ASA 8.x： AnyConnect SSL VPN CAC スマートカードの設定（Windows 用）

目次

概要
前提条件
要件
使用するコンポーネント
表記法
Cisco ASA の設定
配備上の考慮事項
認証、許可、アカウンティング（AAA）設定
LDAP サーバの設定
証明書の管理
キーの生成
ルート CA 証明書のインストール
ASA の登録と ID 証明書のインストール
AnyConnect VPN の設定
IP アドレス プールの作成
トンネル グループおよびグループ ポリシーの作成
トンネル グループ インターフェイスおよびイメージの設定
証明書の照合ルール（OCSP が使用される場合）
OCSP の設定
OCSP レスポンダ証明書の設定
OCSP を使用するための CA の設定
OCSP ルールの設定
Cisco AnyConnect Client の設定
Cisco Anyconnect VPN Client のダウンロード - Windows
Cisco Anyconnect VPN Client の起動 - Windows
新しい接続
リモート アクセスの開始
付録 A：LDAP マッピングおよび DAP
シナリオ 1： リモート アクセス許可ダイヤルインを使用した Active Directory の強制：アクセスの許可/拒否
Active Directory の設定
ASA の設定
シナリオ 2： アクセスを許可または拒否するためのグループ メンバシップを使用した Active Directory の強制
Active Directory の設定
ASA の設定
シナリオ 3： 複数の memberOf 属性のためのダイナミック アクセス ポリシー
ASA の設定
付録 B：ASA CLI 設定
付録 C：トラブルシューティング
AAA および LDAP のトラブルシューティング
例 1： 正しい属性マッピングによる接続の許可
例 2： 設定が誤った Cisco 属性マッピングによる接続の許可
DAP のトラブルシューティング
例 1： DAP による接続の許可
例 2： DAP による接続の拒否
認証局および OCSP のトラブルシューティング
付録 D：MS 内の LDAP オブジェクトの確認
LDAP Viewer

Active Directory サービス インターフェイス エディタ
付録 E
関連情報

概要

このドキュメントでは、認証用の Common Access Card（CAC）を使用して Windows 用の AnyConnect VPN リモート アクセスを実現する、Cisco 適応型セキュリティ アプライアンス（ASA）上でのサンプル設定について説明します。

このドキュメントでは、Cisco ASA と Adaptive Security Device Manager（ASDM）、Cisco AnyConnect VPN Client、Microsoft Active Directory（AD）および Lightweight Directory Access Protocol（LDAP）の設定について扱います。

このガイドの設定では、Microsoft AD および LDAP サーバを使用します。 またこのドキュメントでは、OCSP、LDAP 属性マップ、ダイナミック アクセス ポリシー（DAP）などの高度な機能についても扱います。

前提条件

要件

Cisco ASA、Cisco AnyConnect Client、Microsoft AD/LDAP、および公開キー インフラストラクチャ（PKI）についての基本的な理解があれば、完全な設定を理解するために有益です。 AD グループ メンバシップ、ユーザ プロパティ、および LDAP オブジェクトについて理解していれば、証明書属性と AD/LDAP オブジェクトの間での許可プロセスの関連付けに役立ちます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 8.0(x) 以降が稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）
- ASA 8.x 用の Cisco Adaptive Security Device Manager（ASDM）バージョン 6.x
- Cisco AnyConnect VPN Client（Windows 版）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Cisco ASA の設定

このセクションでは、ASDM を使用した Cisco ASA の設定について扱います。 ここでは、SSL AnyConnect 接続を経由した VPN リモート アクセス トンネルを配備するために必要なステップ

について説明します。 認証には CAC 証明書が使用され、証明書内のユーザ プリンシパル名（UPN）属性が、許可のために Active Directory に取り込まれます。

配備上の考慮事項

- このガイドでは、インターフェイス、DNS、NTP、ルーティング、デバイス アクセス、ASDM アクセスなどの基本的な設定については扱いません。 ネットワーク オペレータはこれらの設定をよく理解しているものとします。詳細は、『マルチファンクション セキュリティ アプライアンス』を参照してください。
- 赤色で強調表示されているセクションは、基本的な VPN アクセスのために必要な必須の設定です。 たとえば、VPN トンネルは CAC カードで設定でき、OCSP チェック、LDAP マッピング、ダイナミック アクセス ポリシー（DAP）チェックを行う必要はありません。 DoD では OCSP チェックが規定されていますが、OCSP を設定しなくてもトンネルは機能します。
- 青色で強調表示されているセクションは、設計にセキュリティを追加するために含めることができる高度な機能です。
- ASDM と AnyConnect/SSL VPN は、同じインターフェイスの同じポートを使用できません。一方または他方のポートを変更してアクセスすることを推奨します。 たとえば、ASDM をポート 445 にし、AC/SSL VPN は 443 のままにします。 ASDM への URL アクセスは、8.x で変更されました。 `https:// <ip_address>` 使用して下さい`: <port>/admin.html.`
- 必要な ASA イメージは最低 8.0.2.19 で、ASDM 6.0.2 です。
- AnyConnect/CAC は Vista でサポートされています。
- ポリシーを強制するための LDAP およびダイナミック アクセス ポリシーのマッピングの例については、付録 A を参照してください。
- LDAP オブジェクトを MS でチェックする方法については、付録 D を参照してください。
- 関連情報を参照して下さい