IPsec(サイト間トンネル)機能 利用時の移行①

第1版



Copyright © NTT Communications Corporation. All right reserved.

更新履	夏歴
-----	----

更新日	更新内容		版数
2017/12/11	初版		1
Copyright © NTT Communication:	s Corporation. All right reserved.	2	ilobal ICT Partner





 $\label{eq:copyright} \texttt{Copyright} \circledast \texttt{NTT} \ \texttt{Communications} \ \texttt{Corporation}. \ \texttt{All right reserved}.$

3

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 (本資料) と②の比較

	設定項目	①資料(本資料)	2資料
初期導入時	vFWのネットワーク設定	10	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。



Copyright © NTT Communications Corporation. All right reserved.

構成および移行フロー



Copyright © NTT Communications Corporation. All right reserved.

5

検証環境構成図 Managed FW差し込みパターン①













手順① M-FW申し込み



Copyright © NTT Communications Corporation. All right reserved.

12

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

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。

CTTConnectation © SOTER > © サービスメニュー	▲ mssowmerol ▲ リクエスト ② サポート ② 管理者メニュー		
現在のワークスペース	ワークスペース切り着え		
SOTest ID w6000720854 @コピー 詳細 アクセス機の編集	averagina 💿 SOTEST 🗦 💇 ป	ezza-	泉リクエスト ● サポート ◇ 取得者
● 利用可能なサービスを見る	入力してください		6 各サービスの説明書
	-ワーク		
『ネットワーク』⇒『クラウド/ナ	田田総切/個使リービス - Flexible InterConnect - Global Flexible InterConnect - OSDN/サーバー、VFR機械ワードウェイ - クラウド/サーバー、Flexible InterConnect - クラウド/サーバー、Enterprise Cloud 1.08 - クラウド/サーバー、SD-Exchange Amazor Bits - グラウド/サーバー、SD-Exchange Amazor Bits - グラウド/サーバー、SD-Exchange Microso	インターネット/加速サービス - Super OCN Flexible Connect - DNS - Akamai Giobal Server Load Balance 開催ゲートウェイ - Distributed Secure Internet GateWay - Distributed Secure Internet GateWay - Cloud Fleatform れ Akare開発	クラウド/サーバー ローカルネットワーク - ロジカルネットワーク - 共通編集ゲートウェイ - ロードパランサー - マネージドロードパランサー
ネットワークセキュリティ』の Managed Firewallをクリックしき	クラウド/サーバー ネットワークセキュリテ・ ファイアウォール Managed Firewall Naraged UTM Managed UTM	r リモートアクセス - Flexible Remote Access	SD-WAN Software-Defined Network Service

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



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。

evice Information			0
×==-	ブラン	構成	ゾーン/グループ
Managed Firewall	2CPU-4GB	Single	zone1-groupa 💌
pyright © NTT Communications Corporation. A	\ll right reserved.	14	Global ICT Par Innovative. Reliable. S



Copyright © NTT Communications Corporation. All right reserved.

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

		フィルター		Q	+□ジカル	ネットワークの作成	章 ロジカルネットワークの削除
□ 名前	割り当てサブネット		管理状態	-	ガレーン	ステータス	アクション
			UP	5	データ用	稼働中	ロジカルネットワークの編集 🔻
			UP	5	データ用	稼働中	ロジカルネットワークの編集 🔻
			UP	Ę	データ用	稼働中	ロジカルネットワークの編集 🝷



