ASA IPsec および IKE デバッグ（IKEv1 アグレッシブ モード）のトラブルシューティングに関するテクニカル ノート

内容

概要

このドキュメントでは、アグレッシブ モードおよび事前共有キー（PSK）の両方を使用する場合の Cisco 適応型セキュリティ アプライアンス（ASA）のデバッグについて説明します。設定への特定のデバッグ行の変換についても説明します。このドキュメントの読者は IPsec およびインターネット キー エクスチェンジ（IKE）に関する基本的な知識を持っていることを推奨します。

このドキュメントでは、トンネルが確立した後の通過トラフィックについては説明しません。

主な問題

IKE および IPsec のデバッグはわかりにくいことがありますが、これらのデバッグを使用して、IPsec VPN トンネル確立の問題を理解できます。

シナリオ

アグレッシブモードは通常、ソフトウェア(Cisco VPN Client)とハードウェアクライアント(Cisco ASA 5505適応型セキュリティアプライアンスまたはCisco IOS?ソフトウェアルータなど)を使用しますが、事前共有キーが使用されている場合にのみ使用されます。メイン モードとは異なり、アグレッシブ モードは 3 つのメッセージで構成されます。

デバッグは、ソフトウェア バージョン 8.3.2 を実行し、EzVPN サーバとして機能する ASA から

行われます。EzVPN クライアントは、ソフトウェア クライアントです。

使用した debug コマンド

このドキュメントで使用する debug コマンドは次のとおりです。

```
debug crypto isakmp 127
debug crypto ipsec 127
```

ASA の設定

この例での ASA の設定は非常に基本的であり、外部サーバは使用されません。

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

デバッグ

注：debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。

サーバ メッセージの説明
クライアントから AM1 を受信します。

AM1を処理します。受信したプロポーザルとトランスフォームを、すでに一致するように設定されてい
関連コンフィギュレーション：
ISAKMP はインターフェイスで有効になっており、クライアントが送信したものと一致するポリシーが
されています。

```
crypto isakmp enable
outside
crypto isakmp policy
10
authentication pre-
share
encryption aes
hash sha
group 2
lifetime 86400
```

ID 名と一致するトンネル グループが存在します。

```
tunnel-group EZ type
remote-access
tunnel-group EZ
general-attributes
default-group-policy
EZ
tunnel-group EZ ipsec-
attributes
pre-shared-key cisco
```

AM2を構成します。このプロセスには次のものが含まれます。
- 選択されたポリシー
- Diffie-Hellman（DH）
- レスポンダ ID
- 認証
- ネットワーク アドレス変換（NAT）検出ペイロード

AM2 を送信します。

クライアントから AM3 を受信します。
AM3 を処理します。 NAT トラバーサル (NAT-T) の使用を確認します。両側でトラフィック暗号化を開 した。
フェーズ 1.5 (XAUTH) を開始して、ユーザ クレデンシャルを要求します。

ユーザ クレデンシャルを受信します。

ユーザ クレデンシャルを処理します。クレデンシャルを検証し、モード設定ペイロードを生成します。
関連コンフィギュレーション：

```
username cisco
password cisco
```

xauth の結果を送信します。

ACK を受信して処理します（「no response from server」）。

モード設定要求を受信します。
モード設定要求を処理します。 これらの値の多くは、通常グループ ポリシー内で設定されます。ただし、この例でのサーバは非常に基 め、ここでは表示しません。

設定されているすべての値を含むモード設定応答を構成します。
関連コンフィギュレーション：
この場合、ユーザには同じ IP が常に割り当てられることに注意してください。

```
username cisco
attributes
vpn-framed-ip-
address 192.168.1.100
255.255.255.0
group-policy EZ
internal
group-policy EZ
attributes
password-storage
enableddns-server value
192.168.1.129
vpn-tunnel-protocol
ikev1
split-tunnel-policy
tunnelall
split-tunnel-network-
list value split default-
domain value
jyoungta-
labdomain.cisco.com
```

モード設定応答を送信します。

フェーズ 1 がサーバで完了します。クイック モード (QM) プロセスを開始します。

クライアントの DPD を構成して送信します。

QM1 を受信します。

QM1 を処理します。
関連コンフィギュレーション：

```
crypto dynamic-map
DYN 10 set transform-
set TRA
```

QM2 を構成します。
関連コンフィギュレーション：

```
tunnel-group EZ
type remote-access !
(tunnel type ra = tunnel
type remote-access)
crypto ipsec transform-
set TRA esp-aes esp-
sha-hmac
crypto ipsec security-
association lifetime
seconds 28800
```

```
crypto ipsec security-
association lifetime
kilobytes 4608000
crypto dynamic-map
DYN 10 set transform-
set TRA
crypto map MAP 65000
ipsec-isakmp dynamic
DYN
crypto map MAP
interface outside
```

QM2 を送信します。

QM3 を受信します。

QM3を処理します。着信および発信セキュリティパラメータインデックス(SPI)を作成します。 ホストの
を追加します。
関連コンフィギュレーション：

```
crypto ipsec transform-
set TRA esp-aes esp-
sha-hmac
crypto ipsec security-
association lifetime
seconds 28800
crypto ipsec security-
association lifetime
kilobytes 4608000
crypto dynamic-map
DYN 10 set transform-
set TRA
crypto dynamic-map
DYN 10 set reverse-
route
```

フェーズ 2 が完了しました。両側で暗号化および復号化しています。

ハードウェア クライアントの場合は、クライアントが自らに関する情報を送信するメッセージを 1 つ以
深く確認すると、EzVPN クライアントのホスト名、クライアント上で実行されているソフトウェア、お
場所と名前がわかります。

トンネルの確認

ISAKMP

sh cry isa sa det コマンドの出力は次のとおりです。

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPSec

トンネルのトリガーには Internet Control Message Protocol（ICMP）が使用されるため、1 つの IPSec SA のみが起動されます。プロトコル 1 は ICMP です。SPI 値は、デバッグでネゴシエートされた値と異なることに注意してください。これは実際には、フェーズ 2 のキー再生成の後と同じトンネルです。

sh crypto ipsec sa コマンドの出力は次のとおりです。

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
 current_peer: 10.48.66.23, username: cisco
 dynamic allocated peer ip: 192.168.1.100

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: C4B9A77C
current inbound spi : EA2B6B15

inbound esp sas:
spi: 0xEA2B6B15 (3928714005)
transform: esp-aes esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 425984, crypto-map: DYN
sa timing: remaining key lifetime (sec): 28714
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000003F
outbound esp sas:
spi: 0xC4B9A77C (3300501372)
transform: esp-aes esp-sha-hmac no compression
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 425984, crypto-map: DYN
sa timing: remaining key lifetime (sec): 28714
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

関連情報

- IPsec に関する Wikipedia 記事
- IPSec のトラブルシューティング：debug コマンドの説明と使用
- テクニカル サポートとドキュメント – Cisco Systems