CLOUDFLARE

Cloudflare連続勉強会 #6

Cloudflare Zero Trustの紹介 (前編)
- 導入準備編

カスタマーサクセス　部長 八塚 俊次郎
カスタマーソリューションエンジニア　西原 誠

Cloudflare Japan
東京都中央区京橋 2-2-1京橋エドグラン 26階
www.cloudflare.com/ja-jp/

Agenda

1 はじめに

2 Cloudflare Zero Trust導入の流れ

3 Cloudflareダッシュボードの初期設定

4 WARPクライアントのインストール

5 Q&A

はじめに

1. はじめに
2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. Q&A

目的

本WebinarはCloudflareのEnterpriseプランのご契約をお持ちのお客様向けにCloudflare製品の機能及び設定概要を紹介することで、製品をよりよくご活用いただくことを主目的とします。

時間配分	内容
50分	メインセッション
10分	Q&A

注意事項

本Webinarご参加に当たっての注意事項を以下記載いたします。

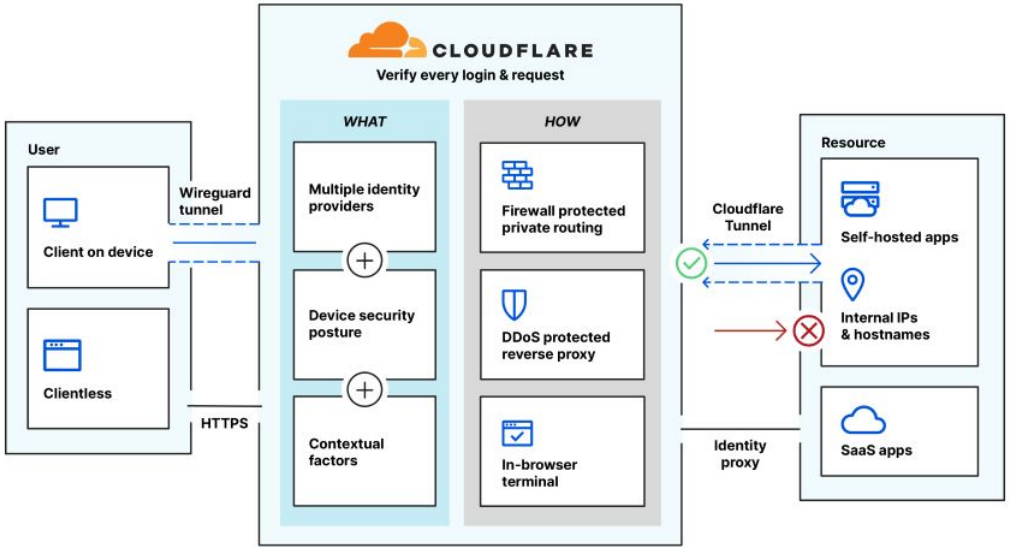
- 本Webinarはレコーディングを行い、後日、弊社Webinarサイトにご登録のお客様は再視聴できるようにいたします。各セッションの最後にはブラウザ上のテキストボックスからご質問を受付けますが、起票者のお名前は伏せてのQ&A対応となります。
- お時間の制約から、Webinar中に頂いたすべてのご質問にお答えできないかもしれません。最善は尽くさせていただければと考えておりますが、その旨、ご了承いただければと思います。
- 本セッションで用いるスライドはセッション終了後、当Webinarのご登録ページからPDF形式でダウンロード頂けます。

Cloudflare Zero Trust導入の流れ

1. はじめに
2. **Cloudflare Zero Trust導入の流れ**
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. Q&A

Cloudflare Zero Trust導入の流れ

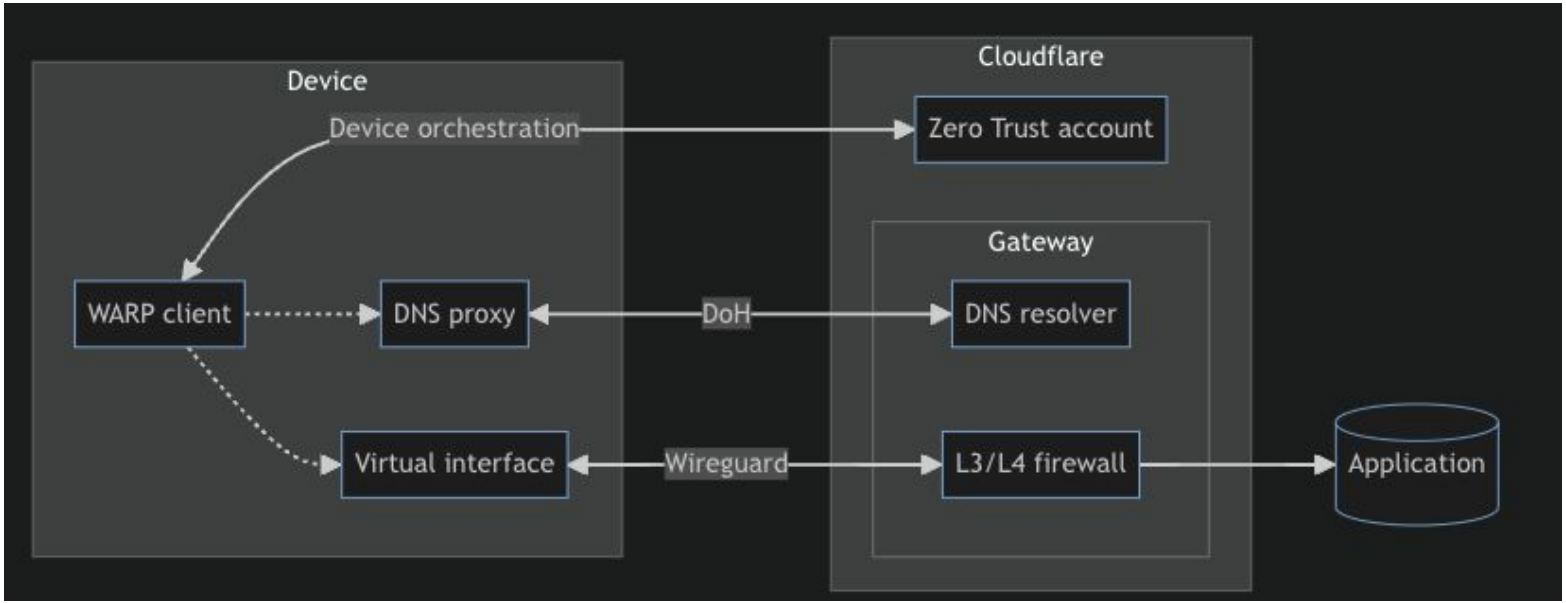
Cloudflare Zero Trust導入の流れとしてはRoadmap to Zero Trustをご参照いただけます。



参照) Cloudflare Zero Trust Network Accessの鳥瞰図

CLOUDFLARE

Cloudflare Zero Trust導入の流れ - WARPのアーキテクチャ



参照) Cloudflare Docs - WARP architecture
Cloudflare Docs - WARP with firewall

Cloudflare Zero Trust導入の流れ - 導入フェーズ定義例

Phase.1)
- ダッシュボードの初期設定
- ZTNAの設定
- WARPの部分展開 (一部ユーザー間での試験導入)

Phase.2)
- SWGの基本設定 (DNS / Networkポリシーの適用)
- WARPの全社展開

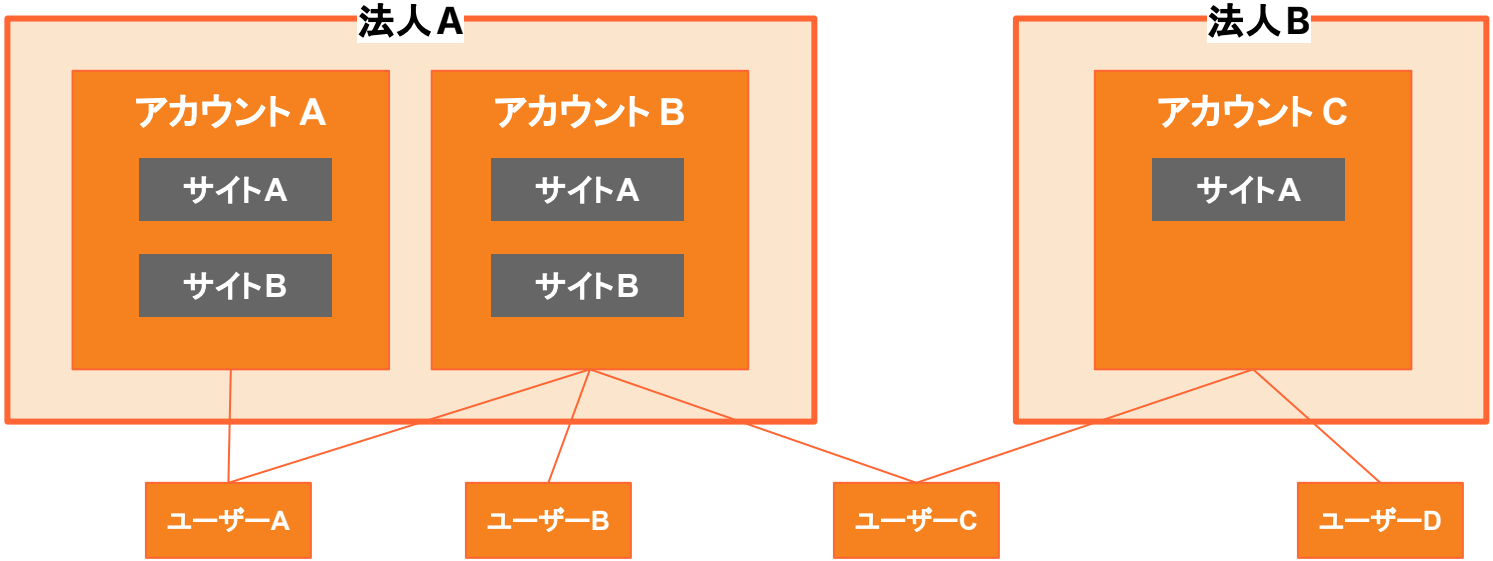
Phase.3)
- SWGの追加設定 (HTTPポリシーの適用※)
- CASB / DLP / RBIの設定

※ SWGで、HTTPSの通信にポリシーを適用させる場合にはTLS Decriptionを有効化いただく必要がありますが、それに伴い特定のサイトアクセスにおいて、証明書エラー (526エラー等)の発生の可能性があります。
個別に後述のDo Not Inspectポリシーもしくは Split Tunnelの設定が必要となりますため、ご注意ください。

参照) Cloudflare Docs - TLS Decription

Cloudflare Zero Trust導入の流れ - 複数アカウントの管理

Enterprise Planご利用のお客様に限っては、検証等を目的として、複数のアカウントに分割した管理も可能となります。
※前提として、ご契約数量（シート数)を分けた管理が必要となります



Cloudflareダッシュボードの初期設定

1. はじめに
2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. Q&A

Cloudflareダッシュボードの初期設定

1. **チーム名の設定**
2. 認証方法の設定
3. ダッシュボードのSSO登録 (オプショナル)
4. Logpush設定

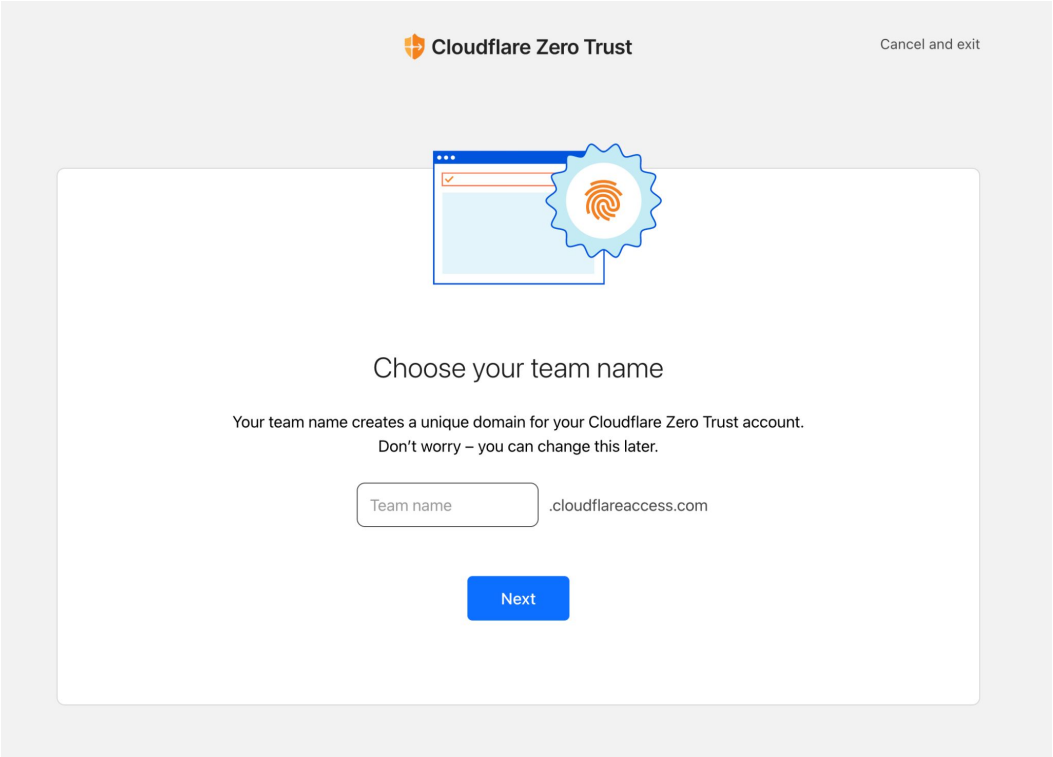
チーム名の設定

1. Cloudflareダッシュボードのアカウントレベルメニューから、Zero Trustをクリック
2. Team名を指定
3. サブスクリプションプランおよびお支払い方法を設定

※Freeプランを選択の際にも、お支払い方法の設定が必要となりますが、実際の引き落としはなされませんので、ご安心ください。

参照) Cloudflare Docs - Start from the Cloudflare Dashboard

チーム名の設定 - 初回設定画面



Cloudflareダッシュボードの初期設定

1. チーム名の設定
2. **認証方法の設定**
3. ダッシュボードのSSO登録 (オプショナル)
4. Logpush設定

認証方法の設定

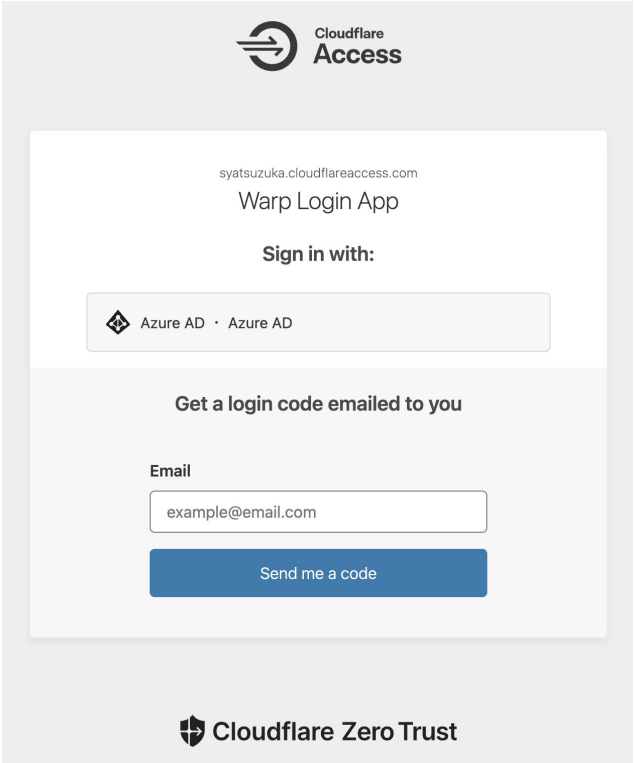
Cloudflare Zero Trustでは大きく、ご登録されたIdPの設定に基づき、以下の2つのレベルでユーザー認証が行われます。

- **Cloudflare Access (ZTNA)における認証イベント**
  App LauncherおよびAccessの機能として登録した"Application"へのアクセス時に行われる認証。
  詳細は後編の「ZTNAの設定」で紹介。

- **Cloudflare Secure Web Gatewayにおける認証イベント (WARPにおけるログイン認証)**
  WARPの初回ログイン時に行われる認証
  詳細は後編の「SWGの設定」で紹介。

※こちらの認証結果を元にAccess, Secure Web Gateway双方のご利用シート数が算出されます。

参照) Cloudflare Docs - Seat Management



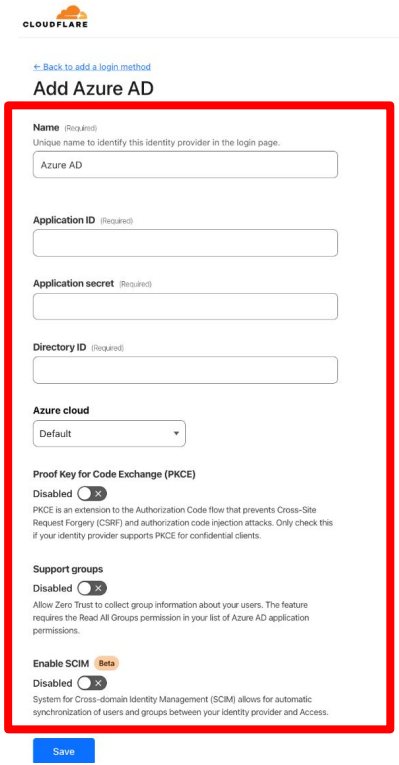
認証方法の設定

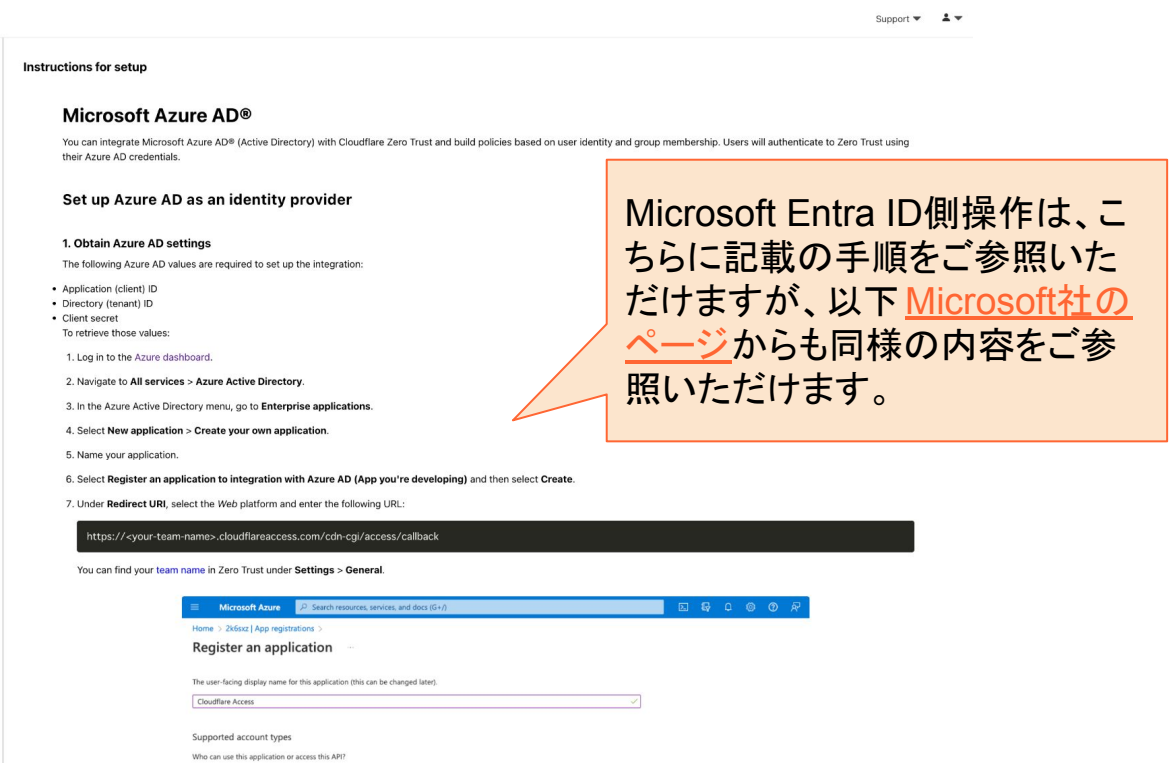
認証方法としては、デフォルトでOne-time PIN login (OTP)を選択いただけますが、ここでは一般的にMicrosoft Entra ID (旧称 Azure Active Directory)の設定の流れを例として紹介させていただきます。

1. IdPのご用意 (例：Microsoft Entra ID)
2. Zero Trustダッシュボードから、Settings > Authenticationをクリック
3. Login methodsカードから、Add Newをクリック
4. IdPを選択 (複数選択可能)
5. 各種項目を入力し、Saveボタンをクリック
6. Testボタンをクリックし、接続が成功することを確認

参照) Cloudflare Docs - SSO Management

認証方法の設定 - Microsoft Entra ID





Microsoft Entra ID側操作は、こちらに記載の手順をご参照いただけますが、以下Microsoft社のページからも同様の内容をご参照いただけます。

認証方法の設定 - Microsoft Entra ID

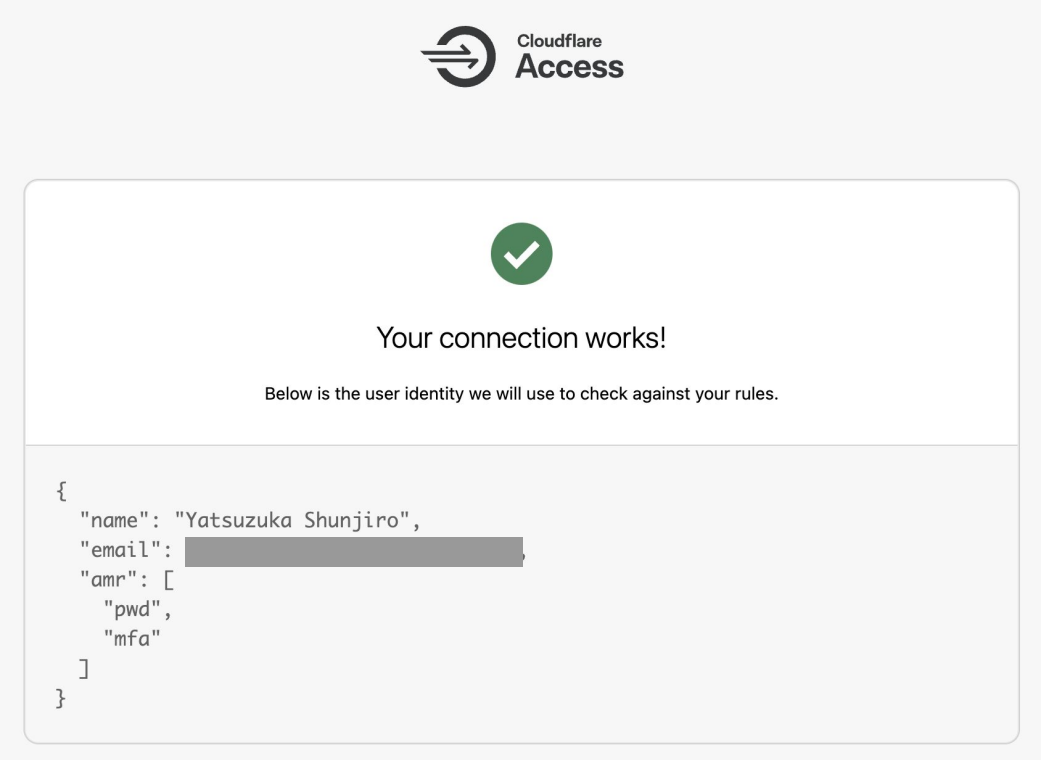
入力項目	設定内容	設定例
Name	SSOのLoginページで表示する名称	“Microsoft Entra ID”
Application ID	(Microsoft Entra IDから取得)	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Application Secret	(Microsoft Entra IDから取得)	
Directory ID	(Microsoft Entra IDから取得)	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Azure Cloud	基本Defaultを選択	“Default”
Proof Key for Code Exchange	CSRF (Cross Site Request Forgery)および認証コードInjectionの回避のためのオプション	“Enabled” | “Disabled”
Support groups	Zero Trustユーザーにおけるグループリスト情報の取得	“Enabled” | “Disabled”
Enable SCIM	SCIM (System for Cross Domain Identity Management)の利用	“Enabled” | “Disabled”

認証方法の設定 - Microsoft Entra ID を使用した SCIM 同期

“クロスドメイン ID 管理システム (SCIM) とは、ID ドメインと IT システムの間で行うユーザー ID 情報の交換を自動化するためのオープンな標準プロトコルです。SCIM を使用すれば、人材管理 (HCM) システムに追加された従業員のアカウントを、確実に Microsoft Entra ID または Windows Server Active Directory によって自動的に作成することができます。ユーザーの属性およびプロファイルは 2 つのシステム間で同期されているので、ユーザーの状態または役割の変更に基づいてユーザーの更新および削除が行われます。”

参照) Microsoft Entra ID を使用した SCIM 同期

認証方法の設定 - Microsoft Entra ID

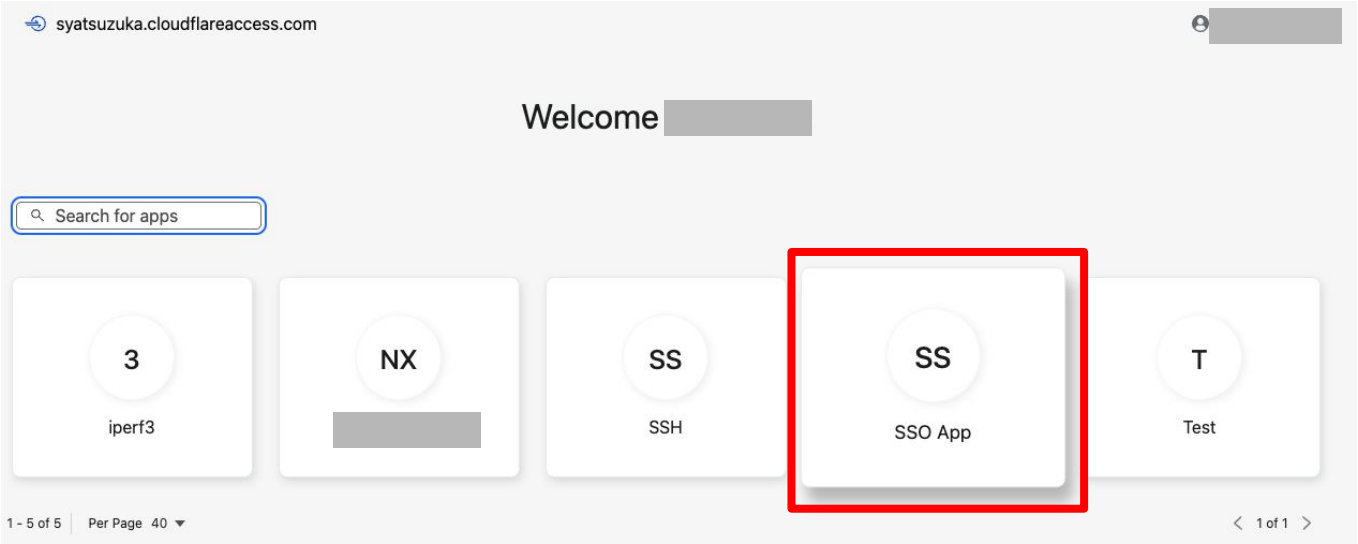


Cloudflareダッシュボードの初期設定

1. チーム名の設定
2. 認証方法の設定
3. **ダッシュボードの SSO登録 (オプショナル)**
4. Logpush設定

ダッシュボードのSSO登録

Cloudflare Dashboardへの認証に、Cloudflare Zero Trustで指定したSSOを経由させることがオプションとして可能となります。
以下はDashboardへのアクセスにZero TrustのSSOを適用の上、Zero TrustのLauncherにアプリケーション登録したイメージです。



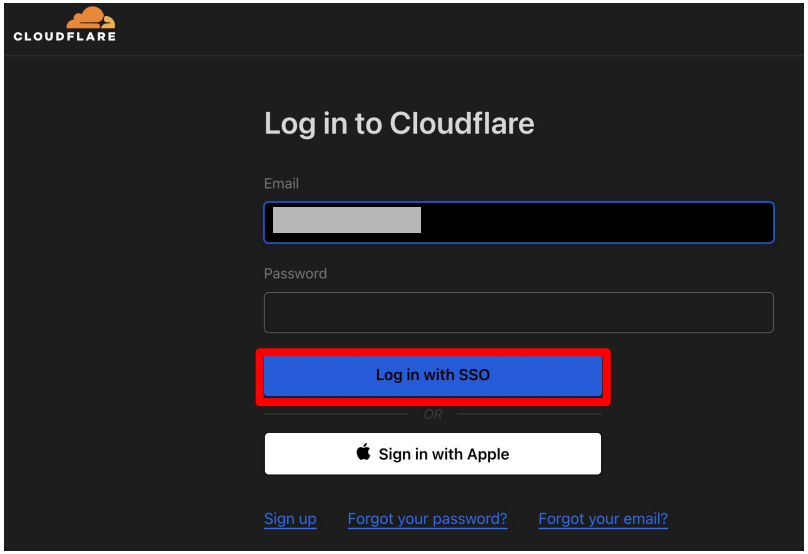
ダッシュボードのSSO登録

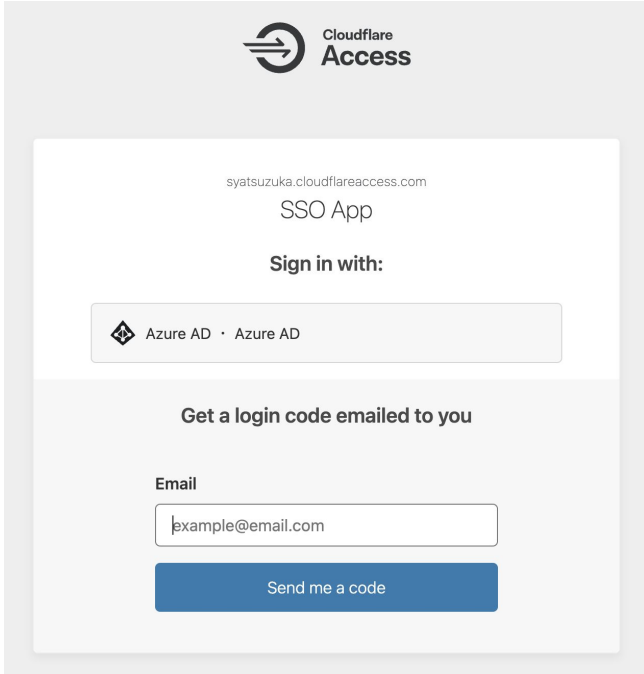
以下にCloudflare DashboardにSSOを適用させる流れを記します。

