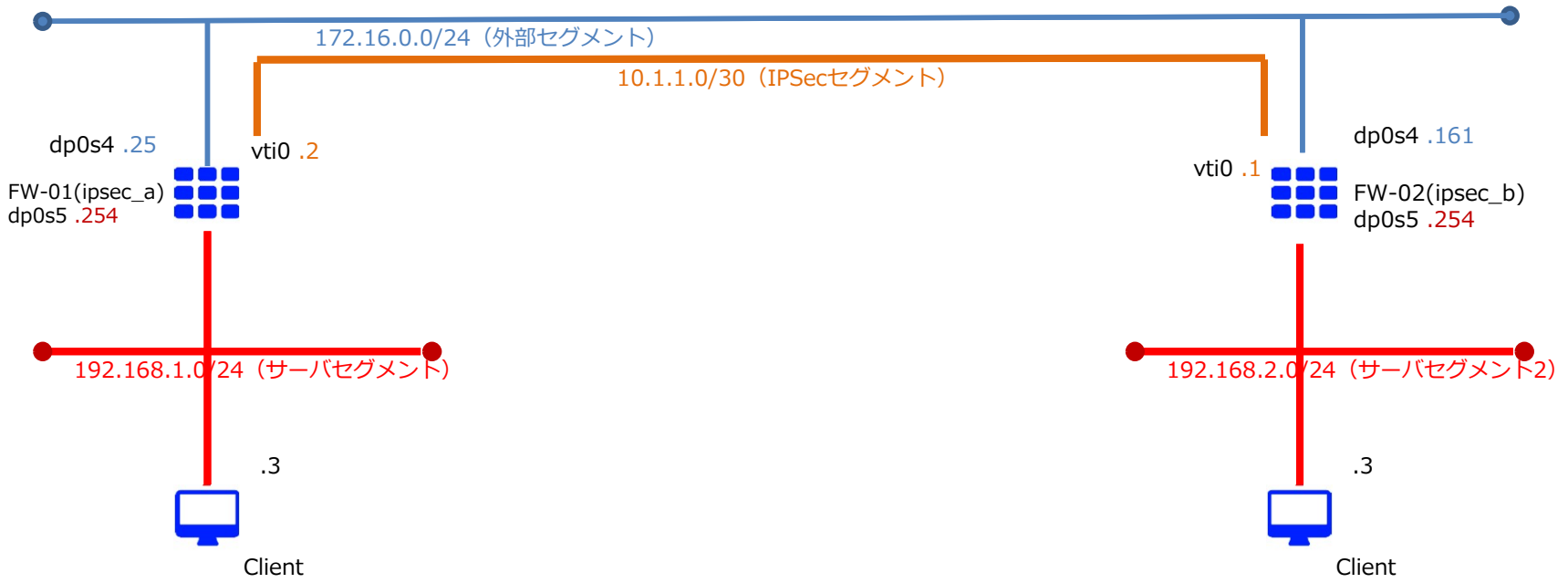
	設定項目	①資料	②資料（本資料）
初期導入時	vFWのネットワーク設定	1回	3回
	ルーティングの追加	無	有
MFWでのIPSec対応後の移行	vFWのLNW切断回数	2回	0回
	MFWのネットワーク設定	1回	0回

※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



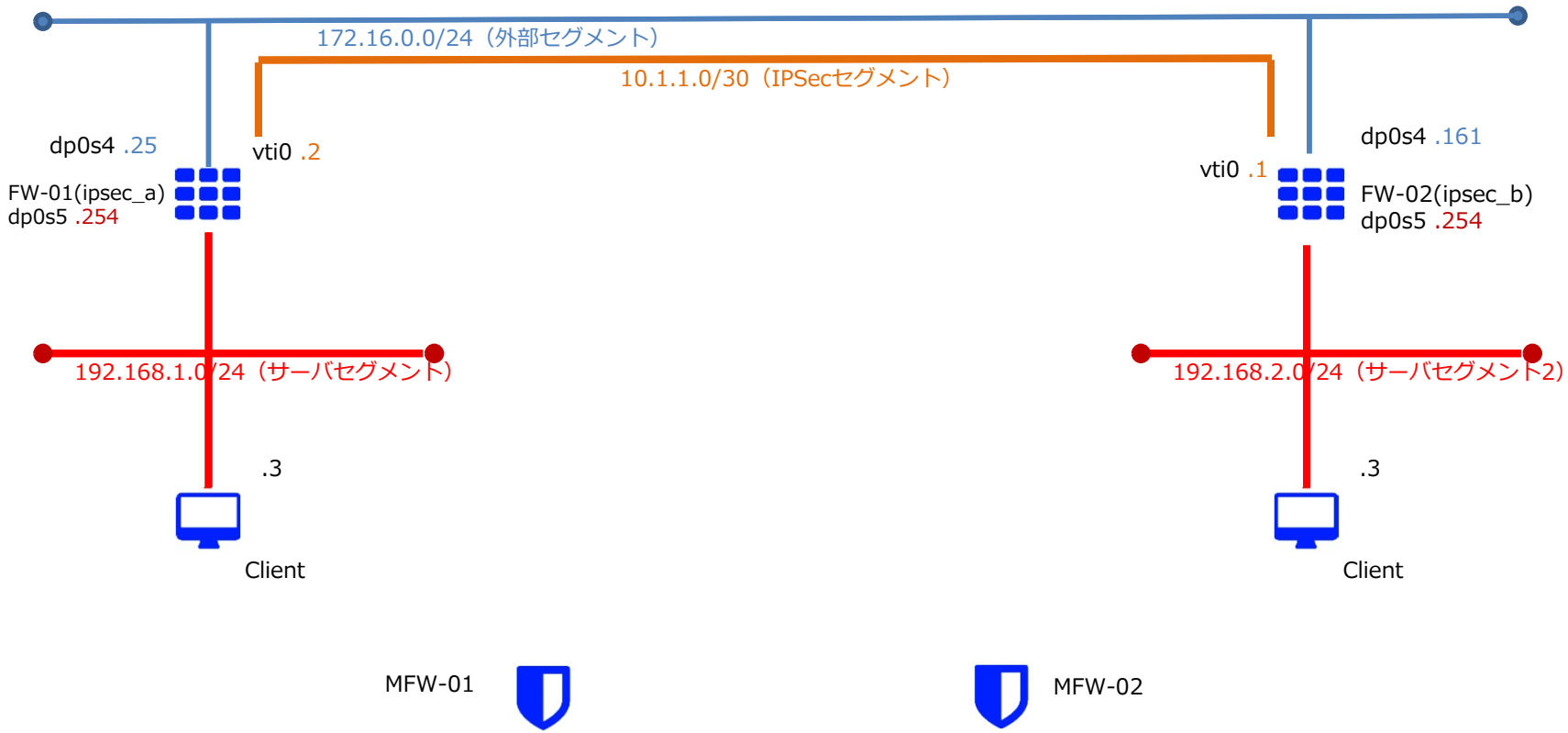
FW-01(ipsec_a)の設定

```
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

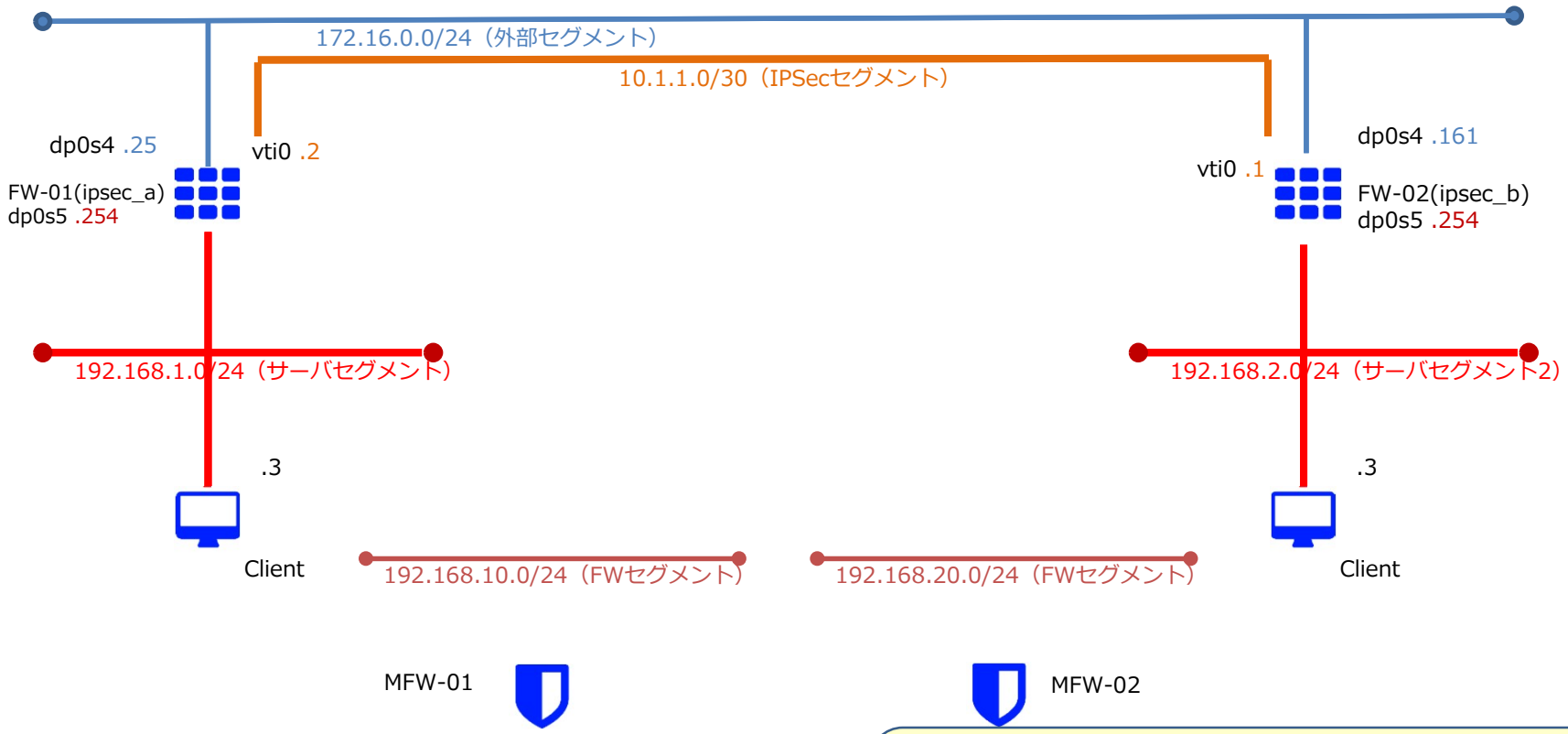
```
set interfaces vti vti0 address '10.1.1.1/30'
set security vpn ipsec esp-group ESP-1W lifetime '3600'
set security vpn ipsec esp-group ESP-1W proposal 1 encryption 'aes256'
set security vpn ipsec esp-group ESP-1W proposal 1 hash 'sha1'
set security vpn ipsec ike-group IKE-1W lifetime '28800'
set 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

