Configurar a autenticação no Open Shortest Path First

Contents

Introduction

Este documento descreve como configurar a autenticação Open Shortest Path First (OSPF) e permitir a flexibilidade para autenticar vizinhos OSPF.

Prerequisites

Requirements

Os leitores deste documento devem estar familiarizados com os conceitos básicos do protocolo de roteamento OSPF. Consulte ou informações sobre o protocolo de roteamento OSPF.

Componentes Utilizados

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

- Cisco 2503 Routers
- Software Cisco IOS® versão 12.2(27)

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

Informações de Apoio

Este documento mostra exemplos de configurações para a autenticação do OSPF que flexibiliza a autenticação dos vizinhos de OSPF. É possível habilitar a autenticação do OSPF a fim de trocar as informações de atualização de roteamento de uma forma segura. A autenticação do OSPF pode ser none (nenhum ou nulo), simple ou MD5. O método de autenticação "none" significa que nenhuma autenticação é usada para o OSPF e é o método padrão. Com a autenticação simples, a senha vai em texto simples pela rede. Com autenticação MD5, a senha não passa pela rede. O MD5 é um algoritmo message-digest especificado na RFC 1321. O MD5 é considerado o modo de autenticação OSPF mais seguro. Ao configurar uma autenticação, é necessário configurar toda uma área com o mesmo tipo de autenticação. Com o Cisco IOS®Software Release 12.0(8), a autenticação é suportada em uma base por interface. Isso é também mencionado na RFC 2328, Apêndice D. Este recurso é adicionado na 'ID de bug Cisco CSCdk33792'.

> **Note**: Apenas clientes registrados da Cisco podem acessar esses sites e ferramentas.

Estes são os três tipos diferentes de autenticação compatíveis com OSPF.

- **Autenticação nula — também conhecida como Tipo 0 e significa que não há informações de autenticação inclusas no cabeçalho do pacote.** Esse é o padrão.
- **Autenticação de texto sem formatação — também conhecida como Tipo 1 e usa senhas de texto não criptografado simples.**
- **Autenticação MD5 — também conhecida como Tipo 2 e usa senhas criptográficas MD5.**

A autenticação não precisa ser definida. No entanto, se estiver configurada, todos os roteadores de peer do mesmo segmento deverão ter a mesma senha e o mesmo método de autenticação. Os exemplos deste documento demonstram configurações para texto simples e para autenticação MD5.

Configurar

Esta seção apresenta informações para configurar as características que este documento descreve.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.

Diagrama de Rede

Configurações para autenticação de texto simples

A autenticação de texto sem formatação é usada quando os dispositivos de uma área não são compatíveis com a autenticação MD5 mais segura. A autenticação de texto simples deixa a inter-rede vulnerável a um ataque de farejador, no qual pacotes são capturados por um analisador de protocolo e as senhas podem ser lidas. No entanto, é útil quando você realiza a reconfiguração OSPF, em vez de segurança. Por exemplo, senhas separadas podem ser usadas em roteadores OSPF mais antigos e mais novos que compartilham uma rede de broadcast comum para impedir a comunicação entre roteadores. As senhas de autenticação de texto simples não precisam ser as mesmas em toda uma área, mas devem ser as mesmas entre vizinhos.

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
  ip address 10.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.168.64.10 255.255.255.0
  ip ospf authentication-key c1$c0

!--- The Key value is set as "c1$c0 ". !--- It is the password that is sent across the network. ! route
10 log-adjacency-changes network 10.70.0.70 0.255.255.255 area 0 network 192.168.10.10 0.0.0.255 area 0
0 authentication !--- Plain text authentication is enabled for !--- all interfaces in Area 0.
```

R1-2503

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.168.0.10 255.255.255.0
 ip ospf authentication-key c1$c0

!--- The Key value is set as "c1$c0 ". !--- It is the password that is sent across the network. ! route
10 network 172.16.0.0 0.0.255.255 area 0 network 192.168.10.10 0.0.0.255 area 0 area 0 authentication !
Plain text authentication is enabled !--- for all interfaces in Area 0.
```

Note: O comando area authentication na configuração permite autenticações para todas as interfaces do roteador em uma área específica. Também é possível usar o comando ip ospf

authentication na interface para configurar a autenticação de texto sem formatação para a interface. Esse comando pode ser usado se um método de autenticação diferente ou se nenhum método de autenticação estiver configurado na área à qual a interface pertence. Isso substitui o método de autenticação configurado para a área. Isto é útil se interfaces diferentes que pertencem à mesma área precisarem utilizar métodos de autenticação diferentes

