Migração rápida de IKEv1 à configuração de túnel IKEv2 L2L no código ASA 8.4

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Por que migre a IKEv2?
Vista geral da migração
Processo de migração
Configuração
Verificação do estabelecimento de túnel IKEv2
Verificação PSK após a migração
IKEv2 e processo de gerenciador do túnel
IKEv2 ao mecanismo de recuo IKEv1
Fortalecer IKEv2
Informações Relacionadas

Introdução

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

Pré-requisitos

Requisitos

Assegure-se de que você tenha uma ferramenta de segurança de Cisco ASA que execute o IPsec com o método de autenticação da chave pré-compartilhada IKEv1 (PSK), e se assegure de que o túnel de IPsec esteja no estado operacional.

Para um exemplo de configuração de uma ferramenta de segurança de Cisco ASA que execute o IPsec com método de autenticação IKEv1 PSK, refira PIX/ASA 7.x e acima: Exemplo da configuração de túnel PIX-à-PIX VPN.

Componentes Utilizados

A informação neste documento é baseada nestes versão de hardware e software.

- Ferramenta de segurança do 5510 Series de Cisco ASA que é executado com versão 8.4.x e mais recente.

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

Convenções

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

Por que migre a IKEv2?

- IKEv2 fornece a melhor resiliência do ataque de rede. IKEv2 pode abrandar um ataque DoS na rede quando valida o iniciador do IPsec. A fim fazer a vulnerabilidade DoS difícil explorar, o que responde pode pedir um Cookie ao iniciador que tem que assegurar o que responde que esta é uma conexão normal. Em IKEv2, os Cookie do que responde abrandam o ataque DoS de modo que o que responde não mantenha um estado do iniciador IKE nem não execute uma operação do D-H a menos que o iniciador retornar o Cookie enviado pelo que responde. O que responde usa o CPU mínimo e não compromete nenhum estado a uma associação de segurança (SA) até que possa completamente validar o iniciador.
- IKEv2 reduz a complexidade no estabelecimento do IPsec entre o produtos VPN diferente. Aumenta a Interoperabilidade e igualmente permite uma maneira padrão para métodos de autenticação do legado. IKEv2 fornece uma Interoperabilidade sem emenda do IPsec entre vendedores desde que oferece Tecnologias incorporados tais como o Dead Peer Detection (DPD), o NAT Traversal (NAT-T), ou o contato inicial.
- IKEv2 tem menos despesas gerais. Com menos despesas gerais, oferece a latência melhorada da instalação SA. Os pedidos múltiplos são permitidos no trânsito (por exemplo, quando um múltiplo dos criança-SA se estabelece paralelamente).
- IKEv2 tem um atraso reduzido SA. Em IKEv1 o atraso da criação SA amplifica enquanto o volume do pacote amplifica. IKEv2 mantém o mesmo retardo médio quando o volume do pacote amplifica. Quando o volume do pacote amplifica, o momento de cifrar e processar o cabeçalho de pacote de informação amplifica. Quando um estabelecimento novo SA deve ser criada, mais tempo está exigido. O SA gerado por IKEv2 é menos do que esse gerado por IKEv1. Para um tamanho do pacote amplificado, o tempo tomado para criar um SA é quase constante.
- IKEv2 tem mais rapidamente rekey o tempo. O IKE v1 toma mais tempo rekey SA do que IKEv2. IKEv2 rekey para o desempenho melhorado ofertas da Segurança SA e diminuem o número de Packets Lost na transição. Devido à redefinição de determinados mecanismos de IKEv1 (tais como o payload ToS, a escolha da vida SA, e da unicidade SPI) em IKEv2, menos pacotes são perdidos e duplicados em IKEv2. Consequentemente, há menos necessidade de rekey SA.

