# User-IDのベストプラクティス

*10.0 (EoL)*

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

## Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

## About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

## Copyright



## Last Revised

November 16, 2020

# Table of Contents


User-IDのベストプラクティス ..... 5
User-IDのベストプラクティスについて ..... 6
GlobalProtect用ユーザーIDベストプラクティス ..... 7
GlobalProtectデプロイメント用のユーザーIDプランニングのベストプラクティス ..... 7
User-ID用ベストプラクティスを使ったGlobalProtectのデプロイ ..... 7
User-ID用GlobalProtectデプロイ後ベストプラクティスの使用 ..... 8
Syslogモニタリング用のUser-IDベストプラクティス ..... 9
Syslogモニタリングデプロイメント用User-IDベストプラクティスの計画 ..... 9
User-ID用ベストプラクティスを使ったsyslogモニタリングのデプロイ ..... 9
User-ID用Syslogモニタリングデプロイ後のベストプラクティスの使用 ..... 10
再配布用のUser-IDベストプラクティス ..... 11
再配布デプロイメント用User-IDプランニングのベストプラクティス ..... 11
User-ID用ベストプラクティスを使った再配布のデプロイ ..... 11
User-ID用の再配布デプロイ後のベストプラクティスの使用 ..... 12
グループマッピング用のUser-IDベストプラクティス ..... 13
グループマッピングデプロイ用User-IDプランニングのベストプラクティス ..... 13
User-IDのベストプラクティスを使ったグループマッピングのデプロイ ..... 14
User-ID用グループマッピングデプロイ後ベストプラクティスの使用 ..... 14
ダイナミックユーザーグループ用のUser-IDベストプラクティス ..... 15
ダイナミックユーザーグループ用のUser-IDプランニングのベストプラクティス ..... 15
User-ID用ベストプラクティスを使ったダイナミックユーザーグループのデプロイ ..... 16
User-ID用ダイナミックユーザーグループデプロイ後ベストプラクティスの使用 ..... 16

# *User-ID*のベストプラクティス


- User-IDのベストプラクティスについて
- GlobalProtect用ユーザーIDベストプラクティス
- Syslogモニタリング用のUser-IDベストプラクティス
- 再配布用のUser-IDベストプラクティス
- グループマッピング用のUser-IDベストプラクティス
- ダイナミックユーザーグループ用のUser-IDベストプラクティス

# User-IDのベストプラクティスについて

User-ID™は、ディレクトリサーバー、ワイヤレスLANコントローラ、VPN、NAC、プロキシなどさまざまなリポジトリからのユーザーコンテキストを活用し、次の事柄を実現しています。

- ユーザーを識別して、その信頼レベルと行動に基づいて、以下の事項に関係なくユーザーに最小権限の原則を適用します。
  - ユーザーの場所（オフィスや自宅など）
  - 使用しているデバイス（iOS、Androidモバイル機器、Mac OS、Windows、Linuxデスクトップ、ラップトップ、Citrix、Microsoft VDI、またはターミナルサーバーなど）
  - ユーザーがアクセスしているアプリケーション
- サードパーティWebサイトでの会社の認証情報の使用から保護し、アプリケーションの変更を行うことなく、任意のアプリケーションに対してネットワーク層での多要素認証（MFA）を有効にすることで、盗まれた認証情報の再利用を防止します。

場所に関係なくネットワーク上のユーザーを一貫して識別する能力により、ユーザーアクティビティへの可視性が向上し、ユーザーおよびグループベースのセキュリティポリシーを有効にして、より詳細な知見を得るための解析を行うことができます（ロギング、レポート、フォレンジックなど）。ネットワークでUser-IDをプランニング、デプロイ、および維持管理するために、次のベストプラクティスガイドラインをご利用ください。

User-IDは、さまざまな機能をサポートしています。このガイドでは、次の機能について説明しています。

- GlobalProtect
- Syslogモニタリング
- 再配布
- グループ マッピング
- ダイナミックユーザー グループ

このガイドラインでは取り上げていないその他の機能の例を次に示します:

- Panoramaが管理するPrisma Access
- 認証情報フィッシングの防止
- 次の項目からのIPアドレス - ユーザー名間マッピング:
  - ネットワーク アクセス制御（NAC）デバイス
  - Authentication Portal（認証ポータル）
  - Active Directory

# GlobalProtect用ユーザーIDベストプラクティス

Palo Alto NetworksはGlobalProtectを、User-ID向けのベストプラクティスソリューションとしてお勧めします。これは、リモートユーザーへの接続性を提供しており、内部ゲートウェイを使って内部ネットワーク上のユーザーのマッピング情報を収集します。ネットワークの接続性、デバイスの姿勢、またはユーザー認証状態に変化があった場合、GlobalProtectはユーザーに認証情報を使った認証を要求し、ユーザーベースのポリシー適用のために正確なユーザーマッピング情報を維持します。

## GlobalProtectデプロイメント用のユーザーIDプランニングのベストプラクティス

- GlobalProtectの適切なデプロイ方法については、『GlobalProtectクイック設定ガイド』を参照してください。User-IDに対しては、Always On VPN Configuration（常にVPN設定オン）およびMixed Internal and External Gateway Configuration（内部および外部ゲートウェイの混在）を使用します。
- ユーザーを識別するすべてのエンドポイント上に、GlobalProtectアプリケーションをインストールします。
- GlobalProtect認証に使用する、ユーザー名のディレクトリ属性を決定します（UserPrincipalName、sAMAccountName、コモンネームなど）。Group Mapping Profile（グループマッピングプロファイル）に、これらの属性をプライマリまたは代替ユーザー名として指定します。
- クライアント証明書認証を使用する場合、証明書のSubject Name（件名）フィールドはユーザー名でなければなりません。User-IDはマシン証明書をサポートしていません。
- 内部ゲートウェイが1つのみ存在しているけれども、そのゲートウェイからマッピング情報を学習する必要がある他のファイアウォールがある場合、マッピング情報を他のファイアウォールに送信するための、再配布のデプロイ方法についてプランニングを行います。
- 複数のソースからマッピングを受け取るかどうかを判断します。受け取る場合はWebインターフェイスまたはCLIを使ってソースを評価して、GlobalProtectから収集したIPアドレスとユーザー名のマッピングを、GlobalProtectよりも精度が低いまたは古い可能性がある、ソースが提供するマッピング情報で上書きできるかどうかを判断します。

## User-ID用ベストプラクティスを使ったGlobalProtectのデプロイ

- GlobalProtectポータルおよびゲートウェイをデプロイします。場所に関係なく、一貫してユーザーを識別するために、内部ゲートウェイと外部ゲートウェイの両方をデプロイします。
- 内部および外部ゲートウェイの両方を使用してネットワークにアクセスする場合は、接続方法としてPre-logon（Always On）（ログオン前（常時オン））または User-log on（Always On）（ユーザーログオン（常時オン））を使用します。
- 認証に証明書を使用する場合は、Simple Certificate Enrollment Protocol（SCEP）を使って、User-Specific Client Certificates for Authentication（認証用のユーザー固有のクライアント証明書）をデプロイします。
- 内部ゲートウェイを使用する場合は、ユーザーを内部ゲートウェイに送信する時期がGlobalProtectアプリケーションに分かるように、Internal Host Detection（内部ホスト検出）を使用します。
- ユーザーの識別は、ソースゾーン内でのみ有効にしてください。たとえば、GlobalProtect外部ゲートウェイを使用する場合、トンネルインターフェイスに関連するゾーン内でUser-IDを有効にします（**Network**（ネットワーク）> **Zones**（ゾーン）> *tunnel-zone*）。
- 複数のソースからユーザーマッピングを受け取る場合、User-IDエージェントの外部GlobalProtectゲートウェイ用GlobalProtectサブネットを除外して、GlobalProtectが提供するユーザーマッピングが、GlobalProtectよりも精度が低い、または古いマッピングを提供するソースにより上書きされないようにしてください。

