O ASA IKEv2 debuga para o Troubleshooting do acesso remoto VPN

Índice

Introdução

Este documento descreve como compreender debuga na ferramenta de segurança adaptável de Cisco (ASA) quando a versão 2 do intercâmbio de chave de Internet (IKEv2) é usada com um Cliente de mobilidade Cisco AnyConnect Secure. Este documento igualmente fornece a informação em como traduzir certo debuga linhas em uma configuração ASA.

Este documento não descreve como passar o tráfego depois que um túnel VPN foi estabelecido ao ASA, nem inclui conceitos básicos do IPsec ou do IKE.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do intercâmbio de pacotes para IKEv2. Para mais informação, refira a eliminação de erros do intercâmbio de pacotes IKEv2 e do nível de protocolo.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 2 do intercâmbio de chave de Internet (IKEv2)
- Versão 8.4 ou mais recente adaptável da ferramenta de segurança de Cisco (ASA)

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.

Edição de núcleo

O centro de assistência técnica da Cisco (TAC) usa frequentemente comandos debug IKE e de IPsec a fim compreender onde há um problema com estabelecimento de túnel do IPSec VPN, mas os comandos podem ser enigmáticos.

Cenário

Comandos debug

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
debug aggregate-auth xml 5
```

Configuração ASA

Esta configuração ASA é restritamente básica, sem o uso dos servidores internos.

```
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0

ip local pool webvpn1 10.2.2.1-10.2.2.10

crypto ipsec ikev2 ipsec-proposal 3des
 protocol esp encryption aes-256 aes 3des des
 protocol esp integrity sha-1
crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside

crypto ca trustpoint Anu-ikev2
 enrollment self
 crl configure

crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 2
```

```
 prf sha
 lifetime seconds 86400

crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
 anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
 anyconnect enable
 tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev2
 default-domain none
 webvpn
 anyconnect modules value dart
 anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
 address-pool webvpn1
 default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
 group-alias ASA-IKEV2 enable
```

Arquivo XML

```
<ServerList>
       <HostEntry>
               <HostName>Anu-IKEV2</HostName>
               <HostAddress>10.0.0.1</HostAddress>
               <UserGroup>ASA-IKEV2</UserGroup>
               <PrimaryProtocol>IPsec</PrimaryProtocol>
       </HostEntry>
</ServerList>
```

> Nota: O nome do grupo de utilizadores no perfil do cliente XML deve ser o mesmo que o nome do grupo de túneis no ASA. Se não, entrada de host inválida do Mensagem de Erro “. Reenter por favor” é visto no cliente de AnyConnect.

Debugar logs e descrições

> Nota: Os logs dos diagnósticos e da ferramenta de relatório (DARDO) são geralmente logs muito tagarelas, assim que determinados do DARDO foram omitidos neste exemplo devido à insignificância.

Descrição de mensagem do server	Debugs

Data: 04/23/2013
Tempo: 16:24:55
Digite: Informações
Fonte: acvpnui

Descrição: Função: ClientIfcBase:: conecte
Arquivo: . \ ClientIfcBase.cpp
Linha: 964
Uma conexão de VPN a Anu-IKEV2 foi pedida pelo usuário.
****
Data: 04/23/2013
Tempo: 16:24:55
Digite: Informações
Fonte: acvpnui

Descrição: Informação do tipo de mensagem enviada ao usuário: Contactando Anu-IKEV2.
****
Data: 04/23/2013
Tempo: 16:24:55
Digite: Informações
Fonte: acvpnui

Descrição: Função: ApiCert:: getCertList
Arquivo: . \ ApiCert.cpp
Linha: 259
Número de Certificados encontrados: 0
****
Data: 04/23/2013
Tempo: 16:25:00
Digite: Informações
Fonte: acvpnui

Descrição: **Iniciando a conexão de VPN ao gateway seguro https://10.0.0.**
IKEV2
****
Data: 04/23/2013
Tempo: 16:25:00
Digite: Informações
Fonte: acvpnagent

Descrição: Túnel iniciado pelo cliente GUI.
****

Data: 04/23/2013
Tempo: 16:25:02
Digite: Informações
Fonte: acvpnagent

Descrição: Função: CIPsecProtocol:: connectTransport
Arquivo: . \ IPsecProtocol.cpp
Linha: 1629
Soquete aberto IKE de 192.168.1.1:25170 a 10.0.0.1:500

O ASA recebe a mensagem IKE_SA_INIT do cliente.

O primeiro par de mensagens é a troca IKE_SA_INIT. Estas mensagens negociam algoritmos criptográficos, nonces da troca, e fazem uma troca do Diffie-Hellman (DH). A mensagem IKE_SA_INIT recebida do cliente contém estes campos:

1. **Encabeçamento ISAKMP** - SPI/version/flags.
2. **SAi1** - Algoritmo criptográfico que o iniciador IKE apoia.
3. **KEi** - Valor de chave pública DH do iniciador.
4. **N** - Nonce do iniciador.

```
**************************************
------------------------------Começos da troca IKE_SA_INIT----------------------
IKEv2-PLAT-4: [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.0.1]:500
InitSPI=0x58aff71141ba436b RespSPI=0x0000000000000000 MID=0000
RECV PACOTE
IKEv2-PROTO-3: RX [L m_id 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: 0000000000000000]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
0000000000000000
IKEv2-PROTO-4: Payload seguinte: SA, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_SA_INIT, bandeiras: INICIADOR
IKEv2-PROTO-4: ID de mensagem: 0x0, comprimento: 528

 Payload seguinte SA: KE, reservado: 0x0, comprimento: 168
IKEv2-PROTO-4:   última proposta: 0x0, reservado: 0x0, comprimento: 16
 Proposta: 1, ID de protocolo: IKE, tamanho SPI: 0, #trans: 18
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 1, reservado: 0x0, identificação: 3DES
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 1, reservado: 0x0, identificação: DES
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 2, reservado: 0x0, identificação: SHA512
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 2, reservado: 0x0, identificação: SHA384
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 2, reservado: 0x0, identificação: SHA256
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 2, reservado: 0x0, identificação: SHA1
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 2, reservado: 0x0, identificação: MD5
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: SHA512
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: SHA384
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: SHA256
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: SHA96
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: MD596
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 4, reservado: 0x0, identificação: DH_GROUP_1536_MODP/Group
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 4, reservado: 0x0, identificação: DH_GROUP_1024_MODP/Group
IKEv2-PROTO-4:     último transforme: 0x0, reservado: 0x0: comprimento
  tipo: 4, reservado: 0x0, identificação: DH_GROUP_768_MODP/Group 1
```

Payload seguinte **KE**: N, reservado: 0x0, comprimento: 104
Grupo DH: 1, reservado: 0x0

ed 4a 54 b1 13 7c b8 89 dos Cb 2e d1 28 fe eb 5e 29
f7 62 13 6b df 95 88 28 vagabundos b5 97 52 e4 ef 1d 28
Ca 06 d1 36 b6 67 dd 4e d8 c7 80 de 20 32 9a c2
36 34 ed 5f c5 b3 3e 1d 83 1a c7 fb 9d b8 c5 f5
vagabundos 4f b6 b2 e2 2d dos vagabundos 43 4f a0 b6 90 9a 11 3f 7c
0a 21 c3 4d d3 0a d2 1e 33 43 E0 d3 5e centímetro cúbico 4b 38
Payload seguinte **N**: VID, reservado: 0x0, comprimento: 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
ce 7c 0b b4
IKEv2-PROTO-5: Analise gramaticalmente o payload específico do vende
Payload seguinte CISCO-DELETE-REASON VID: VID, reservado: 0x0, comprimento: 23
Pacote decifrado: Dados: 528 bytes
IKEv2-PLAT-3: Cargas úteis feitas sob encomenda do processo VID
IKEv2-PLAT-3: Cisco Copyright VID recebido do par
IKEv2-PLAT-3: AnyConnect EAP VID recebido do par
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IN
EV_RECV_INIT
IKEv2-PROTO-3: (6): Verifique a descoberta NAT
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IN
EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): Reoriente a verificação não é precisado, saltando a
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IN
EV_CHK_CAC
IKEv2-PLAT-5: **Pedido novo ikev2 sa admitido**
IKEv2-PLAT-5: Incrementando a contagem de negócio entrante sa por um
IKEv2-PLAT-5: PUNHO INVÁLIDO PSH
IKEv2-PLAT-5: PUNHO INVÁLIDO PSH
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IN
EV_CHK_COOKIE
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento IN
EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_
EV_VERIFY_MSG
IKEv2-PROTO-3: (6): **Verifique a mensagem do init SA**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_
EV_INSERT_SA
IKEv2-PROTO-3: (6): Introduza o SA
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_
EV_GET_IKE_POLICY
IKEv2-PROTO-3: (6): **Obtendo políticas configuradas**

O ASA verifica e processa Mensagem IKE_INIT. O ASA:

1. Escolhe a série cripto de aqueles oferecidos pelo iniciador.
2. Computa sua própria chave secreta DH.
3. Computa um valor SKEYID de qual todas as chaves podem ser derivadas para este IKE_SA. Os encabeçamentos de tudo os mensagens subsequente são cifrado e autenticado. chaves usadas para a criptografia e a proteção da integridade é derivada de SKEYID e são sabidos como:

   SK_e - Criptografia.**SK_a** - Autenticação.**SK_d** - Derivado e usado para a derivação de mais adicional material de ajuste para CHILD_SAs.Um SK_e e um SK_a separados são computado para cada sentido.

Configuração relevante:

```
crypto ikev2 policy 10
 encryption aes-192 integrity
sha group 2  prf sha lifetime
seconds 86400
crypto ikev2 enable outside
```

IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_EV_PROC_MSG
IKEv2-PROTO-2: (6): Processando a mensagem inicial
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_EV_DETECT_NAT
IKEv2-PROTO-3: (6): A descoberta do processo NAT notifica
IKEv2-PROTO-5: (6): Processar nat detecta o src para notificar
IKEv2-PROTO-5: (6): Endereço remoto não combinado
IKEv2-PROTO-5: (6): Processar nat detecta o dst para notificar
IKEv2-PROTO-5: (6): Endereço local combinado
IKEv2-PROTO-5: (6): O host é NAT encontrado fora
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Dados válidos recebidos do modo de configuração
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3: (6): Ajuste dados recebidos do modo de configuração
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_SET_POLICY
IKEv2-PROTO-3: (6): Ajustando políticas configuradas
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_CHK_AUTH4PKI
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_PKI_SESH_OPEN
IKEv2-PROTO-3: (6): Abrindo uma sessão PKI
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GEN_DH_KEY
IKEv2-PROTO-3: (6): Chave pública de computação DH
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_NO_EVENT
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_OK_RECD_DH_PUBKEY_RESP
IKEv2-PROTO-5: (6): Ação: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GEN_DH_SECRET
IKEv2-PROTO-3: (6): Chave secreta de computação DH
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_NO_EVENT
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B

R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5: (6): Ação: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GEN_SKEYID
IKEv2-PROTO-3: (6): **Gerencia o skeyid**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: EV_GET_CONFIG_MODE

O ASA constrói o mensagem de resposta para a troca IKE_SA_INIT.
Este pacote contém:

1. **Encabeçamento ISAKMP** - SPI/version/flags.
2. **SAr1** - Algoritmo criptográfico que o que responde IKE escolhe.
3. **KEr** - Valor de chave pública DH do que responde.
4. **N** - Nonce do que responde.

IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_BLD_INIT: **EV_BLD_MSG**
IKEv2-PROTO-2: (6): **Enviando a mensagem inicial**
IKEv2-PROTO-3: Proposta IKE: 1, tamanho SPI: 0 (negociação inicial), Numérico. transforma: 4
AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Group 1
IKEv2-PROTO-5: Payload específico do vendedor da construção: DELET
REASONIKEv2-PROTO-5: Payload específico do vendedor da construçã
(CUSTOM)IKEv2-PROTO-5: Payload específico do vendedor da construç
(CUSTOM)IKEv2-PROTO-5: A construção notifica o payload: NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: A construção notifica o payload: NAT_DETECTION_DESTINATION_IPIKEv2-PLAT-2: Não recup confiou que os expedidores picam ou nenhuns disponíveis
IKEv2-PROTO-5: Payload específico do vendedor da construção: FRAGMENTATIONIKEv2-PROTO-3: Tx [L m_id 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0]: 0x0
IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B** - r: FC696330E6B94D7F]
IKEv2-PROTO-4: **Ispi** IKEV2 HDR**: 58AFF71141BA436B - rspi: FC696330E6B94D7F**
IKEv2-PROTO-4: Payload seguinte: SA, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_SA_INIT, **bandeiras: QUE RESPONI MSG-RESPONSE**
IKEv2-PROTO-4: ID de mensagem: 0x0, comprimento: 386
Payload seguinte **SA**: KE, reservado: 0x0, comprimento: 48
IKEv2-PROTO-4: última proposta: 0x0, reservado: 0x0, comprimento: 44
Proposta: 1, ID de protocolo: IKE, tamanho SPI: 0, #trans: 4
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento tipo: 2, reservado: 0x0, identificação: SHA1
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento tipo: 3, reservado: 0x0, identificação: SHA96
IKEv2-PROTO-4: último transforme: 0x0, reservado: 0x0: comprimento tipo: 4, reservado: 0x0, identificação: DH_GROUP_768_MODP/Group 1

Payload seguinte **KE**: N, reservado: 0x0, comprimento: 104
Grupo DH: 1, reservado: 0x0

c9 30 f9 32 d4 7c d1 a7 5b 71 72 09 6e 7e 91 0c
ce b4 a4 3c f2 8b 74 4e 20 do E1 59 b4 0b a1 ff 65
37 88 fá 4a 63 centímetro cúbico c4 a4 b6 03 93 89 E1 7e BD 6a
64 9a 38 24 e2 a8 40 f5 a3 d6 f7 ef 1a df 33 centímetros cúbicos

C.C. 9c 34 do fá a1 8e 45 79 1a 7c 29 05 87 8a C.A. 02
98 Cb 41 2e 7d fc c7 76 fe 51 d6 83 1d 03 b0 d7
Payload seguinte **N**: VID, reservado: 0x0, comprimento: 24

ec 97 b8 67 eb f1 97 do fc c2 28 7f 8c 7d b3 1e 51
d5 e7 c2 f5
Payload seguinte VID: VID, reservado: 0x0, comprimento: 23

O ASA manda o mensagem de resposta para a troca IKE_SA_INIT. A troca IKE_SA_INIT está agora completa. O ASA começa o temporizador para o processo de autenticação.

IKEv2-PLAT-4: [IKE_SA_INIT] ENVIADO [10.0.0.1]:500->[192.168.1.1]:25170 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000000 de PACOTE
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento INIT_DONE: EV_DONE
IKEv2-PROTO-3: (6): A fragmentação é permitida
IKEv2-PROTO-3: (6): Cisco DeleteReason Notify é permitido
IKEv2-PROTO-3: (6): Troca completa do init SA
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento INIT_DONE: EV_CHK4_ROLE
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento INIT_DONE: EV_START_TMR
IKEv2-PROTO-3: (6): Começando o temporizador esperar a mensagem do AUTH (segundo 30)
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Evento R_WAIT_AUTH: EV_NO_EVENT

----------IKE_SA_INIT terminam----------
---------- IKE_AUTH começa----------

****
Data: 04/23/2013
Tempo: 16:25:00
Digite: Informações
Fonte: acvpnagent

Descrição: Fixe parâmetros de gateway:
Endereço IP: 10.0.0.1
Porta: 443
URL: "10.0.0.1"

****
Data: 04/23/2013
Tempo: 16:25:02
Digite: Informações
Fonte: acvpnagent

Descrição: Função: CIPsecProtocol:: initiateTur
Arquivo: . \ IPsecProtocol.c
Linha: 345
O túnel de IPsec está inicia
****

Método do AUTH: **IKE - EAP-AnyConnect**
Identidade IKE:
****

Data: 04/23/2013
Tempo: 16:25:00
Digite: Informações
Fonte: acvpnagent

Descrição: **Iniciando a conexão do Cliente de mobilidade Cisco AnyConne**
Secure, versão 3.0.1047
****

Data: 04/23/2013
Tempo: 16:25:02
Digite: Informações
Fonte: acvpnagent

Descrição: Função: ikev2_log
Arquivo: .\ikev2_anyconnect_osal.cpp
Linha: 2730
Pedido recebido estabelecer um túnel de IPsec; seletor = escala de ende
tráfego local: 0.0.0.0-255.255.255.255 Protocolo: 0 intervalos de porta: 0-
seletor = escala de endereço remotos do tráfego: 0.0.0.0-255.255.255.25
Protocolo: 0 intervalos de porta: 0-65535
****

Data: 04/23/2013
Tempo: 16:25:02
Digite: Informações
Fonte: acvpnagent

Descrição: Função: CIPsecProtocol:: connectTransport
Arquivo: . \ IPsecProtocol.cpp
Linha: 1629
Soquete aberto IKE de 192.168.1.1:25171 a 10.0.0.1:4500
****

A autenticação é feita com EAP. Somente um único método de autenticação de EAP é permitido dentro de uma conversação EAP. O ASA recebe a mensagem IKE_AUTH do cliente.

IKEv2-PLAT-4: **[IKE_AUTH]** [192.168.1.1]:25171->[10.0.0.1] **RECV PACC**
4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000001
IKEv2-PROTO-3: **RX** [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:

Quando o cliente incluir um payload IDi
mas não um payload do AUTH, isto indica
o cliente declarou uma identidade mas tem-na não provado lhe. No debuga, o AUTH
o payload não está atual no IKE_AUTH
pacote enviado pelo cliente. O cliente

IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B** - r: FC696330E6B94D7F]
IKEv2-PROTO-4: **Ispi** IKEV2 **HDR: 58AFF71141BA436B - rspi:**
FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, **versão: 2.0**
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, **bandeiras: INICIADOR**
IKEv2-PROTO-4: ID de mensagem: 0x1, comprimento: 540
IKEv2-PROTO-5: (6): O pedido tem o mess_id 1; 1 previsto a 1
Pacote decifrado REAL: Dados: 465 bytes
IKEv2-PROTO-5: Analise gramaticalmente o payload específico do vende
(COSTUME) payload seguinte VID: IDi, reservado: 0x0, comprimento: 20

58 af f6 11 52 8d b0 2c b8 a Dinamarca 30 46 sejam 91 56 fá

envia o payload do AUTH somente depois
A troca EAP é bem sucedida. Se o ASA
é disposto usar um elástico método de autenticação, coloca um EAP
o payload na mensagem 4 e adia a emissão
SAr2, TSi, e TSr até o iniciador
a autenticação está completa na
troca subsequente IKE_AUTH.
O pacote do iniciador IKE_AUTH contém:

1. **Encabeçamento ISAKMP** - SPI/version/flags.
2. **IDi** - O nome de grupo de túneis isso
os desejos do cliente a conectar a
pode ser entregado pelo IDi
payload do tipo ID_KEY_ID dentro
a mensagem inicial do Troca IKE_AUTH. Isto
ocorre quando o profile* do cliente for
preconfigured com um nome do grupo
ou, após um bem sucedido precedente
a autenticação, o cliente tem
pôs em esconderijo o nome do grupo no seu arquivo das preferências.
O ASA
tentativas de combinar um grupo de túneis
nome com os índices do IKE
Payload IDi. Após o primeiro
o IPSec VPN bem

Payload seguinte **IDi**: CERTREQ, reservado: 0x0, comprimento: 28
Tipo identificação: Nome do grupo, reservado: 0x0 0x0
2a 24 41 6e 79 43 6f 6e 6e 65 63 74 43 6c 69 65
6e 74 24 2a
Payload seguinte **CERTREQ**: CFG, reservado: 0x0, comprimento: 25
CERT que codifica o certificado X.509 - assinatura
Data&colon de CertReq; 20 bytes
Payload seguinte **CFG**: SA, reservado: 0x0, comprimento: 196
tipo do cfg: **CFG_REQUEST**, reservado: 0x0, reservado: 0x0
tipo do attrib: endereço IP4 interno, comprimento: 0
tipo do attrib: netmask IP4 interno, comprimento: 0
tipo do attrib: IP4 interno DNS, comprimento: 0
tipo do attrib: IP4 interno NBNS, comprimento: 0
tipo do attrib: expiração do endereço interno, comprimento: 0
tipo do attrib: versão de aplicativo, comprimento: 27
41 6e 79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f
77 73 20 33 2e 30 2e 31 30 34 37
tipo do attrib: endereço IP6 interno, comprimento: 0
tipo do attrib: sub-rede IP4 interna, comprimento: 0
tipo do attrib: Desconhecido - 28682, comprimento: 15
77 69 6e 78 70 36 34 74 65 6d 70 6c 61 74 65
tipo do attrib: Desconhecido - 28704, comprimento: 0
tipo do attrib: Desconhecido - 28705, comprimento: 0
tipo do attrib: Desconhecido - 28706, comprimento: 0
tipo do attrib: Desconhecido - 28707, comprimento: 0
tipo do attrib: Desconhecido - 28708, comprimento: 0
tipo do attrib: Desconhecido - 28709, comprimento: 0
tipo do attrib: Desconhecido - 28710, comprimento: 0
tipo do attrib: Desconhecido - 28672, comprimento: 0
tipo do attrib: Desconhecido - 28684, comprimento: 0
tipo do attrib: Desconhecido - 28711, comprimento: 2
05 7e

sucedido é
estabelecido, os caches de cliente
nome do grupo (grupo aliás) a que
o usuário autenticado. Este grupo
o nome é entregado no IDi
payload da conexão seguinte
tentativa a fim indicar
grupo provável desejado pelo
usuário. Quando a
autenticação de EAP for
especificado ou
implicado pelo cliente
o perfil e o perfil não fazem
contenha o <IKEIdentity>
o elemento, o cliente envia
Tipo payload ID_GROUP IDi
com a corda fixa
$AnyConnectClient$.

3. **CERTREQ** - O cliente é pedindo o ASA para a certificado preferido. Certificado
as cargas úteis do pedido podem ser incluídas
em uma troca quando o remetente
precisa de obter o certificado do
receptor. O pedido do certificado
o payload é processado por
inspeção “da codificação CERT”
campo a fim determinar se o processador tem alguns

tipo do attrib: Desconhecido - 28674, comprimento: 0
tipo do attrib: Desconhecido - 28712, comprimento: 0
tipo do attrib: Desconhecido - 28675, comprimento: 0
tipo do attrib: Desconhecido - 28679, comprimento: 0
tipo do attrib: Desconhecido - 28683, comprimento: 0
tipo do attrib: Desconhecido - 28717, comprimento: 0
tipo do attrib: Desconhecido - 28718, comprimento: 0
tipo do attrib: Desconhecido - 28719, comprimento: 0
tipo do attrib: Desconhecido - 28720, comprimento: 0
tipo do attrib: Desconhecido - 28721, comprimento: 0
tipo do attrib: Desconhecido - 28722, comprimento: 0
tipo do attrib: Desconhecido - 28723, comprimento: 0
tipo do attrib: Desconhecido - 28724, comprimento: 0
tipo do attrib: Desconhecido - 28725, comprimento: 0
tipo do attrib: Desconhecido - 28726, comprimento: 0
tipo do attrib: Desconhecido - 28727, comprimento: 0
tipo do attrib: Desconhecido - 28729, comprimento: 0

Payload seguinte **SA**: TSi, reservado: 0x0, comprimento: 124
IKEv2-PROTO-4: última proposta: 0x0, reservado: 0x0, comprimento: 12
Proposta: 1, ID de protocolo: ESP, tamanho SPI: 4, #trans: 12
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 1, reservado: 0x0, identificação: 3DES
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 1, reservado: 0x0, identificação: DES
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 1, reservado: 0x0, identificação: NULO
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 3, reservado: 0x0, identificação: SHA512
IKEv2-PROTO-4: último transforme: 0x3, reservado: 0x0: comprimento
tipo: 3, reservado: 0x0, identificação: SHA384

Certificados deste tipo. Em caso afirmativo, O campo da “autoridade de certificação” é inspecionado a fim determinar se o processador tem todos os Certificados isso pode ser validado até um de a certificação especificada autoridades. Esta pode ser uma corrente de Certificados.

4. **CFG** - CFG_REQUEST/ CFG_REPLY permite um IKE valor-limite para pedir a informação de seu par. Se um atributo no Configuração CFG_REQUEST o payload não está a um zero-comprimento, ele é tomado como uma sugestão para isso atributo. O CFG_REPLY o payload da configuração pode retornar esse valor ou um novo. Pode igualmente adicionar atributos novos e não inclua algum pediu. Os utilizadores ignoram retornado atributos que não fazem reconheça. Nestes debuga, o cliente está pedindo o túnel configuração no CFG_REQUEST. O ASA as respostas a esta e