1. 担当のCSMへ、SSO Connectorの作成依頼 (SSOに用いるメールアドレスのドメインをご連絡)
2. Zero Trustダッシュボードから、Settings > Authenticationをクリック
3. Cloudflare dashboard SSOカードで該当するドメインを有効化
4. 管理画面をオープンしながら、別のブラウザウィンドウ(もしくは、Chromeをご利用の場合には、Incognitoなど)を利用の上、SSOの動作確認を実施
5. 動作確認ができれば、終了。動作不良が確認された場合には、SSOカードを無効化の上、調査。(もし管理画面をクローズし、SSOの無効化を行えない場合には、弊社サポートもしくは、担当CSMへ無効化を依頼。

参照) Cloudflare Docs - Setup Cloudflare dashboard SSO

ダッシュボードのSSO登録





SSOにより、都度パスワードを入力することなく、Loginへ進むことが可能となります。

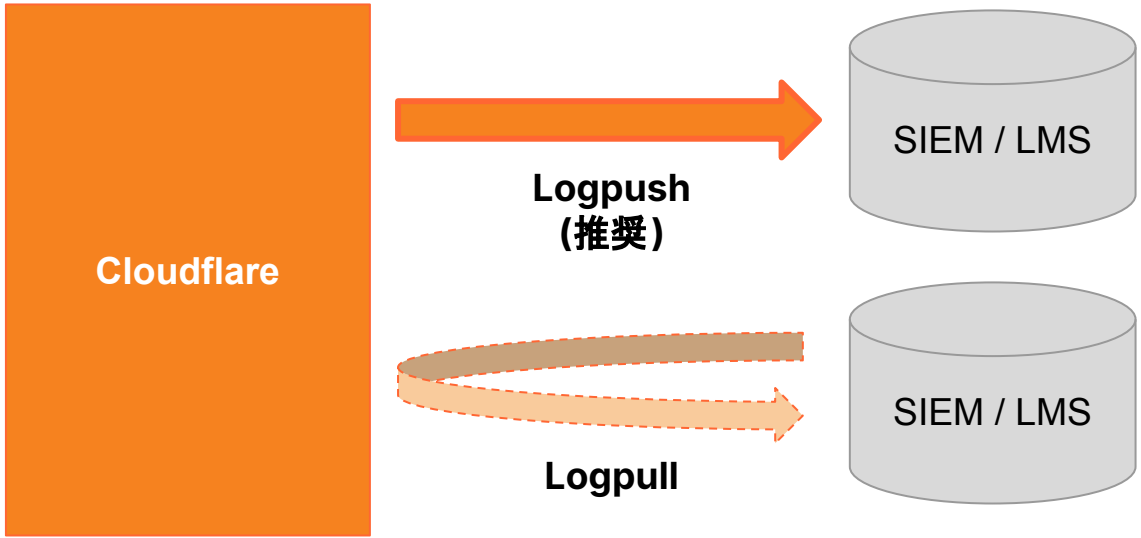
まだ、セッションが確立されていない場合には、初回認証画面へ

Cloudflareダッシュボードの初期設定

1. チーム名の設定
2. 認証方法の設定
3. ダッシュボードのSSO登録 (オプショナル)
4. **Logpush設定**

Logpush設定

Cloudflareでは各種ログ情報を「データセット」という形で外部の SIEM (Security Information and Event Management)もしくはLMS (Log Management System)へ転送することが可能です。
転送の方法としては大きく、Logpushジョブによる転送とLogpullによる転送（取得）が挙げれます。



Logpush設定

以下にLogpushによるログ連携の流れについて、紹介させていただきます。

1. Zero Trustダッシュボードから、Logs > Logpushをクリック
2. Connect a Serviceボタンをクリック
3. 入力項目を設定し、Nextボタンをクリック
4. ログ情報を格納するStorage Serviceを選択

※APIをご利用いただくことで、よりフレキシブルな設定が可能となります。

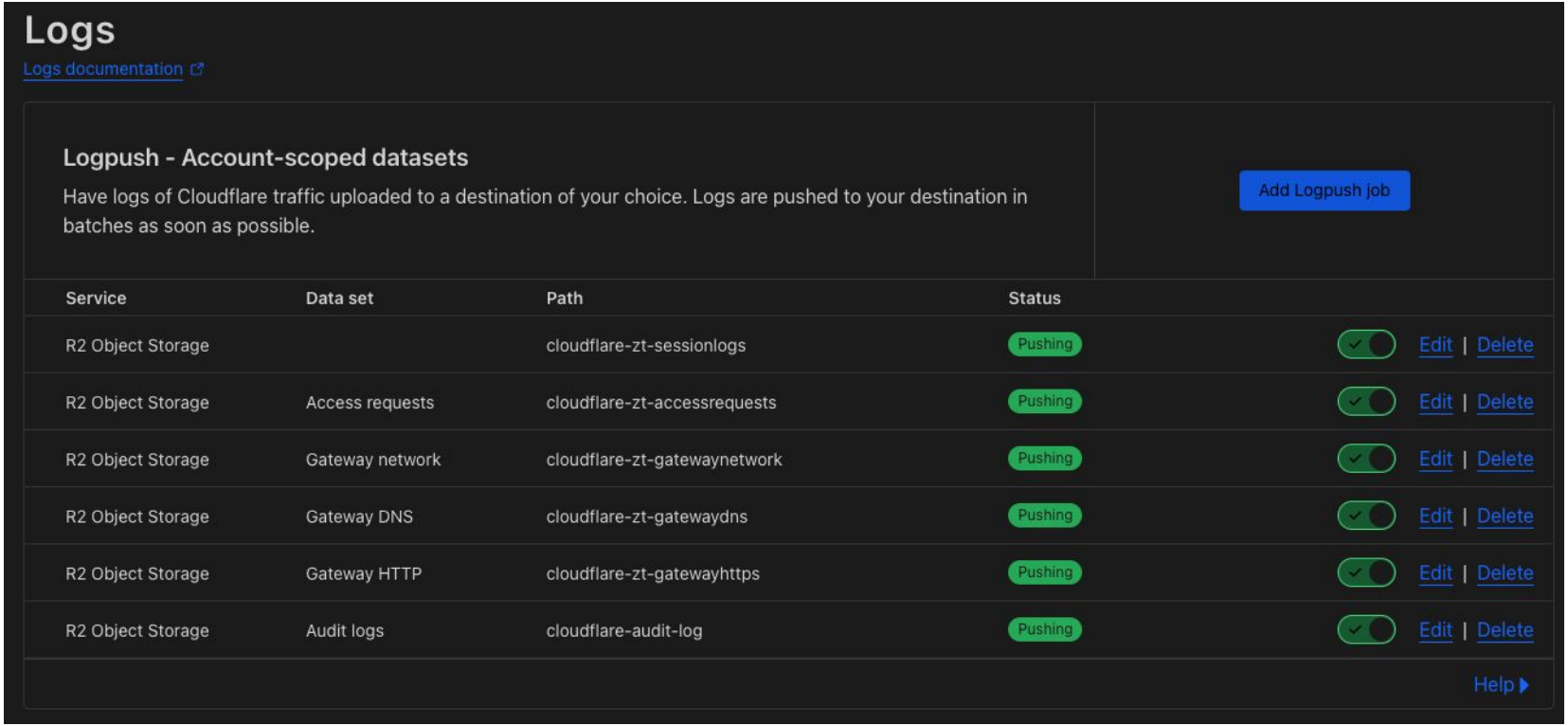
参照) Cloudflare Logpush Integration

Logpush設定

データセット	概要
Gateway DNS	Cloudflare GatewayでDNS Query情報
Gateway HTTP	Cloudflare GatewayでHTTPリクエスト
Gateway Network	Cloudflare Gatewayで検出されたネットワークパケット情報
Audit Logs	Cloudflare Accessを通した認証イベント情報
Access Requests	Cloudflare Accessで保護されたサイトへのHTTPリクエスト
CASB findings	Cloudflare CASBで確認されたセキュリティイシュー
Devise Posture	WARPクライアントによるDevise Postureステータス情報
Session Logs	Cloudflare GatewayでProxyされたネットワークセッションログ

参照) Cloudflare Docs - Zero Trust datasets

Logpush設定


Logs
Logs documentation
Logpush - Account-scoped datasets
Have logs of Cloudflare traffic uploaded to a destination of your choice. Logs are pushed to your destination in batches as soon as possible.
Add Logpush job
Service
Data set
Path
Status
R2 Object Storage
cloudflare-zt-sessionlogs
Pushing
Edit | Delete
R2 Object Storage
Access requests
cloudflare-zt-accessrequests
Pushing
Edit | Delete
R2 Object Storage
Gateway network
cloudflare-zt-gatewaynetwork
Pushing
Edit | Delete
R2 Object Storage
Gateway DNS
cloudflare-zt-gatewaydns
Pushing
Edit | Delete
R2 Object Storage
Gateway HTTP
cloudflare-zt-gatewayhttps
Pushing
Edit | Delete
R2 Object Storage
Audit logs
cloudflare-audit-log
Pushing
Edit | Delete
Help

Logpush設定 - R2にログを格納した際のクエリー実行例

```
$ curl -s -g -X GET
"https://api.cloudflare.com/client/v4/accounts/${CF_ACCOUNT_ID}/
logs/retrieve?start=2023-05-04T16:00:00Z&end=2023-05-06T16:0
0:00Z&bucket=${CF_LOG}&prefix={DATE}" \
-H "X-Auth-Email: ${CF_EMAIL}" \
-H "X-Auth-Key: ${CF_APIKEY}" \
-H "R2-Access-Key-Id: ${R2_ACCESS_KEY_ID}" \
-H "R2-Secret-Access-Key: ${R2_SECRET_ACCESS_KEY}" | jq .
```

参照) Cloudflare Docs - Logs Engine

Logpush設定 - R2にログを格納した際のクエリー実行例

Cloudflareでは各種ログはJSONフォーマットで出力されます。
右図の例は、DLPで検知され、指定されたFirewall Policyでブロックされたログの例となります。

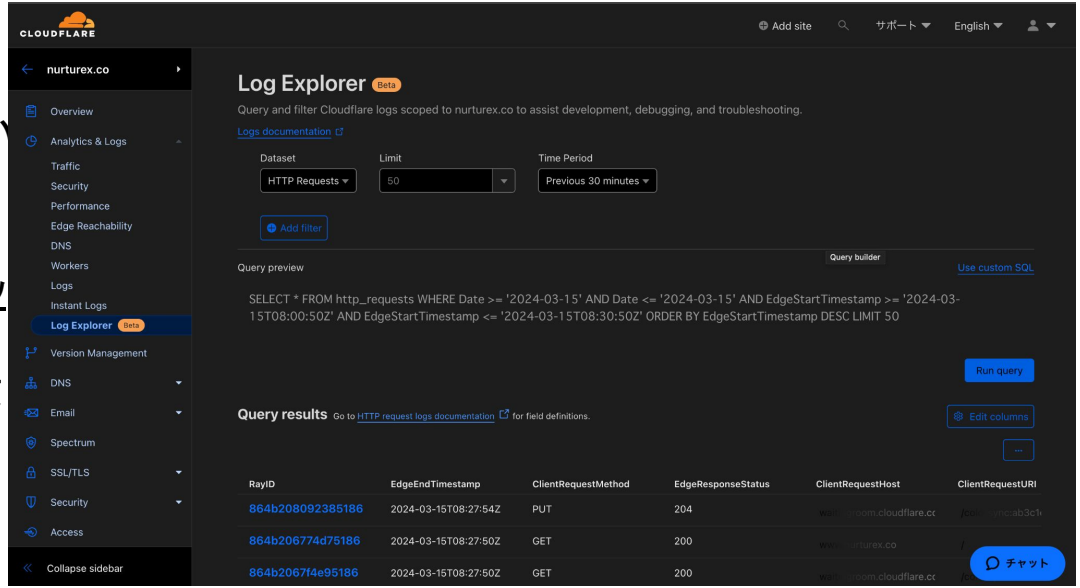

```
{
 "Datetime": "2024-04-05T00:21:44Z",
 "AccountID": "<Account ID>",
 "Action": "block",
 "BlockedFileHash": "",
 "BlockedFileName": "<unknown file name>",
 "BlockedFileReason": "unknown",
 "BlockedFileSize": 0,
 "BlockedFileType": "",
 "DestinationIP": "2404:6800:4004:828::200e",
 "DestinationPort": 443,
 "DeviceID": "<Devise ID>",
 "DeviceName": "WindowsPC",
 "DownloadedFileNames": [],
 "Email": "<Email Address>",
 "FileInfo": {
  "files": [
   {
    "direction": "upload",
    "file_name": "<unknown file name>",
    "file_hash":
"02e131789ea580261172ba96490e40f5e0e78fcf6d7d5fa93152f7bbaad4b16d",
    "file_size": 23367,
    "content_type": "application/vnd.chrome.ukm",
    "action": "block"
   }
  ]
 },
 "HTTPHost": "clients4.google.com",
 "HTTPMethod": "POST",
 "HTTPStatusCode": 302,
 "HTTPVersion": "HTTP/2",
 "IsIsolated": false,
 "PolicyID": "afd4ad33-a437-44f8-8ebc-a0cfb40f1cbe",
 "PolicyName": "Test - DLP",
 "Referer": "",
 "RequestID": "1f4d3b16ff00001f0f0824f400000001",
 "SourceIP": "60.118.112.139",
 "SourceInternalIP": "",
 "SourcePort": 51260,
 "URL": "https://clients4.google.com/ukm",
 "UntrustedCertificateAction": "none",
 "UploadedFileNames": [],
 "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36",
 "UserID": "<User ID>"
}
```

Logpush設定 - Log Explorer (beta)

Log Explorer (beta)を有効化することで、一部ログをR2で管理の上、Cloudflareのダッシュボード上でご確認いただく事が可能となりました。

※今日においてはZero Trustのデータセットは対応されておりませんが、今後対応データセットも増えていくことが期待されます。

参照) Cloudflare Docs - Log Explorer (beta)



WARPクライアントのインストール

1. はじめに
2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. **WARPクライアントのインストール**
5. Q&A

WARPクライアントのインストール

1. **Device Enrollment Permissionの定義**
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. ログの確認
6. その他確認画面

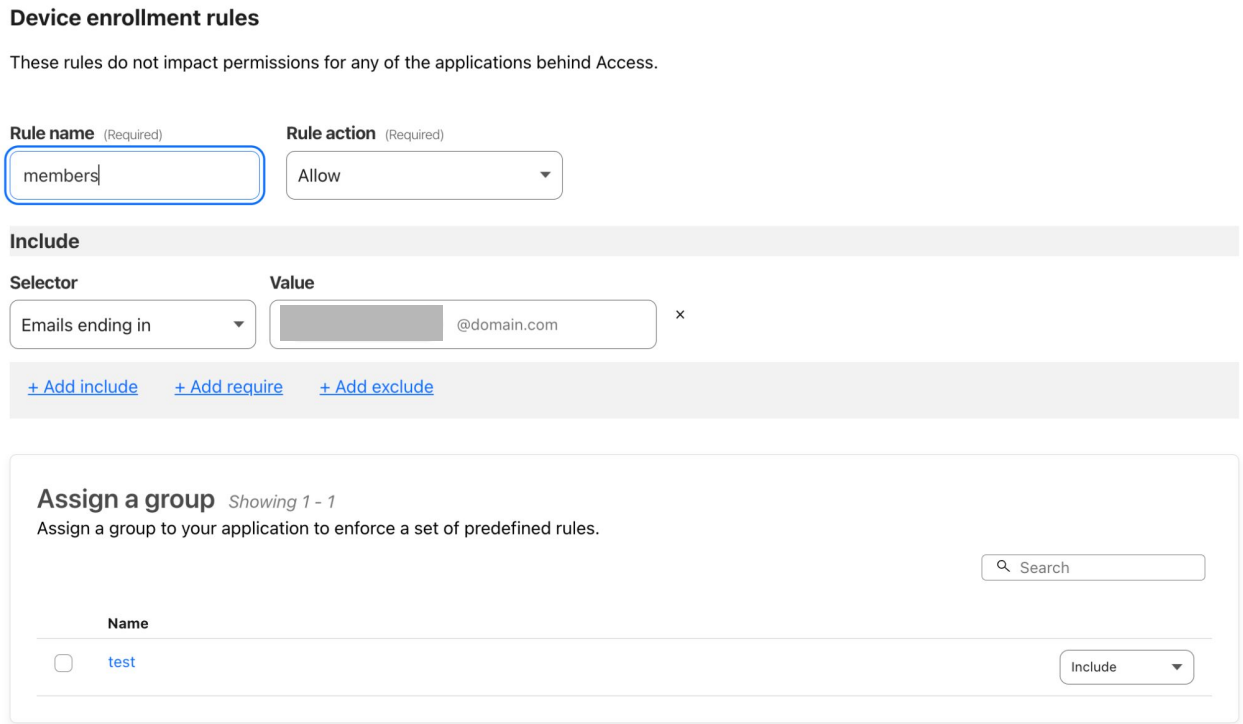
Device Enrollment Permissionの定義

Device Enrollment Permissionは、WARPのTeamへのアクセスを許可する対象ユーザーを指定する設定です。
以下に設定の流れを記載いたします。

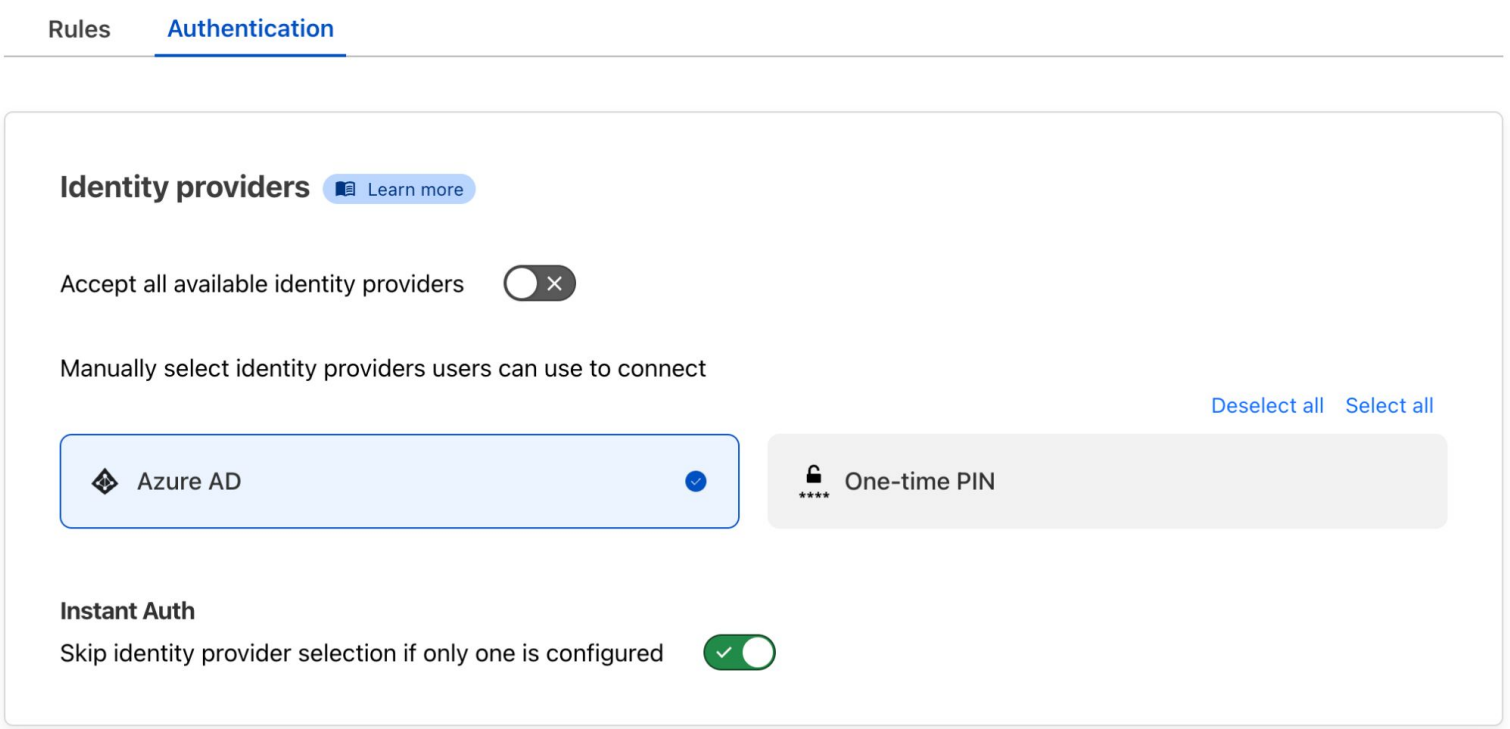
1. Zero Trustダッシュボードから、Settings > WARP Clientへアクセス
2. Device enrollmentカードから、Manageボタンを選択
3. RulesタブでAccess policies (どのユーザーが彼らのデバイスからZero Trust環境への接続を許すか)を定義
4. Authenticationタブで、ユーザーが利用可能なidentity providersを選択
5. Saveボタンをクリック

参照) Cloudflare Docs - Device enrollment permissions

Device Enrollment Permissionの定義



Device Enrollment Permissionの定義



WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. **WARPクライアントのインストール**
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. ログの確認
6. その他確認画面

WARPクライアントのインストール

WARPクライアントのインストールの流れを以下に記します。

1. カスタムルート証明書をCloudflareへアップロード (オプショナル)
2. Zero Trustダッシュボードから、Settings > WARP Clientへアクセス
3. Install CA to system certificate storeを有効化
4. WARPクライアントをダウンロードの上、インストール
5. Zero TrustのTeamへデバイスを登録
   カスタム証明書がアップロードされていない場合には、デフォルトのCloudflare証明書がインストールされます。
6. インストールされた証明書の確認

参照) Cloudflare Docs - Install a certificate using the WARP client

WARPクライアントのインストール - WARPによる証明書のインストール

HTTPSトラフィックのチェック (TLS Decryption)、Data Loss Prevention、アンチウィルススキャニング、Browser Isolationといったセキュリティ機能を利用するには、Cloudflareの証明書設定が必要となります。

デスクトップデバイスにWARPクライアントをインストールする際には、証明書も自動インストールされますが、モバイル端末にWARPクライアントをインストールする際には、手動による証明書のインストールが必要となります。

参照) Cloudflare Docs - User-side certificates

WARPクライアントのインストール - サイレントインストールコマンド

以下コマンドでサイレントインストールが可能です(詳細についてはマイクロソフト社、Apple社にお問い合わせください)

(Windows)

```
PS> msiexec /i "Cloudflare_WARP_Release-x64.msi" /qn ORGANIZATION="your-team-name"
SUPPORT_URL="http://support.example.com"
```

※ご利用のPC環境によっては、コマンドとしてmsiexecではなく、WARPのMSIファイルを直接呼び出すことでもインストールされるケースも確認されております。なお、ORGANIZATIONおよびSUPPORT_URLはオプショナルであり、インストール後に追加設定可能です。

(Mac)

```
$ sudo installer -pkg <WARPパッケージファイル> -target /
```

参照)

Cloudflare Docs - Install WARP

Cloudflare Docs - Manual deployment

WARPクライアントのインストール - WARPのバージョン管理

2023年11月時点においては、WARPは以下の様なバージョン管理がなされ、一つのブランチで継続メンテナンスされる形が取られ、Long Term Supportに相当するバージョンの管理はございません。

YYYY.MM.<パッチバージョン >.<リリースタイプ >

<リリースタイプ>
0: GA
1: αもしくはβバージョン

※ 安定稼働が期待される場合には、MDM等を用いて組織内で所定のバージョンをご利用いただき、その後は動作検証の上で、アップデートを行っていただくことが推奨されます。

参照)

Cloudflare Docs - Download WARP

Cloudflare Docs - Managed deployment

WARPクライアントのインストール - 必要なFirewall設定

WARPをご利用される際には、以下ドキュメントで指定されたポートに対するFirewall設定（穴あけ）が必要となります。

参照) Cloudflare Docs - WARP with firewall

WARPクライアントのインストール - レガシーVPNとの併用

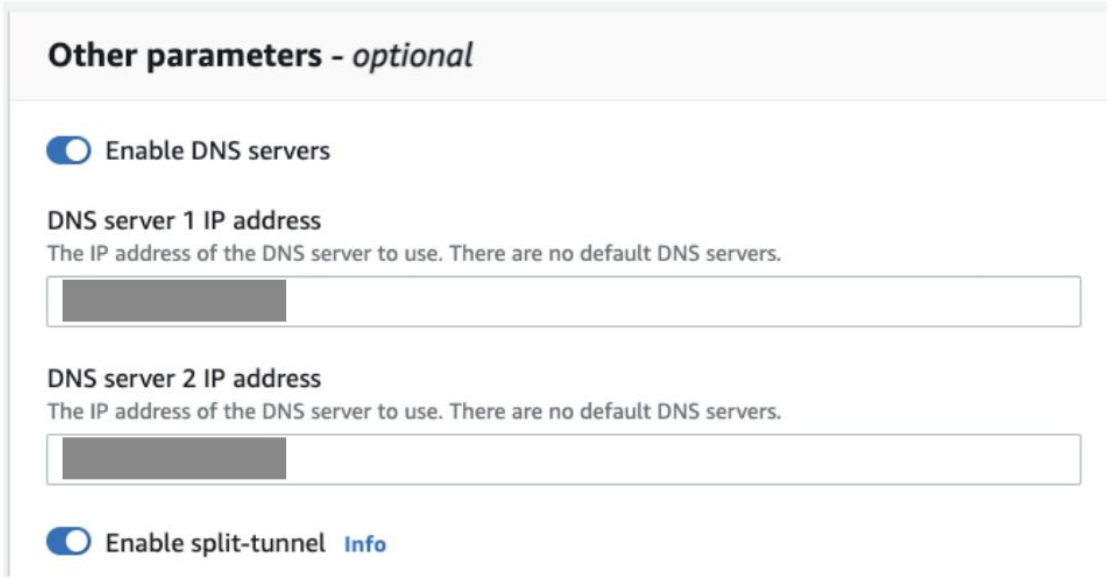
レガシーVPNとの併用をご検討の場合には以下設定の元での動作をご確認いただければと思います。

<VPN側設定>
- サードパーティーVPNにおけるスプリットトンネルの有効化
- サードパーティーVPNにおけるDNS設定の無効化

<WARP側設定>
- VPNで利用されるプライベートIPをスプリットトンネルで除外
- VPNの接続先ホストをスプリットトンネルで除外
- (オプショナル) VPNのプライベートDNSで名前解決させたいドメインをLocal Domain Fallbackで指定

参照) Cloudflare Docs - WARP with legacy VPN

WARPクライアントのインストール - レガシーVPNとの併用



サードパーティーVPNのスプリットトンネルの設定イメージ

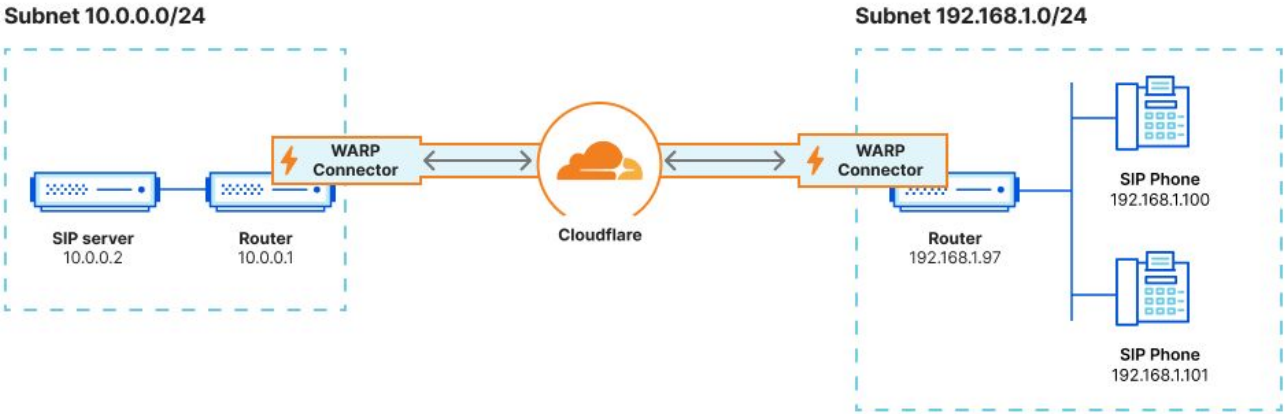
WARPクライアントのインストール - WARP to WARP

WARP to WARPを用いることで、PC間のPeer-to-Peer接続を確立することが可能となります。

参照) Cloudflare Docs - Create private networks with WARP-to-WARP

WARPクライアントのインストール - WARP Connector (Beta)

WARP Connectorを用いることで、cloudflaredなしに、また、個別のPCにWARPをインストールすることなく、複数拠点間の通信が可能となります。
(ただし、認証にはService Tokenが利用されるため、ユーザーの特定ができません)



参照) Cloudflare Docs - Set up WARP Connector

WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. **Zero Trustインスタンスへのログイン**
4. WARPクライアントの詳細設定
5. ログの確認
6. その他確認画面

Zero Trustインスタンスへのログイン

1. メニューバーから、Cloudflareのロゴマークのアイコンをクリック
2. 設定アイコンをクリック
3. Preferences > Accountをクリック
4. Login with Cloudflare Zero Trustを選択
5. 登録したTeam名を入力
6. Teamで登録されている認証ステップを実施