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。

ロジャルクットロークの作品

・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。

ロシカルネットワーク	7071F7X			
ロジカルネ・ナワーク サブネ・オ サ ロジカルネ・ナワーク名	ダネオ・の時間 軽しいロジカルネナワークを作成できます。合わせて、この ロジカルネナワークに割り描できサブネノを次かパネルで			
ブレーン [*] データ用	14.02 (19.2 F.	ロジカルネットワークの作成	× ロジカルネットワー	2の作成 *
ロジカルネットワークの原則		ロジカルネホワーク* サブネットの19日 サブネットる 新しいロジカルネットワークに割り起てるサブ・	ロジカルキッドワーク [*] サブネット [*]	サブネットの お 様 サブネットの追加県性を被用します。
ロジカルキ・ホワークのタグ O 智慧状語 [®] O UP		す。この場合、「キナワークアドレス医権定す キオワークアドレス [®] の 192.168.10.0/24 ゲーウェイドの	JSと変があり DH3 9 ~ J <~ 0	Ъ.
	取55百L 。 戻5 (次へ »	192.168.10.254	МТР U − <i>J</i> (~ Q	ă.
		取は高し 一度る	 泡加の小~ H2天 ●	.a
			サブネットの説明	d
			973-9697 0	ь
			NTT	4
pyright © NTT Communicat	ions Corporation. All right reserved.	17		未5次し < 長る ロジカルネットワークの休止

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。

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	Rot OUVIB			
ロジカルネ・オワーク名	新しいロジカルネットワークを作成で巻ます。合わせて、この ロジカルネットワークに割り崩てるサブネットを次のパネルで			
ブレーン [*] データ用	4x27823.	ロジカルネットワークの作成	* ロジカルネットワークの作成	×,
ロジカルネットワークの説明		ロジカルネットワーク [*] サブネットのWB サブネットのWB	ロジカルキットフーク ¹ リブキット ² リブキットの基礎 こ 04CP 米和 のアドレオリロゴールの	ナブキットの違加属性を補用します。
ロジカルネットワークのタブ 🛛			を作成しま 涙があり 	
管理は思 [*] ● UP		7-+>±√₽₽ 192.168.20.254		
	取り話し (戻る) (次へ)	□ ゲートウェイなし 取け届し (現5)	КТР Ü – <i>S</i> – 0	
		• •		
				_
			NTT	
opyright © NTT Communicatio	ns Corporation. All right reserved.	18	R	9済し 《長ろ ロジカルネットワークの作成



Copyright © NTT Communications Corporation. All right reserved.

手順③-1 M-FWの設定 (Destination NATの設定)



Copyright © NTT Communications Corporation. All right reserved.

Destination NATの設定は下記をご覧ください。。 https://sdpf.ntt.com/services/docs/network-basedsecurity/tutorials/rsts/security/operation/managed_firewall_utm_v2/4330_destination_n at.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。

在のワークスペース SOTest ID ws000072054 @コピー 詳細 アクセス像の編集	<u>ワークスペース切り首ス</u> の元ms 入力	© S0Test > ♥ サービスメニュー		
SOTest ID v=0000720854 @コピー 詳細 <u>アクセス俄の漏</u> 集	99000ee	😋 SOTest 👌 🥺 ೮-೮スメニュー		
ID we000072054 9 コピー 詳細 アクセス俄の編集	voizzon A.tz	SoTest) 🥑 サービスメニュー		
詳細 アクセス風の減速	۵.			
	入力			▲ リクエスト ● サポート 交 管理者
◎ 利田司がかけ」ピフカ日ス		ノてください		10 名サービスの説明書
© 49m948/497−CA236©	-9-0			
	相互接続/間連サー	iz.	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
	- Flexible Interd	nnect	 Super OCN Flexible Connect 	- ロジカルネットワーク
	Global Flexible	InterConnect	- DNS	- 共通機能ゲートウェイ
	クラウド/サー/	ー VPN接続ゲートウェイ	 Akamai FastDNS 	- ロードバランサー
	- クラウド/ サ ー/	- インターネット接続ゲートウェイ	- Akamai Global Server Load Balance	マネージドロードバランサー
	・ クラウド/サー/	- Flexible InterConnect接続ゲートウェイ	 Distributed Secure Internet GateWay 	
	クラウド/サー/	- コロケーション接続		
	- クラウド/サー/	ー リージョン間接続		
	- クラウド/サー/	ー テナント開接线		
	クラウド/サー/	- Enterprise Cloud 1.0接続		
	クラウド/サー/	- SD-Exchange Amazon Web Services		
	世現	- CD Durbanes Canala Claud Distance		
	1995円95-7	- SD-Exchange Google Cloud Platform		
『ネットワーク』⇒『クラウド/サ-	- /	- SD-Exchange Microsoft Azure接线		
	ATTACH I	Auto Auto area	the testing	
ネットワークヤキュリティ』の	059F/ 9 -X-	ネットワークセキュリティ	リモートアクセス	SD-WAN
	- ファイアウォー	6	Flexible Remote Access	 Software-Defined Network Service
Managed Firewallをクリックします	- Managed Firev	BN		
Managed in ewane 222206 s	O - Managed UTM			
	 Managed WAF 			
				Clobal ICT Par
				munications
				innovacive, kellable, se
t © NTT Communications Corporation, All right reserved.	21			