Configurações para autenticação MD5

A autenticação MD5 oferece maior segurança do que a autenticação de texto sem formatação. Esse método usa o algoritmo MD5 para calcular um valor de hash a partir do conteúdo do pacote OSPF e uma senha (ou chave). Este valor de hash é transmitido no pacote, juntamente com uma ID chave e um número de seqüência não decrescente. O receptor, que sabe a mesma senha, calcula seu próprio valor de hash. Se nada na mensagem mudar, o valor de hash do receptor deve corresponder ao valor de hash do remetente que é transmitido com a mensagem.

O ID de chave permite que os roteadores façam referência a várias senhas. Isso torna a migração de senha mais fácil e mais segura. Por exemplo, para migrar de uma senha para outra, configure uma senha em uma ID de chave diferente e remova a primeira chave. O número de sequência impede ataques repetidos em que os pacotes OSPF são capturados, modificados e retransmitidos a um roteador. Assim como ocorre com a autenticação de texto sem formatação, as senhas de autenticação MD5 não têm que ser as mesmas por toda uma área. Entretanto, eles precisam ser os mesmos entre vizinhos.

Note: A Cisco recomenda que você configure o comando service password-encryption em todos os seus roteadores. Isso faz com que o roteador criptografe as senhas em qualquer exibição do arquivo de configuração e proteja a cópia de texto da configuração do roteador contra observação.

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
  ip address 10.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.168.64.10 255.255.255.0
  ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key value (password) is set as "c1$c0 ". ! router ospf 10
network 192.168.10.10 0.0.0.255 area 0 network 10.70.0.70 0.255.255.255 area 0 area 0 authentication me
digest !--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```

R1-2503

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.168.0.10 255.255.255.0
 ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key (password) value is set as "c1$c0 ". ! router ospf 10
network 172.16.0.0 0.0.255.255 area 0 network 192.168.10.10 0.0.0.255 area 0 area 0 authentication mess
```

```
digest !--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```

Note: O comando area authentication message-digest nessa configuração ativa as autenticações para todas as interfaces do roteador em uma área específica. Também é possível usar o comando ip ospf authentication message-digest na interface para configurar a autenticação MD5 para a interface específica. Esse comando pode ser usado se um método de autenticação diferente ou se nenhum método de autenticação estiver configurado na área à qual a interface pertence. Isso substitui o método de autenticação configurado para a área. Isto é útil se interfaces diferentes que pertencem à mesma área precisarem utilizar métodos de autenticação diferentes.

Verificar

As seções a seguir fornecem informações que você pode usar para verificar se suas configurações funcionam corretamente.

Verificar a autenticação de texto simples

Use o comando show ip ospf interface para exibir o tipo de autenticação configurado para uma interface, como essa saída mostra. Aqui, a interface Serial 0 é configurada para a autenticação de texto sem formatação.

```
R1-2503# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.168.0.10/24, Area 0
  Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
```

```
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Simple password authentication enabled
```

O comando show ip ospf neighbor exibe a tabela de vizinhos que consiste nos detalhes do vizinho, como essa saída mostra.

```
R1-2503#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.70.70.70       1   FULL/  -        00:00:31    192.168.64.10     Serial0
```

O comando show ip route exibe a tabela de roteamento, como essa saída mostra.

```
R1-2503#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.70.0.70/32 is subnetted, 1 subnets
O       10.70.70.70 [110/65] via 192.168.64.10, 00:03:28, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.168.10.10/24 is directly connected, Serial0
```

Verificar a autenticação MD5

Use o comando show ip ospf interface para exibir o tipo de autenticação configurado para uma interface, como essa saída mostra. Aqui, a interface Serial 0 foi configurada para a autenticação MD5 com a ID de chave "1".

```
R1-2503#show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.168.0.10/24, Area 0
  Process ID 10, Router ID  172.16.10.36 , Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.70.70.70
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

O comando show ip ospf neighbor exibe a tabela de vizinhos que consiste nos detalhes do vizinho, como essa saída mostra.

