

Firewall Load Balancing Configuration on the CSS 11000

Document ID: 16552



This document contains Flash animation

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Description
- Configurations

Verify

Troubleshoot

Related Information

Introduction

Firewall load balancing allows for redundancy through the firewall. It employs a pair of outside and inside Cisco CSS 11000 content services switches, which communicate with their peer through a Virtual Router Redundancy Protocol (VRRP) connection. The switches on the outside communicate, through the firewall, with the inside switches to maintain path information. The switches are able to maintain flow information through the matrix.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the following software and hardware versions:

- Cisco 11000 Series Content Service Switches

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

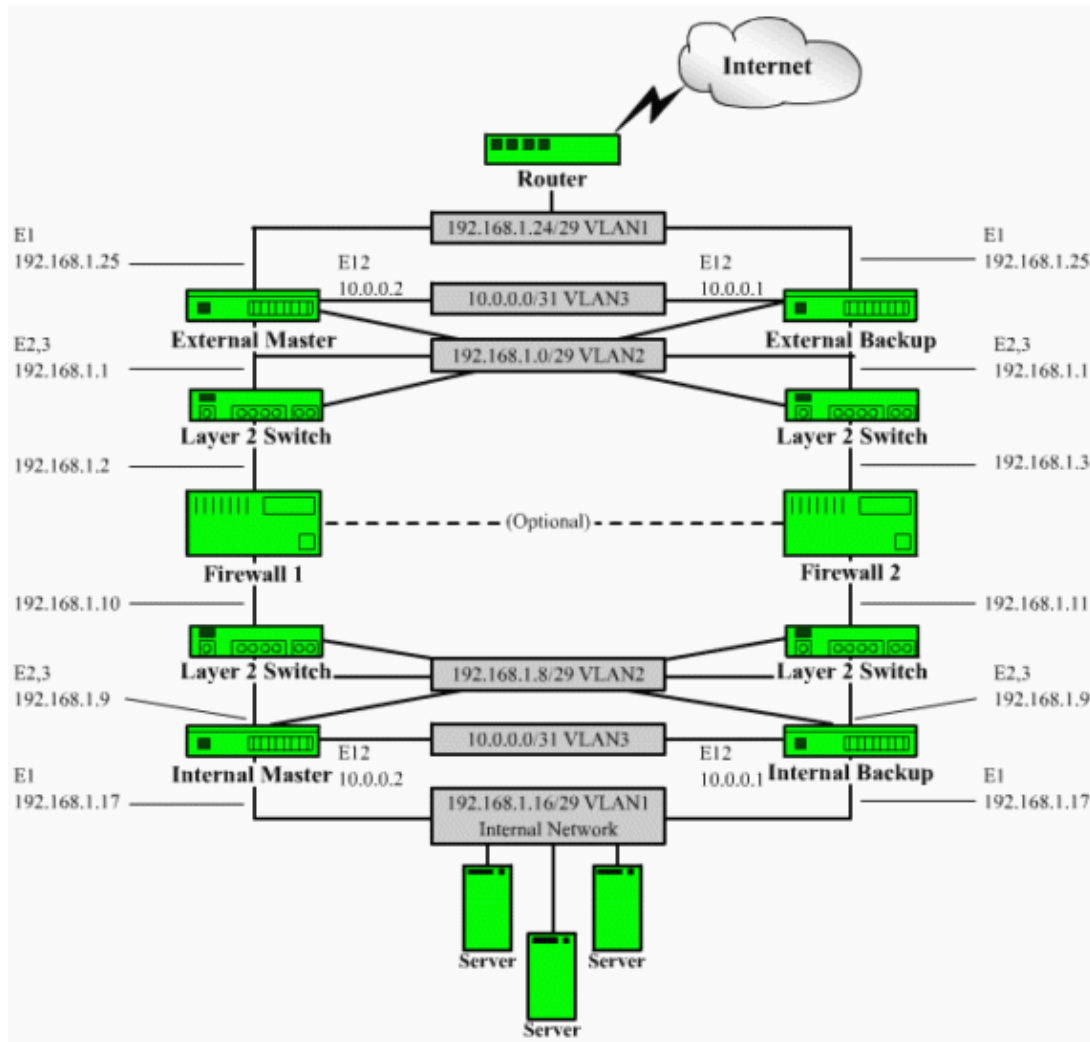
For more information on document conventions, see the Cisco Technical Tips Conventions.


Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

The graphic below shows an example network configuration.



 Refer to the animation of the packets in motion [to see an example of the normal, load-balanced traffic patterns that occur when all devices are properly operating with the configurations shown below.](#)

Description

The firewalls must be configured to pass Internet Control Message Protocol (ICMP) packets between the CSSes. If a link goes down, the redundant path enables.

Configurations

Within this firewall configuration, you must configure both the local and remote CSSes with the same firewall index number.

- ExternalPrimary Configuration
- InternalMaster Configuration
- ExternalBackup Configuration
- InternalBackup Configuration

ExternalPrimary Configuration

```

!***** 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 Configuration

```

!***** 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 Configuration

```
!***** 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 Configuration

```

!***** 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

```

Verify

To verify that the configuration is successful, cause portions of the network to failover and ensure that traffic can still flow.

Note: Once a backup CSS becomes enabled, it stays enabled until it fails, preserving flow information.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [CSS 11000 Series Content Services Switches Technical Support](#)
 - [CSS 11500 Series Content Services Switches Technical Support](#)
 - [Content Networking Devices Technical Support](#)
 - [Cisco Web Network Services Software Technical Support](#)
 - [Cisco WebNS CSS11000 Software Download Page \(registered customers only\)](#)
 - [Cisco WebNS CSS11500 Software Download Page \(registered customers only\)](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 04, 2004

Document ID: 16552
