ポリシー要素

この章では、Cisco ISE および Cisco Secure ACS のポリシー要素について説明します。

Cisco ISE および Cisco Secure ACS パリティ

Cisco ISE には、Cisco Secure ACS とのパリティを実現するための次の機能が導入されています。

- 個々のユーザに設定された日付が特定の期間を超えている場合、ユーザアカウントを無効にします
- すべてのユーザにグローバルに設定された日付が特定の期間を超えている場合、ユーザアカウントを無効にします
- n 日間の設定後にユーザ アカウントをグローバルに無効にします
- n 日間の非アクティブ後にユーザ アカウントを無効にします
- ネットワーク デバイスのすべてのオクテットにおける IP アドレス範囲のサポート
- IPv4 または IPv6 アドレスを持つネットワーク デバイスの設定
- IPv4 または IPv6 アドレスを持つ外部プロキシ サーバの設定
- 最大長のネットワーク デバイス グループ（NDG）名のサポート
- 時間と日付の条件のサポート
- AND 演算子および OR 演算子を持つ複合条件によるサービス選択ルール、認証ルール、および許可（標準および例外）ルールのサポート
- Active Directory での MAR 構成
- Dial-In 属性のサポート

- LDAP のパスワード変更を有効にします
- 各 PSN のプライマリおよびバックアップ LDAP サーバの構成
- RADIUS ポートの構成
- 動的属性で構成される許可プロファイル
- service-type RADIUS 属性の 2 つの新しい値
- 300,000 のユーザに対する内部ユーザ サポートの向上
- 内部ユーザ認証キャッシュ
- 外部 ID ストア パスワードに対する内部ユーザの認証
- 管理ユーザおよび内部ユーザのパスワードのディクショナリ チェック
- 許可されたプロトコルに対する Crytobinding TLV 属性のサポート
- 端末ワイヤレス LAN ユニット（TWLU）クライアントに対する EAP-TLS 認証実行時に長さを含むフラグを使用
- LDAP ID ストアのグループ名属性に対する共通名と識別名のサポート

ポリシー モデル

Cisco Secure ACS と Cisco ISE の両方にはシンプルなルール ベースの認証パラダイムがありますが、Cisco Secure ACS と Cisco ISE は異なるポリシー モデルに基づいており、そのため Cisco Secure ACS 5.5 以降から Cisco ISE への移行ポリシーが少し複雑になっています。

Cisco Secure ACS のポリシー階層は、認証要求をアクセス サービスにリダイレクトするサービス選択ルールで始まります。アクセス サービスは、内部または外部の ID ストアに対してユーザを認証し、定義された条件に基づいてユーザを承認する ID ポリシーと許可ポリシーで構成されます。

認証ポリシーおよび許可ポリシーは、Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 2.6 に移行されます。Cisco ISE は、Cisco Secure ACS のサービス選択ポリシー（SSP）と同様のポリシー セットとをサポートしているため、

Cisco Secure ACS サービス セレクション ポリシーと Cisco ISE ポリシー セット

Cisco Secure ACS サービス選択ポリシー（SSP）は、SSP のルールに基づいて適切なサービスに要求を配信しますが、Cisco ISE ポリシー セットは、ポリシー セットのエントリ基準を含むルールを保持します。ポリシー セットの順序はエントリ ルールと同じ順序で、SSP ルールの順序に類似しています。

複数の SSP ルールが Cisco Secure ACS で同じサービスまたはサービスの再利用を要求する場合があります。しかし、各ポリシー セットは独自のエントリ条件を持っているので、Cisco ISE でポリシー セットを再利用することはできません。複数の SSP ルールによって要求された 1 つのサービスを移行する場合、そのサービスのコピーである複数のポリシーセットを作成する必要があります。つまり、Cisco Secure ACS で同じサービスを要求する SSP ルールごとに Cisco ISE のポリシー セットを作成する必要があります。

Cisco Secure ACS で SSP ルールを無効またはモニタ対象として定義でき、ポリシー セットの同等のエントリ ルールは Cisco ISE で常に有効です。SSP ルールが Cisco Secure ACS で無効またはモニタ対象になっている場合、SSP ルールによって要求されたポリシー サービスは Cisco ISE に移行できません。

Cisco Secure ACS ポリシー アクセス サービスと Cisco ISE ポリシー セット

サービスを要求せずにポリシー サービスを定義できます。つまり、Cisco Secure ACS の SSP ルールによってポリシー サービスを非アクティブとして定義できます。Cisco Secure ACS リリース 5.5 以降には、既成の DenyAccess サービスがあり、そのサービスには Cisco Secure ACS のデフォルトの SSP ルールに対するポリシーも許可されるプロトコルもなく、自動的にすべての要求を拒否します。Cisco ISE には同等のポリシー セットはありません。しかし、Cisco ISE のポリシーセットを参照するエントリ ルールのないポリシーセットを持つことはできません。

許可されるプロトコルは、（特定のポリシーではなく）Cisco Secure ACS リリース 5.5 以降で条件付けられていない（サービス全体を指す SSP の条件を除く）サービス全体に接続されます。許可されるプロトコルは、Cisco ISE で条件付けられた外部ルールの結果としての認証ポリシーだけに適用されます。

ID ポリシーは、Cisco Secure ACS Release 5.5 以降の ID ソース（ID ソースおよび ID ストア順序）になるルールのフラットなリストです。

Cisco Secure ACS リリース 5.5 以降および Cisco ISE リリース 2.6 には、各許可ポリシーに接続されるオプションの例外ポリシーが含まれています。Cisco ISE リリース 2.6 には、例外ポリシーに加えて、すべての許可ポリシーに影響を与えるオプションのグローバル例外ポリシーがあります。Cisco Secure ACS リリース 5.5 以降には、グローバル例外ポリシーに相当するポリシーがありません。認証時には、ローカル例外ポリシーが最初に処理され、続いてグローバル例外ポリシーおよび許可ポリシーが処理されます。

ISE 802.1X サービスに対する FIPS サポート

移行プロセスを完了する前に、Cisco ISE FIPS モードは有効にしないでください。

連邦処理標準（FIPS）をサポートするために、移行ツールはデフォルトのネットワーク デバイス キーラップ データを移行します。

FIPS 準拠およびサポートされているプロトコル：

- ホスト ルックアップの処理（Process Host Lookup）

- Extensible Authentication Protocol-Translation Layer Security（EAP-TLS）
- Protected Extensible Authentication Protocol（PEAP）
- EAP-Flexible Authentication via Secure Tunneling（FAST）

FIPS 非準拠およびサポート対象外のプロトコル：

- EAP- メッセージ ダイジェスト 5（MD5）
- Password Authentication Protocol および ASCII
- Challenge Handshake Authentication Protocol（CHAP）
- Microsoft Challenge Handshake Authentication Protocol version 1（MS-CHAPv1）
- Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）
- Lightweight Extensible Authentication Protocol（LEAP）