Migração rápida de IKEv1 para a configuração do túnel L2L IKEv2 no código ASA 8.4

Contents

Introduction

Este documento fornece informações sobre o IKEv2 e o processo de migração do IKEv1.

Prerequisites

Requirements

Assegure-se de que você tenha um Cisco ASA Security Appliance que execute IPsec com o método de autenticação PSK (Pre-shared key, chave pré-compartilhada) IKEv1 e assegure-se de que o túnel IPsec esteja no estado operacional.

Para obter um exemplo de configuração de um Cisco ASA Security Appliance que executa IPsec com método de autenticação PSK IKEv1, consulte PIX/ASA 7.x ou superior: Exemplo de configuração de túnel PIX para PIX VPN.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software.

- Cisco ASA 5510 Series Security Appliance com versão 8.4.x e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Por que migrar para IKEv2?

- O IKEv2 oferece melhor resiliência de ataque à rede. O IKEv2 pode atenuar um ataque de DoS na rede quando valida o iniciador do IPsec. Para tornar a vulnerabilidade do DoS difícil de ser explorada, o respondente pode pedir um cookie ao iniciador que tem que assegurar ao respondente que essa é uma conexão normal. No IKEv2, os cookies de resposta atenuam o ataque de DoS de modo que o respondente não mantenha um estado do iniciador de IKE ou não execute uma operação D-H a menos que o iniciador retorne o cookie enviado pelo respondente. O respondente usa CPU mínima e não confirma nenhum estado para uma associação de segurança (SA) até que possa validar completamente o iniciador.
- O IKEv2 reduz a complexidade no estabelecimento de IPsec entre diferentes produtos VPN. Aumenta a interoperabilidade e também permite uma maneira padrão de métodos de autenticação legados. O IKEv2 fornece uma interoperabilidade IPsec perfeita entre fornecedores, pois oferece tecnologias integradas, como Detecção de Ponto Morto (DPD - Dead Peer Detection), NAT Traversal (NAT-T) ou Contato Inicial.
- O IKEv2 tem menos sobrecarga. Com menos sobrecarga, ele oferece latência de configuração de SA aprimorada. Várias solicitações são permitidas em trânsito (por exemplo, quando vários SAs filho são configurados em paralelo).
- O IKEv2 tem um atraso de SA reduzido. Em IKEv1, o atraso da criação de SA amplifica à medida que o volume do pacote amplifica. O IKEv2 mantém o mesmo atraso médio quando o volume do pacote amplifica. Quando o volume do pacote amplifica, o tempo para criptografar e processar o cabeçalho do pacote amplifica. Quando um novo estabelecimento de SA deve ser criado, mais tempo é necessário. A SA gerada por IKEv2 é menor que a gerada por IKEv1. Para um tamanho de pacote amplificado, o tempo necessário para criar um SA é quase constante.
- O IKEv2 tem um tempo de rechaveamento mais rápido. O IKE v1 leva mais tempo para mudar a chave SA do que o IKEv2. A chave IKEv2 para SA oferece melhor desempenho de segurança e diminui o número de pacotes perdidos em transição. Devido à redefinição de certos mecanismos de IKEv1 (como payload ToS, escolha de SA lifetime e exclusividade de SPI) em IKEv2, menos pacotes são perdidos e duplicados em IKEv2. Portanto, há menos necessidade de trocar de SAs.

Observação: como a segurança de rede pode ser tão forte quanto o link mais fraco, o IKEv2 não interopera com IKEv1.

Visão geral da migração

Se sua configuração IKEv1, ou mesmo SSL, já existe, o ASA simplifica o processo de migração.

Na linha de comando, insira o comando **migrate**:

```
migrate {l2l | remote-access {ikev2 | ssl} | overwrite}
```

Aspectos importantes:

- Definições de palavra-chave:**l2l** - Converte os túneis L2l atuais de IKEv1 para IKEv2.**remote access** - (**acesso remoto)** Converte a configuração de acesso remoto. Você pode converter os grupos de túnel IKEv1 ou SSL em IKEv2.**overwrite** - Se você tiver uma configuração IKEv2 que deseja sobrescrever, essa palavra-chave converterá a configuração atual do IKEv1 e removerá a configuração supérflua do IKEv2.
- Éimportante observar que o IKEv2 tem a capacidade de usar chaves simétricas e assimétricas para autenticação PSK. Quando o comando **de migração** é inserido no ASA, o ASA cria automaticamente uma VPN IKEv2 com uma PSK simétrica.
- Depois que o comando é inserido, as configurações atuais de IKEv1 não são excluídas. Em vez disso, as configurações de IKEv1 e IKEv2 são executadas em paralelo e no mesmo mapa de criptografia. Você também pode fazer isso manualmente. Quando o IKEv1 e o IKEv2 são executados em paralelo, isso permite que um iniciador de IPsec VPN recue de IKEv2 para IKEv1 quando existe um problema de protocolo ou configuração com IKEv2 que pode levar a uma falha na tentativa de conexão. Quando o IKEv1 e o IKEv2 são executados em paralelo, ele também fornece um mecanismo de reversão e facilita a migração.
- Quando o IKEv1 e o IKEv2 são executados em paralelo, o ASA usa um módulo chamado gerenciador de túnel/IKE comum no iniciador para determinar o mapa de criptografia e a versão do protocolo IKE a serem usados para uma conexão. O ASA sempre prefere iniciar o IKEv2, mas se não puder, ele retorna ao IKEv1.
- Vários peers usados para redundância não são suportados com IKEv2 no ASA. Em IKEv1, para fins de redundância, um pode ter mais de um peer no mesmo mapa de criptografia quando você insere o comando **set peer**. O primeiro peer será o principal e, se falhar, o segundo peer entrará em ação. Consulte a ID de bug da Cisco CSCud22276 (somente clientes registrados), ENH: Suporte a vários pares para IKEv2.

Processo de migração

Configuração

Neste exemplo, a VPN IKEv1 que usa a autenticação PSK (Pre-Shared Key) existe no ASA.

Observação: a configuração mostrada aqui é relevante apenas para o túnel VPN.

Configuração do ASA com uma VPN IKEv1 atual (antes da migração)

```
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
```

```
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset
crypto map vpn interface outside
crypto isakmp disconnect-notify
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3
```

Configuração do ASA IKEv2 (após a migração)

Nota: Alterações assinaladas em itálico a negrito.

```
ASA-2(config)# migrate l2l
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac

crypto ipsec IKEv2 ipsec-proposal goset protocol esp encryption 3des protocol esp integrity sha-
1
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset

crypto map vpn 12 set IKEv2 ipsec-proposal goset
crypto map vpn interface outside
crypto isakmp disconnect-notify

crypto IKEv2 policy 1 encryption 3des integrity sha group 5 prf sha lifetime seconds 86400
crypto IKEv2 enable outside
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3

IKEv2 remote-authentication pre-shared-key ***** IKEv2 local-authentication pre-shared-key *****
```

Verificação do estabelecimento do túnel IKEv2

```
ASA1# sh cry IKEv2 sa detail

IKEv2 SAs:
Session-id:12, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id   Local                Remote     Status        Role
102061223 192.168.1.1/500  192.168.2.2/500  READY    INITIATOR
     Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK,Auth verify: PSK
     Life/Active Time: 86400/100 sec
     Status Description: Negotiation done
     Local spi: 297EF9CA996102A6       Remote spi: 47088C8FB9F039AD
     Local id: 192.168.1.1
     Remote id: 192.168.2.2
      DPD configured for 10 seconds, retry 3
     NAT-T is not detected
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
         remote selector 10.20.20.0/0 - 10.20.20.255/65535
         ESP spi in/out: 0x637df131/0xb7224866

ASA1# sh crypto ipsec sa
interface: outside
   Crypto map tag: vpn, seq num: 12, local addr: 192.168.1.1
     access-list NEWARK extended permit ip 10.10.10.0 255.255.255.0
     10.20.20.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
     current_peer: 192.168.2.2
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

Verificação de PSK após migração

Para verificar sua PSK, você pode executar este comando no modo de configuração global:

```
more system: running-config | beg tunnel-group
```

Processo do IKEv2 e do gerenciador de túnel

Como mencionado anteriormente, o ASA usa um módulo chamado gerenciador de túnel/IKE comum no iniciador para determinar o mapa de criptografia e a versão do protocolo IKE a serem usados para uma conexão. Digite este comando para monitorar o módulo:

```
debug crypto ike-common <level>
```

Os comandos **debug**, **logging** e **show** foram coletados quando o tráfego é transmitido para iniciar o túnel IKEv2. Para maior clareza, parte da saída foi omitida.