→ ご利用のデバイスがチームに登録され、Zero Trustのポリシーが適用されます。

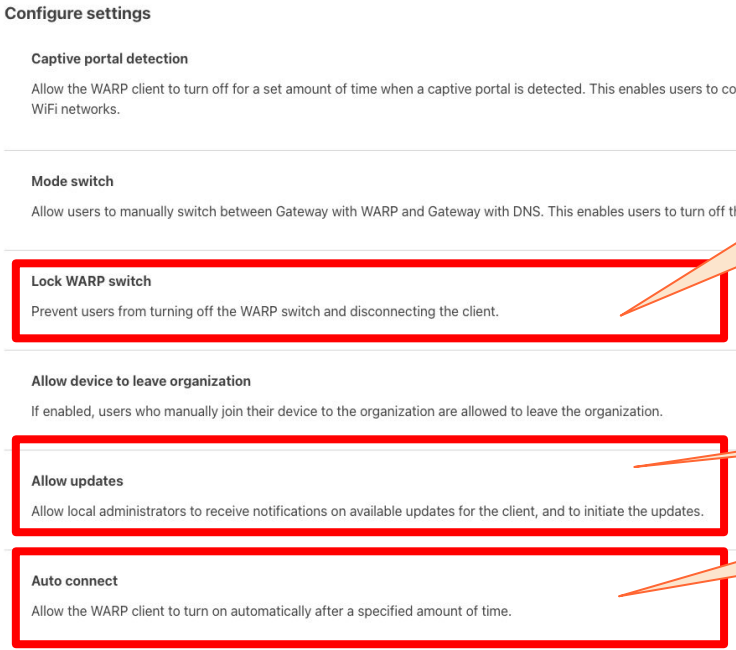
参照) Cloudflare Docs - Manual deployment

WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. **WARPクライアントの詳細設定**
5. ログの確認
6. その他確認画面

WARPクライアントの詳細設定

Settings > WARP ClientのDevice Settingsから、各クライアントに対する詳細設定を行う事が可能です

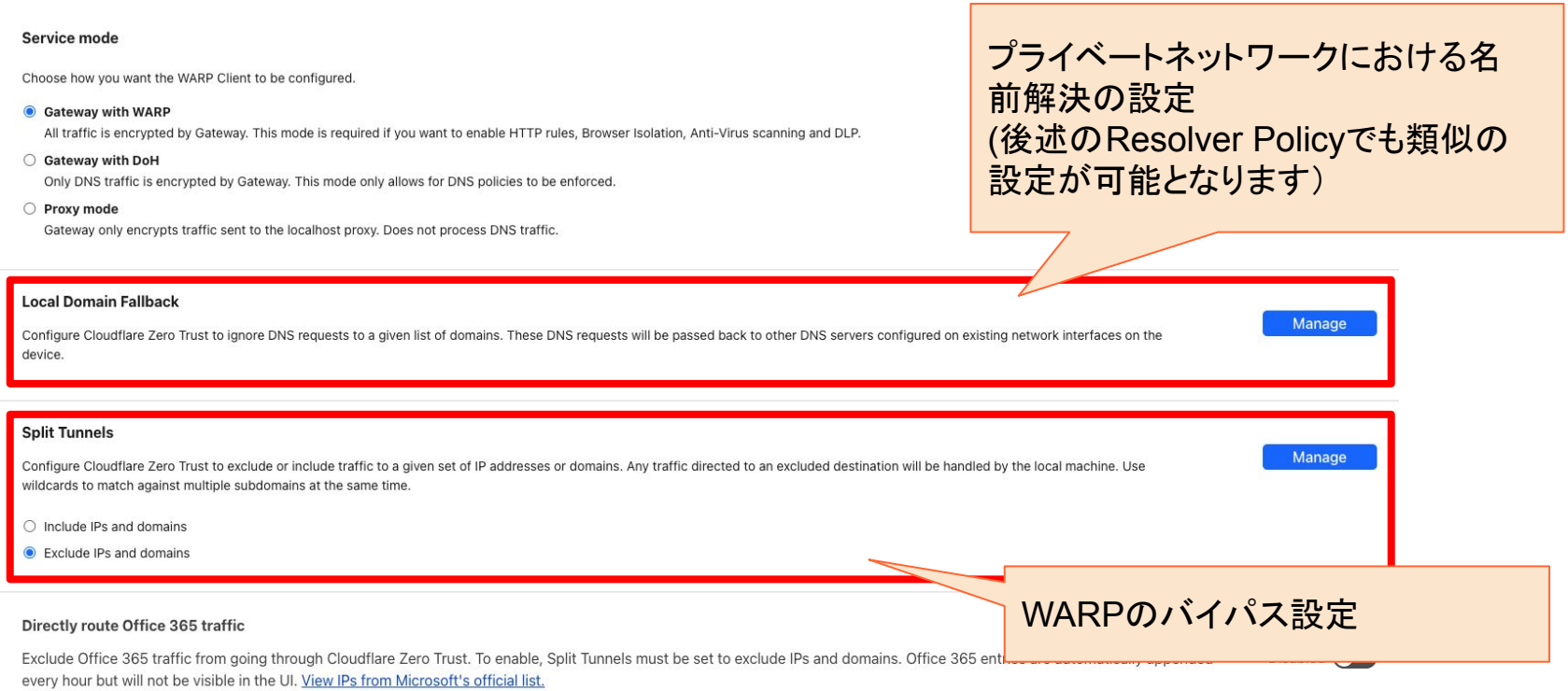


各端末におけるWARPの解除を禁止する設定
(試験導入フェーズにおいては Lockを外すことが推奨)

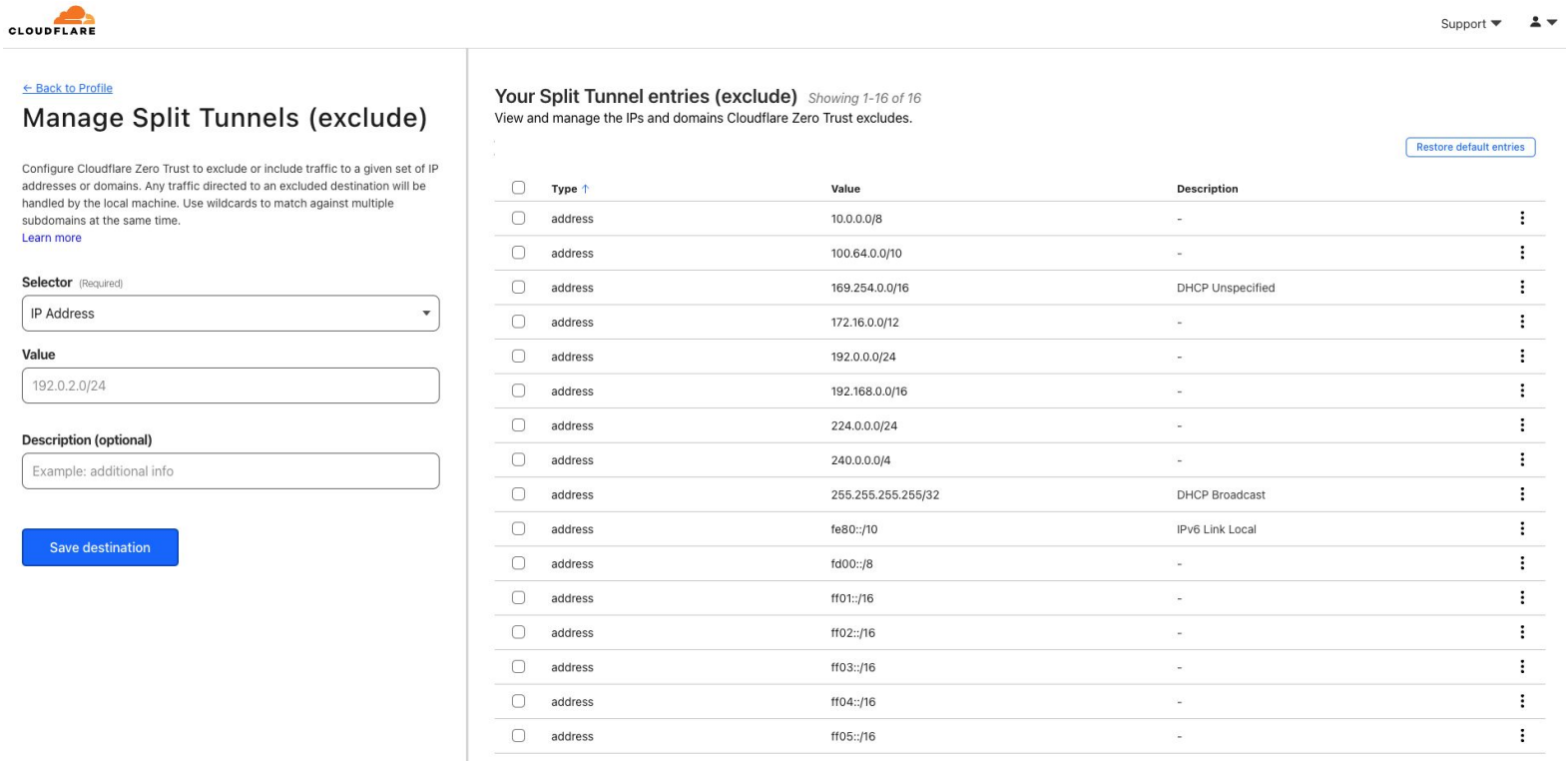
安定稼働のためには自動アップデートをオフにすることを推奨

WARPを解除後、一定時間後に自動で有効化させる設定

WARPクライアントの詳細設定



WARPクライアントの詳細設定 - Split Tunnel



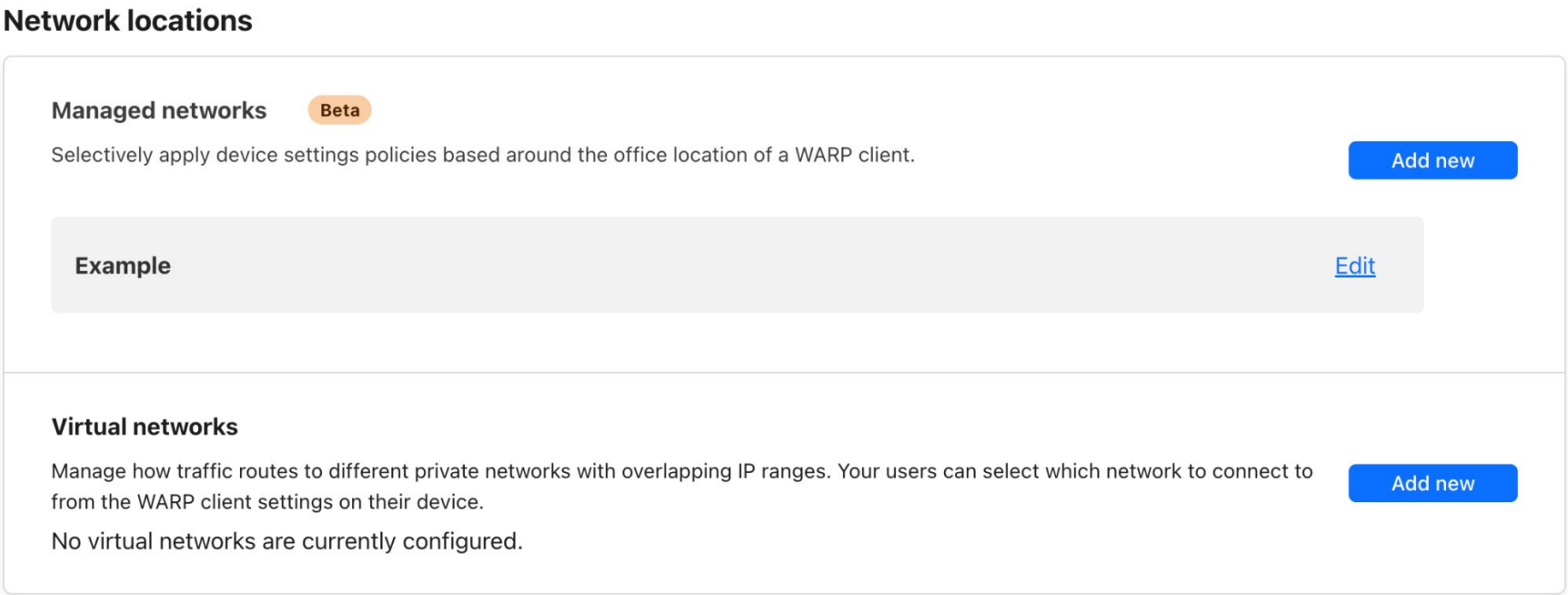
WARPクライアントの詳細設定 - Managed Network

Settings > WARP ClientのManaged networksで、特定のネットワーク環境でのみアクセス可能なサーバーの証明書情報を設定いただくことで、接続先ネットワークに応じてProfile Settingを切り替える事で、接続先ネットワークに応じたSplit Tunnelを設定することが可能となります。

→ Profile Setting (Office)を適用
オフィスネットワークのサーバーに Split Tunnelを適用 (直接アクセス)

→ Profile Setting (Remote)を適用
オフィスネットワークのサーバーに Split Tunnelを非適用 (Cloudflare Tunnel経由)

WARPクライアントの詳細設定 - Managed Network



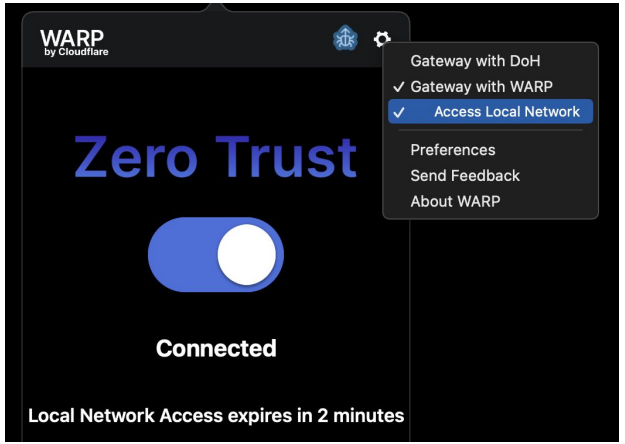
WARPクライアントの詳細設定 - Managed Network

Profile Settingsの適用ルールにManaged Networkを指定した例

参照）Cloudflare Docs - Add a Managed Network

WARPクライアントの詳細設定- Allow users to enable local network exclusionオプション

WARPの設定オプションで、一時的にプライベートネットワークへの直接通信を可能とするオプションがリリースされました。



参照) Cloudflare Docs - WARP Settings - Allow users to enable local network exclusion

WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. **ログの確認**
6. その他確認画面

CLOUDFLARE

ログの確認 - WARPログ

WARPでなにか障害が確認された際には、Cloudflareのサポートチケットを起票の上、以下操作で取得されたWARPログを添付いただければと思います。

(Mac or Linux)
$ warp-diag

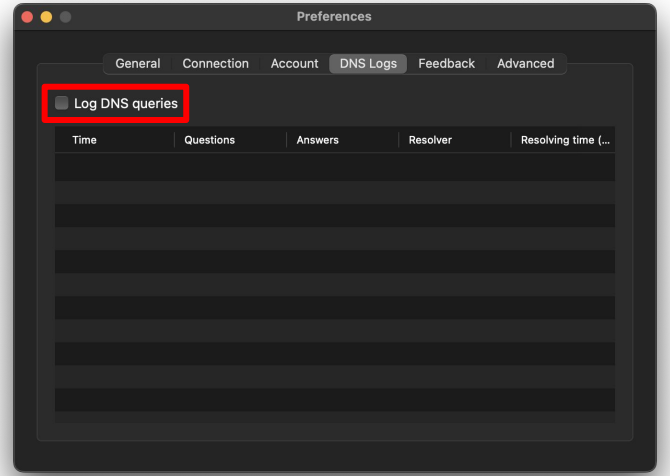
(Windows)
C:¥Users¥xxx> warp-diag

参照) Cloudflare Docs - Debug logs

ログの確認 - その他のログ取得

チケットにてお問い合わせの際、お問い合わせの内容によっては、以下を追加で依頼させていただくケースもございます。

- WARPにおけるDNS Logsの有効化
- 以下ホストへのtraceroute (connectivity check)
  - engage.cloudflareclient.com
  - connectivity.cloudflareclient.com
- Tunnel Logの取得

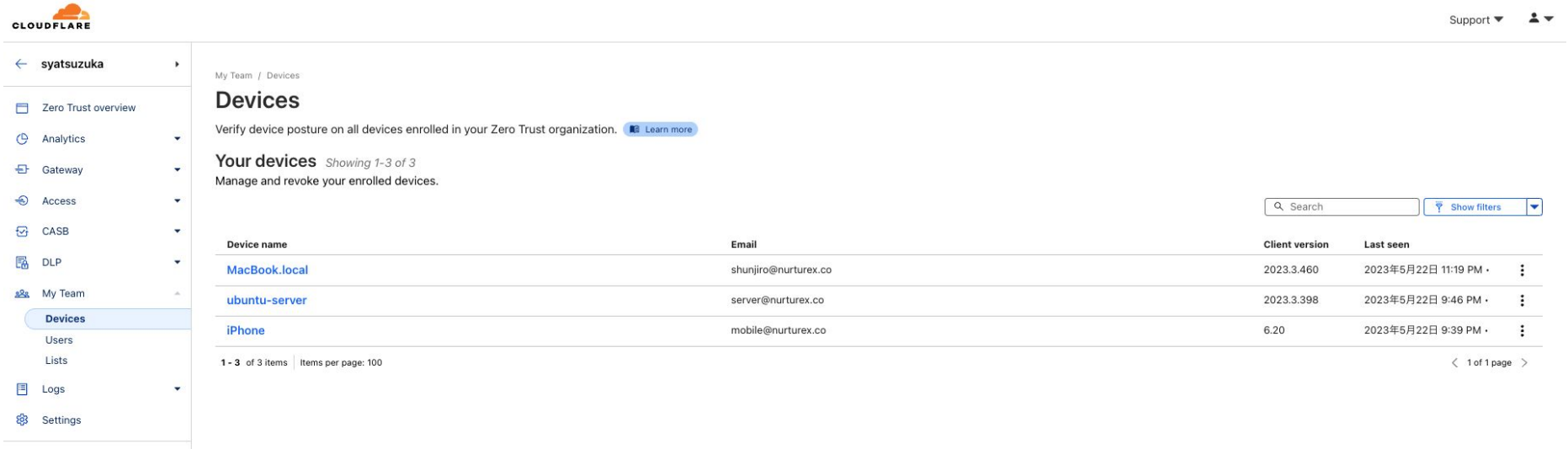


WARPクライアントのインストール

1. Device Enrollment Permissionの定義
2. WARPクライアントのインストール
3. Zero Trustインスタンスへのログイン
4. WARPクライアントの詳細設定
5. ログの確認
6. **その他確認画面**

その他確認画面 - 登録デバイス

1. Zero Trustダッシュボードから、My Teams > Devicesをクリック
   登録デバイスの一覧から、それぞれのデバイスのWARPクライアントバージョン、最終ログイン日時をご確認いただけます。



その他確認画面 - 登録デバイス

MacBook.local

Device details

ACTIVE

Device name	Registration ID
MacBook.local	[redacted]

OS Version	Product version extra	Manufacturer	Model	Mac address	Serial number
13.3.1	-	-	MacBookPro18,3	[redacted]	[redacted]

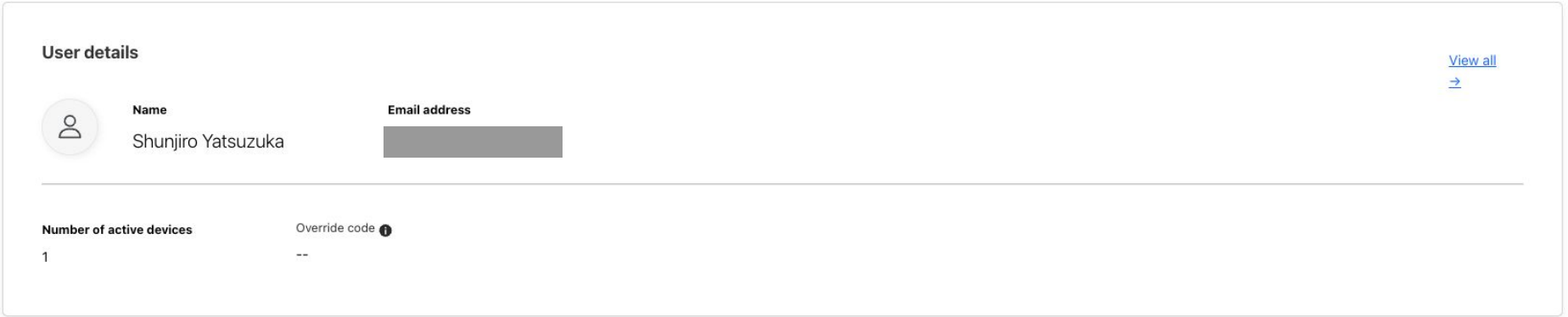
Client details

Client	Status	Client version	Last seen
Cloudflare WARP	Connected	2023.3.460	May 22 2023 • 11:19:14 PM

Virtual network	DoH subdomain	Virtual IP addresses
default	-	IPv4: [redacted] IPv6:

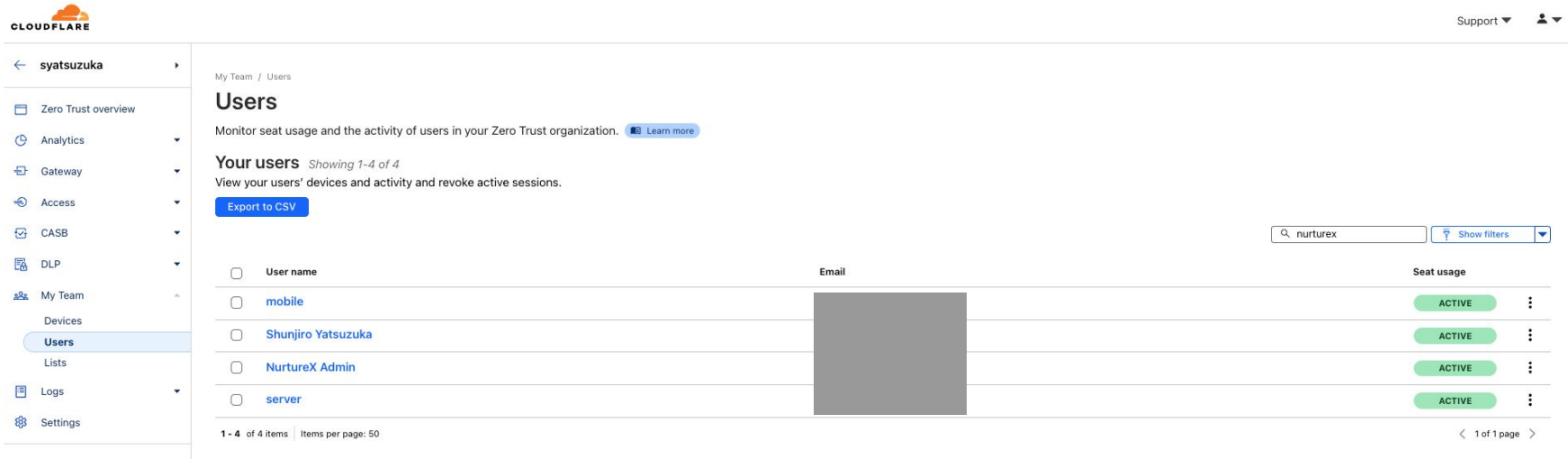
その他確認画面 - 登録デバイス

各登録デバイスから、その利用ユーザーをご確認いただけます。

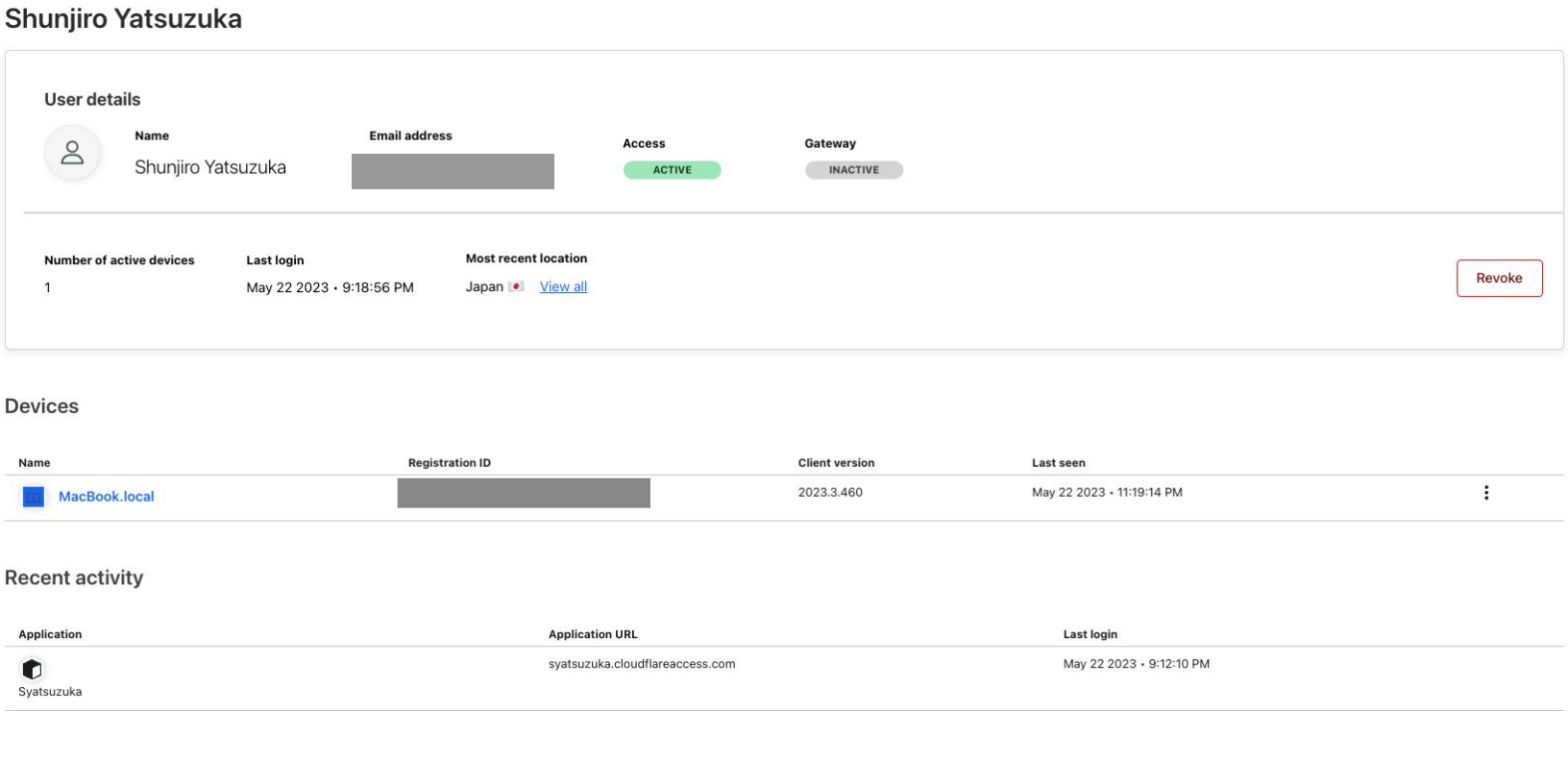


その他確認画面 - 登録ユーザー

1. Zero Trustダッシュボードから、My Teams > Usersをクリック
   登録ユーザーの一覧から、現在のアクティブユーザー、ユーザーの登録解除、最終ログイン日時、ロケーション、利用デバイスを確認可能



その他確認画面 - 登録ユーザー



Q&A

1. はじめに
2. Cloudflare Zero Trust導入の流れ
3. Cloudflareダッシュボードの初期設定
4. WARPクライアントのインストール
5. **Q&A**

Thank you

1 888 99 FLARE
enterprise@cloudflare.com
cloudflare.com

CLOUDFLARE

Cloudflare連続勉強会 #7

Cloudflare Zero Trustの紹介 (後編) - 導入編

カスタマーサクセス　シニアマネージャー　八塚 俊次郎
シニアカスタマーソリューションエンジニア　西原 誠

Cloudflare Japan
東京都中央区京橋 2-2-1京橋エドグラン 26階
www.cloudflare.com/ja-jp/

Agenda

1 はじめに

2 Cloudflare ZTNAの機能および設定

3 Cloudflare SWGの機能および設定

4 Cloudflare CASBの機能および設定

5 Cloudflare DLPの機能および設定

6 Q&A

はじめに

1. はじめに
2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
5. Cloudflare DLPの機能および設定
6. Q&A

目的

本WebinarはCloudflareのEnterpriseプランのご契約をお持ちのお客様向けにCloudflare製品の機能及び設定概要を紹介することで、製品をよりよくご活用いただくことを主目的とします。

時間配分	内容
50分	メインセッション
10分	Q&A

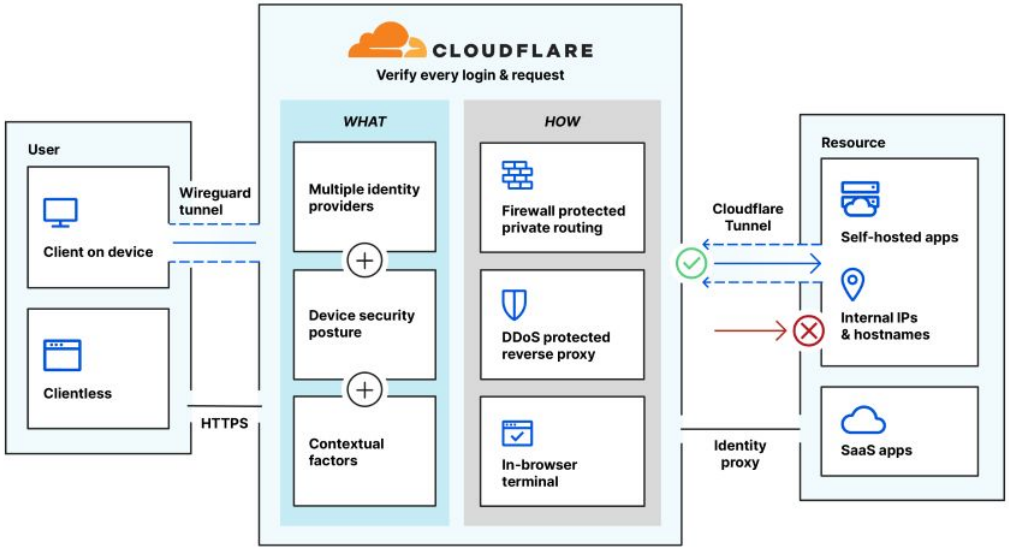
注意事項

本Webinarご参加に当たっての注意事項を以下記載いたします。

- 本Webinarはレコーディングを行い、後日、弊社Webinarサイトにご登録のお客様は再視聴できるようにいたします。各セッションの最後にはブラウザ上のテキストボックスからご質問を受付けますが、起票者のお名前は伏せてのQ&A対応となります。
- お時間の制約から、Webinar中に頂いたすべてのご質問にお答えできないかもしれません。最善は尽くさせていただければと考えておりますが、その旨、ご了承いただければと思います。
- 本セッションで用いるスライドはセッション終了後、当Webinarのご登録ページからPDF形式でダウンロード頂けます。

