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(ネットワーク外側設置構成)

第1版

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

更新履歴

更新日	更新内容	版数
2018/07/25	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)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。

・ 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。

※事前検証を行ってから移行を実施ください。

注意事項

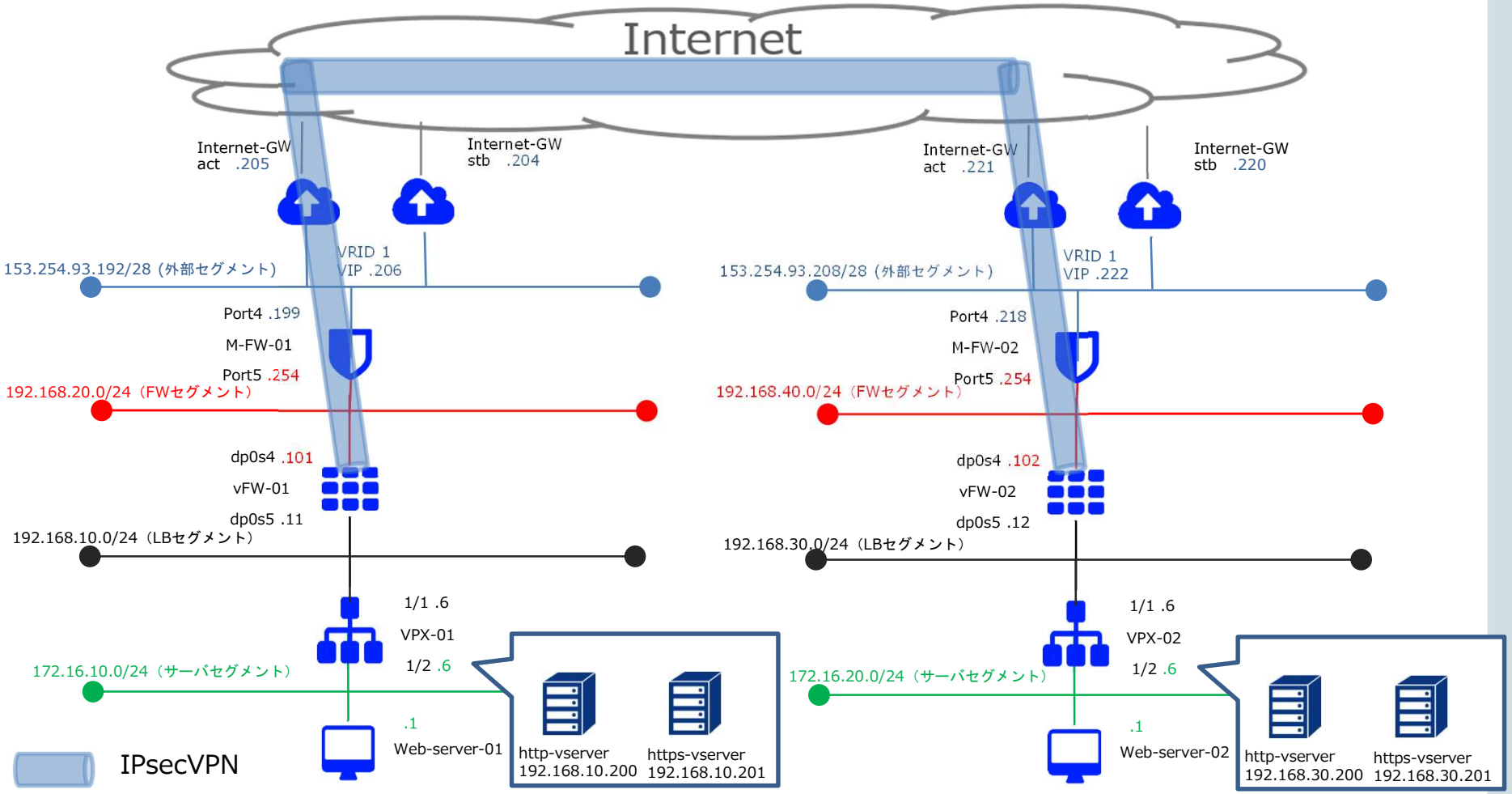
・Internet経由でIPsecをご利用される際、M-FWのInternet Gateway向きIFにプライベートIPアドレスを割り当てた場合、Internet GatewayとM-FWの間にNAT機器をご用意頂く必要がございます。
また下記の要件を満たす必要がございます。
  ・M-FW/UTM間でIPの接続性に問題ないこと
  ・InitiatorからResponder宛にUDP/ポート番号:500、UDP/ポート番号:4500、IP/プロトコル番号:50が通信許可されていること。

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。

・移行に伴い、M-FWに割り当てるIPアドレスをvFWのIPアドレスから変更される際は、各周辺機器の設定変更も考慮して下さい。

構成および移行フロー

移行前構成（vFW構成）



・vFWルールは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

