AMERICAN TECHNOLOGY CLOUD, LLC

mutare

Mutare Voice™

Spam Filter

Feature Description

Get the Message.

Table of Contents

Introduction

Voice spam, including robocalls, abusive callers, scam calls, “spoof” callers, and annoying sales calls, cause employee frustration, lost productivity and damage your bottom line. Mutare has an enterprise solution that dramatically reduces voice spam for inbound calls, is easy to manage and pays for itself in productivity gains almost immediately after switching it on.

The Mutare Voice Spam Filter guards your voice network by filtering incoming calls, allowing legitimate business calls through while blocking spam callers. Unlike some spam solutions that ring your phone and interrupt your workflow, the Mutare Voice Spam Filter is designed to divert spam calls without ever ringing your phone. Because voice calls are the life blood of business, the feature was designed to “do no harm,” stepping out of the call path in the event of a failure and never “listening” into the call medium. The filter simply looks at the call signal data ensuring call integrity and security.

The Mutare Voice Spam Filter can be licensed and deployed as part of a complete Mutare Voice call completion solution or as a stand-alone call filtering solution. This document focuses specifically on the voice spam filter application. For more information on Mutare Voice call completion, please consult with your Mutare Regional Sales Manager.

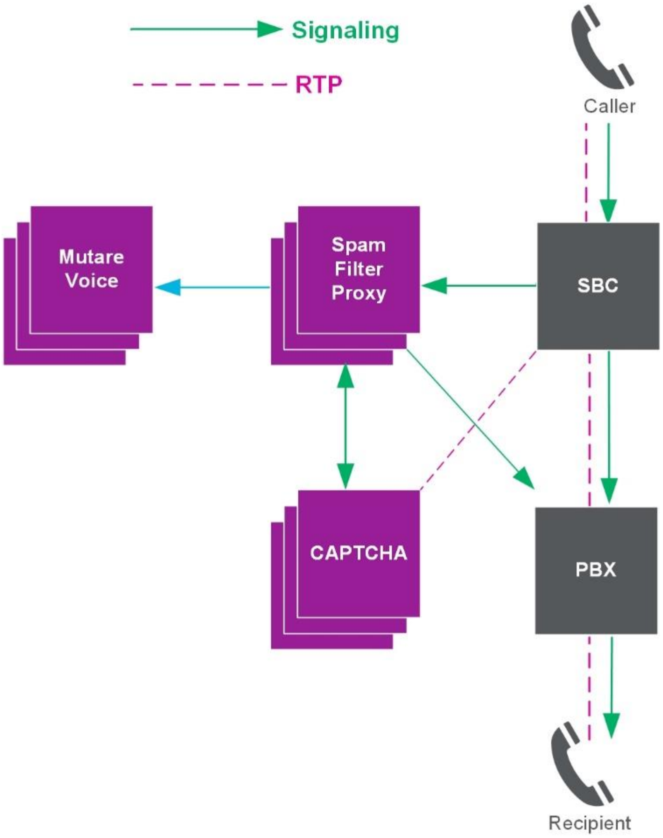
How Mutare Voice Spam Filter Works

The Mutare Voice Spam Filter relies on modern Session Initiation Protocol (SIP) digital communication. It examines the signaling information transmitted with the SIP call to identify the caller ID. Within one second, the filter checks the caller ID against enterprise whitelists and blacklists, as well as dynamic robocall list(s) and, optionally, a spoof call detection system. Whitelisted calls are passed through. Blacklisted or suspect calls are diverted to a recording, filtered through the Mutare CAPTCHA, or simply disconnected based on rules set up by the system administrator. Call screening is typically completed in under a few hundred milliseconds, making the system completely transparent to callers and your employees.

SIP Call Handling

The Mutare Voice Spam Filter employs two virtual servers that work in conjunction with your SIP Session Border Controllers (SBC), plus a third virtual server if deployed with CAPTCHA screening capabilities.

The diagram below depicts a simplified reference architecture.



