Ejemplo de configuración para la Autenticación en OSPF

Contenido

Introducción

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. A partir de Cisco IOS® Software Release 12.0(8), la autenticación se soporta según la interface. Esto también se menciona en RFC 2328, Apéndice D. Esta característica se agrega en el Id. de bug Cisco CSCdk33792 (clientes registrados solamente).

prerrequisitos

Requisitos

Los Quien lea este documento deben ser familiares con los conceptos básicos de OSPF Routing Protocol. Refiera a la primera documentación para información del trayecto más corto abierto en el OSPF Routing Protocol.

Componentes Utilizados

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

- Cisco 2503 Router
- Cisco IOS Software Release 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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Éstos son los tres diversos tipos de autenticación soportados por el OSPF.

- Null Authentication—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 únicamente—También llamada Tipo 1 y utiliza contraseñas de texto sin cifrar simples.
- **Autenticación de MD5** — Esto también se llama Type-2 y utiliza las contraseñas criptográficas 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.

Note: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) para encontrar la información adicional en los comandos usados en este documento.

Diagrama de la red

Este documento utiliza esta configuración de red:

Configuración para autenticación de texto únicamente

Se utiliza el autenticación de texto únicamente cuando los dispositivos dentro de un área no pueden soportar el más seguro autenticación de MD5. 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 usted realiza la reconfiguración de OSPF, bastante que para la Seguridad. Por ejemplo, las contraseñas separadas pueden ser utilizadas en routers OSPF más antiguos o más nuevos que compartan una red de difusión común para evitar que se comuniquen entre sí. 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 70.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.16.64.2 255.255.255.0
  ip ospf authentication-key c1$c0
!--- The Key value is set as "c1$c0 ". !--- It is the
password that is sent across the network. clockrate
64000 ! router ospf 10 log-adjacency-changes network
70.0.0.0 0.255.255.255 area 0 network 192.16.64.0
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 192.16.64.1 255.255.255.0
 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
192.16.64.0 0.0.0.255 area 0 area 0 authentication !---
Plain text authentication is enabled !--- for all
interfaces in Area 0.
```

Note: El comando area authentication en la configuración habilita la autenticación para todas las interfaces del router en una área determinada. Usted puede también utilizar el comando ip ospf authentication bajo interfaz de configurar el autenticación de texto únicamente 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 autentificación 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

Autenticación de MD5 proporciona la mayor seguridad que el autenticación de texto únicamente. 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 nada en el mensaje cambia, el valor de troceo del receptor debe hacer juego el valor de troceo del remitente que se transmite con el mensaje.

El ID clave permite que los routers consulten varias contraseñas. Esto hace la migración de contraseña más fácil y más segura. Por ejemplo, para emigrar a partir de una contraseña a otra, configure una contraseña bajo diversa clave ID y quite la primera clave. El número de secuencia previene los ataques con paquetes copiados, en los cuales los paquetes 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.

Note: Cisco recomienda que usted configura el comando service password-encryption en todo el Routers. Esto hace al router cifrar las contraseñas en cualquier visualización del archivo de configuración y guarda contra la contraseña que es aprendida observando la copia del texto de la configuración del router.

- R2-2503
- R1-2503

R2-2503

```
interface Loopback0
  ip address 70.70.70.70 255.255.255.255
 !
 interface Serial0
  ip address 192.16.64.2 255.255.255.0
  ip ospf message-digest-key 1 md5 c1$c0
!--- Message digest key with ID "1" and !--- Key value
(password) is set as "c1$c0 ". clockrate 64000 ! router
ospf 10 network 192.16.64.0 0.0.0.255 area 0 network
70.0.0.0 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 192.16.64.1 255.255.255.0
 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
192.16.64.0 0.0.0.255 area 0 area 0 authentication
message-digest !--- MD5 authentication is enabled for !-
```

