Cisco VPN 3000コンセントレータでHTTPを使用してCRLチェックを行う

目次

はじめに
前提条件
要件
使用するコンポーネント
表記法
ネットワーク図
VPN 3000 コンセントレータの設定
手順説明
モニタリング
確認
コンセントレータからのログ
正常なコンセントレータ ログ
壊れるログ
トラブルシューティング
関連情報

はじめに

このドキュメントでは、HTTP モードを使用して Cisco VPN 3000 コンセントレータにインストールされた認証局（CA）の証明書に関する証明書失効リスト（CRL）のチェック機能をイネーブルにする方法について説明します。

証明書は全体の有効期間の間有効であると普通期待されます。 ただし証明書が名義変更のような事柄が無効な原因に、主題と CA 間のアソシエーションの変更なれば、とセキュリティ妥協、CA は証明書を取り消します。 X.509 の下で、CA は定期的に各々の取り消された証明書がシリアル番号によって識別される署名された CRL を発行することによって証明書を取り消します。 CRLチェックをイネーブルにすることは VPN コンセントレータが認証のために証明書を使用する度に、確認される証明書は取り消されなかったことを確認するためにまた CRL をチェックすることを意味します。

CRL を保存し、配る CA 使用 Lightweight Directory Access Protocol（LDAP）/HTTP データベース。 それらはまた他の手段を使用するかもしれませんが VPN コンセントレータは LDAP/HTTP アクセスに頼ります。

HTTP CRLチェックは VPN コンセントレータ バージョン 3.6 または それ 以降でもたらされます。 ただし、LDAP ベース CRLチェックは以前の 3.x リリースでもたらされました。 この資料は HTTP を使用してだけ CRLチェックを説明します。

注: VPN 3000 シリーズ・コンセントレータの CRL キャッシュサイズはプラットフォームによって決まり、管理者の希望に従って設定することができません。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- インターネット キー エクスチェンジ（IKE）認証のための証明書を使用して VPN 3.x ハードウェアクライアントからの IPSecトンネルをうまく確立しました（イネーブルになっているCRLチェック無しで）。
- VPN コンセントレータに CA サーバへの接続がいつもあります。
- CA サーバがパブリックインターフェイスに接続される場合、公共（デフォルト）フィルタの必要なルールを開きました。

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。

- VPN 3000 コンセントレータ バージョン 4.0.1 C
- VPN 3.x ハードウェアクライアント
- Windows 2000 サーバで動作している証明書 生成および CRLチェックのための Microsoft CA サーバ。