For each incoming call, the Session Border Controller (SBC) directs the SIP invite to a weighted route pointing to the Mutare Voice Spam Filter proxy server. The proxy does not answer the call and no real time transport protocol (RTP) is passed. The proxy makes an API call containing the caller ID and called party ID to the Mutare Voice servers, where the data is analyzed. This analysis includes spoof detection, rules engine, and external robocall database. At this point, the determination is made on the action to take for the call:

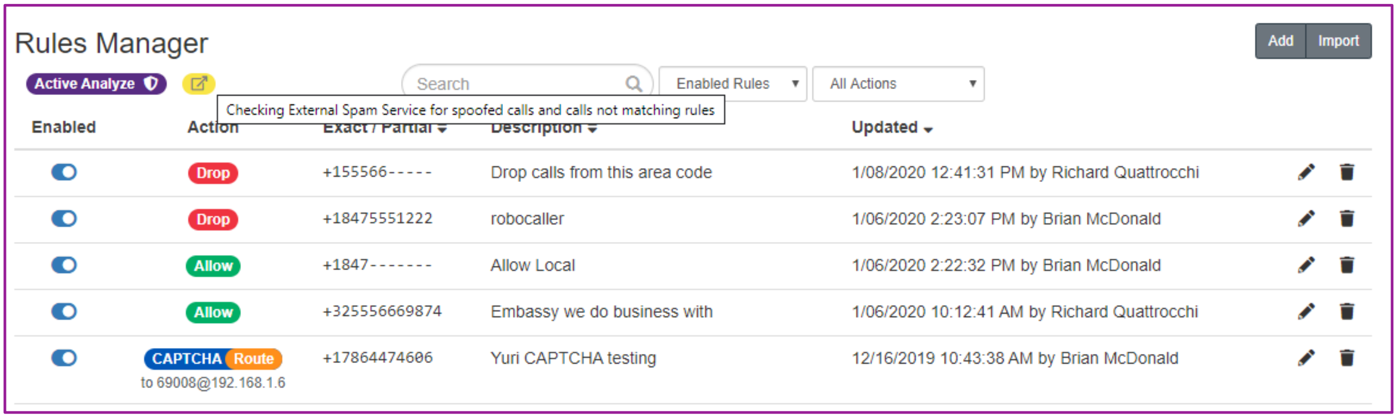
1. Allow - Release the call to its original destination, typically through the PBX as shown.
2. Route – Divert the call to another destination, defined in the Mutare Voice Spam Filter, typically through the PBX as shown.
3. CAPTCHA – Divert the call to the CAPTCHA servers, where the caller is presented with a simple reverse Turing test. If the caller passes, the call is transferred on to its original destination, typically through the PBX as shown. If the caller fails, the call is dropped or diverted to another destination, defined in the Mutare Voice Spam Filter, typically through the PBX as shown.
4. Drop – The call is dropped.

The entire process is completed in a few hundred milliseconds and the system can handle 150 calls per second, serving the needs of any size enterprise.

Rules Management

Mutare Voice Spam Filter includes the option to create enterprise-specific blacklists and whitelists. These are maintained by an administrator through the Rules Manager page. Lists can be synchronized with external databases, updated via upload, or manually edited. The system logs all list activity and filter settings by admin, providing full traceability for troubleshooting.

From the Rules Manager page, Administrators can identify and apply actions to specific numbers or create a rule that applies to all numbers with a partial match (such as a specific area code or DID). The Rules Manager page displays all numbers or partial numbers that have been included, their description and date entered, as well as the action that will be applied to each (Drop, Route or Allow; Drop or Route failed calls if CAPTCHA has been applied).

