Local Traffic Control Policies

This chapter describes how to set up traffic filtering rules in the Clean Access Server. Topics include:

Overview

Traffic control policies let you control what network resources can be accessed, and which users can access them. Traffic control policies are configured by user role, and must be configured for Agent Temporary and Quarantine roles.

Cisco NAC Appliance offers three types of traffic policies:

IP-based policies—IP-based policies are fine-grained and flexible and can stop traffic in any number of ways. IP-based policies are intended for any role and allow you to specify IP protocol numbers as well as source and destination port numbers. For example, you can create an IP-based policy to pass through IPSec traffic to a particular host while denying all other traffic.

Host-based policies—Host-based policies are less flexible than IP-based policies, but have the advantage of allowing traffic policies to be specified by host name or domain name when a host has multiple or dynamic IP addresses. Host-based policies are intended to facilitate traffic policy configuration primarily for Agent Temporary and Quarantine roles and should be used for cases where the IP address for a host is continuously changing or if a host name can resolve to multiple IPs.

Layer 2 Ethernet traffic policies—To support data transfer or similar operations originating at the Layer 2 level, Cisco NAC Appliance Layer 2 Ethernet traffic control policies enable you to allow or deny Layer 2 Ethernet traffic through the CAS based on the type of traffic. Network Frames except for IP, ARP, and RARP frames constitute standard Layer 2 traffic.

Note Layer 2 Ethernet traffic control only applies to Clean Access Servers operating in Virtual Gateway mode.

Traffic control policies are directional. IP-based and Layer 2 Ethernet traffic policies can allow or block traffic moving from the untrusted (managed) to the trusted network, or from the trusted to the untrusted network. Host-based policies allow traffic from the untrusted network to the specified host and trusted DNS server specified.

By default, when you create a new user role:

- All traffic from the untrusted network to the trusted network is blocked.
- All traffic from the trusted network to the untrusted network is allowed.

Since all traffic from the untrusted network is initially blocked, after creating a role you typically must create policies for permitting traffic as appropriate for the role.

Alternatively, a traffic control policy can block traffic to a particular machine or limit users to particular activities, such as email use or web browsing. Examples of policies are:

`deny access to the computer at 191.111.11.1`, or
`allow www communication from computers on subnet 191.111.5/24`

Finally, traffic control policies are hierarchical, and the order of the policy in the policy list affects how traffic is filtered. The first policy at the top of the list has the highest priority. The following examples illustrate how priorities work for Untrusted -> Trusted traffic control policies.

Example 1:

- Priority 1: Deny Telnet
- Priority 2: Allow All

Result: Only Telnet traffic is blocked and all other traffic is permitted.

Example 2 (priorities reversed):

- Priority 1: Allow All
- Priority 2: Deny Telnet

Result: All traffic is allowed, and the second policy blocking Telnet traffic is ignored.

Example 3:

1. Allow TCP *.* 10.10.10.1/255.255.255.255
2. Block TCP *.* 10.10.10.0/255.255.255.0

Result: Allow TCP access to 10.10.10.1 while blocking TCP access to everything else in the subnet (10.10.10.*).

Example 4 (Layer 2 Ethernet - Virtual Gateway mode only):

1. Allow SNA IBM Systems Network Architecture
2. Block ALL All Traffic

Result: Allow only IBM Systems Network Architecture (SNA) Layer 2 traffic and deny all other Layer 2 traffic.

Local vs. Global Traffic Policies

Most traffic control policies are set globally for all Clean Access Servers using the Clean Access Manager global forms. By adding local traffic policies in individual Clean Access Servers, you can specialize filtering for the network managed by that CAS by extending policies defined globally.

This chapter describes the local traffic control policies configured on a CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**.

Note that global policies appear with yellow background while local policies appear with white background in the local list of traffic policies. To delete a policy, use the global or local form you used to create it.

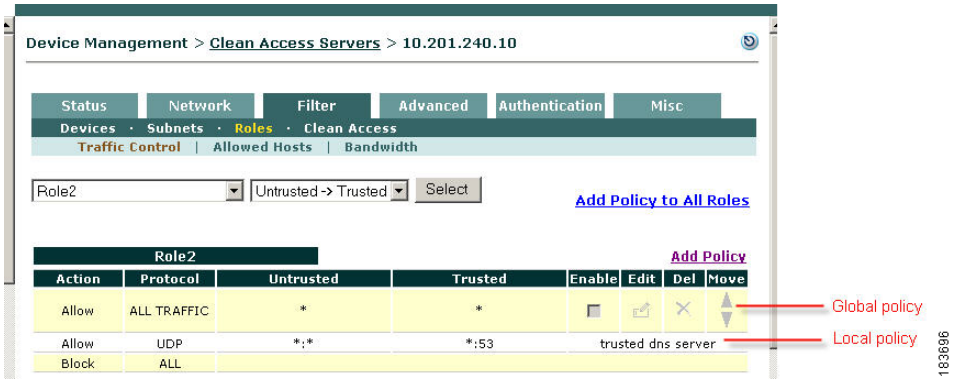
Global policies can only be accessed and modified from the **User Management > User Roles > Traffic Control** global forms. For details, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)*.

