

ホワイトクラウド ASPIRE IPsec VPN 接続構成ガイド

ASA5515 を用いた接続構成例

ソフトバンク株式会社



注意事項

本資料内の記載は、飽くまでも情報提供のみを目的としております。 明示、黙示、または法令に基づく想定に関わらず、これらの情報について ソフトバンク株式会社はいかなる責任も負わないものとします。本資料内 に記載された社名・製品名は、各社の商標、または登録商標です。





版	更新日	更新者	更新内容
初版	2016/10/31	ソフトバンク株式会社	初版作成



目次

1. ホワイトクラウド ASPIRE の IPsec VPN 機能概要	5
1.1. IPsec VPN について	5
1.2. ホワイトクラウド ASPIRE の IPsec VPN 機能	5
2. ASA5515 とホワイトクラウド ASPIRE の接続構成概要	6
2.1. 本資料でご紹介する ASA5515 を用いた構成	6
2.2. 調理傳成	1
3. 構成手順	8
3.1. 設定前の状態について	8
3.1.1. オンプレミス側 ASA5515 の設定	
3.1.2. ホワイトクラウド ASPIRE 側の設定	9
3.2. ASA5515の VPN 設定	10
3.2.1. ファイアウォール オブジェクト設定	
3.2.2. IPsec VPN 設定	
3.2.3. IPsec VPN 設定微調整	
3.3. ホワイトクラウド ASPIRE の VPN 設定	20
3.3.1. VPN 設定	
3.3.2. ファイアウォール設定	
3.4. VPN 接続後の通信確認	
3.4.1. ホワイトクラウド ASPIRE セルフサービスポータルから確認	
3.4.2. Cisco ASDM から確認	
3.4.3. 仮想マシンから確認	
3.5. 参考資料	
3.5.1. 参考:本設定での ASA5515Config設定(抜粋)	
3.5.2. 参考:ASA5515 を用いて複数セグメント間で IPsec VPN を設定する場合	
3.5.2.1. 複数セグメント間での IPsec VPN 設定(ASA5515)	
3.5.2.2. 複数セグメント間での IPsec VPN 設定 (ホワイトクラウド ASPIRE)	
3.5.2.3. VPN 接続後の通信確認時の注意点	



1. ホワイトクラウド ASPIRE の IPsec VPN 機能概要

1.1. IPsec VPN について

IPsec (Security Architecture for Internet Protocol)は、IP 通信を暗号化することによって内容の 秘匿と改ざん防止を実現するプロトコルです。この IPsec によって、異なる場所にあるネットワークや ノードの間を、あたかも専用の回線を引いたかのように接続する技術が IPsec VPN です。 この技術によって、重要性の高いデータ通信を安全に行うことができます。



1.2. ホワイトクラウド ASPIRE の IPsec VPN 機能

データセンタやオフィスなどの拠点との間で安全な通信を行うために、ホワイトクラウド ASPIRE は IPsec VPN 機能を標準搭載しています。ホワイトクラウド ASPIRE からインターネットへの接続に 用いる Edge ゲートウェイが IPsec VPN 機能を提供します。IPsec VPN 接続機能を持つ拠点側の 機器やソフトウェア等と Edge ゲートウェイの間で IPsec VPN による通信を行うことが可能です。



5 / 38 Copyright 2016 SoftBank Corp. All Rights Reserved.

2. ASA5515 とホワイトクラウド ASPIRE の接続構成概要

2.1. 本資料でご紹介する ASA5515 を用いた構成

本資料では拠点側に ASA5515 を設置し、ホワイトクラウド ASPIRE の Edge ゲートウェイとの間を IPsec VPN で接続する設定例をご紹介します。



Cisco 製品の詳細に関しては、公式 Web サイトをご覧ください。 http://www.cisco.com/



2.2. 論理構成

オンプレミスとホワイトクラウド ASPIRE の VPN 接続対象ネットワーク間で通信できるように IPsec VPN を接続します。



次項より記載する構成手順は、上図のうち IPsec VPN 以外の部分が構成された状態を前提としております。本資料の作成にあたり使用した ASA 機器、OS バージョンは、下記となります。

< ASA5515 > 機器:ASA5515 OS Version:9.2(3)4 ASDM Version:7.4(1)



3. 構成手順

3.1. 設定前の状態について VPN 設定前のオンプレミスおよびホワイトクラウド ASPIRE それぞれの状態を示します。

3.1.1. オンプレミス側 ASA5515 の設定



<u>ASA5515</u>

- ・ACL は WAN インターフェースへの設定のみ
- ・NAT は内→外のみ設定(NAPT)
- ・デフォルト GW は WAN 側に設定
- ・インターフェースは次の3つを使用
 - Gi 0/0 (WAN) IP アドレス : X.X.X.X
 - Gi 0/1 (VPN 接続対象 NW) IP アドレス: 192.168.248.253/24
 - Manage (管理用 NW)



3.1.2. ホワイトクラウド ASPIRE 側の設定



Edge ゲートウェイ

- ・ファイアウォールはルールの設定が無いものは全通信拒否
- ・NAT は内→外のみ(NAPT)
- ・VPN 接続対象 NW はデフォルトで存在する標準テナントNWを利用する
- ・インターフェースは次の2つを使用
 - Edge ゲートウェイ (WAN) IP アドレス: Y. Y. Y. Y
 - Edge ゲートウェイ (VPN 接続対象 NW) IP アドレス : 192.168.0.254/24



3.2. ASA5515 の VPN 設定

ASA5515 の VPN 設定手順を記します。大まかなステップは次のとおりです。

- ① ファイアウォール オブジェクト設定
- ② IPsec VPN 設定
- ③ IPsec VPN 設定微調整
- ※前ページに記載された VPN 設定前の状態に至るまでの初期セットアップ手順は省略しております。 初期セットアップ手順はメーカー公開の各種ドキュメントをご参照ください。

http://www.cisco.com/web/JP/techdoc/index.html

※本資料では、Cisco ASDM を利用した設定方法を記載しております。 CLI より設定される場合は、 巻末に参考 Config を記載しておりますのでそちらをご確認ください。

本資料で IPsec VPN の設定に利用する VPN パラメータを下記に示します。

パラメータ	オンプレミス ASA5515	ホワイトクラウド ASPIRE Edgeゲートウェイ
Local Network	192.168.248.0/24	192.168.0.0/24
Remote Network	192.168.0.0/24	192.168.248.0/24
Local ID	-	Y.Y.Y.Y
Remote ID	-	X.X.X.X
Remote IP	Y.Y.Y.Y	X.X.X.X
IKE version	V1	設定変更不可
認証方式	Pre-shared Key	設定変更不可
共有キー/Pre-shared Key	VpnaccessforASPIRE1vpnaccessforASPIRE1	Vpnaccess for ASPIRE1 vpnaccess for ASPIRE1
交換モード	Main mode	設定変更不可
暗号化・Hashアルゴリズム	AES256 / SHA-1	AES256 / SHA-1
Diffie-Hellman Group	group 2 (MODP1024 bits)	設定変更不可
PFS	On	設定変更不可
IKE SA Lifetime	28800 (no kbytes rekeying)	設定変更不可
IPsec SA Lifetime	3600 (no kbytes rekeying)	設定変更不可