前回セッションの振り返り

Cloudflare Zero Trust導入の流れとしてはRoadmap to Zero Trustをご参照いただけます。



参照) Cloudflare Zero Trust Network Accessの鳥瞰図

前回セッションの振り返り

1. **Cloudflare Zero Trust導入の流れ**
2. **Cloudflareダッシュボードの初期設定**
   a. チーム名の設定
   b. 認証方法の設定
   c. ダッシュボードの SSO登録 (オプショナル)
   d. Logpush設定
3. **WARPクライアントのインストール**
   a. Device Enrollment Permissionの定義
   b. WARPクライアントのインストール
   c. Zero Trustインスタンスへのログイン
   d. WARPクライアントの詳細設定
   e. ログの確認
   f. その他確認画面

※前回セッションのレコーディングは Cloudflare Resource Hubからご参照いただけます。

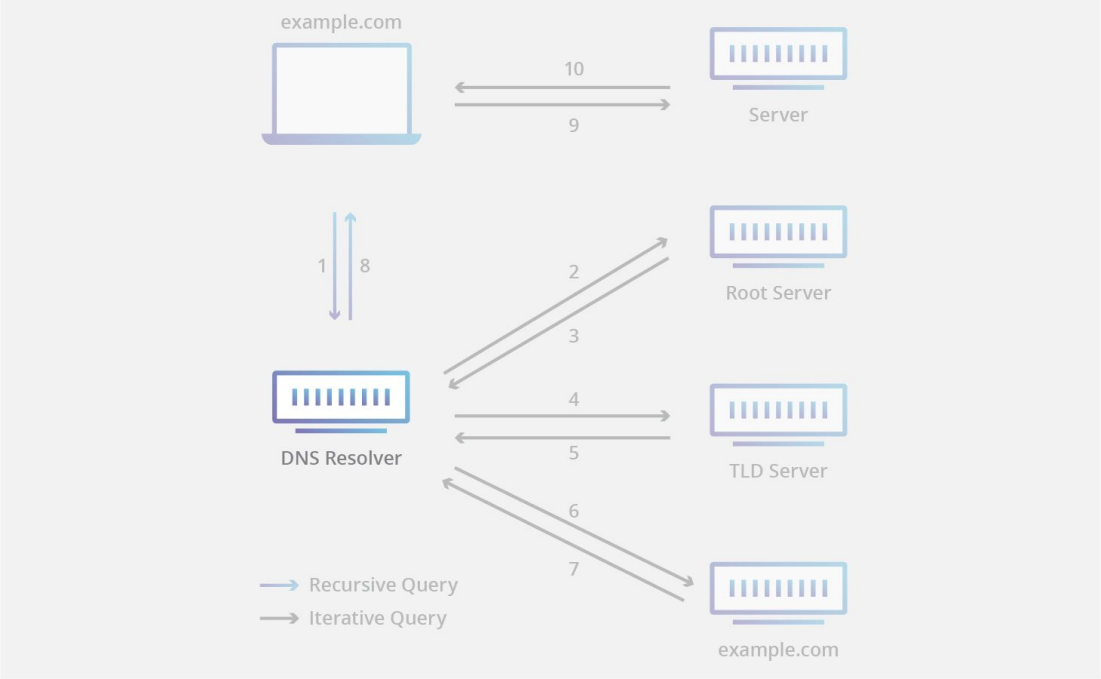
Cloudflare ZTNAの機能および設定

1. はじめに
2. **Cloudflare ZTNAの機能および設定**
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
5. Cloudflare DLPの機能および設定
6. Q&A

ZTNAの設定

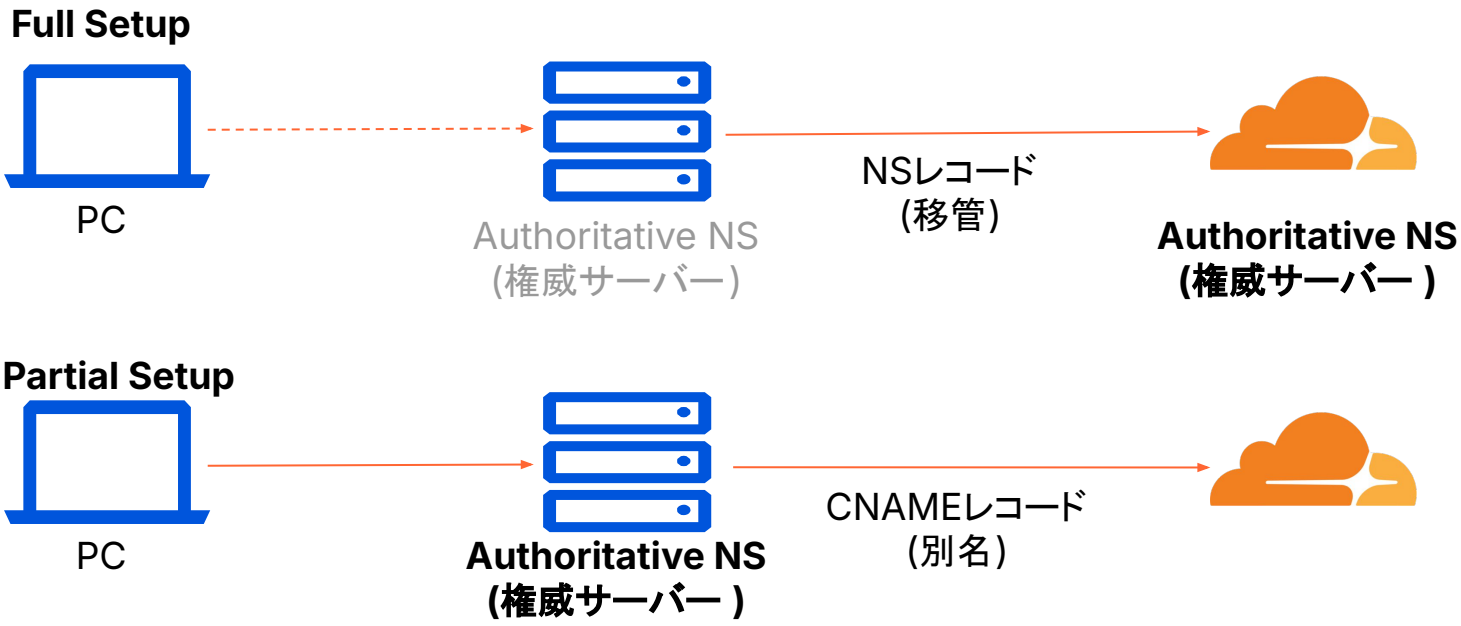
1. **サイトの登録（オプショナル）**
2. Tunnel設定
3. アプリケーションの登録

サイトの登録 - 名前解決の仕組み



参照) What are the different types of DNS server?

サイトの登録 - Full SetupとPartial Setup



CLOUDFLARE

サイトの登録

1. Cloudflareへのサイトの登録
2. DNSのFull Setup
3. DNSのPartial Setup
4. SSL/TLSセットアップ

参照) Cloudflare Docs - Add site to Cloudflare

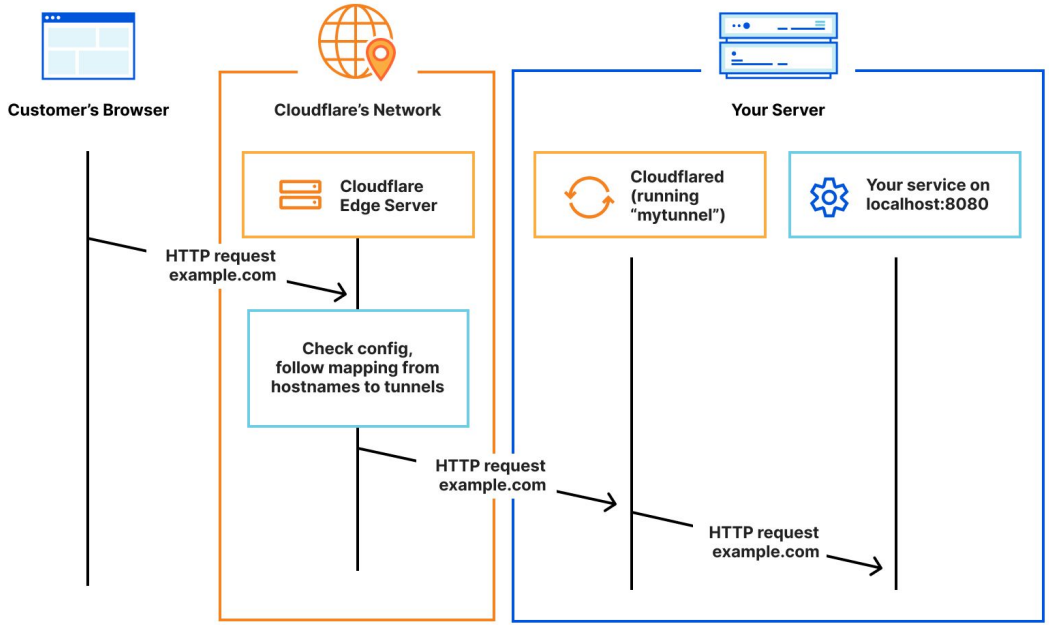
※詳細はCloudflare連続勉強会 #3 - Cloudflare DNSおよびSSL/TLSのご紹介をあわせてご参照くださいませ。

CLOUDFLARE

ZTNAの設定

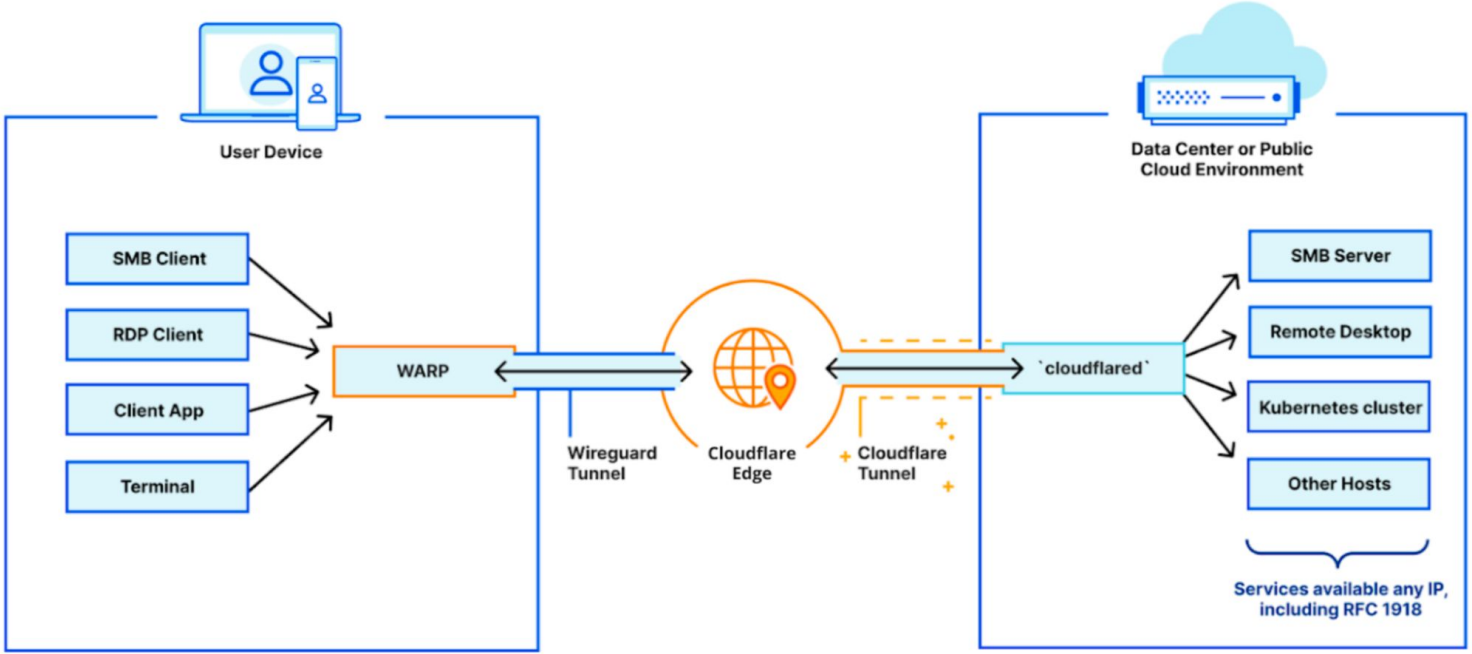
1. サイトの登録 (オプショナル)
2. **Tunnel設定**
3. アプリケーションの登録

Tunnel設定



参照) [Cloudflare Docs - Cloudflare Tunnel]

Tunnel設定



参照) [Cloudflare Docs - Private hostnames and IPs]

Tunnel設定

cloudflaredによるTunnel設定は大きく2つのアプローチがあります。

- Public Hostnameの設定：ホスト名を指定した接続を実現したい場合 (HTTP以外のプロトコルでアクセスさせたい場合には、クライアント端末にcloudflaredの追加インストールが必要になる場合あり)

- Private Networkの設定：プライベートIPアドレスを指定した接続を実現したい場合 (WARP経由でのアクセス)

※SSHサーバーへの接続においては、新たにAccessの認証情報を元にshort-lived certificateを作成し、SSHサーバーへの接続を実現するAccess for Infrastructureをご利用いただけます。

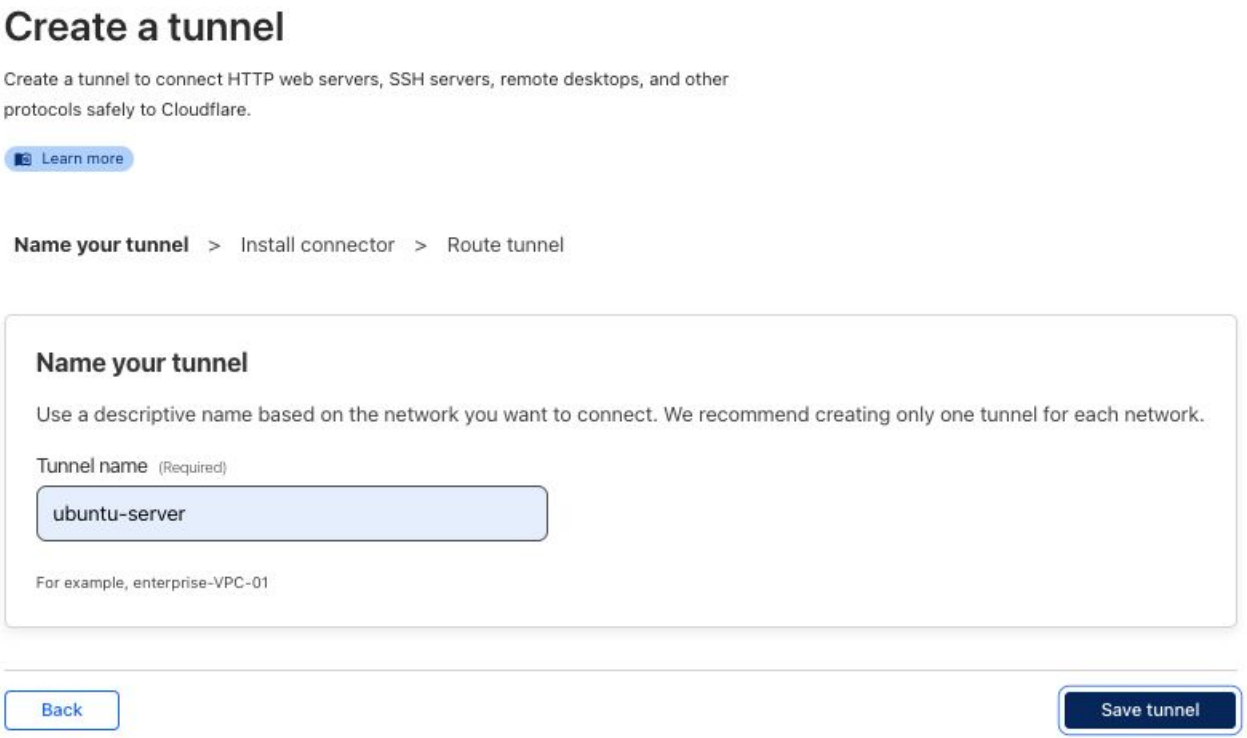
CLOUDFLARE

Tunnel設定

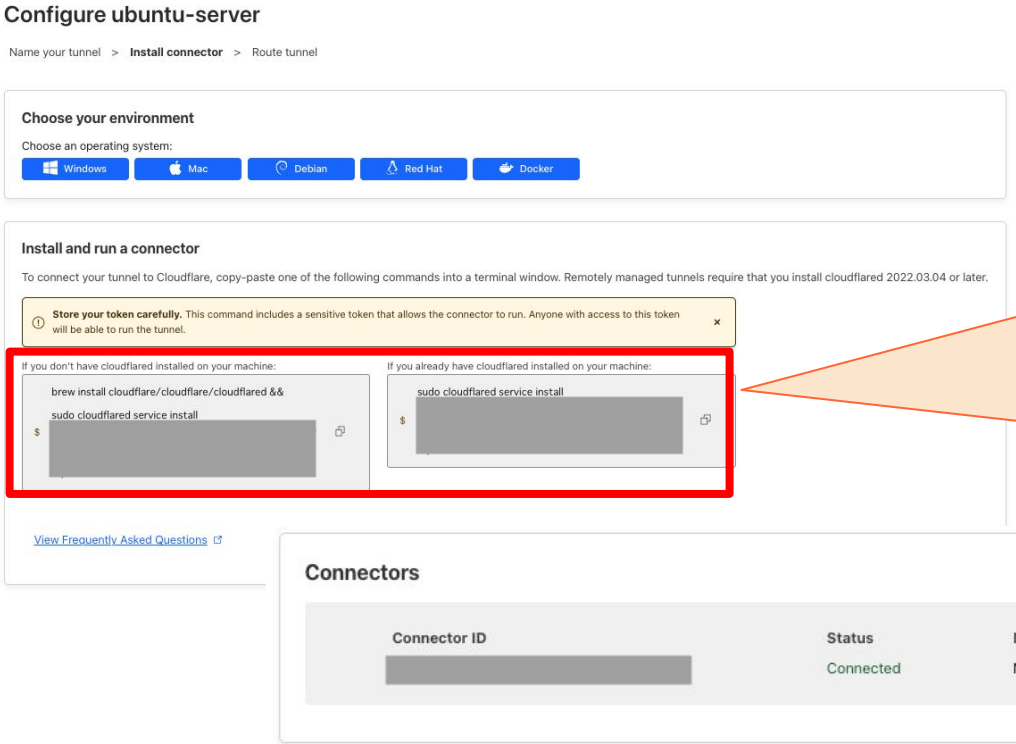
1. Zero Trustダッシュボードから、Access > Tunnelsへアクセス
2. Create a tunnelボタンをクリック
3. Tunnel名を設定
4. Connectorの作成
5. ルーティング設定
6. Save tunnelボタンをクリック
7. 追加設定

参照) Cloudflare Docs - Setup a tunnel through the dashboard

Tunnel設定 - Tunnel名を設定



Tunnel設定 - Connectorの作成

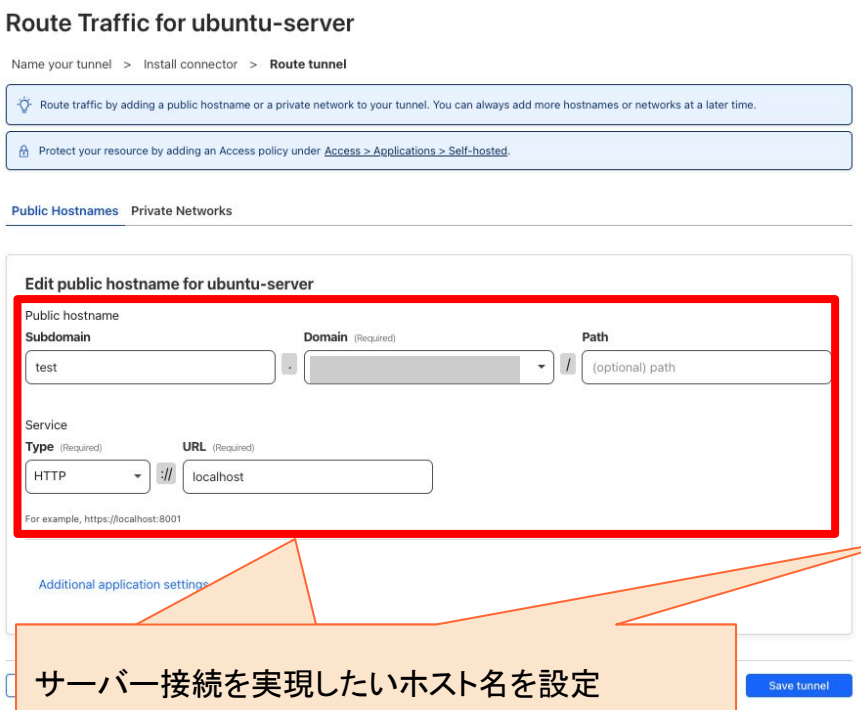


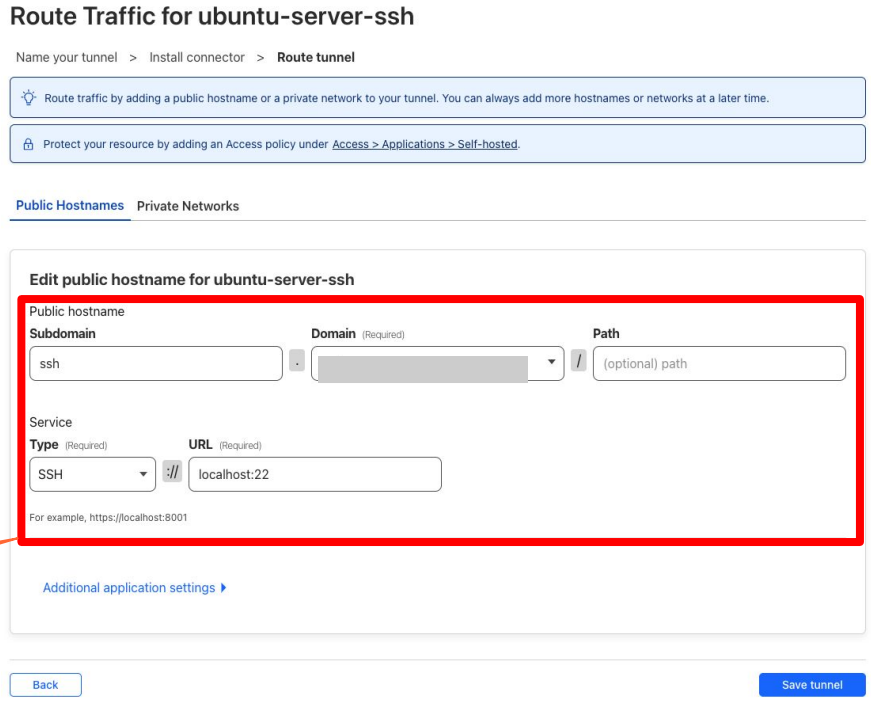
こちらで表示されるコマンドをcloudflaredをインストールしたいホスト上で実行することで、Connectorが作成されます。

※すでに同じサーバー上にConnectorが存在する場合、削除しないと新規Connectorが正しく作成・認識されない場合がありますのでご注意ください。

<既存Connector削除コマンド>
$ sudo cloudflared service uninstall

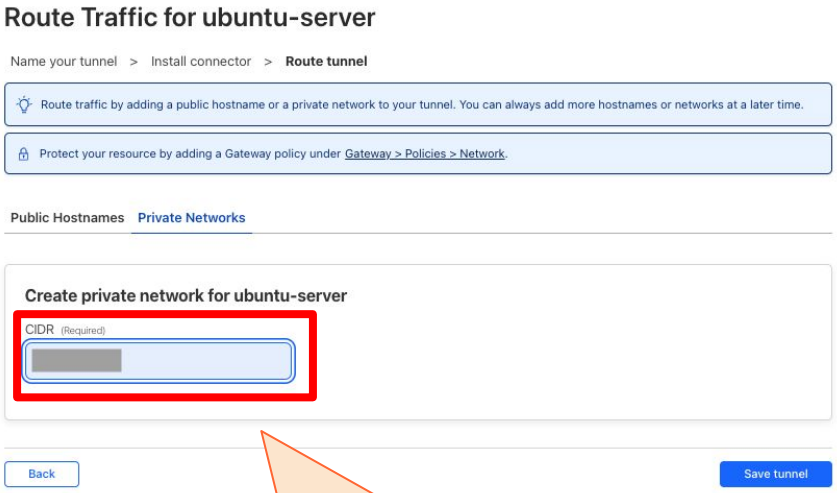
Tunnel設定 - ルーティング設定 (Public Hostnames)





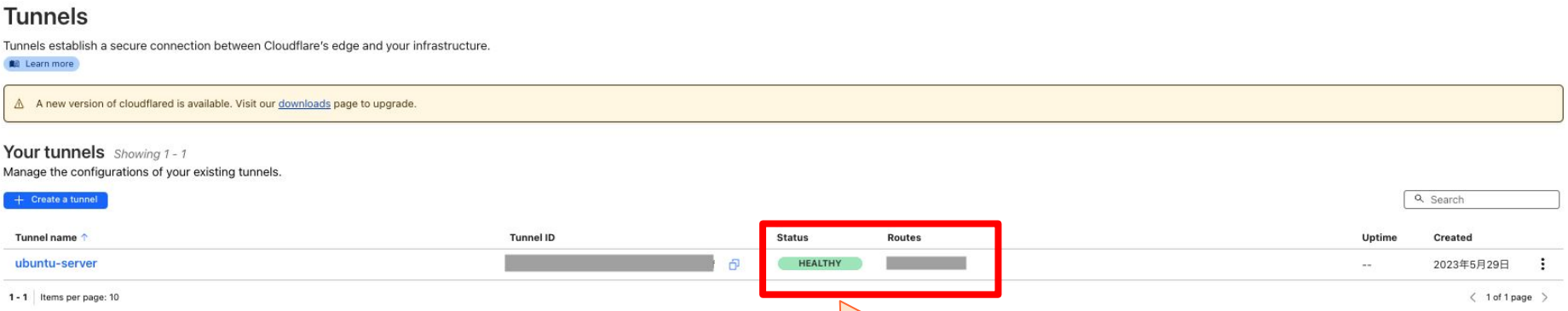
サーバー接続を実現したいホスト名を設定

Tunnel設定 - ルーティング設定 (Private Networks)



サーバー接続を実現したい対象のPrivate IPレンジを設定

Tunnel設定 - Save tunnelボタンをクリック



正しく設定できた場合には、Statusとして”Healthy"、Routesに前段で設定した内容が表示されます。

Tunnel設定 - Save tunnelボタンをクリック

Tunnel設定 - 必要なFirewall設定およびcloudflaredの前提条件

cloudflaredをご利用される際には、以下ドキュメントで指定されたポートに対するFirewall設定（穴あけ）が必要となります。
また、cloudflaredご利用にあたっての前提を含め、以下ご参照ください。

Cloudflare Docs - Tunnel with firewall
https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/deploy-tunnels/tunnel-with-firewall/

Cloudflare Docs - System Requirement
https://developers.cloudflare.com/cloudflare-one/connections/connect-networks/deploy-tunnels/system-requirements/

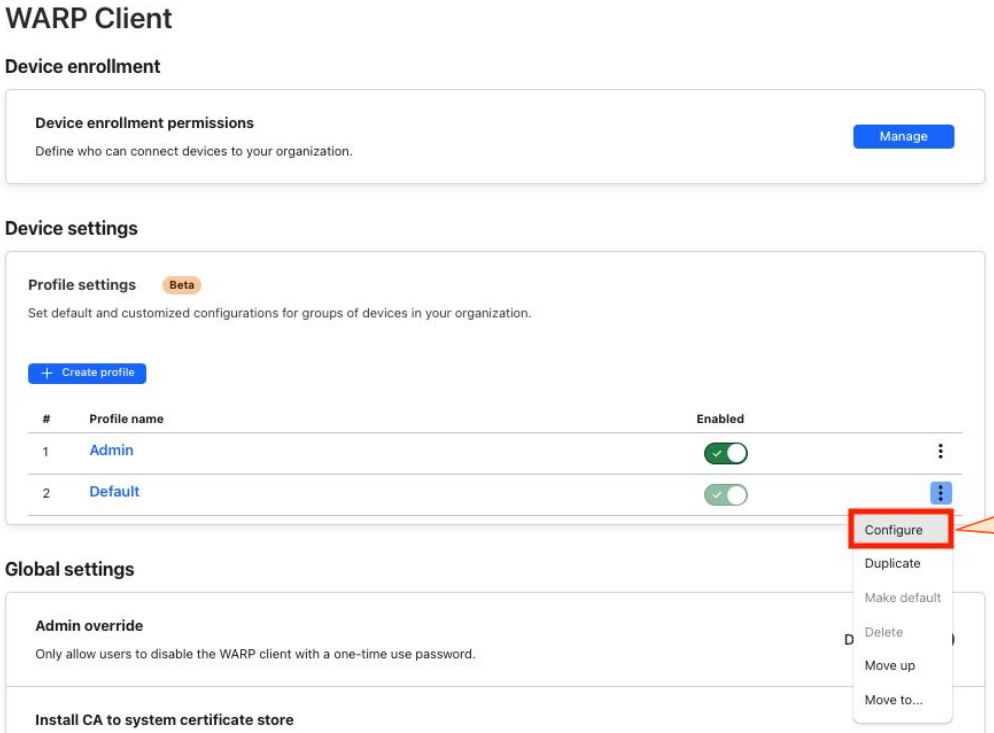
CLOUDFLARE

Tunnel設定 - 追加設定 (Public Hostnames経由での接続：SSH, RDP, SMB)

SSH, RDP, SMBといったプロトコル経由でのサーバーアクセスを利用したい場合には以下追加設定が必要となります。

1. Cloudflaredのインストール
2. 接続対象サーバーごとの追加設定 (SSH, RDP, SMB)
3. Self-hostedアプリケーションの登録 (推奨)※次セクション参照

Tunnel設定 - 追加設定 (Private Network経由での接続：Split Tunnelsからの除外)



Private Network経由で接続させる場合には、WARPクライアントに対して、対象のプライベートIPをSplit Tunnelsの設定に含める必要があります

IP指定でのアクセスを許諾したいユーザーに割り当てられているProfileのConfigureメニューをクリック

Tunnel設定 - 追加設定 (Private Network経由での接続：Split Tunnelsからの除外)

以下は192.168.0.0/16を削除した例

Your Split Tunnel entries (exclude) *Showing 1-14 of 14*

View and manage the IPs and domains Cloudflare Zero Trust excludes.

