CHAPTER 9

User Management: Traffic Control, Bandwidth, Schedule

This chapter describes how to configure role-based traffic control policies, bandwidth management, session and heartbeat timers. Topics include:

For details on configuring user roles and local users, see Chapter 7, "User Management: Configuring User Roles and Local Users."

For details on configuring authentication servers, see Chapter 8, "User Management: Configuring Authentication Servers."

For details on creating and configuring the web user login page, see Chapter 6, "Configuring User Login Page and Guest Access."

Overview

You can control the in-band user traffic that flows through the Clean Access Server with a variety of mechanisms. This section describes the Traffic Control, Bandwidth, and Scheduling policies configured by user role.

For new deployments of Cisco NAC Appliance, by default all traffic from the trusted to the untrusted network is allowed, and traffic from the untrusted network to the trusted network is blocked for the default system roles (Unauthenticated, Temporary, Quarantine) and new user roles you create. This allows you to expand access as necessary for traffic sourced from the untrusted network.

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.

You must create policies to allow traffic as appropriate for the role. Alternatively, you can configure traffic control policies to block traffic to a particular machine or limit users to particular activities, such as email use or web browsing. Examples of traffic policies are:

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

Traffic Policy Priority

Finally, the order of the traffic 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:

1. Deny Telnet
2. Allow All

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

Example 2 (priorities reversed):

1. Allow All
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.

Global vs. Local Scope

This chapter describes global traffic control policies configured under **User Management > User Roles > Traffic Control**. For details on local traffic control policies configured under **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**, see the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.6(1)*.

Note A local traffic control policy in a specific CAS takes precedence over a global policy if the local policy has a higher priority.

Traffic policies you add using the global forms under **User Management > User Roles > Traffic Control** apply to all Clean Access Servers in the CAM's domain and appear with white background in the global pages.

Global traffic policies are displayed for a local CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles** and appear with yellow background in the local list.

To delete a traffic control policy, use the global or local form you used to create it.

Pre-configured default host-based policies apply globally to all Clean Access Servers and appear with yellow background in both global and local host-based policy lists. These default policies can be enabled or disabled, but cannot be deleted. See Enable Default Allowed Hosts, page 9-9 for details.

View Global Traffic Control Policies

Click the **IP** subtab link to configure IP-based traffic policies under **User Management > User Roles > Traffic Control > IP** (Figure 9-2).

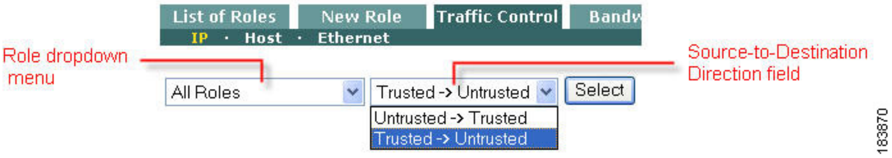
Click the **Host** subtab link to configure Host-based traffic policies under **User Management > User Roles > Traffic Control > Host**. (Figure 9-7).

Click the **Ethernet** subtab link to configure Layer 2 Ethernet traffic control policies under **User Management > User Roles > Traffic Control > Ethernet**. (Figure 9-9)

By default, IP-based traffic policies for roles are shown with the untrusted network as the source and the trusted network as the destination of the traffic. To configure policies for traffic traveling in the opposite direction, choose **Trusted->Untrusted** from the source-to-destination direction field and click **Select**.

You can view IP, Host-based, or Layer 2 Ethernet traffic policies for "All Roles" or a specific role by choosing from the role dropdown menu and clicking the **Select** button (Figure 9-1).

Figure 9-1 Trusted -> Untrusted Direction Field



Role dropdown menu

Source-to-Destination Direction field

Add Global IP-Based Traffic Policies

You can configure traffic policies for all the default roles already present in the system (Unauthenticated, Temporary, Quarantine). You will need to create normal login user roles first before you can configure traffic policies for them (see Chapter 7, "User Management: Configuring User Roles and Local Users.")

This section describes the following:

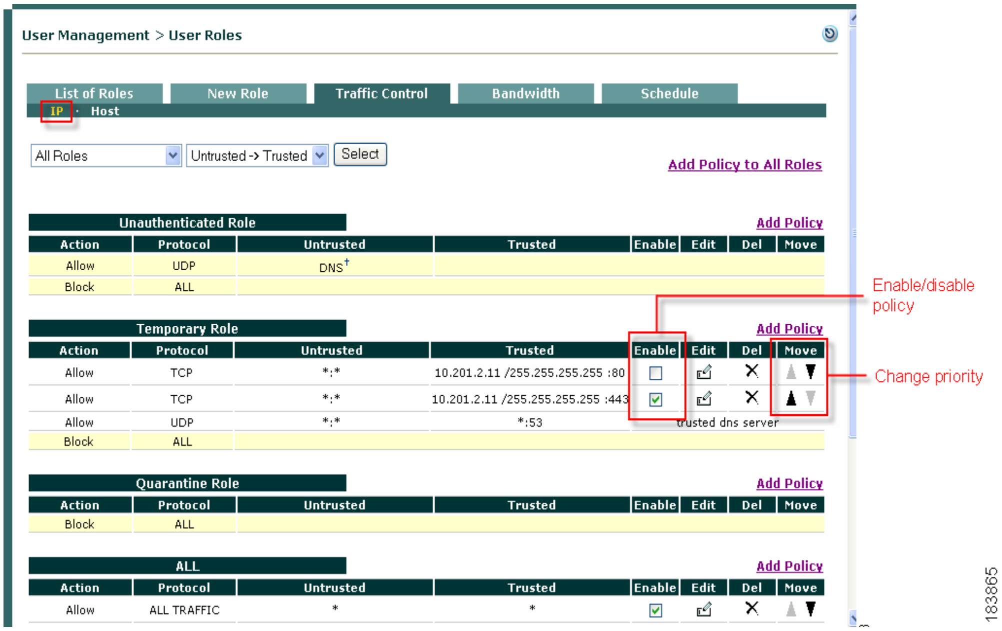
- Add IP-Based Policy, page 9-4
- Edit IP-Based Policy, page 9-7

Add IP-Based Policy

You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring IP-based traffic policies.

1. Go to **User Management > User Roles > Traffic Control > IP**. The list of IP-based policies for all roles displays (Figure 9-2).

Figure 9-2 List of IP-Based Policies



Unauthenticated Role — Add Policy

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	UDP	DNS†					
Block	ALL						

Temporary Role — Add Policy

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*:*	10.201.2.11 /255.255.255.255 :80	□		✕	▼
Allow	TCP	*:*	10.201.2.11 /255.255.255.255 :443	☑		✕	▲
Allow	UDP	*:*	*:53		trusted dns server		
Block	ALL						

Quarantine Role — Add Policy

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Block	ALL						

ALL — Add Policy

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	ALL TRAFFIC	*	*	☑		✕	▼

Enable/disable policy

Change priority

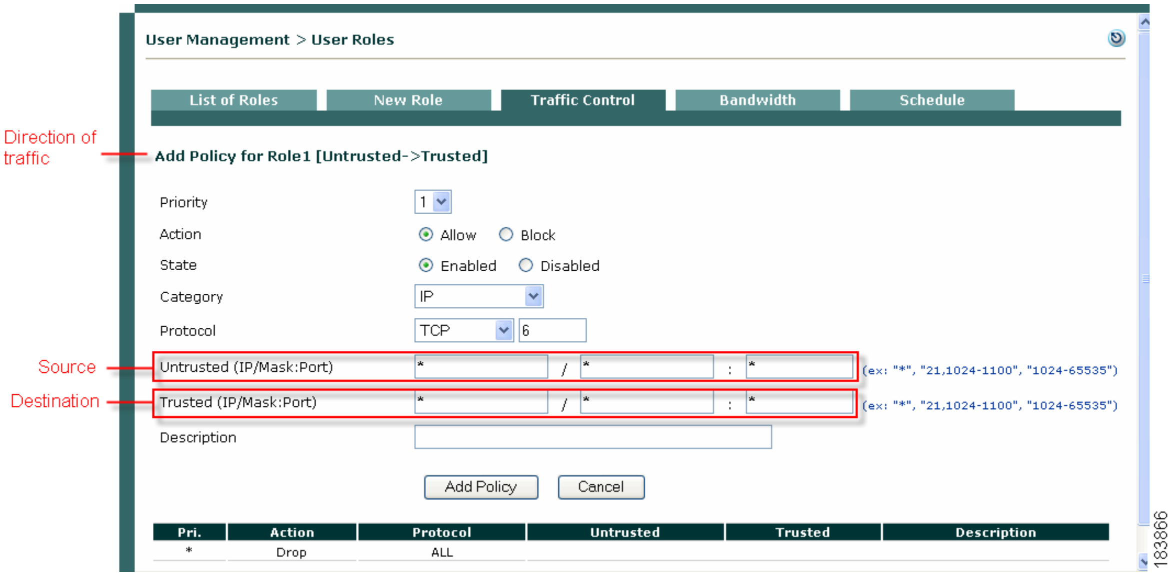
2. Select the source-to-destination direction for which you want the policy to apply. Chose either **Trusted->Untrusted** or **Untrusted->Trusted**, and click **Select**.

