PolicyGuru®

Meta-Policy Controller

Technical Discussion

Release 2.6.x

A product brief from
SecureLogix Corporation

Contents

PolicyGuru® Meta-Policy Controller Technical Overview

Introduction

Strong security against the growing tide of attacks targeting enterprise Voice and Unified Communications (UC) resources has never been more business-critical. Real-time, interactive communications such as UC represent a large quotient of enterprise interactions, transactions, networks, systems, and applications, and these critical resources face a host of security and abuse threats.

While voice network security has always been and remains a serious issue in legacy voice networks, the adoption of VoIP/UC has made it an even larger problem. The transport mechanism itself is not the real target; rather, VoIP has made some newer attacks, such as Telephony Denial of Service (TDoS), more practical and has also made it easier to execute the same sort of inbound, application-level threats and attacks that have been serious issues for many years:, including financial fraud/social engineering, toll fraud, harassing calls, and nuisance calls such as voice SPAM. In addition, other forms of threats and misuse/abuse exist as always, whether or not VoIP is used, such as internal abuse of outbound toll services, unauthorized access to voice systems, and large-scale outsider theft of outbound toll services via compromised IP-PBXs or voice gateways.

These types of voice attacks cannot be adequately addressed with traditional IP firewalls or Session Border Controllers (SBCs/eSBCs), which function at the transport layer or offer only static routing tables that must be manually maintained. Universal, real-time, adaptive UC application-layer security and call control policy is required to adequately address these and other threats. Failure to manage these security issues compromises enterprise productivity, information security, and regulatory compliance, and results in:

- High-profile service outages (TDoS attacks)
- Loss of contact center uptime and impaired customer response times/satisfaction creating Failed Customer Interactions (FCIs) (TDoS attacks and negative-value calls)
- Financial fraud against the enterprise and/or its customers (Social engineering and other fraud schemes)
- Theft of proprietary information and increased compliance costs (Unauthorized access to sensitive resources)
- Financial exposure from theft and/or abuse of toll service (external and internal)
- Loss of safety and business productivity (harassing and malicious calls)

The SecureLogix® PolicyGuru® Meta-Policy Controller addresses these threats and issues with real-time monitoring, protection, and mitigation solutions that provide real-time visibility, alerting, and control of sessions on carrier Session-Initiation Protocol (SIP) trunks across the enterprise UC network.

PolicyGuru® Meta-Policy Controller Solution

PolicyGuru Meta-Policy Controller provides universal security, monitoring, and usage policy implementation and enforcement across your entire voice/UC network from a web-based management graphical user interface (GUI). The solution also provides real-time, drill-down call detail analytics and powerful offline forensic analytics and reporting capabilities. Call and policy processing data for monitored SIP trunks is stored in a centralized database for offline analysis and reporting.

The PolicyGuru Solution monitors SIP signaling to provide real-time visibility and call access control (CAC) of activity across your voice/UC network. Centrally managed policy rules are distributed across the network to specify in real time whether calls are allowed as dialed, terminated, or redirected to a different destination. You can whitelist known allowed calls; blacklist known malicious, fraudulent, or otherwise unauthorized calls; redirect suspicious calls; and watch potentially suspect calls to determine whether they represent misuse/abuse or potential attack activity. Configurable alerts provide immediate notification when a policy rule fires.

In addition to individual call control, SecureLogix® Call Secure™ security analysts can use the PolicyGuru Solution to monitor for and alert on suspicious calling patterns, such as multiple calls from the same source during a defined time window, excessive international call counts or cumulative duration, and other calling patterns that may indicate an attack beginning. These patterns are hallmarks of Toll Fraud, Social Engineering, and TDoS attacks. When such patterns is detected, analysis and appropriate action can be taken to mitigate the malicious activity and protect your voice network resources.

The PolicyGuru Solution is typically deployed in conjunction with the SecureLogix® Call Secure™ Managed Service. The Call Secure Managed Service for your PolicyGuru® Solution provides expert managed services to detect and mitigate threats to customer voice networks. SecureLogix security professionals provide guidance, deploy best-practice, enterprise-wide Unified Communications security policies, and provide incident response to mitigate threats in real time as they evolve. They also provide monitoring, management, and administration of the PolicyGuru System components. Customers can be assured that their voice infrastructure is protected by industry-leading experts against current and developing threats.

Solution Overview

PolicyGuru Meta-Policy Controller has been designed to support today's largest enterprises. The solution consists of a set of applications integrated into your enterprise voice/UC network via a set of dedicated physical or virtual server platforms to implement and enforce universal voice/UC network security, call-access control, usage, and monitoring policy in real time across your enterprise SIP trunks from a web-based management interface.

The PolicyGuru Solution provides a number of powerful voice-network security and management applications built upon a common, extensible architecture platform into which additional planned applications and features are continually integrated to address ever-evolving Unified Communications (UC) network challenges and threats.

The solution supports flexible, distributed deployment models to accommodate different network scenarios: It can be deployed alongside SIP-based infrastructure in the Customer datacenter or hosted in a Cloud offering with connectivity into the enterprise core.

Solution Component Overview

The following components comprise the common architecture upon which the PolicyGuru applications are deployed. See "PolicyGuru® Applications" on page 7 for a discussion of the current applications in the solution and "Architecture Discussion" on page 23 for a more detailed discussion of each solution component.

The PolicyGuru Solution includes one or more Mediation Servers, Database Servers, ENUM Servers, and Metadata Probes. These can all be deployed in a redundant, Enhanced Availability configuration to ensure continual uptime. Each deployment includes the Mediation Server and Database. Depending on the goals of the deployment, the ENUM Server, Metadata Probe, or both are deployed.

- The Mediation Server manages all of the system components and applications, pushes SEP Policy to the ENUM Servers, generates alerts for system events and Policy alerts, receives all call and policy processing data from the ENUM Servers and Probes and stores it in the Database, and provides the data for the real-time Analytics and system event screens.
- The ENUM Server interfaces with one or more Session Border Controllers (SBCs) to enforce user-defined call access control policies that determine whether the call is to be allowed as dialed, terminated, or redirected in real time.

- The Metadata Probe captures SIP/RTP call information (metadata) throughout the call via a passive tap and supports additional types of analytics and reporting using additional header information and mid-call events beyond the information available via ENUM. It does not provide call control.

- The Database Server stores ENUM and SIP call data, Policy processing data, and system events in a relational database for analytics and reporting, and also stores system configuration.

The PolicyGuru Solution is managed via a web-based GUI that provides access to a flexible and powerful Business Rule Management System (BRMS), call data analytics views, and system configuration management. The BRMS enables the construction and enforcement of customized voice/UC network security and business management rules. The BRMS is described in detail in "PolicyGuru® Policy Application" on page 7).

Figure 1 provides a high-level PolicyGuru Meta-Policy Controller deployment illustration.

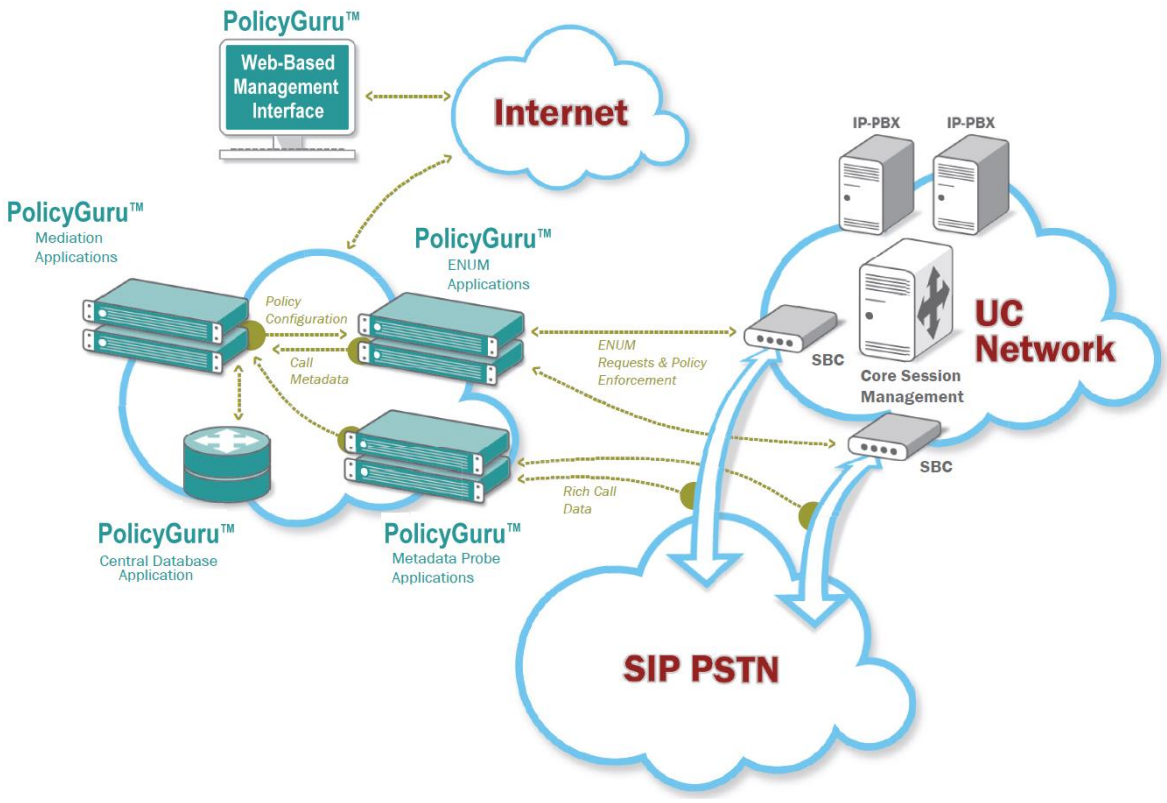

Figure 1: PolicyGuru® Meta-Policy Controller Deployment

PolicyGuru® Applications

PolicyGuru® Policy Application

The PolicyGuru Policy Application enables the construction and enforcement of customized voice/UC network security and business management rules through a flexible and powerful BRMS. These rules are defined, managed, and implemented Enterprise-wide from a web-based management interface.

