Configure la autenticación en Open Shortest Path First

Contenido

Introducción

Este documento describe cómo configurar la autenticación OSPF (Open Shortest Path First) y permitir la flexibilidad para autenticar vecinos OSPF.

Prerequisites

Requirements

Los lectores de este documento deben estar familiarizados con los conceptos básicos del protocolo de ruteo OSPF. Consulte el o la información sobre el protocolo de ruteo OSPF.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Este documento muestra ejemplos de configuración de la autenticación Abrir el trayecto más corto primero (OSPF) que permite la flexibilidad para autenticar vecinos OSPF. Puede habilitar la autenticación en OSPF para intercambiar la información de actualización de ruteo de una forma segura. La autenticación OSPF puede ser none (o null), simple o MD5. El método de autentificación "none" significa que no se utiliza ninguna autenticación para OSPF y es el método predeterminado. Con la autenticación simple, la contraseña entra pasa por la red sin cifrar. Con la autenticación MD5, la contraseña no pasa por la red. MD5 es un algoritmo condensado de mensaje especificado en RFC 1321. MD5 se considera el modo de autenticación OSPF más seguro. Cuando configure la autenticación, debe configurar un área completa con el mismo tipo de autenticación. Con Cisco IOS Software Release 12.0(8), la autenticación se soporta por interfaz. Esto también se menciona en RFC 2328, Apéndice D.

Nota: solo los clientes registrados de Cisco pueden acceder a estos sitios y herramientas.

Estos son los tres tipos diferentes de autenticación compatibles con OSPF:

- **Null Authenticationâ€”Esto es también llamado Tipo 0 y significa que se incluye en el encabezado del paquete información sin autenticación.** Es el valor predeterminado.
- **Autenticación de texto únicamenteâ€”También llamada Tipo 1 y utiliza contraseñas de texto sin cifrar simples.**
- **Autenticación MD5: también se denomina tipo 2 y utiliza las contraseñas cifradas MD5.**

No es necesario establecer la autenticación. Sin embargo, si está configurado, todos los routers pares del mismo segmento deben tener la misma contraseña y método de autenticación. Los ejemplos en este documento demuestran las configuraciones para las autenticaciones de sólo texto y MD5.

Configurar

En esta sección se presenta información para configurar las características que este documento describe.

Diagrama de la red

Este documento utiliza esta configuración de red:

Diagrama de la red

Configuración para autenticación de texto únicamente

La autenticación de texto sin formato se utiliza cuando los dispositivos dentro de un área no admiten la autenticación de MD5 más segura. La autenticación de texto sin formato deja a la interconexión de red vulnerable a un ataque sabueso, en el cual los paquetes son capturados por un analizador de protocolo y las contraseñas pueden ser leídas. Sin embargo, es útil cuando se realiza la reconfiguración OSPF, no por

razones de seguridad. Por ejemplo, se pueden utilizar contraseñas separadas en routers OSPF antiguos y nuevos que comparten una red de difusión común para evitar la comunicación entre routers. Las claves de autenticación de sólo texto no deben ser las mismas dentro de una misma área, pero deben serlo entre los vecinos.

- 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.

  !
 router ospf 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
  area 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.

!
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

!--- Plain text authentication is enabled !--- for all interfaces in Area 0.
```

Nota: El comando **area authentication** de la configuración habilita las autenticaciones para todas las interfaces del router en un área determinada. También puede usar el comando de autenticación de ip ospf en la interfaz con el fin de configurar la autenticación de texto sin formato para la interfaz. Este comando puede ser utilizado si se configura un método de autenticación diferente o si no se configura algún método de autenticación en el área a la cual pertenece la interfaz. Reemplaza el método de autenticación configurado para el área. Esto es útil si distintas interfaces que pertenecen a la misma área necesitan utilizar métodos de autenticación diferentes

Configuraciones para la autenticación MD5

La autenticación de MD5 proporciona mayor seguridad que la autenticación de texto sin formato. Este método utiliza el algoritmo MD5 para calcular un valor de troceo de los contenidos del paquete OSPF y una contraseña (o clave). Este valor de troceo se transmite en el paquete, junto con una identificación de clave y un número de secuencia no decreciente. El receptor, que conoce la misma contraseña, calcula su propio valor de troceo. Si no cambia nada en el mensaje, el valor hash del receptor debe coincidir con el valor hash del remitente que se transmite con el mensaje.

El ID clave permite que los routers consulten varias contraseñas. Esto facilita la migración de contraseñas y la hace más segura. Por ejemplo, para migrar de una contraseña a otra, configure una contraseña en una ID de clave diferente y elimine la primera clave. El número de secuencia impide ataques de reproducción, en los que los paquetes de OSPF se capturan, se modifican y se retransmiten a un router. Al igual que con la autenticación de texto únicamente, las contraseñas de autenticación MD5 no necesitan ser las mismas en todo el área. Sin embargo, no es necesario que sean iguales entre vecinos.

Nota: Cisco recomienda que configure el comando **service password-encryption** en todos sus routers. Esto hace que el router cifre las contraseñas en cualquier visualización del archivo de configuración y proteja la copia de texto de la configuración del router de la observación.

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

> **Nota**: El comando **area authentication message-digest** de esta configuración habilita las autenticaciones para todas las interfaces del router en un área determinada. También puede usar el comando message-digest de autenticación ip ospf en la interfaz con el fin de configurar la autenticación MD5 para la interfaz específica. Este comando puede ser utilizado si se configura un método de autenticación diferente o si no se configura algún método de autenticación en el área a la cual pertenece la interfaz. Reemplaza el método de autenticación configurado para el área. Esto es útil si distintas interfaces que pertenecen a la misma área necesitan utilizar métodos de autenticación diferentes.

Verificación

Estos apartados proporcionan información que puede utilizar para confirmar que sus configuraciones funcionen correctamente.

Verificar la autenticación de texto únicamente

Utilice el comando show ip ospf interface para ver el tipo de autenticación configurada para una interfaz, como muestra este resultado. Aquí, la interfaz Serial 0 está configurada para la autenticación de texto sin formato.

<#root>