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

	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
Network-based Security	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



「デバイス」からいずれかのデバイスを右クリックします。

デバイス	ログ&レポート	サービス	カスタマープロファイル	チケット管理
バイス			オールフィルター ・ 並び	び替え 🔻
ステータ:デバイス名	Hant	HAステータス	領域	

画面右側の「コンフィグ」をクリックします。

デバイス	ログ&レポート	サービス	カスタマープロファイル	チケット管理
			概説 詳細	コンフィグログ
デバイス / FW/UTM				
CNIMDHAT				

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。

	Destination I	NAT
Firewall Policy	 ・追加 サーチ 	
Address Object	NAT Name	External IP … N
▲ ➢NAT Object		
Contraction NAT		
Source NAT		
pyright © NTT Communications Corporations	ion. All right reserved.	

Global ICT Partner

Innovative, Reliable, Seamless,

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 × - 📝 Port4_DNAT NAT Name M-FW01の受信側VIP External IP Address 172.16.0.25 Mapped IP Address 192.168.10.25 FW01のアドレス External Interface port4 Port Forward \square Comment キャンセル **MFW-02** オブジェクト × - 2 Port4DNAT M-FW02の受信側VIP NAT Name External IP Address 172.16.0.161 FW02のアドレス Mapped IP Address 192.168.20.161 External Interface port4 Port Forward \Box Comment

24

キャンセル

保存

lobal ICT Partner

Copyright © NTT Communications Corporation. All right reserved.



Copyright © NTT Communications Corporation. All right reserved.

Source NATの設定は下記をご覧ください。。 https://sdpf.ntt.com/services/docs/network-basedsecurity/tutorials/rsts/security/operation/managed_firewall_utm_v2/4340_source_nat.ht ml

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。

現在のワークスペース	ワークスペース切り替え		
SOTest ID ws0000720854 @ コピー			
詳細 アクセス確の編集	nurications 🔘 SOTEst 🗦	• 9 -EXX=1-	▲ リクエスト ● サポート ☆ 管理者
A DIRECTOCALL NOT A R Z	入力してください		B 各サービスの説明書
③利用可能なカービンをおる	-9-0		
	相互接続/間達サービス	インターネット/間達サービス	クラウド/サーバー ローカルネットワーク
	- Eavible InterConnect	Super OCN Elevible Connert	- 0900-2
	Global Flexible InterConnect	 DNS 	- 共通機能ゲートウェイ
	クラウド/サーバー VPN接続ゲート	ウェイ Akamai FastDNS	- ロードバランサー
	クラウド/サーバー インターネット	接続ゲートウェイ - Akamai Global Server Load Balance	マネージドロードバランサー
	- クラウド/サーバー Flexible Interd	Connect提続ゲートウェイ Distributed Secure Internet GateWay	
	クラウド/サーバー コロケーション	-接続	
	クラウド/サーバー リージョン開設	2.统	
	クラウド/サーバー テナント構接線		
	クラウド/サーバー Enterprise Clo	bud 1.0投统	
	- クラウド/サーバー SD-Exchange	Amazon Web Services	
	接续		
	 クラウト/サーバー SD-Exchange 接続 	Google Cloud Platform	
『ネットワーク』⇒『クラウド/・		Microsoft Azure接现	
	0 1 C	1-11-1 UT-1-2042	60 WAN
ネットワークセキュリティ』の	シンシャパターパー ネタトシークセー	94-F790A	20+WAR
	- ファイアウォール	 Flexible Remote Access 	 Software-Defined Network Service
Managed Firewallをクリックし	- Managed Firewall		
	- Managed UTM		
	 Managed WAF 		
			Global ICT Par
		NTTCo	munications GIODALICI Fal