```
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: SHA256
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: SHA96
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: MD596
IKEv2-PROTO-4:     último transforme: 0x0, reservado: 0x0: comprimento
  tipo: 5, reservado: 0x0, identificação:

 Payload seguinte de TSi: TSr, reservado: 0x0, comprimento: 24
   Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
   Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento:
   porta do começo: 0, porta da extremidade: 65535
   ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
 Payload seguinte de TSr: NOTIFIQUE, reservou: 0x0, comprimento: 24
   Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
   Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento:
   porta do começo: 0, porta da extremidade: 65535
   ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
```

enviam o túnel
atributos de configuração
somente depois
a troca EAP é bem
sucedida.

5. **SAi2** - SAi2 inicia o SA, qual é similar à fase 2 transforme a troca do grupo em IKEv1.
6. **TSi** e **TSr** - O iniciador e seletores do tráfego do que responde contenha, respectivamente, a fonte e endereço de destino do
iniciador e que responde envie e receba cifrado tráfego. A escala de endereço
especifica que todo o tráfego a e de
essa escala é escavada um túnel. Se a
a proposta é aceitável ao que responde, envia o TS idêntico
as cargas úteis
suportam.

Os atributos que o cliente deve entregar para a autenticação do grupo é armazenada no Arquivo de perfil de AnyConnect.

Configuração de perfil

***Relevant:**

```
<ServerList>
<HostEntry>
 <HostName>Anu-IKEV2
</HostName>
 <HostAddress>10.0.0.1
</HostAddress>
 <UserGroup>ASA-IKEV2
</UserGroup>
<PrimaryProtocol>IPsec
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

O ASA gerencie uma resposta à mensagem IKE_AUTH e prepara-se para autenticar-se

Pacote decifrado: Data: 540 bytes
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento

ao cliente.