Restore default entries

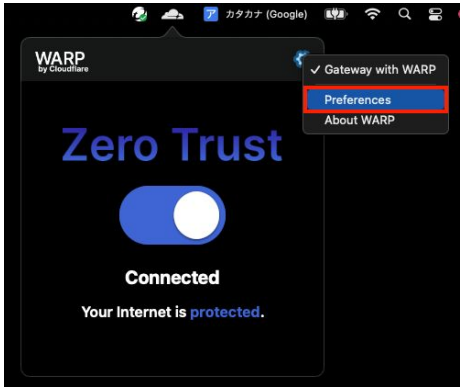
Type	Value	Description
address	10.0.0.0/8	-
address	100.64.0.0/10	-
address	169.254.0.0/16	DHCP Unspecified
address	172.16.0.0/12	-
address	224.0.0.0/24	-
address	240.0.0.0/4	-
address	255.255.255.255/32	DHCP Broadcast
address	fe80::/10	IPv6 Link Local
address	fd00::/8	-
address	ff01::/16	-
address	ff02::/16	-
address	ff03::/16	-
address	ff04::/16	-
address	ff05::/16	-

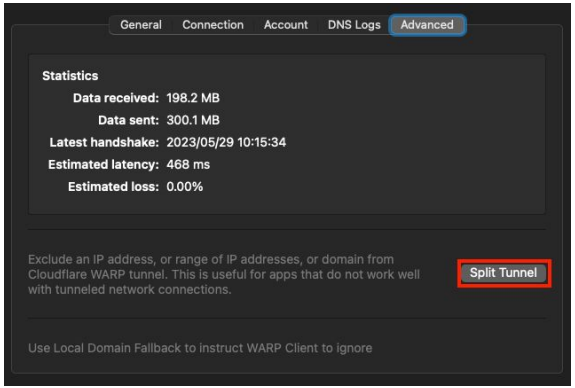
1 - 14 of 14 items | Items per page: 30

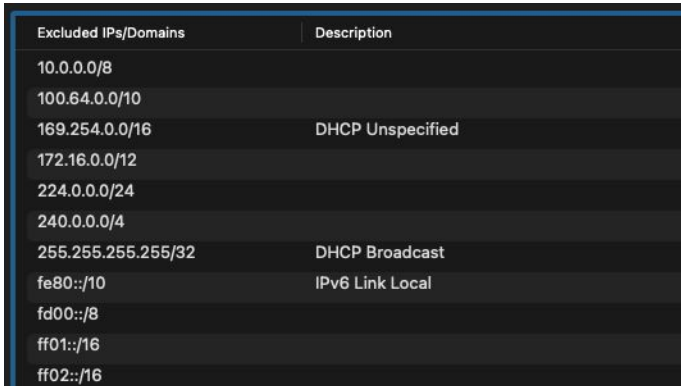
1 of 1 page

Tunnel設定 - 追加設定 (Private Network経由での接続：Split Tunnelsからの除外)

各WARPクライアントに適用されているSplit Tunnelsは、WARPクライアントで以下操作からご確認いただけます。







Tunnel設定 - Tunnelログの取得

Cloudflare Tunnelに関する調査には、Tunnel Logの取得・共有が期待されます。
cloudflaredのインストール先OSによって詳細手順は変わってきますが大きくは以下の流れで取得いただくことになります。

1) cloudflaredの起動オプションを変更の上、再起動 (--loglevel debugを追加)
2) Cloudflareのダッシュボードもしくは、cloudflaredがインストールされている端末からログを参照

参考：Cloudflare Docs - Tunnel Log

CLOUDFLARE

Tunnel設定 - Tunnelログの取得

＜cloudflaredのインストール先が Linux (Ubuntu Server)の場合の Tunnel再起動＞

1)　cloudflaredの起動スクリプトパスを確認
$ systemctl status cloudflared.service

2)　cloudflared起動スクリプトの編集 (--loglevel debugを追記)
$ vi /etc/systemd/system/cloudflared.service

3)　スクリプトファイルのリスタート
$ systemctl restart cloudflared.service

参考：Cloudflare Docs - Tunnel Log

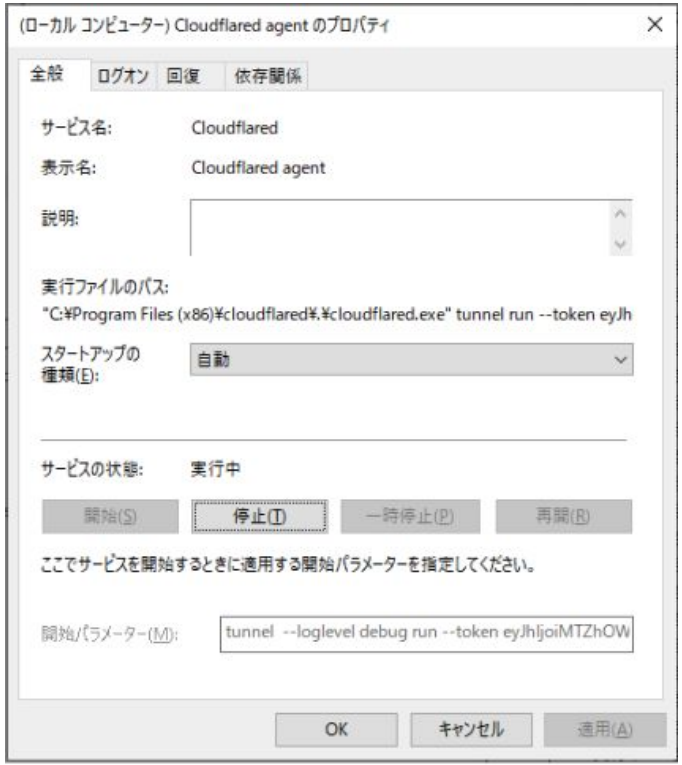
Tunnel設定 - Tunnelログの取得

＜cloudflaredのインストール先がWindowsの場合のTunnel再起動＞

1) サービス管理画面を起動
2) Cloudflaredのサービスをダブルクリック
3) 「実行ファイルのパス」で実行コマンドを除外した、オプション部分をコピーの上、「開始パラメータ」にペーストし、「開始パラメータ」に--loglevel debugを追記
4) 現在動作しているCloudflaredを停止の上、「開始」ボタンをクリック

※今回設定した「開始パラメータ」は永続保存されないため、次回PCを再起動した際には元々の設定に戻る。

参考：Cloudflare Docs - Tunnel Log



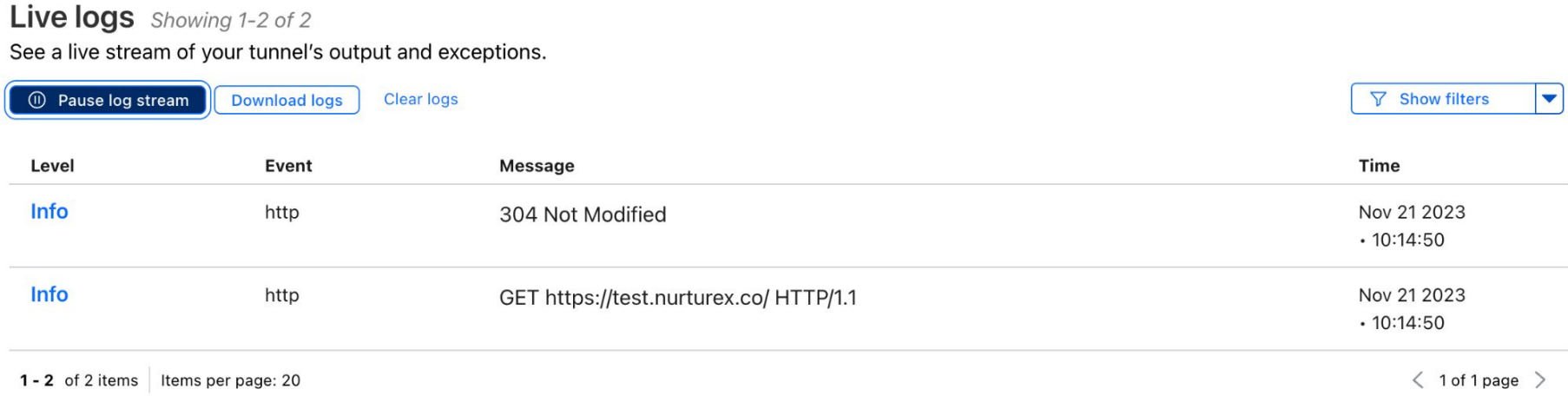
Tunnel設定 - Tunnelログの取得

＜ダッシュボードからのログ参照＞

ご利用のCloudflaredが2023.5.1以上の場合には、以下手順によりダッシュボードからTunnelログをご参照いただけます。

1. Tunnels一覧 (Access > Tunnels)へアクセスし、ログを参照したいTunnel名をクリック
2. ログを参照したいConnectorをクリック (Replica設定をしていない場合には一つのコネクタのみが表示)
3. “Begin Logstream”ボタンをクリックの後、トンネル経由での通信を試行することで、ログが出力
4. 操作終了後、”Pause Logstream”ボタンをクリックし、ログを確認

Tunnel設定 - Tunnelログの取得



Tunnel設定 - Tunnelログの取得

＜cloudflaredがインストールされた端末からの Tunnelログ取得＞

1) cloudflaredでログイン認証
以下コマンドを実行いただくと、ブラウザが自動的に起動し、登録されているIdPを用いた認証が行われます。

$ cloudflared tunnel login

認証が正常に終了すると、ブラウザ上にSuccessの表示が行われコンソールにプロンプトが帰ってきます。

参考：Cloudflare Docs - Tunnel Log

Tunnel設定 - Tunnelログの取得

2) ログ取得

以下コマンドで、ログが標準出力（コンソール出力）されます。ファイルへのリダイレクトをご希望の場合には以下の2つ目のコマンドを実行いただくと、"tunnel_log.txt"にログ情報が出力されます。

$ cloudflared tail <UUID>

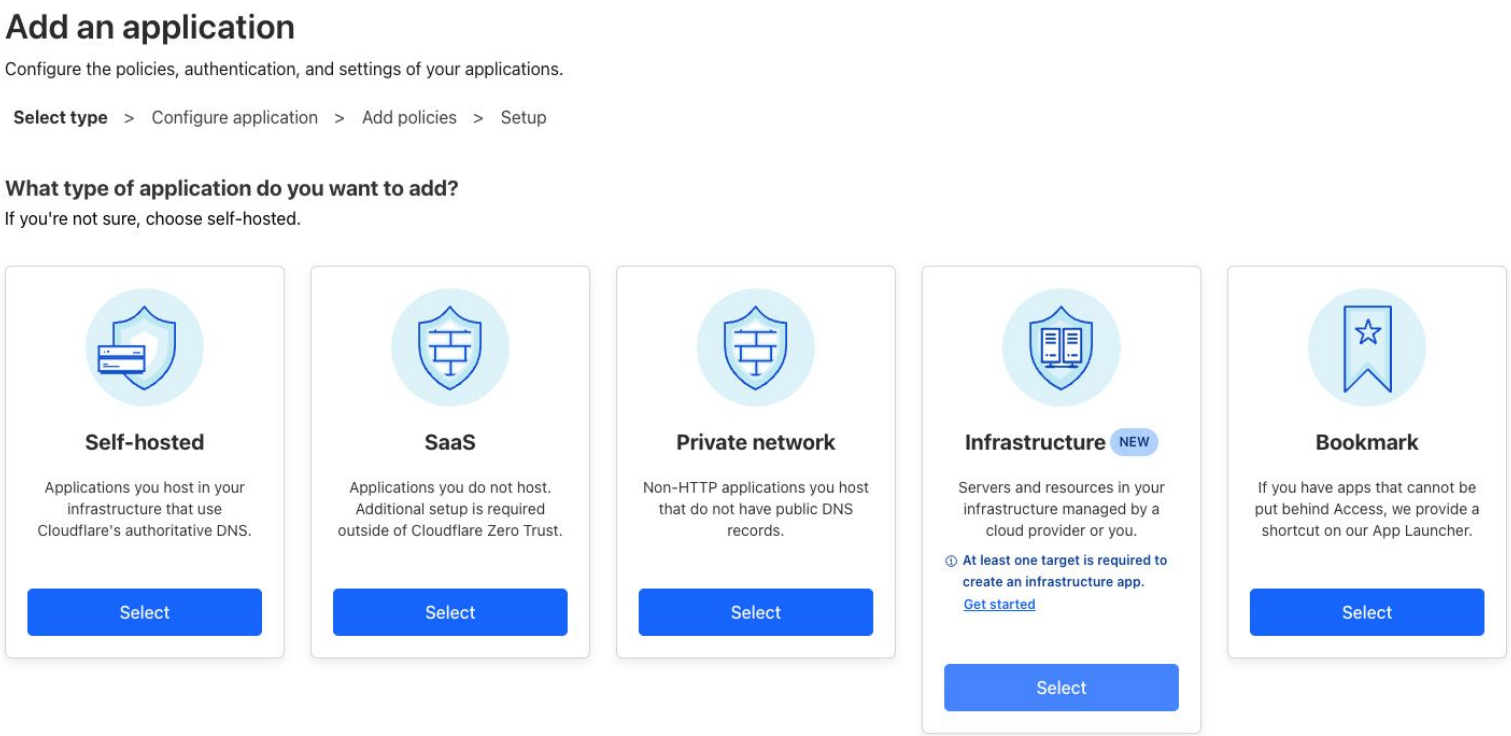
(ログをファイル出力したい場合)
$ cloudflared tail <UUID> > tunnel_log.txt

※tunnel_log.txtは任意のファイル名に変更いただくことも可能です

ZTNAの設定

1. サイトの登録 (オプショナル)
2. Tunnel設定
3. **アプリケーションの登録**

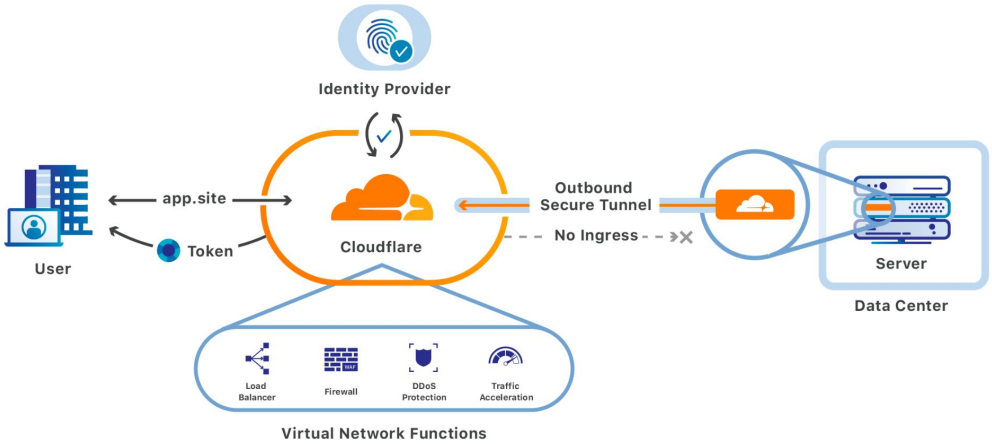
アプリケーションの登録

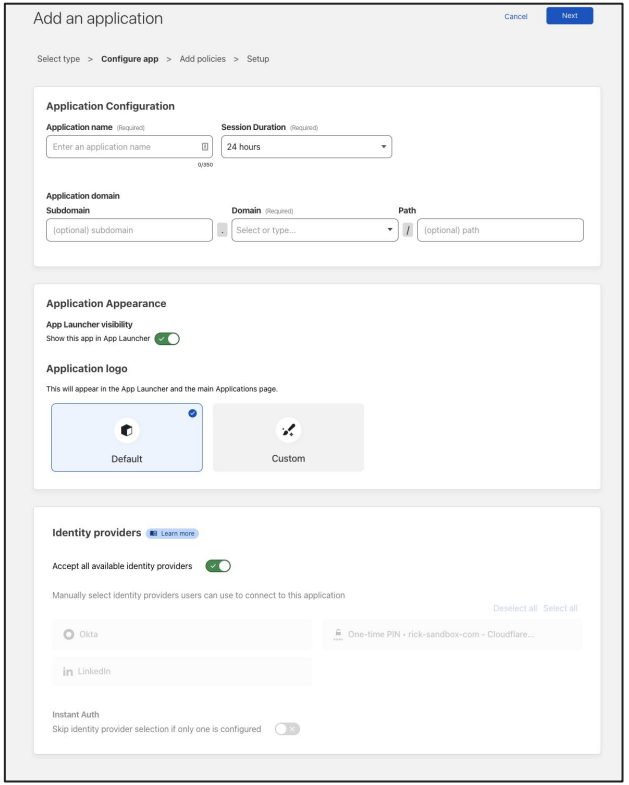


アプリケーションの登録

タイプ	対象	条件
Self-hosted	オンプレ環境で稼働する社内アプリケーション (Cloudflare DNSを利用)	● Cloudflare DNS ● (Cloudflare Tunnel)
SaaS	インターネットで公開されているアプリケーション (SAML連携アプリ)	● Cloudflare AccessとのSSO連携
Private network	インターネットからアクセスできないプライベートネットワークで稼働するアプリケーション(パブリックなDNSレコードの登録なし)	● Cloudflare Tunnel
Bookmark	Cloudflare Accessと連携されていないものの、App Launcherの登録対象としたいアプリケーション	-

アプリケーションの登録 - Self-hosted





参照) [Cloudflare Docs - Add a self-hosted application]

CLOUDFLARE

アプリケーションの登録 - Self-hosted

1. Accessへのアプリケーション登録
   a. Zero Trustダッシュボードから、Access > Applicationsへアクセス
   b. “Add an application”を選択
   c. “Self-hosted”を選択
   d. “Application Name”を設定
   e. “Application Domain”を設定
2. Access Policyの設定
3. Authenticationの設定

参照) Cloudflare Docs - Add a SaaS application to Access

アプリケーションの登録 - Self-hosted

Test

Overview | Policies | Authentication | Settings

Application Configuration

Application name (Required)
Test
4/350

Session Duration (Required)
24 hours

Application domain

Subdomain
test

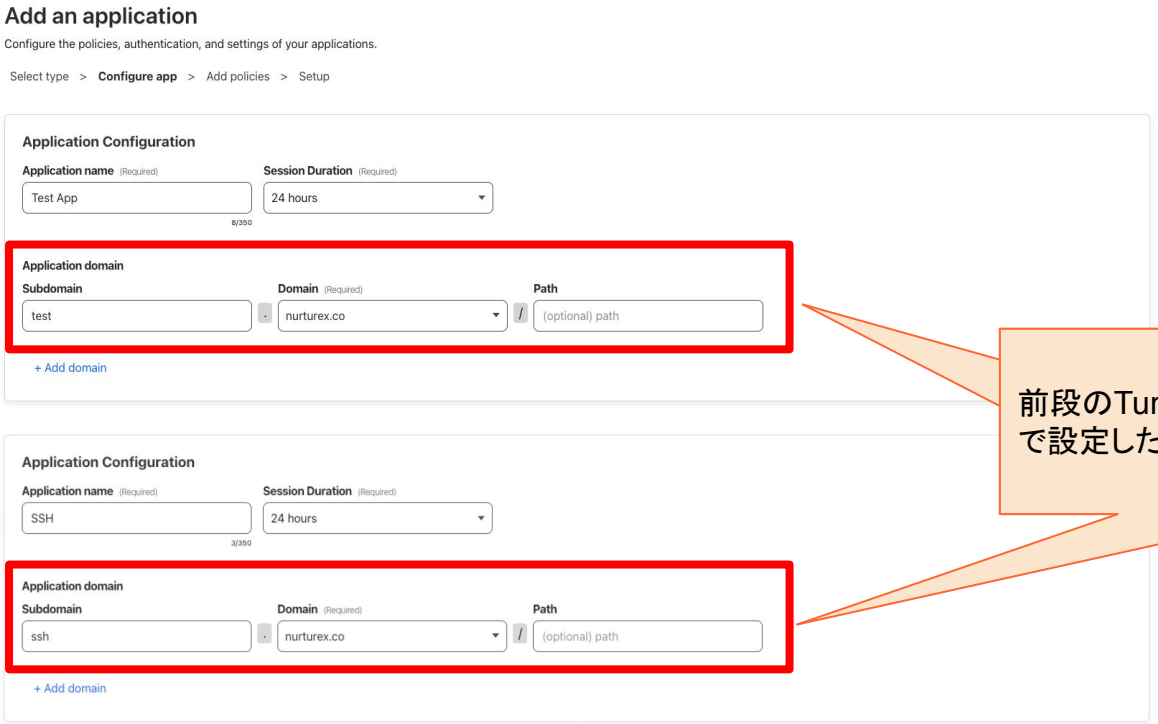
Domain (Required)
nurturex.co

Path
(optional) path

Application Audience (AUD) Tag
[redacted] Copy

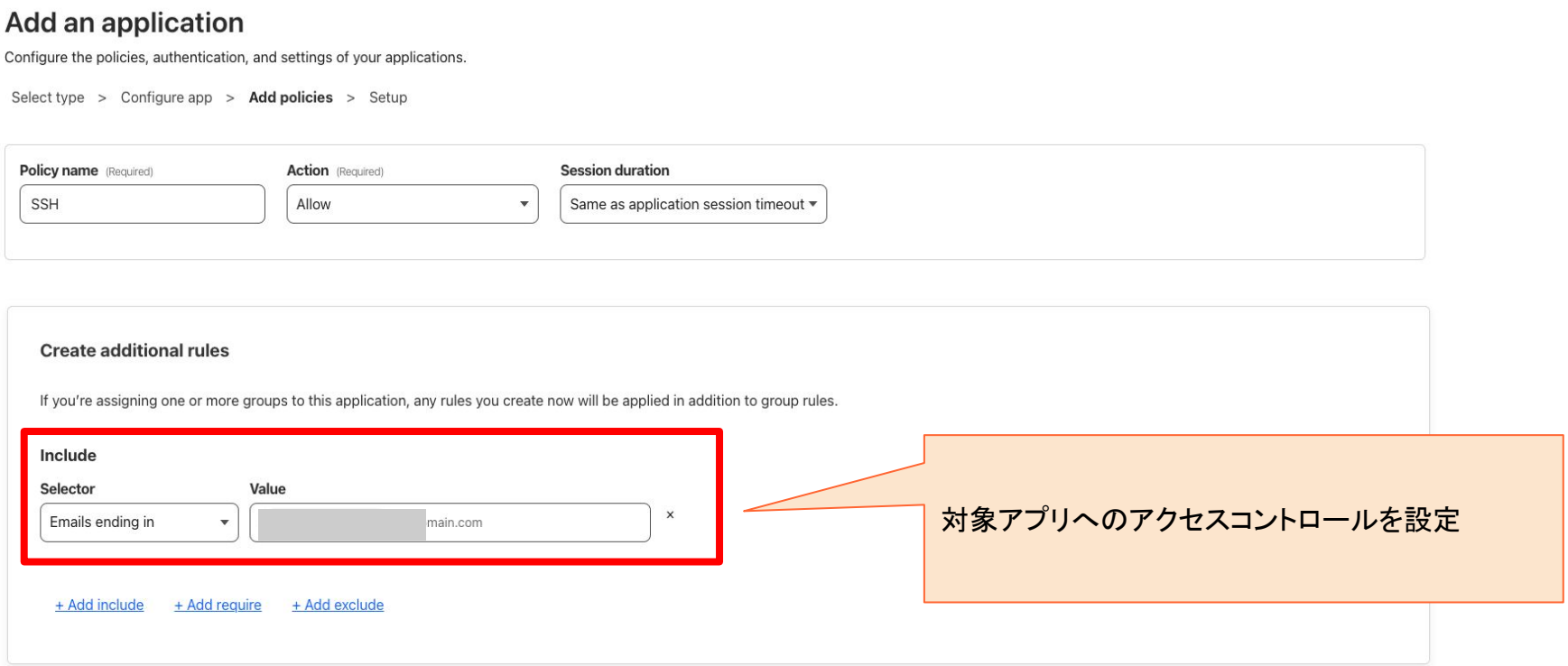
Revoke existing tokens

アプリケーションの登録 - Self-hosted

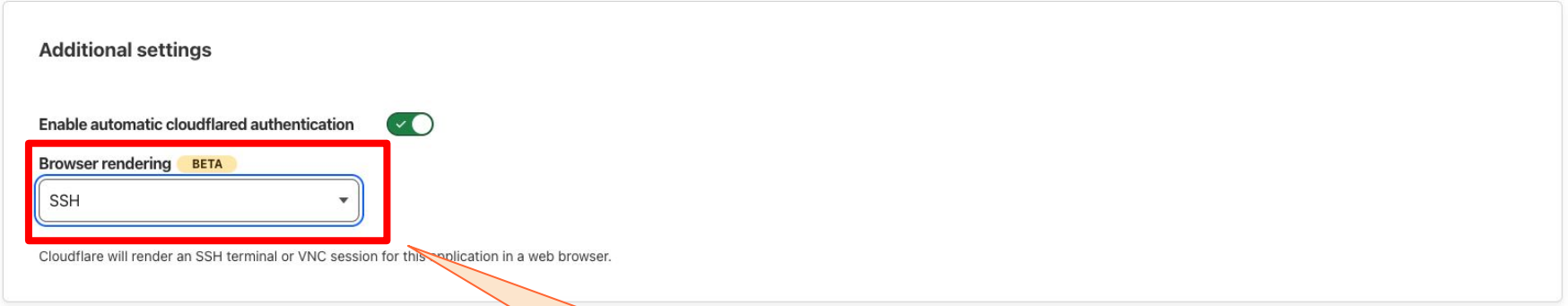


前段のTunnel作成で登録したPublic Hostnames で設定したホスト名を指定

アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)



アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)

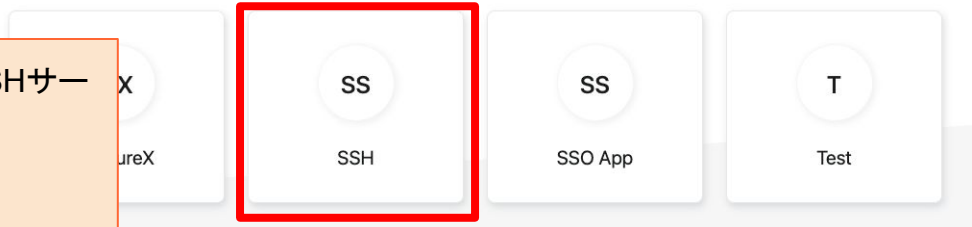


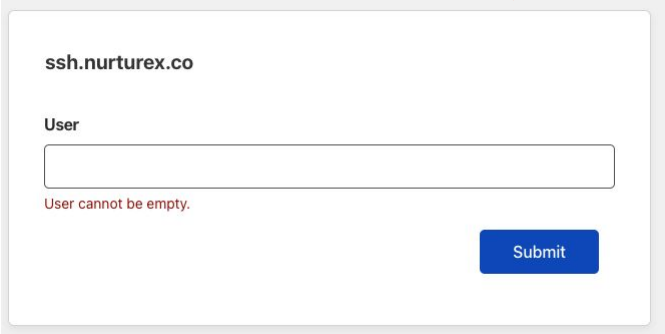
こちらを設定することでブラウザ経由でSSH接続が可能となります

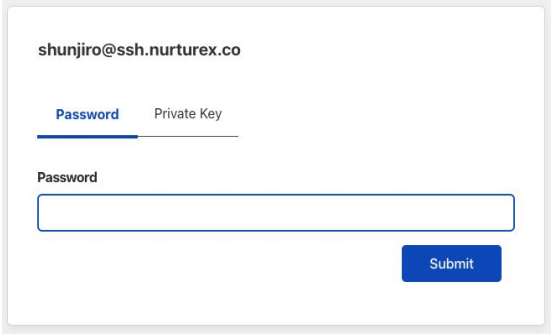
アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)

前段の設定から、ブラウザ経由でSSHサーバーへのアクセスが可能となります

※コンソールからもアクセス可能
$ ssh <ユーザー名> @ <ホスト名>







CLOUDFLARE

アプリケーションの登録 - Self-hosted (SSHサーバーへのアクセス)

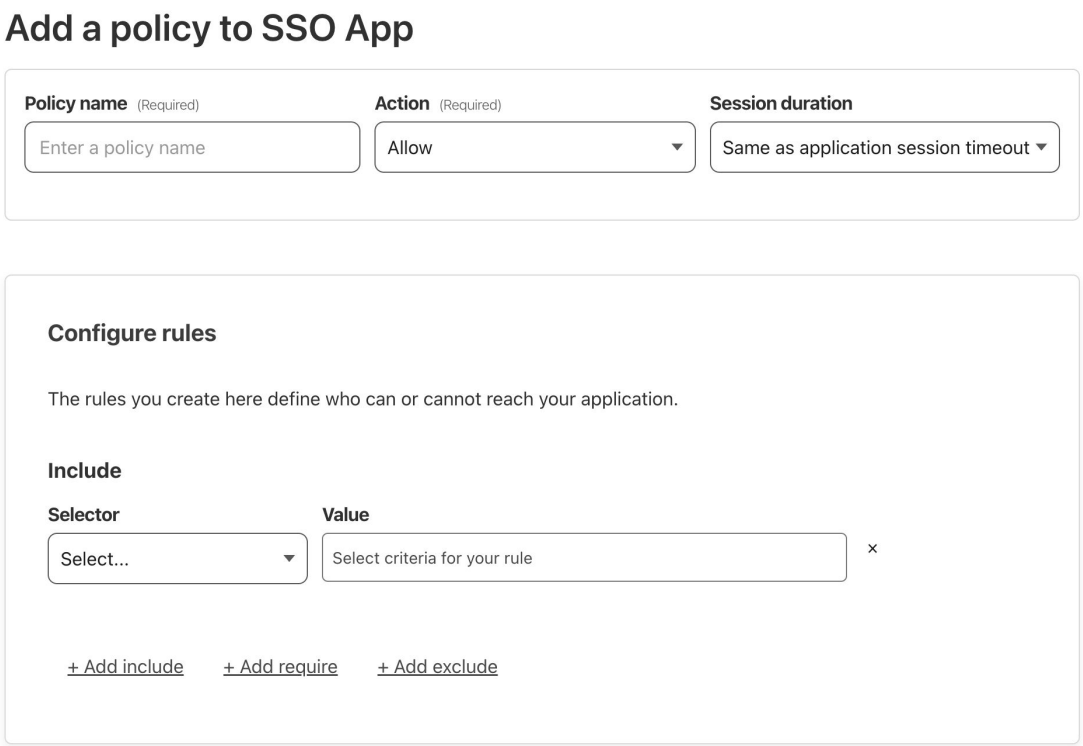
```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

31のアップデートはすぐに適用されます。
これらの追加アップデートを確認するには次を実行してください: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


14 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Last login: Mon Jun  5 09:55:25 2023 from 127.0.0.1
shunjiro@ubuntu-server:~$
```

アプリケーションの登録 - SaaS

1. Accessへのアプリケーション登録
   a. Zero Trustダッシュボードから、Access > Applicationsへアクセス
   b. “Add an application”を選択
   c. “SaaS”を選択
   d. “Entity ID”および”Assertion Consumer Service URL”を設定
   e. “Name ID Format”を選択 (“Unique ID”もしくは”Email”)
   f. “SAML attribute statements (optional)”を設定
2. Access Policyの設定
3. Authenticationの設定

参照) Cloudflare Docs - Add a SaaS application to Access

アプリケーションの登録 - SaaS



アプリケーションの登録

Applications

Protect your Self-Hosted, SaaS and Private applications with Zero Trust policies. Only users who match your policies will have access to your configured applications. Learn more

Your applications *Showing 1-4 of 4*

Manage the policies, authentication, and settings of your configured applications.

Add an application

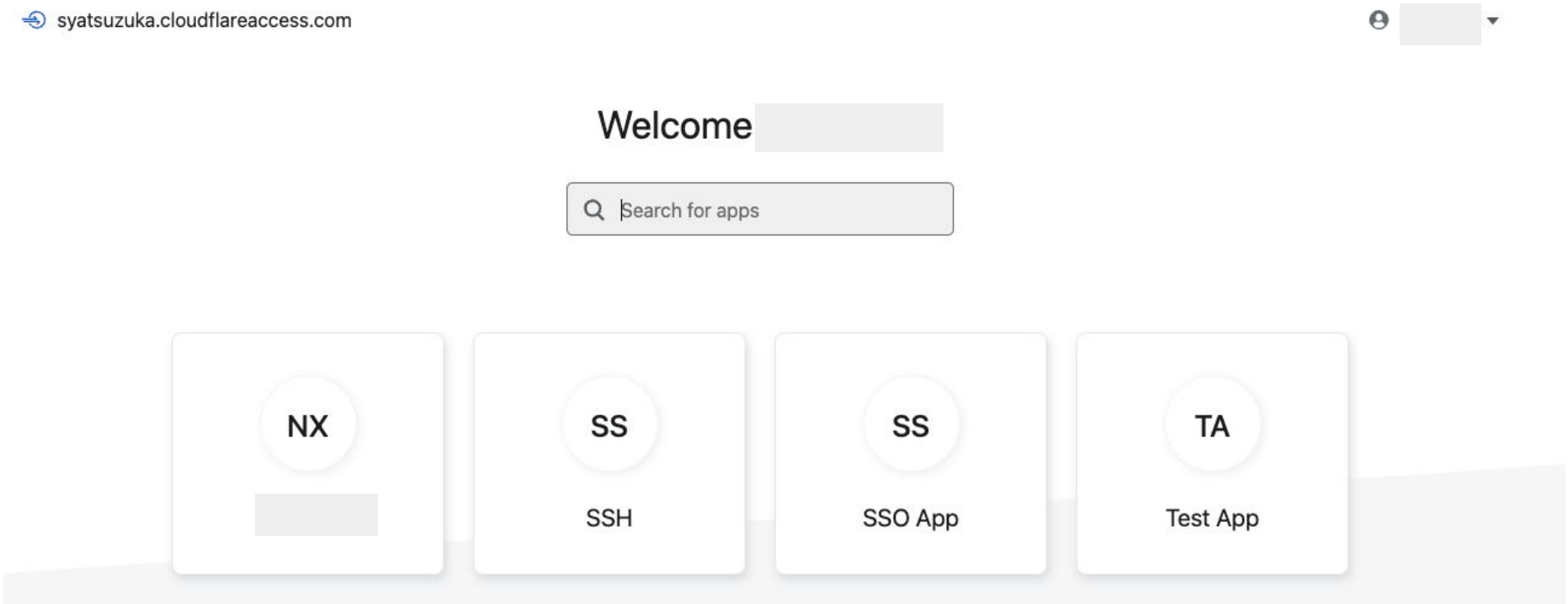
Search

Application name	Application URL	Total Domains	Policies assigned	Type
Test App	test.nurturex.co	1	1	SELF-HOSTED
SSH	ssh.nurturex.co	1	1	BROWSER SSH
NurtureX	https://www.nurturex.co	1	-	BOOKMARK
SSO App	dash.cloudflare.com	1	1	DASH_SSO

1 - 4 of 4 items | Items per page: 10

1 of 1 page

アプリケーションの登録



Cloudflare SWGの機能および設定

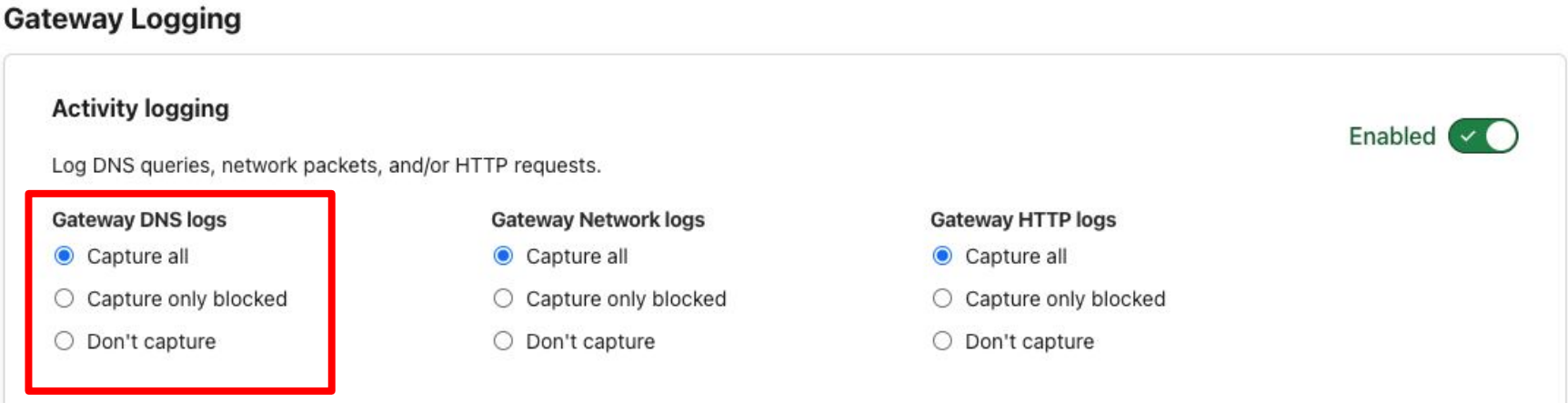
CLOUDFLARE

SWGの設定

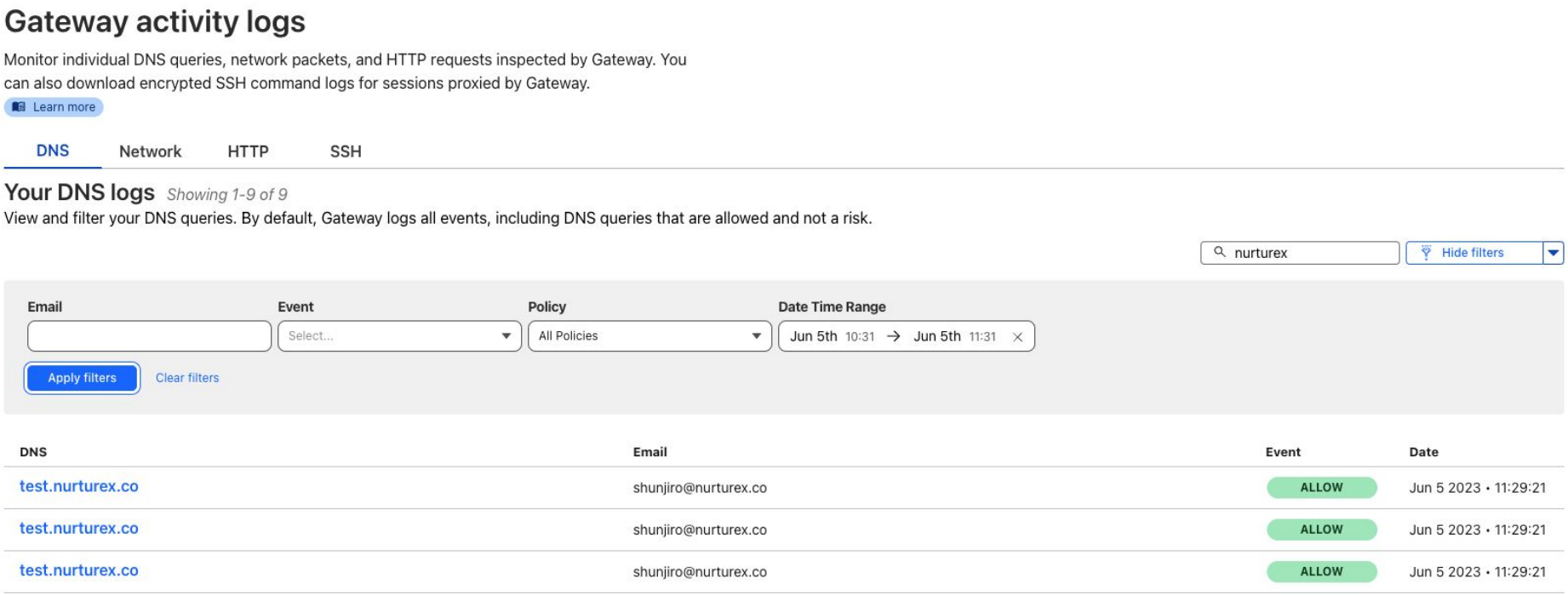
1. **Firewall Policyの設定**
2. Egress Policyの設定
3. Resolver Policyの設定
4. DNS Locationsの設定
5. Proxy Endpointの設定

DNSフィルタリングの設定

1. Zero Trustダッシュボードから、Settings > Networkをクリック
2. Gateway DNS logsに対して　activity loggingを有効化
3. ブラウザから任意のURLにアクセスし、DNSのログが取得されていることを確認する。

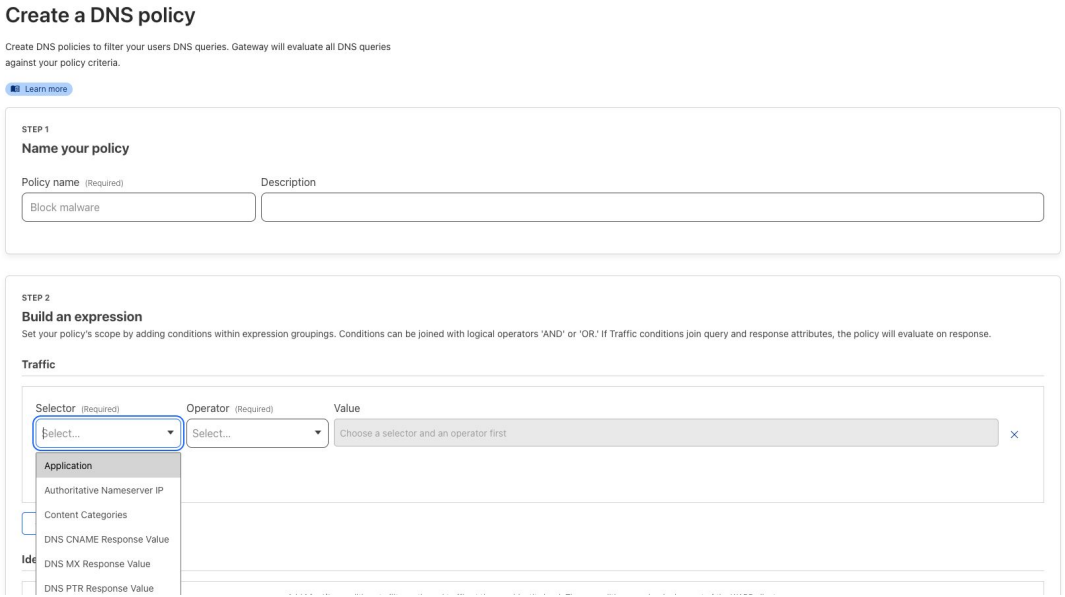


DNSフィルタリングの設定



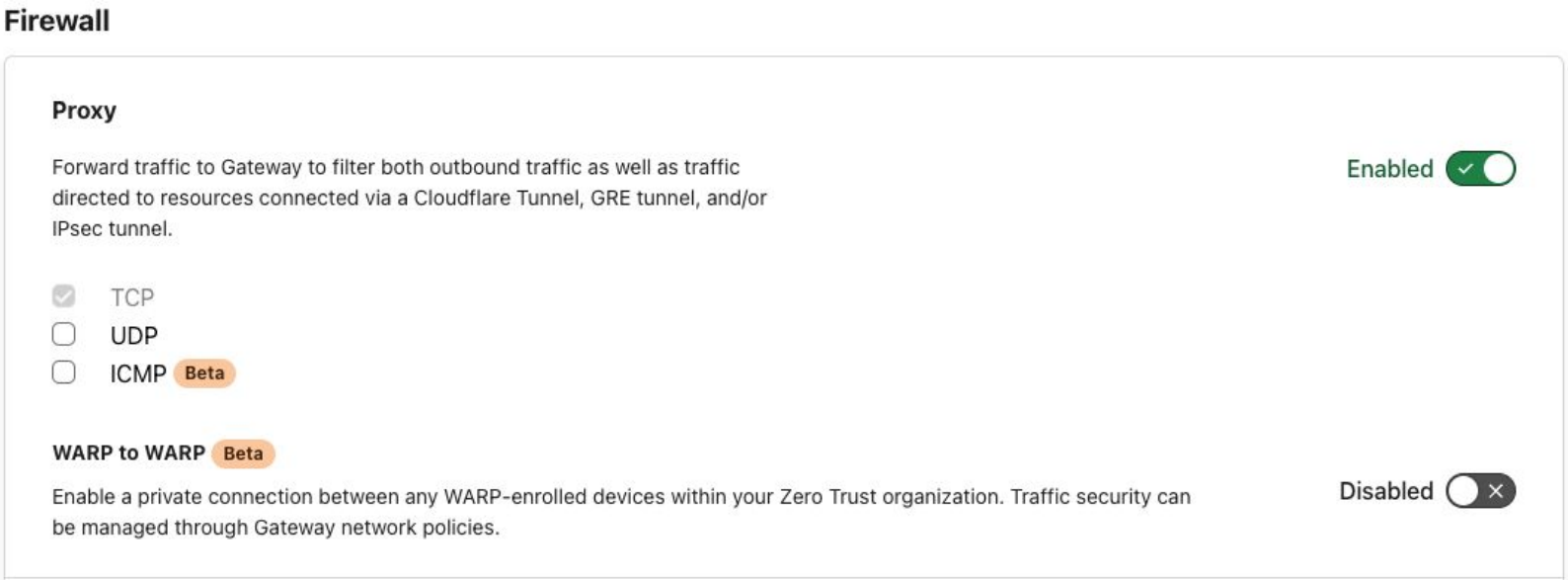
DNSフィルタリングの設定

4. 推奨ポリシーの設定
5. 個別ポリシーの設定 (オプション)



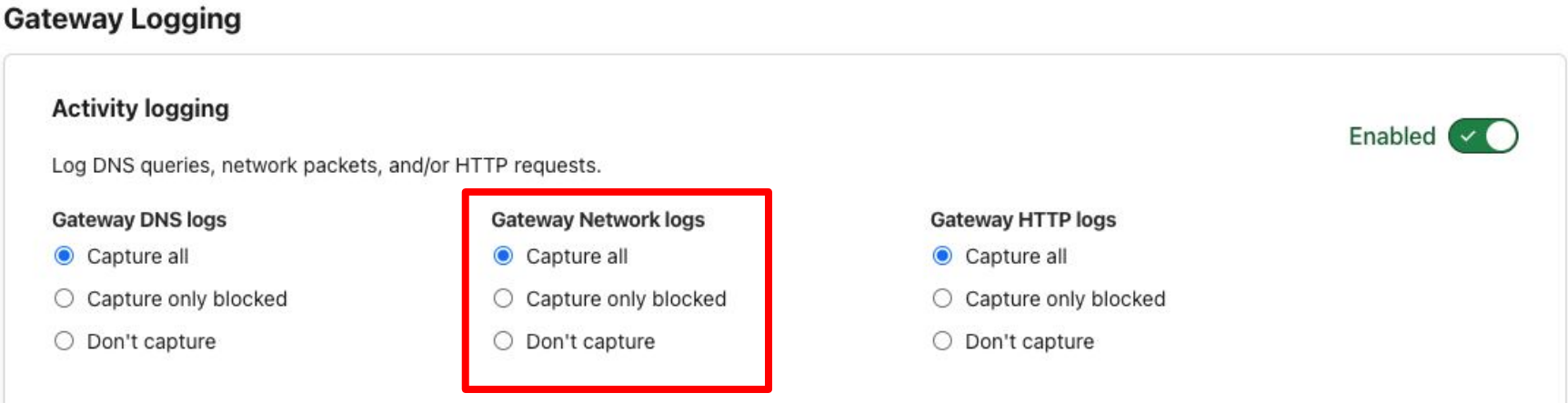
ネットワークフィルタリングの設定

1. Zero Trustダッシュボードから、Settings > Networkをクリック
2. TCPのProxyを有効化されていることを確認 (必要に応じてUDP, ICMPも有効化)



ネットワークフィルタリングの設定

3. Zero Trustダッシュボードから、Settings > Networkをクリック
4. Gateway Network logsに対して　activity loggingを有効化
5. ブラウザから任意のURLにアクセスし、Networkのログが取得されていることを確認する。



ネットワークフィルタリングの設定

Gateway activity logs

Monitor individual DNS queries, network packets, and HTTP requests inspected by Gateway. You can also download encrypted SSH command logs for sessions proxied by Gateway.

Learn more

DNS | Network | HTTP | SSH

Your network logs *Showing 1 - 50*

View and filter your network traffic. By default, Gateway logs all events, including those that are allowed and not a risk.

Search | Hide filters

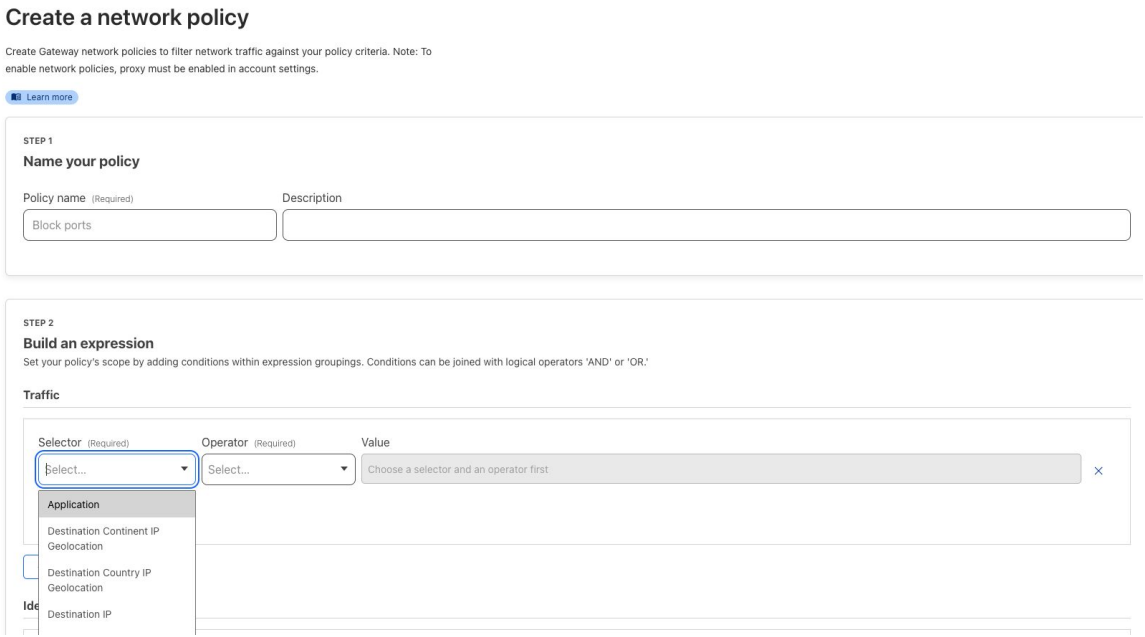
Email	Action	Policy	Virtual Network	Date Time Range
shunjiro@nurturex.co	All Actions	All Policies	All Networks	Jun 5th 13:18 → Jun 5th 14:18

Apply filters | Clear filters

Source IP	Destination IP	Action	Session ID	Time
60.87.88.128	2600:9000:2367:5c00:b:2c2f:2e80:93a1	ALLOW	192B84C89200...	Jun 5 2023 • 14:18:05
60.87.88.128	23.46.229.98	ALLOW	192B899F7A00...	Jun 5 2023 • 14:17:57
60.87.88.128	104.119.246.150	ALLOW	192B96A43200...	Jun 5 2023 • 14:17:55

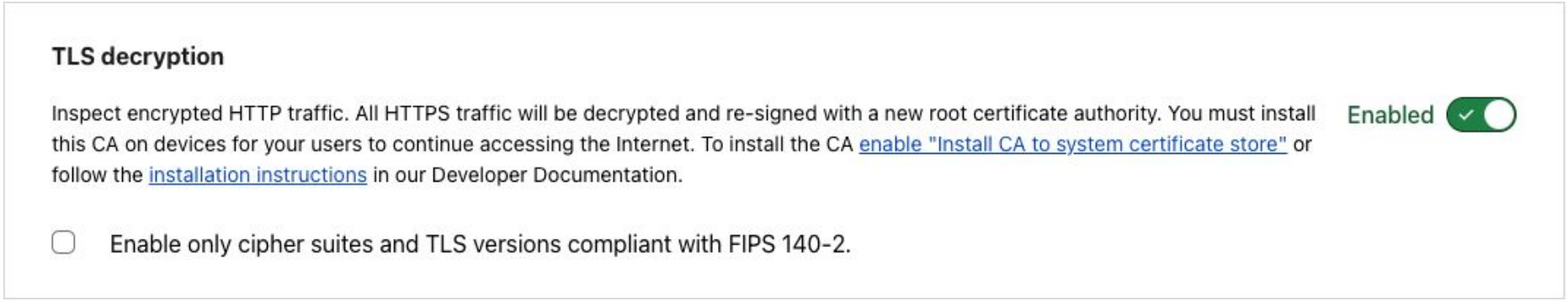
ネットワークフィルタリングの設定

4. 個別ポリシーの設定 (オプション)



HTTPフィルタリングの設定

1. Zero Trustダッシュボードから、Settings > Networkをクリック
2. TLS decriptionを有効化



HTTPフィルタリングの設定

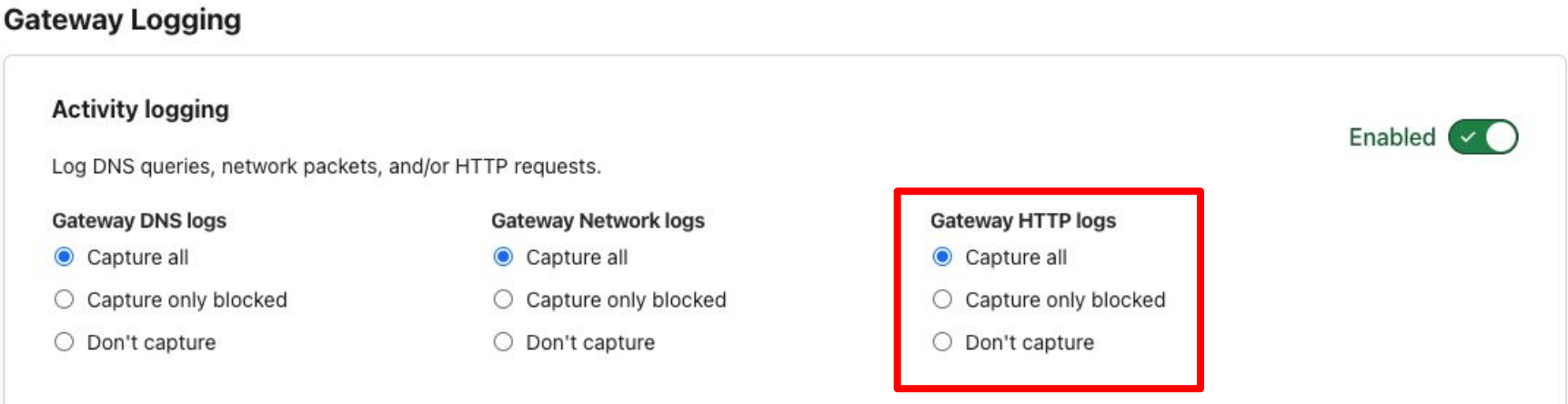
※以下で説明されている通り、TLS decryptionを指定された場合、いくつかのアプリケーションとの通信が阻害される可能性がございます。

その際には、1) untrusted certificate actionをPass throughに設定する、もしくは、2) Do not inspectをアクション指定したGatewayポリシーの作成が対応案としてあげられます。

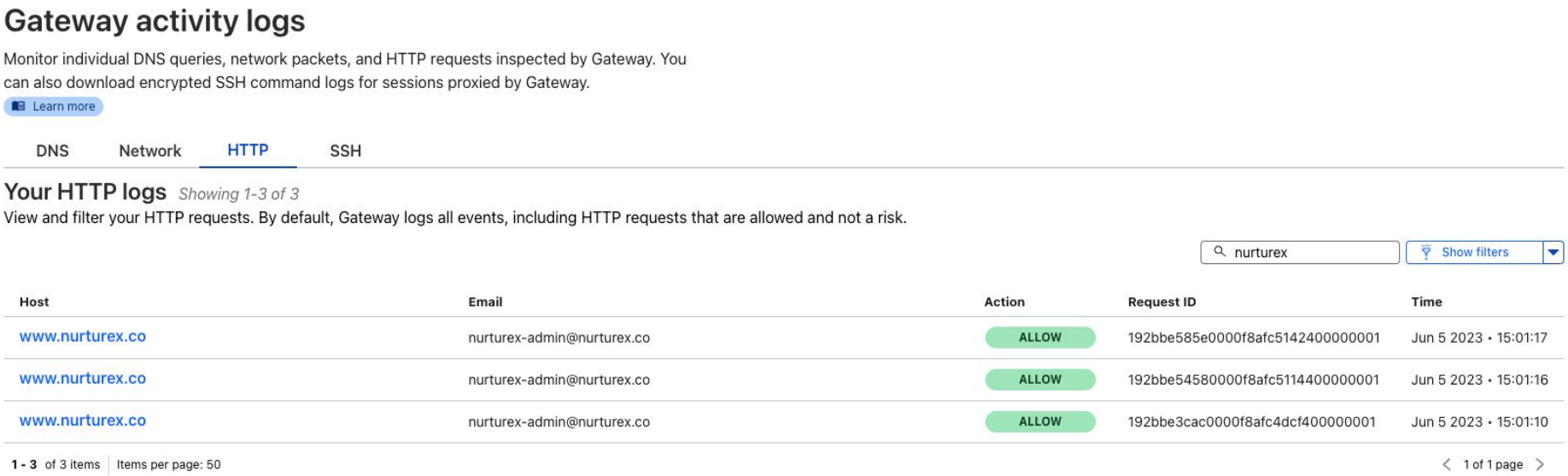
参照) Cloudflare Docs - TLS description
参照) Cloudflare Docs - Do not inspect applications

HTTPフィルタリングの設定

3. Gateway HTTP logsに対して　activity loggingを有効化
4. ブラウザから任意のURLにアクセスし、HTTPのログが取得されていることを確認する。

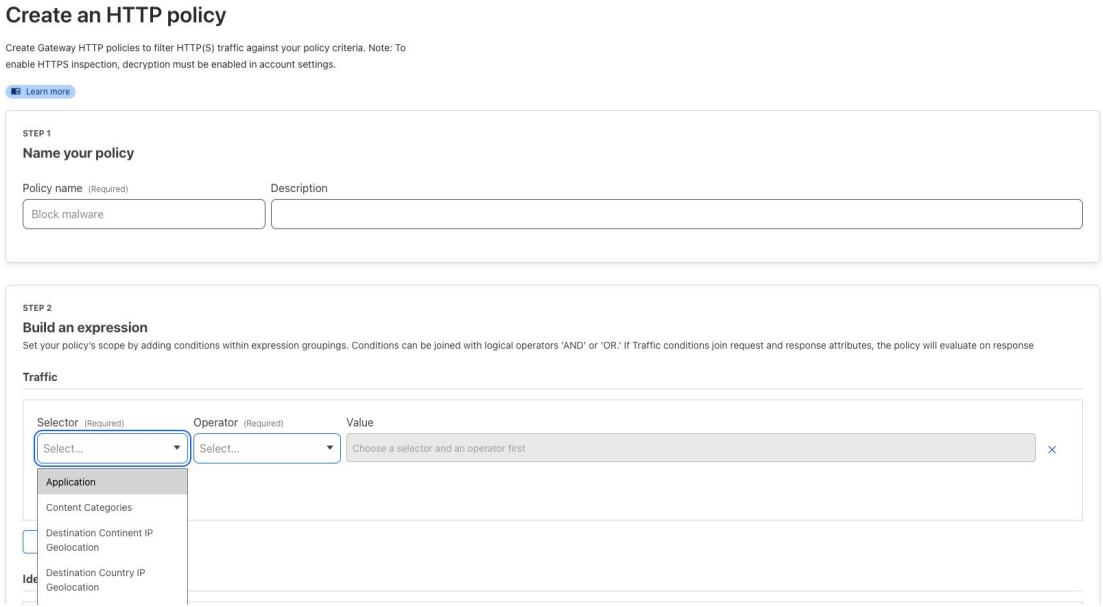


HTTPフィルタリングの設定



HTTPフィルタリングの設定

5. 推奨ポリシーの設定
6. 個別ポリシーの設定 (オプション)