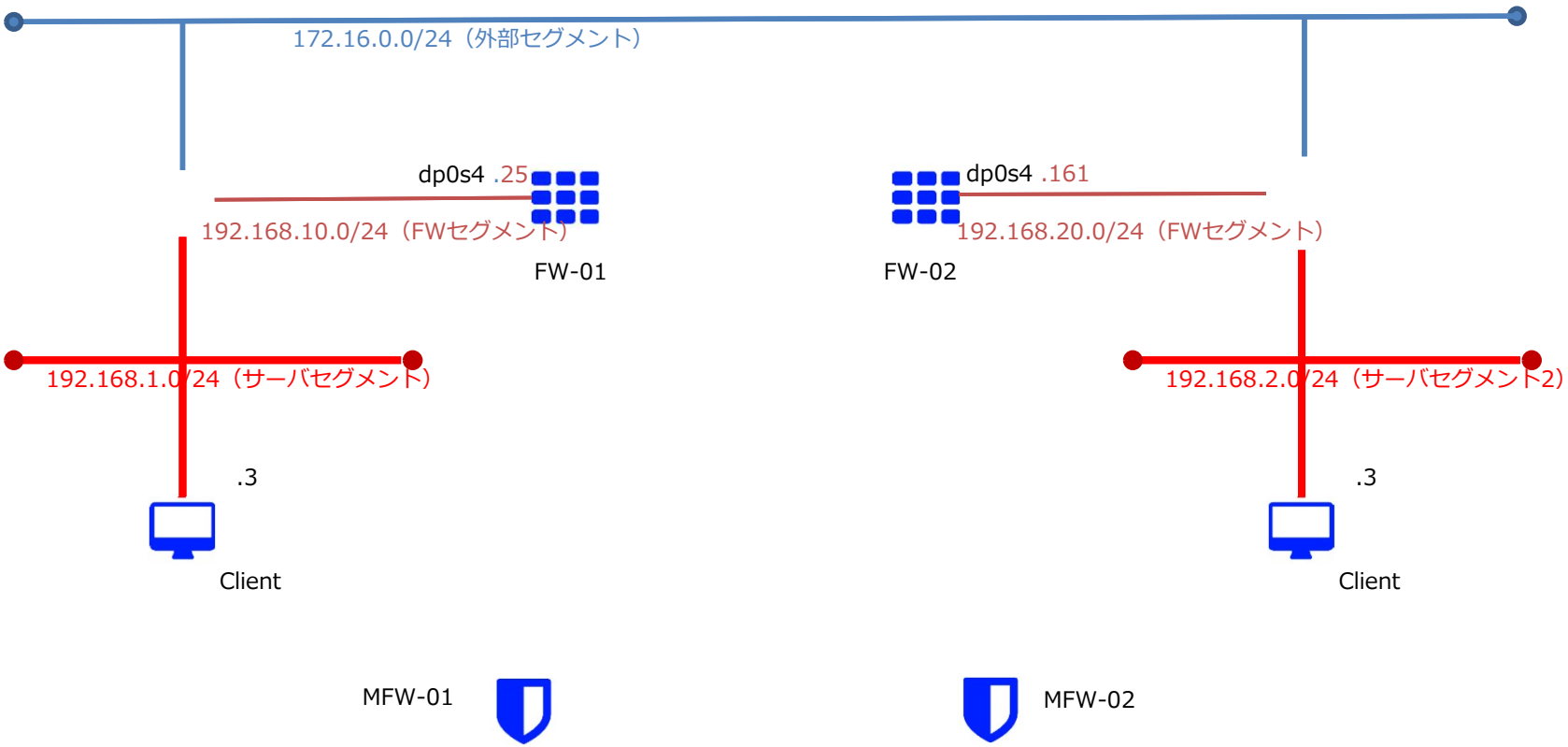
検証環境構成図　Managed FW差し込みパターン①



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

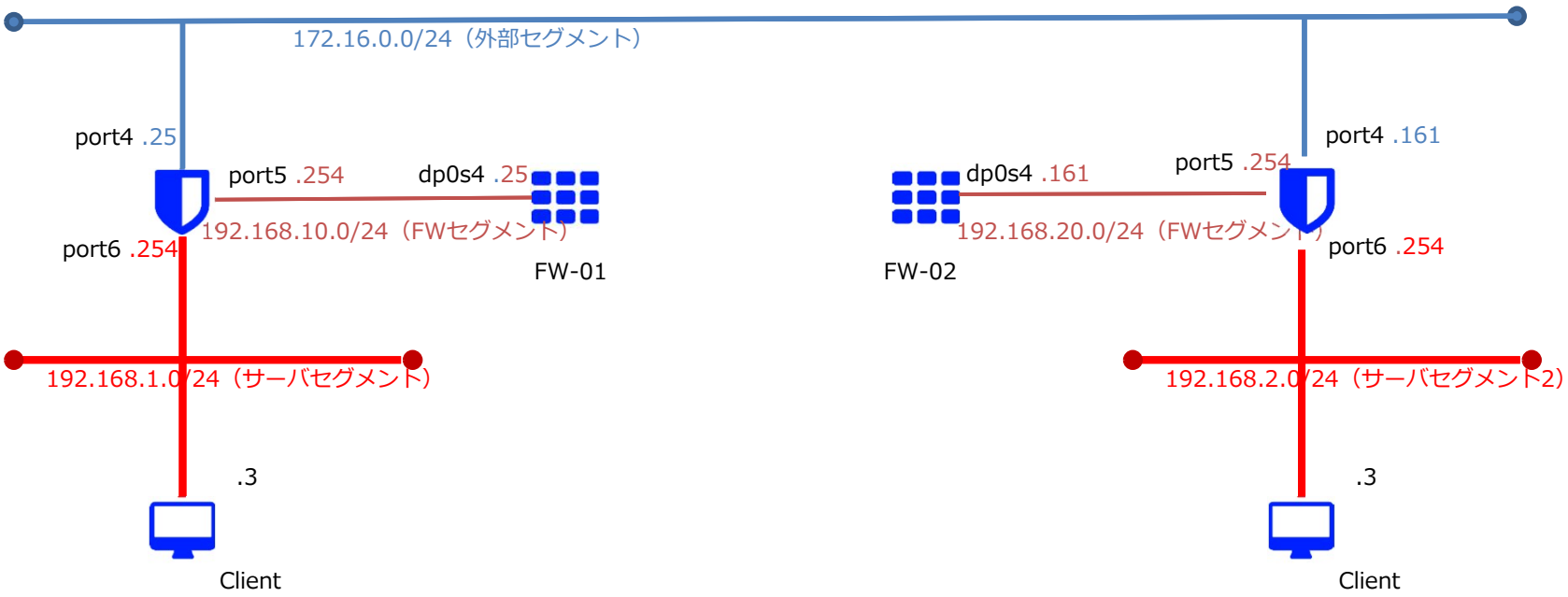
検証環境構成図　Managed FW差し込みパターン①



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

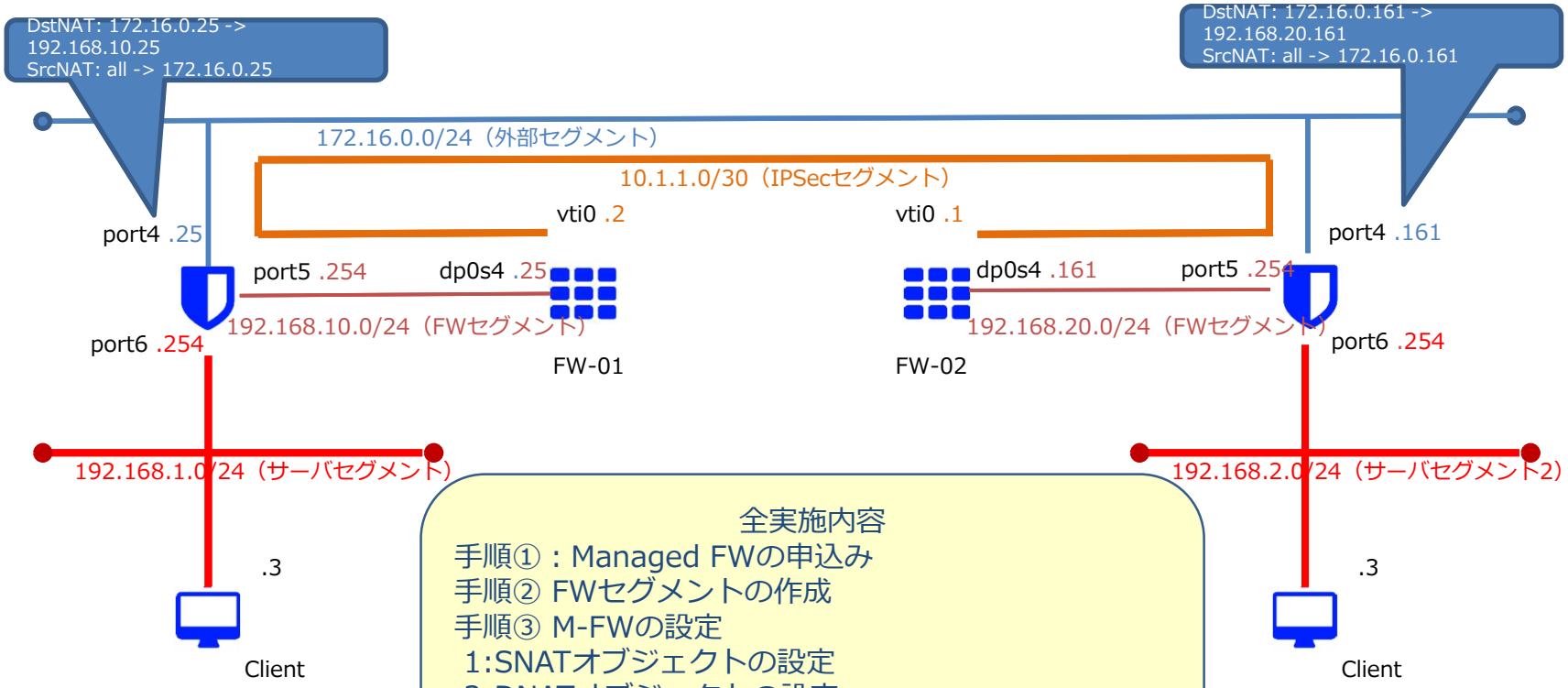
検証環境構成図　Managed FW差し込みパターン①



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

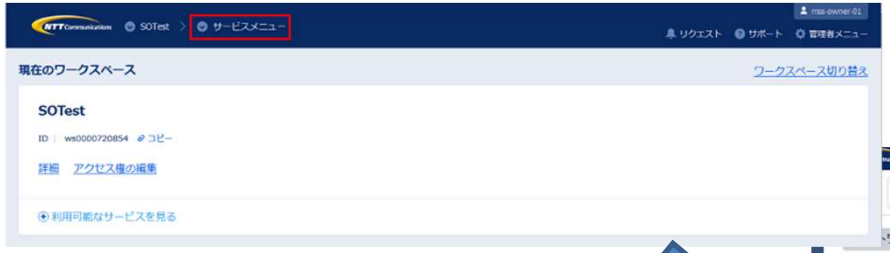
手順①：Managed FWの申込み
手順② FWセグメントの作成
手順③ M-FWの設定
 1:SNATオブジェクトの設定
 2:DNATオブジェクトの設定
 3:ファイアウォールポリシーの設定
 4:ルーティングの設定
手順④ vFWの設定変更
1:ロジカルネットワークの切断(外部セグメント)
（通信断発生）
2:ロジカルネットワークの接続(FWセグメント)
3:vFWの設定変更
手順⑤ M-FWの設定
・ロジカルネットワークの接続（通信断回復）

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。



『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 Managed UTM	Order
	Managed WAF	Order
	Managed Firewall(Version2) Managed UTM(Version2)	Order
	Managed WAF(Version2)	Order
Host-based Security	Managed Anti-Virus Managed Virtual Patch 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 デバイス追加