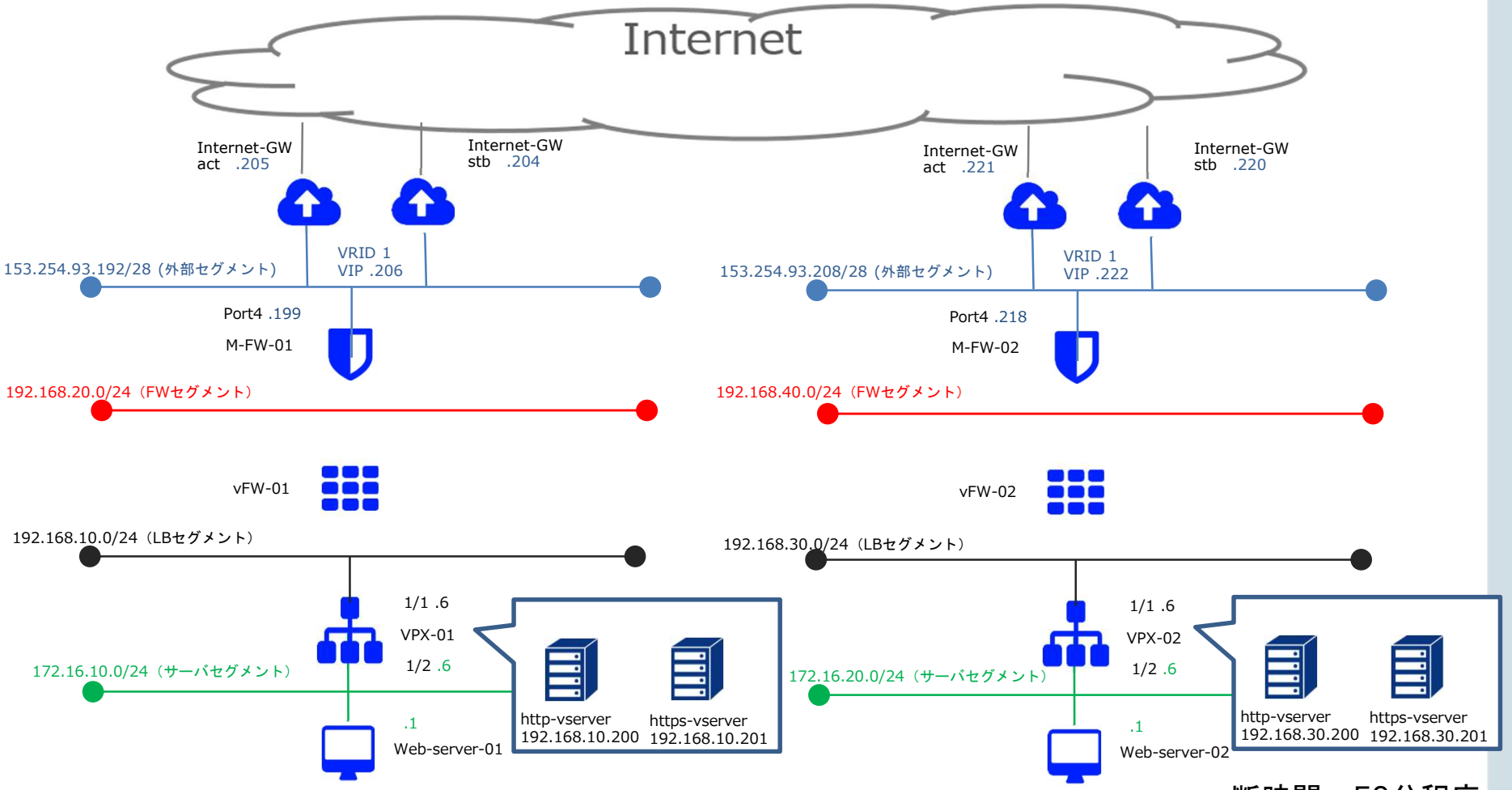
```
set interfaces vti vti0 address '10.1.1.1/30'
set security vpn ipsec esp-group ESP-1W lifetime '3600'
set security vpn ipsec esp-group ESP-1W proposal 1 encryption 'aes256'
set security vpn ipsec esp-group ESP-1W proposal 1 hash 'sha2_256'
set security vpn ipsec ike-group IKE-1W lifetime '28800'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

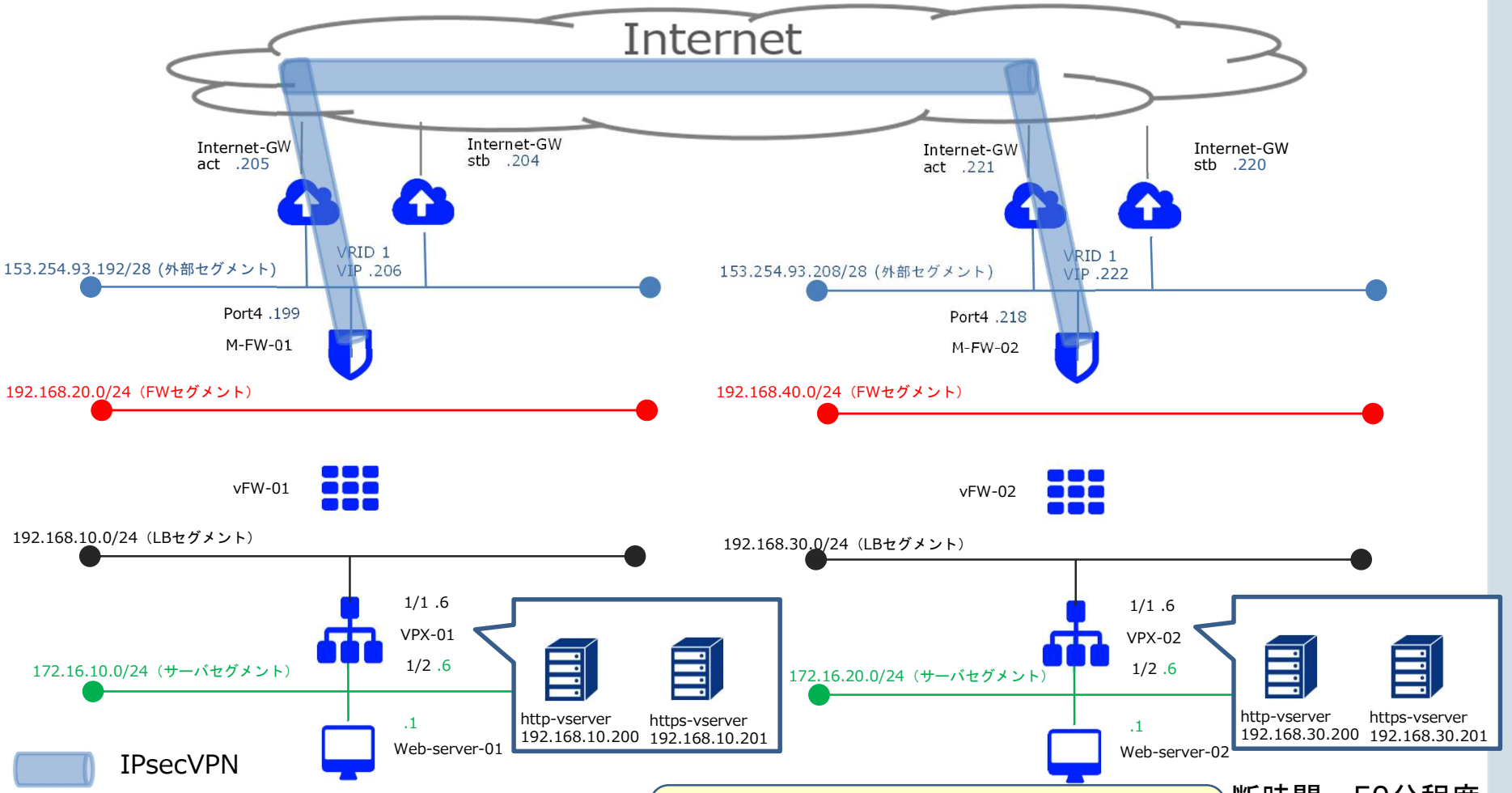


断時間：50分程度
(実測値)

手順① M-FWの設定変更**(通信断発生)**
1. IF切断
手順② vFWの設定変更
1. IF切断

Global ICT Partner
Innovative. Reliable. Seamless.

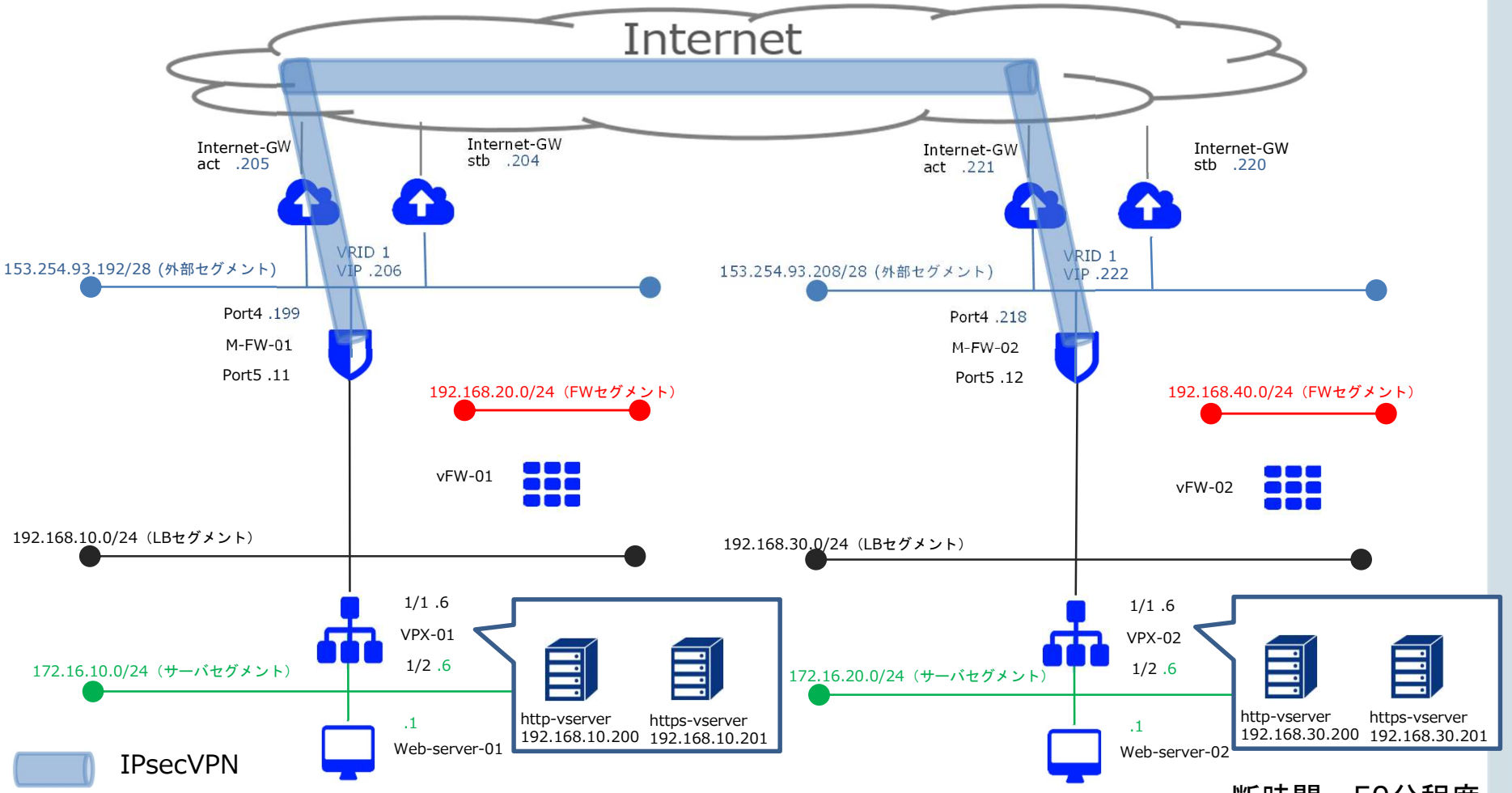
移行時構成②



手順③ M-FW設定
1. IPSecセッティング設定
2. IPSecルーティング設定
3. IPSecポリシー設定
4. IPsecVPN状態確認

断時間：50分程度
(実測値)

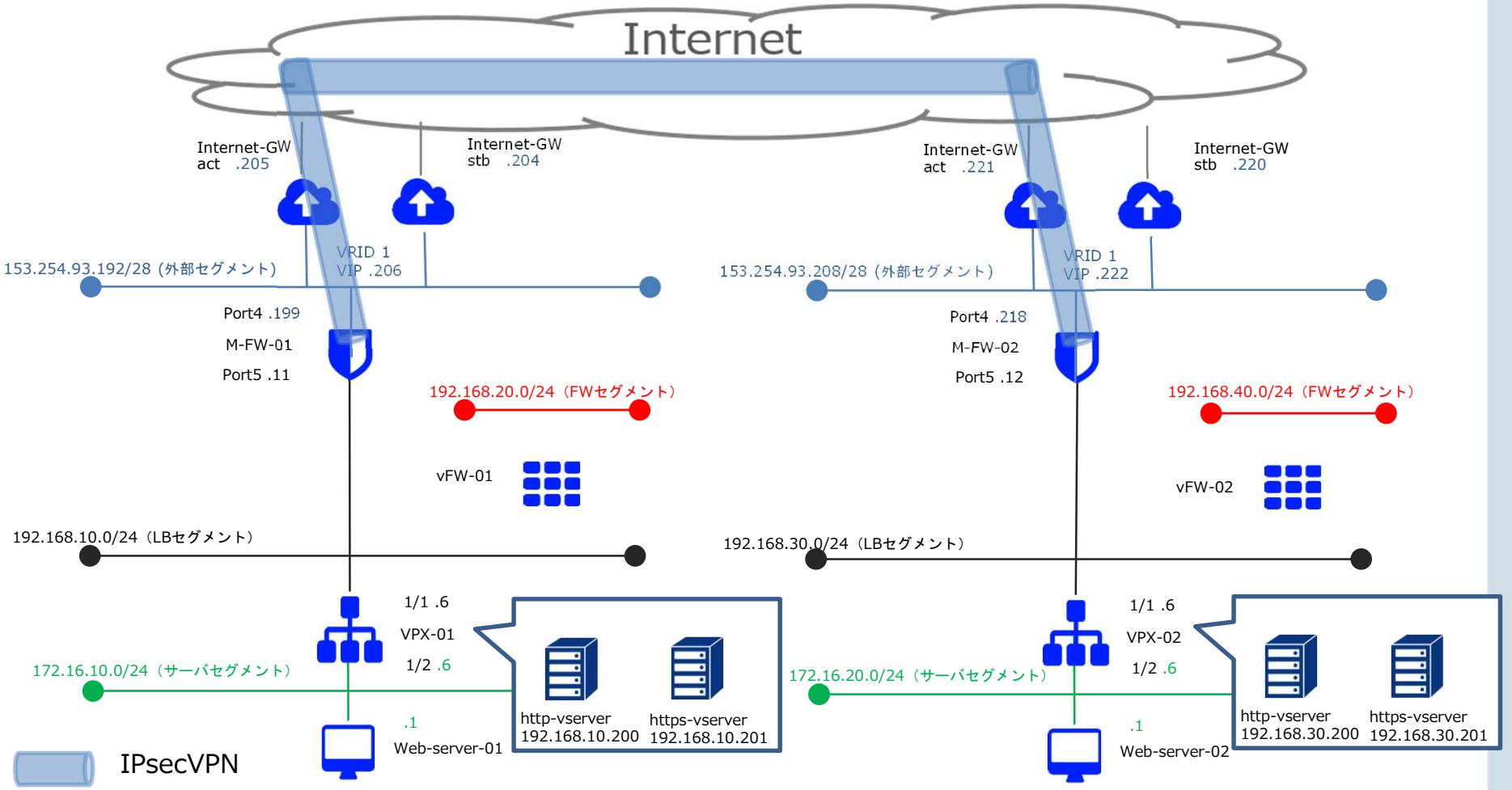
移行時構成③



断時間：50分程度
(実測値)

手順④ M-FW設定
1. IF設定(IPアドレス)を実施**(通信断回復)**

