SUMMIT

JBoss WORLD

PRESENTED BY RED HAT

LEARN. NETWORK. EXPERIENCE OPEN SOURCE.

redhat.

Authentication/Authorization Services with SAML & XACML with JBoss Enterprise Application Platform 6

Tony Stafford, SPAWAR ISSE

Kenny Peeples, Red Hat Architect

Date 06/29/2012

Speaker Introductions

Tony Stafford

- Space and Naval Warfare Systems Center (SPAWAR) Atlantic Cybersecurity Division
- Information Systems Security Engineer for emerging technologies for Cloud, Mobile and SOA
- Lead for Marine Corp, Navy and Intelligence Community projects

Kenneth Peeples

- Red Hat Senior Architect for Public sector projects (DHS, Navy, Marine Corp, FBI, NSA, etc)
- C|HFI and Security+ certified
- OASIS Member, SAML, XACML and AMQP Technical Committees

Agenda

Challenges

Governance

Authentication (AuthN)

Authorization (AuthZ)

OASIS Standards

SAML Standard

XACML Standard

Picketlink in JBoss EAP 6

Web Single-Sign On and Authorization Example

Authentication & Authorization – An Enterprise Challenge

- Security is difficult to implement
  - Application / service developers interviewed reported they spent between 15-20% of their time building security into their software
  - The more complex, the more prone to human error
- Security creates repeat of labor
  - Each application creating one-off solutions
  - Interoperability considerations with System of Systems
- Security policies are often vague and hard to interpret
  - Decomposing IA non-functional requirements into technical implementation takes a lot of time and effort

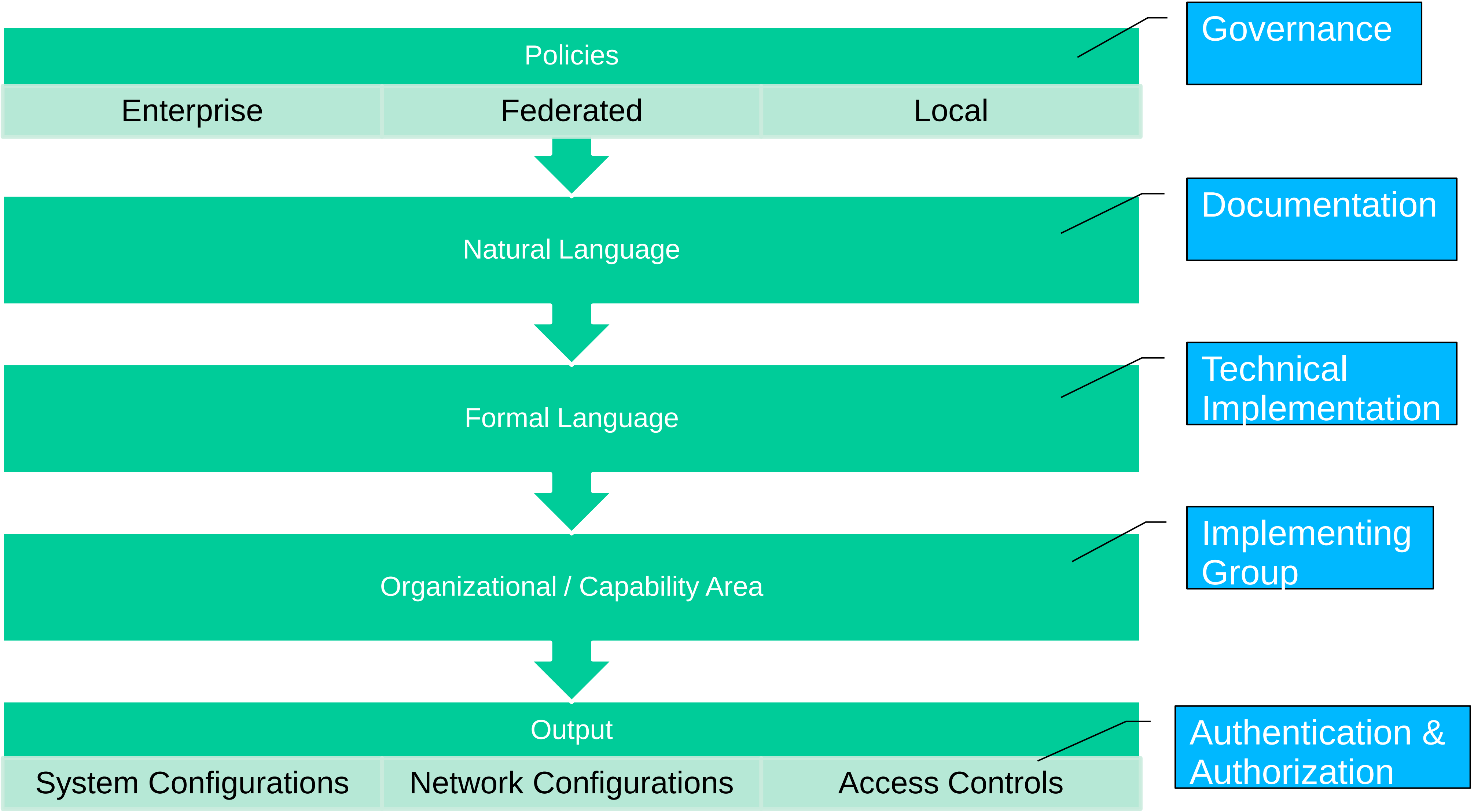
Strategic Solutions – Building a Roadmap

