

# GlobalProtect 設定ガイド(PAN-OS 8.1) V1.0

Palo Alto Networks K.K. 2019/7

# 目次

1.	はじめに	4
2.	GlobalProtect の動作概要	5
2 2	2.1. External Gateway への接続 2.2. Internal Gateway への接続	5 7
3.	GlobalProtect の動作検証用ネットワーク構成	9
4.	初期設定	10
5.	L3 Firewall としての基本的な設定	11
5 5	5.1. ネットワーク設定 5.2. ポリシーの設定	11 14
6.	Active Directory Domain Services の設定	15
6 6 6	6.1. ADDSとDNS Server のインストール 6.2. ADDS の設定 6.3. [参考]パスワードの複雑さの変更 6.4. Active Directory ユーザーの作成	
7.	GlobalProtect の基本的な設定	25
7 7 7 7 7 7 7 7	<ul> <li>7.1. ネットワーク設定</li></ul>	25 30 39 42 43 43 57 58
8.	クライアント証明書認証の設定	67
8 8 8 8 8	<ul> <li>3.1. 全ユーザー共通のクライアント証明書で認証</li> <li>3.2. 各ユーザー個別のクライアント証明書で認証 (SCEP 利用による配布)</li> <li>3.3. CRL によるクライアント証明書の失効管理</li> <li>3.4. OCSP によるクライアント証明書の失効管理</li> <li>3.5. 新規ユーザーだけにクライアント証明書を配布する方法</li> </ul>	
9.	ワンタイムパスワード認証の設定	132
9 9 9 9 9	<ul> <li>9.1. Google Authenticator のインストール</li> <li>9.2. OTP サーバーのインストールと設定</li> <li>9.3. RADIUS 認証の設定</li> <li>9.4. GP Agent からのアクセス</li> <li>9.5. 外部からの接続はパスワードと OTP 両方の入力を強制する設定</li> <li>9.6. VPN の再接続時に一定時間は OTP の再入力を必要としない設定</li> </ul>	
10.	macOS からの接続	151
1 1 1	<ul> <li>10.1. GP Agent (v4.1.10) のダウンロードとインストール</li> <li>10.2. Portal &amp; Gateway へのアクセス</li> <li>10.3. クライアント証明書の失効</li> </ul>	151 153 156
11.	User-ID でアクセス制御	157
1 1	1.1. ユーザー名でアクセス制御  1.2. グループでアクセス制御	157 159
12.	Host Information Profile で制御	162

12.1	. HIP 検証用の事前設定	
12.2	2. HIP オブジェクトと HIP プロファイルの設定	
12.3	3. HIP マッチログの確認	
12.4	l. セキュリティポリシーの設定	
12.5	5. 動作確認	
12.6	6. [参考]各種端末の HIP	
13.	スマートデバイスからの接続	168
13.1	. SCEP によるクライアント証明書のインポート	
13.2	2. 手動によるクライアント証明書のインポート	174
14.	おわりに	191

# 1. はじめに

本ガイドにて、GlobalProtectの設定方法をご紹介します。

GlobalProtect には以下のような特徴があり、それぞれの設定と動作確認の方法を記載しています。

- ① リモートアクセス VPN (IPSec または SSL)
- ② ユーザー識別 (リモートアクセス VPN 時だけでなく、社内 LAN でも)
- ③ クライアント証明書の発行・認証・失効管理 (認証局サーバーとの連携)
- ④ ワンタイムパスワード認証 (OTP サーバーとの連携)
- ⑤ 検疫: Host Information Profile(HIP)でのアクセス制御 (アンチウィルスの有無、HDD 暗号化の有無等で制御)

PA Firewall の機能と共に GlobalProtect を使うことで、外部からのリモートアクセス機能だけでなく、社内 LAN における ユーザー識別や検疫が可能となるので、PA Firewall をより有効に、より強力にご利用いただくことができます。

また、WindowsとmacOSに限定されますが、本ガイドで紹介するほとんどの機能は PA Firewall の標準機能としてご利用いただけます。 ○·PA Firewall の標準機能 / ●·ClobalProtect #ブスクリプション(有償)

		$\bigcirc$ . F		=1成肥 / ●.000		/)//コノ(午頃)
↓機能	OS→	Windows	macOS	iOS	Android	Linux
① リモートアクセス	VPN	$\bigcirc$	$\bigcirc$		•	•
② ユーザー識別		$\bigcirc$	$\bigcirc$		•	$\bullet$
③ クライアント証明書	書認証	$\bigcirc$	$\bigcirc$		•	•
④ ワンタイムパスワ	ード認証	$\bigcirc$	$\bigcirc$	•	•	$\bullet$
⑤ HIP 制御		•	•		•	•

本ガイドを弊社提供の正式ドキュメントと併用して頂き、新規設置作業や日々の運用時の設定変更作業時の参考ドキュメントとしてご活用ください。

※) 本ガイドは、以下の OS バージョンを利用しています。

- PAN-OS: 8.1.7
- GP Agent: 4.1.10 (Windows & macOS)
  - 5.0.5 (iOS & Android)

適用する OS バージョンが異なる場合は、該当する OS のドキュメントを参照してください。

# 2. GlobalProtect の動作概要

設定の解説に入る前に、GlobalProtectの動作を説明します。

ここで説明する動作については、GlobalProtect Agent (以降、GP Agent) ソフトウェアがクライアント PC ヘインストール 済みである前提とします。

## 2.1. External Gateway への接続

GP Agent が、社外=インターネットから自社内 LAN に接続するときの動作フローです。

(1) ポータルへのアクセス



(2) DNS を使って、GP Agent が今どこにいるのか(外部 or 内部)を判断



(3) 世界に複数存在する External Gateway のうち、近い方を選択



(4) External Gateway へのログイン&VPN トンネル確立と、検疫情報(HIP)の送信



VPN トンネル確立後のクライアント PC は、LAN 端末と同様の扱いが可能となり、PA Firewall のセキュリティポリシーの 適用が可能です。

ユーザー認証を実施済みなので、ユーザーID 情報を持つログ出力や、ユーザー名(グループ名)でのポリシーコントールが可能です。

検疫によるポリシーコントロールも可能であり、例えば「ディスクが暗号化されていない PC は特定サーバーへアクセスさせない」という制御も可能です。

## 2.2. Internal Gateway への接続

次は、GP Agent が社内 LAN に接続されたときの動作フローです。

基本的な動作は、「External Gateway への接続」で示したフローと同じで、異なるのは「VPN トンネルを確立しない」点です。

(1) ポータルへのアクセス



(2) DNS を使って、GP Agent が今どこにいるのか(外部 or 内部)を判断



(3) 世界に複数存在する Internal Gateway のうち、近い方を選択



(4) Internal Gateway へのログインと、検疫情報(HIP)の送信 (VPN トンネルは確立しない)



Internal Gateway ログイン後は、LAN 端末として、PA Firewall のセキュリティポリシーの適用が可能です。

ユーザー認証を実施済みなので、ユーザーID 情報を持つログ出力や、ユーザー名(グループ名)でのポリシーコントールが可能です。

社内 LAN においても検疫によるポリシーコントロールが可能であり、例えば「ディスクが暗号化されていない PC は特定サーバーへアクセスさせない」という制御も可能です。

# 3. GlobalProtect の動作検証用ネットワーク構成

以下のネットワーク構成にて、GlobalProtectの動作を確認します。



検証用ネットワーク構成の概要:

- GlobalProtect 設定を行う PA-Firewall は、パブリッククラウド: Microsoft Azure(以降、Azure)上に設置しています。
  - ▶ Azure から提供される Public IP アドレスと、Untrust 側のプライベート IP アドレスは 1 対 1 NAT です。
  - その Public IP アドレスは、Azure の DNS に「gp011.japaneast.cloudapp.azure.com」として登録しています。
- Windows Server 2012 R2(以降、Win2012)を Trust ゾーン側(Azure 内)に設置し、以下の役割をインストールしま す。
  - Active Directory Domain Services (ドメイン: acme.com)
  - 内部 DNS (正引き/逆引き)
  - Active Directory Certificate Services (認証局: クライアント証明書の発行及び管理)
- GP Agent がインストールされたクライアント PC は 4 台あり、以下の状態です。
  - 全て Windows10 です。
  - ▶ ドメイン: acme.com のクライアントです。
  - ▶ ユーザー:w10-003 だけは内部と外部の移動ができるようにしていますが、それ以外は図の通り固定です。
- 「社内 LAN-B」はオンプレミスであり、Azure の「社内 LAN-A」との間を IPSec トンネルで接続しています。
  - ➢ VyOS(仮想ルーター)を利用して、IPSecトンネル接続しています。
  - ▶ 理由:
    - ◆ オンプレミスの仮想版 OTP サーバーを利用するため。

# 4. 初期設定

以下の初期設定は実施済みであるものとします。

これらは、下記 Link からダウンロードできる「PA Series Firewall 設定ガイド(PAN-OS 8.1)」に詳細を記載していますので、必要に応じてご参照ください。

https://live.paloaltonetworks.com/t5/ナレッジドキュメント/PA-Series-Firewall-設定ガイド-PAN-OS-8-1/ta-p/209905

- (1) マネージメント IP の設定
- (2) ライセンス投入
- (3) シグネチャのダウンロードとインストール
- (4) OS アップグレード

# 5. L3 Firewall としての基本的な設定

本ガイドでは、インターネット・ゲートウェイとして設置済みの PA Firewall に GlobalProtect 機能を追加する、という状況を 想定し、まずは PA Firewall が、基本的な L3 ルーティングが行える状態まで設定します。

5.1. ネットワーク設定

ネットワークに関わる設定を行います。

5.1.1. ゾーンの設定

Untrust (インターネット側) と Trust (社内 LAN 側)のゾーンを設定します。

(1) a)「Network」  $\rightarrow$  b)「ゾーン」  $\rightarrow$  c)「追加」をクリックします。

		Dashboard	ACC	Monitor	Policies	Objects	Network Devic	e		参コミット 💣 🎑	🔋 Config 👻 🔍 検索
											😋 🔞 ヘルプ
	٩										0個の項目s → 🗙
$P_{a} = V - v $ b)											
聖バーチャル ワイヤー 愛 仮想ルーター		名前	タイプ	イン 仮想	νターフェイス/ 県システム	ゾーン プロテクション プロファイル	・ パケット バッファ ・ 保護	ログ設定	有効	含まれるネットワ ーク	除外されるネット ワーク
(値) IPSecトンネル デ DHCP デ DNS プロキシ ▶ ⑤ GlobalProtect & QoS											
		c)									
	÷	追加 🕒 削除				1	1				l .

(2) a)名前に「Trust」、b)タイプで「レイヤー3」を選択します。
 c)「ユーザ ID の有効化」にチェックを入れ、d)「OK」をクリックします。

ゾーン	0
名前 Trust a)	ユーザー ID ACL C)
ログ設定 None 🔍	✓ ユーザー ID の有効化
タイプ レイヤー3 b)	■ 許可リスト ▲
<ul> <li>■ インターフェイス▲</li> <li>■ ethernet1/2</li> </ul>	アドレスまたはアドレス グループを選択するか、自分のアド レスを入力してください。 Ex: 192.168.1.20 or 192.168.1.0/24
	<ul> <li>● 追加 ● 削除</li> <li>ごれらのアドレス/サブネットからのユーザーは特定されます。</li> <li>■ 除外リスト ▲</li> </ul>
●追加●削除	アドレスまたはアドレス グループを選択するか、自分のアド レスを入力してください。 Ex: 192.168.1.20 or 192.168.1.0/24
ゾーン プロテクション	
ゾーン プロテクション None マ プロファイル	
パケット バッファ保護の有効化	● 追加
	これらのアドレス/サプネットからのユーザーは特定されません。
	d) <u>o</u> ś <del>*</del> *>±ル

(3) 同様の方法で Untrust ゾーンも設定します。(ただし、Untrust は、ユーザーID は無効化のままでよいです。) 以下は、Trust と Untrust の 2 つのゾーンが生成された状態です。

paloalto		Dashboard	ACC	Monitor	Polic	cies Obje	cts Netv	vork De	vice		🏝 コミット 💰 🌔	≫ Config ▾ 🍳 検索
												😋 🔞 ヘルプ
インターフェイス	٩											2 個の項目s 🏓 🗙
<ul> <li> <sup>1</sup></li></ul>												
( <sup>@</sup> IPSec トンネル <sup>௺</sup> DHCP <sup>™</sup> DNS プロキシ		名前		タイプ		インターフェ イス/仮想シ ステム	ゾーン プロ テクション プロファイル	パケット バ ッファ保護	ログ設定	有効	含まれるネットワー ク	除外されるネットワ ーク
V 😨 GlobalProtect		Trust		layer3							任意	なし
👒 ポータル		Untrust		layer3							任意	なし

## 5.1.2. Ethernet インターフェイスの設定

インターフェイスにゾーン、IP アドレス、仮想ルーターを割り当てます。 また、インターフェイスへの Ping 応答を許可するように、インターフェイス管理プロファイルの設定も合わせて行います。

NETWORKS®	Dashboard	ACC	Monitor	Policies	Objects	Network	Device						
<ul> <li>ゴインターフェイス b)</li> <li>ゴリーン</li> <li>金 (「時間」」」</li> </ul>	Ethernet	Ethernet ループパック トンネル											
● 仮想ルーター 値 IPSec トンネル													
DHCP	インター	・フェイス	インターフェイスタ	イプ 管	「理プロファイル	リンク状態	IP アドレス	仮想ルーター	タグ	VLAN / バーチャル ワイヤー	セキュリティン	バーン	
DNS プロキシ	and ether	net1/1	Layer3		-MGMT		10.9.1.4/24	default	Untagged	none	Untrust	c)	
く GlobalProtect	and ether	net1/2	Layer3	ayer3 IF-MGMT			10.9.2.4/24	default	Untagged	none	Trust		
	and ether	net1/3				Ē	none	none	Untagged	none	none		

(2) インターフェイス管理プロファイル:a)「IF-MGMT」は、b)Pingのみ許可します。

インターフェイス管理プロファイル	0
名前 IF-MGMT a)	
管理サービスの管理	アクセス許可 IP アドレス
HTTP	
HTTPS	
Temperature	
SSH	
ネットワークサービス	
Image Pring Pring D	
HTTP OCSP	
SNMP	
□ 応答ページ	
ニューザー ID	
ニューザー ID Syslog リスナー SSL	A 19-40 - 10 101-0-
ローザー ID Syslog リスナー UDP	Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64
	OK キャンセル

#### 5.1.3. 仮想ルーターの設定

仮想ルーターに、デフォルトルートを設定します。

加えて、社内 LAN-B へのスタティックルートも設定します。

(1) a)「Network」  $\rightarrow$  b)「仮想ルーター」  $\rightarrow$  c)「default」をクリックします。

	Dashboard	ACC Mon	itor Policies	Objects	Network	Device		📥 コミット 💣 🌡	Config 👻 🔍 検索
									😋 🔞 ヘルプ
<b>エレ</b> インターフェイス	۹.								1 個の項目 🚽 🗶
IMI ゾーン 影 VLAN	□ 名前	インターフェイス	設定	RIP	OSPF	OSPFv3	BGP	マルチキャスト	ランタイム状態
● パーチャル ワイヤー ● 仮想ルーター b)	default	C) ethernet1/1 ethernet1/2	ECMP の状態: 無効						詳細ランライム状態
(19) IPSec トンネル デ DHCP PNS プロキシ	4								
Colorenteet									
■ LLDP ■ ネットワーク プロファイル									
	🕂 追加 🔳 削除								

(2) 「スタティックルート」タブ → 「IPv4」タブで、以下のように2つのルートを設定します。

仮想ルーター - default											0 🗆
Router Settings	Lib	IDv6									
スタティック ルート		14 IPV0									
再配信プロファイル					2/17	トホップ				2 個の項目s ➡	×
RIP		名前	宛先	インターフェイス	タイプ	値	管理距離	メトリック	BFD	ルート テープル	
OSPF		default-route	0.0.0.0/0	ethernet1/1	ip-address	10.9.1.1	default	10	None	unicast	
OSPFv3		Int-Route	10.10.222.0/24		ip-address	10.9.2.10	delauit	10	None	unicast	
BGP											
マルチキャスト											
	•	●追加 ■削除	©⊐ピ–								
									_		
										OK ++>	ノセル

## 5.2. ポリシーの設定

Trust ゾーンのクライアント PC が、インターネットにアクセスするためのポリシーを設定します。

#### 5.2.1. セキュリティポリシー

簡易的に、Trust から Untrust は全て許可する設定にしておきます。

(1) a)「Policies」  $\rightarrow$  b)「セキュリティ」  $\rightarrow$  c)「追加」をクリックします。

paloalto	[	Dashboard ACC	N	lonitor	Policies	Obje	cts Ne	etwork Devic	е				📥 コミッ	ト 💣 🐶 Confiç	] <del>-</del> Q.検索
															ら ③ヘルプ
📟 セキュリティ b)	•													2個0	D項目s ⋺ 🗙
SP NAT							送信元		3	<b>ē</b> 先					
😳 ポリシー ベース フォワーディング		名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション	プロファイル	オプション
◎ 復号	1	intrazone-default 🚳	none	intrazone	any	any	any	any	(intrazone)	any	any	any	🕑 許可	none	none
<ul> <li>トンネル検査</li> <li>アプリケーション オーバーライド</li> </ul>	← 2	interzone-default 🥹	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否	none	none
8→認証	1														
Ĵ€DoS プロテクション	6	<b>c)</b>													
	•	追加 🖃 削除 💿 コピー	* オ	ーバーライト	、 * 戻す	🕑 有効化	💽 無効化	移動 - 📔 使用され	れていないル	ールの強調表	示				

(2) a) 以下のように、Trust→Untrust 方向への全許可ポリシーを追加します。

						送信元			弛			
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
1	outbound	none	universal	pag Trust	any	any	any	🕅 Untrust	any	any	any	📀 許可 a)
5	intrazone-default 🥎	none	intrazone	any	any	any	any	(intrazone)	any	any	any	♥ 許可
6	interzone-default 🍪	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否

#### 5.2.2. NAT ポリシー

Trust 発のパケットの送信元 IP アドレスを、eth1/1 の IP アドレスに変換する NAT ポリシーを設定します。

eth1/1の IP アドレスは、Azureの Public IP と1対1で紐付けられているので、この設定によって、送信元は Global IP アドレスに変換されます。

(1) a) 「Policies」  $\rightarrow$  b) 「NAT」  $\rightarrow$  c) 「追加」をクリックします。

	D	ashboard	ACC	Monitor	Policies	Objects	Network	Device		📥 コミット	🗸 💣 🌘 Cor	nfig ▼
												😋 🔞 ヘルプ
	٩										0 1	園の項目s <mark>→</mark> 🗙
SP NAT D										変換済み		
■ポリシー ベース フォワーディング		名前	タグ	送信元ゾーン	宛先ゾーン	宛先インターフェイス	送信元アドレ	ス 宛先アドレス	サービス	送信元変換	宛先変換	
<ul> <li>値 復号</li> <li>         トンネル検査     </li> </ul>	4											
アプリケーション オーバーライド												
≫ 認証 €DoS プロテクション	0	c)										
	÷	追加 🖃 削除	👩 コピー	- 🗹 有効化 🔞	●無効化 移動	• 📔 使用されてい	ないルールの強調	表示				

#### (2) a) 以下のように、Trust→Untrust 方向への送信元 NAT ポリシーを追加します。

				元のパケット						変換済みパケット		
	名前	タグ	送信元ゾーン	宛先ゾーン	宛先インターフェイス	送信元アドレス	宛先アドレス	サービス	送信元変換	宛先変換		
1	outbound	none	🕅 Trust	ුණු Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1 10.9.1.4/24	なし a)		

(3) 「コミット」を実施します。

L3 Firewall としての基本的な設定は以上です。

# 6. Active Directory Domain Services の設定

本ガイドでは、Win2012 に Active Directory Domain Services (以降、ADDS)を認証サーバーとして利用しますので、その設定を行います。

6.1. ADDS と DNS Server のインストール

(1) Server Manager で、「Add roles and features」をクリックします。

<u>E</u>	Server Manager				_	D X
Server	Manager • Dashboard	• ②	Mana	ige Tools	View	Help
Dashboard     Local Server     Local Server     All Servers     AD DS     DNS     File and Storage Services     IN     (2) 「Next 1を力	WELCOME TO SERVER MANAGER  QUICK START  QUIC	server es manage				
	Add Roles and Features Wizard	_ 🗆 X				
Before you begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine features to install based on the computing needs of your organization, such hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features: Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The work settings, such as static IP addresses, are configured If you must verify that any of the preceding prerequisites have been complet complete the steps, and then run the wizard again. To continue, click Next.	DESTINATION SERVER Win2012 acroscom which roles, role services, or as sharing documents, or ted, close the wizard,				
	< Previous Next >	Install Cancel				

(3) 「Role-based or feature-based installation」を選択し、「Next」をクリックします。



## (4) 「Next」をクリックします。



(5) 「Active Directory Domain Services」にチェックを入れます。



#### (6) 「Add Features」をクリックします。



## (7) 「DNS Server」にチェックを入れます。



#### (8) 「Add Features」をクリックします。



#### (9) 何もしないで、「Next」をクリックします。



## (10)「Next」をクリックします。



## (11)「Next」をクリックします。



#### (12)「Install」をクリックします。

<b>a</b>	Add Roles and Features Wizard	
Confirm installa	tion selections	DN SERVER Win2012DC
Before You Begin	To install the following roles, role services, or features on selected server, click Install.	
Installation Type	Restart the destination server automatically if required	
Server Selection	Optional features (such as administration tools) might be displayed on this page because the	y have
Server Roles	been selected automatically. If you do not want to install these optional features, click Previou their check hover.	is to clear
Features	unen erieek boxes.	
AD DS	Active Directory Domain Services	^
DNS Server	DNS Server	
Confirmation	Group Policy Management	
Results	Remote Server Administration Tools         Role Administration Tools         AD DS and AD LDS Tools         Active Directory module for Windows PowerShell         AD DS Tools         Active Directory Administrative Center         AD DS Snap-Ins and Command-Line Tools	=
	apecity on orientoic source pour	
	< Previous Next > Install	Cancel

## (13)「Close」をクリックします。



## 6.2. ADDS の設定

ドメイン名は「acme.com」として設定していきます。

(1) 旗のマークをクリック  $\rightarrow$  「Promote this server to a domain controller」をクリックします。



(2)「Add a new forest」を選択して、「Root domain name:」に、「acme.com(任意)」と入力します。「Next」をクリックします。



#### (3)「Password:」に管理者パスワードを入力して、「Next」をクリックします。

· 🖻 · ·	Active Directory Domain Services C	onfiguration Wizard				
Domain Controlle	r Options		TARGET SERVER Win2012			
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest a Forest functional level: Domain functional level: Specify domain controller capabilities Omain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mod Password: Confirm password:	and root domain Windows Server 2012 R2 Windows Server 2012 R2  e (DSRM) password				
More about domain controller options						
	< Pre	vious Next > Install	Cancel			

#### (4) 表示された警告メッセージは本ガイドでの動作確認に影響ありませんので、「Next」をクリックします。 Active Directory Domain Services Configuration Wizard



#### (5) 「Next」をクリックします。

1	Active Directory Domain Services Configurat	tion Wizard	_ <b>D</b> X
Additional Optior	IS		TARGET SERVER Win2012
Deployment Configuration Domain Controller Options	Verify the NetBIOS name assigned to the domain ar	d change it if necessary	
DNS Options	The Netbios domain name: ACME		
Additional Options			
Paths Davideur Octioner			
Review Options			
Installation			
Results			
Results			
	More about additional options		
	< Previous	Next > Install	Cancel

## (6) 「Next」をクリックします。

<b>a</b>	Active Directory Domain Services	Configuration Wizard	_ <b>D</b> X
Paths			TARGET SERVER Win2012
Deployment Configuration Domain Controller Options	Specify the location of the AD DS data	base, log files, and SYSVOL	
DNS Options	Database folder:	C:\Windows\NTDS	
Additional Options	Log files folder:	C:\Windows\NTDS	
Paths	SYSVOL folder:	C:\Windows\SYSVOL	
Review Options			
Prerequisites Check			
Installation			
Results			
	More about Active Directory paths		
	< P	revious Next > In:	stall Cancel

#### (7) 「Next」をクリックします。



## (8) 「Install」をクリックします。



(9) インストール後、自動的に再起動が行われます。

## 6.3. [参考]パスワードの複雑さの変更

検証環境においては、Active Directory ユーザのデフォルトパスワードポリシーが複雑すぎて、検証しづらい場合があります。その場合は、以下のステップで、変更できます。

(1) 「Server Manager」の右上にある「Tools」→「Group Policy Management」を選択します。



(2)「Group Policy Management」の下の「Forest: acme.com」→「Domains」→「acme.com」→「Default Domain Policy」を右クリックして、「Edit」を選択します。



(3) 「Policies」→「Windows Settings」→「Security Settings」→「Account Policies」→「Password Policy」で表示された パスワードポリシーを、お好みの設定に変更してください。

<u>.</u>	Group Policy Management Editor					
File Action View Help						
<ul> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Windows Settings</li> <li>Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> <li>Security Settings</li> <li>Account Policies</li> <li>Password Policy</li> <li>Account Lockout Policy</li> <li>Kerberos Policy</li> <li>Local Policies</li> <li>Event Log</li> </ul>	<ul> <li>Policy</li> <li>Enforce password history</li> <li>Maximum password age</li> <li>Minimum password age</li> <li>Minimum password length</li> <li>Password must meet complexity requirements</li> <li>Store passwords using reversible encryption</li> </ul>	Policy Setting 0 passwords remembered 0 0 days 7 characters Disabled Disabled				

## 6.4. Active Directory ユーザーの作成

本ガイドのクライアント PC×4 台分の AD ユーザーを登録します。

(1) Win2012 の「Administrative Tools」→「Active Directory Users and Computers」を開きます。
 a)「acme.com」→ b)「Users」を右クリック → c)「New」→ d)「User」をクリックします。

<b>a</b>		Active Dire	ectory Users and	Computers		_ <b>_ ×</b>	
File Action View Help					•		
🗢 🔿 🙍 🚮 🔏 📋 🗶 🗎 🖉	2 🖬 %	i 🗑 🍸 🗾 🐍					
Active Directory Users and Computers [Win20]	l2.acme.com]	Name ^		Туре		Description	^
D Saved Oueries		گ Administrator		User		Built-in account for administering the computer/domain	
⊿ 🟥 acme.com a)		& Allowed RODC Passwo	rd Replication Group	Security Group -	Domain Local	Members in this group can have their passwords replicated	
p Builtin		& Cert Publishers		Security Group -	Domain Local	Members of this group are permitted to publish certificat	
Computers		🎎 Cloneable Domain Cor	ntrollers	Security Group -	Global	Members of this group that are domain controllers may be	
Domain Controllers		& Denied RODC Password	d Replication Group	Security Group -	Domain Local	Members in this group cannot have their passwords replica	
ForeignSecurityPrincipals		& DnsAdmins		Security Group -	Domain Local	DNS Administrators Group	-
	-	A DnsUpdateProxy		Security Group -	Global	DNS clients who are permitted to perform dynamic update	
Delegate Control		🚨 Domain Admins		Security Group -	Global	Designated administrators of the domain	
Find		& Domain Computers		Security Group -	Global	All workstations and servers joined to the domain	
New o)	Compute	r	]	Security Group -	Global	All domain controllers in the domain	
	Contrat			Security Group -	Global	All domain guests	
All Tasks	Contact			Security Group -	Global	All domain users	
View 🕨	Group			Security Group -	Universal	Designated administrators of the enterprise	
Refresh	InetOrgP	erson	omain Controllers	Security Group -	Universal	Members of this group are Read-Only Domain Controllers	
Export List	msDS-Re	sourcePropertyList	wners	Security Group -	Global	Members in this group can modify group policy for the do	
Export Eist	mslmagir	ng-PSPs		User		Built-in account for guest access to the computer/domain	
Properties	MSMO O	ueue Alias		Security Group -	Domain Local		-
Help	Printer		ш			>	
Create a new object	User	d)					
	Shared Fo	lder					

(2) 「w10-001@acme.com(任意)」というユーザを設定します。

New Object - User					
Create in: acme.com/Users					
First name: a) Initials:					
Last name: 001 b)					
Full name: w10 001					
Userlogon name: w10-001 C) @acme.com V					
User logon name (pre-Windows 2000): ACME\ w10-001					
< Back d) Next > Cancel					

(3) a)パスワードを入力し、b)「User must change password ad next login/ユーザーは次回ログイン時にパスワードの変更が必要」のチェックを外します。c)「Next」をクリックします。

New Object - User
Create in: acme.com/Users
Password: Confirm password:
User must change password at next logon b)
User cannot change password
Account is disabled
<pre> C)   &lt; Back Next &gt; Cancel</pre>

## (4) 「Finish」をクリ<u>ックします。</u>

New Object - User	x
Create in: acme.com/Users	
When you click Finish, the following object will be created:	
Full name: w10 001	^
User logon name: w10-001@acme.com	~
< Back Finish	Cancel

(5) [確認のみ] 権限 (Member Of) は、デフォルトの「Domain Users」のままで OK です。

w10 001 Properties								
Remote	control	Remote D	Т	CO	M+			
General	Address	Account	Organiz	ation				
Membe	r Of	Dial-in Environment Sessions						
Member of:								
Jomain Users acme.com/Users								
Add Primary gr	Add Remove Primary group: Domain Users							
Set Prir	nary Group	There is n you have application	io need to o Macintosh ns.	change Primary clients or POSI	grou IX-co	ıp unle mplian	ss t	

- (6) 同様の方法で、後3つのユーザーを登録=合計4つのユーザー登録を行います。
- w10-001
   w10-002
   w10-003
   w10-004

# 7. GlobalProtect の基本的な設定

## 7.1. ネットワーク設定

## 7.1.1. ゾーンの設定

PA Firewall に Corp-VPN ゾーンを新しく追加し、GlobalProtect Agent が VPN 接続すると、そのトンネルインターフェイスが Corp-VPN ゾーンに割り当てられるようにします。

Trust ゾーンを利用することもできますが、制御のしやすさの観点から、VPN 用のゾーンを生成することを推奨します。

(1) a)「Network」  $\rightarrow$  b)「ゾーン」  $\rightarrow$  c)「追加」をクリックします。

paloalto	Dashboard	ACC Moni	tor Policies	Objects N	etwork Device	e		参コミット 💣 🎑	Config ▼ Q 検索
									😋 🕢 ヘルプ
	٩								0個の項目s → 🗙
Per Vーン D)								ユーザー ID	
聖バーチャル ワイヤー   ● 仮想ルーター	□ 名前	タイプ	インターフェイス/ 仮想システム	ゾーン プロテクシ ョン プロファイル	パケット バッファ 保護	ログ設定	有効	含まれるネットワ ーク	除外されるネット ワーク
(値 IPSec トンネル 第 DHCP									
デ DNS プロキシ	-								
& QoS									
	c)								
	🕂 追加 🕒 削除								

(2) 表示された画面で、a)名前に「Corp-VPN」、b) タイプで「レイヤー3」を選択します。
 c)「ユーザーID の有効化」にチェックを入れ、d)「OK」をクリックします。

ゾーン	0
名前 Corp-VPN a)	ユーザー ID ACL
ログ設定 None 💌	✓ ユーザー ID の有効化 C)
タイプレイヤー3 b)	■ 許可リスト ▲
■ インターフェイス ▲	アドレスまたはアドレス グループを選択するか、自分 のアドレスを入力してください。 Ex: 192.168.1.20 or 192.168.1.0/24
●追加●削除	<ul> <li>● 追加</li> <li>● 削除</li> <li>これらのアドレス/サブネットからのユーザーは特定されます。</li> <li>■ 除外リスト ▲</li> </ul>
ゾーン プロテクション ゾーン プロテクショ None ▼ ン プロファイル	アドレスまたはアドレス グループを選択するか、自分 のアドレスを入力してください。 Ex: 192.168.1.20 or 192.168.1.0/24
□ パケット バッファ保護の有効 化	●追加 ● 削除 これらのアドレス/サブネットからのユーザーは特定されません。
	<b>d)</b> OK キャンセル

(3) [確認のみ] 以下は、Corp-VPN ゾーンが追加された状態です。

🐙 paloalto	Deebbeard	ACC	Monitor	Delicion	Objecte	Notwork	Davias			\$ <b>7 2 w b</b>	🖗 Coofia = 🔒 🏟 👼
NETWORKS®	Dasilboard	ACC	WOIIItor	Policies	Objects	Network	Device				🧑 Colling 🔹 化完全
											😋 🔞 ヘルプ
インターフェイス											3個の項目s  🐱
<b>24</b> ゾーン										- 44 - 10	
🐵 仮想ルーター										-9-10	
1 IPSec トンネル					インターフェ	ゾーン プロテ	18th w h 18w				除从されるネットワー
L DHCP	名前		タイプ		イス/仮想シス	クション プロ	ファ保護	ログ設定	有効	含まれるネットワーク	5
覺 DNS プロキシ					テム	ファイル					
V 😨 GlobalProtect	Corp-VPN		layer3							任意	なし
 ◎ ポータル	Trust		layer3							任意	なし
🖲 ゲートウェイ	Untrust		layer3							任意	なし
MDM											

## 7.1.2. トンネルインターフェイスの設定

GP Agent が外部から VPN 接続するためのトンネルインターフェイスを設定し、それを Corp-VPN ゾーンに割り当てます。 複数の Agent が VPN 接続する場合でも、トンネルインターフェイスは一つだけでよいです。

(1) a)「Network」  $\rightarrow$  b)「インターフェイス」  $\rightarrow$  c)「トンネル」タブ  $\rightarrow$  d)「追加」をクリックします。

	Dashboard AC	C Monitor Policies	Objects Network	Device		🏝 コミット 🧉 阔 Config 🕶 🔍 検索
						S @ヘルプ
■インターフェイス b)  ■ゾーン	Ethernet ループバッ	クトンネル				
<ul> <li>         ・ 仮想ルーター         ・         ・         ・</li></ul>	٩	С)				0 個の項目s 🔿 🗙
<sup>▶</sup> DHCP <sup>™</sup> DNS プロキシ	インターフェイス	管理プロファイ ル IP アドレス	仮想ルーター	セキュリティ ゾー ン	機能 コメント	
▼ CollobalProtect のポータル	4					
● ゲートウェイ ● MDM ■ デバイス ゴロック リス						
■ クライアントレス アプ! ■ クライアントレス アプ!						
dos dos		rcsv				

(2) a)インターフェイス名の末尾に、「1」(任意)を入力します。 まず、b)「設定」タブ内の設定を行います。

c)仮想ルーターで「default」を選択します。 d)セキュリティゾーンは「Corp-VPN」を選択します。

トンネル インターフェイス	0
インターフェイス名 tunnel	. <u>1</u> a)
コメント	
Netflow プロファイル None	
D) 設定 IPv4 IPv6 詳細	
「インターフェイスの割り当て先	
仮想ルーター default C)	
セキュリティ ゾーン Corp-VPN d)	
	OK キャンセル

(3) 「IPv4」タブでは、何も設定しません。

トンネル インターフェイス	୭
インターフェイス名 tunnel	. 1
コメント	
Netflow プロファイル None	-
設定 IPv4 IPv6 詳細	
IP	
➡追加 ■削除 ●上へ ●下へ	
	OK キャンセル

(4) a)「IPv6」タブでは、b)「インターフェイスでの IPv6 有効化」にチェックを入れます。
 (コミット時の Warning メッセージを回避するためだけの目的であり、本ガイドでは IPv6 は使いません。)

トンネル インターフェイス			0
インターフェイス名 tunnel		. 1	
コメント			
Netflow プロファイル None 名) 設定 IPv4 IPv6 詳細			~
✓ インターフェースでの IPv6 の有効化	<b>b)</b> インターフェ EUI-64 イス ID		~
■ アドレス	インターフェイス ID	プレフ ィック ス	エニー キャス ト
➡追加 ■削除 ■上へ ■下へ			
		ОК	キャンセル

#### (5)「詳細」タブでは、何も設定しません。

トンネル インターフ	<b>アェイス</b>	0
インターフェイス名	tunnel . 1	
コメント		
Netflow プロファイル	None	~
設定 IPv4 IPv6	詳細	
その他の情報		
管理プロファイル	None	~
MT	J [576 - 1500]	
	0	K キャンセル

(6) 以下は、トンネルインターフェイスが一つ生成された状態です。

■インターフェイス Etherne	t ループ	バック	トンネル					
© IPSecトンネル DHCP インター DHCP インター DNS プロキシ GlobalProtect truncal	-フェイス	管理プロフ	アイル	IP アドレス none	仮想ルーター none.	セキュリティ ゾーン Dane	機能	コメント

- (7) [確認のみ] 仮想ルーターにトンネルインターフェイスが加わります。
  - このことで、VPN 接続したクライアントのインターフェイスが仮想ルーターのインターフェイスとなり、Trust や Untrust ゾーンとのルーティングが可能になります。

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device			<b>*</b> =	ミット 🧉 闷 Config 🕶 🔍 検索
インターフェイス	۹.										<ul> <li>⑦ヘルプ</li> <li>1個の項目</li> </ul>
<i>4</i> 9 <b>. ゾーン</b> ⊕ 仮想ルーター	名前	インターフェ·	12	設定	. II	RIP	OSPF	OSPFv3	BGP	マルチキャスト	ランタイム状態
● IPSec トンネル <sup>●</sup> DHCP <sup>●</sup> DNS プロキシ ▼ CobalProtect	derault	ethernet1/1 ethernet1/2 tunnel.1		スタティック ECMP の状態	: 無効						計和フジライム状態

## 7.1.3. Active Directory への BIND 用ユーザーの設定

PA Firewall が Active Directory からユーザー情報を取得するためのアカウントを、1つ生成します。

(1) Win2012 の「Administrative Tools」→「Active Directory Users and Computers」を開きます。
 a)「acme.com」→ b)「Users」を右クリック → c)「New」→ d)「User」をクリックします。

		Active Dire	ectory Users and	Computers			
File Action View Help							
🗢 🔿 📶 🤾 📋 🗙 🗐 🍳 🗟	2 🖬 🕺	l 🛅 🍸 🗾 🍇					
Active Directory Users and Computers [Win20	Name ^		Туре	Description ^			
Saved Queries		& Administrator		User	Built-in account for administering the computer/domain		
⊿ 🛱 acme.com 🛛 🛛		& Allowed RODC Passwo	ord Replication Group	Security Group - Domain Loo	al Members in this group can have their passwords replicated		
p Bulitin		& Cert Publishers		Security Group - Domain Loo	al Members of this group are permitted to publish certificate:		
Computers		🏽 🍇 Cloneable Domain Cor	ntrollers	Security Group - Global	Members of this group that are domain controllers may be		
Domain Controllers		& Denied RODC Passwor	d Replication Group	Security Group - Domain Loo	Members in this group cannot have their passwords replica		
ForeignSecurityPrincipals	Section 2018 March 1997 March 2018		Security Group - Domain Loo	al DNS Administrators Group =			
User b	Manaded Service Accounts			Security Group - Global	DNS clients who are permitted to perform dynamic update		
Delegate Control		& Domain Admins		Security Group - Global	Designated administrators of the domain		
Find		& Domain Computers		Security Group - Global	All workstations and servers joined to the domain		
New	Compute	r	1	Security Group - Global	All domain controllers in the domain		
	Compute			Security Group - Global	All domain guests		
All Tasks	Contact			Security Group - Global	All domain users		
View +	Group			Security Group - Universal	Designated administrators of the enterprise		
Refresh	InetOrgP	erson	omain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers		
Export List	msDS-Re	sourcePropertyList	wners	Security Group - Global	Members in this group can modify group policy for the do		
Export Listin	ng-PSPs		User	Built-in account for guest access to the computer/domain			
Properties	Properties MSMO Que			Security Group - Domain Loo	al 🗸		
Help	Printer		ш		>		
Create a new object	User	d)					
	Shared Fo	older					

(2)「panagent@acme.com(任意)」というユーザーを生成します。以下 a)~c)の値を入力して、d)「Next」をクリックします。

<u>× ( u)</u>	
	New Object - User
🤱 Create in	: acme.com/Users
First name:	pan a) Initials:
Last name:	agent b)
Full name:	pan agent
User logon name: panagent	C) @acme.com ✓
User logon name (pr ACME¥	e-Windows 2000): panagent
	< Bacid) Next > Cancel

(3) a)パスワードを入力し、b)「User must change password ad next login」のチェックを外します。
 c)「Next」をクリックします。

New Object - User	x
Create in: acme.com/Users	_
Password: ( Confirm password: (	
User must change password at next logon; b) User cannot change password Password never expires Account is disabled	
C) < Back Next > Cancel	

# (4) 「Finish」をクリックします。



- (5) 設定した panagent ユーザーを開きます。
- (6) 「Member Of」タブで、「Add」をクリックし、「Server Operators」を追加します。

pan agent Properties ? X								
Remote control	Remote [	Remote Desktop Services Profile CON						
General Address	Account	Profile	Telephones	Organization				
Member Of	Dial-in	Envi	ironment	Sessions				
Member of:	·							
Name	Active Direct	ory Domain	Services Folder	r				
Domain Users	acme.com/L	sers						
Server Operators	acme.com/B	uiltin						
Add Primary group:	Remove Domain Users							
Set Primary Group	There is n you have application	no need to ( Macintosh ns.	change Primary clients or POSI)	group unless X-compliant				
	ок с	Cancel	Apply	Help				