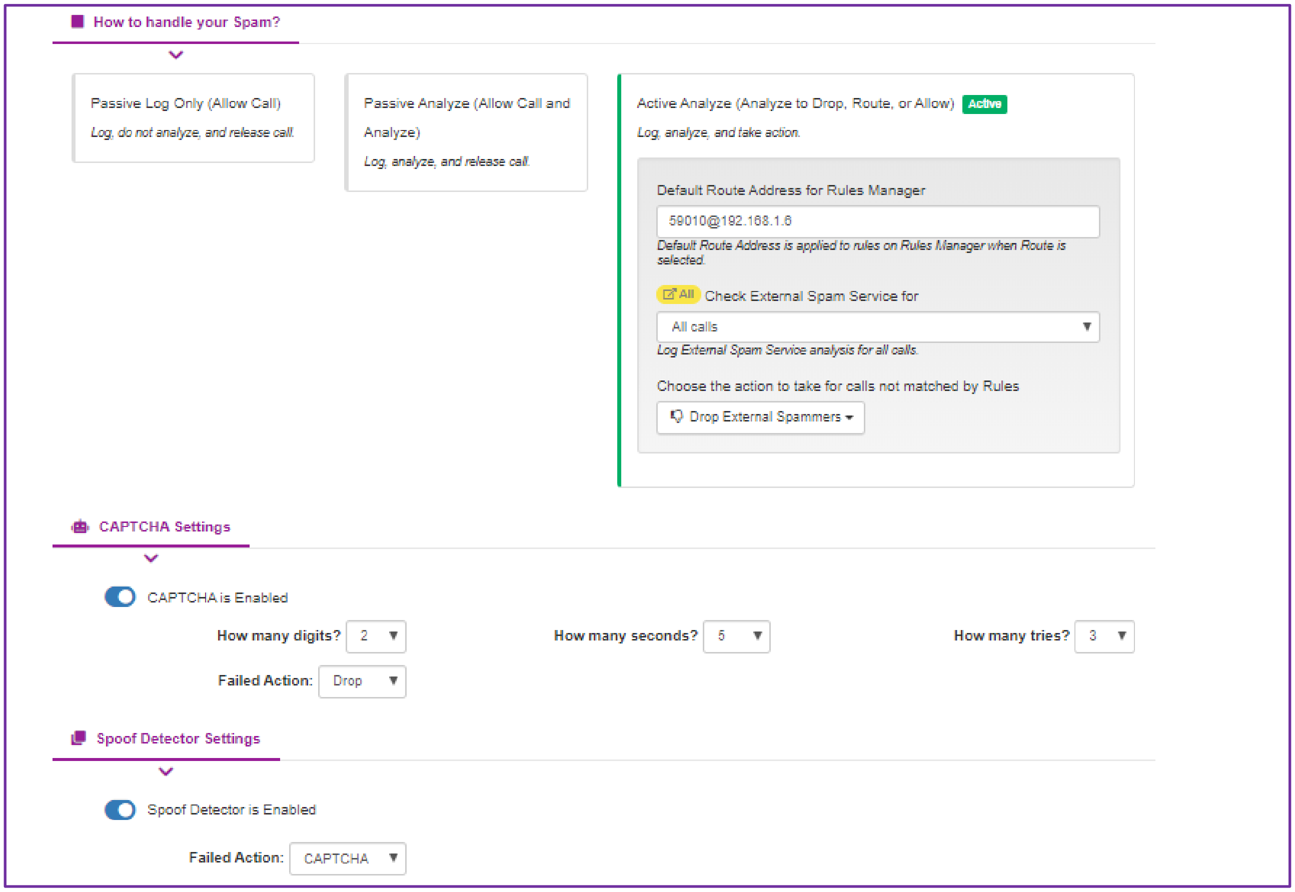


Checking External Spam Service for spoofed calls and calls not matching rules

Enabled	Action	Exact / Partial	Description	Updated		
●	Drop	+155566-----	Drop calls from this area code	1/08/2020 12:41:31 PM by Richard Quattrocchi	✎	🗑
●	Drop	+18475551222	robocaller	1/06/2020 2:23:07 PM by Brian McDonald	✎	🗑
●	Allow	+1847-------	Allow Local	1/06/2020 2:22:32 PM by Brian McDonald	✎	🗑
●	Allow	+325556669874	Embassy we do business with	1/06/2020 10:12:41 AM by Richard Quattrocchi	✎	🗑
●	CAPTCHA Route to 69008@192.168.1.6	+17864474606	Yuri CAPTCHA testing	12/16/2019 10:43:38 AM by Brian McDonald	✎	🗑

Control Panel

The Mutare Voice Spam Filter employs a graphical user web interface for easy administration. From the Control Panel, Administrators configure how identified spam and robocalls will be handled.



How to handle your Spam?

Passive Log Only (Allow Call)
Log, do not analyze, and release call.

Passive Analyze (Allow Call and Analyze)
Log, analyze, and release call.

Active Analyze (Analyze to Drop, Route, or Allow) Active
Log, analyze, and take action.

Default Route Address for Rules Manager: 59010@192.168.1.6
Default Route Address is applied to rules on Rules Manager when Route is selected.

All Check External Spam Service for: All calls ▼
Log External Spam Service analysis for all calls.

Choose the action to take for calls not matched by Rules: Drop External Spammers ▾

CAPTCHA Settings

CAPTCHA is Enabled

How many digits? 2 ▼ How many seconds? 5 ▼ How many tries? 3 ▼

Failed Action: Drop ▼

Spoof Detector Settings

Spoof Detector is Enabled

Failed Action: CAPTCHA ▼

Operating Modes

The Mutare Voice Spam Filter has three operating modes as part of the “do no harm” deployment criteria:

- **Passive Logging Only –** The filter is essentially “off” and only logging calls but not performing any analysis. This gives administrators the ability to rapidly switch off the system, but still retain call logging. This mode is the ultimate “safety valve” to remove the filter from the call flow equation yet maintain call statistics.
- **Passive Analyze Mode –** The filter will log and evaluate calls against the rules engine and, if enabled, an external spam filtering list(s) but releases all calls. If applying an external spam filter, admins have the option to apply the filter to all calls or only those that are not already identified through organization generated rules. This enables admins to monitor, view and report on what

the system would have released or blocked and enables administrators to evaluate performance without actively filtering any calls. This mode can be useful in evaluating the performance of the spam filter before actual use.

- **Active Analyze Mode –** In this mode, your system will filter incoming calls against the enterprise Rules Manager list and, if enabled, an external spam filtering list(s), and take action to drop, route or allow flagged calls. If an external filter is applied, admins can determine whether actions should be applied to no calls, all calls, or only calls not already handled through the enterprise-generated rules. Admins can also specify the diversion behavior for flagged calls, including drop, route, or send through CAPTCHA screening, which is a reverse Turing test used to separate live callers from bots. Calls that pass the CAPTCHA screening will be allowed through; those that fail will be dropped our routed depending on admin preferences.

In Active Analyze Mode, Administrators can select to have the Spam Filter applied to all calls or only calls that do not match rules criteria, and then select what action to apply to identified spam callers; Drop, Route, and send to CAPTCHA screening.

CAPTCHA Settings

The voice CAPTCHA screens incoming calls by answering the call. The caller is challenged with a reverse Turing test and asked to input randomized digits. This test separates bot calls from human calls. Calls that pass CAPTCHA screening are sent to the called party. Calls that fail CAPTCHA will be dropped or redirected. The systems admin can adjust the CAPTCHA settings for number of digits, number of attempts and time out.

Spoof Detector Settings

If the Spoof Detector is enabled, the Spoof Detector Settings section of the Control Panel will be available for managing configurations.

Spoof calls are those that present with a caller ID that does not match the actual caller source and so are suspect scammers. Mutare Voice Spam Filter has built-in analytical tools designed to detect suspected spoof calls and flag them as possible spam. The Spoof Detector can be tuned to a specific organization’s call traffic patterns

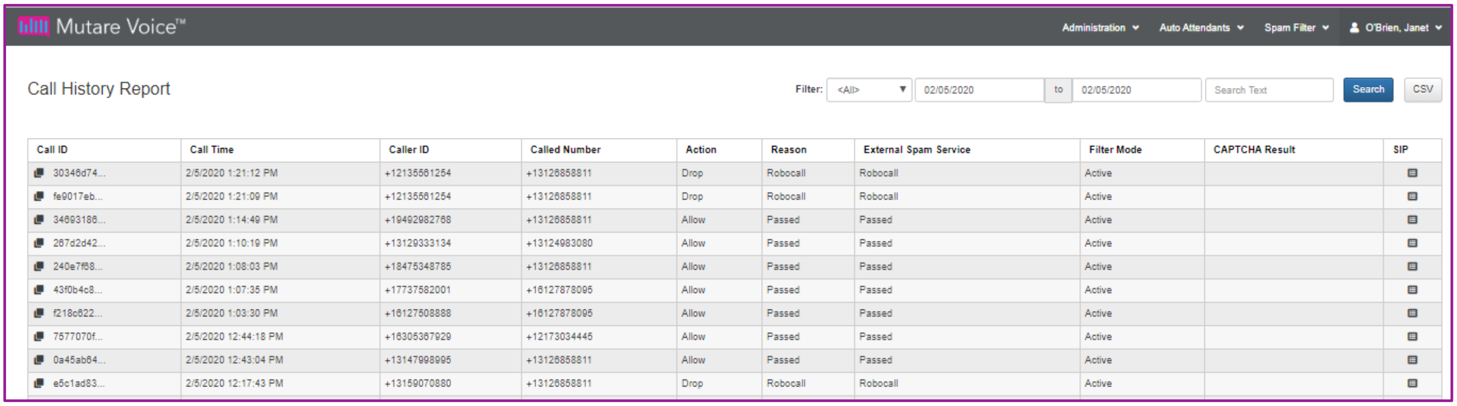
Through the control panel, Administrators can select whether suspected spoof calls will be Dropped, Routed, or sent to the CAPTCHA screening.

Reporting

The Mutare Voice system includes extensive logging of all system functions and provides reports on all filtering actions. Data is displayed in tabular formats and includes graphical summaries. Reporting data can be exported as a .CSV file for use in external analysis and reporting.

Spam Filter Call History Report

The Call History report is a log of all calls identified by Call ID, Call Time, Caller ID, Called Number, Action, Reason, External Spam Filter Service results, the Filter Mode at time of processing, CAPTCHA results, and SIP information.



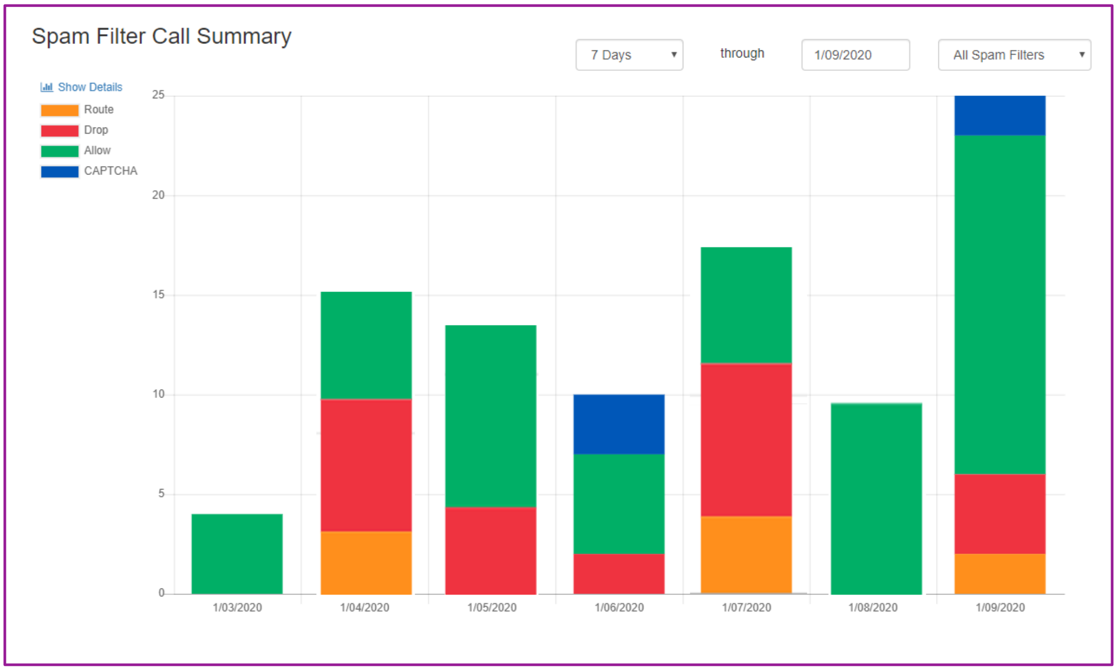
Call History Report

Filter: <All> 02/05/2020 to 02/05/2020 Search Text Search CSV

Call ID	Call Time	Caller ID	Called Number	Action	Reason	External Spam Service	Filter Mode	CAPTCHA Result	SIP
30346d74...	2/5/2020 1:21:12 PM	+12135561254	+13126858811	Drop	Robocall	Robocall	Active		▤
fe9017eb...	2/5/2020 1:21:09 PM	+12135561254	+13126858811	Drop	Robocall	Robocall	Active		▤
34693186...	2/5/2020 1:14:49 PM	+19492982768	+13126858811	Allow	Passed	Passed	Active		▤
267d2d42...	2/5/2020 1:10:19 PM	+13129333134	+13124983080	Allow	Passed	Passed	Active		▤
240e7f68...	2/5/2020 1:08:03 PM	+18475348785	+13126858811	Allow	Passed	Passed	Active		▤
43f0b4c8...	2/5/2020 1:07:35 PM	+17737582001	+16127878095	Allow	Passed	Passed	Active		▤
f218c622...	2/5/2020 1:03:30 PM	+16127508888	+16127878095	Allow	Passed	Passed	Active		▤
7577070f...	2/5/2020 12:44:18 PM	+16305367929	+12173034445	Allow	Passed	Passed	Active		▤
0a45ab64...	2/5/2020 12:43:04 PM	+13147998995	+13126858811	Allow	Passed	Passed	Active		▤
e5c1ad83...	2/5/2020 12:17:43 PM	+13159070880	+13126858811	Drop	Robocall	Robocall	Active		▤

Spam Filter Call Summary Report

The Spam Filter Call Summary report is a graphical presentation of calls that have been processed through the spam filtering system. The overview graph displays how filtered calls have been handled (Route, Drop, or Allow, CAPTCHA screened) during a specified date range.



Spam Filter Call Summary

7 Days through 1/09/2020 All Spam Filters

System Requirements and Functions

- Requires SIP Trunks
  - Utilizes SIP invitation headers to filter calls by header data
- SBC Weighted A/B Routing Configured by System Admin
  - A route points to Mutare Voice Proxy Server
  - B route points to next hop (typically a PBX)
- Proxy Filter Server – Virtual CentOS Linux Server
  - API call to Mutare Voice Server
  - Direct SBC to block call
  - Allow call by sending invite to next hop
  - Route call by diverting invitation header to another resource such as voicemail, IVR, auto attendant or CAPTCHA
- CAPTCHA – Virtual Debian Linux Server
  - Reverse Turing IVR
- Mutare Voice Server – Virtual Windows Server
  - Control Panel
  - Rules Manager
    - Allow call
    - Block call
    - Route call to another resource
    - External Robocall Database (Requires Internet Access)
    - Spoof detection
  - Admin Interface
  - Reporting
    - Log SIP invitation and all actions
    - Call History Report
    - Call Summary
    - CSV File Export

Roadmap

Mutare is dedicated to continuous improvement of the voice spam filter. So long as VoIP calling is virtually free, just like email, bad actors will evolve their techniques, technology and socially engineered scams to make illegal gains using automated voice calls. Mutare maintains a robust roadmap and is continually improving the Mutare Voice Spam Filter to identify new exploits and techniques and use counter measures to cost-effectively stop voice spam. Mutare works with a network of partners including carriers, regulators, database providers, telephony hardware and software vendors, end users and security partners to ensure the voice spam filter is state of the art. To learn more about the Mutare Voice Spam Filter under NDA, please reach out to your Mutare Regional Sales Manager to set up a presentation.