AES を使用した Cisco VPN 3000 コンセントレータとルータの間の LAN-to-LAN IPSec トンネルの設定例

目次

はじめに

このドキュメントでは、Advanced Encryption Standard（AES; 高度暗号化規格）を暗号化アルゴリズムとして使用する、Cisco VPN 3000 コンセントレータと Cisco ルータの間の IPsec トンネルの設定方法について説明します。

AES は、National Institute of Standards and Technology（NIST; 国立標準技術研究所）により暗号化方式として使用されるよう作成された、Federal Information Processing Standard（FIPS: 連邦情報処理標準）公示による新しい標準方式です。 この標準では、Data Encryption Standard（DES; データ暗号規格）を置き換える AES 対称暗号化アルゴリズムを、IPsec と Internet Key Exchange（IKE; インターネット キー エクスチェンジ）両方のプライバシー トランスフォームとして指定しています。 AES には、128 ビット キー（デフォルト）、192 ビット キー、256 ビット キーの 3 つの異なるキー長があります。 Cisco IOS(R) での AES 機能には、新しい暗号化標準である AES のサポートと Cipher Block Chaining（CBC）モードが IPsec に追加されています。

AES に関する 詳細については NIST Computer Security Resource Center のサイトを参照して下さい。

VPN 3000 コンセントレータと PIX Firewall の間の LAN-to-LAN トンネル設定の詳細については、『Cisco VPN 3000 コンセントレータと PIX ファイアウォール の間の LAN-to-LAN IPSec トンネルの設定例』を参照してください。

PIX がソフトウェア バージョン 7.1 を使用している場合の詳細については、『PIX 7.x と VPN 3000 コンセントレータの間の IPsec トンネルの設定例』を参照してください。

前提条件

要件

このドキュメントの内容は、IPsec プロトコルに関する基本的知識が前提となっています。 IPsec に関する知識を深めるには、『IP Security (IPSec) 暗号化の概要』を参照してください。

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。

- ルータの要件 - AES 機能は、Cisco IOS ソフトウェア リリース 12.2(13)T で導入されています。 AES を有効にするには、ルータは IPsec をサポートしていて、「k9」の長さのキーをサポートする IOS イメージが稼働している必要があります (「k9」サブシステム) 。**注:** Cisco 2600XM、2691、3725、および 3745 AES アクセラレーション VPN モジュールでは、AES に対するハードウェア サポートも利用可能です。 この機能には設定上の考慮事項はなく、両方が使用可能である場合はハードウェア モジュールが自動的に選択されます。
- VPN コンセントレータの要件 - AES 機能に対するソフトウェア サポートは、リリース 3.6 で導入されています。 ハードウェア サポートは、新しい拡張型スケーラブル暗号化プロセッサ (SEP-E) により提供されます。 この機能には設定上の考慮事項はありません。**注:** Cisco VPN 3000 コンセントレータ リリース 3.6.3 では、Cisco Bug ID CSCdy88797 (登録ユーザ専用) の問題により、トンネルでは AES とのネゴシエーションが行われません。 この問題は、リリース 3.6.4 以降では解決されています。**注:** Cisco VPN 3000 コンセントレータでは SEP モジュールと SEP-E モジュールのいずれかが使用されますが、両方は使用されません。 同じデバイスに両方のモジュールをインストールしないでください。 すでに SEP モジュールが含まれている VPN コンセントレータに SEP-E モジュールをインストールすると、VPN コンセントレータでは SEP モジュールが無効になり、SEP-E モジュールのみが使用されます。

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。

- Cisco IOS ソフトウェア リリース 12.3(5) が稼働する Cisco 3600 シリーズ ルータ
- ソフトウェア リリース 4.0.3 が稼働する Cisco VPN 3060 コンセントレータ

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。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

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。

設定

このドキュメントでは、次の設定を使用します。

- IPSec ルータ
- VPN コンセントレータ

ipsec_router の設定

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
```

```
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

注: ACL 構文に変更はありませんが、暗号化 ACL では意味が少々異なります。 暗号化 ACL では、permit は一致するパケットを暗号化する必要があることを指定しますが、一方 deny は一致するパケットを暗号化する必要がないことを指定します。

VPN コンセントレータの設定

VPN コンセントレータは、工場出荷時に IP アドレスが事前にプログラムされていません。 コンソール ポートを使用して、メニューベースの Command-Line Interface (CLI; コマンドライン インターフェイス) である初期設定を行う必要があります。 コンソール経由で設定を行う方法の詳

細は、『コンソール経由での VPN コンセントレータの設定』を参照してください。

イーサネット 1（プライベート）インターフェイス上の IP アドレスが設定された後、残りの要素は CLI を使用するか、ブラウザ インターフェイスを介して設定できます。 ブラウザ インターフェイスでは HTTP と HTTP over Secure Socket Layer（SSL）の両方がサポートされています。