移行完了構成（Managed Firewall構成）



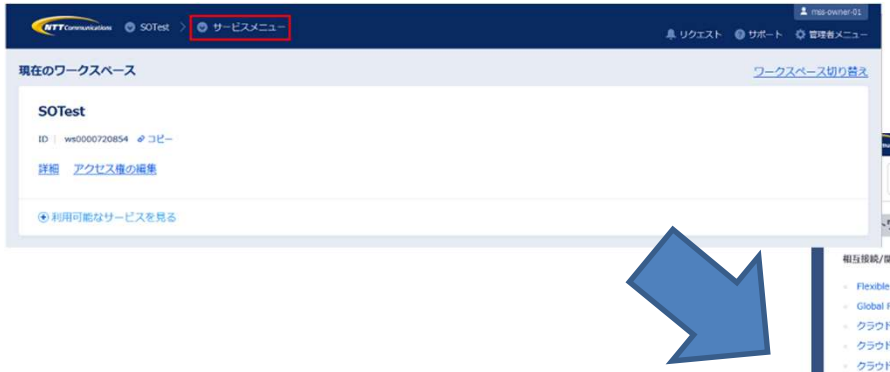
手順① M-FWの設定変更
（インターフェースの切断）

手順① M-FWの設定変更
(インターフェースの切断)

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。



『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の設定
(インターフェースの切断)

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

Security Menu

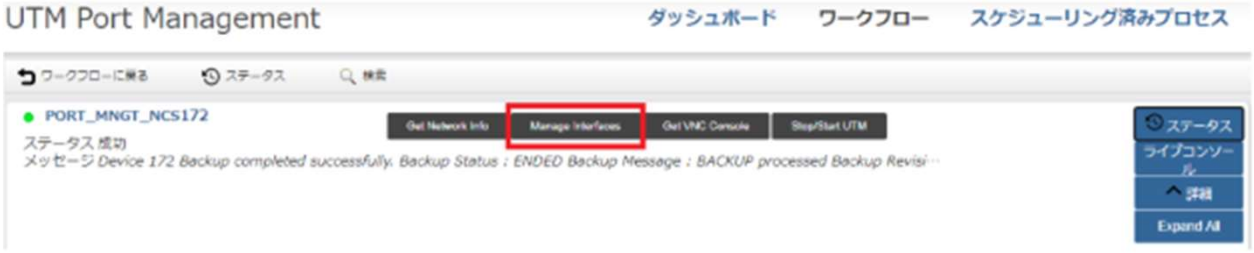
Network-based Security	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
	Managed Firewall(Version2) Managed UTM(Version2)	Order	Operation
	Managed WAF(Version2)	Order	Operation
Host-based Security	Managed Anti-Virus Managed Virtual Patch Managed Host-based Security Package	Order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

手順① M-FWの設定
(インターフェースの切断)

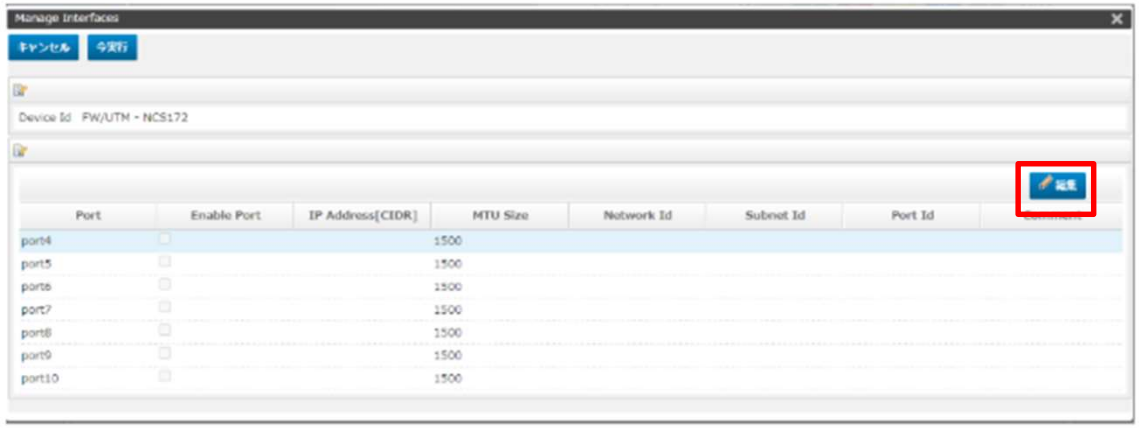
［サービス] -> [ワークフロー] -> ［UTM Port Management］ をクリックすると、インターフェース設定の詳細画面が開きます。
