EzVPN-PAS MENTIONNÉ AILLEURs au guide de transfert de FlexVPN

Contenu

Introduction

Ce document fournit l'assistance dans le procédé de transfert de l'EzVPN (échange de clés Internet (IKE) v1 (IKEv1)) l'installation à FlexVPN (IKEv2) a installé avec en tant que peu de questions comme possibles. Puisque l'Accès à distance IKEv2 diffère de l'Accès à distance IKEv1 de certaines manières qui rendent transfert un bit difficile, ce document vous aide à choisir différentes approches de conception dans le transfert du modèle d'EzVPN au modèle d'Accès à distance de FlexVPN.

Ce document a affaire avec le client IOS FlexVPN ou le client matériel, ce document ne discute pas le client logiciel. Pour plus d'informations sur le client logiciel référez-vous s'il vous plaît :

- FlexVPN : IKEv2 avec l'authentification intégrée de client Windows et de certificat
- Exemple de configuration de client de FlexVPN et d'Anyconnect IKEv2

- Déploiement de FlexVPN : Accès à distance d'AnyConnect IKEv2 avec EAP-MD5

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IKEv2
- Cisco FlexVPN
- Client à mobilité sécurisé Cisco AnyConnect
- **Client VPN Cisco**

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

EzVPN contre FlexVPN

Modèle d'EzVPN - Ce qui se tient

Car le nom suggère, l'objectif de l'EzVPN est de rendre la configuration du VPN sur les clients distants facile. Afin de réaliser ceci, le client est configuré avec les détails minimaux requis pour contacter le serveur correct d'EzVPN, également connu sous le nom de profil de client.

Négociation de tunnel

Modèle de l'Accès à distance VPN de FlexVPN

Serveur de FlexVPN

Une importante différence entre FlexVPN normal et une installation d'Accès à distance de FlexVPN est que le serveur doit s'authentifier aux clients de FlexVPN par l'utilisation des clés pré-partagées et délivre un certificat la méthode (RSA-SIG) seulement. FlexVPN te permet pour décider quelles méthodes d'authentification les utilisations de demandeur et de responder, indépendant de l'un l'autre. En d'autres termes, ils peuvent être identiques ou ils peuvent être différents. Cependant, quand il s'agit d'Accès à distance de FlexVPN, le serveur n'a pas un choix.

Méthodes d'authentification client IOS FlexVPN

Le client prend en charge les ces méthodes d'authentification :

- **RSA-SIG** — Authentification de certificat numérique.
- **Pré-partage** — Authentification (PSK) principale pré-partagée.
- **Protocole EAP (Extensible Authentication Protocol)** - Authentification EAP. L'Eap-support pour le client IOS FlexVPN a été ajouté dans 15.2(3)T.Les méthodes prises en charge d'EAP par le client IOS FlexVPN incluent :Digest 5 de Protocol-message d'authentification extensible (EAP-MD5),Version 2 à échanges confirmés (EAP-MSCHAPv2) de Protocol d'authentification de Protocol-Microsoft d'authentification extensible, etCarte symbolique Protocol-générique d'authentification extensible (EAP-GTC).

Ce document décrit seulement l'utilisation de l'authentification RSA-SIG, pour ces raisons :

- **Extensible** — Chaque client est donné un certificat, et sur le serveur, une partie générique d'identité de client est authentifiée contre elle.
- **Sécurisé** — Plus sécurisés qu'un masque PSK (en cas d'autorisation locale). Bien que, dans le cas de l'autorisation d'AAA (authentification, autorisation, et comptabilité), il soit plus facile d'écrire PSKs distinct basé sur l'identité mutilée d'IKE.

La configuration illustrée de client de FlexVPN dans ce document pourrait sembler peu exhaustif comparé au client d'EasyVPN. C'est parce que la configuration inclut quelques parties de la configuration qui n'ont pas besoin d'être configurées par l'utilisateur dû aux par défaut intelligents. Les par défaut intelligents est le terme utilisé pour se rapporter à la préconfigurer ou à la configuration par défaut pour différentes choses comme la proposition, stratégie, jeu de transformations d'IPSec, et ainsi de suite. Et à la différence des valeurs par défaut IKEv1, les valeurs par défaut IKEv2 intelligentes sont fortes. Par exemple, il se sert de l'Advanced Encryption Standard (AES-256), du Secure Hash Algorithm (SHA-512), et du Group-5 dans les propositions, et ainsi de suite.

Négociation de tunnel

Pour plus d'informations sur l'échange des paquets pour un échange IKEv2, référez-vous à l'échange du paquet IKEv2 et à l'élimination des imperfections de niveau de Protocol.

Première installation

Topologie

Configuration initiale

Hub d'EzVPN - dVTI basé

```
!! 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
```

Client d'EzVPN - Classique (aucun VTI)

```
!! 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
```

Client d'EzVPN - Amélioré (basé sur VTI)

```
!! 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 à l'approche de transfert de FlexVPN

Le serveur qui agit en tant que serveur d'EzVPN peut également agir en tant que serveur de FlexVPN tant que il prend en charge la configuration de l'Accès à distance IKEv2. Pour un support total de la configuration IKEv2, quelque chose au-dessus d'IOS v15.2(3)T est recommandé. Dans ces exemples 15.2(4)M1 a été utilisé.

Il y a deux approches possibles :

1. Le serveur d'EzVPN d'installation comme serveur de FlexVPN, migrent alors les clients d'EzVPN pour fléchir la configuration.
2. Installez un routeur différent en tant que serveur de FlexVPN. Les clients d'EzVPN et les clients migrés de FlexVPN continuent à communiquer par la création d'une connexion entre le serveur de FlexVPN et le serveur d'EzVPN.

Ce document décrit la deuxième approche et utilise un nouveau rai (par exemple, Spoke3), en tant que client de FlexVPN. Ce rai peut être utilisé comme référence afin de migrer d'autres clients

à l'avenir.

Étapes de transfert

Notez que quand vous migrez d'un EzVPN a parlé à un FlexVPN a parlé, vous peut choisir de charger le **config de FlexVPN** sur le rai d'EzVPN. Cependant, dans tous le coupé, vous pourriez avoir besoin d'un accès hors bande de la Gestion (non-VPN) dans la case.

Topologie migrée

Configuration

Hub de FlexVPN

```
!! 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
```

Note au sujet des Certificats de serveur

L'utilisation principale (KU) définit le but ou l'utilisation destinée de la clé publique. Amélioré/a étendu l'utilisation principale (EKU) affine l'utilisation principale. FlexVPN a besoin de que le certificat de serveur a un EKU de **serveur authentique** (OID = 1.3.6.1.5.5.7.3.1) avec les attributs KU de la **signature numérique** et du **chiffrement de clé** pour que le certificat soit reçu par le client.

```
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>
```

Configuration de client de FlexVPN

```
!! 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
```

Note au sujet des certificats client

FlexVPN a besoin de que le certificat client a un EKU de **client authentique** (OID = 1.3.6.1.5.5.7.3.2) avec les attributs KU de la **signature numérique** et du **chiffrement de clé** pour que le certificat soit reçu par le serveur.

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>

Vérification d'exécution de FlexVPN

Serveur de FlexVPN

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)

Distant de FlexVPN

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)
```

Informations connexes

- FlexVPN : IKEv2 avec l'authentification intégrée TechNote de client Windows et de certificat
- Exemple TechNote de configuration de client de FlexVPN et d'Anyconnect IKEv2
- Déploiement de FlexVPN : Accès à distance d'AnyConnect IKEv2 avec EAP-MD5 TechNote
- Échange du paquet IKEv2 et niveau de Protocol mettant au point TechNote
- Cisco FlexVPN
- Négociation IPSec/Protocoles IKE
- Client à mobilité sécurisé Cisco AnyConnect
- Client VPN Cisco
- Support et documentation techniques - Cisco Systems