CLOUDFLARE

SWGの設定

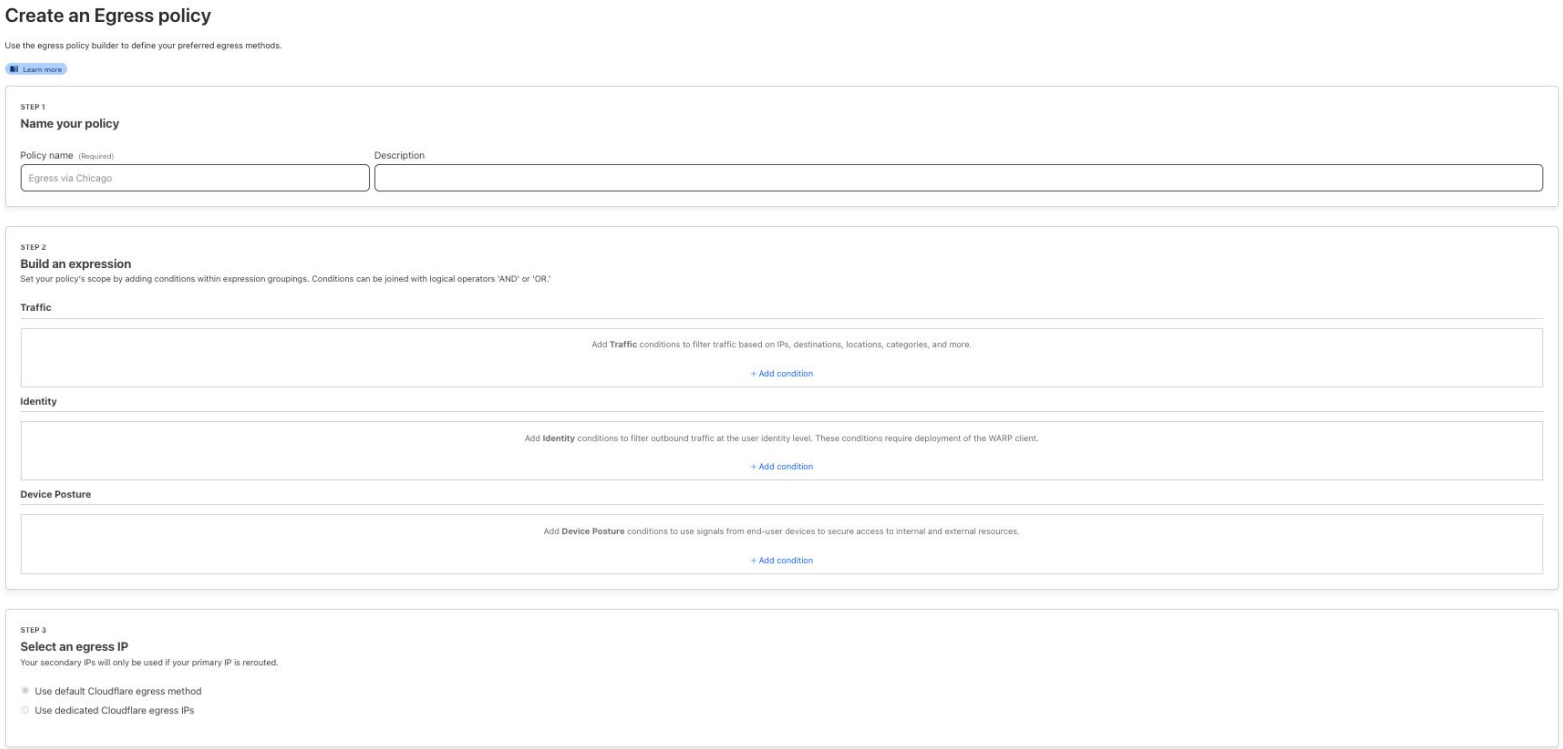
1. Firewall Policyの設定
2. **Egress Policyの設定**
3. Resolver Policyの設定
4. DNS Locationsの設定
5. Proxy Endpointの設定

Egress Policyの設定

Egress Policyを定義いただく場合には、"Dedicated Egress IP"をお買い求めいただく事が前提となります。
"Dedicated Egress IP"がお客様のご利用環境に割り当てられた後、Egress Policyを設定いただくことで、特定の通信に対して、指定のEgress IPから通信をアウトバウンドさせる事が可能となります。

参照) Cloudflare Docs - Egress policies

Egress Policyの設定



CLOUDFLARE

SWGの設定

1. Firewall Policyの設定
2. Egress Policyの設定
3. **Resolver Policyの設定**
4. DNS Locationsの設定
5. Proxy Endpointの設定

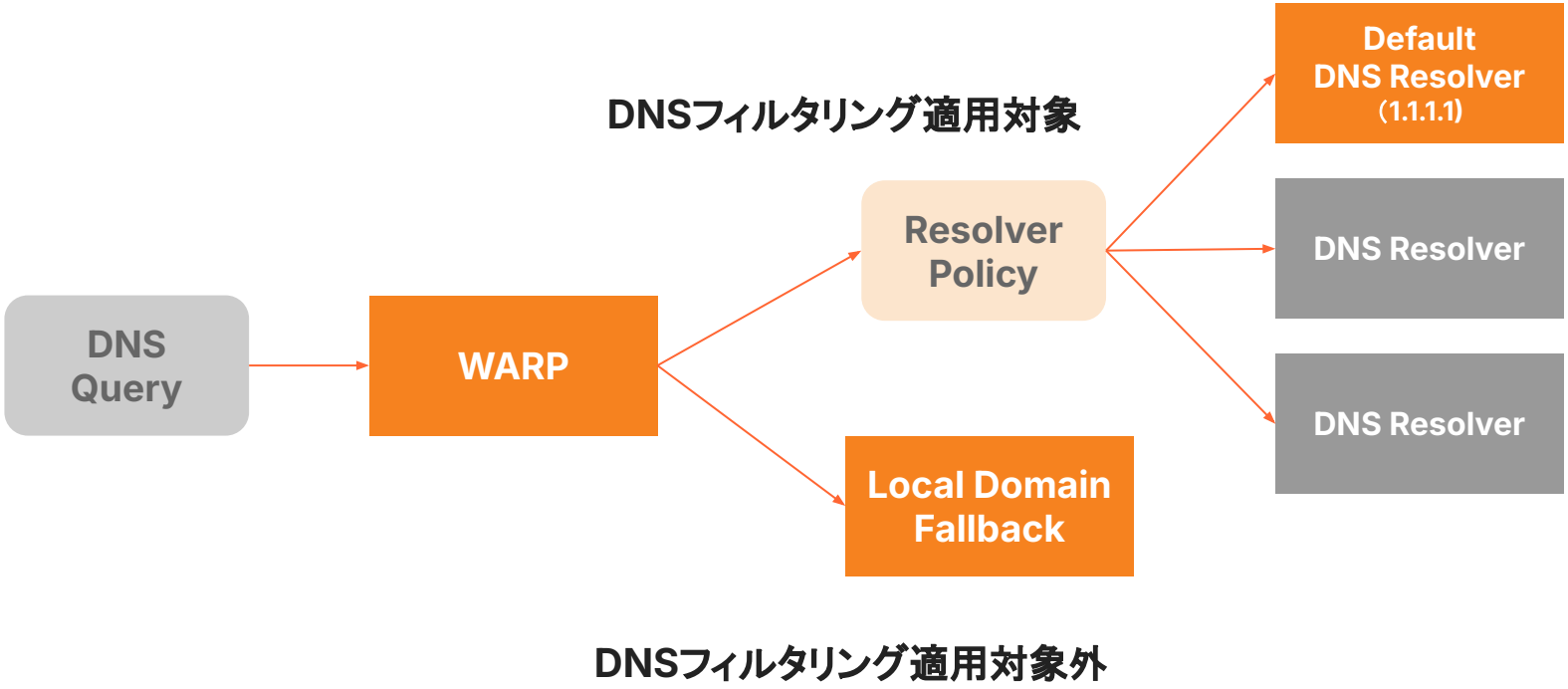
Resolver Policyの設定

Resolver Policyを定義いただくことで、通信ごとに適用させるDNS Resolverを切り替える事が可能となります。

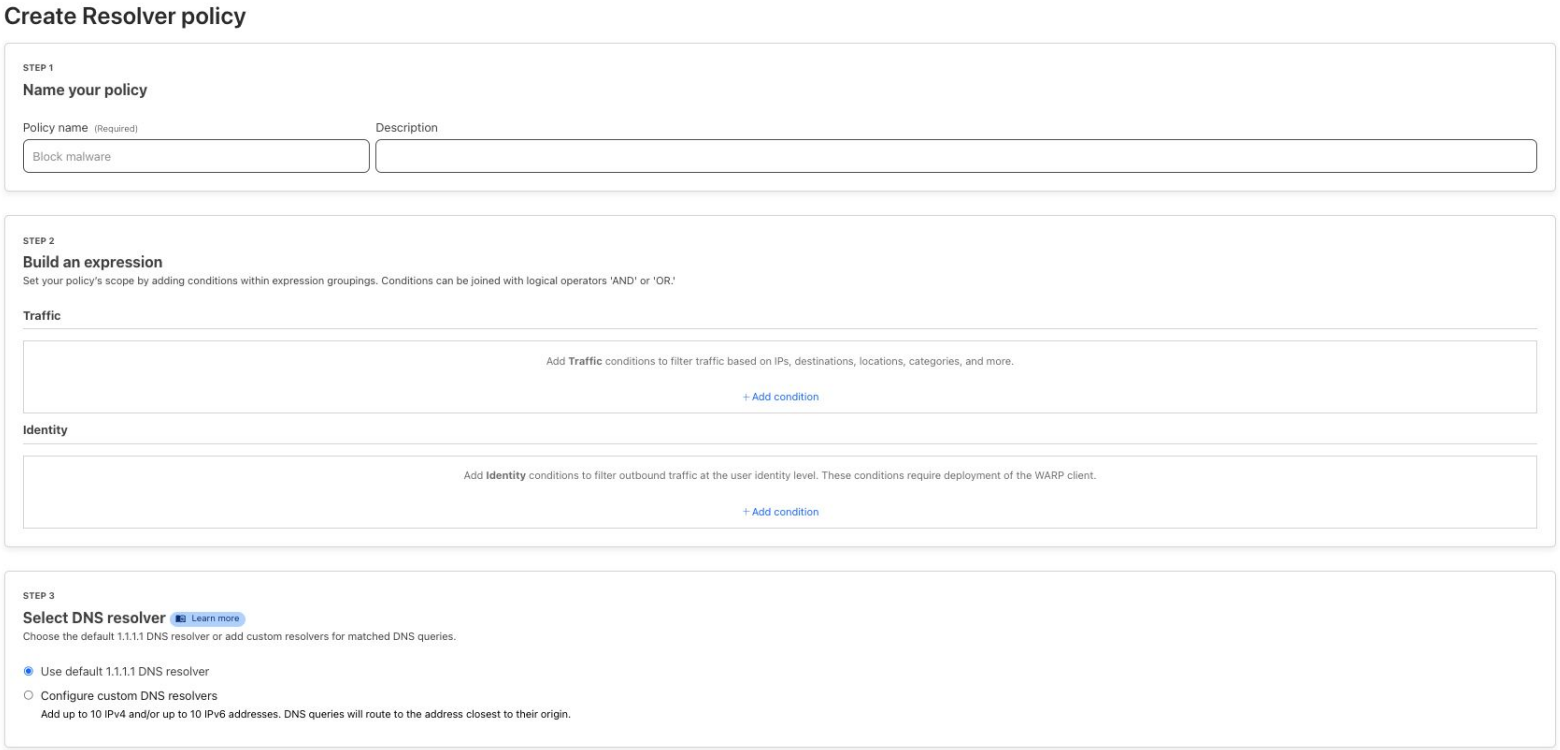
Resolver Policyがリリースされるまでは、Local Domain Fallbackを用いることで、所定のドメイン上のホストへのアクセスに対して、内部DNSによる名前解決を適用させる事が行われてきましたが、その場合にはClouflare Zero Trustで設定されたDNSフィルタリングが適用されない状態にあり、Resolver Policyをご利用いただくことで、名前解決に用いるレゾルバーを切り替えながら、DNSポリシーを適用させる事が可能となります。

参照) Cloudflare Docs - Resolver policies

Resolver Policyの設定



Resolver Policyの設定



CLOUDFLARE

SWGの設定

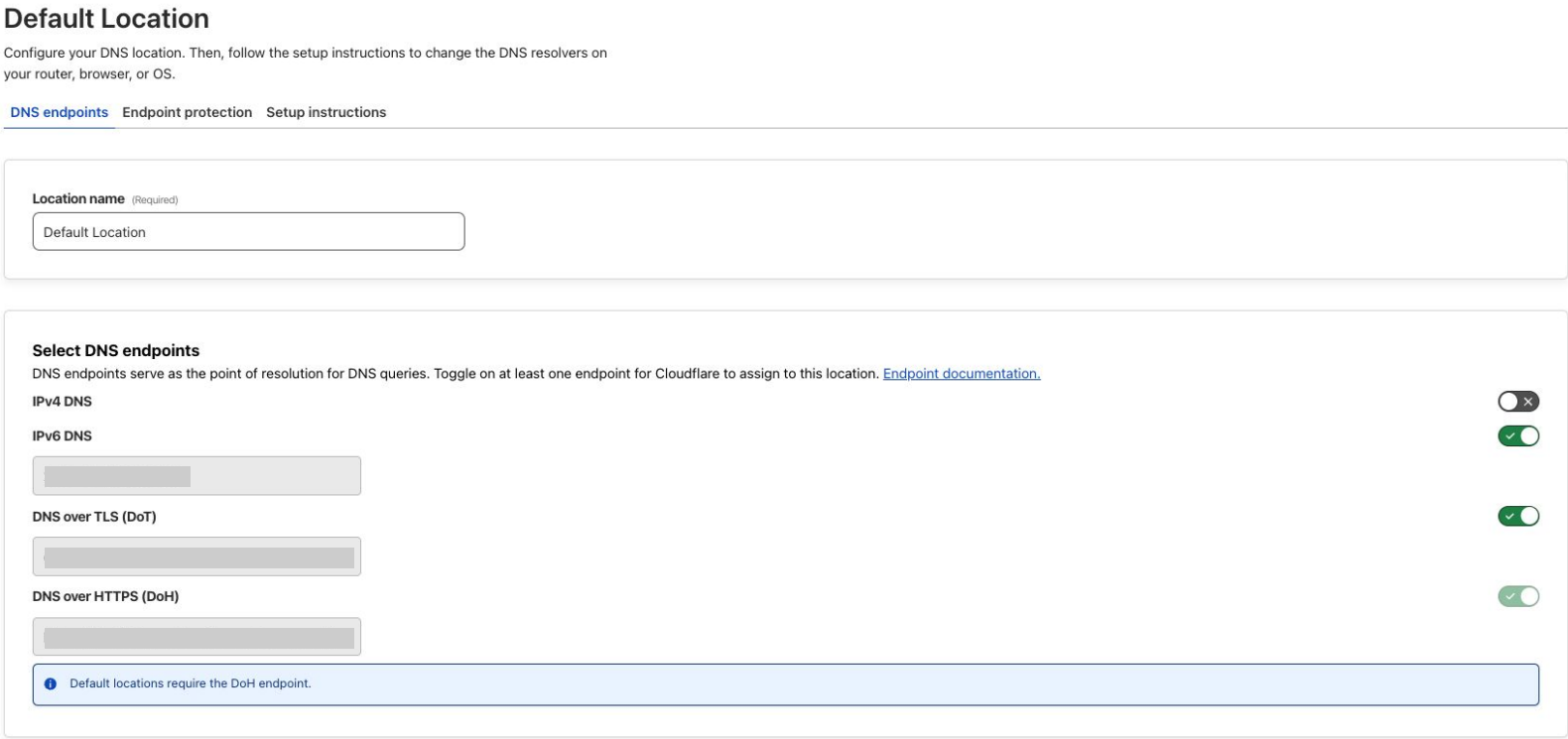
1. Firewall Policyの設定
2. Egress Policyの設定
3. Resolver Policyの設定
4. **DNS Locationsの設定**
5. Proxy Endpointの設定

DNS Locationsの設定

DNS Locationsを定義いただくことで、例としてWARPをインストールしない端末(agentless)のレゾルバーに、定義されたDNS Locationsのエンドポイントを指定いただくことで、ホスト名の名前解決処理にあたり、DNSフィルタリングを適用させる事が可能となります。

参照) Cloudflare Docs - Add locations

DNS Locationsの設定



CLOUDFLARE

SWGの設定

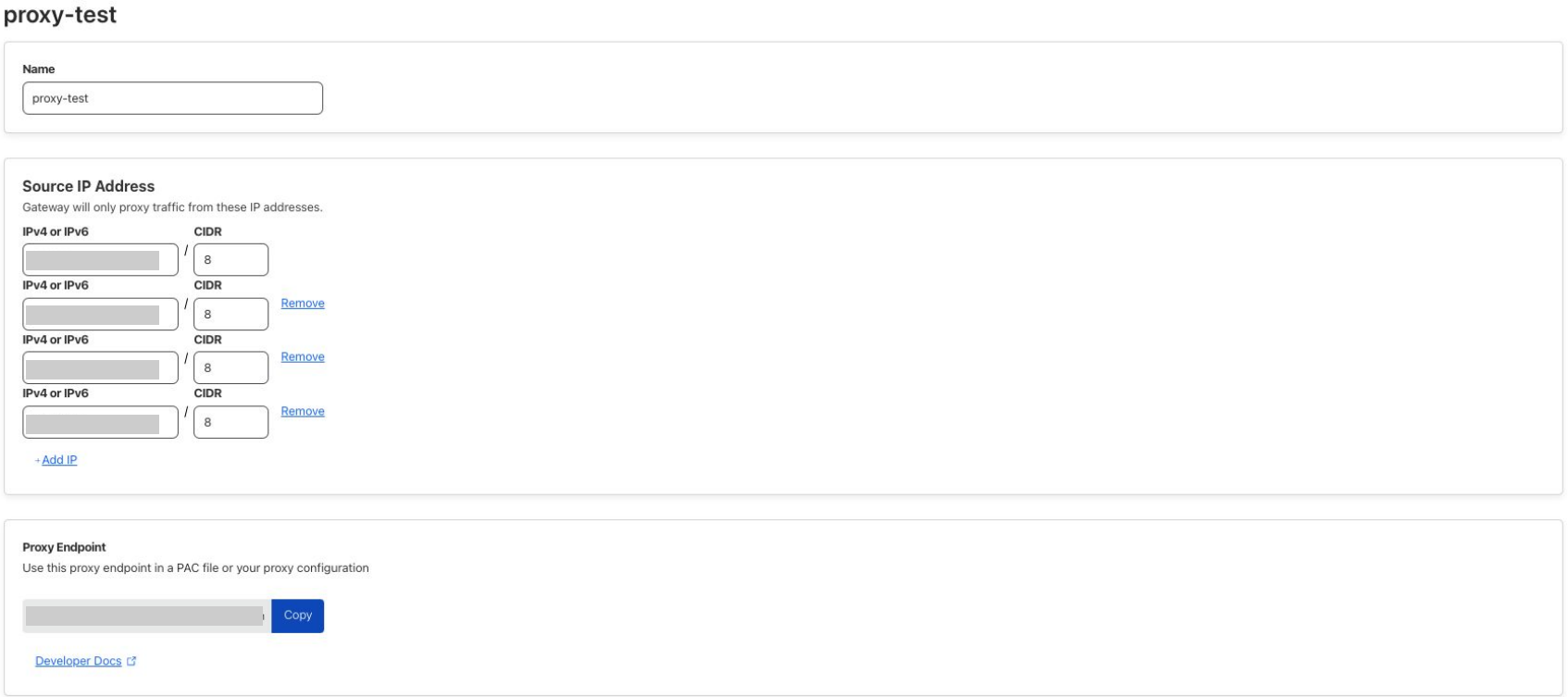
1. Firewall Policyの設定
2. Egress Policyの設定
3. Resolver Policyの設定
4. DNS Locationsの設定
5. **Proxy Endpointの設定**

Proxy Endpointの設定

Proxy Endpointを定義いただくことで、例としてWARPをインストールしない端末(agentless)のPACファイルに、定義されたProxy Endpointを指定することで、HTTPフィルタリングを適用させる事が可能となります。

参照) Cloudflare Docs - Enable Gateway proxy with PAC files

Proxy Endpointの設定



Cloudflare CASBの機能および設定

1. はじめに
2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
4. **Cloudflare CASBの機能および設定**
5. Cloudflare DLPの機能および設定
6. Q&A

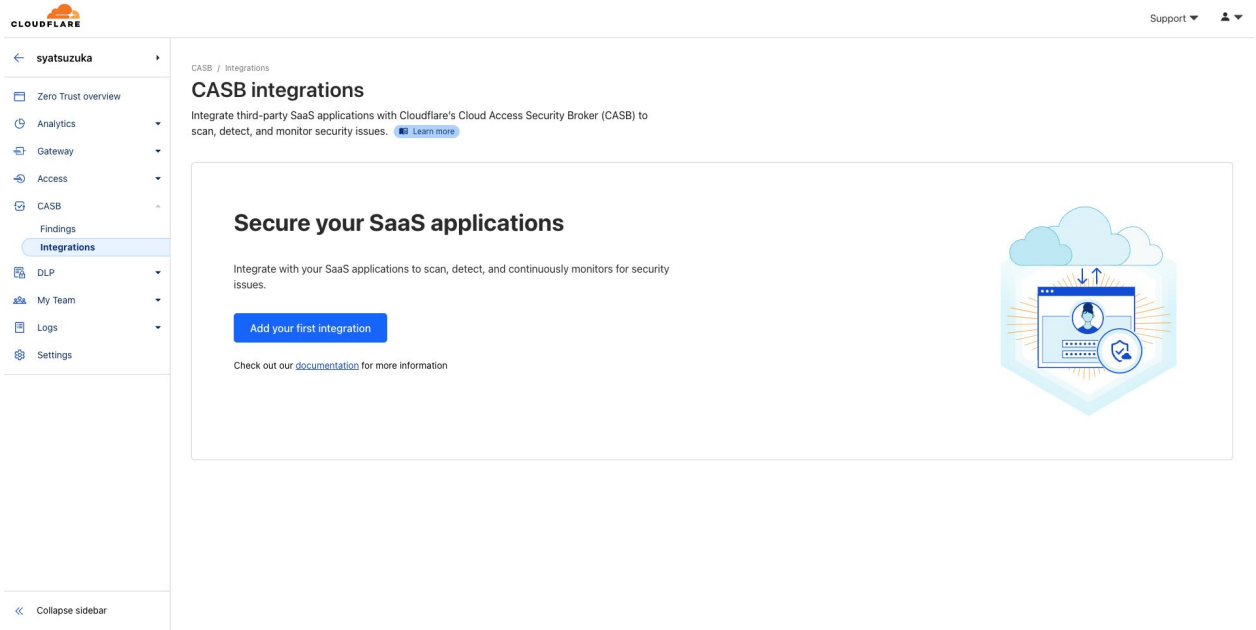
CLOUDFLARE

CASBの設定

1. **Integrationの追加**
2. Integrationの中断・削除

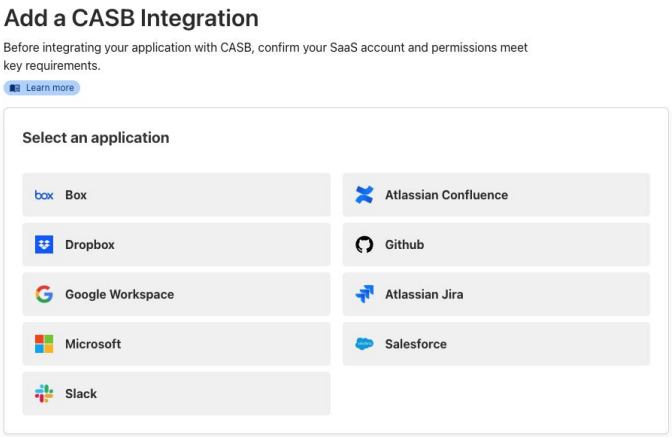
Integrationの追加

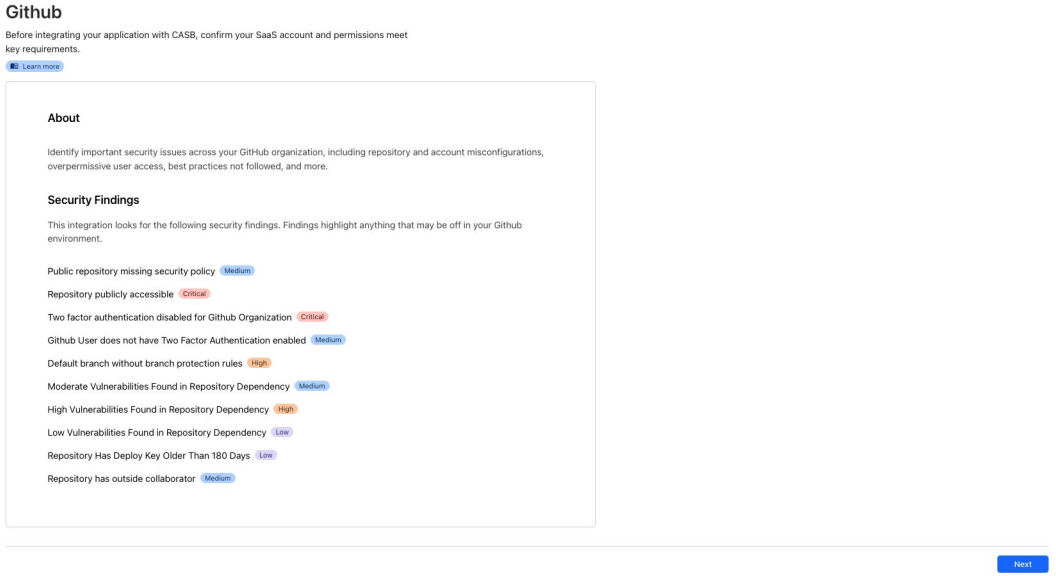
1. Zero Trustダッシュボードから、CASB > Integrationsをクリック
2. Add integrationをクリック



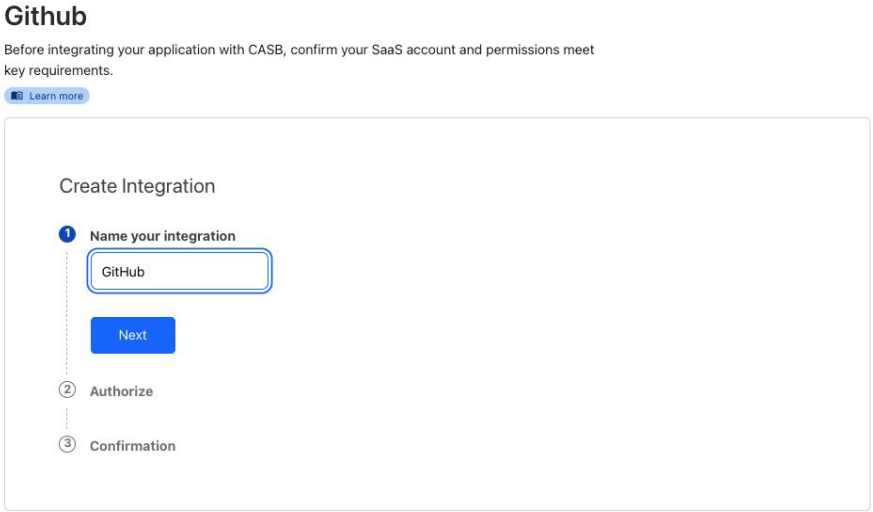
Integrationの追加

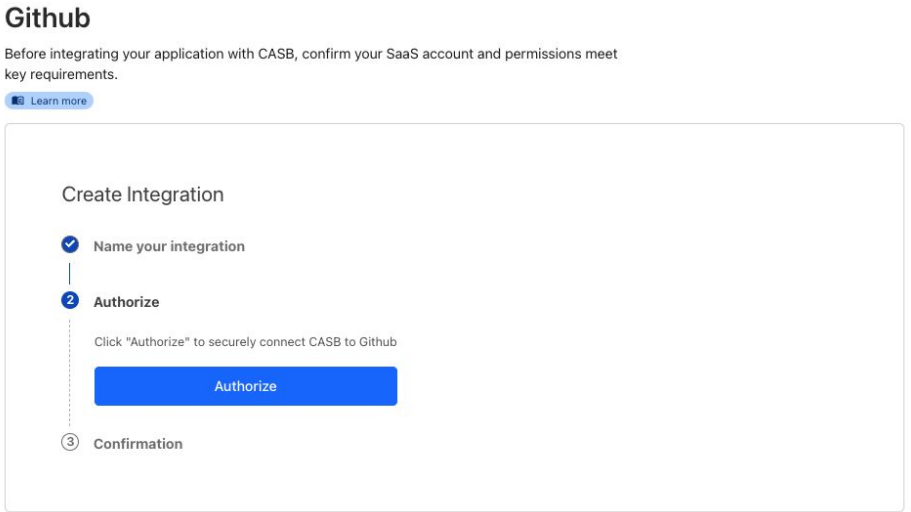
3. 利用可能なSaaSとのIntegrationを選択の上、Addをクリック
4. インストラクションに従い画面操作を進め、Saveボタンをクリック