- GlobalProtectゲートウェイが他のファイアウォールから収集したマッピングを共有するために、再配布を設定します。
- ユーザーが、グループマッピングプロファイル内のプライマリユーザー名または代替ユーザー名属性を使って、GlobalProtectで認証するための、すべてのユーザー名フォーマットを指定します。GlobalProtect認証中にユーザーがドメイン名を指定しない場合、**Allow matching usernames without domains**（ドメインのない一致するユーザー名を許可）（**Device**（デバイス）> **User Identification**（ユーザーID）> **User Mapping**（ユーザーマッピング）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto NetworksUser-ID**エージェントセットアップ））を有効にします。
- セキュリティポリシールールを作成して、それが目的のユーザートラフィックフローに一致しているかどうかをテストします。

## User-ID用GlobalProtectデプロイ後ベストプラクティスの使用

- エンドポイント上でGlobalProtectアプリケーションを保守、アップデートします。アップデートするエンドポイント数が多い場合、Webサーバーでホストアプリケーションをアップデートして、ユーザーが接続したアプリケーションをダウンロードした時のファイアウォールの負荷を減らすか、またはソフトウェア配布ツールを使ってアップデートを管理対象ホストにプッシュ配信します。
- GlobalProtectアプリケーションで、ユーザーが正常に外部ゲートウェイに接続できていることを確認します。
- ファイアウォールがGlobalProtectから、IPアドレスとユーザー名のマッピングを受け取っていることを確認します。
  - Webインターフェイス上で、**Monitor**（監視）> **User-ID**を選択して、**User**（ユーザー）列にユーザー名が表示されることを確認します。
  - CLIコマンドを使って、ファイアウォールが正しくマッピングを受け取っていることを確認します。

# Syslogモニタリング用のUser-IDベストプラクティス

Palo Alto Networksファイアウォールは、syslogメッセージを解析してIPアドレスからユーザー名へのマッピングを取得することができます。syslogメッセージを使って、サードパーティのVPNソリューション、ネットワークアクセスコントロール（NAC）ソリューション、セキュリティ情報イベント管理（SIEM）システムなどの、既存のネットワークサービスおよびデバイスからの認証イベントを使用することができます。ユーザーマッピングを最新の状態に保つために、ログアウトイベントのsyslogメッセージを解析し、古いマッピングを自動的に削除するようにファイアウォールを設定することも可能です。

## Syslogモニタリングデプロイメント用User-IDベストプラクティスの計画

- syslog送信者が使用しているフォーマットを確認して、使用している構文、ドメイン名が含まれているかどうか、およびそれらが条件を満たしているかどうかを判断します。
- ログオンイベント、ログアウトイベント、またはその両方を監視するかどうかを決定します。ログアウトイベントを監視する場合は、syslog送信者がメッセージにIPアドレスとユーザー名の両方を含めているかどうかを確認します。
- syslogメッセージに基づいて、正規表現またはフィールド識別子を使用する必要があるかどうかを判断します。syslogメッセージが一貫しており予測可能な場合は、フィールド識別子を使用します。メッセージが複雑で予測が困難な場合は、正規表現を使用します。
- PAN-OS統合User-IDエージェントを使った（Windows User-IDエージェントではない）、ファイアウォールへのsyslogモニタリングのデプロイを計画します。

## User-ID用ベストプラクティスを使ったsyslogモニタリングのデプロイ

- syslog送信者が異なるフォーマットを使用している場合は、各フォーマットに対してSyslog Parse（Syslog解析）プロファイルを設定します。
- ログインおよびログアウトイベントの両方を監視したい場合は、各イベントタイプに対してSyslog解析プロファイルを設定します。
- システムメッセージにドメイン名が含まれておらず、すべてのドメインに対してユーザー名が一意である場合は、**Allow matching usernames without domains**（ドメインなしで一致するユーザー名を許可）を有効にします。
- PAN-OS統合User-IDエージェントで、トラフィックは暗号化されるため、必ずSSLを使用してsyslogメッセージを確認してください。UDPはトラフィックを平文で送信するため、UDPを使用する必要がある場合は、Syslog送信者とクライアントの両方が専用の安全なネットワークにあることを確認し、信頼されていないホストからファイアウォールにUDPトラフィックが送信されないようにします。
- 監視するすべてのsyslog送信者が、Server Monitoring（サーバーモニタリング）リストに含まれていることを確認します。ファイアウォールは、このリストに記載されていない送信者からのsyslogメッセージを無視してしまいます。
- Filter List（フィルタリスト）内のエントリの順番を、もっとも一致する可能性が高い項目からの順番に並び替えます。たとえば、80%のsyslogメッセージがfilter1に一致し、20%がfilter2に一致すると思う場合は、リスト内でfilter2より前にfilter1を配置します。