User-defined, rule-based PolicyGuru Policies specify the criteria by which a call is considered of interest and the call-control action to be taken if a call triggers a given rule: allow the call as dialed, block the call, or redirect the call to another number. Automated notifications can be configured to alert appropriate personnel when a call triggers a rule. SNMP, syslog, and email alerting are supported.

The PolicyGuru Solution also allows monitoring of traffic patterns to detect and alert for new anomalies or new potential vectors of attack, enabling you to analyze these and quickly adjust the implemented rule set to take appropriate action against new threats or issues.

PolicyGuru Rules are continuously enforced in real time to monitor and secure your enterprise SIP voice network.

Figure 2 shows the Policy Application interface displaying the Call Firewall (SEP) Policy, with a set of user-define Call Firewall Policy Rules shown in the list in the left pane. This set of rules comprises the Call Firewall (SEP) Policy. The rule open in the **Guided Rule Editor** is defined to terminate inbound calls from callers in a Harassing Callers Blacklist.

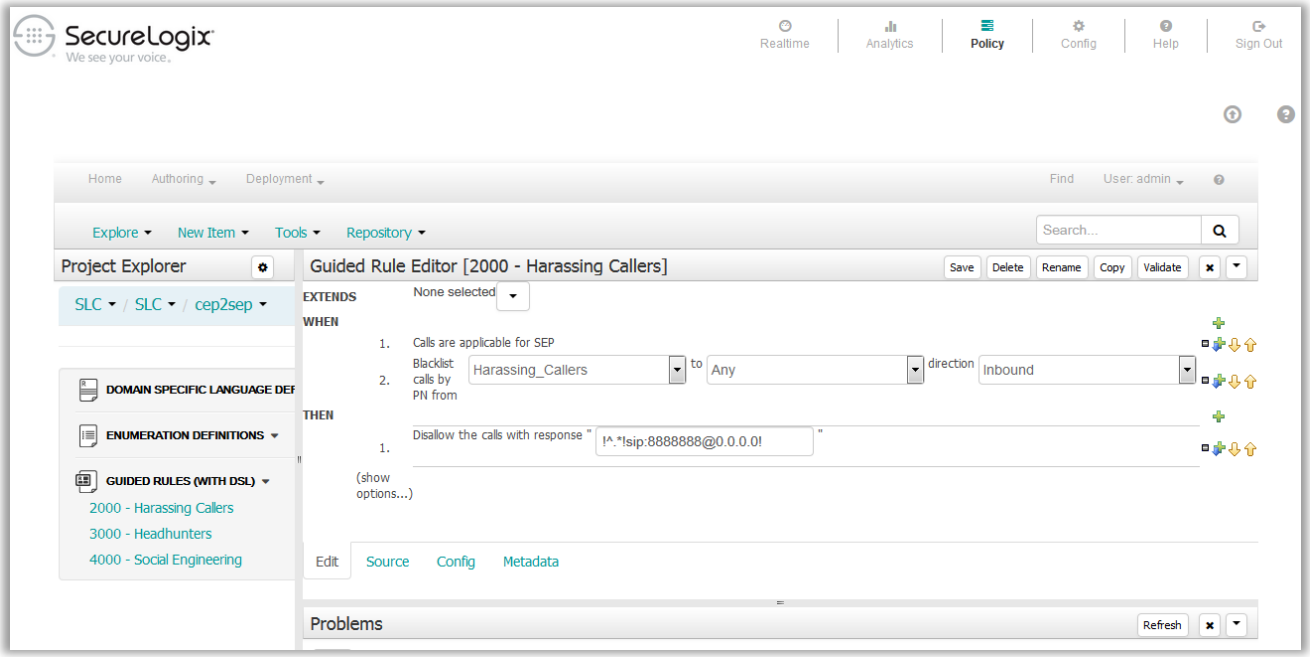

Figure 2: BRMS Interface – Guided Rule Editor

The PolicyGuru Solution provides the following types of policies::

- *Simple Event Processing (SEP) Policy*, which is analogous to Call Firewall policy and provides call access control and monitoring for individual calls and allows you to take call-control and alerting action on calls that match a rule. The rules shown in Figure 2 constitute an SEP Policy. It also provides policy rules defining which inbound calls are to be sent to the SecureLogix® Orchestra One™ Call Authentication Service for verification, if Orchestra One integration is enabled. Orchestra One integration is described in “Authentication via the Orchestra One™ Call Authentication Service” on page 12.

- *Complex Event Processing (CEP)* Policy, which provides alerting for SEP rule firings.

Each of these types of Policies is described in the following sections.

Simple Event Processing (SEP) Policy

In a manner similar to data network firewalls, SEP Call Firewall Policy provides real-time voice/UC application session access control and monitoring on a per-call basis, based on call setup details (source, destination, and direction). SEP Policy Rules define whether specific calls are to be allowed as dialed, blocked, or redirected, and provide the ability to alert on rule firings via corresponding CEP Rules. Calls that match an SEP Rule specifying treatment are terminated or redirected at call setup, preserving your network resources for

legitimate business calls. For example, you can define a rule that dictates that all calls from known harassing callers in a defined "Harassing Callers" List be terminated before they are set up.

Because the call data available in ENUM queries is limited to events that occur at call setup, SEP Rule criteria can include any combination of the following: Source, Destination, and Direction.

The PolicyGuru **Policy** GUI provides an SEP **Guided Rule Editor** that includes a robust set of predefined rule-definition assets for building SEP Rules.

User-defined *Lists* define the phone numbers/URIs to which SEP Rules apply; these are identified as *Blacklists* and *Whitelists*. You can manually add entries to these Lists, or, for large Lists, you can import the entries from a file. Each List can contain either one to many individual phone numbers/URIs, or one to many Regular Expressions, which can be used to define Ranges and Wildcards (such as all phone numbers/URIs in a certain country code or area code).

Lists and SEP Rules work in conjunction to create and implement *Blacklist Rules* and *Whitelist Rules*, as described below.

SEP Rule Types:

- **Whitelist Rules**—*Whitelist Rules* identify calls that are to be allowed and ignored. *Whitelists* are used to specify the phone numbers/URIs to which Whitelist Rules apply. These Rules do not explicitly fire—they represent default Allow rules— and therefore cannot be alerted on, preserving processing resources for true calls of interest. This is especially valuable in high call-volume environments such as Contact Centers. See "Whitelists" below for details about Whitelists.

- **Blacklist Rules**—*Blacklist Rules* specify call-control actions for calls matching the rule: allow the call as originally routed, block the call, or redirect the call to a different destination. Blacklist Rules are the only type of SEP Rule that fires, since they denote calls of interest while Whitelist Rules specify calls to be ignored and allowed by default. This means Blacklist Rules are the only rules that can be alerted on, using a corresponding CEP Alerting Rule. *Blacklists* (described below) are used to specify the phone numbers/URIs to which Blacklist Rules apply.

  It is important to note that Blacklist Rules can denote suspicious or malicious calls and provide protection from them. But they can also be used to create "Watch and Alert" Rules for any key traffic. Or, you can use them to create a Rule to specifically allow ("whitelist") certain calls you want, while a subsequent rule blocks all other calls. For example, this might be valuable in the case of an attack, to ensure network availability for critical calls. See "Blacklists" below for details about Blacklists.

Phone Number/URI Lists:

- **Whitelists**—*Whitelists* define known allowed called and calling numbers/URIs. When you use Whitelists in a Rule, you are specifying that the PolicyGuru Solution is to ignore matching calls. These calls are allowed, and neither event logging nor alerting occurs. The call data is simply stored in the database as an allowed call. These represent known good calls for which you do not want resources to be consumed for processing—for example, numbers on your Customer List at a financial call center.

  If you want to specifically allow certain calls to/from certain numbers but retain the ability to alert for the calls, such as a Watch List, you would not use a Whitelist. Rather, you would define a Blacklist containing those numbers and then use it in a Rule with an Allow action. See "Blacklists" below for details on the distinction.