※備考

・IKE フェーズ 1,2 では同じアルゴリズムを使用

・オンプレミス側の NW 機器でホワイトクラウド ASPIRE の IPsec VPN 仕様に沿ったパラメータを設定する ・ホワイトクラウド ASPIRE 側は、ポリシーベース VPN のみ利用可能



3.2.1. ファイアウォール オブジェクト設定

Cisco ASDM より IPsec VPN の設定に利用するファイアウォールのオブジェクトを設定します。 本資料ではローカル側のオブジェクトはすでに設定されています。ホワイトクラウド ASPIRE の VPN 対象ネットワークを オブジェクトとして登録します。

(1). $\checkmark = = - \pounds \theta$ [Configuration] \rightarrow [Firewall] \rightarrow [Objects] \rightarrow

「Network Objects/Groups」 ヘアクセスし、「Add」 をクリックします。

3		Cisco ASDM 7.4 for ASA - 172.
<u>File View T</u> ools Wi <u>z</u> ard	s <u>W</u> indow <u>H</u> elp	
🚮 Home 🦓 Configuration	👩 Monitoring 🔲 Save 🔇	• Refresh 🔇 Back 🔘 Forward 🤗 Help
Firewall	G Configuration > F	irewall > Objects > <u>Network Objects/Groups</u>
Access Rules	🚱 Add 🚽 🌌 Edit	💼 Delete 🔍 Where Used 🔍 Not Used
Service Policy Rules	Filter	
Eilter Bules	Name	▲ ¹ IP Address Netmask
Public Servers	E-Network Objects	
📲 URL Filtering Serve	rs 👘 🌍 any	
Threat Detection	- 🧼 any4	
Identity Options	🌍 anyɓ	
Identity by TrustSec	Local_192	.168.248.0_24 192.168.248.0 255.255.255.0
Network Objects	/Groups	work 192.168.248.0 255.255.255.0
Service Objects	Groups Managem	ent-network 172.16.10.0 255.255.255.0

(2). ホワイトクラウド ASPIRE 上の VPN 対象ネットワークの情報を入力し「OK」をクリックします。

G	Add Network Object	x
Name:	CloudNW_192.168.0.0_24	
Туре:	Network	~
IP Version:	● IPv4 ○ IPv6	
IP Address:	192.168.0.0	
Netmask:	255.255.255.0	~
Description:	WhiteCloudASPIRE-NW	
NAT	OK Cancel Help	*

Name:任意(本設定では CloudNW_192.168.0.0_24)

Type:Network を選択

IP Version : IPv4 を選択

IP address: ホワイトクラウド ASPIRE の VPN 接続対象 NW のセグメントを入力 Netmask: ホワイトクラウド ASPIRE の VPN 接続対象 NW のサブネットマスクを選択 Description: 任意

11 / 38 Copyright 2016 SoftBank Corp. All Rights Reserved.



3.2.2. IPsec VPN 設定

IPsec VPN を利用する対象ネットワーク、暗号アルゴリズム等の各パラメータを設定します。 Cisco ASDM のウィザードを用いて IPsec VPN を設定します。

(1). メニューより「Wizards」 ヘアクセスし「VPN Wizards」 → 「Site-to-site VPN Wizard」
 をクリックします。

		Cisco ASDM 7.4 for ASA -
File View Tools	Wizards Window Help	
Home 🖓 Confi	Startup Wizard	Back C Forward 2 Help
	VPN Wizards	Site-to-site VPN Wizard
Bookmarks To bookmark a pag node in the naviaga select "Add to book G Go Delet	High Availability and Scalability Wizard Unified Communication Wizard ASDM Identity Certificate Wizard Packet Capture Wizard	AnyConnect VPN Wizard Clientless SSL VPN Wizard IPsec (IKEv1) Remote Access VPN Wizard

(2). 「Next」をクリックします。

6	Site-to-site VPN Connection Setup Wizard	×
VPN Wizard	Introduction Use this wizard to setup new site-to-site VPN turnel. A turnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol. Site-to-Site VPN Local Conference of the top of top of the top of	-
	< Back Next > 取消 Help	



F	<i></i>	Site-to-site VPN Connection Setup Wizard			
Steps	Peer Device Identificati	1			
1. Introduction	This step lets you ident	y the peer VPN device by its IP address and the interface used to	access the peer.		
2. Peer Device Identification	Peer IP Address:	Y.Y.Y.Y			
 Traffic to protect 					
4. Security	VPN Access Interface:	o-internet	~		
6 Summary					
o. cuminary					
	< Back Next >			取消	Help
THE PARTY OF	V DOOK			AXH	Tiep

(3). VPN 接続先の情報を入力し「Next」をクリックします。

Peer IP Address : ホワイトクラウド ASPIRE の Edge ゲートウェイのグローバル IP アドレスを入力 VPN Access Interface : ASA5515の WAN 側インターフェースを選択

(4). VPN 接続対象 NW を設定し「Next」をクリックします。

6		Site-to-site VPN Connection Setup Wizard		×
Steps	Traffic to protect			
1. Introduction	This step lets yo	identify the local network and remote network between which the traffic is to be p	protected using IPsec encryption.	
2. Peer Device Identification	Local Network:	Local 192.168.248.0 24		
 Traffic to protect Security 	Remote Network:	CloudNW_192.168.0.0_24		
5. NAT Exempt				
6. Summary				
			0.0	16
	< <u>B</u> ack <u>N</u>	xt>	取消 Help	



Local Network: オンプレミスの VPN 接続対象 NW を選択 (本設定では Local_192.168.0.0_24) Remote Network: ホワイトクラウド ASPIRE の VPN 接続対象 NW を選択 (本設定では CloudNW_192.168.0.0_24)

(5). セキュリティ(暗号化方式)を設定します。

6	Site-to-	site VPN Connection Setu	p Wizard			×
Steps	Security					
1. Introduction	This step lets you secure the selected tr	affic.				
2. Peer Device Identification	O Simple Configuration					^
3. Traffic to protect	ASA uses the pre-shared key entered	here to authenticate this device with	h the peer. ASDM will selec	t common IKE and IS	AKMP security	
4. Security	parameters for that will allow tunnel e	stablishment. It is recommended that	t this option is also selected	d when configuring th	ne remote peer.	
5. NAT Exempt						
6. Summary	Customized Configuration					
	IKE Version Zuthentication M IKE version 1 Pre-shared Key.	ethods Encryption Algorithms Pe	erfect Forward Secrecy			
	Device Certificate:	None	۹ v	Manage		
	IKE version 2	1				
	Local Pre-shared Key.					
	Local Device Certificate:	None	v 1	Manage		
	Remote Peer Pre-shared Key					
						~
	Kext >				取消 He	p

Customoized Configration : 有効

IKE version1 Pre-shared Key : 共有キーを入力

IKE version2 Pre-shared Key : 共有キーを入力

※Pre-Shared Key (共有シークレット) は、32 ~ 128 文字の範囲内の英数字で指定し少なくとも

1つの大文字、1つの小文字、および1つの数字を含んでいなければなりません。

(本設定では vpnaccessforASPIRE1 vpnaccessforASPIRE1)

