EzVPN-NEM から FlexVPN への移行ガイド

目次

概要
前提条件
要件
使用するコンポーネント
表記法
EzVPN と FlexVPN
EzVPN モデル - 特徴
トンネル ネゴシエーション
FlexVPN リモート アクセス VPN モデル
FlexVPN サーバ
IOS FlexVPN のクライアント認証方式
トンネル ネゴシエーション
初期設定
トポロジ
初期設定
EzVPN から FlexVPN への移行方法
移行したトポロジ
設定
FlexVPN の動作検証
FlexVPN サーバ
FlexVPN リモート
関連情報

概要

このドキュメントでは、EzVPN（インターネット キー エクスチェンジ v1（IKEv1））の 設定から FlexVPN（IKEv2）の設定への移行プロセスを、できるだけ問題なく実行するためのサポートを提供します。 IKEv2 リモート アクセスはいくつかの点で IKEv1 リモート アクセスとは異なるため、移行がやや難しくなります。このドキュメントは EzVPN モデルから FlexVPN リモートアクセス モデルに移行するうえで、さまざまな設計方法を選択するのに役立ちます。

このドキュメントでは IOS FlexVPN クライアント（ハードウェア クライアント）を取り上げており、ソフトウェア クライアントについては説明しません。 ソフトウェア クライアントの詳細については、次を参照してください。

- FlexVPN： 組み込みの Windows クライアントと証明書認証を備えた IKEv2
- FlexVPN および Anyconnect IKEv2 クライアントの設定例
- FlexVPN の展開： EAP-MD5 による AnyConnect IKEv2 リモート アクセス

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IKEv2
- Cisco FlexVPN
- Cisco AnyConnect セキュア モビリティ クライアント
- Cisco VPN Client

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

EzVPN と FlexVPN

EzVPN モデル - 特徴

名前からわかるように、EzVPN の目的は、リモート クライアントで VPN 設定を簡単に行うことです。 これを実現するには、正しい EZVPN サーバ（クライアント プロファイルとも言う）への接続に必要な詳細をできるだけ少なくしてクライアントを設定します。

トンネル ネゴシエーション

FlexVPN リモート アクセス VPN モデル

FlexVPN サーバ

通常の FlexVPN と FlexVPN リモート アクセス設定の主な違いは、サーバが事前共有キーと証明書（RSA-SIG）方式のみを使用して、FlexVPN クライアントに対して自身を認証する必要があることです。 FlexVPN では、発信側と受信側でどの認証方式を使用するかを、互いに独立してユーザが決定できます。 つまり、発信側と受信側で認証方式が異なっていることも、同じであることも可能です。 しかし、FlexVPN リモート アクセスでは、サーバに選択権はありません。

IOS FlexVPN のクライアント認証方式

クライアントは次の認証方式をサポートします。

- **RSA-SIG** — デジタル証明書認証。
- **事前共有** — 事前共有キー（PSK）認証。
- **Extensible Authentication Protocol（EAP）** - EAP 認証。 IOS FlexVPN クライアントの EAP サポートは、15.2(3)T で追加されました。IOS FlexVPN クライアントでサポートされる EAP 方式は次のとおりです。Extensible Authentication Protocol-Message Digest 5（EAP-MD5）Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol Version 2（EAP-MSCHAPv2）Extensible Authentication Protocol-Generic Token Card（EAP-GTC）

このドキュメントでは、次の理由から RSA-SIG 認証の使用についてのみ、説明します。

- **スケーラブル**：各クライアントには証明書が渡され、サーバ上でクライアントの ID の一般的な部分がこれに対して認証されます。
- **セキュア**：ワイルドカード PSK よりセキュリティが高い認証方式です（ローカル認証の場合）。 AAA（認証、認可、アカウンティング）認証の場合、マングルされた IKE ID に基づいて別の PSK を書き込むことがより簡単です。