- **Blacklists**—The *Blacklist* designation does not mean that calls to/from these phone numbers/URIs are disallowed or suspect. Rather, "Blacklists" define phone numbers/URIs against which you want Policy Rules to be applied. They do not necessarily denote suspicious or malicious numbers/URIs, although they can. They can be used for either known disallowed called and calling numbers/URIs, such as harassing callers, or "Watch Lists" you want to evaluate for risk or track for usage (such as call volume to your Customer Service lines during business hours or outbound call volume from your Outbound Sales personnel). Alternatively, they can be used for phone numbers/URIs you want to specifically allow ("whitelist") and track while blocking all other calls. For example, you can specify that inbound calls from phone numbers in a known Harassing Callers list are never to be allowed to any destination and specify a rule action of Terminate to prevent such calls. You can also define a Watch List by placing specific phone numbers/URIs in a Blacklist, and then specify a Rule action of Allow to either watch for calls from/to these phone numbers/URIs to determine whether they pose a threat, or to specifically allow those calls to proceed as dialed while one or more other Rules terminates or redirects all others.

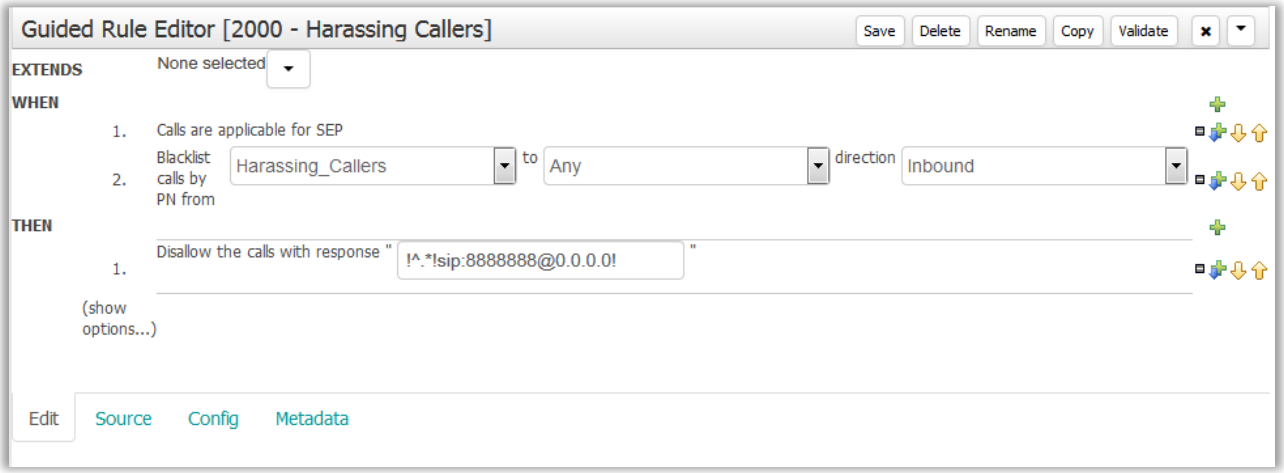

Figure 3: SEP Rule Terminating Harassing Calls

The example SEP Rule in Figure 3 above shows a Blacklist Rule that blocks phone numbers from the **Harassing Callers** Blacklist by supplying a regular expression to route the call to a nonexistent endpoint, resulting in the SBC sending a cause code response, such as a **404 Not Found** response. You can chose regular expressions that suit your enterprise practices, the type of SBC, and the routing/dialing plan used by the SBC.

Intrusion Prevention System (IPS) Policy

IPS Policy provides call-pattern recognition of calling patterns of interest. to perform real-time, adaptive Call Firewall IPS monitoring for your network. For example, Toll Fraud, Social Engineering Fraud schemes, and TDoS attacks are often characterized by a flood of calls from the same source in a short period of time, a sudden large spike in overall inbound calling, or a spike in the count or cumulative duration of outbound International calls. Call Secure Managed Service security analysts define IPS Rules that identify these suspect patterns when a user-defined threshold over a specified amount of time is exceeded and trigger an alert for appropriate investigation and mitigation.

For example, a Toll Fraud IPS Rule might specify a threshold 20 outbound International calls in a 30-minute period during business hours. When the threshold is breached, the Rule fires and the corresponding alert is generated. IPS Rules do not provide call control; only SEP Rules can. However, phone numbers identified by triggering an IPS Rule can be added to SEP Policy Rules for future call treatment (blocking or redirection.)

IPS Policy is only available as part of the Call Secure™ Managed Service for your PolicyGuru System.

Complex Event Processing (CEP) Policy

CEP Rules are used to generate alerts for SEP Rule firings. CEP Rules cannot provide call control; only SEP Rules can.

Figure 4 shows the CEP Policy (partially visible in the left pane). Open in the Guided Rule Editor is a CEP Alerting Rule that generates an SNMP alert when an SEP Rule terminating harassing callers fires.

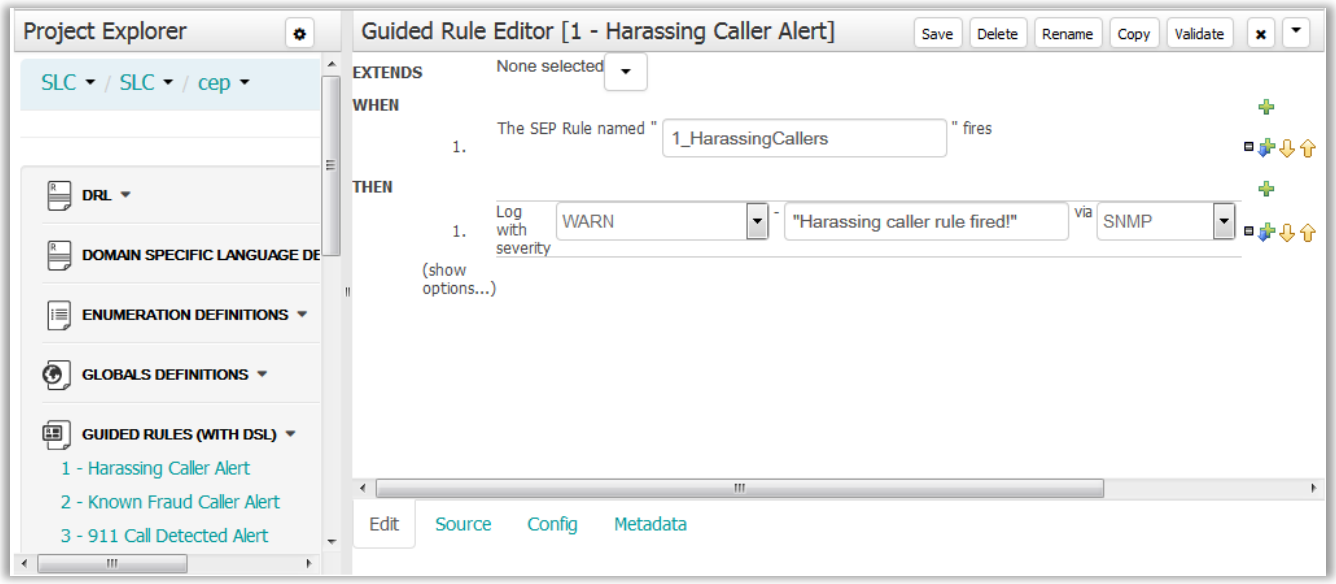

Figure 4: CEP Alerting Rule for SEP Rule Firing

The PolicyGuru BRMS interface provides a CEP Guided Rule Editor for defining Alerting Rules for your SEP Policy Rules. This set of rules, as shown in the left pane of Figure 4, constitutes a CEP Policy.

Authentication via the Orchestra One™ Call Authentication Service

The SecureLogix® Orchestra One™ Call Authentication Service (o1) provides organizations with a powerful tool to reestablish confidence in incoming calls. Orchestra One uses an integrated suite of independent checks and verifications applied to inbound calls to the organization. Orchestra One returns a score representing a level of confidence that the call is genuine and not spoofed or potentially malicious. Organizations use Orchestra One to implement score-based call handling to provide agents and administrative phone system users with the information they need to handle calls in a risk-aware manner.

The Orchestra One Service is implemented via a public REST API using strong encryption and highly available cloud resources. Customer premise systems use the REST POST method to provide details for each inbound call of interest in an authentication request to Orchestra One. Orchestra One verifies the authenticity of the source number and various attributes of the call and then returns a score result. Once the POST has been carried out, other customer premise systems can obtain the score using the REST GET method by providing the CALL ID from the SIP invite message.

The PolicyGuru Solution provides an integration that enables the PolicyGuru Mediation Server to send call authentication requests to Orchestra One. The PolicyGuru Solution can be configured to send verification requests for all inbound calls to Orchestra One, or SEP Policy Rules can be defined that specify only certain source and/or destination numbers for which call verification requests are to be sent, such as contact center lines. Figure 5 shows an Orchestra One Authentication Request Rule defined to query Orchestra One for inbound calls to the corporate contact center.