シングル構成の場合、［Cluster Port Management］及び［Cluster Route Management］は使用しません 。

手順① M-FWの設定
(インターフェースの切断)

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① M-FWの設定変更
(インターフェースの切断)

［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。

手順① M-FWの設定変更
(インターフェースの切断)

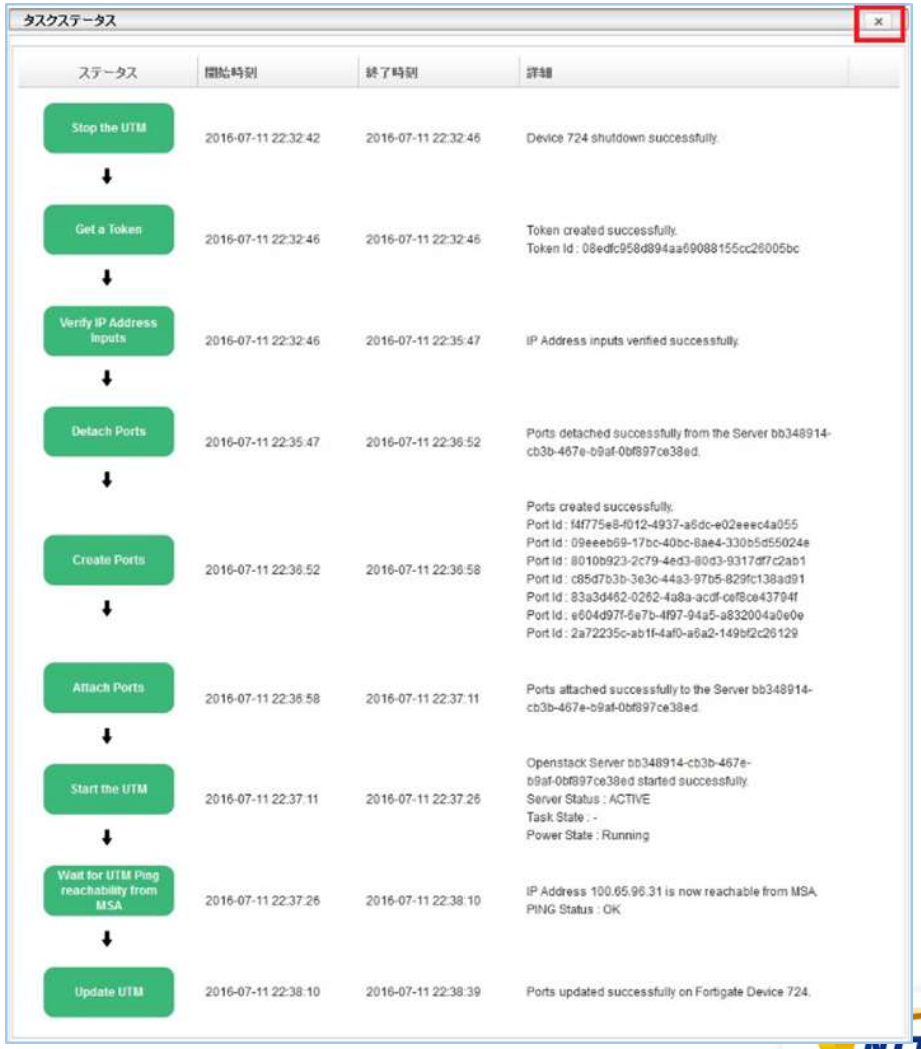
使用するポート設定が準備できたら、Manage Interfaces画面で［今実行］をクリックします。
通信断が発生します。

手順① M-FWの設定
(インターフェースの切断)

[タスク ステータス]が表示されます。

手順① M-FWの設定
(インターフェースの切断)

すべてのステータスが「緑色」になれば正常終了です。



手順① M-FWの設定変更
(インターフェースの切断)

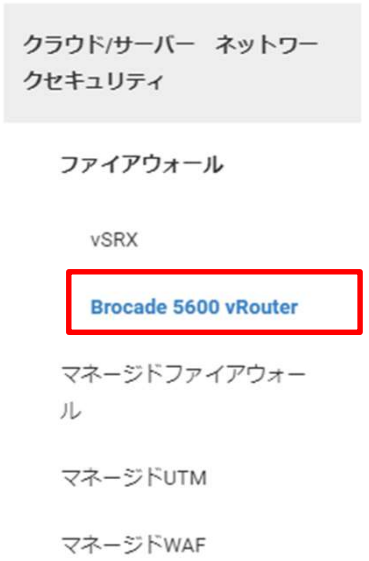
対向のM-FWにて同様の手順でインターフェースの設定変更をお願いいたします。

手順② vFWの設定変更
（インターフェースの切断）

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



手順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。

「ロジカルネットワークの切断」をクリック

手順② vFWの設定変更
（インターフェースの切断）

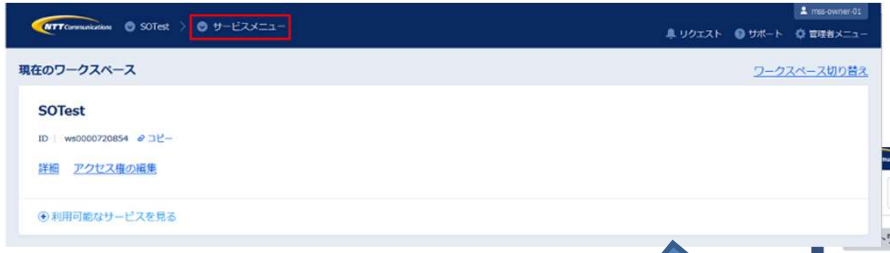