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

	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
Network-based Security	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



「デバイス」からいずれかのデバイスを右クリックします。

7/12	ログ&レポート	サービス	カスタマーフロファイル	チケット管理
バイス			オールフィルター • 並び	ξ λ . ▼
	HAペア	HAステータス	領域	
ステータ、デバイス名				

画面右側の「コンフィグ」をクリックします。

デバイス	ログ&レポート	サービス	カスタマープロファイル	チケット管理
FW/UTM			概説 詳細 コン	/フィグ ログ
<i>デバ</i> イス / FW/UTM				
CNINDHAN				

 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。

	0	Source NAT
 A Constant Section NAT Constant Section NAT Constant Section NAT 	^	◆ 追加 サーチ NAT Name
▲ Service Service Object		





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 Start IP Address End IP Address Comment	Port5_SNAT 172.16.0.25 172.16.0.25	SNAT後のアドレスを StartとEndに入力	
			キャンセル 保存

MFW-02

オブジェクト				×
NAT Name Start IP Address End IP Address Comment	Port5_SNAT 172.16.0.161 172.16.0.161	SNAT後のアドレスを StartとEndに入力		キャンセル 保存
Copyright © NTT Commu	unications Corporation. All righ	t reserved.	29	Global ICT Partner Innovative. Reliable. Seamless.

手順③-3 M-FWの設定(ファイ アウォールポリシーの設定)



Copyright © NTT Communications Corporation. All right reserved.

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.

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。



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

	Managed Firewall Managed UTM	Order	Operation
	Managed WAF	Order	Operation
Network-based Security	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



「デバイス」からいずれかのデバイスを右クリックします。

デバイス	ログ&レポート	サービス	カスタマープロファイル	チケット管理
バイス			オールフィルター ・ 並び動	łż. •
ステータ:デバイス名	HAペア	HAステータス	領域	

画面右側の「コンフィグ」をクリックします。

デバノフ	LL	#_ビフ	カフタマープロファイル	チケット等項
7/17		9-CX	7798-707747	デジット官理
			_	
FW/UTM			概説 詳細 コン	/フィグ ログ
デバイス / FW/UTM				
CNIMDHET				

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。

	Firewall Policy
▲ ➢Networking	● 追加 サーチ
Bouting	ID E····
▲ ÈFirewall Policy	
Firewall Policy	
Converget © NTT Communications Corporation	All right reserved



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 Z 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一
· Source 文信侧八一下
Incoming Interface Port4
Source Address all ・ 送信元アドレス
Destination
Outgoing Interface Port5 送信側ポート
Destination Address Type
O Address Object Object ONAT 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 保護



