

The Protector That Your System Deserves



## PRODUCT OVERVIEW

# **sipPROT**

---

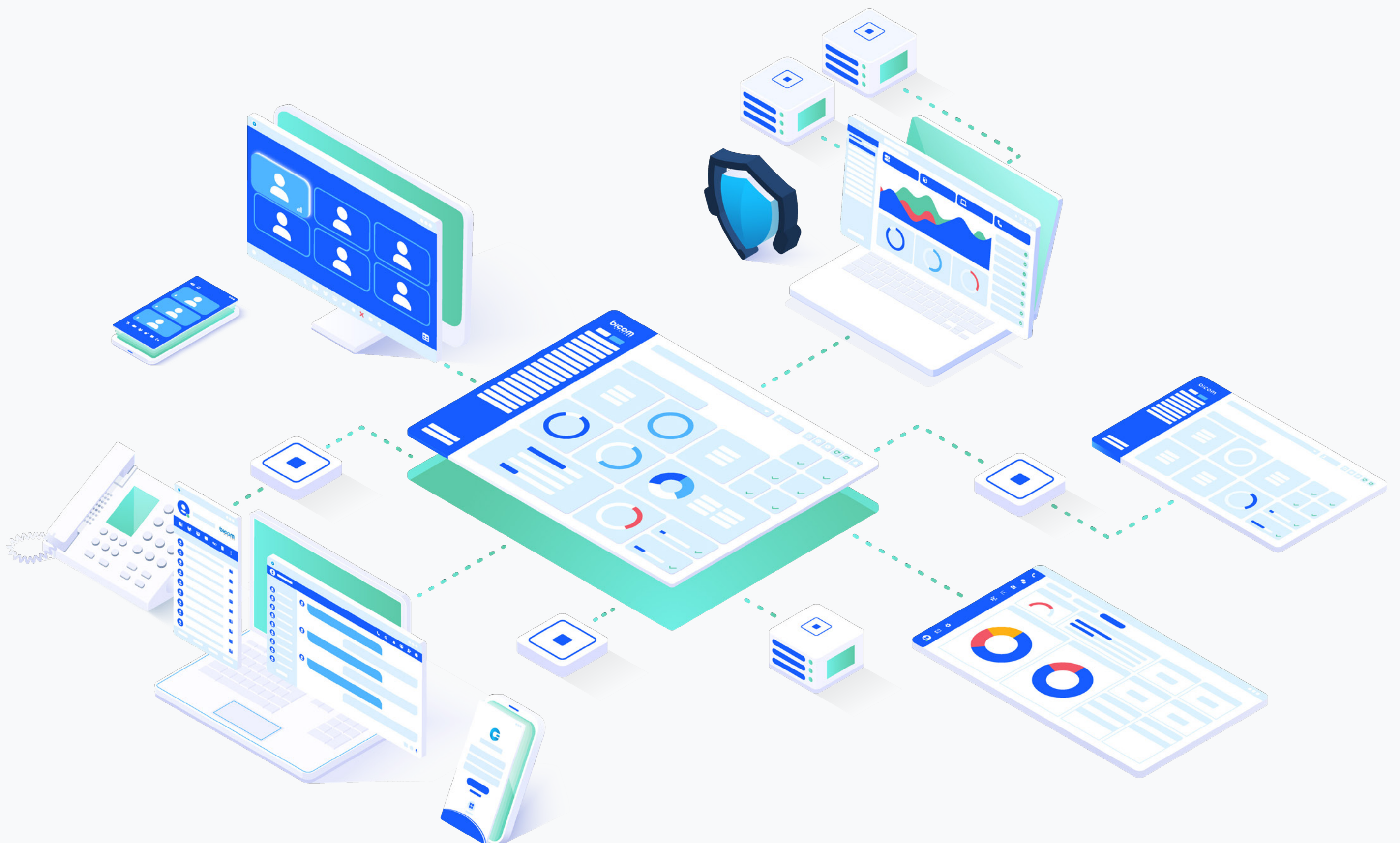


[wiki.bicomsystems.com](http://wiki.bicomsystems.com)