```
-- all interfaces in Area 0.
```

Note: El comando area authentication message-digest en esta configuración habilita la autenticación para todas las interfaces de router de una área particular. Usted puede también utilizar el comando ip ospf authentication message-digest bajo interfaz de configurar autenticación de 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 autentificación configurado para el área. Esto es útil si distintas interfaces que pertenecen a la misma área necesitan utilizar métodos de autenticación diferentes.

Verificación

Estas secciones proporcionan la información que usted puede utilizar para confirmar su trabajo de las configuraciones correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Verificar la autenticación de texto únicamente

Utilice el comando show ip ospf interface de ver el tipo de autenticación configurado para una interfaz, como esta salida muestra. Aquí, la interfaz del serial0 se configura para el autenticación de texto únicamente.

```
R1-2503# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.16.64.1/24, 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 visualiza la tabla de vecino que consiste en los detalles del vecino, pues esta salida muestra.

```
R1-2503# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
70.70.70.70       1   FULL/  -        00:00:31    192.16.64.2     Serial0
```

El comando show ip route visualiza la tabla de ruteo, pues esta salida muestra.

```
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

     70.0.0.0/32 is subnetted, 1 subnets
O       70.70.70.70 [110/65] via 192.16.64.2, 00:03:28, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.16.64.0/24 is directly connected, Serial0
```

Verificar la autenticación MD5

Utilice el comando show ip ospf interface de ver el tipo de autenticación configurado para una interfaz, como esta salida muestra. Aquí, la interfaz del serial0 se ha configurado para autenticación de MD5 con la clave ID el "1".

```
R1-2503# show ip ospf interface serial0
Serial0 is up, line protocol is up
  Internet Address 192.16.64.1/24, 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 70.70.70.70
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

El comando show ip ospf neighbor visualiza la tabla de vecino que consiste en los detalles del vecino, pues esta salida muestra.

```
R1-2503# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
70.70.70.70       1   FULL/  -        00:00:34    192.16.64.2     Serial0
R1-2503#
```

El comando show ip route visualiza la tabla de ruteo, pues esta salida muestra.

```
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
```

```
     70.0.0.0/32 is subnetted, 1 subnets
O       70.70.70.70 [110/65] via 192.16.64.2, 00:01:23, Serial0
     172.16.0.0/28 is subnetted, 1 subnets
C       172.16.10.32 is directly connected, Loopback0
C    192.16.64.0/24 is directly connected, Serial0
```

Troubleshooting

Estas secciones proporcionan la información que usted puede utilizar para resolver problemas sus configuraciones. Publique el **comando debug ip ospf adj** para capturar el proceso de autenticación. Este **comando debug** debe ser publicado antes de que se establezca la relación de vecino.

Note: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Solución de problemas de la autenticación de texto únicamente

La salida **ajuste OSPF del IP DEB** para el R1-2503 muestra cuando el autenticación de texto únicamente es acertado.

```
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 192.16.64.1 on Serial0 is dead,
  state DOWN
00:50:57: OSPF: 70.70.70.70 address 192.16.64.2 on Serial0 is dead,
  state DOWN
00:50:57: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 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 70.70.70.70 on Serial0,
  state 2WAY
00:51:13: OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2486 opt 0x42
  flag 0x7 len 32
00:51:13: OSPF: Rcv DBD from 70.70.70.70 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 70.70.70.70 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 70.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x3 len 72
00:51:13: OSPF: Database request to 70.70.70.70
00:51:13: OSPF: sent LS REQ packet to 192.16.64.2, length 12
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x2487 opt 0x42
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Send DBD to 70.70.70.70 on Serial0 seq 0x2488 opt 0x42
  flag 0x1 len 32
00:51:13: OSPF: Rcv DBD from 70.70.70.70 on Serial0 seq 0x2488 opt 0x42
```