Note A local traffic control policy for a CAS takes precedence over a global policy for all Clean Access Servers if the local policy has a higher priority.

View Local Traffic Control Policies

To view and configure local traffic control role policies, go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**. The policies appear by role in the **Traffic Control** form, as shown in Figure 7-1.

Figure 7-1 Local Traffic Control Policies



By default, the page lists the policies for traffic traveling from the untrusted network as the source to the trusted network as the destination. To view the policies for the opposite direction, with the trusted network as the source and the untrusted network as the destination, choose **Trusted -> Untrusted** from the direction field and click **Select**.

Figure 7-2 Trusted -> Untrusted Direction Field

You can similarly display the policies for a single role by choosing the role from the role dropdown menu and clicking **Select**.

The priority of a policy corresponds to the order in which it appears in the list, the first item having the highest priority. You can change a policy's priority by clicking the corresponding up or down arrow in the **Move** column.

Add Local IP-Based Traffic Control Policies

Traffic control policies permit or block traffic to resources on the network and are created per role. Before creating a traffic control policy, make sure the role to which you want to assign the policy already exists. You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring IP-based traffic policies.

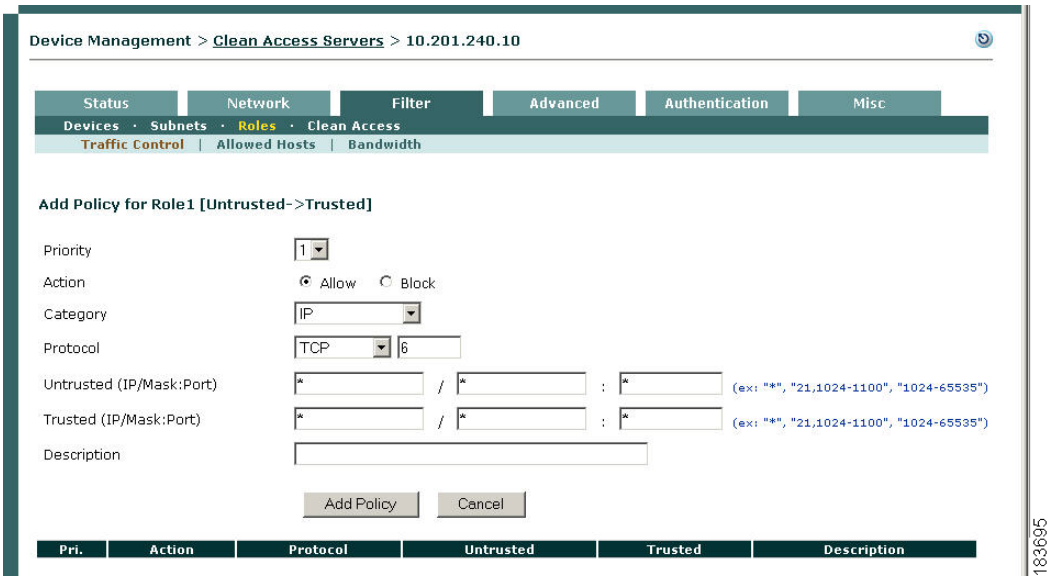
Add / Edit Local IP-Based Traffic Policy

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**.
2. In the **Traffic Control** form, select the source-to-destination direction for which you want the policy to apply. Chose either **Trusted -> Untrusted** or **Untrusted -> Trusted**, and click **Select**.
3. For a new policy:
   - Click the **Add Policy** link next to the role for which you want to create the policy, or
   - Click **Add Policy to All Roles** to add the new policy to all the roles (except the Unauthenticated role) at once.

   To modify an existing policy:
   - Click **Edit** next to the policy you want to modify.

   Figure 7-3 shows the Add Policy form.

Figure 7-3 Add New Local IP Policy



Note The **Add Policy to All Roles** option adds the policy to all roles except the Unauthenticated role. Once added, traffic policies are modified individually and removed per role only.

4. Set the **Priority** of the policy from the **Priority** dropdown menu. The IP policy at the top of the list will have the highest priority in execution. By default, the form displays a priority lower than the last policy created (1 for the first policy, 2 for the second policy, and so on). The number of priorities in the list reflects the number of policies created for the role. The built-in **Block All** policy has the lowest priority of all policies by default.

Note To change the **Priority**, of a policy later, click the Up or Down arrows for the policy in the **Move** column of the IP policies list page.