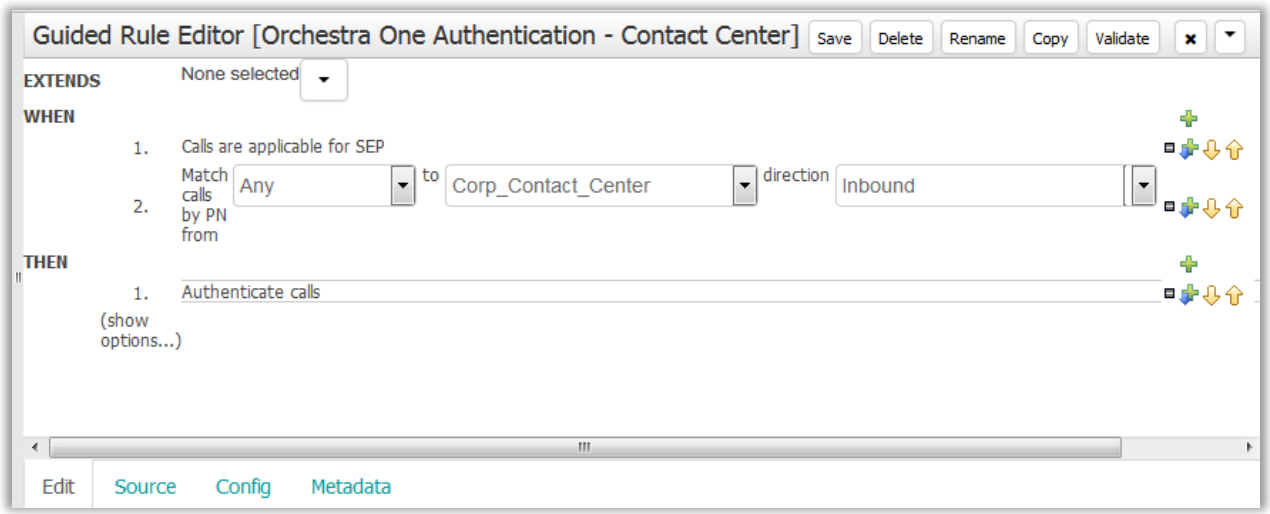

Figure 5: Orchestra One Authentication Request SEP Rule

See the SecureLogix website or contact your SecureLogix Sales Representative for more information about the Orchestra One Call Authentication Service.

Call Control

The PolicyGuru Solution ENUM Server is designed on the model that real-time call events dictate the routing decisions the SBC needs to execute, based on a user-defined Policy. In contrast, the other Open Source and Commercial ENUM servers available today implement static routing decisions defined at time of provisioning.

The PolicyGuru ENUM Server is a unique type of DNS Server that evaluates called and calling numbers/URIs to determine in real time whether should be allowed as dialed, rerouted, or terminated before call set up, based on the user-defined PolicyGuru SEP Rules being enforced. For each call, the SBC sends an ENUM request containing the source and destination information from the SIP INVITE to the ENUM Server prior to routing the call. The PolicyGuru ENUM Server processes the ENUM requests according to the installed SEP Policy Rules and returns a response to the SBC dictating the call treatment (allow as originally routed, terminate, or redirect to a different destination). The SBC routes the call according to this policy-dictated response. If allow

is specified, the ENUM Server returns the ENUM response with the destination endpoint host address unchanged. If redirection is specified, the ENUM Server returns the valid substitution endpoint host address in the ENUM response. If termination is specified, the ENUM Server returns a non-routable endpoint host address, such as `sip:888888@0.0.0.0`, in the ENUM response, which results the SBC sending a cause code such as a **404 Not Found**. (These responses are user configurable. Regex configuration for termination and redirection may vary, depending on factors such as the type of SBC and its configuration.) SEP Policy processing adds no latency to the call.

Monitor-Only Mode

For environments that do not want or cannot implement call-control policy (such as 9-1-1 call centers), the PolicyGuru Solution can be deployed in a monitor-only mode. In this configuration, no ENUM Servers are deployed, since their function is to make Policy-based call control available. Instead, only one or more Metadata Probes are deployed with the solution. As previously mentioned, the Metadata Probe provides SIP call data to the PolicyGuru application via a passive tap. While the Metadata Probe cannot be used for call control, its data can be used for monitoring and alerting, analytics, and reporting, and is used for Orchestra One call authentication queries. .

Analytics & Reporting

The web-based management GUI provides a predefined set of drill-down, real-time Analytics views that afford a graphical representation of call and Policy disposition events. You can choose to view Call Detail Analytics for either ENUM-derived data or SIP Call Detail/Phone Number Analytics for Metadata Probe-derived data, as described below.

ENUM Call Detail Analytics

Available Real-Time ENUM Call Detail Analytics views (as shown in Figure 6 below) include:

- Average Calls per Second (CPS)
- Total Calls
- Policy Dispositions
- Top 10 Sources
- Top 10 Destinations
- Counts by Source Country
- Counts by Destination Country

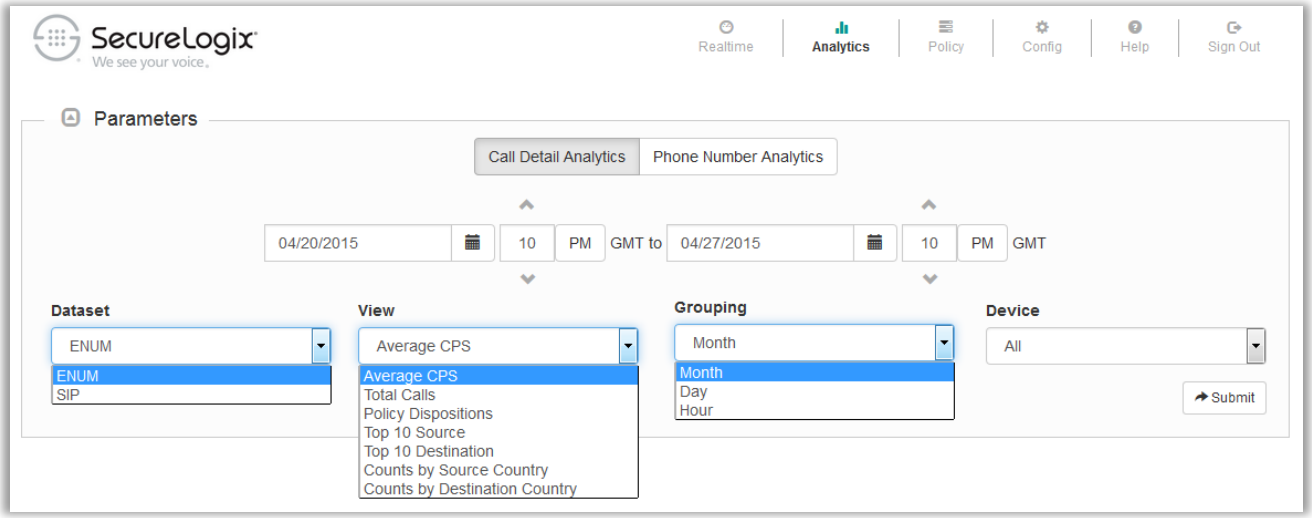

Figure 6: Real-Time Call Detail Analytics Options

When you select criteria and click **Submit**, a drill-down view of the resulting analysis appears, as shown in Figure 7, which illustrates the **Policy Dispositions** Analytics view (that is, allowed, terminated, and redirected).

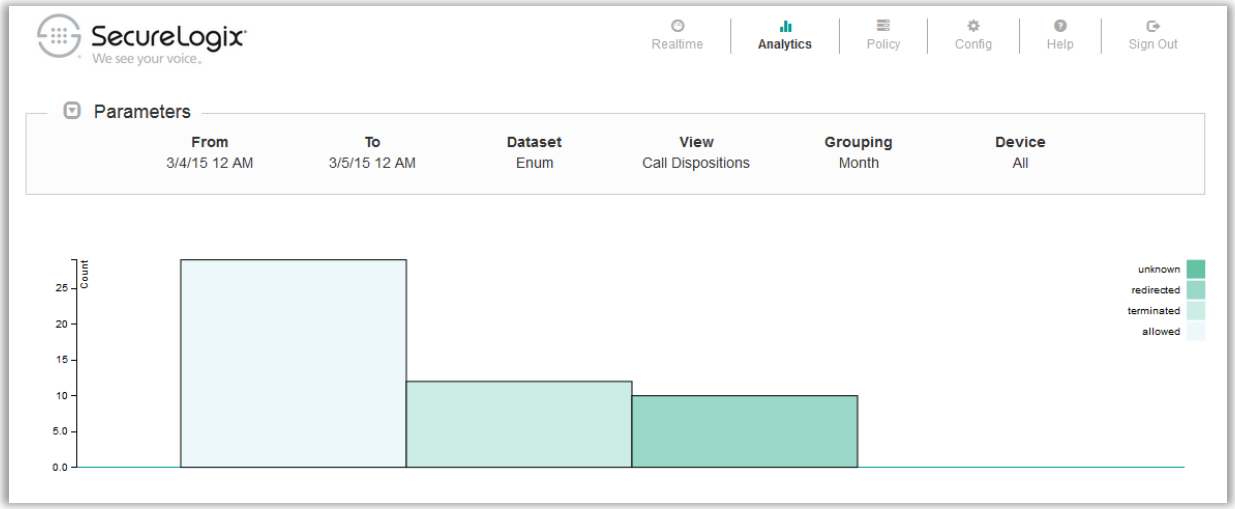

Figure 7: Level 1 Analytics – Policy Dispositions

When you hover your mouse cursor over the data in the display, details about the data appear as an onscreen tooltip. Clicking the display provides a drill-down view of the selected information. Figure 8 shows an example of this view.