# User-ID用Syslogモニタリングデプロイ後のベストプラクティスの使用

- syslogメッセージがSyslog Parse（Syslog解析）プロファイルに一致しており、ファイアウォールがsyslogメッセージから、IPアドレスとユーザー名のマッピングを受信していることを確認します。
- ファイアウォールがsyslog送信者からメッセージを受信し、ユーザーを正しくマップしていることを確認するには、`show user server-monitor statistics` CLIコマンドを使用します。

# 再配布用のUser-IDベストプラクティス

大規模なネットワークでは、すべてのファイアウォールがマッピング情報ソースに直接クエリを送るよう設定する代わりに、再配信を通じてすでに他のファイアウォール上に存在しているマッピング情報を収集するようにファイアウォールを設定することで、リソースを合理的に使用できます。

## 再配布デプロイメント用User-IDプランニングのベストプラクティス

- 再配布アーキテクチャのプランニング考慮すべきファクター：
  - どのファイアウォールがすべてのデータタイプ（IPアドレスとユーザー名のマッピングまたはデバイスの隔離情報など）に対してポリシーを適用し、どのファイアウォールがデータのサブセットを受け取るのか？
  - IPアドレスとユーザー名のマッピングが必要なIP範囲は？
  - ユーザーマッピングを提供する内部ゲートウェイがある場合、そのデータを必要とするその他のデバイスは？それらが保有している機能とロールは？
  - すべてのデータを集計するために必要なホップ数を最低限に抑える方法は？IPアドレスとユーザー名のマッピングの最大許容ホップ数は10で、ユーザー名からタグへのマッピングおよびIPアドレスからタグへのマッピングの最大許容ホップ数は1です。
  - ユーザーマッピングの情報ソースをクエリするファイアウォールの数を最小化する方法は？クエリを行うファイアウォールの数が少なければそれだけファイアウォールとソースのプロセス負荷も低下します。
- 再配布Hubに最適なオプションを決定します:
  - 大規模なUser-IDデプロイ環境には、専用のVM-Seriesファイアウォールが最適です。ユーザーマッピングのみを再配布する場合は、VM-50で十分です。IPアドレスからタグへのマッピングも再配布する場合は、VM-300またはそれ以上のシリーズを使用することをお勧めします。
  - 中規模から小規模の環境の場合、およびユーザーマッピングの収集にsyslogまたはサーバーモニタリングを使用しない場合は、Panoramaが適しています。
- ネットワーク要件に基づいて、使用するトポロジのタイプを判断します。
  - 単一リージョン用ハブアンドスポーク
  - 複数リージョン用ハブアンドスポーク
  - 階層構造

## User-ID用ベストプラクティスを使った再配布のデプロイ

- 再配布する情報のソースを設定します:
  - User-ID IPアドレスからユーザー名へのマッピング（Windows User-IDエージェントを含む）
  - ダイナミック アドレス グループの IP アドレスとタグのマッピング
  - ダイナミック ユーザー グループのユーザー名とタグのマッピング
  - HIPベースのポリシー適用のデータ
  - デバイス隔離情報
- エージェントがデータの再配布に含めるネットワーク、およびIPアドレスからタグへのマッピングまたはIPアドレスからユーザー名へのマッピングの再配布から除外するネットワークを設定します。
- Include/Exclude Networks（包含/除外ネットワーク）リストを使用し、再配布エージェントがマッピングを再配布する際に含めるか、除外するサブネットワークを定義します。
- 再配布を通じて特定のデータタイプを受け取るネットワークまたはリソースを設定します。