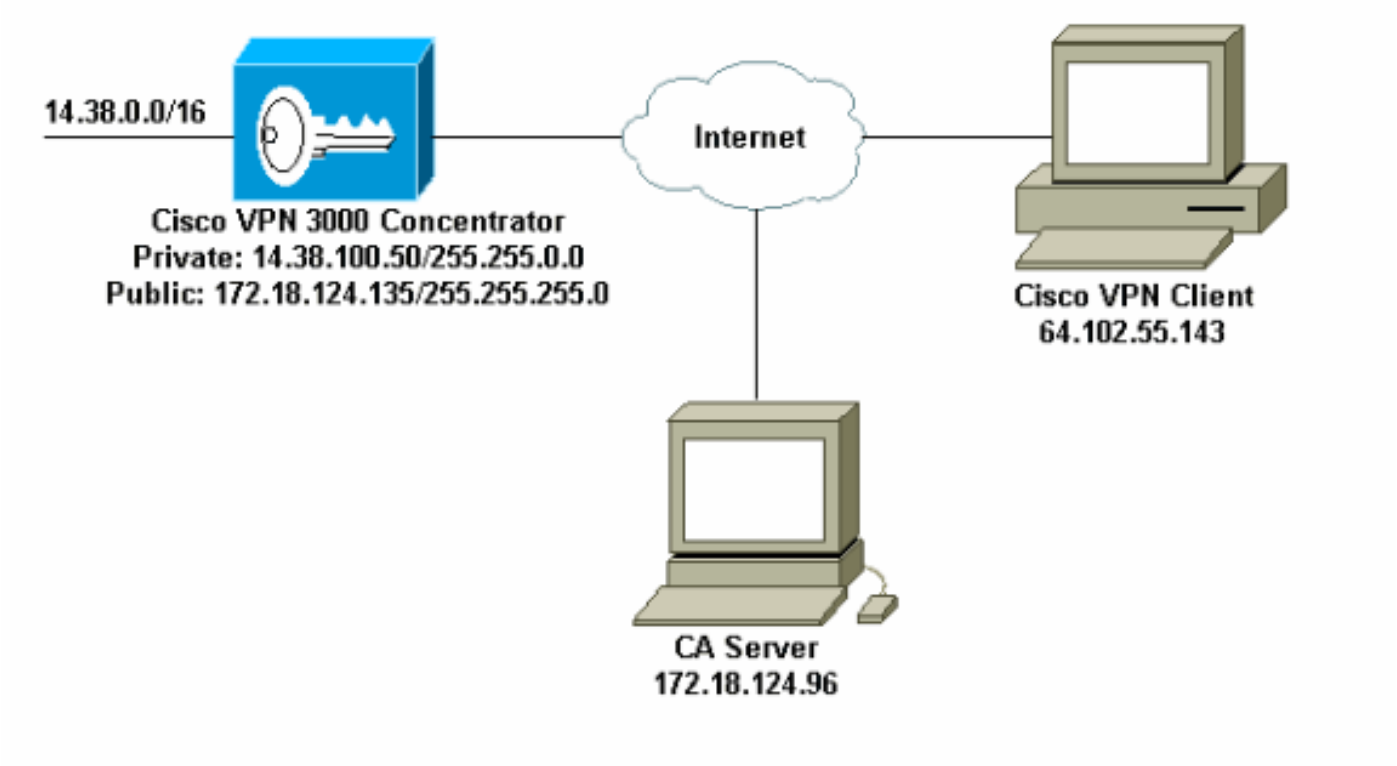
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

