CHAPTER 12

Configuring Objects

Objects are reusable components for use in your configuration. They can be defined and used in ASA 1000V configurations in the place of inline IP addresses. Objects make it easy to maintain your configurations because you can modify an object in one place and have it be reflected in all other places that are referencing it. Without objects you would have to modify the parameters for every feature when required, instead of just once. For example, if a network object defines an IP address and subnet mask, and you want to change the address, you only need to change it in the object definition, not in every feature that refers to that IP address.

This chapter describes how to configure objects, and it includes the following sections:

Note For other objects, see the following sections:

- Class Maps—See Chapter 22, "Getting Started with Application Layer Protocol Inspection."
- Inspect Maps—See Chapter 22, "Getting Started with Application Layer Protocol Inspection."
- TCP Maps—See the "Configuring Connection Settings" section on page 27-5.

Configuring Network Objects and Groups

This section describes how to use network objects and groups and includes the following topics:

Network Object Overview

A network object can contain a host, a network IP address, or a range of IP addresses, and it can also enable NAT rules. (See Chapter 15, "Configuring Network Object NAT," for more information.)

Network objects let you predefine host and network IP addresses so that you can streamline subsequent configurations. For example, when you configure a security policy, such as an access rule or a AAA rule, you can choose these predefined addresses instead of typing them in manually. Moreover, if you change the definition of an object, the change is inherited automatically by any rules that use the altered object.

You can add network objects manually, or you can let ASDM automatically create objects from existing configurations, such as access rules and AAA rules. If you edit one of these derived objects, it persists even if you later delete the rule that used it. Otherwise, derived objects only reflect the current configuration if you refresh.

A network object group is a group that contains multiple hosts and networks together, so a network object group can also contain other network object groups. You can also specify a network object group as the source address or destination address in an access rule.

When you are configuring rules, the ASDM window includes an Addresses side pane that shows available network objects and network object groups; you can add, edit, or delete objects directly in the Addresses pane. You can also drag additional network objects and groups from the Addresses pane to the source or destination of a selected access rule.

Also, you can create a named object within a network object group, which provides the ability to modify an object in one place and have it be reflected in all other places that are referencing it. Otherwise, modifying an object requires a manual process of changing all IP address and mask pairs in the configuration. In addition, you can attach a named object to (or detach it from) one or more object groups to ensure that objects are not duplicated but are used efficiently. The object can then be re-used and cannot be deleted if other modules are still referencing it.

Configuring a Network Object

For information about network objects, see the "Network Object Overview" section on page 12-2.

To add or edit a network object, perform the following steps:

Step 1 Choose **Configuration > Firewall > Objects > Network Objects/Group**.

Step 2 Click **Add**, and choose **Network Object** to add a new object, or choose an existing object to edit, and click **Edit**.

You can also add or edit network objects from the Addresses side pane in a rules window or when you are adding a rule.

To find an object in the list, enter a name or IP address in the Filter field, and click **Filter**. The wildcard characters asterisk (*) and question mark (?) are allowed.

The Add/Edit Network Object dialog box appears.

Step 3 Fill in the following values:

- Name—The object name. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must contain 64 characters or fewer.
- Type—Either Network, Host, or Range.
- IP Address—Either a host or network address. If you select Range as the object type, the IP Address field changes to allow you to enter a Start Address and an End address.

- Netmask—Enter the subnet mask.
- Description—(Optional) The description of the network object (up to 200 characters in length).

Note To add NAT rules to the network object, see Chapter 15, "Configuring Network Object NAT," for more information.

Step 4 Click **OK**.

Step 5 Click **Apply** to save the configuration.

You can now use this network object when you create a rule. If you edited an object, the change is inherited automatically by any rules using the object.

Note You cannot delete a network object that is in use.

Configuring a Network Object Group

For information about network object groups, see the "Network Object Overview" section on page 12-2.

To configure a network object or a network object group, perform the following steps:

Step 1 Choose **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 2 Click click **Add > Network Object Group** to add either a new object or a new object group.

