

Cisco Clean Access (NAC Appliance) Bandwidth Management Configuration Example

Document ID: 98583

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Control Bandwidth Usage

- Configure Bandwidth Settings for a Role

Troubleshoot

[NetPro Discussion Forums – Featured Conversations](#)

Related Information

Introduction

Cisco Clean Access (NAC Appliance) allows you to control how much network bandwidth is available to users by role. You can independently configure bandwidth management using global forms in the Clean Access Manager (CAM) as needed for system user roles, or only on certain Clean Access Servers (CASes) using local forms. However, the option must first be enabled on the CAS for this feature to work. You can also specify bandwidth constraints for each user within a role or for the entire role.

For example, for a CAM that manages two CASes, you can specify all the roles and configure bandwidth management on some of the roles as needed (for example, guest role, quarantine role, temporary role, and so forth). If bandwidth is only important in the network segment where CAS1 is deployed and not on the network segment where CAS2 is deployed, you can then turn on bandwidth management on CAS1 but not CAS2.

With bursting, you can allow for brief deviations from a bandwidth constraint. This accommodates users who need bandwidth resources intermittently (for example, when users download and read pages), while users that attempt to stream content or transfer large files are subject to the bandwidth constraint. By default, roles have a bandwidth policy that is unlimited (specified as -1 for both upstream and downstream traffic).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Clean Access (NAC Appliance) with version 3.6.

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 the Cisco Technical Tips Conventions for more information on document conventions.

Control Bandwidth Usage

Configure Bandwidth Settings for a Role

Complete these steps in order to configure bandwidth settings for a role:

1. Choose **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Bandwidth** in order to enable bandwidth management on the CAS.
2. Select **Enable Bandwidth Management** and click **Update**.
3. Choose **User Management > User Roles > Bandwidth** and click the **Edit** button next to the role for which you want to set bandwidth limitations. The Bandwidth form appears as this example shows:

The screenshot shows a web interface for configuring bandwidth settings for a user role. The breadcrumb navigation is "User Management > User Roles". Below this is a horizontal menu with five tabs: "List of Roles", "New Role", "Traffic Control", "Bandwidth", and "Schedule". The "Bandwidth" tab is selected. The form contains the following fields:

- Role Name:** Temporary Role
- Upstream Bandwidth:** 500 Kbits/sec (with a note: "(the minimum recommended value is 100; use -1 for unlimited)")
- Downstream Bandwidth:** 4000 Kbits/sec (with a note: "(the minimum recommended value is 100; use -1 for unlimited)")
- Burstable Traffic:** 1 (with a note: "(from 1 to 10; the burst rate is determined by multiplying this number by the bandwidth)")
- Shared Mode:** A dropdown menu showing "Each user owns the specified bandwidth".
- Description:** An empty text input field.

At the bottom of the form are two buttons: "Save" and "Cancel".

Note: Alternatively, you can go to **User Management > User Roles > List of Roles** and click the **BW** button next to the role.

4. Set the maximum bandwidth in kilobits per second for upstream and downstream traffic in Upstream Bandwidth and Downstream Bandwidth. Upstream traffic moves from the untrusted to the trusted network, and downstream traffic moves from the trusted to the untrusted network.
5. Enter a Burstable Traffic level from 2 to 10 in order to allow brief (one second) deviations from the bandwidth limitation. A Burstable Traffic level of 1 has the effect of disabling bursting.

The Burstable Traffic field is a traffic burst factor used to determine the capacity of the bucket. For example, if the bandwidth is 100 Kbps and the Burstable Traffic field is 2, then the capacity of the bucket is $100 \text{ Kb} * 2 = 200 \text{ Kb}$. If a user does not send any packets for awhile, the user has at most 200

Kb tokens in their bucket. Once the user needs to send packets, the user is able to send out 200 Kb packets right away. Thereafter, the user must wait for the tokens that come in at the rate of 100 Kbps to send out additional packets. This can be thought of as a way to specify that for an average rate of 100 Kbps, the peak rate is approximately 200 Kbps. Hence, this feature is intended to facilitate bursty applications such as web browsing.

6. In the Shared Mode field, choose either one of these settings:

- ◆ **All users share the specified bandwidth** This setting applies for all users in the role. In this case, the total available bandwidth is a set amount. In other words, if a user occupies 80 percent of the available bandwidth, only 20 percent of the bandwidth is available for other users in the role.
- ◆ **Each user owns the specified bandwidth** This setting applies to each user. The total amount of bandwidth in use might fluctuate as the number of online users in the role increases or decreases, but the bandwidth for each user is the same.

Optionally, you can type a Description of the bandwidth setting.

7. Click **Save** when you are done.

The bandwidth setting is now applicable for the role and appears in the Bandwidth tab.

Note: If bandwidth management is enabled, devices allowed via a device filter without specifying a role use the bandwidth of the Unauthenticated Role.

Troubleshoot

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

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco NAC Appliance \(Clean Access\) – Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Sep 10, 2007

Document ID: 98583