- Security Governance
  - Policies
  - Standards
  - Technological Implementation
- Single Sign-On
  - Open Standard
  - Interoperable
- Authorization
  - Policy Driven
  - Tailored to Enterprise Needs

Governance – Waiting is the Hardest Part

- Common Governance Challenges
  - Vague or Undefined
    - What does the technical implementation of the bureaucratic policy look like?
    - Standards identification
  - Specifications
    - Identity
    - Authentication
    - Role or Attribute definition
  - Broad Enterprise Needs
    - How does my system fit into the overall architecture?
    - What does my system need to interoperate with?

Digital Policy Lifecycle – People to Machines



Policies

Enterprise | Federated | Local

Natural Language

Formal Language

Organizational / Capability Area

Output

System Configurations | Network Configurations | Access Controls

Governance

Documentation

Technical Implementation

Implementing Group

Authentication & Authorization

SAML & XACML – Killing Many Birds with Two Stones

- SAML
    - Open Identity and Authentication Standard
        - Managed by OASIS
        - Extensible
- XACML
    - Open Authorization Standard
        - Managed by OASIS
        - Extensible
- Mapping
    - Standardize SAML & XACML
    - Decompose universal Roles or Attributes

Authentication (AuthN) and Authorization (AuthZ)

What is Authentication?

Verification that the user’s identity is valid. Authentication is based on three factor types:

- What the user *knows* such as a password or PIN
- What the user *has* such as a token or Smart card
- What the user *is (physically)* such as a fingerprint or retina

What is Authorization?

The granting of access rights to a user, program or process

What is OASIS?

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society.

OASIS promotes industry consensus and produces worldwide standards for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

https://www.oasis-open.org/

What is OASIS (Continued)?

OASIS Security Service (SAML- Security Assertion Markup Language) TC

- *Defining and maintaining a standard, XML-based framework for creating and exchanging security information between online partners*
- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

OASIS eXtensible Access Control Markup Language (XACML) TC

- *Representing and evaluating access control policies*
- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

OASIS Web Services Secure Exchange (WS-SX) TC

- *Defining WS-Security extensions and policies to enable the trusted exchange of multiple SOAP messages*
- The WS-Trust specification defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens.
- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-sx

What is SAML?

The Security Assertion Markup Language (SAML), developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information.

Security Assertion Markup Language (SAML) includes XML based assertions, protocols, bindings and profiles.

http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

SAML Components

SAML **Core** includes syntax for assertions and protocols.

SAML **Assertions** include statements made by an authority.

SAML **Protocol** describes the manner in which assertions are requested and received.

SAML **Binding** maps SAML messages to standard messaging/communication protocols.

SAML **Profile** is a use case using a collection of assertions, protocols and bindings.

http://saml.xml.org/saml-specifications

SAML Assertions

SAML Assertions include statements made by an authority.