You can also add or edit network object groups from the Addresses side pane in a rules window, or when you add a rule.

To find an object in the list, enter a name or IP address in the Filter field, and click Filter. The wildcard characters asterisk (*) and question mark (?) are allowed.

The Add Network Object Group dialog box appears.

Step 3 In the Group Name field, enter a group name.

Use characters a to z, A to Z, 0 to 9, a period, a comma, a dash, or an underscore. The name must contain 64 characters or fewer.

Step 4 (Optional) In the Description field, enter a description, up to 200 characters in length.

Step 5 You can add existing objects or groups to the new group (nested groups are allowed), or you can create a new address to add to the group:

- To add an existing network object or group to the new group, double-click the object in the Existing Network Objects/Groups pane.

  You can also select the object, and then click **Add**. The object or group is added to the right-hand Members in Group pane.

- To add a new address, fill in the values under the Create New Network Object Member area, and click **Add**.

  The object or group is added to the right-hand Members in Group pane. This address is also added to the network object list.

To remove an object, double-click the object in the Members in Group pane, or select the object and click **Remove**.

Step 6 After you add all the member objects, click OK.

You can now use this network object group when you create a rule. For an edited object group, the change is inherited automatically by any rules using the group.

Note You cannot delete a network object group that is in use.

Using Network Objects and Groups in a Rule

When you create a rule, you can enter an IP address manually, or you can browse for a network object or group to use in the rule. To use a network object or group in a rule, perform the following steps:

Step 1 From the rule dialog box, click the **...** browse button next to the source or destination address field.

The Browse Source Address or Browse Destination Address dialog box appears.

Step 2 You can either add a new network object or group, or choose an existing network object or group by double-clicking it.

To find an object in the list, enter a name or IP address in the Filter field, and click **Filter**. The wildcard characters asterisk (*) and question mark (?) are allowed.

- To add a new network object, see the "Configuring a Network Object" section on page 12-2.
- To add a new network object group, see the "Configuring a Network Object Group" section on page 12-3.

After you add a new object or double-click an existing object, it appears in the Selected Source/Destination field. For access rules, you can add multiple objects and groups in the field, separated by commas.

Step 3 Click **OK**.

You return to the rule dialog box.

Viewing the Usage of a Network Object or Group

To view which rules use a network object or group, in the Configuration > Firewall > Objects > Network Objects/Group pane, click the magnifying glass Find icon.

The Usages dialog box appears, listing all the rules currently using the network object or group. This dialog box also lists any network object groups that contain the object.

Configuring Service Objects and Service Groups

This section describes how to configure service objects and service groups, and it includes the following topics:

Information about Service Objects and Service Groups

A service object contains a protocol and optional (source and/or destination) port and an associated description. You create and use a service object in ASA 1000V configurations in the place of an inline IP address in a configuration. You can define an object with a particular IP address/mask pair or a protocol (and optionally a port) and use this object in several configurations.

The advantage to using an object is that whenever you want to modify the configurations related to this IP address or protocol, you do not need to search the running configuration and modify the rules in all places. You can modify the object once, and then the change automatically applies to all rules that use this object.

Service objects can be used in NAT configurations, access lists, and object groups.

You can associate multiple services into a named service group. You can specify any type of protocol and service in one group or create service groups for each of the following types:

- TCP ports
- UDP ports
- ICMP types
- IP protocols

Multiple service groups can be nested into a “group of groups” and used as a single group.

You can use a service group for most configurations that require you to identify a port, ICMP type, or protocol. When you are configuring NAT or security policy rules, the ASDM window even includes a Services pane at the right that shows available service groups and other global objects; you can add, edit, or delete objects directly in the Services pane.

You can also create a named object in a service object group, which provides the ability to modify an object in one place and have it be reflected in all other places that are referencing it. Otherwise, modifying an object requires a manual process of changing all IP address and mask pairs in the configuration. In addition, you can attach a named object to (or detach a named object from) one or more object groups to ensure that objects are not duplicated but are used efficiently. (A named service object may be attached to or detached from a service object group only, not an object group of another type.) The object can then be re-used and cannot be deleted if other modules are still referencing it.

