for mapping the target name or address information of an HTTP request to the appropriate hostname.

To satisfy this specification, an application server must establish servlet policy context identifiers sufficient to differentiate all instances of a web application deployed on the logical host or on any other logical host that may share the same policy statement repository. One way to satisfy this requirement is to compose policy context identifiers by concatenating the hostname with the context path (as defined in the Servlet specification) identifying the web application at the host.

When an application is composed of multiple web modules, a separate policy context must be defined per module. This is necessary to ensure that url-pattern based and servlet name based policy statements configured for one module do not interfere with those configured for another.

3.1.3 Translating Servlet Deployment Descriptors

A reference to a `PolicyConfiguration` object must be obtained by calling the `getPolicyConfiguration` method on the `PolicyConfigurationFactory` implementation class of the provider configured into the container. The policy context identifier used in the call to the `getPolicyConfiguration` method must be a `String` composed as described in Section 3.1.2, "Servlet Policy Context Identifiers," on page 23. The `security-constraint` and `security-role-ref` elements in the deployment descriptor must be translated into permissions and added to the `PolicyConfiguration` object as defined in the following sections. Before the translation is performed, all policy statements must have been removed[2] from the policy context associated with the returned `PolicyConfiguration`.

3.1.3.1 Translating security-constraint Elements

The paragraphs of this section describe the translation of security-constraints into WebResourcePermission and WebUserDataPermission objects constructed using qualified URL pattern names. In the exceptional case, as defined in "Qualified URL Pattern Names", where a pattern is made irrelevant by a qualifying pattern, the permission instantiations that would result from the translation of the pattern, as described below, must not be performed. Otherwise, the translation of URL patterns in security constraints must yield an equivalent translation to the

---

2. This can be achieved by passing `true` as the second parameter in the call to `getPolicyConfiguration`, or by calling `delete` on the *PolicyConfiguration* before calling `getPolicyConfiguration` to transition it to the open state.