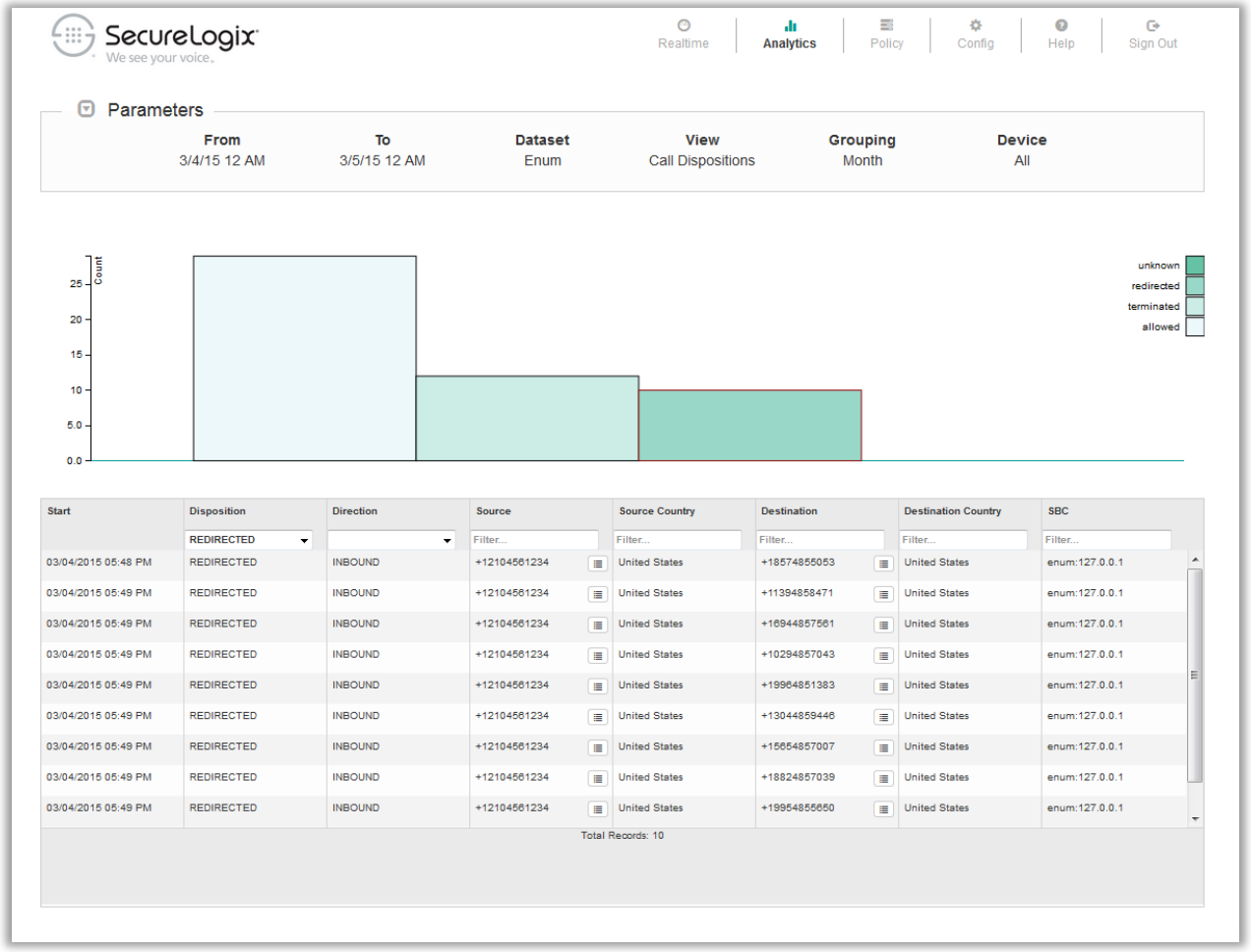

Figure 8: Real-Time Drill-Down Call Detail Analytics – Policy Dispositions Call Details

Real-time Analytics provides more than a view of the information; it also allows you to take action regarding the called and calling numbers provided in the call details. From this drill-down detail view, you can click the icon to the right of any source or destination and add it to a Whitelist or Blacklist, as appropriate, without needing to toggle between screens. You can also export the data from the displayed view by clicking an icon, for offline analysis.

All data for each monitored trunk is also stored in the central PolicyGuru database, where it is available for offline reporting and in-depth Business Intelligence (BI) analysis via third-party tools such as Splunk.

When the PolicyGuru Solution is used in conjunction with SecureLogix® Call Secure™ Managed Service, SecureLogix Analysts also provide complex BI data analysis and reporting.

SIP Call Data Analytics

SIP Call Data Analytics provides views using the complete SIP metadata derived by the Metadata Probe. Available Real-Time SIP Call Detail Analytics views (as shown in Figure 9 below) include:

- Average CPS
- Total Calls
- Call Dispositions
- Top 10 Sources
- Top 10 Destinations
- Counts by Source Country
- Counts by Destination Country
- Concurrent Calls

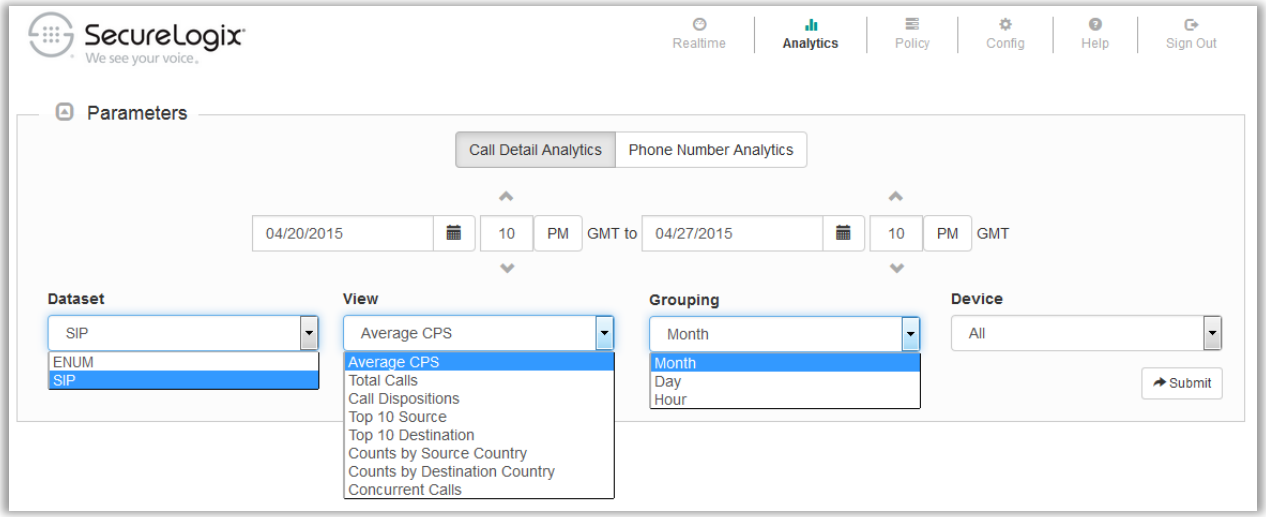

Figure 9: SIP Call Detail Analytics Options

As with ENUM Call Detail Analytics, when you select criteria and click **Submit** to retrieve SIP call detail data, a drill-down view of the resulting analysis appears, and clicking the display provides a drill-down view of the selected information as shown in Figure 10, which shows the **Top Ten Source** view. As with ENUM Call Detail Analytics, you can click the icon to the right of the phone number details to add the number to a Whitelist or Blacklist. You can also export the data from the displayed view for offline analysis by clicking an icon,.

