

在CSS 11000上的的防火墙负载均衡的配置

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[说明](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

防火墙负载均衡允许冗余通过防火墙。它使用一对外部和内部的Cisco CSS 11000内容服务交换机/该交换机通过虚拟路由器冗余协议(VRRP)连接与它们的对等体进行通信。外部的交换机通过防火墙与内部交换机保留路径信息。交换机能通过矩阵维护流信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于下列软件和硬件版本：

- Cisco 11000系列内容服务交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

下面的图形显示示例网络配置。

参考[数据包的动画在行动的](#) 参见正常的示例，发生的负载均衡的流量模式，当所有设备适当地操作与如下所示的配置。

说明

必须配置防火墙传递互联网控制消息协议(ICMP)数据包在CSS之间。如果链路断开，冗余路径enable (event)。

配置

在此防火墙配置内，您必须使用相同防火墙索引编号配置本地和远程CSS。

- [外部主配置](#)
- [InternalMaster配置](#)
- [外部备份配置](#)
- [InternalBackup配置](#)

```
外部主配置
|***** 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配置
|***** 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

```

外部备份配置

```

!***** 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配置

```

!***** 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

```

验证

如果要验证配置是否成功，请对网络进行分区故障切换操作，以确保数据流仍处于流动状态。

注意：一旦启用备份CSS，如果不发生，它将一直处于启用状态，并且同时保留流信息。

故障排除

目前没有针对此配置的故障排除信息。