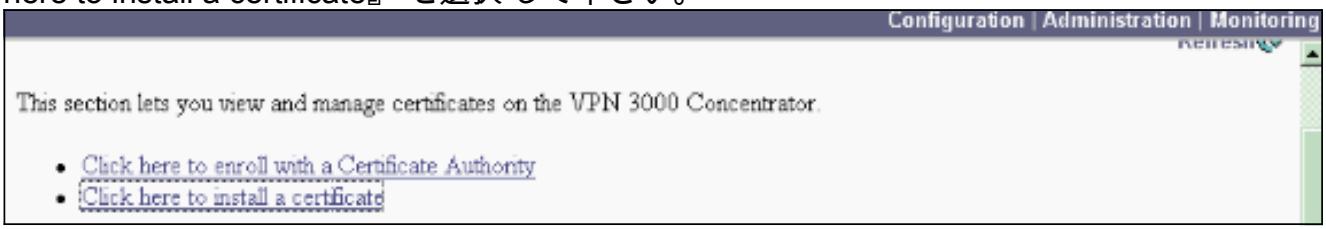


VPN 3000 コンセントレータの設定

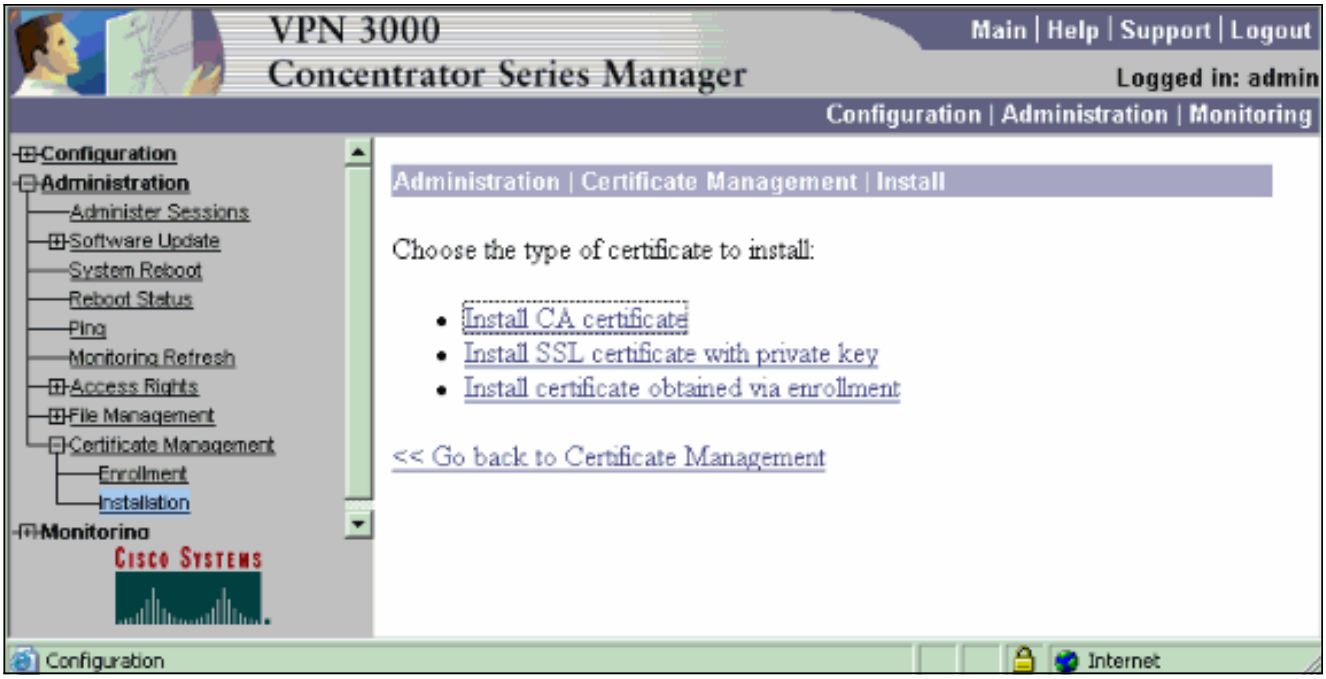
手順説明

VPN 3000 コンセントレータを設定するためにこれらのステップを完了して下さい:

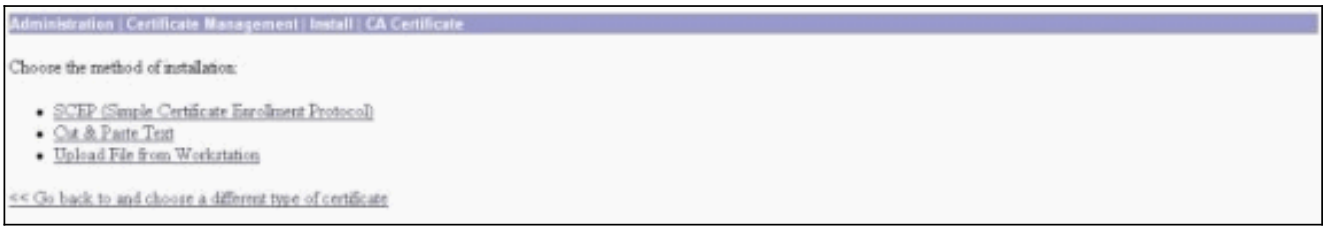
1. 証明書がない場合証明書を要求するために Administration > Certificate Management の順に選択 して下さい。VPN コンセントレータでルート証明をインストールするために『Click here to install a certificate』 を選択 して下さい。