5. Set the **Action** of the traffic policy as follows:
   - **Allow** (default)– Permit the traffic.
   - **Block** – Drop the traffic.
6. Set the **Category** of the traffic as follows:
   - **ALL TRAFFIC** (default) – The policy applies to all protocols and to all trusted and untrusted source and destination addresses.
   - **IP** – If selected, the **Protocol** field displays as described below.
   - **IP FRAGMENT** – By default, the Clean Access Server blocks IP fragment packets, since they can be used in denial of service attacks. To permit fragmented packets, define a role policy allowing them with this option.
7. The **Protocol** field appears if the **IP** Category is chosen, displaying the options listed below:
   - **CUSTOM:** – Select this option to specify a different protocol number than the protocols listed in the **Protocol** dropdown menu.
   - **TCP (6)** – For Transmission Control Protocol. TCP applications include HTTP, HTTPS, and Telnet.
   - **UDP (17)** – For User Datagram Protocol, generally used for broadcast messages.
   - **ICMP (1)** – For Internet Control Message Protocol.
   - **ESP (50)** – For Encapsulated Security Payload, an IPsec subprotocol used to encrypt IP packet data typically in order to create VPN tunnels
   - **AH (51)** – Authentication Header, an IPSec subprotocol used to compute a cryptographic checksum to guarantee the authenticity of the IP header and packet.
8. In the **Untrusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the untrusted network to which the policy applies. An asterisk in the IP/Mask:Port fields means the policy applies for any address/application.

   If you chose TCP or UDP as the **Protocol**, also type the TCP/UDP port number for the application in the **Port** text field.

Note You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring TCP/UDP ports. For example, you can specify port values such as: "*****" or "**21, 1024-1100**" or "**1024-65535**" to cover multiple ports in one policy. Refer to http://www.iana.org/assignments/port-numbers for details on TCP/UDP port numbers.

9. In the **Trusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the trusted network to which the policy applies. An asterisk in the IP/Mask:Port fields means the policy applies for any address/application. If you chose TCP or UDP as the **Protocol**, also type the TCP/UDP port number for the application in the **Port** text field.
10. Optionally, type a description of the policy in the **Description** field.
11. Click **Add Policy** when finished. If modifying a policy, click the **Update Policy** button.

Note The traffic direction you select for viewing the list of policies (Untrusted -> Trusted or Trusted -> Untrusted) sets the source and destination when you open the **Add Policy** form:

- The first IP/Mask/Port entry listed is the source.
- The second IP/Mask/Port entry listed is the destination.

Add Local Host-Based Traffic Control Policies

Local host-based policies allow you to control user traffic to host sites for users in a role and for a particular Clean Access Server.

Default host policies for the Unauthenticated, Temporary, and Quarantine roles are automatically retrieved and updated after a Cisco NAC Appliance **Update** or **Clean Update** is performed from the CAM.

You can configure custom DNS host-based policies for a role by host name or domain name when a host has multiple or dynamic IP addresses. Note that to use any host-based policy, you must first add a Trusted DNS Server for the user role.

Note

- After a software upgrade, new default host-based policies are disabled by default but enable/disable settings for existing host-based policies are preserved.
- After a Clean Update, all existing default host-based policies are removed and new default host-based policies are added with default disabled settings.
- The host-based policies have higher priority than IP-based Traffic Policies. The traffic that passes through an allowed host is always allowed, even if an IP-based policy denies it.

See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)* for details on the automatic **Updates** downloaded to the CAM under **Device Management > Clean Access > Updates**.

Enable Proxy Traffic

You can enable an individual CAS to parse host policies when user traffic passes through a specified proxy server by redirecting user session packets to a local Proxy Server or to the URL of a preconfigured Proxy PAC (Proxy Auto Configuration) file reachable from the CAS.

When the **Parse Proxy Traffic** option is checked for an individual CAS, and a proxy server is specified on the CAS **Proxy** page, the CAS will check the payloads of GET, POST, and CONNECT HTTP/HTTPS/FTP requests to make sure that the host is on the host policy list before allowing traffic

to the proxy server. This allows users to access only the host sites enabled for a role (e.g. Temporary or Quarantine users that need to meet requirements) when the specified proxy server is used. Note that the "parse proxy traffic" feature is enabled per CAS, and you must specify the Proxy server IP and port on the CAS **Proxy** page and enable the **Parse Proxy Traffic** option for this feature to take effect.