# WHAT IS sipPROT?

sipPROT is Bicom Systems' own answer for a defensive measure against SIP attacks. It's a module that works together with PBXware and SERVERware that monitors live SIP traffic and detects potential abnormalities. Once detected, sipPROT locks them out by updating the firewall or by blocking the IP address directly, without requiring any input from your end other than adjusting the length of the lockout period.

sipPROT is equipped with a strong defensive arsenal which protects some of the core aspects of the system, be it from SIP attacks through the use of SIP scanner protection and SIP protocol anomaly detection, or from TFTP attacks by utilizing TFTP brute force protection, all of which are some of the most common and damaging cyber security risks.








## Swift Threat Response

sipPROT rapidly detects and blocks potential security threats in your SIP system, safeguarding it without permanent lockouts. This automated defense minimizes manual intervention and ensures system security.

## Efficient Security Management

sipPROT streamlines security with auto-provisioning attack detection, allowlist/denylist management, and GeoIP blocking. It identifies vulnerabilities, simplifies list management, and enhances security efficiency, reducing administrative workload.



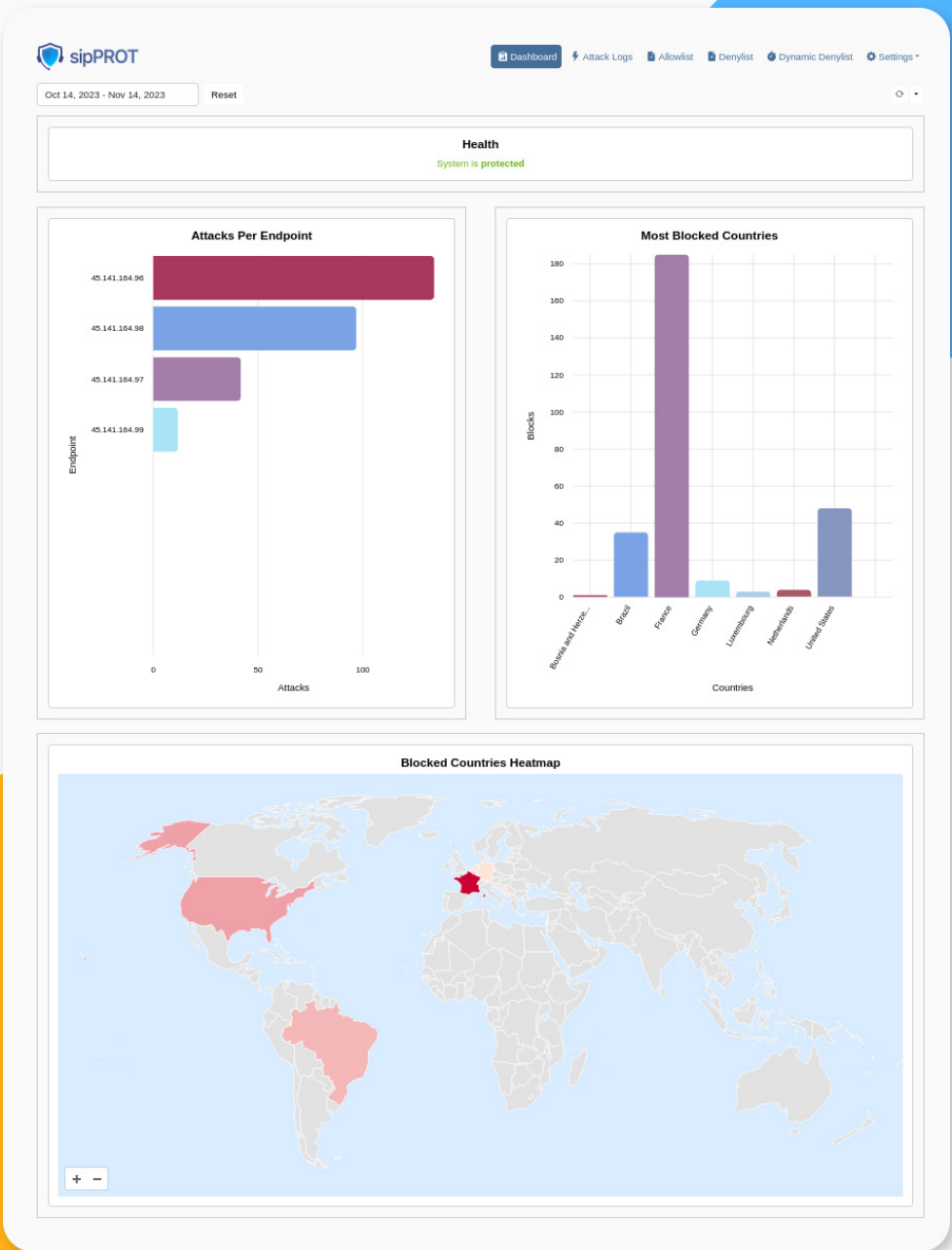


# Essential Unified Communications Features & Benefits

## DETAILED DASHBOARD

Gain complete insight into the inner workings of host operations and actions through the sipPROT dashboard.

Check anything from firewall status to number of attacks per endpoint as well as the corresponding geo-IP data.



## COMPLETE HOST OVERVIEW

Have full insights into the current status of every host within the cluster. Everything from host name and IP address, to each host's Kernel and sipPROT version as well as their sipPROT and Geo protection activity status, making host management a breeze.

