識別名ベースのクリプト マップ

機能の履歴

リリース	変更内容
12.2(4)T	この機能が導入されました。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

この章では、Cisco IOS Release 12.2(4)T の識別名ベースの暗号マップ機能について説明します。次のセクションで構成されています。

- 機能の概要 （1 ページ）
- サポートされるプラットフォーム （2 ページ）
- サポートされている規格 MIB および RFC （3 ページ）
- 前提条件 （3 ページ）
- 設定作業 （3 ページ）
- 設定例 （6 ページ）

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、暗号化されたインターフェイスとピアが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

識別名ベースの暗号マップ機能では、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。

機能制限

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』
- Next Generation Encryption （NGE）ホワイトペーパー。

サポートされ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

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

サポートされている規格 MIB および RFC

標準

なし

MIB

なし

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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 ポリシーの作成についての詳細は、『*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。

暗号マップエントリの作成についての詳細は、『*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 ベースの暗号マップの設定 （4 ページ） （必須）
- （ホスト名によって認証された）DN ベースの暗号マップの設定 （4 ページ） （必須）

- DN ベースの暗号マップへの ID の適用 （5 ページ） （必須）
- DN ベースの暗号マップの確認 （5 ページ） （任意）

（DN によって認証された）DN ベースの暗号マップの設定

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。

手順の概要

1. Router(config)# **crypto identity** *name*
2. Router(crypto-identity)# **dn** *name=string* [,*name=string*]

手順の詳細

	コマンドまたはアクション	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 ベースの暗号マップの設定

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。

手順の概要

1. Router(config)# **crypto identity** *name*
2. Router(crypto-identity)# **fqdn** *name*

手順の詳細

	コマンドまたはアクション	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

	コマンドまたはアクション	目的
		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 ベースの暗号マップへの ID 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。

手順の概要

1. Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp**
2. Router(config-crypto-map)# **identity** *name*

手順の詳細

	コマンドまたはアクション	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。 このコマンドを適用した場合、**identity** *name* でリストされているコンフィギュレーションと一致するホストだけが、指定した暗号マップを使用できます。 （注） 暗号マップ内に **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 ベースの暗号マップの確認

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

DN ベースの暗号マップの設定例

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 aes
 hash sha
 authentication rsa-sig
 group 14
 lifetime 5000
crypto isakmp policy 20
 encryption aes
 hash sha
 authentication pre-share
 group 14
 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
!
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。