※ホワイトクラウド ASPIRE では IKE version2 は利用できません。ASA5515 の Setup Wizard の仕様上、 IKE version2 の Pre-shared Key を入力しないと他の設定タブへ画面遷移ができません。



(6).「IKE version」 タブをクリックします。「IKE version2」 のチェックを外します。

٦	Site-to-site VPN Connection Setup Wizard	×
Steps	Security	
1. Introduction	This step lets you secure the selected traffic.	
2. Peer Device Identification	Simple Configuration	^
3. Traffic to protect	ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security	
4. Security	parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.	
5. NAT Exempt		
6. Summary	Customized Configuration	
	IKE Version 1 IKE version 1 IKE version 2	

(7).「Encription Algorithms」タブを選択し利用する暗号化方式が含まれていることを確認します。

E	Site-to-site VPN Connection Setup Wizard	×
Steps	Security	
Steps 1. Introduction 2. Peer Device Identification 3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	Security This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. • Customized Configuration You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you. IKE Version Authentication Methods Encryption Algorithms Perfect Forward Secrecy IKE version 1 IKE version 1 IKE Policy crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-s Manage IPsec Proposal (AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-MD5, ES) Select	
	< <u>B</u> ack Next> 取消 H	elp

本設定では下記を利用します。

IKE Policy : pre-share-aes-256-sha IPsec Proposal : ESP-AES-256-SHA



(8).「Perfect Forward Security」を設定し、「Next」をクリックします。

6	Site-to-site VPN Connection Setup Wizard	×
Steps	Security	
1. Introduction	This step lets you secure the selected traffic.	
2. Peer Device Identification	Simple Configuration	^
3. Traffic to protect	ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security	
4. Security	parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.	
5. NAT Exempt		
6. Summary	Customized Configuration	
	IKE Version Authentication Methods Encryption Algorithm Perfect Forward Secrecy	1
	Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. It ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future Diffie-Hellman Group: group2 v	
	Kext > The set → The set →	lp

Enable Perfect Foard Security : 有効 Diffie-Hellman Group : Group2

(9). NAT Exempt を設定し、「Next」 をクリックします。

5	Site-to-site VPN Connection Setup Wizard	×
Steps 1. Introduction 2. Peer Device Identification 3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	NAT Exempt This step allows you to exempt the local network addresses from network translation. Exempt ASA side host/network from address translation Local v	
	< Back Next > 取消	Help

Export ASA Side host/network from address translation : 有効 NAT から除外するホストまたはネットワークを選択(本設定では Local)

> **16 / 38** Copyright 2016 SoftBank Corp. All Rights Reserved.



(10). 設定内容を確認し「Finish」をクリックします。

VPN Wizard	Summary	
Branch	Here is the summary of the configuration.	
	Name	Value
T = ISP	E Summary	
TOTAL	Peer Device IP Address	Y.Y.Y.Y
Hom	VPN Access Interface	to-Internet
(Corporate)	Protected Traffic	Local Network: 192.168.248.0/24 Remote Network: 192.168.0.0/24
Network	IKE Version Allowed	IKE version 1 only
a str	Authentication Method	
GLAMP WAR	IKE v1	Use pre-shared key
- Star	Encryption Policy	
	Perfect Forward Secrecy (PFS)	Enabled using Diffie-Hellman Group: group2
	E IKE v1	
	IKE Policy	crack-aes-256-sha, rsa-sig-aes-256-sha, pre-share-aes-256-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-sha, crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-3des-sha, rsa-sig-3des-sha, pre-share-3des-sha, crack-des-sha, rsa-sig-des-sha, pre-share-des-sha
- 6	IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
	Network Address Translation	The protected traffic is not subjected to network address translation

3.2.3. IPsec VPN 設定微調整

(1). VPN 設定の微調整を行います。「Edit」をクリックします。

Cisco ASDM 7.4 for ASA - 172.16.10.254										
File View Tools Wizards Windo	w Help				Type topic to	search	Go	alada		
Home 🖓 Configuration 🔯 Monitoring 🔚 Save 💽 Refresh 🔇 Back 🔘 Forward 🦓 Help										
Site-to-Site VPN	Site-to-Site VPN									
Connection Profiles	Manage site-1 Access Interface Enable interfa	-to-site VPN connections. Here is a video on how to setup a site-to-site VPN connection. ces faces for IPsec access.								
Advanced	Interface	Allow I	(E v1 Access	Allow IKE v2 Access						
Tunnel Groups	Local to-Internet	Local Contraction								
KE Parameters INE Parameters IPsec Proposals (Transforn IPsec Prefragmentation Pol E Certificate to Connection F III System Options III Crypto Engine ACL Manager	Bypass int Access lists f	erface acces rom group po les	ss lists for inbound VI olicy and user policy a	² N sessions Iways apply to the traffic.						
	Connection pr to be encrypte	ofile identifi ed, and other Edit <mark>a (</mark> Dele	es the peer of a site- parameters. You can ste	to-site connection. It specifies wha configure the mapping from certific	at data traffic cate to connec	is to be encr; ction profile h	ypted, how the c ere.	lata traffic is		
	Name	Interface	Local Network	Remote Network	IKEv1 Ena	IKEv2 Ena	Group Policy	NAT Exempt		
	Y.Y.Y.Y	to-Internet	📑 Local_192.168.24	8.0_24 🛃 CloudNW_192 168.0.0_24	V		GroupPolicy	✓		



(2).「Crypto Map Entry」の「Security Association Lifetime」の設定を修正します。

Basic	Priority:	1	
Advanced	Perfect Forward Secrecy.	🔿 Disable 🔘 Enable	
Tunnel group		Diffie-Hellman Group: group2	
	NAT-T:	✓ Enable	
	Reverse Route Injection:	Enable	
	Security Association Lifetime	e	
	Time:	8 : 0 : 0 hh:n	nmiss
	Traffic Volume:	✓ unlimited KBy	tes



Traffic Volume : unlimited

(3).「Tunnel group」の「IKE Keepalives」の設定を修正します。「Disable keepalives」を選択し、「OK」をクリックします。

Advanced Crvnto Man Entry	Certificate Settings Send Certificate Chain: Enable IKE Peer ID Validation: Required IKE Keepalive O Disable keepalives O Monitor keepalives Confidence Interval: seconds Retry Interval: seconds O Headend will never initiate keepalive monitoring	>
Find:	Next Previous OK Cancel Help	



(4).「Site-to-Site VPN」の「IKE Paramater」の設定を修正します。

メニューより「Configuration」→「Site-to-Site VPN」→「Advanced」→「IKE Paramater」へ アクセスします。「Identity Sent to Peer」の「Identity:」を「Automatic」もしくは「Address」 へ変更します。