You can even remove hosts that sipPROT is not running on at the click of a button or navigate back to the host's corresponding attack log to make host-related actions easier to decide on.

Attack Logs					Host: SW-public1	
Search		Attack Type	Mar 29, 2024 - Apr 5, 2024		Reset	15 Per Page
Attacker IP Address	Victim IP Address	Attack Type	User Agent	Time		
> 45.143.9.162	45.141.164.100	OPTIONS	friendly-scanner	Apr 5, 2024 08:37:16 CEST	<input type="checkbox"/>	
> 45.143.9.162	45.141.164.95	OPTIONS	friendly-scanner	Apr 5, 2024 08:37:16 CEST	<input type="checkbox"/>	
> 45.143.9.162	45.141.164.101	OPTIONS	friendly-scanner	Apr 5, 2024 08:37:16 CEST	<input type="checkbox"/>	
> 45.143.9.162	45.141.164.92	OPTIONS	friendly-scanner	Apr 5, 2024 08:37:16 CEST	<input type="checkbox"/>	
> 174.142.205.18	45.141.164.92	OPTIONS	friendly-scanner	Apr 5, 2024 08:34:04 CEST	<input type="checkbox"/>	
> 188.166.166.80	45.141.164.97	REGISTER	FPBX	Apr 5, 2024 07:58:49 CEST	<input type="checkbox"/>	
> 188.166.166.80	45.141.164.97	REGISTER	FPBX	Apr 5, 2024 07:58:49 CEST	<input type="checkbox"/>	
> 188.166.166.80	45.141.164.97	REGISTER	FPBX	Apr 5, 2024 07:58:49 CEST	<input type="checkbox"/>	
> 188.166.166.80	45.141.164.97	REGISTER	FPBX	Apr 5, 2024 07:58:49 CEST	<input type="checkbox"/>	
> 185.224.128.12	45.141.164.100	OPTIONS	friendly-scanner	Apr 5, 2024 07:27:02 CEST	<input type="checkbox"/>	
> 185.224.128.12	45.141.164.101	OPTIONS	friendly-scanner	Apr 5, 2024 07:27:02 CEST	<input type="checkbox"/>	
> 185.224.128.12	45.141.164.96	OPTIONS	friendly-scanner	Apr 5, 2024 07:27:02 CEST	<input type="checkbox"/>	
> 185.243.5.55	45.141.164.92	OPTIONS	friendly-scanner	Apr 5, 2024 06:41:19 CEST	<input type="checkbox"/>	
> 185.243.5.55	45.141.164.95	OPTIONS	friendly-scanner	Apr 5, 2024 06:41:19 CEST	<input type="checkbox"/>	
> 188.166.166.80	45.141.164.97	REGISTER	FPBX	Apr 5, 2024 06:39:38 CEST	<input type="checkbox"/>	
2,023 total						

# DYNAMIC BLOCKING AND UNBLOCKING

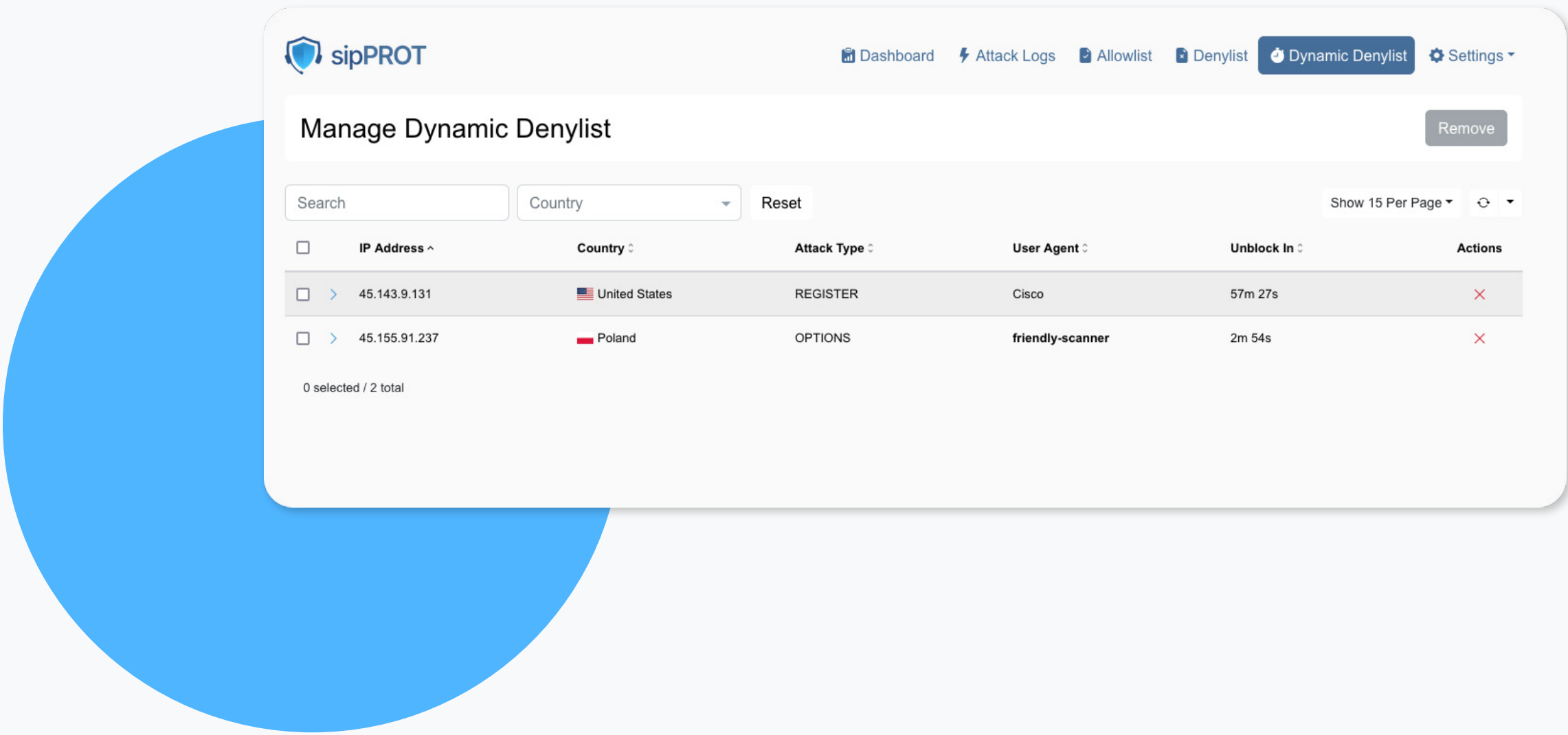
One of sipPROTs main assets is its ability to react quickly when it detects a threat, automatically blocking down the IP address of a potential attack and keeping your system safe from what would've been a potential breach.

When an IP address gets dynamically blocked on one host, it gets locked out across all hosts.

The lock isn't permanent, but the time can be adjusted to a length more suitable to your preferences so the user isn't permanently locked out from your services due to the nature of dynamic IPs in most ISPs which can lead to the specific IP address no longer being compromised.

And all of this is done with minimal manpower requirements to maintain it, allowing you to free it up for other tasks.

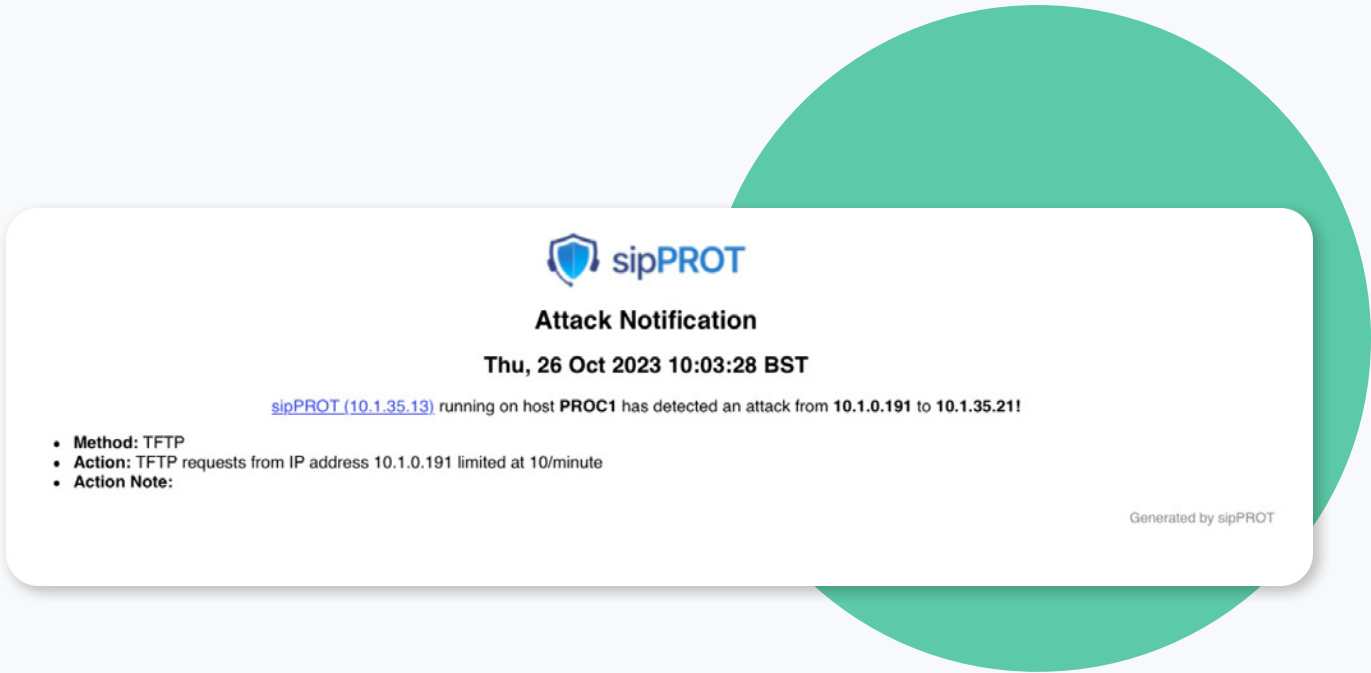
sipPROT covers both IPv4 and IPv6 address ranges, providing you with the utmost level of safety in that regard.



# AUTO-PROVISIONING ATTACK DETECTION

One of the most vulnerable points of a SIP system tends to be its auto-provisioning service, but with sipPROT, even that area is covered thanks to its TFTP Brute Force Attack detection.

It easily spots potential attacks on the system that are trying to redirect all of the requests and messing with the system to whatever degree and stop them in their tracks.



# CLEAR AND INTUITIVE ATTACK LOG

In order to improve response times and reduce confusion, sipPROT displays a list of all SIP attacks that have targeted the current system with each one containing the relevant information needed for administrators to assess risks and execute swift action when needed.

Each individual log contains the attacker's and victim's IP addresses, the type and time of attack and the User Agent with more information available upon expansion of an individual attack instance.

The screenshot shows the 'Attack Logs' interface in sipPROT. It includes a search bar, a date range selector (Oct 10, 2023 - Oct 17, 2023), and a 'Reset' button. The table displays the following columns: Attacker IP Address, Victim IP Address, Attack Type, User Agent, and Time. The first row is expanded, showing additional details like Host Name (SW-public1), sipPROT Version (5.1.0+build.1160.rev.3071795), and Kernel Version (5.15.103-commware-00013-gc005a5174808).

Attacker IP Address	Victim IP Address	Attack Type	User Agent	Time
89.239.39.42	45.141.164.98	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 18:11:05 CEST
45.95.146.4	45.141.164.98	REGISTER	PBX	Oct 8, 2023 17:55:30 CEST
89.239.39.42	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 17:07:36 CEST
89.239.32.85	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 13:35:01 CEST
89.239.32.85	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 12:32:47 CEST
89.239.32.85	45.141.164.96	REGISTER	VaxSIPUserAgent/3.5	Oct 8, 2023 11:31:31 CEST
45.143.9.130	45.141.164.98	REGISTER	Cisco UCM 12.0.1	Oct 8, 2023 06:04:36 CEST
45.143.9.130	45.141.164.96	REGISTER	friendly-scanner	Oct 8, 2023 02:58:02 CEST
198.50.119.225	45.141.164.98	REGISTER	FPBX	Oct 8, 2023 01:51:03 CEST
45.143.9.130	45.141.164.97	REGISTER	friendly-scanner	Oct 8, 2023 00:52:03 CEST
198.50.119.225	45.141.164.97	REGISTER	FPBX	Oct 8, 2023 00:40:22 CEST
198.50.119.225	45.141.164.98	REGISTER	FPBX	Oct 7, 2023 23:31:54 CEST
45.143.9.142	45.141.164.97	REGISTER	friendly-scanner	Oct 7, 2023 15:37:58 CEST
45.143.9.142	45.141.164.96	REGISTER	Cisco UCM 12.0.1	Oct 7, 2023 00:07:56 CEST
167.172.180.195	45.141.164.98	REGISTER	FPBX	Oct 6, 2023 23:03:32 CEST

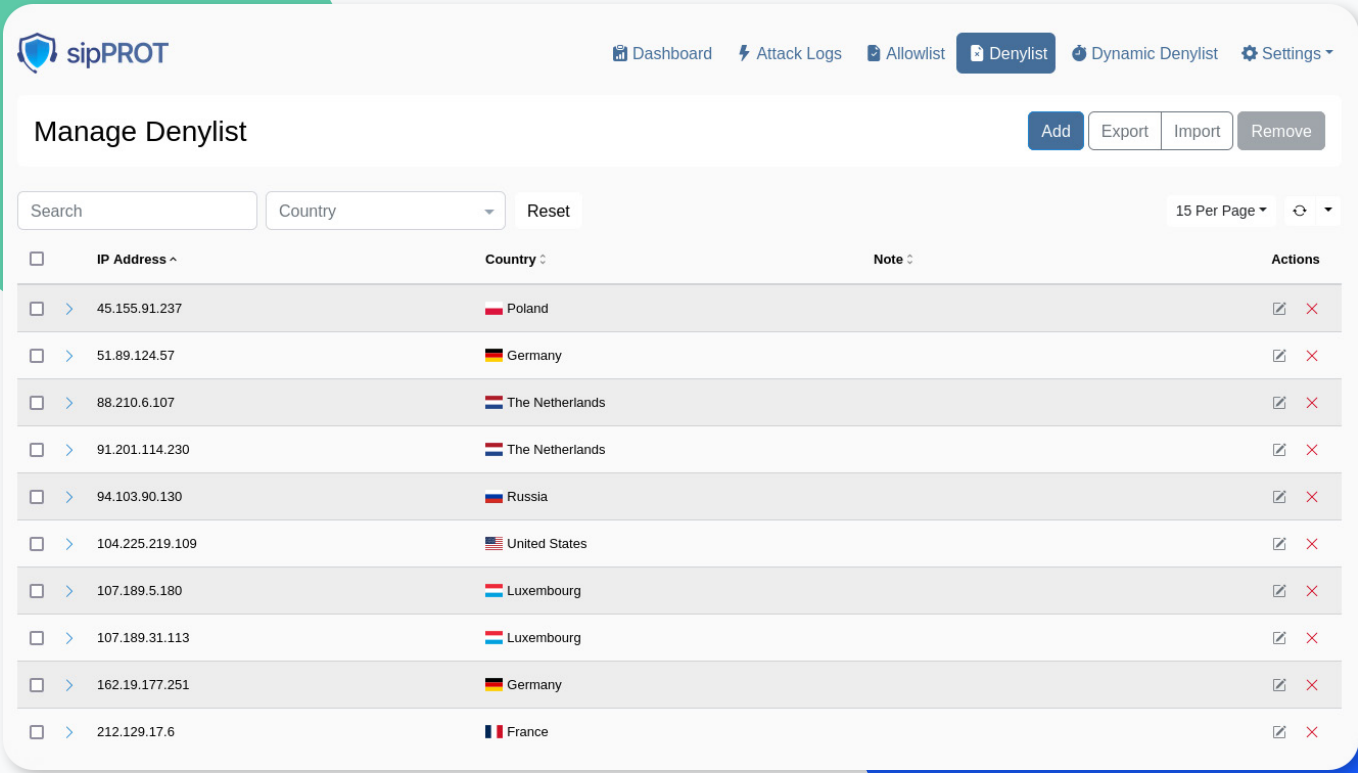


# MANAGEMENT OF ALLOWLISTS AND DENYLISTS

sipPROT has another excellent quality of life feature which will save your system admins a lot of man hours, the ability to import and export allowlists and denylists from one system to another in .csv format.

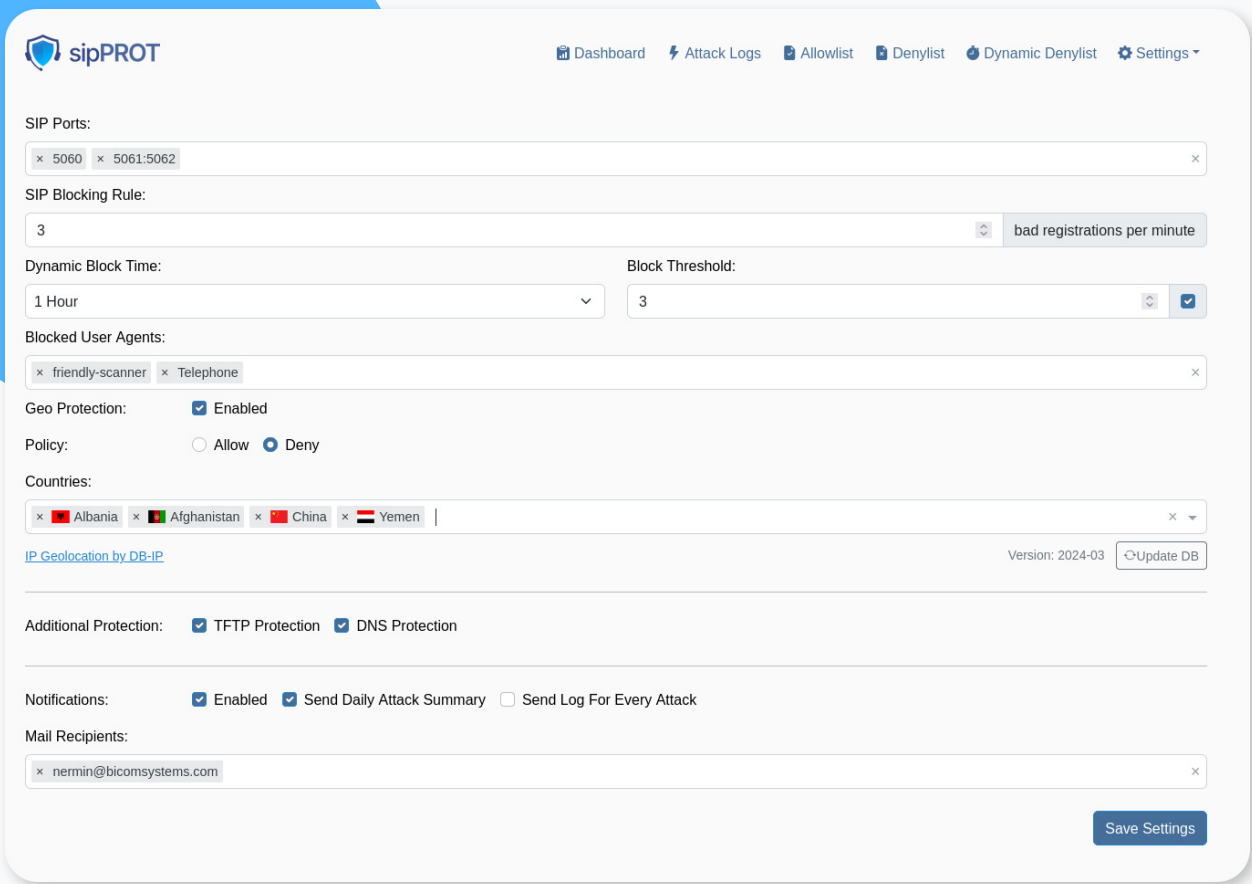
They can also add specific notes to specific IP addresses if necessary so they could be given more attention as well as remove IP addresses from the same lists in bulk and define multiple SIP ports to be protected.

All of this serves to greatly improve their workflow and eliminates a lot of the tedium from their day-to-day duties.



## GeoIP BLOCKING

Utilize the full power of sipPROT through the use of GeoIP blocking, allowing system admins to lock out the IP range of an entire country in case of a large SIP attack or for any other valid reason.



## SIP INVITEs RATE LIMITER

Help admins better manage spam invites and offer them more control over incoming SIP traffic with the SIP INVITEs Rate Limiter, allowing them to reject the spam while logging it in the attack log for future monitoring and action.

# Expert Support at Your Fingertips

Our highly trained experts are always available to address any system-related issues or questions that you may have, ensuring seamless operations and peace of mind.





# CONTACT BICOM SYSTEMS TODAY

to find out more about our services



## Bicom Systems (USA)

2719 Hollywood Blvd  
B-128  
Hollywood, Florida  
33020-4821  
United States  
Tel: +1 (954) 278 8470  
Tel: +1 (619) 760 7777  
Fax: +1 (954) 278 8471  
sales@bicomsystems.com



## Bicom Systems (CAN)

Hilyard Place  
B-125  
Saint John, New Brunswick  
E2K 1J5  
Canada  
Tel: +1 (647) 313 1515  
Tel: +1 (506) 635 1135  
sales@bicomsystems.com



## Bicom Systems (UK)

Unit 5 Rockware BC  
5 Rockware Avenue  
Greenford  
UB6 0AA  
United Kingdom  
Tel: +44 (0) 20 33 99 88 00  
sales@bicomsystems.com



## Bicom Systems (FRA)

c/o Athena Global Services  
Telecom  
229 rue Saint-Honoré – 75001  
Paris  
Tel : +33 (0) 185 001 000  
www.bicomsystems.fr  
sales@bicomsystems.fr



## Bicom Systems (ITA)

Via Marie Curie 3  
50051 Castelfiorentino  
Firenze  
Italy  
Tel: +39 0571 1661119  
sales@bicomsystems.it



## Bicom Systems (RSA)

12 Houtkapper Street  
Magaliessig  
2067  
South Africa  
Tel: +27 (10) 0011390  
sales@bicomsystems.com

## Follow us



[www.bicomsystems.com](http://www.bicomsystems.com)