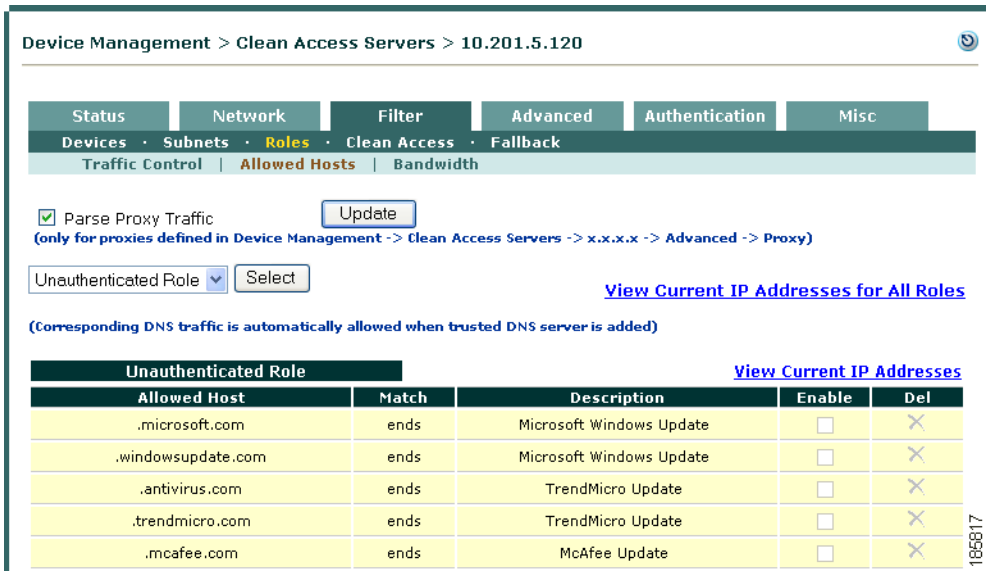
To enable host policies when traffic is going through proxy server specified on the CAS:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Proxy**.

Step 2 Specify the proxy source as described in Configure Proxy Server Settings on the CAS, page 4-47.

Step 3 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** (see Figure 7-4).

Figure 7-4 CAS—Allowed Hosts



Step 4 Enable the **Parse Proxy Traffic** option. This setting applies to all roles (Unauthenticated, Temporary, Quarantine, and normal user login roles).

When the **Parse Proxy Traffic** option is enabled for an individual CAS, the CAS checks the payloads of GET, POST and CONNECT HTTP/HTTPS/FTP requests to make sure that the host is on the host policy list before allowing traffic to the proxy server specified on the **Proxy** page. This allows users to access only the host sites enabled for the associated role when the specified proxy server is used. Note that you must specify the Proxy server IP and port (as described above) before enabling the **Parse Proxy Traffic** option on *each* CAS in your deployment.

Note When using proxy settings, also make sure DNS settings are properly configured on the CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Network > DNS**. See Configure DNS Servers on the Network, page 4-24 for details.

Step 5 Click the **Update** button.

Enable Proxy on CAS

When administrators apply Host Policies to the Unauthenticated Role, the CAS acts as a proxy for the client machine. If the CAS itself requires a proxy to access the network, you must modify the **/perfigo/access/apache/conf/httpd.conf** file configuration to feature a **`ProxyRemote * http://`***`<proxy>`***`:`***`<port>`** statement associated with an appropriate **`ProxyAllow`** statement.

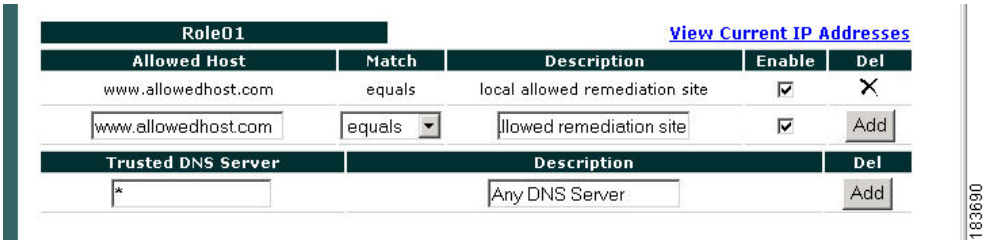
The following example illustrates a part of sample **httpd.conf** file that shows the **`ProxyRemote`** statement associated with an appropriate **`ProxyAllow`** statement:

```
<VirtualHost _default_:880>
    # TRACE OFF
    TraceEnable off
    RewriteEngine On
    RewriteRule ^perfigo$ "/perfigo/access/apache/www/fcgi-bin/proxy.fcgi"
    ProxyAllow "/proc/click/dnshandler/proxyallow"
    ProxyRemote * http://proxyID.mycompany.com:<port-number>/
    ProxyRequests On
</VirtualHost>
```

Note Refer to http://httpd.apache.org/docs for more apache syntax/usage references.

Add Local Allowed Host

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** and select the role for which to add a DNS host.



