

リモートアクセスだけではない！  
GlobalProtectのヒミツ。



# 目次

- GlobalProtectの概要
- GlobalProtectの動作
- [参考] Windowsでの接続方法
- [参考] iOSでの接続方法
- まとめ

# GlobalProtectの概要

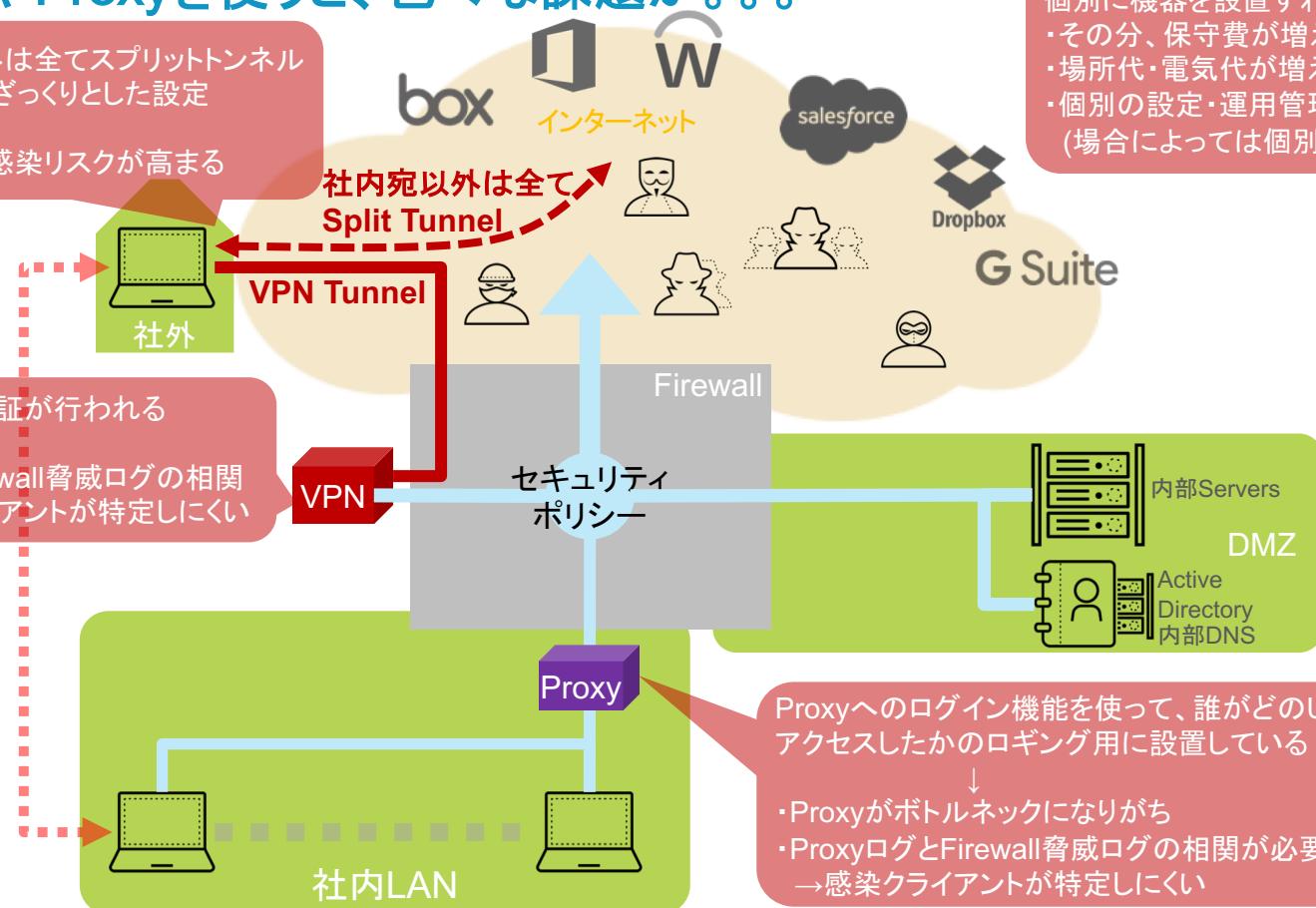
# VPN装置やProxyを使うと、色々な課題が。。。

社内サブネット宛以外は全てスプリットトンネルを使う、というような、ざっくりとした設定

↓  
インターネットからの感染リスクが高まる

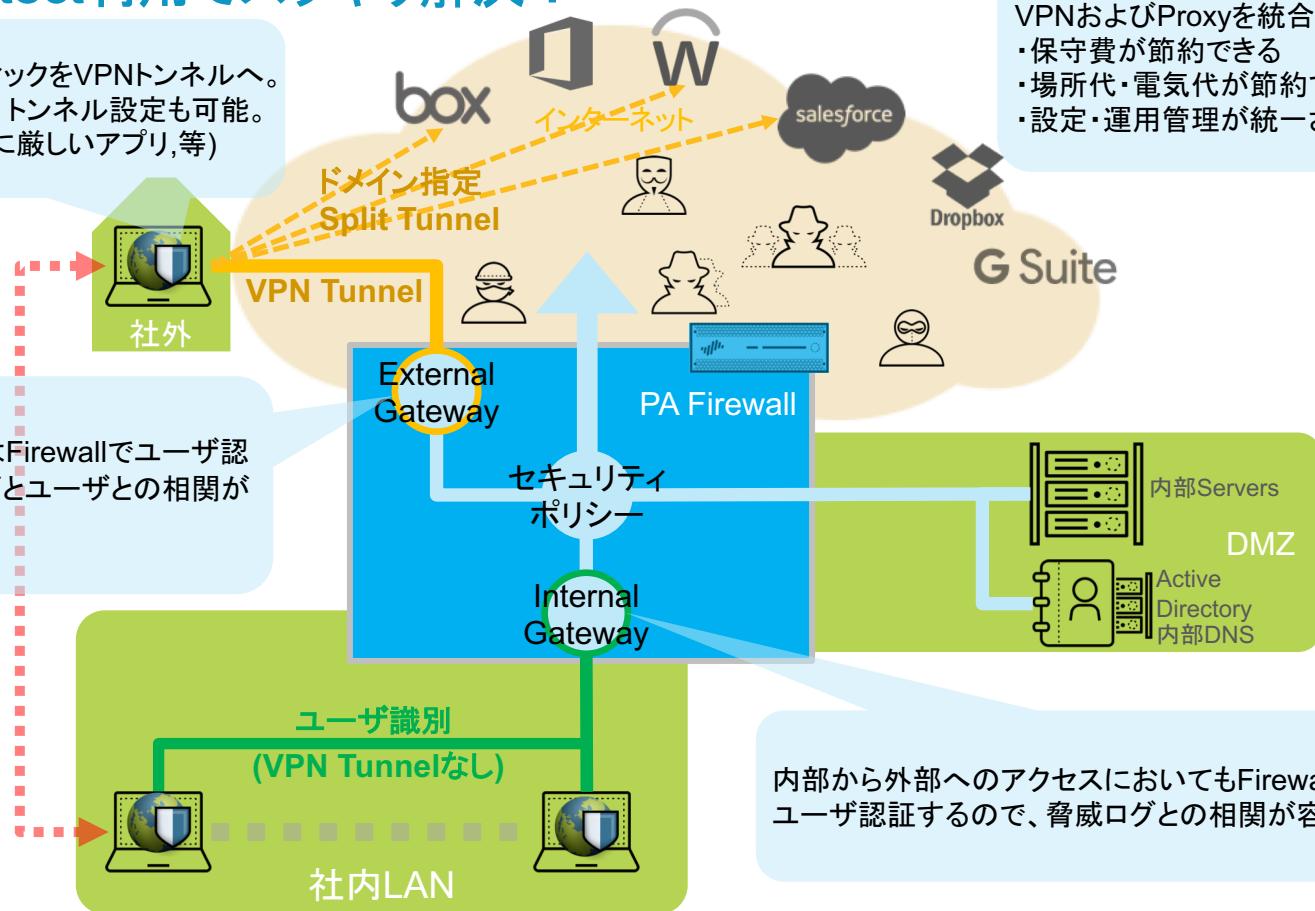
VPN装置でユーザ認証が行われる

↓  
・VPN認証ログとFirewall脅威ログの相関が必要 → 感染クライアントが特定しにくい



# GlobalProtect利用でスッキリ解決！

- ・基本は全てのトラフィックをVPNトンネルへ。
- ・きめ細かいスプリットトンネル設定も可能。  
(広帯域アプリ/遅延に厳しいアプリ、等)



# 概ねVPN専用装置は。。。

- 脅威防御の機能を持っていない。
  - 結果、Net-Generation Firewallに委ねる。
- 内部プロキシの代わりになることはできない。
  - 内部LANのユーザーを(VPNトンネルを確立しないで)識別する機能がない。
  - クライアントがアクセスしたWebサイトのURLをロギングする機能がない。
- 検疫的な動作は、外部からのリモートアクセスに限定される。
  - リモートアクセス時にVPN端末の情報を収集できるが、内部LANで利用することは想定されていない。
- スプリットトンネルは「社内サブネット以外全て」というざっくり設定。
  - インターネットへはほぼそのまま通信する形態。
  - 脅威への感染リスクが高まる。かなり危険。

# GlobalProtectなら!

## Next Generation Firewallによる高度な脅威防御が使える

- ・アプリケーション識別
- ・DNSセキュリティ(New)、IPS、アンチウィルス、アンチスパイウェア、URLフィルタリング、ゼロデイ攻撃の脅威検出 (Wildfire)

## 内部プロキシーの代わりとして動作できる

- ・ユーザ識別 (しかも自動的にログイン)
- ・URLロギング (ロギングだけならライセンス不要)

## 内外問わず、検疫的な動作ができる

- ・リモートアクセス時だけでなく、内部LANにいる場合でも端末情報を収集し、ポリシーを適用できる

## きめ細かいスプリットトンネル設定ができる

- ・ドメイン単位
- ・ビデオストリーミングはアプリケーション単位

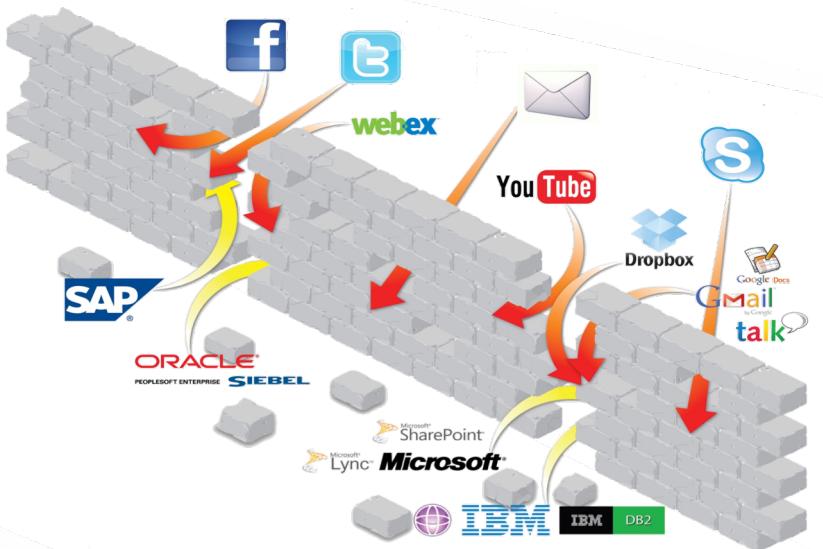


# GlobalProtectの概要: Next Generation Firewallによる高度な脅威防御が使える

# App-ID™ : アプリケーションを識別することの必要性

## 従来型ファイアウォールの問題点

- ・アプリケーション識別機能なし
- ・ポート番号ではアプリケーション制御不可能
- ・暗号技術の広がり (SSL)
- ・外部へのボットネット通信(C&C)検知不可能



