

## **SRC Service Management Applications**

---

The SRC application library provides the following service management applications:

- SRC SOAP Gateway on page 1
- Deep Packet Inspection Integration Application on page 1
- Threat Mitigation Portal on page 2

### **SRC SOAP Gateway**

The SRC SOAP Gateway (SRC-SG) allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a SOAP interface. This feature is useful for business-to-business situations, such as a wholesaler-retailer environment. Typically, the wholesaler owns and administers the SRC components, and the retailer maintains a database of subscribers. Retailers purchase services from one or more wholesalers and sell the services to their subscribers. Using information provided by the wholesaler, the retailer creates a gateway client to communicate with the components in the SRC software.

The SRC-SG provides the Dynamic Service Activator which allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.

### **Deep Packet Inspection Integration Application**

The SRC software has been integrated with the Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. With this solution, providers can identify, monitor, and control traffic on a per-application or per-subscriber basis.

Application traffic such as peer-to-peer file sharing or instant messaging, which in many cases originates or terminates outside of a provider's network, can cause abusive or indiscriminate consumption of bandwidth and impact a provider's ability to deliver its own services. In particular, services that require higher, guaranteed levels of performance, such as Voice-over-IP (VoIP) or video-on-demand (VoD), can be impacted. Having visibility into applications that are transported over the network and their associated bandwidth consumption at various times is important as is the ability to control those applications.

The DPI solution allows providers to implement service control policies on specific traffic flows quickly and effectively. Such policies include throttling back, capping volume, or even enhancing bandwidth or service quality for sanctioned peer-to-peer applications.

#### **Benefits of the DPI Integration**

By identifying and effectively controlling traffic at the application level, service providers can:

- Put usage controls on applications on a subscriber basis. For example, you can put a quota limit on the amount of peer-to-peer traffic that a subscriber can consume in a month.

Once subscribers have used their quota, you can apply a policy that throttles back on or blocks a subscriber's peer-to-peer traffic, bill the subscriber for additional usage, or allow the subscriber to purchase additional quota.

- Limit the total percentage of network resources that a specific type of traffic is allowed to consume.
- Provide higher or guaranteed levels of performance for premium services by applying QoS control to application sessions. For example, two subscribers start an Xbox Live session. The Ellacoya DPI platform detects activity for this application, and sends application usage counters to the SRC software. The SRC software pushes policies that deliver a specific level of QoS for this application session to a router or other network device.
- Charge subscribers based on their usage of premium content-based services.
- Offer and charge for tiered Internet services based on both speed and application.
- Better support network planning functions by gaining an in depth understanding of traffic flows and patterns on a per subscriber and per application basis.

## ***Threat Mitigation Portal***

The Threat Mitigation Portal (SRC-TMP) application allows service providers to respond to threats on the SRC-managed network. The application for the SRC-TMP can be customized based on customer-supplied data to control the description and recommended actions for each type of threat. The application includes the ability to log all user operations to provide an audit trail of actions.

The application uses these components to respond to threats:

- Juniper Networks Intrusion Detection and Prevention (IDP) Sensors to detect the threats.
- Juniper Networks NetScreen-Security Manager to manage the IDP Sensors and to signal the SRC-TMP when a threat is detected.
- The SRC-TMP, which is the user interface for the application, to manage threats and act upon them.