

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Información general](#)

[Actualice el código FWSM](#)

[Habilite un nuevo VLA N del Switch que no sea actualmente funcionando](#)

[Defina los VLA N del Firewall en el Switch](#)

[FWSM básico para la configuración de failover](#)

[Confirme la configuración y la configuración](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar y actualizar un Firewall Services Module (FWSM) de repuesto para uno que ha fallado. Este documento también describe cómo configurar el switch Catalyst 6500 Series para minimizar el tiempo de inactividad. Esto se aplica a FWSM como parte de un par de fallas, y a un FWSM que ya se haya intercambiado físicamente (consulte la guía de instalación del hardware para ver información detallada).

[prerrequisitos](#)

[Requisitos](#)

Antes de que usted complete los procedimientos en este documento:

- Asegúrese que las propiedades básicas de su Switch estén configuradas. **Nota:** Este documento no describe la configuración inicial del FWSM y del Switch. Bastante, asume el FWSM y el Switch trabajados con éxito antes de una falla de hardware.

[Componentes Utilizados](#)

La información en este documento se basa en el Módulo de servicios de firewall Cisco Catalyst de la serie 6500.

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 Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Información general

Estos pasos le dan instrucciones en la configuración, la actualización, y el reemplazo del FWSM. Los pasos se explican en el detalle adicional en las secciones restantes de este documento.

1. Defina un VLAN distinto como VLA N del Firewall (quite las viejas definiciones de VLAN del Firewall) en el Switch con el reemplazo FWSM.
2. Conecte un PC en el Catalyst 6000 y asigne el puerto del switch al mismo VLA N que usted acaba de definir.
3. La sesión al FWSM y habilita una interfaz.
4. Utilice el PC como servidor TFTP para descargar el software. Asegúrese de que usted utilice la misma versión del código que el dispositivo activo actual.
5. Configure las configuraciones básicas de la Conmutación por falla en el FWSM y restablezca los VLA N viejos del Firewall y la interfaz de la Conmutación por falla (quite la interfaz configurada para el TFTP). Ahora, la réplica de la configuración ocurre y el FWSM se convierte en el respaldo.

Actualice el código FWSM

Para ejecutar la Conmutación por falla, los dos FWSM deben funcionar con la misma versión del código. En caso de que el RMA'd FWSM no venga con la misma versión del código que el Firewall activo, complete estos pasos para actualizar.

Descargue el [software FWSM \(clientes registrados solamente\)](#) a su servidor TFTP.

Habilite un nuevo VLA N del Switch que no sea actualmente funcionando

Complete estos pasos:

1. Agregue el VLA N al Switch. El VLA N no puede ser un VLA N reservado. Utilice el **comando** `vlan vlan_number` de agregar el VLA N si usted funciona con el software de Cisco IOS® en el Switch. Utilice el **comando** `vlan vlan_number del conjunto` de agregar el VLA N si usted se ejecuta software del sistema operativo Catalyst en el Switch.

2. Asigne el VLA N al puerto del switch con el cual usted planea conectar el PC. Ingrese estos comandos para asignar un VLA N a un puerto, usando el Cisco IOS

```
Software:router(config)#interface type slot/portrouter(config-if)#switchportrouter(config-if)#switchport mode accessrouter(config-if)#switchport access vlan vlan_idIngrese este comando para asignar un VLA N a un puerto, usando software del sistema operativo Catalyst:set vlan vlan_number mod/ports
```

3. Copie los viejos comandos del Firewall a la libreta para apoyarlos. Después, quítelos y después substituya substituyendo el VLA N definido en los pasos 1 y 2. Para el Cisco IOS

```
Software:Router(config)#firewall vlan-group firewall_group  
vlan_rangeRouter(config)#firewall module module_number vlan-group firewall_groupPara software del sistema operativo Catalyst:Console> (enable) set vlan vlan_list firewall-vlan mod_num
```

