How To: Configure a Cisco ASA 5505 for Video Conferencing

There are five main items which will need to be addressed in order to successfully permit H.323 video conferencing traffic through the Cisco ASA. These items are:

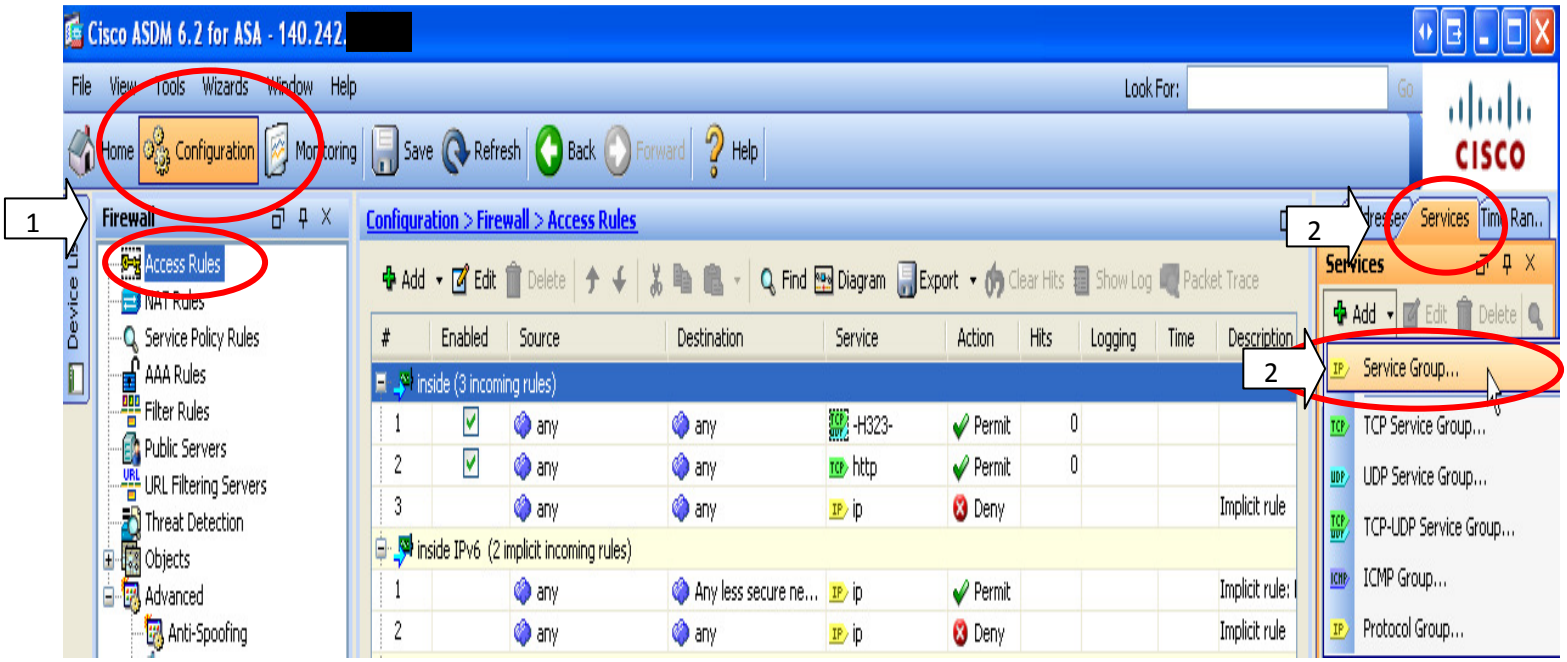
1. Create an IP Service Group
2. Create Network Objects
3. Define NAT Rules
4. Define Access Rules
5. Confirm the ACL Manager

NOTE: With the Cisco ASA 5505 there are no fixup protocols to configure; however, common issues noted with many Cisco ASA models relate to their use of fixup protocols. It is important to ensure that you *disable* the following if they are enabled on your ASA.

Fixup Protocol H323 **Fixup Protocol H323 RAS** **Fixup Protocol H323 H225**

Create an IP Service Group

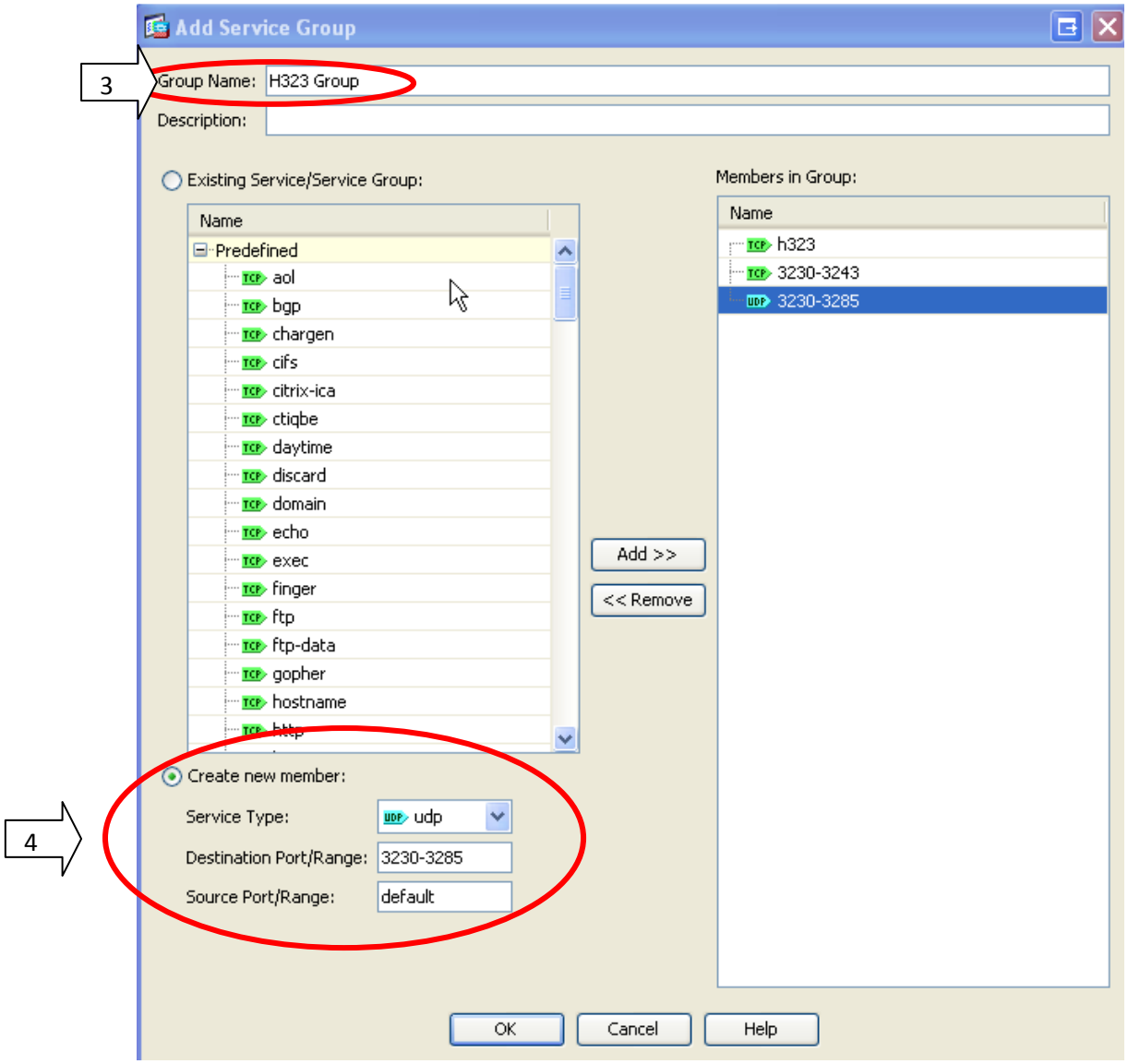
1) From the ASDM configuration tool, click on *Configuration*, *Firewall,* and then *Access Rules.*
2) Click on the *Services* tab from the menu which appears on the right, and then click *Add* and select *Service Group…*



3) In the window that appears enter a Group Name, such as *H323-Group.* A description can be entered if desired, but it is not necessary.
4) Click the radial button *Create new member:* We will be creating three new services, configure these services with the following parameters:

Service Type: TCP	Service Type: TCP	Service Type: UDP
Destination Port/Range: 1720	Destination Port/Range: 3230-3243	Destination Port/Range: 3230-3285
Source Port/Range: default	Source Port/Range: default	Source Port/Range: default

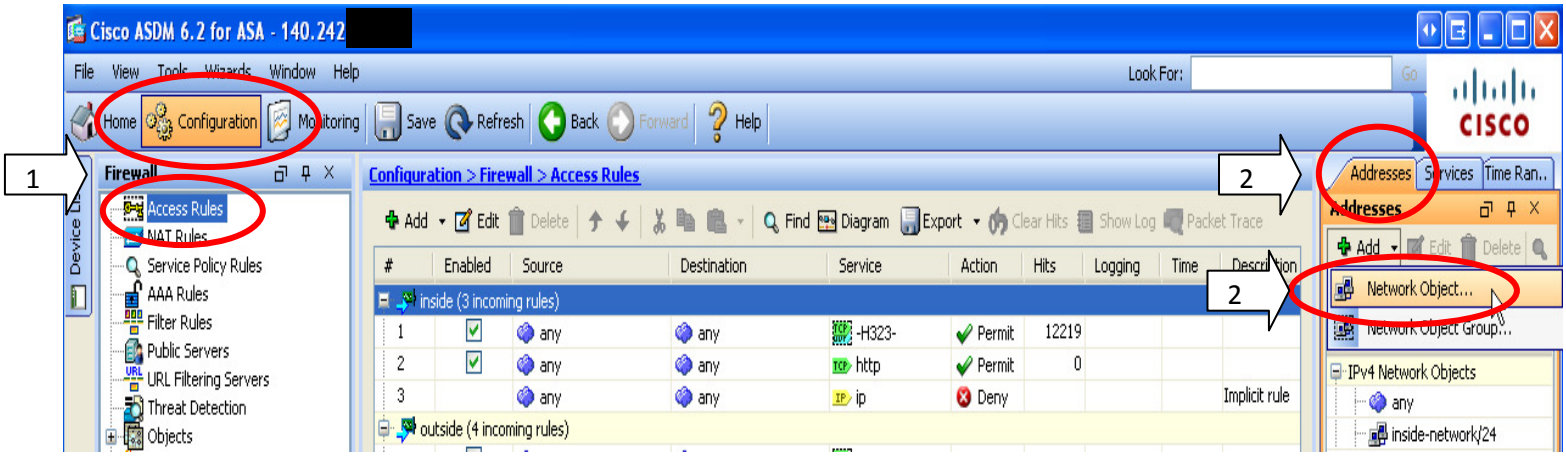
Ensure you click *Add >>* after creating each of these services. When you are finished your group will look like this. (**Note:** Typically ASA's have a predefined service for TCP 1720, so rather than see TCP 1720, you may see TCP h323 as shown below.)



5) Click *OK*, congratulations you have successfully created the IP Service Group!

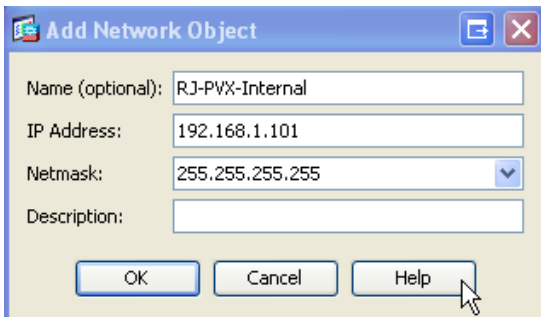
Create Network Objects

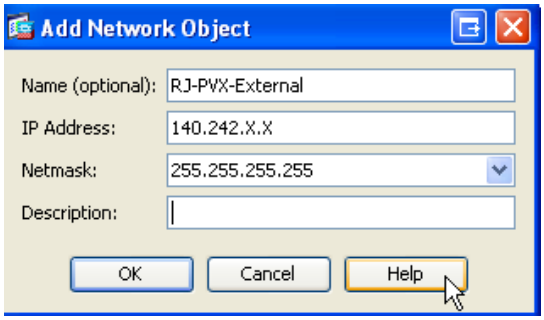
1) From the ASDM configuration tool, click on *Configuration*, *Firewall,* and then *Access Rules.*
2) Click on the *Addresses* tab from the menu which appears on the right, and then click *Add* and select *Network Object…*

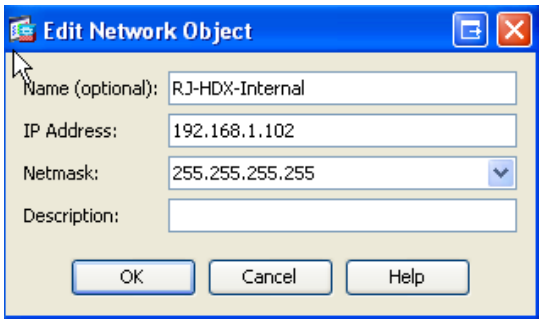


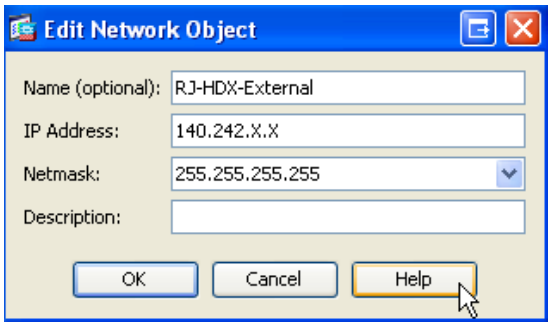
3) In the window that appears you can enter a name and description for your object, if no name is entered then the IP address will be displayed. Two objects must be created for each system that is expected to make and receive calls through the ASA, one reflecting the internal IP configuration, and one reflecting the external IP the system will be translated to.

   Since all the Objects we will create are hosts, the subnet mask will always be *255.255.255.255*, which tells the ASA the object is referring to only one IP address. Your entries should resemble the following:





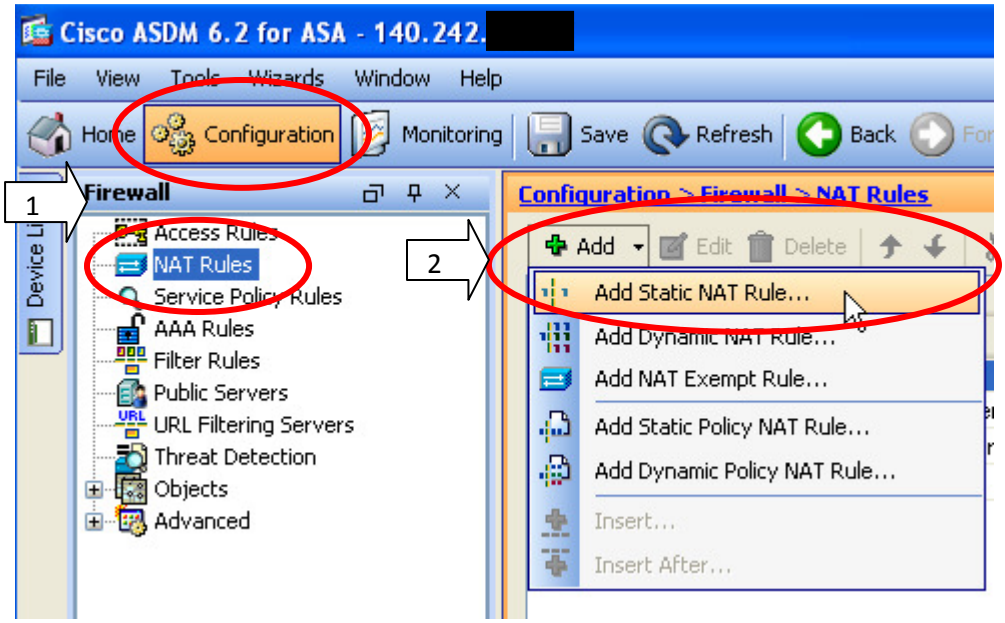




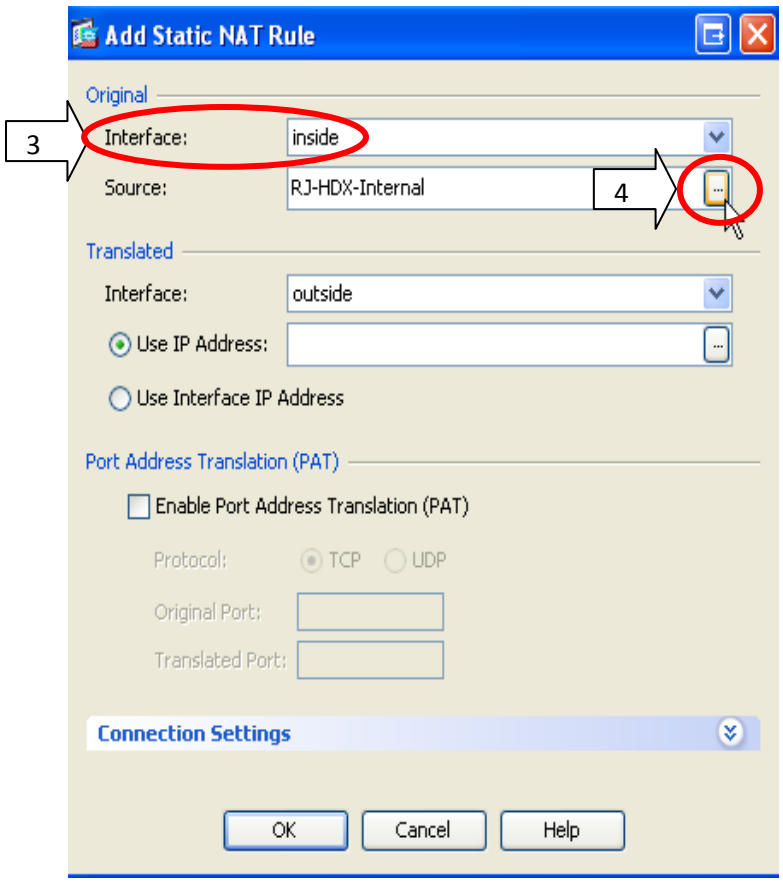
4) Once you have completed the above for all systems which are required to traverse the ASA, you are finished. Congratulations, you have successfully created your Network Objects!

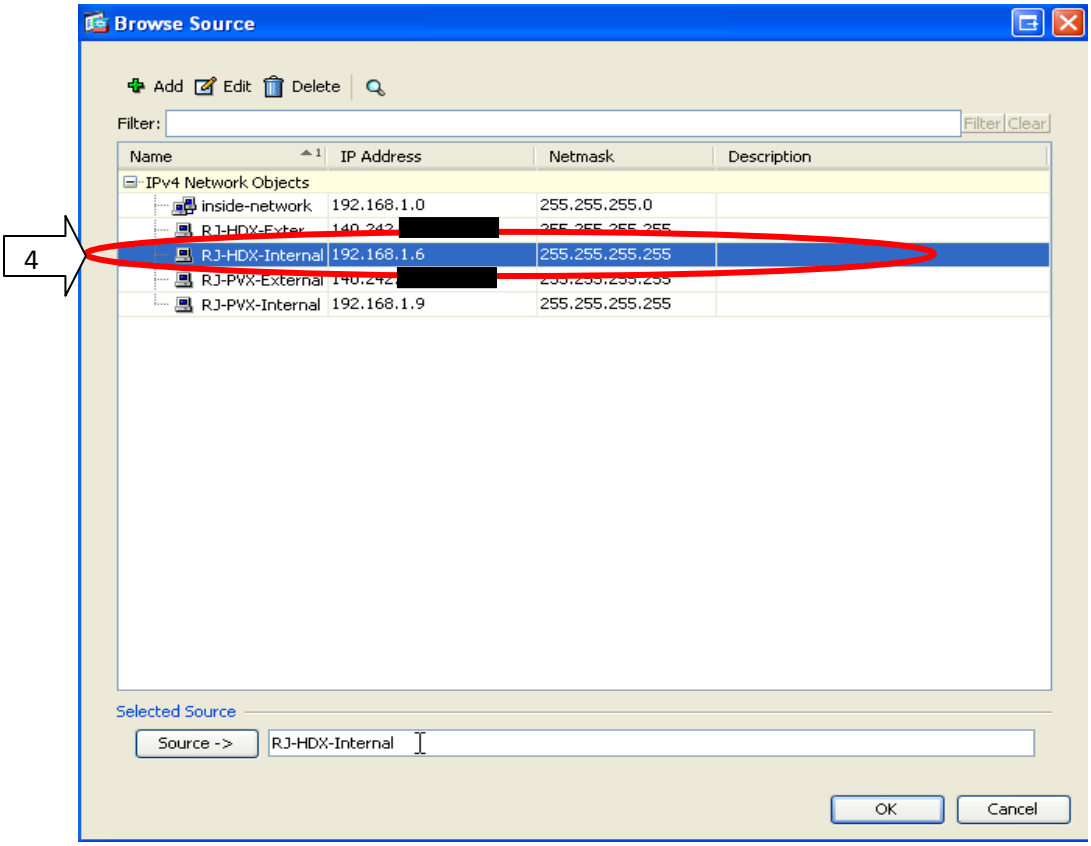
Define NAT Rules

1) From the ASDM configuration tool, click on *Configuration*, *Firewall,* and then *NAT Rules.*
2) In the center window, click *Add*, and then *Add Static NAT Rule…*



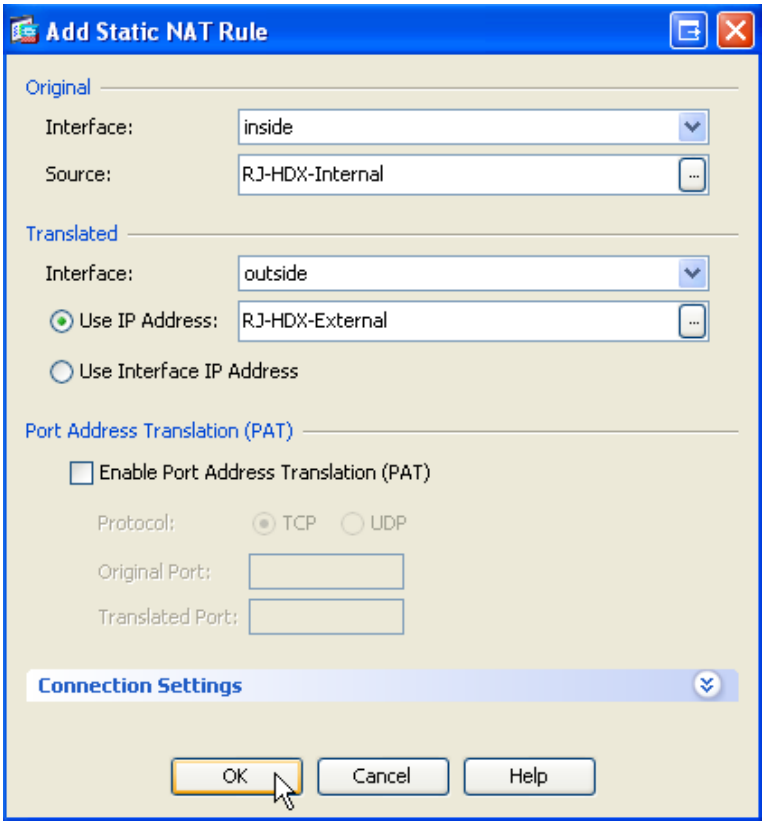
3) In the window that appears, the *Original Interface* should be set to *Inside*.
4) The *Original Source:* is configured by selecting the "…" icon at the right of the *Source:* text box, this icon will display another window where you will select the *Internal* network object we created earlier.



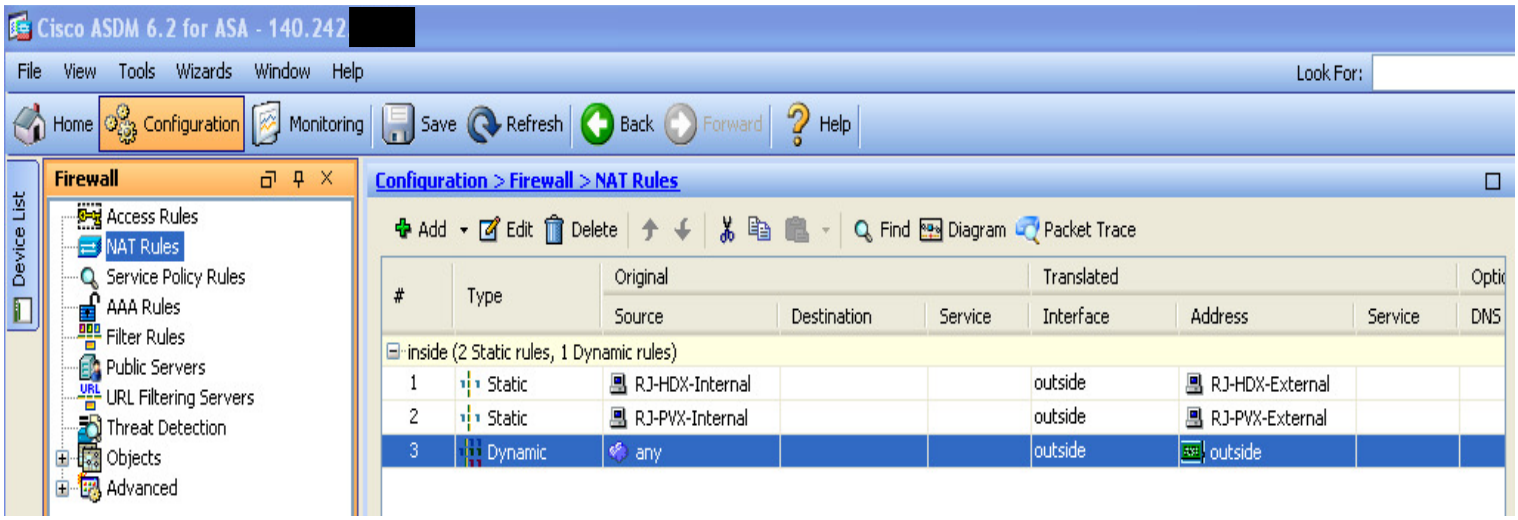


5) The *Translated Source:* should be set to *Outside.* The radial button for *Use IP Address:* should be selected. Click the "…" icon just like in step 4, but for this step, ensure you selected the *External* network object created previously which corresponds to the *Internal* object you selected in step 4.

The finished NAT rule should resemble the following:



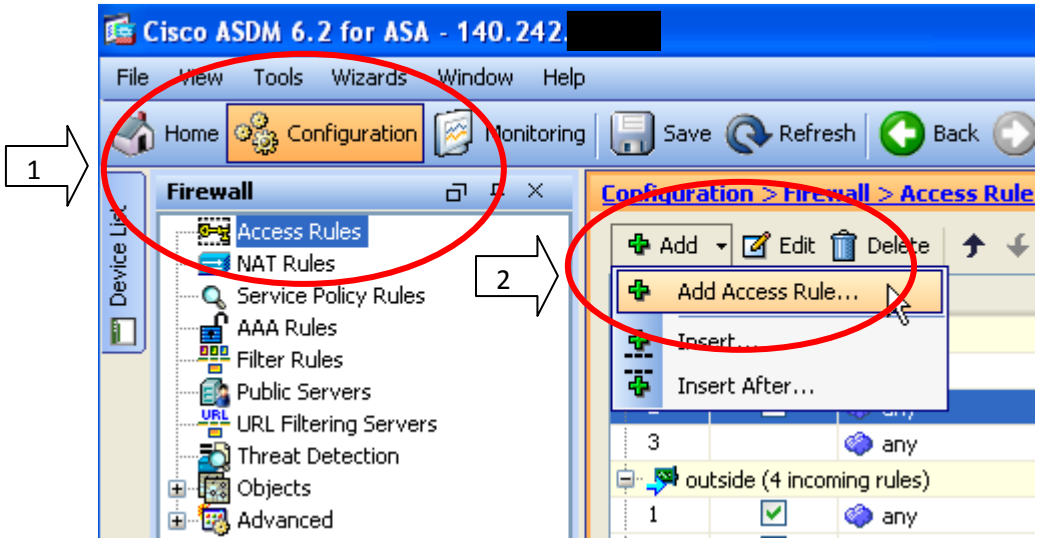
6) When you are finished click *OK.* Repeat steps 1 – 5 for each system required to traverse the ASA. When you are finished your main *NAT Rules* window should resemble the following:



Congratulations, you have successfully configured your NAT Rules!

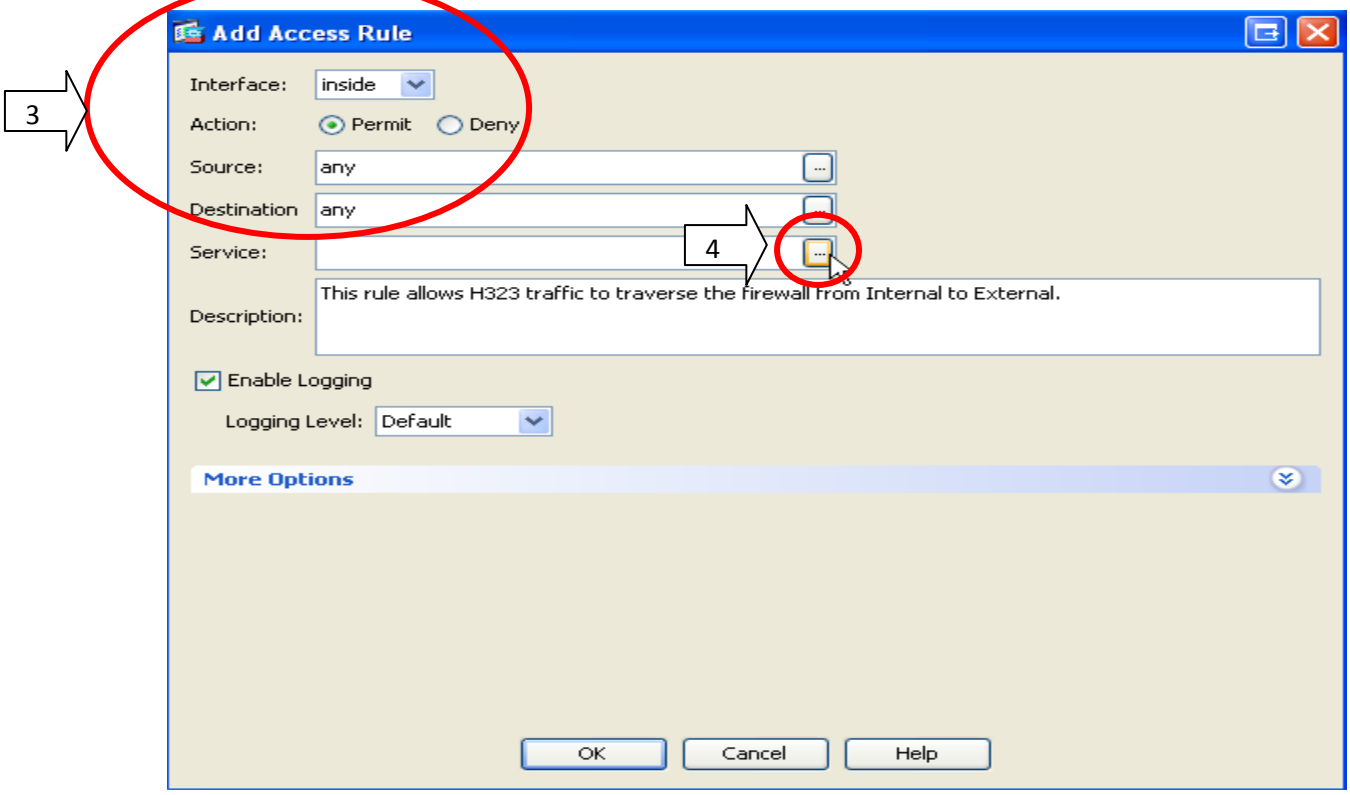
Define Access Rules

1) From the ASDM configuration tool, click on *Configuration*, *Firewall,* and then *Access Rules.*
2) In the center window, click *Add*, and then *Add Access Rule…*

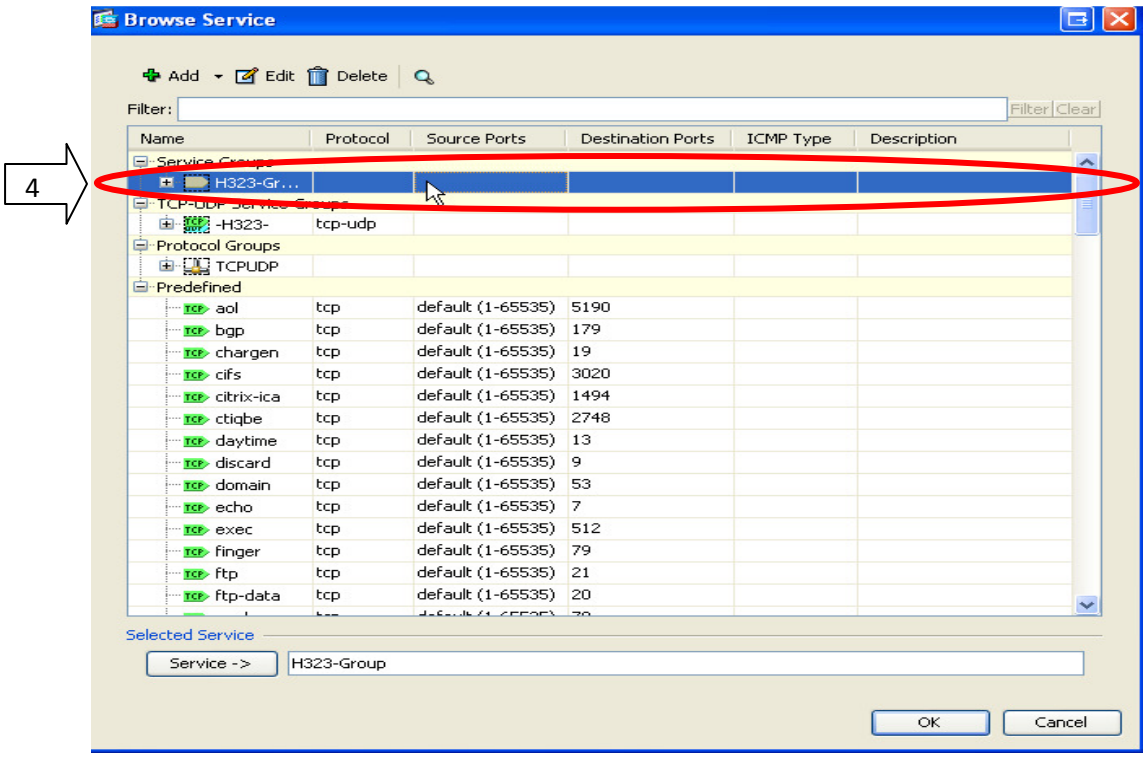


3) In the window that appears, configure the first access rule with the following parameters:

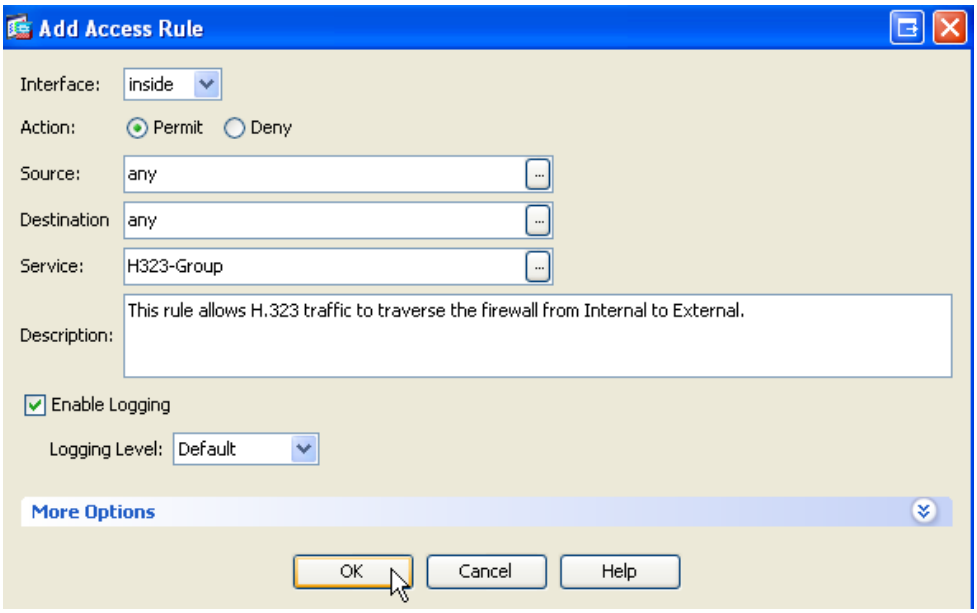
Interface: *Inside*
Action: *Permit*
Source: *Any*
Destination: *Any*



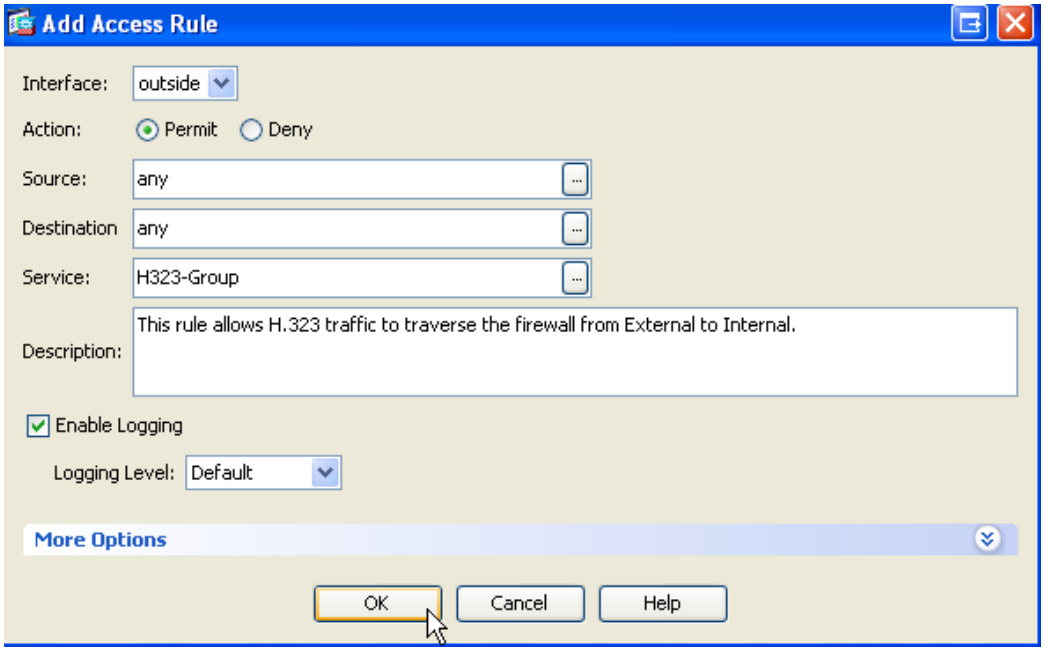
4) To configure the *Service:* select the "…" icon, in the window that appears, select the *H323-Group* we configured earlier and click *OK.*



The finished rule should resemble the following:



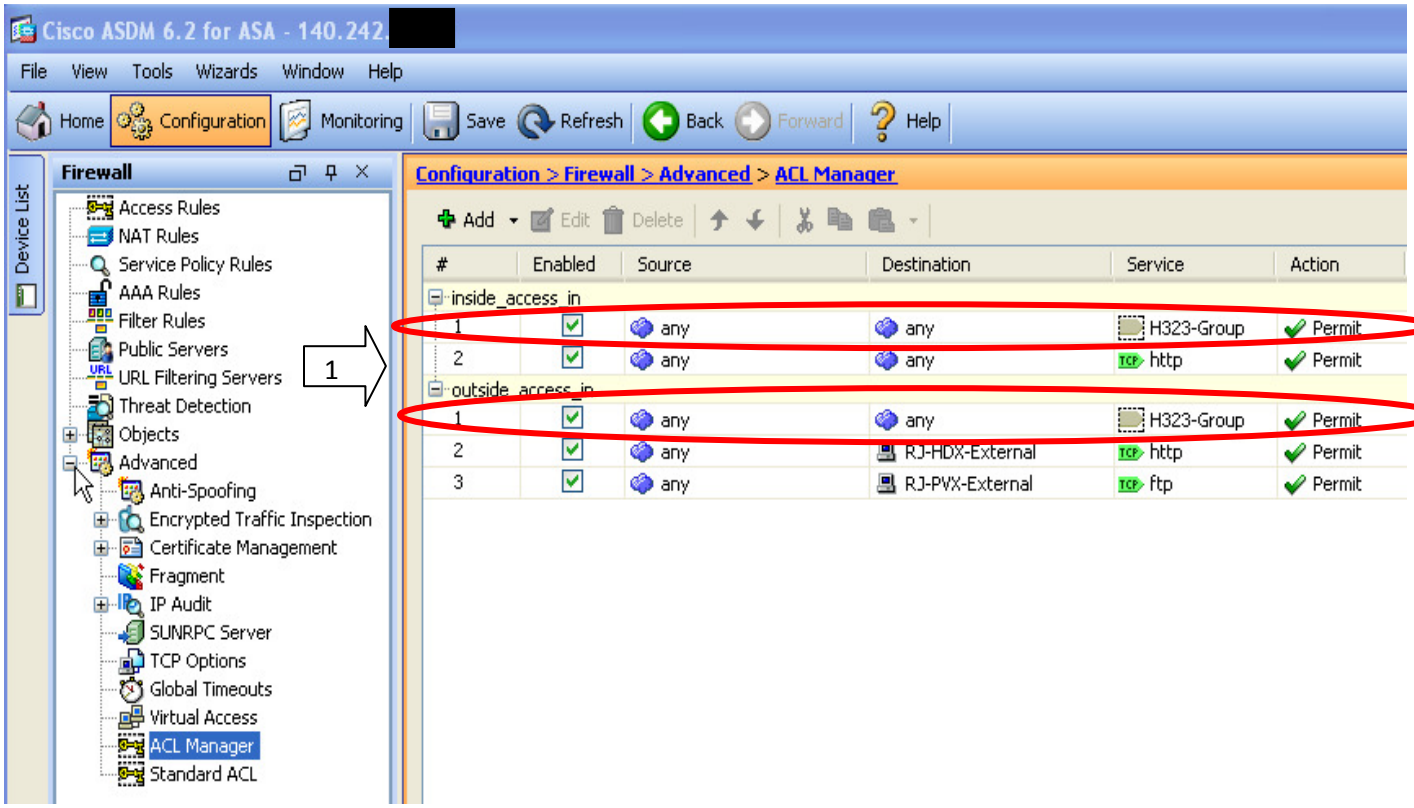
5) In order to create the Access Rule which will allow traffic to traverse the firewall from External to Internal, repeat the steps above, but ensure the *Interface:* is set to *Outside* as shown below.



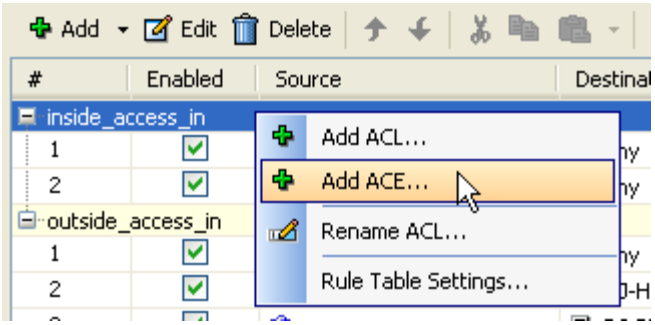
Congratulations, you have successfully configured your Access Rules!

Confirm the ACL Manager

1) From the ASDM configuration tool, click on *Configuration*, *Firewall.* Then expand the *Advanced* menu by clicking the + icon next to *Advanced*, and then click *ACL Manager.* In most cases the ASA will automatically create the appropriate ACL entries during the while completing the previous sections of this guide. If your ACL Manager does not show the access rules for the H323-Group, as shown in the image below, proceed to step 2.



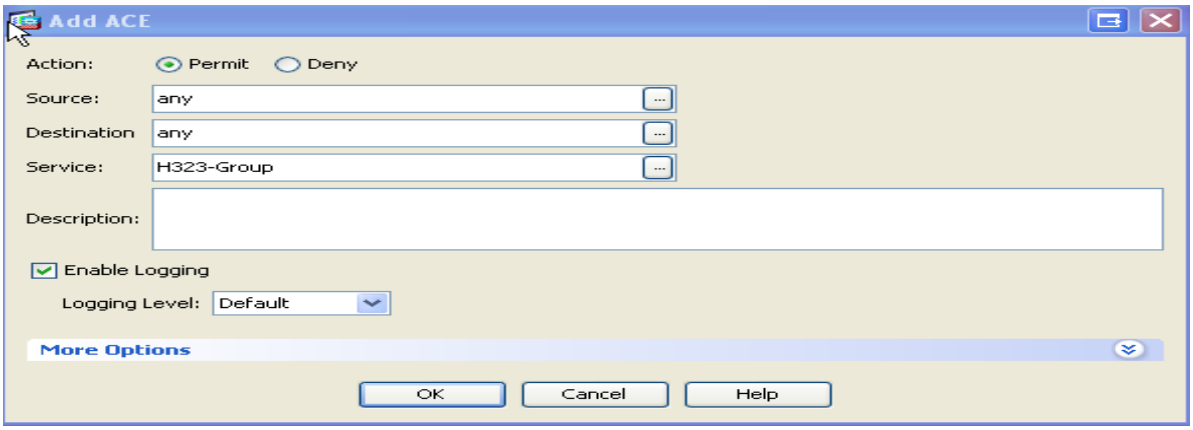
2) In the center window, right click the *Inside_Access_In* ACL, and then *Add ACE…*



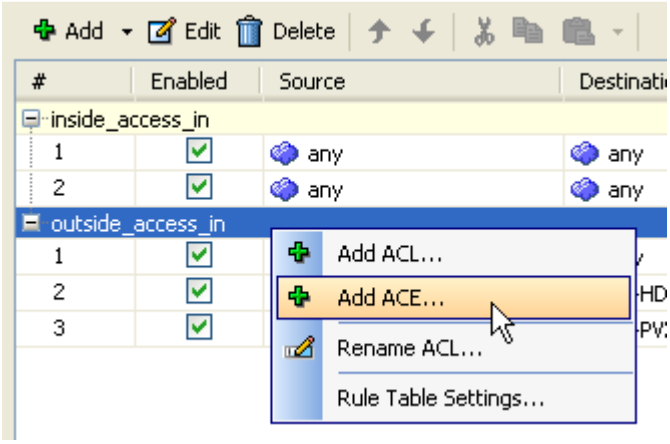
3) In the window that appears, ensure the following parameters are configured:

   Action: *Permit*
   Source: *Any*
   Destination: *Any*
   Service: *H323-Group*

   Once the ACE is configured with the above parameters, shown below, click *OK.*



4) In the center window, right click the *Outside_Access_In* ACL, and then *Add ACE…*



5) Configure the ACE with the same parameters from step 3. When you are finished the ACL Manager should now resemble the image from step 1.

   Congratulations, your ACL Manager should now be appropriately configured!

Important: Be sure to Apply and Save your new ASA configuration when finished!

Bonus Section: Fixup Protocols

Unsure if you have Fixup Protocols enabled on your Cisco device? No problem, you can Telnet, SSH or Console into your firewall and determine if they are active.

NOTE: If you are unfamiliar with the terms described below or how to enter the appropriate configuration modes, you should probably not be modifying the firewall in this manner, please contact one of the firewall administrators for further assistance!

Enter *Global Configuration Mode* on your Cisco device; you can confirm you are on the correct mode by the way the device name appears on screen. (<Device name> (config) followed by the # sign)

Cisco_ASA (config) #

Once you are in *Global Configuration Mode*, enter the command '*show fixup*'. The output of this command will let you know what fixup protocols are currently enabled on the device. It will appear similar to the output shown below:

```
Pix(config)# show fixup
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
Pix(config)#
```

Simply type *NO* followed by the fixup protocol you need disabled, in order to disable that particular fixup protocol.

EX:

Pix (config) # no fixup protocol h323 h225 1720

This will disable the H.323 fixup protocol, repeat this command until all h323 fixup protocols have been disabled.