パロアルトネットワークスの  
次世代ファイアウォール PAシリーズ

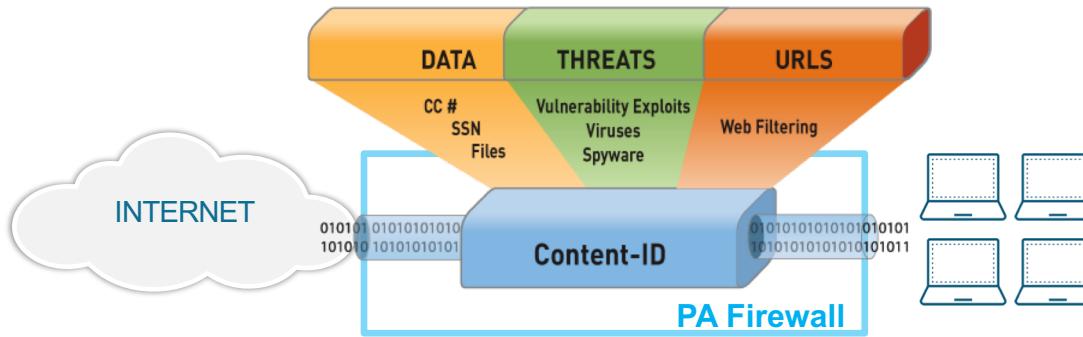


## トラフィックをアプリケーション識別 すべて「見える化」App-ID

- ・アプリケーション単位でアクセス許可/禁止が可能 (例)P2P、宅ファイル便、Dropbox、Twitter、Skype、2チャンネルなどの利用ログや利用禁止など
- ・認知できないアプリケーションの禁止 潜在的セキュリティリスクの低減が可能



# Content-ID™:高速処理を実現したコンテンツセキュリティ



## シングルエンジン＆ストリームベースで3つのコンテンツセキュリティ機能を提供

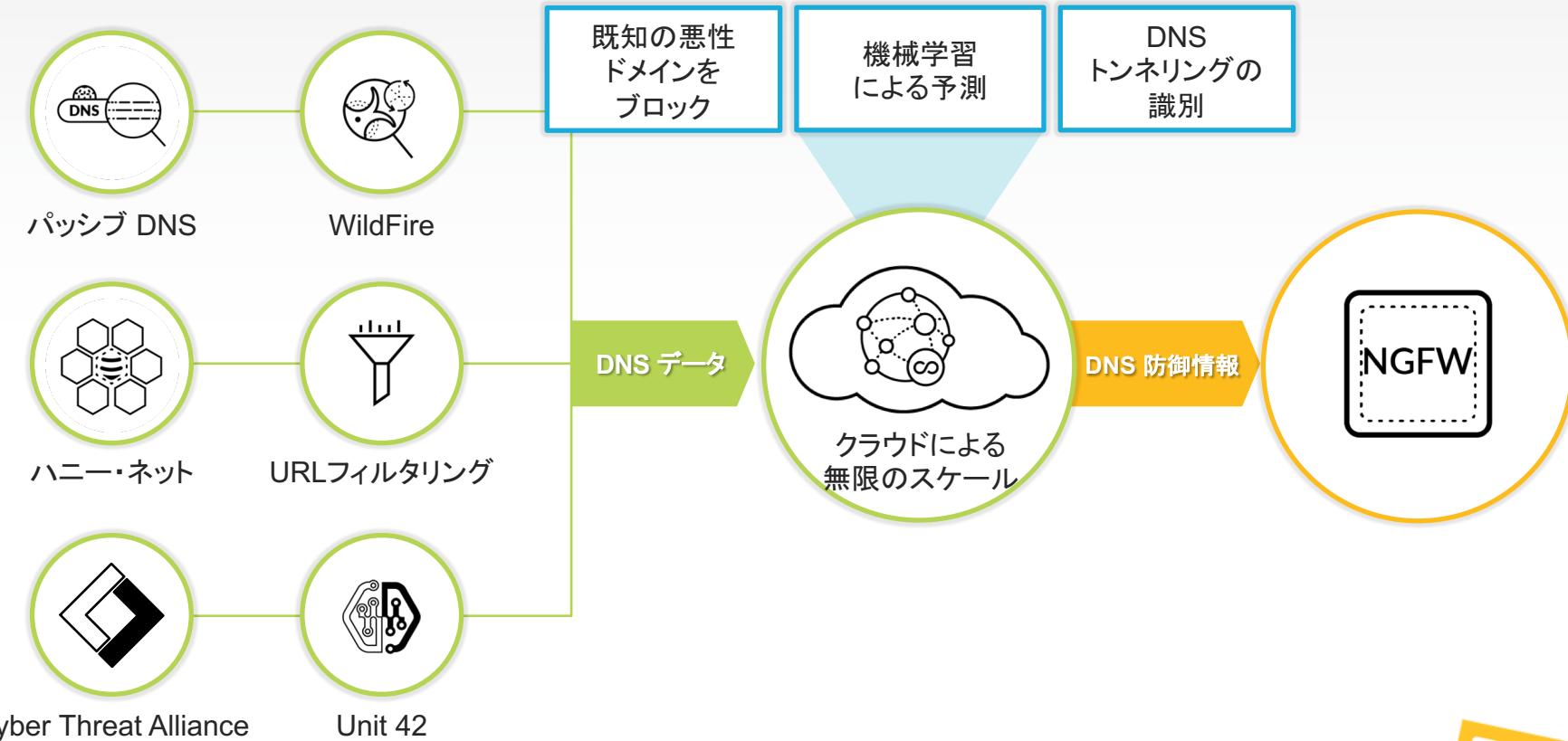
- ファイルおよびデータフィルタリング
  - ファイルタイプまたはデータパターン(クレジットカード番号や文字列パターン等)によるフィルタリング
- 脅威防御
  - 脆弱性攻撃 (IPS)、アンチウイルス、アンチスパイウェア
- URLフィルタリング
  - 63カテゴリに分別された 2000万を超える URL 情報を元にしたWebアクセス制御

◆フル機能利用にはサブスクリプションの購入が必要。

# Content-ID™: DNSセキュリティ

New

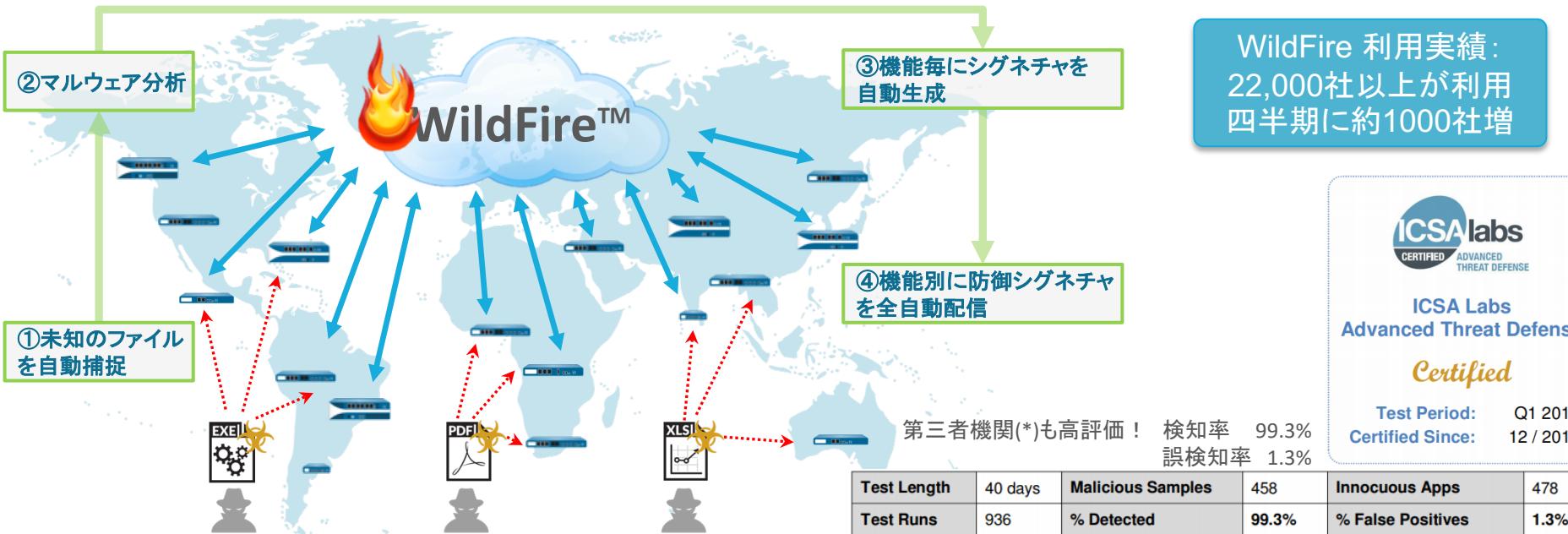
PAN-OS9.0~



# 未知のマルウェア対策サンドボックス – WildFire™

- 世界最大規模のマルウェア分析クラウドサービス

- サンドボックスと呼ばれる技術で、世界中から収集した未知のファイルを一度仮想環境で分析し、未知のマルウェアを発見→「既知」のマルウェアに！
- 5分間隔で防御シグネチャを世界中に配信
- クラウドを利用しているため最新脅威への即時対応や**機能拡張**が容易



# GlobalProtectの概要: 内部プロキシーの代わりとして動作する

# なぜプロキシーを利用する？

- キャッシュのため?
  - SSL暗号が大半の今となっては、(SSL復号しない)Proxyでキャッシュできないので、あまり意味がない。
- ユーザごとのURLログ?
  - これのためだけにプロキシーを設置?
- それなら、Firewallに統合した方が合理的！

