

CSS 11000 でのファイアウォール ロード バランシングの設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

ファイアウォール ロード バランシングは、ファイアウォールによる冗長性を許容します。これは、外部、内部ペアの Cisco CSS 11000 コンテンツ サービス スイッチを使用し、Virtual Router Redundancy Protocol (VRRP) 接続により相手ピアと通信します。外部のスイッチは、ファイアウォールを通して内部スイッチと通信しパス情報を保守します。スイッチは、マトリックスによりフロー情報の保守が可能です。

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。

- Cisco 11000 シリーズ Content Service スイッチ

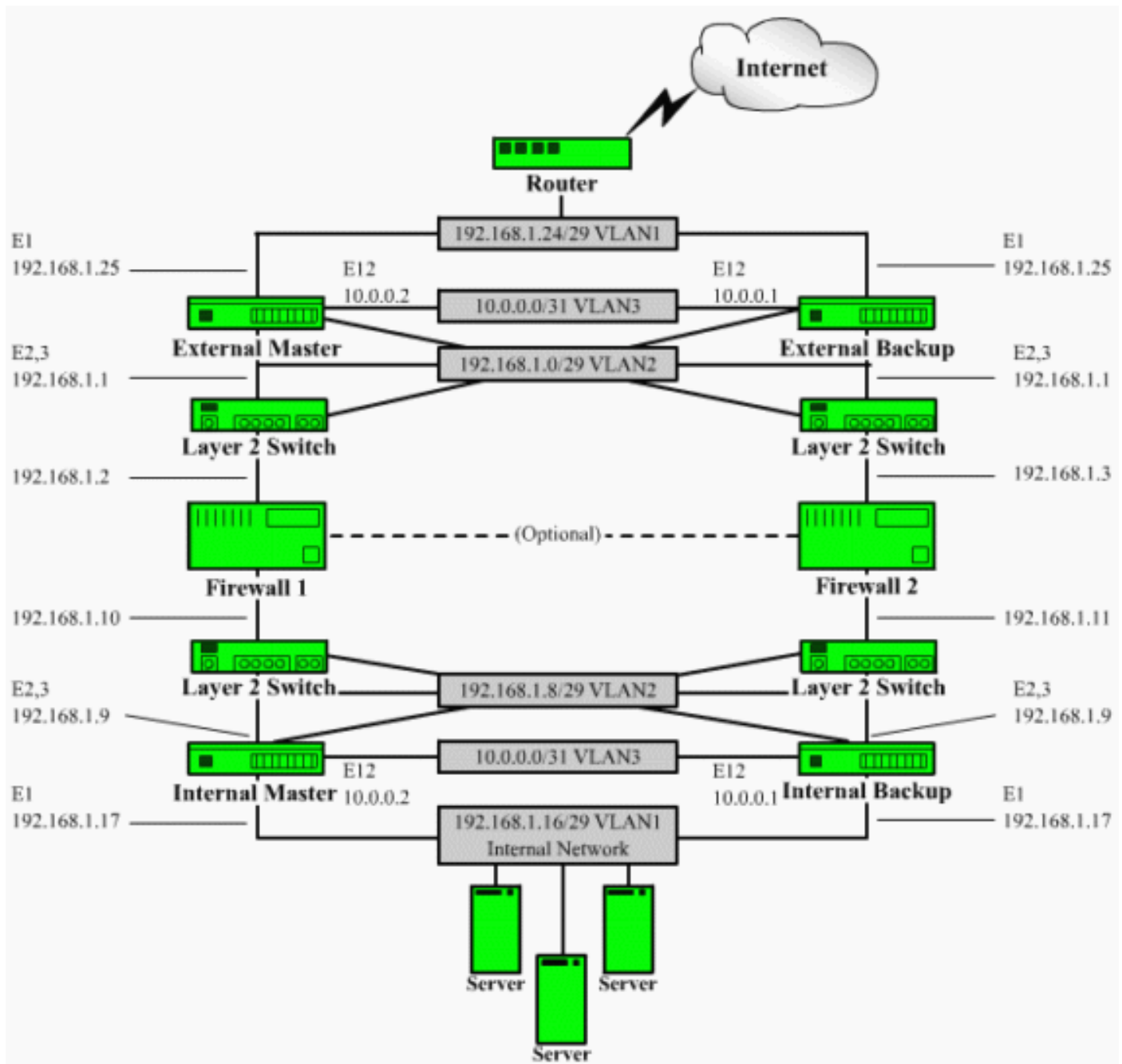
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ネットワーク図

グラフィックは下記のネットワーク例ネットワーク構成を示します。



標準の例を参照するために動きのアニメーションをすべてのデバイスが下記に示されているコンフィギュレーションと正しく動作していると思われる負荷バランシングされたトラフィックパターン参照して下さい。

説明

ファイアウォールは CSSes の間でインターネット制御メッセージ プロトコル (ICMP) パケットを渡すために設定する必要があります。リンクがダウンすると、冗長パスが有効になります。

