

Chapter 12

Defining Actions to Be Taken for Subscriber Traffic

This chapter describes how the SDX can manage subscriber traffic that IDP identifies as malicious. The chapter contains the following sections:

- Actions to Be Taken for Subscriber Traffic on page 185
- Redirecting Web Requests to an IDP Captive Portal on page 186
- Developing and Customizing the Sample IDP Captive Portal on page 188
- Applying SDX Services to Subscribers Associated with Problem Traffic on page 193

Actions to Be Taken for Subscriber Traffic

When IDP processes subscriber traffic that it receives, it identifies malicious traffic as defined by IDP security rules that are configured within IDP. For SDX-managed subscriber traffic, you can configure the SDX software to:

- Redirect subscriber Web requests to an IDP captive portal page that provides information about the problem encountered.
- Activate SDX services to take actions such as limiting the bandwidth available to the subscriber.
- Send e-mail to the subscriber to provide information about a problem encountered by mapping IP addresses to subscriber names.
- Enable in IDP actions that the SDX software takes in response to an incident reported by IDP


Redirecting Web Requests to an IDP Captive Portal

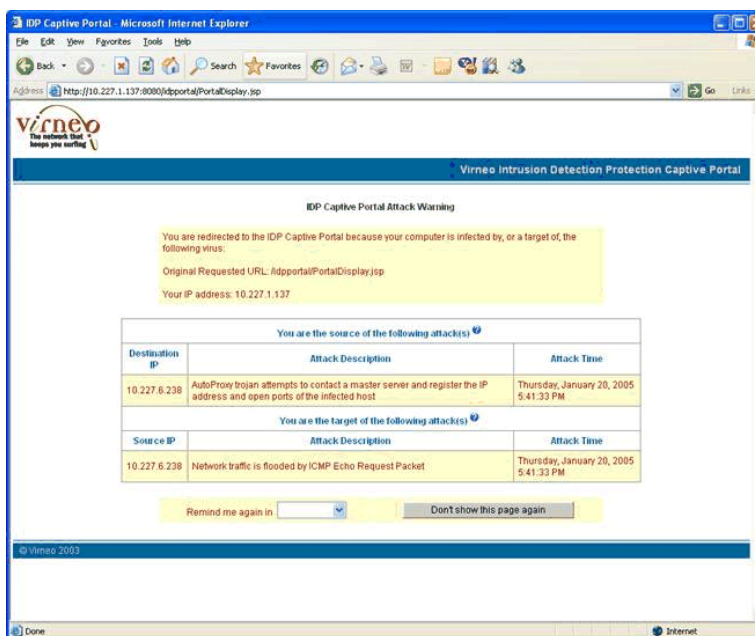
You can configure the SDX software to redirect subscriber Web requests to an IDP captive portal page in response to IDP security rules that detect problem traffic sent by or received by a subscriber. A captive portal is simply a Web page that receives redirected HTTP requests. The SDX application library provides a sample IDP captive portal that is a Java 2 Platform, Enterprise Edition (J2EE) Web application. We provide the application for demonstration purposes. You use an SDX service to redirect Web requests to a captive portal.

You can use the sample IDP captive portal as a basis for a captive portal for your environment, or you can develop a different captive portal based on the sample.

The sample IDP captive portal:

- Provides the source IP address or destination IP address of the problem traffic and provides a description of the incident.

The following page shows a sample IDP captive portal page that identifies incoming as well as outgoing traffic problems that IDP detected. The help buttons  provide information about what the subscriber can do in response to the problem. For example, for the incoming traffic the Help could recommend that the subscriber use firewall software.



- Displays general information if the SDX software cannot collect information about the type of traffic that causes a problem; for example, if the IDP management server cannot access the record servlet in the IDP captive portal.
- Lets the subscriber display the Web page that he or she was trying to access when the request was redirected to the captive portal page and be reminded of the error at another time.

- Lets the subscriber prevent display of the IDP captive portal page again for the same incident.

This feature is useful for a subscriber who is addressing a detected problem and who does not want to be redirected to the IDP captive portal page again while addressing the issue. It is not intended that the subscriber simply ignore the problem.

If a new problem occurs, the portal displays a new page.

Sequence for Redirecting Traffic

The sample IDP captive portal takes the following actions in response to incidents detected by IDP:

1. The portal's record servlet records HTTP messages that it receives from the IDP management server. The messages include the source and destination IP addresses of problem traffic and a problem description.
2. The IDP management server activates a service that policy-routes the subscriber's Web traffic to the SDX redirect server.
3. When the subscriber tries to access the Web, the SDX redirect server responds to the subscriber's Web traffic by redirecting the subscriber to the IDP captive portal through an HTTP redirect process.
4. The IDP captive portal then retrieves the subscriber's IP address and the stored messages for this IP address, and displays messages appropriate to the subscriber.

About the Record Servlet

The record servlet receives messages from the SDX `idpsdx.py` script that runs in IDP. It posts messages to a specified URL. The default URL is `http(s):// <hostname > : <port > /idpPortal/Record`.

The following example shows the type of information that IDP sends to the record servlet. The parameter name in the message appears to the left of the equals sign and the value to the right.

```
fixed.timeGeneratedGMT=2005/01/20 17:41:33
fixed.timeReceivedGMT=2005/01/20 17:41:44
fixed.deviceAddress=10.227.6.116
fixed.devinVIN=A97B-3867-3062-D6E6
fixed.sourceAddress=10.227.6.238
fixed.sourcePort=35170
fixed.destinationAddress=10.227.6.252
fixed.destinationPort=8
fixed.inboundInterface=eth0
fixed.outboundInterface=
fixed.virtualDevice=s0
fixed.attack=ICMP:EXPLOIT:FLOOD
fixed.policy=FirstPolicy
fixed.policyVersion=6
fixed.rulebase=IDS
```

```

fixed.ruleNumber=10
fixed.miscellaneous=repeated 3 times
fixed.bytes=0
fixed.packets=0
fixed.elapsed=0
fixed.protocol=ICMP
fixed.category=ATTACK
fixed.subCategory=ICMP_FLOOD
fixed.action=NONE
fixed.severity=MEDIUM
fixed.isAlert=no

```

The record servlet maps addresses to messages for the types of incidents to be recorded to:

- fixed.sourceAddress—Source IP address
- fixed.destinationAddress—Destination IP address

If the servlet receives more than one record for the same source and destination address at the same time (fixed.timeGeneratedGMT) with the same ID (fixed.attack), the servlet stores the record once and increases the value of a counter by one for each subsequent occurrence.

For information about the SDX `idpsdx.py` script that runs in IDP Manager, see *Chapter 7, Enabling SDX Actions from IDP Manager*.

Developing and Customizing the Sample IDP Captive Portal

The `/webapp` directory on the SDX application library CD contains the `idpPortal.war` file. The `idpPortal.war` file provides:

- Complete source code for the IDP captive portal in the `WEB-INF/src` directory
- Documentation for the Java classes used in the sample IDP captive portal in the `/javadoc` directory

For information about expanding the `idpPortal.war` file, see *Configuring Properties for the Sample IDP Captive Portal* on page 189.

The IDP captive portal uses the SAE CORBA remote application programming interface (API) to perform actions such as activating, deactivating, or scheduling services. For information about the SAE CORBA remote API, see the SAE CORBA remote API online documentation on the SDX software distribution in the directory `SDK/doc/idl/index.html`.

The tasks to deploy the sample IDP captive portal are:

1. Configuring Properties for the Sample IDP Captive Portal on page 189
2. Deploying the Updated WAR File on page 193
3. Accessing the IDP Captive Portal on page 193
4. Configuring the Redirect Server to Redirect Traffic to the IDP Captive Portal on page 193

Configuring Properties for the Sample IDP Captive Portal

The sample IDP captive portal provided with the SDX software is designed to be used with the IDP integration implementation and the sample data. To use the sample IDP captive portal, edit the *WEB-INF/portal.props*. The */opt/UMC/idp/idpPortal.war* file contains the *WEB-INF/portal.props* file.

To edit the *WEB-INF/portal.props* file:

1. Copy the *idpPortal.war* file to a temporary folder, and work in that folder.
2. Extract the *WEB-INF/portal.props* file from the *idpPortal.war* file.

jar xvf idpPortal.war WEB-INF/portal.props

3. With a text editor, edit the *WEB-INF/portal.props* file:
 - Review the basic portal properties, and update as needed.
See *Basic Portal Properties* on page 190.
 - Review the entries for the SAE locator, and change them as needed to accommodate your SDX configuration.
See *Locator Properties* on page 191.
 - Configure properties in the network information collector (NIC) proxy configuration section of the file.

For information about the values to configure for NIC properties, see *SDX Network Guide: SAE, Juniper Networks Routers, and NIC, Chapter 7, Configuring Applications to Communicate with an SAE*.

4. Replace the *WEB-INF/portal.props* file and any other updated files in the *idpPortal.war* file.

jar uvf idpPortal.war WEB-INF/portal.props

Basic Portal Properties

In the *WEB-INF/portal.props* file, you can modify the following properties. These properties specify how the portal uses records received from IDP.

Attack.Record.number

- Maximum number of incident records to be stored for use by the IDP captive portal.
- Value—Integer in the range 1–2147483648
- Default—100

Attack.Record.removeStep

- Number of records to be deleted when the number of records stored reaches the limit specified by the `Attack.Record.number` property. The records are sequentially removed, starting with the oldest record, then the next oldest, and so forth.
- Value— < number >
- Guidelines—This number must be less than the value configured for `Attack.Record.number`.
- Default—10

DateTime.Format

- Format in which to display the date and time of an incident.
- Value—yyyy/MM/dd hh:mm:ss, where yyyy represents the year, MM the month, dd the day, hh the hour, mm the minute, and ss the second
- Guidelines—For more information about this property, including its value see <http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html>
- Default—No value

<incident-name>

- Name of a parameter that indicates the type of security incident encountered, and provides a description of the parameter.
- Value— < parameter > = < description >
- Guidelines—Enter the parameter and description in the section "Attack Name and the corresponding description."

For information about security parameters, see the IDP documentation at

<http://www.juniper.net/techpubs/software/management/idp/>

- Default—No value
- Example
 - ICMP.EXPLOIT.FLOOD = Network traffic that is flooded by ICMP Echo Request Packet
 - TROJAN.AUTOPROXY.INFECTED-HOST = AutoProxy trojan attempts to contact a master server and register the IP address and open ports of the infected host

Attack.Captive.service

- Name of the service for the IDP captive portal. The IDP management server activates this service for subscribers who receive or send malicious traffic. If you use a “remind me later” control on the Web page and the subscriber selects this control, the portal deactivates this service and schedules service activation for a later time. If you use a “don't show this page again” control and the subscriber selects this control, the portal deactivates this service.
- Value— < service name >
- Default—Quarantine

Attack.showRemindLater

- Specifies whether the IDP captive portal page provides the Remind me again in field. This field lets subscribers specify a time at which the portal reminds them of the security incident.
- Value—true or false
- Default—true

Attack.showIgnore

- Specifies whether the IDP captive portal page provides the Don't show this page again field. The field lets subscribers stop display of the captive portal page for incidents that have already been detected. The portal displays another page when another incident occurs.
- Value—true or false
- Default—true

Locator Properties

In the *WEB-INF/portal.props file*, you can modify the following properties. Change these properties to conform to your configuration.

Factory.locator

- Method that the portal uses to locate the SAE.
- Value
 - net.juniper.smgt.ssp.LocalFeatureLocator—Uses the locally configured object reference
 - net.juniper.smgt.ssp.DistributedFeatureLocator—Uses NIC configuration
- Guidelines—If you specify net.juniper.smgt.ssp.LocalFeatureLocator, configure a value for LocalFeatureLocator.objectRef.

LocalFeatureLocator.objectRef

- Location of the SAE server.
- Value—Location in one of the following formats:
 - Absolute path to the interoperable object reference (IOR) file in the form file:// < absolutePath >
 - Corbaloc URL in the format corbaloc:: < host > : < port > /SAE
 - < host > —IP address or host on which the SAE is installed.
 - < port > —Port used by the SAE on the specified host. The default is 8801.
 - The actual IOR in the form IOR: < objectReference >
- Default—No value
- Examples
 - Absolute path—file:///opt/UMC/sae/var/run/sae.ior
 - corbaloc URL—corbaloc::10.10.6.171:8801/SAE
 - Actual IOR—
IOR:0000000000000002438444C3A736D67742E6A756E697...

DistributedFeatureLocator.locName

- Namespace for the NIC proxy configuration.
- Value— < namespace >
- Default—/, which indicates the root namespace
- Example—DistributedFeatureLocator.locName = /nicProxy indicates that the NIC proxy configuration is in /nicProxy.

Config.java.naming.provider.url

- Location of the LDAP server.
- Value—ldap:// < IP address > : < port number >
- Default—No value
- Example—ldap://127.0.0.1:389

Config.net.juniper.smgmt.des.backup_provider_urls

- Location of a backup LDAP server.
- Value—ldap:// < IP address > : < port number > , with more than one URL separated by commas
- Default—No value

Deploying the Updated WAR File

To deploy the updated WAR file for the application:

- Copy the file to the deployment directory for your Web server.

If you are using JBoss, copy the file to the `/opt/UMC/jboss/server/default/deploy` directory. JBoss automatically starts the Web application when a new WAR file is copied into the `deploy` directory.

Accessing the IDP Captive Portal

Access the portal to ensure that you can view the page and to review the page setup. To access the IDP captive portal:

- Enter a URL in the following form in your Web browser, and press Enter.

```
http(s)://<host>:<port>/idpPortal
```

Configuring the Redirect Server to Redirect Traffic to the IDP Captive Portal

To configure the SDX redirect server to redirect Web requests to the IDP captive portal:

1. Follow the instructions for configuring the redirect server in *SDX Subscribers and Subscriptions Guide, Chapter 9, Overview of the Residential Portal*.
2. In the `/opt/UMC/redir/etc/redir.properties` file, specify the URL of the IDP captive portal for the `redir.url` property. This entry has the form

```
redir.url = http(s):// < host > : < port > /idpPortal/PortalDisplay.jsp
```

Applying SDX Services to Subscribers Associated with Problem Traffic

You can configure services to control subscriber traffic, such as limiting bandwidth available to a subscriber, in response to detection of malicious traffic sent or received by a subscriber. The following procedure describes how to configure policies to decrease the amount of bandwidth available to the subscriber and to redirect subscriber Web requests to an IDP captive portal as implemented in the sample data. You can also create separate services or a service for only one of these actions.

To limit bandwidth and redirect subscriber Web requests to a captive portal:

1. In Policy Editor, create a policy that defines an action to be taken, such as a policy that limits a subscriber's bandwidth and redirects Web requests to a captive portal.

For a sample policy group, see `policyGroupName = Quarantine, ou = idp, o = Policies, o = UMC` in the sample data.

2. (Optional) In SDX Admin, create a scope for the value-added services that define actions to be taken in response to IDP rules configured in IDP.

3. If you created a scope in Step 2:
 - a. In that scope, create a value-added service that defines actions to be taken in response to IDP rules. Then set the type to normal, and specify the policy group configured in Step 1.

For a sample service, see *serviceName = Quarantine, l = IDP-Subscriber, o = Scopes, o = umc* in the sample data.
 - b. Assign the scope to a subscriber folder to make the service available to subscribers.
4. Create service subscriptions for subscribers. In the sample data, we create a subscription at the folder level to allow all subscribers in the folder to inherit the subscription.

For a sample implementation, see *serviceName = Quarantine, ou = subscribers, retailerName = SP-IDP, o = Users, o = umc* in the sample data.