# URLロギング:いつ/誰が/どこへアクセスしたのかを詳細に記録

	Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application
	03/10 23:01:03	streaming-media	www.youtube.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	216.58.197.238	youtube-base
	03/10 23:01:03	search-engines	www.google.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.27.68	google-base
	03/10 23:01:03	search-engines	www.google.co.jp/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.26.35	ssl
	03/10 23:01:03	computer-and-internet-info	play.googleapis.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.25.74	google-base
	03/10 23:01:01	computer-and-internet-info	md-hq5rprlg0kbm.blob.core.windows.net/	trust	untrust	10.10.2.10	acme\ct7-001	52.239.145.20	ssl
	03/10 23:01:01	computer-and-internet-info	globalprotect001.japaneast.cloudapp.azure.com/	trust	untrust	10.10.2.6	acme\w10-002	52.246.166.216	ssl
	03/10 23:01:00	computer-and-internet-info	play.googleapis.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.25.74	google-base
	03/10 23:01:00	content-delivery-networks	geo2.ggpht.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.25.193	ssl
	03/10 23:01:00	computer-and-internet-info	app-measurement.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.26.46	ssl
	03/10 23:01:00	search-engines	www.googleapis.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.26.46	google-base
	03/10 23:01:00	computer-and-internet-info	app-measurement.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.26.46	ssl
	03/10 23:01:00	computer-and-internet-info	app-measurement.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	172.217.26.46	ssl
	03/10 23:00:59	computer-and-internet-info	jpe-agentservice-prod-1.azure-automation.net/	trust	untrust	10.10.2.10	acme\ct7-001	138.91.9.98	ssl
	03/10 23:00:58	computer-and-internet-info	zrdfepirv2ty1prdstr02a.blob.core.windows.net/	trust	untrust	10.10.2.10	acme\ct7-001	40.115.231.94	ssl
	03/10 23:00:58	computer-and-internet-info	md-hq5rprlg0kbm.blob.core.windows.net/	trust	untrust	10.10.2.10	acme\ct7-001	52.239.145.20	ssl
	03/10 23:00:57	content-delivery-networks	lh5.googleusercontent.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	216.58.197.129	ssl
	03/10 23:00:56	content-delivery-networks	lh3.googleusercontent.com/	Corp-VPN	untrust	172.16.99.7	acme\jos-001	216.58.197.129	ssl
	03/10 23:00:55	computer-and-internet-info	zrdfepirv2ty1prdstr02a.blob.core.windows.net/	trust	untrust	10.10.2.10	acme\ct7-001	40.115.231.94	ssl
	03/10 23:00:55	computer-and-internet-info	md-hq5rprlg0kbm.blob.core.windows.net/	trust	untrust	10.10.2.10	acme\ct7-001	52.239.145.20	ssl
	03/10 23:00:54	computer-and-internet-info	jpe-agentservice-prod-1.azure-automation.net/	trust	untrust	10.10.2.10	acme\ct7-001	138.91.9.98	ssl

いつ?

どのような?  
カテゴリ(有償)

どこへ?  
URL (SSLでもFQDN表示)

どこから?

だれが?  
ユーザの情報

リモートから

社内LANから

内部LANでも  
ユーザ識別

# GlobalProtectの概要: 内外問わず、検疫的な動作ができる

# HIPチェック

## Host Information Profile

### (端末の情報プロファイル)

リモートアクセスだけでなく、内部LANにおいても、HIPの取得ができる。

取得した端末情報をを使って、セキュリティポリシーを適用できる。

#### 使い方の例：

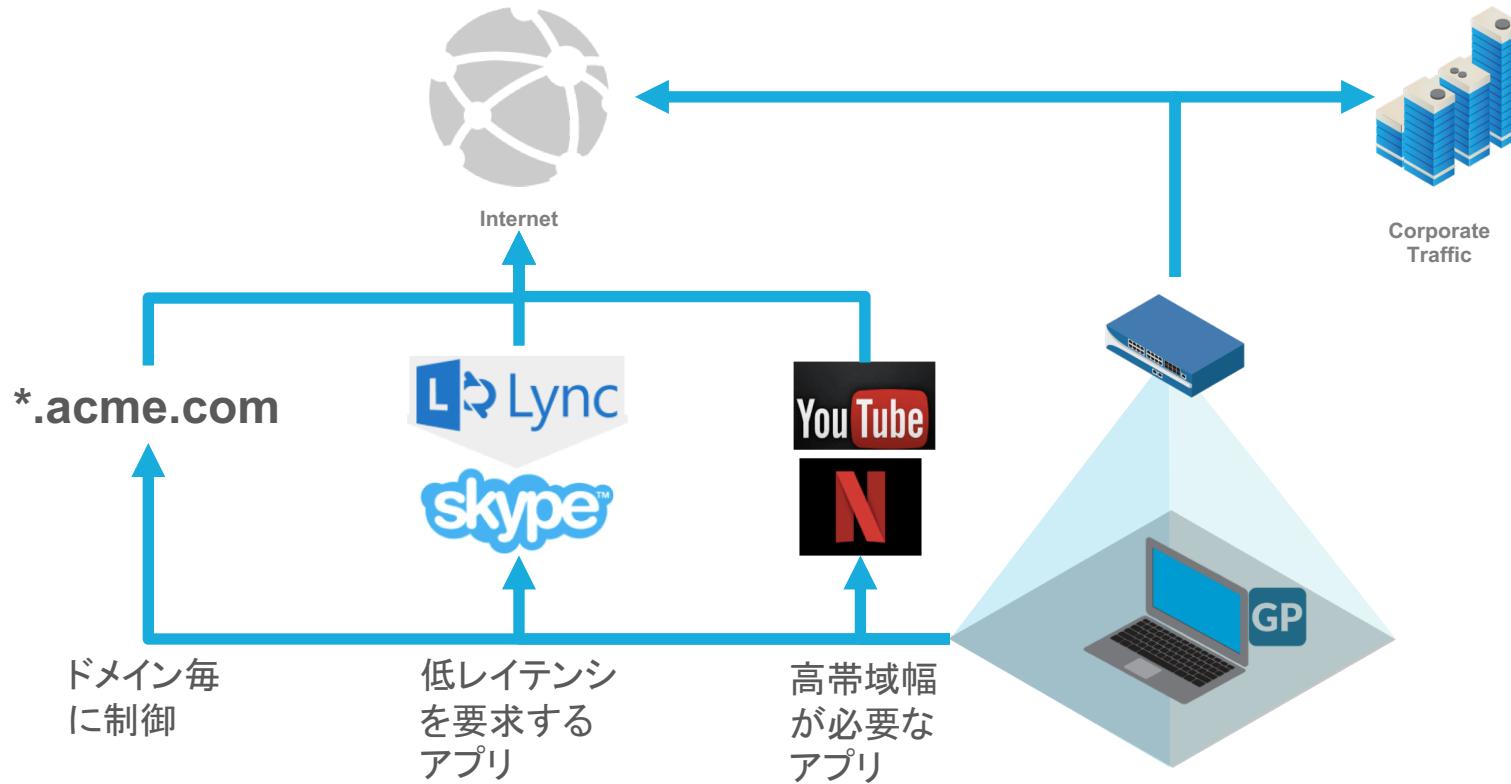
ディスクが暗号化されていない端末は、機密情報を持つ社内サーバにはアクセスさせない。

#### Windows10の例：

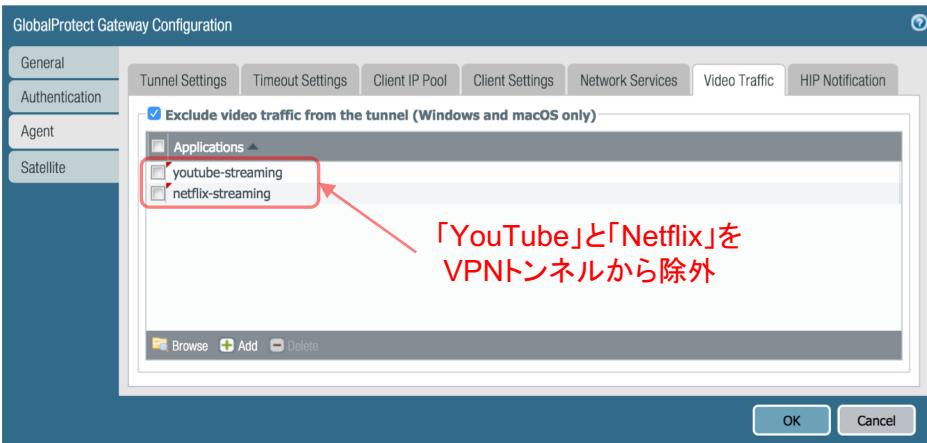
Log Details								
Report Generated	03/21/2019 17:10:57							
User Information	User: w10-002			IP Address: 10.10.2.6				
Host Information	Machine Name: WIN10-002			Domain: acme.com				
OS	Microsoft Windows 10 Pro , 64-bit			Host ID: a2b6e750-465a-4309-ae4a-155d8575fd5				
Client Version	4.1.10-4							
Network Information								
Interface		MAC Address		IP Address				
Microsoft Hyper-V Network Adapter		00-0D-3A-51-A6-3E		10.10.2.6 fe80::c16f:787a:60d4:58b9				
PANG Virtual Ethernet Adapter #2		02-50-41-00-00-01		169.254.73.224 fe80::a437:5532:7c73:49e0				
Software Loopback Interface 1		127.0.0.1 ::1						
Anti-Malware								
Software	Vendor	Version	Engine Version	Definition Version	Date			
Windows Defender	Microsoft Corporation	4.13.17134.1	1.1.15700.9	1.289.1652.0	3/20/2019 ✓			
Disk Backup								
Software	Vendor	Version	Last Backup					
Windows Backup and Restore	Microsoft Corporation	10.0.17134.1	n/a					
Windows File History	Microsoft Corporation	10.0.17134.1	n/a					
Disk Encryption								
Software	Vendor	Version						
BitLocker Drive Encryption	Microsoft Corporation	10.0.17134.1						
Drive	State							
D:\	unencrypted							
C:\	unencrypted							
Firewall								
Software	Vendor	Version	Enabled					
Windows Firewall	Microsoft Corporation	10.0.17134.1	✗					
Patch Management								
Software	Vendor	Version	Enabled					
Windows Update Agent	Microsoft Corporation	10.0.17134.1	✓					
Missing Patches								
Title	KB Article ID	Severity						
2018-09 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347)	4100347	2						
Definition Update for Windows Defender Antivirus - KB2267602 (Definition 1.289.1716.0)	2267602	1						

