Exemple de configuration d'équilibrage de charge du pare-feu avec CSM

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour l'installation de l'Équilibrage de charge de pare-feu (FWLB) tout en à l'aide de seulement un module de commutation de contenu (CSM). FWLB exige de la batterie de Pare-feu d'être entourée par des équilibreurs de charge. C'est de garantir que le trafic en entrée et en sortie d'une session simple est chargement équilibré au même Pare-feu. En utilisant un CSM, vous pouvez utiliser le même module pour réaliser le travail des deux loadbalancers. Ce document t'affiche comment réaliser ceci.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 3.x courante CSM

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer le CSM pour FWLB comme décrit dans ce document.

Note: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise la configuration suivante :

Version 3.x courante CSM

```
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 !
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **affichez le vserver d'*emplacement* modèle 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
```

- **affichez le détail de *nom de* nom de vserver d'*emplacement* modèle 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 det
FTP_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
```

- affichez le détail de conns d'*emplacement* modèle 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 = False

In  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 = False

In  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 = False

In  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
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si vous rencontrez le problème avec cette installation, la première chose à faire est de vérifier s'il y a n'importe quel hit sur le vserver en émettant la commande de **vserver d'*emplacement* modèle csm d'exposition**. Si vous ne voyez pas un hit, assurez-vous que le vserver est en service. Assurez-vous que le trafic est envoyé au CSM utilisant un tracé de renifleur. Quand vous voyez des hit, émettez la commande de **détail de conns d'*emplacement* modèle csm d'exposition** de vérifier qu'une entrée a été créée pour la connexion que vous recherchez. Vous devrez alors employer un renifleur de nouveau pour s'assurer que le trafic est envoyé au Pare-feu correct (vous pouvez également utiliser n'importe quel type d'ouvrir une session le Pare-feu). Poursuivez de cette façon de suivre le chemin du trafic.

Informations connexes

- Configurer le mode sécurisé (de routeur) sur le CSM
- Support matériel de module de commutation de contenu
- Téléchargements de logiciel du module de commutation de contenu (clients enregistrés seulement)
- Support technique - Cisco Systems