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

Vista geral da migração

Se seu IKEv1, ou mesmo o SSL, configuração já existem, o ASA faz o processo de migração simples. Na linha de comando, incorpore o comando da **migração**:

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

Coisas da nota:

- Definições da palavra-chave:**l2l** - Isto converte túneis atuais IKEv1 l2l a IKEv2.**Acesso remoto** - Isto converte a configuração do Acesso remoto. Você pode converter o IKEv1 ou os grupos de túneis SSL a IKEv2.**overwrite** - Se você tem uma configuração IKEv2 que você deseje overwrite, a seguir esta palavra-chave converte a configuração IKEv1 atual e remove a configuração IKEv2 supérflua.
- Éimportante notar que IKEv2 tem a capacidade para usar simétrico assim como chaves assimétricas para a autenticação PSK. Quando o comando da **migração** é incorporado no ASA, o ASA cria automaticamente um IKEv2 VPN com um PSK simétrico.
- Depois que o comando é incorporado, as configurações IKEv1 atuais não estão suprimidas. Em lugar de IKEv1 e configurações IKEv2 executadas paralelamente e no mesmo crypto map. Você pode fazer este manualmente também. Quando IKEv1 e IKEv2 são executado paralelamente, este permite um iniciador do IPSec VPN à reserva de IKEv2 a IKEv1 quando um protocolo ou o problema de configuração existe com IKEv2 que pode conduzir à falha da tentativa de conexão. Quando IKEv1 e IKEv2 executado paralelamente, ele igualmente fornecerem um mecanismo do rollback e facilitarem a migração.
- Quando IKEv1 e IKEv2 executado paralelamente, ASA usarem um módulo chamado o túnel manager/IKE comum no iniciador para determinar o crypto map e a versão do protocolo IKE se usar para uma conexão. O ASA prefere sempre iniciar IKEv2, mas se não pode, cai de volta a IKEv1.
- Os peer múltiplos usados para a Redundância não são apoiados com o IKEv2 no ASA. Em IKEv1, para fins de redundância, um pode ter mais de um par sob o mesmo crypto map quando você inscreve o **comando set peer**. O primeiro par será o preliminar e se falha, o segundo par retrocederá dentro. Refira a identificação de bug Cisco CSCud22276 (clientes registrados somente), ENH: Os peer múltiplos apoiam para IKEv2.

Processo de migração

Configuração

Neste exemplo, IKEv1 VPN que usa a chave pré-compartilhada (PSK) autenticação existe no ASA.

Nota: A configuração mostrada aqui é somente relevante ao túnel VPN.

Configuração ASA com um IKEv1 atual VPN (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 ASA IKEv2 (após a migração)

Nota: Mudanças marcadas nos itálicos e 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 de 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 PSK após a migração

A fim verificar seu PSK, você pode executar este comando no modo de configuração global:

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

IKEv2 e processo de gerenciador do túnel

Como mencionado antes, o ASA usa um módulo chamado o túnel manager/IKE comum no iniciador para determinar o crypto map e a versão do protocolo IKE usar-se para uma conexão. Incorpore este comando monitorar o módulo:

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

Debugar, **registrar**, e os **comandos show** foram recolhidos quando o tráfego é passado para iniciar o túnel IKEv2. Para maior clareza, alguma 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.
```

IKEv2 ao mecanismo de recuo IKEv1

Com o IKEv1 e o IKEv2 paralelamente, o ASA prefere sempre iniciar IKEv2. Se o ASA não pode, cai de volta a IKEv1. O módulo comum do túnel manager/IKE controla este processo. Neste exemplo no iniciador, IKEv2 SA foi cancelado e IKEv2 é agora propositadamente desconfigurado (a proposta IKEv2 é removida) demonstrar o mecanismo recuar.

```
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
```

Fortalecer IKEv2

A fim fornecer a segurança adicional quando IKEv2 é usado, estes comandos opcionais são altamente recomendados:

- **Cookie-desafio IKEv2 cripto**: Permite o ASA de enviar desafios do Cookie aos dispositivos de peer em resposta aos pacotes iniciados SA entreabertos.

- **MAX-sa cripto do limite IKEv2**: Limita o número das conexões IKEv2 no ASA. À revelia, o máximo permitido a conexão IKEv2 iguala o número máximo de conexão especificada pela licença ASA.
- **MAX-em-negociação-sa cripto do limite IKEv2**: Limita o número da em-negociação IKEv2 (abra) SA no ASA. Quando usado conjuntamente com o comando **cripto do Cookie-desafio IKEv2**, assegure-se de que o ponto inicial do Cookie-desafio esteja mais baixo do que este limite.
- Use chaves assimétricas. Após a migração, a configuração pode ser alterada para usar como mostrado chaves assimétricas 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 realizar que a configuração precisa de ser espelhada no outro par para a chave pré-compartilhada IKEv2. Não trabalhará se você seleciona e cola a configuração de um lado ao outro.

Nota: Estes comandos são desabilitados à revelia.

Informações Relacionadas

- Suporte técnico & documentação