対向のvFWにて同様の手順でFWセグメントとLBセグメントのインターフェースの切断をお願いいたします。

手順③-1 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。



『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

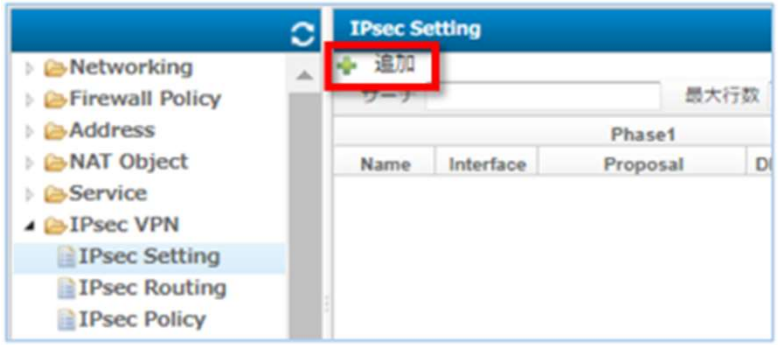
手順②-2 M-FWの設定
(IPsecセッティングの設定)

「デバイス」からいずれかのデバイスを右クリックします。

画面右側の「コンフィグ」をクリックします。

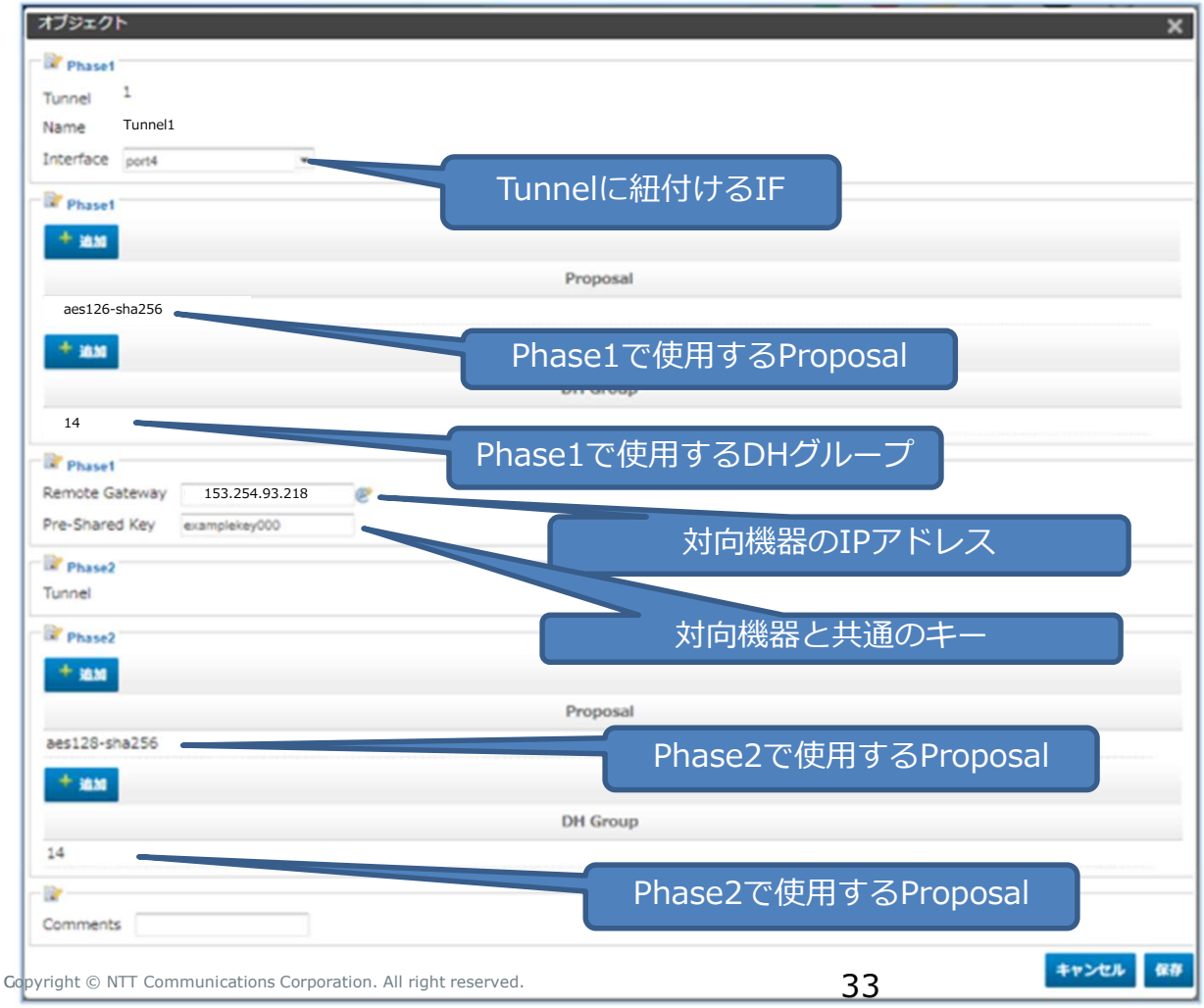
手順②-2 M-FWの設定
(IPsecセッティングの設定)

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。



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。

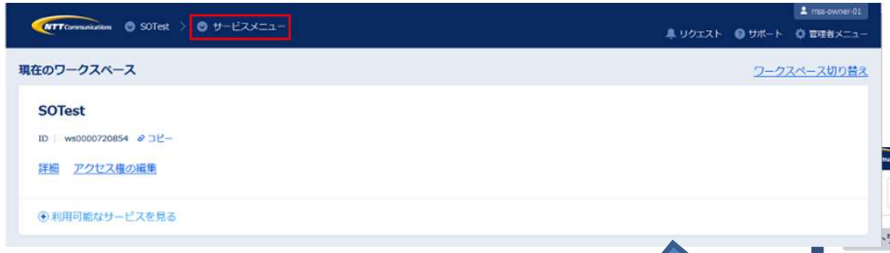
手順③-2 M-FWの設定
(IPsecルーティングの設定)

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。



『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

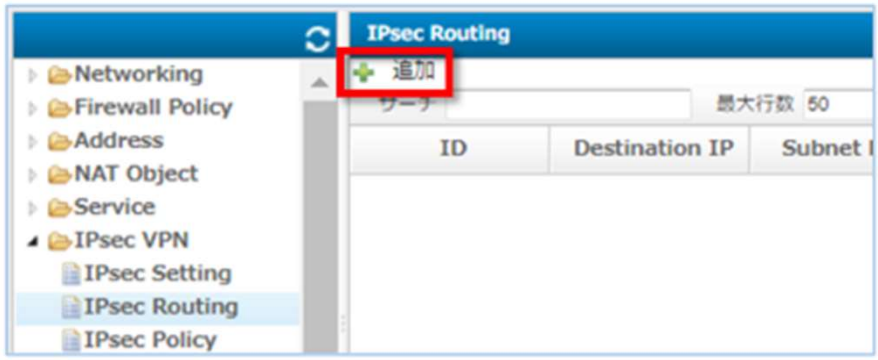
手順②-3 M-FWの設定
(IPsecルーティングの設定)

「デバイス」からいずれかのデバイスを右クリックします。

画面右側の「コンフィグ」をクリックします。

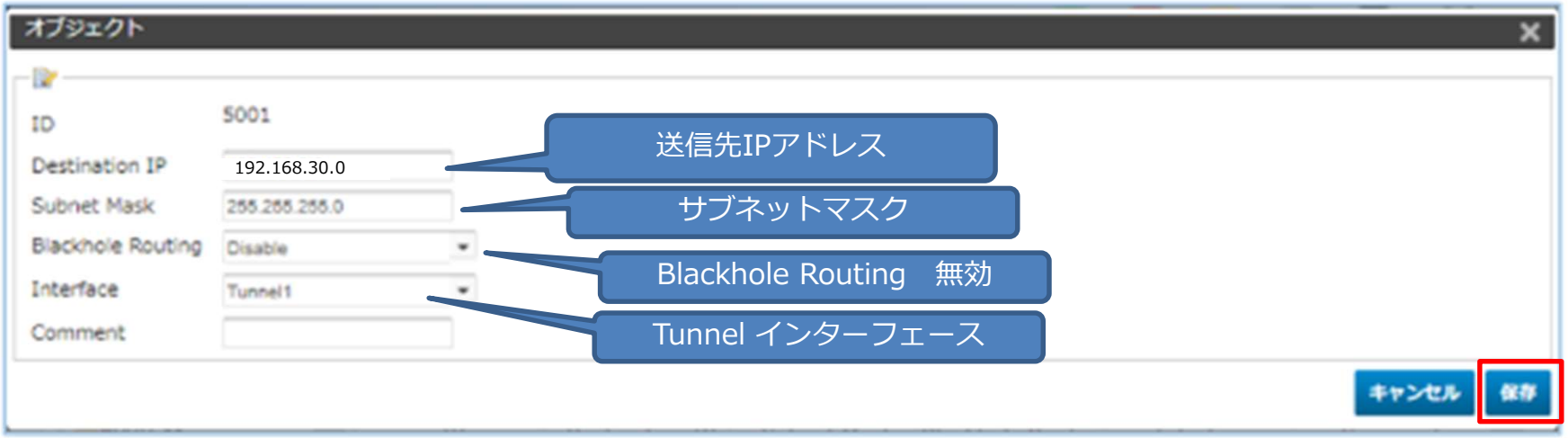
手順②-3 M-FWの設定