## 7.2. ユーザー認証の設定

PA Firewall が、Win2012を認証サーバーとして利用できるように設定します。

#### 7.2.1. サービスルートおよび DNS の設定

PA Firewall デフォルト状態では、DNS および LDAP の参照先はマネージメントインターフェイス側になっています。 本ガイドの構成では、Win2012 は Trust ゾーン(eth1/2)側に設置されているので、その方向に DNS と LDAP の参照先を 変更します。

7.2.1.1. DNS サーバーの参照設定

まず、PA Firewall が参照する DNS サーバーを、Win2012 に設定します。

(1) a)「Device」 → b)「セットアップ」 → c)「サービス」で表示された「サービス」の d) 🔯 をクリックします。

naloalto								
NETWORKS®	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	
し、セットアップ b) る 設定監査	管理	操作 サー	-ビス イン C)	ノターフェイス	ス テレメト	עב – יי	テンツロ พ	lildFire セッミ
パスワード プロファイル 管理者	サービ	2					*	
<ul> <li>☆ 管理者ロール</li> <li>認証プロファイル</li> <li>認証シーケンス</li> </ul>		更	更新サ- 新サーバー ID の	-パー updates. D確認 ☑ DNS サーバー	paloaltonetwork	ks.com	<u>d)</u>	

(2) a)「プライマリ DNS サーバー」に、Win2012 の IP アドレスを設定します。
 b)「OK」をクリックします。

サービス	0
サービス NTP	
更新サーバー Ц	pdates.paloaltonetworks.com
	]更新サーバー ID の確認
DNS 設定	
DNS	● サーバー ○ DNS プロキシ オブジェクト
プライマリ DNS サーバー	10.9.2.5 a)
セカンダリ DNS サーバー	
FQDN 更新時間 (秒)	1800
Proxy Server	
サーバー	
ポート	[1 - 65535]
ユーザー	
パスワード	
再入力 パスワード	
	b) OK キャンセル

## 7.2.1.2. サービスルートの設定

PA Firewall の LDAP と DNS のサービスルートを eth1/2 へ変更します。

(1) a)「Device」 → b)「セットアップ」 → c)「サービス」 → d)「サービスルートの設定」で表示された画面で、e)のよう に、DNS および LDAP の送信元インターフェイスおよび送信元アドレスを eth1/2 に変更します。 f)「OK」をクリックします。



(2) 「コミット」します。

## 7.2.2. LDAP サーバーとの接続設定

認証サーバーとして利用する Active Directory (Win2012)との接続設定を行います。

(1) a)「Device」  $\rightarrow$  b)「LDAP」  $\rightarrow$  c)「追加」をクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	📥 コミット 🤞	î 闷 Config 🗸 🔍 検索
									5 ⑦ヘルプ
▽ 👩 サーバー プロファイル	۹.								0 個の項目s  🔁 🗙
崎 SNMP トラップ 崎 Syslog	🔲 名前			場所			サーバー	その他	
	× ·								
▲ SARL ナイングター認証 ■ マルチファクター認証 マ 回 ローカル ユーザー データベー 8 ユーザー 第 ユーザー グループ	C) € 追加 □ 削除 @	<b>)</b> ⊐ピ–							

(2) a)名前に「acme-Idap-server(任意)」と入力します。
 b)「SSL/TLS で保護された接続を要求」のチェックを外します。(AD 側の設定に依存します。)
 c)「追加」をクリックし、d)名前に「AD(任意)」、LDAP サーバーに「10.9.2.5」と入力します。
 e)タイプで「active-directory」を選択し、f)ベース DN は「DC=acme,DC=com」を選択します。
 (LDAP サーバーとの接続ができていなければ、ベース DN が取得できないので、選択できません。)
 g)に AD 上で生成済みのユーザー「panagent@acme.com」、h)にそのパスワードを設定します。
 i)「OK」をクリックします。

LDAP サーバー プロファイル		0
プロファイル名 acme-Idap-server a)		
□ 管理者使用のみ		
サーバリスト	サーバー設定	
名前 LDAP サーバー ポート	タイプ	active-directory
AD 10.9.2.5 d) 389	ベース DN	DC=acme,DC=com
	バインド DN	panagent@acme.com g)
c)	パスワード	h)
● 追加 ■ 削除	再入力 パスワード	••••••
LDAPサーバーのIPアドレスまたはFQDNを入力してください	バインドのタイム	30
	アウト	
	検索のタイムアウ	30
	百世行明度	60
	4-3 EV1 1 EV14	
		i) OK <mark>キャンセル</mark>

## 7.2.3. グループマッピングの設定

Active Directory (LDAP サーバー)から、ユーザーとグループのマッピング情報を取得します。

グループマッピングは、ある特定のグループだけ認証して VPN 接続させたい場合や、グループ単位のセキュリティポリシーを設定したい、という場合に必要となる設定です。

(1) a)「Device」 → b)「ユーザーID」 → c)「グループマッピング設定」 → d)「追加」をクリックします。

paloalto	Dashboard ACC M	onitor Policies Objects	Network Device	<b>*</b> =	1ミット 省 闷 Config 🗸 🔍 検索
			a)		5 ③ヘルプ
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	ユーザーマッピング 接続のセ	キュリティ ユーザー D エージュ	シト ターミナル サービス エージェント	グループマッピング設定	キャプティブ ポータルの設定
□ 間っ加量 ■ 設定監査 ● パスワード プロファイル				C)	0 個の項目s 🍑 🗶
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	□ 名前	有効	サーバー プロファイル	更新間隔 (秒	)
る 望 管理者ロール 総 認証プロファイル 42	4				
図コーザー ID b)					
<ul> <li>WM 情報ソーム</li> <li>▶ </li> <li>▶ </li> <li>↓ 証明書の管理</li> </ul>	(d)				
◎応答ページ	日前除				

- (2) a) 名前に「dc-for-group-mapping(任意)」を入力します。
  - b) サーバープロファイルは設定済みの「acme-Idap-server」を選択します。
  - c) ドメインに「acme」を入力します。
  - d) LDAP との更新間隔のデフォルトは 3600 秒と長いので、検証用に最短の「60」秒にしておきます。(任意)
  - e)「OK」をクリックします。

グループマッピン	ч <b>л</b>	0
名前 do	c-for-group-mapping a)	
サーバープロファ	マイル ユーザーおよびグループ属性 許可リストのグループ化 カスタムグループ	
サーバー プロファ イル	acme-Idap-server b)                  更新問照 60	
Domain Setting		
ユーザー ドメイン	acme C)	
Group Objects		
検索フィルタ		
オブジェクト クラ	group	
2		
User Objects		
検索フィルタ		
オブジェクト クラ	person	
2		
	☑ 有効	
	e) OK キャンセ/	IL

(3) 「コミット」を実施します。

(4) a)「Monitor」 → b)「システム」の c)検索フォームに「(subtype eq userid)」と入力します。

d)のログが出力されていれば OK です。 イベント:「connect-Idap-server」

オブジェクト: 「10.9.2.5」 (AD(LDAP)サーバーの IP アドレス)

内容: 「Idap cfg dc-for-group-mapping connected to server 10.9.2.5:389, initiated by:10.9.2.4」 (10.9.2.4: PA Firewall の eth1/2 の IP アドレス)

paloalto	Dashboard	ACC	Monito	or Policies Obj	jects Netwo	brk Device	<b>舎</b> コミッ
							手
▽ 🔂 ログ	(subtype eq u	iserid)	1				
N トラフィック 図	受信日時	タイプ	重大度	イベント	オブジェクト	内容	_
locul フィルタリング	03/28 02:01:11	userid	informatio al	connect-Idap-sever	10.9.2.5	Idap cfg dc-for-group-mapping connected to server 10.9.2.5:389, initiated by: 10.9.2.4	)
NildFireへの送信	03/27 02:41:56	userid	informational	connect-client		User-ID Client is connected to collector (null): Serial-number panorama2, vsys_id 1	4
💼 データ フィルタリング	03/27 02:41:56	userid	informational	connect-client		User-ID Client is connected to collector (null): Serial-number panorama, vsys_id 1	
📑 HIP マッチ	03/27 02:40:07	userid	informational	disconnect-client		User-ID Client is disconnected from collector (null): IP panorama2, port 0, vsys_id 1	
💷 ユーザー ID	03/27 02:40:07	userid	informational	disconnect-client		User-ID Client is disconnected from collector (null): IP panorama, port 0, vsys_id 1	
📤 トンネル検査	03/27 01:46:36	userid	informational	connect-client		User-ID Client is connected to collector (null): Serial-number panorama2, vsys_id 1	
	03/27 01:46:36	userid	informational	connect-client		User-ID Client is connected to collector (null): Serial-number panorama, vsys_id 1	
🖳 🤄 システム D)	03/27 01:43:54	userid	informational	disconnect-client		User-ID Client is disconnected from collector (null): IP panorama2, port 0, vsys_id 1	
<b>エ</b> アラーム	03/27 01:43:54	userid	informational	disconnect-client		User-ID Client is disconnected from collector (null): IP panorama, port 0, vsys_id 1	
<ul> <li>副認証</li> </ul>	03/27 00:38:02	userid	informational	connect-client		User-ID Client is connected to collector (null): Serial-number panorama2, vsys_id 1	
↓ ■ 統合済み	03/27 00:38:02	userid	informational	connect-client		User-ID Client is connected to collector (null): Serial-number panorama, vsys_id 1	

(5) a)「Device」  $\rightarrow$  b)「ユーザーID」  $\rightarrow$  c)「グループマッピング設定」  $\rightarrow$  d)「dc-for-group-mapping」をクリックします。

paloalto	Dashboard A	CC Monitor	Policies Objects	Network Device		🏝 ユミット 🔒 🎑 Co
				a)		
<ul> <li>◎ 管理者ロール</li> <li>※認正プロファイル</li> <li>※認正プロファイル</li> <li>※認証シーケンフ</li> <li>※ 認知シーケンフ</li> </ul>	ユーザー マッピング 。	接続のセキュリティ	ィ ユーザー ID エージェ	ント ターミナル サービ	スエージェント グループマッピング設定 C)	キャプティブ ポータルの設定 11
	□ 名前	_	有効		サーバー プロファイル	更新問隔 (秒)
▼ 4 回 証明書の管理	dc-for-group-mapping	d)			acme-Idap-server	default

(6) a)「許可リストのグループ化」  $\rightarrow$  b)「DC=acme,DC=com」  $\rightarrow$  c)「cn=users」を展開します。



(7) スクロールダウンして、a) [cn=domain users]を選択  $\rightarrow b$ ) +をクリック  $\rightarrow c$ )の状態にして、 d) [OK]をクリックします。

名前 dc-for-group-mapping サーバー プロファイル ユーザーおよびグループ属性 許可リストのグループ化 カスタムグループ 使用可能なグループ 含まれたグループ く cn=domain computers cn=domain quests cn=domain users a) cn=domain users a) cn=enterprise read-only domain controllers cn=rars and is servers cn=raead-only domain controllers	グループマッピング		Ø
サーバー プロファイル ユーザーおよびグループ属性 許可リストのグループ化 カスタムグループ 使用可能なグループ	名前 dc-for-group-mapping		
使用可能なグループ	サーバー プロファイル ユーザーおよびグル	レープ属性 許可リストのグループ化	カスタム グループ
Cn=domain computers     Cn=domain controllers     Cn=domain users     Cn=domain users     Cn=anterprise read-only domain controllers     Cn=enterprise read-only domain controllers     Cn=rars and ias servers     Cn=raed-only domain controllers	使用可能なグループ	含まれたグループ	
S cn=schema admins	cn=domain computers cn=domain controllers cn=domain users cn=domain users cn=enterprise read-only domain controlle cn=group policy creator owners cn=ras and ias servers cn=ras and ias servers cn=raed-only domain controllers cn=schema admins	s acme\domain users C)	

- (8) 「コミット」を実施します。
- (9) [確認のみ] CLI で以下のコマンドを実行して、グループマッピング状態を確認できます。

admin-admin@PA-VM> show user group-mapping state all

Group Mapping(vsys1, type: active-directory): dc-for-group-mapping Bind DN : panagent@acme.com Base : DC=acme,DC=com Group Filter: (None) User Filter: (None) Servers : configured 1 servers 10.9.2.5(389) Last Action Time: 1733 secs ago(took 0 secs) Next Action Time: In 1867 secs Number of Groups: 1 cn=domain users, cn=users, dc=acme, dc=com

## 7.2.4. 認証プロファイルの設定

認証プロファイルを設定して、GlobalProtect Portal および Gateway が、Active Directory(=LDAP サーバー)をユーザー 認証サーバーとして利用できるようにします。

(1) a)「Device」  $\rightarrow$  b)「認証プロファイル」  $\rightarrow$  c)「追加」をクリックします。

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device			\$	コミット
セットアップ		1				L	a)				
<ul> <li>■ 高可用性</li> <li>№ 設定監査</li> <li>ペマード プロファイル     <li>管理者     </li> </li></ul>		名前	場所	ţ,	ロック 午容ログイン回数	<b>アウト</b> ロックアウト時間 (分)	許可リスト	認証	サーバー プロフ ァイル	認証ファクター	その他
る 管理者ロール 後認証プロファイル b) 第該証シーケンス 国ユーザー ID											
<ul> <li>         WM 情報ソース</li></ul>			除 🙆 コピー								

- (2) a)名前に「Auth-Profile01(任意)」を入力します。
   「認証」タブで、
   b)タイプは「LDAP」を選択します。
   c)サーバープロファイルは設定済みの「acme-Idap-server」を選択します。
   d)ログイン属性に「sAMAccountName」と入力します。
  - e)ドメインに「acme」と入力します。

認証プロファイル		0							
名前 Auth-Profile01 a)									
認証度詳細									
タイプ	LDAP b)	~							
サーバー プロファイル	acme-Idap-server C)	~							
ログイン属性	sAMAccountName d)								
パスワード失効の警告	7 パスワード失効の警告をユーザーに通知するまでの日数								
ユーザー ドメイン	acme e)								
ユーザー名修飾子	%USERINPUT%	~							
「シングル サインオン									
Kerberos レルム									
Kerberos キータフ	「[インポート]をクリックして、このフィールド: X インポート								
	OK キャンセ	: <i>I</i> L							
(3) a)「詳細」タブ → 許可リストの b)「追加」をクリックします。
 c)グループマッピングの「許可リストのグループ化」で指定したグループ「domain users」を選択します。
 d)「OK」をクリックします。

認証プロファイル	0
名前 Auth-Profile01	
認証 度 詳細	
<u>()</u> () 許可リスト	
■ 許可リスト ▲	
C)	
● 追加	
- アカウントのロックアウト	1
許容ログイン回数 0	
ロックアウト時間 (分) 0	
	1
<b>d)</b> OK キャンセル	,

(4) 「コミット」を実施します。

#### 7.2.5. 認証テスト

認証プロファイルの設定が正しく動作するかを、CLI でテストできます。

(1) ユーザーグループを確認します。

admin-admin@Azure-PA-VM> show user group list

cn=domain users, cn=users, dc=acme, dc=com

Total: 1 \* : Custom Group

----

(2) グループ内のユーザーを確認します。

admin-admin@Azure-PA-VM> show user group name "cn=domain users, cn=users, dc=acme, dc=com"

short name: acme¥domain users

source type: Idap
source: dc-for-group-mapping

- [1 ] acme¥admin-admin
- [2 ] acme¥panagent
- [3 ] acme¥w10-001
- [4 ] acme¥w10-002
- [5 ] acme¥w10-003
- [6 ] acme¥w10-004

(3) 試しに、acme¥w10-003 をテストしてみます。

admin-admin@Azure-PA-VM> test authentication authentication-profile Auth-ProfileO1 username acme¥w10-003 password Enter password : (パスワードを入力します)

Target vsys is not specified, user "acme¥w10-003" is assumed to be configured with a shared auth profile.

Do allow list check before sending out authentication request... user "acme¥w10-003" is a member of allowed group "cn=domain users, cn=users, dc=acme, dc=com" on vsys "vsys1" Authentication to LDAP server at 10.9.2.5 for user "acme¥w10-003" Egress: 10.9.2.4 Type of authentication: plaintext Starting LDAP connection... Succeeded to create a session with LDAP server DN sent to LDAP server: CN=w10 003, CN=Users, DC=acme, DC=com User expires in days: never

Authentication succeeded for user "acme¥w10-003"

(←認証が成功したことを示しています。)

(4) [参考] グループマッピングのデフォルトの更新間隔は 3600 秒=1時間です。
 (本ガイドでは既述の設定で、60 秒に短縮しました。)
 AD ユーザーを新しく追加したとき、即座にグループマッピングに反映させたい場合には、PA Firewall の以下のコマンドで、強制的に再読み込みする必要があります。

admin-admin@Azure-PA-VM> debug user-id refresh group-mapping all

group mapping 'dc-for-group-mapping' in vsys1 is marked for refresh.

# 7.3. SSL 証明書の生成

GP Agent から Portal や Gateway への接続には HTTPS が使われるので、そのためには SSL 証明書が必要です。 それらを PA Firewall 内で生成します。

#### 7.3.1. 認証局証明書の生成

(1) a)「Device」 → 「証明書の管理」の下の b)「証明書」 → c)「デバイス証明書」→ d)「生成」をクリックします。

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device		
▼「肩証明書の管理	デバイス証明書	デフォルト	の信頼され	た証明機関					
<ul> <li>              ⋥ 証明書             b)</li></ul>	C) 名前	++-	プジェクト	子でLLL-75 1001人で 発行	诸	CA		+-	
■ SSL/HS ゲービス グロン ■ SCEP ■ SSL 復号化例外 ■ SSL 復号化例外	4			201.					
<ul> <li>□ ログ設定</li> <li>▽ 10 サーバー プロファイル</li> <li>10 SNMP トラップ</li> </ul>			(b)	1					
Syslog	■削除 無効化 更	新 📥 インポ・	-ト 露生成	🛓 証明書のエ	クスポート 🚽	🛓 HA キーのインオ	(ート 📥 HA キー	-のエクスポート	R PDF/CSV

(2) a)証明書名に「PA-Certificate-Authority(任意)」と入力します。
 b)共有名にも「PA-Certificate-Authority(任意)」と入力します。
 c)認証局にチェックを入れます。
 d)「生成」をクリックします。

証明書の生成	0
証明書タイプ <sup>(</sup>	・ローカル 〇 SCEP
証明書名	PA-Certificate-Authority a)
共通名	PA-Certificate-Authority b)
署名者	II明音に衣記される IP まだは FUDN
	7 認証局 C)
OCSP レスポンダ	~
▲ 暗号設定	
アルゴリズム	RSA
ピット数	2048 💌
ダイジェスト	sha256 💌
有効期限 (日)	365
証明書の属性	
□ タイプ	値
● 追加 ■ 削除	
	d) <sub>牛成</sub> キャンセル

(3) 生成が成功したことを示すメッセージが出力されたら、「OK」をクリックします。

## 7.3.2. GlobalProtect 用のサーバー証明書の生成

生成した認証局証明書を使って、GlobalProtect Portal および Gateway に設定するサーバー証明書を生成します。

7.3.2.1. 外部用サーバー証明書の生成 (Portal & External Gateway 兼用)

本ガイドの構成では、Portal と External Gateway で同じ IP アドレスを共有するので、サーバー証明書も共有することにし、外部用に1つだけサーバー証明書を生成します。(それぞれ、別々のサーバー証明書を発行しても問題ありません。)

- (1) a) 証明書名に「External-Gateway(任意)」と入力します。
  - b) 共有名は、ネットワーク構成に従い、「gp011.japaneast.cloudapp.azure.com」と入力します。
  - c) 署名者は生成した認証局「PA-Certificate-Authority」を選択します。
  - d)「追加」をクリックして、e)「Host Name」を選択し、「gp011.japaneast.cloudapp.azure.com」を入力します。
  - f)「生成」をクリックします。

証明書の生成		0
証明書タイプ	・ローカル 〇 SCEP	
証明書名	External-Gateway	a)
共通名	gp011.japaneast.cloudapp.azure.com	b)
署名者	PA-Certificate-Authority	- <b>C</b> )
[	認証局	
OCSP レスポンダ		-
▲ 暗号設定		
アルゴリズム	RSA	~
ピット数	2048	~
ダイジェスト	sha256	~
有効期限 (日)	365	
証明書の属性		
■ タイプ 値		
Host Name gp01	11.japaneast.cloudapp.azure.com	∋)
d)		
● 追加 ■ 削除		
	f) 生成 キャン	ノセル

- (2) 生成が成功したことを示すメッセージが出力されたら、「OK」をクリックします。
- ※ Portal のサーバー証明書の共通名:「gp011.japaneast.cloudapp.azure.com」と、
   クライアント PC 上の GP Agent に、宛先として設定する Portal の FQDN が一致する必要があります。
   (理由: GP Agent は、Web ブラウザと同様に、サーバー証明書の共通名: Common Name (CN) をチェックしており、宛先 FQDN と CN が一致しなければ証明書エラーとなって、接続できません。)

よって、この FQDN:「gp011.japaneast.cloudapp.azure.com」は、外部 DNS でアドレス解決できる状態になっている必要があります。

本ガイドでは、Azure を使っており、この FQDN が Azure の DNS サーバーにエントリーされるように設定しています。

## 7.3.2.2. 内部用サーバー証明書の生成 (Internal Gateway 用)

Internal Gateway が利用するサーバー証明書を生成します。

- (1) a) 証明書名に「Internal-Gateway(任意)」と入力します。
  - b) 共有名は、ネットワーク構成に従い、「trust.acme.com」と入力します。
  - c) 署名者は生成した認証局「PA-Certificate-Authority」を選択します。
  - d)「追加」をクリックして、e)「Host Name」を選択し、「gp011.japaneast.cloudapp.azure.com」を入力します。
  - f)「生成」をクリックします。

証明書の生成	0
証明書タイプ	・ローカル O SCEP
証明書名	Internal-Gateway a)
共通名	rrust.acme.com b) I明書に表記される IP または FODN
署名者	PA-Certificate-Authority
	認証局
OCSP レスポンダ	<b>V</b>
▲ 暗号設定	
アルゴリズム	RSA
ピット数	2048 💌
ダイジェスト	sha256 💌
有効期限 (日)	365
証明書の属性	
🔳 タイプ 🏾 値	
Host Name trust	acme.com e)
d)	
🕂 追加 🗖 削除	
	「) 生成 キャンセル

(2) 生成が成功したことを示すメッセージが出力されたら、「OK」をクリックします。

※ Internal Gateway のサーバー証明書の共通名:「trust.acme.com」と、
 Portal から GP Agent に送られる Internal Gateway の FQDN が一致する必要があります。
 (理由: GP Agent は、Web ブラウザと同様に、サーバー証明書の共通名: Common Name (CN) をチェックしており、宛先 FQDN と CN が一致しなければ証明書エラーとなって、接続できません。)

よって、FQDN:「trust.acme.com」は、内部 DNS でアドレス解決できる状態になっている必要があります。

# 7.4. SSL / TLS サービスプロファイルの設定

SSL / TLS サービスプロファイルを使用して、GP Agent~GP Portal/Gateway 間で使用するサーバー証明書の指定と、 許可する SSL/TLS のプロトコルバージョンを指定することができます。 本ガイドでは、SSL/TLS プロトコルバージョンはデフォルトのままとします。

(1) a)「Device」→「証明書の管理」の下の b)「SSL/TLS サービス プロファイル」→ c)「追加」をクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	
<u>@</u> VM 情報ソース	•						a)	
<ul> <li>▼ (詞証明書の管理</li> <li>(詞 証明書)</li> <li>(詞 証明書プロファイル</li> <li>(品 OCSP レスポンダ)</li> </ul>	□ 名前				場所			証明
☆ SSL/TLS サービス プロファイル は SCEP 合 SSL 復号化例外	b)							
© いらくーク 値 ログ設定 ▼ <sup>(2)</sup> サーバー プロファイ II.	C) ❶ 追加	<b>ヨ</b> 削除 🚳 コ t	2— 🖹 PDF/CSV	I				

(2) Portal と External-Gateway 用の SSL/TLS サービスプロファイルを生成します。
 a)名前に「External\_SSL\_Service\_Profile(任意)」と入力します。
 b)証明書は作成済みの「External-Gateway」を選択します。
 c)「OK」をクリックします。

SSL/TLS サービス プロ	コファイル 💿
名前 Exte	rnal_SSL_Service_Profile a)
証明書 Exte	rnal-Gateway b) 👻
プロトコル設定	
最小バージョン TLS	iv1.0
最大バージョン Max	x 💌
	C) OK キャンセル

(3) Internal-Gateway 用の SSL/TLS サービスプロファイルを生成します。
 a)名前に「Internal\_SSL\_Service\_Profile(任意)」と入力します。
 b)証明書は作成済みの「Internal-Gateway」を選択します。
 c)「OK」をクリックします。

SSL/TLS サービス	プロファイル	0				
名前	Internal_SSL_Service_Profile	a)				
証明書	証明書 Internal-Gateway					
プロトコル設定						
最小バージョン	TLSv1.0	-				
最大バージョン	Max	-				
		t + 2 + 1				
		44700				

# 7.5. Gatewayの設定

2つの Gateway (External と Internal) を設定します。

7.5.1. External Gatewayの設定

インターネット側から VPN 接続する対象となる Gateway の設定です。

(1) a)「Network」 →「GlobalProtect」の下の b)「ゲートウェイ」 → c)「追加」をクリックします。

paloalto	Dashboard	ACC Monitor	Policies Objects N	etwork Device		å⊐≤:	ット 省 🖓 Config - 🔍 検索
							5 のヘルプ
ゴンターフェイス	٩						0個の項目s → 🗙
■ ワーン ● 仮想ルーター ● IPSec トンネル	🗖 名前	場所	ローカル インターフェ ス	イ ローカル IP	トンネル	最大ユーザー	情報
上 DHCP のNS プロキシ							
▼ SolobalProtect	4						
	4						
日 クライアントレス アプリ つライアントレス アプリ つライアントレス アプリ つライアントレス アプリ	c)						
- 0oc	書追加 □ 削除 ■	2 PDF/CSV					

(2) a)「全般」タブで、b)名前に「External-Gateway(任意)」と入力します。
 c)インターフェイスは「ethernet1/1」を選択します。
 d)IPv4 アドレスは「10.9.1.4/24」を選択します。

GlobalProtect ゲー	トウェイ設定					0
全般 自	名前	External-Gateway	b)			
認証	ネットワーク設定					
エージェント	インターフェイス	ethernet1/1		c)		
	IP アドレス タイフ	IPv4 Only				~
サテライト	IPv4 アドレス	10.9.1.4/24		d)		
				/		
					ОК	キャンセル

(3) a)「認証」タブで、b)SSL/TLS サービスプロファイルで設定済みの「External\_SSL\_Service\_Profile」を選択します。
 c)「追加」をクリックします。



(4) a)名前に「ADAuth(任意)」と入力し、b)認証プロファイルは設定済みの「Auth-Profile01」を選択します。
 c)「OK」をクリックします。

GlobalProtect グー	トウェイ設定	0
全般	サーバー認証	
認証	SSL/TLS サービス プロフ External_SSL_Service_Profile	-
エージェント	クライアント認証 💿	
- ) - ) - ) - · · ·	クライアン 名前 ADAuth a)	
サテライト	S Any マ	ラベル 認証メッセージ
	認証プロファイル Auth-Profile01 b) マ	
	GlobalProtect アプリのログイン画面	
	ユーザー名のラベル Username	
	パスワードラベル Password	
	認証メッセージ Enter login credentials	
	認証メッセージの長さは最大 256 文字です。	
	● 注加 ( C) OK キャンセル	
	証明書プロファイル WIN2012-CA-Profile	-
		OK キャンセル

(5) a)「エージェント」タブ → b)「トンネル設定」タブで、c)「トンネルモード」にチェックを入れ、「tunnel.1」を選択します。
 d)「IPSec の有効化」にチェックが入っていることを確認します。
 このことで、SSL-VPN よりも IPSec が優先的に使われます。

GlobalProtect ゲー	-トウェイ設定	ଡ
全般	b) トンネル設定 Timeout Settings クライアント IP プール クライアントの設定 ネットワークサービス	動
認証 エージェント名	() <sup>22</sup> トンネル モード C)	
サテライト	トンネルインターフェイ tunnel.1	×
	撮大ユーザー」[1 - 500] ✓ IPSec の有効化 d)	
	GlobalProtect の IPSec 暗  default 号	~
	□ X-Auth サポートの有効化 グループ名	
	グループパスワード	
	■ IKE キー再生成での認証をスキップ	
	OK <b>**</b> *	セル

(6) a)「エージェント」タブ → b)「クライアントの設定」タブで、c)「追加」をクリックします。



(7) a)「認証オーバーライド」タブで、b)名前に「Auth-Override(任意)」と入力します。

GlobalProtect ゲートウェイ設定					0
全般 トンネル設定 Timeout	Settings クライア:	ントアプール	クライアントの設定	ネットワークサービス	重
				0	×
エー 認証オーバーライド ユーザー/	ユーザー グループ	IP プール	トンネルの分割		ð
名前 Auth-Override	b	)		]	
認証オーバーライド	クッキーを生成し.7	「認証」を			
	クッキーを至成して     クッキーを受け入れ	いて認証上書さ			
Cookle 有効期間		* 24			
クッキーの暗号化/復号化用の証明	None			-	
				OK キャンセル	
				OK キャン	セル

(8) a)「IP プール」タブ → b)「追加」をクリック → c)プールアドレス「172.16.1.1-172.16.1.99」と入力します。
 この IP アドレスが、GP Agent の VPN 確立後、クライアント PC の VPN インターフェイスに割当てられます。
 d)「OK」をクリックします。



(9) a)「エージェント」タブ → b)「ネットワークサービス」タブで、c)プライマリ DNS に「10.9.2.5」と入力します。
 この設定が、GP Agent の VPN 確立後、クライアント PC の VPN インターフェイスに割り当てられます。
 d)「OK」をクリックします。

GlobalProtect ゲ-	-トウェイ設定					0
全般	トンネル設定	Timeout Settings	クライアント IP プール	クライアントの設定	<b>b)</b> ネットワークサービス	重
asan エージェント <sup>6</sup>	継承ソース (離)	None 、 継承ソース状態	のチェック			-
サテライト	プライマリ DNS	10.9.2.5	c)			-
	セカンダリ DNS	None				~
	プライマリ WINS	None				~
	セカンダリ WINS	None				-
		🗌 DNS サフィック	スの継承			
	DNS サフィックス	クライアントの DM	IS サフィックスをカンマ区切り	)で入力 (例: hr.mycompany.	com, mycompany.com)	
					d) ок ≠+>+	ะม

## 7.5.2. Internal Gatewayの設定

社内 LAN から GP Agent が接続する Gateway の設定です。 VPN トンネルは確立しないのが特徴です。(VPN トンネルを確立する設定も可能です。)

(1) a)「Network」 →「GlobalProtect」の下の b)「ゲートウェイ」 → c)「追加」をクリックします。



(2) a)「全般」タブで、b)名前に「Internal-Gateway(任意)」と入力します。
 c)インターフェイスは「ethernet1/2」を選択します。
 d)IPv4 アドレスは「10.9.2.4/24」を選択します。



(3) a)「認証」タブで、b)SSL/TLS サービスプロファイルで設定済みの「Internal\_SSL\_Service\_Profile」を選択します。
 c)「追加」をクリックして、d) External-Gateway と同様の方法で、認証サーバーを指定します。
 e)「OK」をクリックします。

GlobalProtect ゲー	-トウェイ設定						0
全般 認証 a)	サーバー認証 SSL/TLS サービス T	プロフ <mark>Internal_SSL</mark> ァイル	Service_Profile	b)			•
エージェント サテライト	クライアント認証			ユーザータのラベ			
	<ul> <li>名前</li> <li>ADAuth</li> </ul>	OS Any	認証プロファイル Auth-Profile01	Username	パスワードラベル Password	認証メッセー Enter login credentials	.9 d)
	€) ●追加 ■ 削除	<b>⊙</b> ⊐ピー 읍上へ	●下へ				
	証明書プロフ:	ァイル None					•
					e) 📃	ОК <b>+</b> †	ンセル

(4) 「コミット」を実施します。

## 7.6. 内部 DNS の設定

Portal 設定の前に、内部 DNS の設定を行います。

GP Agent は、自身が今いる場所が外部か内部かの特定や、Gatewayのサーバー証明書の CN と自身が接続しようとしている宛先 FQDN が一致しているかどうかをチェックする際に DNS を利用するので、DNS 設定にも注意を払う必要があります。

本ガイドでは、Win2012を内部 DNS として利用しており、Internal Gateway との接続時には、この DNS が正しく設定されている必要があります。

#### 7.6.1. DNS の逆引き設定

GP Agent は、現在外部にいるのか内部にいるのかの判断をするために、DNS の逆引きを利用します。 GP Agent が Portal にアクセスした際に、Portal から DNS 逆引き用 IP アドレスを受け取り、その IP アドレスの逆引きが 成功することによって、GP Agent は、「内部にいる」と判断します。

よって、内部 DNS が逆引きに応答できるように設定しておきます。

- (1) Win2012 で、「Administration Tools」→「DNS」を選択します。
- (2) 表示された DNS Manager で、a)「Reverse Lookup Zones」を右クリック → b)「New Zone」を選択します。



(3) a)「Primary zone」を選んで、b)「Next」をクリックします。



(4) a)「To all DNS servers running on domain controllers in this domain」を選択して、b)「Next」をクリックします。

New Zone Wizard
Active Directory Zone Replication Scope You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated: O To all DNS servers running on domain controllers in this forest: acme.com
$\odot$ To all DNS servers running on domain controllers in this domain: acme.com <sup>a)</sup>
O To all domain controllers in this domain (for Windows 2000 compatibility): acme.com
○ To all domain controllers specified in the scope of this directory partition:
× .
< Back Next > b) Cancel

(5) a)「IPv4 Reverse Lookup Zone」を選択して、b)「Next」をクリックします。



(6) a)Network ID を選択して、「10.9.2.」と入力し、b)「Next」をクリックします。

New Zone Wizard
Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names.
To identify the reverse lookup zone, type the network ID or the name of the zone.          Network ID:       a)         10       9       a)         Network ID:       a)         The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.         If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa         Reverse lookup zone name:       2.9, 10.in-addr.arpa
< Back Next > b) Cancel

(7) a)「Allow only secure dynamic updates」を選択して、b)「Next」をクリックします。



(8) a)「Finish」で完了です。



# 7.6.2. DNS の正引き設定

GP Agent が Internal Gateway へ接続する際には、Internal Gateway が持つサーバー証明書の Common Name: 「trust.acme.com」と、GP Agent が Portal から受け取った Internal Gateway の FQDN が一致する必要があります。

そのためには、GP Agent が「trust.acme.com」の DNS 問合せを行い、その IP アドレス解決ができる必要があるので、その設定を行います。

(1) DNS Manager で、a)「acme.com」を右クリック → b)「New Host (A or AAAA)」を選択します。



- (2) a) Name に「trust」と入力します。
  - b) IP address に「10.9.2.4」と入力します。
  - c) 逆引き生成するために「Create associated point (PTR) record」にチェックを入れます(必須ではありません)。
  - d)「Add Host」をクリックします。

New Host	x
Name (uses parent domain name if blank):	
trust	a)
Fully qualified domain name (FQDN):	_
trust.acme.com.	
IP address:	
10.9.2.4	D)
Create associated pointer (PTR) record	c)
Allow any authenticated user to update DNS records with the same owner name	:
d) Add Host Cancel	

(3) a)「OK」をクリックします。



(4) Win2012 で、「Administration Tools」→「Services」を選択して起動します。
 一覧から「DNS Server」を見つけ出し、右クリックして「Restart」を選択して、サービスを再起動します。

#### 7.6.3. 内部 DNS ゾーンの確認

設定された DNS ゾーン内容を確認しておきます。

(1) 逆引きゾーンの確認

本ガイドでは、逆引きは「10.9.2.5 Pointer (PTR) win2012.acme.com」を使います。

Å	DNS Manager						
File Action View Help							
🗢 🏟 🖄 📰 🗙 🗊 🍳 🗟 🚺 🚦 🕯	Ĩ						
DNS DNS	Name	Туре	Data	Timestamp			
⊿	(same as parent folder)	Start of Authority (SOA)	[12], win2012.acme.com.,	static			
Forward Lookup Zones	🗐 🗐 (same as parent folder)	Name Server (NS)	win2012.acme.com.	static			
Reverse Lookup Zones	10.9.2.4	Pointer (PTR)	trust.acme.com.	static			
2.9.10.in-addr.arpa	10.9.2.5	Pointer (PTR)	win2012.acme.com.	static			

#### (2) 正引きゾーンの確認

本ガイドでは、Internal Gateway への接続に、「trust.acme.com: 10.9.2.4」を使います。

DNS Manager							
File Action View Help	File Action View Help						
🚊 DNS	Name	Туре	Data 📩	Timestamp			
⊿ 📋 Win2012	ForestDnsZones						
🔺 🚞 Forward Lookup Zones	📔 DomainDnsZones						
Image:	🔲 _udp						
⊿ 🛐 acme.com	📋 _tcp						
▷ iii _msdcs	🚊 _sites						
▷ ites	msdcs						
⊳ 🛄 _tcp	🗐 trust	Host (A)	10.9.2.4	static			
▷ iii _udp ▷ iii DomainDnsZones	win2012	Host (A)	10.9.2.5	static			

(3) [参考] 本ガイドでは、Portal および External Gateway の FQDN:「gp011.japaneast.cloudapp.azure.com」への 接続時に参照する外部 DNS は、Azure の公開 DNS を利用します。

## 7.6.4. Portal の設定

GP Agent が最初にアクセスする、Portal の設定を行います。

(1) a)「Network」 → 「GlobalProtect」の下の b)「ポータル」 → c)「追加」をクリックします。

paloalto		Dashboard	ACC	Monitor	Policies	Objects	Network	Device		占 コミット 🧉	' 闷 Config 🗸 🔍 検索
											ら のヘルブ
インターフェイス	٩										0個の項目s → 🗙
I <sup>III</sup> ソーン ⊕ 仮想ルーター <sup>III</sup> IPSec トンネル		2 名前	場	所	インター	フェイス	IP	SSL/TLS サービス: ロファイル	プ認証プロファイル	証明書プロファイル	情報
DHCP DNS プロキシ											
マ SolobalProtect SolobalProtect SolobalProtect ト)	4										
	6	;)									
🔊 デバイス ブロック リス	<b>æ</b> ;	自加 🛛 削除 🍕	デケットの	主成 📴 PDF/CSV							

(2) a)「全般」タブで、b)名前に「Portal(任意)」と入力します。
 c)インターフェイスは「ethernet1/1」を選択します。
 d)IPv4 アドレスは「10.9.1.4/24」を選択します。

GlobalProtect ポー	-タルの設定		0
全般 a)	名前	Portal b)	
認証	ネットワーク設定		
エージェント	インターフェイス	ethernet1/1 C)	~
	IP アドレス タイプ	IPv4 Only	~
クライアント	IPv4 アドレス	10.9.1.4/24 d)	~
サテライト	Appearance		
	ポータルのログイン ペ	factory-default	-
	-9		
	ポータルのランディン グ ページ	factory-default	~
	アプリケーションのへ	None	~
	ルプ ページ		
		OK <b>#</b> *>	セル

(3) a)「認証」タブで、b)SSL/TLS サービスプロファイルで「External\_SSL\_Service\_Profile」を選択します。
 c)「追加」をクリックします。

GlobalProtect ポー	タルの設定	0
全般	サーバー認証	
<sub>認証</sub> a)	SSL/TLS サービス プロフ External_SSL_Service_Profile b)	~
エージェント	クライアント認証	
サテライト	■ 名前 OS 認証プロファイル ユーザー名のラ パスワードラペ ペル ル	認証メッセージ
	<ul> <li>C)</li> <li>● 削除 ③ コピー ● 上へ ● 下へ</li> </ul>	
	証明書フロファイル None	•
		K キャンセル

(4) a)名前に「ADAuth(任意)」と入力し、b)認証プロファイルは設定済みの「Auth-Profile01」を選択します。
 c)「OK」をクリックします。

GlobalProtect ポー	タルの設定	0
全般	サーバー認証	
認証	ssL/n クライアント認証 🛛 🕥	<b>v</b>
エージェント	名前 ADAuth a)	
カライアントレ	クライ OS Any マ	54 
7747214	a 認証プロファイル Auth-Profile01 b)	べ 認証メッセージ
サテライト	GlobalProtect アブリのログイン画面	_
	ユーザー名のラベル Username	
	パスワードラベル Password	
	認証メッセージ Enter login credentials	
	認証メッセージの長さは最大 256 文字です。	
	C) OK キャンセル	
	証明書プロファイル None	v
Lar		OK キャンセル

(5) a)「エージェント」タブで、b)「追加」をクリックします。

GlobalProtect ポー	-タルの設定			Ø
全般	エージェント			
認証	🔲 設定 コ	ーザー/ユーザー グループ	OS 外部ゲートウェイ	クライアント証明
エージェント	a)			
クライアントし				
サテライト				
	b)			
	●追加 ●削除 ⊙コピ	ר ער ער ער ש		
	🔲 信頼されたルート CA	ローカルルート証明書ス トアでインストール	エージェント ユーザーのオーバ ーライド キー	
			再入力 エージェント ユーザーの オーバーライド キー	••••
	●追加 ■ 削除			
				OK キャンセル