Three different types of assertions:

- Authentication Assertion - Subject was authenticated by specified method at specified time
- Attribute Assertion - Subject is associated with one or more supplied attributes
- Authorization Decision Assertion - Subject has been granted/denied access to the specified resource

SAML Assertion Example

```
<saml:Assertion xmlns:saml=”urn:oasis:names:tc:SAML:2.0:assertion”
  Version="2.0"
  IssueInstant="2005-01-31T12:00:00Z">
  <saml:Issuer Format=urn:oasis:names:SAML:2.0:nameid-format:entity>
    http://idp.example.org
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
        j.doe@example.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2005-01-31T12:00:00Z"
    NotOnOrAfter="2005-01-31T12:10:00Z">
  </saml:Conditions>
  <saml:AuthnStatement
    AuthnInstant="2005-01-31T12:00:00Z" SessionIndex="67775277772">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

What is an Identity Provider (IDP)?

The Identity Provider authenticates the user and provides an authentication token to the service provider.

The identity provider authenticates the user through one of the authentication types.

The identity provider handles the management of user identities in order to free the service provider from this responsibility.

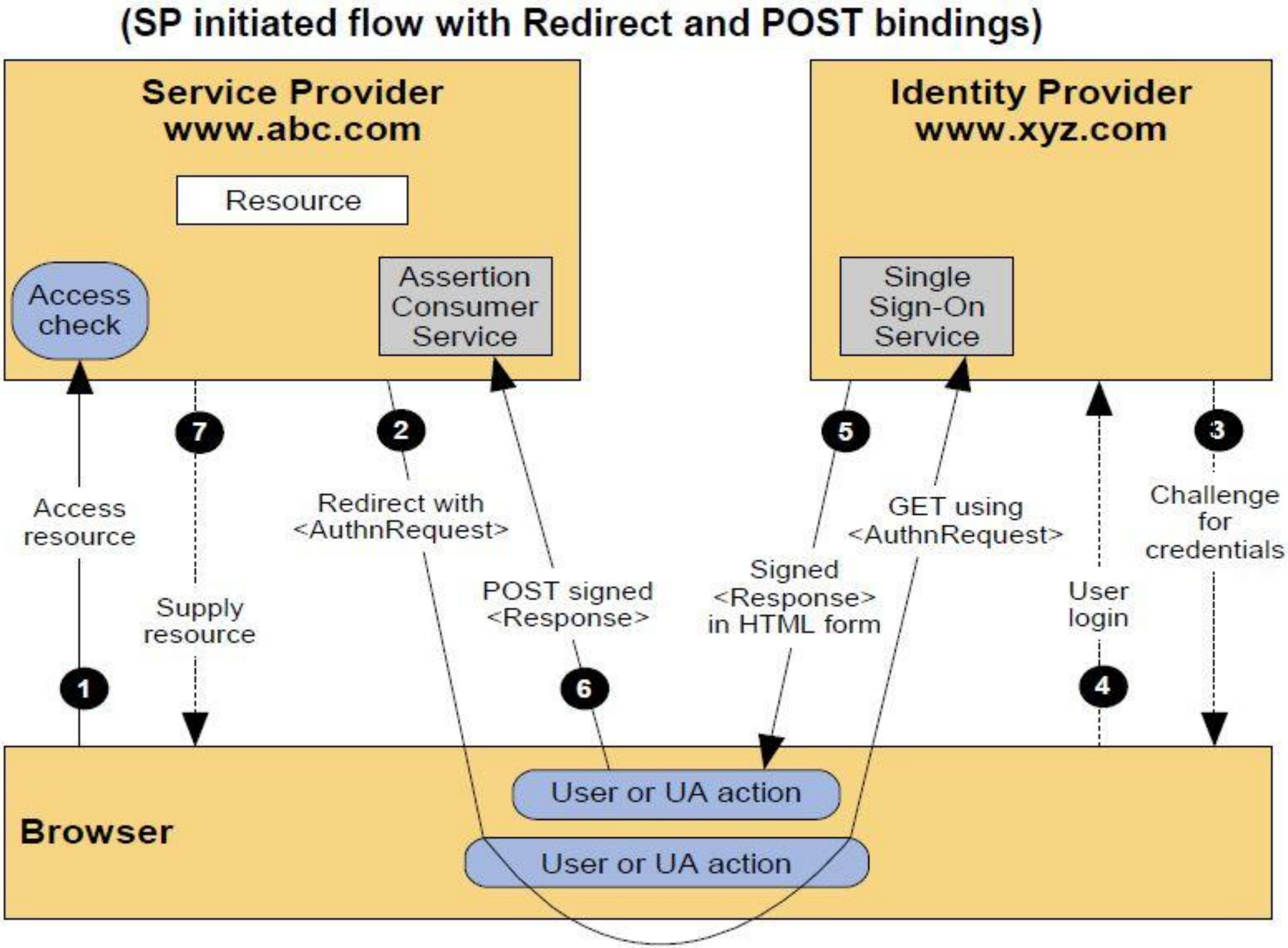
What is a Service Provider (SP)?

A service provider is a application that provides services to the end user. Service providers do not authenticate users but instead request authentication decisions from an identity provider.

What is a Security Token Service (STS)?

WS-Trust defines the concept of a security token service (STS), a service that can issue, cancel, renew and validate security tokens, and specifies the format of security token request and response messages.

Web Browser SAML SSO Profile



What is XACML?

XACML is an OASIS standard that describes both a policy language and an access control decision request/response language (both written in XML).