(IPsecルーティングの設定)

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。



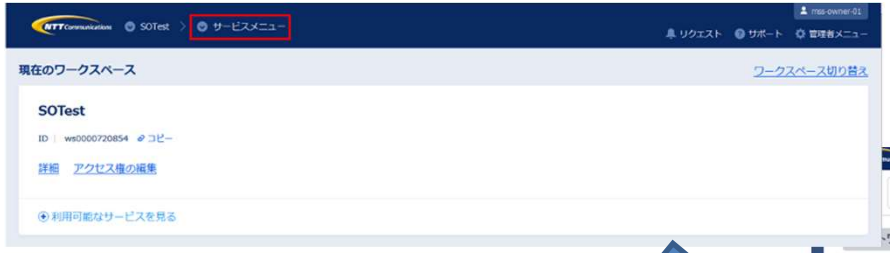
手順③-3 M-FWの設定
(IPSecポリシーの設定)

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。



『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

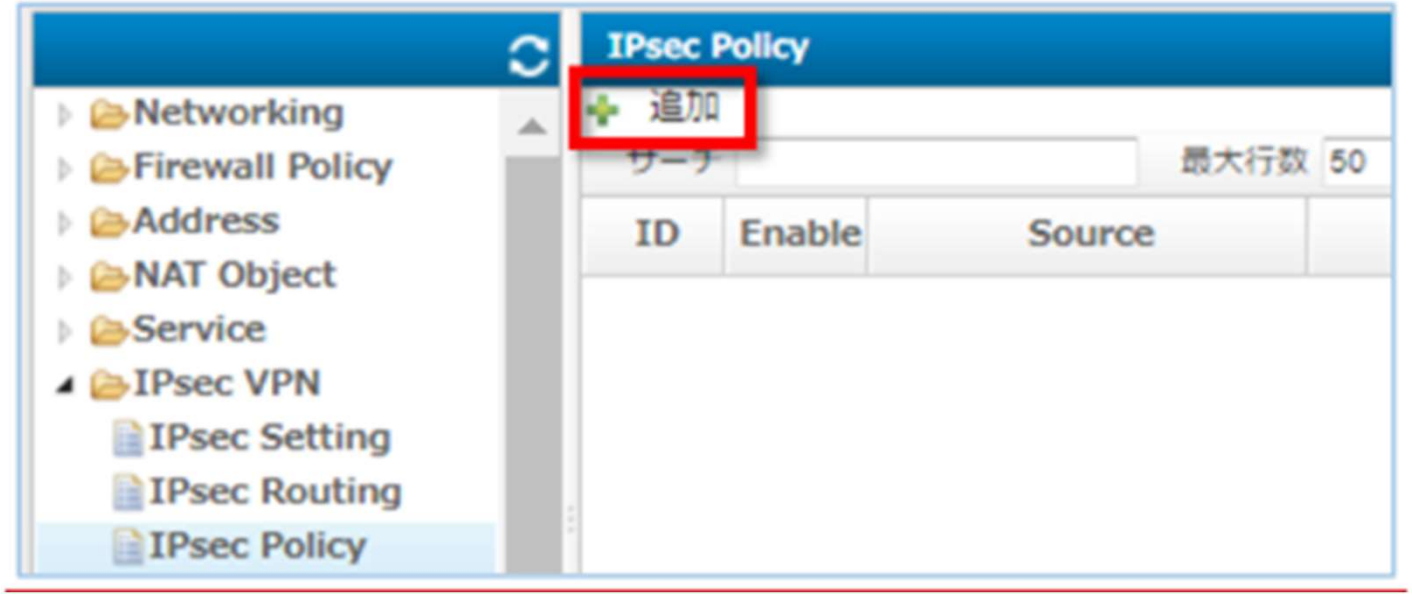
手順②-4 M-FWの設定
(IPsecポリシーの設定)

「デバイス」からいずれかのデバイスを右クリックします。

画面右側の「コンフィグ」をクリックします。

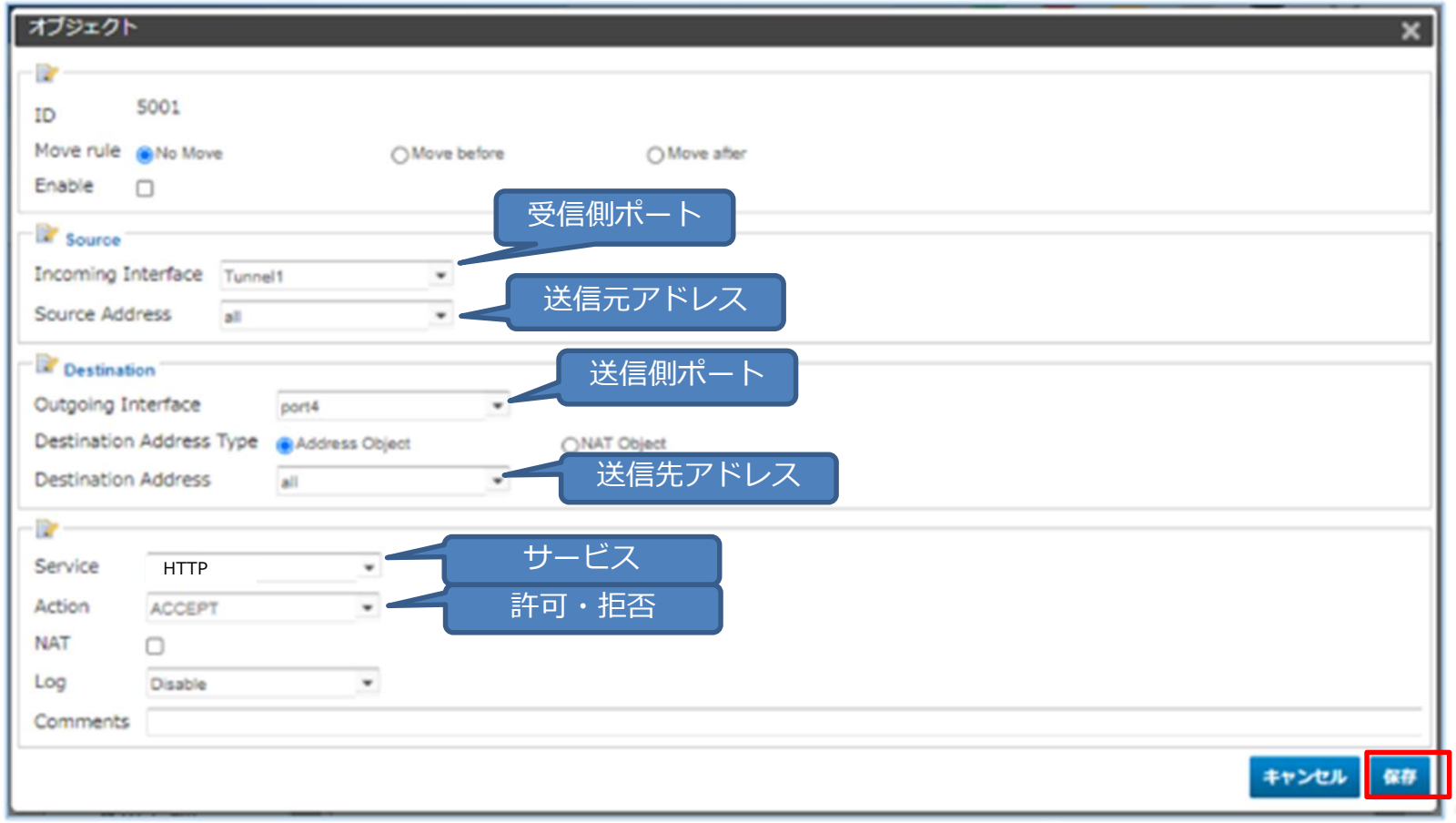
手順②-4 M-FWの設定
(IPsecポリシーの設定)

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。



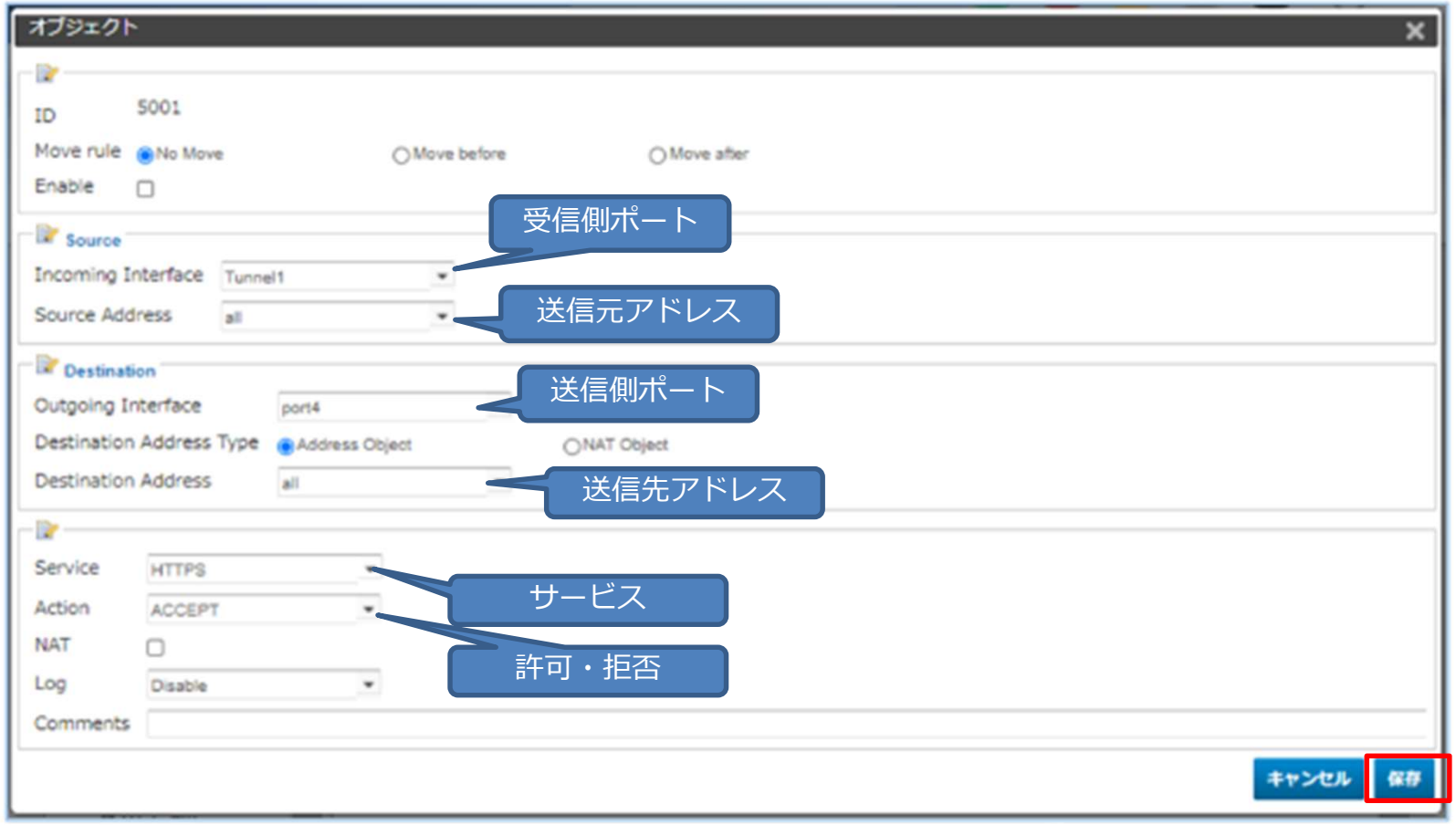
手順②-4 M-FWの設定
(IPsecポリシーの設定)

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。



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。



手順③ 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。

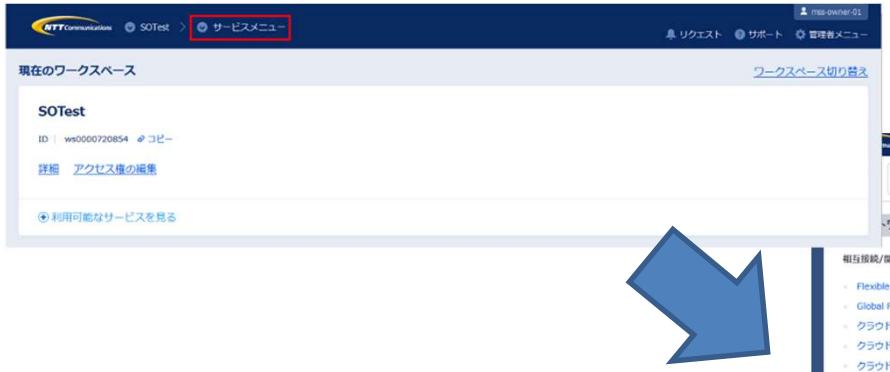
手順③-4 M-FWの設定
(IPsec状態確認)