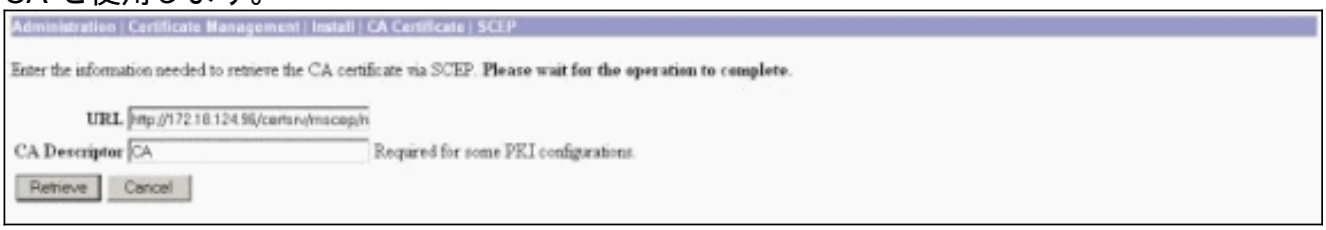
2. 『Install CA certificate』 を選択 して下さい。



3. CA 証明書を取得するために『SCEP（Simple Certificate Enrollment Protocol）』を選択して下さい。

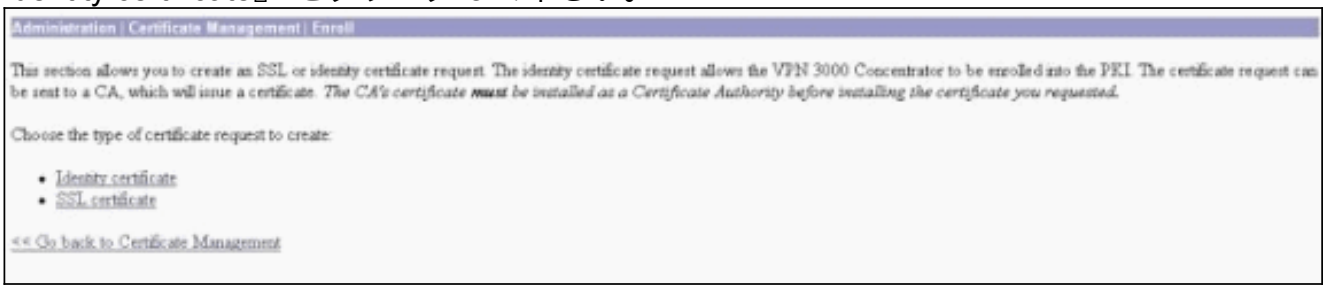


4. SCEP ウィンドウから、URL ダイアログボックスで CA サーバの完全な URL を入力して下さい。この例では、CA サーバの IP アドレスは 172.18.124.96 です。 この例が Microsoft の CA サーバを使用するので、完全な URL は http://172.18.124.96/certsrv/mscep/mscep.dll です。 次に、CA Descriptor ダイアログボックスで 1語記述子を入力して下さい。 この例は CA を使用します。

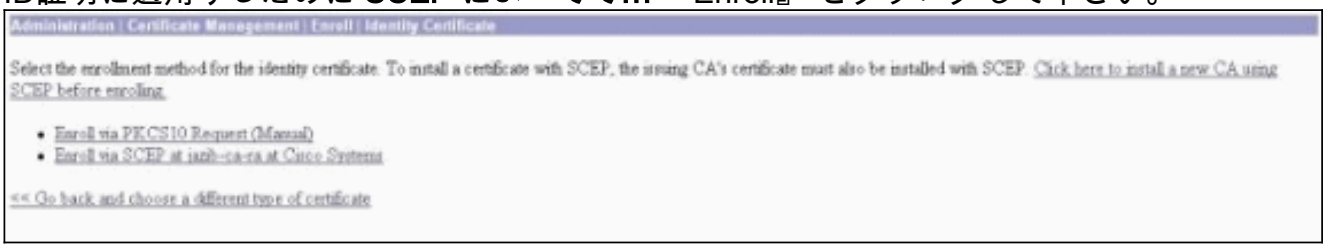


5. [Retrieve] をクリックします。CA 認証は Administration > Certificate Management ウィンドウの下で現われる必要があります。 証明書が表示されない場合、手順 1 に戻り、手順を繰り返します。

