Contenido

Introducción

Este documento proporciona una configuración de muestra para la configuración del Equilibrio de carga de firewall (FWLB) mientras que usa solamente un módulo content switching (CS). El FWLB requiere la granja del Firewall ser rodeado por los balanceadores de la carga. Éste es garantizar que el tráfico entrante y saliente de una sola sesión es carga equilibrada al mismo Firewall. Al usar un CS, usted puede utilizar el mismo módulo para hacer el trabajo de ambos loadbalancers. Este documento le muestra cómo alcanzar esto.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Versión ejecutable CSM 3.x

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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

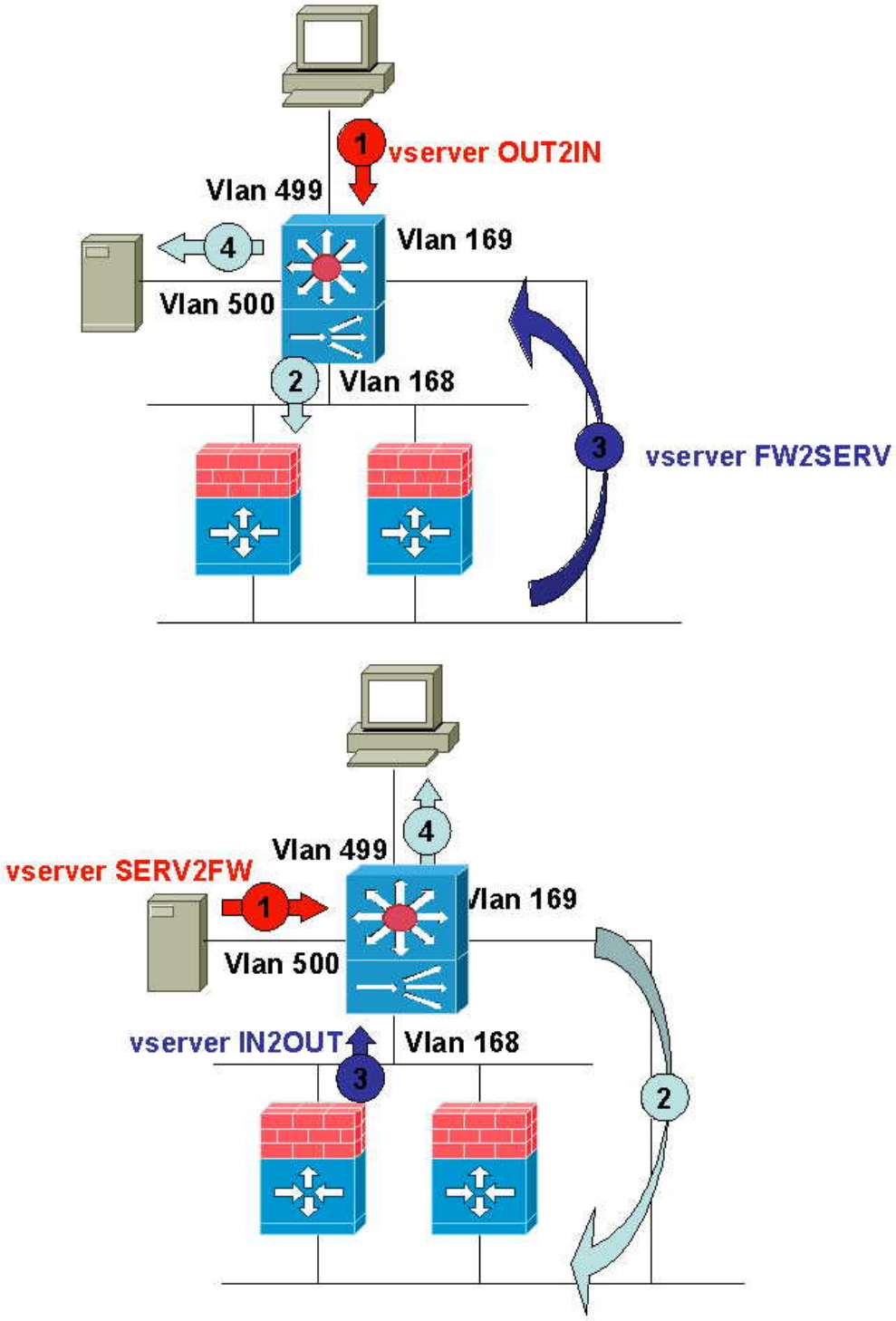
Configurar

En esta sección, le presentan con la información para configurar el CS para el FWLB según lo descrito en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa esta configuración:

Versión ejecutable CSM 3.x

```
module ContentSwitchingModule 4  vlan 499 client!---
Outside world or client side. ip address 192.168.10.97
255.255.254.0 gateway 192.168.10.1! vlan 500 server!---
Inside world or server side. ip address 192.168.20.97
255.255.254.0! vlan 168 server!--- Firewall outside
interface. ip address 192.168.168.97 255.255.255.0! vlan
169 server!--- Firewall inside interface. ip address
192.168.169.97 255.255.255.0!! serverfarm FORWARD!---
Serverfarm to simply forward the traffic with no NATing.
no nat server no nat client predictor forward!
serverfarm FWLB_IN2OUT!--- Firewall farm used for
outbound traffic from inside to outside. no nat server
no nat client real 192.168.169.1 backup real
192.168.169.2!--- Use a backup real if your firewalls
support stateful failover. inservice real 192.168.169.2
backup real 192.168.169.1 inservice! serverfarm
FWLB_OUT2IN!--- Firewall farm for inbound traffic from
outside to inside. no nat server no nat client real
192.168.168.1 backup real 192.168.168.2 inservice real
192.168.168.2 backup real 192.168.168.1 inservice !---
The default is round robin load balancing. !--- If you
need to guarantee *parent* connections are going !--- to
the same firewall, you may need to issue the !---
predictor hash address command or sticky with reverse
sticky.! vserver FW2SERV!--- Vserver to catch traffic
coming from the firewall and forward it to the server.
virtual 192.168.20.0 255.255.254.0 any!--- The Virtual
IP (VIP) is a subnet that matches the internal network.
vlan 169!--- Specify that the vserver only applies to
traffic from VLAN 169. serverfarm FORWARD persistent
rebalance inservice! vserver IN2OUT!--- Vserver to catch
traffic coming from the firewall and !--- forward it to
the outside. virtual 0.0.0.0 0.0.0.0 any vlan 168
serverfarm FORWARD!--- Serverfarm to forward traffic
with no load balancing and no NATing. persistent
rebalance inservice! vserver OUT2IN!--- Vserver to catch
traffic from the outside world and load balance it to
the firewall. virtual 192.168.20.0 255.255.254.0 any
vlan 499!--- Limit the vserver to traffic on VLAN 499
only. serverfarm FWLB_OUT2IN!--- Use the firewall farm
define in FWLB_OUT2IN. persistent rebalance inservice!
vserver SERV2FW!--- Vserver to catch the server response
and load balance it to the firewall. virtual 0.0.0.0
0.0.0.0 any vlan 500 serverfarm FWLB_IN2OUT persistent
rebalance inservice! !--- Same rules, however, for FTP
traffic. !--- This is recommended in order to tie the
control channel !--- with the data channel.! vserver
FTP_FW2SERV virtual 192.168.20.0 255.255.254.0 tcp ftp
service ftp vlan 169 serverfarm FORWARD persistent
rebalance inservice! vserver FTP_OUT2IN virtual
192.168.20.0 255.255.254.0 tcp ftp service ftp vlan 499
serverfarm FWLB_OUT2IN persistent rebalance inservice!
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

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

- **muestre el vserver del *slot* Mod csm**`show mod csm 4 vservers vserver type prot virtual vlan state conns----------OUT2IN SLB any 192.168.20.0/23:0 499 OPERATIONAL 0 FW2SERV SLB any 192.168.20.0/23:0 169 OPERATIONAL 0 SERV2FW SLB any 0.0.0.0/0:0 500 OPERATIONAL 0 IN2OUT SLB any 0.0.0.0/0:0 168 OPERATIONAL 0 FTP_OUT2IN SLB TCP 192.168.20.0/23:21 499 OPERATIONAL 1 FTP_FW2SERV SLB TCP 192.168.20.0/23:21 169 OPERATIONAL 1`
- **muestre el detalle del *nombre del* nombre del vserver del *slot* Mod csm**`show mod csm 4 vservers name FTP_OUT2IN`vserver type prot virtual vlan state conns----------FTP_OUT2IN SLB TCP 192.168.20.0/23:21 499 OPERATIONAL 1 cpu0#show mod csm 4 vservers name FTP_OUT2IN detFTP_OUT2IN, type = SLB, state = OPERATIONAL, v_index = 26 virtual = 192.168.20.0/23:21 bidir, TCP, service = ftp, advertise = FALSE idle = 3600, replicate csrp = none, vlan = 499, pending = 30 max parse len = 2000, persist rebalance = TRUE ssl sticky offset = 0, length = 32 conns = 1, total conns = 1 Default policy: server farm = FWLB_OUT2IN, backup = <not assigned> sticky: timer = 0, subnet = 0.0.0.0, group id = 0 Policy Tot matches Client pkts Server pkts ---------- (default) 1 11 10`
- **muestre el detalle del conns del *slot* Mod csm**`sho mod csm 4 conns detail prot vlan source destination state ----------In TCP 499 192.168.11.46:2830 192.168.21.240:0 ESTAB Out TCP 168 192.168.21.240:0 192.168.11.46:2830 ESTAB vs = (n/a), ftp = Data, csrp = FalseIn TCP 169 192.168.11.46:2830 192.168.21.240:0 ESTAB Out TCP 500 192.168.21.240:0 192.168.11.46:2830 ESTAB vs = (n/a), ftp = Data, csrp = FalseIn TCP 169 192.168.11.46:2829 192.168.21.240:21 ESTAB Out TCP 500 192.168.21.240:21 192.168.11.46:2829 ESTAB vs = FTP_FW2SERV, ftp = Control, csrp = FalseIn TCP 499 192.168.11.46:2829 192.168.21.240:21 ESTAB Out TCP 168 192.168.21.240:21 192.168.11.46:2829 ESTAB vs = FTP_OUT2IN, ftp = Control, csrp = False`

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si usted experimenta el problema con esta configuración, la primera cosa a hacer es marcar si hay ninguno golpeado en el vserver publicando el comando del **vserver del *slot* Mod csm de la demostración**. Si usted no ve un golpe, aseegurese el vserver está en el servicio. Aseegurese el tráfico se envía al CS usando una traza de sniffer. Cuando usted ve los golpes, publique el **comando detail del conns del *slot* Mod csm de la demostración** de verificar que una entrada fue creada para la conexión que usted está buscando. Usted entonces necesitará utilizar un sniffer otra vez para aseegurarse el tráfico se envía al Firewall correcto (usted puede también utilizar cualquier tipo de abrir una sesión el Firewall). Procede esta manera de seguir la trayectoria del tráfico.

Información Relacionada

- Configuración del modo seguro (router) en el CSM

- Soporte del hardware del módulo content switching
- Descargas del software del módulo content switching (clientes registrados solamente)
- Soporte Técnico - Cisco Systems