

```

</Apply>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">2a00:1620:0:ff20.*</AttributeValue>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
    <EnvironmentAttributeDesignator
      AttributeId="urn:fedora:names:fedora:2.1:environment:httpRequest:clientIpAddress"
      DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Apply>
  </Apply>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">150\.\.145\.\.48\.\.*</AttributeValue>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
    <EnvironmentAttributeDesignator
      AttributeId="urn:fedora:names:fedora:2.1:environment:httpRequest:clientIpAddress"
      DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Apply>
  </Apply>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">10\.\.1\.\.48\.\.*</AttributeValue>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
    <EnvironmentAttributeDesignator
      AttributeId="urn:fedora:names:fedora:2.1:environment:httpRequest:clientIpAddress"
      DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Apply>
  </Apply>
</Apply>
</Condition>
</Rule>
</Policy>

```

8.1.6 data/fedora-xacml-policies/repository-policies/default/deny-unallowed-file-resolution.xml

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyId="deny-file-resolve-if-not-allowed-dir" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
  combining-algorithm:first-applicable">
  <Description>deny any file datastream resolution if not in allowed file patterns</Description>
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <AnyResource/>
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#string">urn:fedora:names:fedora:2.1:action:id-
            retrieveFile</AttributeValue>
          <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
            AttributeId="urn:fedora:names:fedora:2.1:action:id"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
  <!-- uncomment (and change the deny rule id) if access via the file protocol is desired.
  The regular expression determines the locations and files allowed for retrieval; it must match the canonical
  file URI for a resource.
  Restricting access to administrators will allow datastreams in control group 'M' to be ingested from the file
  system.
  Restricting access by URI only will allow datastreams in control group 'E' to be located on the file system.
  -->
  <Rule RuleId="1" Effect="Permit">
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-match">
        <AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">^file://srv/storage/scansioni/.*</AttributeValue>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
          <ResourceAttributeDesignator AttributeId="urn:fedora:names:fedora:2.1:resource:datastream:fileUri"
            DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </Apply>
      </Apply>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-in">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">administrator</AttributeValue>
        <SubjectAttributeDesignator AttributeId="fedoraRole" DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </Apply>
    </Condition>
  </Rule>
  <!--
  <Rule RuleId="1" Effect="Deny">
  </Rule>
  -->
</Policy>

```