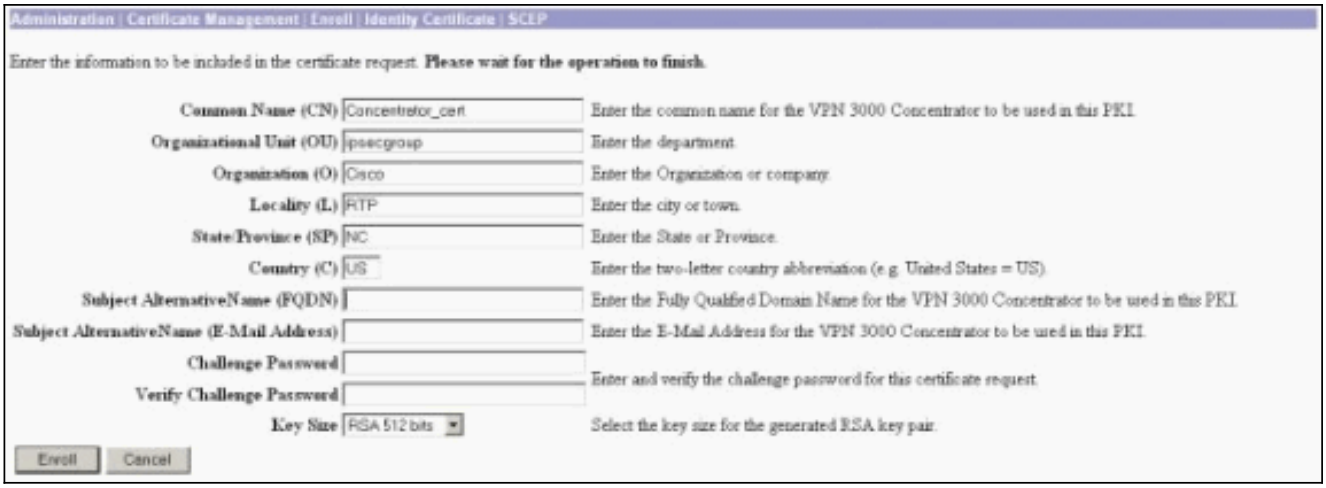
6. CA 認証があったら、Administration > Certificate Management > Enroll の順に選択 し、『 Identity certificate』 をクリック して下さい。



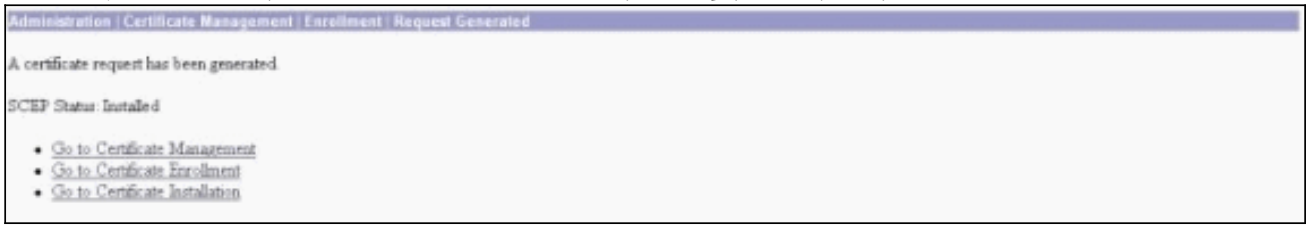
7. ID証明に適用するために **SCEP によってで...** 『Enroll』 をクリック して下さい。