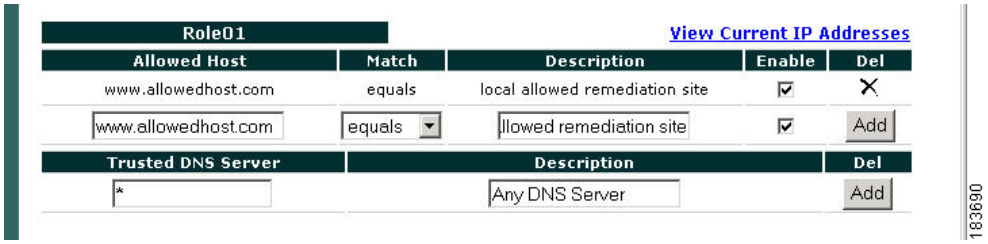
2. Type the hostname in the **Allowed Host** field (e.g. “allowedhost.com”).
3. In the **Match** dropdown menu, select an operator to match the host name: equals, ends, begins, or contains.
4. Type a description for the host in the **Description** field, such as “Allowed Host Update”.
5. Click **Enable**.
6. Click **Add**.

Note You must add a Trusted DNS Server to the role to enable host-based traffic policies for the role.

Add Local Trusted DNS Server

To add a local trusted DNS server:

1. Enter an IP address in the **Trusted DNS Server** field, or enter an asterisk "*" to specify any DNS server.



2. Type a description for the DNS server in the **Description** field.
3. Click **Add**.

Note When a trusted DNS server is added, an IP-based traffic policy allowing that server is automatically added for the role.

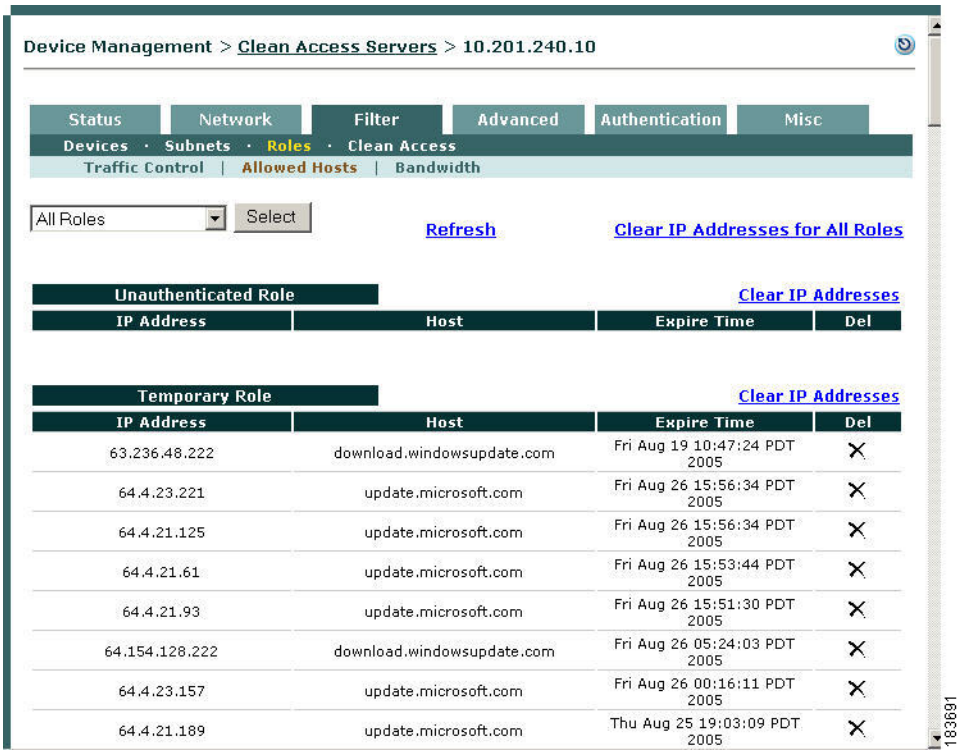
Note When you add a specific DNS server, then use this form later to add any ("*") DNS server, the previously added server becomes a subset of the overall policy allowing all DNS servers, and will not be displayed. If you later delete the any ("*") DNS server policy, the specific trusted DNS server you had previously allowed will be displayed again.

View IP Addresses Used by DNS Host

You can view the IP addresses used for the DNS host when clients connect to the host to update their systems.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts**.
2. To view all IP addresses for DNS hosts accessed across all roles, click the **View Current IP addresses for All Roles** at the top of the page**.**

Figure 7-5 View Current IP Addresses for All Roles



Note You can view this list from the CAS management pages, but modifying this list is done from the Clean Access Manager global filters forms. See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)* for details.

3. To view the IP addresses for DNS hosts accessed by clients in a specific role, click the **View Current IP addresses** link next to the desired role.
4. The IP address, Host name, and Expire time will display for each IP address accessed. The Expire time is based on the DNS reply TTL. When the IP address for the DNS host reaches the Expire time, it becomes invalid.

Add Layer 2 Ethernet Traffic Control Policies

Note Layer 2 Ethernet traffic control only applies to Clean Access Servers operating in Virtual Gateway mode.

Layer 2 Ethernet traffic control policies enable administrators to allow or block Layer 2 Ethernet traffic based on the type of Layer 2 traffic passing through the CAS.