```
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

El comando show ip ospf neighbor muestra la tabla de vecinos, que consta de los detalles de vecinos, como muestra este resultado.

<#root>

```
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
```

El comando show ip route muestra la tabla de routing, como muestra este resultado.

<#root>

```
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 la autenticación MD5

Utilice el comando show ip ospf interface para ver el tipo de autenticación configurada para una interfaz, como muestra este resultado. Aquí, la interfaz Serial 0 se ha configurado para la autenticación de MD5 con la ID de clave "1".

<#root>

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

El comando show ip ospf neighbor muestra la tabla de vecinos, que consta de los detalles de vecinos, como muestra este resultado.

<#root>

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#
```

El comando show ip route muestra la tabla de routing, como muestra este resultado.

<#root>

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 secciones brindan información que puede utilizar para la solución de problemas en sus configuraciones. Ejecute el **comando debug ip ospf adj para capturar el proceso de autenticación.** Este comando **debug** debe ejecutarse antes de establecer la relación de vecino.

> **Nota**: Consulte Información Importante sobre los Comandos Debug antes de utilizar los comandos **debug**.

Solución de problemas de la autenticación de texto únicamente

El resultado **deb ip ospf adj para R1-2503 se muestra cuando la autenticación de texto sin formato es correcta.**

<#root>

```
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#
```

Este es el resultado del **comando debug ip ospf adj cuando se produce un error de coincidencia en el tipo de autenticación configurada en los routers.** Este resultado muestra que el router R1-2503 utiliza autenticación de tipo 1, mientras que el router R2-2503 está configurado para la autenticación de tipo 0. Esto significa que el router R1-2503 está configurado para la autenticación de texto sin formato (tipo 1), mientras que el router R2-2503 está configurado para la autenticación nula (tipo 0).

<#root>

```
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.

Este es el resultado del **comando debug ip ospf adj cuando se produce un error de coincidencia en los valores de la clave de autenticación (contraseña).** En este caso, ambos routers están configurados para la autenticación de texto sin formato (tipo 1), pero hay un error de coincidencia en los valores de la clave (contraseña).

<#root>

```
R1-2503#
```

```
debug ip ospf adj

00:51:33: OSPF: Rcv pkt from 192.168.64.10, Serial0 : Mismatch
Authentication Key - Clear Text
```

Solución de problemas de autenticación de MD5

Este es el resultado del **comando debug ip ospf adj para R1-2503 cuando la autenticación de MD5 es correcta.**

<#root>

```
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#
```

Este es el resultado del **comando debug ip ospf adj cuando se produce un error de coincidencia en el tipo de autenticación configurada en los routers.** Este resultado muestra que el router R1-2503 utiliza autenticación de tipo 2 (MD5), mientras que el router R2-2503 usa autenticación de tipo 1 (autenticación de texto sin formato).

<#root>

```
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.

Este es el resultado del **comando debug ip ospf adj cuando se produce un error de coincidencia en las ID de las claves usadas para la autenticación.** Este resultado muestra que el router R1-2503 utiliza autenticación de MD5 con la ID de clave 1, mientras que el router R2-2503 utiliza autenticación de MD5 con la ID de clave 2.

<#root>

```
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
```

Este resultado del **comando debug ip ospf adj para R1-2503 muestra cuando la clave 1 y la clave 2 para la autenticación de MD5 están configuradas como parte de la migración.**

<#root>

```
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#
```

Información Relacionada

- **Configuración de la autenticación OSPF en un link virtual**
- **¿Por qué el comando show ip ospf neighbor informa que los vecinos se encuentran en el estado inicial?**
- **Comandos OSPF**
- **Ejemplos de configuración de OSPF**
- **Página de Soporte de IP Routing**
- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).