```
R1-2503#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.70.70.70       1   FULL/  -        00:00:34    192.168.64.10     Serial0
R1-2503#
```

O comando show ip route exibe a tabela de roteamento, como essa saída mostra.

```
R1-2503#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.70.0.70/32 is subnetted, 1 subnets
O       10.70.70.70 [110/65] via 192.168.64.10, 00:01:23, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.168.10.10/24 is directly connected, Serial0
```

Troubleshoot

Estas seção fornecem informações que você pode usar na solução de problemas de suas configurações. Execute o comando **debug ip ospf adj para capturar o processo de autenticação.** Esse comando **debug** deve ser emitido antes que o relacionamento de vizinhança seja estabelecido.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos **debug** .

Solucionar problemas de autenticação de texto simples

A saída **deb ip ospf adj para R1-2503 mostra quando a autenticação de texto sem formatação é bem-sucedida.**

```
R1-2503#debug ip ospf adj
00:50:57: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:50:57: OSPF: Interface Serial0 going Down
00:50:57: OSPF: 172.16.10.36 address 192.168.0.10 on Serial0 is dead,
  state DOWN
00:50:57: OSPF: 10.70.70.70 address 192.168.64.10 on Serial0 is dead,
  state DOWN
00:50:57: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from
  FULL to DOWN, Neighbor Down: Interface down or detached
00:50:58: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
```

```
  seq 0x80000009
00:50:58: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to down
00:51:03: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:51:03: OSPF: Interface Serial0 going Up
00:51:04: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000A
00:51:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to up
00:51:13: OSPF: 2 Way Communication to 10.70.70.70 on Serial0,
  state 2WAY
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x7 len 32
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x19A4 opt 0x42
  flag 0x7 len 32 mtu 1500 state EXSTART
00:51:13: OSPF: First DBD and we are not SLAVE
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x2 len 72 mtu 1500 state EXSTART
00:51:13: OSPF: NBR Negotiation Done. We are the MASTER
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x3 len 72
00:51:13: OSPF: Database request to 10.70.70.70
00:51:13: OSPF: sent LS REQ packet to 192.168.64.10, length 12
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x1 len 32
00:51:13: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Exchange Done with 10.70.70.70 on Serial0
00:51:13: OSPF: Synchronized with 10.70.70.70 on Serial0, state FULL

!--- Indicates the neighbor adjacency is established. 00:51:13: %OSPF-5-ADJCHG: Process 10, Nbr
10.70.70.70 on Serial0 from LOADING to FULL, Loading Done 00:51:14: OSPF: Build router LSA for
area 0, router ID 172.16.10.36, seq 0x8000000B R1-2503#
```

Essa é a saída do comando **debug ip ospf adj quando há uma incompatibilidade no tipo de autenticação configurado nos roteadores.** Essa saída mostra que o Roteador R1-2503 usa a autenticação tipo 1, enquanto que o roteador R2-2503 está configurado para autenticação tipo 0. Isso significa que o Roteador R1-2503 está configurado para autenticação de texto sem formatação (Tipo 1), enquanto que o Roteador R2-2503 está configurado para autenticação nula (Tipo 0).

```
R1-2503#debug ip ospf adj
00:51:23: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication type.

!--- Input packet specified type 0, you use type 1.
```

Essa é a saída do comando **debug ip ospf adj quando há uma incompatibilidade nos valores da chave de autenticação (senha).** Nesse caso, ambos os roteadores estão configurados para autenticação de texto sem formatação (Tipo 1), mas há uma incompatibilidade nos valores da chave (senha).

```
R1-2503#debug ip ospf adj
00:51:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - Clear Text
```

Autenticação de solução de problemas MD5

Esta é a saída do comando **debug ip ospf adj para R1-2503 quando a autenticação MD5 é bem-sucedida.**

```
R1-2503#debug ip ospf adj
00:59:03: OSPF: Send with youngest Key 1

00:59:13: OSPF: Send with youngest Key 1
00:59:17: %LINK-3-UPDOWN: Interface Serial0, changed state to down
00:59:17: OSPF: Interface Serial0 going Down
00:59:17: OSPF: 172.16.10.36 address 192.168.0.10 on Serial0 is dead,
  state DOWN
00:59:17: OSPF: 10.70.70.70 address 192.168.64.10 on Serial0 is dead,
  state DOWN
00:59:17: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from
  FULL to DOWN, Neighbor Down: Interface down or detached
00:59:17: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000E
00:59:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to down
00:59:32: %LINK-3-UPDOWN: Interface Serial0, changed state to up
00:59:32: OSPF: Interface Serial0 going Up
00:59:32: OSPF: Send with youngest Key 1
00:59:33: OSPF: Build router LSA for area 0, router ID 172.16.10.36,
  seq 0x8000000F
00:59:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
  changed state to up