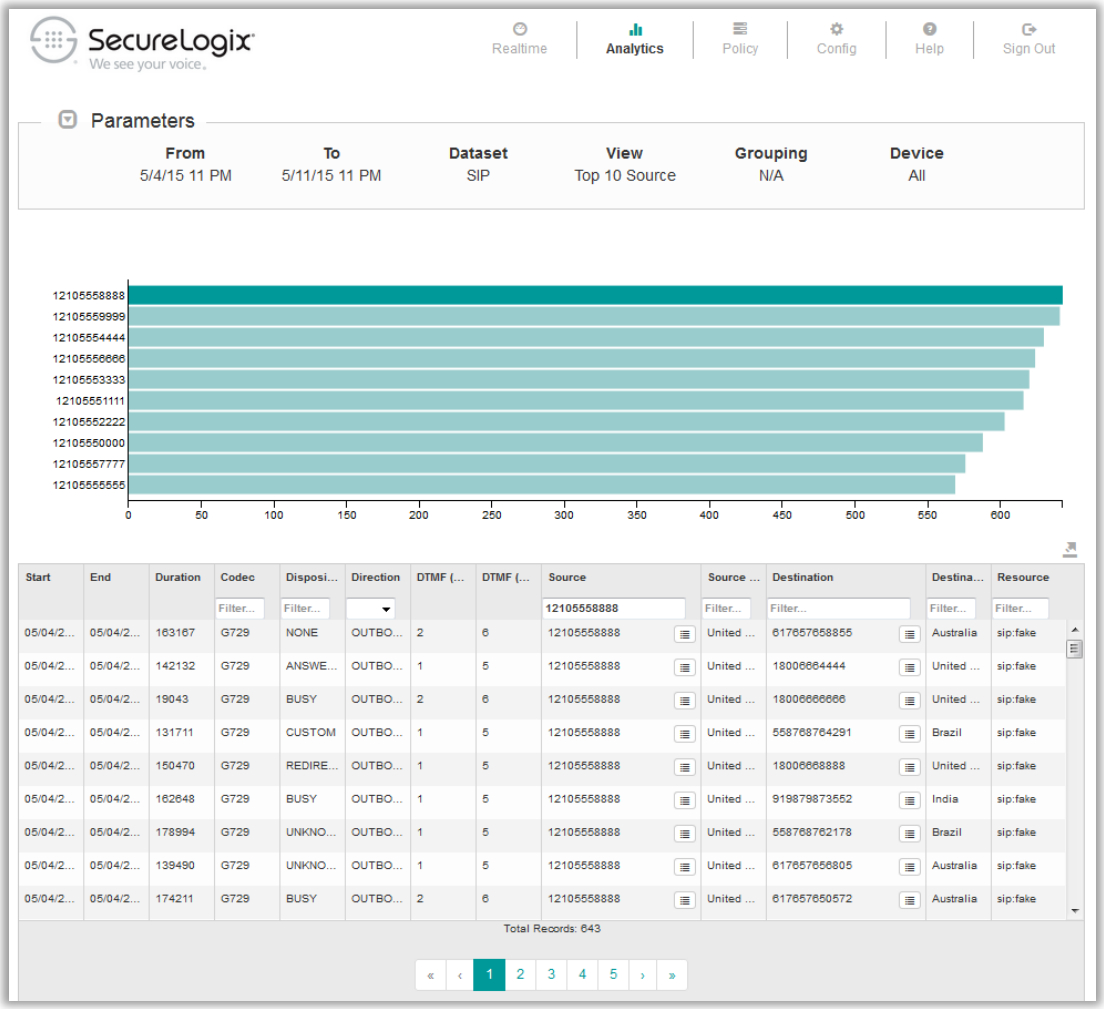

Figure 10: Real-Time Drill-Down SIP Call Data Analytics—Top Ten Source Call Details

In addition to the drill-down call data retrieval functionality, SIP Phone Number Analytics provides a "drill up" feature for forensic analysis of a specific suspect phone number or portion of a phone number (such as +1210). You can search on a specific phone number or portion of a number and retrieve detailed analytics views showing all calling activity associated with those phone number criteria, as shown in Figure 11 and Figure 12.

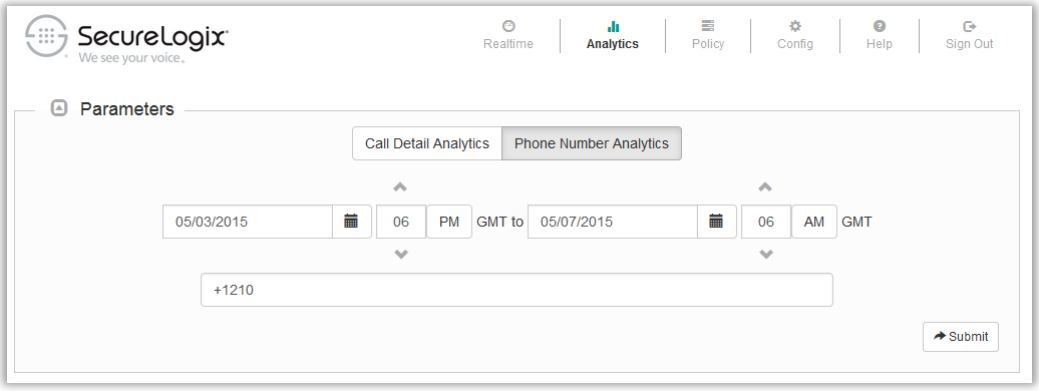

Figure 11: Real-Time Drill-Down SIP Call Data Phone Number Analytics

Figure 12: Real-Time SIP Call Data Phone Number Analytics Results

Alerting and System Events

The PolicyGuru Solution provides various means of alerting users of policy events and system-level concerns at the platform or application layer. Alerts can easily be integrated into Enterprise back-office infrastructure via the industry-standard APIs the PolicyGuru Solution provides.

The PolicyGuru Solution provides the following six methods of reporting policy and system events:

- Local log files on the Server
- Real-time web-interface status display of system events
- Email notifications
- SNMP traps
- Syslog notifications

Real-Time Status GUI

The **Realtime** status screen shows the current calls per second (CPS) for all monitored trunks and a table of up to 20 Policy and system event alert logs occurring in the last 24 hours. This status screen is illustrated in Figure 13.

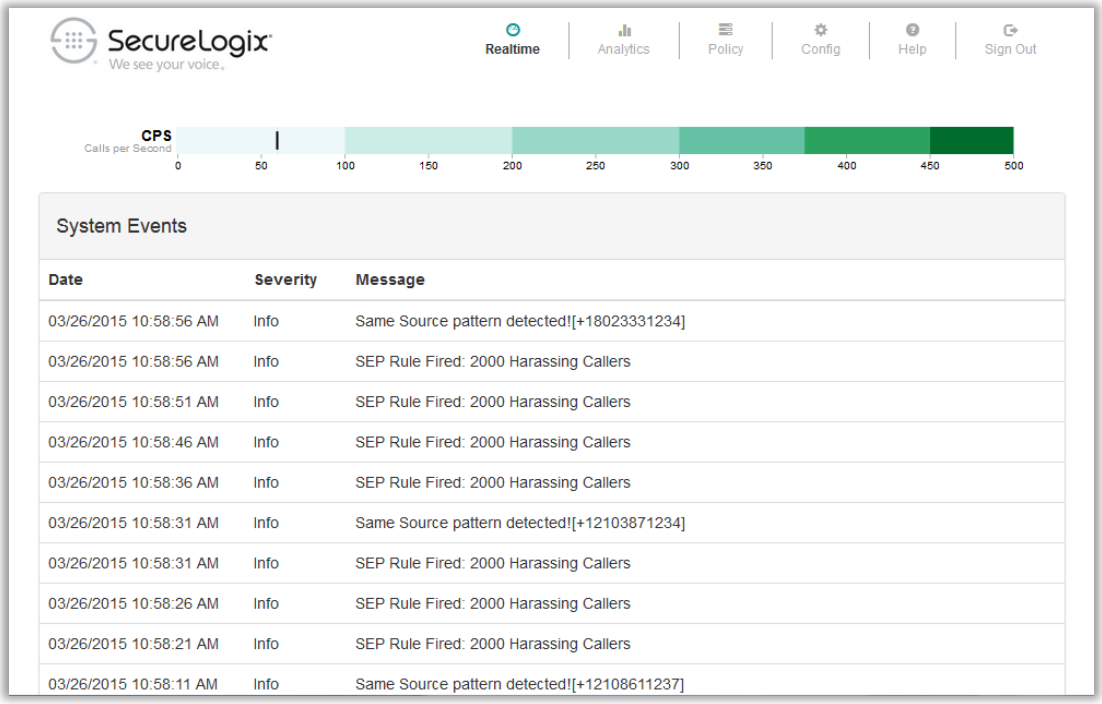

Figure 13: Realtime Status Display Showing Rule-Fired Alerts

Entries in the **Realtime** status screen are color-coded by the severity level, with **INFO** messages in white and progressively deeper colors (these colors may vary based on your display settings) for increasing severities.

System Event Logging

In addition to the **Realtime** status display and alerting, system events are stored in the PolicyGuru Database, from which they can be queried by either a third-party reporting tool or by using a REST API query by event count and/or date/time range.

SNMP

The PolicyGuru Solution supports SNMP alerting in the form of SNMP traps. SNMP is handled internally by the PolicyGuru software and produces SNMP v2 UDP packets based on system configuration. You can also use NetSNMP, available in the Linux installation, with the PolicyGuru Solution to support SNMP monitoring. All 54 Linux MIBS provided by CentOS 6.6 are available with NetSNMP. Operating system, hardware, software, application, health and status, and policy events can all be monitored via SNMP with proper system configuration.

Syslog Notifications

The PolicyGuru Solution supports syslog alerting for Policy Rule firings and system events. Syslog is handled internally by the PolicyGuru software and produces syslog messages based on system configuration via the Management GUI. In addition, monitoring processes are built into the PolicyGuru Solution that provide available syslog alerting for application health and status.

Application State and Health Status

Each application provides monitoring functions to track and provide notifications of application state and health/status changes. These monitoring functions poll for application and key process status using configurable polling intervals. If an application or key process is detected to be in unavailable an unstable state, the monitor attempts to autonomously restarts the affected process to allow the application to recover and resume full functionality, with no user intervention required. Notifications also alert when user intervention is required to remedy an issue.

Status changes are sent to log files on the server. Syslog alerting can also be configured to alert for key health and status indicators, such as application/process restarts. NOC monitoring notifications can be configured for these application health and status notifications.

Policy Rule-Fired Alerts and Notifications

Rules can be configured to alert on SEP Rule firings and for specific SEP Policy dispositions (Allowed, Terminated, Redirected). All of the alerting and logging types mentioned above are available for Policy monitoring.