設定値を入力して、 [保存] をクリックします。

MFW-01&MFW-02

P 4 Wore nulle Wore before Wore aller Sector Address Ports Sector Address Type Address Object Orget Sectoration Address Type Address Object Orget Sectoration Address Type Address Object Orget Sectoration Address Type Address Object Orget Sector Address Type Address Object Object Object Sector Address Type Address Object Object Object Sector Address Type Address Object Object Object Sector Address Type Address Object	オブジェクト						×		
p 4 Wove rule No Move before Nove after Source Constructions of the source of the so	- P								
Wove rule Now before Output Starce Starce </td <td>ID 4</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	ID 4								
Enable Source Source Incoming Interface Destination Destination Destination Destination Destination Destination Destination Address Service Actions Service AT Vise Outgoing Interface Address Use Outgoing Interface Address Outset Vise Outgoing Interface Address Vise Outgoing Interface Address Source Comment Service Service Service Service Service Set	Move rule	No Move	Mov	/e before	O Move after				
Source 受信側ボート ncoming Interface Port5 Source Address 画 Destination 送信側ボート Dutgoing Interface Port4 Destination Address Type Address Object Ont4 Object Destination Address 画 Service ALL VI mode Use Outgoing Interface Address UVUs Outgoing Interface Address Use NAPT Object NAT Tobject Object SNAT用に作成したオブジェクト SNAT用に作成したますジェクト og ALL	Enable 🔽	l.							
ncoming Interface Ports Source Address a Destination Address Type Sestination Address State Sestination Address Type Sestination Address Type Sestination Address Sestination Address Set Type Type Type Type Type Type Type Type	Source			受信側ポート					
Source Address a Destination Address Type Address Object ONT Object Destination Address Type Address Object Ont Address Object Obje	Incoming Inter	rface Port5							
Destination Dutgoing Interface Port4 Destination Address Type Address Object ONAT Object Destination Address al ONAT Object Service ALL Action ACCEPT At One Use Outgoing Interface Address Ouse NAPT Object SNAT Object SNAT	Source Addre	ess all	•						
Dutyoing Interface Point Destination Address Type Destination Address Type Destination Address Type Destination Address II Destination	Destination	3		送信御光					
Destination Address Type extination Address	Outgoing Inter	rface	Port4						
Destination Address Pestination Address Pestination Address Pestination Address Pestination Address Pestination Address Pertia Action ACCEPT Action ACCEPT Action ACCEPT Use Outgoing Interface Address Use NAPT Object VAT Object Port5_SNAT Option SinAT Comment Pertia SinAT用に作成したオブジェクト Comment Pertia SinATHIC Pertia SinATHIC	Destination A	ddress Type	Address Object		iect				
Service ALL Action ACCEPT VAT C VAT C VAT C VAT Outgoing Interface Address Use NAPT Object VAPT Object Port5_SNAT Og ALL Comment SnAT用に作成したオブジェクト Comment Comment ght © NTT Communications Corporation. All right reserved. 35	Destination A	ddress	all	•	1001				
Service ALL ・ Action ACCEPT ・ VAT で VAT mode Use Outgoing Interface Address Use NAPT Object VAPT Object Port5_SNAT ・ SNAT用に作成したオブジェクト .og ALL ・ Comment ght © NTT Communications Corporation. All right reserved. 35	· 📝								
Action ACCEPT ・ VAT @ VAT mode Use Outgoing Interface Address Use NAPT Object VAPT Object Port5_SNAT ・ SNAT用に作成したオブジェクト .og ALL ・ Comment	Service	ALL	•						
NAT wode Use Outgoing Interface Address Use NAPT Object NAPT Object Port5_SNAT SNAT用に作成したオブジェクト ALL C Comment Comment ght © NTT Communications Corporation. All right reserved. 35	Action	ACCEPT	•						
NAT mode Use Outgoing Interface Address Use NAPT Object Og ALL Comment Comment ght © NTT Communications Corporation. All right reserved. Use Outgoing Interface Address SNATT Object SNAT用に作成したオブジェクト SNAT用に作成したオブジェクト SNAT用に作成したオブジェクト SNATTのジェクト SNATTのジェクト SNATTのジェクト SNATTのジェクト	NAT								
NAPT Object Port5_SNAT SNAT用に作成したオブジェクト 	NAT mode	OUse Outgoir	g Interface Address	Use NAPT Object					
ALL Comment Seam 1 Innovative. Reliable. Seamless. ght © NTT Communications Corporation. All right reserved. 35	NAPT Object	Port5_SNAT	•	SNAT用	に作成したオン	ブジェクト			
Comment Sight © NTT Communications Corporation. All right reserved. 35	Log	ALL	•						
ביישע און איז									
ight © NTT Communications Corporation. All right reserved. 35	Commont								
ight © NTT Communications Corporation. All right reserved. 35	Comment							Global ICT	Partner
ight © NTT Communications Corporation. All right reserved. 35							キャンセル 保存	innovative. Relia	ble. Seamless.
	right © NTT Cor	mmunications C	orporation. All right	reserved.		35			