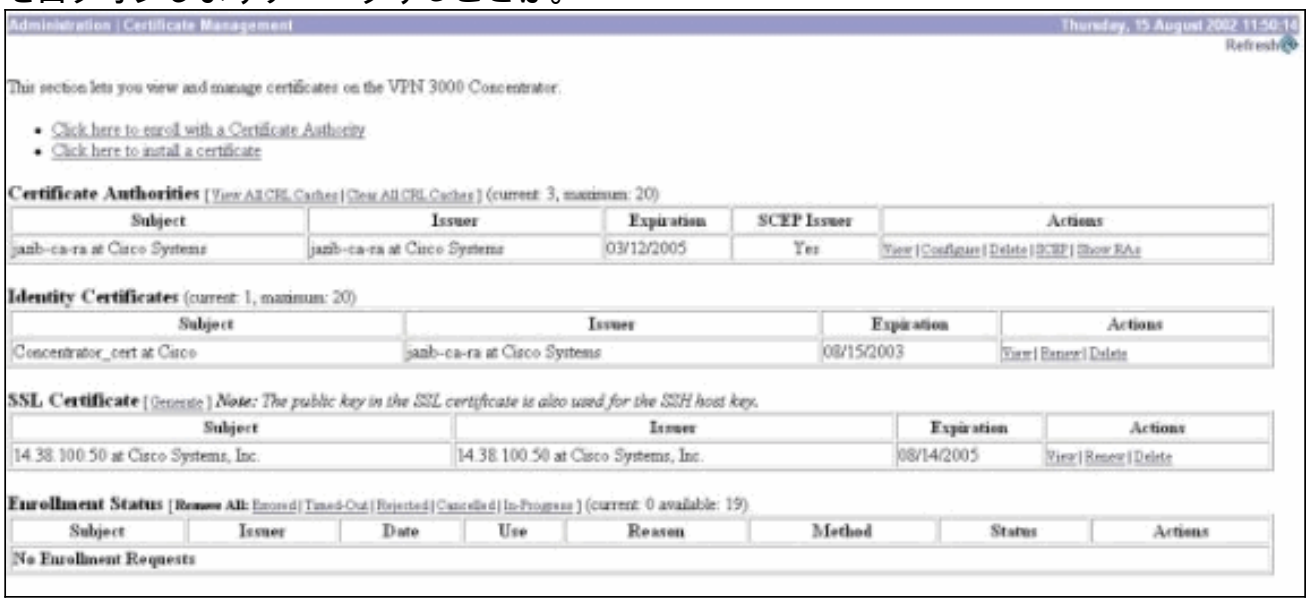
8. 登録書式に記入するためにこれらのステップを完了して下さい:Common Name （ CN ）フィールドで公開鍵インフラストラクチャ （ PKI ）で使用されるべき VPN コンセントレータのための Common Name を入力して下さい。Organizational Unit （ OU ）フィールドで部門を入力して下さい。 OU は設定された IPSec グループ名を一致する必要があります。組織（ o ）フィールドで組織か会社を入力して下さい。局所性（ l ）フィールドで都市か町を入力して下さい。State/Province （ SP ）フィールドで状態か地域を入力して下さい。国（ c ）フィールドで国を入力して下さい。完全修飾ドメイン名 （ FQDN ）フィールドで PKI で使用されるべき VPN コンセントレータのための完全修飾ドメイン名 （ FQDN ）を入力して下さい。認証対象代替名（ e メールアドレス）フィールドで PKI で使用されるべき VPN コンセントレータのための e メールアドレスを入力して下さい。Challenge Password フィールドで証明書要求のためのチャレンジ パスワードを入力して下さい。Verify Challenge Password フィールドでチャレンジ パスワードをもう一度入力して下さい。キーサイズ ドロップダウン リストから作成された RSA キーペアにキーサイズを選択して下さい。



9. ポーリング状態の SCEP ステータスを『Enroll』 を選択 し、表示して下さい。
10. CA サーバに移動し、アイデンティティ証明書を承認します。 それが CA サーバで承認されれば、SCEP ステータスはインストールする必要があります。