Management Application

The web-browser-based PolicyGuru Management Application provides access to system configuration and monitoring, List management, user account management, and all of the PolicyGuru Applications. All of these are accessed through the Management Application.main menu. Figure 14 below shows the **System** management screen, which shows the ENUM Servers and Metadata Probes in the deployment. This screen is part of the **Config** application.

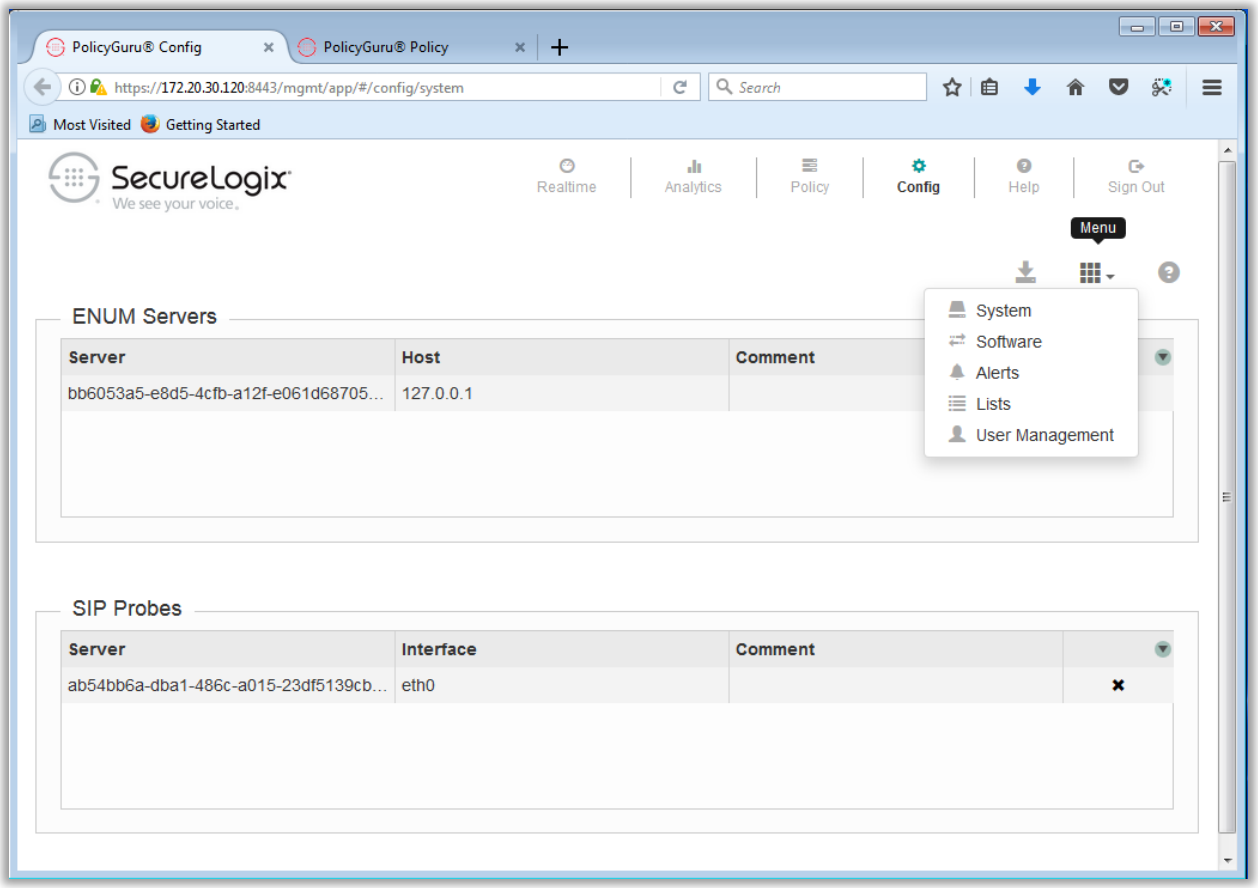

Figure 14: Web-Based Management Application

Architecture Discussion

The highly extensible PolicyGuru Solution platform architecture provides a robust environment that supports rapid integration of new feature sets and capabilities to address the ever-evolving voice/UC network threats and challenges. The solution provides features to monitor for, alert, protect, prevent, and mitigate current, pervasive real-world threats and issues based on call setup information and mid-call SIP signaling information, such as SIP header information, codec, and duration.

The PolicyGuru Solution architecture:

- Provides standards-based interfaces to the SBC.
- Is interoperable with multiple vendors.
- Is scalable, flexible, survivable.
- Is remotely upgradable.

As introduced earlier, the solution is typically deployed on dedicated server platforms running the PolicyGuru Software. Most applications can also be deployed virtually on datacenter COTS hardware that meet minimum resource requirements, or in a Cloud hosting environment. As described earlier, the PolicyGuru Solution architecture includes one or more Mediation Servers, one or more Database Servers, and one or more ENUM Servers and/or one or more Metadata Probes. Each of these applications can be deployed in a redundant, enhanced-availability configuration. See “Enhanced-Availability Deployment Model” on page 26 for details.

Each of these Server applications can be remotely managed via SSH. A high-level description of each component follows.

PolicyGuru Server Applications

Mediation Server

The Mediation Server hosts multiple applications, including the analytics data processing, Policy event processing, Orchestra One integration, and web-interface application(s), along with supporting services for communication to/from the ENUM Servers and Metadata Probes in the network. The Mediation Server sends the SEP Policy Rules configuration to the ENUM Server for real-time processing, receives call data and SEP Policy processing results from the ENUM Server, and generates configured alerts when SEP Rules fire. The Mediation Server sends all SEP Rule configuration and List

updates to the ENUM Servers for immediate enforcement when you install the Policy. The Mediation Server stores all of this data in the central PolicyGuru Database, where it is available for the real-time status and analytics displays and for offline reporting and analytics.

The Mediation Server is the federation point for system management, user interaction and account permissions configuration, and Policy management.

Database Server

The Database Server is housed in a PostgreSQL RDBMS. All call records, policy-processing data, and system events are stored in this database. Up to 13 months of data can be retained in the active database.

ENUM Server

The PolicyGuru ENUM Server provides the Call Processing and Call Control application that interfaces with the SBCs in your network to enforce the Call Firewall security and usage policy rules it receives from the Mediation Server to allow, block, or redirect calls. It provides supporting services for communication to/from the Mediation Server, to which it sends SEP Policy processing results and call data.

As previously discussed, the PolicyGuru ENUM Server is a unique type of DNS Server that accepts and responds to Naming Authority Pointer (NAPTR) type DNS requests from authorized ENUM Clients (e.g., SBCs). This enables the PolicyGuru Solution to provide real-time, policy- based routing decisions to one or more SBCs for security and monitoring policy enforcement.

Before a call leaves the egress interface on the SBC, the SBC provides the source and destination phone numbers in the DNS request to the PolicyGuru ENUM Server and then uses the ENUM Server's policy-based response for continued routing of the call. The ENUM Server processes the source and destination in the DNS request against its PolicyGuru SEP Policy and then responds to the SBC. The ENUM Server's policy-based response dictates how the SBC routes the call—use the original routing, redirect to a routable destination specified in a policy rule, or terminate the call by redirecting to a non-routable destination. PolicyGuru ENUM processing introduces no significant latency to call setup.

The ENUM Server hosts the PolicyGuru Call Processing application, along with supporting services for communication to/from the Mediation Server, from which the ENUM Server receives the policy configuration instructions it executes. SEP Policy enforcement is local to the ENUM Server; it receives policy enforcement instructions from the Mediation Server and then autonomously executes that SEP Policy in response to ENUM requests. When you add or update SEP Policy Rules, you choose when to commit (install) them. When you commit the rule changes, the Mediation Server immediately sends those changes to the ENUM Server, which begins enforcing them as soon as installation completes. The ENUM Server returns policy processing results and call metadata to the Mediation Server, which transfers them to the central database.

ENUM Servers are typically deployed in active-active pairs for redundancy. Each pair of ENUM Servers can support up to 30 SBCs. Each SBC in the enterprise is configured for requests and responses with a given pair of ENUM Servers. In the recommended redundant configuration, each SBC should be configured to first direct its ENUM requests to ENUM Server A, and if it fails to respond, to send the request to ENUM Server B.

A monitoring process on the ENUM Server continually polls the health and status of its processes. When any component of the ENUM Server is determined to be unstable, unavailable, or unreliable, the monitor brings down the ENUM listener port to force failover to the next ENUM Server, and then autonomously shuts down and restarts all components of the affected ENUM Server to attempt to return it to availability.

The ENUM Server is built to Internet Engineering Task Force (IETF) standards to ensure flexibility and interworking with multiple vendors' edge and core SIP devices. The solution supports Acme Packet/Oracle, Sonus, and Cisco CUBE SBCs that have ENUM licensed. Multiple SBCs of the same type can integrate with a given ENUM Server. The Mediation Server supports communication with multiple ENUM Servers, each of which may be integrated with different types of SBCs.

Metadata Probe

The Metadata Probe gathers real-time SIP signaling metadata for use in call monitoring and tracking decisions across the Enterprise network. Via a passive tap, the Probe captures complete call information (metadata) throughout the call, beyond the source and destination information that is available at call setup in ENUM requests. This enables Analytics and reporting to also use additional header information and post-connect call data, such as duration, call state, codec, and call disposition. The Probe sends this additional metadata to the Mediation Server for onscreen analytics reporting, and storage in the central database for offline analysis and reporting. Additionally, if Orchestra One integration is enabled, the Probe data is used in the Orchestra One requests.