Integrationの追加

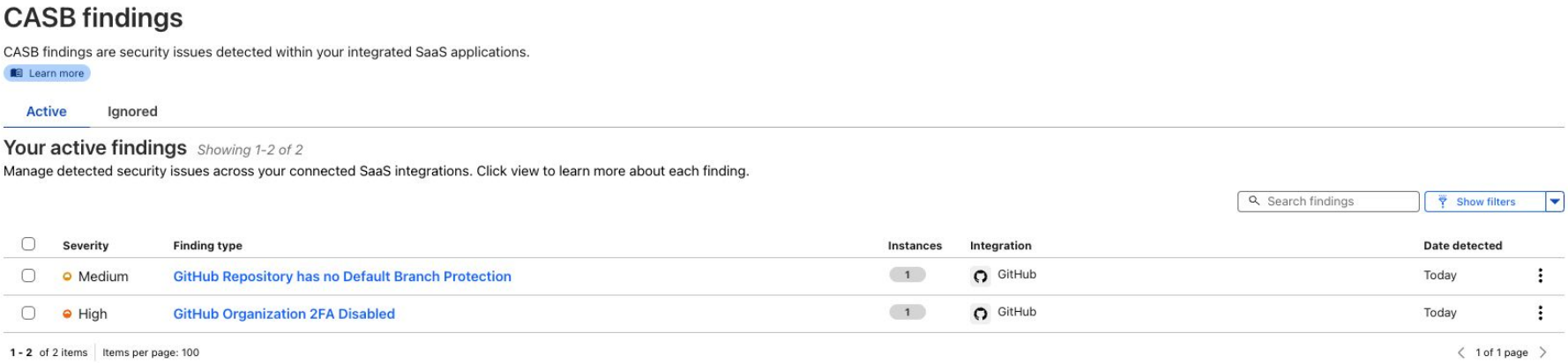




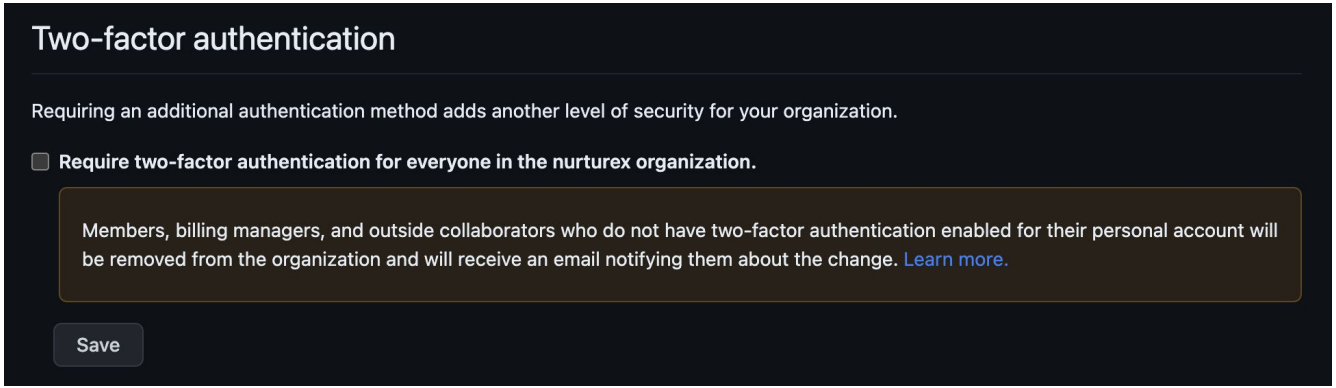
Integrationの追加

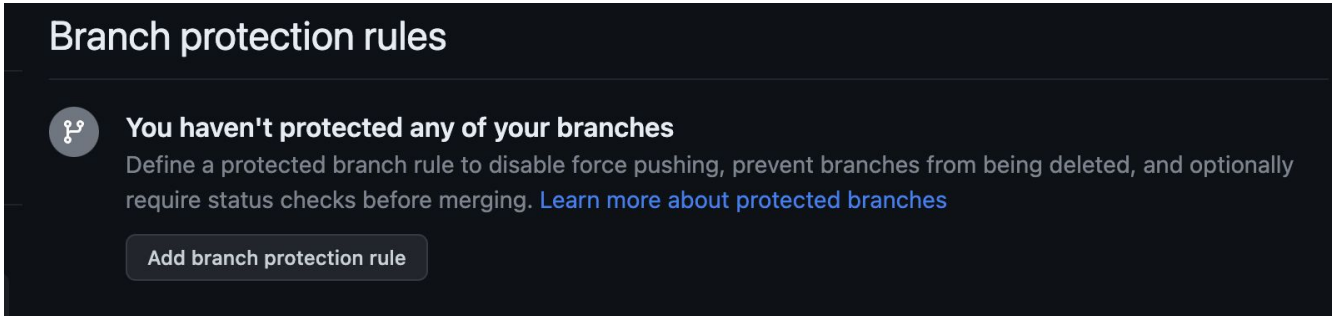
5. Finding pageへリダイレクトされ、検出されたイシューを確認できる

※セキュリテイ対策がとられた後、次回の自動検査で解消が確認されれば、Active Instancesの表示は自動で消えます。



Integrationの追加





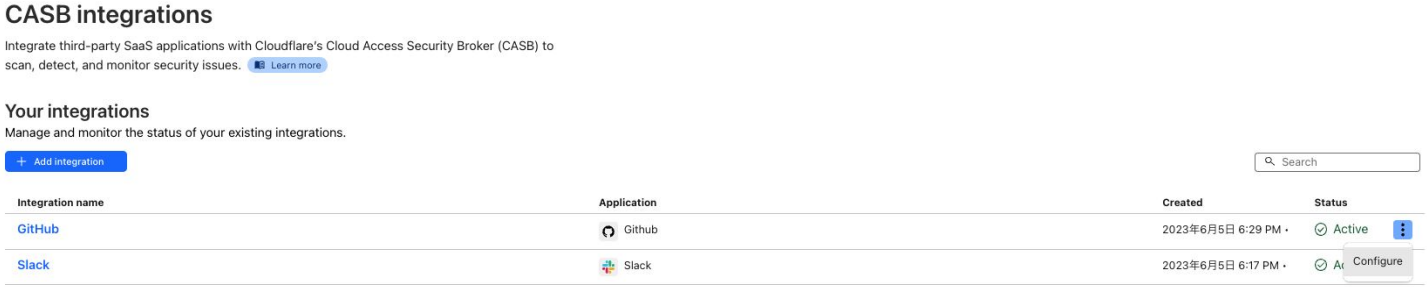
CLOUDFLARE

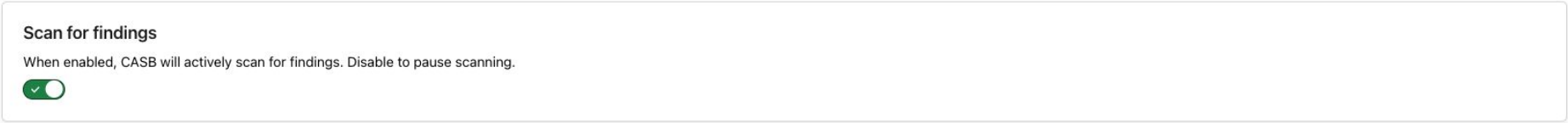
CASBの設定

1. Integrationの追加
2. **Integrationの中断・削除**

Integrationの中断・削除

1. Zero Trustダッシュボードから、CASB > Integrationsをクリック
2. 中断対象とするIntegrationからConfigurationを選択し、Scan for findingsを無効化。もしくは不要であれば同画面からDeleteボタンをクリック





Cloudflare DLPの機能および設定

1. はじめに
2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
5. **Cloudflare DLPの機能および設定**
6. Q&A

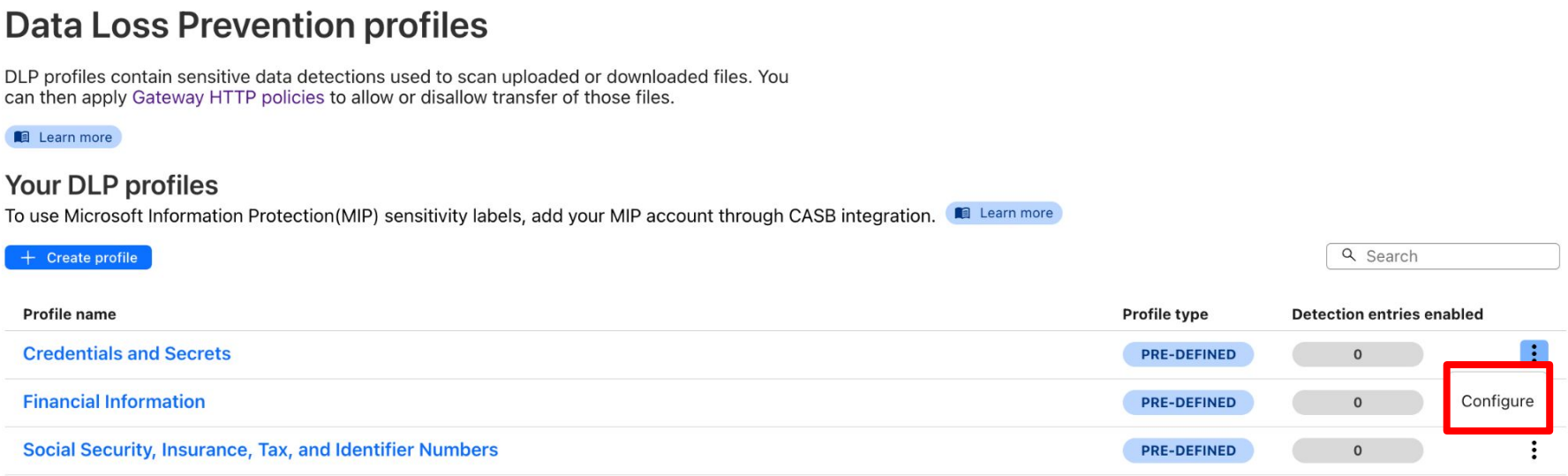
DLPの設定

1. **DLP Profileの設定**
2. DLPポリシーの作成
3. DLPログの確認

参照) Cloudflare Docs - Scan HTTP Traffic with DLP

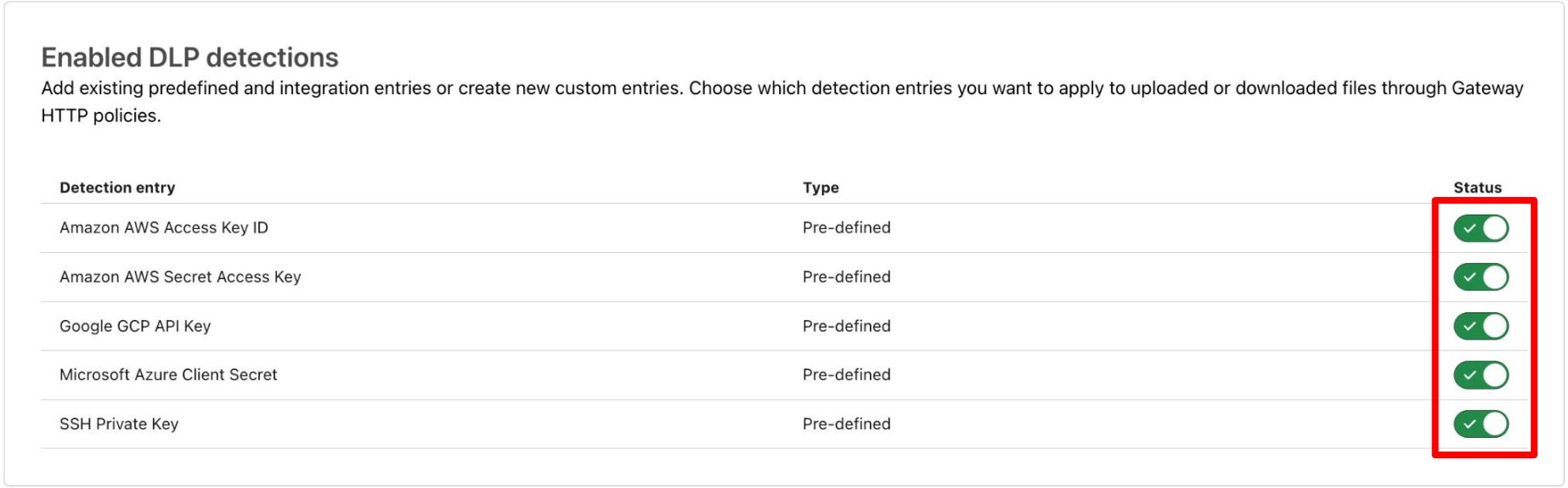
DLP Profileの設定

1. Zero Trustダッシュボードから、DLP > DLP Profileをクリック
2. 設定対象のPredefined Profileを選択し、Configureをクリック



DLP Profileの設定

3. 有効化したいDetection Entryを選択の上、Save Profileボタンをクリック



Enabled DLP detections

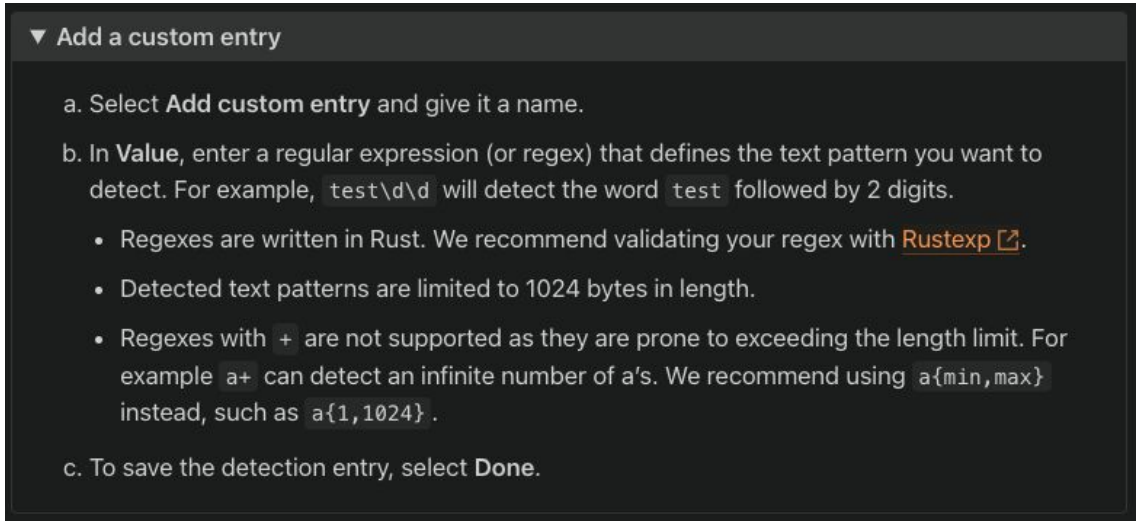
Add existing predefined and integration entries or create new custom entries. Choose which detection entries you want to apply to uploaded or downloaded files through Gateway HTTP policies.

Detection entry	Type	Status
Amazon AWS Access Key ID	Pre-defined	
Amazon AWS Secret Access Key	Pre-defined	
Google GCP API Key	Pre-defined	
Microsoft Azure Client Secret	Pre-defined	
SSH Private Key	Pre-defined	

DLP Profileの設定

4. 必要に応じて、Custom Policyを個別追加

参照) Cloudflare Docs - Configure a DLP profile
参照) Cloudflare Docs - Build a custom profile



▼ Add a custom entry

a. Select **Add custom entry** and give it a name.

b. In **Value**, enter a regular expression (or regex) that defines the text pattern you want to detect. For example, `test\d\d` will detect the word `test` followed by 2 digits.

- Regexes are written in Rust. We recommend validating your regex with Rustexp.
- Detected text patterns are limited to 1024 bytes in length.
- Regexes with `+` are not supported as they are prone to exceeding the length limit. For example `a+` can detect an infinite number of a's. We recommend using `a{min,max}` instead, such as `a{1,1024}`.

c. To save the detection entry, select **Done**.

DLPの設定

1. DLP Profileの設定
2. **DLPポリシーの作成**
3. DLPログの確認

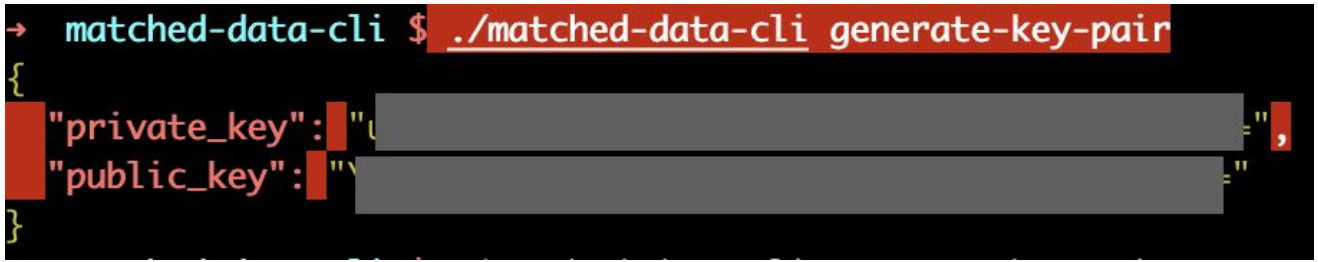
参照) Cloudflare Docs - Scan HTTP Traffic with DLP

CLOUDFLARE

DLPポリシーの作成

1. matched-data-cliをダウンロード
2. ローカルPCでコマンド実行
   $ ./matched-data-cli generate-key-pair
3. ここで得られたpublic_keyおよびprivate_keyは後続の操作で利用するため、メモに取っておく

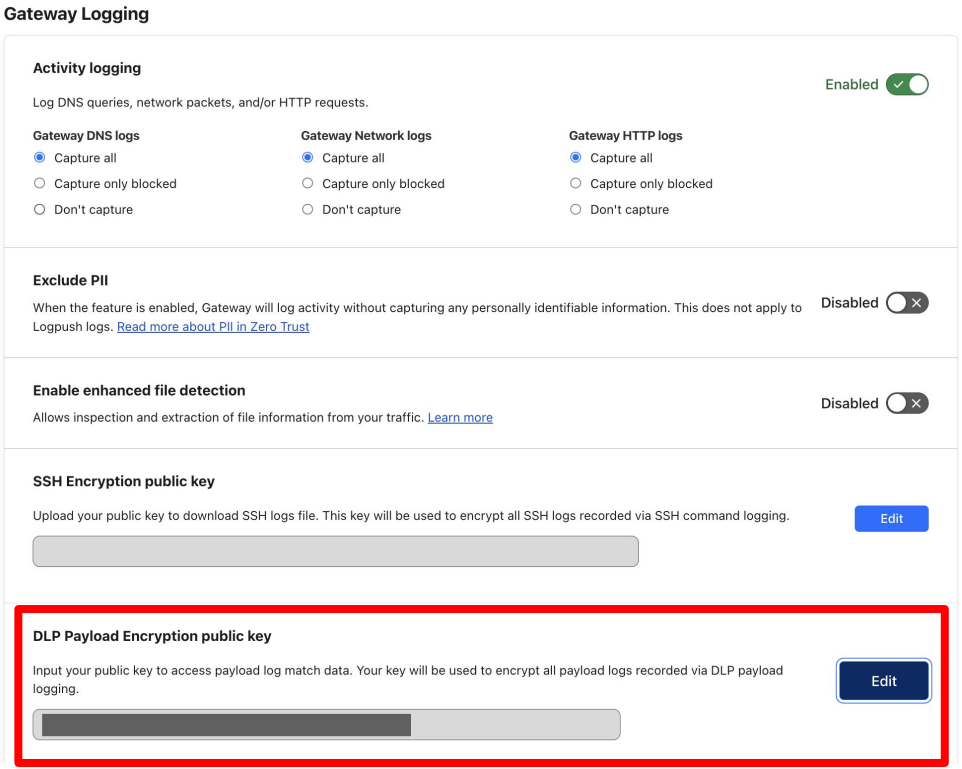
参照) Cloudflare Docs - Generate a key pair in the commandline



DLPポリシーの作成

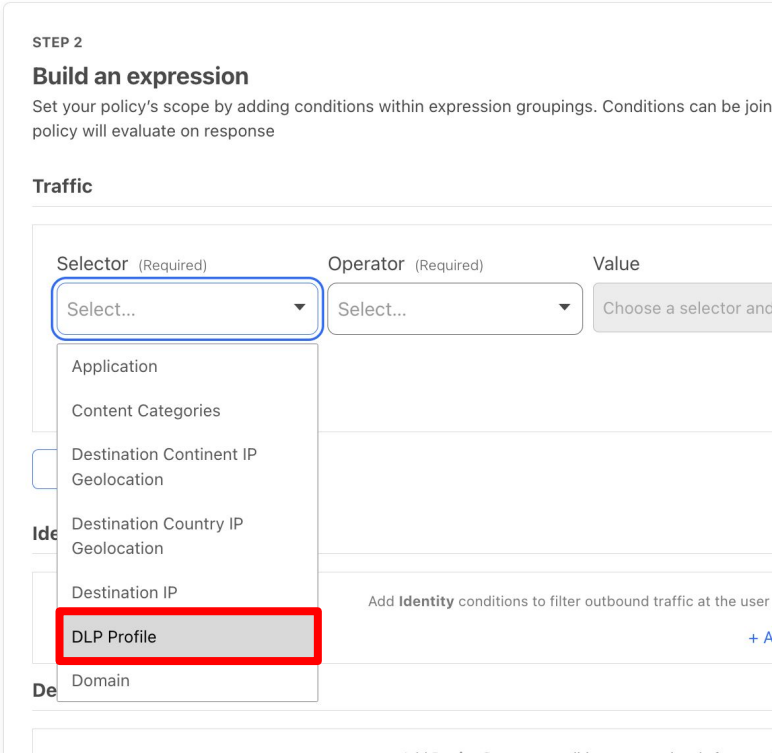
4. Zero Trustダッシュボードから、Setting > Networkをクリック
5. DLP Payload Encryption public keyに前段で確認したpublic keyを入力の上、保存

参照) Cloudflare Docs - Upload the public key to Cloudflare



DLPポリシーの作成

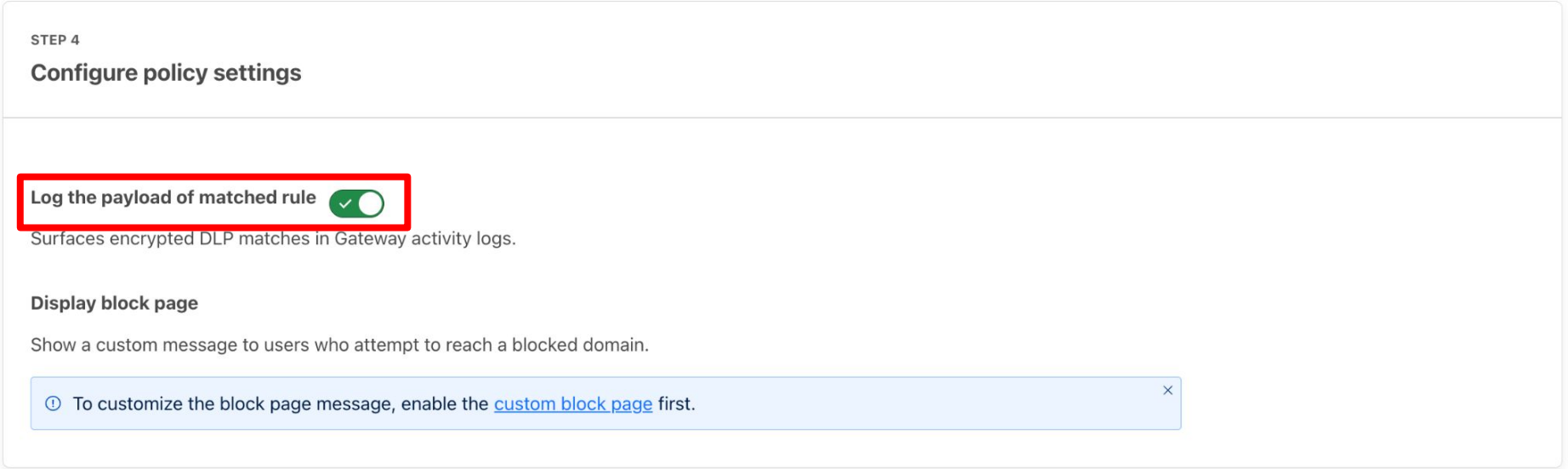
6. Zero Trustダッシュボードから、Gateway > Firewall Policies > HTTPをクリック
7. Add a policyボタンをクリック
8. TrafficのSelectorから、DLP Profileを選択
9. Actionを選択



DLPポリシーの作成

10. Configure policy settingsで”Log the payload of matched rule”をチェック
11. Create a policyボタンをクリック

→ これでDLPポリシーによるスキャンが開始



DLPポリシーの作成

参照) Cloudflare Docs - Create a DLP policy
参照) Cloudflare Docs - Common DLP policies

DLPの設定

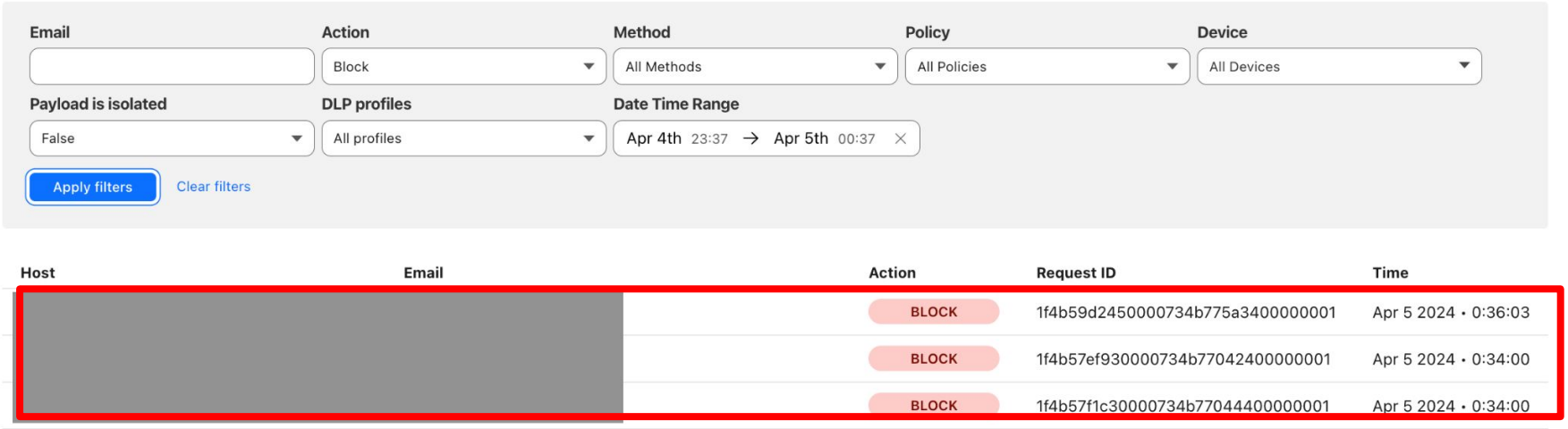
1. DLP Profileの設定
2. DLPポリシーの作成
3. **DLPログの確認**

参照) Cloudflare Docs - Scan HTTP Traffic with DLP

DLPログの確認

1. Zero Trustダッシュボードから、Logs > Gateway > HTTPをクリック
2. policyもしくはDLP profilesに作成したDLPポリシーもしくは、DLP profileを選択の上、検索

→ DLPポリシーでブロックされた通信を確認

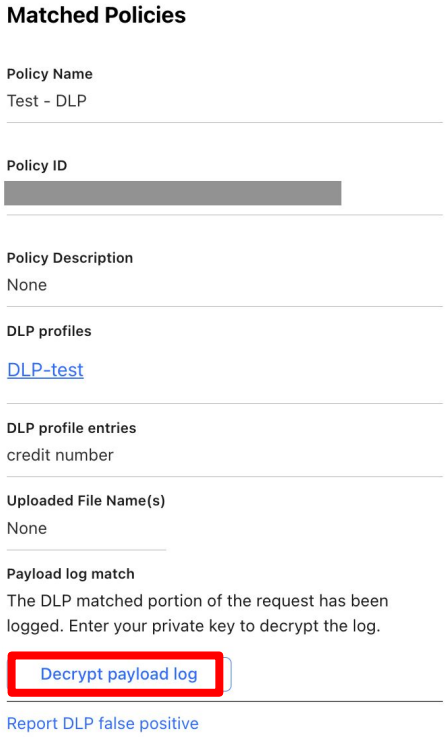


DLPログの確認

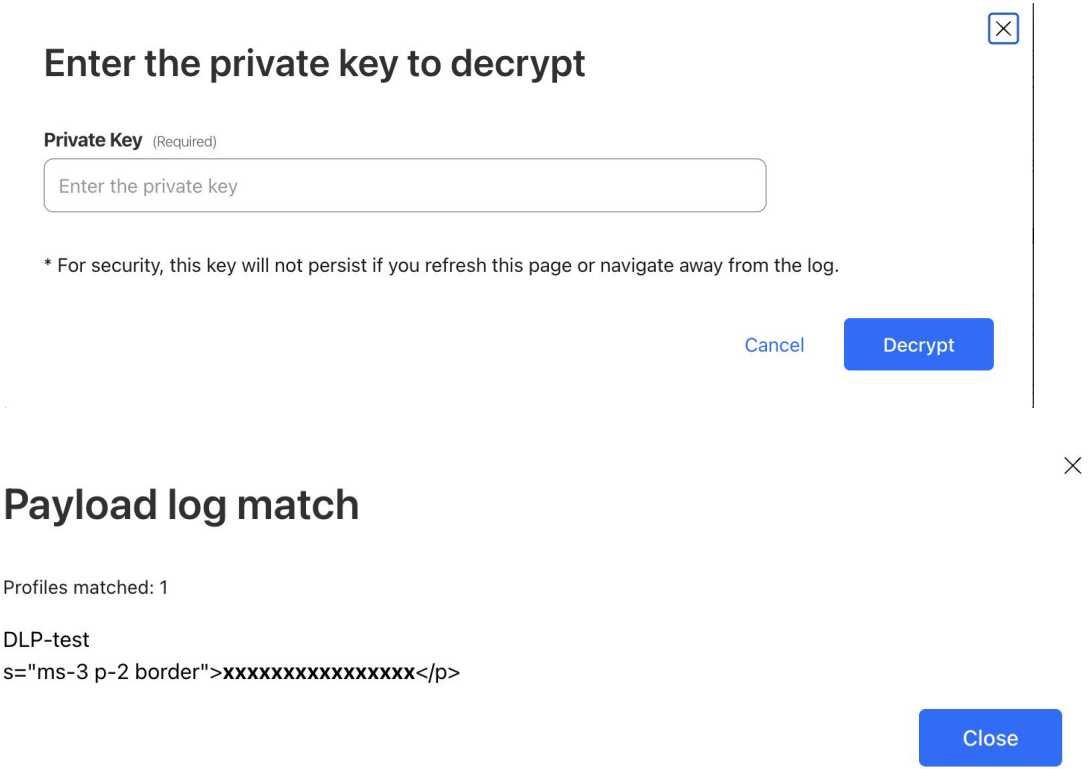
3. 該当レコードの一つを選択し、詳細ビューを表示
4. Decrypt payload logボタンをクリックし、表示されるダイアログでPrivate Keyを入力

→ 検知対象となった情報を特定するログ情報が表示される

参照) Cloudflare Docs - View payload logs



DLPログの確認


Enter the private key to decrypt
Private Key (Required)
Enter the private key
* For security, this key will not persist if you refresh this page or navigate away from the log.
Cancel
Decrypt
Payload log match
Profiles matched: 1
DLP-test
s="ms-3 p-2 border">xxxxxxxxxxxxxxxx</p>
Close

DLPログの確認 - Scan for sensitive data (CASBとの連携)

CASBとDLPをあわせてご利用いただくことで、SaaSアプリケーション上のデータに対して、DLPを適用することで、機密データの漏洩を検知することも可能です。
検知された場合には、CASB Findingsおよび、DLPログからその内容をご確認いただけます。

参照) Cloudflare Blog - Cloudflare CASB とDLPが連携してデータを保護する仕組み
参照) Cloudflare Docs - Scan for sensitive data

Q&A

1. はじめに
2. Cloudflare ZTNAの機能および設定
3. Cloudflare SWGの機能および設定
4. Cloudflare CASBの機能および設定
5. Cloudflare DLPの機能および設定
6. **Q&A**

Thank you

1 888 99 FLARE
enterprise@cloudflare.com
cloudflare.com