- Habilite una interfaz en el FWSM y la dirección IP:

```
nameif interface interface_name
security_lvl ip address interface_name ip_address [mask]
interface interface_name fwsm(config-
interface) no shutdown
```
- Pruebe la Conectividad entre el FWSM y el PC, usando el ping. Utilice los theis ordenan para descargar la imagen del servidor TFTP cuando se confirma la Conectividad. Recargue el FWSM cuando la descarga es completa.

```
FWSM#copy tftp://server[/path]/filename
flash: Por ejemplo, ingrese este comando:
FWSM#copy tftp://209.165.200.226/cisco/c6svc-fwm-
k9.2-1-1.bin flash:
```

Defina los VLA N del Firewall en el Switch

Substituya los comandos que usted quitó en el [paso 1 de la](#) actualización el procedimiento de código FWSM.

- Para el Cisco IOS Software:

```
Router(config)#firewall vlan-group firewall_group
vlan_range Router(config)#firewall module module_number vlan-group firewall_group
```
- Para software del sistema operativo Catalyst:

```
Console> (enable) set vlan vlan_list firewall-
vlan mod_num
```

FWSM básico para la configuración de failover

Ponga algunas configuraciones básicas FWSM para prepararla para la reintroducción en los pares. Entonces configure de nuevo los VLA N de los grupos/Firewall del Firewall del Switch para incluirla nuevamente dentro del par de fallas.

- Quite el viejos nameif y dirección IP definidos en el [paso 4 del](#) permiso un nuevo VLA N del Switch que no sea actualmente procedimiento funcionando.
- Defina el dispositivo como el primario o secundario.

```
FWSM(config)#fail lan unit
{primary|secondary}
```
- Ingrese este comando en el espacio de la ejecución del sistema de configurar la interfaz VLAN de la Conmutación por falla para el modo de contexto múltiple:

```
primary(config)#failover lan interface interface_name vlan vlan
```
- Ingrese este comando de fijar el IP Address de la interfaz de la Conmutación por falla:

```
primary(config)#failover interface ip failover_interface ip_address mask standby
ip_address
```
- Habilite el failover:

```
FWSM(config)#failover
```

Este resultado muestra un ejemplo:

```
FWSM(config)#failover lan unit secondary
FWSM(config)#failover interface ip fover
10.1.1.10 255.255.255.0 standby 10.1.1.11
FWSM(config)#failover LAN Interface fover vlan
50
FWSM(config)#failover
```

Aparece el siguiente resultado:

```
FWSM(config)#failover lan unit
secondary
FWSM(config)#failover interface ip fover 10.1.1.10 255.255.255.0 standby
10.1.1.11
FWSM(config)#failover LAN Interface fover vlan 50
FWSM(config)#failover
```

Confirme la configuración y la configuración

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Publique este comando show:

```
fwsd(config)#show failover
Failover On
Failover unit Primary
Failover LAN Interface fover
Vlan
```

```
150Unit Poll frequency 15 secondsInterface Poll frequency 15 secondsInterface Policy
50%Monitored Interfaces 249 of 250 maximumConfig sync: activeLast Failover at: 10:58:08 Apr 15
2004          This host: Primary - Standby          Active time: 0(sec)
admin Interface inside (10.6.8.91): Normal          admin Interface outside (70.1.1.2):
Normal          Other host: Secondary - Active          Active time: 2232 (sec)
admin Interface inside (10.6.8.100): Normal          admin Interface outside (70.1.1.3):
Normal
```

Marque para ver que este host está en el recurso seguro. También marque para ver si usted puede hacer ping los dispositivos de sus interfaces del FWSM. Si usted quisiera que el nuevo dispositivo llegara a ser activo, no utilice el **ningún comando failover activo** de forzar la Conmutación por falla.

Ingrese este comando en el módulo activo a la Conmutación por falla al módulo en espera:

```
primary(config)#no failover active
```

Ingrese este comando en el módulo en espera de forzarlo para llegar a ser activo:

```
secondary(config)#failover active
```

Refiérase [con la Conmutación por falla](#) para más detalles en las opciones y resolver problemas de configuración de failover.

[Información Relacionada](#)

- [Soporte de productos del Módulo de servicios de firewall Cisco Catalyst de la serie 6500](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)