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_view.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)

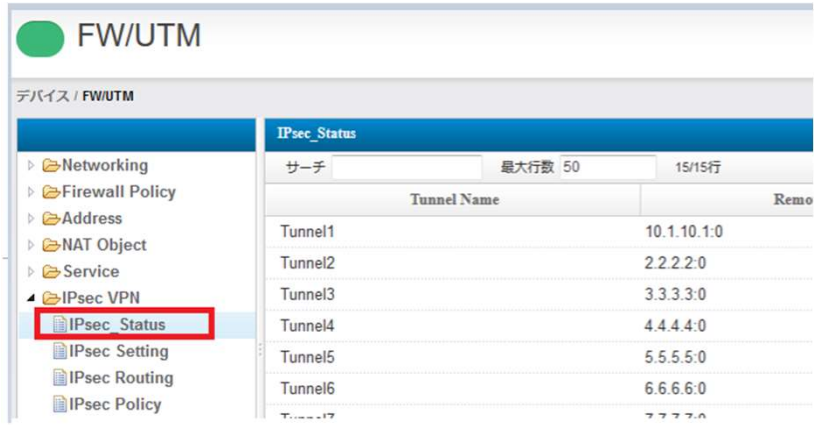
Managed Firewall(Version2)の「Operation」をクリックしてください。

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

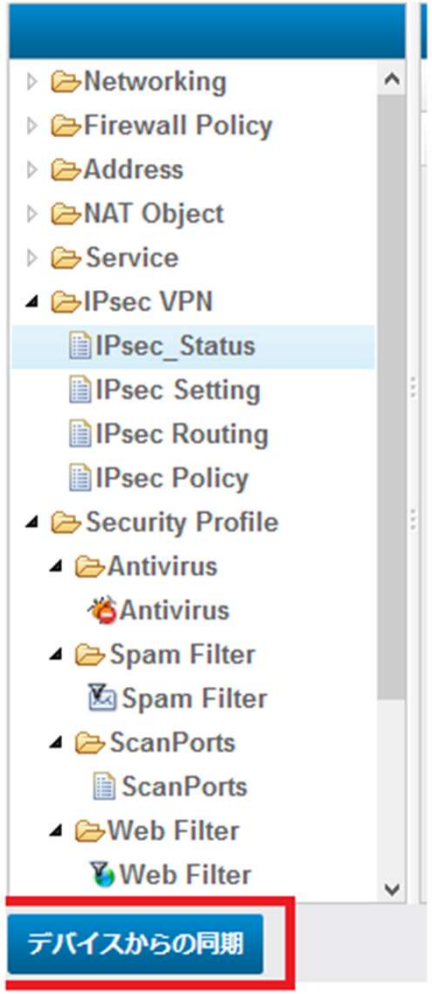
手順④-2 M-FWの設定
(IPsec状態確認)

[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 セッティング 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。



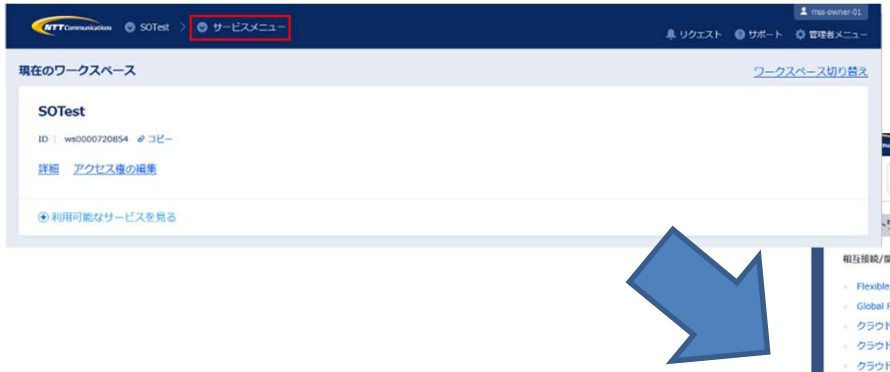
手順④ M-FWの設定
（インターフェースの設定）

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。



『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)

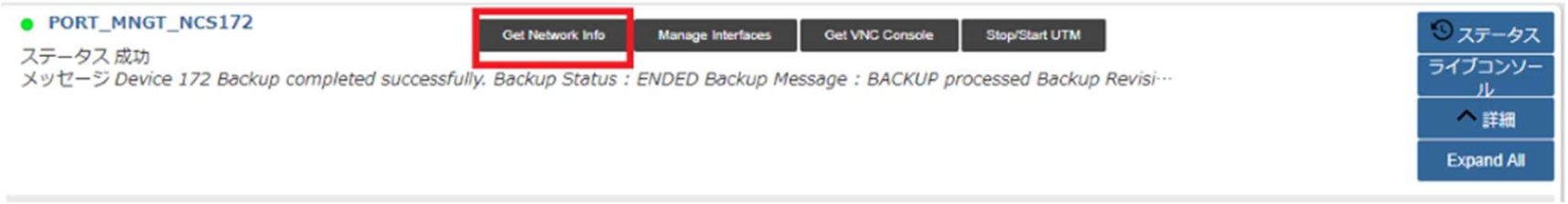
Managed Firewall(Version2)の「Operation」をクリックしてください。

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)

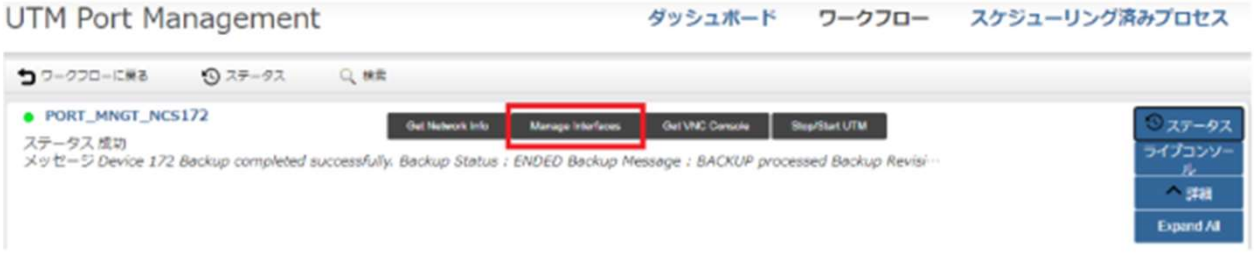