R_WAIT_AUTH: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Parando o temporizador para esperar a mensagem AUTH
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_CHK_NAT_T
IKEv2-PROTO-3: (6): Verifique a descoberta NAT
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_CHG_NAT_T_PORT
IKEv2-PROTO-2: (6): Flutuador detectado NAT à porta 25171 do init, port do resp
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_PROC_ID
IKEv2-PROTO-2: (6): Parameteres válidos recebidos na identificação de processo
IKEv2-PLAT-3: (6) método do AUTH do par ajustado a: 0
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEI
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Obtendo políticas configuradas
IKEv2-PLAT-3: Conexão de cliente nova de AnyConnect detectada basea payload ID
IKEv2-PLAT-3: my_auth_method = 1
IKEv2-PLAT-3: (6) método do AUTH do par ajustado a: 256
IKEv2-PLAT-3: supported_peers_auth_method = 16
IKEv2-PLAT-3: (6) tp_name ajustado a: Anu-ikev2
IKEv2-PLAT-3: **ponto da confiança ajustado a:** Anu-ikev2
IKEv2-PLAT-3: P1 ID= 0
IKEv2-PLAT-3: Traduzindo IKE_ID_AUTO a = 9
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_SET_POLICY
IKEv2-PROTO-3: (6): **Ajustando políticas configuradas**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Verifique a política do par
IKEv2-PROTO-3: (6): **Certificado de harmonização encontrado**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Dados válidos recebidos do modo de configuração
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_WAIT_AUTH: EV_SET_RECD_CONFIG_MODE
IKEv2-PLAT-3: (6) o hostname DHCP para o DDNS é ajustado a: winxp64template

IKEv2-PROTO-3: (6): Ajuste dados recebidos do modo de configuração
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_CHK_AUTH4EAP
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_WAIT_AUTH: EV_CHK_EAP
IKEv2-PROTO-3: (6): **Verifique para ver se há a troca EAP**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Gerencia meus dados de autenticação**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_CHK4_SIGN
IKEv2-PROTO-3: (6): Obtenha meu método de autenticação
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_SIGN
IKEv2-PROTO-3: (6): **Dados do AUTH do sinal**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_BLD_AUTH: EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_BLD_EAP_AUTH_REQ: EV_AUTHEN_REQ
IKEv2-PROTO-2: (6): **Pedindo o autenticador para enviar o pedido EAP**
Valor criado do configuração-**AUTH do** nome de elemento
Vpn adicionado do valor do cliente do nome do atributo ao configuração-A
do elemento
O nome adicionado do atributo datilografa o valor olá! ao configuração-AU
elemento
Valor criado 9.0(2)8 da versão do nome de elemento
Valor adicionado 9.0(2)8 da versão do nome de elemento ao configuraçã
do elemento
Nome adicionado do atributo que avalia o SG à versão do elemento
Mensagem gerada XML abaixo
<? xml version="1.0" encoding="UTF-8"?>
type= " do " vpn do client=” do <config-AUTH **olá!** " >
<version who="sg">9.0(2)8</version>
</config-auth>

IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_BLD_EAP_AUTH_REQ: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: (6): Ação: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento
R_BLD_EAP_AUTH_REQ: EV_CHK_REDIRECT
IKEv2-PROTO-3: (6): Reoriente a verificação com plataforma para a funç
balanceamento de carga
IKEv2-PLAT-3: Reoriente a verificação na plataforma
IKEv2-PLAT-3: ikev2_osal_redirect: Sessão aceitada por 10.0.0.1

IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Evento R_BLD_EAP_AUTH_REQ: EV_SEND_EAP_AUTH_REQ
IKEv2-PROTO-2: (6): **Enviando o pedido EAP**
IKEv2-PROTO-5: Payload específico do vendedor da construção: CISCO-GRANITEIKEv2-PROTO-3: (6): Construção
Payload seguinte **IDr**: CERT, reservado: 0x0, comprimento: 36
Tipo identificação: ASN1 DN DER, reservado: 0x0 0x0

30 1a 31 18 30 16 06 09 2a 86 48 86 f7 0d 01 09
02 16 09 41 53 41 2d 49 4b 45 56 32
Payload seguinte **CERT**: CERT, reservado: 0x0, comprimento: 436
CERT que codifica o certificado **X.509** - assinatura Data&colon CERT; 431 bytes
Payload seguinte CERT: AUTH, reservado: 0x0, comprimento: 436
CERT que codifica o certificado X.509 - assinatura Data&colon CERT; 431 bytes
Payload seguinte do **AUTH**: EAP, reservado: 0x0, comprimento: 136
Método RSA do AUTH, reservado: 0x0, 0x0 reservado Data&colon do AUTH; bytes 128
Payload seguinte **EAP**: NENHUNS, reservado: 0x0, comprimento: 154
Código: pedido: **identificação**: 1, **comprimento**: 150
Digite: Desconhecido - 254
Dados EAP: 145 bytes

IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f
IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B** - r: FC696330E6B94D7F]
IKEv2-PROTO-4: **Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F**
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, **bandeiras: QUE RESPONDE RESPONSE**
IKEv2-PROTO-4: ID de mensagem: 0x1, comprimento: 1292
Payload seguinte ENCR: VID, reservado: 0x0, comprimento: 1264 Data&colon cifrado; 1260 bytes

O ASA envia o payload do AUTH a fim pedir credenciais do usuário do cliente. O ASA envia o método do AUTH como o “RSA,” assim que ele envia seu próprio certificado ao cliente, assim que o cliente pode autenticar o server ASA. Desde que o ASA é disposto usar um método de autenticação extensível, coloca um payload EAP na mensagem 4 e adia a emissão de SAr2, de TSi, e de TSr até que a autenticação do iniciador esteja completa em uma troca subsequente IKE_AUTH. Assim, aquelas três cargas úteis não estão atuais no debugam.

O pacote EAP contém:

1. **Código: pedido** - Este código é enviado pelo autenticador ao par.
2. **identificação: 1** - A identificação ajuda o fósforo as respostas EAP com os pedidos. Aqui o valor é 1, que indica que é o primeiro pacote na troca EAP. Este pedido EAP tem o “configuração-AUTH” tipo de “olá!; ” é enviado do ASA ao cliente a fim iniciar a troca EAP.
3. **Comprimento: 150** - O comprimento do pacote EAP inclui o código, a identificação, o comprimento, e os dados EAP.
4. **Dados EAP**.

A fragmentação pode resultar se os Certificados são

IKEv2-PROTO-5: (6): Fragmentando o pacote, fragmento MTU: 544, **núm fragmentos: 3,** fragmento ID: 1

grandes ou se os certificates chain são incluídos. As cargas úteis do iniciador e do que responde KE podem igualmente incluir as grandes chaves, que podem igualmente contribuir à fragmentação.

```
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
****************************************
Data: 04/23/2013
Tempo: 16:25:02
Digite: Informações
Fonte: acvpnagent

Descrição: Função: ikev2_verify_X509_SIG_certs
Arquivo: .\ikev2_anyconnect_osal.cpp
Linha: 2077
Pedindo a aceitação do certificado do usuário
****************************************
Data: 04/23/2013
Tempo: 16:25:02
Digite: Erro
Fonte: acvpnui

Descrição: Função: CCapiCertificate:: verifyChainPolicy
Arquivo: . \ Certificados \ CapiCertificate.cpp
Linha: 2032
Função invocada: CertVerifyCertificateChainPolicy
Código de retorno: -2146762487 (0x800B0109)
Descrição: Um certificate chain processado, mas terminado em um certifi
raiz que não seja confiado pelo fornecedor da confiança.
****************************************
Data: 04/23/2013
Tempo: 16:25:04
Digite: Informações
Fonte: acvpnagent

Descrição: Função: CEAPMgr:: dataRequestCB
Arquivo: . \ EAPMgr.cpp
Linha: 400
Tipo proposto EAP: EAP-ANYCONNECT
****************************************
```

O cliente responde ao pedido EAP com uma resposta.
O pacote EAP contém:

1. **Código: resposta** - Este código é enviado pelo par ao autenticador em resposta ao pedido EAP.
2. **identificação: 1 -** A identificação ajuda o

```
IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
RECV PACOTE
IKEv2-PROTO-3: RX [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, bandeiras: INICIADOR
IKEv2-PROTO-4: ID de mensagem: 0x2, comprimento: 332
```

fósforo as respostas EAP com os pedidos. Aqui o valor é 1, que indica que esta é uma resposta ao pedido enviado previamente pelo ASA (autenticador). Esta resposta EAP tem o tipo do “configuração-AUTH” de “init”; o cliente está inicializando a troca EAP e está esperando o ASA para gerar o pedido de autenticação.

3. **Comprimento: 252** - O comprimento do pacote EAP inclui o código, a identificação, o comprimento, e os dados EAP.
4. **Dados EAP**.

O ASA decifra esta resposta, e o cliente diz que recebeu o payload do AUTH no pacote anterior (com o certificado) e recebeu o primeiro pacote de requisição EAP do ASA. Este é o que o pacote de resposta EAP do “init” contém.