次のパラメータは、コンソールを使用して設定されます。

- Time/Date - 正確な時刻と日付が非常に重要です。 これによりロギングとアカウンティングのエントリが正確になり、システムが有効なセキュリティ認証を作成するのに役立ちます。
- Ethernet 1 (private) interface - IP アドレスおよびマスク（このドキュメントのネットワークトポロジでは 172.16.1.1/24）。

この段階で、VPN コンセントレータは、内部ネットワークから HTML ブラウザによってアクセスできます。 CLI モードでの VPN コンセントレータの設定の詳細は、『CLI を使用したクイックコンフィギュレーション』を参照してください。

1. Web ブラウザからプライベート インターフェイスの IP アドレスを入力し、GUI インターフェイスを有効にします。save needed アイコンをクリックして、変更をメモリに保存します。 工場出荷時のデフォルトのユーザ名とパスワードは「admin」で、大文字と小文字が区別されます。
2. 始動 GUI、> イーサネット 2 インターフェイスを設定する**イーサネット 2（パブリック）** Configuration > Interfaces の順に選択 した後。
3. >IP Routing > Default Gateways をプライベート ネットワークの他のサブネットに到達するために設定します IPsec のためのデフォルト（インターネット）ゲートウェイおよびトンネル デフォルト（中）ゲートウェイを Configuration > System の順に選択 して下さい。このシナリオでは、内部ネットワーク上では 1 つのサブネットのみ使用できます。
4. 暗号化されるべきトラフィックを定義するネットワークリストを作成するために > Network Lists > Add を Configuration > Policy Management > Traffic Management の順に選択 して下さい。このリストに記載されているネットワークは、リモート ネットワークに到達できます。 次のリストに示されているネットワークが Local ネットワークです。 Generate Local List をクリックすると、RIP を介して Local ネットワーク リストを自動的に生成することもできます。
5. このリストのネットワークはリモート ネットワークであり、手動で設定する必要があります。 これを行うには、到達可能な各サブネットのネットワーク/ワイルドカードを入力します。完了時の 2 つのネットワーク リストは次のとおりです。
6. LAN-to-LAN トンネルを Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add の順に選択 し、定義して下さい。このウィンドウには 3 つのセクションがあります。 上部のセクションはネットワーク情報用で、下部の 2 つのセクションは Local および Remote ネットワーク リスト用です。 Network Information セクションで、AES 暗号化、認証タイプ、IKE プロポーザルを選択し、事前共有キーを入力します。 下部のセクションで、すでに作成した Network リスト（それぞれ Local リストと Remote リストの両方）を指定します。
7. Add をクリックした後、接続が正しい場合、IPSec LAN-to-LAN-Add-Done ウィンドウが表示されます。このウィンドウにはトンネル設定情報の概要が表示されます。 また、Group Name、SA Name、および Filter Name が自動的に設定されます。 この表では任意のパラメータを編集できます。この時点で IPsec LAN-to-LAN トンネルが設定され、作業を開始できます。 何らかの理由でトンネルが機能しない場合は設定ミスをチェックできます。
8. **LAN-to-LAN** Configuration > System > Tunneling Protocols > IPsec の順に選択 するとき作成された LAN-to-LAN IPSec パラメータを以前に表示または修正できます。次の図ではトン

ネルの名前として「test」が表示され、またリモート エンドのパブリック インターフェイスはシナリオに従って 30.30.30.1 となっています。

9. IKE プロポーザルが Inactive Proposals リスト内にある場合、時としてトンネルがアップ状態にならない場合があります。 アクティブIKE 提案を設定するために Configuration > System > Tunneling Protocols > IPSec > IKE Proposals の順に選択 して下さい。IKE プロポーザルが「Inactive Proposals」リスト内にある場合、その IKE プロポーザルを選択して Activate ボタンをクリックすると、それを有効にできます。 次の図では、選択されたプロポーザル「IKE-AES256-SHA」が Active Proposals リスト内にあります。
10. SA パラメータが正しいかどうか確認するために Configuration > Policy Management > Traffic Management > Security Associations の順に選択 して下さい。
11. SA 名前をクリックして下さい（この場合、**L2L: テストは**）、それから SAS を確認するために『Modify』 をクリック し。パラメータの一部がリモート ピアの設定と一致しない場合、ここで変更できます。

確認

ルータの設定の確認

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。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto isakmp sa**：現在ピアにあるすべての IKE SA を表示します。 状態 QM_IDLE は、SA がピアと認証された状態であり、後続のクイック モードの交換に使用できることを示します。 そのため、現在はアイドル状態にあります。

```
ipsec_router#show crypto isakmp sa

 dst             src             state    conn-id   slot

 20.20.20.1      30.30.30.1      QM_IDLE        1      0
```