- 再配布エージェントとクライアント間の相互認証にカスタム証明書を使用するには、Authentication with Custom Certificates for Redistribution（再配布をカスタム証明書で認証）を有効にします。
- データの再配布にはVM-Seriesファイアウォールまたは Panoramaを使用します。Panoramaはエージェントまたはクライアントになれるため、Panoramaでのデータ再配布の設定には、**Panorama** > **Data Redistribution**（データの再配布）を使用します。
- ポリシーを適用するファイアウォールが、GlobalProtectゲートウェイおよびデータセンターでもあるため、リモートユーザーとローカルユーザーの両方からのマッピングが必要な場合、双方向の再配布を有効にしてください。
- 最適なレジリエンスを確保するために、リージョン間ではなく単一のリージョン内でのみ双方向の再配布を有効にする必要があります。

## User-ID用の再配布デプロイ後のベストプラクティスの使用

- エージェントがクライアントに正しくデータを再配布したかどうかを確認するには、「データ再配布の設定」の最後の2つのステップを行ってください。

# グループマッピング用のUser-IDベストプラクティス

個々のユーザーではなくユーザー グループ メンバーシップに基づいてポリシー ルールを定義すると、グループ メンバーシップが変更されるたびにルールを更新する必要がなくなるため、管理が簡略化されます。LDAPデプロイ環境でグループマッピングを設定するための、お勧めするベストプラクティスを次に示します。

次のセクションは、オンプレミスディレクトリサービスに対してグループマッピングをデプロイするためのベストプラクティスについて説明しています。

## グループマッピングデプロイ用User-IDプランニングのベストプラクティス

- ディレクトリサービス（Active DirectoryやOpenLDAPなどのLDAPベースのサービス）、およびディレクトリサーバー用のトポロジを識別します。検討事項の一例を以下に示します:
  - 存在しているディレクトリサーバー、データセンター、およびドメインコントローラの数は？
  - グループ情報の主なソースは？
  - ディレクトリサーバーに関連して、ドメインコントローラはどこに配置されているのか？
  - ディレクトリサーバーとドメインコントローラは異なるリージョンに存在しているのか？
  - ローカルのリソースおよびリージョン向けのリソースは？
- グループマッピングの主なソースがActive Directoryサーバーであるデプロイ環境の場合:
  - ドメインが 1 つの場合、ファイアウォールを接続性が最も良いドメイン コントローラに接続する LDAP サーバー プロファイルを持つグループ マッピング設定が 1 つだけ必要です。冗長性を確保するために、ドメイン コントローラを LDAP サーバープロファイルに最大 4 つまで追加します。
  - ユニバーサルグループがある場合は、SSLのポート3268または3269でグローバルカタログサーバーのルートドメインに接続するLDAPサーバープロファイルを作成し、ポート636でLDAPを使用して、ルートドメイン コントローラーに接続する別の LDAP サーバー プロファイルを作成します。TLSを使用しない場合は、ポート389を使用してください。これにより、すべてのドメインとサブドメインでユーザーとグループの情報を利用できるようになります。
  - ユニバーサルグループが存在せず、複数のドメインやまたは複数のフォレストがある場合には、ファイアウォールを各ドメイン/フォレストのドメイン サーバーに接続するLDAPサーバープロファイルを持つグループ マッピング設定を作成する必要があります。異なるフォレスト内のユーザー名が一意になるようにする必要があります。
  - グループ マッピングを使用する前に、ユーザーベースのセキュリティポリシールールの Primary Username（プライマリ ユーザー名）を設定します。この属性は、ポリシー設定、ログ、およびレポート内のユーザーを識別すします。
- LDAPディレクトリでまだ利用可能ではないカスタムグループを作成するには、ユーザー属性を使ってカスタムグループを作成します。
- 同じベース識別名（DN）またはLDAPサーバーを使用する、複数のグループマッピング設定を作成する場合、グループマッピング設定に重複するグループが含まれないようにしてください。たとえば、あるグループマッピング設定のInclude（包含）リストに、別のグループマッピング設定にも存在しているグループを含めることはできません。
- 各ドメイン内のすべてのユーザーとグループに対して、ユーザー名とグループ属性が一意であることを確認してください。
- グループの包含リストを使用する、またはカスタム検索フィルタを適用して、グループベースのセキュリティポリシーおよび設定内で使用するグループのみを取得します。