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))



Copyright © NTT Communications Corporation. All right reserved.

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	ターフェ-	ースド	削除
1. ファ- 2. ファ- クリッ	イアウォール一覧から イアウォールインタフ ックして「ロジカルネ	5対象vFWを選択 フェースタブから ミットワークの切	、 対象の 5、対象の 〕断」を選)インタフェース 訳	スの右側	」「▼」を
概要 ファイア ファイア 名前 説 スロ・ 明 号	^ッ ウォールインターフェイス ット番 ロジカルネットワーク	IPアドレス	仮想IPアド レス	Enterprîse C loud 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			-	с. С	稼働中	ファイア:ロジカルネットワークの切断
Copyright © NTT Comm	unications Corporation. All right reserved.		38			Communications Global ICT Partner Innovative. Reliable. Seamless.

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))



Copyright © NTT Communications Corporation. All right reserved.

39

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 [.]	インダ	ヲーフェ-	-Zì	自加
1. 2.	ファイア ファイア クリック	ウォール一覧から対約 ウォールインタフェ- して「ロジカルネッ	象vFWを選択 ースタブから トワークの接	て 5、対象の 5続」を選	マンタフェース 択	スの右側	」「▼」を
概要 名前 明	ファイアウォー スロット番 号	ルインターフェイス ロジカルネットワーク	IPアドレス	仮想IPアド レス	Enterprîse C loud 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 💌
dp0s5 -	2			-	-	稼働中	ロジカルネットワークの接続 ファイアウロジカルネットワークの切断
Copyright © N	IT Communicatio	ns Corporation. All right reserved.		41		NT	Communications Global ICT Partner Innovative. Reliable. Seamless.

手順④-3 vFWの設定変更 (IPSecの設定追加)



Copyright © NTT Communications Corporation. All right reserved.

42

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)



Copyright © NTT Communications Corporation. All right reserved.

44

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。

	2 77		
SOTest			
ID ws0000720854 & 22-	nurications 🔘 SOTest 📏 🥥 🖽 — E	ixxoa-	▲ リクエスト ● サポート 🗘 管理者
詳細 アクセス種の編集	入力してください		◎ 各サービスの説明書
●利用可能なサービスを見る	-9-9		
『ネットワーク』⇒『クラウド/サー/	和正道境が/開放サービス - Flexible InterConnect Global InterConnect Global InterConnect クラウド/サーバー VPN時がケードウェイ クラウド/サーバー Parkible InterConnect クラウド/サーバー Flexible InterConnect クラウド/サーバー Parkible InterConnect クラウド/サーバー ロク・ションパ株 クラウド/サーバー ロク・ションパ株 クラウド/サーバー SD-Exchange Amazon V 地域 クラウド/サーバー SD-Exchange Google Cl 勝続 クラウド/サーバー SD-Exchange Morosoft	インターネット/回達サービス - Super OCN Flexible Connect - DNS - Atamai FastDNS - Atamai Global Server Load Dalance EV-ウェイ - Distributed Secure Internet GateWay E Web Services oud Platform AzuretBRE	クラウド/サーバー ローカルネットワーク - ロジカルネットワーク - 共連編章ゲートウェイ - ロードパランサー - マネーシドロードパランサー
ネットワークセキュリティーの	クラウド/サーバー ネットワークセキュリティ	リモートアクセス	SD-WAN
Managed Firewallをクリックします。	 ファイアウォール Managed Firewall Managed UTM Managed WAF 	Plexible Remote Access	 Software-Defined Network Service