(6) a)「認証」タブで、b)名前に「GP-Agent (任意)」と入力します。

設定					0					
認証	ユーザー/ユーザー グル	ープ 内部 外部	ß アプリケーション	データ収集						
a)	名前	GP-Agent	b)							
	クライアント証明書	None	<b>v</b>							
		秘密鍵など、選択した	クライアントの証明書は、ク	ワライアントマシンにインストーノ	しされます。					
	ユーザー認証情報の保存	Yes			~					
認証オーバーライド										
	□ クッキーを生成して認証上書き									
		🗌 クッキーを受け入れ	て認証上書き							
	Cookie 有効期間		▼ 24							
クッ	キーの暗号化/復号化用の証	None			<b>v</b>					
	明音									
ダイナ	トミック バスワード(2要素認	証)を必要とするコンホ	(ーネント							
	ポータル			□ 外部ゲートウエイ-マニュア	ルのみ					
	内部ゲートウ	エイ-全部		── 外部ゲートウエイ-自動検出						
保存し オプシ	た認証情報を使用するのでは ョンを選択してください。それ	ょく、ユーザーを認証す れにより、常に選択した	るには、ワンタイムパスワ- オプションごとに新たな認言	ード(OTP)などのダイナミックパス 証情報の入力を求めるメッセージ	マードを使用する が表示されます。					
				O	キャンセル					

- (7) a)「内部」タブをクリックします。
  - GP Agent が社内 LAN に接続されていることを検出するために、内部 DNS の逆引きを利用しますが、その設定をこの「内部ホスト検出 IPv4」で行います。
  - b)「内部ホスト検出 IPv4」にチェックを入れます。
  - c) 内部 DNS の逆引きができる IP アドレス「10.9.2.5」を入力します。
  - d) 内部 DNS の逆引きで返答されるホスト名「win2012.acme.com」を入力します。
  - e)「追加」をクリックします。

- グループ	内部	外部	アプリケーション	データ収集	
D)	a)		○ 内部ホスト検	± IPv6	
			C) IP アドレス	z	
.acme.com			d) ホストキ	3	
アドレス			送信元 IP		DHCP オプション 43 コ
					サブオブション コード を指定します (10進 数)。GlobalProtetエ ージェントは、サブオ ブションコードで定義 された値からゲートウ ェイアドレスを読み込 みます。
					+ 追加 ■ 削除
	- グルーフ つ) acme.com アドレス	- グループ 内部 a) acme.com アドレス	- グループ 内部 外部 acme.com アドレス	- グルーフ 内部 外部 アブリケーション つ) a) C) acme.com d) アドレス 文信元 IP メ信元 IP	- グループ 内部 外部 アプリケーション データ収集 a)

(8) a)名前に「trust.acme.com(任意)」と入力します。
 b)アドレスは「FQDN」を選択し、「trust.acme.com」と入力します。
 ※この FQDN が、Internal Gateway 用 SSL/TLS サービスプロファイルに設定したサーバー証明書の Common Name と一致する必要があります。
 c)「OK」をクリックします。

設定			
◎ 内部ホスト検出 IPv4	デーグループ 内部 外部 アプリゲーション   内部ゲートウェイ		
ホスト名 win20	名前 trust.acme.com アドレス ● FQDN ○ IP	a) b)	
日本前	trust.acme.com 送信元アドレス A		HCP オプション 43 コ - ド
	アドレスを選択するか IP サブネットまたは範囲を入力 (e.g 192.168.75.1-192.168.75.100)	. 192.168.74.0/24,	ナプオプション コード E指定します (10 進 纹)。 GlobalProtectエ -ジェントは、サプオ プションコードで定義 さわた 伝わらゲートゥ
	<ul> <li>● 潮除</li> <li>C)</li> </ul>	DK キャンセル	cイアドレスを読み込 cイアドレスを読み込 yます。
●追加●割除●			追加 O Nith
			OKキャンセル

- (9) a)「外部」タブをクリックします。
  - b)「追加」をクリックします。
  - c) 名前に「External-Gateway(任意)」と入力します。

d) FQDN を選択し、「gp011.japaneast.cloudapp.azure.com」と入力します。

※この FQDN が、External Gateway 用 SSL/TLS サービスプロファイルに設定したサーバー証明書の Common Name と一致する必要があります。

e)「送信元地域」で「Any」を選択します。

f)「OK」をクリックします。

設定		0
認証 ユーザー/ユ- カットオフ時間(秒) 5	ーザーグループ 内部 外部 アプリケーション データ収集 a)	
外部ゲートウェイ	外部ゲートウェイ ⑦	
■ 名前	名前 External-Gateway アドレス ● FQDN ○ IP	1
<b>b)</b> ● 追加 ■ 別際 サードパーティ VPN	☑ Any Highest ⊖)	
● 油加 ● 副務	● 追加 ● 削除	J
	f)     ок     ++>       ++>       0K       ++>       ++>       ++>       0K       ++>       ++>       ++>       0K       ++>	zJL

- (10) a) 「アプリケーション」タブをクリックします。
  - b) ウェルカムページで「factory-default」を選択します。

設定									0	
認証	E ユーザー/ユーザーク	<b>バ</b> ループ	内部	外部	アフ	プリケーション	データ収集			
- <b>7</b> -	プリケーション設定					<b>ロ</b> ) ウェル	カム ページ facto	ory-default	b) 🚽	
接	続手段	User-logor	(Always	On)		GlobalProtect	アプリの無効化			
GI 新	obalProtect アプリ設定の更 間隔 (時間)	24 [1 - 16	8]				パスコード			
국	ーザーが GlobalProtect アプ を無効化できるようにする	Allow				再入力	パスコード			
コリう	ーザーが GlobalProtect アプ をアップグレードできるよ にする	Allow with Prompt				無効にでき	る最大回数 0			
シ (V	シングルサインオン Yes (Windows のみ)の使用				タイムアウトの無効化(分)					
日認み	ログアウト時にサインオンの Yes 認証情報を消去 (Windows の み)			fes			Mobile Security Manager の設定			
ケ デ (V	ルベロス認証の失敗時には フォルトの認証を使用 Vindows のみ)	Yes				2/17/242	-ジャ			
VF ウ	N接続の自動復元タイムア ト時間(分)	30 [0 - 18	0]				登録ポート 443	3	~	
VE	№ 接続回復の試みの間の待	5 [1 - 60]								
								OK <b>‡</b> †	ンセル	

- (11) a)「データ収集」タブでは、何も設定しません。
  - b) HIP データの収集が有効になっていることを確認します。
  - c)「OK」をクリックします。

設定 で
認証 ユーザー/ユーザーグループ 内部 外部 アプリケーション データ収集
カテゴリの除外 カスタムチェック
Q ① 個の項目s ● 2
■ カテゴリ ペンダー
● 追加 ● 削除
C) OK キャンセル

(12) a)「追加」→ b)信頼されたルート CA に、生成済みの「PA-Certificate-Authority」を選択し、c)「ローカルルート証明 書ストアでインストール」にチェックを入れます。 d)「OK」をクロックレます。

d)「OK」をクリックします。

GlobalProtect ポー	タルの設定				ଡ			
全般	エージェント							
認証	■ 設定	ユーザー/ユーザー グループ	os	外部ゲートウェイ	クライアント証明 書			
エージェント	GP-Agent	any	any	External-Gateway				
クライアントし								
サテライト								
	●追加 ●削除 😒	1 <b>2- 8</b> 14 874						
	■ 信頼されたルート C	A ローカルルート証明書	ス エージ	エージェント ユーザーのオーバ ••••				
	PA-Certificate-Autho	rityb)	C) = 1 +	ーフ1 ト +ー リエージョント フーザーの				
			-/ 1977.	オーバーライド キー				
			- 11					
				d)	OK キャンセル			

※ この設定をするだけで、GP Agent がインストールされたクライアント PC(Windows)の「信頼されたルート証明書発行 機関」フォルダ(macOS の場合は「キーチェーンアクセス」)に、ルート証明書をインポートすることができます。

PA Firewall が生成した証明書以外のルート証明書であっても、ここに指定すれば、クライアント PC ヘインポートできます。(その場合は、そのルート証明書を事前に PA Firewall ヘインポートしておく必要があります。)

<sup>(13) 「</sup>コミット」を実施します。

# 7.7. ポリシーの設定

Trust→Untrust 方向の既存ポリシーに、Corp-VPN ゾーンを加えます。 Corp-VPN→Trust ゾーンへの通信も許可したいので、そのポリシーも追加します。

7.7.1. セキュリティポリシー

	-			-		送信元		5	统			
ーベースフォワ	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
	1 outbound C)	none	universal	(22) Trust	any	any	any	pag Untrust	any	any	any	⊘許可
ル検査 ケーション オー	2 intrazone-default 🍪	none	intrazone	any	any	any	any	(intrazone)	any	any	any	⊘ 許可
1 2321	3 interzone-default 🍪	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否

(2) a)「送信元」タブ → b)「追加」をクリックして、c)「Corp-VPN」ゾーンを追加します。



(3) a) は、outbound ポリシーの送信元ゾーンに、Trust と Corp-VPN の 2 つが設定された状態です。 加えて、b) のように、Corp-VPN→Trust 方向のポリシーも追加します。

						送信元			洗			
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サーピス	アクション
1	outbound	none	universal	Corp-VPN	any	any	any	🙉 Untrust	any	any	any	📀 許可
				ma Trust a								
2	VPN-to-Trust	none	universal	Corp-VPN	any	any	any	🚧 Trust	any	any	any	⊘許可 b)
3	intrazone-default 🥎	none	intrazone	any	any	any	any	(intrazone)	any	any	any	♥許可
4	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否

# 7.7.2. NAT ポリシー

NAT の outbound ポリシーにも、送信元ゾーンに Corp-VPN を加えて、PA Firewall 経由でインターネットへ通信できるようにし、「コミット」を実施します。

		Dashboard	ACC	Monitor	Policies	Objects	Network De	evice			
■ セキュリティ	•					元のパイ	- w K				<b>みパケット</b>
歳 QoS ■ポリシー ベース フォワ	名前	5	· グ 送信元ゾー	シ 宛先ゾー:	<ul><li>シ 宛先・</li></ul>	インターフェイス	送信元アドレス	宛先アドレス	サービス	送信元変換	宛先変換
首 復号 ▲ トンネル検査 Ⅲ アプリケーション オー 参 認証	1 outb	ound no	one paq Corp-Vi paq Trust	PN 🔎 Untrus	t any		any	any	any	dynamic-ip-and-port ethernet1/1 10.9.1.4/24	なし

# 7.8. GP Agent の設定

GP Agent をクライアント PC にインストールする際には、PA Firewall の Portal に Web ブラウザでアクセスし、PA Firewall からダウンロードします。

そのためには、事前に PA Firewall に GP Agent をダウンロード&アクティベーションしておく必要があります。

# 7.8.1. GlobalProtect Agent のダウンロード&アクティベーション

(1) a)「Device」  $\rightarrow$  b)「GlobalProtect クライアント」  $\rightarrow$  c)「今すぐチェック」 をクリックします。 現在リリースされている GlobalProtect Agent のバージョンの一覧が得られます。 本ガイドでは、d) 4.1.10 を利用することにします。アクション列の「ダウンロード」をクリックします。

paloalto	Dashboard	ACC Monitor	Policies Objects	Network De	evice		📥 コミット
TACACS+	۹.						
🌇 LDAP 🏝 Kerberos	パージョン 🔻	サイズ	リリース日	ダウンロード済み	現在アクティベーション 済み	アクション	
A マルチ ファクター認証	5.0.1	59 MB	2019/03/11 16:23:18			ダウンロード	リリース ノート
▽ □□ ローカル ユーザー データベー	5.0.0	58 MB	2019/02/11 14:22:59			ダウンロード ダウンロード	リリース ノート
<u>8</u> ユーザー	4.1.11	59 MB	2019/04/08 13:58:42				リリース ノート
🕵 ユーザー グループ	4.1.10	58 MB	2019/02/20 14:50:25			ダウンロード	リリース ノート 👌
📴 スケジュール設定されたログ	4.1.9	58 MB	2019/01/23 08:39:38			タワンロード	リリース ノート
® ソフトウェア	4.1.8	58 MB	2018/12/11 16:06:53			ダウンロード	リリース ノート
🕵 GlobalProtect クライアント b	4.1.7	58 MB	2018/11/27 06:18:49			ダウンロード	リリース ノート
🐏 ダイナミック史新	4.1.6	57 MB	2018/10/15 16:26:22			ダウンロード	リリース ノート
	4.1.5	57 MB	2018/09/10 12:47:13			ダウンロード	リリース ノート
<i>₽</i> サポート	4.1.4	57 MB	2018/08/06 17:42:34			ダウンロード	リリース ノート
	ら 今すぐチェック	📥 アップロード 📘 フ	ァイルからアクティベーション				

# (2) 「アクティベーション」をクリックします。

	Dashboard	ACC Monitor	Policies Objects	Network Dev	/ice		🍐 コミット
h TACACS+	•						
A CONTRACTOR	バージョン▼	サイズ	リリース日	ダウンロード済み	現在アクティペーション 済み	アクション	
Ing SAML アイテンティティ フ Ing マルチ ファクター認証	5.0.1	59 MB	2019/03/11 16:23:18			ダウンロード	リリース ノート
▽ □ ローカル ユーザー データベー	5.0.0	58 MB	2019/02/11 14:22:59			ダウンロード	リリース ノート
3 ユーザー	4.1.11	59 MB	2019/04/08 13:58:42			ダウンロード	リリース ノート
🕵 ユーザー グループ	4.1.10	58 MB	2019/02/20 14:50:25	✓		アクティベーション	リリース ノート
📴 スケジュール設定されたログ	4.1.9	58 MB	2019/01/23 08:39:38			ダウンロード	リリース ノート
◎ ソフトウェア	4.1.8	58 MB	2018/12/11 16:06:53			ダウンロード	リリース ノート
😢 GlobalProtect クライアント	4.1.7	58 MB	2018/11/27 06:18:49			ダウンロード	リリース ノート
🔁 ダイナミック更新	4.1.6	57 MB	2018/10/15 16:26:22			ダウンロード	リリース ノート
	4.1.5	57 MB	2018/09/10 12:47:13			ダウンロード	リリース ノート
ジサポート	4.1.4	57 MB	2018/08/06 17:42:34			ダウンロード	リリース ノート
🔒 マスター キーおよび診断	😋 今すぐチェック	📥 アップロード 📘 ファ	イルからアクティペーション				

#### (3) 「はい」をクリックします。



(4) 成功を示すメッセージが出たら、「閉じる」をクリックします。

# 7.8.2. クライアント PC への GP Agent のインストール

(1) a) GP Agent をインストールするクライアント PC (例:Windows10) から、Web ブラウザを使って、Portal (gp011.japaneast.cloudapp.azure.com) ヘアクセスします。
 b) Active Directory に登録されているユーザー名(例:w10-001)とパスワードを入力し「LOG IN」をクリックします。

GlobalProtect Portal × +	- 🗆 X
そ み C A 保護されていない通信 https://gp011.japaneast.cloudapp.azure.com/global-protect/login.esp a)	⊠ ☆ ❷ :
GlobalProtect Portal Usernam Passwor	

(2) OS 環境に合う GlobalProtect Agent をダウンロードします。この例では、Windows 64 bit 版を選択しています。



(3) ダウンロードした msi 形式ファイルを実行します。

## (4) 「Next」をクリックします。

🔀 GlobalProtect		-		$\times$
Welcome to the GlobalP	rotect Setuj	o Wizard	palo	alto
The installer will guide you through the st computer.	eps required to insta	ll GlobalProtect v4.1	.10 on your	
WARNING: This computer program is pro Unauthorized duplication or distribution or or criminal penalties, and will be prosecut	otected by copyright f this program, or any red to the maximum e	law and internationa y portion of it, may re extent possible unde	al treaties. sult in seve r the law.	re civil
	Cancel	< Back	Nex	t>

#### (5) 「Next」をクリックします。

🛃 GlobalProtect		-		×
Select Installation Folder	.,	<i>µ</i> ,	aloa	etworks.
The installer will install GlobalProtect to the following folder. To install in this folder, click "Next". To install to a different folder,	enter it belo	ow or cl	ick "Brow	ise".
zoider: C:\Program Files\Palo Alto Networks\GlobalProtect\		D	Browse isk Cost	
Cancel	< Back		Next	>

#### (6) 「Next」をクリックします。

( ) = =					
🛃 GlobalProtect			-		×
Confirm Installation			ul <sup>lu</sup>	oalog	alto
The installer is ready to install GlobalProte	ct on your compute	۲.			
Click "Next" to start the installation.					
	Cancel	< Back		Next	>

(7) ユーザー権限でログインしている Windows クライアント PC の場合、ここで管理者権限を求められます。
 管理者 ID およびパスワードの入力が必要です。

(8) 「Close」をクリックします。GP Agent のインストールは完了です。



(9) Windows10 へのインストールが完了すると、GP Agent は常駐プログラムとしてタスクトレイに入ります。

# 7.8.3. Portal & Gateway へのアクセス

イントールが完了した GP Agent から、まずは Portal、その後 Gateway へ接続できることを確認します。

7.8.3.1. Internal Gateway ヘログイン

社内 LAN 上の Windows10 (ユーザー: w10-003) から接続する例です。

(1) 表示された以下の GP Agent の画面で、a) Portal の FQDN:「gp011.japaneast.cloudapp.azure.com」を入力します。
 b)「Connect」をクリックします。



- (2) 初めて Portal にアクセスした際には、以下の「Server Certificate Error」が出ます。「Continue」をクリックします。
  - (Portal の設定で、Portal からルート証明書:「PA-Certificate-Authority」がインポートされるように設定したので、 2回目以降にこのエラーメッセージを見ることはありません。)

Server Certif	icate Error	×
	There is a problem with the security certificate, so the identity of gp011.japaneast.cloudapp.azure.com cannot be verified. Please contact the Help Desk for your organization to have the issue rectified. The communication with gp011.japaneast.cloudapp.azure.com may have been compromised. We recommend that you do not continue with this connection. Error details:	
	The gp011.japaneast.cloudapp.azure.com certificate is not signed by a trusted certificate authority.	
	Show Certificate Continue Cancel	

(3) Active Directory に登録されているユーザー名(例:w10-003)とパスワードを入力し「Sign In」をクリックします。

GlobalProte	ect >	<
	Sign In Enter login credentials	
	Portal: gp011.japaneast.cloudapp.azure.com	
	Password	
	Cancel Sign In	

(4) 内部接続(Internal-Gateway への接続)の場合には、a)のように「Connected - Internal」と表示されます。
 b)の Welcome メッセージは、初回は表示されますが、デフォルトで「Do not show this again」にチェックが入っているので、このチェックを OFF にしない限りは、2回目以降は表示されません。





 (6)「Connection」タブをクリックして、Internal-Gateway である「trust.acme.com」の Authenticated が「Yes」であることを 確認します。

(Internal Gateway の場合、「Connected - Internal」と表示されても、Internal Gateway へのログインができていない 場合があります。その場合、まずは内部 Gateway のサーバー証明書 CN の FQDN が、Portal の「エージェント」→ 「内部」タブの設定と一致しているかを確認してください。)

Copper					
neral Connec	tion Host Profile	Troubleshooting	Notification		
Gateway		Туре	Tunnel	Authenticated	
External-Gater	way	External	No		
trust.acme.com	n	Internal	No	Yes	
;ateway IP: ;ateway Locati Protocol: Jptime:	on:				
ytes In:		Bytes	Out:		
ackets In:		Packet	s Out:		
ackets I/Error:		Packet	s O/Error:		

(7) [確認のみ] PA Firewall で生成したルート証明書がインポートされていることを確認します。 例:Chrome ブラウザ →「設定」→「詳細設定」→「証明書の管理」で表示された画面で、「Trusted Root Certification Authorities」タブ内を確認します。



7.8.3.2. External Gateway へのログイン

インターネット上の Windows10 (ユーザー: w10-003) から接続する例です。

(1) 最初に Portal ヘログインする際に、Username と Password を入力したので、社外へ持ち出した場合は、デフォルト では、Username と Password を入力することなく、自動的に接続されます。



(2) [確認のみ]GP Agent の右上にある 🍄 をクリックして、「Settings」を選択します。

「Connection」タブをクリックして、以下の状態を確認します。

- External-Gateway で、Tunnel が Yes
- Assigned local IP:172.16.1.x (Pool 設定した IP アドレス)
- Protocol: IPSec

👂 GlobalProtect Se	ttings				
eneral Connection	Host Profile	Troubleshooting	Notification		
Gateway		Туре	Tunnel	Authenticated	
External-Gateway		External	Yes	Yes	
Assigned local IP: Gateway IP: Gateway Location: Protocol:	172. 2 IPSe	16.1.1 36 c			
Assigned local IP: Gateway IP: Gateway Location: Protocol: Uptime:	172. 2 IPSe 00:0	16.1.1 36 c 3:03			
Assigned local IP: Gateway IP: Gateway Location: Protocol: Uptime: 	172. 2 IPSe 00:0	16.1.1 36 c 3:03 883 Byte:	s Out:	419341	
Assigned local IP: Gateway IP: Gateway Location: Protocol: Uptime: Bytes In: Packets In:	172. 2 IPSe 00:0 1366 390	16.1.1 36 c 3:03 83 Byte: Pack	: Out: ets Out:	419341 680	

(3) 再接続して挙動を確かめたい場合には、GP Agent の右上にある をクリックして、「Refresh Connection」をクリックしてください。



GlobalProtect の基本的な設定は以上です。

# 7.8.4. [参考] GP Agent のアップグレード

GlobalProtect Agent を、4.1.10→4.1.11 ヘアップグレードする手順です。

#### 7.8.4.1. PA Firewall 側の準備

(1) a)「Device」  $\rightarrow$  b)「GlobalProtect クライアント」 で 4.1.11 をダウンロード後、c)「アクティベーション」をクリックします。

paloalto	Dashboard	ACC	Monitor Policies	Objects Network	Device	å-1	ミット 🧃 🕼 Config 🗸
NET WORKS	Daoinosaira	100		- Hotholik	a)		S
	•						78 個の項目
Kerberos	バージョン マ	サイズ	リリース日	ダウンロード済み	現在アクティベーション済み	アクション	
🍇 SAML アイテンティティ フ	5.0.1	59 MB	2019/03/11 16:23:18			ダウンロード	リリース ノート
▼ ◎ □ーカル ユーザー データベー	5.0.0	58 MB	2019/02/11 14:22:59			ダウンロード	リリース ノート
<u>8</u> ユーザー	4.1.11	59 MB	2019/04/08 13:58:42	<b>~</b>		アクティベーション C	リリース ノート
🕵 ユーザー グループ	4.1.10	58 MB	2019/02/20 14:50:25	¥	<b>v</b>	再アクティブ化	リリース ノート
🖻 スケジュール設定されたログ	4.1.9	58 MB	2019/01/23 08:39:38			ダウンロード	リリース ノート
<u>● ∀7+ ⇒= 7</u>	4.1.8	58 MB	2018/12/11 16:06:53			ダウンロード	リリース ノート
🔇 GlobalProtect クライアントD	4.1.7	58 MB	2018/11/27 06:18:49			ダウンロード	リリース ノート
1999 ダイナミック更新	4.1.6	57 MB	2018/10/15 16:26:22			ダウンロード	リリース ノート
	4.1.5	57 MB	2018/09/10 12:47:13			ダウンロード	リリース ノート
	4.1.4	57 MB	2018/08/06 17:42:34			ダウンロード	リリース ノート
□ マスダー キーおよび診断	😋 今すぐチェック	📥 アップロード	칠 ファイルからアクティベ	ーション			

#### (2) 「はい」をクリックします。

GlobalPr	otect クライアン	<mark>ィト バージ</mark> ョン 4.1	.11 のアクテ	ィベーション
?	これにより、次の GlobalProtect クラ ます。 続行します	D接続時に GlobalProte ライアント ソフトウェ すか?	ct ユーザーのコン アの新しいバー	ノビュータにダウンロードされる ジョンがアクティベーションされ
		はい	いいえ	

#### 7.8.4.2. クライアント側の動作

(1) クライアントが Gateway ヘ再接続した際に、以下の画面が出力されます。 「Yes」をクリックします。



(2) 数秒後に、以下のメッセージが出力されます。

「Yes」をクリックすると、新しい GP Agent が自動的にインストールされて、GP Agent の再起動が行われます。 よって、GP Agent のアップデートを行うクライアントは、一時的な通信停止を伴います。



## 7.8.5. [参考] GP Agent の挙動の変更方法

GP Agent の挙動を変更する方法について、記載しておきます。

例えば、GP Agent のデフォルトの挙動は、「User-logon(Always On)」となっており、Windows にログオンすると同時に、 常に PA Firewall に接続した状態を維持するようになっています。

この挙動を、「ユーザーが VPN 接続したい時だけ、手動で接続させるようにしたい。」という場合には、Portal の設定で変更することができます。

(1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリック → a)「アプリケーションタブ」で表示される以下の画面で、「接続手段」を b)「Ondemand (Manual user initiated connection)」に変更し、c)「OK」をクリックします。

設定		0
認証 ユーザー/ユーザー 2	ブループ 内部 外部	アプリケーション アプリケーション アプリケーション
アプリケーション設定		ウェルカム ページ factory-default
接続手段	On-demand (Manual user initiated connection)	D) GlobalProtect アプリの無効化
GlobalProtect アプリ設定の更 新問隔 (時問)	24 [1 - 168]	パスコード
ユーザーが GlobalProtect アプ リを無効化できるようにする	Allow	再入力 パスコード
ユーザーが GlobalProtect アプ リをアップグレードできるようにする	Allow with Prompt	無効にできる最大回数 0 タイムアウトの無効化(分) 0
シングルサインオン (Windows のみ)の使用	Yes	
ログアウト時にサインオンの 認証情報を消去 (Windows の み)	Yes	Mobile Security Manager の設定 モバイル セキュリティ マネ
ケルペロス認証の失敗時には デフォルトの認証を使用 (Windows のみ)	Yes	-ジャ 登録ボート 443 マ
VPN接続の自動復元タイムア ウト時間(分)	30 [0 - 180]	
unu initi mile a 243. a BB a (t	F.F. 203	
		C) OK キャンセル

- (2) 「コミット」を実施します。
- (3) クライアントが再ログインすると、「Disconnect」が現れるようになります。クリックすると切断されます。



(4) この設定によって、GP Agent が自動接続することなく、以下の状態で待機するようになります。 「Connect」をクリックすることで、接続できます。



# 8. クライアント証明書認証の設定

前セクションまでで設定したユーザー名とパスワードによる認証に加え、2要素目としてのクライアント証明書認証を追加 する方法を示します。

## 8.1. 全ユーザー共通のクライアント証明書で認証

簡易的な方法として、「全ユーザーが共通のクライアント証明書を持ち、そのクライアント証明書を持たないクライアントPC は接続させない」という設定を行います。

「各ユーザーにその共通クライアント証明書を配布して、インポート作業をしてもらう」というのも一つの手段ですが、その手間を省く目的で、GlobalProtectでは、「ユーザ名とパスワード認証の際に、同時にクライアント証明書を配布する」という機能が提供されていますので、その設定を行います。

#### 8.1.1. 全ユーザー共通のクライアント証明書の生成

(1) a)「Device」→「証明書の管理」の下の b)「証明書」→ c)「デバイス証明書」→ d)「生成」をクリックします。

	Dashboard ACC	Monitor	Policies	Objects	Network	Device			📥 🗆 3	ミット	e 🗋
▽ (肩証明書の管理 「尾 証明書 b) ● 証明書プロファイル	デバイス証明書	デフォルトの	信頼された証	明機関							3
禄 OCSP レスポンダ В SSL/TLS サービス プロファイル 国 SCEP ▲ SSL 復号化例外	□ 名前	<b>サ</b> フ	゚ジェクト		発行者		CA	+ -	有効期限	状態	アル ゴリ ズム
◎応答ページ	1 🔲 🔻 🙀 PA-Certifi	cate-Authority CN :	= PA-Certificate-	-Authority	CN = PA-	Certificate-Authority		7	Mar 27 08:16:22 2020 GMT	有効	RSA
▼ 1 サーバー プロファイル	Extern	al-Gateway CN gp0	= 1 <u>1 japaneas</u> t.clo	oudapp.azure.com	CN = PA-	Certificate-Authority		•	Mar 29 04:17:54 2020 GMT	有効	RSA
iii) SNMP トラップ iiii) Syslog	🗖 📮 Intern	al-Gateway CN	tru <mark>6</mark> .) cme.co	m	CN = PA-	Certificate-Authority		•	Mar 29 04:19:00 2020 GMT	有効	RSA
	■削除 無効化	更新 📥 インポート	👼 生成 🚢 🗄		-ト 📥 HA 🕈	ーのインポート 📥 HA:	キーのエク	スポー	– ト 📴 PDF/CSV		

(2) a)証明書名および共通名に「Common-ClientCert(任意)」と入力し、c)署名者に「PA-Certificate-Authority」を選択して、e)「生成」をクリックします。

証明書の生成		0
証明書タイプ	・ローカル O SCEP	
証明書名	Common-ClientCert	a)
共通名	Common-ClientCert	b)
署名者	PA-Certificate-Authority	🖵 C)
l í	認証局	
OCSP レスポンダ		-
▲ 暗号設定		
アルゴリズム	RSA	~
ピット数	2048	~
ダイジェスト	sha256	-
有効期限 (日)	365	
証明書の属性		
🔲 タイプ 値		
🖶 追加 🖃 削除		
	e) <sub>生成</sub> キャ	ンセル

(3) Gateway 用のサーバー証明書と同じ形で、クライアント証明書が生成されます。

	Dashboard ACC Monitor Policies Objects Network Device 🍰 コミット 🗗 😡 Config								
◎ セットアップ う 設定監査	デバイス証明書 デフォルト	の信頼された証明機関	_						
ペパスワード プロファイル 会 管理者								3 個の1	
20 管理者ロール	□ 名前	サブジェクト	発行者	CA	<b>+</b>	有効期限	状態	アルゴリズム	
22 23 23 23 23 23 24 24 24 24 24 24 24 24 24 24 24 24 24	PA-Certificate-Authority	CN = PA-Certificate-Authority	CN = PA-Certificate-Authority		<b>v</b>	Mar 27 08:16:22 2020 GMT	有効	RSA	
III ユーザー ID	External-Gateway	${\sf CN} = {\tt gp011.japaneast.cloudapp.azure.com}$	CN = PA-Certificate-Authority		<b>v</b>	Mar 29 04:17:54 2020 GMT	有効	RSA	
型VM 情報ソース	Internal-Gateway	CN = trust.acme.com	CN = PA-Certificate-Authority		7	Mar 29 04:19:00 2020 GMT	有効	RSA	
◇ 4回証明書の管理	Common-ClientCert	CN = Common-ClientCert	CN = PA-Certificate-Authority		<b>v</b>	Mar 29 05:48:03 2020 GMT	有効	RSA	
🔁 証明書プロファイル								••••••	

## 8.1.2. 証明書プロファイルの設定とGatewayへの割当て

証明書プロファイル設定し、それを Portal や Gateway に割当てることで、クライアント証明書認証が可能になります。 このプロファイルでは、クライアント証明書認証に使用する、証明書発行機関の証明書(ルート証明書)を指定します。

(1) a)「Device」→「証明書の管理」の下の b)「証明書プロファイル」→ c)「追加」をクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Object	s Netwo	rk Devid	e				
▽「眞証明書の管理	۹.						<u>a)</u>					
<ul> <li>○ IF III (日本)</li> <li>○ IF U スティント</li> <li>○ SSL/TLS サービス プロフ:</li> <li>○ SSL/TLS サービス プロフ:</li> <li>○ SSL 復長化例外</li> </ul>	■ 名前	場所	ユーザー名 フィールド	ユーザー ド メイン	名前	CA デフォルト OCSP URL	OCSP 検証証 明書	CRL の使用	OCSP の使用	CRL 受信の 有効期限	OCSP 受信の 有効期限	証明書の有 効期限
◎ 応答ページ ◎ ログ設定 ▼ ◎ サーバー プロファイル		t 🔞 בצ– 🛙	🔁 PDF/CSV									

(2) a)名前に「Common-ClientCert-Profile(任意)」と入力し、b)「追加」をクリックします。
 表示された画面で c)CA 証明書「PA-Certificate-Authority」を選択し、d)「OK」をクリックします。
 e)「OK」をクリックします。



(3) a)  $[Network] \rightarrow b)$  [f] f → c) [External-Gateway] [f] f → b) [f] f → c) [External-Gateway] [f] [f] [f] f → b) [f] [f]

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device			
V 😵 GlobalProtect	۹.									
$( \frac{6}{2} \pi - 9 \mu )$	🗌 名前		場所	F	コーカル インタ・	ーフェイス		ローカル IP	トンネル	
	🗉 🔲 External-Gat	eway C		e	thernet1/1			10.9.1.4/24	tunnel.1	
🔊 デバイス ブロック リスト	🗄 📄 Internal-Gate	eway	4	e	thernet1/2			10.9.2.4/24		
🖳 クライアントレス アプリ										
🕲 クライアントレス アプリ										

(4) a)「認証」タブ → b)証明書プロファイルで「Common-ClientCert-Profile」を選択し、d)「OK」をクリックします。

GlobalProtect ゲー	・トウェイ設定					
全般 認証 a) エージェント	<b>サーバー認証</b> SSL/TLS サービス プロ ァイ	フ External_SSL_Ser ル	vice_Profile			
サテライト	クライアント認証					
99 94 K	■ 名前	os	認証プロファイル	ユーザー名のラベ ル	パスワードラベル	認証メッセージ
	ADAuth	Any	Auth-Profile01	Username	Password	Enter login credentials
	🕂 追加 🕒 削除 💿	⊐K- €FV S	下へ			
	証明書プロファイ	Common-ClientCe	ert-Profile	b)		-
					c)	DKキャンセル

- (5) 同様の方法で、Internal-Gateway にも証明書プロファイルを割り当てます。
- 8.1.3. Portal から共通クライアント証明書を配布する設定
- (1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの Portal をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「ローカル」を選択し、c)「Common-ClientCert」を選択します。

設定							0
認証	ユーザー/ユーザー グル	ープ内部	外部	アプリケーション	データ収集		
a)	名前	GP-Agent			-		
	クライアント証明書	ローカル	þ	Common-ClientCe	rt	c)	~
		秘密鍵など、選	択したクライ	アントの証明書は、ク	ライアントマシン	にインストールされま	す。
	ユーザー認証情報の保存	Yes					<b>v</b>
BELLY	-/-21 5		成して認証し	- # ÷			
		クッキーを受	け入れて認証	-=c E上書き			
	Cookie 有効期間			▼ 24			
クッゴ	キーの暗号化/復号化用の証	None					~
	明書						
ダイナ	ミック バスワード(2要素認	証)を必要とする	らコンポーネン	v.h			
	□ ポータル				□ 外部ゲート	ウエイ-マニュアルのみ	
	内部ゲートウ	フエイ-全部			□ 外部ゲート!	ウエイ-自動検出	
保存した オプショ	と認証情報を使用するのでは ョンを選択してください。それ	なく、ユーザーを れにより、常に選	認証するには 択したオプシ	、 ワンタイムパスワー /ョンごとに新たな認証	-ド(OTP)などのダ E情報の入力を求る	イナミックパスワード かるメッセージが表示。	を使用する されます。
						d) <sub>ок</sub>	キャンセル

(2) 「コミット」を実施します。

## 8.1.4. GP Agent からのログイン(1)

GP Agent (例えば、w10-001, w10-002) から Portal ヘログインすると、Personal の証明書ストアへ、共通クライアント証明書がインポートされます。

[確認のみ] 例:Chrome ブラウザ →「設定」→「詳細設定」→「証明書の管理」で表示された画面で、「Personal」タ ブをクリックし、クライアント証明書がインポートされていることを確認します。

Certificates									>
Intended pu	irpose:	<all></all>							~
Personal	Other Peop	le Int	termediate Certifica	ation Au	thorities	Truste	ed Root (	Certification 4	ŀ
Issued 7	Го		Issued By		Expiratio	F	riendly N	Name	
Com	mon-ClientC	ert	PA-Certificate-Aut	thority	3/29/202	20 <	<none></none>		
Import	. Exp	ort	Remove					Advance	
									d
Certificate	intended p	urposes	3						d
Certificate Server Aut	intended pi	urposes , Client	s Authentication, IP	security	end syst	:em			d
Certificate	intended po thentication	urposes , Client	s Authentication, IP	security	end syst	em		View	d
Certificate Server Aut	intended p	urposes , Client	s : Authentication, IP	security	r end syst	em		View	d

## 8.1.5. 共通クライアント証明書配布の解除

GP Agent への共通クライアント証明書の配布が完了したら、配布設定を解除します。

 (1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「None」を選択し、 c)「OK」をクリックします。

設定			0
認証 ユーザー/ユ	ーザー グループ 内部	外部 アプリケーション	データ収集
<u>a)</u>	名前 GP-Agent		
クライ	アント証明書 None	b)	
	秘密鍵など、選択	したクライアントの証明書は、ク	ライアントマシンにインストールされます。
ユーザー認	証情報の保存 Yes		<b>v</b>
- 認証オーバーライド -			
	□ クッキーを生成	成して認証上書き	
	□ クッキーを受け	ナ入れて認証上書き	
Cod	kie 有効期間 Hours	▼ 24	
クッキーの暗号化/	復号化用の証 None		<b>v</b>
	明香		
ダイナミック パスワー	-ド(2要素認証)を必要とする:	コンポーネント	
	ポータル		□ 外部ゲートウエイ-マニュアルのみ
	内部ゲートウエイ-全部		□ 外部ゲートウエイ-自動検出
保存した認証情報を使 オプションを選択して	用するのではなく、ユーザーを読 ください。それにより、常に選折	8証するには、ワンタイムパスワー Rしたオプションごとに新たな認証	ド(OTP)などのダイナミックパスワードを使用する 情報の入力を求めるメッセージが表示されます。
			C) OK キャンセル

(2) 「コミット」を実施します。

8.1.6. GP Agent からのログイン(2)

クライアント証明書を配布されていないクライアント (例:w10-003) からは接続できません。



## 8.2. 各ユーザー個別のクライアント証明書で認証 (SCEP 利用による配布)

今度は、「各ユーザーが個別のクライアント証明書を持ち、そのクライアント証明書を持たないクライアント PC は接続させない」という設定を行います。

「各ユーザーに個別のクライアント証明書を渡して、インポート作業をしてもらう」というのも一つの手段ですが、その手間を 省く目的で、GlobalProtect では、SCEP (Simple Certificate Enrollment Protocol) を利用して、「ユーザ名とパスワード認 証と同時に、ユーザ毎のクライアント証明書を配布する」という機能が提供されていますので、その設定を行います。

8.2.1. SCEP サーバーのインストール

本ガイドでは、認証サーバーとして Win2012 の Active Directory を利用しているので、このサーバーを Certification Authority (認証局) として設定し、このサーバーから、ユーザー認証と同時にクライアント証明書を発行するのが効率的です。

Win2012 の Active Directory Certificate Services (以降、ADCS)は SCEP に対応しているので、その設定を行って利用 することにします。

#### 8.2.1.1. IIS のインストール

SCEP でクライアント証明書を発行する際に利用されるプロトコルは HTTP であり、Win2012 では IIS (Internet Information Service)が利用されます。よって IIS をインストールします。

(1) Win2012 の Server Manager で、「Add roles and features」をクリックします。



#### (2) 「Next」をクリックします。


### (3) 「Role-based or feature-based installation」を選択して、「Next」をクリックします。



(4) 本ガイドの構成は、Windows サーバーは一台なので、そのまま「Next」をクリックします。

2	Add Kol	es and Features	Wizard
Select destinati	on server		DESTINATION SERV Win2012.acme.co
Before You Begin Installation Type Server Selection	h to install roles and features.		
Server Roles	Server Pool		
Features Confirmation	Filter:		
	Name	IP Address	Operating System
	Win2012.acme.com	10.9.2.5	Microsoft Windows Server 2012 R2 Datacenter
	1 Computer(s) found This page shows servers	that are running Wi	indows Server 2012, and that have been added by using
	Add Servers command in	n Server Manager. O	Offline servers and newly-added servers from which data

(5) 「Web Server (IIS)」の先頭のチェックボックスをクリックします。





# (7) 「Next」をクリックします。



# (8) なにも選択せず、「Next」をクリックします。



# (9) 「Next」をクリックします。



# (10) デフォルトのまま、「Next」をクリックします。



# (11)「Install」をクリックします。



### (12) http://127.0.0.1 にアクセスして、IIS が動作することを確認します。



8.2.1.2. ADCS のインストール

ADCS にはいくつかの役割がありますが、ここでは以下2つが必要です。

- Certification Authority (以降、CA)
- Network Device Enrollment Service (以降、NDES)

加えて、以下も同時にインストールしておきます(\*)。

• Certification Authority Web Enrollment (以降、CAWE)

(\*) NDES インストール後に CAWE をインストールすると、Web ブラウザを使ったクライアント証明書発行機能が期待通 りに動作しませんでした(Web ブラウザで IIS ヘアクセスしても、ユーザー単位の認証画面が表示されませんでした)。 この 2 つの機能はどちらも、IIS の「Windows Authentication」を使うので、そこで何らかの問題が発生していると思わ れますが、この事象のトラブルシューティングは、本ガイドの本質ではないので、それ以上は追求しておりません。 [利用 OS]: Windows Server 2012R2 Version 6.3 (build 9600) そのため、CAWE は、後章の「スマートデバイスからの接続」で必要になりますので、先にインストールしておきます。