00:59:42: OSPF: Send with youngest Key 1
00:59:42: OSPF: 2 Way Communication to 10.70.70.70 on Serial0,
  state 2WAY

!--- Both neighbors configured for Message !--- digest authentication with Key ID "1". 00:59:42:
OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2125 opt 0x42 flag 0x7len 32 00:59:42: OSPF: Send
with youngest Key 1 00:59:42: OSPF: Rcv DBD from 10.70.70.70 on Serial0 seq 0x11F3 opt 0x42 flag
0x7 len 32 mtu 1500 state EXSTART 00:59:42: OSPF: First DBD and we are not SLAVE 00:59:42: OSPF:
Rcv DBD from 10.70.70.70 on Serial0 seq 0x2125 opt 0x42 flag 0x2 len 72 mtu 1500 state EXSTART
00:59:42: OSPF: NBR Negotiation Done. We are the MASTER 00:59:42: OSPF: Send DBD to 10.70.70.70
on Serial0 seq 0x2126 opt 0x42 flag 0x3 len 72 00:59:42: OSPF: Send with youngest Key 1
00:59:42: OSPF: Send with youngest Key 1 00:59:42: OSPF: Database request to 10.70.70.70
00:59:42: OSPF: sent LS REQ packet to 192.168.64.10, length 12 00:59:42: OSPF: Rcv DBD from
10.70.70.70 on Serial0 seq 0x2126 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Send DBD to 10.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x1len 32 00:59:42: OSPF: Send
with youngest Key 1 00:59:42: OSPF: Send with youngest Key 1 00:59:42: OSPF: Rcv DBD from
10.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Exchange Done with 10.70.70.70 on Serial0 00:59:42: OSPF: Synchronized with 10.70.70.70 on
Serial0, state FULL 00:59:42: %OSPF-5-ADJCHG: Process 10, Nbr 10.70.70.70 on Serial0 from
LOADING to FULL, Loading Done 00:59:43: OSPF: Build router LSA for area 0, router ID
172.16.10.36, seq 0x80000010 00:59:43: OSPF: Send with youngest Key 1 00:59:45: OSPF: Send with
youngest Key 1 R1-2503#
```

Essa é a saída do comando **debug ip ospf adj quando há uma incompatibilidade no tipo de autenticação configurado nos roteadores.** Essa saída mostra que o roteador R1-2503 usa a autenticação tipo 2 (MD5), enquanto que o Roteador R2-2503 usa a autenticação tipo 1 (autenticação de texto sem formatação).

```
R1-2503#debug ip ospf adj
00:59:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication type.

!--- Input packet specified type 1, you use type 2.
```

Essa é a saída do comando **debug ip ospf adj quando há uma incompatibilidade nas IDs de chave que são usadas para autenticação.** Essa saída mostra que o roteador R1-2503 usa a autenticação MD5 com a ID de chave 1, enquanto que o Roteador R2-2503 usa a autenticação MD5 com a ID de chave 2.

```
R1-2503#debug ip ospf adj
00:59:33: OSPF: Send with youngest Key 1
00:59:43: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - No message digest key 2 on interface
```

Essa saída do comando **debug ip ospf adj para R1-2503 mostra quando ambas as chaves 1 e 2 para autenticação MD5 são configuradas como parte da migração.**

```
R1-2503#debug ip ospf adj

00:59:43: OSPF: Send with youngest Key 1
00:59:53: OSPF: Send with youngest Key 2

!--- Informs that this router is also configured !--- for Key 2 and both routers now use Key 2.
01:00:53: OSPF: 2 Way Communication to 10.70.70.70 on Serial0, state 2WAY R1-2503#
```

Informações Relacionadas

- Configurando a autenticação OSPF em um enlace virtual
- Por que o comando show ip ospf neighbor revela vizinhos em estado init?
- Comandos de OSPF
- Exemplos de configuração de OSPF
- Página de Suporte do IP Routing
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.