# GlobalProtectの概要: きめ細かいスプリットトンネル設定ができる

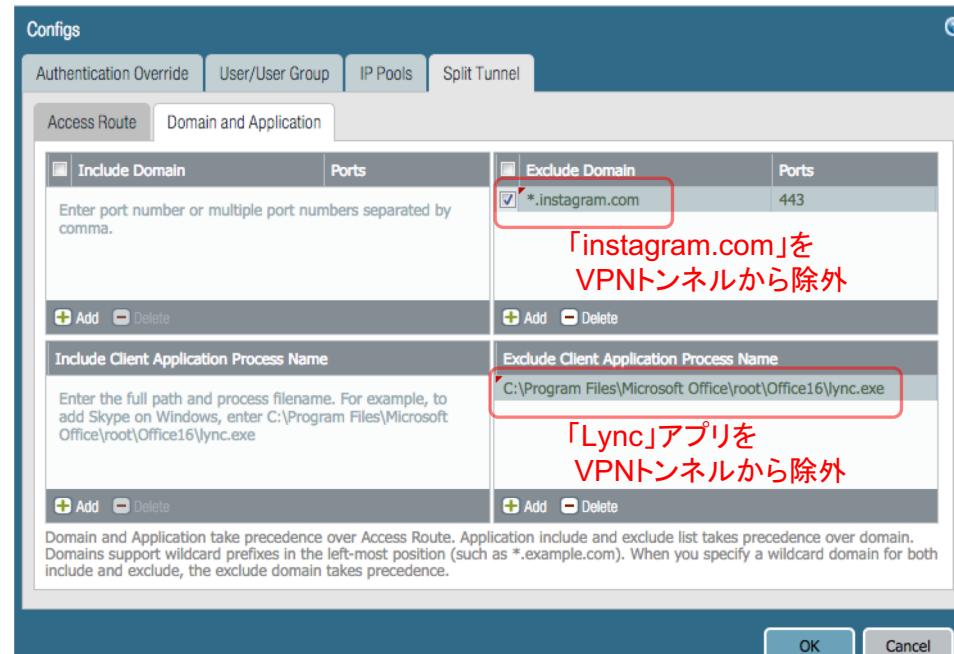
# 高帯域幅 / レイテンシに敏感なアプリをトンネルからきめ細かく除外



# 高帯域幅 / レイテンシに敏感なアプリをトンネルからきめ細かく除外 (設定)



Network > GlobalProtect > Gateways > external-gateway > Agent > Video Traffic

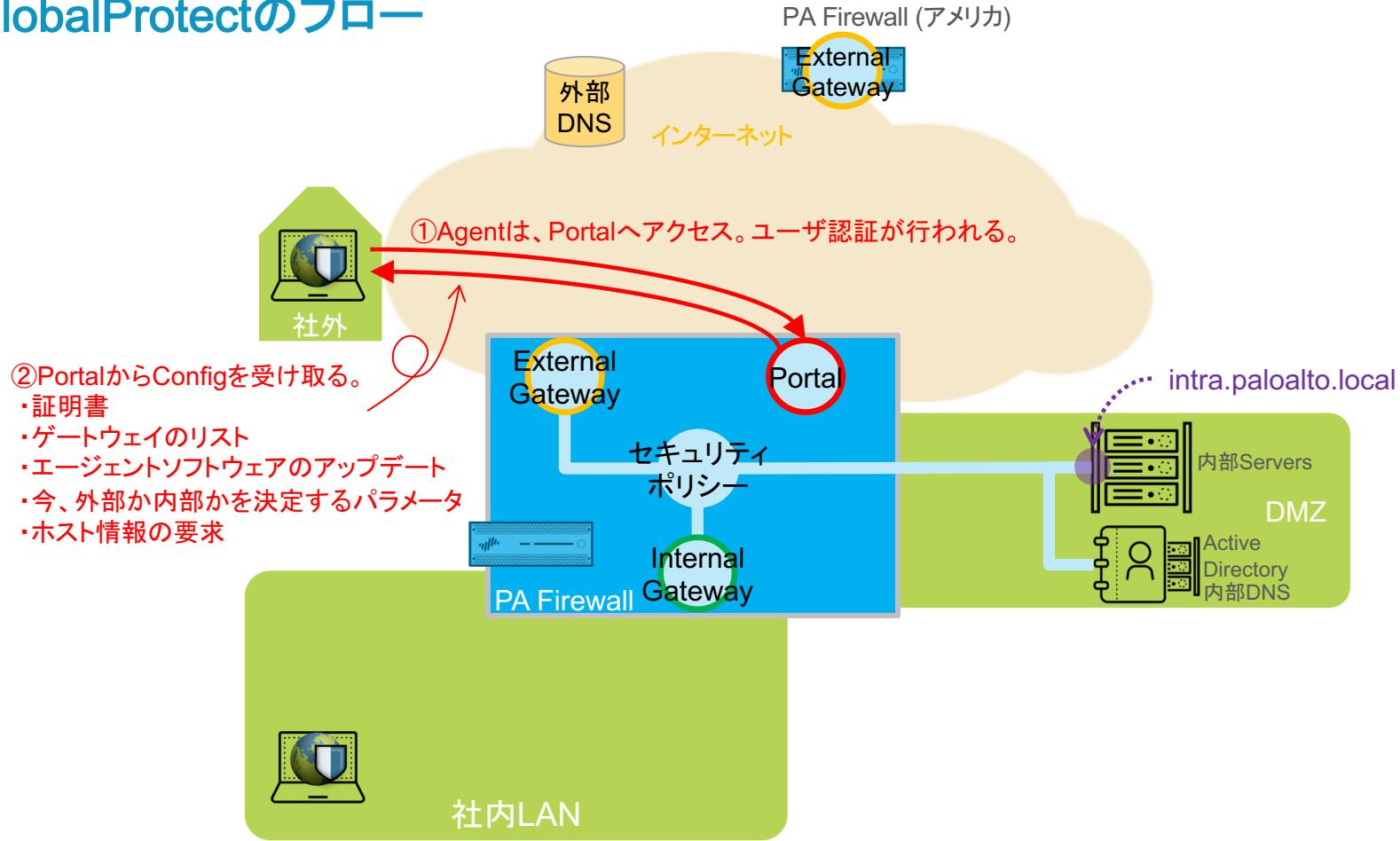


Network > GlobalProtect > Gateways > external-gateway > Agent  
> Client Settings > Split Tunnel > Domain and Application