- (1) IIS と同様に、Win2012 の Server Manager で、「Add roles and features」をクリックします。
- (2) 以下の画面までは「Next」をクリックして進めます。

以下の画面で、「Active Directory Certificate Service」の先頭のチェックボックスをクリックします。

	Add Notes and reatures wizard	
Select server roles Before You Begin	Select one or more roles to install on the selected server.	DESTINATION SERVER Win2012.acme.com
Installation Type Server Selection Server Roles Features Confirmation Results	Active Directory Certificate Services       ^         Active Directory Certificate Services       ^         Active Directory Gederation Services       ^         Active Directory Rightweight Directory Services       ^         Application Server       DHCP Server         DHCP Server       *         > Im File and Storage Services (2 of 12 installed)       ^         Hyper-V       Network Policy and Access Services         Print and Document Services       *         Remote Access       *         Remote Desktop Services       *	Description Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	< Previous Next	> Install Cancel



# (4) 他は選択せず、「Next」をクリックします。



# (5) 何も選択せず、「Next」をクリックします。



77

# (6) 「Next」をクリックします。



(7) 「Certification Authority」に加え、まず、「Certification Authority Web Enrollment」にチェックを入れます。 Add Roles and Features Wizard



### (8) 「Add Features」をクリックします。

🚡 Add Roles and Features Wizard 🗙				
Add features that are required for Certification Authority Web Enrollment?				
You cannot install Certification Authority Web Enrollment unless the following role services or features are also installed.				
▲ Web Server (IIS)				
⊿ Web Server				
▲ Common HTTP Features				
HTTP Redirection				
▲ Health and Diagnostics				
Logging Tools				
Request Monitor				
Tracing				
▲ Application Development ∨				
Include management tools (if applicable)				
Add Features Cancel				

# (9) さらに「Networks device Enrollment Service」にもチェックを入れ、「Next」をクリックします。



## (10)「Install」をクリックします。



### (11)「Close」をクリックします。



# 8.2.2. NDES 用のアカウント設定

PA Firewall が各ユーザー個別のクライアント証明書を NDES に要求する際には、その権限を持つアカウントの設定が必要です。

NDES を設定する際にも、その権限アカウントが要求されるので、事前に「panagent」に権限を設定しておきます。

(1) Win2012 の「Administrative Tools」→「Active Directory Users and Computers」を開きます。
 「acme.com」→「Users」で、設定済みの「panagent」をダブルクリックします。

pan agent Properties ? X					
Membe	r Of	Dial-in	Envi	ronment	Sessions
General	Address	Account	Profile	Telephones	Organization
User logor	n name:				
panagent	1		@acme	.com	~
User logor	n name (pre-)	Windows 200	0):		
ACME\			panager	nt	
Logon	Hours	Log On T	o		
Account of Use	Unlock account  Account options:  User must change password at next logon User cannot change password Password never expires Store password using reversible encryption				
Account expires            Never             End of:        Saturday     May       18, 2019					
	OK Cancel Apply Help				

(2) そのアカウントの「Member of」タブで「Add」をクリックし、「IIS\_IUSRS」権限を加え、「OK」をクリックします。

pan agent Properties ? X					x	
Remote control	Remote D	Remote Desktop Services Profile			CO	M+
General Address	Account	Profile	Telephones	0	)rgani;	ation
Member Of	Dial-in	Env	vironment		Sessio	ns
Member of:						
Name	Active Directo	ory Domair	n Services Folde	er		
Domain Users	acme.com/U	sers				
IIS_IUSRS	acme.com/Bu	uiltin				
Server Operators	acme.com/Bu	uiltin				
						-
Add F	Remove					
						_
Primary group: D	omain Users					
	There is a		-h Dim			
Set Primary Group	you have	o need to Macintosh	change Primary clients or POS	IX-co	ip unie mpliar	t ss
	applications.					
		I	Annelia			
0	K C	ancel	Apply		He	eip

# 8.2.3. ADCS の設定

ADCS の CA と NDES のインストールが完了し、「panagent」へ必要な権限を付与しましたので、次は設定を行います。

8.2.3.1. CA の設定

- (1) Server Manager で警告を示すマークをクリックします。
  - 「Configure Active Directory Certificate Service on the destination server」をクリックします。



(2) 管理者権限を持つユーザーが選択されていることを確認して、「Next」をクリックします。



(3)「Network Device Enrollment Service」も同時にチェックを入れると、以下のように「Certification Authority」を先にインストールするように警告が出ますので、「Certification Authority」と「Certification Authority Web Enrollment」にだけチェックを入れて、「Next」をクリックします。



# (4) 「Enterprise CA」が選択された状態で、「Next」をクリックします。



(5)「Root CA」が選択された状態で、「Next」をクリックします。

<b>a</b>	AD CS Configuration		^
СА Туре	DESTINA Win20	TION SE 12.acm	RVER e.com
Credentials Role Services Setup Type CA Type Private Key	Specify the type of the CA When you install Active Directory Certificate Services (AD CS), you are creating or exter public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy ar own self-signed certificate. A subordinate CA receives a certificate from the CA above hierarchy.	ending a nd issue: it in the	s its 9 PKI
Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	<ul> <li>Root CA Root CAs are the first and may be the only CAs configured in a PKI hierarchy.</li> <li>Subordinate CA Subordinate CAs require an established PKI hierarchy and are authorized to issue of the CA above them in the hierarchy.</li> </ul>	ertificat	es by
	More about CA Type		
	< Previous Next > Configure	Can	cel

(6) 「Create a new private key」が選択された状態で、「Next」をクリックします。



(7)	本ガイドではデフォルト値を使います。「Next」をクリ	リック	します	•

<b>a</b>	AD CS Configuration	_ <b>_</b> ×
Cryptography for	CA	DESTINATION SERVER Win2012.acme.com
Credentials Role Services	Specify the cryptographic options	
Setup Type	Select a cryptographic provider:	Key length:
CA Type	RSA#Microsoft Software Key Storage Provider	2048 💌
Private Key Cryptography CA Name Validity Period Certificate Database Confirmation	Select the hash algorithm for signing certificates issued by this CA: SHA256 SHA384 SHA512 SHA1 MD5	
	Allow administrator interaction when the private key is accessed by More about Cryptography	by the CA.
	< Previous Next >	Configure Cancel

## (8) 本ガイドでは、表示された値をそのまま使います。「Next」をクリックします。

<b>A</b>	AD CS Configuration
CA Name	DESTINATION SERVER Win2012.acme.com
Credentials Role Services Setup Type	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is added to all
CA Type Private Key	certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified. Common name for this CA:
Cryptography CA Name	acme-Win2012-CA
Validity Period	Distinguished name suffix:
Certificate Database	DC=acme,DC=com
Confirmation	Preview of distinguished name:
Progress	CN=acme-Win2012-CA,DC=acme,DC=com
Kesuits	More about CA Name
	< Previous Next > Configure Cancel

(9) 本ガイドではデフォルト値を使います。「Next」をクリックします。



# (10) 本ガイドではデフォルト値を使います。「Next」をクリックします。

<b>b</b>	AD CS Configuration	_ <b></b> X
CA Database		DESTINATION SERVER Win2012.acme.com
Credentials Role Services	Specify the database locations	
Setup Type	Certificate database location:	
CA Type	C:\Windows\system32\CertLog	
Private Key	Certificate database log location:	
Cryptography	C:\Windows\system32\CertLog	
CA Name		
Validity Period		
Certificate Database		
Confirmation		
Progress		
Results		
	More about CA Database	
	< Previous Next >	Configure Cancel

# (11)「Configure」をクリックします。

<b>è</b>	AD CS Con	figuration	
Confirmation			DESTINATION SERVER Win2012.acme.com
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	To configure the following roles, Active Directory Certificat Certification Authority CA Type: Cryptographic provider: Hash Algorithm: Key Length: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location: Certificate Dat	role services, or features, click Conf e Services Enterprise Root RSA#Microsoft Software Key Storay SHA1 2048 Disabled 3/30/2024 4:10:00 PM CN=acme-Win2012-CA,DC=acme,I C:\Windows\system32\CertLog C:\Windows\system32\CertLog	igure. ge Provider DC=com
		< Previous Next >	Configure

# (12)「Close」をクリックします。

à	AD CS Configuration	_ <b>_</b> ×
Results		DESTINATION SERVER Win2012.acme.com
Credentials	The following roles, role services, or features w	vere configured:
Role Services	Active Directory Certificate Services	
Setup Type		
СА Туре	More about CA Configuration	Configuration succeeded
Private Key		• • • • • • •
Cryptography	Certification Authority Web Enrollment	Configuration succeeded
CA Name	More about web enforment configuration	
Validity Period		
Certificate Database		
Confirmation		
Progress		
Results		
	< Previous	Next > Close Cancel

# (13) 続けて NDES の設定を行いますので、「Yes」をクリックします。

AD CS Configuration	
Do you want to configure additional role services ?	
Yes No	

## 8.2.3.2. NDES の設定

### (1) 管理者権限を持つユーザーが選択されていることを確認して、「Next」をクリックします。 \_ 🗆 X AD CS Configuration DESTINATION SERVER Credentials Win2012.acme.com Credentials Specify credentials to configure role services Role Services To install the following role services you must belong to the local Administrators group: Standalone certification authority Certification Authority Web Enrollment Online Responder Online Kesponder To install the following role services you must belong to the Enterprise Admins group: Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service Network Device Enrollment Service Certification Admin Credentials ACME\admin-admin Change... More about AD CS Server Roles < Previou: Next > Configure Cancel

(2) 「Network device Enrollment Service」にチェックを入れて、「Next」をクリックします。



#### (3) 「Select」をクリックします。



### (4) Panagent の認証が必要です。パスワードを入力して、「OK」をクリックします。



(5) ACME¥panagent が選択された状態で、「Next」をクリックします。



(6) 本ガイドでは、Country/Region:で「JP(Japan)」を選択し、他はブランクのまま、「Next」をクリックします。



# (7) 本ガイドでは、デフォルト値を利用します。「Next」をクリックします。

i 🛍	AD CS Configuration								
Cryptography for	DESTINATION SERVER Win2012.acme.com								
Credentials Role Services Service Account for NDES	Configure CSPs for the RA	; (CSPs) and key lengths for							
RA Information	the signature and encryption keys.	Key length:							
Confirmation	Cryptography for NDES signature key provider Confirmation Microsoft Strong Cryptographic Provider 🔹								
Progress	Encryption key provider:	Key length:							
Nesults	Microsoft Strong Cryptographic Provider	2048							
	More about Cryptography for NDES								
	< Previous Next >	Configure Cancel							

#### (8) 「Configure」をクリックします。



### (9) 「Close」をクリックします。



### 8.2.3.3. NDES の動作確認

設定した NDES が動作することを確認します。

NDES 設定を行った Win2012 へ到達できる IP アドレスを持つ端末(例:w10-001)から、下記 Link ヘアクセスします。

http://win2012.acme.com/certsrv/mscep\_admin

#### (2) panagent アカウントでログインします。

win2012.acme.com/certsrv/mscep_ad × +		- 🗆 X
← → C ③ win2012.acme.com/certsn	r/mscep_admin/	☆ 😁 :
	ログイン       http://win2012.acme.com       このサイトへの接続ではプライパシーが保護されません       ユーザー名       パスワード       ログイン       キャンセル	

## (3) 以下のような画面が出力されれば、OK です。

Network Device Enrollment Servi × +	-		×							
	Image: Image	Θ	:							
Network Device Enrollment Service										
Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certific Protocol (SCEP).	ate Enrollr:	ment								
To complete certificate enrollment for your network device you will need the following information:	To complete certificate enrollment for your network device you will need the following information:									
The thumbprint (hash value) for the CA certificate is: EFE71552 52EA21E0 478599DC 42BC97F3										
The enrollment challenge password is: 026C52277AB4BA0C										
This password can be used only once and will expire within 60 minutes.										
Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.										
For more information see Using Network Device Enrollment Service.										

## 8.2.4. PA Firewall の SCEP 設定

SCEP を使って、PA Firewall が ADCS と接続し、GP Agent の各ユーザーに個別のクライアント証明書が配布できるまでの設定を行います。

### 8.2.4.1. サービスルートの変更

本ガイドの環境では、ADCS(Win2012)が Trust ゾーンに設置されているので、サービスルートを変更します。

 (1) a)「Device」→ b)「セットアップ」→ c)「サービス」→ d)「サービスルートの設定」で表示された画面で、e)のよう に、SCEPの送信元インターフェイスおよび送信元アドレスを eth1/2 に変更します。
 f)「OK」をクリックします。



(2) 「コミット」を実施します。

## 8.2.4.2. SCEP の設定

(1) a)「Device」→「証明書の管理」の下の b)「SCEP」→ c)「追加」をクリックします。

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	
▽ 뎙 証明書の管理	٩.							
■ 証明書 ■ 証明書プロファイル	🔲 名前				場所			CA-IDENT 名
₩OCSP レスポンダ								
iscep b)								
<ul> <li>SSL 復亏化例外</li> <li>応答ページ</li> </ul>	4							
■ ログ設定 マ 0 サーバー プロファイル								
SNMP トラップ	c)							
"I Sysiog	●追加	🛚 削除 💿 コピ	— 🖹 PDF/CSV	ı.				

- (2) a) 名前に「WIN2012\_SCEP(任意)」と入力します。ワンタイムパスワード(チャレンジ):
  - ウノダイムハスワート(ティレノン): い OOED エッレンジズ[ダノナニック」た 翌日
  - b) SCEP チャレンジで「ダイナミック」を選択します。
  - c) サーバーURL に「http://win2012.acme.com/certsrv/mscep\_admin/」と入力します。
  - d) ユーザー名:「acme¥panagent」と入力します。
  - e) パスワードおよび再入力パスワードに、panagent のパスワードを入力します。
  - 設定:

f) サーバーURL に「http://win2012.acme.com/certsrv/mscep/mscep.dll」と入力します。

- g) CA-IDENT 名に「WIN2012-CA(任意)」と入力します。
- 暗号設定:
- h) ビット数は「2048」を選択します。
- i) CSR のダイジェストは「sha1」を選択します。
- j)「OK」をクリックします。

SCEP 設定	0									
名前 WIN2012_SCEP a)										
ワン タイム パスワード (チャレンジ)										
SCEP チャレンジ ダイナミック b)	'イナミック b)									
サーバー URL http://win2012.acme.com/certsrv/mscep_admin/ C)										
ユーザー名 acme\panagent d)										
パスワード •••••••••• 再入力 パスワード •••••••	e)									
サーバー URL http://win2012.acme.com/certsrv/mscep/mscep.dll f)										
CA-IDENT & WIN2012-CA 9)										
サブジェクト CN=\$USERNAME										
サブジェクトの代替名タイプ None 🔍										
暗号設定										
ビット数 2048 h) CSR のダイジェスト sha1	i) 💌									
✓ デジタル署名として使用 ✓ 鍵の暗号化1	こ使用									
CA 証明書フィンガープリン										
۲.										
SCEP Server SSL Authentication										
CA 証明書 None マ クライアント証明書 None	~									
	OKキャンセル									

## 8.2.4.3. ルート証明書が自動的にインポートされたことの確認

[確認のみ] a)「Device」→「証明書の管理」の下の b)「証明書」をクリックします。 実施した SCEP 設定により、c) Win2012 の CA のルート証明書が自動的に取り込まれます。

maloalto						_							
NETWORKS®	Dashbo	oard ACC	Monitor	Policies	Objects	Network	Device					2	コミット 🧉 陽 Confi
<ul> <li>◎ セットアップ</li> <li>◎ 設定監査</li> <li>◆ パスワード プロファイル</li> <li>● 第四半</li> </ul>	5	デバイス証明書	デフォルトの	)信頼された証	明機関								4 佃の:
◎ 管理者ロール		名前		サブジェクト			発行者		CA	+-	有効期限	状態	アルゴリズム
総認証プロファイル 認証シーケンス		▼ 🗐 PA-Certificate	-Authority	CN = PA-Certifi	cate-Authority		CN = PA-Ce	rtificate-Authority			Mar 27 08:16:22 2020 GMT	有効	RSA
III ユーザー ID		External-G	ateway	CN = gp011.jap	oaneast.cloudap	p.azure.com	CN = PA-Ce	rtificate-Authority			Mar 29 04:17:54 2020 GMT	有効	RSA
<ul> <li>         VM 情報ソース      </li> </ul>		🚰 Internal-Ga	ateway	CN = trust.acm	e.com		CN = PA-Ce	rtificate-Authority			Mar 29 04:19:00 2020 GMT	有効	RSA
v ■証明書 b)		Common-C	ClientCert	CN = Common	ClientCert		CN = PA-Ce	rtificate-Authority			Mar 29 05:48:03 2020 GMT	有効	RSA
日 証明音プロファイル 同 CCSP レスポンダ		₩IN2012_SCI	EP	DC = com, DC	= acme, CN = a	cme-Win2012-CA	DC = com, acme-Win2	DC = acme, CN = )12-CA			Mar 30 07:16:52 2024 GMT	有効	<sup>RSA</sup> C)

# 8.2.4.4. 証明書プロファイルの設定

**n** paloalto

Win2012 のルート証明書を使った証明書プロファイルを設定します。

(1) a)「Device」→「証明書の管理」の下の b)「証明書プロファイル」→c)「追加」をクリックします。

NETWORKS <sup>®</sup>	Dashboard	ACC	Monitor	Policies	Objects	Ne	twork	Device						
▽ 🔓 証明書の管理	•													
同証明書										CA				
マ OCSP レスホンダ														
B SSL/TLS サービス プロファイル 国 SCEP	□ 名前				提研	ユーザ 一名フ	ユーザ	之前			デフォ ルト	OCSP 检亚亚	CRL の	OCSP
☐ SSL 復号化例外	12 12 199				~00171	ィール ド	イン	12.89			OCSP URL	明書	使用	の使用
◎ い合ペーシ □ ログ設定														
▽ 🗿 サーバー プロファイル	Comr	non-ClientCert-Pr	ofile					PA-Certificate-A	uthority					
Syslog														
🗟 電子メール 📑 HTTP	c)													
	🕂 追加	🖃 削除 🚳 コヒ	2— 📑 PDF/CS1	V										

- (2) a) 名前に「WIN2012-CA-Profile(任意)」と入力します。
  - b)「追加」をクリックして、c)「WIN2012\_SCEP」を選択します。
  - d)「OK」をクリックします。

証明書プロフ	ッテイル	0
名前	WIN2012-CA-Profile	a)
ユーザー名フ ィールド	None	
ユーザー ドメ イン		
CA 証明書	■ 名前 デフォルト OCSP URL ■ WIN2012_SCEP C) b)	OCSP 検証証明書
	● 追加 ● 削除	
	<ul> <li>デフォルト OCSP URL (http:// または https:// で開始する必要あり)</li> <li>CRLの使用</li> <li>CRL 受信の有効期限(秒) 5</li> <li>OCSP の使用</li> <li>OCSP か使用</li> </ul>	<ul> <li>証明書状態が不明な場合にセッション</li> <li>をプロック</li> </ul>
	CRLより OCSP を優先 証明書の有効期限(秒) 5	<ul> <li>タイムアウト時間内に証明書状態を取 得できない場合にセッションをブロッ ク</li> </ul>
		証明書が認証側デバイスに発行されな かった場合セッションをプロック
		<ul> <li>期限切れ証明書のセッションをプロック</li> </ul>
		d) ок <i>‡</i> +>>tu

## 8.2.4.5. Portal の設定

(1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「SCEP」を選択し、c)設定済みの SCEP 設定:「WIN2012\_SCEP」を選択します。

設定							0				
認証	ユーザー/ユーザー グル-	ープ内部	外部	アプリケーション	データ収集						
a)	名前	GP-Agent									
	クライアント証明書	SCEP		b) WIN2012_SCEP		C)	•				
		秘密鍵など、選	択したクラー	イアントの証明書は、ク	ライアントマシン	/にインストールされます。					
	ユーザー認証情報の保存	Yes					~				
認証オ	認証オーバーライド										
	I	🗌 クッキーを生	成して認証	E上書き							
	l	🗌 クッキーを受	け入れて認	き書き							
	Cookie 有効期間			▼ 24							
クッゴ	キーの暗号化/復号化用の証	None					-				
	明書										
ダイナ	ミック パスワード(2要素認識	証)を必要とする	5コンポーネ	シト							
	□ ポータル				□ 外部ゲート	ウエイ-マニュアルのみ					
	□ 内部ゲートウエイ-全部 □ 外部ゲートウエイ-自動検出										
保存した オプショ	た認証情報を使用するのではな ョンを選択してください。それ	ょく、ユーザーを ぃにより、常に選	認証するに 択したオプ	は、ワンタイムパスワー <sup>?</sup> ションごとに新たな認証	-ド(OTP)などのダ E情報の入力を求め	イナミックパスワードを かるメッセージが表示され	使用する lます。				
						OK ŧ	ャンセル				

(2) a)「アプリケーション」タブ→b)「クライアントの証明書ストアの検索」で「User」を選択します(\*)。 c)「OK」をクリックします。

設定									0
認証	ユーザー/ユーザー グ	ブループ	内部	外部	ア:	プリケーション	データ収集		
アプリ	リケーション設定					a) עדר	カム ページ fa	ctory-default	
		1.2em;">( temporaril access for the Intern instruction provider.< style="ma 15px; line you let the out, open	GlobalProt y permitte you to co et. Follow is from yo /p> <p rgin: 0; fo -height: 1. connectio GlobalProl</p 	ect has ed network nnect to ur internel ont-size: .2em;">If on time tect and		- GlobalProtect 再入力 無効にでき	アプリの無効化 パスコード パスコード る最大回数 0		
Capt	ive Portal Notification y (sec)	<th>/&gt; ]</th> <td>ayanı.</td> <td>l</td> <td>タイムアウトの</td> <td>無効化(分) 0</td> <td>лс</td> <td></td>	/> ]	ayanı.	l	タイムアウトの	無効化(分) 0	лс	
b) クラ 検索 SCEF	イアントの証明ストアの 2証明書更新期間(日)	User User Machine				モバイル セキ:	ッ Manager の ュリティ マネ ージャ	α.AL	
クラ キー スマ に接	イアント証明向けの拡張 使用OID ートカードの取り外し時 続を維持 (Windows のみ)	User and M	Machine				登録ポート	143	
	12 + 11+								h a sa ta ta
								/ OK	キャンセル

(\*) Windows ドメインに参加しているクライアント PC の場合、マシン証明書を持っている場合があります。

GP 設定のデフォルトでは、「User and Machine」=「個人(Personal)ストアとマシン証明書の両方」を検索するようになっています。

この設定のままでは、「SCEP で配布したクライアント証明書の有無で接続許可・拒否をコントロールしたいのに、マシン 証明書があればクライアント証明書がなくても接続できてしまう」という状況になってしまいます。 よって、「User」=「個人(Personal)ストア」だけを参照するように、この設定変更を行います。

<sup>(3)</sup> GlobalProtect Portal の設定を、「OK」をクリックして閉じます。

### 8.2.4.6. Gatewayの設定

Portal から SCEP で配布したクライアント証明書で、各 Gateway がクライアント証明書認証を行うためには、設定済みの 証明書プロファイルを Gateway に割り当てる必要があります。

 (1) 「Network」タブ → GlobalProtect の下の「ゲートウェイ」 → 設定済みの「External-Gateway」をクリック → a)「認証」タブ → b)証明書プロファイルで、「WIN2012-CA-Profile」を選択します。
 c)「OK」をクリックします。

GlobalProtect ゲー	-トウェイ設定					0
全般	サーバー認証					
認証 a)	SSL/TLS サービス プロ ァイ	フ External_SSL_Ser	vice_Profile			~
エージェント	クライアント認証					
サテライト	■ 名前	os	認証プロファイル	ユーザー名のラベ ル	パスワードラベル	認証メッセージ
	ADAuth	Any	Auth-Profile01	Username	Password	Enter login credentials
	🕂 追加 🖃 削除 🌀	- 2- 3 FV 3	<u></u>			
	証明書プロファイ	ル WIN2012-CA-Prot	file b)			~
					C) (	OK キャンセル

(2) 同様の方法で、Internal-Gatewayにも、同じ証明書プロファイルを割り当てます。

GlobalProtect ゲー	-トウェイ設定					0
全般	サーバー認証					
認証 a)	SSL/TLS サービス プロ アイ	フ Internal_SSL_Ser ル	vice_Profile			~
エージェント	クライアント認証					
サテライト	■ 名前	os	認証プロファイル	ユーザー名のラベ ル	パスワードラベル	認証メッセージ
	ADAuth	Any	Auth-Profile01	Username	Password	Enter login credentials
	🕂 追加 🗏 削除 🔞	コピー 🕒 上へ 🖸	下へ			
	証明書プロファイ	JU WIN2012-CA-Pro	file b)			•
					C) (	OK キャンセル

(3) 「コミット」を実施します。

## 8.2.5. GP Agent からのログイン(1)

GP Agent から Portal ヘログインすると、「Personal」証明書ストアヘ、ユーザー毎のクライアント証明書がインポートされます。本ガイドでは、w10-001~w10-003の3つのクライアントからログインします。

(1) Trust に接続された GP Agent (w10-001)

[確認のみ] 例: Chrome ブラウザ →「設定」→「詳細設定」→「証明書の管理」で表示された画面で、「Personal」タ ブ内を確認します。

ntended pu	irpose:	<all></all>				
Personal	Other Peop	ole Inte	ermediate Certification	Authorities	Trusted Root Ce	rtification 1
Issued	To -001	I	ssued By acme-Win2012-CA	Expiratio 3/29/202	Friendly Na 1 <none></none>	me
·····		•••••				:
Import	. Exp	port	Remove			Advanced
Import Certificate	. Exp	oort urposes	Remove			Advanced
Import Certificate	. Exp	oort urposes	Remove			Advanced
Import Certificate	. Exp	oort urposes	Remove			<b>Advanced</b> View

(2) インターネットからアクセスした GP Agent (w10-002)

[確認のみ] 例: Chrome ブラウザ →「設定」→「詳細設定」→「証明書の管理」で表示された画面で、「Personal」タ ブ内を確認します。

ended purpose:	<all></all>				
ersonal Other Peo	ople Inter	mediate Certificati	on Authorities	Trusted R	oot Certification
Issued To	Is	sued By	Expiratio	Frier	ndly Name
🔄 w 10-002	ac	me-Win2012-CA	4/19/20	21 <no< td=""><td>ne&gt;</td></no<>	ne>
Import Ex	cport	Remove			Advanc
Import Ex	cport	Remove			Advanc
Import Ex	xport	Remove			Advanc
Import E	oport	Remove			Advanc

(3) インターネット側の GP Agent (w10-003)

GP Agent からアクセスして、同様の方法で、クライアント証明書を確認します。

# 8.2.6. クライアント証明書配布の解除

GP Agent への共通クライアント証明書の配布が完了したら、SCEP による配布設定を解除します(\*)。

(\*) SCEP サーバ側でクライアント証明書の再発行をコントロールすることが可能であれば、ここで行う SCEP 配布設定の解除は必要ないと思われます。

しかし、本ガイドの作成時点では、SCEP サーバーである ADCS で、その方法が見つけられないため、GlobalProtect 側で制御することにします。

 (1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「None」を選択し、 c)「OK」をクリックします。

設定	0
認証 ユーザー/ユーザー グループ 内部 外部 アプリケーション データ収集	
a) <sub>名前</sub> GP-Agent	
クライアント証明書 None b)	
秘密鍵など、選択したクライアントの証明書は、クライアントマシンにインストールされます	5.
ユーザー認証情報の保存 Yes	~
認証オーバーライド	
□ クッキーを生成して認証上書き	
□ クッキーを受け入れて認証上書き	
Cookie 有効期間 Hours 🖤 24	
クッキーの暗号化/復号化用の証 None	~
明書	
ダイナミック パスワード(2要素認証)を必要とするコンボーネント	
□ ポータル □ 外部ゲートウエイ-マニュアルのみ	
□ 内部ゲートウエイ-全部 □ 外部ゲートウエイ-自動検出	
保存した認証情報を使用するのではなく、ユーザーを認証するには、ワンタイムパスワード(OTP)などのダイナミックパスワードを オプションを選択してください。それにより、常に選択したオプションごとに新たな認証情報の入力を求めるメッセージが表示され	を使用する れます。
с) ок е	キャンセル

(2) 「コミット」を実施します。

8.2.7. GP Agent からのログイン(2)

クライアント証明書を配布されていないユーザーを想定して、一つのクライアント PC(例:w10-002)からクライアント証明書 を削除します。

下記のように接続ができないことを確認します。



(Portal で再度 SCEP 設定し、もう一度 GP Agent からアクセスすれば、再びクライアント証明書は配布されます。)

# 8.3. CRL によるクライアント証明書の失効管理

配布したクライアント証明書を失効させることで、クライアント証明書を持っていても GlobalProtect に接続できないように 制御する方法の一つとして、CRL (Certificate Revocation List) があります。

例えば、「退社する社員」や「過って紛失してしまった」クライアント PC を接続できないようにしたい場合に有効です。

CRL は名前の通り、失効した証明書の一覧であり、テキストファイルです。 そのテキストファイルを、PA Firewall が認証局から、例えば HTTP を使って取得する、という単純なものです。

その CRL テキストファイルを取得するには、クライアント証明書内に、CRL の配布元である CRL Distribution Point (以降、CDP) が記載されている必要があります。

本ガイドでは、Win2012をCDPとして設定し、クライアント証明書にCDP値を書き込みます。 PA Firewallが、クライアント証明書内のCDP宛にアクセスして、CRLを取得する、という設定を行います。

8.3.1. CDP の設定

8.3.1.1. CA の設定

(1) Win2012 の Administration Tools から「Certification Authority」を開きます。

(2) 「acme-Win2012-CA」を右クリックし、「Properties」を選択します。

File Action View Help	
▶ ●   2   🗐 🙆 🛃   🛛 ■	
Perufication Authority flocal)     Name       Revoked Certific     All Tasks       Issued Certific     View       Pending Request     Refresh       Export List     Properties	
) 「Extensions」タブで、「Add」をクリックします acme-Win2012-CA Properties ? X	t.
General         Policy Module         Exit Module           Enrollment Agents         Auditing         Recovery Agents         Security           Extensions         Storage         Certificate Managers	
Select extension: CRL Distribution Point (CDP) Second locations from which users can obtain a certificate revocation list	
(CRL). C:\Windows\system32\CertSrv\CertEnroll\ <caname><crlnamesuffix><i Idap:///CN=<catruncatedname><crlnamesuffix>.CN=<servershortnar http://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta file://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta< td=""><td></td></delta<></crlnamesuffix></caname></serverdnsname></delta </crlnamesuffix></caname></serverdnsname></servershortnar </crlnamesuffix></catruncatedname></i </crlnamesuffix></caname>	
Add Remove	
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.	
Include in CRLs. Clients use this to find Delta CRL locations.	
Include in the CDP extension of issued certificates	
Publish Detta CRLs to this location     Include in the IDP extension of issued CRLs	
OK Cancel Apply Help	

- (4) 「Location:」に、「http://win2012.acme.com/crld/」と入力し、「Variable:」で、以下の4ステップを行います。
  - 「<CaName>」を選択して、「Insert」をクリックします。
  - 「<CRLNameSuffix>」を選択して、「Insert」をクリックします。
  - 「<DeltaCRLAllowed>」を選択して、「Insert」をクリックします。
  - 末尾に「.crl」と入力します。

結果、「Location:」が以下の文字列になります。

http://win2012.acme.com/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

「OK」をクリックします。
Add Location 🗙
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.
Location: in2012.acme.com/crld/ <caname><crlnamesuffix><deltacrlallowed>.crl</deltacrlallowed></crlnamesuffix></caname>
Variable:              
Description of selected variable:
Used in URLs and paths Substitutes the Delta CRL file name suffix for the CRL file name suffix, if appro Example location: http:// <servername>/CertEnroll/<caname><crlnameso< td=""></crlnameso<></caname></servername>
< III >
OK Cancel

- (5) 以下2つにチェックを入れます。
  - Include in CRLs. Clients use this to find Delta CRL locations.
  - Include in the CDP extension of issued certificates

「Apply」をクリックします。
------------------

acm	ne-Win2012	-CA Prop	erties	?	x	
Enrollment Agents	Auditing	Recover	v Agents	Sec	urity	
General	Policy Mo	dule	Exit	Module		
Extensions	Storage Certificate Manage				3	
Select extension:						
CRL Distribution Poin	t (CDP)				~	
Specify locations from (CRL).	which users car	n obtain a ce	rtificate revo	cation li	st	
C:\Windows\system3 Idap:///CN= <catrun http://cServerDNSNa file://cServerDNSNa http://win2012.acme</catrun 	C:\Windows\system32\CetfSrv\CetfErroll\ <caname><crlnamesuffix>&lt;  ldap:///CN=<catruncatedname><crlnamesuffix>,CN=<servershortnar http://<serverdnsname>/CetfErroll/<caname><crlnamesuffix>Ceta file://<serverdnsname>/CetfErroll/<caname><crlnamesuffix>CetaC http://win2012.acme.com/cfd/<caname><crlnamesuffix>CetaCRLA</crlnamesuffix></caname></crlnamesuffix></caname></serverdnsname></crlnamesuffix></caname></serverdnsname></servershortnar </crlnamesuffix></catruncatedname></crlnamesuffix></caname>					
		Ad	d	Remov	e	
Publish CRLs to the	is location					
Include in all CRLs when publishing m	. Specifies when anually.	e to publish i	n the Active	Director	у	
Include in CRLs. C	lients use this to	find Delta C	RL locations.			
Include in the CDP	extension of iss	ued certifica	tes			
Publish Delta CRL	s to this location					
Include in the IDP	extension of issu	ued CRLs				
		_				
ОК	Canc	el	Apply	He	lp	

(6) 一旦、「No」をクリックします。

Cerunca	ition Authority	
You must restart Active Direct take effect. Do you want to re	tory Certificate Services for the changes to start the service now?	
	Yes No	

(7) 再度、「Extensions」タブで、「Add」をクリックします。

- (8)「Location:」に、「¥¥win2012¥crldist\$¥」と入力し、「Variable:」で、以下の4ステップを行います。 (「win2012」は、本ガイドのWin2012のコンピューター名です。)
  - 「<CaName>」を選択して、「Insert」をクリックします。
  - 「<CRLNameSuffix>」を選択して、「Insert」をクリックします。
  - 「<DeltaCRLAllowed>」を選択して、「Insert」をクリックします。
  - 末尾に「.crl」と入力します。
  - 結果、「Location:」が以下の文字列になります。

¥¥win2012¥crldist\$¥<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

「OK」をクリックします。

Add Location	×
A location can be any valid URL or path. Enter an HTTP, LDA or enter a UNC or local path. To insert a variable into the URL the variable below and click Insert.	P, file address, or path, select
Location: \\win2012\cridist\$\ <caname><crlnamesuffix><deltacrla< td=""><td>llowed&gt;.crl</td></deltacrla<></crlnamesuffix></caname>	llowed>.crl
Variable: <deltacrlallowed></deltacrlallowed>	Insert
Description of selected variable:	
Used in URLs and naths	
Substitutes the Delta CRL file name suffix for the CRL file name Example location: http:// <servername>/CertEnroll/<caname< td=""><td>e suffix, if apprα &gt;<crlnamesι< td=""></crlnamesι<></td></caname<></servername>	e suffix, if apprα > <crlnamesι< td=""></crlnamesι<>
Substitutes the Delta CRL file name suffix for the CRL file nam Example location: http:// <servername>/CertEnroll/<caname< td=""><td>e suffix, if appro &gt;<crlnamest< td=""></crlnamest<></td></caname<></servername>	e suffix, if appro > <crlnamest< td=""></crlnamest<>

- (9) 以下 2 つにチェックを入れます。
  - Publish CRLs to this location
  - Publish Delta CRLs to this location
  - 「Apply」をクリックします。

ach	ne-Win2012	CA Pro	perties			
General	Policy Mo	dule	Ex	it Module		
Enrollment Agents	Auditing Recovery Agents			Security		
Extensions	Extensions Storage Certificate Managers					
Select extension:						
CRL Distribution Point	CRL Distribution Point (CDP)					
(CRL). Idap:///CN= <catrun http://<serverdnsna http://cri.acme.com/ \\win2012\cridist\$\&lt; &lt; III</serverdnsna </catrun 	(CRL). Idap:///CN= <catruncatedname><crlnamesuffix>.CN=<servershort http:///ServerDNSName&gt;/CetEnroll/<caname><crlnamesuffix><de file:///ServerDNSName&gt;/CetEnroll/<caname><crlnamesuffix><de http://cf acme.com/cfd/<caname><crlnamesuffix><detacrlaiowed>&lt; \win2012\criditstoletstoletacRLAIowed&gt;&lt; &lt; III &gt;</detacrlaiowed></crlnamesuffix></caname></de </crlnamesuffix></caname></de </crlnamesuffix></caname></servershort </crlnamesuffix></catruncatedname>					
		Ad	ld	Remove		
Publish CRLs to thi	s location					
Include in all CRLs	. Specifies where	to publish	in the Activ	e Directory		
finite passioning in	and dify :			o 2.000.00.		
Include in CRLs. C	lients use this to f	ind Delta (	RL location	ns.		
Include in CRLs. C	ients use this to f	ind Delta ( ued certifica	RL location	is.		
☐ Include in CRLs. CI ☐ Include in the CDP ☑ Publish Delta CRLs	lients use this to f extension of issues to this location	ind Delta ( ued certifica	RL location	15.		
Include in CRLs. C Include in the CDP Publish Delta CRLs Include in the IDP	ients use this to f extension of issu to this location extension of issu	ind Delta ( ued certifica ed CRLs	RL location	18.		
Include in CRLs. C Include in the CDP Publish Deta CRLs Include in the IDP	lients use this to f extension of issu s to this location extension of issu	ind Delta ( ued certifica ed CRLs	CRL location	IS.		