IKEv2-PROTO-5: (6): O pedido tem o mess_id 2; 2 previstos a 2
Pacote decifrado REAL: Dados: bytes 256
Payload seguinte **EAP**: NENHUNS, reservado: 0x0, comprimento: 256
Código: resposta: **identificação: 1**, **comprimento**: 252
Digite: Desconhecido - 254
Bytes **EAP data:247**
Pacote decifrado: Data: 332 bytes
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Evento R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Parando o temporizador para esperar a mensagem AUTH
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Evento R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Evento R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Processando a resposta EAP**
Mensagem recebida XML abaixo do cliente
<? xml version="1.0" encoding="UTF-8"?>
type= " init " do " vpn” do client= do <config-AUTH >
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<group-select>ASA-IKEV2</group-select>
<group-access>ASA-IKEV2</group-access>
</config-auth>
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Evento R_PROC_EAP_RESP: **EV_RECV_EAP_AUTH**
IKEv2-PROTO-5: (6): Ação: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Evento R_BLD_EAP_REQ: **EV_RECV_EAP_REQ**

Este é o segundo pedido enviado pelo ASA ao cliente. O pacote EAP contém:

1. **Código: pedido** - Este código é enviado pelo autenticador ao par.
2. **identificação: 2** - A identificação ajuda o fósforo as respostas EAP com os pedidos. Aqui o valor é 2, que indica que é o segundo pacote na troca. Este pedido tem o tipo do “configuração-AUTH” de “solicitação de autorização”; o ASA está pedindo que o cliente

IKEv2-PROTO-2: (6): Enviando o pedido EAP
Mensagem gerada XML abaixo
<? xml version="1.0" encoding="UTF-8"?>
type= " solicitação de autorização " do " vpn” do client= do <config-AUTH >
<version who="sg">9.0(2)8</version>
is-for= " SG " do <opaque >
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash>
</opaque>
<csport>443</csport>
id= <authentic " cano principal " >
<form>
username” do label= " " username” do name= do " texto do type= do <input: “></input>
senha” do label= " da " senha” do name= da " senha do type= do <input: “></input>

****
Data: 04/23/2013
Tempo: 16:25:04
Digite: Informações
Fonte: acvpnui

Descrição: Função: SDIMgr:: ProcessPromptDa
Arquivo: . \ SDIMgr.cpp
Linha: 281
O tipo do autenticação não
****
Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnui

Descrição: Função: Connec
userResponse

envia as credenciais da autenticação de usuário.

3. **Comprimento: 457** - O comprimento do pacote EAP inclui o código, a identificação, o comprimento, e os dados EAP.
4. **Dados EAP**.

Payload **ENCR**:
Este payload é decifrado, e seus índices são analisados gramaticalmente como cargas úteis adicionais.

O cliente envia uma outra mensagem do iniciador IKE_AUTH com o payload EAP.

</form>
</authentic>
</config-auth>
IKEv2-PROTO-3: (6): Pacote de construção para a criptografia; os índices são:
Payload seguinte **EAP**: NENHUNS, reservado: 0x0, comprimento: 461
Código: pedido: identificação: 2, comprimento: 457
Digite: Desconhecido - 254
Dados EAP: 452 bytes

IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0]: 0x2
IKEv2-PROTO-3: **HDR[i:58AFF71141BA436B** - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, bandeiras: **QUE RESPONDE MSG-RESPONSE**
IKEv2-PROTO-4: ID de mensagem: 0x2, comprimento: 524
Payload seguinte **ENCR**: EAP, reservado: 0x0, comprimento: 496
Data&colon cifrado; 492 bytes

IKEv2-PLAT-4: **[IKE_AUTH] ENVIADO** [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000002 de **PACOTE**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Evento R_BLD_EAP_REQ: EV_START_TMR
IKEv2-PROTO-3: (6): **Começando o temporizador esperar a mensagem do AUTH do usuário** (segundo 120)
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Evento R_WAIT_EAP_RESP: EV_NO_EVENT
IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000 RECV PACOTE
IKEv2-PROTO-3: RX [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:

Arquivo: . \ ConnectMgr.cpp
Linha: 985
Processando a resposta de usuário.
****

O pacote EAP contém:

1. **Código: resposta** - Este código é enviado pelo par ao autenticador em resposta ao pedido EAP.
2. **identificação: 2** - A identificação ajuda o fósforo as respostas EAP com os pedidos. Aqui o valor é 2, que indica que esta é uma resposta ao pedido enviado previamente pelo ASA (autenticador).
3. **Comprimento: 420** - O comprimento do pacote EAP inclui o código, a identificação, o comprimento, e os dados EAP.
4. **Dados EAP**.

IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: **Tipo da troca: IKE_AUTH, bandeiras: INICIADOR**
IKEv2-PROTO-4: ID de mensagem: 0x3, comprimento: 492
IKEv2-PROTO-5: (6): O pedido tem o mess_id 3; 3 previstos a 3

Pacote decifrado REAL: Dados: 424 bytes
Payload seguinte **EAP**: NENHUNS, reservado: 0x0, comprimento: 424
Código: resposta: identificação: 2, comprimento: 420
Digite: Desconhecido - 254
Dados EAP: 415 bytes

O ASA processa esta resposta. O cliente tinha pedido que o usuário incorpora credenciais. Esta resposta EAP tem o tipo do “configuração-AUTH” de “autêntico-resposta.” Este pacote contém as credenciais incorporadas pelo usuário.

Pacote decifrado: Dados: 492 bytes
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Parando o temporizador para esperar a mensagem AUTH
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Processando a resposta EAP**
Mensagem recebida XML abaixo do cliente
<? xml version="1.0" encoding="UTF-8"?>
type= " autêntico-resposta " do " vpn” do client= do <config-AUTH >
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<session-token></session-token>
<session-id></session-id>
is-for= " SG " do <opaque >
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash></opaque>
<authentic>
<password>cisco123</password>
<username>Anu</username></authentic>
</config-auth>
IKEv2-PLAT-1: **EAP: Autenticação de usuário iniciada**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento

```
R_PROC_EAP_RESP: EV_NO_EVENT
IKEv2-PLAT-5: EAP: Na rechamada AAA
Resumo recuperado CERT do server:
DACE1C274785F28BA11D64453096BAE294A3172E
IKEv2-PLAT-5: EAP: sucesso na rechamada AAA
IKEv2-PROTO-3: Resposta recebida do autenticador
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento
R_PROC_EAP_RESP: EV_RECV_EAP_AUTH
IKEv2-PROTO-5: (6): Ação: Action_Null
```

O ASA constrói um terceiro pedido EAP na troca.
O pacote EAP contém:

1. **Código: pedido** - Este código é enviado pelo autenticador ao par.
2. **identificação: 3** - A identificação ajuda o fósforo as respostas EAP com os pedidos. Aqui o valor é 3, que indica que é o terceiro pacote na troca. Este pacote manda o tipo do “configuração-AUTH” de “terminar”; o ASA recebeu uma resposta, e a troca EAP está completa.
3. **Comprimento: 4235** - O comprimento do pacote EAP inclui o código, a identificação, o comprimento, e os dados EAP.
4. **Dados EAP**.

Payload **ENCR**:
Este payload é decifrado, e seus índices são analisados gramaticalmente como cargas úteis adicionais.

```
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento
R_BLD_EAP_REQ: EV_RECV_EAP_REQ
IKEv2-PROTO-2: (6): Enviando o pedido EAP
Mensagem gerada XML abaixo
<? xml version="1.0" encoding="UTF-8"?>
o type= " do " vpn do client=” do <config-AUTH termina " >
<version who="sg">9.0(2)8</version>
<session-id>32768</session-id>
<session-token>18wA0TtGmDxPKPQCJywC7fB7EWLCEgz-
ZtjYpAyXx2yJH0H3G3H8t5xpBOx3Ixag</session-token>
id= <authentic " sucesso " >
<message id="0" param1="" param2=""></message>
</authentic>

IKEv2-PROTO-3: (6): Pacote de construção para a criptografia; os índices
 Payload seguinte EAP: NENHUNS, reservado: 0x0, comprimento: 4239
  Código: pedido: identificação: 3, comprimento: 4235
  Digite: Desconhecido - 254
Dados EAP: 4230 bytes

IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, bandeiras: QUE RESPONDE
RESPONSE
IKEv2-PROTO-4: ID de mensagem: 0x3, comprimento: 4300
 Payload seguinte ENCR: EAP, reservado: 0x0, comprimento: 4272
Bytes data&colon;4268 cifrados
IKEv2-PROTO-5: (6): Fragmentando o pacote, fragmento MTU: 544, núm
fragmentos: 9, fragmento ID: 2
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
```

```
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento
R_BLD_EAP_REQ: EV_START_TMR
IKEv2-PROTO-3: (6): Começando o temporizador esperar a mensagem d
AUTH do usuário (segundo 120)
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Evento
R_WAIT_EAP_RESP: EV_NO_EVENT
***************************************
Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnagent

Descrição: Perfil atual: Anyconnect-ikev2.xml
Ajustes de configuração recebidos da sessão de VPN:
 Mantenha instalado: habilitado
 Ajustes do proxy: não altere
 Servidor proxy: nenhum
 Proxy PAC URL: nenhum
 Exceções de proxy: nenhum
 Lockdown do proxy: habilitado
 A separação exclui: a preferência do acesso do LAN local é desabilitada
 A separação inclui: Desabilitado
 DNS em divisão: Desabilitado
 Convite do LAN local: a preferência do acesso do LAN local é desabilitad
 Regras do Firewall: nenhum
 Endereço de cliente: 10.2.2.1
 Máscara do cliente: 255.0.0.0
 Endereço do IPv6 do cliente: desconhecido
 Máscara do IPv6 do cliente: desconhecido
 MTU: 1406
 Manutenção de atividade IKE: 20 segundos
 IKE DPD: 30 segundos
 Timeout de sessão: segundos 0
 Intervalo da disconexão: 1800 segundos
```

Idle timeout: 1800 segundos
Servidor: desconhecido
Host MUS: desconhecido
Mensagem do usuário DAP: nenhum
Estado da quarentena: Desabilitado
Sempre no VPN: não deficiente
Duração de aluguel: segundos 0
Domínio padrão: desconhecido
Home Page: desconhecido
Disconexão da remoção da placa inteligente: habilitado
Resposta da licença: desconhecido
****

O cliente envia o pacote do iniciador com o payload EAP. O pacote EAP contém:

1. **Código: resposta** - Este código é enviado pelo par ao autenticador em resposta ao pedido EAP.
2. **identificação: 3** - A identificação ajuda o fósforo as respostas EAP com os pedidos. Aqui o valor é 3, que indica que esta é uma resposta ao pedido enviado previamente pelo ASA (autenticador). O ASA recebe agora o pacote de resposta do cliente, que tem o tipo do "configuração-AUTH" de "ack"; esta resposta reconhece a mensagem "completa" EAP enviada previamente pelo ASA.
3. **Comprimento: 173** - O comprimento do pacote EAP inclui o código, a identificação, o comprimento, e os dados EAP.
4. **Dados EAP**.

IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
RECV PACOTE
IKEv2-PROTO-3: RX [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: **Tipo da troca: IKE_AUTH, bandeiras: INICIADOR**
IKEv2-PROTO-4: ID de mensagem: 0x4, comprimento: 252
IKEv2-PROTO-5: (6): O pedido tem o mess_id 4; 4 previstos a 4

Pacote decifrado REAL: Dados: 177 bytes
Payload seguinte **EAP**: NENHUNS, reservado: 0x0, comprimento: 177
Código: resposta: identificação: 3, comprimento: 173
Digite: Desconhecido - 254
Dados EAP: 168 bytes

O ASA processa este pacote. A troca EAP é bem sucedida.

Bytes packet:Data:252 decifrados
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Evento R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Parando o temporizador para esperar a mensagem AUTH
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B

O ASA prepara-se para enviar o grupo de túneis configuração no próximo pacote, que

foi pedido previamente pelo cliente dentro
o payload IDi. O ASA recebe pacote de resposta do cliente, que
tem o tipo do “configuração-AUTH” de “ack”. Isto
a resposta reconhece o EAP “termine” a mensagem que foi enviada pelo
ASA previamente.

Configuração relevante:

```
tunnel-group ASA-IKEV2
type remote-access
tunnel-group ASA-IKEV2
general-attributes
 address-pool webvpn1
 authorization-server-group
 LOCAL default-group-policy
ASA-IKEV2
tunnel-group ASA-IKEV2
webvpn-attributes
 group-alias ASA-IKEV2
enable
```

A troca EAP é agora bem sucedida.

O pacote EAP contém:

1. Código: **sucesso** - Este código é
   enviado pelo
   autenticador ao
   par após conclusão de um EAP
   método de autenticação. Isto
   indica que o par tem
   autenticado com
   sucesso ao
   autenticador.
2. **identificação: 3** - A
   identificação ajuda o fósforo
   Respostas EAP com os pedidos.
   Aqui o valor é 3, que
   indica que esta é uma resposta a
   o pedido enviado
   previamente pelo
   ASA (autenticador). O terceiro grupo
   dos pacotes na troca era

R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Evento R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Evento R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Processando a resposta EAP**
Mensagem recebida XML abaixo do cliente
<? xml version="1.0" encoding="UTF-8"?>
type= " ack " do " vpn” do client= do <config-AUTH >
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
</config-auth>

IKEv2-PLAT-3: (6) aggrAuthHdl ajustado a 0x2000
IKEv2-PLAT-3: (6) **tg_name ajustado a: ASA-IKEV2**
IKEv2-PLAT-3: (6) **tipo do grp do tunn ajustado a: RA**
IKEv2-PLAT-1: **EAP: Autenticação bem sucedida**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Evento R_PROC_EAP_RESP: EV_RECV_EAP_SUCCESS
IKEv2-PROTO-2: (6): Enviando o mensagem de status EAP
IKEv2-PROTO-3: (6): Pacote de construção para a criptografia; os índices
 Payload seguinte **EAP**: NENHUNS, reservado: 0x0, comprimento: 8
  Código: sucesso: identificação: 3, comprimento: 4

IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, bandeiras: QUE RESPONDE RESPONSE
IKEv2-PROTO-4: ID de mensagem: 0x4, comprimento: 76
 Payload seguinte ENCR: EAP, reservado: 0x0, comprimento: 48
Bytes data:44 cifrados

IKEv2-PLAT-4: **[IKE_AUTH] ENVIADO** [10.0.0.1]:4500->[192.168.1.1]:251 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000 **PACOTE**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Evento R_PROC_EAP_RESP: EV_START_TMR
IKEv2-PROTO-3: (6): Começando o temporizador esperar a mensagem d AUTH (segundo 30)
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Evento **R_WAIT_EAP_AUTH_VERIFY**: EV_NO_EVENT

bem sucedido, e a troca EAP
é bem sucedido.

3. **Comprimento: 4** - Comprimento do EAP o pacote inclui o código, identificação, comprimento, e dados EAP.
4. **Dados EAP**.

Desde que a troca EAP é bem sucedida, o cliente envia o pacote do iniciador IKE_AUTH com o payload do AUTH. O payload do AUTH é gerado da chave secreta compartilhada.

IKEv2-PLAT-4: [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
RECV PACOTE
IKEv2-PROTO-3: RX [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, **bandeiras: INICIADOR**
IKEv2-PROTO-4: ID de mensagem: 0x5, comprimento: 92
IKEv2-PROTO-5: (6): O pedido tem o mess_id 5; 5 previsto a 5

Bytes packet:Data:28 decifrados REAIS
Payload seguinte do **AUTH**: NENHUNS, reservado: 0x0, comprimento: 2
Método PSK do AUTH, reservado: 0x0, 0x0 reservado
Dados do AUTH: 20 bytes
Pacote decifrado: Dados: 92 bytes

Quando a autenticação de EAP for especificada ou implicado pelo perfil do cliente e
o perfil não contém o elemento do <IKEIdentity>, o cliente envia um tipo payload ID_GROUP IDi com a corda fixa *$AnyConnectClient$*. O ASA processa esta mensagem.

IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_WAIT_EAP_AUTH_VERIFY: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Parando o temporizador para esperar a mensagem AUTH
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_GET_EAP_KEY
IKEv2-PROTO-2: (6): Envie o AUTH, para verificar o par depois que troca
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_VERIFY_AUTH
IKEv2-PROTO-3: (6): **Verifique dados de autenticação**
IKEv2-PROTO-3: (6): **Use a chave preshared para a identificação *$AnyConnectClient$*, chave len 20**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_GET_CONFIG_MODE
IKEv2-PLAT-3: Resposta do modo de configuração enfileirada
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_NO_EVENT
IKEv2-PLAT-3: PSH: client-os-version= dos client-os=Windows do client=AnyConnect client-version=3.0.1047

Configuração relevante:

```
crypto dynamic-map dynmap 1000
set ikev2 ipsec-proposal 3des
crypto map crymap 10000
ipsec-isakmp dynamic dynmap
crypto map crymap interface
outside
```

IKEv2-PLAT-3: Resposta do modo de configuração terminada
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_OK_GET_CONFIG
IKEv2-PROTO-3: (6): Tenha os dados do modo de configuração a enviar
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_CHK4_IC
IKEv2-PROTO-3: (6): Processando o contato inicial
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): Reoriente a verificação é feito já para esta sessão, saltando a
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_PROC_SA_TS
IKEv2-PROTO-2: (6): **Processando a mensagem do AUTH**
IKEv2-PLAT-1: **Crypto map: Dynmap 1000 segs.s do mapa. Seletor ajusta usando o IP atribuído**
IKEv2-PLAT-3: **Crypto map: fósforo no dynmap 1000 segs.s do mapa din**
IKEv2-PLAT-3: PFS desabilitado para a conexão RA
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_NO_EVENT
IKEv2-PLAT-2: Rechamada recebida PFKEY SPI para SPI 0x30B848A4, FALSO
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_VERIFY_AUTH: EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2: (6): **Processando a mensagem do AUTH**

O ASA constrói o mensagem de resposta IKE_AUTH com as cargas úteis SA, de TSi, e de TSr.
O pacote do que responde IKE_AUTH contém:

1. **Encabeçamento ISAKMP** - SPI/version/flags.
2. **Payload do AUTH** - Com o método de autenticação escolhido.
3. **CFG** - CFG_REQUEST/CFG_REPLY permite que um ponto final IKE peça a informação de seu par. Se um atributo no payload da configuração CFG_REQUEST não

IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento **R_BLD_AUTH**: EV_MY_AUTH_METHOD
IKEv2-PROTO-3: (6): **Obtenha meu método de autenticação**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_BLD_AUTH: EV_GET_PRESHR_KEY
IKEv2-PROTO-3: (6): **Obtenha a chave preshared do par para *$AnyConnectClient$***
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_BLD_AUTH: EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Gerencia meus dados de autenticação**
IKEv2-PROTO-3: (6): **Use a chave preshared para a identificação hostname=ASA-IKEV2, chave len 20**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento R_BLD_AUTH: EV_CHK4_SIGN
IKEv2-PROTO-3: (6): Obtenha meu método de autenticação
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento

está a um zero-comprimento, está tomado como uma sugestão para esse atributo. O payload da configuração CFG_REPLY pode retornar esse valor ou um novo. Pode igualmente adicionar atributos novos e para não incluir algum pediu. Os utilizadores ignoram os atributos retornados que não reconhecem. O ASA responde ao cliente com os atrributes da configuração de túnel no pacote CFG_REPLY.