```
  flag 0x0 len 32 mtu 1500 state EXCHANGE
00:51:13: OSPF: Exchange Done with 70.70.70.70 on Serial0
00:51:13: OSPF: Synchronized with 70.70.70.70 on Serial0, state FULL
!--- Indicates the neighbor adjacency is established. 00:51:13: %OSPF-5-ADJCHG: Process 10, Nbr
70.70.70.70 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#
```

Ésta es la salida del **comando debug ip ospf adj** cuando hay una discordancía en el tipo de autenticación configurado en el Routers. Esta salida muestra que el router R1-2503 utiliza la autenticación del tipo 1 mientras que configuran al router R2-2503 para la autenticación del tipo 0. Esto significa que configuran al router R1-2503 para el autenticación de texto únicamente (tipo 1) mientras que configuran al router R2-2503 para la autenticación nula (tipo 0).

```
R1-2503# debug ip ospf adj
00:51:23: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication type.
!--- Input packet specified type 0, you use type 1.
```

Ésta es la salida del **comando debug ip ospf adj** cuando hay una discordancía en los valores de la clave de autenticación (contraseña). En este caso, configuran a ambo Routers para el autenticación de texto únicamente (tipo 1) pero hay una discordancía en los valores dominantes (de la contraseña).

```
R1-2503# debug ip ospf adj
00:51:33: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication Key - Clear Text
```

Solución de problemas de autenticación de MD5

Éste es el **comando debug ip ospf adj** hecho salir para el R1-2503 cuando autenticación de MD5 es acertado.

```
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 192.16.64.1 on Serial0 is dead,
  state DOWN
00:59:17: OSPF: 70.70.70.70 address 192.16.64.2 on Serial0 is dead,
  state DOWN
00:59:17: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 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 70.70.70.70 on Serial0,
  state 2WAY
```

```
!--- Both neighbors configured for Message !--- digest authentication with Key ID "1". 00:59:42:
OSPF: Send DBD to 70.70.70.70 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 70.70.70.70 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 70.70.70.70 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 70.70.70.70
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 70.70.70.70
00:59:42: OSPF: sent LS REQ packet to 192.16.64.2, length 12 00:59:42: OSPF: Rcv DBD from
70.70.70.70 on Serial0 seq 0x2126 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Send DBD to 70.70.70.70 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
70.70.70.70 on Serial0 seq 0x2127 opt 0x42 flag 0x0 len 32 mtu 1500 state EXCHANGE 00:59:42:
OSPF: Exchange Done with 70.70.70.70 on Serial0 00:59:42: OSPF: Synchronized with 70.70.70.70 on
Serial0, state FULL 00:59:42: %OSPF-5-ADJCHG: Process 10, Nbr 70.70.70.70 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#
```

Ésta es la salida del **comando debug ip ospf adj** cuando hay una discordancía en el tipo de autenticación configurado en el Routers. Esta salida muestra que el router R1-2503 utiliza la autenticación del tipo-2 (MD5) mientras que el router R2-2503 utiliza la autenticación del tipo 1 (autenticación de texto únicamente).

```
R1-2503# debug ip ospf adj
00:59:33: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication type.
!--- Input packet specified type 1, you use type 2.
```

Ésta es la salida del **comando debug ip ospf adj** cuando hay una discordancía en la clave ID que se utiliza para la autenticación. Esta salida muestra que el router R1-2503 utiliza autenticación de MD5 con la clave ID 1, mientras que el router R2-2503 utiliza autenticación de MD5 con la clave ID 2.

```
R1-2503# debug ip ospf adj
00:59:33: OSPF: Send with youngest Key 1
00:59:43: OSPF: Rcv pkt from 192.16.64.2, Serial0 : Mismatch
Authentication Key - No message digest key 2 on interface
```

Esta salida del **comando debug ip ospf adj** para el R1-2503 muestra cuando la clave 1 y la clave 2 para autenticación de MD5 se configuran como parte de la migración.

```
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 70.70.70.70 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 la tecnología OSPF

- Soporte Técnico y Documentación - Cisco Systems