```
ASA1(config)# logging enable
ASA1(config)# logging list IKEv2 message 750000-752999
ASA1(config)# logging console IKEv2
ASA1(config)# exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5

%ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-5-750001: Local:192.168.1.1:500 Remote:192.168.2.2:500 Username:Unknown
Received request to establish an IPsec tunnel; local traffic selector = Address Range:
10.10.10.11-10.10.10.11 Protocol: 0
```

```
Port Range: 0-65535; remote traffic selector = Address Range:
10.20.20.21-10.20.20.21 Protocol: 0 Port Range: 0-65535
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv2.  Map Tag = vpn.  Map Sequence Number = 12.
IKEv2-PLAT-3: attempting to find tunnel group for IP: 192.168.2.2
IKEv2-PLAT-3: mapped to tunnel group 192.168.2.2 using peer IP
    26%ASA-5-750006: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA UP. Reason: New Connection Established
43%ASA-5-752016: IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x0000000000000000 MID=00000000
IKEv2-PROTO-3: (12): Insert SA
IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000000
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PROTO-3: (12): Verify peer's policy
IKEv2-PROTO-3: (12): Get peer authentication method
IKEv2-PROTO-3: (12): Get peer's preshared key for 192.168.2.2
IKEv2-PROTO-3: (12): Verify authentication data
IKEv2-PROTO-3: (12): Use preshared key for id 192.168.2.2, key len 5
IKEv2-PROTO-2: (12): SA created; inserting SA into database
IKEv2-PLAT-3:
CONNECTION STATUS: UP... peer: 192.168.2.2:500, phase1_id: 192.168.2.2
IKEv2-PROTO-3: (12): Initializing DPD, configured for 10 seconds
IKEv2-PLAT-3: (12) DPD Max Time will be: 10
IKEv2-PROTO-3: (12): Checking for duplicate SA
Mar 22 15:03:52 [IKE COMMON DEBUG]IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager Removed entry.
Map Tag = vpn.  Map Sequence Number = 12.
```

Mecanismo de Fallback IKEv2 para IKEv1

Com IKEv1 e IKEv2 em paralelo, o ASA sempre prefere iniciar o IKEv2. Se o ASA não puder, ele retorna ao IKEv1. O módulo comum do gerenciador de túnel/IKE gerencia esse processo. Neste exemplo no iniciador, o SA IKEv2 foi limpo e o IKEv2 está agora propositalmente mal configurado (a proposta IKEv2 é removida) para demonstrar o mecanismo de retorno.

```
ASA1# clear  crypto  IKEv2 sa

%ASA-5-750007: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA DOWN. Reason: operator request
ASA1(config)# no crypto map vpn 12 set IKEv2 ipsec-proposal GOSET
ASA1# (config ) logging enable
ASA1# (config ) logging list IKEv2 message 750000-752999
ASA1# (config ) logging console IKEv2
ASA1# (config ) exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5
%ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-4-752010: IKEv2 Doesn't have a proposal specified
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv1.  Map Tag = vpn.  Map Sequence Number = 12.
```

```
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv2 Doesn't have a proposal specified
%ASA-5-752016: IKEv1 was successful at setting up a tunnel.  Map Tag = vpn.
Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv1 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.

ASA1(config)# sh cry IKEv2 sa
There are no IKEv2 SAs
ASA1(config)# sh cry IKEv1 sa
IKEv1 SAs:
  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1   IKE Peer: 192.168.2.2
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE
```

IKEv2 reforçado

Para fornecer segurança adicional quando IKEv2 é usado, estes comandos opcionais são altamente recomendados:

- **Criptografar desafio de cookie IKEv2**: Permite que o ASA envie desafios de cookie para dispositivos pares em resposta a pacotes iniciados por SA meio abertos.
- **Limite de IKEv2 de criptografia max-sa**: Limita o número de conexões IKEv2 no ASA. Por padrão, a conexão IKEv2 máxima permitida é igual ao número máximo de conexões especificadas pela licença ASA.
- **Limite de IKEv2 de criptografia max-in-negotiation-sa**: Limita o número de SAs de negociação (aberta) de IKEv2 no ASA. Quando usado em conjunto com o comando **crypto IKEv2 cookie-Challenge**, certifique-se de que o limite de desafio de cookie seja inferior a esse limite.
- Usar chaves assimétricas. Após a migração, a configuração pode ser modificada para usar chaves assimétricas como mostrado aqui:

```
ASA-2(config)# more system:running-config
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key cisco1234
 IKEv2 remote-authentication pre-shared-key cisco1234
 IKEv2 local-authentication pre-shared-key cisco123
```

Éimportante perceber que a configuração precisa ser espelhada no outro peer para a chave pré-compartilhada IKEv2. Isso não funcionará se você selecionar e colar a configuração de um lado para o outro.

Observação: esses comandos são desativados por padrão.

Informações Relacionadas

- Suporte técnico e documentação