- **show crypto ipsec sa**：現在の SA で使用されている設定を表示します。 ピア IP アドレス、ローカルとリモートの両端のアクセスが可能なネットワーク、および使用されている変換セットをチェックします。 2 つの ESP SA が、各方向に 1 つずつあります。 AH 変換セットは使用されているため、空の状態です。

```
ipsec_router#show crypto ipsec sa

interface: Ethernet1/0

        Crypto map tag: vpn, local addr. 30.30.30.1

        protected vrf:

         local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

        remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

        current_peer: 20.20.20.1:500

          PERMIT, flags={origin_is_acl,}

         #pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145
```

```
 #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

 #pkts compressed: 0, #pkts decompressed: 0

 #pkts not compressed: 0, #pkts compr. failed: 0

 #pkts not decompressed: 0, #pkts decompress failed: 0

 #send errors 6, #recv errors 0

 local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

 path mtu 1500, media mtu 1500

 current outbound spi: 54FA9805

inbound esp sas:

spi: 0x4091292(67703442)

 transform: esp-256-aes esp-md5-hmac ,

 in use settings ={Tunnel, }

 slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

 sa timing: remaining key lifetime (k/sec): (4471883/28110)

 IV size: 16 bytes

 replay detection support: Y

inbound ah sas:

inbound pcp sas:

 outbound esp sas:

spi: 0x54FA9805(1425709061)

 transform: esp-256-aes esp-md5-hmac ,

 in use settings ={Tunnel, }

 slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn

 sa timing: remaining key lifetime (k/sec): (4471883/28110)

 IV size: 16 bytes

 replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

- show crypto engine connections active - すべての暗号化エンジンに対する現在アクティブな暗号化セッション接続を表示します。 接続 ID はそれぞれ固有のものです。 暗号化および復号化されるパケットの数が最後の 2 つのカラムに表示されます。

```
ipsec_router#show crypto engine connections active
   ID     Interface     IP-Address   State   Algorithm          Encrypt Decrypt

    1     Ethernet1/0   30.30.30.1   set     HMAC_SHA+AES_256_C       0       0
```

```
2000      Ethernet1/0    30.30.30.1    set      HMAC_MD5+AES_256_C        0       19

2001      Ethernet1/0    30.30.30.1    set      HMAC_MD5+AES_256_C       19        0
```

VPN コンセントレータの設定の確認

VPN コンセントレータの設定を確認するには、次の手順を実行します。

1. VPN コンセントレータで Monitoring > Statistics > IPsec の順に選択 するときルータの **show crypto ipsec sa** および **show crypto isakmp sa コマンド**に類似した、IPsec および IKE 統計情報を表示できます。
2. ルータ上の show crypto engine connections active コマンドと同じように、VPN コンセントレータ上の Administration-Sessions ウィンドウを使用すると、すべてのアクティブな IPsec LAN-to-LAN 接続またはトンネルのパラメータと統計を表示できます。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

ルータのトラブルシューティング

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto engine**：暗号化されたトラフィックを表示します。 暗号化エンジンは、暗号化と復号化を実行する実際のメカニズムです。 暗号化エンジンは、ソフトウェアであることも、あるいはハードウェア アクセラレータであることも可能です。
- **debug crypto isakmp** — IKE フェーズ 1.の Internet Security Association and Key Management Protocol（ISAKMP）ネゴシエーションを表示します。
- **debug crypto ipsec** — IKE フェーズ 2.の IPsec ネゴシエーションを表示します。

詳細情報とサンプル出力については、『IPSec のトラブルシューティング - debug コマンドの理解と使用』を参照してください。

VPN コンセントレータのトラブルシューティング

Ciscoルータの **debug コマンド**に類似した、すべてのアラームを表示するためにイベント クラスを設定できます。

1. イベント クラスの記録を回すために Configuration > System > Events > Classes > Add の順に選択 して下さい。IPsec に使用可能なクラスは次のとおりです。IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE
2. 上記のクラスを追加する際、アラームが送信される Severity レベルに基づいて、各クラスの Severity レベルを選択することもできます。アラームは、次のいずれかの方式により処理できます。ログコンソール上での表示UNIX Syslog サーバへの送信電子メールとして送信 Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）サーバへトラップとして送信

3. イネーブルになったアラームを監視するために Monitoring > Filterable Event Log の順に選択 して下さい。

関連情報

- Advanced Encryption Standard (AES)
- DES/3DES/AES VPN 暗号化モジュール
- VPN コンセントレータ ソフトウェアのアップグレード
- VPN コンセントレータ - リリース ノート
- IP インターフェースを設定する VPN コンセントレータ
- IPSec の設定例
- 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 シリーズ 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 プロトコルに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems