```
<!--
The following security-constraint excludes access to the patterns
and method combinations defined by the two contained web-re-
source-collections. The first collection excludes access by all
methods except GET and POST, while the second collection excludes
access by all HTTP methods.
-->
<security-constraint>
   <web-resource-collection>
      <web-resource-name>sc1.c1</web-resource-name>
      <url-pattern>/a/*</url-pattern>
      <url-pattern>/b/*</url-pattern>
      <url-pattern>/a</url-pattern>
      <url-pattern>/b</url-pattern>
      <http-method-omission>GET</http-method-omission>
      <http-method-omission>POST</http-method-omission>
   </web-resource-collection>

   <web-resource-collection>
      <web-resource-name>sc1.c2</web-resource-name>
      <url-pattern>*.asp</url-pattern>
   </web-resource-collection>
   <auth-constraint/>
</security-constraint>

<!--
The following security-constraint restricts access to the pat-
terns and method combinations defined by the two contained web-
resource-collections to callers in role R1 who connect using a
confidential transport.
-->
<security-constraint>
   <web-resource-collection>
      <web-resource-name>sc2.c1</web-resource-name>
      <url-pattern>/a/*</url-pattern>
      <url-pattern>/b/*</url-pattern>
      <http-method>GET</http-method>
   </web-resource-collection>

   <web-resource-collection>
      <web-resource-name>sc2.c2</web-resource-name>
      <url-pattern>/b/*</url-pattern>
      <http-method>POST</http-method>
   </web-resource-collection>
```

```
    <auth-constraint>
        <role-name>R1</role-name>
    </auth-constraint>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

TABLE 3-4 contains the qualified URL pattern names that would result from the translation of the `security-constraint` elements (including the qualified form of the default pattern). The second column of TABLE 3-4 contains the canonical form of the qualified names. The values in the second column have been derived from the values in the first column by removing qualifying patterns matched by other qualifying patterns.

TABLE 3-4 Qualified URL Pattern Names from Example

Qualified URL Pattern Name	*Canonical Form*
/a	/a
/b	/b
/a/*:/a	/a/*:/a
/b/*:/b	/b/*:/b
.asp:/a/:/b/*	*.asp:/a/*:/b/*
/:/a:/b:/a/*:/b/*:*.asp	/:/a/*:/b/*:*.asp

TABLE 3-5 represents the permissions and PolicyConfiguration operations that would result from the translation of the security-constraint elements.The names appearing in the second column of the table are those found in the first column of TABLE 3-4. As noted previously, any equivalent form of the qualified names, including their canonical forms, could have been used in the permission constructions.

TABLE 3-5 Permissions and PolicyConfiguration Operations from Example

Permission Type	*Name*	*Actions*	*Policy Configuration Add To*
WebResource	/a/*:/a	!GET,POST	excluded
WebUserData	/a/*:/a	!GET,POST	excluded
WebResource	/b/*:/b	!GET,POST	excluded
WebUserData	/b/*:/b	!GET,POST	excluded
WebResource	/a	!GET,POST	excluded
WebUserData	/a	!GET,POST	excluded
WebResource	/b	!GET,POST	excluded
WebUserData	/b	!GET,POST	excluded
WebResource	*.asp:/a/*:/b/*	null[1]	excluded
WebUserData	*.asp:/a/*:/b/*	null	excluded
WebResource	/a/*:/a	GET	role(R1)
WebResource	/b/*:/b	GET,POST	role(R1)
WebUserData	/a/*:/a	GET:CONFIDENTIAL	unchecked
WebUserData	/b/*:/b	GET,POST:CONFIDENTIAL	unchecked
WebResource	/a/*:/a	POST	unchecked
WebUserData	/a/*:/a	POST	unchecked
WebResource	/a	GET,POST	unchecked
WebUserData	/a	GET,POST	unchecked
WebResource	/b	GET,POST	unchecked
WebUserData	/b	GET,POST	unchecked
WebResource	/:/a:/b:/a/*:/b/*:*.asp	null	unchecked
WebUserData	/:/a:/b:/a/*:/b/*:*.asp	null	unchecked

1.The canonical form for the set of all HTTP Methods (including all extension methods) is null.