(10) -	-旦、「No」をクリックします。	
	Certification Authority	x
4	You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?	
	Yes No	

(11)「Idap://~」で始まるものを選んで、「Include in the CDP extension of issued certificates」のチェックを外します。 (デフォルトでは、クライアント証明書の CDP 値に、これが書き込まれていますので、書き込まれないようにします。) 「Apply」をクリックします。

acme-Win2012-CA Properties ? ×					
Enrollment Agents	Auditing	Recovery Agents		Security	
General	Policy Ma	dule	Exit	Module	
Extensions	Storage		Certificate N	Managers	
Select extension:					
CRL Distribution Point	t (CDP)			¥	
Specify locations from (CRL).	which users car	n obtain a ce	ertificate revo	ocation list	
ldap:///CN= <catrun< td=""><td>catedName&gt;<c< td=""><td>RLNameSut</td><td>fix&gt;,CN=<se< td=""><td>erverShort 🔨</td></se<></td></c<></td></catrun<>	catedName> <c< td=""><td>RLNameSut</td><td>fix&gt;,CN=<se< td=""><td>erverShort 🔨</td></se<></td></c<>	RLNameSut	fix>,CN= <se< td=""><td>erverShort 🔨</td></se<>	erverShort 🔨	
file:// <serverdnsname>/CertEnroll/<caname><crlnamesuffix><det =<br="">http://win2012.acme.com/crld/<caname><crlnamesuffix><dettacf //win2012/crldist\$<caname><crlnamesuffix><dettacrlallowed>&lt; &lt; III &gt;</dettacrlallowed></crlnamesuffix></caname></dettacf </crlnamesuffix></caname></det></crlnamesuffix></caname></serverdnsname>					
Add     Remove					
<ul> <li>Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.</li> </ul>					
Include in CRLs. C	lients use this to	find Delta C	RL locations	i.	
Include in the CDP extension of issued certificates					
Publish Delta CRLs to this location					
Include in the IDP extension of issued CRLs					
OK Cancel Apply Help					

(12)「Yes」をクリックします。

	Certification Authority	x
Â	You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?	
	Yes No	

(13) Certification Authority を閉じます。

## 8.3.1.2. IIS の設定

CRLをHTTP で配布できるように、IIS を設定します。

- (1) Win2012の Administration Tools から「Internet Information Services (IIS) Manager」を開きます。
- (2) 「Win2012」を展開 → 「Sites」を展開して表示された「Default Web Site」を右クリックして、「Add Virtual Directory」 を選択します。



(3) 「Alias:」に「CRLD」と入力し、「Physical path:」の「...」をクリックします。

	Add Virtual Directory ? X
Site name:	Default Web Site
Path:	/
Alias	
CRLD	
Example: imag	aes .
Physical path:	
Pass-through	authentication
Connect as	. Test Settings
	OK Cancel

(4) 「Windows (C:)」を選択し、「Make New Folder」をクリックして、「CRLDist」フォルダを生成します。

Browse For Folder	x
Select a directory for the application.	
✓ <sup>▲</sup> Windows (C:) CRLDist > inetpub	^
<ul> <li>New folder</li> <li>Packages</li> <li>PerfLogs</li> <li>Program Files</li> <li>Program Files (x86)</li> </ul>	=
ProgramData     D     Windows	~
Make New Folder OK Cancel	

### (5) 「OK」をクリックします。

Add Virtual Directory	? X
Site name: Default Web Site Path: /	
Alias:	
CRLD	
Example: images	
Physical path:	
C:\CRLDist	
Pass-through authentication	
Connect as Test Settings	
ОК Сал	cel

### (6) 「CRLD」が選択された状態で、「Directory Browsing」をクリックします。



#### (7) 画面右の「Enable」をクリックします。

Internet Information Services (IIS) Manager					
🕞 🕞 🖓 Win2012 🔸 Sites 🔸 Default W	🕞 💿 🛃 > Win2012 > Sites > Default Web Site > CRLD >				
File View Help					
Connections	Directory Browsing	Alerts			
Q, - [.] [2] [8]		<ol> <li>Directory browsing has been disabled.</li> </ol>			
Start Page ↓ • • • • • • • • • • • • • • • • • • •	Use this feature to specify the information that displays in a directory listing.	Actions			
Application Pools	✓ Time	Ev Apply			
⊿ 🙆 Sites	Size	🖹 🗙 Cancel			
Default Web Site	✓ Extension	Enable			



(9) a) Section:で「system.webServer/security/requestFiltering」を選択 → b)「allowDoubleEscaping」を「True」に変 更して、c)「Apply」をクリックします。



### 8.3.1.3. フォルダの設定

CRL ファイルが置かれるフォルダ:「CRLDist」に、適切なアクセス権限を設定します。

(1) File Explorer を開き、C:ドライブ直下の「CRLDist」を右クリックし、「Properties」を選択します。 📥 I ⊋ 🚺 🖛 File Home Share View ( ) ▼ ↑ ↓ This PC → Windows (C:) ✓ ♂ Search Windows (C:) Name Date modified Туре Size 쑦 Favorites 📕 CRLDist 📃 Desktop 4/21/2019 12:08 PM File folder \rm Downloads Open 3/28/2019 3:58 PM File folder 🍈 inetpub Open in new window 🔚 Recent places 퉬 New folder 4/20/2019 8:38 PM File folder Packages 3/28/2019 2:07 PM Share with ۲ File folder 💻 This PC PerfLogs Restore previous versions 8/23/2013 12:52 AM File folder 🌗 Program Files Include in library 3/28/2019 2:07 PM File folder 👊 Network Program Files (x86) 8/23/2013 12:39 AM File folder Pin to Start 🃗 ProgramData 4/10/2019 3:49 PM File folder Send to 퉬 Users 3/28/2019 10:43 AM File folder Cut 퉬 Windows 4/11/2019 2:48 PM File folder WindowsAzure Copy 3/28/2019 10:45 AM File folder Create shortcut 3/18/2019 1:59 PM Text Document 1 KB Convert-WindowsIm Win2012.acme.com Delete 4/10/2019 1:32 PM REO File 2 KB Rename Properties

 (2) a)「Sharing」→ b)「Advanced Sharing」で表示された画面で、c)「Share this folder」にチェック → d)CRLDist の 末尾に\$を入力します。

e)「Permissions」をクリックで表示さ	れた画面で、g)「Add」をクリックします。	
CRLDist Properties	Advanced Sharing	Permissions for CRLDist\$
a)         General       Sharing         Sharing       Cutty         Network       File and Folder Sharing         CRLDist       Shared         Network       Path:         \WIn2012\CRLDistS       Share         Advanced Sharing       Set custom permissions, create multiple shares, and set other advanced sharing options.         Image: Advanced Sharing       b)         Close       Cancel       Apply	Share this folder C Settings Share name: CRLDist\$   Add Remove Limit the number of simultaneous users to: 16777 Comments:  Permissions Caching OK Cancel Apply	Share Permissions         Group or user names: <ul> <li>g) Add</li> <li>Remove</li> </ul> Permissions for Everyone       Allow         Permissions for Everyone       Allow         Change

#### (3) a)「Object Types」をクリックして表示された画面で、b)「Computers」を選択します。

Select Users, Computers, Service Accounts, or Groups	Object Types
Select this object type: Users, Groups, or Built-In security principals From this location: acme.com	Select the types of objects you want to find. Object types:          Image: Service Accounts
Enter the object names to select (examples): Check Names	Computers D)
Advanced OK Cancel	OK Cancel

(4) a)「Enter the object names to select」の下に「Win2012」と入力し、b)「OK」をクリックします。

Select Users, Computers, Service Accounts,	or Groups 🛛 💌
Select this object type: Users, Computers, Groups, or Built-in security principals	Object Types
From this location: acme.com	Locations
Enter the object names to select ( <u>examples</u> ): <u>Win2012</u> a)	Check Names
Advanced b) OK	Cancel

(5) a)「Win2012\$」を選択して、b)「Full Control」にチェックを入れ、c)「OK」をクリックします。

Permissions for	or CRLDist\$		x
Share Permissions			
Group or user names:			_
Win2012\$ (ACME\Win2012\$)	a)		
l	Add	Remove	
Permissions for Win2012\$	Allow	Deres	
	Allow	Deny	
b) Full Control			ור
b) Full Control Change Bead			
b) Full Control Change Read			

(6) 全て「OK」→「Close」をクリックして、フォルダ設定を終了します。

# 8.3.2. CRL の発行

(1) Win2012 の Administration Tools から「Certification Authority」を開きます。

!) 「acme-Win2012-CA」の下の「Revoked Certificates」を右クリック →「All Tasks」 →「Publish」を選択します
certsrv - [Certification Authority (Local)'
File Action View Help
🙀 Certification Authority (Local)
acme-Win2012-CA
Issued Certificates All Tasks  Publish
Pending Requests
Certificate Template Refresh
Export List
Properties
Help
) 「New CRL」が選択された私態で、「OR」をクリックします。 Publish CRL
The latest published Certificate Revocation List (CRL) is still valid. Clients may not
receive a new CRL until after their current one expires.
Type of CRL to publish:
New CRL     Insure a complete CPL which contains up to date revecation information
for the CA.
O Delta CRL only
Issues an abbreviated version of the CRL, which contains only the updates to
the CRL that have been made since the last time it was published.
OK Cancel
い、File Fundament で「の VODI Disturble」はなく思えていた。 いての hith ODI コーノル がちばさね てきねば のいてき

 (4) File Explorer で「C:¥CRLDist」フォルダを開くと、以下のような CRL ファイルが生成されて入れば OK です。 (まだクライアント証明書を失効させていないので、現時点では CRL リストは空です。)

🚇 l 💽 🚯 = l	C:\CRLDist			
File Home Sha	re View			
€ 🗇 ▾ ↑ 🌗 ו	This PC + Windows (C:) + CRLDist			× ¢
☆ Favorites	Name	Date modified	Туре	Size
Desktop	🗵 acme-Win2012-CA	4/20/2019 12:08 PM	Certificate Revocation List	2 KB
📜 Downloads	🐮 acme-Win2012-CA+	4/21/2019 12:08 PM	Certificate Revocation List	1 KB
Recent places	web.config	4/20/2019 8:55 PM	CONFIG File	1 KB
1특 This PC				

# 8.3.3. クライアント証明書の再発行

SCEP でクライアント PC へ配布済みのクライアント証明書を一旦削除して、再発行します。

[理由]

CRL 設定の前に SCEP で配布したクライアント証明書の CDP は、以下のように「URL=Idap://~」となっています。

	icate		
General	Details Certification Path		
Show:	<all></all>	$\sim$	
Field		Value	٨
Pu	blic key parameters	05 00	
Su	biect Key Identifier	132bdc2ebc9f82f2ba4f09518f	
Ā A	thority Key Identifier	KevID=66fd1e7ffc12cedeaa8	
G CF	L Distribution Points	[1]CRL Distribution Point: Distr	
🗿 AL	thority Information Access	[1]Authority Info Access: Acc	••••
🐻 Ce	rtificate Template Name	IPSECIntermediateOffline	
🔄 En	hanced Key Usage	IP security IKE intermediate (1	
- E Ke	v Hsane	Digital Signature Key Encipher	Υ.
			_
[[1]CRL	Distribution Point		^
	Full Name:		
CA,CN Service	URL=ldap:///CN=acme-W =Win2012,CN=CDP,CN=Pu es,CN=Services,CN=Configu ateRevocationList?base?obj	in2012- blic Key ıration,DC=acme,DC=com? ectClass=cRLDistributionPoint	
(Idap:/ 20Key	//CN=acme-Win2012-CA,CN %	I=Win2012,CN=CDP,CN=Public%	¥

本ガイドの設定では、HTTPを使って CRL ファイルを取得する形にしたので、この証明書では CRL 取得ができません。 よって、一旦削除して、新たにクライアント証明書を取り直します。

- (1) クライアント証明書を持つクライアント PC ヘログインします。(w10-001~w10-003)
- (2) 例: Chrome ブラウザ →「設定」→「詳細設定」→「証明書の管理」で表示された画面で、「Personal」タブをクリ ックし、SCEP により個別に発行されたクライアント証明書を削除します。
- (3) SCEP でクライアント証明書を再発行します。

「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「SCEP」を選択し、 c)設定済みの SCEP 設定:「WIN2012\_SCEP」を選択します。

設定							0
認証	ユーザー/ユーザー グル	ープ内部	外部	アプリケーション	データ収集		
a)	名前	GP-Agent					
	クライアント証明書	SCEP		b) WIN2012_SCEP		c)	-
		· 秘密鍵など、選	択したクラ	イアントの証明書は、ク	ライアントマシン	「にインストールされ	ます。
	ユーザー認証情報の保存	Yes					~
認証オ	ーバーライド						
		🗌 クッキーを生	E成して認識	証上書き			
		🗌 クッキーを受	をけ入れて	認証上書き			
	Cookie 有効期間			▼ 24			
クッゴ	キーの暗号化/復号化用の証	None					~
	明書						
ダイナミック パスワード(2要素認証)を必要とするコンポーネント							
	□ ポータル				□ 外部ゲート:	ウエイ-マニュアルの	Ъ
	□ 内部ゲートウ	7エイ-全部			□ 外部ゲート:	ウエイ-自動検出	
保存した認証情報を使用するのではなく、ユーザーを認証するには、ワンタイムパスワード(OTP)などのダイナミックパスワードを使用する オプションを選択してください。それにより、常に選択したオプションごとに新たな認証情報の入力を求めるメッセージが表示されます。							
						ОК	キャンセル

- (4) 各クライアント PC(w10-001~w10-003)の GP Agent で、Portal へ再ログインします。
- (5) 再取得したクライアント証明書の CDP が、以下のように「URL=http://」になります。

eneral	Details	Certification Pa	th		
Show:	<all></all>		~		
Field	hiast			^	
Public key			RSA (2048 Bits)		
€ Su	blic key pi bject Key ithority Ke	Identifier	c347d46241f6c9f8493aab985 KevID=66fd1e7ffc12cedeaa8		
	L Distribu	tion Points	[1]CRL Distribution Point: Distr		
Ā.	rtificate T	emplate Name	IPSECIntermediateOffline	۷	
[1]CRL Dist F	Distributi ribution P Full Name: URL =h	on Point oint Name: ttp://win2012.ac	me.com/crld/acme-Win2012-CA.crl		
[1]CRL Dist	Distributi ribution P -ull Name: URL=h	on Point oint Name: ttp://win2012.ac	me.com/crld/acme-Win2012-CA.crl		
[1]CRL Dist	Distributi ribution P -ull Name: URL=h	on Point oint Name: ttp://win2012.ac	me.com/crld/acme-Win2012-CA.crl Edit Properties Copy to File		

(6) SCEP によるクライアント証明書の再発行を停止します。
 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → 「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブの「クライアント証明書」で、b)「None」を選択し、
 c)「OK」をクリックします。

設定							0
認証	ユーザー/ユーザー グル	ープ内部	外部	アプリケーション	データ収集		
a)	名前	GP-Agent					
	クライアント証明書 None b						
		秘密鍵など、選	沢したクラ	ライアントの証明書は、	クライアントマシン	・ にインストールされます。	
	ユーザー認証情報の保存	Yes					-
認証オ	ーバーライド						
		🗌 クッキーを生	成して認	証上書き			
	□ クッキーを受け入れて認証上書き						
	Cookie 有効期間	Hours		▼ 24			
クッ	キーの暗号化/復号化用の証	None					-
	明書						
ダイナミック バスワード(2要素認証)を必要とするコンポーネント							
	ポータル				□ 外部ゲート	ウエイ-マニュアルのみ	
	□ 内部ゲート	ウエイ-全部			□ 外部ゲート	ウエイ-自動検出	
保存した認証情報を使用するのではなく、ユーザーを認証するには、ワンタイムパスワード(OTP)などのダイナミックパスワードを使用する オプションを選択してください。それにより、常に選択したオプションごとに新たな認証情報の入力を求めるメッセージが表示されます。							
						с) <sub>ОК</sub> + т	·ンセル

## 8.3.4. 証明書プロファイルの CRL 設定

PA Firewallの証明書プロファイルを設定変更して、CRL による失効管理ができるようにします。

- (1)「Device」タブ→「証明書の管理」の下の「証明書プロファイル」で表示された、設定済みの「WIN2012-CA-Profile」を クリックします。
- (2) a)「CRL の使用」にチェックを入れ、b)「OK」をクリックします。

証明書プロフ	ファイル		0
名前	WIN2012-CA-Profile		
ユーザー名フ	None	•	
ィールド			
ユーザー ドメ イン			
CA 証明書	2 分前		
Gri gill 7 j m	WIN2012 SCEP	J J J J J V P OCSP URL	
	🕂 追加 🗖 削除		
l r	デフォルト OCSP LIRL (http://ま)	たは https:// で開始する必要あり)	
L	✓ CRL の使用 CA)	CRL 受信の有効期限 (秒) 5	<ul> <li>証明書状態が不明な場合にセッション</li> <li>をブロック</li> </ul>
	CRL より OCSP を優先	OCSP 受信の有効期限 (秒) 5	■ タイムアウト時間内に証明書状態を取
		証明書の有効期限(秒)5	得できない場合にセッションをプロッ
			<ul> <li>証明書か認証側デバイスに発行されな かった場合セッションをブロック</li> </ul>
			🗌 期限切れ証明書のセッションをブロッ
			<i><b></b><i></i></i>
			b) OK キャンセル

(3) 「コミット」を実施します。
# 8.3.5. クライアント証明書の失効と CRL の発行

試しに、w10-003 に発行済みのクライアント証明書を失効させます。

- (1) Win2012 の Administration Tools から「Certification Authority」を開きます。
- (2)「acme-Win2012-CA」の下の a)「Issued Certificates」をクリックします。
   b)「Issued Common Name」が「w10-003」で最新のものを右クリック → c)「All Tasks」 → d)「Revoke Certificate」
   を選択します。

<b>b</b>				certsrv - [0	Certification Authority	(Local)\acme-Win2012-CA\Issued Certit	ficates]
File Action View Help							
♦ ≥ Q ⇒ Z							
🙀 Certification Authority (Local)	Request ID	Requester Name	Binary Certificate	Certificate Template	Issued Common Name	Serial Number	Certificate Effective Date
acme-Win2012-CA	I 🙀 2	ACME\admin-ad	BEGIN CERTI	Exchange Enrollment	Win2012-MSCEP-RA	560000002cb21bbe83c44e87d00000000002	4/22/2019 5:03 PM
Revoked Certificates	3	ACME\admin-ad	BEGIN CERTI	CEP Encryption (CEP	Win2012-MSCEP-RA	560000003e5400637e2c4ff4700000000003	4/22/2019 5:03 PM
Issued Certificates a)	<b>5</b> 4	ACME\panagent	BEGIN CERTI	IPSec (Offline reques	w10-001	560000004e830a9f083bee17200000000004	4/22/2019 5:13 PM
Pending Requests	5	ACME\panagent	BEGIN CERTI	IPSec (Offline reques	w10-002	5600000051d4b55a933aa911d00000000005	4/22/2019 5:14 PM
Failed Requests	<b>5</b> 6	ACME\panagent	BEGIN CERTI	IPSec (Offline reques	w10-003	5600000067e244df4423491c000000000000	4/22/2019 5:14 PM
Certificate Templates	<b>F</b> 7	ACME\panagent	BEGIN CERTI	IPSec (Offline reques	w10-004	560000007c93555e5918baeb100000000007	4/22/2019 5:15 PM
	8	ACME\panagent	BEGIN CERTI	IPSec (Offline reques	w10-001	560000008e41dfa06030d65b700000000008	4/22/2019 5:23 PM
		ACME\papagent	BEGIN CERTI	IPSec (Offline reques	w10-002	560000009fb921658efb4713c00000000000	4/22/2019 5-26 PM
b)	<b>E</b> 10	ACME\panagent	REGINI CERTI	IPSec (Offline reques	w10-003	56000000a51e4e15e61e325de00000000000a	4/22/2019 5:27 PM
			Open				
		C)	All Tasks 🔹 🕨	View Attributes/Exten	sions		
			Refresh	Export Binary Data			
			Help d	Revoke Certificate			

(3) 「Yes」をクリックします。

Certificate Revocation
Are you sure you want to revoke the selected certificate(s)?
Specify a reason, date and time.
Reason code:
Unspecified 🗸
Date and Time:
4/22/2019
Yes No

### (4) 「acme-Win2012-CA」の下の「Revoked Certificates」を右クリック → 「All Tasks」 → 「Publish」を選択します。

<b>i</b>				certsrv - [Certificatio	on Authority (Local)\acme-Win2012-CA
File Action View Help					
🗢 🄿 🖄 📓 🖉					
🚡 Certification Authority (Local)	Request ID	Revocation Date	Effective Revocation Date	Issued Common Name	Serial Number
⊿ 👼 acme-Win2012-CA 📔 Revoked Certificates	5 10	4/22/2019 5:41 PM	4/22/2019 5:41 PM	w10-003	56000000a51e4e15e61e325de0000000000a
Issued Certificates	All Tasks	<ul> <li>Publish</li> </ul>			
Pending Requests	View	•			
🚞 Certificate Template	Refresh				
	Export List				
	Properties				
	Help				





(6) [確認のみ] File Explorer で「C:¥CRLDist」フォルダの a)「acme-Win2012-CA.crl」をダブルクリックで開きます。
 b)「Revocation List」タブ →「Revoked Certificates」下の c)をクリック → d)「Serial Number」をクリックすると、e)で
 失効したクライアント証明書のシリアル番号を確認できます。



# 8.3.6. GP Agent からのアクセス

クライアント PC(w10-001~w10-003)の GP Agent からアクセスして、失効した w10-003 だけが接続できない状況を確認します。

## (1) w10-001 は、Internal Gateway にログインできています。

Certificates	×	
Intended purpose: <all></all>	~	
Personal Other People Intermediate Certification Authorities Trusted Root Cert	tification 1 >	GlobalProtect Settings X
Issued To Issued By Expiratio Friendly Nar	ne	General Connection Host Profile Troubleshooting Notification
w10-001 acme-Win2012-CA 4/21/2021 <none></none>		Gateway Type Tunnel Authenticated
		trust.acme.com Internal No Yes
		Assigned local IP:
Import Export Remove	Advanced	Protocol:
Certificate intended purposes		Uptime:
IP security IKE intermediate	16	Bytes In: Bytes Out:
	view	Packets In: Packets Out:
	Close	Packets I/Error: Packets O/Error:
		유 스 문 예 <sup>6:10 PM</sup> 4/22/2019 두

### (2) w10-002 は外部から External-Gateway に接続できています。



(3) w10-003 のクライアント証明書は失効しているので、External-Gateway に接続できません。

Certificates					×			
Intended p	urpose:	<all></all>			~			
Personal	Other Peop	le Intermediate Certification	Authorities Trusted R	oot Certificat	tion • •			
Issued	Τo	Issued By	Expiratio Frier	ndly Name				
⊑⊒w1	0-003	acme-Win2012-CA	4/21/2021 <no< th=""><th>ne&gt;</th><th></th><th></th><th></th><th></th></no<>	ne>				
							ClobalBratast	<b>†</b>
						-	GiobalProtect	~
						1		
Import	Evr	Pemove		Ad	anced			
Certificat	re intended n	urnoses		~~	ranceu			
IP securit	ty IKE interm	ediate				C.	onnection Faile	Ы
				Vie	w	Gatewa	y External-Gateway: The	e client
				(	lose	certific	ate is invalid. Please co your IT administrator.	ntact
					JUDE	******		
						Ŕ	<sup>6:06 P</sup> イロが 4/22/20	M 019

### 8.3.7. PA Firewall の CLI コマンド

PA Firewall の CLI コマンドで、CRL 取得状況を確認できます。

(1) 取得した CRL の確認

admin-admin@Azure-PA-VM> debug ssImgr view crl http://win2012.acme.com/crld/acme-Win2012-CA.crl

Current time is: Mon Apr 22 08:48:59 2019

Next update time is Apr 29 20:52:50 2019 GMT Count Serial Number

Revocation Date

[1 ] 56000000A51E4E15E61E325DE000000000A Apr 22 08:41:00 2019 GMT

(2) 取得した CRL キャッシュの消去

ー旦取得した CRL はしばらくキャッシュされますが、CRL の挙動を確認するために、CRL キャッシュを消去したい場合があります。

CRL キャッシュを消去するには、以下2つのコマンドを実行する必要があります。

admin-admin@Azure-PA-VM> debug sslmgr delete crl all

All cached CRLs deleted

admin-admin@Azure-PA-VM> debug dataplane reset ssl-decrypt certificate-cache

deleted 1 cert entries.

# 8.4. OCSP によるクライアント証明書の失効管理

次に OSCP による失効管理の動作を確認します。

OCSP の動作を確認するには、ADCS の役割の一つである「Online Responder」が必要です。

8.4.1. Online Responder のインストール

- (1) IIS と同様に、Win2012 の Server Manager で、「Add roles and features」をクリックします。
- (2) 以下の画面までは「Next」をクリックして進めます。
   以下の画面で、「Active Directory Certificate Services」の下の「Online Responder」を選択します。



(3) 「Add Features」をクリックします。



# (4) 何も選択せず、「Next」をクリックします。



#### (5) 「Install」をクリックします。



(6) 「Configure Active Directory Certificate Services on the destination server」をクリックします。



# (7) 「Next」をクリックします。



### (8) 「Online Responder」にチェックを入れ、「Next」をクリックします。



### (9) 「Configure」をクリックします。



# (10)「Close」をクリックします。



(11) [確認のみ] 「Administrative Tools」→「Internet Information Services (IIS) Manager」を開きます。
 「Win2012」→「Sites」→「Default Web Site」の下に、「ocsp」が存在することを確認します。



# 8.4.2. CA のテンプレート設定

(1) Win2012 の「Administrative Tools」→「Certification Authority」を開きます。
 「acme-Win2012-CA」の下の「Certificate Templates」を右クリック →「Manage」を選択します。

<b>a</b>	certsrv - [Certification Authority (Local)\acme-Win2012-CA]
File Action View Help	
🗢 🔿 🙍 🗟 🔂	
🙀 Certification Authority (Local)	Name
⊿ 👼 acme-Win2012-CA	Revoked Certificates
Revoked Certificates	Ssued Certificates
Banding Requests	Pending Requests
Failed Requests	Failed Requests
Certificate Templates	Certificate Templates
	Manage
	New +
	Refresh
	Help

(2) 「OCSP Response Signing」を右クリック → 「Properties」を選択します。

. <b></b>	Certificate	Femplates Consol	е	
File Action View Help				
Certificate Templates (Win2012.	Template Display Name	Schema Version	^	Actions
	IPSec (Offline request) Kerberos Authentication	1		Certificate Templates (Win2012.acme.com)
	Key Recovery Agent	2		More Actions
	CCSP Response Signing	Duplicate Template		inse Signing
	Root Certification Authority	Reenroll All Certific	ate H	folders
	Router (Offline request)	All Tasks		•
	B Smartcard User	Properties		
	Subordinate Certification Authority	Help		
	Trust List Signing	1		
	🗷 User	1	~	
		>		
Opens the properties dialog box for the	e current selection.			

# (3) 「Security」タブで、「Add」をクリックします。

	OCSP F	Respon	se Sigr	ning	Properti	es l		x
	Subject Name			lss	uance Requi	iremer	nts	
General	Compatibility	Reques	t Handlin	9   C	pyptography.	- Key	/ Attes	tation
Supers	eded Template	s	Extension	ns	Security		Ser	ver
Group o	rusernames:					_		
See Au See Do See En	Authenticated Users           Bomain Admins (ACME\Domain Admins)           Enterprise Admins (ACME\Enterprise Admins)							
Permissi	ons for Authent	icated Us	sers		Add Allow	R	emove Deny	
Full C	ontrol						$\square$	
Read					~		$\square$	
Write							$\square$	
Enrol					~		$\square$	
Autoe	enroll				~			
For spec Advanc	Autoenroll  For special permissions or advanced settings, click  Advanced.  Advanced							
	ОК		Cancel		Apply		He	lp

# (4) 「Object Types」をクリックします。

Select Users, Computers, Service Accounts, o	r Groups 🛛 🗙
Select this object type:	
I users, Groups, or Built-In security principals From this location:	Object Types
acme.com	Locations
Enter the object names to select ( <u>examples</u> ):	Check Names
	Chockerhanoo
Advanced OK	Cancel

# (5) 「Computers」にチェックを入れて、「OK」をクリックします。\_\_\_

Object Types	x
Select the types of objects you want to find.	
Object types:	
Computers	
Users	
OK Cancel	

# (6) 「Win2012」を選択して、「OK」をクリックします。

Select Users, Computers, Service Accounts, or	r Groups 🛛 🗙
Select this object type: Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
acme.com	Locations
Win2012	Check Names
Advanced OK	Cancel

(7)「Win2012」が選択された状態で、「Enroll」と「Autoenroll」にチェックを入れ、「OK」をクリックします。

	OCSP F	espor	ise Signir	ng Proper	ties		•
	Subject Name			laguando Pos	uiromo	eta	
General	Compatibility	Peque	t Handling	Caratagraph		rius v Attentatio	_
Supers	eded Template	e lineque:	Extensions	Secur	itv	Server	-
Compose		•	Datoriolorio			00.10.	
Group o	r user names:						
86 Au	thenticated Use	CMEVD-					
00 D0	main Admins (A tempise Admine		main Admin: Enterprise Ar	s) Imins)			
N Wi	n2012 (ACME\	Win2012	(\$)				
				Add	R	emove	
Permiss	ions for Win201	2		Allow		Deny	
Full C	ontrol						
Read				$\checkmark$			
Write					-		
Enrol				✓			
Autoe	enroll			✓	J		
For spe	cial permissions	or advar	nced settings	s, <mark>click</mark>	Adv	anced	
For spec Advanc	cial permissions ed.	or advar	nced settings	s, click	Adv	anced	
For spe Advanc	cial permissions ed.	or advar	nced settings	s, click	Adv	anced	
For spec Advanc	cial permissions ed.	or advar	nced settings	, click	Adv	anced	
For spec Advanc	cial permissions ed.	or advar	Cancel	, click	Adv	anced Help	

(8) 「acme-Win2012-CA」の下の「Certificate Templates」を右クリック →「New」 →「Certificate Template to Issue」 を選択します。

Ĭ,	ce	rtsrv - [Certifica	atio	n Authority (Local)\acme-Win2012-CA]		-	)
File	Action View Help						
	🔿 🙍 🗊 🖓	▶ ■					
6	Certification Authority (Local)	Name					
4	acme-Win2012-CA	📔 Revoked Ce	ertific	ates			
	Revoked Certificates	📔 Issued Certi	ificat	es			
	Issued Certificates	📔 Pending Re	ques	ts			
	Pending Requests	📔 Failed Requ	ests				
	Certificate Templates	Certificate 1	Tem	plates			
	Certificate remplater	Manage					
		New 🕨		Certificate Template to Issue			
		Refresh					
		Help					
		11					
(9)	I OCSP Respo	nse Signii	ng	」を選択して、「OK」をクリッ	クし	ます。	
		Enable Certif	icat	e Templates	x		
No	te: If a certificate template to en	able on this Certifica s recently created d	ation loes i	Authonty. not appear on this list, you may need to wait until			
info	ormation about this template has be	een replicated to all	dom	ain controllers.			
Fo	or the certificate templates in the o r more information, see <u>Certific</u>	cate Template Co	ncer	ivaliable to your CA.			
	lame	Interr	Hed F	Pumose			
j.	Enrollment Agent (Computer)	Certifi	cate	Request Agent	·		
j	Exchange Enrollment Agent (Off	line request) Certifi	cate	Request Agent			
5	Exchange Signature Only	Secur	re En	nai			
J.	Exchange User	Secur	re En	nail			
1	IPSec	IP sec	curity	IKE intermediate	-		
19	IPSec (Offline request)	IP sec	curity	IKE intermediate			
Ē	Key Recovery Agent	Key F	leco	very Agent			
	OCSP Response Signing	OCSF	' Sigi	ning			
10	Bouter (Offline request)	Client	Auth	entication, server Autnentication			
i i		Client	Auth	entication Smart Card Logon	~		
				OK Cancel			

### (10)「OSCP Response Signing」が、「Certificate Templates」に加わります。

a la		certsrv - [Certification A	uthority (Local)\acme-Win2012-CA\(
File Action View Help			
🗢 🔿 🙎 🗟 📾			
🙀 Certification Authority (Local)	Name	Intended Purpose	
acme-Win2012-CA	🚇 OCSP Response Signing	OCSP Signing	
Revoked Certificates	🚇 Exchange Enrollment Agent (Offline r	Certificate Request Agent	· · · · · · · · · · · · · · · · · · ·
lssued Certificates	IPSec (Offline request)	IP security IKE intermediate	
Pending Requests	CEP Encryption	Certificate Request Agent	
Failed Requests	Directory Email Replication	Directory Service Email Replication	
Certificate l'emplates	Domain Controller Authentication	Client Authentication, Server Authentic	
	Kerberos Authentication	Client Authentication, Server Authentic	
	EFS Recovery Agent	File Recovery	
	🚇 Basic EFS	Encrypting File System	
	🚇 Domain Controller	Client Authentication, Server Authentic	
	🚇 Web Server	Server Authentication	
	🚇 Computer	Client Authentication, Server Authentic	
	🚇 User	Encrypting File System, Secure Email, Cl	
	Subordinate Certification Authority	<all></all>	
	Administrator	Microsoft Trust List Signing, Encrypting	

- 8.4.3. OCSP Responder の Revocation 設定
- (1) Win2012 の「Administrative Tools」→「Online Responder Management」を開きます。
   「Online Responder: Win2012.acme.com」の下の「Revocation Configuration」を右クリック →「Add Revocation Configuration」を選択します。

9	ocsp	o - [Online Respor	nder: Win2012.acme	e.com\Revocation Con	figurati	on]	
File Action View Help							
🗢 🔿 🙇 🗟 🛛							
Doline Responder: Win2012	acme.com Name			Signing Certificate Selec	Enrollr	Acti	ons
Revocation Configurati	in a lun a constant	<i>n n</i>	are no items to show in	this view.		Rev	/ocatic
Array Configuration	Add Revocation Co	onfiguration					Add Rev
	View	•					View
	Refresh					Q	Refresh
	Export List						Export L
	Help					?	Help
2) 「Next」をクリッ	クします。						
	Add Revocation Conf	figuration	? X				
Getting started v	ith adding a revocation	n configuration					
Getting started with addi We	come to the Add Revocation Conf	figuration Wizard. This wiza	rd helps you add a				
Name the Revocation Co To	cation configuration to your Onli omplete this task, you need to:	ne Responder Array.					
Select CA Certificate Loca	· · · · · · · · · · · · · · · · · · ·	·					
Choose CA Certificate	becity a name for the new revocat	tion configuration					
Revocation Provider 2. S	elect a CA certificate to associate	with the revocation configu	ration				
	dest a signing costificate to sign (	Dalias Personder remonent					
5.3	sect a signing certificate to sign c	online Responder responses					
4. (	onfigure the revocation provider t	that will process revocation	status requests				
	_						
	< Previous	Next > Finis	h Cancel				
	•						

### (3) 名前に「OCSP001(任意)」と入力し、「Next」をクリックします。

Add Revocation Configuration					
Name the R	Revocation Configuration				
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate Select Signing Certificate Revocation Provider	The Revocation Configuration name is used to help you identify this revocation configuration. It is recommended to use a name that can identify the CA you would like to associate with this Revocation Configuration.           Name:         DCSP001	1			

(4) 「Select a certificate for an Existing enterprise CA」を選択して、「Next」をクリックします。



(5) 「Browse」をクリックして現れた画面で、「acme-Win2012-CA」が選択された状態で、「OK」をクリックします。



# (6) 「Next」をクリックします。



(7) 「Automatically select a signing certificate」が選択された状態で、「Next」をクリックします。

	Add Revocation Configuration	~
Select Signi	ng Certificate	
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate Select Signing Certificate Revocation Provider	Revocation information is signed before it is sent to a client. The Online Responder can select a signing certificate automatically, or you can manually select a signing certificate for each Online Responder.	
	< Previous Next > Finish Cancel	

(8) 「Provider」をクリックします。

	Add Revocation Configuration	?	x
Revocation	Provider		
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate Select Signing Certificate Revocation Provider	A revocation provider is the component of an Online Responder that processes certificate status requests. To view and edit the properties of the revocation provider, click the Provider butto	n.	
	< Previous Next > Finish Can	cel	

(9) 検証用に、「Refresh CRLs based on their validity periods」のチェックを外して、最短の5分に変更し、「OK」をクリックします。(デフォルトでは、証明書を失効しても2日間程度反映されないため。)

Revocation Provider Properties	Revocation Provider Properties				
This revocation provider determines the revocation status of c based on CRLs issued by the CA. Identify the locations for the CRLs.	This revocation provider determines the revocation status of certificates based on CRLs issued by the CA. Identify the locations for the CRLs.				
Base CRLs:					
http://win2012.acme.com/crld/acme-Win2012-CA.crl	Move up Move down				
Add Edit Delete					
Delta CRLs:					
	Move up				
× (	Move down				
Add Edit Delete					
Refresh CRLs based on their validity periods					
Update CRLs at this refresh interval (min): 5					
ОК	Cancel				

### (10)「Finish」をクリックします。

	Add Revocation Configuration ? ×						
Revocation	Provider						
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate Select Signing Certificate Revocation Provider	A revocation provider is the component of an Online Responder that processes certificate status requests. To view and edit the properties of the revocation provider, click the Provider button Provider.						
	< Previous Next > Finish Canc	el					

### (11) 設定した「OCSP001」が、「Working」となったことを確認します。



(12)「Revocation Configuration」 → 「OCSP001」を右クリック → 「Edit Properties」を選択します。



(13) 「Signing」タブ → 「Enable NONCE extension support」にチェックを入れ、「OK」をクリックします。

Properties for Revocation Configuration: OCSP001
Local CRL Revocation Provider Signing
The selected hash algorithm is used by the Online Responders to sign responses sent to clients.
Hash algorithm: SHA1
Do not prompt for credentials for cryptographic operations
Automatically use renewed signing certificates.
<ul> <li>Enable NONCE extension support</li> </ul>
Use any valid OCSP signing certificate
Online Responder Identifiers All responses will include the following Online Responder identifier:
Key hash of the signing certificate
◯ Subject of the signing certificate
OK Cancel Help

# 8.4.4. 証明書プロファイルの OCSP 設定

PA Firewall の証明書プロファイルを設定変更して、OCSP による失効管理ができるようにします。

- (1)「Device」タブ→「証明書の管理」の下の「証明書プロファイル」で表示された、設定済みの「WIN2012-CA-Profile」を クリックします。
- (2) a)「CRL の使用」のチェックを外し、「OCSP の使用」にチェックを入れます。
   b)「WIN2012\_SCEP」をクリックして表示された画面で、
   c)「デフォルト OSCP URL」に「http://win2012.acme.com/ocsp」と入力し、d)「OK」をクリックします。

証明書プロフ	リアイル		C
名前	WIN2012-CA-Profile		
ユーザー名フ ィールド	None	w.	
ユーザー ドメ イン			
CA 証明書	vinzo12_SCEP b)	デフォルト OCSP URL	OCSP 検証証明書
		証明書プロファイル	0
	● 追加 ● 削除	CA 証明書 WIN201 デフォルト OCSP URL http://w	I2_SCEP  vin2012.acme.com/ocsp C
Γ	<u>テフォルト OCSP URL (http://</u> またはh □ CRL の使用	OCSP 校註註明書 None	OK キャンセル
<u> </u>		証明書の有効期限(秒)5	<ul> <li>マイムアワト時间内に証明書次態を取 得できない場合にセッションをプロッ う</li> </ul>
			証明書が認証側デバイスに発行されな かった場合セッションをブロック
			<ul> <li>期限切れ証明書のセッションをブロッ</li> <li>ク</li> </ul>
			<b>d)</b> OK キャンセル

(3) 「コミット」を実施します。

# 8.4.5. GP Agent からのアクセス

クライアント PC(w10-001~w10-003)の GP Agent からアクセスして、失効した w10-003 だけが接続できない状況を確認します。

- (1) w10-001とw10-002は接続できることを確認します。
- (2) CRL と同様に、W10-003 は失効しているので、接続できないことを確認します。



# 8.4.6. PA Firewall の CLI コマンド

PA Firewall の CLI コマンドで、OCSP 取得状況を確認できます。

#### (1) 取得した OCSP の状態確認

admin-admin@Azure-PA-VM> debug sslmgr view ocsp all

Current time is: Tue Apr 23 06:44:03 2019

Count Reaso	n	Serial Number (HEX)	Status	Nex	t l	Jpdate			Revo	ocat	ion	Time		
		Issuer Name Hash OCSP Responder URL												
[	1]	1D000000684A4703D8F85832C00000000006 9737e19d	valid	Apr	24	4 18:35:48	2019	GMT						
[	2]	http://win2012.acme.com/ocsp 1D0000000775C6FD389164B1BB00000000007 9737e19d	valid	Apr	24	4 18:35:48	2019	GMT						
[	3]	http://win2012.acme.com/ocsp 1D0000000849EDE4ABEB4CB8A40000000008 9737e19d http://win2012.acme.com/ocsp	revoked	Apr	24	4 18:35:48	2019	GMT	Apr	23	06:2	25:00	2019	GMT

(2) 取得した OCSP キャッシュの消去

CRL 同様に OCSP もキャッシュされます。 OCSP キャッシュを消去するには、以下 2 つのコマンドを実行する必要があります。

admin-admin@Azure-PA-VM> debug sslmgr delete ocsp all admin-admin@Azure-PA-VM> debug dataplane reset ssl-decrypt certificate-cache

Online Responder のキャッシュが最短でも5分なので、サーバー上でクライアント証明書を失効して、OSCP キャッシュを 消去しても、その失効が反映されるには、最大5分待つ必要があります。

# 8.5. 新規ユーザーだけにクライアント証明書を配布する方法

ここまでの設定で、Active Directory に登録されている既存ユーザーへの SCEP によるクライアント証明書の配布が完了し、「ユーザ名&パスワード + クライアント認証(+失効管理)」という2要素認証が可能となりました。

次に発生する要件として、「既存ユーザーはこの2要素認証を維持しつつ、新入社員にだけクライアント証明書を配布したい」という状況が想定されます。

一つの案として、以下にその方法を記載します。

8.5.1. Active Directory に新グループを追加

「新入社員を AD の User として登録する際に、新入社員用グループ:「Newly-Hired」を割り当てることで、そのグループ だけにクライアント証明書を配布する」という設定方法を示します。

この設定方法を使えば、新入社員が入社したタイミングでは、ADの設定で、そのユーザーにグループを割り当てるだけよく、GlobalProtect設定を変更する必要はありません。

(1) Win2012 の「Administrative Tools」→「Active Directory Users and Computers」を開きます。





(2) Group Name に「Newly-Hired(任意)」と入力し、「OK」をクリックします。

New O	bject - Group					
Create in: acme.com/Users						
Group name:						
Newly-Hired						
Group name (pre-Windows 2000):						
Newly-Hired						
Group scope	Group type					
O Domain local	<ul> <li>Security</li> </ul>					
<ul> <li>Global</li> </ul>	O Distribution					
O Universal						
OK Cancel						

# 8.5.2. グループマッピングの追加

 (1) PA Firewall の「Device」タブ →「ユーザーID」 →「グループマッピング設定」タブで表示された、設定済みの「dc-for-group-mapping」をクリックします。
 a)「許可リストのグループ化」 →「DC=acme, DC=com」を展開 →「cn=users」を展開し、b)「cn=newly-hired」を 選択 → c) [+]をクリックして、d)の状態にします。e)「OK」をクリックします。



(2) 「コミット」を実施します。

### 8.5.3. Portal の設定

Portal のエージェント設定を、Newly-Hired 用に追加します。

(1) 「Network」タブ → GlobalProtect の下の「ポータル」 → 設定済みの「Portal」をクリック → a)「エージェント」タブ → b)設定済みの「GP-Agent」の先頭にチェックを入れ、c)「コピー」をクリックします。

GlobalProtect ポー	-タルの設定					0
全般	エージェント					
認証	■ 設定	ユーザー/ユーザー グル ープ	os	外部ゲートウェイ	クライアント証 書	明
エージェントa)	🔽 GP-Agent	any	any	External-Gateway		
クライアントレ	b)					
サテライト						
	c)					-1
	🕂 追加 🖃 削除 📀 コピー 💽 🛛	EA . ♥ FA				
	■ 信頼されたルート CA トプ	ーカルルート証明書ス Pでインストール	エージェン	ト ユーザーのオーバ ーライド キー	••••	
	PA-Certificate-Authority	ŧ	再入力 エージ	ジェント ユーザーの	••••	
			2	オーバーライド キー		
	🕂 追加 🖃 削除					
				(	OK キャン	セル

(2) a)「認証」タブで、b)名前を「GP-Agent\_for\_NH(任意)」に変更します。b)「SCEP」を選択して、d)設定済みの「WIN2012\_SCEP」を選択します。

設定	0
認証 ユーザー/ユーザー グループ 内部 外部 アプリケーション データ収集	
a) 名前 GP-Agent_for_NH b)	
クライアント証明書 SCEP C) WIN2012_SCEP d)	~
秘密鍵など、選択したクライアントの証明書は、クライアントマシンにインストールされます。	
ユーザー認証情報の保存 Yes	~
認証オーバーライド	
クッキーを生成して認証上書き	
□ クッキーを受け入れて認証上書き	
Cookie 有効期間 Hours 🛛 👻 24	
クッキーの暗号化/復号化用の証 None	
明書	
ダイナミック パスワード(2要素認証)を必要とするコンポーネント	
□ ポータル □ 外部ゲートウエイ-マニュアルのみ	
□ 内部ゲートウエイ-全部 □ 外部ゲートウエイ-自動検出	
保存した認証情報を使用するのではなく、ユーザーを認証するには、ワンタイムパスワード(OTP)などのダイナミックパスワードを使用する オプションを選択してください。それにより、常に選択したオプションごとに新たな認証情報の入力を求めるメッセージが表示されます。	5
ОК <b>+</b> *уъ	۷

(3) a)「ユーザー/ユーザーグループ」タブで、b)「ユーザー/ユーザーグループ」の下で「acme¥newly-hired」を選択しま  $f_{o}c$ )「OK」をクリックします。

設定							0
認証	ユーザー/ユーザー グループ a)	内部 外部	アフ	プリケーション	データ収集		
🗹 ហទ្	ずれか			選択	~		
os	*			■ ユーザー/ユー ■ acme\newly-h acme\domain acme\newly-h	・ザー グループ × ired users ired	b)	~
🕂 追加	□ ■ 削除			●追加 ■削除	:		
						с) <sub>ОК</sub>	キャンセル

(4) a)「GP-Agent\_for\_NH」の先頭にチェックを入れて、b)「上へ」をクリックして、上部へ移動します。
 c)「OK」をクリックします。

GlobalProtect ポー	-タルの設定					0
全般	エージェント					
認証	10 設定	ユーザー/ユーザー グループ	os	外部ゲートウェイ	クライアント証明	
エージェント	GP-Agent_for_NH	cn=newly-hired,cn=users,dc=acme,dc	=com any	External-Gateway	scep a)	
	GP-Agent	any	any	External-Gateway		
クライアントレ						
サテライト						
		b)				- 11
	🕂 追加 🖃 削除 😒 コ	ピー 🕒 上へ 🖻 下へ				
	🔲 信頼されたルート C4	ローカルルート証明書ストア でインストール	エージェント	ユーザーのオーバ ••• ーライド キー	•	-1
	PA-Certificate-Author	ity 🗾	再入力 エージ	ェント ユーザーの •••	•	
			オ・	ーバーライド キー		
	+ 追加 ■ 削除					
					OK =+7	ンセル

- (5) 「コミット」を実施します。
- 8.5.4. 新規ユーザーを「Newly-Hired」グループに入れる

w10-004を新入社員と想定して、「Newly-Hired」グループのメンバーにします。

- (1) Win2012 の「Administrative Tools」 → 「Active Directory Users and Computers」を開きます。
   「acme.com」 → 「Users」で、「w10 004」をクリックします。
- (2) a)「Member Of」タブで、b)「Add」をクリック → c)「Newly-Hired」を追加して、d)「OK」をクリックします。

w10 004 Properties ? X							
Remote control Remote Deskton Services Profile COM+							
Remote control		M+					
General Address	Account Dial in	Organiz	zation				
a)							
Member of:							
Name	Active Directo	ory Domain	Services Folder	r			
Domain Users	acme.com/Us	sers					
Newly-Hired	acme.com/Us	sers			c)		
b)							
Add	Remove						
					-		
Primary group: [	)omain Users						
	There is n	o need to c	hange Primary (	aroup unle	ess		
Set Primary Group	Set Primary Group you have Macintosh clients or POSIX-compliant						
applications.							
d)	ок с	ancel	Apply	He	elp		

### 8.5.5. GP Agent からのアクセス

「Newly-Hired」グループだけにクライアント証明書が配布されることを確認します。

(1) Active Directory の設定を即時反映させたい場合は、PA Firewall で下記のコマンドを実行します。
 (先の設定で、グループマッピング設定を 60 秒に設定していれば、1 分で反映されます。)

admin-admin@Azure-PA-VM> debug user-id refresh group-mapping all

group mapping 'dc-for-group-mapping' in vsys1 is marked for refresh.

