

# Terminating VPN Traffic on a CSS Load-Balanced Firewall

Document ID: 12650

---

## **Introduction**

### **Prerequisites**

Requirements

Components Used

Conventions

### **Background Information**

#### **Problem**

#### **Workaround**

Requirements

Procedure

### **Related Information**

---

## **Introduction**

This document discusses the termination of Virtual Private Network (VPN) traffic on a Content Service Switch (CSS) load-balanced firewall.

## **Prerequisites**

### **Requirements**

Cisco recommends that you have knowledge of these topics:

- VPN
- CSS
- IP Security (IPSec)

### **Components Used**

The information in this document is based on the Cisco CSS 11000 series content services 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**

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## **Background Information**

Cisco usually recommends that you send IPSec traffic around a CSS, or terminate IPSec traffic before the CSS. There is no value in sending this type of encrypted traffic through a CSS. However, in some cases, IPSec traffic must traverse the CSS.

One such case is when you use two switches in a firewall load–balancing situation, and the Virtual Private Network (VPN) termination point is on the firewall. The firewall load–balancing feature of the CSS ensures that all traffic, in either direction between a pair of IP addresses, flows through the same firewall.

## Problem

The CSS does not set up a flow for IPSec traffic. Therefore, the CSS cannot guarantee that the traffic passes through the same firewall on which the traffic came in.

**Note:** If you send too much IPSec traffic through the CSS 11000, you can easily overwhelm the box. The CSS 11000 design is not based upon a central processor architecture (like in a basic switch). Therefore, there are limits as to how many tunnels can traverse the box.

## Workaround

### Requirements

The workaround for this problem requires that:

- You know all VPN source addresses.
- VPN traffic always terminates at the same firewall.
- VPN traffic does not have to be firewall load–balanced.

### Procedure

On the bottom firewall, place static routes for all source addresses that use VPN to enter the network. Static routes must point return traffic to the same firewall on which VPN traffic was terminated. In most cases, this is feasible only if the VPN traffic is a small percentage of all the traffic that passes through the firewalls, because the traffic is not firewall load–balanced.

---

## Related Information

- [Cisco CSS 11000 Series Support Page](#)
- [Firewall Load Balancing Configuration on the CSS 11000](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

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

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 01, 2006

Document ID: 12650

---