دليل الترحيل من EzVPN-NEM إلى FlexVPN

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
EzVPN مقابل FlexVPN
طراز EzVPN - ما يتميز به
تفاوض النفق
نموذج VPN FlexVPN للوصول عن بعد
خادم FlexVPN
طرق مصادقة عميل IOS FlexVPN
تفاوض النفق
الإعداد الأولي
طوبولوجيا
التهيئة الأولية
نهج الترحيل من شبكة EzVPN إلى شبكة FlexVPN
طبولوجيا مهاجرة
التكوين
التحقق من عملية FlexVPN
خادم FlexVPN
FlexVPN Remote
معلومات ذات صلة

المقدمة

يقدم هذا المستند المساعدة في عملية الترحيل من إعداد IKEv1 (Internet Key Exchange v1) EzVPN) إلى إعداد IKEv2) FlexVPN) مع أقل عدد ممكن من المشاكل. نظرا لأن IKEv2 Remote Access يختلف عن IKEv1 Remote Access بطرق معينة تجعل الترحيل صعبا بعض الشيء، يساعدك هذا المستند على إختيار أساليب تصميم مختلفة في الترحيل من طراز EzVPN إلى طراز FlexVPN Remote Access.

يتعامل هذا المستند مع عميل IOS FlexVPN أو عميل الأجهزة، ولا يناقش هذا المستند عميل البرنامج. لمزيد من المعلومات حول عميل البرنامج، يرجى الرجوع إلى:

- FlexVPN: IKEv2 مع مصادقة مدمجة لعميل Windows والشهادة
- مثال تكوين عميل FlexVPN و AnyConnect IKEv2
- نشر FlexVPN: الوصول عن بعد إلى AnyConnect IKEv2 باستخدام EAP-MD5

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- IKEv2
- FlexVPN من Isco
- Cisco AnyConnect Secure Mobility Client
- عميل شبكة VPN من Cisco

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

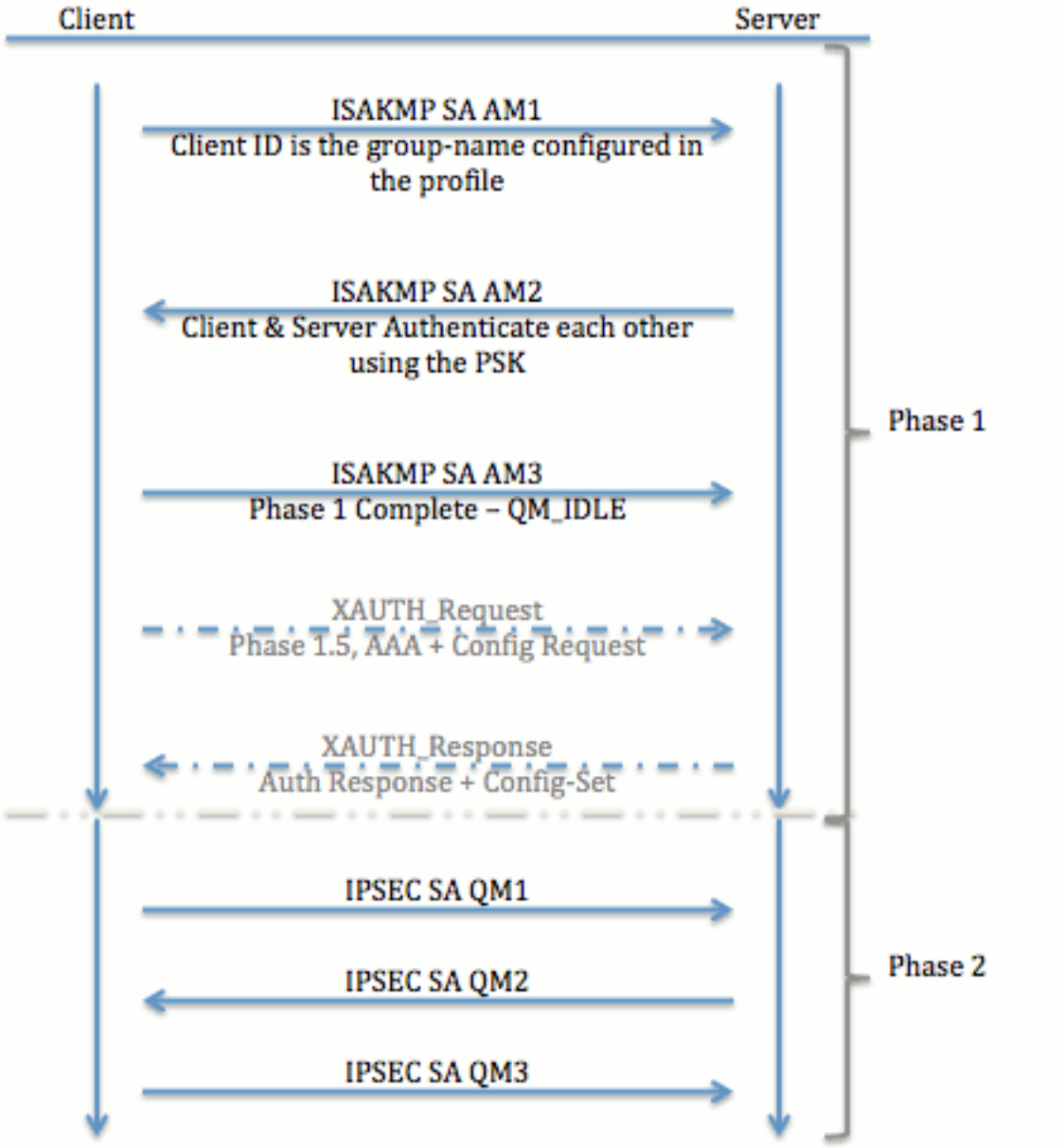
راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

FlexVPN مقابل EzVPN

طراز EzVPN - ما يتميز به

كما يقترح الاسم، يتمثل الهدف من EzVPN في تسهيل تكوين الشبكة الخاصة الظاهرية (VPN) على العملاء البعيدين. ولتحقيق ذلك، يتم تكوين العميل بأقل التفاصيل اللازمة للاتصال بخادم EzVPN الصحيح، المعروف أيضا بملف تعريف العميل.

تفاوض النفق



نموذج VPN FlexVPN للوصول عن بعد

خادم FlexVPN

هناك فرق مهم بين FlexVPN العادي وإعداد FlexVPN للوصول عن بعد هو أن الخادم يحتاج إلى مصادقة نفسه على عملاء FlexVPN من خلال إستخدام طريقة الشهادات والمفاتيح المشتركة مسبقا (RSA-SIG) فقط. يتيح لك FlexVPN تحديد طرق المصادقة التي يستخدمها البادئ والمستجيب بشكل مستقل عن بعضهم البعض. بمعنى آخر، يمكن أن يكونا نفس الشيئ أو يمكن أن يكونا مختلفين. ومع ذلك، فعندما يتعلق الأمر بالوصول عن بعد إلى FlexVPN، لا يكون لدى الخادم خيار.

طرق مصادقة عميل IOS FlexVPN

يدعم العميل طرق المصادقة التالية:

- **RSA-SIG** — مصادقة الشهادة الرقمية.
- **مشاركة مسبقة** — مصادقة مفتاح مشترك مسبقا (PSK).

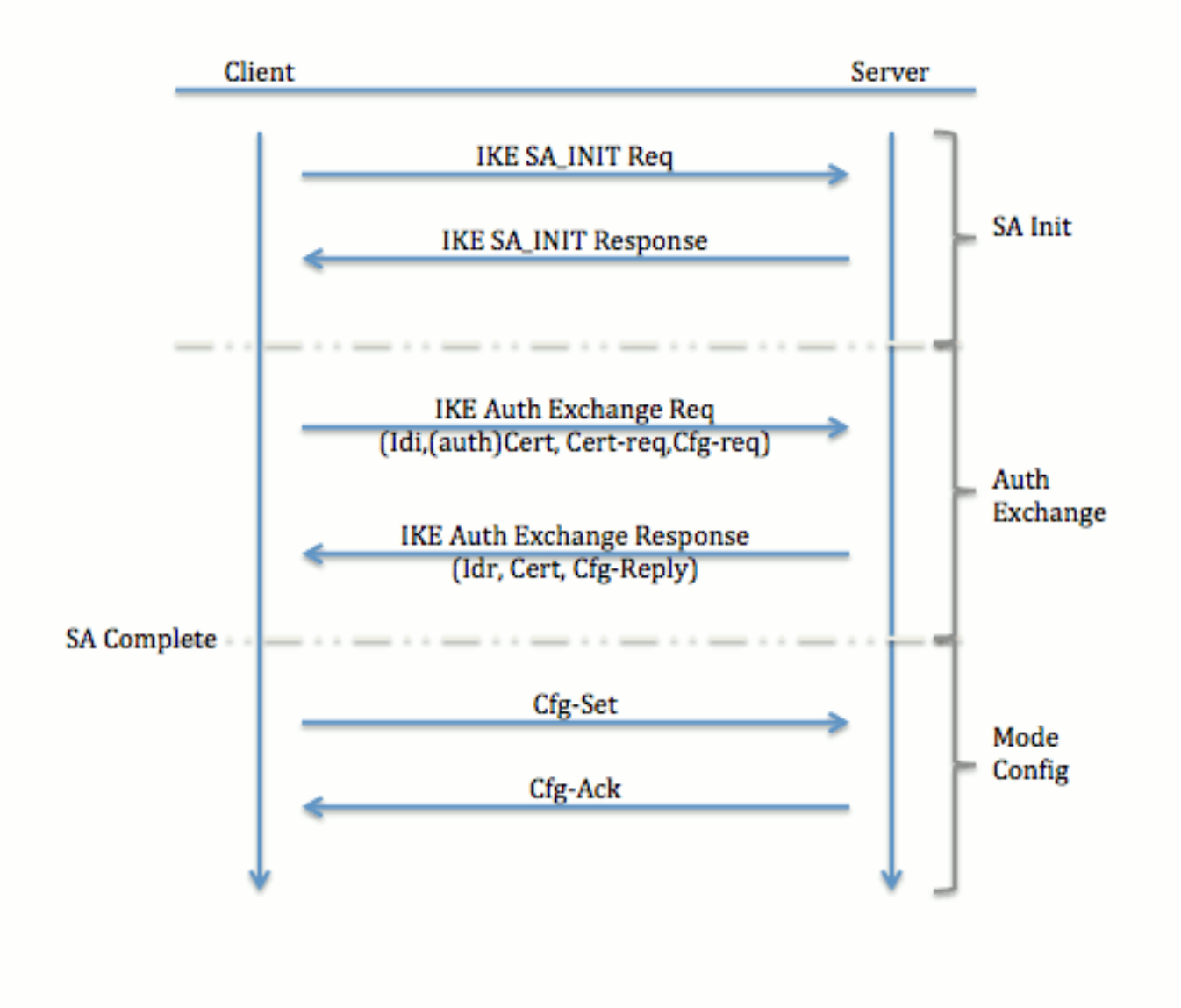
- **بروتوكول المصادقة المتوسع (EAP)** - مصادقة EAP. تمت إضافة دعم EAP لعميل IOS FlexVPN في الإصدار 15.2(3)T.تتضمن أساليب EAP المدعومة من قبل عميل IOS FlexVPN:بروتوكول المصادقة المتوسع-الرسالة Digest 5 (EAP-MD5)،بروتوكول المصادقة المتوسع - بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي ل Microsoft الإصدار 2 (EAP-MSCHAPv2)، وبطاقة الرمز المميز العامة لبروتوكول المصادقة المتوسع (EAP-GTC).

يصف هذا المستند فقط إستخدام مصادقة RSA-SIG، لهذه الأسباب:

- **قابل للتطوير** — يحصل كل عميل على شهادة، وعلى الخادم، تتم مصادقة جزء عام من هوية العميل مقابل ذلك.
- **آمن** — أكثر أمانا من PSK لأحرف البدل (في حالة التفويض المحلي). وعلى الرغم من أنه في حالة تفويض المصادقة والتفويض والمحاسبة (AAA)، يكون من الأسهل كتابة PSKs منفصلة استنادا إلى هوية IKE المدارة.

قد يبدو تكوين عميل FlexVPN الظاهر في هذا المستند غير شامل إلى حد ما مقارنة بعميل EasyVPN. وذلك لأن التكوين يتضمن بعض أجزاء التكوين التي لا يلزم تكوينها بواسطة المستخدم بسبب الافتراضيات الذكية. الافتراضيات الذكية هي المصطلح المستخدم للإشارة إلى التكوين المهيأ مسبقا أو الافتراضي لأشياء مختلفة مثل الاقتراح والسياسة ومجموعة تحويل IPSec وما إلى ذلك. وعلى عكس قيم IKEv1 الافتراضية، تكون قيم IKEv2 الافتراضية الذكية قوية. على سبيل المثال، فإنه يستخدم معيار التشفير المتقدم (AES-256) وخوارزمية التجزئة الآمنة (SHA-512) والمجموعة 5 في العروض وما إلى ذلك.

تفاوض النفق

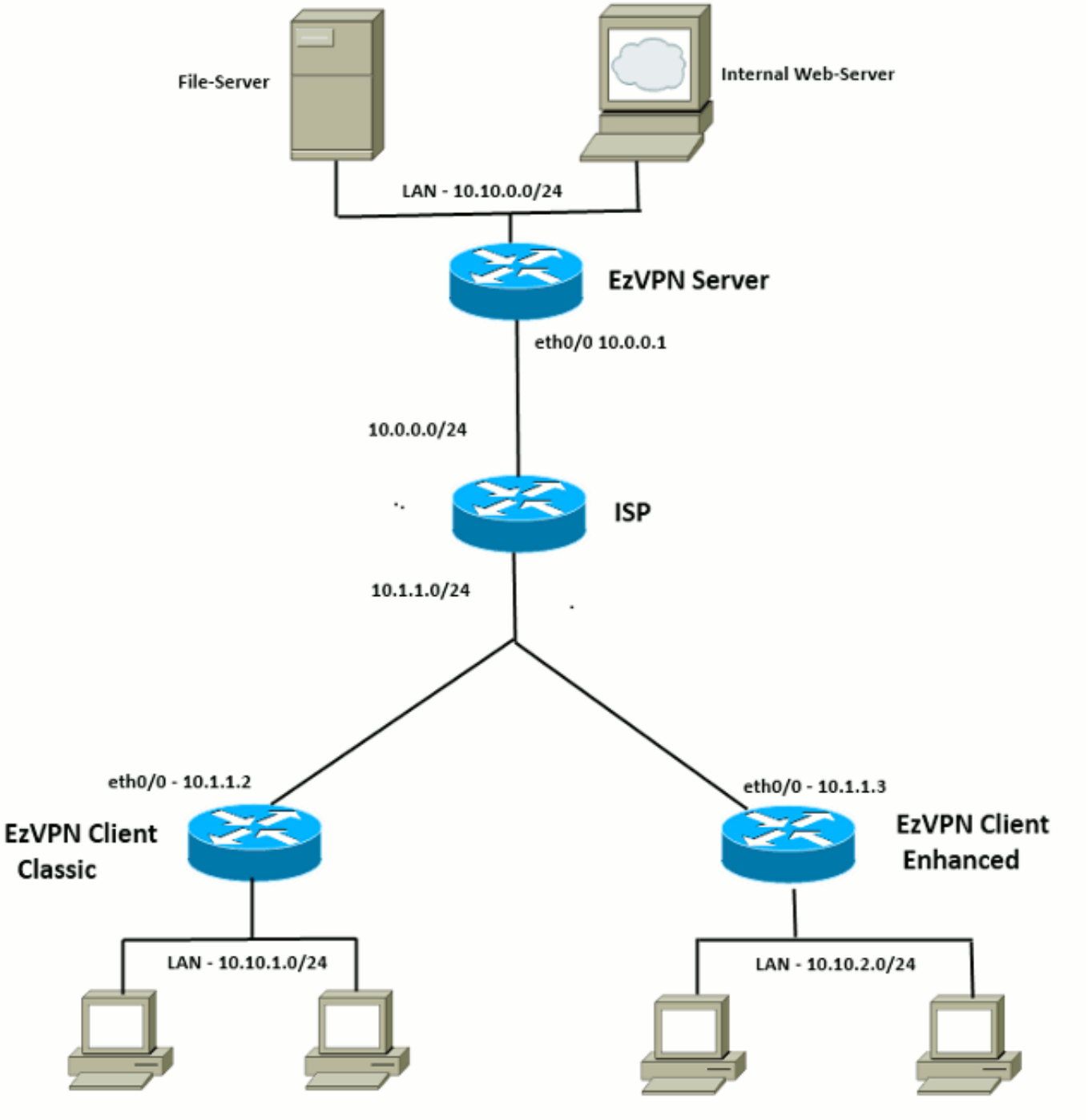


لمزيد من المعلومات حول تبادل الحزم الخاصة بتبادل IKEv2، ارجع إلى تبادل حزم IKEv2 وتصحيح مستوى

البروتوكول.

الإعداد الأولي

طوبولوجيا



التهيئة الأولية

لوحة وصل EzVPN - المستندة إلى dVTI

```
.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
```

عميل EzVPN - تقليدي (لا يوجد 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
```

عميل EzVPN - المحسن (المستند إلى 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
```

نهج الترحيل من شبكة EzVPN إلى شبكة FlexVPN

كما يمكن للخادم الذي يعمل كخادم EzVPN العمل كخادم FlexVPN طالما أنه يدعم تكوين الوصول عن بعد إلى IKEv2. للحصول على دعم تكوين IKEv2 بالكامل، يوصى بأي شيء أعلى من IOS v15.2(3)T. في هذه الأمثلة، تم إستخدام 15.2.M1(4).

هناك نهجان محتملان:

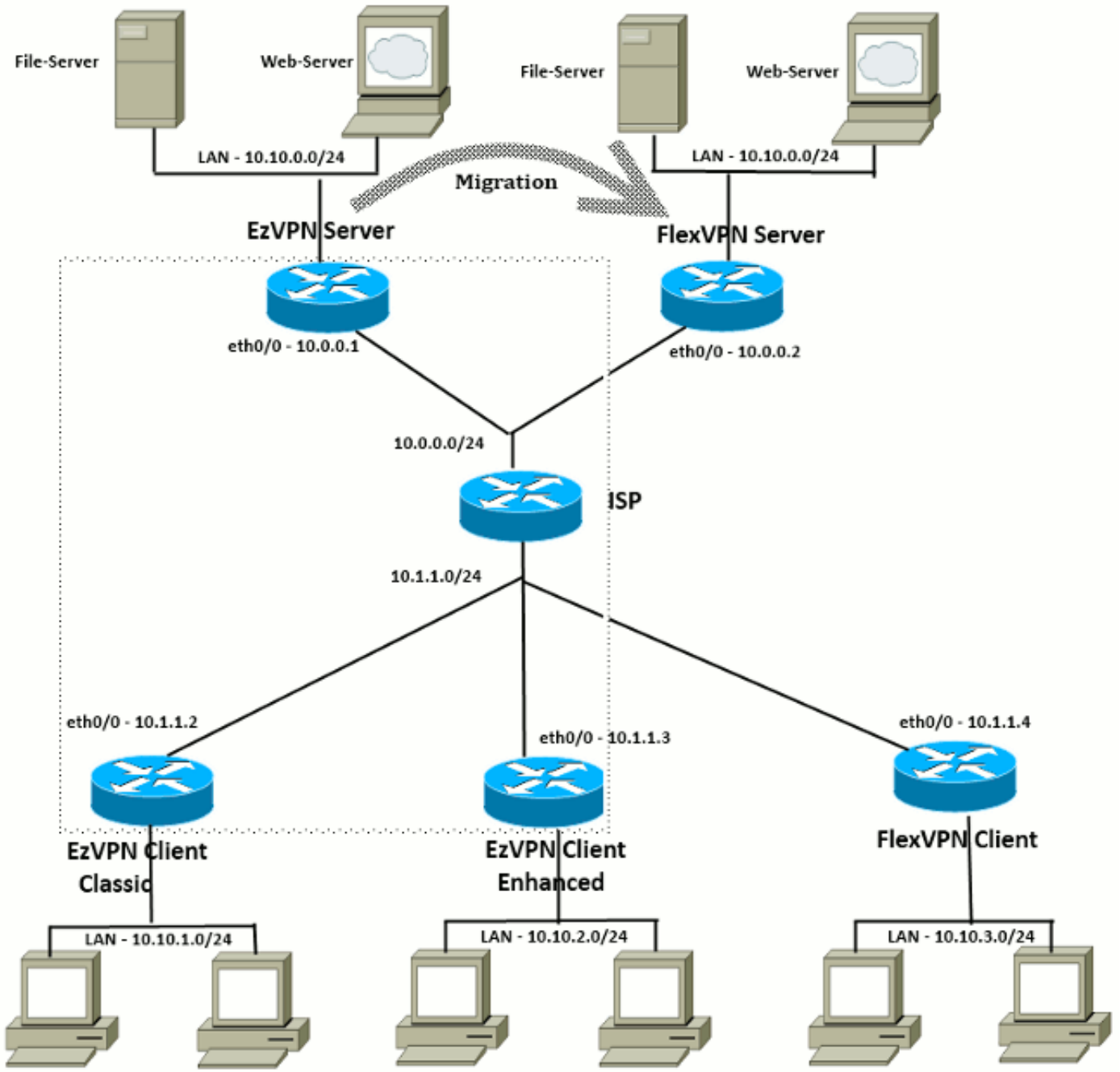
1. قم بإعداد خادم EzVPN كخادم FlexVPN، ثم قم بترحيل عملاء EzVPN إلى Flex Configuration.
2. إعداد موجه مختلف كخادم FlexVPN. يستمر عملاء EzVPN وعملاء FlexVPN المرحلون في الاتصال من خلال إنشاء اتصال بين خادم FlexVPN وخادم EzVPN.

يصف هذا المستند النهج الثاني ويستخدم نغمة جديدة (مثل Talk3)، مثل عميل FlexVPN. يمكن إستخدام هذه المحادثة كمرجع لترحيل عملاء آخرين في المستقبل.

خطوات الترحيل

لاحظ أنه عند الترحيل من شبكة EzVPN التي يتم التحدث بها إلى شبكة FlexVPN، يمكنك إختيار تحميل **تكوين FlexVPN** على شبكة EzVPN التي يتم التحدث بها. ومع ذلك، قد تحتاج، طوال عملية التوصيل، إلى وصول إدارة خارج النطاق (بخلاف VPN) إلى المربع.

طبولوجيا مهاجرة



التكوين

```
                                                    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
```

ملاحظة حول شهادات الخادم

يعرف إستخدام المفتاح (KU) الغرض أو الاستخدام المقصود للمفتاح العام. يعمل إستخدام المفتاح المحسن/الموسع (EKU) على تحسين إستخدام المفتاح. يتطلب FlexVPN أن تحتوي شهادة الخادم على EKU **لمصادقة الخادم** (OID = 1.3.6.1.5.5.7.3.1) مع سمات KU **للتوقيع الرقمي** و**تشفير المفاتيح** لكي يتم قبول الشهادة من قبل العميل.

```
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>

تكوين عميل 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
```

ملاحظة حول شهادات العميل

يتطلب FlexVPN أن تحتوي شهادة العميل على EKU **لمصادقة العميل** (OID = 1.3.6.1.5.5.7.3.2) مع سمات KU **للتوقيع الرقمي** و**تشفير المفاتيح** لكي يتم قبول الشهادة من قبل الخادم.

```
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>
```

التحقق من عملية FlexVPN

خادم 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
     none/none            READY          10.1.1.4/500          10.0.0.2/500         1
: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
     none/none            READY          10.1.1.4/500          10.0.0.2/500         1

: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
                                                      255.255.255.0 10.10.3.0
```

```
                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
                  is variably subnetted, 9 subnets, 4 masks 10.0.0.0/8
               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 Remote

```
                                     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
     none/none            READY          10.0.0.2/500          10.1.1.4/500         1
: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
     none/none            READY          10.0.0.2/500          10.1.1.4/500         1
```

```
: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
                                                255.255.255.255 10.10.10.1
                                                   255.255.255.0 10.10.0.0


                               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
```

معلومات ذات صلة

- FlexVPN: IKEv2 مع ملاحظة فنية مدمجة حول عميل Windows ومصادقة الشهادات
- مثال تكوين عميل FlexVPN و AnyConnect IKEv2 Client Configuration TechNote
- نشر FlexVPN: الوصول عن بعد إلى AnyConnect IKEv2 باستخدام EAP-MD5 TechNote
- ملاحظة فنية حول تصحيح أخطاء مستوى البروتوكول وتبديل حزم IKEv2
- FlexVPN من Isco
- مفاوضة IPSec/بروتوكولات IKE
- Cisco AnyConnect Secure Mobility Client

- عميل شبكة VPN من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).