

# Filtering the NIMDA Virus on CSS 11000

Document ID: 16554

---

- Introduction**
- Before You Begin**
  - Conventions
  - Prerequisites
  - Components Used
- Configuring the CSS 11000**
- Verify**
- Troubleshoot**
- Related Information**

---

## Introduction

This document provides information on how to filter the NIMDA virus on the CSS 11000. It should be noted that these are the same instructions used for filtering Code Red on CSS 11000.

## Before You Begin

### Conventions

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

### Prerequisites

There are no specific prerequisites for this document.

### Components Used

The information in this document is based on the software and hardware versions below.

- This software release on the CSS 11000 is 5 Build 2.
- This hardware revision is that of a CSS 11150.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## Configuring the CSS 11000

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

Use the following procedure to configure the CSS 11000.

1. Ensure that your CSS is running the most recent version of code. See [Upgrading Your CSS Software](#).
2. Create a dummy service with no keepalive type nor method, also pointing to a nonexistent IP address:

```
!***** SERVICE *****  
service dummy
```

```
ip address 10.10.10.10
keepalive type none
active
```

**Note:** Additional resources are tied up when the CSS continually tries to contact a nonexistent service until it times out. It is suggested that a Real machine capable of responding with TCP RST be installed to handle all redirected requests.

**Note:** It is important that the dummy service has an IP address in a directly connected subnet to the CSS. This will keep the unwanted traffic from traversing any additional routers, keeping network overhead to a minimum.

3. Create header-field-group such that the CSS will be able to inspect all incoming content requests for HTTP header fields.

```
!***** HEADER FIELD GROUP *****
header-field-group .ida
  header-field .ida request-line contain ".ida"

header-field-group cmd.exe
  header-field cmd.exe request-line contain "cmd.exe"

header-field-group default.ida
  header-field default.ida request-line contain "default.ida"

header-field-group root.exe
  header-field root.exe request-line contain "root.exe"

header-field-group x.ida
  header-field x.ida request-line contain "x.ida"
```

4. Apply header-field-group and dummy service to content rules.

```
!***** OWNER *****
owner myrule

content block_.ida
  protocol tcp
  port 80
  url "/*"
  header-field-rule .ida weight 0
  add service dummy
  active

content block_cmd.exe
  protocol tcp
  port 80
  url "/*"
  header-field-rule cmd.exe weight 0
  add service dummy
  active

content block_default.ida
  protocol tcp
  port 80
  url "/*"
  header-field-rule default.ida weight 0
  add service dummy
  active

content block_root.exe
  protocol tcp
  port 80
  url "/*"
  header-field-rule root.exe weight 0
```

```

add service dummy
active

content block_x.ida
protocol tcp
port 80
url "/*"
header-field-rule x.ida weight 0
add service dummy
active

```

**Note:** If the CSS is not configured with Layer 5 rules, the proposed configuration will have an impact on performance, as all rules with TCP port 80 will be processed as Layer 5.

## Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool ( registered customers only) , which allows you to view an analysis of **show** command output.

- **show summary** – Verifies the Layer 3 status.
- **show service summary** – Displays the server state.

The following is the command output of the **show summary** command.

```

44-css150#show summary
Global Bypass Counters:
  No Rule Bypass Count:    11
  Acl Bypass Count:       0

Owner          Content Rules  State  Services  Service Hits
-----
myrule         block_.ida    Active dummy      50
               block_x.ida   Active dummy       0
               block_cmd.exe Active dummy     96
               block_root.exe Active dummy     14
               block_default.id Active dummy       0

44-css150#

```

The following is the command output of the **show service summary** command.

```

44-css150# show service summary

Service Name          State  Conn  Weight  Avg  State
                   Load  Transitions
-----
dummy                 Alive    0     1     2     6
ns-ms1                 Alive    0     1     2     4
ns-ms2                 Alive    0     1     2    10
web1                   Alive    0     1     2     0

```

# Troubleshoot

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

---

## Related Information

- [How to Protect Our Network from the NIMDA Virus](#)
  - [PSIRT Advisories](#)
  - [Technical Support – Cisco Systems](#)
- 

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: May 03, 2004

Document ID: 16554

---