(2) w10-004 (Newly-Hired グループのメンバー)からアクセスします。個別のクライアント証明書が発行されることを確認します。

Certificates ×	
Intended purpose: <all> &lt;</all>	
Personal Other People Intermediate Certification Authorities Trusted Root Certification	
Issued To         Issued By         Expiratio         Friendly Name           Image: Win2012-CA         4/22/2021 <none></none>	
	GlobalProtect 🌣
Import Export Remove Advanced Certificate intended purposes	
IP security IKE intermediate View Close	Connected You are securely connected to the corporate network
	x <sup>R</sup> へ 문 (小) <sup>6:51</sup> AM 4/23/2019 ▽

(3) w10-002 がクライアント証明書を保持している場合は削除します。 w10-002 からアクセスします。

「Newly-Hired」グループではないため、クライアント証明書が配布されないので、接続できません。

Certificates	×			
Intended purpose: <all></all>	~			
Personal Other People Intermediate Certification Authorities Trusted Ro	ot Certification 💶 🕨			
Issued To Issued By Expiratio Friend	lly Name			a a
(空)				
			GlobalProtect	\$
			200	
Import Export Remove	Advanced			
Certificate intended purposes				
	View	Gateway	External-Gateway: Req	) uired
	Class	client conta	ertificate not found. Ple Ict your IT administrato	ase r.
	Close		ore a	
		R	ヘ 받 ↓) <sup>6:56 AN</sup> 4/23/20 <sup>-</sup>	19 🖓

 (4) 新入社員(本ガイドでは w10-004)へのクライアント証明書配布完了を確認した後は、Active Directory で、w10-004 から「Newly-Hired」グループを削除する、という運用は必要です。

# 9. ワンタイムパスワード認証の設定

GlobalProtect は、ワンタイムパスワード(以降、OTP)を利用して、認証を強化したい、というニーズに対応することもできます。

本ガイドでは、比較的簡単にインストールできる、RADIUS プロトコルを使った OTP サーバー:RCDevs SA 提供の 「WebADM Server Free Edition」を、ネットワーク構成図中の社内 LAN-B (オンプレミス側) に設置して、利用することにし ます。

# 9.1. Google Authenticator のインストール

OTP には「Google Authenticator」を使いますので、スマートデバイス(iOS または Android)にインストールします。

App Store (iOS) または Google Play (Android) からダウンロード&インストールできます。

# 9.2. OTP サーバーのインストールと設定

# 9.2.1. サーバーの初期設定

(1) 下記の RCDevs の Web サイト Link から、OTP サーバーの仮想マシンイメージをダウンロードします。

https://www.rcdevs.com/downloads/VMWare+Appliances/

	Home	Solutions	Products	Demos	Downloads	News	Forum	Company	Store	Docs	۹
DOWNLOAD SE	ECT	ION	-								
Find below RCDevs' software download categories. Please click on the category you want to enter. For documentation materials, please take a look at our <u>ONLINE DOCUMENTATIONS and HOWTOS</u> . Please contact us at <u>RCDevs Sales</u> for questions and commercial license.											
Virtual Appliance (OpenLDAP – CentOS 7)	*		1.6.9	-3	732M	20	)19-02-12	2	Dow	mload	
Virtual Appliance (OpenLDAP - CentOS 6)	*		1.6.9	-3	447M	20	019-02-12	2	Dow	nload	

(2) 本ガイドでは、社内 LAN-B(サブネット: 10.10.222.0/24)にこの仮想マシンを展開します。
 (RCDevs-VM.ovf ファイルを VMware 環境にインポートします。)

#### (3) 起動後、コンソール画面で、以下の通り設定します。

CentOS Linux 7 (Core) Kernel 3.10.0-957.5.1.el7.x86\_64 on an x86\_64 rcum? login: root (automatic login) Last login: Mon Apr 29 23:52:15 on tty1 -bash: plymouth: command not found Welcome to RCDeus VMWare Appliance 1.6.9! Please identify a location so that time zone rules can be set correctly. lease select a continent or ocean. 1) Africa 2) Americas 3) Antarctica 4) Arctic Ocean 5) Asia 6) Atlantic Ocean 7) Australia 8) Europe 9) Indian Ocean 10) Pacific Ocean 11) none - I want to specify the time zone using the Posix TZ format. #? 5 Please select a country. 18) Israel 35) Palestine36) Philippines 1) Afghanistan 19) Japan 2) Armenia 3) Azerbaijan 37) Qatar 20) Jordan 21) Kazakhstan 38) Russia 4) Bahrain 5) Bangladesh 22) Korea (North) 39) Saudi Arabia 40) Singapore 41) Sri Lanka 42) Syria 23) Korea (South) 6) Bhutan 24) Kuwait Brunei 8) Cambodia 25) Kyrgyzstan 43) Taiwan 44) Tajikistan 9) China 26) Laos 10) Cyprus 11) East Timor 27) Lebanon 28) Macau 45) Thailand 29) Malaysia 46) Turkmenistan 12) Georgia 13) Hong Kong 47) United Arab Emirates 30) Mongolia 14) 31) Myanmar (Burma) 48) Uzbekistan India 32) Nepal 33) Oman 34) Pakistan 15) Indonesia 49) Vietnam 16) Iran 50) Yemen 17) Iraq #? 19 The following information has been given: Japan Therefore TZ='Asia/Tokyo' will be used. Local time is now: Mon Apr 1 11:28:50 JST 2019. Universal Time is now: Mon Apr 1 02:28:50 UTC 2019. This VM is running with dynamic IP assignment (DHCP) The current IP address is 10.10.222.105 Do you want to configure a static IP ([y]/n)? y Please type the fixed IP address [10.10.222.105]: 10.10.222.201 Please type the network mask [255.255.255.0]: gpath.dimeter 255.255.255.0 Please type the gateway address [10.10.222.2]: 10.10.222.2 Please type your primary DNS server IP [8.8.8.8]: 10.9.2.5 Please type your secondary DNS server IP []: 8.8.8.8 Fixed IP address: 10.10.222.201 Network address: 10.10.222.0 Network mask: 255.255.255.0 Gateway IP address: 10.10.222.2 Primary DNS server: 10.9.2.5 Secondary DNS server: 8.8.8.8 Do you confirm ([y]/n): y Writing /etc/sysconfig/network-scripts/ifcfg-ens32 Restarting network... Setting up WebADM server... Choose a directory template: 1) Default configuration (RCDevs Directory) 2) Other generic LDAP server (Novell eDirectory, Oracle, OpenLDAP) 3) Active Directory without schema extention Choose a template number [11]: 3 Please type the name/ip of the LDAP server [localhost]:10.9.2.5 Please type the port fort LDAP [389]: 変更なければ enter 389 Checking port...Ok Checking port...Ok Please choose the encryption ([TLS]/SSL/NONE)?NONE Please type domain FQDN (i.e. dc=lab,dc=local) []:<mark>dc=acme,dc=com</mark> Please type a user with read/write acces to LDAP [cn=Administrator,cn=Users,dc=acme,dc=com]:<mark>cn=admin-admin,cn=Users,dc=acme,dc=com</mark> Please type the user password: Testing user access..Ok Please type the WebADM container [cn=WebADM,dc=acme,dc=com]:

#### ~中略~ (以降、設定はありません。)

Starting services... [ 225.572422] radiusd[5900]: Checking system architecture... Ok [ 225.572422] radiusd[5903]: Checking server configuration... Ok [ 225.57260] webadn[5903]: Checking server configuration... Ok [ 229.85722] radiusd[5901]: Checking server configurations... Ok [ 229.85722] radiusd[5901]: Checking server configurations... Ok [ 229.85723] webadn[5991]: Checking server configurations... Ok [ 229.85723] webadn[5991]: Checking server configurations... Ok [ 229.85724] webadn[5991]: Checking server configurations... Ok [ 229.85724] webadn[5991]: Checking server configurations... Ok [ 229.65777] webadn[5991]: No Enterprise license found (using bundled Freeware license) [ 220.667281] lightsolf: Starting OpenOTP RADIUS Bridge... Ok [ 220.657281] lightsolf: Starting OpenOTP RADIUS Bridge... Ok [ 221.655652] webadn[5991]: Starting UebOM Session server... Ok [ 223.652652] webadn[5991]: Starting UebOM Session server... Ok [ 223.612691] webadn[5991]: Starting UebOM Server: JOM Server 1 (10.9.2.5) [ 223.612691] webadn[5991]: Connected JOM Server: Start Scion Server (1:7.0.0.1) [ 223.612691] webadn[5991]: Connected JOM Server: Session Server (1:1) [ 223.612691] webadn[5991]: Connected JOM Server: Session Server (1:1) [ 223.612691] webadn[5991]: Connected Session server: Session Server (1:1) [ 223.612691] webadn[5991]: Connected Session server: Session Server (1:1) [ 223.612693] webadn[5991]: Checking Server: Session Server (1:1) [ 223.612693] webadn[5991]: Checking Server: Mill Server (1:7.0.0.1) [ 223.612693] webadn[5991]: Checking Server: Session Server (1:1) [ 224.047533] webadn[5991]: Checking Server: Session Serv

### 9.2.2. WebADM の設定

### 9.2.2.1. WebADM の初期設定

- (1) <u>https://10.10.222.201</u> へ、到達可能な PC からアクセスします。
- (2) WebADM に、以下の値を使ってログインします。

, , , , , , , , , , , , , , , , , , ,	
	No Domain has been configured! Please use your LDAP DN for login:
	User DN: cn=admin.admin,cn=use Password: ••••••
	Login
	Applications △ Web Services

User DN: cn=admin-admin,cn=users,dc=acme,dc=com Password: (AD の管理者パスワード)

# (3) ログイン直後の画面です。 画面下方にある「Create default containers and objects」をクリックします。



# (4) 「OK」をクリックします。



# (5) 「logout」をクリックして、一旦 logout します。



(6) 今度は、AD の管理者 Username と Password でログインします。

Freeware Edition v1.6.9-3
Please enter your username and password:
Username: admin-admin
Password:
Login
& Applications On Wab San Joos

# (7) 「Admin」タブをクリックします。



### (8) Local Domains をクリックします。



### (9) 「CN=Default, CN=Domains~」をクリックします。



(10) Object Name に「acme」と入力して「Rename」をクリックします。

CN=Builtin     CN=Computers     CN=Computers     CN=ForeignSecurityPrincip     Q. CN=ForeignSecurityPrincip     Q. CN=Infrastructure	WebADM Freeware Editi Copyright © 2010-2019 RCDevs S	ion v1.6.9-3 6A, Al Rights Reserved learch   Import   Databases   Statistics   Applications	About Logout	۵
CN=LostAndFound		Object CN=acme.CN=Domains.CN=Wel	bADM.DC=acme.DC=com	
CN=Managed Service Accoun			minamahi Prinamanahi kati Prinamana dala	
CN=NTDS Quotas	LDAP Actions	Object Details		
CN=Program Data	Delete this object Obj	ject class(es): bootableDevice, device		
CN=System	Copy this object Cor	nfig type: WebADM LDAP Domain		
CN=TPM Devices	Move this object Obj	ject is valid: Yes [Details]		
E CN=Users (28)	Let Export to LDIF We	bADM settings: 1 settings [CONFIGURE]		
CN=Allowed RODC Password	Unlock WebApp access     Wei	BDADM data: None [EDIT]		
CN=Cert Publishers	CD Advanced edit mode			
CN=Cloneable Domain Contr	Object Name			
CN=Denied RODC Password R			acme	Rename
CN=DnsAdmins	Add Attribute (4)		WebADM User Data	\$ Add
CN=DnsUpdateProxy				
CN=Domain Admins	WebADM Settings		Edit Domain Settings	
CN=Domain Computers	[add values] [delete attribute]		User Search Base: cn=users.dc=acme.dc=com	
CN=Domain Controllers	Object GUID		/670aafc1_cad0_40a1_8772_d7328b05c2821	
CN=Domain Guests	[delete attribute]		{01388101-0800-4381-0112-013200300202}	
CN=Domain Users	WebADM Object Type		WebADM LDAP Domain (Domain)	
CN=Enterprise Admins	Account Modified			
CN=Enterprise Read-only D	[delete attribute]		02-04-2019	
CN=Group Policy Creator O	Account Created		01.01.2010	
CN=Guest	[delete attribute]		01-04-2019	
CN=Protected Users				
CN=RAS and IAS Servers		Apply Changes / Dele	te Selected	

(11) Admin タブをクリックして、以下の状態(先頭が CN=acme)に変化したことを確認します。



# (12) 「Applications」タブをクリックします。 「MFA Authentication Server (OpenOTP)の下 → 「Status: Not Registered」の右横の「REGISTER」をクリックしま



### (13)「Status: Enabled」に変わります。

LDAP Server 1 (Active Directory)	WebADM Freeware E	Edition v1.6.9-3	
No. 13)	Copyright © 2010-2019 RCD		
🗉 🊕 CN=Builtin	Admin Create	Search Import Databases Statistics Applications About Logout	
CN=Computers			
CN=ForeignSecurityPrincip		Registered Applications and Services	
CN=Infrastructure	Categories		
CN=LostAndFound	Categories	Web Services	
CN=Managed Service Accoun	✓ Authentication (2)	MFA Authentication Server (OpenOTP) v1.4.2-2 (Commercial)	
CN=NTDS Quotas	SMS Relay (1)	Multi-factor authentication service supporting OATH	
CN=Program Data	Self-Service (3)	HOTP/TOTP/OCRA, FIDO, YubiKey, SMS OTP and Mail OTP.	
CN=System	Signature (1)	Latest Version: 1 4.3-3 (DOWNLOAD)	
CN=TPM Devices	Single Sign-On (2)	Status: Enabled [CONFIGURE] [REMOVE]	
E CN=Users (30)			
CN=Allowed RODC Password		Service URL (SSL): https://10.10.222.201:8443/openotp/	
CN=Cert Publishers		Service URL (STD): http://10.10.222.201:8080/openotp/	

# 9.2.2.2. OTP の有効化

### ユーザー毎に OTP 登録を行って、OTP 認証ができる状態にします。

(1) まず、w10-001 で OTP が使えるようにします。「CN=w10 001」をクリックします。



(2) 「User Activated:」の右横の「Activate Now!」をクリックします。

- 💓 🔛	T III III DONOOO				
🗉 🚮 🖸	N=Users (28)	WebADM Freeware	Edition v1.6.9-3		
🗆 🗳	CN=Allowed RODC Password	Copyright © 2010-2019 RC			
🗆 🗳	CN=Cert Publishers	Admin Crea	te Search Import Databases Statist	cs Applications About Logout	
🗆 🗉 🤹	CN=Cloneable Domain Contr				
🗆 🧃	CN=Denied RODC Password R		Object CN=w10 001,0	N=Users,DC=acme,DC=com 🕕	
🗆 🧃	CN=DnsAdmins	LDAD Astists	Object Details		
🗆 🧃	CN=DnsUpdateProxy	LDAP Actions	Object Details		
🗆 🛛 💰	CN=Domain Admins	Delete this object	Object class(es): person, user		
🗆 🗖	CN=Domain Computers	Copy this object	Account is unique: tes (in ch=users,dc=acme,o	c=com)	
🗆 🧃	CN=Domain Controllers	Export to LDIF	User activated.		
🗆 🧃	CN=Domain Guests	Change password			
🗆 🗳	CN=Domain Users	Create certificate			
🗆 🗳	CN=Enterprise Admins	Advanced edit mode			
🗆 🗳	CN=Enterprise Read-only D				
🗆 🗳	CN=Group Policy Creator O	Object Name		w10 001	Rename
🗉 🧟	CN=Guest	Add Attribute (14)		Country	
🗆 🖉	CN=Protected Users	Lammalantananana, ( · · · )		Country	₹ Add
🗆 🧳	CN=RAS and IAS Servers	Add Extension (3)		WebADM Account	Add
🗆 🖉	CN=Read-only Domain Contr				
🗆 🗳	CN=Schema Admins	Account Expires		Never	Reset
🗆 🖉	CN=WinRMRemoteWMIUsers	[delete attribute]			
•	CN=admin-admin	Last Bad Logon Password [delete attribute]		30-03-2019	Reset

#### (3) 「Proceed」をクリックします。



### (4) 「Extend Object」をクリックします。

CN=Users (28)     CN=U	WebAOM Freeware Edition v1.6.9-3
CN=Allowed RODC Password	Copyright © 2010-2019 RCDevs SA, All Rights Reserved
CN=Cert Publishers	# Home Admin Create Search Import Databases Statistics Applications About Locout
CN=Cloneable Domain Contr	
CN=Denied RODC Password R	Add Extension WebADM Account to <u>CN=w10 001,CN=Users,DC=acme,DC=com</u>
CN=DnsAdmins	The object will be extended with the objectclass WebADM Account
CN=DnsUpdateProxy	No new attribute will be added to the object during extension.
CN=Domain Admins	
CN=Domain Computers	Extend Object Cancel
- A Obi-Damaia Castallara	

# (5) 「MFA Authentication Server」をクリックします。



### (6) 「Register / Unregister OTP Tokens」をクリックします。

	WebADM Freeware Edition v1.6.9 Copyright © 2010-2019 RCDevs SA, All Rights	-3 Reserved	
CN=Cert Publishers     CN=Cloneable Domain Contr	Admin Create Search Imp	port Databases Statistics Applications About Logout	
CN=Denied RODC Password R	Open	nOTP User Actions for CN=w10 001,CN=Users,DC=acme,DC=com (13	3)
CN=DnsAdmins	Find below the user actions supported by MEA Au	uthentication Server (OpenOTP)	
CN=DnsUpdateProxy	Find below the user actions supported by MFA A	autentication Server (OpenOTP).	
CN=Domain Admins			
CN=Domain Computers		You must register a hardware or software Token before	
CN=Domain Controllers		a user can start using it.	
CN=Domain Guests		You can use this action to update inventory data and enable/disable Tokens too	
CN=Enterprise Admins		Pagister / Unregister EDO Devises	
CN=Enterprise Read-only D		You must register a EIDO Devices	
CN=Group Policy Creator O		start using it.	
CN=Guest		Resynchronize Tokens	
CN=Protected Users		Event-based and time-based tokens can get out of	
(7) 「I use a QRCode-base 表示された QR コードを、 ([例:iOS の場合] 上段	d Authenticator (Event-bas 、スマートデバイスの Google cの[+]をクリックして、下段に	sed)」を選択します。 e Authenticator でスキャンします。 こ表示された「バーコードをスキャン」を	クリックします。)
QRコードスキャンが終れ	っったら、「Register」をクリッ	クします。	
CN=Program Data	WebADM Freeware Edition v1.6.9	-3	
CN=System	Copyright © 2010-2019 RCDevs SA, All Rights	Reserved	
CN=TPM Devices	Home Admin Create Search Imp	port Databases Statistics Applications About Logout	
CN=Users (28)			
CN=Allowed RODC Password	Regist	ter / Unregister OTP Tokens for CN=w10 001,CN=Users,DC=acme,DC	=com
CN=Cert Publishers	You must register a Hardware or Software Token	for the user to start using it.	
CN=Cloneable Domain Contr	The registration consists in synchronizing a Secre	et Key and an initial Token state.	
CN=DesAdmins	Instructions to register a QRCode-based Software	re Token:	
CN=DnsUpdateProxy	1. Install the software Token on the mobile devi	/ice.	
🖸 🂑 CN=Domain Admins	2. Start your software Token and Scan the QR	Code displayed below.	
CN=Domain Computers	3. Click the 'Register' button below after scanni	ling.	
CN=Domain Controllers			
CN=Domain Guests	R	Register Token: Primary Token	
CN=Domain Users	—	Luce a Hardware Token (Inventoried)	
CN=Enterprise Admins		I use a Yubikey Token (Inventoried or YubiCloud)	
CN=Enterprise Read-only D		- Luce a QRCode based Authenticator (Time based)	-
CN=Group Policy Creator O		I use a QRCode-based Authenticator (Event-based	0
CN=Protected Lisers			
CN=RAS and IAS Servers		E State State	
CN=Read-only Domain Contr		三級の必要のない。	
CN=Schema Admins		· · · · · · · · · · · · · · · · · · ·	
CN=WinRMRemoteWMIUsers			マートナハイスの
CN=admin-admin	(E	Enlarge) Google	Authenticator で
CN=ios 001			スキャンする
CN=ios 002			
		自然が記念が見て	
CN=pan agent CN=pu10 001 CN=pu10 001			
CN=w10.002		Optional Information	
CN=w10 003	E	Expiration Date:	
Create / Search			
Details / Check      M     CN=WebADM		Register Cancel	
OU=Domain Controllers			



# 9.2.2.3. OTP の動作確認

Google Authenticator との連携が正しく動作するかをテストします。



🗆 🖉	CN=Read-only Domain Contr	# Home	Admin Create	Search Impor	t Datab	ases Statistics	Applications	About Logout		
🗆 🧃	CN=Schema Admins					ou can use the act	ion to import a P	SKC (KFC-0030)		
🗆 🧃	CN=WinRMRemoteWMIUsers				C	ATH Token key file.				
. 🤇	CN=admin-admin				ء 🌭	xport OATH-PSKC	File			
🗉 🤵	CN=krbtgt				• Y	ou can use the act	ion to export the	registered OATH		
🗉 🤵	CN=pan agent					oken to a PSKC (RI	FC-6030) file.			
•	CN=w10 001				<b>1</b>	est User Authentic	cation			
	CN=w10 002					ou can use this ac	ction to test a us	er authentication		
•	CN=w10 003					ith OpenOTP.				
•	CN=w10 004				- <b>T</b>	est User Confirma	tion			
Cr	reate / Search				Y 1	ou can use this	action to tes	t a transaction		
T De	etails / Check				С	onfirmation with Op	enorp.			
🗄 🐼 C	N=WebADM									
🗉 灥 🖸	U=Domain Controllers					0	Cancel			
Create	Search									

(3) スマートデバイス(例:iOS)の Google Authenticator を開き、 C をクリックして表示された数字が OTP です。



# (4) 「LDAP Password」と「OTP Password」を入力し、「Start」をクリックします。

1.00						75			31 5172	/
	CN=Allowed RODC Password	WebADM Freeware Edition v1.6.9-3	3							
	CN=Cert Publishers	Copyright © 2010-2019 RCDevs SA, All Rights R								5 44
	CN=Cloneable Domain Contr	at these is to be a second sec		0	Va. / I					
	CN=Denied RODC Password R	Admin Create Search Impor	n Databases ;	Statistics	Applications	About	Logout			
	CN=DnsAdmins	Test	t User Authentication	n for <u>CN=w1</u>	001,CN=Use	rs,DC=ac	me,DC=cor	n		
	CN=DnsUpdateProxy	N								
	CN=Domain Admins	You can use this page to test a user OpenOTP auth Some fields are optional and depend on your Open	nentication request.							
	CN=Domain Computers		ion garaton.							
	CN=Domain Controllers	Server Status: Accepting Requests								
	CN=Domain Guests	Server: MFA Authentication Server 1.4.2-2 (WebA	ADM 1.6.9-3)							
	CN=Domain Users	Listener: 10.10.222.201:8080 (HTTP/1.1.SSL)	(64 DIT)							
	CN=Enterprise Admins	Uptime: 27639 (0 days)								
	CN=Enterprise Read-only D	Memory: 825.70K								
	CN=Group Policy Creator O	Active Requests: 0								
	CN=Group-A									
	CN=Group-B		1 1 - <b>1 1</b> - 1	• • •						
	CN=Guest		Login Method:	<ul> <li>Norma</li> </ul>	al O Simple					
	CN=Newly-Hired		Username:	w10-001						
	CN=Protected Users		o o o marrie.	w10-001						
	CN=RAS and IAS Servers		Domain:	acme 🛊						
	CN=Read-only Domain Contr		I DAP Password							
	CN=Schema Admins		Ebra Tubballa.							
	CN=WinRMRemoteWMIUsers		OTP Password:			1				
	ON=admin-admin					_				
	CN=krbtgt		Simulated Client:	[Default	1 🕈					
	Solution CN=pan agent		Simulated Source:							
•	CN=w10 001									
	CN=w10 002		Simulated Options:	:						
	CN=w10 003									
	CN=w10 004		Request Settings:							
*	Create / Search									
H 🔊	CN=WebADM		Browser Context:	ffb2020e	e4aed3a1849	efb5ce78	35335			
□ <u> </u>	OU=Domain Controllers									
Crea	te / Search			Start	Cancel					
T Deta	ils / Check									

### (5) 「Success」と表示されれば、Google Authenticator と同期できています。



(6) 既述の「OTP の有効化」を繰り返して、他ユーザー(w10-002~w10-004)も OTP が使えるようにします。
 (Google Authenticator は、一つのアプリで複数のユーザーを登録できます。)

# 9.3. RADIUS 認証の設定

OTP サーバー:「WebADM Server Free Edition」は RADIUS なので、PA Firewall で、RADIUS 認証に関わる設定を行います。

9.3.1. サービスルートの変更

OTP サーバー(RADIUS サーバー)は、Trust ゾーン側に設置されているので、サービスルートを変更します。

(1) a)「Device」  $\rightarrow$  b)「セットアップ」  $\rightarrow$  c)「サービス」  $\rightarrow$  d)「サービスルートの設定」で表示された画面で、e)のよう に、Radius の送信元インターフェイスおよび送信元アドレスを eth1/2 に変更します。 f)「OK」をクリックします。

paloalto	shboard ACC Monitor Policies	Objects Network	Device	
NETWORKE*         Date           ● セットアップ b)         ● 設定監査           ● パスフード プロファイル         ● 管理者           ● プロファイル         ● 管理者           ● 管理者         ● 一           ● 管理者         ● 一           ● 管理者         ● 一           ● 管理者         ● 一           ● 認知         ● 一           ● 副書の管理         ● 証明書           ● 証明書         ● 証明書           ● 証明書         ● 証明書           ● 証明書         ● 証明書           ● SSL 復号化例外         ● ふ 密客ページ           ● SSL 復号化例外         ● ふ 密客ページ           ● SNL 復号化例外         ● ふ 密客ページ           ● SNA         ● クロファイル           ■ SNMP トラップ         ● Syslog           ● 音子メール         ● HTTP           ■ Netflow         ● ADUS           ● TACCS+         ● LDAP           ● Kerberos         ● SAML アイデンティティ プロバイダ           ● コーガー コーガー データペース         ● コーザー           ● コーガー         ● コーザー	shboard ACC Monitor Policies 管理 操作 サービス インターフェイス サービス 更新サーバー ID の確認 DNS サーバー フライマリ DNS サーバー 10.9.2.5 セカンダリ DNS サーバー 10.9.2.5 セカンダリ DNS サーバー 8.8.8.8 FQDN 更新時間 (秒) 1800 Proxy Server プライマリ NTP サーバー アドレス セカンダリ NTP サーバー アドレス サービス機能 ジサービス ルートの設定 d	Objects         Network           テレメトリー         コンテン           *           iloaltonetworks.com           サービス ルートの設定           すべてに管理インターフ           IPv4           IPv6           アIIa           Netflow           NTP           Panorama           フロセン           マ Radius           SLEP           SNMP トラップ           Syslog           Tacplus           UID Agent           URL Updates           マ Midfire Private           選択されたサービス ルートの	Device a) ツ ID WildFire セッ エイスを使用 ④ カスタマ ズクオルトを使用 デフォルトを使用 フォャー	<ul> <li>ション HSM</li> <li>マイズ</li> <li>ズイズ</li> <li>ズイズ</li> <li>ズクボルトを使用</li> <li>デフォルトを使用</li> </ul>
<ul> <li></li></ul>			, , , , , , , , , , , , , , , , , , ,	OKキャンセル

(2) 「コミット」を実施します。

# 9.3.2. RADIUS サーバープロファイルの設定

RADIUS サーバーとの接続用パラメーターを指定する、サーバープロファイル設定を行います。

(1) a)「Device」タブ  $\rightarrow$  b)「RADIUS」  $\rightarrow$  c)「追加」をクリックします。

	Dashboard	ACC	Monitor	Policies	Objects	Network	Device		
_									
▽ 🕼 サーバー プロファイル	٩								
III SNMP トラップ IIII Syslog	🔲 名前				場所			サーバー	
■ 電子メール									
Netflow									
RADIUS									
Nerderos SAML アイデンティティ プロバ	1								
🛃 マルチ ファクター認証	C) Etaba	御絵 - 👩 つ 🕫							
		- 1 C -							

- (2) a)プロファイル名に「RADIUS-OTP(任意)」と入力します。
  - b)認証プロトコルで「PAP」を選択します。
    - c)「追加」をクリックします。

d)名前に「OTP-Server(任意)」、RADIUS Server に「10.10.222.201」、シークレットに「testing123」と入力します。

RADIUS サーバー プロ	ファイル			0
プロファイル名	RADIUS-OTP 2	1)		
	🗌 管理者使用のみ			
サーバー設定				
タイムアウト (秒	) 3			
再試行	<u>ј</u> 3			
認証プロトコル	PAP	b)		~
サーバー				
名前	RADIUS Server	シークレット	ポート	
OTP-Server	10.10.222.201	******	d) <sub>1812</sub>	
C)				
● 追加				
RADIUS サーバーの IP ア	ドレスまたは FQDN をフ	力してください		
			е) ок	キャンセル
### 9.3.3. 認証プロファイルの設定

認証プロファイルを設定して、GlobalProtect Portal および Gateway が、OTP サーバー(=RADIUS サーバー)をユーザ 一認証サーバーとして利用できるようにします。

(1) a)「Device」  $\rightarrow$  b)「認証プロファイル」  $\rightarrow$  c)「追加」をクリックします。

paloalto	Dashboard ACC	M	lonitor	Policies	Objects Network Device				📥 コミット 🧉 阔 Config	▼ ♀検索
										ら ③ヘルブ
😡 セットアップ	•								1 個0	の項目 🔿 🙁
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	🗆 名前	場所	<b>ロック</b> 許容ログ イン回数	<mark>アウト</mark> ロックア ウト時間 (分)	許可リスト	認証	サーバー ブロファイル	認証ファ クター	その他	ロックされ たユーザー
	C)	) J.Y		0	Cn=domain users,cn=users,dc=acme,dc=com	LDAP	acme-ldap-server		ログイン属性: sAMAccountName パスワード失効メッセージ: 7 日	none

(2) a)名前に「Auth-Profile01(任意)」を入力します。
 「認証」タブで、
 b)タイプは「RADIUS」を選択します。
 c)サーバープロファイルは設定済みの「RADIUS-OTP」を選択します。
 d)ドメインに「acme」と入力します。

認証プロファイル	0
名前 RADIUS-OTP-Profile 2)	
認証 度 詳細	
タイプ RADIUS b)	-
サーバー プロファイル RADIUS-OTP C)	~
□ RADIUS からユーザー グループを取得	
ユーザー ドメイン acme d)	
ユーザー名修飾子 %USERINPUT%	-
シングル サインオン	
Kerberos レルム	
Kerberos キータブ [インポート] をクリックして、このフィールド: X インポート	
OK =++>	セル

(3) a)「詳細」タブ → 許可リストの b)「追加」をクリックします。
 c)グループマッピングの「許可リストのグループ化」で指定したグループ「domain users」を選択します。
 d)「OK」をクリックします。

認証プロファイル	0
名前 RADIUS-OTP-Profile	
認証 度 詳細 a) 許可リスト	
■ 許可リスト▲ ✓ Security constraints of the security o	
● 追加 ● 削除	
アカウントのロックアウト	
許容ログイン回数 0	
ロックアウト時間 (分) 0	
d) OK キャンセノ	IL I

### 9.3.4. External Gateway の認証設定の変更

インターネットからのリモートアクセス VPN の場合だけ、ワンタイムパスワード認証を強制し、社内 LAN では、Active Directory 認証のまま利用する、という形態を想定します。

よって、Portal および Internal Gateway に変更は加えず、External Gateway のみ設定変更します。

(1) 「Network」タブ → GlobalProtect の下の「ゲートウェイ」→設定済みの「External-Gateway」をクリックします。
 a)「認証」タブ → b)設定済みの「ADAuth」をクリックします。

GlobalProtect ゲー	-トウェイ設定						0
全般 認証 a)	サーバー認証 SSL/TLS サービス	、プロフ Ex	ternal_SSL_Service_Profile				~
エージェント	クライアント認証	アイル					
サテライト	■ 名前	os	認証プロファイル	ユーザー名のラベル	パスワードラベル	認証メッセージ	
	ADAuth	Any	Auth-Profile01	Username	Password	Enter login credentials	
	➡追加 ■削除	t 💿 コピー	OLA OTA	_	_	_	
	証明書プロフ	ファイル Wi	N2012-CA-Profile				-
						OK キャン	セル

(2) a)名前に「RADIUS-OTP(任意)」と入力し、b)認証プロファイルは設定済みの「RADIUS-OTP-Profile」を選択します。
 c)「OK」をクリックします。

クライアント認証	0
名前	RADIUS-OTP a)
os	Any
認証プロファイル	RADIUS-OTP-Profile b)
GlobalProtect アプリのログ	ブイン画面
ユーザー名のラベル	Username
パスワードラベル	Password
認証メッセージ	Enter login credentials
	認証メッセージの長さは最大 256 文字です。
	<b>C)</b> OK キャンセル

(3) 「コミット」を実施します。

### 9.4. GP Agent からのアクセス

- (1) OTP 登録したユーザー名を持つクライアント PC から GP Agent で再アクセスします。
- (2) 以下のように、「Enter your TOKEN password」メッセージが出るので、Google Authenticator の OTP を入力し、「OK」をクリックします。

GlobalProtect Login	×	
Sign In Enter your TOKEN password	ок	
٩.	~ 탄 <	x) 1:02 PM ↓ 4/1/2019 ↓

(3) 接続できれば、OTP は正しく設定できています。



### 9.5. 外部からの接続はパスワードとOTP 両方の入力を強制する設定

例えば、以下のような要件があるとします。

- インターネットからの VPN 接続時の認証は、認証強化の目的で、OTP だけでなくパスワードも入力させたい。
- 逆に社内 LAN では、何も入力することなく、自動的に接続させたい。

この要件は、Portal の設定で実現できます。

(1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの「Portal」をクリック →「エージェント」タブ → 設定済みの「GP-Agent」をクリックで表示される a)「認証」タブを開きます。 「ダイナミック パスワード (2 要素認証)を必要とするコンポーネント」の下の b)「外部ゲートウェイ-」で始まる 2 つに

チェックを入れます。c)「OK」をクリックします。

設定						0
認証 a)	ユーザー/ユーザー グル	ープ内部	外部	アプリケーション	データ収集	
/_	名前	GP-Agent				
	クライアント証明書	None		-		
		秘密鍵など、選	択したクラ	ライアントの証明書は、ク	ライアントマシン	vにインストールされます。
	ユーザー認証情報の保存	Yes				▼
認証オ	トーバーライド					
		🗌 クッキーを	主成して認	証上書き		
		🗌 クッキーをき	受け入れて	認証上書き		
	Cookie 有効期間	Hours		▼ 24		
クッ	キーの暗号化/復号化用の証					<b>v</b>
	明書					
ダイナ	・ミック バスワード(2要素認	証)を必要とす	るコンポー	ネント		L 3
	🗌 ポータル				☑ 外部ゲート	ウエイ-マニュアルのみ D)
	□ 内部ゲートウ	フエイ-全部			☑ 外部ゲート	ウエイ-自動検出
保存し オプシ	た認証情報を使用するのでは <sup>た</sup> ョンを選択してください。それ	なく、ユーザーを れにより、常に選	記証する 選択したオ	には、ワンタイムパスワー プションごとに新たな認証	- ド(OTP)などのダ E情報の入力を求る	イナミックパスワードを使用する かるメッセージが表示されます。
						C) OK キャンセル

(2) 「コミット」を実施します。

(3) 外部のクライアント PC(例:w10-002)からアクセスすると、以下のように、External-Gateway が、パスワードの入力を 求めてくるようになります。(この後、OTP(TOKEN)の入力を要求する画面に遷移します。)

GlobalProte	ect X
•	Sign In Enter login credentials
	Gateway: External-Gateway Username w10-002
	Password

(4) 内部のクライアント(例:w10-001)では、いままで通り、認証情報の入力を要求されることなく Internal-Gateway に接続できます。

### 9.6. VPN の再接続時に一定時間は OTP の再入力を必要としない設定

例えば、突然のクライアント PC の停止やサスペンドモードなどによって、一時的に VPN 接続が切断されて、再接続する 場合に、その都度 OTP を入力するのは不便だと感じる場合があります。

それを回避するために、「一度 OTP 認証が成功したクライアント PC は、一定時間は再認証を必要としない」とする設定が可能です。

- (1) 「Network」タブ → GlobalProtect の下の「ゲートウェイ」 → 設定済みの「External-Gateway」をクリックします。
  - a)「エージェント」タブ → b)「クライアントの設定」タブ → c)設定済みの「Auth-Override」をクリックします。 d)「クッキーを生成して認証上書き」&「クッキーを受けいれて認証上書き」の両方にチェックを入れます。