3. Click the **Add Policy** link next to the user role to create a new policy for the role, or click **Add Policy to All Roles** to add the new policy to all roles (except the Unauthenticated role) at once.

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. The **Add Policy** form for the role appears (Figure 9-3).

Figure 9-3 Add IP-Based Policy



Add Policy for Role1 [Untrusted->Trusted]

Priority: 1
Action: ● Allow ○ Block
State: ● Enabled ○ Disabled
Category: IP
Protocol: TCP 6
Untrusted (IP/Mask:Port): * / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port): * / * : * (ex: "*", "21,1024-1100", "1024-65535")
Description:

Pri.	Action	Protocol	Untrusted	Trusted	Description
*	Drop	ALL			

5. 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 (Figure 9-2).

6. Set the **Action** of the traffic policy as follows:
   - **Allow** (default)—Permit the traffic.
   - **Block**—Drop the traffic.
7. Set the **State** of the traffic policy as follows:
   - **Enabled** (default)—Enable this traffic policy immediately for any new traffic for the role.
   - **Disabled**—Disable this traffic policy for the role, while preserving the settings of the policy for future use.

Note To enable/disable traffic policies at the role level, click the corresponding checkbox in **Enable** column of the IP policies list page (Figure 9-2).

8. 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 Manager blocks IP fragment packets, since they can be used in denial-of-service (DoS) attacks. To permit fragmented packets, define a role policy allowing them with this option.
9. 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)**—Select for Transmission Control Protocol. TCP applications include HTTP, HTTPS, and Telnet.
    - **UDP (17)**—Select for User Datagram Protocol, generally used for broadcast messages.
    - **ICMP (1)**—Select for Internet Control Message Protocol. If selecting ICMP, also choose a **Type** from the dropdown menu.
    - **ESP (50)**—Select for Encapsulated Security Payload, an IPsec subprotocol used to encrypt IP packet data typically in order to create VPN tunnels.
    - **AH (51)**—Select for Authentication Header, an IPSec subprotocol used to compute a cryptographic checksum to guarantee the authenticity of the IP header and packet.
10. 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.

11. 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.

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:

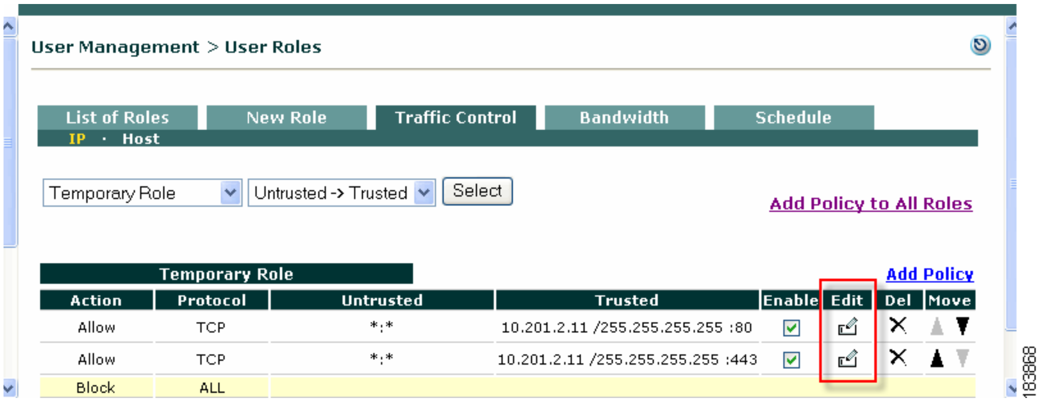
- The first IP/Mask/Port entry listed is the source.
- The second IP/Mask/Port entry listed is the destination.

12. Optionally, type a description of the policy in the **Description** field.
13. Click **Add Policy** when finished. If modifying a policy, click the **Update Policy** button.

Edit IP-Based Policy

1. Go to **User Management > User Roles > Traffic Control > IP**.
2. Click the **Edit** button for the role policies you want to edit (Figure 9-4).

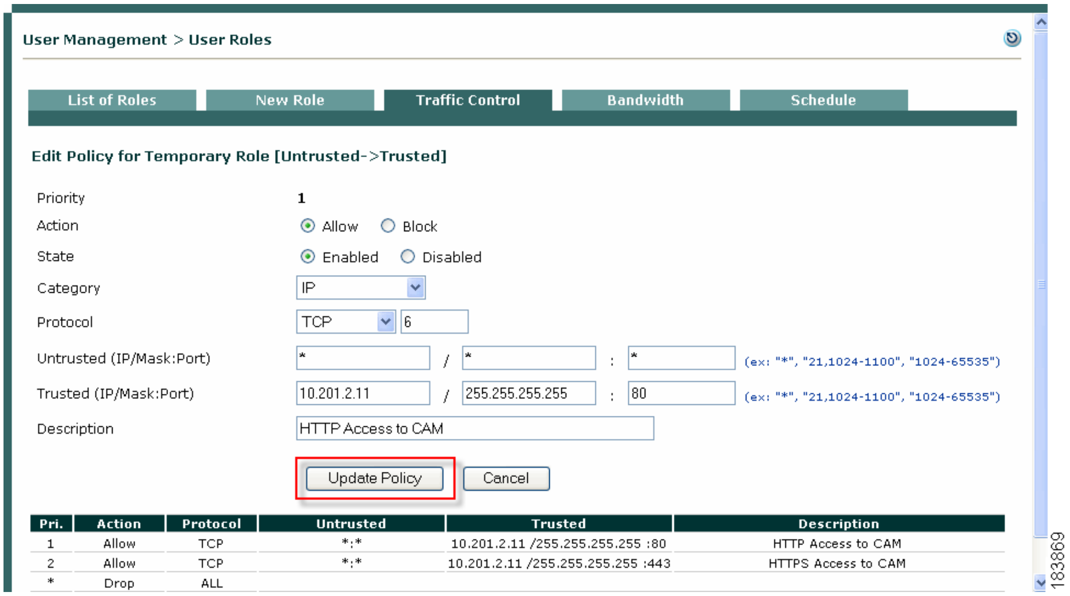
Figure 9-4 Edit IP Policy



Temporary Role							
Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*:*	10.201.2.11 /255.255.255.255 :80	☑			
Allow	TCP	*:*	10.201.2.11 /255.255.255.255 :443	☑			
Block	ALL						

3. The **Edit Policy** form for the role policy appears (Figure 9-5).

Figure 9-5 Edit IP Policy Form



Edit Policy for Temporary Role [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
State	● Enabled ○ Disabled
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port)	10.201.2.11 / 255.255.255.255 : 80 (ex: "*", "21,1024-1100", "1024-65535")
Description	HTTP Access to CAM

Pri.	Action	Protocol	Untrusted	Trusted	Description
1	Allow	TCP	*:*	10.201.2.11 /255.255.255.255 :80	HTTP Access to CAM
2	Allow	TCP	*:*	10.201.2.11 /255.255.255.255 :443	HTTPS Access to CAM
*	Drop	ALL			

4. Change properties as desired.

Note You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards such as: "*" or "**21, 1024-1100**" or "**1024-65535**" for TCP/UDP ports. See http://www.iana.org/assignments/port-numbers for details on TCP/UDP ports.

5. Click **Update Policy** when done.

Note that you cannot change the policy priority directly from the **Edit** form. To change a **Priority**, click the Up or Down arrows for the policy in the **Move** column of the IP policies list page.

Add Global Host-Based Traffic Policies

Default host 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 (see Retrieving Cisco NAC Appliance Updates, page 10-8 for complete details on Updates).

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. Once the host-based policy is setup and all the IP Addresses are resolved, it enables all traffic types to the host machine.

Allowing DNS addresses to be configured per user role facilitates client access to the Windows or antivirus update sites that enable clients to fix their systems if Agent requirements are not met or network scanning vulnerabilities are found. 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.

This section describes the following:

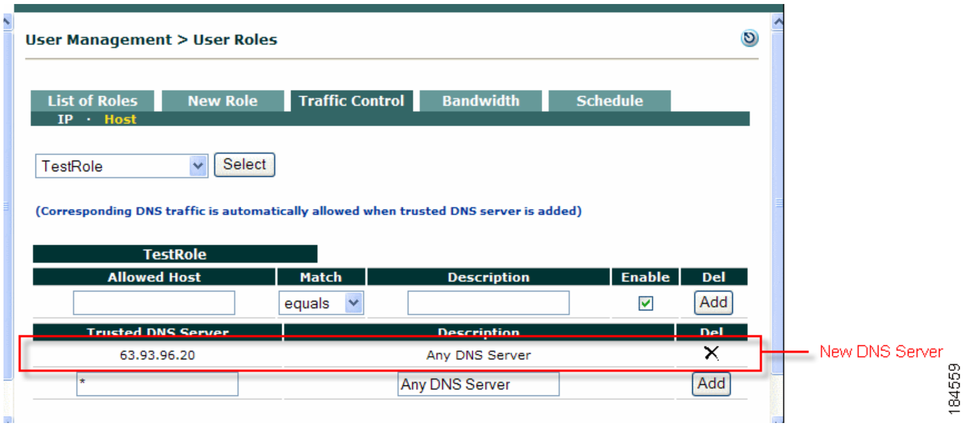
- Add Trusted DNS Server for a Role, page 9-8
- Enable Default Allowed Hosts, page 9-9
- Add Allowed Host, page 9-10
- Proxy Servers and Host Policies, page 9-12

Add Trusted DNS Server for a Role

To enable host-based traffic policies for a role, add a Trusted DNS Server for the role.

1. Go to **User Management > User Roles > Traffic Control** and click the **Host** link.
1. Select the role for which to add a trusted DNS server.
2. Type an IP address in the **Trusted DNS Server** field, or an asterisk "*" to specify any DNS server.

Figure 9-6 Add Trusted DNS Server



TestRole

(Corresponding DNS traffic is automatically allowed when trusted DNS server is added)

TestRole				
Allowed Host	Match	Description	Enable	Del
	equals		☑	Add

Trusted DNS Server	Description	Del
63.93.96.20	Any DNS Server	✕
*	Any DNS Server	Add

3. Optionally type a description for the DNS server in the **Description** field.
4. The **Enable** checkbox should already be selected.
5. Click **Add**. The new policy appears in the **Trusted DNS Server** column.

Note

- When a Trusted DNS Server is added on the **Host** form, an IP-based policy allowing DNS/UDP traffic to that server is automatically added for the role (on the **IP** form).
- When you add a specific DNS server, then later add Any ("*") DNS server to the role, 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 previously allowed is again displayed.

Enable Default Allowed Hosts

Cisco NAC Appliance provides default host policies for the Unauthenticated, Temporary, and Quarantine roles. Default Host Policies are initially pulled down to your system, then dynamically updated, through performing a Cisco NAC Appliance **Update** or **Clean Update**. Newly added Default Host Policies are disabled by default, and must be enabled for each role under **User Management > User Roles > Traffic Control > Hosts**.

To enable Default Host Policies for user roles:

Step 1 Go to **Device Management > Clean Access > Updates**. (See Figure 10-5 on page 10-11.)

Step 2 Click **Update** to get the latest Default Host Policies (along with Cisco NAC Appliance updates). Updating Default Host Policies does not overwrite any user-defined settings for existing Default Host Policies.

Step 3 Go to **User Management > User Roles > Traffic Control > Host**. (see Figure 9-7 on page 9-10.)

Step 4 Choose the role (Unauthenticated, Temporary, or Quarantine) for which to enable a Default Host Policy from the dropdown menu and click **Select**.

Step 5 Click the **Enable** checkbox for each default host policy you want to permit for the role.

Step 6 Make sure a Trusted DNS server is added (see Add Trusted DNS Server for a Role, page 9-8).

Step 7 To add additional custom hosts for the roles, follow the instructions for Add Allowed Host, page 9-10.

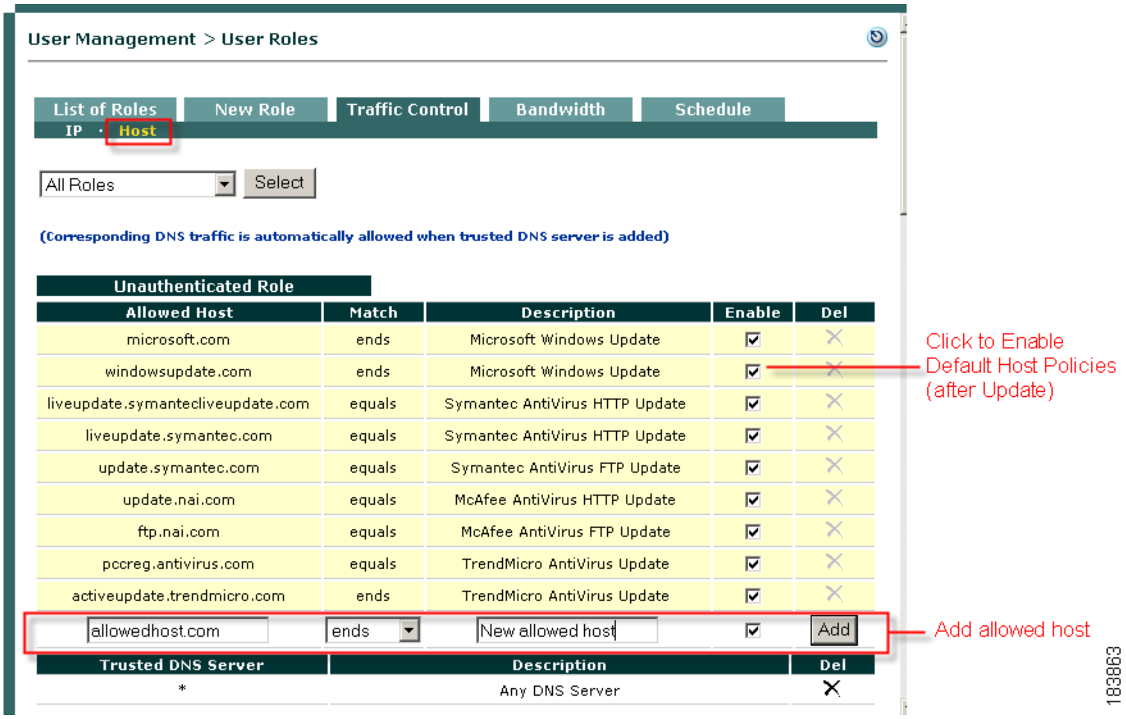
Note See Retrieving Cisco NAC Appliance Updates, page 10-8, for complete details on configuring Updates.

Add Allowed Host

The Allowed Host form allows you to supplement Default Host Policies with additional update sites for the default roles, or create custom host-based traffic policies for any user role.

1. Go to **User Management > User Roles > Traffic Control** and click the **Host** link.

Figure 9-7 Add Allowed Host



(Corresponding DNS traffic is automatically allowed when trusted DNS server is added)

Unauthenticated Role

Allowed Host	Match	Description	Enable	Del
microsoft.com	ends	Microsoft Windows Update	☑	✕
windowsupdate.com	ends	Microsoft Windows Update	☑	✕
liveupdate.symantecliveupdate.com	equals	Symantec AntiVirus HTTP Update	☑	✕
liveupdate.symantec.com	equals	Symantec AntiVirus HTTP Update	☑	✕
update.symantec.com	equals	Symantec AntiVirus FTP Update	☑	✕
update.nai.com	equals	McAfee AntiVirus HTTP Update	☑	✕
ftp.nai.com	equals	McAfee AntiVirus FTP Update	☑	✕
pccreg.antivirus.com	equals	TrendMicro AntiVirus Update	☑	✕
activeupdate.trendmicro.com	ends	TrendMicro AntiVirus Update	☑	✕
allowedhost.com	ends	New allowed host	☑	Add

Trusted DNS Server	Description	Del
*	Any DNS Server	✕

Click to Enable Default Host Policies (after Update)

Add allowed host

2. Select the role for which to add a DNS host.
3. Type the hostname in the **Allowed Host** field (e.g. "allowedhost.com").
4. In the **Match** dropdown menu, select an operator to match the host name: **equals**, **ends**, **begins**, or **contains**.
5. Type a description for the host in the **Description** field (e.g. "Allowed Update Host").
6. The **Enable** checkbox should already be selected.
7. Click **Add**. The new policy appears above the **Add** field.

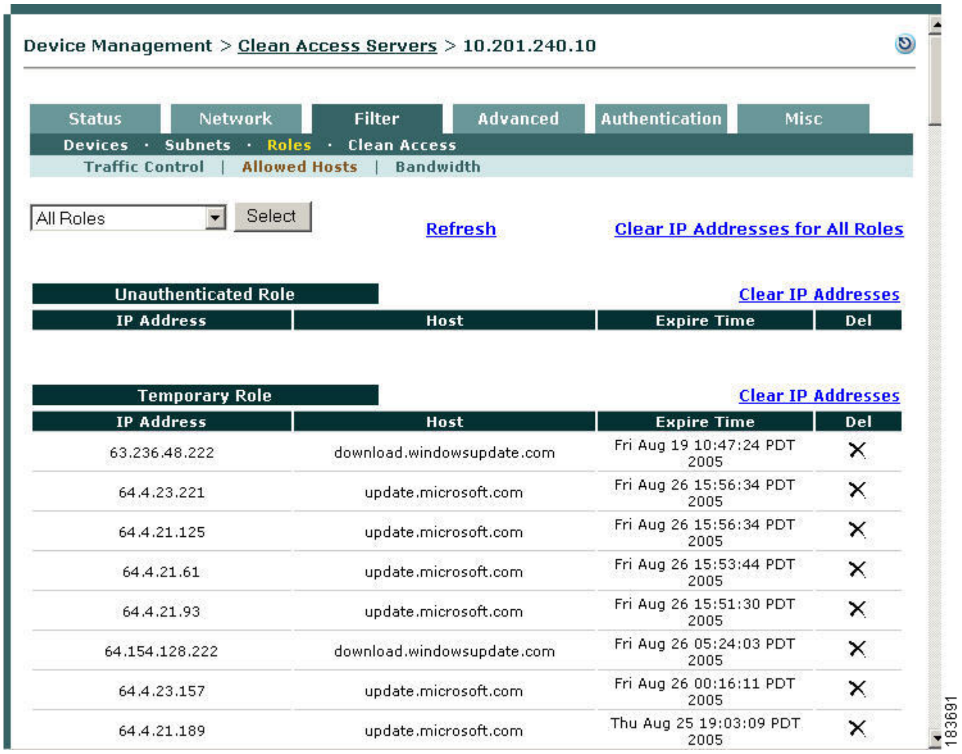
Note You must add a Trusted DNS Server to the role to enable host-based traffic policies for the role.

View IP Addresses Used by DNS Hosts

You can view the IP addresses used for the DNS host when clients connect to the host to update their systems. Note that these IP addresses are viewed per Clean Access Server from the CAS management pages.

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.
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. Note that 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.

Figure 9-8 View Current IP Addresses for All Roles


Device Management > Clean Access Servers > 10.201.240.10
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Traffic Control | Allowed Hosts | Bandwidth
All Roles
Select
Refresh
Clear IP Addresses for All Roles
Clear IP Addresses
Clear IP Addresses
183691

Unauthenticated Role

IP Address	Host	Expire Time	Del

Temporary Role

IP Address	Host	Expire Time	Del
63.236.48.222	download.windowsupdate.com	Fri Aug 19 10:47:24 PDT 2005	✕
64.4.23.221	update.microsoft.com	Fri Aug 26 15:56:34 PDT 2005	✕
64.4.21.125	update.microsoft.com	Fri Aug 26 15:56:34 PDT 2005	✕
64.4.21.61	update.microsoft.com	Fri Aug 26 15:53:44 PDT 2005	✕
64.4.21.93	update.microsoft.com	Fri Aug 26 15:51:30 PDT 2005	✕
64.154.128.222	download.windowsupdate.com	Fri Aug 26 05:24:03 PDT 2005	✕
64.4.23.157	update.microsoft.com	Fri Aug 26 00:16:11 PDT 2005	✕
64.4.21.189	update.microsoft.com	Thu Aug 25 19:03:09 PDT 2005	✕

Tip To troubleshoot host-based policy access, try performing an **`ipconfig /flushdns`** from a command prompt of the test client machine. Cisco NAC Appliance needs to see DNS responses before putting corresponding IP addresses on the allow list.

Proxy Servers and Host Policies

You can allow users to access only the host sites enabled for a role (e.g. Temporary or Quarantine users that need to meet requirements) when a proxy server specified on the CAS is used.

Note that proxy settings are local policies configured on the CAS using the CAS management pages, and the following pages must be configured to enable this feature:

- **Device Management > Clean Access Servers > Manage [CAS_IP] > Advanced > Proxy**
- **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** (the **Parse Proxy Traffic** option must be enabled)

For complete details, see the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.6(1)*.

See also Proxy Settings, page 6-2 for related information.

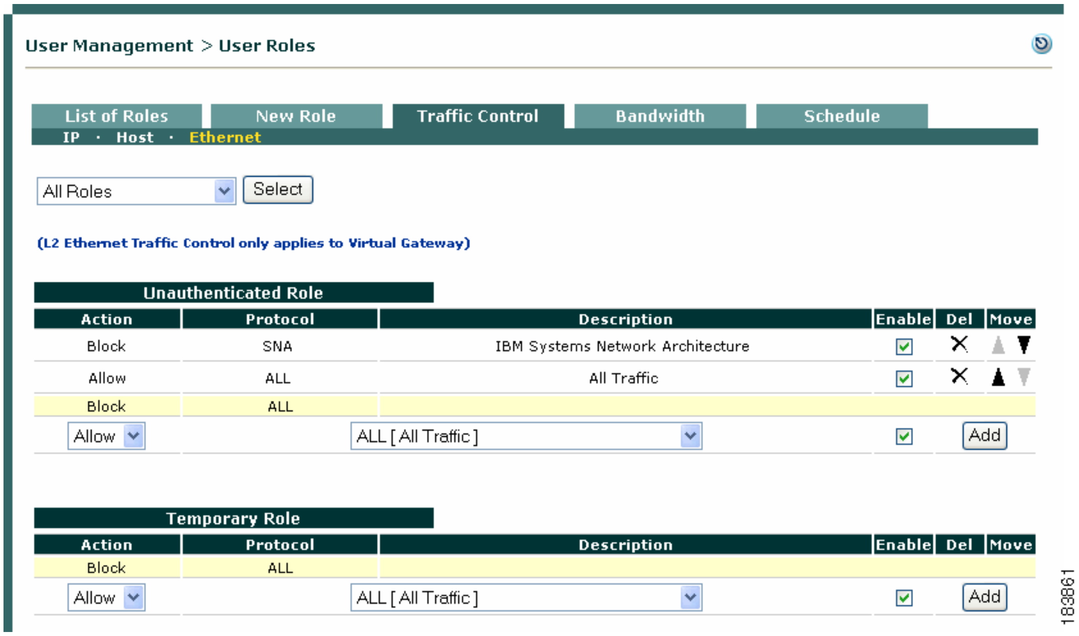
Add Global Layer 2 Ethernet Traffic Policies

Note Layer 2 Ethernet traffic control only applies to Clean Access Servers operating in Virtual Gateway mode where Layer 2 Ethernet Control has been enabled on the CAS configuration page.

You can configure traffic policies for all the default roles already present in the system (Unauthenticated, Temporary, Quarantine). You will need to create normal login user roles first before you can configure traffic policies for them (see Chapter 7, "User Management: Configuring User Roles and Local Users.")

1. Go to **User Management > User Roles > Traffic Control > Ethernet**. The list of Layer 2 Ethernet traffic control policies for all roles appears (Figure 9-2).

Figure 9-9 Layer 2 Ethernet Traffic Control Policies



User Management > User Roles

(L2 Ethernet Traffic Control only applies to Virtual Gateway)

Unauthenticated Role

Action	Protocol	Description	Enable	Del	Move
Block	SNA	IBM Systems Network Architecture	☑	✕	▲ ▼
Allow	ALL	All Traffic	☑	✕	▲ ▼
Block	ALL				
Allow	ALL [All Traffic]		☑	Add	

Temporary Role

Action	Protocol	Description	Enable	Del	Move
Block	ALL				
Allow	ALL [All Traffic]		☑	Add	

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 in Cisco NAC Appliance. Additional preset options may become available with future releases 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.

Control 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).

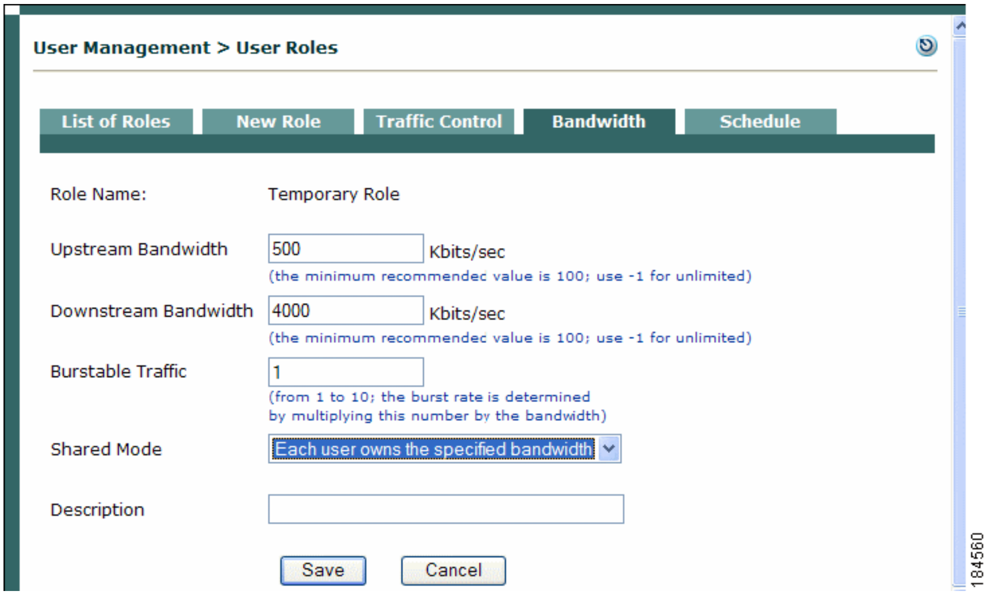
To configure bandwidth settings for a role:

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**.

Note See the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.6(1)* for details on local bandwidth management.

3. From **User Management > User Roles > Bandwidth**, click the **Edit** button next to the role for which you want to set bandwidth limitations. The **Bandwidth** form appears as follows:

Figure 9-10 Bandwidth Form for User Role



User Management > User Roles

Role Name: Temporary Role

Upstream Bandwidth 500 Kbits/sec
(the minimum recommendec value is 100; use -1 for unlimited)

Downstream Bandwidth 4000 Kbits/sec
(the minimum recommendec value is 100; use -1 for unlimited)

Burstable Traffic 1
(from 1 to 10; the burst rate is determined
by multiplying this number by the bandwidth)

Shared Mode Each user owns the specified bandwidth

Description

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 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.
6. 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 the same.
7. Optionally, type a **Description** of the bandwidth setting.
8. Click **Save** when finished.

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

Note If bandwidth management is enabled, devices allowed via device filter without specifying a role will use the bandwidth of the Unauthenticated Role. See Global Device and Subnet Filtering, page 3-10 for details.

Configure User Session and Heartbeat Timeouts

Timeout properties enhance the security of your network by ensuring that user sessions are terminated after a configurable period of time. The are three main mechanisms for automated user timeout:

- Session Timer
- Heartbeat Timer
- Certified Device Timer (see Configure Certified Device Timer, page 12-14)

This section describes the Session and Heartbeat Timers.

Session Timer

The Session Timer is an absolute timer that is specific to the user role. If a Session Timer is set for a role, a session for a user belonging to that role can only last as long as the Session Timer setting. The Session Timer has a built-in value of 5 minutes that gets added to the configured session timeout value specific to the user role. A user session corresponding to a user role gets cleared at the end of configured session timout + built-in 5 minute value. For example, if user A logs in at 1:00pm and user B logs in at 1:30pm, and if both belong to role Test with Session Timer set for 115 minutes, user A will be logged out at 3:00pm and user B will be logged out at 3:30pm. When session timeouts, the user is dropped regardless of connection status or activity.

Heartbeat Timer

The Heartbeat Timer sets the number of minutes after which a user is logged off the network if unresponsive to ARP queries from the Clean Access Server. This feature enables the CAS to detect and disconnect users who have left the network (e.g. by shutting down or suspending the machine) without actually logging off the network. Note that the Heartbeat Timer applies to all users, whether locally or externally authenticated.

The connection check is performed via ARP query rather than by pinging. This allows the heartbeat check to function even if ICMP traffic is blocked. The CAS maintains an ARP table for its untrusted side which houses all the machines it has seen or queried for on the untrusted side. ARP entries for machines are timed out through normal ARP cache timeout if no packets are seen from the particular machine. If packets are seen, their entry is marked as fresh. When a machine no longer has a fully resolved entry in the CAS's ARP cache and when it does not respond to ARPing for the length of the Heartbeat Timer setting, the machine is deemed not to be on the network and its session is terminated.

In-Band (L2) Sessions

For in-band configurations, a user session is based on the client MAC and IP address and persists until one of the following occurs:

- The user logs out of the network through either the web user logout page or the Agent logout option.
- An administrator manually removes the user from the network.
- The session times out, as configured in the Session Timer for the user role.
- The CAS determines that the user is no longer connected using the Heartbeat Timer and the CAM terminates the session.
- The Certified Device list is cleared (automatically or manually) and the user is removed from the network.

OOB (L2) and Multihop (L3) Sessions

The Session Timer works the same way for multi-hop L3 In-Band deployments as for L2 (In-Band or Out-of-Band) deployments.

For L3 deployments, user sessions are based on unique IP address rather than MAC address.

The Heartbeat Timer behaves as inactivity/idle timer for L3 deployments in addition to L2 deployments. For L3 deployments, the Heartbeat Timer now behaves as described in the following cases:

- **L3 deployments where routers do not perform proxy ARP:**

  If the Clean Access Servers sees no packets from the user for the duration of time that the heartbeat timer is set to, then the user will be logged out. Even if the user's machine is connected to the network but does not send a single packet on the network that reaches the CAS, it will be logged out. Note that this is highly unlikely because modern systems send out many packets even when the user is not active (e.g. chat programs, Windows update, AV software, ads on web pages, etc.)

- **L3 deployments where the router/VPN concentrator performs proxy ARP for IP addresses on the network:**

  In this scenario, if a device is connected to the network the router will perform proxy ARP for the device’s IP address. Otherwise, if a device is not connected to the network, the router does not perform proxy ARP. Typically only VPN concentrators behave in this way. In this case, if the Clean Access Server sees no packets, the CAM/CAS attempts to perform ARP for the user. If the router responds to the CAS because of proxy ARP, the CAM/CAS will not logout the user. Otherwise, if the router does not respond to the CAS, because the device is no longer on the network, the CAM/CAS will log out the user.

- **L3 deployments where the router/VPN concentrator performs proxy ARP for the entire subnet:**

  In this scenario, the router/VPN concentrator performs proxy ARP irrespective of whether individual devices are connected. In this case, the Heartbeat Timer behavior is unchanged, and the CAM/CAS never log out the user.

Note

- The Heartbeat Timer does not apply to Out-of-Band users.
- When the Single Sign-On (SSO) feature is configured for multi-hop L3 VPN concentrator integration, if the user’s session on the CAS times out but the user is still logged in on the VPN concentrator, the user will be able to log back into the CAS without providing a username/password, due to SSO.

Session Timer / Heartbeat Timer Interaction

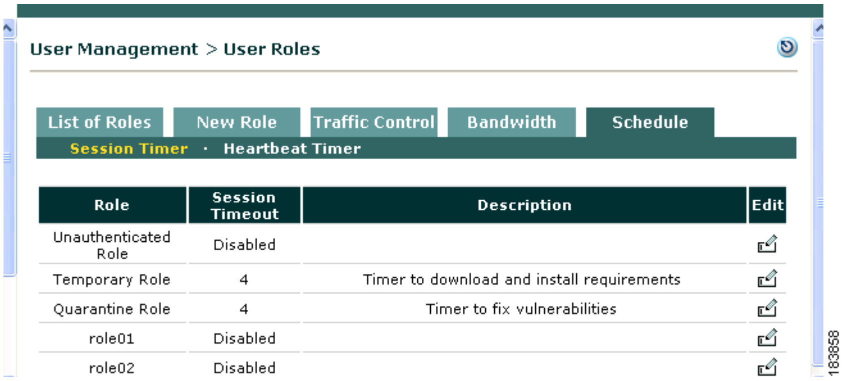
- If the Session Timer is zero and the Heartbeat Timer is not set—the user is not dropped from the Online Users list and will not be required to re-logon.
- If the Session Timer is zero and the Heartbeat Timer is set— the Heartbeat Timer takes effect.
- If the Session Timer is non-zero and the Heartbeat Timer is not set— the Session Timer takes effect.
- If both timers are set, the first timer to be reached will be activated first.
- If the user logs out and shuts down the machine, the user will be dropped from the Online Users list and will be required to re-logon.
- If the DHCP lease is much longer than the session timeout, DHCP leases will not be reused efficiently.

For additional details, see Interpreting Active Users, page 12-18.

Configure Session Timer (per User Role)

1. Go to **User Management > User Roles > Schedule > Session Timer**.

Figure 9-11 Session Timer



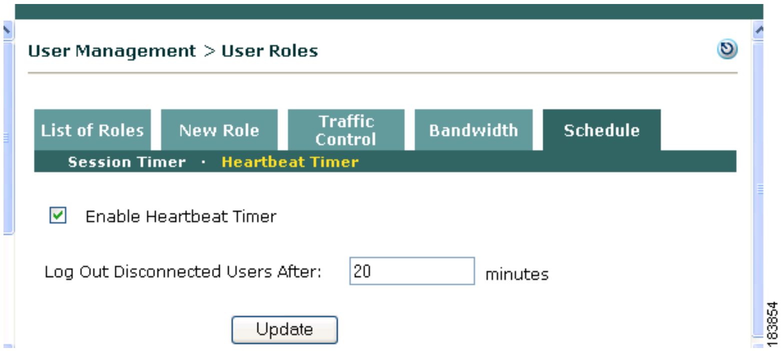
Role	Session Timeout	Description	Edit
Unauthenticated Role	Disabled		✎
Temporary Role	4	Timer to download and install requirements	✎
Quarantine Role	4	Timer to fix vulnerabilities	✎
role01	Disabled		✎
role02	Disabled		✎

2. Click the **Edit** button next to the role for which you want to configure timeout settings.
3. Select the **Session Timeout** check box and type the number of minutes after which the user's session times out. The timeout clock starts when the user logs on, and is not affected by user activity. After the session expires, the user must log in again to continue using the network.
4. Optionally, type a description of the session length limitation in the **Description** field.
5. Click **Update** when finished.

Configure Heartbeat Timer (User Inactivity Timeout)

1. Open the **Heartbeat Timer** form in the **Schedule** tab.

Figure 9-12 Heartbeat Timer



☑ Enable Heartbeat Timer

Log Out Disconnected Users After: 20 minutes

2. Click the **Enable Heartbeat Timer** checkbox.
3. Set the number of minutes after which a user is logged off the network if unreachable by connection attempt in the **Log Out Disconnected Users After** field.
4. Click **Update** to save your settings.

Note that logging a user off the network does not remove them from the Certified Devices List. However, removing a user from the Certified Devices List also logs the user off the network. An administrator can drop users from the network individually or terminate sessions for all users at once. For additional details see Clear Certified or Exempt Devices Manually, page 12-13 and Interpreting Event Logs, page 14-4.

Note The Agent does not send a logout request to the CAS when the client machine is shut down based on Cisco NAC Appliance session-based connection setup.

Configure Policies for Agent Temporary and Quarantine Roles

This section demonstrates typical traffic policy and session timeout configuration needed to:

- Configure Agent Temporary Role, page 9-18
- Configure Network Scanning Quarantine Role, page 9-21

Configure Agent Temporary Role

Users who fail a system check are assigned to the Agent Temporary role. This role is intended to restrict user access to only the resources needed to comply with the Agent requirements.

Unlike Quarantine roles, there is only one Agent Temporary role in the Cisco NAC Appliance system. The role can be fully edited, and is intended as single point for aggregating the traffic control policies that allow users to access required installation files. If the Temporary role is deleted, the Unauthenticated role is used by default. The name of the role that is used for the Temporary role (in addition to the version of the Agent) is displayed under **Device Management > Clean Access > Clean Access Agent > Distribution**.

Both session timeout and traffic policies need to be configured for the Temporary role. The Temporary role has a default session timeout of 4 minutes, which can be changed as described below. The Temporary and quarantine roles have default traffic control policies of Block All traffic from the untrusted to the trusted side. Keep in mind that while you associate requirements (required packages) to the normal login roles that users attempt to log into, clients will need to meet those requirements while still in the Temporary role. Therefore, traffic control policies need to be added to the Temporary role to enable clients to access any required software installation files from the download site(s).

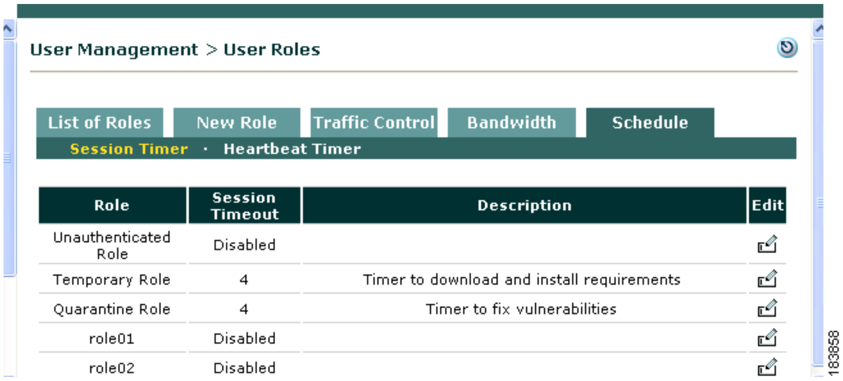
Note If the user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example), and the **Logoff NAC Agent users from network on their machine logoff or shutdown after** <*x*> **secs** option in the CAM **Device Management > Clean Access > General Setup > Agent Login** web console page has not been enabled, the client machine remains in the Temporary role until the Session Timer expires and the user is given the opportunity to perform login/remediation again.

Configuring Agent-Based Posture Assessment, page 10-33 provides complete details on Agent Requirement configuration. See also User Role Types, page 7-3 for additional information.

Configure Session Timeout for the Temporary Role

1. Go to **User Management > User Roles> Schedule**.
2. The **Session Timer** list appears.

Figure 9-13 Schedule Tab

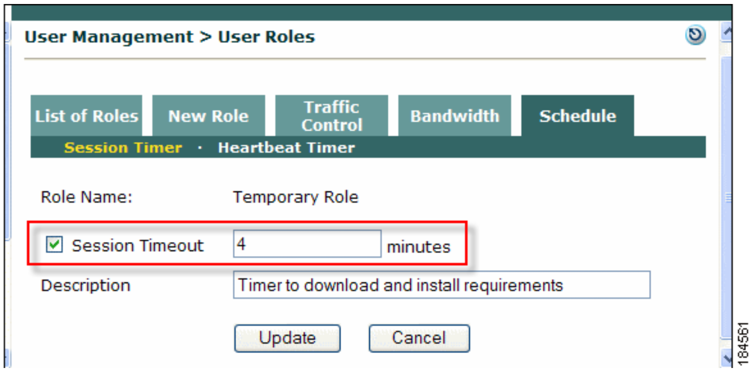


User Management > User Roles

Role	Session Timeout	Description	Edit
Unauthenticated Role	Disabled		✎
Temporary Role	4	Timer to download and install requirements	✎
Quarantine Role	4	Timer to fix vulnerabilities	✎
role01	Disabled		✎
role02	Disabled		✎

3. Click the **Edit** button for the Temporary Role.
4. The **Session Timer** form for the Temporary Role appears (Figure 9-14).

Figure 9-14 Session Timer—Temporary Role



Role Name: Temporary Role

☑ Session Timeout 4 minutes

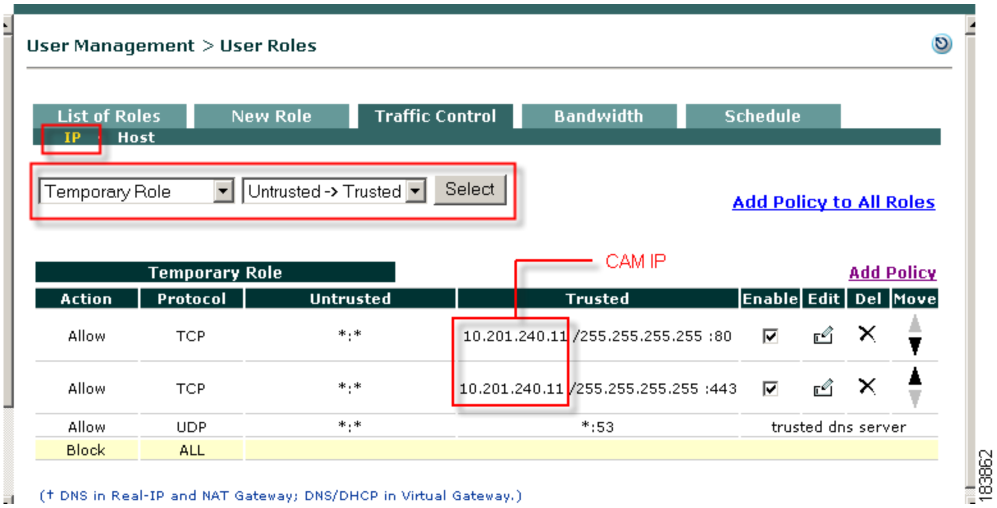
Description Timer to download and install requirements

5. Click the **Session Timeout** checkbox.
6. Type the number of minutes for the user session to live (default is 4 minutes). Choose a value that allows users to download required files to patch or configure their systems.
7. Optionally, type a **Description** for the session timeout requirement.
8. Click **Update**. The Temporary role will display the new time in the **Session Timer** list.

Configure Traffic Control Policies for the Temporary Role

9. From **User Management > User Roles**, click the **Traffic Control** tab. This displays **IP** traffic policy list by default.
10. Choose **Temporary Role** from the role dropdown and leave **Untrusted->Trusted** for the direction and click **Select**. This displays all IP policies for the Temporary role.

Figure 9-15 IP Traffic Policies—Temporary Role



Temporary Role ▾ Untrusted -> Trusted ▾

Temporary Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*:*	10.201.240.11/255.255.255.255 :80	☑		✕	▼
Allow	TCP	*:*	10.201.240.11/255.255.255.255 :443	☑		✕	▲
Allow	UDP	*:*	*:53	trusted dns server			
Block	ALL						

(† DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway.)

11. To configure an **IP** policy, click the **Add Policy** link next to the Temporary role. For example, if you are providing required software installation files yourself (e.g. via a File Distribution requirement for a file on the CAM), set up an Untrusted->Trusted IP-based traffic policy that allows the Temporary role access to port 80 (HTTP) of the CAM (for example, 10.201.240.11

/255.255.255.255:80). If you want users to be able to correct their systems using any other external web pages or servers, set up permissions for accessing those web resources. For further details on the **Add Policy** page, see Add IP-Based Policy, page 9-4.

12. To configure **Host** policies, click the **Host** link at the top of the **Traffic Control** tab. Configure host-based traffic policies enabling access to the servers that host the installation files, as described in the following sections:
    - Enable Default Allowed Hosts, page 9-9
    - Add Allowed Host, page 9-10
    - Adding Traffic Policies for Default Roles, page 9-26

Configure Network Scanning Quarantine Role

See Chapter 13, "Configuring Network Scanning" for complete details on network scanning configuration.

Cisco NAC Appliance can assign a user to a quarantine role if it discovers a serious vulnerability in the client system. The role is a mechanism intended to give users temporary network access to fix their machines. Note that quarantining vulnerable users is optional. Alternatives include blocking the user or providing them with a warning. If you do not intend to quarantine vulnerable users, you can skip this step.

Create Additional Quarantine Role

By default, the system provides a default Quarantine role with a session time out of 4 minutes that only needs to be configured with traffic policies. The following describes how to create an additional quarantine role, if multiple quarantine roles are desired.

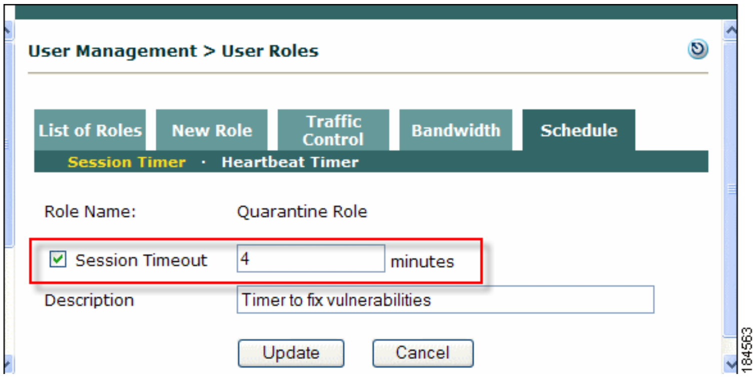
1. Go to **User Management > User Roles > New Role**.
2. Type a **Role Name** and **Role Description** of the role. For a quarantine role that will be associated with a particular login role, it may be helpful to reference the login role and the quarantine type in the new name. For example, a quarantine role associated with a login role named "`R1`" might be "R1-Quarantine."
3. In the **Role Type** list, choose **Quarantine Role**.
4. Configure any other settings for the role as desired. Note that, other than name, description, and role type, other role settings can remain at their default values. (See Add New Role, page 7-7 for details.)
5. Click the **Create Role** button. The role appears in the **List of Roles** tab.

Configure Session Timeout for Quarantine Role

By default, the system provides a default Quarantine role with a session time out of 4 minutes. The following steps describe how to configure the session timeout for a role.

1. Go to **User Management > User Roles > Schedule > Session Timer**.
2. Click the **Edit** button next to the desired quarantine role.
3. The **Session Timer** form for the quarantine role appears:

Figure 9-16 Session Timer—Quarantine Role



Role Name: Quarantine Role

☑ Session Timeout 4 minutes

Description Timer to fix vulnerabilities

4. Click the **Session Timeout** check box.
5. Type the number of minutes for the user session to live. Choose an amount that allows users enough time to download the files needed to fix their systems.
6. Optionally, type a **Description** for the session timeout requirement.
7. Click **Update**. The new value will appear in the **Session Timeout** column next to the role in the **List of Roles** tab.

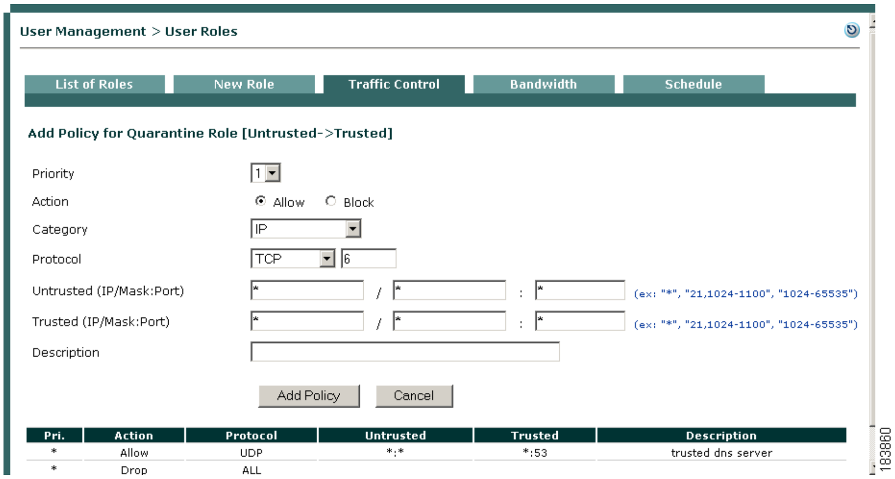
Setting these parameters to a relatively small value helps the CAS detect and disconnect users who have restarted their computers without logging out of the network. Note that the Session Timer value you enter here may need to be refined later, based on test scans and downloads of the software you will require.

Note The connection check is performed by ARP message; if a traffic control policy blocks ICMP traffic to the client, heartbeat checking still works.

Configure Traffic Control Policies for the Quarantine Role

1. From **User Management > User Roles > List of Roles**, click the **Policies** button next to the role (or you can click the **Traffic Control** tab, choose the quarantine role from the dropdown menu and click **Select**).
2. Choose the **Quarantine Role** from the role dropdown, leave **Untrusted->Trusted** for the direction and click **Select**. This displays all IP policies for the Quarantine role.
3. To configure an **IP** policy, click the **Add Policy** link next to the Quarantine role.

Figure 9-17 Add Policy—Quarantine Role



Add Policy for Quarantine Role [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Description	

Pri.	Action	Protocol	Untrusted	Trusted	Description
*	Allow	UDP	*:*	*:53	trusted dns server
*	Drop	ALL			

4. Configure fields as described in Add IP-Based Policy, page 9-4.
   - If you are providing required software installation files from the CAM (e.g. via network scanning Vulnerabilities page), set up an Untrusted->Trusted IP-based traffic policy that allows the Quarantine role access to port 80 (HTTP) of the CAM (for example, 10.201.240.11 /255.255.255.255:80).
   - If you want users to be able to correct their systems using any other external web pages or servers, set up permissions for accessing those web resources. See also Adding Traffic Policies for Default Roles, page 9-26.
5. To configure **Host** policies, click the **Host** link for the Quarantine role at the top of the **Traffic Control** tab. Configure host-based traffic policies enabling access to the servers that host the installation files, as described in the following sections:
   - Enable Default Allowed Hosts, page 9-9
   - Add Allowed Host, page 9-10
   - Adding Traffic Policies for Default Roles, page 9-26

After configuring the quarantine role, you can apply it to users by selecting it as their quarantine role in the **Block/Quarantine users with vulnerabilities in role** option of the **General Setup** tab. For details, see Client Login Overview, page 1-6.

When finished configuring the quarantine role, load the scan plugins as described in Load Nessus Plugins into the Clean Access Manager Repository, page 13-6.

Example Traffic Policies

This section describes the following:

- Allowing Authentication Server Traffic for Windows Domain Authentication, page 9-24
- Allowing Traffic for Enterprise AV Updates with Local Servers, page 9-24
- Allowing Gaming Ports, page 9-24
- Adding Traffic Policies for Default Roles, page 9-26

Allowing Authentication Server Traffic for Windows Domain Authentication

If you want users on the network to be able to authenticate to a Windows domain prior to authenticating to the Cisco NAC Appliance, the following minimum policies allow users in the Unauthenticated role access to AD (NTLM) login servers:

Allow	TCP	*:*	Server/255.255.255.255: 88
Allow	UDP	*:*	Server/255.255.255.255: 88
Allow	TCP	*:*	Server/255.255.255.255: 389
Allow	UDP	*:*	Server/255.255.255.255: 389
Allow	TCP	*:*	Server/255.255.255.255: 445
Allow	UDP	*:*	Server/255.255.255.255: 445
Allow	TCP	*:*	Server/255.255.255.255: 135
Allow	UDP	*:*	Server/255.255.255.255: 135
Allow	TCP	*:*	Server/255.255.255.255: 3268
Allow	UDP	*:*	Server/255.255.255.255: 3268
Allow	TCP	*:*	Server/255.255.255.255: 139
Allow	TCP	*:*	Server/255.255.255.255: 1025

Allowing Traffic for Enterprise AV Updates with Local Servers

In order to allow definition updates for enterprise antivirus products, such as Trend Micro OfficeScan, the Temporary role needs to be configured to allow access to the local server for automatic AV definition updates.

For Trend Micro OfficeScan, the Temporary role policy needs to allow access to the local server with AutoPccP.exe. The Agent calls the Trend client locally, and the Trend client in turn runs the AutoPccP.exe file either on a share drive (located at \\<trendserverip\ofcscan\Autopccp.exe) or through HTTP (depending on your TrendMicro configuration) and downloads the AV patches.

Allowing Gaming Ports

To allow gaming services, such as Microsoft Xbox Live, Cisco recommends creating a gaming user role and to add a filter for the device MAC addresses (under **Device Management > Filters > Devices > New**) to place the devices into that gaming role. You can then create traffic policies for the role to allow traffic for gaming ports.

Microsoft Xbox

The following are suggested policies to allow access for Microsoft Xbox ports:

- Kerberos-Sec (UDP); Port 88; UDP; Send Receive
- DNS Query (UDP); Port 53; Send 3074 over UDP/tcp
- Game Server Port (TCP): 22042
- Voice Chat Port (TCP/UDP): 22043-22050

- Peer Ping Port (UDP): 13139
- Peer Query Port (UDP): 6500

Other Game Ports

Table 9-1 shows suggested policies to allow access for other game ports (such as PlayStation).

Table 9-1 Traffic Policies for Other Gaming Ports [1]

Protocol Port	Protocol
2300-2400	UDP
4000	TCP, UDP
4000	TCP, UDP
80	TCP
2300	UDP
6073	UDP
2302-2400	UDP
33334	UDP
33335	TCP
6667	TCP
3783	TCP
27900	TCP
28900	TCP
29900	TCP
29901	TCP
27015	TCP
2213 + 1 for each client (i.e. first computer is 2213, second computer is 2214, third computer is 2215, etc.)	TCP
6073	TCP
2302-2400	UDP
27999	TCP
28000	TCP
28805-28808	TCP
9999	TCP
47624	TCP
2300-2400	TCP
2300-2400	UDP
6073	UDP
2302-2400	UDP
47624	TCP

Table 9-1 Traffic Policies for Other Gaming Ports [1]

Protocol Port	Protocol
2300-2400	TCP
2300-2400	UDP
5120-5300	UDP
6500	UDP
27900	UDP
28900	UDP
3782	TCP
3782	UDP
27910	TCP, UDP
6073	UDP
2302-2400	UDP
47624	TCP
2300-2400	TCP
2300-2400	UDP
4000	TCP
7777	TCP, UDP
4000	TCP
27015-27020	TCP
6667	TCP
28800-29000	TCP

[1] See also http://www.us.playstation.com/support.aspx?id=installation/networkadaptor/415013907.html for additional details.

For additional details, see:

- Device Filters and Gaming Ports, page 3-16
- http://www.cisco.com/warp/customer/707/ca-mgr-faq2.html#q16
- Add New Role, page 7-7

Adding Traffic Policies for Default Roles

Create Untrusted -> Trusted traffic policies for the default roles (Unauthenticated, Temporary, and Quarantine) to allow users access to any of the resources described below.

Unauthenticated Role

If customizing the web login page to reference logos or files on the CAM or external URL, create IP policies to allow the Unauthenticated role HTTP (port 80) access to the CAM or external server. (See also Upload a Resource File, page 6-13 and Create Content for the Right Frame, page 6-11 for details.)

Agent Temporary Role

- If providing definition updates for enterprise antivirus products, allow access to the local update server so that the Agent can trigger a live update (see Allowing Traffic for Enterprise AV Updates with Local Servers, page 9-24).

> **Note** This behavior is only applicable to the Cisco NAC Agent/Clean Access Agent because the Cisco NAC Web Agent does not support automatic remediation.

- If providing required software packages from the CAM (e.g, via File Distribution), create IP policies to allow Temporary role access to port 80 (HTTP) of the CAM. Make sure to specify IP address/subnet mask to allow access only to the CAM (for example, 10.201.240.11/255.255.255.255:80).
- Enable Default Host Policies and Trusted DNS Server and/or create new allowed Host policies to allow users access to update sites (see Enable Default Allowed Hosts, page 9-9).
- Set up any additional traffic policies to allow users in the Temporary role access to external web pages or servers (for example, see Configure Network Policy Page (Acceptable Use Policy) for Agent Users, page 10-7).

Quarantine Role

- If providing required software packages from the CAM (e.g. via network scanning Vulnerabilities page), create IP policies to allow the Quarantine role access to port 80 (HTTP) of the CAM. Make sure to specify the IP address and subnet mask to allow access only to the CAM (for example, 10.201.240.11 /255.255.255.255:80).
- Enable Default Host Policies and Trusted DNS Server and/or create new allowed Host policies to allow users access to update sites (see Enable Default Allowed Hosts, page 9-9).
- Set up any additional traffic policies to allow users in the Quarantine role access to external web pages or servers for remediation.

Table 9-2 summarize resources, roles and example traffic policies for system roles

Table 9-2 Typical Traffic Policies for Roles

Resource	Role	Example Policies (Untrusted -> Trusted)
IP-Based Traffic Policies		
Logo/right-frame content for Login page (logo.jpg, file.htm)	Unauthenticated	**IP (Files on CAM or External Server):** Allow TCP *.* <*CAM_IP_address* or *external_server_IP_address*> / 255.255.255.255: http (80)
User Agreement Page (UAP.htm)		
Redirect URL after blocked access (block.htm) — optional		
Network Policy Page (AUP.htm)	Temporary	
File Distribution Requirement file (Setup.exe)		
Vulnerability Report file (fixsteps.htm; stinger.exe)	Quarantine	

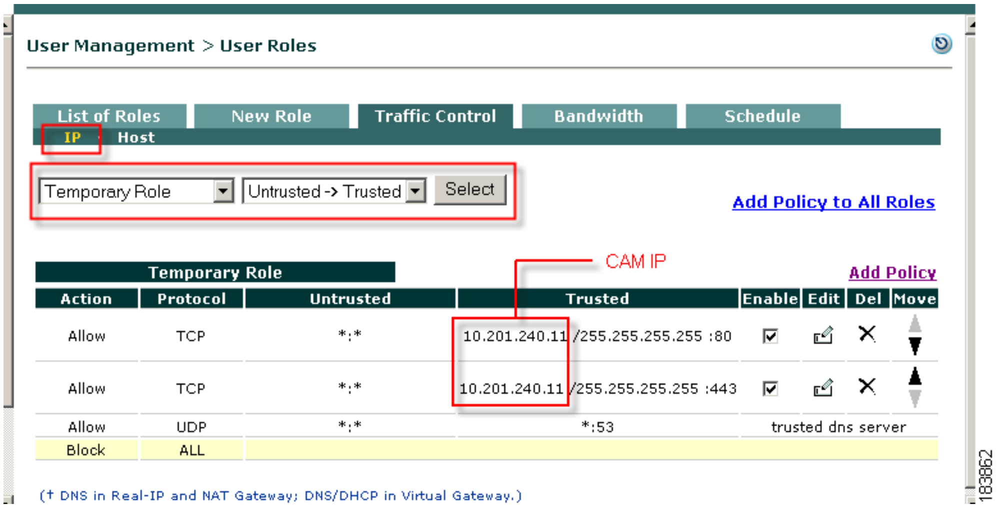
Table 9-2 Typical Traffic Policies for Roles

Resource	Role	Example Policies (Untrusted -> Trusted)
Host-Based Traffic Policies		
Enable Trusted DNS Server	All roles using Host policies	**Trusted DNS Server:** e.g. 63.93.96.20, or * (Any DNS Server)
Link Distribution Requirement (external website)	Temporary	**Default Host:** windowsupdate.com, or **Custom Host:** database.clamav.net (equals)
Vulnerability Report (link to external website)	Quarantine	
Other		
Proxy server in environment	Any role with access via proxy	**IP:** <*proxy_IP_address*>/255.255.255.255:http(80) **Host:** proxy-server.com (equals)
Full network access	Normal Login Role	Allow ALL TRAFFIC * /*

For further details, see:

- Upload a Resource File, page 6-13
- Create Content for the Right Frame, page 6-11
- Create File Distribution/Link Distribution/Local Check Requirement, page 10-78
- Configure Vulnerability Handling, page 13-13

Figure 9-18 Example Traffic Policies for File Distribution Requirement (File is on CAM)



Temporary Role

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*:*	10.201.240.11 /255.255.255.255 :80	☑		✕	▼
Allow	TCP	*:*	10.201.240.11 /255.255.255.255 :443	☑		✕	▲
Allow	UDP	*:*	*:53	trusted dns server			
Block	ALL						

(† DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway.)

Troubleshooting Host-Based Policies

For host-based policies, the CAS needs to see DNS responses in order to allow the traffic. If having trouble with host-based policies, check the following:

- Make sure allowed hosts are enabled.
- Make sure a DNS server has been correctly added to the list of DNS servers to track (you can also add an asterisk ("*") to track any DNS server).
- Make sure the DNS server is on the trusted interface of the CAS. If the DNS server is on the untrusted side of the CAS, the CAS never sees the DNS traffic.
- Make sure DNS reply traffic is going through the CAS. For example, ensure there is no alternate route for return traffic (i.e. trusted to untrusted) where traffic goes out through CAS but does not come back through the CAS. This can be tested by adding a "Block ALL" policy to the "Trusted to Untrusted" direction for the Unauthenticated or Temporary Role. If DNS, etc. still succeeds, then there is an alternate path.
- Make sure the DNS server listed for the client is correct.
- Make sure proxy settings are correct for the client (if proxy settings are required)
- Check **Device Management > CCA Servers > Manage [CAS_IP] > Filters > Roles > Allowed Hosts > View Current IP Address List** to see the list of current IPs that are being tracked through the host based policies. If this list is empty, users will see a security message.