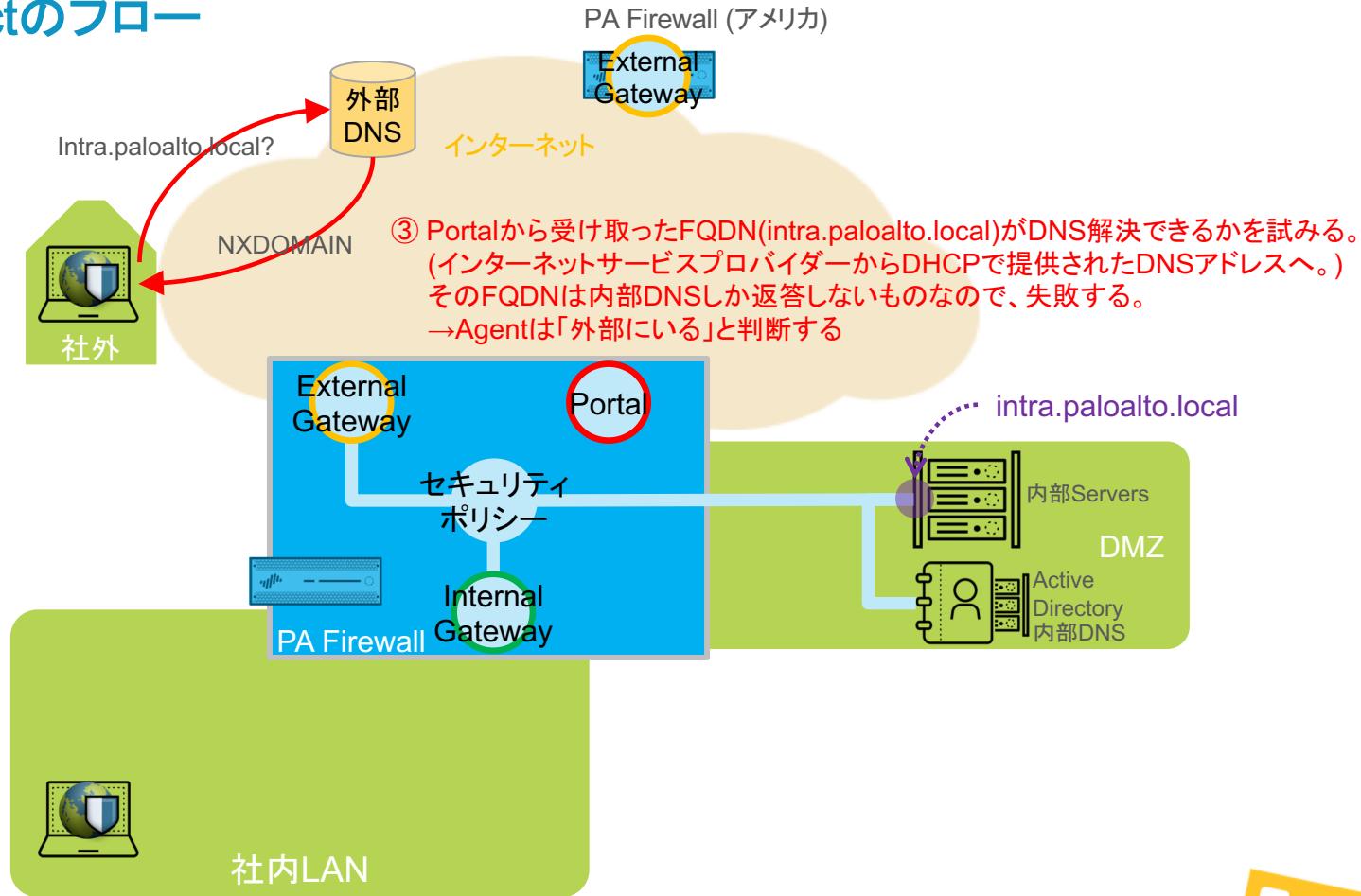


# GlobalProtectの動作

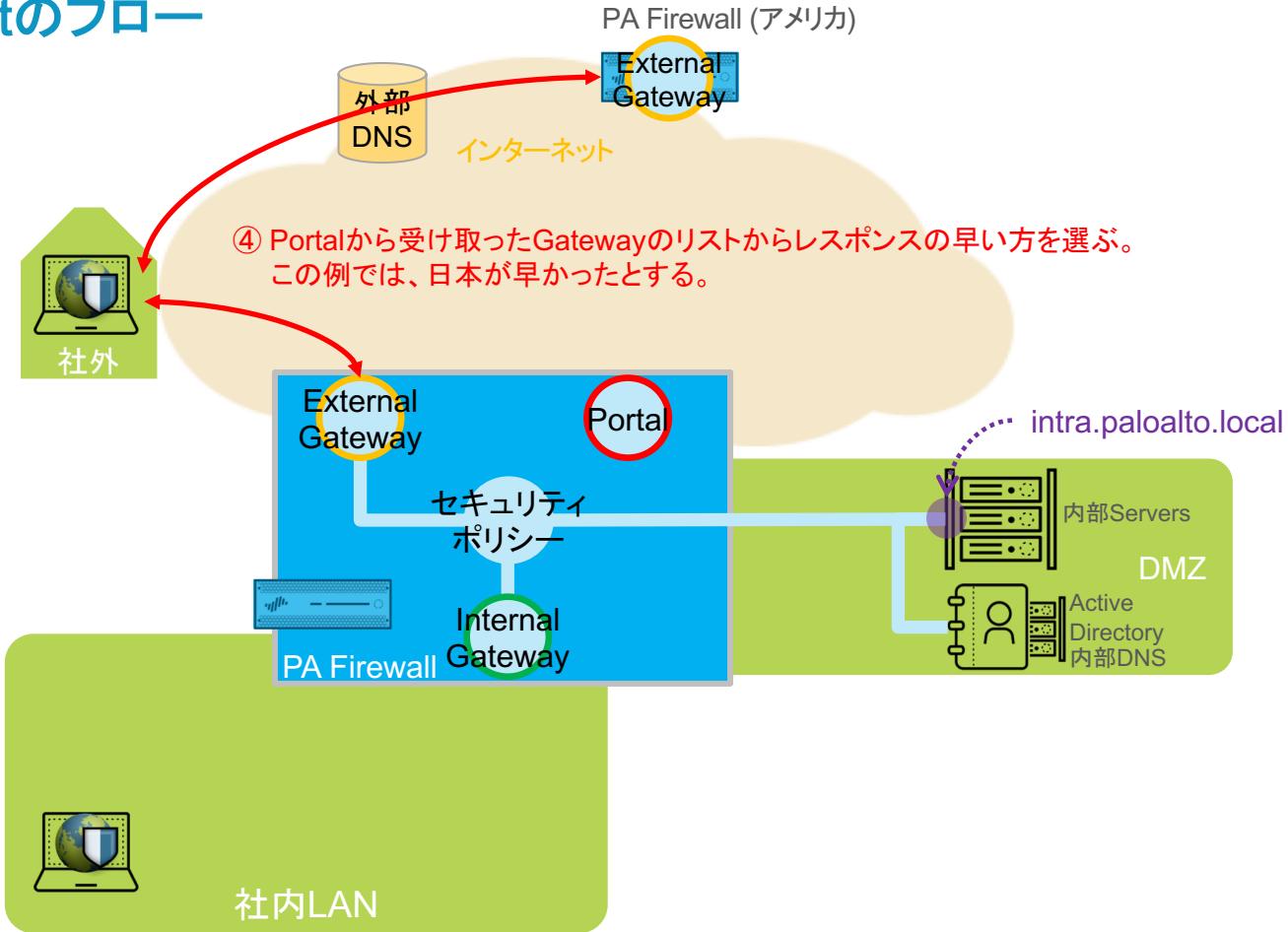
# GlobalProtectのフロー



# GlobalProtectのフロー



# GlobalProtectのフロー

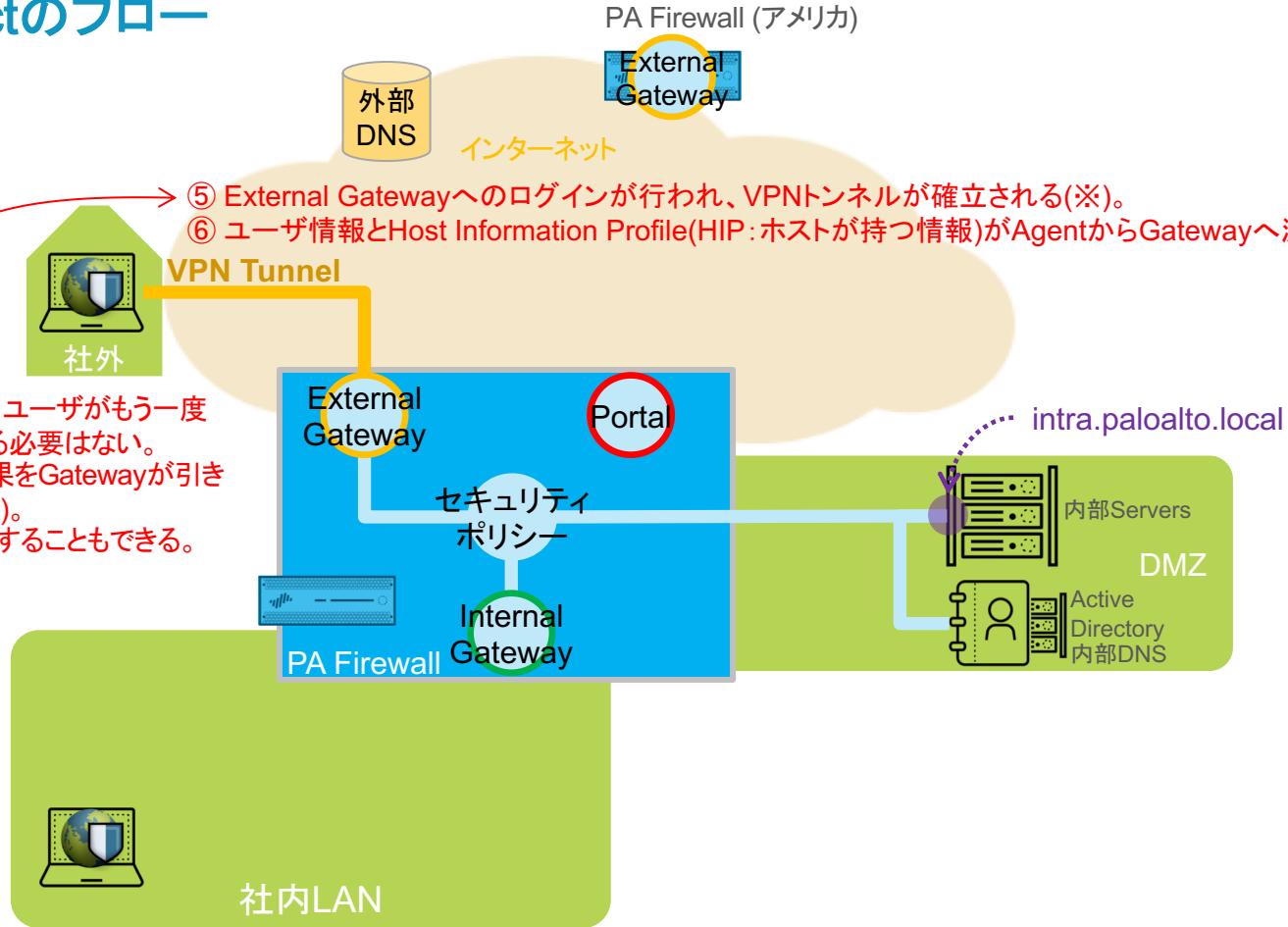


# GlobalProtectのフロー

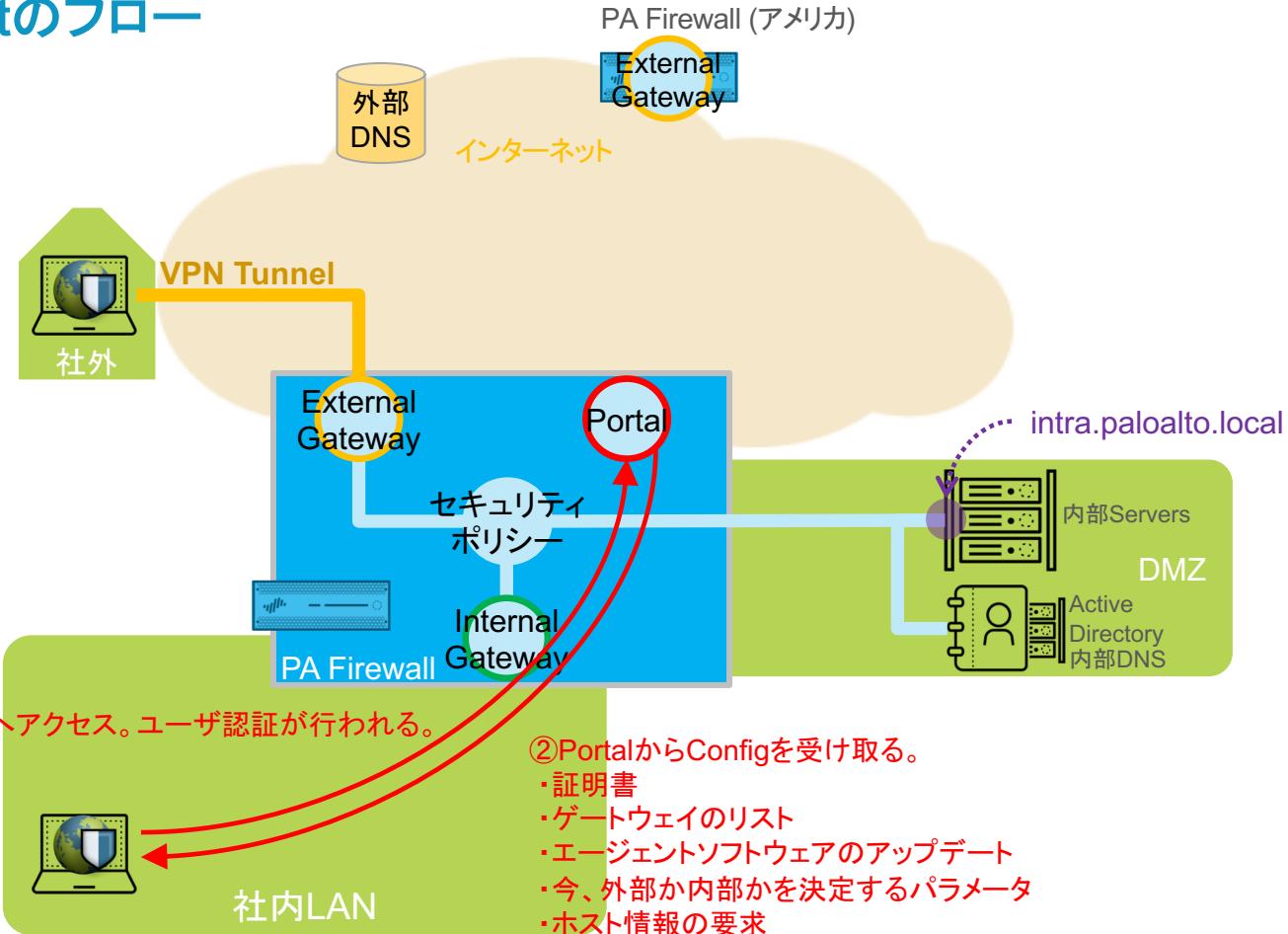
(※)

- Gatewayへのログイン時に、ユーザがもう一度クリデンシャル情報を入力する必要はない。Portalでユーザ認証をした結果をGatewayが引き継ぐことができる(Cookie設定)。
- ワンタイムパスワードを強制することもできる。