設定

このファイアウォール設定では、ローカルおよびリモートの CSS を同じファイアウォール インデックス番号で設定する必要があります。

- [ExternalPrimary の設定](#)
- [InternalMaster の設定](#)
- [ExternalBackup の設定](#)
- [InternalBackup の設定](#)

ExternalPrimary の設定

```
!***** GLOBAL
*****

!--- Enable switch redundancy. ip redundancy !--- Define
Firewall Path 1. ip firewall 1 192.168.1.2 192.168.1.10
192.168.1.9 !--- Define Firewall Path 2. ip firewall 2
192.168.1.3 192.168.1.11 192.168.1.9 !--- Tie routes to
the firewall paths
!--- serving as the destination. ip route 192.168.1.8
255.255.255.248 firewall 1 1 ip route 192.168.1.8
255.255.255.248 firewall 2 1 ip route 192.168.1.16
255.255.255.248 firewall 1 1 ip route 192.168.1.16
255.255.255.248 firewall 2 1 !*****
INTERFACE ***** interface ethernet-2
bridge vlan 2 interface ethernet-3 bridge vlan 2
interface ethernet-12 bridge vlan 3
!***** CIRCUIT
***** circuit VLAN1 !--- Enable
redundancy on the outside of the switch. redundancy ip
address 192.168.1.25 255.255.255.248 circuit VLAN2 !---
Enable redundancy on the inside of the switch.
redundancy ip address 192.168.1.1 255.255.255.248
circuit VLAN3 !--- Enable redundancy protocol between
switches. redundancy-protocol ip address 10.0.0.2
255.255.255.252
```

InternalMaster の設定

```
!***** GLOBAL
*****

!--- Enable switch redundancy. ip redundancy !--- Same
paths as before, but now from the perspective
!--- of the inside switch. ip firewall 1 192.168.1.10
192.168.1.2 192.168.1.1 ip firewall 2 192.168.1.11
192.168.1.3 192.168.1.1 ip route 0.0.0.0 0.0.0.0
firewall 1 1 ip route 0.0.0.0 0.0.0.0 firewall 2 1
!***** INTERFACE
***** interface ethernet-1 bridge
vlan 2 interface ethernet-2 bridge vlan 2 interface
ethernet-12 bridge vlan 3 !*****
CIRCUIT ***** circuit VLAN1
redundancy ip address 192.168.1.17 255.255.255.248
circuit VLAN2 redundancy ip address 192.168.1.9
255.255.255.248 circuit VLAN3 redundancy-protocol ip
address 10.0.0.2 255.255.255.252
!***** SERVICE
***** service Server1 ip address
192.168.1.200 active service Server2 ip address
192.168.1.201 active !***** OWNER
```

```
***** owner foo.com content
L3_Basic vip address 192.168.1.100 add service Server1
add service Server2 active
```

ExternalBackup の設定

```
!***** GLOBAL
*****
ip redundancy
ip firewall 1 192.168.1.2 192.168.1.10 192.168.1.9
ip firewall 2 192.168.1.3 192.168.1.11 192.168.1.9
ip route 192.168.1.8 255.255.255.248 firewall 1 1
ip route 192.168.1.8 255.255.255.248 firewall 2 1
ip route 192.168.1.16 255.255.255.248 firewall 1 1
ip route 192.168.1.16 255.255.255.248 firewall 2 1

!***** INTERFACE
*****
interface ethernet-1
  bridge vlan 2
interface ethernet-2
  bridge vlan 2
interface ethernet-12
  bridge vlan 3

!***** CIRCUIT
*****
circuit VLAN1
  redundancy
  ip address 192.168.1.25 255.255.255.248
circuit VLAN2
  redundancy
  ip address 192.168.1.1 255.255.255.248
circuit VLAN3
  redundancy-protocol
  !--- The one difference. ip address 10.0.0.1
  255.255.255.252
```

InternalBackup の設定

```
!***** GLOBAL
*****
ip redundancy
ip firewall 1 192.168.1.10 192.168.1.2 192.168.1.1
ip firewall 2 192.168.1.11 192.168.1.3 192.168.1.1
ip route 0.0.0.0 0.0.0.0 firewall 1 1
ip route 0.0.0.0 0.0.0.0 firewall 2 1

!***** INTERFACE
*****
interface ethernet-1
  bridge vlan 2
interface ethernet-2
  bridge vlan 2
interface ethernet-12
  bridge vlan 3

!***** CIRCUIT
*****
circuit VLAN1
  redundancy
  ip address 192.168.1.17 255.255.255.248
circuit VLAN2
```

```
redundancy
ip address 192.168.1.9 255.255.255.248
circuit VLAN3
redundancy-protocol
!--- The one difference. ip address 10.0.0.1
255.255.255.252 !***** SERVICE
***** service Server1 ip address
192.168.1.200 active service Server2 ip address
192.168.1.201 active !***** OWNER
***** owner foo.com content
L3_Basic vip address 192.168.1.100 add service Server1
add service Server2 active
```

確認

設定が正常であることを確認するために、ネットワークの部分をフェールオーバーに引き起こし、トラフィックがまだフローできるようにして下さい。

注: バックアップ CSS が有効になると、フロー情報を維持しつつ、フェールするまで有効状態を保ちます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。