5	Cisco ASDM 7.4 for ASA - 172.16.10.25
File View Tools Wizards Windo	ow Help
💣 Home 🦓 Configuration 🔯 Monit	toring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦓 Help
ू Site-to-Site VPN 🗗 म	<u>Configuration > Site-to-Site VPN > Advanced</u> > <u>IKE Parameters</u>
Connection Profiles Group Policies Certificate Management Identity Certificates CA Certificates Advanced Tunnel Groups KE Policies KE Parameters	NAT Transparency Enable IPsec over NAT-T (must be enabled for AnyConnect IPsec conr NAT Keepalive: 20 Seconds Enable IPsec over TCP (IKEv1 only) Enter up to 10 comma-separated TCP port(
IPsec Proposals (Transform IPsec Prefragmentation Pol Income Connection File	Identity: Automat V Key Id String:

(5).「System Options」の「IPsec Security Association Lifetime」を修正し「Apply」を クリックします。

Cisco ASDM 7.4 for ASA - 172.16.10.254								
File View Tools Wizards Windo	w Help Type topic to search Go	ahaha						
🚳 Home 🦓 Configuration 🔯 Monit	toring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦓 Help	CISCO						
Site-to-Site VPN 리 무	Configuration > Site-to-Site VPN > Advanced > System Options							
Connection Profiles Group Policies Certificate Management CA Certificates CA CA C	Limit the maximum number of active IPsec VPN sessions. This limit affect calculated load percentage for VPN Load Balancing. Maximum IPsec Sessions: Reclassify existing flows when VPN tunnels establish Preserve stateful VPN flows when the tunnel drops IPsec Security Association Lifetime	ts the						
Certificate to Connection Prof System Options	Time: 1: 0: 0 hhommess							
ACL Manager								
	ESP v3 Enable PMTU (Path Maximum Transmission Unit) Aging							
» •	Apply Reset							

19 / 38 Copyright 2016 SoftBank Corp. All Rights Reserved.



Time : 1:00:00 Traffic Volume : unlimited

3.3. ホワイトクラウド ASPIRE の VPN 設定 ホワイトクラウド ASPIRE とオンプレミスの ASA5515 を IPsec VPN で接続する設定を行います。

3.3.1. VPN 設定

(1). Web ブラウザからホワイトクラウド ASPIRE のセルフサービスポータルへアクセスし、 ユーザ名とパスワードを入力してログインします。

ASPIRE セルフポータルサイト	
ユーザ名: パスワード: ロヴイン	
SoftBank	

(2). 2段階認証に設定したパターンの場所の数字を入力し、ログインをクリックします。

											Ē	S	oft	Ba	nk
			AS	PÍR	ÈE -	セル	フポー	-タル	サイ	Þ					
	ಕのマ.	2段階 ス目に3	認証に該 表示され	定され ている	たパタ 数字を)	ーンにう 入力して	合った場 て「ログ	所と順 イン」し	番で、 してくた	ざさい。					
5	0	8	6	1	5	5	2	0	3	7	2				
1	3	3	7	0	4	8	3	8	9	1	0				
9	2	3	9	6	6	4	7	7	5	6	6				
2	5	4	1	9	1	2	7	8	0	4	4				
パスワード:															
				=	So	ftBa	ank								

(3). テナント設定をクリックします。

SoftBank		A	ASPÍRE	セルフボータ	test-admin1(ユーザ管理者(契約番 〇 環境設定 サポート				
ダッシュボード	仮想マシングループ	仮想マシン	カタログ	ネットワーク	D Ø	¥-ב	テナント設定]	
「「「「」」「「」」「「」」「「」」「「」」「「」」「「」」「「」」「」」「」	<- ド 服に更新	ダッシュホート VC01_C リソース CPU	temmitted_01 使用量 6 0 GHz/10 (-APU1608194			ルIPアドレス 契	約数 2回	

(4). 左側のメニューより「Edge ゲートウェイ」をクリックします。表示された Edge ゲートウェイ名 (本資料では APUXXXXXX-EdgeGW01)を右クリックし、「サービス設定」をクリックします。

Soft	Bank
------	------

Soft	Bank		ASPIRE	セルフポータ	test-admin1(ユーザ管理者(契約者 <mark>〇</mark> 環境設定 サポート				
ダッシュポード	仮想マシングループ	仮想マシン	カタログ	ネットワーク	D7	ユーザ	テナント設定		
■ 契約リソー。 リソース 最新の情	ス 使用量の表示 i報に更新	Edgeゲートウ	II						
▼ Edgeグート	·ウェイ	୯ ॥ ଦ	All Fields	Search					
最新の信	報に更新	名前		ステータス	使用済みNIC数	外部ネットワ	ーク数 テナントネ	ットワーク数 Ed	geゲートウェイサ
▶設定		APUXXXXXXX -E	dgeGW01 サービス級 ネットワー サービス網 両デプロイ プロパティ	足 りきし ク/標成 成の再利用		1	5	S	

(5). 左側のメニューより「VPN」をクリックします。「VPN を有効化」のチェックボックスを 有効化し、「追加」をクリックします。

サービスの構成 NAT ファイアウォール 固定ルーティング VPN	IPSec VPNid、ペ オンプレミスとら ※IPSec VPNid、 VPNを有刻 公開IPの構 (公開IPの構)	ゲートワエイ間でセキュアな D間、このテナント内、テナ 両サイトでの接続構成没定: 効化 改 変れの外部ネットワークにつ!	VPNトンネル設定ができ: ント間に対して、サイト が必要となります。 ハて構成できます。これ1	ます。 ソーサイト [、] は、NATを	VPNを構成で 使用している	きます。 3環境において便利です。		
	名前	ローカルエンド	ピアエンドポイント	有効	ステ	ローカルネットワ	ピアネットワーク	ピアテナント
	追加	集前除					OK	++>t

(6). VPN パラメータを入力し、「OK」をクリックします。

SoftBank

VPNの構成の追加		X
VPNの構成の追加	名前 *	IPSEC-ASA5515
	U-7-J	
	有効化	回有効化
	VPNの確立先	リモートネットワーク
	ローカルネットワーク	
	ピアネットワーク *	192.168.248.0/24
VPNの構成の追加	ローカルエンドポイント	SharedExternal01 V公開IPを使用
	ローカルID *	Y.Y.Y.Y
	ピアID *	X.X.X.X ビアを一高に藻別する ID. ビア アドレスがこの、または別のテナントネットワーク上にある場合は、これがビアのネイティ ブ IP アドレスである必要があります。ビアが NAT'd の場合は、これがプライベート ビア IP アドレスである必要がありま す。
	ピアIP *	: X.X.X.X ビアにアクセスする IP アドレス、ビアが NAT'd の場合は、これが NAT の公開側である必要があります。
	暗号化プロトコル	AES-256 ~
	共有キー	VpnaccessforASPIRE1vpnaccessforASPIRE1 共有シークレットは、32~128 文字の範囲内の英物字で指定し、少なくとち 1 つの大文子、1 つの小文子、および 1 つの 教字を含んていなければなりません。 図 キーを表示
	MTU *	1500 ~
		OK キャンセル

名前:任意(本設定では IPSEC-ASA5515)

説明:任意

有効化 : チェックボックス をオン

VPN の確立先: リモート ネットワーク を選択

ローカルネットワーク: ホワイトクラウド ASPIRE の VPN 接続対象 NW を選択

(本設定では APUXXXXXX-SFNW01)

ピアネットワーク: オンプレミスの VPN 接続対象 NW を指定(本設定では 192.168.248.0/24)

ローカルエンドポイント: Edge ゲートウェイが接続している共有インターネット接続ネットワーク名を選択

(本設定では SharedExternal01)

ローカル ID: ホワイトクラウド ASPIRE のグローバル IP アドレス

ピア ID: オンプレミスの ASA5515 のグローバル IP アドレス (本設定では X.X.X.X)

23 / 38

Copyright 2016 SoftBank Corp. All Rights Reserved.