4. **SAr2** - SAr2 inicia o SA, que é similar à fase 2 transforma a troca do grupo em IKEv1.
5. **TSi** e **TSr** - Os seletores do tráfego do iniciador e do que responde contêm, respectivamente, o endereço de rementente e destinatário do iniciador e o que responde a fim enviar e receber o tráfego criptografado. A escala de endereço especifica que todo o tráfego a e dessa escala está escavado um túnel. Se a proposta é aceitável ao que responde, envia cargas úteis idênticas TS para trás.

Payload **ENCR**:
Este payload é decifrado, e seus índices são analisados gramaticalmente como cargas úteis adicionais.

R_BLD_AUTH: EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento
R_BLD_EAP_AUTH_VERIFY: EV_GEN_AUTH
IKEv2-PROTO-3: (6): Gerencia meus dados de autenticação
IKEv2-PROTO-3: (6): Use a chave preshared para a identificação
hostname=ASA-IKEV2, chave len 20
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento
R_BLD_EAP_AUTH_VERIFY: EV_SEND_AUTH
IKEv2-PROTO-2: (6): **Envie o AUTH, para verificar o par depois que troca**
IKEv2-PROTO-3: Proposta ESP: 1, tamanho SPI: 4 (negociação de IPSe
Numérico. transforma: 3
AES-CBC SHA96
IKEv2-PROTO-5: A construção notifica o payload:
ESP_TFC_NO_SUPPORTIKEv2-PROTO-5: A construção notifica o paylo
NON_FIRST_FRAGSIKEv2-PROTO-3: (6): Pacote de construção para a
criptografia; os índices são:
Payload seguinte do **AUTH**: CFG, reservado: 0x0, comprimento: 28
Método PSK do AUTH, reservado: 0x0, 0x0 reservado
Data&colon do AUTH; 20 bytes
Payload seguinte **CFG**: SA, reservado: 0x0, comprimento: 4196
tipo do cfg: **CFG_REPLY,** reservado: 0x0, reservado: 0x0

tipo do attrib: endereço IP4 interno, comprimento: 4

01 01 01 01
tipo do attrib: netmask IP4 interno, comprimento: 4

00 00 00 00
tipo do attrib: expiração do endereço interno, comprimento: 4

00 00 00 00
tipo do attrib: versão de aplicativo, comprimento: 16

41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
tipo do attrib: Desconhecido - 28704, comprimento: 4

00 00 00 00
tipo do attrib: Desconhecido - 28705, comprimento: 4

00 00 07 08
tipo do attrib: Desconhecido - 28706, comprimento: 4

00 00 07 08
tipo do attrib: Desconhecido - 28707, comprimento: 1

01
tipo do attrib: Desconhecido - 28709, comprimento: 4

00 00 00 1e
tipo do attrib: Desconhecido - 28710, comprimento: 4

```
  00 00 00 14
 tipo do attrib: Desconhecido - 28684, comprimento: 1

  01
 tipo do attrib: Desconhecido - 28711, comprimento: 2

  05 7e
 tipo do attrib: Desconhecido - 28679, comprimento: 1

  00
 tipo do attrib: Desconhecido - 28683, comprimento: 4

  80 0b 00 01
 tipo do attrib: Desconhecido - 28725, comprimento: 1

  00
 tipo do attrib: Desconhecido - 28726, comprimento: 1

  00
 tipo do attrib: Desconhecido - 28727, comprimento: 4056

  3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31
  2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54
  46 2d 38 22 3f 3e 3c 63 6f 6e 66 69 67 2d 61 75
  74 68 20 63 6c 69 65 6e 74 3d 22 76 70 6e 22 20
  74 79 70 65 3d 22 63 6f 6d 70 6c 65 74 65 22 3e
  3c 76 65 72 73 69 6f 6e 20 77 68 6f 3d 22 73 67
  22 3e 31 30 30 2e 37 28 36 29 31 31 36 3c 2f 76
  65 72 73 69 6f 6e 3e 3c 73 65 73 73 69 6f 6e 2d
  69 64 3e 38 31 39 32 3c 2f 73 65 73 73 69 6f 6e
<snip>
  72 6f 66 69 6c 65 2d 6d 61 6e 69 66 65 73 74 3e
  3c 2f 63 6f 6e 66 69 67 3e 3c 2f 63 6f 6e 66 69
  67 2d 61 75 74 68 3e 00
 tipo do attrib: Desconhecido - 28729, comprimento: 1

  00
 Payload seguinte SA: TSi, reservado: 0x0, comprimento: 44
IKEv2-PROTO-4:   última proposta: 0x0, reservado: 0x0, comprimento: 40
 Proposta: 1, ID de protocolo: ESP, tamanho SPI: 4, #trans: 3
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 1, reservado: 0x0, identificação: AES-CBC
IKEv2-PROTO-4:     último transforme: 0x3, reservado: 0x0: comprimento
  tipo: 3, reservado: 0x0, identificação: SHA96
IKEv2-PROTO-4:     último transforme: 0x0, reservado: 0x0: comprimento
  tipo: 5, reservado: 0x0, identificação:

 Payload seguinte de TSi: TSr, reservado: 0x0, comprimento: 24
  Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
  Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento:
  porta do começo: 0, porta da extremidade: 65535
  ADDR do começo: 10.2.2.1, ADDR do fim: 10.2.2.1
 Payload seguinte de TSr: NOTIFIQUE, reservou: 0x0, comprimento: 24
```

```
  Numérico dos TS: 1, 0x0 reservado, 0x0 reservado
  Tipo TS: TS_IPV4_ADDR_RANGE, identificação proto: 0, comprimento:
  porta do começo: 0, porta da extremidade: 65535
  ADDR do começo: 0.0.0.0, ADDR do fim: 255.255.255.255
IKEv2-PROTO-3: Tx [L m_id 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f
IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: Ispi IKEV2 HDR: 58AFF71141BA436B - rspi:
FC696330E6B94D7F
IKEv2-PROTO-4: Payload seguinte: ENCR, versão: 2.0
IKEv2-PROTO-4: Tipo da troca: IKE_AUTH, bandeiras: QUE RESPONDE
RESPONSE
IKEv2-PROTO-4: ID de mensagem: 0x5, comprimento: 4396
 Payload seguinte ENCR: AUTH, reservado: 0x0, comprimento: 4368
Data&colon cifrado; 4364 bytes
```

O ASA manda este mensagem de resposta IKE_AUTH, que é fragmentado em nove pacotes. A troca IKE_AUTH está completa.

```
IKEv2-PROTO-5: (6): Fragmentando o pacote, fragmento MTU: 544, núm
fragmentos: 9, fragmento ID: 3
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PLAT-4: [IKE_AUTH] ENVIADO [10.0.0.1]:4500->[192.168.1.1]:251
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000
PACOTE
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento
AUTH_DONE: EV_OK
IKEv2-PROTO-5: (6): Ação: Action_Null
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento
AUTH_DONE: EV_PKI_SESH_CLOSE
*************************************************
Data: 04/23/2013
Tempo: 16:25:07
```

Digite: Informações
Fonte: acvpnagent

Descrição: Função: ikev2_log
Arquivo: .\ikev2_anyconnect_osal.cpp
Linha: 2730
A conexão IPSec foi estabelecida.
****
Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnagent

Descrição: Registro da sessão IPSec:
Criptografia: AES-CBC
PRF: SHA1
HMAC: SHA96
Método local do AUTH: PSK
Método remoto do AUTH: PSK
Identificação da sequência: 0
Tamanho chave: 192
Grupo DH: 1
Rekey o tempo: 4294967 segundos
Endereço local: 192.168.1.1
Endereço remoto: 10.0.0.1
Porta local: 4500
Porta remota: 4500
ID de sessão: 1
****
Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnui

Descrição: **O perfil configurado no gateway seguro é: Anyconnect-ikev2.x**
****
Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnui

Descrição: Informação do tipo de mensagem enviada ao usuário:
Estabelecendo a sessão de VPN…
****
----------Extremidades da troca IKE_AUTHENTIC----------

****
Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpndownloader

Descrição: Função: ProfileMgr:: loadProfiles

Arquivo: . \ Api \ ProfileMgr.cpp
Linha: 148
Perfis carregados:
Usuários de C:\Documents and Settings\All \ dados do aplicativo \ Cisco \
mobilidade segura Client\Profile\anyconnect-ikev2.xml de Cisco AnyConn
****
****
Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpndownloader

Descrição: Configurações de preferências atuais:
ServiceDisable: falso
CertificateStoreOverride: falso
CertificateStore: Todos
ShowPreConnectMessage: falso
AutoConnectOnStart: falso
MinimizeOnConnect: verdadeiro
LocalLanAccess: falso
AutoReconnect: verdadeiro
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: falso
AutoUpdate: verdadeiro
RSASecurIDIntegration: Automático
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEstablishment: LocalUsersOnly
ProxySettings: Nativo
AllowLocalProxyConnections: verdadeiro
PPPExclusion: Disable
PPPExclusionServerIP:
AutomaticVPNPolicy: falso
TrustedNetworkPolicy: Desligue
UntrustedNetworkPolicy: Conecte
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: falso
ConnectFailurePolicy: Fechado
AllowCaptivePortalRemediation: falso
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: falso
AllowVPNDisconnect: verdadeiro
EnableScripting: falso
TerminateScriptOnNextEvent: falso
EnablePostSBLOnConnectScript: verdadeiro
AutomaticCertSelection: verdadeiro
RetainVpnOnLogoff: falso
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: falso
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSofTokenIntegration: falso