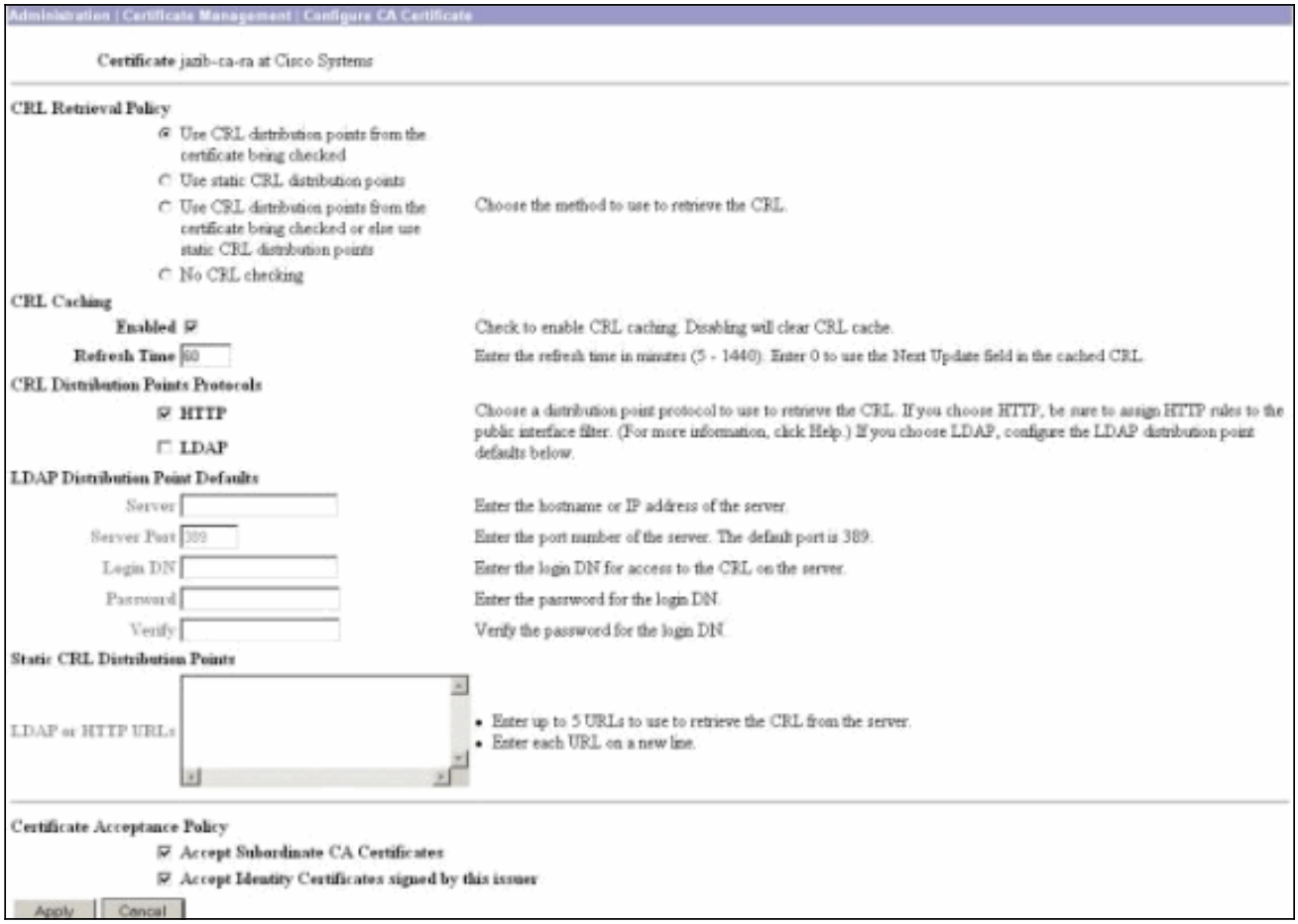
11. 証明書管理の下で、ID証明を見るはずです。場合、トラブルシューティングの CA サーバを口グオンしますチェックすることは。



12. 証明書に CRL Distribution Point （CDP）があるかどうか見るために受け取った証明書で『View』 を選択 して下さい。CDP はこの証明書の発行元からのすべての CRL ディストリビューション ポイントをリストします。 証明書の CDP がある、および CA サーバにクエリーを送信したらのに DNS名を使用したら場合- IP アドレスの… VPN コンセントレータで DNSサーバをホスト名を変換するために定義してもらうことを確かめて下さい。 この場合、例 CA サーバのホスト名は DNSサーバの 172.18.124.96 の IP アドレスに解決する jazib パソコンです。