ピア IP: オンプレミスの ASA5515 のグローバル IP アドレス (本設定では X.X.X.X)

暗号化プロトコル: AES-256

共有キー: 3.2.2. の(5).で設定した事前共有キーを指定

(本設定では vpnaccessforASPIRE1 vpnaccessforASPIRE1)

キーの表示 : 無効を推奨(共有キーの内容確認のため一時的に ON にする場合以外は OFF を推奨) MTU: 1500

(7). VPN 設定が完了しました。しかし、この時点ではまだ VPN 設定は Edge ゲートウェイに 反映されていません。引き続きファイアウォールを設定します。

ОНСР ЧАТ	(PSec VPNは、ゲートウ: オンプレミスとの間、この ※(PSec VPNは、両サイ	ェイ関でゼキュアなVPNトン。 りテナント内、テナント関にす ドでの授続債成設定が必要とな	約1.股圧ができます。 すして、サイトツーサイ ごります。	·トVPN 순제	極できます.			
ファイアワォール 固定ルーティング	✓ VPNを有効化 公開IPの構成							
ファイアワォール J定ルーティング	✓ VPNを有効化 公開IPの構成 公開IPは、それぞれの外8	₽キットワークについて積成T	réat, chia. NAI	を使用し	cいる環境におい)て便利です。		
7アイアワォール J定ルーティング PN	✓ VPNを有効化 公開IPの構成 公開IPは、それぞれの外後 名前	^{8ネットワークについて構成1} ローカルエンドポイント	rきます。これは、NAT ピアエンドポイ	⁻ ⁻ を使用し 有効	c いる環境におい ステータス	いて便利です。 ローカルネット	ビアネットワーク	ピアテロ

3.3.2. ファイアウォール設定

(1). オンプレミスとホワイトクラウド ASPIRE の VPN 対象 NW 間の通信を許可するファイアウォール 設定を追加します。「ファイアウォール」より「追加」をクリックします。

₽ 「 マイアワォール コルーティング	ファイアウ とができま ビファ・ デフォル	ォールにより、宿) す。 イアウォールを ・トアクション(€のネットワーク トラフ・ 有効化 ● 拒否 ○許可	(ックを許可または拒否する	5ようルール設定できます。	、これらのルールの順序1;	4. ルール内の順爵で変更する
 ・ドバランサー	唐番	▲ 名前	<u>у-</u> д	ターゲット	ブロトコル	アクション	有効
	追加	編集 削	9 %				

(2).ポップアップしたウィザード内へオンプレミスからホワイトクラウド ASPIRE への通信(Inbound)を 許可するパラメータを入力し、「OK」ボタンをクリックします。

SoftBank

ファイアウォールルールの	追加		X
77-77-14-14-05运加	有効	□有効化	^
3	名前 *	IPSEC-IN	
6	順番 *	1 1~999の間で入力お開いいたします。	
	ソース *	192.168.248.0/24 自然に解決、IP アドレス、CIDR、IP 新用、「anvi」、「internal」 および fexternal」 です。	- 1
	ソースポート	任意 💟 any	- 1
	ターグット *	192.168.0.0/24 有効な優は、IPアドレス、CIDR、IP範囲、「any」、「internal」 および fexternal」です。	
	ターゲットポート	任意 💟 any	~
	プロトコル *	任意	
	アクション	●許可 ○拒否	~
		ОК	キャンセル

有効 :チェックボックスをオン

名前 : 任意(本設定では IPSEC-IN)

順番:任意(重複しない番号を割り当て)

ソース:オンプレミスの VPN 接続対象 NW を指定(本設定では、192.168.248.0/24)

ソースポート:任意(本設定では、ANY)

ターゲット: ホワイトクラウド ASPIRE の VPN 接続対象 NW を指定(本設定では、192.168.0.0/24) ターゲットポート: 任意(本設定では、ANY)

プロトコル :任意

アクション :許可

(3). 続いて、反対方向の通信のファイアウォール設定を追加します。「追加」をクリックします。

ヽ ヽ アイアワオール	ファイア・ とがてき: 「ファ	フォールにより、 得定 ます。 イアウォールを有 	のチットワーク トラフィックを許可 動化	または拒否するようルール設定	test. Ch	5のルールの順序は.	ルール内の順適で変更する
モルーティング N	テノオ)	レトアクション ● 名前	ッ拒否 ○ 許可 ソース	ターゲット	プロトコル	アクション	有効
ードバランサー	1	IPSEC-IN	192.168.248.0/24:any	192.168.0.0/24:any	任意	許可	1

25 / 38 Copyright 2016 SoftBank Corp. All Rights Reserved.

SoftBank

(4). ポップアップしたウィザード内にホワイトクラウド ASPIRE からオンプレミスへの通信 (Outbound)を許可するパラメータを入力し、「OK」ボタンをクリックします。

ファイアウォールルール	しの追加		X
77-7714-14-1405追加	有効	☑ 有効化	^
	名前 *	IPSEC-OUT	
	顺番 *	2 1~999の間で入力お預いいたします。	
	ソース *	192.168.0.0/24 有効な販売は、IP アドレス、CIDR、IP 範囲、「anv」、「internal」および「external」です。	
	ソースポート	任意 💟 any	_
	ターグット *	192.168.248.0/24 有効な優は、IP アドレス、CIDR、IP 範囲、「any」、「internal」 および fexternal」 です。	
	ターグットポート	任意 💟 any	v
	プロトコル *	任意	
	アクション	●許可 ○拒否	~
		OK	キャンセル

有効 :チェックボックスをオン

名前 : 任意 (本設定では IPSEC-OUT)

順番:任意(重複しない番号を割り当て)

ソース: ホワイトクラウド ASPIRE の VPN 接続対象 NW を指定(本設定では、192.168.0.0/24) ソースポート: 任意(本設定では、ANY)

ターゲット: オンプレミス側 VPN 接続対象 NW を指定(本設定では、192.168.248.0/24) ターゲットポート:任意(本設定では、ANY)

プロトコル : 任意

アクション :許可

(5). VPN 設定とファイアウォール設定をホワイトクラウド ASPIRE へ反映させる為、「OK」を クリックします。

HCP AT マイアワォール コエルーティング	ファイア とができ ☑ ファ デフォ	ウォールにより、 得足 ます。 > イアウォールを有 ルトアクション ④	のキットワーク トラフィックを許 9効化 0 拒否 〇 許可	可または絶否するようルール役を	ರ್ಶಕ್ರ ದಗಿಂ	カルールの城序は、ルー	-ル内の順爵で変更するこ
PN	順番	▲ 名前	ソース	ターゲット	プロトコル	アクション	有効
ードバランサー	1	IPSEC-IN	192.168.248.0/24:any	192.168.0.0/24:any	任意	許可	~
	2	IPSEC-OUT	192.168.0.0/24:any	192.168.248.0/24:any	任意	許可	1
	4						
	ì£ hO	編集 削防	A.				