  - e) Cookie 有効期間は、検証用に 5 分に設定します。
  - f) PA Firewall で生成した証明書を一つ(ここでは PA-Certificate-Authority)を選択します。
  - g)「OK」をクリックします。

GlobalProtect ゲ-	ートウェイ設定			_		0
全般	トンネル設定 Timeout Se	tings クライアント IP プール	<b>b)</b> クライアントの設定	ネットワークサービス	動画トラフィック	HIP通知
エージェント	a) 国設定	設定		ゆづール トンクルの分	(#1)	0 2 8
サテライト	Auth-Override C)	名前 Auth-Override			<b>百</b> 7	
		認証オーバーライド	☑ クッキーを生成して言	8証上書き d)		
		Cookie 有効期間	✓ クッキーを受け入れて Minutes	(認証上書き ) 5 e) 5 f)		
		クッキーの暗号化/復号化用の証明	月 PA-Certificate-Authority 書	I)		<b>Y</b>
	🖶 追加 🖨 削除 💿 コピー				g) ок	キャンセル
						OK キャンセル

このことで、一度 External-Gateway で認証が成功すると、External-Gateway が GP Agent に対して 5 分間有効な Cookie を渡します。

5分以内に再認証が行われた場合には、GP Agent はその Cookie を External-Gateway に渡すことで、認証を免除される、という仕組みです。

- (2) 認証が成功したクライアント PC から、5 分以内に再認証を実施します。 「パスワードの入力を要求されない」ことを確認します。
- (3) 認証が成功したクライアント PC から、5 分経過後に再認証を実施します。 「パスワードの入力を要求される」ことを確認します。

(実環境では5分は短すぎるので、デフォルトの24時間または適切と思われる時間を設定してください。)

# 10.macOS からの接続

macOS の GP Agent から VPN 接続を行う場合のステップを記載します。 Windows との動作の差は、ほぼありません。

- ユーザー名: mac-001
- グループ: Domain Users, Newly-Hired (SCEP でのクライアント証明書配布用)
- WebADM で OTP 登録済み

10.1. GP Agent (v4.1.10) のダウンロードとインストール

(1) Web ブラウザで GP Portal: 「gp011.japaneast.cloudapp.azure.com」へ HTTPS でアクセスし、ログインします。



(2) Mac 用の GP Agent をクリックすると、ダウンロードが始まります。



(3) ダウンロードした GlobalProtect.pkg ファイルを展開すると、インストールが始まります。 「Continue」をクリックします。

• • •	💝 Install GlobalProtect	6
	Welcome to the GlobalProtect Installer	
<ul> <li>Introduction</li> <li>Destination Select</li> <li>Installation Type</li> <li>Installation</li> <li>Summary</li> </ul>	You will be guided through the steps necessary to install this software.	
	Go Back Continue	

# (4)「Continue」をクリックします。(Uninstall したい場合にも、この pkg ファイルから実施できます。)

	🥪 Install GlobalProtect		
	Custom Install on "Macintosh HD"		
	Package Name	Action	Size
Introduction	GlobalProtect	Install	25.6 MB
Destination Select	Uninstall GlobalProtect	Skip	Zero KB
Installation Type			
Installation			
Summary			
	Space Required: 25.6 MB	Remainir	ig: 28.78 GB
		Co Pask	Cantinua
		GO Back	Continue

### (5) 「Install」をクリックします。

	😺 Install GlobalProtect	
	Standard Install on "Macintosh HD"	
Introduction	This will take 25.6 MB of space on your computer.	
Destination Select	Click Install to perform a standard installation of this software	
Installation Type	on the disk "Macintosh HD".	
Installation		
<ul> <li>Summary</li> </ul>		
	Go Back Instal	

(6) ここで、インストール権限を持つユーザーのパスワード入力を求められます。 その後、インストールが開始されます。

## 10.2. Portal & Gateway へのアクセス

10.2.1. External Gateway へのログイン

インターネット上の macOS から接続する例です。

(1) 表示された以下の GP Agent の画面で、a) Portal の FQDN:「gp011.japaneast.cloudapp.azure.com」を入力します。
 b) 「Connect たんしいん」ます。



(2) Active Directory に登録されているユーザー名とパスワードを入力し「Sign In」をクリックします。



(3) OTPトークンを入力して、「OK」をクリックします。



### (4) 接続された状態です。



(5) [確認のみ]GP Agent の右上にある 🍄 をクリックして、「Settings」を選択します。

「Connection」タブをクリックして、以下の状態を確認します。

- ۲
- External-Gateway で、Tunnel が Yes Assigned local IP: 172.16.1.x (Pool 設定した IP アドレス)

0	GlobalProtect Settings						
General	Connection	Host Profile	Troubleshooting	Notification			
Gateway		Tunnel	Authenticated	TYPE			
External-Gatew	ay	Yes	Yes	External			
Assigned Loc	al IP: 17	2.16.1.21					
Assigned Loc Gateway IP:	al IP: 17 2	2.16.1.21 B					
Assigned Loc Gateway IP: Protocol:	al IP: 17 2 IP	2.16.1.21 Sec					

optimer			
Bytes In:	9165	Bytes Out:	10195
Packets In:	54	Packets Out:	66
Packets I/Error:	0	Packets O/Error:	0

(6) macOS のキーチェーンアクセスを開きます。

「Newly-Hired」グループのメンバーなので、このユーザー個別のクライアント証明書が発行されています。

		Keychain Access		
Click to lock the	login keychain.			Q Search
Keychains login Local Items System System Roots	Certificate Bundent	mac-001 ssued by: acme-Win2012-CA Expires: Monday, May 3, 2021 18:47:46 This certificate is valid	i Pacific Daylight Time	
	Name	$\sim$ Kind	Expires	Keychain
Category	🕨 📴 mac-001	certificate	May 3, 2021 1	18:47:46 login
A. Passwords Secure Notes				
My Certificates				
T Keys	_			
			1 itom	
			ritem	

(7) Portal に設定したルート証明書も発行されています。

•			Keych	ain Access			
	Click to unlock the	System keychair	1.			Q Sea	rch
	Keychains Iogin Local Items System System Roots	Certificate But	PA-Certificate-A Root certificate auth Expires: Friday, Marc This certificate ha	ority hority ch 27, 2020 1:16:22 P hs custom trust settin	acific Daylight Time Igs	e	
		Name		~ Kind	Expires		Keychain
	Category	PA-Cert	tificate-Authority	certificate	Mar 27, 202	20 1:16:22	System
/ ::::::::::::::::::::::::::::::::::	Passwords Secure Notes My Certificates Keys Certificates	📰 com.apj 📰 com.apj	ole.systemdefault ole.kerberos.kdc	certificate certificate	Sep 13, 203 Sep 13, 203	38 19:49:22 38 19:49:27	System System
		+ i 👓	ру		3 items		

10.2.2. Internal Gateway へのログイン

社内 LAN の macOS から接続する例です。

(1) 最初に Portal ヘログインする際に、Username と Password を入力したので、社内 LAN での接続では、Username と Password を入力することなく、自動的に接続されます。



 (2)「Connection」タブをクリックして、Internal-Gateway である「trust.acme.com」の Authenticated が「Yes」であることを 確認します。

0	GlobalProtect	GlobalProtect Settings								
General Connection	Host Profile	Troubleshooting	Notification							
Gateway	Tunnel	Authenticated	TYPE							
trust.acme.com	No	Yes	Internal							

## 10.3. クライアント証明書の失効

macOS のクライアント証明書を失効させた場合の挙動です。

- (1) ユーザー:mac-001を「Newly-Hired」グループから外し、ADCS でクライアント証明書を失効させます。
- (2) GP Agent から再接続すると、接続に失敗し、クライアント証明書が無効であることを示すメッセージが出力されます。



※ macOS の場合、クライアント証明書を削除して、認証が拒否される動作を確認するのが難しいです。 macOS の場合、キーチェインアクセスからクライアント証明書を削除しても、GP Agent (v4.1.10) が、自身のキャッシュからクライアント証明書を復活させる動作となることを確認しました。 (削除前のシリアル番号と、削除後に復活するクライアント証明書のシリアル番号が同じになっているはずです。)

この点は、Windows GP agent とは異なる点です。

# 11. User-ID でアクセス制御

ここまでの GlobalProtect 設定によって、外部からはもちろんのこと、内部でもユーザー識別が行われる状態になっています。

ここでは、このユーザー識別された情報を使って、アクセス制御する方法を記載します。

### 11.1. ユーザー名でアクセス制御

個々のユーザー単位で、セキュリティポリシーによるアクセス制御を行う例です。

以下の要件を想定します。

- VPN 接続した全クライアント PC から内部 DNS への到達は、主に PA Firewall 経由でのインターネット接続に必要である。
- 一方で、一部の VPN 接続ユーザーのみ、内部サーバーへ接続させたい。 (あるユーザーを急遽一時的に通過させる必要が出てきた場合、など)
- (1) VPN から内部 DNS へ到達するためのセキュリティポリシーを追加します。
   「Policies」タブ →「セキュリティ」で表示されたセキュリティーポリシーに、「VPN-to-Trust-DNS」の行を「VPN-to-Trust」の上に追加します。

						送信元		宛先				
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
1	outbound	none	universal	pag Corp-VPN pag Trust	any	any	any	🕅 Untrust	any	any	any	📀 許可
2	VPN-to-Trust-DNS	none	universal	Corp-VPN	any	any	any	🙀 Trust	any	🔲 dns	👷 application-default	📀 許可
3	VPN-to-Trust	none	universal	Corp-VPN	any	any	any	(22) Trust	any	any	any	📀 許可
4	RDP	none	universal	(22) Untrust	💽 JP	any	any	🚧 Trust	any	🗊 ms-rdp	any	📀 許可
5	intrazone-default 🇠	none	intrazone	any	any	any	any	(intrazone)	any	any	any	📀 許可
6	interzone-default 🅎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否

(2) 「VPN-to-Trust」ポリシーへ、「w10-002」と「w10-003」だけ、内部サーバーに到達させる設定を行います。
 「VPN-to-Trust」をクリックします。

a)「ユーザー」タブ → b)「追加」をクリック →c)「送信元ユーザー」で、例えば"w10"と入力すると、その文字を持つユ ーザーの一覧が表示されます。



(3) a)「acme¥w10-002」と「acme¥w10-003」を追加して、b)「OK」をクリックします。

セキュ	リティポリ	ノシールーノ	r						0
全般	送信元	ユーザー	宛先	アプリケーシ	′ヨン	サービス/URL た	コテゴリ	アクション	
選択		V			any	~			
■ 送(	言元ユーザー no)w10-002	*			HI HI	> プロファイル ▲			
✓ acn	ne\w10-002	a)							
🛨 追加	0 🖃 削除				<b>€</b> 追カ	1 🗖 削除			1
							b)	OKキャン	セル

### (4) 「VPN-to-Trust」のセキュリティポリシーの「ユーザー」列に2つのユーザーが追加された状態です。

					送信元		宛先					
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
1	outbound	none	universal	Corp-VPN	any	any	any	🕅 Untrust	any	any	any	⊘ 許可
2	VPN-to-Trust-DNS	none	universal	Corp-VPN	any	any	any	🕅 Trust	any	🔲 dns	👷 application-default	⊘ 許可
3	VPN-to-Trust	none	universal	Corp-VPN	any	S acme\w10-002 acme\w10-003	any	🚧 Trust	any	any	any	⊘ 許可
5	intrazone-default 🥎	none	intrazone	any	any	any	any	(intrazone)	any	any	any	⊘ 許可
6	interzone-default 🥎	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否

# 

セキュ	リティ ポリシ-	ールール			0
全般	アクション				
アクシ	コン設定			ログ設定	
	アクション	Deny ICMP 送信到達不能	~	<ul> <li>□ セッション開始時にログ</li> <li>✓ セッション終了時にログ</li> </ul>	
プロフ	ァイル設定			ログ転送 None	·
プロ	コファイル タイプ	None	•		
					ו

- (6) 「コミット」を実施します。
- (7) 外部の w10-002, w10-003 は Win2012 の IIS「<u>http://win2012.acme.com</u>」に到達できますが、w10-004 は到達で きないことを確認します。

(Web ブラウザのキャッシュが表示される場合があるので、ブラウザのリロードボタンで確認してください。)

(8)	「Monitor」タブ	$\rightarrow$	「トラフィック」で、	w10-002,	w10-003 (a	t allow、	. w10-004 (a	t deny	であることな	を確認します	す。
-----	-------------	---------------	------------	----------	------------	----------	--------------	--------	--------	--------	----

	受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IPプロトコル	アプリケーション	アクション	ルール	セッション終了理由
Þ	04/29 20:00:00	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
Þ	04/29 19:59:59	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/29 19:59:59	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/29 19:59:54	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/29 19:59:54	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/29 19:59:54	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
Þ	04/29 19:59:51	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
Þ	04/29 19:59:51	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
Þ	04/29 19:59:51	drop	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
Þ	04/29 19:59:27	end	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-rst-from-server
P	04/29 19:59:22	end	Corp-VPN	Trust	172.16.1.6	acme\w10-003	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-rst-from-server

## 11.2. グループでアクセス制御

ユーザ名ではなく、グループ名でのアクセス制御も可能です。

こちらの方が、最初に PA Firewall を設定しておけば、あとは Active Directory 側の設定変更で制御できるので、使い勝手は良いと思います。

### 11.2.1. Active Directory の設定

(1) Win2012 の「Administrative Tools」→「Active Directory Users and Computers」を開きます。
 a)「acme.com」→ b)「Users」を右クリック → c)「New」→ d)「Group」をクリックします。



(2) Group Name に「group-A(任意)」と入力し、「OK」をクリックします。

New Objec	t - Group 🛛 🗙
Create in: acme.com/Users	
Group name:	
group-A	
Group name (pre-Windows 2000):	
group-A	
Group scope	oup type
O Domain local	Security
Global	Distribution
○ Universal	
	OK Cancel

(3) 同様に、「group-B(任意)」も設定します。

(4) ユーザーをグループのメンバーにします。グループ割り当ては以下とします。
 group-A: w10-001, w10-002
 group-B: w10-003, w10-004

	w10 002	2 Prope	rties	? X
Remote control	Remote D	esktop Se	ervices Profile	COM+
General Address Member Of	Account Dial-in	Profile Env	Telephones	Organization
Member of:	Dialini		Informeric	363510115
Name	Active Directo	ory Domain	Services Folde	er
Domain Users	acme.com/Us	sers	1	
group-A	acme.com/Us	sers		
Add	Remove			
Primary group: E	Domain Users There is n you have application	o need to Macintosh ıs.	change Primary clients or POSI	group unless X-compliant
C	ок с	ancel	Apply	Help

### 11.2.2. PA Firewall の設定

グループマッピングで、「group-A」と「group-B」を追加します。

(1) PA Firewall の「Device」タブ → 「ユーザーID」 → 「グループマッピング設定」タブで表示された、設定済みの「dcfor-group-mapping」をクリックします。

a)「許可リストのグループ化」→「DC=acme, DC=com」を展開 → 「cn=users」を展開し、b)「cn=group-a」を選択 → c) [+]をクリック、同様に「cn=group-b」も追加して、d)の状態にします。e)「OK」をクリックします。

グループマッピング	0
名前 dc-for-group-mapping a) サーバー プロファイル ユーザーおよびグループ属性 許可リストのグループ化 カスタム グループ	
使用可能なグループ 会まれたグループ 会まれたグループ 会まれたグループ 会acme\domain users acme\group-a 会acme\group-a 会acme\group-b 会acme\group	
e) OK ++>tel	۷

(2) 「コミット」を実施します。

(3)「VPN-to-Trust」ポリシーへ、「group-B」だけ、内部サーバーに到達させる設定を行います。
 「VPN-to-Trust」をクリックします。
 a)「ユーザー」タブ → b)「追加」をクリック →c)「送信元ユーザー」で「acme¥group-b」のみを追加します。
 (前項で設定したユーザーは削除してください。)



(4) 「VPN-to-Trust」のセキュリティポリシーの「ユーザー」列に「group-b」だけが追加された状態です。

					送信元							
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
1	outbound	none	universal	Corp-VPN	any	any	any	🕅 Untrust	any	any	any	⊘ 許可
2	VPN-to-Trust-DNS	none	universal	Corp-VPN	any	any	any	m Trust	any	🗊 dns	👷 application-default	⊘ 許可
3	VPN-to-Trust	none	universal	Corp-VPN	any	🥵 acme\group-b	any	🚧 Trust	any	any	any	⊘ 許可
5	intrazone-default 🇠	none	intrazone	any	any	any	any	(intrazone)	any	any	any	⊘許可
6	interzone-default 🇠	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否

- (5) 「コミット」を実施します。
- (6) 外部の w10-002~w10-004 のクライアント PC から、Win2012 の IIS「<u>http://win2012.acme.com</u>」にアクセスします。

「group-B」である外部の w10-003, w10-004 は到達できますが、「group-A」の w10-002 は到達できないことを確認 します。(Web ブラウザのキャッシュが表示される場合があるので、ブラウザのリロードボタンで確認してください。)

(7) 「Monitor」タブ → 「トラフィック」で、w10-003, w10-004 は allow、w10-002 は deny であることを確認します。

	受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IPプロトコル	アプリケーション	アクション	ルール	セッション終了理由
<b>P</b>	04/30 12:05:47	end	Corp-VPN	Trust	172.16.1.6	acme\w10-003	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin
<b>P</b>	04/30 12:05:45	end	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin
<b>P</b>	04/30 12:05:32	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
<b>P</b>	04/30 12:05:32	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
Þ	04/30 12:05:32	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny

 本ガイドでは、社内 LAN に接続された「group-A」の w10-001 は、Win2012 と同一サブネットに設置しているので、 「<u>http://win2012.acme.com</u>」にアクセス可能ですが、例えば Win2012 を DMZ ゾーンに設置した場合に、同様の制御 を行えば、社内 LAN からの接続においても、ユーザー名またはグループ名によるアクセス制御が可能です。

# 12. Host Information Profile で制御

Host Information Profile (以降、HIP) を設定することで、端末が持つセキュリティ情報でアクセス制御を行うことができます。一般的に「検疫」と言われる機能です。

例えば、端末の以下のような状態に応じてアクセス制御が可能です。

- アンチウィルスソフトウェアがインストールされているか
- パーソナルファイアウォールが動作しているか
- ハードディスクが暗号化されているか

本ガイドでは、比較的簡単に試すことができる、「パーソナルファイアウォールが動作している端末だけ、社内サーバーへ アクセスさせる」という設定を行います。

### 12.1. HIP 検証用の事前設定

w10-002のWindows10で、Windows標準のパーソナルファイアウォールを停止します。

「Control Panel」→「System and Security」→「Windows Defender Firewall」で表示された画面左側の、 Turn Windows Defender
 Firewall on or off
 をクリックして、パーソナルファイアウォールを停止します。

### 12.2. HIP オブジェクトと HIP プロファイルの設定

(1) a)「Objects」→ b)「HIP オブジェクト」→ c)「追加」をクリックします。

	Dashboard	ACC Monitor	Policies	Objects	Network	Device		
	۹.							
HIP オブジェクト b) ⊡ HIP プロファイル	🗌 名前		場所			カテゴリ	基準	
● 外部ダイナミック リスト								
↓ スパイウェア ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓  ↓								
●URL カテゴリ マ 図 セキュリティ プロファイル								
アンチウイルス								
1 脆弱性防御		)コピー 🎼 PDF/CSV						

(2) a)「全般」タブで、b)名前に「Windows(任意)」と入力します。
 c)「ホスト情報」にチェックを入れ、d)OS で「含む」「Microsoft」「All」を選択します。

HIP オブジェクト									0
全般 a)	設定				_				
モバイル デバイス	名前	Windows		b)					
パッチ管理	内容								
ファイアウォール	- <mark>▽</mark> ホスト情報 - C)								
アンチマルウェア	ドメイン	None	-						
	OS	含む	~	Microsoft	•	All			d) -
77 20 790 51	クライアント バー ジョン	None	♥						
ディスク暗号化	ホスト名	None	~						
データ損失防止	ホスト ID	None	~						
カスタムチェック	ーモバイル デバイス	ネットワーク情報	l –						
	ネットワーク	None							-
	この一致基準はモハ	ベイル デバイスの	みに	適用されます。					
							ОК	+	ャンセル

(3) a)「ファイアウォール」タブで、b)「ファイアウォール」にチェックを入れます。
 c)有効で「yes」を選択し、d)「OK」をクリックします。

HIP オブジェクト		0
全般	Zファイアウォール b)	
モバイル デバイス	✓ インストール済み	有効 yes C
パッチ管理	•	0個の項目s → 🗙
ファイアウォール8	)	
アンチマルウェア		
ディスクバックア		
ディスク暗号化		
データ損失防止		
カスタムチェック	➡ 追加 ■ 削除	
	□ ベンダーの除外	
		d) OK キャンセル

(4) a)「Objects」  $\rightarrow$  b)「HIP プロファイル」  $\rightarrow$  c)「追加」をクリックします。

paloalto	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	
≫タグ ▼ 😮 GlobalProtect					<u>a)</u>			
HIP オブジェクト     DHIP プロファイル b)     の     が部ダイナミック リスト     マ    のカスタム オブジェクト	名前		場所		-	-致		
<ul> <li>■ データ パターン</li> <li>□ スパイウェア</li> <li>● 脆弱性</li> <li>■ 山田 カテゴリ</li> </ul>								
	2) 追加 🕒 削除 🧕	)วช– 🕅 🥸	DF/CSV					

(5) a)名前に「HIP-Profile01(任意)」と入力します。

b) 
⊕「条件の追加」をクリックして表示された左側のウィンドウの c) 
⊕ をクリックすると、d)「一致」に「Windows」が 加えられます。e)「OK」をクリックします。

HIP オブジェクト	/プロフ	ァイル ビル	ダ区	HIP プロファイル	0
● AND ○ OR [	NOT			名前 HIP-Profile01 a) 内容	-
名前 Windows	タイプ	<u>1 個の項目</u> 場所	⇒ ×	一致 <sup>"Windows"</sup> d)	]
	3		<u>c)</u>	① ● 条件の追加 b) e) OK キャンセル	

(6) 「コミット」を実施します。

# 12.3. HIP マッチログの確認

(1) a)「Monitor」タブ → b)「HIP マッチ」で表示されたログで、c)送信元ユーザー列が「acme¥w10-002」であるログの先頭にある

paloalto		Dashboard	ACC	Monitor Po	olicies Objec	ts Network	Device		
▼ <b>@□</b> グ	۹.								
■、トラフィック 動 参感		受信日時	送信元 IPv4	送信元 IPv6	送信元ユーザー	マシン名	オペレーティング システム	HIP	HIP タイプ
Burl フィルタリング	Þ	04/30 14:49:26	10.9.2.6		acme\w10-001	WIN10-001	Windows	HIP-Profile01	profile
NildFireへの送信	Ð	04/30 14:49:26	10.9.2.6		acme\w10-001	WIN10-001	Windows	Windows	object
	P	04/30 14:49:06	172.16.1.8		acme\w10-004	WIN10-004	Windows	HIP-Profile01	profile
■ ユーザー ID	Þ	04/30 14:49:06	172.16.1.8		acme\w10-004	WIN10-004	Windows	Windows	object
☆ トンネル検査     □ マニナ	Þ	04/30 14:48:51	172.16.1.6		acme\w10-003	W10-003	Windows	HIP-Profile01	profile
◎ 設定	Ð	04/30 14:48:51	172.16.1.6		acme\w10-003	W10-003	Windows	Windows	object
R 75-4	Þ	04/30 14:48:24	172.16.1.12		acme\w10-002	WIN10-002	Windows	HIP-Profile01	profile
	Þ	04/30 14:48:24	172.16.1.12		acme\w10-002	WIN10-002	Windows	Windows	object

# (2) w10-002 が持つ HIP の情報の一覧が表示されます。Windows Firewall が停止していることを検出しています。

ロク詳細					
生成済みレポート	04/30/2019 05:53:31				
ユーザー情報	User: w10-002	IP アドレス: 172.16.1.12			
ホスト情報	マシン名: WIN10-002	ドメイン: acme.com			
OS	Microsoft Windows 10 Pro N , 64-bit	ホスト ID: 73f9b513-7053-	14ca-a92c-768	79a3eb5c3	
クライアント バージョン	4.1.10-4				
	インターフェイス	MAC アドレス	IP アドレス		
	PANGP Virtual Ethernet Adapter	02-50-41-00-00-01	172.16.1.12		
ネットワーク情報		02 50 11 00 00 01	fe80::b402:cb	6:92e2:8301	
	Microsoft Hyper-V Network Adapter	00-0D-3A-50-EC-D2	fe80::c90b:9c	le9:a01b:c184	
	Software Loopback Interface 1		127.0.0.1		
アンチマルウェア					
ソフトウェア ベンダー	バージョン エンジン バージ	ョン 定義バージョン 日付	リアルタイ	ム保護 最終ス	(キャン
Windows Defender Microsoft Cor	poration 4.18.1807.18075 1.1.15900.4	1.293.496.0 4/30/20	)19 🗸	n/a	
Disk Backup					
ソフトウェア	ベンダー	バージョン	最終バッ	クアップ	
Windows Backup and Restore	Microsoft Corporation	10.0.17763.1	n/a		
Disk Encryption	Picrosoft Corporation	10.0.17705.1	Tiya		
ソフトウェア	ベンダー		バージ	ョン	
BitLocker Drive Encryption	Microsoft Corp	oration	10.0.17	763.1	
ドライブ	状態				
D:\	unencrypted				
C:\	unencrypted				
Firewall					
ソフトウェア	ベンダー	バージョ	עו	有効	1
Windows Firewall	Microsoft Corporation	10.0.177	63.1	×	
Patch Management	671 <i>4</i> -			15-21-21	方か
Windows Undate Agent	Microsoft Cor	noration		10.0 17763 1	19 X/J
未定義パッチ	Pictosofe Cor	poration		10.0.17703.1	
タイトル				KB 項目 ID	重大度
2019-02 Cumulative Update for	NET Framework 3.5 and 4.7.2 for Windows	10 Version 1809 for x64 (KB4	486553)	4486553	1
Definition Update for Windows D	Defender Antivirus - KB2267602 (Definition 1	.293.501.0)	,	2267602	
二					
アージ損失防止	are di	15-21-21		右州	
ファウエア	~>>-	ハーション		1FI X0	
カスタム チェック					
レジストリ キー					
プロセス					
プロパティ リスト ファイル					

### 12.4. セキュリティポリシーの設定

(1)「Policies」タブ →「セキュリティ」で表示されたセキュリティーポリシーの「VPN-to-Trust」をクリックします。
 a)「ユーザー」タブで、b)「送信元ユーザー」は(残って入れば)全て削除します。

c)「追加」をクリックして、d)設定済みの「HIP-Profile01」を選択します。
e)「OK」をクリックします。

セキュリティ ポリシー ルール									0
全般	送信元	ユーザー a)	宛先	アプリケーシ	′ヨン	サービス/URL ナ	コテゴリ	アクション	
any		~			選択	~			
☑ 送(	言元ユーザー	<b>A</b>		_	🗖 HI	P プロファイル ▲			
			t	)	HIF	P-Profile01	d)		- 1
				Ľ					
					(c)				-1
🕂 追加	🛛 🖃 削除				も追	□□ 削除			
							e)	OK キャン*	セル

(2) 「VPN-to-Trust」の HIP プロファイル列に、「HIP-Profile01」が適用された状態です。

					送信元		宛	包先				
	名前	タグ	タイプ	ゾーン	アドレス	ユーザー	HIP プロファイル	ゾーン	アドレス	アプリケーション	サービス	アクション
1	outbound	none	universal	Corp-VPN	any	any	any	🕅 Untrust	any	any	any	🕏 許可
2	VPN-to-Trust-DNS	none	universal	Corp-VPN	any	any	any	ma Trust	any	📰 dns	👷 application-default	📀 許可
3	VPN-to-Trust	none	universal	Corp-VPN	any	any	n HIP-Profile01	🕅 Trust	any	any	any	📀 許可
5	intrazone-default 🇠	none	intrazone	any	any	any	any	(intrazone)	any	any	any	⊘ 許可
6	interzone-default 🇠	none	interzone	any	any	any	any	any	any	any	any	◎ 拒否

(3) 「コミット」を実施します。

### 12.5. 動作確認

外部の w10-002~w10-004 のクライアント PC から、Win2012 の IIS「<u>http://win2012.acme.com</u>」にアクセスします。

w10-003とw10-004 は到達できますが、Windows Firewall が停止している w10-002 は到達できないことを確認します。(Web ブラウザのキャッシュが表示される場合があるので、ブラウザのリロードボタンで確認してください。)

(-)										=			
	受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	IP プロトコル	アプリケーション	アクション	ルール	セッション終了理由
Þ	04/30 15:37:49	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/30 15:37:49	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/30 15:37:49	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/30 15:37:46	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/30 15:37:46	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
P	04/30 15:37:46	drop	Corp-VPN	Trust	172.16.1.12	acme\w10-002	10.9.2.5	80	tcp	not-applicable	deny	interzone-default	policy-deny
Þ	04/30 15:37:21	end	Corp-VPN	Trust	172.16.1.6	acme\w10-003	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin
P	04/30 15:37:19	end	Corp-VPN	Trust	172.16.1.8	acme\w10-004	10.9.2.5	80	tcp	web-browsing	allow	VPN-to-Trust	tcp-fin

(2) 「Monitor」タブ → 「トラフィック」で、w10-003, w10-004 は allow、w10-002 は deny であることを確認します。

# 12.6. [参考]各種端末の HIP

参考までに、その他の OS の HIP 情報を記載しておきます。

### 12.6.1. macOS

ログ詳細				: 20 €
生成済みレポート	05/04/2019 19:06:36			
ユーザー情報	User: mac-001	IP アドレン	ス: 172.16.1.21	
ホスト情報	マシン名: Takuya's Mac	ドメイン:		
OS	Apple Mac OS X 10.12.6	ホスト ID:	00:0c:29:7f:b4:2d	
クライアント バージョン	4.1.10-4			
	インターフェイス	MAC アドレス	IP アドレス	
ネットワーク情報	en0	00:0c:29:7f:b4:2d	192.168.55.146	
			fe80::1c1f:40ec:22de:750c	
マンチマルウェア				_
アンテマルウェア			リフリクノノク語	目的フォット
	y 19997-939	定義ハーション ロハ	リアルフィム味識	取殺人イヤン
Gatekeeper Apple Inc. 10.12.0			*	nya
Disk Backup				
ソフトウェア べい	ンダー バージ	ヨン最新	<b>ミバックアップ</b>	
Time Machine App	le Inc. 1.3	n/a		
Disk Encryption				
ソフトウェア	ベンター	7.	ージョン	
FileVault	Apple Inc.	10.	12.6	
F717		び懸		
Macintosn HD		unencrypted		
Firewall				
ソフトウェア	×2	ダー バー	ジョン	有効
Mac OS X Builtin Firewall	Apple	e Inc. 10.1	2.6	×
Patch Management				
ソフトウェア	ベンダー	バージョン	有效	b
Software Update	Apple Inc.	2.2.1	×	
未定義バッチ				
タイトル		KB 項目 ID	重大	、度
データ損失防止				
ソフトウェア	ベンダー	バージョン		有効
NA747177				
レジストリキー				
プロセス				
プロパティ リスト ファイル				

# 12.6.2. iOS

ログ詳細					0 =			
生成済みレポート	04/02/2019 14:27:4	46						
ユーザー情報	User: ios-001		IPアド	レス: 172.16.1.8				
ホスト情報	マシン名:	の iPhone	FXT	ドメイン:				
OS	Apple iOS 12.2		ホスト	ホスト ID: 7E0182036 BEB439F3C492				
クライアント バージョン	5.0.4-19							
WiFi SSID								
	インターフェイス	MAC 7F	レス	IP アドレス				
ネットワーク情報	pdp_ip0 pdp_ip1 en0 en1 awdl0 utun1 utun3 ipsec0 ipsec1 utun2	02:00:00:0 02:00:00:0 02:00:00:0	0:00:00 0:00:00 0:00:00	10.56.137.49           re80:11826         2:c163           2001:268:9         :14a8:918           2001:268:9         :14a8:918           2001:268:9         :14a8:918           2001:268:9         :14a8:918           2001:268:10         :6ae:19a:8           2001:268:10         :6ae:19a:8           2001:268:10         :3ae:19a:8           10.137.120.72         re80::309:61ac           re80::664:01         :39:61ac           re80::664:01         :39:61ac           re80::664:01         :69:7c           2001:268:10         :48a:19a:8           re80::664:01         :69:7c           2001:268:10         :48a:19a:8           re80::664:01         :78:97c           2001:268:10         :48a:19a:8           re80::664:01         :78:97c           2001:268:10         :48a:19a:8           re80::664:01         :78:97c           2001:268:10         :48a:19a:8           re80::664:01         :78:97c           2001:268:10         :48a:19a:8	2:8e6d:43cc fc26:54e2 be:ea42 b:3a2:6968 be:ea42 bbe:ea42 bbe:ea42			
モバイル デバイス								
デバイス状態				Sh45 17 ht	All the			
載続ナエックイン日時 				复解日時	700 171			
9 11					, w			
デバイスの準拠性								
管理対象 root 化/jailbre	ak ディスク暗号化が	設定されてい	ません	パスコードが設定されていません	マルウェアあり			
デバイス情報								
デバイス モデル	電話番号	シリアル番号						
IMEI	ICCID	UDID						
		7E0182036	NECON	B439F3C492				
カスタム チェック								
レジストリキー								
プロセス								
プロパティ リスト ファイル	L							

# 12.6.3. Android

ログ詳細					0 🗆 🛛	
生成済みレポート	05/02/2019 14:11:21					
ユーザー情報	User: ard-001			IP アドレス: 172.16.1.15		
ホスト情報	マシン名: KYT31-293c715391			ドメイン:		
OS	Google Android 5.1			ホスト ID: 16184518278e32c		
クライアント バージョン	5.0.0-2					
WiFi SSID	66D0DCAD73C5026179	F2DF027872892E				
	インターフェイス	MAC アドレス		IP アドレス		
ネットワーク情報	wlan0 tun0 lo	80:73:9F:AF:60:A9		192.168.0.14 240:36:e868:1:8273:9fff:fe fe80::8273:9fff:fe6.f60a9 240f:36:e868:1:343e:7d40: 172.16.1.15 ::1	ee63:67a3	
モバイル デバイス						
デバイス状態						
最終チェックイン日時		登録日時			場所	
タ グ					, @	
デバイスの準拠性						
管理対象 root 化/jailbreak	ディスク暗号化が設定	されていません	バスコ	コードが設定されていません	マルウェアあり	
デバイス情報						
デバイス モデル	70	話番号		シリアル番号		
IMEI	10	CID		UDID		
カスタム チェック						
レジストリ キー						
プロセス						
プロパティ リスト ファイル						

# 12.6.4. Linux

ログ詳細			0 =×					
生成済みレポート	03/01/2019 09:33:53							
ユーザー情報	User: ct7-001	Jser: ct7-001 IP アドレス: 10.10.2.10						
ホスト情報	マシン名: centos7	ッン名: centos7 ドメイン:						
os	Linux CentOS 7.6.1810	ホスト ID: CA4248C4-08	3D3-1147-9843-6EC0CDCD3FC1					
クライアント バージョン	5.0.0-79							
	インターフェイス	MAC アドレス	IP アドレス					
ネットワーク情報	eth0	00:0D:3A:51:3B:A3	10.10.2.10 fe80::20d:3aff:fe51:3ba3					
カスタム チェック								
レジストリ キー								
プロセス								
プロパティ リスト ファイ	JL							

# 13.スマートデバイスからの接続

スマートフォンとタブレット PC をまとめて「スマートデバイス」と呼ぶことにします。

iOS で接続する場合を例として、スマートデバイスからの接続を確認します。

### 13.1. SCEP によるクライアント証明書のインポート

### 13.1.1. 課題

iOS や Android は基本的には、アプリケーションから OS の証明書ストア領域への直接のアクセスができないようになっています。

よって、iOS や Android の GP Agent アプリケーションが GP Portal から SCEP で受け取ったクライアント証明書は、そのアプリ内で一時的にキャッシュされるだけで、スマートデバイス OS の証明書ストアには保存されません。

また、iOS や Android の GP Agent アプリケーションが再度 GP Portal へ接続する際には、アプリ内のキャッシュフォル ダを全てクリーンアップしてから接続する仕様になっています。

そのため、「SCEP 利用によるスマートデバイスへのクライアント証明書は、SCEP で配信し続ける」必要があるので、 SCEP 利用の場合は事実上、ID&パスワード認証だけの場合と大差ないことになります。

以降、その挙動を確認します。

13.1.2. 正常な動作の確認

ここまでの設定では、ログインアカウントを「Newly-Hired」グループのメンバーにすることで、SCEP によるクライアント証明書の配布が可能になっていますので、アカウントをその状態にします。

- AD ユーザ名: ios-002
- AD グループ: Domain users (デフォルト) Newly-Hired (SCEP でのクライアント証明書配布用)
- ワンタイムパスワード: WebADM へ登録済み

13.1.2.1. iOS の GP Agent のダウンロード&インストール

App Store ヘアクセスし、GP Agent をダウンロード&インストールします。

21:20	<b>, 11</b> 4G 🔳 )
	⊗ キャンセル
GlobalProtect™ ৺গ্ৰন্ম	開く
$\begin{array}{c c} \hline \\ \hline $	2000     Ja € ●       Implementary     V       Xettarger     V
**/**/*******************************	calitonia-pe Chemai-pe
0         z         x         c         b           123         usee         issi         issi         issi	K28. Nongkang-gar Valand-gar

### 13.1.2.2. External-Gateway へのログイン

- (1) 初期設定です。
  - a) 通知の許可はどちらでも構いません。
  - b) Portal の宛先:「gp011.japaneast.cloudapp.azure.com」を入力します。
  - c) iOS の VPN 設定を許可するかどうかを確認されますので、「Allow」をクリックします。



- d) パスコードを入力します。
- e) 独自サーバー証明書を利用しているので、最初だけは、証明書の警告がでますが「続行」をクリックします。



(2) サインインします。
 a) ユーザ名とパスワードを入力し、「サインイン」をクリックします。
 b) ワンタイムパスワードを入力し、「サインイン」をクリックします。

戻る GlobalProtect		
$+$ $/ \times / \times /$		キャンセル GlobalProtect
		サインイン
gp011.japaneast.cloudapp.azure.com		51212
Enter login credentials		Enter your TOKEN password
Username		Secure ID
ios-002		•••••
Password		
a)		b)
サインイン		サインイン
	$  \rightarrow  $	

(3) 接続完了です。

a)の×をクリックして消去するか、b)をクリックして「次回から表示しない」をチェックしてください。 外部からの接続が成功した場合には c)盾のマークが表示され、d)External-Gatewayと表示されます。



### 13.1.2.3. [参考] Internal-Gateway へのログイン

社内 LAN に接続した場合は、ここまでの Portal および Internal Gateway の設定のままであれば自動的に接続され、 a)家のマークになり、b)Internal Network と表示されます。



13.1.3. SCEP を無効化した場合の動作の確認

ここまでの設定で、Gatewayには証明書プロファイルを設定してクライアント証明書認証を行う状態にしているので、そこに接続できたということは、「iOS にも SCEP によるクライアント証明書の配布はできている」ということになります。

しかし、SCEPを無効にする=ログインアカウントを「Newly-Hired」グループから外すと、接続できなくなります。 そのため、スマートデバイスの場合は、SCEPを無効にすることはできない=配信し続ける必要がある、ということです。



### 13.1.4. スマートデバイスだけに SCEP を常時有効にする

必要最低限の設定だけで、スマートデバイスだけに SCEP でクライアント証明書を配信し続ける方法を記載します。

(1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの「Portal」をクリック → a)「エージェント」タブ →
 b)設定済みの「GP-Agent\_for\_NH」の先頭にチェックを入れ、c)「コピー」をクリックします。

GlobalProtect ポー	ータルの設定						0
全般	エージェント						
認証	□ <sub>設定</sub> 、 b)	ユーザー/ユーザー グループ		OS	外部ゲートウ	±√	クライ アント 証明書
クライアントレ	GP-Agent_for_NH	cn=newly- hired,cn=users,dc=acme,dc=o	com	any	External-Gate	way	scep
55455K	GP-Agent	any		any	External-Gate	way	
サテライト							
	 ●追加 ■削除 <mark>●</mark> コピ	- Ola Ora					
	■ 信頼されたルート CA	ローカルルート証明書ス トアでインストール	エージェン	ット ユー	·ザーのオーバ ーライド キー	••••	
	PA-Certificate-Authority		再入力 エー	ージェン オーバ・	ト ユーザーの ーライド キー	••••	
	● 追加 ■ 削除						
					(	ОК	キャンセル