Default traffic control policies for the Unauthenticated, Temporary, and Quarantine roles are automatically retrieved and updated after an Agent **Update** or **Clean Update** is performed from the CAM.

Note

- After a software upgrade, new default Layer 2 Ethernet traffic control policies are disabled by default but enable/disable settings for existing Ethernet traffic control policies are preserved.
- After a Clean Update, all existing Layer 2 Ethernet traffic control policies are removed and new default Ethernet traffic control policies are added with default disabled settings.

See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)* for details on the automatic **Updates** downloaded to the CAM under **Device Management > Clean Access > Updates**.

Enable Layer 2 Ethernet Traffic Control

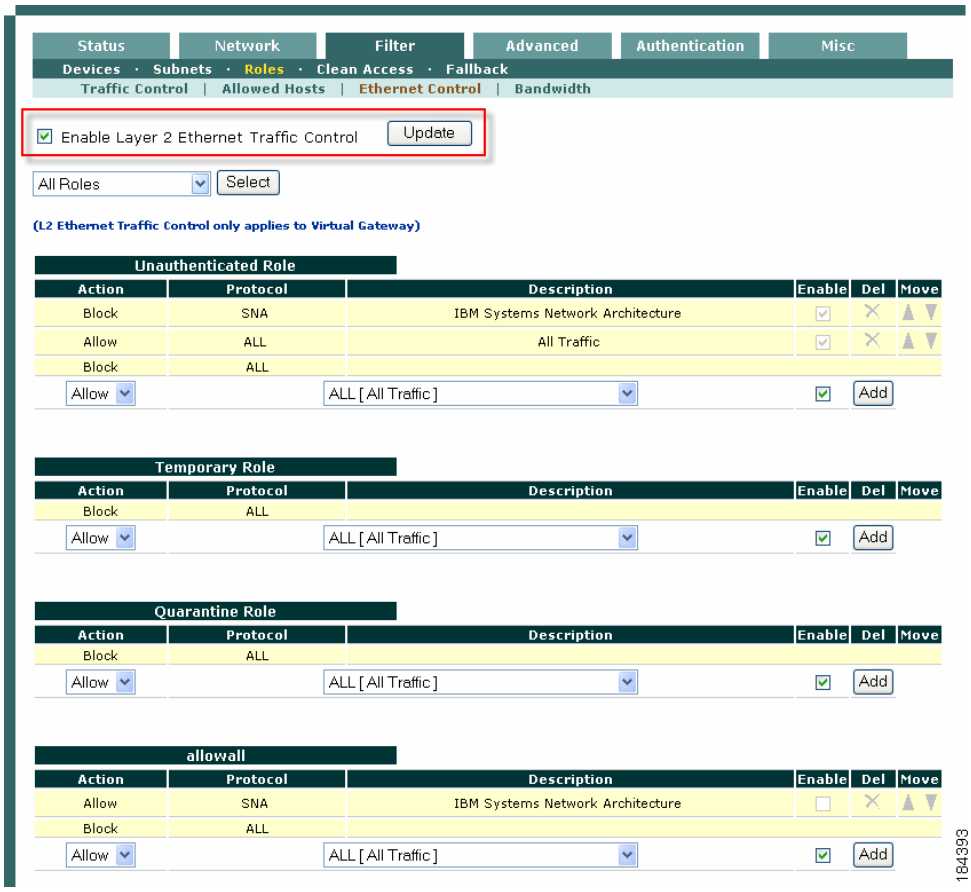
You can configure an individual CAS to allow or block specified Layer 2 Ethernet traffic based on control policies.

When the **Enable Layer 2 Ethernet Traffic Control** option is checked for an individual CAS, the CAS will apply relevant Layer 2 Ethernet traffic control policies to the traffic passing through the CAS, allowing or blocking packets based on the type of Layer 2 traffic passing through the CAS.

To enable Layer 2 Ethernet traffic control on the CAS:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Ethernet Control** (see Figure 7-6).