(6).完了するまで待機します。変更は数秒で完了します。

サービスの構成 DHCP NAT ファイアワオール	ファイア・ とかできま 2ファ デフォル	フォールにより 得走 たす。 イアウォールを有 ノトアクション ④	のネットワーラ トラフィック&st - - 渤化 - 0 将可	可または姿否するようルール投産	ರಶಕ್ರ ದಗಳು	75ルールスの解除は、ルー	北内の樹脂で変更するこ
固定ルーティンク VPN	順番	- 名前		ターゲット	プロトコル	アクション	有効
n-k/(52#-	1	IPSEC-IN	192.168.248.0/24:any	192.168.0.0/24:any	任意	許可	
19	2	IPSEC-OUT	192.168.0.0/24:any	192.168.248.0/24:any	任意	許可	
	《 注意为口						>
						ОК	キャンセル



(7).設定が完了しました。

Soft	Bank		ASPIRE	セルフポータ	ータルサイト fest-a			admin1(ユーザ管理者(契約番号 🜔 環境設定 サポート		
ダッシュボード	仮想マシングループ	仮想マシン	カタログ	ネットワーク	ログ	ユーザ	テナント設定			
■ 契約リソー リソース 最新の個	ス (使用量の表示 i報に更新	Edgeゲートウ	エイ							
▼Edgeゲート 最新の間	-ウエイ 報に更新	C III Q 名前	All Fields	Search マステータス	使用済みNI	C数 外部ネット	ワーク数 テナント	ネットワーク数 Edgeゲートウェイサイズ		
▶設定		APU1608194-E	dgeGW01	~	6	1	5	s		

3.4. VPN 接続後の通信確認

オンプレミスとホワイトクラウド ASPIRE の VPN 接続対象 NW の間で通信が行えることを 確認します。

3.4.1. ホワイトクラウド ASPIRE セルフサービスポータルから確認

ホワイトクラウド ASPIRE のセルフサービスポータルより「Edge ゲートウェイ」 ヘアクセスします。 「サービス設定」より「VPN」を表示し、以下のように「ステータス」に緑色のチェックが 表示されていれば、VPN 接続は正常に確立されています。

サービスの構成)	
DHCP NAT ファイアワォール 固定ルーティング	[PSec VPNは、ゲートウェイ間でゼキュアなVPNトンネル設定ができます。 オンプレミスとの間、このテナント内、テナント間に対して、サイトツーサイトVPNを標成できます。 ※[PSec VPNは、面サイドでの授祝機成設定が必要となります。 ☑ VPNを有効化 公開IPの構成								
VPN	名前	ローカルエンドポイント	ピアエンドポイ	有効	ステータス	ローカルネット	ピアネットワーク	ピアテラ	
ロードバランサー	IPSEC-ASA5515	Y.Y.Y.Y	X.X.X.X	~	~	192.168.0.0/24	192.168.248.0/24	-	

以下のように、「ステータス」表示に異常を示す赤色のマークが表示されている場合は、ASA5515、 もしくはホワイトクラウド ASPIRE の VPN 設定に誤りがないかを確認して下さい。(※1) VPN 確立先のアドレスや VPN 接続対象 NW、暗号化設定(事前共有キーやアルゴリズムの選択)に 誤りがある場合、VPN 接続が正常に確立できません。

VPN	名前	ローカルエンドポイント	ピアエンドボイ	有効	ステータス	ローカルネット	ピアネットワーク	ピアテロ
ロードバランサー	IPSEC-ASA5515	Y.Y.Y.Y	X.X.X.X	~	0	192.168.0.0/24	192.168.248.0/24	-

※1 : VPN 接続が正常に確立されるまで多少時間が必要な場合があります。



3.4.2. Cisco ASDM から確認

「Monitoring」より「VPN Statistics」を展開し、「Sessions」をクリックします。 以下のように表示されていれば、VPN 接続は正常に確立されています。

	(Cisco ASDM 7.4	for ASA -	172.16.10.2	254	_	
File	e View Tools Wizards Window	v Help	Refresh	Type topic to Back	search	Go	
List		Monitoring > VPN	> VPN Sta	tistics > Sessi	ons		
VPN Statistics VPN Cluster Loads VPN Cluster Loads Crypto Statistics Global IKE/IPsec Statistics Protocol Statistics		Type Site-to-Site VPN IKEv1 IPsec	Active 1 1	Cumulative	Peak Concurrent 5 5	Inactive 1 1	
	ULAN Mapping Sessions Clientless SSL VPN VPN Connection Graphs WSA Sessions	Filter By. IPsec S Connection Profile IP Address	ite-to-Site Protocol Encryptior	Login Durat	All Sessions Time ion		Details
		Y.Y.Y.Y Y.Y.Y.Y	IKEv1 IPse IKEv1 (1)A	c 18:57:35 iES256 1. Oh:16m	5 JST Tue Oct 25 201 53s	6	Logout

3.4.3. 仮想マシンから確認

オンプレミス、ホワイトクラウド ASPIRE 双方の VPN 接続対象 NW 上の仮想マシンから ping やリモートアクセスなどを実行し、双方間での疎通確認を行います。

(オンプレミス側からの確認例)

下記はオンプレミスの VPN 接続対象 NW 上の仮想マシン(Windows)から ping を実行した確認例です。

IP Address: 192,168,248,200	Y
	×
Logon Domain: 🕢 管理者: Windows PowerShell 🗕 🗖	~
Logon Server: PS_C:VilcoroVAdministrator> ping 192, 162, 0, 150	
MAC Address:	Ê
Machine Doma 192,168.0.150 に ping を送信しています 32 バイトのデータ	: 🗖
Memory: 192.168.0.150 からの応答: バイト数 =32 時間 =6ms TTL=63	
Network Card: 192.168.0.150 からの応答: バイト数 =32 時間 =6ms TTL=63	
Network Speec 192.168.0.150 からの応答: バイト数 =32 時間 =5ms TTL=63	
Network Type: 192.168.0.150 からの応答: バイト数 =32 時間 =5ms TTL=63	
OS Version:	
Service Pack: 192.168.0.150 の ping 統計:	
Snapshot Time $ / / ケット数: 送信 = 4、文信 = 4、損失 = 0 (0% の損失) の 期 知 知 知 知 知 知 知 知 知 知 知 知 知 知 知 知 知 知 $	5
Subnet Mask:	
System Type: PS C-YllsersYddministrator	
User Name:	~
Volumes: < III	>

29 / **38** Copyright 2016 SoftBank Corp. All Rights Reserved.