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

	Managed Firewall Managed UTM	Order	Operation
Network-based Security	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



[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。

デバイス	ログ&レポート	サービス	カスタマープロファイル	チケット管理
ワークフロー		ダッシュボ	ード ワークフロー スケジ	ューリング済みプロセス
Detection_Accuracy				
Device Config Export				
ECL_WAF_Intermediate_Co	rtificate			
ECL_WAF_Local_Certificate				
Cluster Port Management				
Cluster Route Management				
BUTM Port Management				
WAF Port Management				
Ping Execution				



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。



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。

- Device Id FW/UTM	- NCS172								
							122		
Port	Enable Port	IP Address[CIDR]	MTU Size	Network Id	Subnet Id	Port Id	Comment		
port4		1	500						
port5		1	500						
porté		1	500						
port?		1	500						
port8		1	500						
port9		1	500						
port10		1	500						
								Global ICT	Par

[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

2			
Port	port4		
Enable Port			
IP Address[CIDR]	172.16.0.25/24	-	
MTU Size	1500		
Network Id	external_segment		Port4に接続するネットワークアドレス
Subnet Id	172.16.0.0/24	-	
Port Id			
Comment			

MFW-02

キャンセル保存			
2			
Port	port4		
Enable Port		Port4に付与するIPアドレス	
IP Address[CIDR]	172.16.0.161/24		
MTU Size	1500		
Network Id	external_segment	Port4に接続するネットワークアドレス	
Subnet Id	172.16.0.0/24		
Port Id			
Comment			
			Innovative. Reliable. Seamless.
Copyright © NTT	Communications Corporation. All right reserved.	50	

[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

2		
Port	port5	
Enable Port		Port4に付与すスIPアドレス
IP Address[CIDR]	192.168.10.254/24	
MTU Size	1500	
Network Id	net_seg_a	Port4に接続するネットワークアドレス」
Subnet Id	192.168.10.0/24 🔹	
Port Id		
Comment		

MFW-02



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。

						x
4 - NC5172						
						e 22
Enable Port	IP Address[CIDR]	MTU Size	Network Ed	Subnet Id	Port Id	Comment
51	10.1.1.254/24	1500	testi	10.1.1.0/24		
		1500				
		1500				
		1500				
		1500				
		1500				
		1500				
	Enable Port	Enable Port IP Address[CIDR]	Enable Port IP Address[CIDR] MTU Size Enable Port IP Address[CIDR] MTU Size I 0.1.1.254/24 1500 I 15	Enable Port IP Address[CIDR] MTU Size Network Id IO.1.1.254/24 1500 1mt1 10.1.1.254/24 1500 1mt1 1500 1500 1500 1500 1500 1500 1500 1500 1500	Enable Port IP Address[CIDR] MTU Size Network Id Subnet Id IO.1.1.254/24 1500 text1 10.1.1.0/24 IO.1.1.254/24 1500 text1 10.1.1.0/24 IO.1.1.254/24 1500 text1 10.1.1.0/24 IO.1.1.254/24 1500 text1 10.1.1.0/24 IO.1.1.254/24 1500 text1 10.1.1.0/24	Enable Port IP Address[CIDR] MTU Size Network Id Subnet Id Port Id IO.1.1.254/24 1500 10.1.1.0/24 10.1.1.0/24 10.1.1.0/24 IO.1.1.254/24 1500 10.1.1.0/24 <td< td=""></td<>



[タスク ステータス]が表示されます。

タスクステータス				×
ステータス	用给种刻	转了時刻	詳細	
Verity IP Address, MTU Inputs	2020-08-24 05:49:23	2020-08-24 05:49:26	IP Address inputs verified successfully.	