Figure 7-6 CAS—Ethernet Control



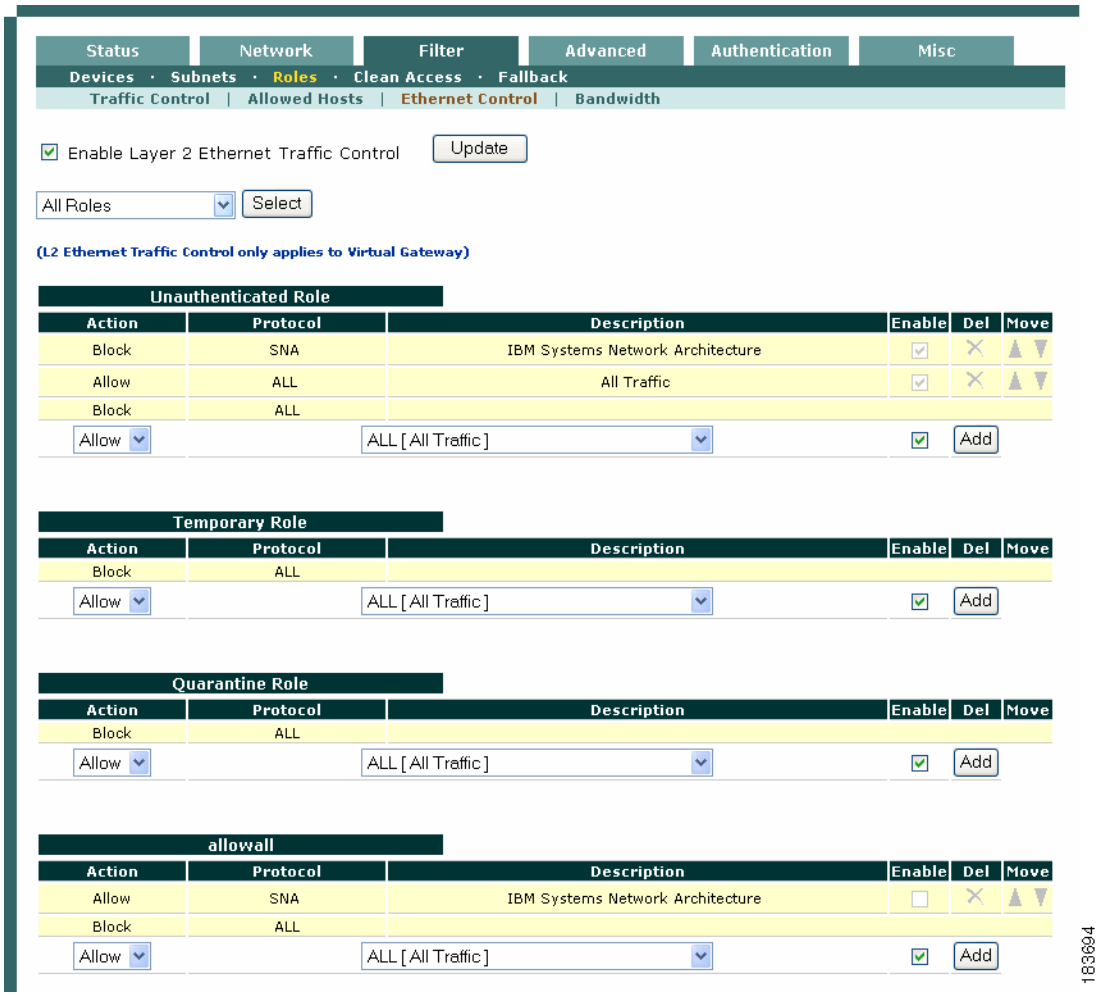
2. Click the checkbox for **Enable Layer 2 Ethernet Traffic Control**.
3. Click the **Update** button.

Add Layer 2 Ethernet Traffic Control

To add a Layer 2 Ethernet traffic control policy:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Ethernet Control** and select the role for which to allow or block Layer 2 Ethernet traffic.

Figure 7-7 Adding Layer 2 Ethernet Traffic Control



2. Select either **Allow** or **Block** from the **Action dropdown** menu.
3. Specify the type of Layer 2 Ethernet traffic to either allow or block in the **Protocol** dropdown menu.

Note Except for allowing all Layer 2 traffic, only the "IBM Systems Network Architecture (SNA)" protocol is available with Cisco NAC Appliance release 4.1(1) and later. Additional preset options may become available through the Cisco NAC Appliance update service on the Clean Access Manager.

4. Click **Enable**.
5. Click **Add**.

After you "Add" a traffic control policy, the CAM automatically populates the Description column for the entry with the description of the option you specified in the **Protocol** dropdown menu.

Controlling Bandwidth Usage

Cisco NAC Appliance lets you control how much network bandwidth is available to users by role. You can independently configure bandwidth management using global forms in the CAM as needed for system user roles, or only on certain Clean Access Servers 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 managing two CASs, you can specify all the roles and configure bandwidth management on some of the roles as needed (e.g. guest role, quarantine role, temporary role, etc.). 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.