The policy language is used to describe general access control requirements, and has standard extension points for defining new functions, data types, combining logic, etc.

The request/response language lets you form a query to ask whether or not a given action should be allowed, and interpret the result.

The response always includes an answer about whether the request should be allowed using one of four values: Permit, Deny, Indeterminate (an error occurred or some required value was missing, so a decision cannot be made) or Not Applicable (the request can't be answered by this service).

http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

Actors within the XACML Domain

PAP (Policy Administration Point) - Point which manages policies

PDP (Policy Decision Point) - Point which evaluates and issues authorization decisions

PEP (Policy Enforcement Point) - Point which intercepts user's access request to a resource and enforces PDP's decision.

PIP (Policy Information Point) - Point which can provide external information to a PDP, such as LDAP attribute information.

XACML Elements

XACML Policies

- A PolicySet contains one or more policies
- A Policy contains a set of rules (Permit or Deny) applicable to a Target (Resource, Subject and Action).
- A Rule has one or more Conditions.
- A Condition is a Boolean function.

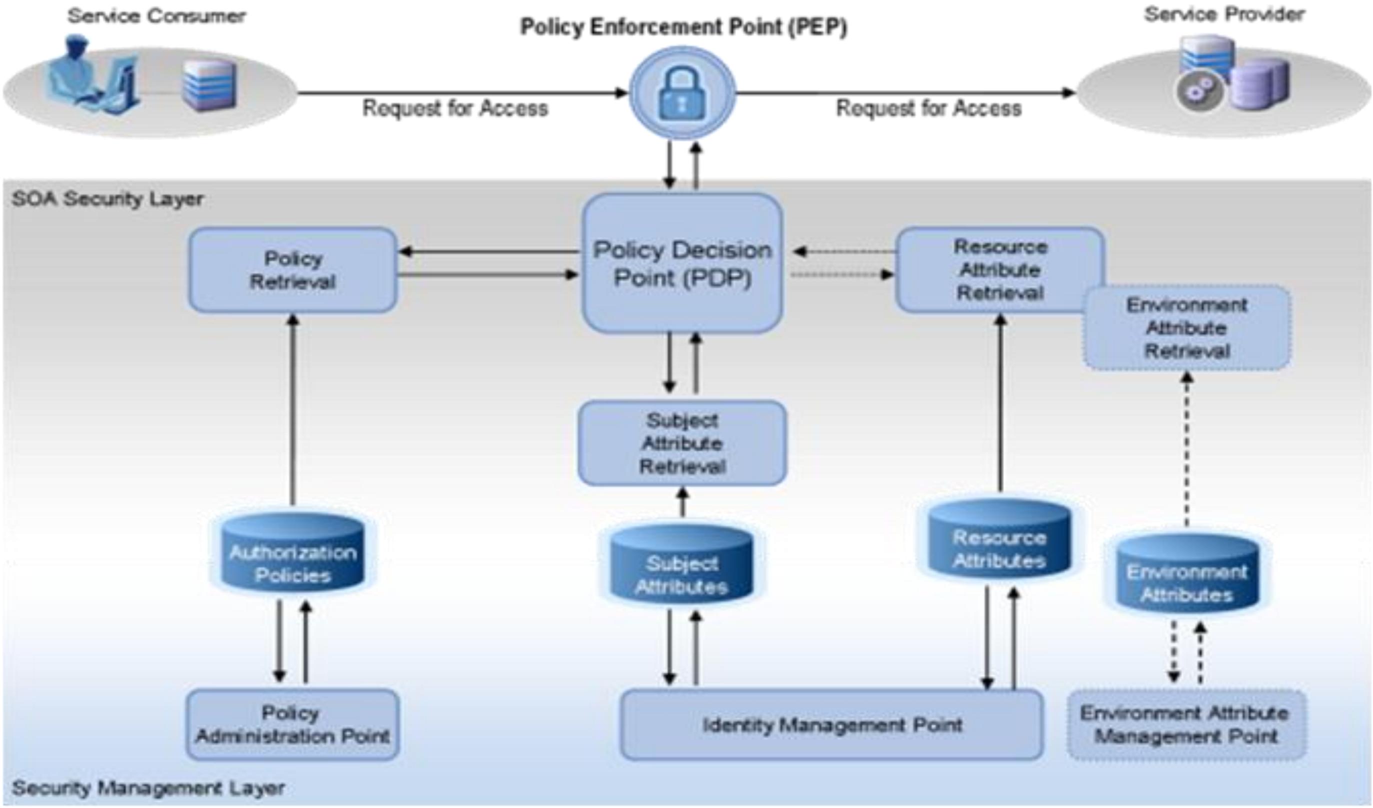
XACML Request

- Contains details on the subject, resource and action.

Decision (Permit, Deny, Not Applicable, Indeterminate) can be based on

- Resource Properties
- Subject Attributes
- Action
- Environmental Conditions (Date/Time, IP Address etc)
- Combining Algorithms (Policy Combining and Rule Combining)

Data Flow Model for XACML


Service Consumer
Policy Enforcement Point (PEP)
Service Provider
Request for Access
Request for Access
SOA Security Layer
Policy Retrieval
Policy Decision Point (PDP)
Resource Attribute Retrieval
Environment Attribute Retrieval
Subject Attribute Retrieval
Authorization Policies
Subject Attributes
Resource Attributes
Environment Attributes
Policy Administration Point
Identity Management Point
Environment Attribute Management Point
Security Management Layer

The Policy Enforcement Point (PEP) acts as an interceptor. In the component or container where an access decision is to be made, the PEP will create an XACML request based on various parameters of the call. It then asks the PDP for an access decision. The PDP will use one or more policies to make an access decision.

XACML Policy

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
      access_control-xacml-2.0-policy-schema-os.xsd"
    PolicyId="urn:oasis:names:tc:xacml:2.0:jboss-test:XV:policy"
     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
   <Description> Policy for Subject RBAC</Description>
  <Target/>
  <Rule RuleId="urn:oasis:names:tc:xacml:2.0:jboss-test:XVI:rule"
        Effect="Permit">
      <Description>
      jduke can read or write resource information when he has a role of ServletUserRole
       </Description>
       <Target>
          <Subjects>
              <Subject>
                 <SubjectMatch
                       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                     <AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string">jduke</AttributeValue>
                     <SubjectAttributeDesignator
                            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                            DataType="http://www.w3.org/2001/XMLSchema#string"/>
                  </SubjectMatch>
                  <SubjectMatch
                        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                      <AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string">ServletUserRole</AttributeValue>
                      <SubjectAttributeDesignator
                            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                            DataType="http://www.w3.org/2001/XMLSchema#string"/>
                  </SubjectMatch>
              </Subject>
          </Subjects>
```

XACML Policy (Continued)

```
        <Resources>
           <Resource>
                <ResourceMatch
                      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                   <AttributeValue
                          DataType="http://www.w3.org/2001/XMLSchema#anyURI">/xacml-subjectrole/test</AttributeValue>
                    <ResourceAttributeDesignator
                          AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id“
                          DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                  </ResourceMatch>
             </Resource>
          </Resources>
          <Actions>
              <Action>
                  <ActionMatch
                        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                     <AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
                      <ActionAttributeDesignator
                            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id“
                            DataType="http://www.w3.org/2001/XMLSchema#string"/>
                  </ActionMatch>
              </Action>
              <Action>
                  <ActionMatch
                        MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                     <AttributeValue
                            DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
                      <ActionAttributeDesignator
                            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id“
                            DataType="http://www.w3.org/2001/XMLSchema#string"/>
                  </ActionMatch>
           </Action>
          </Actions>
      </Target>
  </Rule>
</Policy>
```

XACML Request

```
<Request>
 <Subject SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
    DataType="http://www.w3.org/2001/XMLSchema#string"
    Issuer="jboss.org">
  <AttributeValue>jduke</AttributeValue>
  </Attribute>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
    DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="jboss.org">
  <AttributeValue>ServletUserRole</AttributeValue>
  </Attribute>
 </Subject>
  <Resource>
   <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
     DataType="http://www.w3.org/2001/XMLSchema#anyURI">
   <AttributeValue>http://localhost:8080/xacml-subjectrole/test</AttributeValue></Attribute>
  </Resource>
  <Action>
   <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
     DataType="http://www.w3.org/2001/XMLSchema#string"
     Issuer="jboss.org">
    <AttributeValue>read</AttributeValue>
    </Attribute>
    </Action>
   <Environment>
   <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
     DataType="http://www.w3.org/2001/XMLSchema#dateTime">
  <AttributeValue>20011-10-18T01:38:32.687000000-05:00</AttributeValue>
  </Attribute>
  </Environment>
</Request>
```

XACML Response

```
<Response>
 <Result ResourceId=“http://localhost:8080/xacml-subjectrole/test">
  <Decision>Permit</Decision>
  <Status>
   <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
  </Status>
 </Result>
</Response>
```

Picketlink within JBoss EAP 6

Picketlink is fully supported in EAP 6

Documentation - https://docs.jboss.org/author/display/PLINK/Home

Components – IDP, STS, PEP, PDP

Subprojects – IDM, Federated Identity, AuthZ, XACML, Negotiation

http://www.jboss.org/picketlink

Picketlink with JBoss EAP 6 (Continued)

The Picketlink Module is included with EAP ***${jboss.home.dir}*/modules/org/picketlink**

The configuration (module.xml) and jar (picketlink-core-2.1.1.Final.jar and picketlink-jbas7-2.1.1.Final.jar) files are located within the main folder. The **module.xml** should contain

```
<module xmlns="urn:jboss:module:1.1" name="org.picketlink">
    <resources>
     <resource-root path="picketlink-core-2.1.1.Final.jar"/>
     <resource-root path="picketlink-jbas7-2.1.1.Final.jar"/>
    </resources>
    <dependencies>
                            ...
    </dependencies>
</module>
```

Quickstarts

- SAML Examples
- WS-Trust Security Token Service
- XACML Examples
- Deploying and Running on AS

https://docs.jboss.org/author/display/PLINK/PicketLink+Quickstarts

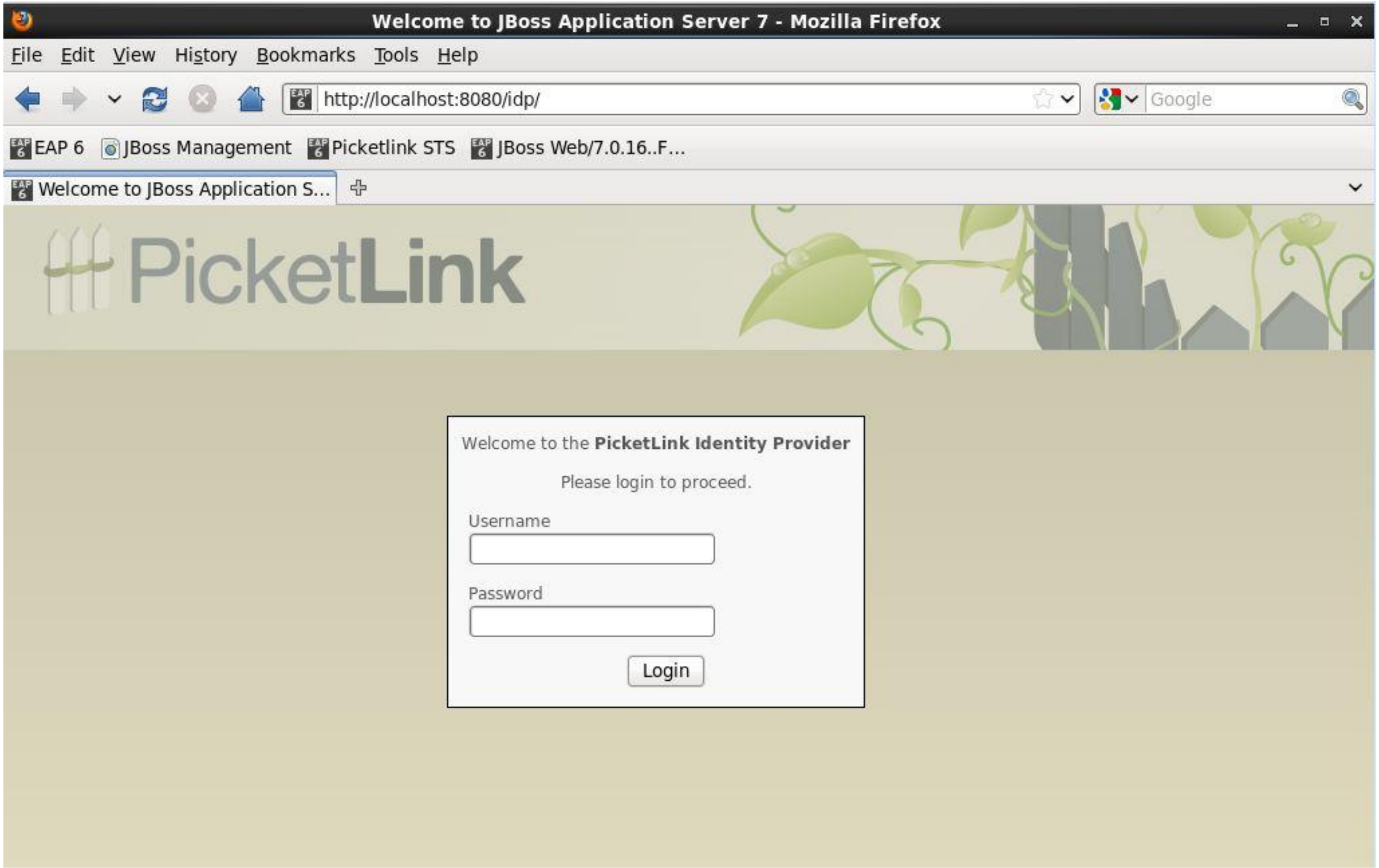
Web Application SSO with SAML Example

Demonstration of Sales and Employee Web Applications (Service Providers - SP) and SAML SSO with the Identity Provider (IDP)

Relevant wars

- Idp.war – Identity Provider
- picketlink-sts.war – WS-Trust implementation
- sales-post.war - BindingType="POST"
- employee.war - BindingType="REDIRECT"

Identity Provider Login


Welcome to JBoss Application Server 7 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/idp/
Google
EAP 6
JBoss Management
Picketlink STS
JBoss Web/7.0.16..F...
Welcome to JBoss Application S...
PicketLink

Welcome to the **PicketLink Identity Provider**

Please login to proceed.

Username

Password

Login

picketlink.xml (IDP)

```
<PicketLink xmlns="urn:picketlink:identity-federation:config:2.1">
  <PicketLinkIDP xmlns="urn:picketlink:identity-federation:config:2.1">
    <IdentityURL>${idp.url::http://localhost:8080/idp/}</IdentityURL>
    <Trust>
            <Domains>localhost,jboss.com,jboss.org,amazonaws.com</Domains>
    </Trust>
  </PicketLinkIDP>
  <Handlers xmlns="urn:picketlink:identity-federation:handler:config:2.1">
    <Handler
            class="org.picketlink.identity.federation.web.handlers.saml2.SAML2IssuerTrustHandler" />
    <Handler
            class="org.picketlink.identity.federation.web.handlers.saml2.SAML2LogOutHandler" />
    <Handler
    class="org.picketlink.identity.federation.web.handlers.saml2.SAML2AuthenticationHandler“ />
    <Handler
            class="org.picketlink.identity.federation.web.handlers.saml2.RolesGenerationHandler" />
  </Handlers>
  </PicketLink>
```

picketlink.xml (Web Applications)

```
<PicketLink xmlns="urn:picketlink:identity-federation:config:2.1">
  <PicketLinkSP xmlns="urn:picketlink:identity-federation:config:1.0"
    ServerEnvironment="tomcat" BindingType="POST">
    <IdentityURL>${idp.url::http://localhost:8080/idp/}</IdentityURL>
    <ServiceURL>${sales-post.url::http://localhost:8080/sales-post/}</ServiceURL>
  </PicketLinkSP>
  <Handlers xmlns="urn:picketlink:identity-federation:handler:config:2.1">
    <Handler
    class="org.picketlink.identity.federation.web.handlers.saml2.SAML2LogOutHandler“ />
    <Handler
    class="org.picketlink.identity.federation.web.handlers.saml2.SAML2AuthenticationHandler" />
    <Handler
    class="org.picketlink.identity.federation.web.handlers.saml2.RolesGenerationHandler" />
  </Handlers>
</PicketLink>
```

jboss-web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<jboss-web>
  <security-domain>sp</security-domain>
  <context-root>sales-post</context-root>
  <valve>
    <class-name>org.picketlink.identity.federation.bindings.tomcat.sp.ServiceProviderAuthenticator</class-name>
 </valve>
</jboss-web>
```

standalone.xml

```
<security-domain name="idp" cache-type="default">
        <authentication>
          <login-module code="UsersRoles" flag="required">
            <module-option name="usersProperties" value="users.properties"/>
            <module-option name="rolesProperties" value="roles.properties"/>
          </login-module>
        </authentication>
</security-domain>
<security-domain name="picketlink-sts" cache-type="default">
        <authentication>
          <login-module code="UsersRoles" flag="required">
            <module-option name="usersProperties" value="users.properties"/>
             <module-option name="rolesProperties" value="roles.properties"/>
          </login-module>
        </authentication>
</security-domain>
<security-domain name="sp" cache-type="default">
        <authentication>
          <login-module code="org.picketlink.identity.federation.bindings.jboss.auth.SAML2LoginModule" flag="required"/>
        </authentication>
</security-domain>
<security-domain name="xacml-test" cache-type="default">
        <authentication>
          <login-module code="org.jboss.security.auth.spi.UsersRolesLoginModule" flag="required"/>
        </authentication>
        <authorization>
          <policy-module code="org.jboss.security.authorization.modules.XACMLAuthorizationModule" flag="required"/>
        </authorization>
</security-domain>
```

jboss-deployment-structure.xml

```
<jboss-deployment-structure>
<deployment>
    <!-- Add picketlink module dependency -->
    <dependencies>
      <module name="org.picketlink" />
    </dependencies>
  </deployment>
</jboss-deployment-structure>
```

Web Application XACML Authorization Example

Demonstration of the use of the PEP and PDP with the Web Application xacml-subjectrole

Relevant wars

- xacml-subjectrole.war

jbossxacml-config.xml

```
<ns:jbosspdp xmlns:ns="urn:jboss:xacml:2.0">
 <ns:Policies>
   <ns:Policy>
      <ns:Location>jboss-xacml-policy.xml</ns:Location>
   </ns:Policy>
 </ns:Policies>
 <ns:Locators>
   <ns:Locator Name="org.jboss.security.xacml.locators.JBossPolicySetLocator"/>
   <ns:Locator Name="org.jboss.security.xacml.locators.JBossPolicyLocator"/>
 </ns:Locators>
</ns:jbosspdp>
```

jboss-web.xml

```
<!DOCTYPE jboss-web PUBLIC
"-//JBoss//DTD Web Application 2.4//EN"
"http://www.jboss.org/j2ee/dtd/jboss-web_4_0.dtd">
<jboss-web>
<security-domain>java:/jaas/xacml-test</security-domain>
</jboss-web>
```

Additional References

https://community.jboss.org/wiki/ProtectingEJBwebserviceswithXACMLAbeginnerstutorial

https://community.jboss.org/wiki/SAMLWSIntegrationwithPicketLinkSTS

http://server.dzone.com/articles/security-features-jboss-510-2

http://www.jboss.org/picketlink/Fed.html

Contact Information

Tony Stafford, SPAWAR ISSE

tony.stafford@navy.mil

Kenny Peeples, Red Hat Architect

kpeeples@redhat.com

LIKE US ON FACEBOOK

www.facebook.com/redhatinc

FOLLOW US ON TWITTER

www.twitter.com/redhatsummit

TWEET ABOUT IT

#redhat

READ THE BLOG

summitblog.redhat.com

GIVE US FEEDBACK

www.redhat.com/summit/survey