The Metadata Probe can be deployed in redundant sets (N+1) to provide redundancy. In this recommended configuration, a monitoring process on the Probe continually polls the health and status of its processes. When any component of the Probe is determined to be unstable, unavailable, or unreliable, it closes the tap link on that Probe to force failover to the next Probe. The monitor autonomously shuts down and restarts all components of the affected Probe to attempt to return it to availability. The passive tap device is configured to send the SIP data to whichever Probe has its port open.

Web-Based Management Graphical User Interface (GUI)

The web-based management GUI provides access to the system for policy implementation and management, graphical drill-down call and policy result analytics, system alert monitoring, user account permission configuration, and remote system management.

Enhanced-Availability Deployment Model

The PolicyGuru Solution can be deployed in a distributed Enhanced Availability model to allow for rapid system recovery in the event of active management cluster failure. In this configuration model, you deploy two Mediation Server and Database Server pairs at separate sites as active and warm-standby management cluster pairs. These sites can be in different locations on the same campus or in different locations across the country or continent. Global deployments where the two locations are on different continents are not supported.

In this model, one Mediation Server/Database Server pair is the active pair at any time to support normal operations, while the secondary pair is in warm-standby mode, ready to be placed in the active role if normal operations of the currently active pair are impaired. The secondary servers are powered on but are not active at the PolicyGuru application level. The standby Database Server is regularly synchronized with the active Database Server and the active Mediation Server configuration is regularly backed up to the standby Mediation Server so its configuration can be imported in a matter of minutes to the standby when failover is needed. These synchronization and backup processes are automated on a regular, configurable schedule (at least daily).

When failover to the standby cluster is warranted, you simply bring up the PolicyGuru application services on the warm standby Mediation Server and Database and then point the ENUM Servers and Probes to their IP addresses to restore full functionality. After issues that warranted the failover are addressed, the formerly active server pair assumes the warm standby mode, including receiving automated Database synchronization and Mediation Server configuration backup from the now-active management pair.

SecureLogix® Server Platforms

SecureLogix® Server Platforms are rack- mountable server platforms that support one or more of the PolicyGuru® Meta-Policy Controller applications: Mediation Server, Real-Time Database, ENUM Server, and Metadata Probe.

SecureLogix offers lines of general purpose compute servers, network-optimized servers, and storage servers in sizes to accommodate any size deployment: micro, small, large, extra-large (XL), 2XL, and 4XL.

- **C-Series SecureLogix® Servers**—General purpose compute servers that support the PolicyGuru ENUM Server and Mediation Server applications.
- **N-Series SecureLogix® Servers**—Network-optimized servers that support the PolicyGuru Metadata Probe application.
- **S-Series SecureLogix® Servers**—Storage-optimized servers that support the PolicyGuru Database.

Call Capacities

The PolicyGuru Solution supports high-volume SIP networks with either centralized or distributed trunking. Call capacities depend on the server platform resources, whether both the Metadata Probe and ENUM Server are deployed, and the number and type of installed policy rules in the deployment. In a physical deployment on the XL sized SecureLogix Servers, the PolicyGuru Solution was tested to support up to 150 CPS.

In a virtual deployment, comparable call capacities apply when appropriate resources are supplied to the virtual machines.

Solution Security

The PolicyGuru Solution was designed and implemented to a high standard of security. For example, port/IP security is managed via Iptables configuration, and IPSec can be configured between components for additional security. Web GUI connections are always secured with TLS.

Access to the PolicyGuru Applications is only allowed for authorized users and access is controlled by either user accounts with strong password restriction capabilities or by LDAP authentication. One of these methods of user identification is required to log into any solution component. Idle GUI and SSH session timeouts help to guard against unauthorized access via an unattended workstation.

Since the PolicyGuru Applications run on dedicated, general-purpose systems, SecureLogix follows and recommends accepted industry best practices for the configuration and set up of these systems. Obviously, these practices include keeping all system patches up to date and eliminating any services running on those systems that are not required to support PolicyGuru Solution operation. SecureLogix continuously monitors industry sources for information on security advisories and issues associated with these systems and passes along this information to customers as they are identified.

Only necessary applications are running on any PolicyGuru Server or the operating system on the host platform to ensure a high standard of security. During the installation of the operating system, all services that are not necessary for the system to function properly are disabled. Each of the open ports on PolicyGuru Solution components has been configured to communicate only with other servers in the deployment, with the exception of SSH, ARP, and ICMP traffic. ICMP traffic can be disabled if the administrator wishes. Username and password or LDAP authentication is required to access any open port. The Linux kernel also runs the Iptables firewall for port/IP security.

User Account Management

Access to the system is controlled by user accounts with strong password restriction capabilities or by LDAP authentication. Both Active Directory and OpenLDAP are supported for LDAP authentication. When LDAP authentication is used, LDAP groups can be used to provide application-level permissions that govern which authorized users can access the Realtime, Policy, System Configuration, and Analytics Web applications. LDAP groups also can be used to govern who is authorized to log in to the host platforms via SSH.

Figure 15 shows the **User Management** GUI for configuring LDAP group-based Web-application-user permissions.

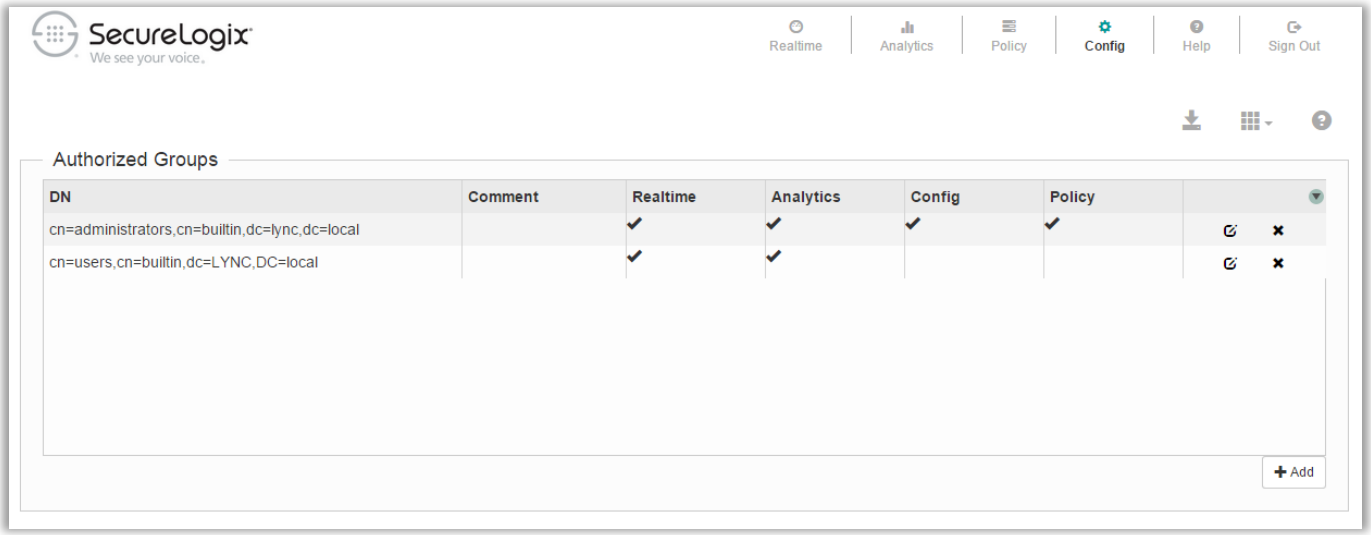

Figure 15: LDAP Group-Based Application Permissions Configuration

Reliability

All components in the PolicyGuru Solution can be deployed in a redundant, fault-tolerant configuration to ensure reliability and Policy processing and system availability.

After you define and install the SEP (Firewall) Policy on the ENUM Servers in your deployment, the ENUM Servers enforces the policy autonomously, even in the unlikely event that connection to the Mediation Server is temporarily disrupted. As mentioned earlier, ENUM Servers are typically deployed in active-active pairs for HA; the SBC is configured to automatically send ENUM requests to the second active ENUM Server if one server in the redundant pair is temporarily unavailable, ensuring that your security policy is continuously enforced.

During an unlikely disconnection from the Mediation Server, the ENUM Server retains the call and policy processing data and then sends it to the Mediation Server when the connection is restored. The Mediation Server runs the installed CEP policy against the call data when it receives it, fires any applicable Alerting rules, and stores the data in the database as usual.

System and Network Considerations

Supported SBCs

The PolicyGuru Solution supports SBCs from ACME Packet/Oracle, Sonus, and Cisco Systems.

Software Updates

Updates to the installed PolicyGuru Solution can be remotely applied via SSH. The solution uses YUM/RPM as a vehicle for operating system and application updates from a configurable repository, secured over a secure means.

Supported Browsers

The web-browser-based Management GUI supports following browsers:

- Internet Explorer (version 11 or later)
- Mozilla Firefox
- Google Chrome

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • (210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • https://support.securelogix.com