最新のお客さまネットワーク情報を参照可能にするため、設定対象のデバイスをクリックで選択して［Get Network Info］をクリックします。



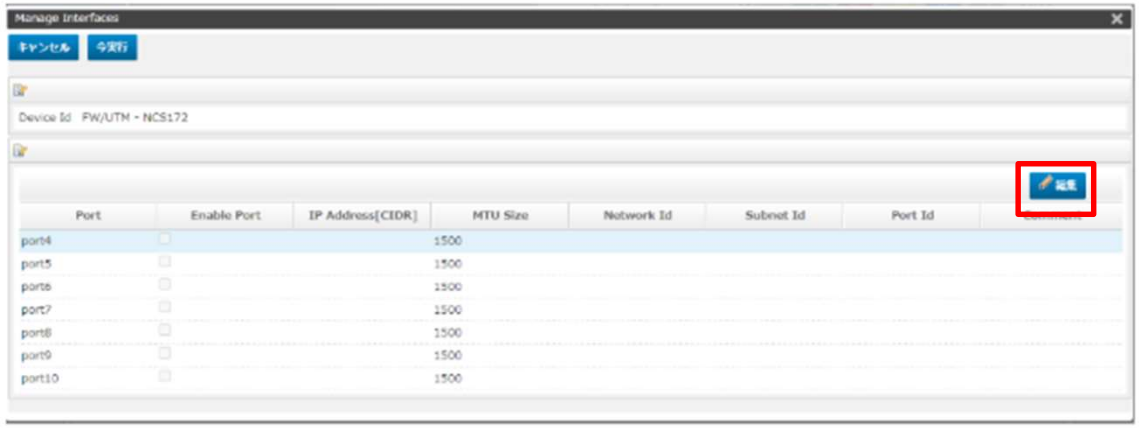
［タスク ステータス］が表示されます。Get Network Infoのタスクが「緑色」になれば正常終了です。[クローズ]で閉じてください。

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。

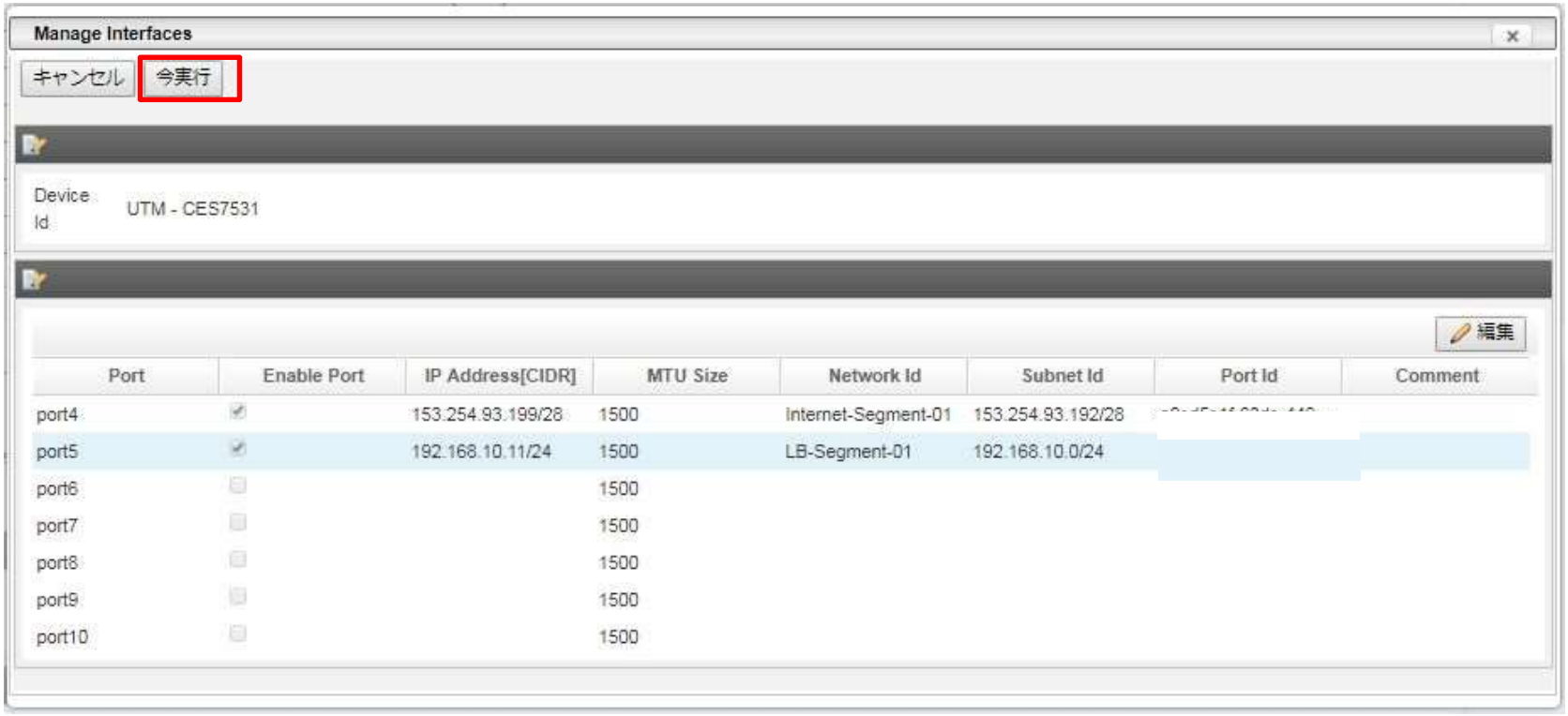


手順④-1 M-FWの設定
(インターフェースの設定)

［Enable Port］をチェックすると設定値を入力できます。
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。

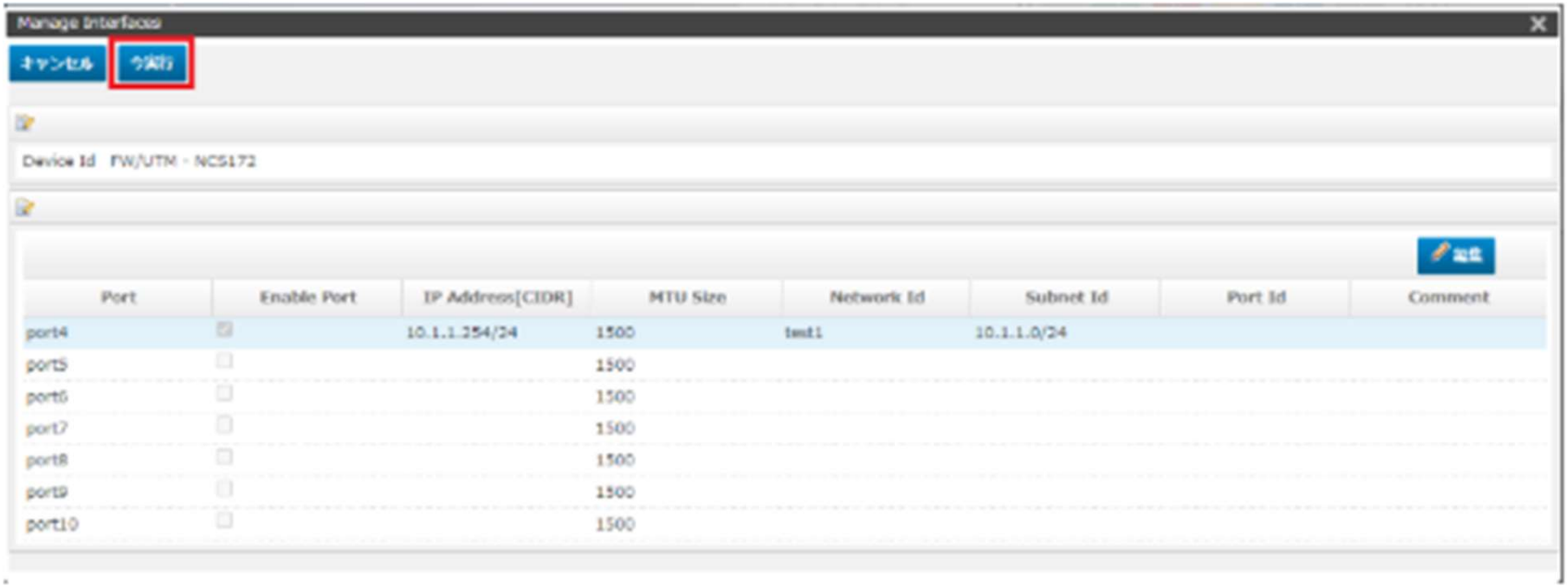
手順④ M-FWの設定
(インターフェースの設定)

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。



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。
M-FWのGlobal IPアドレスはvFWで使用していたGlobal IPアドレスを設定ください。

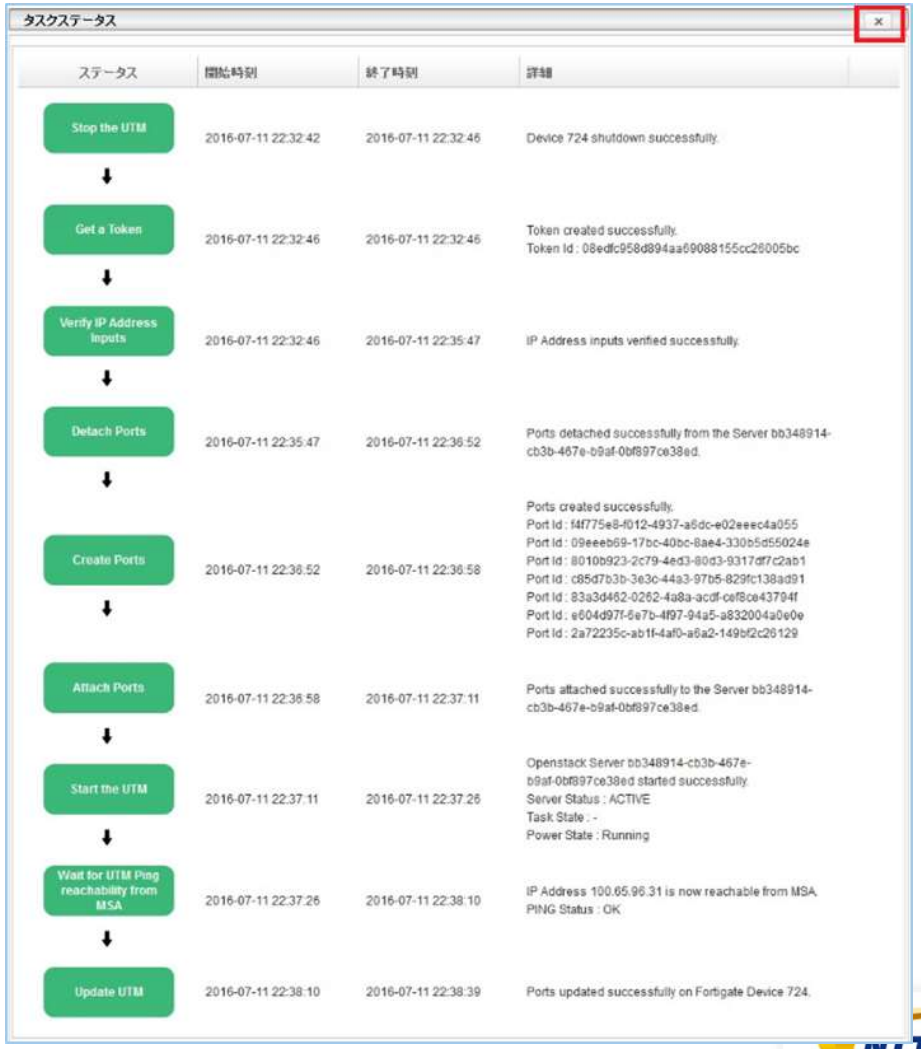


手順④-1 M-FWの設定
(インターフェースの設定)

[タスク ステータス]が表示されます。

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。



手順④ M-FWの設定
(インターフェースの設定)

対向の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。