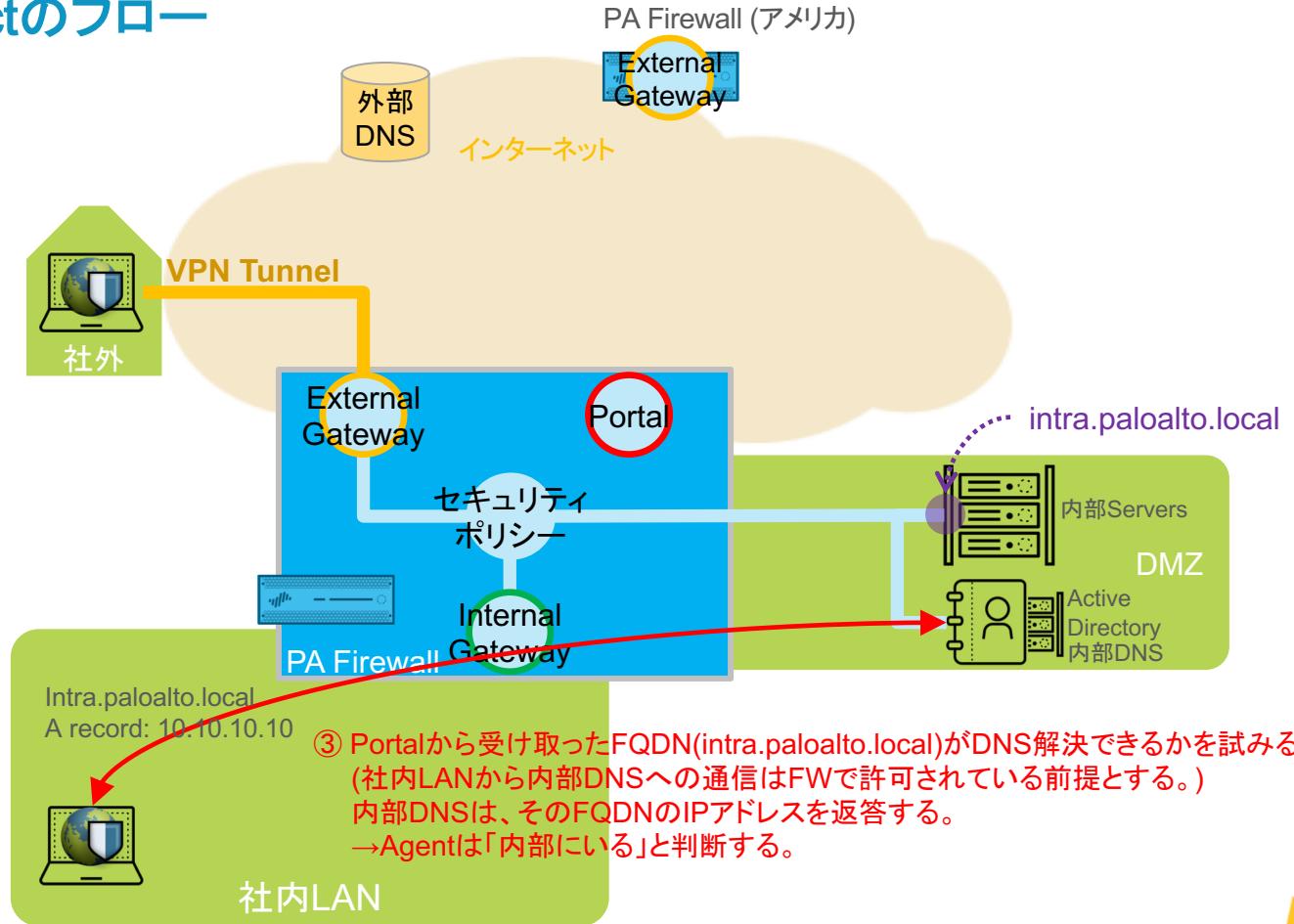
→ ⑤ External Gatewayへのログインが行われ、VPNトンネルが確立される(※)。  
⑥ ユーザ情報とHost Information Profile(HIP:ホストが持つ情報)がAgentからGatewayへ渡される。



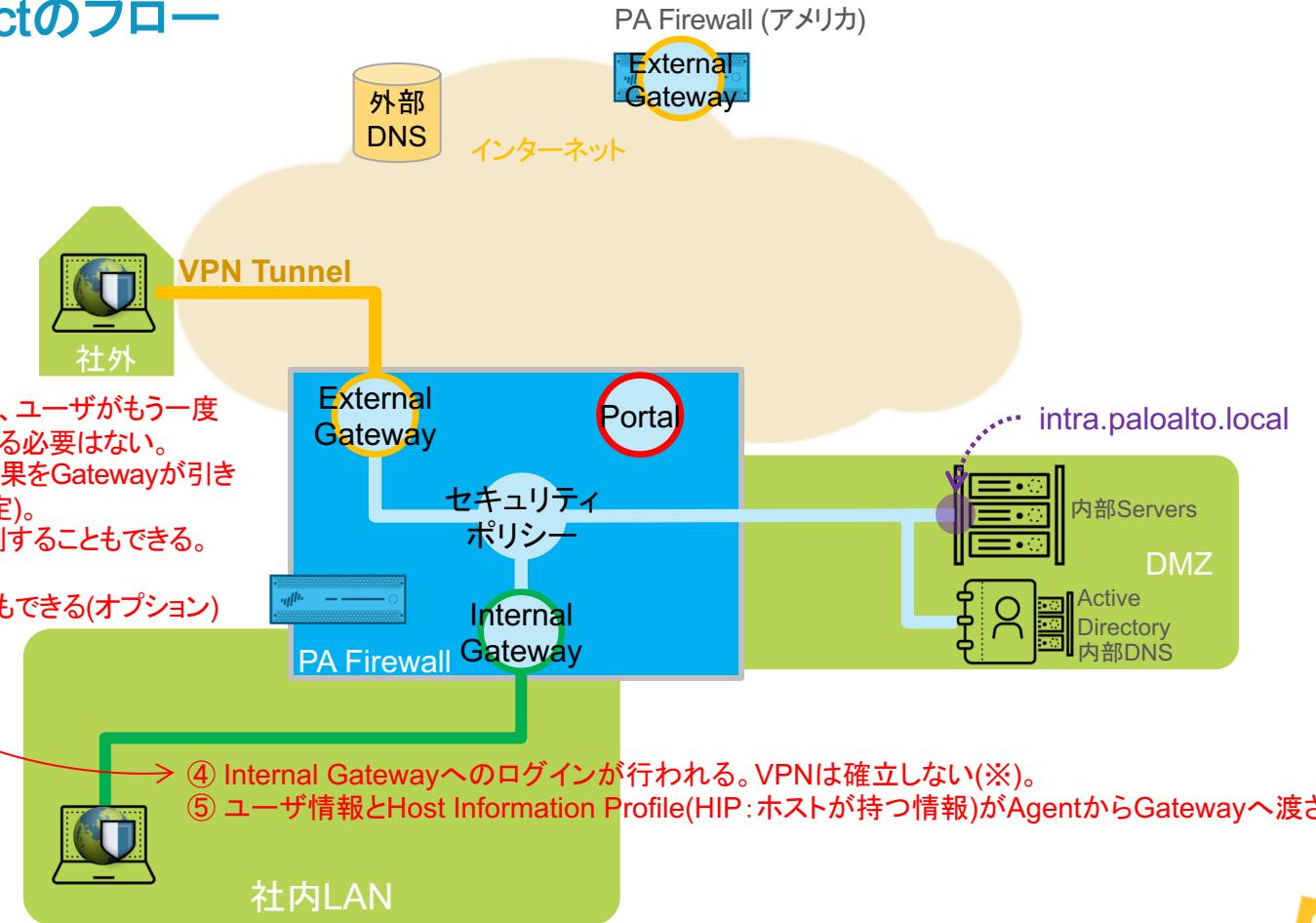
# GlobalProtectのフロー



# GlobalProtectのフロー

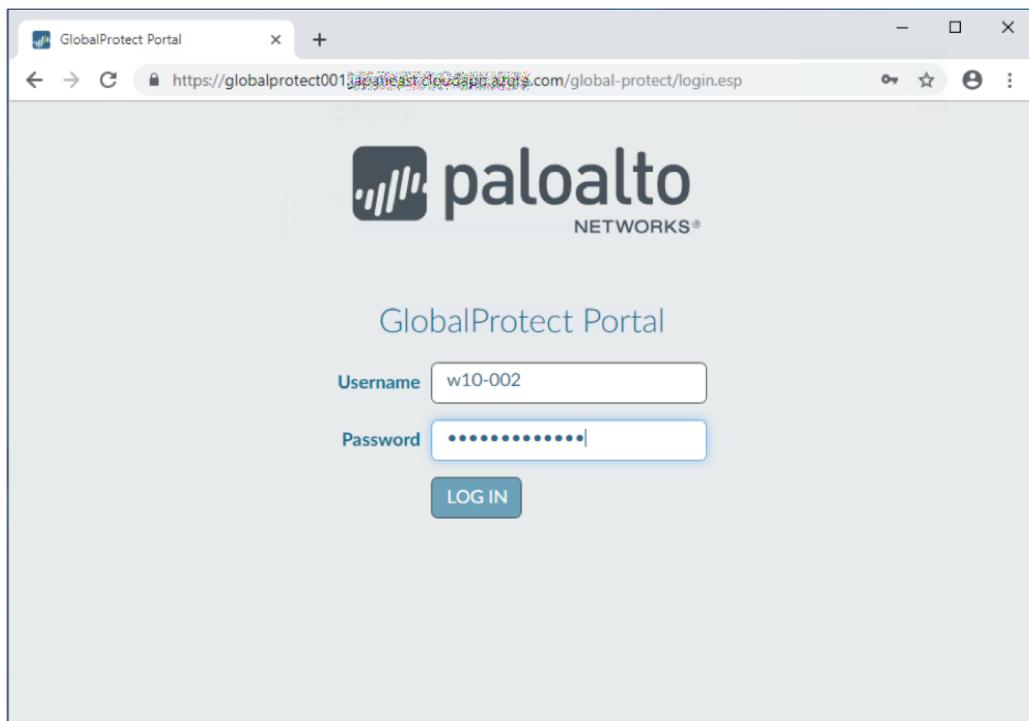


# GlobalProtectのフロー



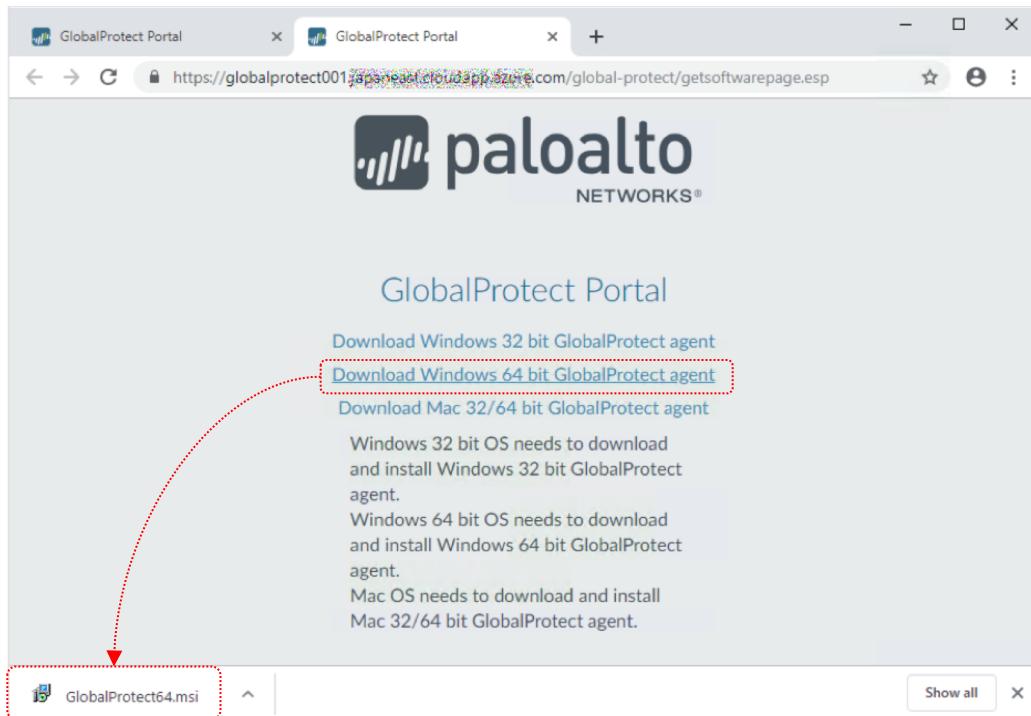
## [参考] Windowsでの接続方法

# ① Global ProtectのPortalへログイン（インストール前）



- GlobalProtectのPortal設定を行なったPA FirewallへWebブラウザでアクセスします。
- ユーザ名とパスワードを入力し、LOG INします。