AllowIPsecOverSSL: falso
ClearSmartcardPin: verdadeiro
****

Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnui

Descrição: Informação do tipo de mensagem enviada ao usuário:
Estabelecendo o VPN - Sistema de exame…
****

Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnui

Descrição: Informação do tipo de mensagem enviada ao usuário:
Estabelecendo o VPN - Adaptador de VPN de ativação…
****

Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnagent

Descrição: Função: CVirtualAdapter:: DoRegistryRepair
Arquivo: . \ WindowsVirtualAdapter.cpp
Linha: 1869
Chave de controle encontrada VA:
SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000\Control
****

Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnagent

Descrição: **Uma interface de rede nova foi detectada.**
****

Data: 04/23/2013
Tempo: 16:25:07
Digite: Informações
Fonte: acvpnagent

Descrição: Função: CRouteMgr:: logInterfaces
Arquivo: . \ RouteMgr.cpp
Linha: 2076
Função invocada: logInterfaces
Código de retorno: 0 (0x00000000)
Descrição: Lista de interface do endereço IP de Um ou Mais Servidores C
ICM NT:
10.2.2.1
192.168.1.1
****

Data: 04/23/2013

Tempo: 16:25:08
Digite: Informações
Fonte: acvpnagent

Descrição: Configuração do host:
Endereço público: 192.168.1.1
Máscara pública: 255.255.255.0
Endereço privado: 10.2.2.1
Máscara privada: 255.0.0.0
Endereço privado do IPv6: N/A
Máscara privada do IPv6: N/A
Peer remotos: 10.0.0.1 (porta TCP 443, porta 500 UDP), 10.0.0.1 (porta 4
UDP)
Redes privadas: nenhum
Redes públicas: nenhum
Módo de túnel: sim
****

A conexão é incorporada no base de dados da associação de segurança (SA), e o estado É REGISTRADO. O ASA igualmente executa algumas verificações como o stats comum do cartão do acesso (CAC), a presença da duplicata SA, e os valores de grupos como o Dead Peer Detection (DPD) e assim por diante.

IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento AUTH_DONE: **EV_INSERT_IKE**
IKEv2-PROTO-2: (6): **SA criado; introduzindo o SA no base de dados**
IKEv2-PLAT-3:
STATUS DE CONEXÃO: ACIMA… do par: 192.168.1.1:25171, phase1_id
$AnyConnectClient$
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento AUTH_DONE: **EV_REGISTER_SESSION**
IKEv2-PLAT-3: (6) **username ajustado a: Anu**
IKEv2-PLAT-3:
STATUS DE CONEXÃO: … Par **REGISTRADO**: 192.168.1.1:25171, **phas**
$AnyConnectClient$
IKEv2-PROTO-3: (6): DPD de inicialização, configurado pelos segundos 1
IKEv2-PLAT-3: (6) mib_index ajustado a: 4501
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento AUTH_DONE: EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: (6): Material de chave IPSec da carga
IKEv2-PLAT-3: Crypto map: fósforo no dynmap 1000 segs.s do mapa dina
IKEv2-PLAT-3: (6) o **tempo máximo DPD será: 30**
IKEv2-PLAT-3: (6) o **tempo máximo DPD será: 30**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento AUTH_DONE: EV_START_ACCT
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento AUTH_DONE: EV_CHECK_DUPE
IKEv2-PROTO-3: (6): **Verificação para ver se há duplicata SA**
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento AUTH_DONE: EV_CHK4_ROLE
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento PRONTO: EV_R_UPDATE_CAC_STATS

IKEv2-PLAT-5: Pedido novo ikev2 sa ativado
IKEv2-PLAT-5: Contagem do decréscimo para o negócio entrante
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento
PRONTO: EV_R_OK
IKEv2-PROTO-3: (6): Começando o temporizador suprimir do contexto da
negociação
IKEv2-PROTO-5: (6): Trace-> SA S: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Evento
PRONTO: EV_NO_EVENT
IKEv2-PLAT-2: PFKEY recebidos adicionam o SA para SPI 0x77EE5348,
FALSO
IKEv2-PLAT-2: Atualização recebida SA PFKEY para SPI 0x30B848A4, e
FALSO
****

Data: 04/23/2013
Tempo: 16:25:08
Digite: Informações
Fonte: acvpnagent

Descrição: **A conexão de VPN foi estabelecida e pode agora passar dado**
****

Data: 04/23/2013
Tempo: 16:25:08
Digite: Informações
Fonte: acvpnui

Descrição: Informação do tipo de mensagem enviada ao usuário:
Estabelecendo o VPN - Configurando o sistema…
****

Data: 04/23/2013
Tempo: 16:25:08
Digite: Informações
Fonte: acvpnui

Descrição: Informação do tipo de mensagem enviada ao usuário:
Estabelecendo o VPN…
****

Data: 04/23/2013
Tempo: 16:25:37
Digite: Informações
Fonte: acvpnagent

Arquivo: . \ IPsecProtocol.cpp
Linha: 945
O túnel de IPsec é estabelecido
****

Verificação do túnel

AnyConnect

O exemplo de saída do comando do **anyconnect do detalhe da mostra VPN-sessiondb** é:

```
Session Type: AnyConnect Detailed

Username     : Anu                    Index        : 2
Assigned IP  : 10.2.2.1                Public IP    : 192.168.1.1
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : AES192 AES256          Hashing      : none SHA1 SHA1
Bytes Tx     : 0                      Bytes Rx     : 11192
Pkts Tx      : 0                      Pkts Rx      : 171
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : ASA-IKEV2              Tunnel Group : ASA-IKEV2
Login Time   : 22:06:24 UTC Mon Apr 22 2013
Duration     : 0h:02m:26s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 192.168.1.1
  Encryption   : none                   Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
  Client Type  : AnyConnect
Client Ver   : 3.0.1047
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 25171                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : AES192                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86254 Seconds
  PRF          : SHA1                   D/H Group    : 1
  Filter Name  :
  Client OS    : Windows
IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 0.0.0.0/0.0.0.0/0/0
  Remote Addr  : 10.2.2.1/255.255.255.255/0/0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28654 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607990 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 11192
  Pkts Tx      : 0                      Pkts Rx      : 171
 NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 146 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
Redirect URL :
```

ISAKMP

O exemplo de saída do comando **cripto ikev2 sa da mostra** é:

```
ASA-IKEV2#  show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
     Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
   Life/Active Time: 86400/112 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
```

O exemplo de saída do **comando detail cripto ikev2 sa da mostra** é:

```
ASA-IKEV2# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
 55182129    10.0.0.1/4500         192.168.1.1/25171      READY    RESPONDER
      Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
      Life/Active Time: 86400/98 sec
      Session-id: 2
      Status Description: Negotiation done
      Local spi: FC696330E6B94D7F       Remote spi: 58AFF71141BA436B
      Local id: hostname=ASA-IKEV2
      Remote id: *$AnyConnectClient$*
      Local req mess id: 0              Remote req mess id: 9
      Local next mess id: 0             Remote next mess id: 9
      Local req queued: 0               Remote req queued: 9       Local window:
1                  Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is detected  outside
      Assigned host addr: 10.2.2.1
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
           Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec

O exemplo de saída do **comando show crypto ipsec sa** é:

```
ASA-IKEV2# show crypto ipsec sa
interface: outside
    Crypto map tag: dynmap, seq num: 1000, local addr: 10.0.0.1

   local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 192.168.1.1, username: Anu
      dynamic allocated peer ip: 10.2.2.1

     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
```

```
  #pkts decaps: 163, #pkts decrypt: 108, #pkts verify: 108
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #send errors: 0, #recv errors: 55

   local crypto endpt.: 10.0.0.1/4500, remote crypto endpt.: 192.168.1.1/25171
    path mtu 1488, ipsec overhead 82, media mtu 1500
    current outbound spi: 77EE5348
    current inbound spi : 30B848A4

inbound esp sas:
   spi: 0x30B848A4 (817383588)
      transform: esp-aes-256 esp-sha-hmac no compression
      in use settings ={RA, Tunnel,  NAT-T-Encaps, }
      slot: 0, conn_id: 8192, crypto-map: dynmap
      sa timing: remaining key lifetime (sec): 28685
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
      0xFFAD6BED 0x7ABFD5BF
  outbound esp sas:
    spi: 0x77EE5348 (2012107592)
       transform: esp-aes-256 esp-sha-hmac no compression
      in use settings ={RA, Tunnel,  NAT-T-Encaps, }
       slot: 0, conn_id: 8192, crypto-map: dynmap
       sa timing: remaining key lifetime (sec): 28685
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
       0x00000000 0x00000001
```

Informações Relacionadas

- RFC 4306, protocolo do intercâmbio de chave de Internet (IKEv2)
- RFC 3748, Extensible Authentication Protocol (EAP)
- RFC 5996, versão do protocolo 2 do intercâmbio de chave de Internet (IKEv2)
- Suporte Técnico e Documentação - Cisco Systems