(ホワイトクラウド ASPIRE 側からの確認例)

ホワイトクラウド ASPIRE のセルフポータルサイトから「仮想マシン」をタブをクリックし、 対象の仮想マシンを右クリックして「コンソールを開く」をクリックします。

	ASPIRE	セルフボータ	ル サイト		test-ac	dmin1(ユーザ管理者) 環境設定 サボ
仮想マシン	カタログ	ネットワーク	D 7	ユーザ	テナント設定	

仮想マシン

e III (🗨 All Field	ls	Se.	arch					
ステータス	メディア	名前	CPU	メモリ	os		ネットワーク	IPアドレス	仮想マシングループ 🔺
のパワーオン	0	testvm	1vCPU	1GB	CentOS 4/5/6/7 (6	64-bit)	NIC#0 : APU	192.168.0.150	test-group1
🙂 パワーオン	0	Win2012	コンワール	を聞く		Serv	NIC#O : aspi	172.24.0.200	test01
			パワーオン 05のシヤ*	。 ットダウン					
			パワーオフ	ļ					

ポップアウトしたコンソール内をクリックし、必要に応じてログイン操作等を行います。コンソール よりオンプレミスの仮想マシンへ通信ができることを確認します。

下記は Linux から ping を実行した確認例です。

testvm (32c36c4123b04d9dbd09d9fab9691368)	Toggle RelativePad	switch Japanes
[root@localhost ~]# ping -c 4 192.168	.248.200	
PING 192.168.248.200 (192.168.248.200) 56(84) bytes	of data.
64 bytes from 192.168.248.200: icmp_s	eq=1 ttl=127 ti	ime=5.95 ms
64 bytes from 192.168.248.200: icmp_s	eq=2 ttl=127 ti	me=5.67 ms
64 bytes from 192.168.248.200: icmp_s	eq=3 ttl=127 ti	me=5.86 ms
64 bytes from 192.168.248.200: icmp_s	eq=4 ttl=127 ti	me=6.03 ms
192.168.248.200 ping statistics - 4 packets transmitted, 4 received, 0% rtt min/avg/max/mdev = 5.677/5.882/6. [root@localhost ~]#	 packet loss, t 032/0.142 ms	ime 3010ms;

ホワイトクラウド ASPIRE への IPsec VPN 接続手順は以上です。

30 / 38 Copyright 2016 SoftBank Corp. All Rights Reserved.



3.5. 参考資料

```
3.5.1. 参考:本設定での ASA5515Config設定(抜粋)
```

```
ASA5515, 8192 MB RAM, CPU Clarkdale 3058 MHz, 1 CPU (4 cores)
: Hardware:
ASA Version 9.2 (3) 4
!
interface GigabitEthernet0/0
nameif to-Internet
security-level 0
ip address X.X.X.X 255.255.255.248
ļ
interface GigabitEthernet0/1
nameif Local
security-level 99
ip address 192.168.248.253 255.255.255.0
!
interface Management0/0
management-only
nameif Management
security-level 100
ip address 172.16.10.254 255.255.255.0
!
object network Local_192.168.248.0_24
subnet 192.168.248.0 255.255.255.0
object network CloudNW_192.168.0.0_24
subnet 192.168.0.0 255.255.255.0
description WhiteCloudASPIRE-NW
access-list Local_access_in_1 extended permit ip object Local_192.168.248.0_24 any
access-list to-Internet_cryptomap_1 extended permit ip object Local_192.168.248.0_24 object
CloudNW_192.168.0.0_24
!
nat (Local,to-Internet) source static Local_192.168.248.0_24 Local_192.168.248.0_24 destination static
CloudNW_192.168.0.0_24 CloudNW_192.168.0.0_24 no-proxy-arp route-lookup
!
object network Local_192.168.248.0_24
nat (any,to-Internet) dynamic interface
```



! route to-Internet 0.0.0.0 0.0.0.0 X.X.X.1 1 ļ ## 本設定に利用しない暗号化方式は記載していません crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac crypto ipsec security-association lifetime seconds 3600 crypto ipsec security-association lifetime kilobytes unlimited crypto ipsec security-association pmtu-aging infinite crypto map to-Internet_map 1 match address to-Internet_cryptomap_1 crypto map to-Internet_map 1 set pfs crypto map to-Internet_map 1 set peer Y.Y.Y.Y crypto map to-Internet_map 1 set ikev1 transform-set ESP-AES-256-SHA crypto map to-Internet_map 1 set security-association lifetime seconds 28800 crypto map to-Internet_map 1 set security-association lifetime kilobytes unlimited crypto map to-Internet_map interface to-Internet crypto ca trustpool policy crypto ikev1 enable to-Internet crypto ikev1 policy 30

authentication pre-share

encryption aes-256

hash sha

group 2

lifetime 86400

group-policy GroupPolicy_Y.Y.Y.Y internal

group-policy GroupPolicy_Y.Y.Y.Y attributes

vpn-tunnel-protocol ikev1

tunnel-group Y.Y.Y.Y type ipsec-121

tunnel-group Y.Y.Y.Y general-attributes

default-group-policy GroupPolicy_Y.Y.Y.Y

tunnel-group Y.Y.Y ipsec-attributes

ikev1 pre-shared-key <Pre-Shared Key>

isakmp keepalive disable

ikev2 remote-authentication pre-shared-key <Pre-Shared Key>

ikev2 local-authentication pre-shared-key <Pre-Shared Key>

!



3.5.2. 参考: ASA5515 を用いて複数セグメント間で IPsec VPN を設定する場合

下記のように複数のネットワーク間で IPsec VPN を設定することもできます。 参考としてホワイトクラウド ASPIRE 側の3つのネットワークとオンプレミス側の3つのネットワーク間で IPsec VPN を構築する例を記載します。

·論理構成図



・ネットワーク図





3.5.2.1. 複数セグメント間での IPsec VPN 設定 (ASA5515)

Cisco ASDM より複数セグメント間での IPsec VPN を設定する場合の異なる設定箇所を記載します。

・ファイアウォール オブジェクト設定

VPN 接続対象 NW を全て登録します。

- 🛃 CloudNW_192.168.0.0_24	192.168.0.0	255.255.255.0	WhiteCloudASPIRE-NW	
GloudNW_192.168.1.0_24	192.168.1.0	255.255.255.0		
CloudNW_192.168.2.0_24	192.168.2.0	255.255.255.0		
📲 Local_192.168.248.0_24	192.168.248.0	255.255.255.0		to-Internet (P)
	192.168.249.0	255.255.255.0		to-Internet (P)
- 🛃 Local_192.168.250.0_24	192.168.250.0	255.255.255.0		to-Internet (P)



・VPN 設定

(1). VPN ウィザードの 3STEP 目の「Traffic to protect」で VPN 接続対象 NW を全て設定し、 「Next」 をクリックします。

Stens	Traffic to protect	
1. Introduction	This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.	
 Peer Device Identification Tratificate evolution 	Local Network: Local_192.168.248.0_24, Local_192.168.249.0_24, Local_192.168.250.0_24	
4. Security	Remote Network: CloudNW_192.168.0.0_24, CloudNW_192.168.1.0_24, CloudNW_192.168.2.0_24	