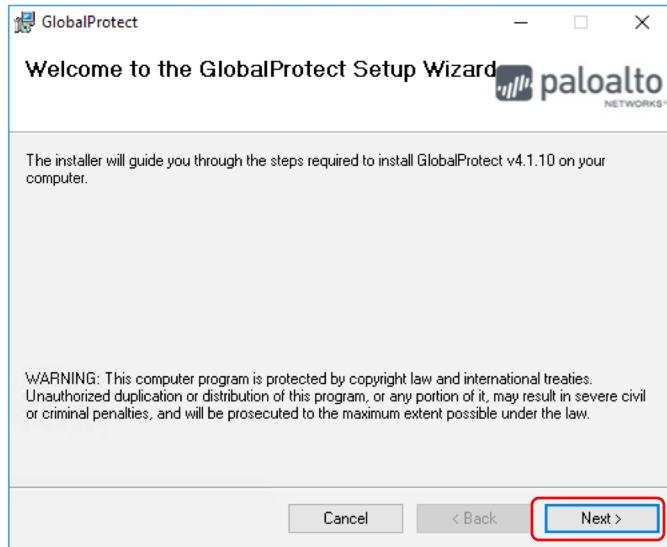
## ② GP Agentのダウンロード



- 端末環境に合ったGlobalProtect Agentをダウンロードします。
- ダウンロードした実行形式ファイル(.msi)を実行します。

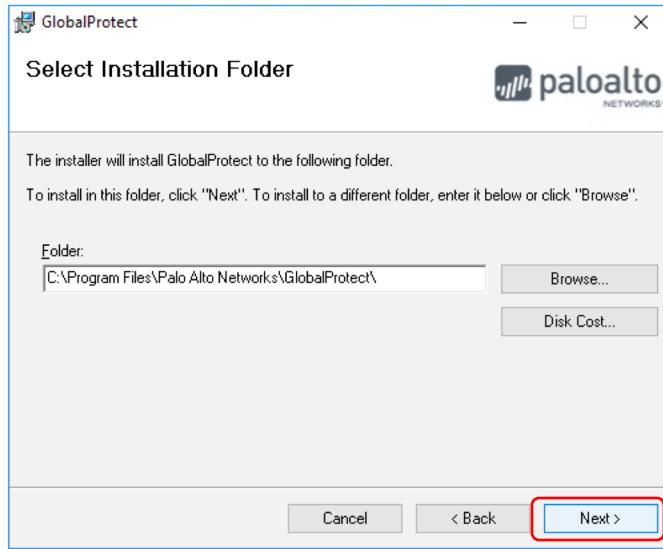
### ③ GP Agentのダウンロード(1)

- Nextをクリックします。



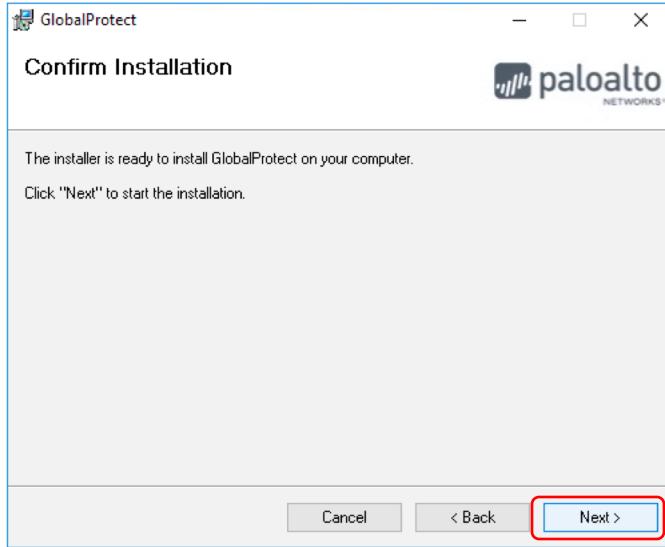
### ③ GP Agentのダウンロード(2)

- Nextをクリックします。



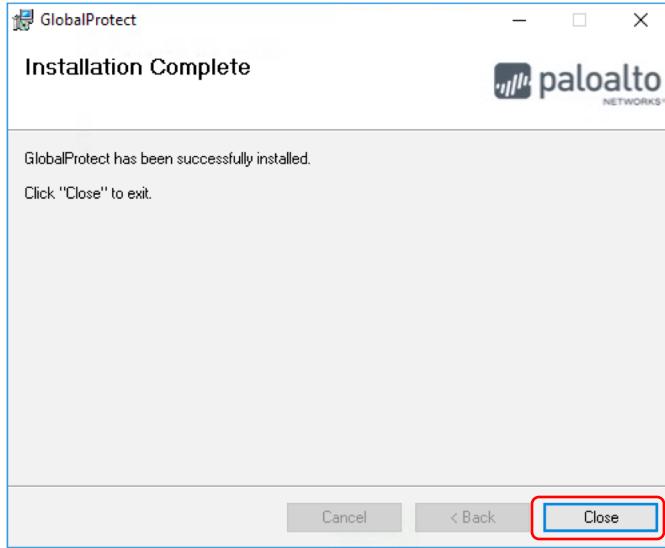
### ③ GP Agentのダウンロード(3)

- Nextをクリックします。

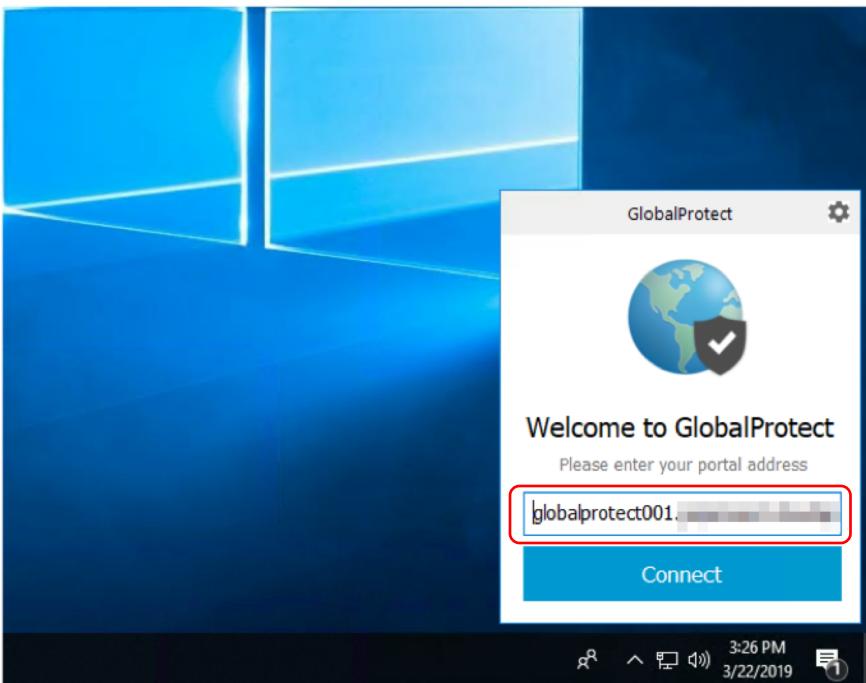


### ③ GP Agentのダウンロード(4)

- Closeをクリックします。

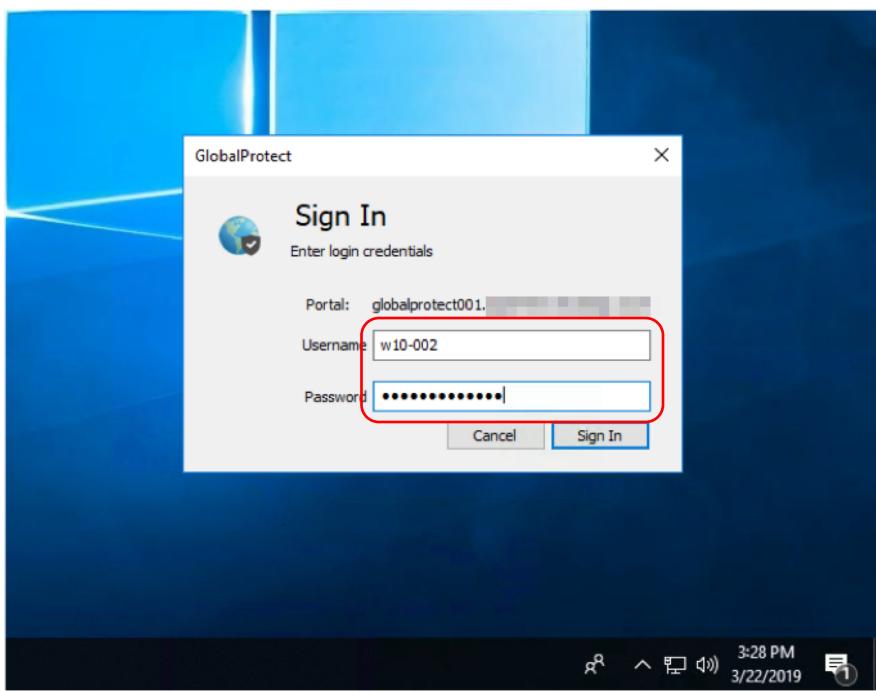


## ④ GP Agentからのアクセス(1)



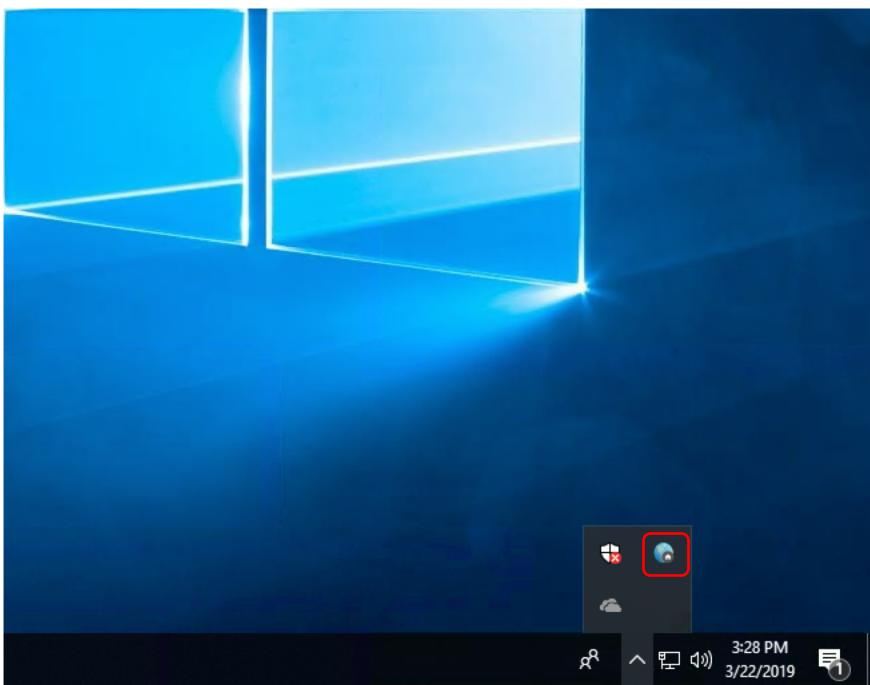
- PA FirewallのPortalを宛先として入力します。
- Connectをクリックします。

