識別名ベースのクリプト マップ

機能の履歴

リリース	変更点
12.2(4)T	この機能が追加されました。

この章では、Cisco IOS Release 12.2(4)T の識別名ベースのクリプト マップ機能について説明します。次の項で構成されています。

- 「機能の概要」（P.1）
- 「サポートされているプラットフォーム」（P.2）
- 「サポートされている規格、MIB、および RFC」（P.3）
- 「前提条件」（P.3）
- 「設定作業」（P.3）
- 「設定例」（P.5）
- 「コマンド リファレンス」（P.6）

機能の概要

識別名ベースのクリプト マップ機能により、証明書（特に特定の識別名（DN）持つ特定の証明書）を持つピアの選択された暗号化インターフェイスだけに、アクセスを制限するようにルータを設定できます。

以前まで、暗号化ピアからルータが証明書または共有秘密を受け入れる場合、Cisco IOS では暗号化ピアの IP アドレスによって制限する以外、ピアが暗号化インターフェイスと通信するのを防ぐ方法がありませんでした。この機能により、ピアが自身の認証に使用した DN に基づいて、ピアが使用できるクリプト マップを設定し、特定の DN を持つピアがアクセスできる暗号化インターフェイスを制御できます。

利点

識別名ベースのクリプト マップ機能では、暗号化インターフェイスを選択し、特定の証明書（なかでも特別な DN を持つ証明書）を持つピアがそのインターフェイスにアクセスしないよう、ルータに制限を設定できます。

制約事項

システム要件

この機能を設定するには、ルータが IP セキュリティをサポートする必要があります。

パフォーマンス上の影響

アクセスを制限する DN が多い場合、少数のアイデンティティ セクションを参照する多数のクリプト マップを指定するよりも、多数のアイデンティティ セクションを参照する少数のクリプト マップを指定することを推奨します。

関連資料

次のマニュアルには、識別名ベースのクリプト マップ機能の関連情報が記載されています。

- 『*Cisco IOS Security Command Reference*』
- 『*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T*』

サポートされているプラットフォーム

この機能は、次のプラットフォームでサポートされます。

- Cisco 1700 シリーズ
- Cisco 2600 シリーズ
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 シリーズ
- Cisco 7200 シリーズ
- Cisco uBR905 ケーブル アクセス ルータ
- Cisco uBR925 ケーブル アクセス ルータ

Feature Navigator を使用したプラットフォーム サポートの判別

Cisco IOS ソフトウェアは、特定のプラットフォームがサポートされている機能セットにパッケージングされています。この機能のプラットフォーム サポートに関する最新情報を入手するには、Feature Navigator にアクセスしてください。新しいプラットフォーム サポートが機能に追加されると、Feature Navigator によって、サポートされているプラットフォームのリストが自動的に更新されます。

Feature Navigator は Web ベースのツールであり、特定の機能セットがサポートされている Cisco IOS ソフトウェア イメージ、および、特定の Cisco IOS イメージ内でサポートされている機能を素早く特定できます。

Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、http://www.cisco.com/register にある指示に従って、Cisco.com 上にアカウントを作成できます。

Feature Navigator は定期的に更新されています（Cisco IOS ソフトウェアの主要なリリース時およびテクノロジー リリース時）。最新情報については、次の URL から Feature Navigator ホームページにアクセスしてください。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

サポートされている規格、MIB、および RFC

規格

なし

MIB

なし

選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

RFC

なし

前提条件

DN ベースのクリプト マップを設定する前に、次の作業を実行する必要があります。

- ピアごとに IKE ポリシーを作成します。

  IKE ポリシーの作成に関する詳細については『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「*Configuring Internet Key Exchange for IPsec VPNs*」の章を参照してください。
- IPSec のクリプト マップ エントリを作成します。

  クリプト マップ エントリの作成に関する詳細については『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「*Configuring Security for VPNs with IPsec*」の章を参照してください。

設定作業

クリプト マップ エントリの作成に関する詳細については、「IPsec VPN のセキュリティの設定」を参照してください。一覧内の各作業は、必須と任意に分けています。

- 「（DN によって認証された）DN ベースのクリプト マップの設定」（必須）
- 「（ホスト名によって認証された）DN ベースのクリプト マップの設定」（必須）
- 「DN ベースのクリプト マップへのアイデンティティの適用」（必須）
- 「DN ベースのクリプト マップの確認」（任意）

（DN によって認証された）DN ベースのクリプト マップの設定

DN によって認証されたピアだけが使用できる DN ベースのクリプト マップを設定するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto identity name`	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。
ステップ 2	`Router(crypto-identity)# dn name=string [,name=string]`	ルータの証明書内にある DN に、ルータのアイデンティティを関連付けます。 （注） ピアのアイデンティティは、交換された証明書のアイデンティティと一致する必要があります。

（ホスト名によって認証された）DN ベースのクリプト マップの設定

ホスト名によって認証されたピアだけが使用できる DN ベースのクリプト マップを設定するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto identity name`	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。
ステップ 2	`Router(crypto-identity)# fqdn name`	ピアの認証に使用したホスト名にルータのアイデンティティを関連付けます。 （注） ピアのアイデンティティは、交換された証明書のアイデンティティと一致する必要があります。

DN ベースのクリプト マップへのアイデンティティの適用

（クリプト マップのコンテキスト内で）アイデンティティを適用するには、グローバル コンフィギュレーション モードの開始時に次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# crypto map map-name seq-num ipsec-isakmp`	クリプト マップ エントリを作成または変更し、クリプト マップ コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-crypto-map)# identity name`	クリプト マップに対して ID を適用します。 このコマンドが適用されると、**identity** *name* 内に表示された設定と一致するホストだけが指定のクリプト マップを使用できます。 **（注）** クリプト マップ内に **identity** コマンドが表示されない場合は、暗号化ピアの IP アドレスを除き、暗号化接続に制約はありません。

DN ベースのクリプト マップの確認

この機能が適切に設定されているかを確認するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# show crypto identity`	設定したアイデンティティを表示します。

トラブルシューティングのヒント

暗号化ピアが接続を確立しようと試み、それが DN ベースのクリプト マップ設定によってブロックされた場合、次のエラー メッセージが記録されます。

```
<time>: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT: encrypted connection attempted with a peer
without the configured certificate attributes.
```

設定例

ここでは、次の設定例について説明します。

- 「DN ベースのクリプト マップ設定例」

DN ベースのクリプト マップ設定例

次の例では、DN およびホスト名によって認証された DN ベースのクリプト マップを設定する方法を示します。間にコマンドを説明するためのコメントが含まれています。

```
! DN based crypto maps require you to configure an IKE policy at each peer.
crypto isakmp policy 15
 encryption 3des
 hash md5
 authentication rsa-sig
 group 2
 lifetime 5000
crypto isakmp policy 20
 authentication pre-share
 lifetime 10000
crypto isakmp key 1234567890 address 171.69.224.33
!
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
!
```

コマンド リファレンス

この機能に関連して、次の新しいコマンドが追加されています。これらのコマンドおよびこの機能に使用されているその他のコマンドのコマンド ページを参照するには、『*Cisco IOS Master Commands List*』（http://www.cisco.com/en/US/products/ps6441/products_product_indices_list.html）にアクセスしてください。

- **crypto identity**
- **dn**
- **fqdn**
- **identity**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『Master Command List』を参照してください。