EzVPN-NEM ao guia de migração de FlexVPN

Índice

Introdução

Este documento fornece o auxílio no processo de migração do EzVPN (intercâmbio de chave de Internet v1 (IKEv1)) a instalação a FlexVPN (IKEv2) setup com como poucas edições como possíveis. Desde que o Acesso remoto IKEv2 difere do Acesso remoto IKEv1 em determinadas maneiras que fazem migração um bit difícil, este documento ajuda-o a escolher aproximações diferentes do projeto na migração do modelo do EzVPN ao modelo do Acesso remoto de FlexVPN.

Este documento trata o cliente IO FlexVPN ou o cliente da ferragem, este documento não discute o cliente de software. Para obter mais informações sobre do cliente de software refira por favor:

- FlexVPN: IKEv2 com cliente do Windows incorporado e certificado de autenticação
- Exemplo da configuração de cliente de FlexVPN e de Anyconnect IKEv2
- Desenvolvimento de FlexVPN: Acesso remoto de AnyConnect IKEv2 com EAP-MD5

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- IKEv2
- Cisco FlexVPN
- Cliente de mobilidade Cisco AnyConnect Secure
- Cisco VPN Client

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

EzVPN contra FlexVPN

Modelo do EzVPN - O que está para fora

Porque o nome sugere, o objetivo do EzVPN é fazer a configuração de VPN nos clientes remotos fácil. A fim conseguir isto, o cliente é configurado com os detalhes mínimos necessários contactar o servidor de EzVPN correto, igualmente conhecido como o perfil do cliente.

Negociação do túnel

Modelo do acesso remoto VPN de FlexVPN

Server de FlexVPN

Uma diferença importante entre FlexVPN normal e uma instalação do Acesso remoto de FlexVPN é que o server precisa de se autenticar aos clientes de FlexVPN com o uso das chaves pré-compartilhada e do método dos Certificados (RSA-SIG) somente. FlexVPN permite que você decida que métodos de autenticação os usos do iniciador e do que responde, independente de se. Ou seja podem ser os mesmos ou podem ser diferentes. Contudo, quando se trata do Acesso remoto de FlexVPN, o server não tem uma escolha.

Métodos de authenticação do cliente IO FlexVPN

Os suportes ao cliente estes métodos de autenticação:

- **RSA-SIG** — Autenticação do certificado digital.
- **PRE-parte** — Autenticação da chave pré-compartilhada (PSK).
- **Extensible Authentication Protocol (EAP)** - Autenticação de EAP. O EAP-apoio para o cliente IO FlexVPN foi adicionado em 15.2(3)T.Os métodos de EAP apoiados pelo cliente IO FlexVPN incluem:Resumo de mensagem de protocolo 5 da autenticação extensível (EAP-MD5),A autenticação extensível Protocolo-Microsoft desafia a versão 2 do protocolo de autenticação de cumprimento (EAP-MSCHAPv2), ePlaca de token Protocolo-genérica da autenticação extensível (EAP-GTC).

Este documento descreve somente o uso da autenticação RSA-SIG, por estas razões:

- **Escalável** — Cada cliente é dado um certificado, e no server, uma identidade genérica do cliente é autenticada parte de contra ela.
- **Fixe** — Mais seguro do que um convite PSK (em caso da autorização local). Embora, no caso da autorização AAA (autenticação, autorização e relatório), seja mais fácil escrever os PSK separados baseados na identidade massacrada IKE.

A configuração de cliente de FlexVPN mostrada neste documento pôde parecer pouco exaustiva comparada ao EasyVPN o cliente. Isto é porque a configuração inclui algumas partes da configuração que não precisam de ser configuradas pelo usuário devido aos padrões espertos. Os padrões espertos são o termo usado para referir PRE-configurado ou a configuração padrão para várias coisas como a proposta, política, IPsec transforma o grupo, e assim por diante. E ao contrário dos valores padrão IKEv1, os valores padrão IKEv2 espertos são fortes. Por exemplo, utiliza o Advanced Encryption Standard (AES-256), o algoritmo de mistura segura (SHA-512), e o Group-5 nas propostas, e assim por diante.

Negociação do túnel

Para obter mais informações sobre da troca dos pacotes para uma troca IKEv2, refira a eliminação de erros do intercâmbio de pacotes IKEv2 e do nível de protocolo.

Instalação inicial

Topologia

Configuração inicial

Hub do EzVPN - dVTI baseado

```
!! 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
```

Cliente ezvpn - Clássico (nenhum 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
```

Cliente ezvpn - Aumentado (VTI-baseado)

```
!! 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 aproximação da migração de FlexVPN

O server que atua como um servidor de EzVPN pode igualmente atuar como um server de FlexVPN enquanto apoia a configuração do Acesso remoto IKEv2. Para um apoio completo da configuração IKEv2, qualquer coisa acima de IO v15.2(3)T é recomendado. Nestes exemplos 15.2(4)M1 foi usado.

Há duas aproximações possíveis:

1. O servidor de EzVPN da instalação como o server de FlexVPN, migra então os clientes ezvpn para dobrar a configuração.
2. Setup um roteador diferente como um server de FlexVPN. Os clientes ezvpn e os clientes migrados de FlexVPN continuam a comunicar-se através da criação de uma conexão entre o server de FlexVPN e o servidor de EzVPN.

Este documento descreve a segunda aproximação e usa um spoke novo (por exemplo, Spoke3), como o cliente de FlexVPN. Este spoke pode ser usado como uma referência a fim migrar no futuro outros clientes.

Etapas da migração

Note que quando você migrar de um EzVPN falou a um FlexVPN falou, você pode escolher carregar a **configuração de FlexVPN no** spoke do EzVPN. Contudo, durante todo corte-sobre, você pôde precisar um acesso de gerenciamento (NON-VPN) fora da banda à caixa.

Topologia migrada

Configuração

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 sobre certificados de servidor

O uso chave (KU) define a finalidade ou o uso pretendido da chave pública. Aumentado/estendeu o uso chave (EKU) refina o uso chave. FlexVPN exige que o certificado de servidor tem um EKU do **AUTH do server** (OID = 1.3.6.1.5.5.7.3.1) com os atributos KU da **assinatura digital** e da **cifragem da chave** para que o certificado esteja aceitado pelo cliente.

```
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>
```

Configuração de cliente 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 sobre certificados de cliente

FlexVPN exige que o certificado de cliente tem um EKU do **AUTH do cliente** (OID = 1.3.6.1.5.5.7.3.2) com os atributos KU da **assinatura digital** e da **cifragem da chave** para que o certificado esteja aceitado pelo server.

```
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>
```

Verificação da operação de FlexVPN

Server 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)
```

Telecontrole 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)
```

Informações Relacionadas

- FlexVPN: IKEv2 com cliente do Windows incorporado e certificado de autenticação TechNote
- Exemplo TechNote da configuração de cliente de FlexVPN e de Anyconnect IKEv2
- Desenvolvimento de FlexVPN: Acesso remoto de AnyConnect IKEv2 com EAP-MD5 TechNote
- Intercâmbio de pacotes IKEv2 e nível de protocolo que debugam TechNote
- Cisco FlexVPN
- Negociação IPsec/Protocolos IKE
- Cliente de mobilidade Cisco AnyConnect Secure
- Cisco VPN Client
- Suporte Técnico e Documentação - Cisco Systems