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

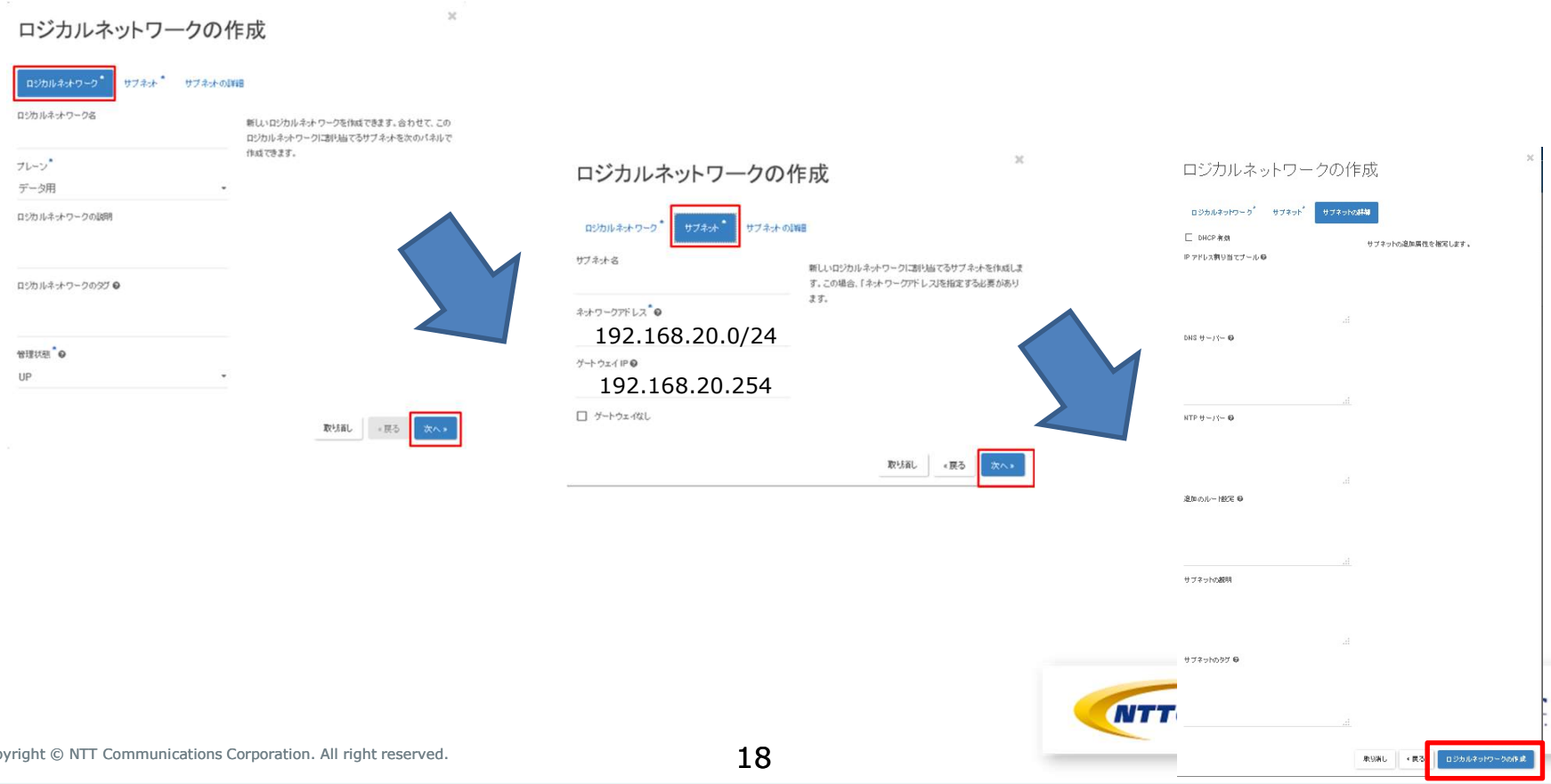
1．ロジカルネットワークの作成ボタンを押下します。

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。
・サブネットタグから、必要項目を設定し、「次へ」を選択。
(ネットワークアドレスに、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。

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。
・サブネットタグから、必要項目を設定し、「次へ」を選択。
(ネットワークアドレスに、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。