(2). 設定確認画面にて VPN 接続対象 NW が全て含まれていることを確認します。

6	Site-to-site V	/PN Connection Setup Wizard
VPN Wizard Branch	Summary Here is the summary of the configuration.	
	Name	Value
ST IN	Summary Peer Device IP Address VPN Access Interface	to-Internet
(Corporate)	Protected Traffic	Local Network: 192.168.248.0/24, 192.168.249.0/24, 192.168.250.0/24 Remote Network: 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24
Network	IKE Version Allowed	IKE version 1 only

(3). VPN 設定の微調整を実施していない場合は同様に実施します。

			Cisco ASDM 7.4	for ASA - 172.1	5.10.254			_ _ X
<u>F</u> ile	<u>View Tools Wizards Windo</u> Home Configuration Monite	w <u>H</u> elp pring 🔲 Save 🌘	🔁 Refresh 🚺 Back 🌔	Forward 7 Hel] >	ype topic to search	G	° ululu cisco
	Site-to-Site VPN 🗗 무	Configuration	> Site-to-Site VPN > Co	onnection Profiles				
Bookmarks	Connection Profiles	Manage site-1 Access Interface Enable interfac	to-site VPN connections. Her is ces for IPsec access.	re is a video on how to) setup a site-to-s	ite VPN connection	2	e
		Interface	Allow IKE v1 Access	Allow IKE v2 Ac	cess			
		Local						
		Bypass int Access lists fi Connection Profi Connection pr to be encrypte to be accypte Add for Name	erface access lists for inbou rom eroup policy and user po les ofile identifies the peer of a ad, and other parameters. You Edit Delete	nd VPN sessions licy always apply to th site-to-site connectio a can configure the ma Remote Network	e traffic. n. It specifies what pping from certific	i data traffic is to b ate to connection pr	e encrypted, how ti rofile here.	ne data traffic is
			LUCAL NetWork	CloudNW 192.18	INEVI ENADIED	INEV2 ENADIED	Group Policy 21	NMI EXEMPT
		to-	Internet Cocal_192.168	CloudNW_192.161	2			



3.5.2.2. 複数セグメント間での IPsec VPN 設定 (ホワイトクラウド ASPIRE)

ホワイトクラウド ASPIRE のセルフポータルサイトより複数セグメント間での IPsec VPN を設定する 場合の異なる設定箇所を記載します。

・VPN 設定

(1). VPN の構成の追加時に設定する VPN を全て選択します。

V P Nの構成の追加			X
V P N の構成の追加	名前 * 説明	IPSEC-ASA5515	^
	有効化 VPNの <u>確立</u> 先		1
	ローカルネットワーク	aspire-demo-nw1 aspire-demo-nw2 IPSEC-nw2 IPSEC-nw1 APUXXXXXXSSFNW01	
	ピアネットワーク *	192.168.248.0/24,192.168.;	~

ローカルネットワーク : Ctrl キーを押しながら、設定したいテナントネットワーク名を選択 ピアネットワーク : 設定するネットワークを ","(カンマ)で区切ります。

(2). 設定した対象 NW を下記のように確認できます。

サービスの構成			
DHCP NAT ファイアワォール 固正ルーティング	[PSec VPNIは、ゲートウ オンプレミスとの間、こc ※[PSec VPNIは、両サイ ✓ VPNを有効化 公開IPの構成 公開IPは、それぞれの外径	ェイ関でゼキュアなVPNトンネル設定ができます。 のテナント内、テナント間に対して、サイトツーサイトVPNを構成できま。 ドでの投設構成設定が必要となります。 卵ネットワークについて構成できます。これは、NAT 会使用している環境	す。 において便利です。
VPN	名前	ロトピュ有乳スミローカルネットワーク	ピアネットワーク
ロードバランサー	IPSEC-ASA5515	21 12 🗸 🚫 192.168.2.0/24,192.168.1.0/24,192	192.168.248.0/24,192.168.249.0/24,192.168.



・ファイアウォール設定

(1). 通信させたいすべてのトラフィックルールをファイアウォールに設定します。

サービスの構成							D		
DHCP NAT ファイアワオール 肉素ルーティング	ファイアウォールにより、 将足のネットワーク トラフィックを許可または拒否するようルール設足できます。これらのルールの順序は、ルール内の順要で変更するこ とができます。 「ファイアウォールを有効化 デフォルトアクション ④ 拒否 〇 許可								
VPN	順番	≜ 名前	ソース	ターゲット	プロトコル	アクション	有効		
ロードバランサー	1	IPSEC-IN	192.168.248.0/22:any	192.168.0.0/22:any	任意	許可	1		
10	2	IPSEC-OUT	192.168.0.0/22:any	192.168.248.0/22:any	任意	許可	1		

本資料の構成ですべてのトラフィックルールを VPN 対象 NW 毎に設定すると、 最低でも 3 × 3 × 2 (ln/Out) = 18 本のルール設定が必要です。 ネットワークをサマライズすることで設定本数を減らすことができます。

3.5.2.3. VPN 接続後の通信確認時の注意点

稀に ASPIRE 上のステータスが有効となっていても双方での IPsec VPN のネゴシエーションの 一部が失敗し、その一部のルールの通信が不可となるケースがあります。 その場合は、オンプレミスのネットワーク機器で IPsec VPN の SA を削除してください。

サービスの構成								
DHCP NAT ファイアワォール 固定ルーティング	IPSec VPNは、ゲートウェイ間でゼキュアなVPNトンネル設定ができます。 オンプレミスとの間、このテナント内、テナント間に対して、サイトツーサイトVPNを構成できます。 ※IPSec VPNは、面サイドでの接続機能設定が必要となります。 ✓ VPNを有効化 公開IPの構成 公開IPの構成							
VPN	名前	ローカルエンドポイント	ピアエンドポイ	有効	ステータス	ローカルネット	ピアネットワーク	ピアテラ
ロードバランサー	IPSEC-ASA5515	Y.Y.Y.Y	X.X.X.X	1	1	192.168.0.0/24	192.168.248.0/24	-

ASA5515 の場合は Cisco ASDM より「Monitoring」、「VPN Statistics」、「Sessions」より 「Logout」をクリックすることで SA を削除できます。

Cisco ASDM 7.4 for ASA - 172.16.10.254									
File	e View Tools Wizards Window) Home 鑬 Configuration 🝺 Monito	v Help ring 🔲 Save 🔇 F	efresh 🔇 Back	Torward ? Help	ype topic to search	Go	cisco		
e List	VPN 37 P	Monitoring > VPN > VPN Statistics > Sessions							
Devic	Sessions VPN Cluster Loads Crypto Statistics Gompression Statistics Gompression Statistics Global IKE/IPsec Statistics Votocol Statistics Voto Nanning Sessions	Type Site-to-Site VPN IKEv1 IPsec	Active	Cumulative 1 10 1 10	Peak Concurrent	Inactive 1 1			
	Clientless SSL VPN	Filter By IPsec Site	ilter						
	Sessions	Connection Profile IP Address	Protocol Encryption	ogin Time Bytes T Duration Bytes P			Details		
		Y.Y.Y.Y Y.Y.Y.Y	IKEv1 IPsec IKEv1: (1)AES256	20:20:58 JST Tue Oct 25 2016 1.0h:01m:40s	6 402006 398106				

37 / 38 Copyright 2016 SoftBank Corp. All Rights Reserved.



以上