## ④ GP Agentからのアクセス(2)



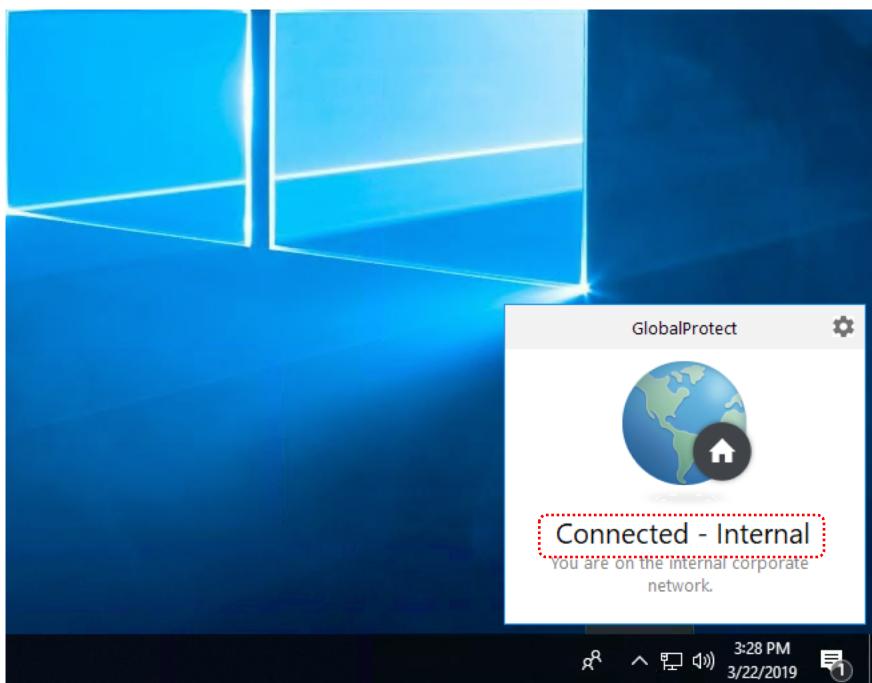
- ユーザ名とパスワードを入力します。
- Sign In をクリックします。
- 2回目以降は入力することなく、Windows側のクリデンシャル情報で自動的にログインできます。

## ④ GP Agentからのアクセス(3)



- ログインすると、タスクトレイに  
入ります。

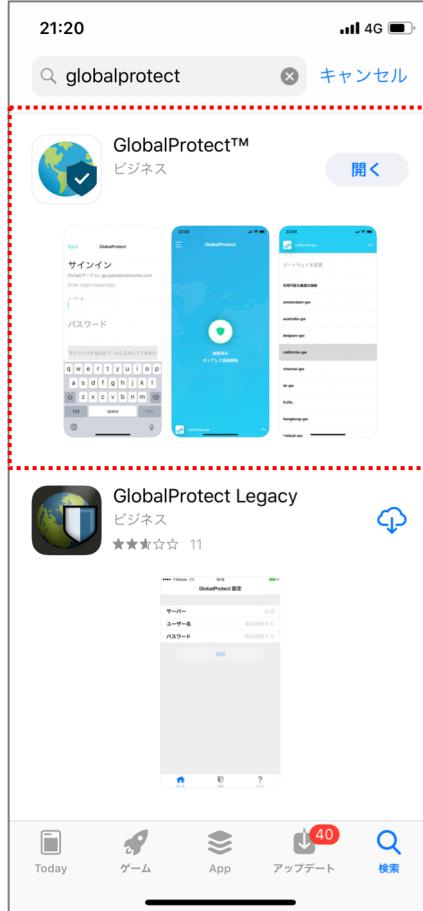
## ④ GP Agentからのアクセス(4)



- クリックすると、状態が確認できます。
- 本例では、内部LANに(VPNトンネルなしで)接続しています。

## [参考] iOSでの接続方法

# ① ダウンロード&インストール



- App Storeから、GlobalProtect Agentソフトウェアをダウンロード&インストールします。
- 「開く」をクリックします。

## ② 通知の設定



- 通知の許可・許可しないを選択します。
  - どちらでも構いません。お好みで。

### ③ 証明書の許可 (独自証明書の場合)



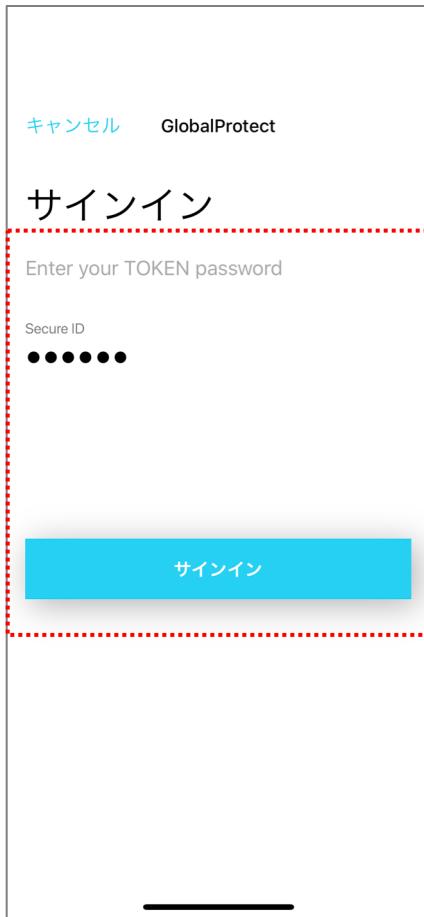
- 独自証明書の場合、続行するかどうかの確認が行われます。
  - 接続するためには「続行」を選択します。

## ④ 接続設定



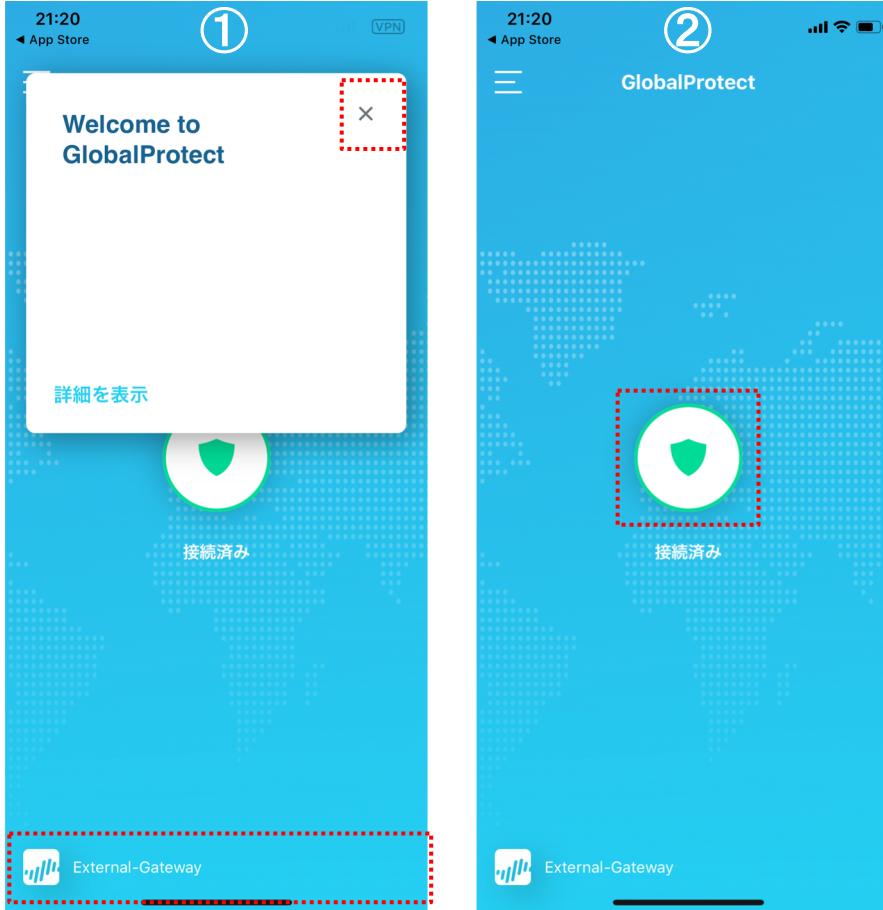
- 以下を入力します。
  - Portalのドメイン名またはIPアドレスを入力
  - Username
  - Password
- 「サインイン」をクリックします。

## ⑤ ワンタイムパスワードを利用している場合



- ワンタイムパスワードを利用している場合、TOKENを求められるので、入力します。
- 「サインイン」をクリックします。

## ⑥-1 External Gatewayへの接続完了



- ①は、External Gatewayに接続された状態です。
- 「×」をクリックすると、②の状態になります。
- 中央のアイコンは盾のマーク。

## ⑥-2 Internal Gatewayへの接続完了



- Internal Gatewayに接続すると、下方の表示が「Internal Network」と表示されます。
- 中央のアイコンは建物のマーク。

## まとめ

- GlobalProtectを使うことで、外部からのリモートアクセスだけでなく、内部LANでも、ユーザ&端末の識別が可能。
- GlobalProtectは、PA Firewallにアドオンできるので、PA Firewallの先進的な脅威防御機能とのインテグレーションが容易。
- GlobalProtectは、iOSやAndroidなどのモバイル端末へも対応。
- VPN装置やProxyを個別設置するよりも、それらの機能を統合した方がより効率的な使いができる。

# THANK YOU