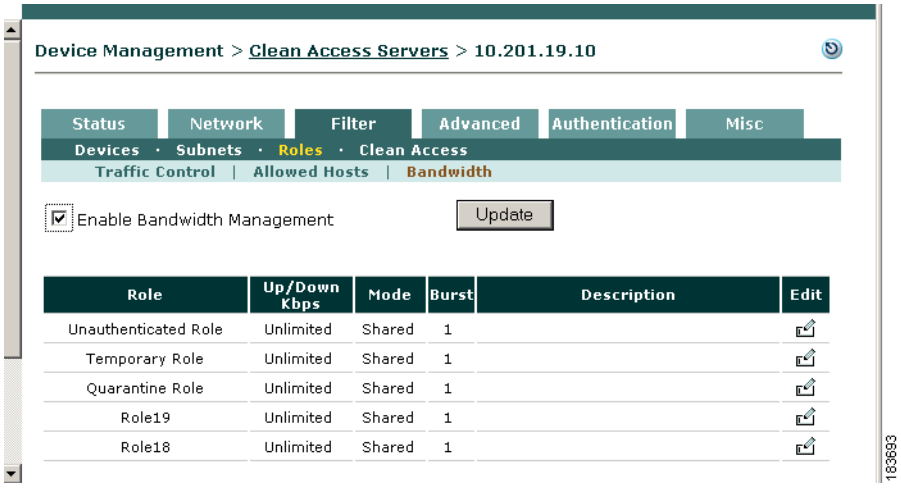
With bursting, you can allow for brief deviations from a bandwidth constraint. This accommodates users who need bandwidth resources intermittently (for example, when downloading and reading pages), while users attempting to stream content or transfer large files are subject to the bandwidth constraint.

By default, roles have a bandwidth policy that is unlimited (specified as -1 for both upstream and downstream traffic).

To configure local bandwidth settings for a role:

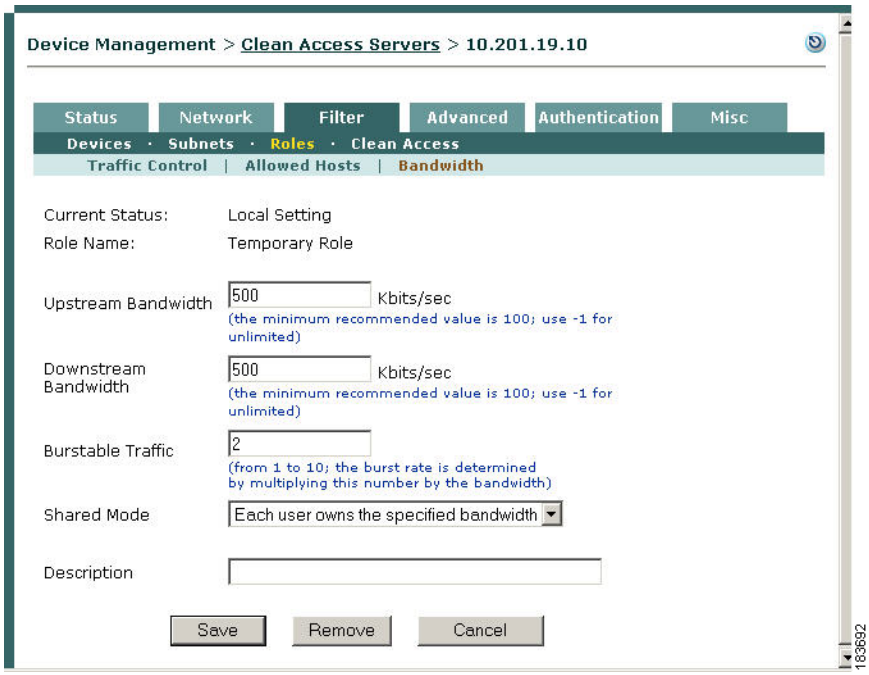
1. First, enable bandwidth management on the CAS by going to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Bandwidth**.
2. Select **Enable Bandwidth Management** and click **Update**.

Figure 7-8 Enable Bandwidth Management for the CAS



3. Click the **Edit** button next to the role for which you want to set bandwidth limitations. The **Role Bandwidth** form appears.

Figure 7-9 Local Bandwidth Form for User Role



4. The **Current Status** field lists either:
   - **Default Setting**: Local bandwidth management is not enabled (and settings from **User Management > User Roles > Bandwidth** are being used), or a local policy has not been set.
   - **Local Setting**: The configured local settings for this CAS apply for the selected role.
5. The **Role Name** fields lists the user role for which to configure local settings.
6. 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 (managed) to trusted side, while downstream traffic moves from the trusted to untrusted side.
7. Enter a **Burstable Traffic** level from 2 to 10 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 will be 100Kb*2=200Kb. If a user does not send any packets for a while, the user would have at most 200Kb tokens in his bucket, and once the user needs to send packets, the user will be able to send out 200Kb packets right away. Thereafter, the user must wait for the tokens coming in at the rate of 100Kbps to send out additional packets. This can be thought of as way to specify that for an average rate of 100Kbps, the peak rate will be approximately 200Kbps. Hence, this feature is intended to facilitate bursty applications such as web browsing.
8. In the **Shared Mode** field, choose either:
   - **All users share the specified bandwidth** – The 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 will be available for other users in the role.
   - **Each user owns the specified bandwidth** – The setting applies to each user. The total amount of bandwidth in use may fluctuate as the number of online users in the role increases or decreases, but the bandwidth for each user is equal.

9. Optionally, type a **Description** of the bandwidth setting.
10. Click **Save** when finished.

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

See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)* for additional details on bandwidth management.