- ディレクトリ内でグループが変更される頻度を評価して、グループマッピングプロファイルに適したUpdate Interval（更新間隔）の値を決定します。たとえば、グループが頻繁に変更されている場合は小さな値を設定し、一般的に変更が行われないような場合は大きな値を設定します。
- ログ、レポート、ポリシー設定内でユーザーを表す、ユーザー名属性を決定します。User-IDソースがユーザー名を異なるフォーマットで送信している場合、それらのユーザー名を代替属性として指定します。

プライマリユーザー名、代替ユーザー名、およびメール属性は、各ユーザーに対して一意でなければなりません。

## User-IDのベストプラクティスを使ったグループマッピングのデプロイ

- ディレクトリからのカスタムグループのみを使用する場合、使用しないグループをInclude（包含）リストに追加して、User-IDがディレクトリからすべてのグループを取得することを防止します。
- ポリシールールを特定のグループに制限するには、**Group Include List**（グループ包含リスト）を使用します。代わりに、ファイアウォールで追跡する、グループ マッピングのグループをフィルタリングするには、**Search Filter**（検索フィルタ）(LDAP クエリ)、**Object Class**（オブジェクト クラス）を入力します。LDAPディレクトリでグループが利用可能になっていない場合、ユーザー属性を使ってファイアウォール上にカスタムグループを作成することができます。カスタムグループを形成するために使われる属性が、ディレクトリ上でインデックスが作成されている属性であることを確認してください。
- レポートやログでユーザーを識別する、プライマリユーザー名を指定します。

## User-ID用グループマッピングデプロイ後ベストプラクティスの使用

- LDAPサーバーへの接続性を確認するには、`show user group-mapping state all` CLIコマンドを使用します。
- グループのメンバーシップを参照するには、`show user group name` <グループ名>コマンドを実行します。
- セキュリティポリシー内でグループを使用する前に、グループ内にユーザーが存在していることを確認します。どのグループが現在ポリシー内で使用できるのか確認するには、`show user group` CLIコマンドを使用します。
- グループマッピングを変更した場合は、手動でキャッシュを更新してください。キャッシュを手動で更新するには、`debug user-id refresh group-mapping all` コマンドを実行します。

# ダイナミックユーザーグループ用のUser-IDベストプラクティス

ダイナミックユーザーグループにより、手動でポリシーを変更したり、グループを作成、更新したりすることなく、ユーザー行動、ビジネスニーズ、または潜在的な脅威に関する変化に対処することができます。ダイナミックユーザーグループは、次のようなセキュリティポリシーの作成に役立ちます。

- ユーザーに対する時間が限定されたリソースへのアクセス
- ユーザーの可視性を維持しながら、不審なユーザ行動や悪意のあるアクティビティを自動修復

タグを使ってグループの条件を定義し、変更内容をコミットした後、ダイナミックユーザーグループのメンバーシップは、ユーザーのタグに基づいて自動的に更新されます。

## ダイナミックユーザーグループ用のUser-IDプランニングのベストプラクティス

- ビジネスニーズやユーザー行動の変化などの要因に基づいて、ファイアウォールにどのようにユーザーアクセスを制御させるのかを判断します。
  - セキュリティポリシーを介してアクセスを許可または制限しますか？
  - ユーザーにMFAを要求しますか？
  - ユーザーのトラフィックを復号化して、ユーザーアクティビティの可視性をさらに強化しますか？
- 指定したダイナミックユーザーグループ内の、ユーザーのメンバーシップの期間を判断します。
  - ファイアウォールは時間に基づいて（例:契約者が一時的なリソースアクセスに必要な時間数）、ユーザーをグループから自動的に削除しますか？
  - ユーザーをグループに関連付ける、または関連付けを解除するために、ファイアウォールには特定のイベントが必要ですか（例:悪意のあるアクティビティ）？
- ユーザー行動またはビジネスニーズの変化を識別するために、ファイアウォールが生成するイベントを評価します。API、自動タグ設定を介してタグを割り当てる、またはWebインターフェイスを使って手動でタグを割り当てることができます。
  - ユースケースに応じて、ユーザーをグループ化するために使用するタグ、およびタグの生成方法を決定します。
  - たとえば、ユーザーのリスクレベルを「高リスク」、「中リスク」、「低リスク」など、セキュリティデバイスとアプリケーションから得られる知見に基づいて行動を評価し、それらのイベントに基づいてユーザーにタグを自動的に割り当てます。
- タグのユーザー情報ソースを判別します:
  - ファイアウォールログ
    - 認証、データ、脅威、トラフィック、トンネル検査、URL、および WildFire ログの場合、ログ転送プロファイルを作成し、ビルトインのアクションを使用します。
    - User-ID、HIP Match、GlobalProtect、および IP-Tag ログの場合、ログ設定を行います。
  - Cortex XSOAR
  - Splunkなどのセキュリティ情報およびイベント管理システム（SIEMS）
  - カスタムAPIスクリプト
- 複数のソースからのタグをまとめて、ダイナミックユーザーグループの条件を定義します。たとえば、確実度レベルに基づいて、単一のアプリケーションではなく、複数のセキュリティアプリケーションからユーザーの認証情報が不正利用されたことを知らせるアラートを受信した場合にのみ、ユーザーアクセスを拒否することができます。

## User-ID用ベストプラクティスを使ったダイナミックユーザーグループのデプロイ

- ダイナミックユーザーグループに追加するユーザーが大量に存在している場合、または他のセキュリティアプリケーションからのイベントに基づいてユーザーを追加したい場合は、Webインターフェイスの代わりにAPIを使ってユーザーを追加します。
- APIを使用するか、またはユーザーをこのグループから削除する時期（例:契約の失効）を表すTimeout（タイムアウト）を手動で設定します。
- ダイナミックユーザーグループを、ユーザーアクセスを制御するソースユーザーとして使用し、MFAを有効にする、またはダイナミックユーザーグループのメンバーであるユーザーのトラフィックを復号化する、セキュリティポリシールールを作成します。
- ユーザータグの情報を提供するために、ソースを設定します。
  - ファイアウォールログを使用する場合、自動タグ設定を設定して、ユーザーにタグを設定します。
  - Splunkを使用する場合、Palo Alto Networks app for Splunkを使ってユーザーにタグを割り当てることができます。
  - Cortex XSOARまたは他のセキュリティオーケストレーション、オートメーション、およびレスポンス（SOAR）プラットフォームでプレイブックを使用して、特定のイベントに基づいてユーザーにタグを適用します。
  - カスタムスクリプトを使用する場合、API を使ってタグを記入するようにスクリプトを変更します。
  - ファイアウォールのインターフェイスを使って、ユーザーをグループに手動で追加します。

## User-ID用ダイナミックユーザーグループデプロイ後ベストプラクティスの使用

- 目的のユーザーのみがグループのメンバーシップを保有していることを確認します。グループ内に、そのグループに所属していないユーザーが存在している場合（例:「contractor-access」グループに正社員が存在している）Unregister Users（ユーザーの登録を解除）して、ユーザー名とタグのマッピングを削除して、それをグループからDelete（削除）します。
- User-IDログを参照して、ファイアウォールがユーザーのタグを正しく生成していることを確認します。
- ダイナミックユーザーグループの詳細を確認するには、CLIコマンドを使用します（例:グループに関連付けられているユーザーを参照する）。
- Traffic（トラフィック）およびThreat（脅威）ログのダイナミックユーザーグループ列を使って、ファイアウォールがグループに目的のセキュリティポリシーを適用していることを確認します。
- ユーザータグを他のファイアウォールに再配布して、すべてのファイアウォールに一貫したセキュリティポリシーを適用します。ユーザーを再配布できるのは、1つのホップのみであることに注意してください。