1 台の CSM を使用するファイアウォール負荷分散の設定例

目次

概要

このドキュメントでは、コンテンツ スイッチング モジュール（CSM）を 1 つしか使用していないにもかかわらず、ファイアウォール ロード バランシング（FWLB）を設定する設定例について説明します。 FWLB で、ファイアウォール ファームがロード バランサで囲まれている必要があります。 これは、単一のセッションの着信および発信トラフィックが同じファイアウォールにロード バランシングされていることを保証するためです。 CSM を使用する場合、両方のロードバランサのジョブを実行するために、同じモジュールを使用できます。 このドキュメントでは、その実現方法を説明します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CSM Running バージョン 3.x

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

ここでは、このドキュメントで説明されている FWLB 用の CSM を設定するための情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

このドキュメントでは次の設定を使用しています。

CSM Running バージョン 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 !
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show mod csm slot vserver**

```
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
```

- **show mod csm slot vserver name name detail**

```
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
```

- **show mod csm slot conns detail**

```
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
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

この設定で問題が発生する場合、最初にすることは、**show mod csm slot vserver コマンド**を発行して、vserver 上にヒットがあるかどうかを確認することです。 ヒットがない場合は、vserver がサービス中であることを確認します。 スニファ トレースを使用して、トラフィックが CSM に送信されることを確認してください。 ヒットがある場合は、**show mod csm slot conns detail コマンド**を発行して、探している接続に対してエントリが作成されたことを確認します。 その後、再度スニファを使用して、トラフィックが正しいファイアウォールに送信されることを確認する必要があります (ファイアウォール上で任意のタイプのロギングを使用することもできます)。 この方法を進めて、トラフィックのパスを追跡します。

関連情報

- CSM でのセキュア (ルータ) モードの設定
- コンテンツ スイッチング モジュール ハードウェアに関するサポート
- コンテンツ スイッチング モジュール ソフトウェアのダウンロード (登録ユーザ専用)
- テクニカルサポート - Cisco Systems