When you delete a service object or service group, it is removed from all service groups and access rules where it is used.

If a service group is used in an access rule, do not remove the service group unless you want to delete the access rule. A service group used in an access rule cannot be made empty.

For information about adding or editing a service object, see the “Adding and Editing a Service Object” section on page 12-6.

For information about adding or editing a service group, see the "Adding and Editing a Service Group" section on page 12-7.

Adding and Editing a Service Object

This section includes the following topics:

Adding a Service Object

To add a service object, perform the following steps:

Step 1 In the Configuration > Firewall > Objects > Service Object/Group pane, click **Add**.

Step 2 Choose **Service Object** from the drop-down list.

Step 3 In the name field, enter a name for the service object. Use characters a to z, A to Z, 0 to 9, a period, a dash, a comma, or an underscore. The name must be 64 characters or fewer.

Step 4 From the Service Type field, choose the desired type: tcp, udp, icmp, or icmp6 protocol.

Step 5 (Optional) If you chose tcp or udp as the Service Type, enter the following:

- Destination Port/Range
- Source Port/Range—Lists the protocol source ports/ranges.
- Description—Lists the service group description.

Step 6 (Optional) If you chose icmp or icmp6 as the Service Type, enter the following:

- ICMP type—Lists the service group ICMP type.
- Description—Lists the service group description.

Step 7 If you chose protocol as the Service Type, enter the following:

- Protocol—Lists the service group protocol.
- Description—Lists the service group description.

Step 8 Click OK to save the configuration.

Editing a Service Object

To edit a service object, perform the following steps:

Step 1 Go to **Configuration > Firewall > Objects > Service Object/Group** pane.

Step 2 Select an existing service object under the Name column.

Step 3 Click **Edit**.

Depending upon the type of a service object you choose edit, the appropriate Edit window appears:

- Service Object—Edit Service Object window appears.

- Service Group—Edit Service Group appears.
- Protocol Group—Edit Protocol Group window appears.

Step 4 Enter the necessary changes.

Step 5 Click OK to save the configuration.

Note You can also click Delete to delete a service object.

Adding and Editing a Service Group

You can associate multiple service objects into a named service group. You can specify any type of protocol and service in one group or create service groups for each of the following types:

- TCP ports
- UDP ports
- ICMP types
- IP protocols

Multiple service groups can be nested into a "group of groups" and used as a single group.

This section includes the following topics:

- Adding a Service Group, page 12-7
- Editing a Service Group, page 12-8

Adding a Service Group

To add a service object or service group, perform the following steps:

Step 1 In the Configuration > Firewall > Objects > Service Object/Group pane, click **Add**.

Step 2 Choose **Service Group** from the drop-down list.

The Add Service Group dialog box appears.

Step 3 In the Name field, enter a name for the new service group. The name can be up to 64 characters in length and must be unique for all object groups. A service group name cannot share a name with a network object group.

Step 4 In the Description field, enter a description for this service group, up to 200 characters in length.

Step 5 By default you can add a service group from an existing service/service group. Select the group from the Name field, and click Add to add the service to the group.

Optionally, you can create a new member:

- Click the **Create new member** radio button.
- Select the Service type from the drop-down list.
- Enter the destination port/range.
- Enter the source port/range.

Step 6 Click Add to add the new service.

Step 7 Click OK to save the configuration.

Editing a Service Group

To edit a service group, perform the following steps:

Step 1 Go to the **Configuration > Firewall > Objects > Service Object/Group** pane.

Step 2 Select the existing service group that you want to edit, and click **Edit**.

Depending upon the type of a service object you choose edit, the appropriate windows appears:

- Service Object—Edit Service Object window appears.
- Service Group—Edit Service Group appears.
- Protocol Group—Edit Protocol Group window appears.

Step 3 Enter the necessary changes.

Step 4 Click OK to save the configuration.

Note You can also click Delete to delete a service group. When you delete a service group, it is removed from all service groups where it is used. If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.

The Configuration > Global Objects > Service Groups > Add/Edit Service Group dialog box lets you assign services to a service group. This dialog box name matches the type of service group you are adding; for example, if you are adding a TCP service group, the Add/Edit TCP Service Group dialog box is shown.

Fields

- Group Name—Enter the group name, up to 64 characters in length. The name must be unique for all object groups. A service group name cannot share a name with a network object group.
- Description—Enter a description of this service group, up to 200 characters in length.
- Existing Service/Service Group—Identifies items that can be added to the service group. Choose from already defined service groups, or choose from a list of commonly used port, type, or protocol names.
  - Service Groups—The title of this table depends on the type of service group you are adding. It includes the defined service groups.
  - Predefined—Lists the predefined ports, types, or protocols.
- Create new member—Lets you create a new service group member.

  - Service Type—Lets you select the service type for the new service group member. Service types include TCP, UDP, TCP-UDP, ICMP, and protocol.
  - Destination Port/Range—Lets you enter the destination port or range for the new TCP, UDP, or TCP-UDP service group member.
  - Source Port/Range—Lets you enter the source port or range for the new TCP, UDP, or TCP-UDP service group member.
  - ICMP Type—Lets you enter the ICMP type for the new ICMP service group member.
  - Protocol—Lets you enter the protocol for the new protocol service group member.
- Members in Group—Shows items that are already added to the service group.
- Add—Adds the selected item to the service group.
- Remove—Removes the selected item from the service group.

Browse Service Groups

The Browse Service Groups dialog box lets you choose a service group. This dialog box is used in multiple configuration screens and is named appropriately for your current task. For example, from the Add/Edit Access Rule dialog box, this dialog box is named “Browse Source Port” or “Browse Destination Port.”

Fields

- Add—Adds a service group.
- Edit—Edits the selected service group.
- Delete—Deletes the selected service group.
- Find—Filters the display to show only matching names. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
  - Filter field—Enter the name of the service group. The wildcard characters asterisk (*) and question mark (?) are allowed.
  - Filter—Runs the filter.
  - Clear—Clears the Filter field.
- Type—Lets you choose the type of service group to show, including TCP, UDP, TCP-UDP, ICMP, and Protocol. To view all types, choose **All**. Typically, the type of rule you configure can only use one type of service group; you cannot select a UDP service group for a TCP access rule.
- Name—Shows the name of the service group. Click the plus (+) icon next to the name of an item to expand it. Click the minus (-) icon to collapse the item.

Guidelines and Limitations for Objects and Groups

The following guidelines and limitations apply to object groups:

- Objects and object groups share the same name space.

- Object groups must have unique names. While you might want to create a network object group named “Engineering” and a service object group named “Engineering,” you need to add an identifier (or “tag”) to the end of at least one object group name to make it unique. For example, you can use the names “Engineering_admins” and “Engineering_hosts” to make the object group names unique and to aid in identification.
- You cannot remove an object group or make an object group empty if it is used in a command.
- Unique qualified names for object groups are supported only in the VNMC mode on the ASA 1000V.

Configuring Regular Expressions

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so that you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match a URL string inside an HTTP packet. This section describes how to create a regular expression and includes the following topics:

Creating a Regular Expression

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match a URL string inside an HTTP packet.

Guidelines

Use **Ctrl+V** to escape all of the special characters in the CLI, such as question mark (?) or a tab. For example, type **d[Ctrl+V]?g** to enter **d?g** in the configuration.

See the **regex** command in the command reference for performance impact information when matching a regular expression to packets.

Note As an optimization, the ASA 1000V searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like “http://”, be sure to search for “http:/” instead.

Table 12-1 lists the metacharacters that have special meanings.

Table 12-1 regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp*)	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x*} or {*x*,}	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc*]	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc*]	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a*-*c*]	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [**a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
“”	Quotation marks	Preserves trailing or leading spaces in the string. For example, **“ test”** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.

Table 12-1 regex Metacharacters (continued)

Character	Description	Notes
\	Escape character	When used with a metacharacter, matches a literal character. For example, \[matches the left square bracket.
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

Detailed Steps

Configuration > Global Objects > Regular Expressions > Add/Edit a Regular Expression Fields

- Name—Enter the name of the regular expression, up to 40 characters in length.
- Value—Enter the regular expression, up to 100 characters in length. You can enter the text manually, using the metacharacters in Table 12-1, or you can click **Build** to use the Building a Regular Expression dialog box.
- Build—Helps you build a regular expression using the Building a Regular Expression dialog box.
- Test—Tests a regular expression against some sample text.

Building a Regular Expression

The Configuration > Global Objects > Regular Expressions > Add/Edit a Regular Expression > Build Regular Expression dialog box lets you construct a regular expression out of characters and metacharacters. Fields that insert metacharacters include the metacharacter in parentheses in the field name.

See Table 12-1 on page 12-11 for more information about metacharacters.

Detailed Steps

Build Snippet—This area lets you build text snippets of regular text or lets you insert a metacharacter into the Regular Expression field.

- Starts at the beginning of the line (^)—Indicates that the snippet should start at the beginning of a line, using the caret (^) metacharacter. Be sure to insert any snippet with this option at the beginning of the regular expression.
- Specify Character String—Enter a text string manually.
  - Character String—Enter a text string.

  - Escape Special Characters—If you entered any metacharacters in your text string that you want to be used literally, check this box to add the backslash (\) escape character before them. for example, if you enter “example.com,” this option converts it to “example\.com”.
  - Ignore Case—If you want to match upper and lower case characters, this check box automatically adds text to match both upper and lower case. For example, entering “cats” is converted to “[cC][aA][tT][sS]”.
- Specify Character—Lets you specify a metacharacter to insert in the regular expression.
  - Negate the character—Specifies not to match the character you identify.
  - Any character (.)—Inserts the period (.) metacharacter to match any character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
  - Character set—Inserts a character set. Text can match any character in the set. Sets include:

    [0-9A-Za-z]

    [0-9]

    [A-Z]

    [a-z]

    [aeiou]

    [\n\f\r\t] (which matches a new line, form feed, carriage return, or a tab)

    For example, if you specify [0-9A-Za-z], then this snippet will match any character from A to Z (upper or lower case) or any digit 0 through 9.
  - Special character—Inserts a character that requires an escape, including \, ?, *, +, |, ., [, (, or ^. The escape character is the backslash (\), which is automatically entered when you choose this option.
  - Whitespace character—Whitespace characters include \n (new line), \f (form feed), \r (carriage return), or \t (tab).
  - Three digit octal number—Matches an ASCII character as octal (up to three digits). For example, the character \040 represents a space. The backslash (\) is entered automatically.
  - Two digit hexadecimal number—Matches an ASCII character using hexadecimal (exactly two digits). The backslash (\) is entered automatically.
  - Specified character—Enter any single character.
- Snippet Preview—*Display only.* Shows the snippet as it will be entered in the regular expression.
- Append Snippet—Adds the snippet to the end of the regular expression.
- Append Snippet as Alternate—Adds the snippet to the end of the regular expression separated by a pipe (|), which matches either expression it separates. For example, **dog|cat** matches dog or cat.
- Insert Snippet at Cursor—Inserts the snippet at the cursor.

Regular Expression—This area includes regular expression text that you can enter manually and build with snippets. You can then select text in the Regular Expression field and apply a quantifier to the selection.

- Selection Occurrences—Select text in the Regular Expression field, click one of the following options, and then click **Apply to Selection**. For example, if the regular expression is “test me,” and you select “me” and apply **One or more times**, then the regular expression changes to “test (me)+”.
  - Zero or one times (?)—A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose.

  - One or more times (+)—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
  - Any number of times (*)—A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, etc.
  - At least—Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.
  - Exactly—Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.
  - Apply to Selection—Applies the quantifier to the selection.
- Test—Tests a regular expression against some sample text.

Testing a Regular Expression

The Configuration > Global Objects > Regular Expressions > Add/Edit a Regular Expression > Test Regular Expression dialog box lets you test input text against a regular expression to make sure it matches as you intended.

Detailed Steps

- Regular Expression—Enter the regular expression you want to test. By default, the regular expression you entered in the Add/Edit Regular Expression or Build Regular Expression dialog box is input into this field. If you change the regular expression during your testing, and click **OK**, the changes are inherited by the Add/Edit Regular Expression or Build Regular Expression dialog boxes. Click **Cancel** to discard your changes.
- Test String—Enter a text string that you expect to match the regular expression.
- Test—Tests the Text String against the Regular Expression,
- Test Result—*Display only.* Shows if the test succeeded or failed.

Creating a Regular Expression Class Map

A regular expression class map identifies one or more regular expressions. You can use a regular expression class map to match the content of certain traffic; for example, you can match URL strings inside HTTP packets.

Detailed Steps

Configuration > Global Objects > Regular Expressions > Add/Edit Regular Expression Class Map dialog box Fields:

- Name—Enter a name for the class map, up to 40 characters in length. The name “class-default” is reserved. All types of class maps use the same name space, so you cannot reuse a name already used by another type of class map.
- Description—Enter a description, up to 200 characters in length.
- Available Regular Expressions—Lists the regular expressions that are not yet assigned to the class map.
  - Edit—Edits the selected regular expression.
  - New—Creates a new regular expression.
- Add—Adds the selected regular expression to the class map.

- Remove—Removes the selected regular expression from the class map.
- Configured Match Conditions—Shows the regular expressions in this class map, along with the match type.
  - Match Type—Shows the match type, which for regular expressions is always a positive match type (shown by the icon with the equal sign (=)) the criteria. (Inspection class maps allow you to create negative matches as well (shown by the icon with the red circle)). If more than one regular expression is in the class map, then each match type icon appears with "OR" next it, to indicate that this class map is a "match any" class map; traffic matches the class map if only one regular expression is matched.
  - Regular Expression—Lists the regular expression names in this class map.

Configuring Time Ranges

Use the Configuration > Global Objects > Time Ranges pane to create a reusable component that defines starting and ending times that can be applied to various security features. Once you have defined a time range, you can select the time range and apply it to different options that require scheduling.

The time range feature lets you define a time range that you can attach to traffic rules, or an action. For example, you can attach an access list to a time range to restrict access to the ASA 1000V.

A time range consists of a start time, an end time, and optional recurring entries.

For detailed steps on adding a time range to an access rule, see the "Adding a Time Range to an Access Rule" section on page 12-15.

Note Creating a time range does not restrict access to the device. This pane defines the time range only.

Fields

- Name—Specifies the name of the time range.
- Start Time—Specifies when the time range begins.
- End Time—Specifies when the time range ends.
- Recurring Entries—Specifies further constraints of active time of the range within the start and stop time specified.

Add/Edit Time Range

The Configuration > Global Objects > Time Ranges > Add/Edit Time Range dialog box lets you define specific times and dates that you can attach to an action. For example, you can attach an access list to a time range to restrict access to the ASA 1000V. The time range relies on the system clock of the ASA 1000V; however, the feature works best with NTP synchronization.

Adding a Time Range to an Access Rule

You can add a time range to an ACL to specify when traffic can be allowed or denied through an interface.

To add a time range to an ACL, perform the following steps:

Step 1 Choose **Configuration > Firewall > Access Rules**.

Step 2 Click **Add**. The Add Access Rule window appears.

Step 3 From the Interface drop down list, choose the desired interface.

The management interface is for management only and cannot be used to configure an access rule.

Step 4 Click **Permit** or **Deny** to permit or deny the action.

Step 5 In the Source field, enter an IP address.

Step 6 In the Destination field, enter an IP address.

Step 7 Select the service type.

Step 8 Click **More Options** to expand the list.

Step 9 To the right of the Time Range drop down list, click the browse button.

The Browse Time Range window appears.

Step 10 Click **Add**.

The Add Time Range window appears.

Step 11 In the Time Range Name field, enter a time range name, with no spaces.

Step 12 Choose the Start Time and the End Time by doing one of the following:

a. Allow the default settings, in which the Start Now and the Never End radio buttons are checked.

b. Apply a specific time range by clicking the **Start at** and **End at** radio buttons and selecting the specified start and stop times from the lists.

The time range is inclusive of the times that you enter.

Step 13 (Optional) To specify additional time constraints for the time range, such as specifying the days of the week or the recurring weekly interval in which the time range will be active, click **Add**, and do one of the following:

a. Click **Specify days of the week and times on which this recurring range will be active**, and choose the days and times from the lists, and click **OK**.

b. Click **Specify a weekly interval when this recurring range will be active**, and choose the days and times from the lists, and click **OK**.

Step 14 Click OK to apply the time range.

Step 15 Click OK to apply the access rule.

Note Creating a time range does not restrict access to the device. This pane defines the time range only.

Add/Edit Time Range Field Descriptions

- Time Range Name—Specifies the name of the time range. The name cannot contain a space or quotation mark, and must begin with a letter or number.
- Start now/Started—Specifies either that the time range begin immediately or that the time range has begun already. The button label changes based on the Add/Edit state of the time range configuration. If you are adding a new time range, the button displays “Start Now.” If you are editing a time range for which a fixed start time has already been defined, the button displays “Start Now.” When editing a time range for which there is no fixed start time, the button displays “Started.”

- Start at—Specifies when the time range begins.
  - Month—Specifies the month, in the range of January through December.
  - Day—Specifies the day, in the range of 01 through 31.
  - Year—Specifies the year, in the range of 1993 through 2035.
  - Hour—Specifies the hour, in the range of 00 through 23.
  - Minute—Specifies the minute, in the range of 00 through 59.
- Never end—Specifies that there is no end to the time range.
- End at (inclusive)—Specifies when the time range ends. The end time specified is inclusive. For example, if you specified that the time range expire at 11:30, the time range is active through 11:30 and 59 seconds. In this case, the time range expires when 11:31 begins.
  - Month—Specifies the month, in the range of January through December.
  - Day—Specifies the day, in the range of 01 through 31.
  - Year—Specifies the year, in the range of 1993 through 2035.
  - Hour—Specifies the hour, in the range of 00 through 23.
  - Minute—Specifies the minute, in the range of 00 through 59.
- Recurring Time Ranges—Configures daily or weekly time ranges.
  - Add—Adds a recurring time range.
  - Edit—Edits the selected recurring time range.
  - Delete—Deletes the selected recurring time range.

Add/Edit Recurring Time Range

The Configuration > Global Objects > Time Ranges > Add/Edit Time Range > Add/Edit Periodic Time Range pane lets you fine time ranges further by letting you configure them on a daily or weekly basis.

For detailed steps on adding a recurring time range to an access rule, see the "Adding a Time Range to an Access Rule" section on page 12-15.

Note Creating a time range does not restrict access to the device. This pane defines the time range only.

Add/Edit Recurring Time Range Field Descriptions

- Days of the week
  - Every day—Specifies every day of the week.
  - Weekdays—Specifies Monday through Friday.
  - Weekends—Specifies Saturday and Sunday.
  - On these days of the week—Lets you choose specific days of the week.
  - Daily Start Time—Specifies the hour and the minute that the time range begins.
  - Daily End Time (inclusive) area—Specifies the hour and the minute that the time range ends. The end time specified is inclusive.
- Weekly Interval

- From—Lists the day of the week, Monday through Sunday.
- Through—Lists the day of the week, Monday through Sunday.
- Hour—Lists the hour, in the range of 00 through 23.
- Minute—Lists the minute, in the range of 00 through 59.