このドキュメントに示されている FlexVPN のクライアント設定は、EasyVPN クライアントと比較すると、若干複雑に見える可能性があります。 これは、スマート デフォルトにより、ユーザの設定を必要としない一部設定が含まれているためです。 スマート デフォルトとは、提案、ポリシー、IPSec トランスフォーム セットなど、さまざまな内容が事前に設定されているか、またはデフォルト設定であることを示すのに使用される用語です。 IKEv1 のデフォルト値とは異なり、IKEv2 スマート デフォルト値は強力です。 たとえば、提案では Advanced Encryption Standard（AES-256）、セキュア ハッシュ アルゴリズム（SHA-512）およびグループ 5 を使用できます。

トンネル ネゴシエーション

IKEv2 エクスチェンジのパケット交換に関する詳細は、「IKEv2 のパケット交換とプロトコル レベル デバッグ」を参照してください。

初期設定

トポロジ

初期設定

EzVPN ハブ - dVTI ベース

```
!! AAA Config for EzVPN clients. We are using Local AAA Server.
aaa new-model
aaa authentication login default local
aaa authorization network default local

!! ISAKMP Policy
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2

!! ISAKMP On-Demand Keep-Alive
```

```
crypto isakmp keepalive 10 2

!! EzVPN Split ACL
access-list 101 permit ip 10.10.0.0 0.0.0.255 any

!! EzVPN Client Group Configuration. This is what holds all the config attributes
crypto isakmp client configuration group cisco
 key cisco
 dns 6.0.0.2
 wins 7.0.0.1
 domain cisco.com
 acl 101
 save-password

!! ISAKMP Profile. This ties Client IKE identity to AAA.
!! And since this is dVTI setup, ISAKMP Profile tells the IOS
!!   from which Virtual-Template (VT1) to clone the Virtual Access interfaces
crypto isakmp profile vi
   match identity group cisco
   client authentication list default
   isakmp authorization list default
   virtual-template 1

!! IPSec Transform Set.
crypto ipsec transform-set set esp-3des esp-sha-hmac

!! IPSec Profile. This ties Transform set and ISAKMP Profile together.
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi

!! The loopback interface. And virtual-template borrows the address from here.
interface Loopback0
 ip address 10.10.10.1 255.255.255.252

!! dVTI interface.
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
```

EzVPN クライアント - クラシック (VTI なし)

```
!! ISAKMP On-Demand Keep-Alive
crypto isakmp keepalive 10 2

!! EzVPN Client - Group Name and The key (as configured on the Server),
!!   Peer address and XAUTH config go here.
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 local-address Ethernet0/0
 mode network-extension
 peer 10.0.0.1
 username cisco password cisco
 xauth userid mode local

!! EzVPn outside interface - i.e. WAN interface
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 crypto ipsec client ezvpn ez

!! EzVPN inside interface
```

```
!! Traffic sourced from this LAN is sent over established Tunnel
interface Ethernet0/1
 ip address 10.10.1.1 255.255.255.0
 crypto ipsec client ezvpn ez inside
```

EzVPN クライアント - 拡張 (VTI ベース)

```
!! VTI -
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4

!! ISAKMP On-Demand Keep-Alive
crypto isakmp keepalive 10 2

!! EzVPN Client - Group Name and The key (as configured on the Server),
!!   Peer address and XAUTH config go here.
!! Also this config says which Virtual Template to use.
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 local-address Ethernet0/0
 mode network-extension
 peer 10.0.0.1
 virtual-interface 1
 username cisco password cisco
 xauth userid mode local

!! EzVPn outside interface - WAN interface
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 crypto ipsec client ezvpn ez

!! EzVPN inside interface -
!! Traffic sourced from this LAN is sent over established Tunnel
interface Ethernet0/1
 ip address 10.10.2.1 255.255.255.0
 crypto ipsec client ezvpn ez inside
```