13. 受け取った証明書の CRLチェックをイネーブルにするために CA 認証で『Configure』 をクリック して下さい。受け取った証明書の CDP があり、それを使用するために望んだら『Use CRL distribution points from the certificate being checked』 を選択 して下さい。システムがネットワーク ディストリビューション ポイントから CRL を取得し、検査しなければならないので CRLチェックをイネーブルにすることはシステム 応答時間を遅らせるかもしれません。 またネットワークが遅いですまたは混雑させる、CRLチェックは失敗するかもしれません。 これらの潜在的な問題を軽減するイネーブル CRL キャッシング。 従ってこれはローカル揮発性 メモリで取得された CRL を保存し、VPN コンセントレータが証明書の取り消しのステータスをもっとすぐに確認するようにします。イネーブルになられていて CRL キャッシュが VPN コンセントレータは証明書の取り消しのステータスをチェックする必要があるときかどうかキャッシュで存在 する必須 CRL まずチェックし、CRL のシリアル番号のリストに対して証明書のシリアル番号をチェックします。 証明書はシリアル番号がある場合取り消されたと考えられます。 VPN コンセントレータは外部サーバからキャッシュされた CRL の有効期間が切れたらか、または設定されたリフレッシュ 時間が経過したらときキャッシュの必須 CRL を見つけない CRL をどちらか取得します。 VPN コンセントレータは外部サーバから新しい CRL を受け取るとき、新しい CRL のキャッシュをアップデートします。 キャッシュは 64 まで CRL が含まれている場合があります。**注**: メモリで存在 する CRL キャッシュ。 従って、VPN コンセントレータをリブートすることは CRL キャッシュを消去します。 VPN コンセントレータはそれとして更新済 CRL の CRL キャッシュを処理します新しい ピア認証要求を再読み込みします。『Use static CRL distribution points』 を選択 する場合、このウィンドウで規定 されるように 5 つまでの静的な CRL ディストリビューション ポイントを、使用できます。 このオプションを選択する場合、少なくとも 1 URL を入力して下さい。また『Use CRL distribution points from the certificate being checked』 を選択 することができますまたは『Use static CRL distribution points』 を選択 して下さい。 VPN コンセントレータが証明書の 5 つの CRL ディストリビューション ポイントを見つけることができない場合 5 の限界まで静的な CRL ディストリビューション ポイントを、追加します。 このオプションを選択する場合、少なくとも 1 つの CRL Distribution Point プロトコルを有効に して下さい。 また少なくとも 1 つの (および以上 5) 静的な CRL ディストリビューション ポイントを入力して下さい。CRLチェックを無効に したいと思ったら『No CRL Checking』 を選択 して下さい。CRL キャッシングの下で、VPN コンセントレータが取得された CRL をキャッシュするように**イネーブルになった**ボックスを選択して下さい。 デフォルトは CRL キャッシングを有効に することではないです。 CRL キャッシングを (ボックスを選択解除にして下さい) 無効に する時、CRL キャッシュは消去されます。チェックされる証明書からの CRL ディストリビューション ポイントを使用する CRL 検索ポリシーを設定したら CRL を取得するのに使用するようにディストリビューション ポイント プロトコルを選択して下さい。 CRL を取得するた

めにこの場合『HTTP』 を選択 して下さい。 CA サーバがパブリックインターフェイスの方にある場合パブリックインターフェイス フィルタに HTTP ルールを割り当てて下さい。



モニタリング

すべての CRL キャッシュを Administration > Certificate Management の順に選択 し、VPN コンセントレータが CA サーバからの CRL をキャッシュしたかどうか見るために『View』 をクリック して下さい。

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

コンセントレータからのログ

CRLチェックがはたらくことを確かめることを VPN コンセントレータのこれらのイベントが可能にして下さい。

1. ログ レベルを設定するために Configuration > System > Events > Classes の順に選択 して下さい。
2. クラスネームの下で **IKE**、**IKEDBG**、**IPSEC**、**IPSECDBG**、または **CERT を**選択して下さい。
3. **追加しか**、または**修正し**、『Severity to Log option 1-13』 を選択 しますクリックして下さい。
4. 修正したいと思ったら『Apply』 をクリック して下さいまたは New エントリを追加したい

と思う場合**追加して下さい。**

正常なコンセントレータ ログ

CRLチェックが正常である場合、これらのメッセージはフィルタリング可能イベントログで見られます。

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2

1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)

1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

正常なコンセントレータ ログの完全な出力のための正常なコンセントレータ ログを参照して下さい。

壊れるログ

成功しなかったの CRLチェックがフィルタリング可能イベントログで、これらのメッセージ見られれば。

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5

1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.

1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

壊れるコンセントレータ ログの完全な出力のための取り消された コンセントレータ ログを参照して下さい。

正常なクライアント ログの完全な出力のための正常なクライアント ログを参照して下さい。

壊れるクライアント ログの完全な出力のための取り消された クライアント ログを参照して下さい。

トラブルシューティング

トラブルシューティング情報詳細については VPN 3000 コンセントレータの接続に関する問題のトラブルシューティングを参照して下さい。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 クライアントに関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems