Configuring SESM Features

This chapter describes how to configure the following SESM features:

Automatic Service Connections

An automatically connected service is a service that SSG connects immediately after the subscriber authenticates, without requiring the subscriber to explicitly select the service. This section describes two topics related to automatic connections:

Configuring Automatic Services

In general, if a service is marked as an auto connect service, the SSG performs the automatic connection after the subscriber authenticates. There is a special case with SESM in LDAP mode in which SESM is involved with automatic connection.

Configuring a Service for Automatic Connection

A subscriber profile specifies services for automatic connection. The subscriber profile also controls whether or not the service is hidden or not. If an auto connect service is hidden, it does not appear in the service list displayed on a service connection page.

In RADIUS mode, to configure a service for automatic connection, use the Account-Info A attribute in the subscriber profile. See Table C-6 on page C-11 for more information.

In LDAP mode, to configure a service for automatic connection:

- Subscribers can use the web portal's self-management features to select and deselect the auto connect feature for a service.
- Administrators can use CDAT to maintain subscriber profiles. See the *Cisco Distributed Administration Tool Guide* for information.

Configuring SESM to Request Automatic Connections in LDAP Mode

In LDAP mode, the SSG performs automatic connections if it has the service list. If SSG does not have the service list, the SESM application can perform the automatic connections. During RDP installation, the Add Services option configures RDP to either:

- Return a service list to SSG—In this case, RDP includes the subscriber's service list and related information in replies to SSG, and SSG performs automatic connections for services marked for auto connection in the subscriber's profile.

  The service information consumes memory on the SSG host.

- Not return a service list to SSG—In this case, SSG cannot perform automatic connections. The advantage to this configuration is that it saves memory on the SSG host.

  In this case, you can configure the SESM application to perform automatic connections. The following line in the application MBean configuration file (for example, nwsp/config/nwsp.xml) controls whether the SESM web application performs automatic connections:

  ```
  <Set name="autoConnect" type="boolean">false</Set>
  ```

  Change the value to `true` to enable automatic connections by the SESM web application.

To change the setting of the RDP service list option, reinstall RDP.

Subscriber Experiences with Automatic Connections

This section describes the behavior of the SESM portal application regarding automatically connected services.

Connection Status for Auto Connect Services

The status page in an SESM portal shows the status for all services, including automatically connected services. In NWSP, the selection page includes service status indicators for each service listed. Hidden services are not listed. See the "Configuring a Service for Automatic Connection" section on page 10-1 for an explanation of a hidden service.

Immediately after logging in, the service status for auto connect services might display as not connected. This happens if the service indicators display before the connection is completed. Proxy and tunnel services, for example, can take a while to connect. If the subscriber refreshes the window or selects the status window, the automatically connected services display with a connected status.

Pop-Up Window for Auto Connect Services

If the subscriber's home URL is set to an autoconnect service, the pop-up window for the service might appear before the connection completes. If this occurs, the following message appears in the pop-up window:

```
Page cannot be displayed.
```

The URL is correct. If the subscriber waits a short time and resubmits the request using the URL already displayed in the window, the service pages appear.

Changing the Auto Connect Property for a Service

In LDAP mode, a subscriber can use the SESM self-management features to select or deselect the auto connect property. These changes are recorded immediately in the LDAP directory, but the change is not effective immediately. Changes are not visible in SESM until the cache timeout period in RDP elapses.

For example, a subscriber might select the auto connect property for a service, log out of SESM, log back in, and notice that the service was not automatically connected. Caching in the RDP causes this delay.

Caching in RDP improves system performance. The deployer can turn off caching or reduce the cache period, but those actions impact performance.

Disconnecting Auto Connect Services

A subscriber can disconnect an auto connected service at any time. The disconnected status persists as long as the subscriber remains authenticated. The SESM single sign-on option affects whether a subscriber remains authenticated across SESM sessions. If the subscriber has to reauthenticate after the SESM session expires, the SSG reconnects all auto connect services.

The SESM session might expire, for example, because the subscriber closed the browser or navigated away from the SESM pages. When the SESM session expires:

- With single sign-on, subscribers are not required to reauthenticate.
- Without single sign-on, subscribers are required to reauthenticate when they navigate back to the SESM portal application. As a result of the reauthentication, SSG reconnects the auto connect services.

We recommend running SESM portal applications with single sign-on turned on.

Location Awareness

This section describes the SESM location awareness features. It includes the following topics:

You can enhance location awareness features with arbitrary attributes, as described in the "Arbitrary Attributes" section on page 10-9.

Overview of Location Awareness

The SESM location awareness feature relies on the physical location characteristics of an edge session. SESM obtains this location information from the SSG as part of the session's initial connection request. The specific attributes used to determine the location, and hence the location branding, are configurable.

The location attributes can consist of the client IP address., client subnet, MAC address, VPI/VCI, SSG subinterface, and MSISDN, depending on the network deployment, and are valid even before the session authenticates.

The SESM portal can use the location as a dimension in the user shape to help determine the resources to use in the returned JSPs.

Note Location and locale are two different dimensions of the user shape. The locale dimension identifies subscriber language and character set preferences. SESM obtains the locale from the subscriber browser settings. The locale is available before the subscriber authenticates.

Some examples of using location information in customized SESM portals are:

- Location-based branding—Brand the portal pages and offer free or different services accordingly.
- Personalized portals—Taylor the subscriber experience based on location characteristics.
- Access policies—Allow free services to a certain segment of subscribers based on connection characteristics, such as VPI ranges or subinterface ranges. For example, location awareness could permit certain subscribers from a certain location to gain access to the Internet service without authentication.
- Redirections—Redirect all browsers with particular location characteristics to a specified portal page.

Location Awareness Configuration Methods

SESM offers two ways to configure location awareness. Table 10-1 describes these two methods.

Table 10-1 Location Attributes

Feature	MBean	Attributes That Determine Location	Restrictions
Location awareness using complete ID attributes **Note** This is the recommended method for defining location awareness.	Location MBean	One of the following attributes or a combination of attributes: • Subscriber IP address range • Virtual path identifier (VPI) range • Subinterface, such as an Ethernet interface More attributes might be added in future releases.	Requires the SSG complete ID feature in one of the following Cisco IOS releases: • Release 12.3(1)T • Release 12.2(8)B, X train
Location awareness using IP subnets	SSG MBean	One of the following: • If the port-bundle host key feature is used—SSG IP address subnetwork ranges • If the port-bundle host key feature is not used—Subscriber IP address subnetwork ranges	Does not work if load balancing is implemented. Will be phased out in future releases.

If both of the above location awareness methods are configured for the same SESM portal, the location derived from the IP subnet method takes precedence. If the session does not match the criteria configured for the IP subnet method (in the SSG MBean), then the portal examines the complete ID criteria in the Location MBean.

Using Location to Control the Look and Feel of Portal Pages

When the SESM portal identifies the location (based on configured attributes), it sets the "LOCATION" attribute in the SESMSession object created for the subscriber. For the location determination to be meaningful, the portal must use the "LOCATION" attribute. For example:

- The portal can use the location as a dimension in the user shape to help determine the resources to use in the returned JSPs. NWSP uses this method to determine a location-specific image to use in the NWSP banner. See the *Subscriber Edge Services Manager Web Developer Guide* for more information about the user shape mechanism, the location attribute in the locationDimension.jsp, and the SESMSession object.
- The portal can associate attributes to a location using the SESM arbitrary attributes feature. See the "Arbitrary Attributes" section on page 10-9 for more information.

Location Names

Any value is acceptable for a location name, but the name must match the intended uses. For example:

- NWSP uses the location dimension in the user shape to return different images on JSP pages based on location. To implement this usage, NWSP uses the configured location name to identify the subdirectory containing the correct image for each location. Therefore, the configured names must match the subdirectory names. For examples, see the following:

```
nwsp
    webapp
       london
       newyork
       paris
```

- NWSP associates arbitrary attributes to locations. The location names in the arbitrary attributes configuration must match the names used in location awareness configuration. For examples, see the "Configuring Arbitrary Attributes" section on page 10-10.

Configuring Location Awareness Based on Complete ID Attributes

The complete ID is the complete set of identifying attributes available about an edge session. SSG makes this set of attributes available to SESM. The SESM location awareness feature uses a subset of the complete ID attributes. The complete ID attributes that are currently supported for location awareness are listed in Table 10-1.

Note To use location awareness based on complete ID, your SSG platforms must be running Cisco IOS Release 12.3(1)T or the X train for Release 12.2(8)B.

Use the Location MBean to define location names and the attributes that are associated with each location. For information about the Location MBean, see the "Multikey Authentication" section on page 10-28.

Using Multiple Attributes for the Same Location

You can use multiple attributes to define a location. For example, the installed nwsp.xml file configures a “paris” location that applies to all sessions with a VPI from 1 to 3 on the subinterface ATM3/0. Both requirements must match for the location to apply to a session.

Each attribute definition in a location is restricted to one value or one range. However, you can define more than one location with the same name using the same attributes, but with different attribute values. For example, you could define two “london” locations, each one using a different IP address range.

Using Duplicate, Overlapping and Nested Attributes for Different Locations

This section describes the situation when a session’s attributes match the criteria for more than one location. SESM offers two ways to resolve the location in these cases:

- Identify the first matching location—The portal associates the first location whose configured attributes match all of the attributes of the edge session. The ordering of locations in the configuration file is important. NWSP implements location awareness using this method.
- Identify all matching locations—This feature provides a way to process nesting and overlapping locations. The portal must be customized to process all matching locations in some way. To implement this feature, see the next section.

Implementing Nested and Overlapping Locations

To implement nested or overlapping locations, you can customize the portal to use the getLocations method. This method returns an iterator over all the locations that match the attributes for the session, in the order that the locations appear in the configuration file.

Overlapping Locations

Overlapping locations occur when there is a possibility of sessions existing that match more than one location. They may or may not be defined on the basis of the same parameter types.

In the following example, two locations overlap for sessions with a client IP address in the range 10.4.0.0 to 10.8.0.0.

- Location A is defined for client IP range 10.0.0.0 to 10.8.0.0.
- Location B is defined for client IP range 10.4.0.0 to 10.32.0.0.

In the following example, two locations overlap for sessions with a client IP address in the range 10.0.0.0 to 10.8.0.0 that are connected via the subinterface Ethernet 0/0.

- Location A is defined for client IP range 10.0.0.0 to 10.8.0.0.
- Location B is defined for the sub-interface Ethernet 0/0.

Nested Locations

Nested locations are a specialization of the overlapping concept. Nesting occurs when one location is a subset of another. In the following example, Location A is nested inside location B.

- Location A is defined for the sub-interface ATM0 and VPI number 1 to 3.
- Location B is defined for the sub-interface ATM0.

When defining nested interfaces, it is usually best to define the smallest location first. In the example above, this would be Location A. This is because only the first match is returned when looking for a single location, so any nested locations would effectively get hidden if they were not placed in the configuration before the location they are nested inside.

There is no restriction on how deeply locations can be nested.

Configuring Location Awareness Based on IP Address Subnets

To configure locations based on IP address subnets, use the SSG MBean. Use setSubnetAttribute entries with the SESSION_LOCATION argument. The following example from nwsp.xml shows the attributes required for location awareness:

```
<Call name="setSubnetAttribute"><Arg>ipAddress</Arg><Arg>mask</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>location</Arg></Call>
```

Table 5-5 on page 5-7 describes how to format subnet entries. The following points relate specifically to location awareness:

- *ipAddress* and *mask* indicate one of the following:
  - A range of subscriber IP addresses (a subnet)—Use the IP address and Mask fields to indicate a subnet of IP addresses to associate with the same location. If port-bundle host key is configured on the SSG, the range will apply to SSG IP addresses, rather than subscriber IP addresses.
  - A specific IP address—The IP address is that of the client, or, if port-bundle host key is configured on the SSG, one of the SSG IP addresses specified in the port-bundle host key port map configuration.
- *location* is the location you want to associate with *ipAddress.* Any value is acceptable, but it must match your intended uses.
- Any value is acceptable, but it must match your intended uses. For example:
  - NWSP uses different images for each location. The images are stored in subdirectories whose

Example 1—Location Associated with Subscriber IP Addresses

The following example associates locations with subscriber subnets. The example associates a different subscriber network with each of the three example locations defined in Step 2. In the NWSP application, when subscribers from the 144.0.0.0 network point their browsers to the NWSP URL, they receive a page containing the words New York under the NWSP logo.

```
<Call name="setSubnetAttribute"><Arg>10.0.0.0</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
<Call name="setSubnetAttribute"><Arg>1.0.0.0</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>paris</Arg></Call>
<Call name="setSubnetAttribute"><Arg>144.0.0.0</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>newyork</Arg></Call>
```

Example 2—Location Associated with SSG IP Address

When the port-bundle host key feature is configured on the SSG, location must be associated with an SSG IP address, rather than the subscriber's IP address. In the following example, the IP address is an SSG source IP address included in the port mappings during port-bundle host key configuration.

```
<Call name="setSubnetAttribute"><Arg>10.52.199.20</Arg><Arg>255.255.255.255</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
```

Demonstrating Location Awareness

The NWSP application illustrates location awareness by changing the look of the banner on the NWSP logon page. The location determines which city name appears in the NWSP logo. The installed nwsp/docroot directory includes subdirectories for three locations: london, paris, and newyork. These subdirectories contain the images used in this demonstration. If you want to use different city values, you must provide the corresponding images. The application code that displays the banner is in locationDimension.jsp.

Demonstration Procedure Using Complete ID Attributes

To demonstrate location awareness based on Complete ID attributes, use the following procedure:

Step 1 Install SESM in RADIUS or LDAP mode, using a typical or custom installation. (Do not use Demo.)

Note You cannot use Demo mode to show location awareness using complete ID attributes.

Step 2 Comment out the location subnet entries in the SSG MBean.

Step 3 Edit the Location MBean to include a specific IP address for the “paris” location. Use the IP address of a client machine that is available for the demonstration. Use the same IP address in the start and end parameters.

For example:

```
<Set name="name">london</Set>
<Set name="parameters">
<Array class="com.cisco.sesm.core.location.LocationParameter">
<Item>
<New class="com.cisco.sesm.core.location.IPRangeParam">
<Set name="start" type="String">needIPaddress</Set>
<Set name="end" type="String">needIPaddress</Set>
</New>
</Item>
</Array>
</Set>
```

Step 4 Add a new location to the Location MBean for “newyork.” (Use this value because the installed files include a subdirectory and an image for the newyork value.) For example, insert these lines into the locations array:

```
<Item>
<New class="com.cisco.sesm.core.location.Location">
    <Set name="name">newyork</Set>
    <Set name="parameters">
        <Array class="com.cisco.sesm.core.location.LocationParameter">
           <Item>
              <New class="com.cisco.sesm.core.location.IPRangeParam">
                 <Set name="start" type="String">needIPaddress</Set>
                 <Set name="end" type="String">needIPaddress</Set>
              </New>
           </Item>
        </Array>
    </Set>
</New>
</Item>
```

Step 5 Start NWSP using the NWSP startup script.

Step 6 Open browsers on each of the client systems.

Step 7 From each browser, go to the SESM URL. For example, go to http://*serverName*:8080.

Step 8 Notice the images in the banners on each browser. One should say London; the other should say New York.

Step 9 On a third machine, repeat steps 7 through 9. The banner should not include a city name, because the third browser's IP address is not associated with any location in the configuration file.

Demonstration Procedure Using Subnet Entries

To demonstrate location awareness based on subnet entries, use the following procedure:

Step 1 Install SESM in Demo mode.

Step 2 Edit setSubnetAttribute parameters in the SSG MBean to include specific IP addresses for two different client machines that are available for the demonstration. For example:

```
<Call name="setSubnetAttribute"><Arg>NEED_REAL_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>london</Arg></Call>
<Call name="setSubnetAttribute"><Arg>NEED_REAL_IP_ADDRESS</Arg><Arg>255.0.0.0</Arg>
    <Arg>SESSION_LOCATION</Arg><Arg>paris</Arg></Call>
```

Step 3 Start NWSP using the NWSP startup script.

Step 4 Open browsers on each of the client systems.

Step 5 From each browser, go to the SESM URL. For example, go to http://*serverName*:8080.

Step 6 Notice the images in the banners on each browser. One should say London; the other should say Paris.

Step 7 On a third machine, repeat steps 7 through 9. The banner should not include a city name, because the third browser's IP address is not associated with any location in the configuration file.

Arbitrary Attributes

This section describes the arbitrary attribute feature. It includes the following sections:

Description of Arbitrary Attributes

The arbitrary attribute feature lets the deployer create any arbitrary attribute and associate it with other known attributes. To use the arbitrary attribute feature, you configure a multidimensional table consisting of the known attribute values and the arbitrary attributes you are associating.

For example, NWSP uses arbitrary attributes to associate URLs with locations. In this case, the elements in the multi-dimensional table are as follows:

- One dimension of the table consists of the location values, which must be defined using the location awareness feature.
- Another dimension is the URL to associate with each location.

At run time, SESM constructs a reference table holding all of the configured values. The arbitrary attribute values are available for use by the SESM portal. For example, NWSP uses arbitrary attributes associated with locations to help determine the initial URL for an Internet service pop-up window.

Configuring Arbitrary Attributes

To configure the SESM portal to associate arbitrary attribute values to locations, use the following procedure:

Step 1 In the WebApp MBean, use addDimension calls to configure the arbitrary attribute reference table.

Step 2 The format for an addDimension call is:

```
<Call name="addDimension">
      <Arg type="int">attributeID</Arg>
      <Arg>attributeKey</Arg>
      <Arg>attributeResult</Arg>
```

An example from nwsp.xml is:

```
<Call name="addDimension">
      <Arg type="int">1</Arg>
      <Arg>london</Arg>
      <Arg>http:\\www.london.com</Arg>
```

Where:

- *attributeID* identifies a category of entries in the attribute table. Use the same *attributeID* for all entries associated with the same purpose.
- *attributeKey* identifies the location values. For example, the installed WebApp MBean includes the values london, paris, and newyork. The location values must be defined in the location awareness feature.

Note Make sure the location values match exactly the definitions used for location awareness. For example, the “London” and “london” are considered different values.

Note The user shape mechanism and the addDimension calls are different features. The user shape mechanism has no dependencies on any values defined in the addDimension calls.

- *attributeResult* defines a URL that you want to associate with the *attributeKey.*

Demonstrating Arbitrary Attribute Assignments in NWSP

The arbitrary attribute used in this demo determines the first URL that the browser attempts to display after the subscriber connects to an Internet service. The code that implements this demo is in initUser.jsp. The code determines the initial URL as follows (the second item uses the arbitrary attribute feature):

1. If the subscriber request was captured by the SESM Captive Portal application, the subscriber's initial URL request is used.
2. Otherwise, if a location in an addDimension call matches the LOCATION attribute from the SESMSession object, the URL associated with the location is used.
3. Otherwise, if the subscriber profile includes a non-blank H attribute, that URL is used.

Demonstration Procedure

To demonstrate the use of an arbitrary attribute to control an item on a JSP page, use the following procedure.

Step 1 Configure location awareness. You can use either location awareness method: subnets configured in the SSG MBean, or complete ID attributes configured in the Location MBean.

Step 2 Edit the parameters to the addDimension calls in the WebApp MBean. Make sure the second argument in the addDimension call matches exactly the location strings you defined for location awareness. The installed nwsp.xml file contains the following lines:

```
<Call name="addDimension">
      <Arg type="int">1</Arg>
      <Arg>london</Arg>
      <Arg>http://www.london.com</Arg>
    </Call>
    <Call name="addDimension">
      <Arg type="int">1</Arg>
      <Arg>paris</Arg>
      <Arg>http://www.paris-france.org/</Arg>
    </Call>
```

Step 3 Start NWSP using the NWSP startup script.

Step 4 Start a browser on a system whose location was configured in Step 1.

Step 5 Go to the NWSP URL.

Step 6 Login using the following values:

- RADIUS mode demos:
  - User: radiususer
  - Password: cisco
- LDAP mode demos:
  - User: golduser
  - Password: cisco

Step 7 Select the Internet service from the NWSP service list (if the Internet service was not automatically configured.)

A service pop-up window appears, attempting to go to the URL in the addDimension call. For example, the london location attempts to go to www.london.com.

Note If you configured the Captive Portal application, the browser's original request is honored instead of the arbitrary attribute associated with the location.

Personal Firewalls

This section describes how to configure and use the SESM personal firewall features. Topics are:

Overview of Firewall Features

The SESM personal firewall feature provides a way for subscribers to restrict or permit traffic to and from their connection by making choices on web portal pages. Deployers can also apply firewall controls on subscriber traffic.

The NWSP application includes two personal firewall pages:

- My Firewall page—This is a basic firewall page that allows subscribers to create filters on specific applications and protocols. The subscriber can choose to permit or deny all traffic for each of the applications/protocols. The list of applications and protocols that appears on the My Firewall page is preconfigured by the deployer in the Firewall MBean.
- Advanced Firewall page—This page provides a way for the subscriber to create more specific filters than the basic page. They can create filters that permit or deny traffic for specific source and destination IP addresses, ranges of IP addresses, or ports.

The deployer-imposed firewall controls cannot be changed by the subscriber. The deployer-imposed controls are added to subscriber profiles using CDAT. These controls have a higher priority and can therefore override the personal firewalls entered by subscribers.

Required Deployment Options

The SESM firewall features are supported only when SESM is running in LDAP mode with RDP deployed in non-Proxy mode. The SSG (or some other cooperating network element that can process extended access control lists) is required.

Underlying Technology

The underlying technology for the SESM personal firewall features is extended access control lists (ACLs). The ACLs are attributes in subscriber profiles in an LDAP directory.

The ACLs are stored in the subscriber profiles as a standard RADIUS attribute with number 26 (vendor specific attribute), subattribute number 1 (Cisco AV-pair). A subscriber profile might have many ACL entries, which together determine which traffic is permitted and denied on the connection.

The ACLs are added to the profile in two ways:

- The SESM portal creates the ACLs and adds them to the profile as a result of subscriber entries on the portal firewall pages.
- Deployer administrators manually create correctly formatted ACLs and enter them in the subscriber profile using CDAT.

SESM and SSG (or another cooperating network element) implement the personal firewall ACLs as follows:

- SSG sends an access-request message to RDP.
- During authentication processing, RDP obtains the subscriber profile from the directory and includes all of the profile information, including the ACLs, in the access request reply it sends back to the SSG.
- The SSG applies the ACLs against traffic to and from the subscriber's connection.

Firewall Priorities

The SSG or other cooperating network element applies the ACLs in a subscriber's profile, in a prioritized order, to each packet. When the conditions specified in an ACL match the packet, the permit or deny action specified in the ACL is applied to the packet, and no further ACLs are examined for that packet.The order in which ACLs are applied affects the filtering outcome.

In the SESM ACLs in a subscriber profile, priority is based on an ACL number . (The lowest ACL number is applied first.) The ACL numbering scheme used by SESM enforces the following general priorities:

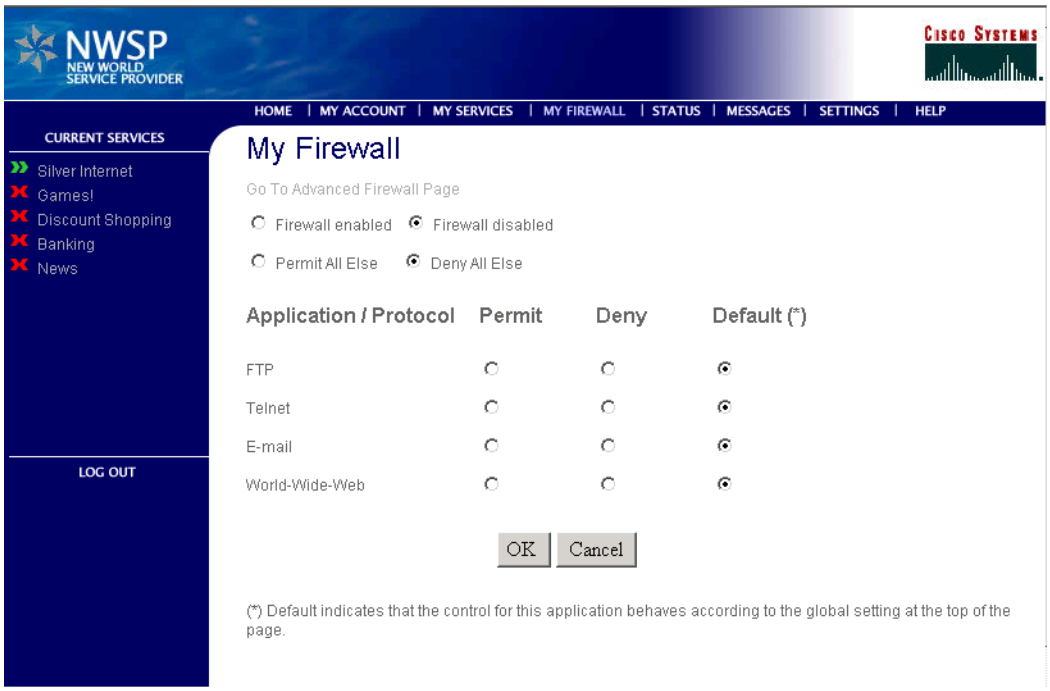
- Administrative ACLs have the highest priority. These ACLs are entered by the deployer in CDAT should contain ACL numbers in the range from 100 to 109. It is up to the administrators entering the ACLs to enforce this convention.
- ACLs generated from the Advanced Firewall page have the next priority. The SESM portal automatically assigns these ACL numbers.
- ACLs generated from the My Firewall page have the lowest priority. The SESM portal automatically assigns these ACL numbers.

See the "ACL Number Assignments" section on page 10-23 for a description of how SESM assigns the ACL numbers to ensure that the most specific ACLs are applied first, and the more general ACLs last.

My Firewall Page

Figure 10-1 shows the NWSP My Firewall page as it appears if there are no ACLs in the subscriber profile, or if the only ACLs in the profile are deployer-imposed ACLs. (Deployer-imposed ACLs are ones with ACL numbers in the 100 to 109 range.)

Figure 10-1 My Firewall Page in NWSP



A description of the My Firewall page follows.

- Firewall Enabled or Disabled—When the page displays, this button indicates whether any subscriber-entered filters exist for this subscriber:
  - Enabled—At least one subscriber-entered filter exists in the subscriber's profile. The filters can be those entered on the My Firewall or Advanced Firewall page. Administrative ACLs, if any exist in the profile, are not considered.
  - Disabled—This subscriber profile contains no subscriber-entered filters. If the window opens with Enabled selected, and the subscriber clicks **Disabled** followed by **OK**, it deletes all subscriber-entered filters from the subscriber profile. The action does not delete administrative ACLs if the adminstrator used the reserved administrative ACL numbers (numbers 100 through 109.)

Note Once deleted, the ACLs cannot be retrieved. They must be reentered.The deployer might want to customize the NWSP My Firewall page to remove the Disable button or move the button to the Advanced Firewall page.

- Permit All Else or Deny All Else buttons

  When a subscriber profile contains one or more ACLs, an implicit default denies all other traffic not addressed by the existing ACLs. This deny-all-else implicit default is imposed by the Cisco router hosting the SSG or other cooperating network element.

  The Permit All Else or Deny All Else radio buttons offer a way for the subscriber to explicitly impose a default behavior. A deployer could decide not to display these buttons and allow the implicit behavior to operate. In this case, the page would not need the Deny button next to each application.

  When firewalls are enabled, the subscriber must consider whether to permit or deny traffic for each of the applications listed on the Firewall page. To do this, the subscriber can:

  – Consider each application separately, and select whether to permit or deny traffic for it.

  – Allow the default action to apply. They choose the default action by selecting either the Permit All Else or Deny All Else button.

- Applications/Protocols

  Lists the applications available for firewall settings. This list is configured by the deployer, as described in the "Configuring the Firewall Pages" section on page 10-18. For each application in the list, the subscriber can specify whether to deny or permit traffic. The ACLs that NWSP generates for this page will specify that all source and all destination IP addresses are subject to the control being defined in the ACL.

Note The subscriber can use the Advanced Firewall Page to obtain finer control in the ACLs, such as specifying specific IP addresses or ports that are subject to the control.

- Permit/Deny/Default buttons—The portal determines the initial setting for each item in the Application/Protocol list, as follows:

  – If no ACLs exist or if only one ACL exists in the subscriber's profile for the application/protocol, **Default** is selected. In a typical production deployment, most applications initially appear in the default state, because there are no specific ACLs in the subscriber profiles.

  – If the application/protocol has more than one ACL in the subscriber profile:

    If all ACLs have the same permission (that is, all are permit or all are deny), then the corresponding **Permit** or **Deny** is selected.

    Otherwise, if some ACLs specify permit and others deny, then **Default** is selected for that application.

First Time Access of My Firewall Page

The default state of a subscriber profile is one in which no ACLs are defined. The first time the subscriber goes to the My Firewall page, the settings are:

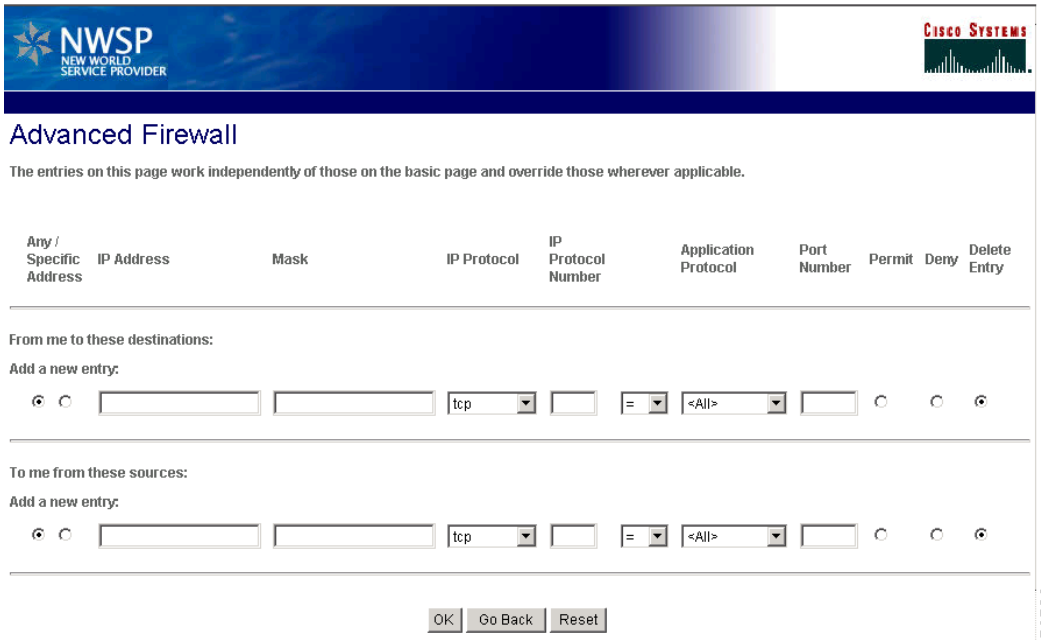
- Firewall Disabled—Indicating that there are no ACLs imposing any controls on traffic to or from the subscriber.
- Deny All Else—Ignore this button when firewalls are disabled.
- For all applications and protocols, the Default buttons are selected.

When ACLs exist in the subscriber profile, the SESM portal analyzes the ACLs and renders the page based on the ACLs, as described in the previous section.

Advanced Firewall Page

Figure 10-2 shows the Advanced Firewall page.

Figure 10-2 Advanced Firewall Page in NWSP



A description of the Advanced Firewall page follows.

- From me/To me entries—Subscribers can enter filters for upstream or downstream traffic.
  - From me to these destinations— These entries filter messages that the subscriber can initiate.The filters are based on the destination IP address, port, protocol, and application entered by the subscriber.

    The source is the subscriber. In the NWSP application, the source IP address for these entries is always set to “any” and source port is not specified. SESM developers can alter the Advanced Firewall JSP, adding fields to let the subscriber enter source IP address and port.

    The ACLs generated from these entries are known as inacls. The inacls specify filters for traffic travelling upstream into the SSG host or other routing device. For more information about inacls, see the “References for More Information about Access Control Lists” section on page 10-27.
  - To me from these sources—These ACLs filter messages that the subscriber can receive. The filters are based on the source IP address, port, protocol, or application entered by the subscriber.

    The destination is the subscriber. In the NWSP application, the destination IP address for these entries is always set to “any” and destination port is not specified. SESM developers can alter the Advanced Firewall JSP, adding fields to let the subscriber enter destination IP address and port.

    The ACLs generated from these entries are known as outacls. The outacls specify filters for traffic travelling downstream, out from the SSG host or other routing device. For more information about outacls, see the “References for More Information about Access Control Lists” section on page 10-27.

See the *Subscriber Edge Services Manager Web Developer Guide* and the SESM javadoc for more information about development options for JSP pages.

- Any/Specific Address—Indicates whether this ACL applies to any IP address or to specific IP addresses provided in the IP Address and Mask fields.
- IP Address and Mask—Specifies the source or destination IP address or address range that is being permitted or denied. Any ACL can specify IP addresses. Be sure to click the Specific Address radio button (above) if you are including an IP address.

  The mask for ACLs is inverted from the more familiar net mask. Bits in the mask are zero if the respective bit in the address should match. For example, if the ACL should filter addresses x.x.x.0, then the mask is 0.0.0.255.
- IP Protocol—Specifies the Internet protocol to filter:
  - Any IP—Filters all IP traffic.
  - tcp—Filters TCP traffic.
  - udp—Filters UDP traffic.
  - <0-255>—Filters traffic based on a protocol number specified in the IP Protocol Number field.
- IP Protocol Number—A number in the range 0 through 255. Protocol numbers refer to protocol configurations on the SSG host or other routing device. For example, TCP corresponds to the protocol number 6.
- Port Operator (=, !=, >, <)—Valid only when IP Protocol is TCP or UDP. The operator applies to the application protocol port number. (Each application protocol name is an alias to a port number.) The operator is used to compare the port in a packet to the port specified in the ACL.
  - = requires the port values to match
  - != requires that the port values not match
  - > requires that the port in the packet be greater than the port value specified in the ACL
  - < requires that the port in the packet be less than the port value specified in the ACL
- Application Protocol—Valid only when IP Protocol is TCP or UDP. An ACL can filter on a specific application carried on the TCP or UDP protocols. (On the SSG host or other routing device, each application is configured on a unique port. The ACLs filter on those port numbers or the aliases to those port numbers.) To specify the application port to filter, either:
  - Choose <0-65535> from this drop down list and provide the appropriate port number in the Port Number field.

    Choose an application from the Application drop down list. This list consists of all of the application port aliases configured in the Firewall MBean for TCP. The corresponding port number automatically appears in the Port Number field.

    In NWSP, the Application drop down list is meaningful only when IP Protocol is TCP. If IP Protocol is UDP, the subscriber must choose <0-65535> and explicitly enter the correct UDP port number in the Port Number field.

Note If the subscriber chooses an application from the list when IP Protocol is UDP, NWSP uses the port number that corresponds to the selected application. The deployer could customize NWSP to implement a separate drop down list for UDP applications. Alternatively, the deployer could remove the Internet Protocol and Internet Protocol Number fields, making TCP the default, in which case the existing list of applications would always be appropriate.

- Port Number—Valid only when IP Protocol is TCP or UDP and Application Protocol is <0-65535>. Enter the application port to filter. The port number must match the port configured for the application or protocol on the SSG host device or other cooperating network element.
- Permit—Adds the permit keyword to the generated ACL. The permit keyword allows a message to travel to its destination when the message matches the conditions in the ACL.
- Deny—Adds the deny keyword to the generated ACL. The deny keyword prevents a message from traveling to its destination when the message matches the conditions in the ACL..
- Delete Entry—Deletes this ACL from the subscriber profile. If this is a new entry, using this button has no effect on the subscriber profile.

Note To be added to the subscriber profile, a new entry must have either the Permit or Deny button selected.

- The three action buttons at the bottom of the window are:
  - OK—Adds the changes to the subscriber profile.
  - Go Back— It cancels any changes you made on the page since last using OK and returns to the My Firewall page
  - Reset—Cancels any changes you made on the page since last using OK and redisplays the page, showing the settings that currently exist in the subscriber profile.

Configuring the Firewall Pages

To configure the SESM firewall features, use the Firewall MBean, described in the "Firewall MBean" section on page 5-11.

Configuring the Application/Protocol List on the My Firewall Page

The Application/Protocol list on the My Firewall page is configured by the deployer as follows:

- The applications that appear in the list are configured in the Firewall MBean.
- The displayed text that represents an application in the list is obtained from a resource bundle in the portal application's directory.

Configuring the Drop Down Lists on the Advanced Firewall Page

The contents of the drop down lists on the Advanced Firewall page are configured by the deployer as follows:

- The IP Protocol drop down list shows the list of Internet protocols configured in the Firewall MBean.
- The Application/Protocol drop down list shows the port aliases configured for TCP applications in the Firewall MBean.

Note Developers can customize the Advanced Firewall JSP, hardcoding options rather than using the values obtained from the Firewall MBean.

ACLs Generated from Entries on the Firewall Pages

This section describes the ACLs that are automatically generated by the SESM portal. The section includes the following topics:

Viewing Generated ACLs

The deployer administrators can view all ACLs in a subscriber profile using CDAT. The ACLs appear in the Local RADIUS attribute field. The field contains all ACLs automatically generated by the SESM portal as a result of subscriber actions on the basic and advanced firewall pages, as well as any administrative ACLs directly entered by the deployer.

Depending upon CDAT privileges, which are assigned within CDAT, the administrator might be permitted to add, change and delete ACLs from the profile through CDAT.

NWSP does not provide a way for subscribers to view the generated ACLs.

Generated ACLs for the My Firewall Page

This section describes the ACLs that are automatically generated by NWSP from entries on the My Firewall page.The My Firewall page always results in ACLs that filter on:

- Any source and any destination address.
- A specific port number associated with the chosen application.

Subscribers must use the Advanced Firewall page to create ACLs that filter on specific addresses or multiple port numbers.

The ACLs generated from the My Firewall page are in the following form:

[inacl# | outacl#]*Number=permission protocol* any any eq *portNumber* [established]

Where:

- inacl# or outacl# is used, depending on the value of the direction attribute in the Firewall MBean.
  - inacl#—Applies the ACL to upstream traffic, which is traffic from the subscriber
  - outacl#—Applies the ACL to downstream traffic, which is traffic to the subscriber

  All TCP connections require a return path. A block on upstream traffic also affects the traffic traveling in the opposite direction, and vice-versa, if there is no ACL allowing established connections in the same direction as the block. For example, blocks on downstream traffic and an ACL allowing established connections on downstream traffic would allow the TCP upstream traffic.

  The choice of whether to control the in or out direction in the My Firewall ACLs is a matter of preference for the deployer to decide. All ACLs generated from the My Firewall page use the same direction.
- *Number* is in the range from 110 to 196. SESM assigns the ACL number as described in the "ACLs Generated from Entries on the Firewall Pages" section on page 10-19.

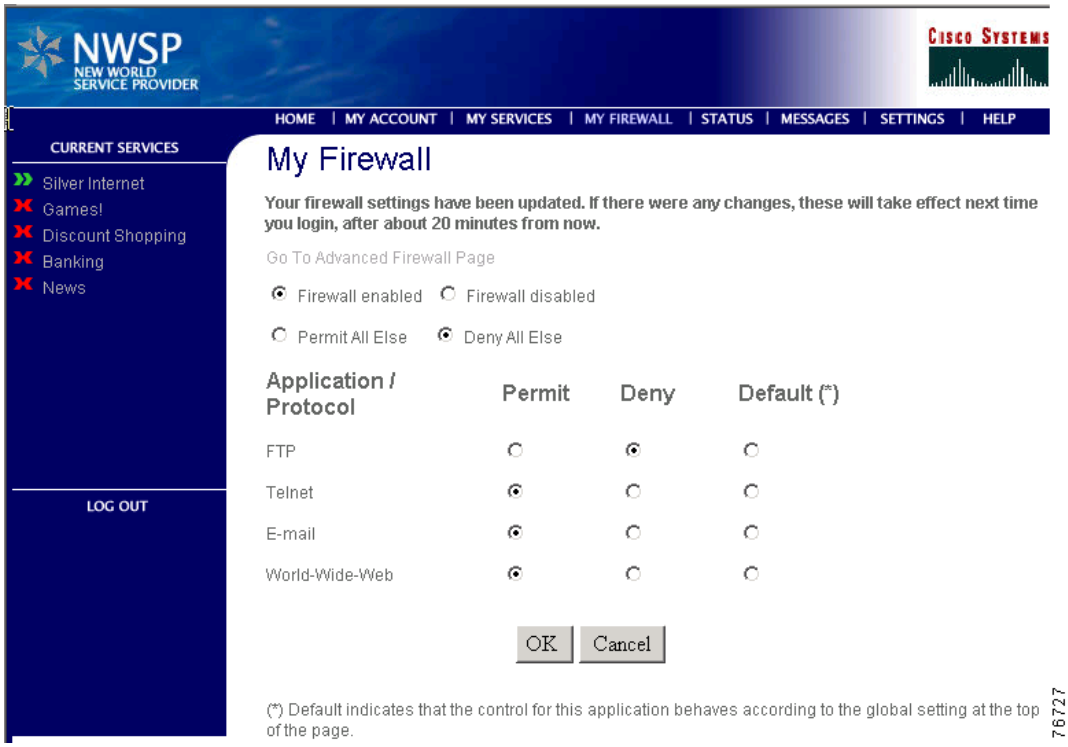
- *permission* is one of the following values:
  - permit
  - deny
- *protocol* is the configured protocol for the application, as defined in the Firewall MBean. Examples are tcp, udp, ip, and so on.
- "any any" are keywords in the source IP address and destination IP address fields. The keyword "any" specifies that all source and all destination IP addresses are subject to the control being defined in this ACL. Subscribers must use the Advanced Firewall page to create filters on specific IP addresses.
- "eq" is a keyword in the operator field. The keyword "eq" specifies that the filter applies to traffic whose source or destination port matches (equals) the value in *portNumber*. All ACLs generated from the My Firewall page use the "eq" keyword. Subscribers must use the Advanced Firewall page to specify other operators.
- *portNumber* is the port number related to the application, as defined in the Firewall MBean.
- established is a keyword used in the automatically generated ACLs for TCP return connections. In the Firewall MBean, an application named return is configured. Also in the Firewall MBean, the ReturnOption attribute specifies the permission to use in the TCP return connection ACLs.

For more information, see the "Firewall MBean" section on page 5-11.

My Firewall Example

Figure 10-3 shows an example My Firewall page.

Figure 10-3 My Firewall Example



The settings shown in Figure 10-3 result in the following ACLs:

Cisco_AV:ip:inacl#196=deny ip any any

Cisco_AV:ip:outacl#196=deny ip any any

Cisco_AV:ip:outacl#129=permit tcp any any established

Cisco_AV:ip:inacl#128=deny tcp any any eq 21

Cisco_AV:ip:inacl#128=permit tcp any any eq 23

Cisco_AV:ip:inacl#158=permit tcp any any eq 25

Cisco_AV:ip:inacl#158=permit tcp any any eq 109

Cisco_AV:ip:inacl#158=permit tcp any any eq 110

Cisco_AV:ip:inacl#158=permit tcp any any eq 143

Cisco_AV:ip:inacl#138=permit tcp any any eq 80

Cisco_AV:ip:inacl#138=permit tcp any any eq 443

Generated ACLs for the Advanced Firewall Page

This section describes the ACLs that are automatically generated by the SESM portal based on subscriber entries on the Advanced Firewall page. The ACLs generated from the Advanced Firewall page are in the following form:

{inacl# | outacl#}*Number=permission protocol* {any | *sourceIPaddress sourceMask*} [*operator port*] {any | *destinationIPaddress destinationMask*} [*operator port*] [established]

Where:

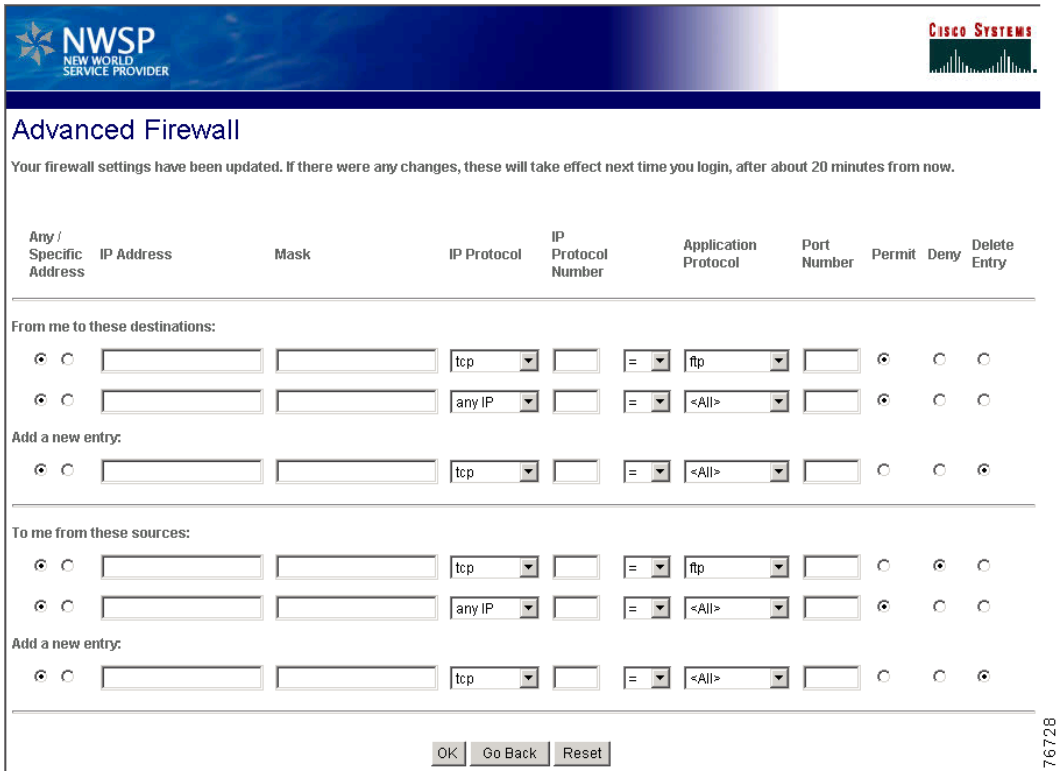
- inacl# or outacl# is used, depending on which section on the Advanced Firewall page the subscriber used:
  - inacl#—The subscriber entered the ACL in the "From me to these destinations" section. The ACL applies to upstream traffic, which is traffic from the subscriber.
  - outacl#—The subscriber entered the ACL in the "To me from these sources" section. The ACL applies to downstream traffic, which is traffic to the subscriber.

  All connections have a return path. A block on upstream traffic also affects the traffic traveling in the opposite direction, and vice-versa. The choice of whether to control the in or out direction in the Advanced Firewall is a matter of preference for the subscriber.
- *Number* is in the range from 110 to 196. SESM assigns the ACL number as described in the "ACLs Generated from Entries on the Firewall Pages" section on page 10-19.
- *permission* matches the choice selected by the subscriber on the Advanced Firewall page:
  - permit
  - deny
- *protocol* is the protocol that the subscriber selected from the drop down list on the Advanced Firewall page (ip, tcp, or udp.)
- *sourceIPaddress sourceMask*—The values entered by the subscriber in "To me from these sources" entries.
- *operator port*—The operator matches the subscriber selection on the Advanced Firewall page. Operator values in ACLs are: eq, ne, lt, gt.
- *destinationIPaddress destinationMask* —The values entered by the subscriber in "From me to these destinations" entries.
- *portNumber* is the port number related to the protocol, as defined in the Firewall MBean.

Advanced Firewall Example

Figure 10-4 shows sample settings on the Advanced Firewall page.

Figure 10-4 Advanced Firewall Example



The settings shown in Figure 10-4 result in the following ACLs:

Cisco_AV:ip:inacl#118=permit tcp any any eq 21

Cisco_AV:ip:outacl#118=deny tcp any eq 21 any

Cisco_AV:ip:inacl#193=permit ip any any

Cisco_AV:ip:outacl#193=permit ip any any

ACL Number Assignments

ACL numbers affect the order in which the SSG or other cooperating network element applies ACLs to the packet. Lower numbers are processed first. ACL processing stops the first time the ACL conditions match the packet information, and the deny or permit action in the matching ACL is carried out. The ACL number, therefore, can affect the filtering outcome.

ACL numbers are not permanent. Each time a subscriber uses the firewall pages to add or change ACL entries, the SESM portal reexamines all ACLs in the subscriber's profile and reassigns ACL numbers.

When the portal assigns ACL numbers to the automatically generated ACLs, it enforces the conventions and priorities described in Table 5-1.

Table 10-2 ACL Numbers for Automatically Generated ACLs

Priority	ACL Number	Explanation
Highest Priority	100 - 109	Reserved for administrative ACLs.
	110 - 119	ACLs from the Advanced Firewall page, when no application is specified. The explanation below for the 3rd digit applies to these ACLs as well.
	120 - 189	ACLs from the My Firewall page. The numbers within this range are assigned as follows: • 1st digit—Is always 1 (1xx) • 2nd digit—Indicates the number of ACL entries that currently exist in the subscriber's profile for the same application: – 12x—Applications with 1 ACL entry – 13x—Applications with 2 ACL entries – ...and so on – 18x—applications with 7 or more ACL entries • 3rd digit—Indicates how specific the IP addresses and ports are, with lower numbers (higher priority) given to ACLs containing the most specific address and port information: – 1x0—Not used. – If neither source nor destination addresses are "any": 1x1—Both source and destination ports are specified 1x2—Either source or destination port is specified 1x3—Neither source nor destination port is specified – If either source or destination addresses is "any" 1x4—Both source and destination ports are specified 1x5—Either source or destination port is specified 1x6—Neither source nor destination port is specified – If both source and destination ports are "any" 1x7—Both source and destination ports are specified 1x8—Either source or destination port is specified 1x9—Neither source nor destination port is specified Example: A profile contains two ACLs for the same application, both with specific source addresses, destination addresses of "any", and no ports. The ACL number for both is 136.
	190 not used 191 - 193	Internet protocol (IP) settings on the Advanced Firewall page: • 191—Both source and destination addresses are specified • 192—Either source or destination address is specified • 193—Neither source nor destination address is specified
Lowest priority	194 - 196	Internet protocol (IP) settings on the My Firewall page: • 194—Both source and destination addresses are specified • 195—Either source or destination address is specified • 196—Neither source nor destination address is specified

Subscriber Experiences with Personal Firewalls

This section describes how the personal firewall feature works from the subscriber point of view.

Creating Personal Firewalls

Subscribers create their personal firewalls by clicking radio buttons on the My Firewall page. The SESM portal creates the ACLs based on the information from the My Firewall page and adds the ACLs to the subscriber profile in the LDAP directory.

When New ACLs Take Effect

Although the LDAP directory is updated with the new information, the new ACLs do not take effect until a subscriber reauthenticates (logs out and logs in again). Also, the RDP cache must be refreshed, which by default takes 10 minutes. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time.

Interaction Between Entries on the My Firewall and Advanced Firewall Pages

The ACLs created from the Advanced Firewall pages have higher priority than ACLs created from the My Firewall page. Therefore, the subscriber might see filtering information on the My Firewall page that does not get applied to traffic because it is overridden by filters on the Advanced Firewall page.

Similarly, ACLs created by administrators (if they use the reserved ACL numbers 100 through 109) have the highest priority. Therefore, the subscriber might see filters on either the My Firewall or Advanced Firewall page that does not get applied to traffic because it is overridden by the administrative filters.

Safeguards

SESM and SSG include the following safeguards regarding firewalls:

- Subscribers cannot inadvertently deny themselves access to the SSG or the default network. SSG does not apply ACLs if the packet is going to the default network.
- Subscribers cannot inadvertently deny themselves access to open garden services. SSG does not use the subscriber's personal ACLs on packets coming from and going to open-garden services or in local-forwarding. (A set of host ACLs might apply in these cases.)
- ACLs generated from the Firewall pages are correctly formatted.
- Subscribers must have the SESMFirewall permission to use the firewall pages. Subscriber permissions are assigned in CDAT, in the user and group windows.
- Administrators must have the appropriate permissions to add or update user profiles. Administrator permissions are assigned in CDAT.

Deployer-Imposed Firewalls

This section describes how to configure and use the administrative firewall feature. It includes the following topics:

Restrictions

Deployer-imposed firewalls can be used in conjunction with the subscriber self-configured firewalls, with the following restrictions:

- You should test the ACLs before moving them to a production environment.

  In SESM Release 3.1(7), you must enter a correctly formatted ACL in CDAT. CDAT does not analyze or validate your ACL entry.

Caution The SSG does not allow a subscriber to authenticate if the profile contains an incorrectly formatted ACL.

- You should create ACLs using ACL numbers in the range from 100 to 109.

  The ACL numbers from 100 to 109 are reserved for administrator use. By using these numbers, you ensure that these ACLs are processed first, making them the highest priority.

  If you create ACLs in CDAT using ACL numbers in the range from 110 to 196, (the ACLs reserved for use by the subscriber self-configured ACLs), you risk the following:

  – You might interfere with the personal firewall settings created by the subscriber.

  – You provide the opportunity for the subscriber to reverse your settings.

Procedure for Entering ACLs in CDAT

To enter deployer-imposed ACLs, use the following procedure:

Step 1 Start the CDAT application.

Step 2 Log in as an administrator with permissions to modify subscriber profiles.

Step 3 Access the subscriber or group profile.

Step 4 Enter the ACLs in the Local RADIUS attribute field, using the format described in the following section.

Step 5 If a subscriber is currently logged into an SESM session, the new ACLs do not take effect until the subscriber reauthenticates (logs out and logs in again). Also, the RDP cache needs to be refreshed, which by default takes 10 minutes. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time.

ACL Format for CDAT Entries

This section describes the format of the firewall entries in the Local RADIUS attribute field in CDAT. The ACLs entered in CDAT can use the full range of ACL options as described in the Cisco IOS documentation for extended ACLs.

The general format for the Local RADIUS attribute field is:

attribute:*value*

In the case of the firewall ACL entries:

- *attribute* is Cisco_AV
- *value* is the ACL whose format is described below

The format of the ACLs entered by administrators is:

Cisco_AV:ip:*direction*acl#*ACLnumber=permission protocol source destination*

Where:

- *direction* is one of the following:
  - in
  - out
- acl# is a required string
- *ACLnumber* is in the range from 100 to 109. The numbers indicate priority in the ACL evaluation. ACLs with the lowest numbers are analyzed first. The order is important because ACL processing stops when the first match occurs.

  ACLs whose numbers are in the range 100 to 109 will have higher priority than any ACLs created by subscribers using the My Firewall page. (The range of ACL numbers reserved for use by the My Firewall page is 110 to 196.)

  ACLs whose numbers are in the range 100 to 109 cannot be modified by the subscriber (because the My Firewall page will not modify ACLs whose numbers are in that range), although the subscriber can delete those ACLs along with all others with the Disable Firewall button.
- *permission* is one of the following values: permit or deny
- *protocol* is the configured protocol for the application, as defined in the Firewall MBean. Examples are tcp, udp, ip, and so on.
- *source* and *destination* are in the form:

  {any | *IPaddress mask*} [*portOperator portNumber*]

  where *portOperator* values are: lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). The range operator requires two port numbers. All other operators require one port number.

Example

The following examples, using ACL number 100, were set by an administrator in CDAT.

Cisco_AV:ip:inacl#100=permit tcp any 10.0.0.0 0.0.0.0 eq 80

Cisco_AV:ip:outacl#100=permit tcp any any established

Note There is an implicit deny at the end of an ACL list. When an ACL list exists, only explicitly permitted traffic is permitted.

References for More Information about Access Control Lists

The SESM firewall feature creates extended ACLs. For more information about ACL formats and processing, refer to the Cisco IOS documentation on extended ACLs. The following references point to documentation for Cisco IOS Release 12.2:

- Configuration Guide—In the *Configuring IP Services* guide, see the “Filtering IP Packets Using Access Lists” section. The online link is:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm#xtocid14

- Command reference—In the *Cisco IOS IP Command Reference, Volume 1 of 3, Addressing and Services*, see the "IP Services Commands" section. The online link is:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/1rfip1.htm

Multikey Authentication

To implement multikey authentication:

1. Add the authentication fields to the portal logon page.

   This step requires portal customization. SESM is installed with an example 3-field authentication page that you can implement The example authentication fields are: username, password and telephone number. (Telephone number is the RADIUS attribute CALLING_STATIOIN_ID).

   To change the NWSP logon page to prompt for these three keys and process them:

   a. Edit nwsp/webapp/WEB-INF/web.xml.

   b. Change the following line:

      <servlet-class>com.cisco.sesm.webapp.control.AccountLogonControl</servlet-class>

      to: <servlet-class>com.cisco.sesm.webapp.control.AccountLogon3KeyControl</servlet-class>

   c. Change the following line:

      <param-value>/pages/accountLogon.jsp</param-value>

      to: <param-value>/pages/accountLogon3Key.jsp</param-value>

2. In LDAP mode, configure RDP to authenticate on the same fields that are specified on the logon page.

   You can configure RDP to use any number of fields for authentication. Any standard RADIUS attribute field is a valid key.

   a. Edit the DESSAuthenticationHandler Mbean from the RDP management console, or manually edit rdp.xml.

   b. Add items to the AuthAttribute attribute. To configure with the installed example in NWSP that uses three keys, make sure the following items are listed in AuthAttribute, in this order: USER_PASSWORD, CALLING_STATION_ID. (The USER_NAME attribute is always used for authentication and should not appear in the AuthAttribute array.)

3. In RADIUS mode, logic to authenticate with multiple keys must exist in the RADIUS server you are using. Verify that this logic exists with your RADIUS server vendor.

4. Make sure that the subscriber profiles includes the values against which to authenticate. In LDAP mode, administrators can enter the APN and NAS identifier attributes as group values. See the *Cisco Distributed Administration Tool Guide* for more information.

Quality of Service

Quality of Service (QoS) features control IP traffic transmission rates. The QoS features in SESM deployments are implemented using SSG hierarchical policing features. See the SSG documentation for information about enabling and configuring hierarchical policing. See the "Related Documentation" section on page -xv for an URL to the online location of SSG documents.

SSG supports per-subscriber and per-service hierarchical policing. The parameters that implement these policies are specified in subscriber and service profiles:

- To implement per-subscriber policies—Use the Q attribute in the subscriber profiles.
- To implement per-service policies—Use the Q attribute in a service profile.

See the "Configuring Service Profiles" section on page C-6 and the "Configuring Subscriber Profiles" section on page C-11 for a summary of RADIUS profile formats. See the *Cisco Distributed Administration Tool Guide* for information about creating profiles in an LDAP directory.