EzVPN から FlexVPN への移行方法

EzVPN サーバとして機能するサーバは、IKEv2 リモート アクセス設定をサポートしている場合、FlexVPN サーバとしても動作できます。 完全な IKEv2 設定をサポートするには、IOS v15.2(3)T よりも上のバージョンが推奨されます。 次の例では、15.2(4)M1 が使用されています。

2 通りの方法が考えられます。

1. EzVPN サーバを FlexVPN サーバとして設定し、次に EzVPN クライアントを Flex 設定に移行します。
2. 別のルータを FlexVPN サーバとして設定します。 EzVPN クライアントと、移行された FlexVPN クライアントは、FlexVPN サーバと EzVPN サーバ間の接続を作成することにより、引き続き通信を行います。

このドキュメントでは、2 番目の方法について説明し、FlexVPN クライアントとして新しいスポーク (Spoke3 など) を使用します。 このスポークは、将来、他のクライアントを移行するための基準として使用できます。

移行の手順

EzVPN スポークから FlexVPN スポークに移行する場合は、EzVPN スポークで FlexVPN config を ロードするよう選択できます。 ただし、全カットオーバーを通じて、ボックスへのアウトオブバンド（非 VPN）管理アクセスが必要になる場合があります。

移行したトポロジ

設定

FlexVPN ハブ

```
!! AAA Authorization done Locally
aaa new-model
aaa authorization network Flex local

!! PKI TrustPoint to Sign and Validate Certificates.
!! Contains Identity Certificate and CA Certificate
crypto pki trustpoint FlexServer
 enrollment terminal
 revocation-check none
 rsakeypair FlexServer
 subject-name CN=flexserver.cisco.com,OU=FlexVPN

!! Access-list used in Config-Reply in order to push routes
access-list 1 permit 10.10.0.0 0.0.0.255

!! IKEv2 Authorization done locally. Used in Config-Set.
crypto ikev2 authorization policy FlexClient-Author
 def-domain cisco.com
 route set interface
 route set access-list 1

!! IKEv2 Proposal. Optional Config. Smart-Default takes care of this.
crypto ikev2 proposal FlexClient-Proposal
 encryption aes-cbc-128 aes-cbc-192 3des
 integrity sha256 sha512 sha1
 group 5 2

!! If IKEv2 Proposal was left out default, then IKEv2 Policy can be left out too.
!! Ties Proposal to Peer address/fvrf
crypto ikev2 policy FlexClient-Policy
 match fvrf any
 proposal FlexClient-Proposal

!! IKEv2 Profile. This is the main Part
!! Clients are configured to send their FQDN. And we match the domain 'cisco.com'
!! We are sending 'flexserver.cisco.com' as the fqdn identity.
!! Local and Remote authentication is RSA-SIG
!! Authorization (config-reply) is done locally with the user-name
!!   'FlexClient-Author'
!! This whole profile is tied to Virtual-Template 1
crypto ikev2 profile FlexClient-Profile
 match identity remote fqdn domain cisco.com
 identity local fqdn flexserver.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint FlexServer
 aaa authorization group cert list Flex FlexClient-Author
 virtual-template 1

!! IPSec Transform set. Optional Config, since Smart Default takes care of this.
```

```
crypto ipsec transform-set ESP-AES-SHA1 esp-aes esp-sha-hmac

!! IPSec Profile ties default/Configured transform set with the IKEv2 Profile
crypto ipsec profile FlexClient-IPSec
 set transform-set ESP-AES-SHA1
 set ikev2-profile FlexClient-Profile

!! Loopback interface lends ip address to Virtual-template and
!!   eventually to Virtual-Access interfaces spawned.
interface Loopback0
 ip address 10.10.10.1 255.255.255.252

!! The IKEv2 enabled Virtual-Template
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel protection ipsec profile FlexClient-IPSec

!! WAN interface
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0

!! LAN interfaces
interface Ethernet0/1
 ip address 10.10.0.1 255.255.255.0
```

サーバ証明書についての注意

キーの使用状況（KU）は公開キーの目的または意図した使用法を定義します。 拡張キーの使用状況（EKU）はキーの使用状況を改良したものです。 FlexVPN では、証明書がクライアントに受け入れられるために、サーバ証明書に**デジタル署名**と**鍵暗号化**の KU 属性を持つ EKU、**server auth**（OID = 1.3.6.1.5.5.7.3.1）が必要です。

```
FlexServer#show crypto pki certificates verbose Certificate Status: Available Version: 3
Certificate Serial Number (hex): 09 Certificate Usage: General Purpose Issuer: l=lal-bagh c=IN
o=Cisco ou=TAC cn=Praveen Subject: Name: flexserver.cisco.com ou=FlexVPN cn=flexserver.cisco.com
CRL Distribution Points: http://10.48.67.33:80/Praveen/Praveen.crl <snip> Signature Algorithm:
MD5 with RSA Encryption Fingerprint MD5: F3646C9B 1CC26A81 C3CB2034 061302AA Fingerprint SHA1:
7E9E99D4 B66C70E3 CBA8C4DB DD94629C 023EEBE7 X509v3 extensions: X509v3 Key Usage: E0000000
Digital Signature Non Repudiation Key Encipherment <snip> Authority Info Access: Extended Key
Usage: Client Auth Server Auth Associated Trustpoints: FlexServer Storage: nvram:lal-bagh#9.cer
Key Label: FlexServer Key storage device: private config CA Certificate <snip>
```

FlexVPN のクライアント設定

```
!! AAA Authorization done Locally
aaa new-model
aaa authorization network Flex local

!! PKI TrustPoint to Sign and Validate Certificates.
!! Contains Identity Certificate and CA Certificate
crypto pki trustpoint Spoke3-Flex
 enrollment terminal
 revocation-check none
 subject-name CN=spoke3.cisco.com,OU=FlexVPN
 rsakeypair Spoke3-Flex

!! Access-list used in Config-Set in order to push routes
access-list 1 permit 10.10.3.0 0.0.0.255

!! IKEv2 Authorization done locally. Used in Config-Set.
crypto ikev2 authorization policy FlexClient-Author
 route set interface
 route set access-list 1
```

```
!! IKEv2 Proposal. Optional Config. Smart-Default takes care of this.
crypto ikev2 proposal FlexClient-Proposal
 encryption aes-cbc-128 aes-cbc-192 3des
 integrity sha256 sha512 sha1
 group 5 2


!! If IKEv2 Proposal was left out default, then IKEv2 Policy can be left out too.
!! Ties Proposal to Peer address/fvrf
crypto ikev2 policy FlexClient-Policy
 match fvrf any
 proposal FlexClient-Proposal

!! IKEv2 Profile. This is the main Part
!! Server is configured to send its FQDN type IKE-ID,
!!    and we match the domain 'cisco.com'
!! (If the IKE-ID type is DN (extracted from the certificate),
!!    we will need a certificate map)
!! We are sending 'spoke3.cisco.com' as the IKE-identity of type fqdn.
!! Local and Remote authentication is RSA-SIG
!! Authorization (config-set) is done locally using the user-name filter
!!    'FlexClient-Author'
crypto ikev2 profile FlexClient-Profile
 match identity remote fqdn flexserver.cisco.com
 identity local fqdn spoke3.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint Spoke3-Flex
 aaa authorization group cert list Flex FlexClient-Author

!! IPSec Transform set. Optional Config, since Smart Default takes care of this.
crypto ipsec transform-set ESP-AES-SHA1 esp-aes esp-sha-hmac

!! IPSec Profile ties the transform set with the IKEv2 Profile
crypto ipsec profile FlexClient-IPSec
 set transform-set ESP-AES-SHA1
 set ikev2-profile FlexClient-Profile

!! FlexVPN Client Tunnel interface.
!! If IP-Address of the tunnel is negotiated,
!!   FlexVPN server is capable of assigning an IP through Config-Set
interface Tunnel0
 ip unnumbered Ethernet0/1
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexClient-IPSec

!! Final FlexVPN client Part.
!! Multiple backup Peer and/or Multiple Tunnel source interfaces can be configured
crypto ikev2 client flexvpn FlexClient
  peer 1 10.0.0.2
  client connect Tunnel0

!! WAN interface
interface Ethernet0/0
 ip address 10.1.1.4 255.255.255.248

!! LAN Interface
interface Ethernet0/1
 ip address 10.10.3.1 255.255.255.0
```

クライアント証明書についての注意

FlexVPN では、証明書がサーバに受け入れられるために、クライアント証明書に**デジタル署名**と**鍵暗号化**の KU 属性を持つ EKU、**server auth**（OID = 1.3.6.1.5.5.7.3.1）が必要です。

```
Spoke3#show crypto pki certificates verbose Certificate Status: Available Version: 3 Certificate
Serial Number (hex): 08 Certificate Usage: General Purpose Issuer: l=lal-bagh c=IN o=Cisco
ou=TAC cn=Praveen Subject: Name: spoke3.cisco.com ou=FlexVPN cn=spoke3.cisco.com <snip> Subject
Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Signature Algorithm:
MD5 with RSA Encryption Fingerprint MD5: 2381D319 906177E1 F45019BC 61059BD5 Fingerprint SHA1:
D81FD705 653547F2 D0916710 E6B096A1 23F6C467 X509v3 extensions: X509v3 Key Usage: E0000000
Digital Signature Non Repudiation Key Encipherment <snip> Extended Key Usage: Client Auth Server
Auth Associated Trustpoints: Spoke3-Flex Storage: nvram:lal-bagh#8.cer Key Label: Spoke3-Flex
Key storage device: private config CA Certificate <snip>
```

FlexVPN の動作検証

FlexVPN サーバ

```
FlexServer#show crypto ikev2 session IPv4 Crypto IKEv2 Session Session-id:5, Status:UP-ACTIVE,
IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status 1 10.0.0.2/500 10.1.1.4/500
none/none READY Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth
verify: RSA Life/Active Time: 86400/7199 sec Child sa: local selector 10.0.0.2/0 -
10.0.0.2/65535 remote selector 10.1.1.4/0 - 10.1.1.4/65535 ESP spi in/out: 0xA9571C00/0x822DDAAD
FlexServer#show crypto ikev2 session detailed IPv4 Crypto IKEv2 Session Session-id:5, Status:UP-
ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status 1 10.0.0.2/500
10.1.1.4/500 none/none READY Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign:
RSA, Auth verify: RSA Life/Active Time: 86400/7244 sec CE id: 1016, Session-id: 5 Status
Description: Negotiation done Local spi: 648921093349609A Remote spi: 1C2FFF727C8EA465 Local id:
flexserver.cisco.com Remote id: spoke3.cisco.com Local req msg id: 2 Remote req msg id: 5 Local
next msg id: 2 Remote next msg id: 5 Local req queued: 2 Remote req queued: 5 Local window: 5
Remote window: 5 DPD configured for 0 seconds, retry 0 NAT-T is not detected Cisco Trust
Security SGT is disabled Initiator of SA : No Remote subnets: 10.10.3.0 255.255.255.0 Child sa:
local selector 10.0.0.2/0 - 10.0.0.2/65535 remote selector 10.1.1.4/0 - 10.1.1.4/65535 ESP spi
in/out: 0xA9571C00/0x822DDAAD AH spi in/out: 0x0/0x0 CPI in/out: 0x0/0x0 Encr: AES-CBC, keysize:
128, esp_hmac: SHA96 ah_hmac: None, comp: IPCOMP_NONE, mode transport FlexServer#show ip route
static 10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks S 10.10.3.0/30 is directly
connected, Virtual-Access1 FlexServer#ping 10.10.3.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/5/13 ms


FlexServer#show crypto ipsec sa | I ident|caps|spi local ident (addr/mask/prot/port):
(10.0.0.2/255.255.255.255/47/0) remote ident (addr/mask/prot/port):
(10.1.1.4/255.255.255.255/47/0) #pkts encaps: 205, #pkts encrypt: 205, #pkts digest: 205 #pkts
decaps: 200, #pkts decrypt: 200, #pkts verify: 200 current outbound spi: 0x822DDAAD(2184043181)
spi: 0xA9571C00(2841058304) spi: 0x822DDAAD(2184043181)
```

FlexVPN リモート

```
Spoke3#show crypto ikev2 session IPv4 Crypto IKEv2 Session Session-id:4, Status:UP-ACTIVE, IKE
count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status 1 10.1.1.4/500 10.0.0.2/500
none/none READY Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth
verify: RSA Life/Active Time: 86400/7621 sec Child sa: local selector 10.1.1.4/0 -
10.1.1.4/65535 remote selector 10.0.0.2/0 - 10.0.0.2/65535 ESP spi in/out: 0x822DDAAD/0xA9571C00
Spoke3#show crypto ikev2 session detailed IPv4 Crypto IKEv2 Session Session-id:4, Status:UP-
ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status 1 10.1.1.4/500
10.0.0.2/500 none/none READY Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign:
RSA, Auth verify: RSA Life/Active Time: 86400/7612 sec CE id: 1016, Session-id: 4 Status
Description: Negotiation done Local spi: 1C2FFF727C8EA465 Remote spi: 648921093349609A Local id:
```

```
spoke3.cisco.com Remote id: flexserver.cisco.com Local req msg id: 5 Remote req msg id: 2 Local
next msg id: 5 Remote next msg id: 2 Local req queued: 5 Remote req queued: 2 Local window: 5
Remote window: 5 DPD configured for 0 seconds, retry 0 NAT-T is not detected Cisco Trust
Security SGT is disabled Initiator of SA : Yes Default Domain: cisco.com Remote subnets:
10.10.10.1 255.255.255.255 10.10.0.0 255.255.255.0 Child sa: local selector 10.1.1.4/0 -
10.1.1.4/65535 remote selector 10.0.0.2/0 - 10.0.0.2/65535 ESP spi in/out: 0x822DDAAD/0xA9571C00
AH spi in/out: 0x0/0x0 CPI in/out: 0x0/0x0 Encr: AES-CBC, keysize: 128, esp_hmac: SHA96 ah_hmac:
None, comp: IPCOMP_NONE, mode transport Spoke3#ping 10.10.0.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.10.0.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/5/12 ms

Spoke3#show crypto ipsec sa | I ident|caps|spi local ident (addr/mask/prot/port):
(10.1.1.4/255.255.255.255/47/0) remote ident (addr/mask/prot/port):
(10.0.0.2/255.255.255.255/47/0) #pkts encaps: 300, #pkts encrypt: 300, #pkts digest: 300 #pkts
decaps: 309, #pkts decrypt: 309, #pkts verify: 309 current outbound spi: 0xA9571C00(2841058304)
spi: 0x822DDAAD(2184043181) spi: 0xA9571C00(2841058304)
```

関連情報

- FlexVPN： 組み込みの Windows クライアントと証明書認証を備えた IKEv2 TechNote
- FlexVPN および Anyconnect IKEv2 クライアントの設定例 TechNote
- FlexVPN の展開： EAP-MD5 による AnyConnect IKEv2 リモート アクセス TechNote
- IKEv2 のパケット交換とプロトコル レベル デバッグ TechNote
- Cisco FlexVPN
- IPSec ネゴシエーション/IKE プロトコル
- Cisco AnyConnect セキュア モビリティ クライアント
- Cisco VPN クライアント
- テクニカルサポートとドキュメント - Cisco Systems