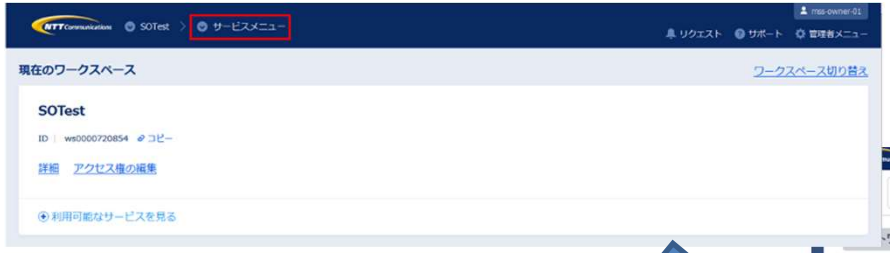
手順③ M-FWの設定

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。



『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

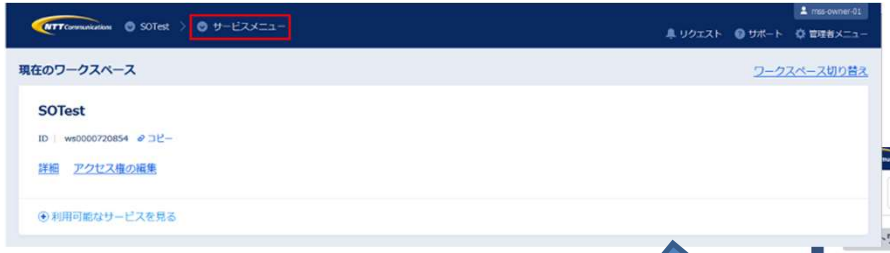
MFW-02

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。



『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。

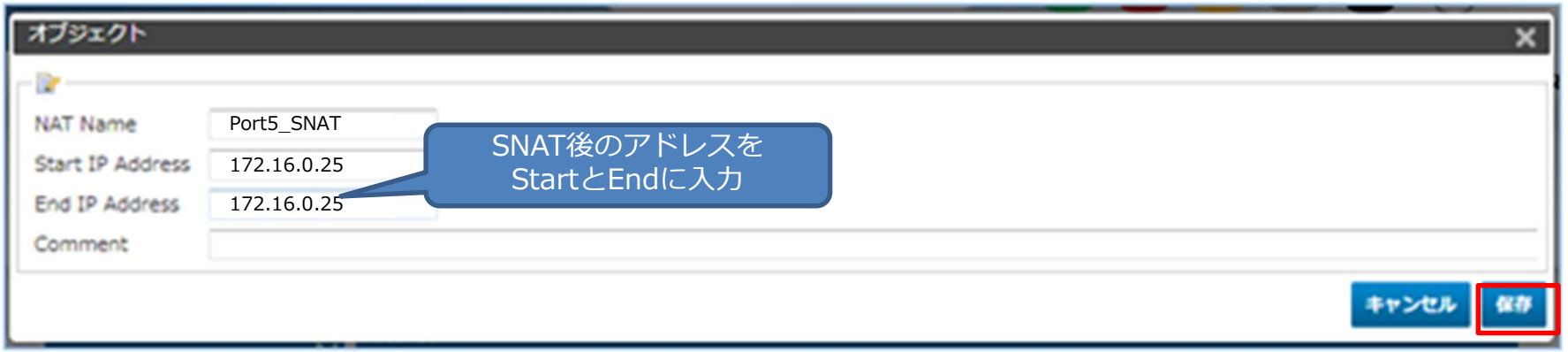
画面右側の「コンフィグ」をクリックします。

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。

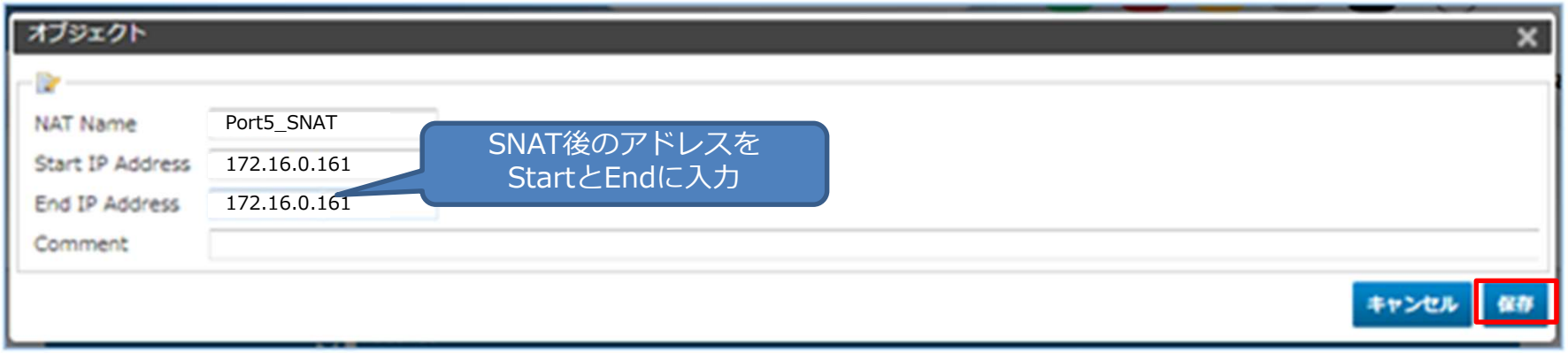
手順③-2 M-FWの設定(SNATの設定)

設定値を入力して、［保存］をクリックします。

MFW-01



MFW-02



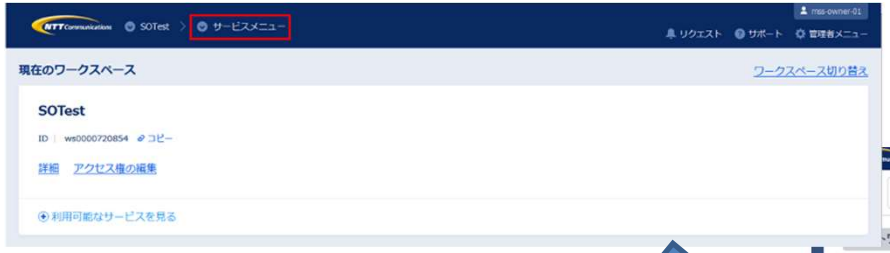
手順③-3 M-FWの設定(ファイアウォールポリシーの設定)

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。



『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。

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。

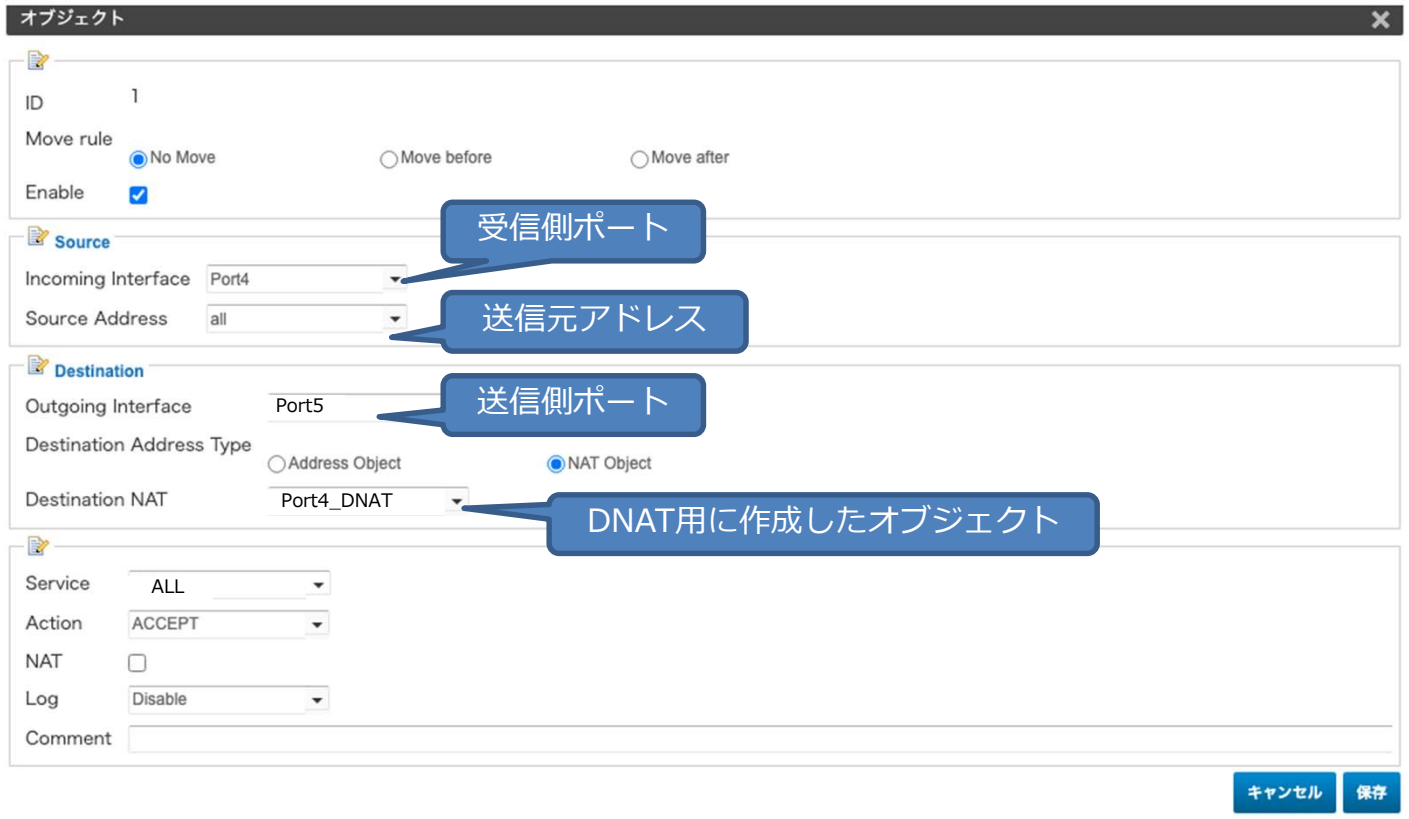
画面右側の「コンフィグ」をクリックします。

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



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

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。

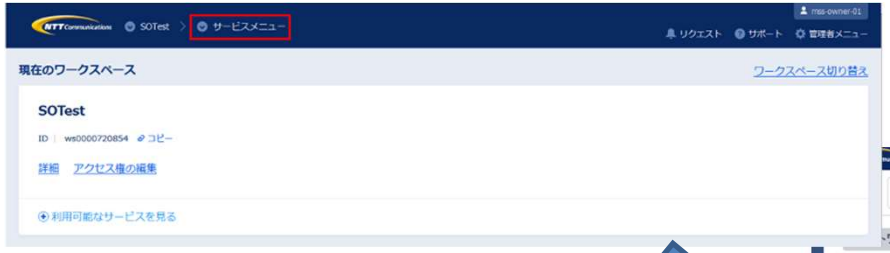
MFW-01＆MFW-02

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。



『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

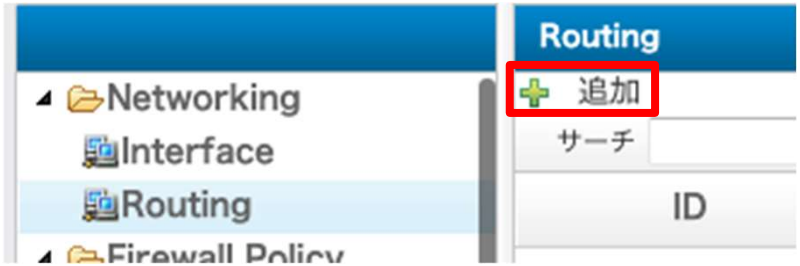
Managed Firewall(Version2)の「Operation」をクリックしてください。

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

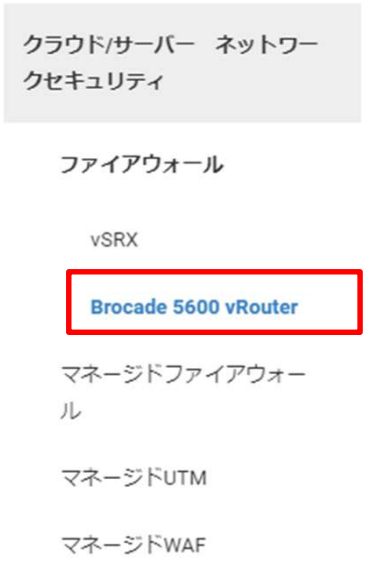
MFW-02

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



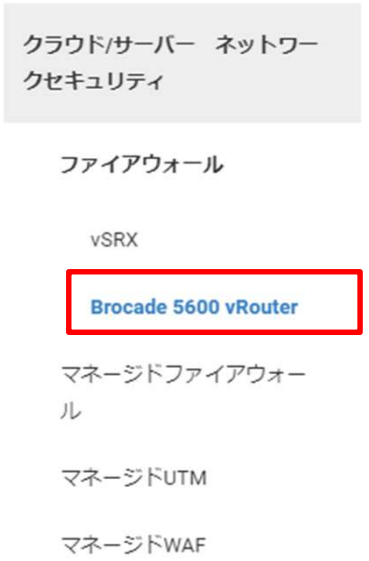
手順④-1 vFWのインターフェース削除

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

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



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

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

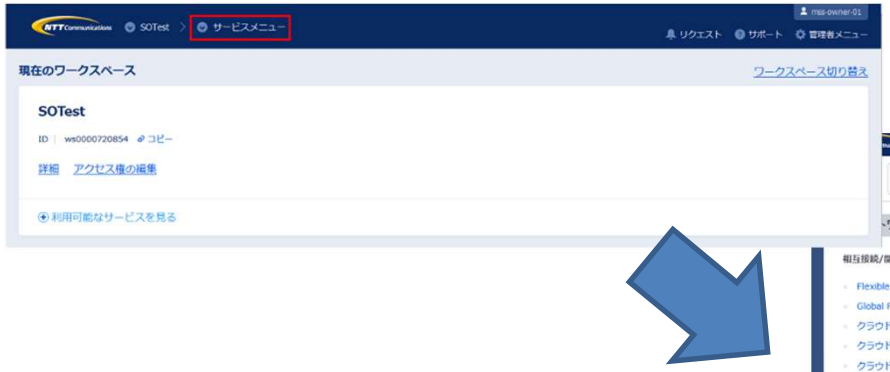
手順⑤M-FWの設定
(インターフェースの設定)

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。



『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

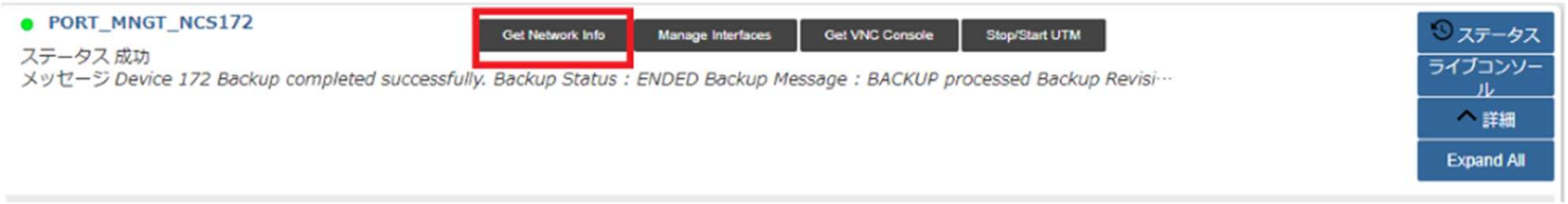
Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order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

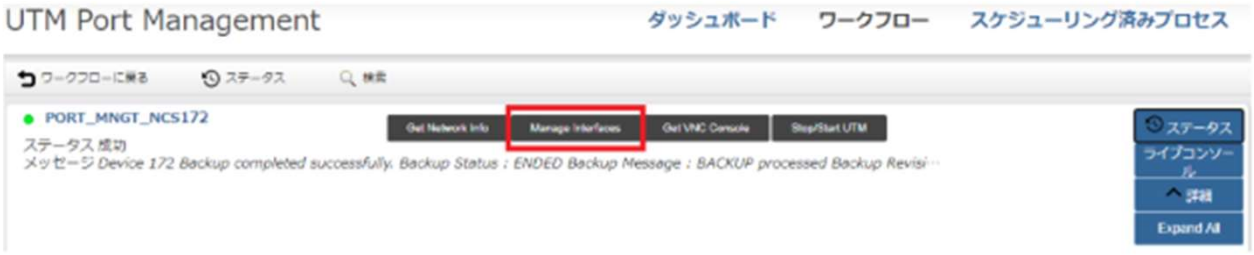
最新のお客さまネットワーク情報を参照可能にするため、設定対象のデバイスをクリックで選択して［Get Network Info］をクリックします。



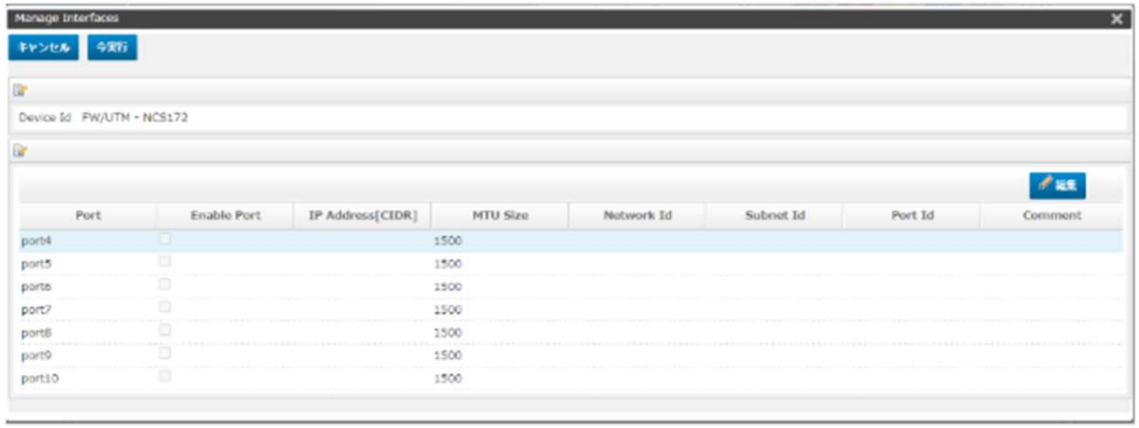
［タスク ステータス］が表示されます。Get Network Infoのタスクが「緑色」になれば正常終了です。[クローズ]で閉じてください。

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。



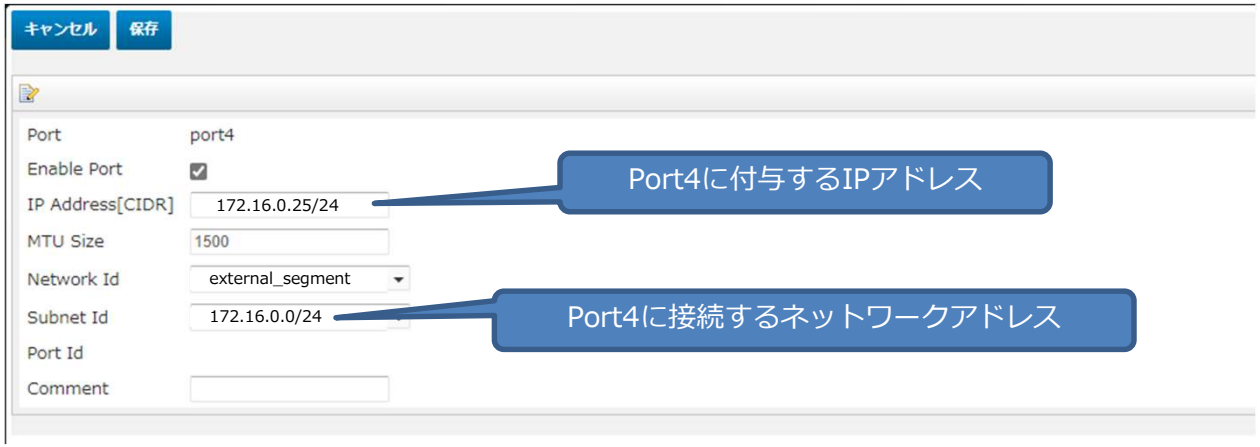
［Manage Interfaces］の画面が開きます。Port 2,3は［Manage Interfaces］の画面には表示されません。設定対象のポートをクリックで選択して、［編集］をクリックします。



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

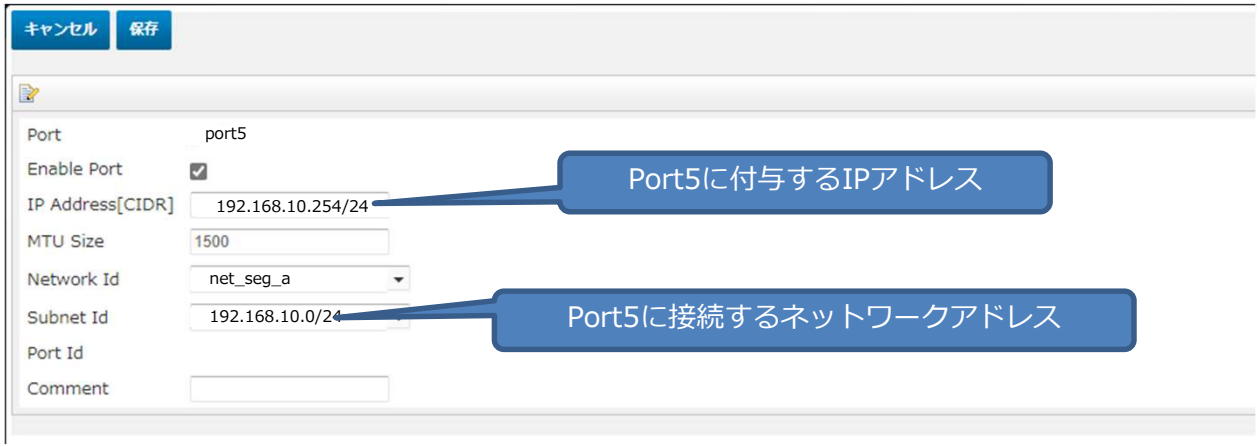


MFW-02

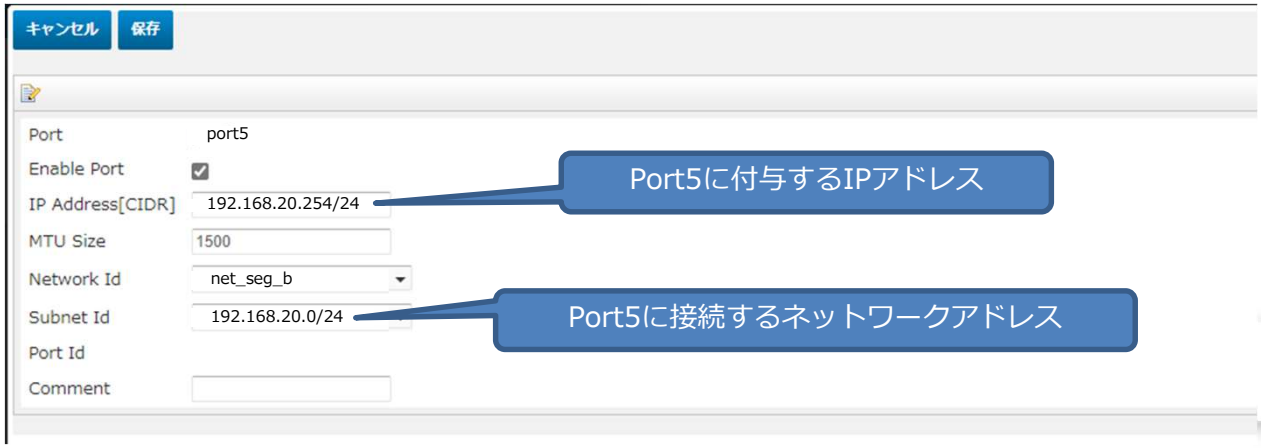
手順⑤ M-FWの設定

［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



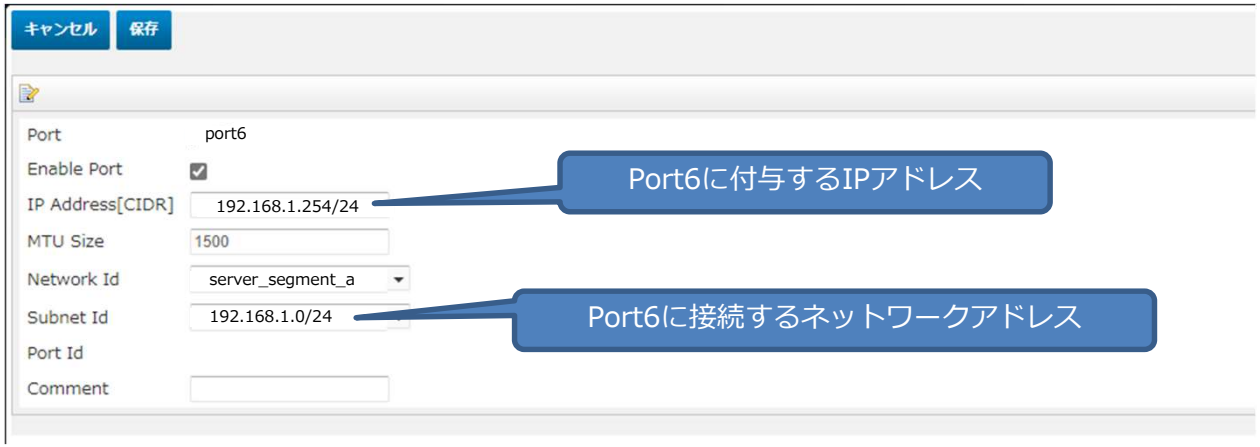
MFW-02



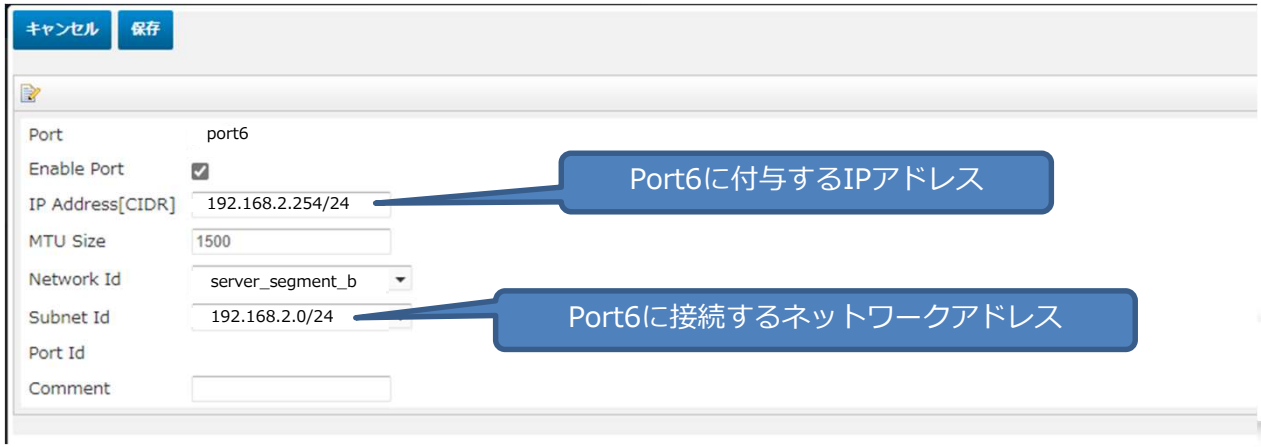
手順⑤ M-FWの設定

［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

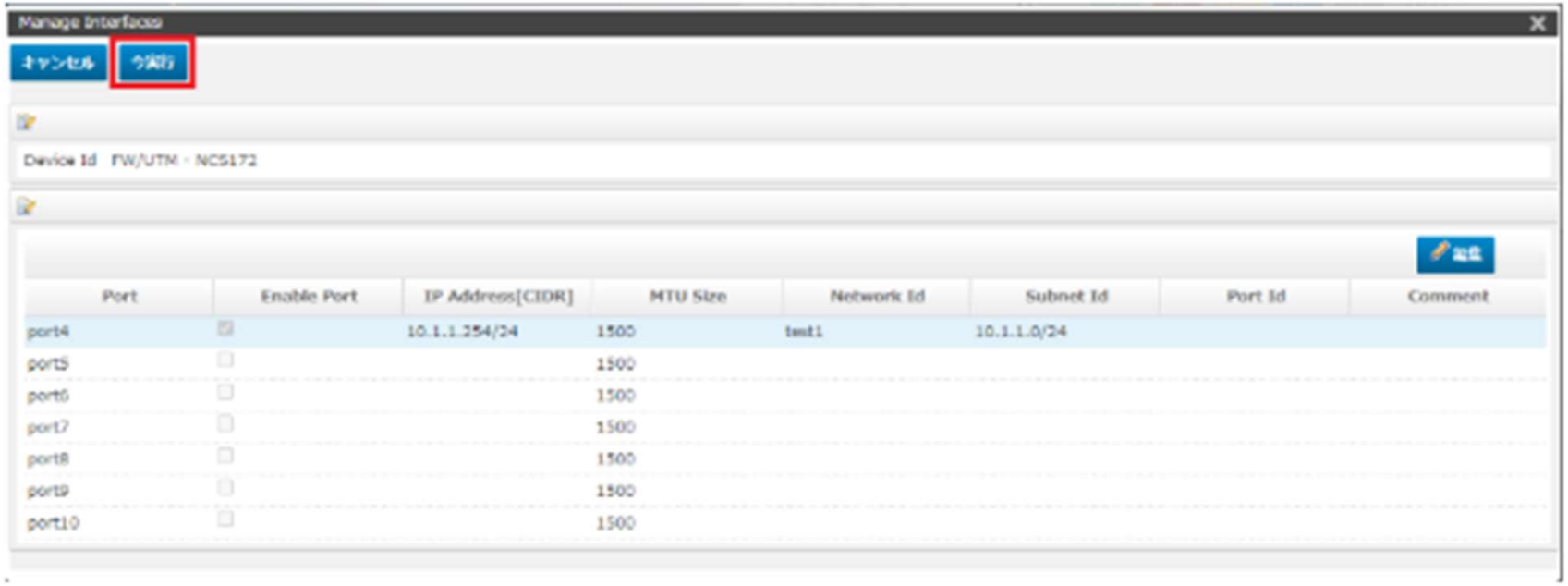


MFW-02



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。

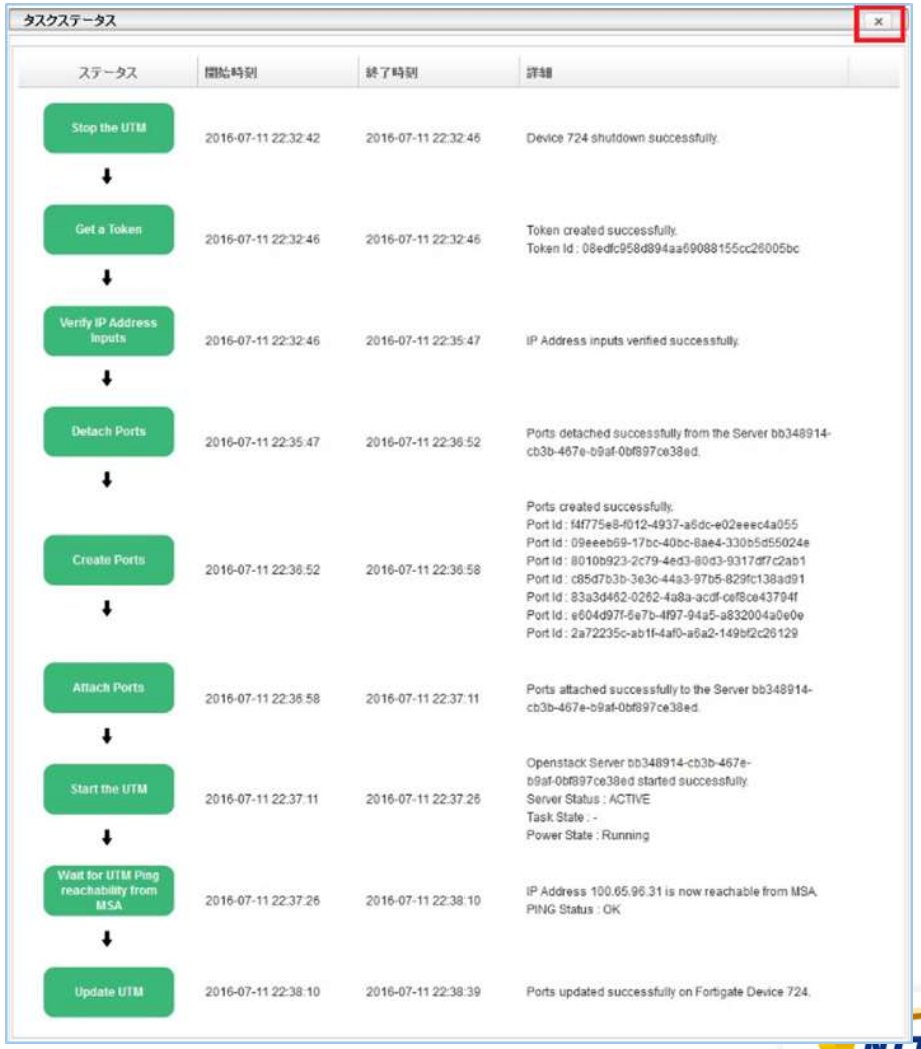


手順⑤ M-FWの設定

[タスク ステータス]が表示されます。

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。



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
------------                            -------------
172.16.0.161                              192.168.10.25
    Tunnel  State  Bytes Out/In     Encrypt      Hash    A-Time  L-Time  Proto
    ------  -----  -------------  -----------  --------  ------  ------  -----
    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
------------                            -------------
172.16.0.25                               192.168.20.161
    Tunnel  State  Bytes Out/In     Encrypt      Hash    A-Time  L-Time  Proto
    ------  -----  -------------  -----------  --------  ------  ------  -----
    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.
```