すべてのステータスが「緑色」になれば正常終了です。

ネスクステータス				×
ステータス	關始時刻	終了時刻	3748	
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 : 08edfc958d894aa69088155cc28005bc	
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 22:38:52	2016-07-11 22:38:58	Ports created successfully. Port Id: 14177588-012-4937-a8dc-e02aeec4a055 Port Id: 09eeeb69-17bc-40bc-8ae4-330b5d55024e Port Id: 8010b923-2c79-4ed3-0003-9317477c2ab1 Port Id: 08507b3b-3a36-44a3-97b5-829fc138ad91 Port Id: 83a34462-0282-4a8a-acdr-0818c43794f Port Id: 83a34462-0282-4a8a-acdr-0818c43794f Port Id: 8404497f-8e7b-4f97-94a5-a832004a0e0e Port Id: 2a72235c-ab1f-4af0-a8a2-149bf2c28129	
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 me UTM	2016-07-11 22:37:11	2016-07-11 22:37 26	Openstack Server bb348914-cb3b-467e- b9af-0bf897co38ed started successfully. Server Status : ACTIVE Task State : - Power Stats : 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.	

Global ICT Partner Innovative. Reliable. Seamless.

Copyright © NTT Communications Corporation. All right reserved.

54

ファイアウォールのトンネル状態確認

FW01(ipsec_a)

user-ad	min@	vyatta:~\$	show vpr	n ipsec sa						
Peer ID	/ IP		Lo	ocal ID / IP						
172.16.	0.161			192.168.10.	25					
Tunn	el Sta	ate Bytes	Out/In	Encrypt	Hash ,	A-Time	L-Time	Proto		
vti	up	0.0/0.0	aes25	of shal	492	3600	al			

FW02(ipsec_b)

user-admin@vyatta:~\$ show [.]	/pn 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 504.0/588.0	aes256 sha1 439 3600 all



ファイアウォールのvtiOインタフェース状態

FW01(IPsec-a)

user-admin	@vyatta:~\$ show interf	aces	
Codes: S - 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	
dp0s5	192.168.1.254/24	u/u	
vti0	10.1.1.2/30	u/u	

FW-02(IPsec-b)

user-admir Codes: S -	@vyatta:~\$ show interfac State, L - Link, u - Up, D -	ces · Down, A - Admin Down
Interface	IP Address	S/L Description
dp0s4 dp0s5	 192.168.20.161/24 192.168.2.254/24	u/u u/u u/u
vti0	10.1.1.1/30	u/u



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 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=62 time=5.41 ms 64 bytes from 192.168.2.3: icmp_seq=2 ttl=62 time=3.19 ms 64 bytes from 192.168.2.3: icmp_seq=3 ttl=62 time=3.53 ms 64 bytes from 192.168.2.3: icmp_seq=4 ttl=62 time=3.36 ms 64 bytes from 192.168.2.3: icmp_seq=5 ttl=62 time=3.00 ms ^C --- 192.168.2.3 ping statistics ---5 packets transmitted, 5 received, 0% packet loss, time 4005ms rtt min/avg/max/mdev = 3.001/3.701/5.417/0.878 ms [test-user@ipsec-test-a ~]\$



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 (192,168,2,3,229,173).
150 Here comes the directory listing.
ftp>
ftp> put test_file
227 Entering Passive Mode (192,168,2,3,178,172). 150 Ok to send data.
ftp>
ftp> dir 227 Entering Decring Made (102,160,2,2,222,247)
150 Here comes the directory listing.
-rw-rr 1 1001 1001 19 Jul 15 13:00 test_file 226 Directory send OK.
ftp> bye 221 Goodbye.