(2) 「認証」タブで、b)名前を「GP-Agent\_for\_SD(任意)」に変更します。

設定						Ø		
認証 ユーザー/ユーザー グル	ープ内部	外部	アプリケーション	データ収集				
名前	GP-Agent_for_S	SD	b)					
クライアント証明書	SCEP		WIN2012_SCEP			~		
	秘密鍵など、選	択したクラ	イアントの証明書は、ク	ライアントマシン	にインストールされ	<b>こます。</b>		
ユーザー認証情報の保存 Yes								
認証オーバーライド								
クッキーを生成して認証上書き								
	🗌 クッキーを受	そけ入れて調	忍証上書き					
Cookie 有効期間			▼ 24					
クッキーの暗号化/復号化用の証	None					~		
明書								
ダイナミック バスワード(2要素読	(証)を必要とする	5コンポー:	ネント					
□ ポータル				□ 外部ゲート	ウエイ-マニュアルの	み		
内部ゲート	ウエイ-全部			□ 外部ゲート	ウエイ-自動検出			
保存した認証情報を使用するのではなく、ユーザーを認証するには、ワンタイムパスワード(OTP)などのダイナミックパスワードを使用する オプションを選択してください。それにより、常に選択したオプションごとに新たな認証情報の入力を求めるメッセージが表示されます。								
					ОК	キャンセル		

(3) a)「ユーザー/ユーザーグループ」タブで、b)「ユーザー/ユーザーグループ」を削除します。 c)「追加」をクリックして、d)「Android」と「iOS」を追加します。

設定				0
認証 ユーザー/ユーザー グループ a)	内部 外部 アフ	プリケーション 🦷	データ収集	
🔲 いずれか		any	-	
os 🔺		🔲 ユーザー/ユーザー	ー グループ 🔺	
ios d)				b)
C)				
●追加		→追加 ● 削除		_
			e)	OK キャンセル

(4)「GP-Agent\_for\_SD」の先頭にチェックを入れて、b)「上へ」をクリックして、先頭に移動します。

GlobalProtect ポー	-タルの設定				0
全般	エージェント				
認証 エージェント	■ 設定	ユーザー/ユーザー グループ	OS	外部ゲートウェイ	クライア ント証明 書
クライアントし	GP-Agent_for_SD	any	Android iOS	External-Gateway	scep
サテライト	GP-Agent_for_NH	cn=newly- hired,cn=users,dc=acme,dc	any	External-Gateway	scep
	GP-Agent	any	any	External-Gateway	
	●追加 ■削除 ⊙コピー	b) ●上へ			
	🗐 信頼されたルート CA	ローカルルート証明書ス トアでインストール	エージェント	ユーザーのオーバ •••• ーライド キー	
	PA-Certificate-Authority	ų	再入力 エージュ オー	ェント ユーザーの -バーライド キー	
	➡追加 ■ 削除				
				ОК	キャンセル

(5) 「コミット」を実施します。

### 13.1.4.2. 接続確認

- (1) AD 上で、ユーザー:「ios-002」が、まだ「Newly-Hired」グループのメンバーの場合は、そのグループを削除します。
- (2) ユーザー: 「ios-002」で、iOS を使って接続できることを確認します。

### 13.2. 手動によるクライアント証明書のインポート

一般的に、クライアント証明書認証に期待する動作は以下2つです。

- クライアント証明書が失効した端末は接続できない
- クライアント証明書を持っていないデバイスは接続できない

SCEP 利用の場合は既述の通り、スマートデバイスだけには Portal からクライアント証明書を配布し続ける必要があるので、期待する上記 2 つの効果が得られません。

よって上記2つの期待値を満たすには、スマートデバイスにはSCEPは利用せず、手動でクライアント証明書をインポートする方法を検討する必要があります。

iOS12の GP Agent 5.0以降でクライアント証明書を利用するには、「MDM」または「Apple Configurator 2」を使ってインポートする必要があります。

(以下、参考 URL)

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g00000boSUCAY

本ガイドでは、無償で使える「Apple Configurator 2」を使って、iOS ヘインポートするステップを示します。

13.2.1. Certification Authority Web Enrollment のインストール

クライアント証明書と秘密鍵をセットで出力する PKCS#12 形式のクライアント証明書ファイルが生成できるようにするには、Win2012 の Certification Authority Web Enrollment を有効にする必要があります。 (本ガイドでは、既に CA のインストール時に同時にインストール済みですが、念のため、以下にステップを記載します。)

- (1) Win2012 の Server Manager で、「Add roles and features」をクリックします。
- (2) 以下の画面までは「Next」をクリックして進めます。

以下の画面で、「Active Directory Certificate Services」の下の「Certificate Authority Web Enrollment」を選択してイ ンストールを行います。



#### (3) 「Configure Active Directory Certificate Services on the destination server」をクリックします。



### (4) 「Next」をクリックします。



### (5) 「Certificate Authority Web Enrollment」にチェックを入れ、「Next」をクリックします。



### (6) 「Configure」をクリックします。





### 13.2.2. [参考] クライアント証明書発行には IIS の HTTPS 化が必須

Win2012 の Web ブラウザ(IE)で、「http://win2012.acme.com/certsrv/」へアクセスして、クライアント証明書を生成したい ユーザ名とパスワードを入力すると、生成ステップの途中まで進めますが、以下のように警告が出てそれ以上はすすめなく なります。



よって、IISを HTTPS 対応にしなければなりません。

### 13.2.3. IIS の HTTPS 化

IIS を HTTPS 化しますが、「適当なサーバ証明書を割り当てて HTTPS 化すればよい」というものではなく、若干ステップが多めです。

### 13.2.3.1. CA の設定

- (1) Win2012 の Administration Tools から「Certification Authority」を開きます。
- (2) 「acme-Win2012-CA」の下の「Certificate Templates」を右クリックし、「Manage」を選択します。



#### (3) 「Web Server」を右クリックし、「Duplicate Template」を選択します。

		Certificate Templates Consol	e
File Action View Help			
Certificate Templates (Win2012)	Template Display Name	Schema Version	Versi. Actions
	Workstation Authentication	2	101.8 Certificate Tem
	B Web Server	Duplicate Template	4.1 More Actions
	🖳 🖳 User Signature Only	Dupileuce remplace	4.1
	🗵 User	All Tasks	3.1 Web Server
	💷 Trust List Signing	Properties	3.1 More Actions
	Subordinate Certification Authority		5.1
	Register Smartcard User	Help	11.1
	Smartcard Logon	1	6.1
	Router (Offline request)	1	4.1 =
	Root Certification Authority	1	5.1
	I Bara Mara	~	

(4)「General」タブで、「Template display name」に「SSL\_Certificate(任意)」と入力します。「Security」タブで、「Add」をクリックします。

Properties of New Template			Prop	perties (	of New	Template	×
Subject Name Server Issuance Requirements	1	Subject N	lame	Sen	/er	Issuance	e Requirements
Superseded Templates Extensions Security		Compatibility	General	Request	Handling	Cryptograp	hv Kev Attestation
Compatibility General Request Handling Cryptography Key Attestation		Supersed	led Templa	tes	Exte	ensions	Security
Template display name:		Group or use	rnames:				
SSL Certificate		& Authent	ticated Use	rs			
		👗 admin-a	idmin				
		Sector 20 Sector	Admins (A	CME\Dom	ain Admin	s)	
Template name:		as Enterpr	se Aamins	(ACME \E	iterprise A	umins)	
SSL_Certificate							
Validity period: Benewal period:							
						Add	Remove
		Permissions f	for Authenti	icated Use		Allow	( Denv
		Full Contro	d	00.00 000			
Publish certificate in Active Directory		Read	<i>,</i>			~	
Do not automatically reenroll if a duplicate certificate exists in Active Directory		Write					
Directory		Enroll					
		Autoenroll					
		For special p	emissions	or advanc	ed setting	s, click	Advanced
		Advanced.					
OK Cancel Apply Help		L	ОК		Cancel	Apply	Help

(5) 「Object Type」をクリックして、「Computers」にチェックを入れて「OK」をクリックします。

Colort Harry Commutery Convict Accounts on County X	Object Types
Select Users, Computers, Service Accounts, or Groups         Select this object type:         Users, Groups, or Built-in security principals         Prom this location:         acme.com         Enter the object names to select (examples):         Check Names	Select the types of objects you want to find. Object types: Built in security principals         IO: Securits         IO: Computers         IO: Securits         IO: Secur
Advanced OK Cancel	OK Cancel

(6) 「Enter the object name to select」の下で「Win2012」を選択して、「OK」をクリックします。

Select Users, Computers, Service	Accounts, or	Groups X
Select this object type: Users, Computers, Groups, or Built-in security principals		Object Types
From this location: acme.com		Locations
Enter the object names to select ( <u>examples</u> ): Win2012		Check Names
Advanced	ОК	Cancel

(7)「Security」タブで、「Win2012」を選択し、「Enroll」にチェックを入れます。
 「Subject Name」タブで、「Build from this Active Directory information」を選択します。
 「Subject name format:」の下で「Common Name」を選択し、「DNS name」にチェックをいれます。
 「OK」をクリックします。

Properties of New Template	Properties of New Template
Subject Name         Server         Issuance Requirements           Compatibility         General         Request Handling         Cryptography, Key Attestation           Superseded Templates         Extensions         Security	Compatibility         General         Request Handling         Cryptography         Key Attestation           Superseded Templates         Extensions         Security           Subject Name         Server         Issuance Requirements
Group or user names:	Supply in the request Use subject information from existing certificates for autoenrollment renewal requests (")  Build from this Active Directory information Select this option to enforce consistency among subject names and to simplify certificate administration.  Subject name format: Common name Include e-mail name in subject name Include this information in alternate subject name: Email name DIS name DUSer principal name (UPN) Service principal name (SPN)
OK Cancel Apply Help	Control is disabled due to <u>compatibility settings</u> OK Cancel Apply Help

### (8) 「Certificate Templates」を右クリックし、「New」 → 「Certificate Template to Issue」をクリックします。

	Certsrv -	[Certification Authority (Local)\acme-win2012-CA
File Action View Help		
◆ ⇒ 2 0 ₪ 0		
<ul> <li>Certification Authority (Local)</li> <li>a arme-Win2012-CA</li> <li>Revoked Certificates</li> <li>Issued Certificates</li> <li>Pending Requests</li> <li>Failed Requests</li> <li>Certificates</li> <li>Manage</li> </ul>	Name PSec (Offline request) V5 Workstation Authentication OCSP Response Signing Exchange Enrollment Agent (Offline r PSec (Offline request) CEP Encryption	Intended Purpose Client Authentication, IP security IKE intermediate Client Authentication OCSP Signing Certificate Request Agent IP security IKE intermediate Certificate Request Agent
New	Certificate Template to Issue	Firectory Service Email Replication
View Refresh Export List Help		Client Authentication, Server Authentication, Smart Car File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication
	🕮 Computer	Client Authentication. Server Authentication

) 「SSL_Certific	cate」を選択して、「OK」をクリック	フします。	
	Enable Certificate Templates		
Select one Certificate Template Note: If a certificate template th information about this template h All of the certificate templates in For more information, see <u>C</u>	to enable on this Certification Authority. at was recently created does not appear on this list, you may has been replicated to all domain controlliers. the organization may not be available to your CA. ertificate Template Concepts.	need to wait until	
Name	Intended Purpose		^
🗷 Exchange User	Secure Email		
🗷 IPSec	IP security IKE intermediate		
🗷 Key Recovery Agent	Key Recovery Agent		
RAS and IAS Server	Client Authentication, Server Authentication		
Router (Offline request)	Client Authentication		
🗷 Smartcard Logon	Client Authentication, Smart Card Logon		
Smartcard User	Secure Email, Client Authentication, Smart Card Logon		=
SSL_Certificate	Server Authentication		
🚇 Trust List Signing	Microsoft Trust List Signing		
🚇 User Signature Only	Secure Email, Client Authentication		
			~
		)K Cance	el

13.2.3.2. MMC からサーバ証明書を生成

MMC で、先ほど生成した Certificate Template を使って、IIS 用のサーバー証明書を生成します。

(1) Win2012 のデスクトップの左下にある
 表示された画面左上の検索で、「mmc.exe」と入力し、MMC を起動します。



(2) MMC で「File」 → 「Add/Remove Snap-in…」をクリックします。



### (3) 「Certificate」を選んで、「Add」をクリックします。

allable snap-ins: nap-in	Vendor	~	Selected snap-ins:	Edit Extensions
Active Directory Do	Microsoft Cor			Edit Extensions
Active Directory Site	Microsoft Cor			Remove
Active Directory Use	Microsoft Cor	=		
ActiveX Control	Microsoft Cor			Mayella
ADSI Edit	Microsoft Cor			move op
Authorization Manager	Microsoft Cor			Move Down
Certificate Templates	Microsoft Cor		Add >	
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
Disk Management	Microsoft and			
DNS	Microsoft Cor	$\sim$		Advanced
cription:				
o Costificatos seas in alla	un unu te broure	the	contants of the contificate stores for yourself a continu	ar a computer
e Certificates snap-in allo	ows you to browse	the	contents of the certificate stores for yourself, a service	e, or a computer.

# (4)「Computer account」を選択して「Next」をクリックします。 「Local Computer」が選択された状態で、「Finish」をクリックします。

Certificates snap-in	Select Computer
This snap-in will always manage certificates for: My user account Computer account Computer account Computer account Computer account	Select the computer you want this snap-in to manage.         This snap-in will always manage: <ul> <li>Local computer:</li> <li>Another computer:</li> <li>Another computer:</li> <li>Browse</li> </ul> Allow the selected computer to be changed when launching from the command line. This only applies if you save the console. <ul> <li>Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.</li> </ul> <ul> <li>Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.</li> </ul> <ul> <li>Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.</li> </ul>

### (5) 「OK」をクリックします。

	Loc e	_	Selected shap-ins:	
nap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor		Certificates (Local Compute	Pemove
Active Directory Site	. Microsoft Cor	≡		Kellove
Active Directory Use	. Microsoft Cor			
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			
Authorization Manager	Microsoft Cor			Move Down
Certificate Templates	Microsoft Cor		AUU >	
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
Disk Management	Microsoft and	-		Advanced
. DNS	Microsoft Cor	$\sim$		Advanced
(6) 「Console Root」 → 「Certificates (Local Computer)」 → 「Personal」 → 「Certificates」を右クリック → 「All Tasks」→「Request New Certificate…」を選択します。



# (7) 「Next」をクリックします

(7) 「Next」をクリックします。	「Next」をクリックします。
Certificate Enrollment	Certificate Enrollment
Before You Begin The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks. Before requesting a certificate, verify the following:	Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.
Your computer is connected to the network	Active Directory Enrollment Policy v
	Configured by you Add New
Next Cancel	→ Next Cancel
	「Finish」をクリックします。

#### Jerundate」を迭折して「Enron」をクリックします。

Certificate Enrollment     Request Certificates     You can request the following types of certificates. Select the certificates you want to request, and then cick Enroll.     Image:			_ <b></b>			_ <b>D</b> X
Request Certificates   You can request the following types of certificates. Select the certificates you want to request, and the cick forroll.   Improve (Offline request)   Improve (Offlin	Certificate Enrollment			📮 Certificate Enrollment		
You can request the following types of certificates, select the certificates you want to request, and then cick Enroll.	Request Certificates			Certificate Installation F	Results	
IPsec (Offline request)       ↓ STATUS: Available       Details ∨         ▲ More information is required to enroll for this certificate. Click here to configure settings.       IPsec (Offline request) V5       ↓ STATUS: Available       Details ∨         ▲ More information is required to enroll for this certificate. Click here to configure settings.       IPsec (Offline request) V5       ↓ STATUS: Available       Details ∨         ▲ More information is required to enroll for this certificate. Click here to configure settings.       IPsec (Offline request) V5       ↓ STATUS: Available       Details ∨         ○ CCSP Response Signing       ↓ STATUS: Available       Details ∨       IPsec (Offline request) ∨       IPsec (Offline request) ∨       ↓ STATUS: Available       Details ∨         ○ SSL_Certificate       ↓ STATUS: Available       Details ∨       IPsec (Offline request) ∨       ↓ Status: Available       Details ∨         ○ SNow all templates       IPsec (Offline request) ∨       ↓ Status: Available       Details ∨       ↓	You can request the following types of click Enroll.	certificates. Select the certificates you w	ant to request, and then	The following certificates have	e been enrolled and installed on this computer.	
More information is required to enroll for this certificate. Click here to configure settings.         IPSec (Offline request) V5	IPSec (Uttline request)	U SIBIUS: Available		Active Directory Enrollme	nt Policy	
□ IPSec (Offline request) V5       ↓ STATUS: Available       Details ∨         ▲ More information is required to enroll for this certificate. Click here to configure settings.	More information is require	ed to enroll for this certificate. Click here	to configure settings.	SSL_Certificate	🖌 STATUS: Succeeded	Details 🗸
More information is required to enroll for this certificate. Click here to configure settings. Charles Authentication COCSP Response Signing COCSP Response Signing SSL_Certificate SSL_Certificate SSL_Certificate SSL_Certificate Comparison Status: Available Details v Comparison Co	IPSec (Offline request) V5	i) STATUS: Available	Details 🗸			
Cremeros Authentication       Image: Status: Available       Details ~         OCSP Response Signing       Image: Status: Available       Details ~         Image: SSL_Certificate       Image: Status: Available       Details ~         Image: Show all templates       Image: Status: Available       Image: Status: Available	More information is require	ad to enroll for this certificate. Click here	to configure settings.			
□ OCSP Response Signing       ③ STATUS: Available       Details ∨         ☑ SSL_Certificate       ④ STATUS: Available       Details ∨         □ Show all templates       □	Kerberos Authentication	i) STATUS: Available	Details 🗸			
☑ SSL_Certificate     ③ STATUS: Available     Details ∨     ∨       □ Show all templates     □     □	OCSP Response Signing	③ STATUS: Available	Details 🗸 🗮			
Show all templates	✓ SSL_Certificate	(j) STATUS: Available	Details 🗸 🗸			
	Show all templates					
kinich kinich			Enroll Cancel			Finish
			Cancer	$\rightarrow$		

## (8) サーバー証明書が生成されます(テンプレートが「SSL\_Certificate」となっているもの)。

<b>a</b>	Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]							
🚟 File Action View Favorites	Window Help							
🗢 🄿 🖄 🖬 🔏 🖬								
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template	
⊿ 🖈 Certificates (Local Computer)	🕼 acme-Win2012-CA	acme-Win2012-CA	5/6/2024	Server Authentication, Clie	<none></none>		Root Certification Aut	
⊿ 🧮 Personal	🕼 acme-Win2012-CA	acme-Win2012-CA	4/23/2024	<all></all>	<none></none>		Root Certification Aut	
Certificates	🚰 ard-001	acme-Win2012-CA	5/4/2021	Server Authentication	ard-001		Web Server	
Trusted Root Certification A	🕼 ios-002	acme-Win2012-CA	5/4/2021	Server Authentication	ios-002		Web Server	
Enterprise Trust	🕼 Win2012.acme.com	acme-Win2012-CA	4/9/2020	Directory Service Email Rep	<none></none>		Directory Email Replica	
Intermediate Certification A	Win2012.acme.com	acme-Win2012-CA	4/9/2020	Client Authentication, Serv	<none></none>		Domain Controller Aut	
Trusted Publishers	Win2012.acme.com	acme-Win2012-CA	4/9/2020	Client Authentication, Serv	<none></none>		Kerberos Authentication	
Untrusted Certificates	Win2012.acme.com	acme-Win2012-CA	5/18/2019	OCSP Signing	<none></none>		OCSP Response Signing	
Third-Party Root Certificatic	Win2012.acme.com	acme-Win2012-CA	5/5/2021	Server Authentication	<none></none>		SSL Certificate	
Irusted People	Win2012-MSCEP-RA	acme-Win2012-CA	4/21/2021	Certificate Request Agent	<none></none>		CEP Encryption	
Client Authentication Issuer	Win2012-MSCEP-RA	acme-Win2012-CA	4/22/2021	Certificate Request Agent	<none></none>		CEP Encryption	

# 13.2.3.3. IIS の設定

生成したサーバ証明書を、IIS に割り当てます。

- (1) Win2012 の Administration Tools から「Internet Information Service (IIS) Manager」を開きます。
- (2) 「Win2012」→「Sites」→「Default Web Site」を右クリック →「Edit Bindings…」を選択します。



(3) 「Add」をクリックします。「Type:」で https を選択し、「SSL certificate:」で、生成したサーバ証明書を選択し、「OK」をクリックします。

※ 同-	-名のものが複数存在してい	てどれが該当するかわからなし	い場合は「View」をクリックします。
------	---------------	----------------	---------------------

Site Bindings	? X	Add Site Binding	x
Type Host Name Port IP Address Binding Informa http 80 *	Add Edit Remove Browse	Type:       IP address:       Port:         https       V       All Unassigned       443         Host name:	
	Close	OK Canc	el

(4) ※「Subject Alternative Name」に「DNS Name=Win2012.acme.com」と記載されたものが該当します。

	Certificate	^
General Details Certif	fication Path	
Channe Lealle		
SHOW. <aii></aii>	¥	
Field	Value	^
Subject Key Identit	fier 1c 6b 8f 16 e3 aa 01 a6 4d 0	01
Authority Key Iden	ntifier KeyID=c6 d6 43 28 fe 2e f3	3
CRL Distribution Po	ints [1]CRL Distribution Point: Dis	str
Authority Informat	ion Access [1]Authority Info Access: Ac	e
Subject Alternative	Name DNS Name=Win2012.acme.	com
Key Usage	Digital Signature, Key Endpr	ier 🚊
Thumbprint algorith	nm sha1	
Thumbprint	2e 66 44 ec 60 63 ef f6 17 1	a 🗸
DNS Name=Win2012.a	cme.com	
	Edit Properties Copy to	File
		OK

# 13.2.4. クライアント証明書の発行

- (1) Win2012 の Web ブラウザ(IE)から、「https://win2012.acme.com/certsrv/」へアクセスします。
- (2) クラアイアント証明書を生成したいユーザー(例: ios-002)でログインします。



#### (3) 「Request a certificate」をクリックします。

			_ <b>_</b> ×
← ⊖ @ https://win2012.acme.com/certsrv/	- <b>≙</b> ¢	Search	<u>ب</u> ∂ ★ \$
Ø Microsoft Active Directory ×			
Microsoft Active Directory Certificate Services acme-Win2012-C	A		Home
Welcome			
Use this Web site to request a certificate for your Web bro you can verify your identity to people you communicate w upon the type of certificate you request, perform other se	owser, e-mail client, /ith over the Web, si curity tasks.	or other progra gn and encrypt	am. By using a certificate, t messages, and, depending
You can also use this Web site to download a certificate a revocation list (CRL), or to view the status of a pending re	authority (CA) certific equest.	cate, certificate	e chain, or certificate
For more information about Active Directory Certificate So Documentation.	ervices, see <u>Active [</u>	Directory Certifi	icate Services
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL			

#### (4) 「User Certificate」をクリックします。



# (5) 以下のような警告がでますが、「Yes」をクリックします。



## (6) 「Submit」をクリックします。

	_ <b>□</b> ×
← → Mttps://win2012.acme.com/certsrv/certrqbi.asp?type=0	▶ → 命★袋
Microsoft Active Directory ×	
Microsoft Active Directory Certificate Services – acme-Win2012-CA	Home ^
User Certificate - Identifying Information	
No further identifying information is required. To complete your certificate, press submit.	
More Options >>	
Submit >	

## (7) 以下のような警告がでますが、「Yes」をクリックします。



# (8) 「Install this certificate」をクリックします。



# (9) Web ブラウザ(IE)の<sup>20</sup>をクリック → 「Internet Options」を選択します。

			Ŀ	- 🗆 🗙
← ⊖ @ https://win2012.acme.com/certsrv/certrmpn.asp	- <b>≙</b> ¢	Search	- ۵	🟦 🖈 🇱
Microsoft Active Directory ×			Print	· ·
			File	•
Microsoft Active Directory Certificate Services acme-Win2012-CA			Zoom (100%)	•
			Safety	•
Certificate Installed		_	Add site to Apps	
Your now cortificate has been successfully installed			View downloads	Ctrl+J
Tour new certificate has been successfully installed.			Manage add-ons	
		_	F12 Developer Tools	
			Go to pinned sites	
			Compatibility View settings	
		_	Report website problems	
			Internet options	
		_	About Internet Explorer	

## (10)「Content」タブで、「Certificates」をクリックします。

Internet Options							x
General Security Privacy Content Connections Programs Adva							ed
Certific	Certificates						
Use certificates for encrypted connections and identification.							
Clear SSL state Certificates					Publishe	ers	
AutoComplete							
AutoComplete stores previous entries on webpages and suggests matches for you.					Setting	gs	

# (11)「Personal」タブで、「ios 002」のクライアント証明書を選択し、「Export」をクリックします。

	Certifica	tes		x
Intended purpose:	<all></all>			~
Personal Other Peop	le Intermediate Certification	Authorities   Tr	usted Root Certificatio	< >
Issued To	Issued By	Expiratio	Friendly Name	
ios 002	acme-Win2012-CA	5/5/2020	<none></none>	
Import Exp	ort		Adva	nced
Encrypting File System	n, Secure Email, Client Autheni	tication	View	
			Clo	se

# (12)「Next」をクリックします。

「Yes, export the private key」を選択して、 「Next」をクリックします。

X	X
Certificate Export Wizard	Certificate Export Wizard
	S S Certificate Export Wizard
Welcome to the Certificate Export Wizard	Export Private Key You can choose to export the private key with the certificate.
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	Do you want to export the private key with the certificate? • Yes, export the private key
To continue, dick Next	O No, do not export the private key
Next Cancel	Next Cancel
」→ 以下の状態で「Next」をクリックします。	パスワードを入力して、「Next」をクリックします。
x	x
📀 🍠 Certificate Export Wizard	) Sertificate Export Wizard
Export File Format Certificates can be exported in a variety of file formats.	Security To maintain security, you must protect the private key to a security principal or by
	using a password.
Select the format you want to use:	Group or user names (recommended)
O DER encoded binary X.509 (.CER)	Add
O Base-64 encoded X.509 (.CER)	Remove
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
Indude all certificates in the certification path if possible	
<ul> <li>Personal information Exchange - PRCS #12 (PPA)</li> <li>Include all certificates in the certification path if possible</li> </ul>	
Delete the private key if the export is successful	✓ Password:
Export all extended properties	
O Microsoft Serialized Certificate Store (.SST)	Confirm password:
Cancel →	Next Cancel
ファイル名を指定して、「Next」をクリックします。	
ファイル名:「ios-002-user.pfx」	「Finish」をクリックします。
X	x
📀 🥩 Certificate Export Wizard	📀 🕖 Certificate Export Wizard
File to Export Specify the name of the file you want to export	Completing the Certificate Export Wizard
File name:	You have successfully completed the Certificate Export wizard.
- Process Frank, Carrier Screentable Aca care and this	You have specified the following settings:           File Name         C:\Users\admin-admin\Desktop\os-001
	Export Keys Yes Include all certificates in the certification path. Yes
	File Format Personal Information Exchange (*,pfx
	< <u> </u>
Next Cancel	Finish Cancel
	, concer

# 13.2.5. Apple Configurator 2 によるプロファイルの生成と iOS へのインポート

「Apple Configurator 2」を使って、生成したクライアント証明書を iOS ヘインポートします。

- (1) 本ソフトウェアは、macOS 10.14 Mojave にのみ対応していますので、その OS が稼働する Mac を準備します。
- (2) クライアント証明書「ios-002-user.pfx」と、ルート証明書「acme-Win2012-CA」をその Mac にコピーします。
- (3) macOS の App Store で本ソフトウェアを検索し、インストールし、起動します。
- (4) 「ファイル」→「新規プロファイル」をクリックします。

🗯 Apple Configurator 2	<mark>ファイル</mark> 編集 アクション 表	表示 アカウント ウインドウ	ヘルプ
	新規プロファイル 第N	すべてのデバイス	
	新規フルーフリント #B 新規ウインドウ て#N		? ヘルプ Q 検索
すべてのデバイス 監視対象 監	開く… <b>第</b> 0 最近使った項目を開く ▶		

(5) a)「一般」で、名前(任意)を入力します。本ガイドでは「testv2」としています。

🛯 🦂 a) —般	
<b>制限</b> 構成されていません	名前 プロファイルの表示名 - デパイス上に表示されます b)
	testv2
構成されていません	識別子
グローバルHTTPプロキシ     構成されていません	一度のブロファイル面別子 - デバイスにプロファイルをインストールする と、同じ識別子でインストールされたプロファイルがすべて置き換えられ ます
ONSプロキシ	kishimototakuyanoMacBook-Pro.C0C565B2-3104-4A12-B7F4-4
構成されていません	組織
() コンテンツフィルタ	プロファイルを作成した組織の名前
第成されていません	[オプション]
<sup>2</sup> meter 証明書	脱明
の用のせての ドを進き注す	フロファイルの内容や目的の概要

(6) a)「証明書」で「構成」ボタンを押して、c)Win2012のルート証明書「acme-Win2012-CA」を指定します。
 c)[+]をクリックし、d)クライアント証明書「ios-002-user.pfx」を追加します。
 e)にクライアント証明書生成時に指定したパスワードを入力します。

•••			estvz.mobilecomig		
٥	<b>一般</b> 必須	証明書			-+
	<b>制限</b> 構成されていません		<b>証明書名</b> 証明書の名前または説明	b)	C)
	<b>ドメイン</b> 構成されていません		acme-Win2012-CA 証明書または識別子データ		
	<b>グローバルHTTPプロキシ</b> 構成されていません		デパイスに含まれるPKCS1(.cerなど)またはPKCS12(.p12) ファイル		
<b>S</b>	<b>DNSプロキシ</b> 構成されていません		Certificate         acme-Win2012-CA           ルート認証局         有効期限: 2024年5月6日 月曜日 16時38分53秒		
	<b>コンテンツフィルタ</b> 構成されていません		<ul> <li>□ 日本標準時</li> <li>③ "acme-Win2012-CA"証明書は信頼されていま</li> <li>▶ 詳細な情報</li> </ul>		
Chapter States	<b>証明書 る)</b> 2個のペイロードを構成済み				
	<b>証明書の透明性</b> 構成されていません	証明書			- +
P	<b>バスコード</b> 構成されていません		<b>証明書名</b> 証明書の名前または説明	d)	
((;	Wi-Fi 構成されていません		ios-002-user.pfx 証明書または識別子データ		
	VPN 1個のペイロードを構成済み		デバイスに含まれるPKCS1 (.cerなど) またはPKCS12 (.p12) ファイル		
	<b>AirPlay</b> 構成されていません		Certificate 的		
4	<b>AirPlayセキュリティ</b> 構成されていません		130mlik: 2020年5月5日 久曜日 19時30万5449 日本標準時 ③ "ios 002、Users"証明書は信頼されていません		
-	<b>AirPrint</b> 構成されていません		▶ 詳細な情報		
↔	<b>カレンダー</b> 構成されていません		<b>パスワード</b> PKCS12ファイルを保護するパスワード。入力要求なしのインストールの	e)	
M	<b>照会したカレンダー</b> 構成されていません		ために使用されます ••••••		
	Which do				

- (7) a)「VPN」で「構成」ボタンを押して、b)接続名に「GPsslvpn(任意)」と入力します。
  - c) 接続のタイプで「カスタム SSL」を選択します。
  - d) 識別子とサーバには「gp011.japaneast.cloudapp.azure.com」と入力します。
  - e) アカウントには「ios-002」と入力します。
  - f) ユーザ認証で「証明書」を選択して、g) 資格情報で「ios-002-user.pfx」を選択します。

■ 一般 必須	VPN	Corvernophoconny		-+
御限 樹成されていません		<b>接続名</b> 接続の表示名(デバイス上に表示) CPsslynn	b)	
<ul> <li>ドメイン 構成されていません</li> <li>グローバルHTTPプロキシ</li> </ul>		<b>接続のタイプ</b> このポリシーで有効な接続のタイプ	C)	
<ul> <li>         構成されていません     </li> <li> <b>DNSプロキシ</b> 構成されていません     </li> </ul>		■ 調別子 カスタムSSL VPNの識別子 ■ の01 increased to low damp growth growth	d)	
コンテンツフィルタ 構成されていません		gp011,apaneast.cloudapp.azure.com     サーパのホスト名またはIPアドレス     011		
証明書     2個のペイロードを構成済み       2個のペイロードを構成済み     証明書の透明性		gpu11.japaneast.cioudapp.azure.com <b>アカウント</b> 接続を認定するためのユーザアカウント	e)	
パスコード 構成されていません		ios-002 <b>プロバイダバンドル識別子</b> この構成に使用するプロバイダのバンドル識別子		
Wi-Fi 構成されていません		[デバイス上で設定] <b>カスタムデータ</b> カスタムデータのキーと文字列値		
UPN さ) 1個のペイロードを構成済み さ)		キー ^ 値		
<ul> <li>構成されていません</li> <li>AirPlayセキュリティ 構成されていません</li> </ul>				
<b>AirPrint</b> 構成されていません				
<ul> <li>カレンダー</li> <li>構成されていません</li> <li>昭会したカレンダー</li> </ul>		<u>→</u> ー <b>&gt; 認証</b> 接続の認証タイプ 証明書	†)	
満成されていません		<b>資格情報</b> 接続を認証するための資格情報	g)	

- (8) 「ファイル」→「保存」を選択して、任意の場所に、「testv2.mobileconfig」を保存します。
- (9) iOS 端末を、macOS とライトニングケーブルで接続します。
- (10) Apple Configurator 2 が iOS 端末を認識した状態で、「アクション」→「追加」→「プロファイル…」を選択して、 「testv2.mobileconfig」ファイルを選択します。

🗯 Apple Configurator 2 ファイル 編集	<mark>アクション</mark> 表示 アカウント ウインドウ ヘルプ
	<u>追加</u> 別除 変更 書き出す 復元
	<sup>本</sup> <sup>準備…</sup> バックアップから復元… 20 認識した状態
	適用 🕨 💽 🕞 📔
	バックアップ Coogle Kage Coogle
	Ifee 🕒 🎯 💿

# (11) iOS を確認します。 a)「閉じる」をクリックして、「設定」App を確認します。 b)「プロファイルがダウンロードされました」をクリックして表示された画面で、c)「インストール」をクリックします。

14:	14 m	14:05 🕫	ull 4G 😥	14:05 প	atl 4G 👀
ŗ			設定	キャンセル プロファ・	イルをイ… インストール C)
Ama	on Music 5172817	プロファイルがダウ	>>□→□−ドされました <mark>b)</mark> >	testv2	
		▶ 機内モード	$\bigcirc$	署名者 未署名 内容 VPN設定:1	
		ᅙ Wi-Fi 66D0	DCAD73C5026179F2D >	証明書: 2	
		Bluetooth	オン >	詳細	>
	プロファイルがダウンロードさ	(い) モバイル通信	>		プロファイルを削除
X	プロファイルをインストールするには*設 定* Appで再確認してください。	💿 インターネッ	ト共有 オフ >	- · · · / · / · / · / / / / / / / / / /	シロシアゴルと削除
1			$\bigcirc$		
and the second					
		通知 通知	>		
with the second		◀泖 サウンドと触	党 >		
The second		🕒 おやすみモー	۲ >		
- Aller		🔀 スクリーンタ	ть >		
- Alian					
LONGM	Prime video	② 一般	>		
No.		→ 🕄 שאעב - <u>א</u>	センター >	→ <u> </u>	→

下記のような警告が出ますが、d)および e)の「インストール」をクリックします。 e)「完了」をクリックします。

f)「未署名」の状態ですが、クライアント証明書認証としては問題ありません。

14:06 🕫	uti 4G 📢	14:06 🕫		nil 4G 🗩	14:06 🕫		all 🕈 🚳
キャンセル 警告	インストール	キャンセル	警告	インストール		インストール完	了 完了
管理対象外ルート証明書	d)	管理対象外ルート証明書					e)
証明書"acme-Win2012-CA <sup>*</sup> を と、iPhoneにある信頼できる 加されます。"証明書信頼設定" で、この証明書はWebサイト月 ん。	インストールする 証明書のリストに追 で有効にするま 目には信頼されませ	証明書*acme-Win2 と、iPhoneにある信 加されます。*証明書 で、この証明書はW ん。	012-CA"をイ 頼できる証明 信頼設定"で ebサイト用に	ンストールする 月書のリストに追 有効にするま こは信頼されませ	() 第名: 内:	testv2	f)
					学知	10077101-12	!/:
VPN		VPN			pt-mu		~
お使いのiPhoneのネットワーク VPNサーバより保護、フィルタ 視されている可能性があります	クトラフィックは ≀リング、または監 ⁻。	お使いのiPhoneのネ VPNサーバより保護 視されている可能性	ットワークト 、フィルタリ があります。	、ラフィックは リング、または監			
未署名のプロファイル		未署名のプロファイル					
このプロファイルは署名されて	いません	このプロファイルは	署名されてい	ません			
		<b>1</b>	ンストール -ャ <b>ンセル</b>	e)			
		→		-	$\rightarrow$		_

# 13.2.6. Portal の設定変更

SCEP 利用のステップで、スマートデバイスへはクライアント証明書を常時配布する設定にしているはずですので、それを 停止します。

- (1) 「Network」タブ → GlobalProtect の下の「Portal」 → 設定済みの「Portal」をクリック → a)「エージェント」タブ →
   b)設定済みの「GP-Agent\_for\_SD」をクリックします。
- (2) a)クライアント証明書を「None」に設定して、b)「OK」をクリックします。

設定						0
認証 ユーザー/ユーザー グル	ノープ 内部	外部	アプリケーション	データ収集		
名前	GP-Agent_for_S	D				
クライアント証明書	None		▼ a)			
	秘密鍵など、選	沢したクラ	ライアントの証明書は、ク	ライアントマシン	にインストールされ	ます。
ユーザー認証情報の保存	¥ Yes					~
認証オーバーライド						
	🗌 クッキーを生	成して認	証上書き			
	🗌 クッキーを受	け入れて	認証上書き			
Cookie 有効期間			▼ 24			
クッキーの暗号化/復号化用の証	None					~
明書						
ダイナミック バスワード(2要素語	8証)を必要とする	コンポー	ネント			
□ ポータル				□ 外部ゲート!	ウエイ-マニュアルのる	Ъ
□ 内部ゲート	ウエイ-全部			□ 外部ゲート !	ウエイ-自動検出	
保存した認証情報を使用するのでは オプションを選択してください。そ	なく、ユーザーを れにより、常に選	認証する( 択したオン	こは、ワンタイムパスワー プションごとに新たな認証	-ド(OTP)などのダ E情報の入力を求め	イナミックパスワー かるメッセージが表示	ドを使用する tされます。
					b) ок	キャンセル

- (3) 「コミット」を実施します。
- 13.2.7. iOS からのアクセス

外部の iOS から接続できることを確認します。

GlobalProtect	15:45 🕫	<b>() \$</b> In
接続済み 建築構造	<u> </u>	alProtect
使数済存 Eternal-Gateway		
Image: State Stat		
使続声み 提続声子 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		
接続满み 接続満み External-Gateway	******************	
iteista a		
使数满存? 提数满存?	*********	
接続済み 接続済み External-Gateway		
接続済み 接続済み		
12 Martin 12 Martin 12 Martin 12 Martin 12 Martin 12 Martin 14 Mar		
接続済み 接続済み External-Gateway	111.	
接続済み 提続済み		
增越清み 可能 External-Gateway	····	
提起済み 可能 External-Gateway		
提続声74		
The External-Gateway		<b>ទ続済み</b>
्यागि External-Gateway		
عليه المراجع ال		
्रागि External-Gateway	*******	
्यागि External-Gateway		
۲ الله External-Gateway		
ျှ/ု External-Gateway		
ျှ/ါ External-Gateway		
יון אין External-Gateway		
ျှ/ါ <mark>၊</mark> External–Gateway		
ulle External-Gateway		
ျ/။ External-Gateway		
	External-Gatewa	iý

以上で終了です。

# 14.おわりに

PA Firewallのアドオン機能である GlobalProtectの基本的な設定方法に関しては以上です。

パロアルトネットワークスでは、この他にも様々なセキュリティソリューションを展開しています。

- Cortex XDR
  - ネットワーク、エンドポイント、クラウドから集めたログデータを、総合的かつ多面的に判断して脅威を検知および 対処する Detection & Response サービス
- Prisma Access
  - 遠隔拠点やモバイルユーザーの VPN アクセスを、エンタープライズレベルのセキュリティで提供するクラウド型 VPN サービス
- Prisma SaaS
- SaaS セキュリティに特化した、Cloud Access Security Broker (CASB)サービス
- Prisma Public Cloud
  - パブリッククラウド環境で生じる新たなセキュリティ脅威を検出/排除し、コンプライアンス準拠を継続的にサポート するクラウドベースのセキュリティサービス

これらの強力なセキュリティソリューションによって、パロアルトネットワークスが、皆様のネットワークが抱える様々なセキュリティの課題を包括的に解決することができます。

これらの具体的な内容に関しては、弊社にお気軽にお問合せください。

また本ガイドに記載されていない PA シリーズの設定方法に関するより詳細が必要な場合は、各種 WEB サイトにてご確認いただくか、ご購入元にお問い合わせください。

<パロアルトネットワークス WEB サイトの紹介>

パロアルトネットワークス総合サイト https://www.paloaltonetworks.jp/

ナレッジベース総合サイト(英語) https://support.paloaltonetworks.com/

ライブコミュニティ(英語・一部日本語) https://live.paloaltonetworks.com/

パロアルトネットワークス株式会社 〒100-0010 東京都千代田区内幸町2丁目1-番6号 日比谷パークフロント 15 階

本資料はパロアルトネットワークスのエンジニアが特定のソフトウェアバージョンの動作仕様に基づいて作成した構築・設計を補助するための資料であり、 メーカー公式資料とは異なります。資料の記載内容に誤りがあった際には指摘に基づいて修正を行いますが、内容についての責任は一切負いません。 また、修正、変更、改訂は予告無く行われます。