RELEASE NOTES

sipPROT 5.1

bicom SYSTEMS

wiki.bicomsystems.com

Table of Contents

FEATURES

sipPROT 5.1 comes with a complete makeover, including various enhancements, a faster in-memory database and an updated user interface aimed at boosting the overall functionality and user experience of sipPROT.

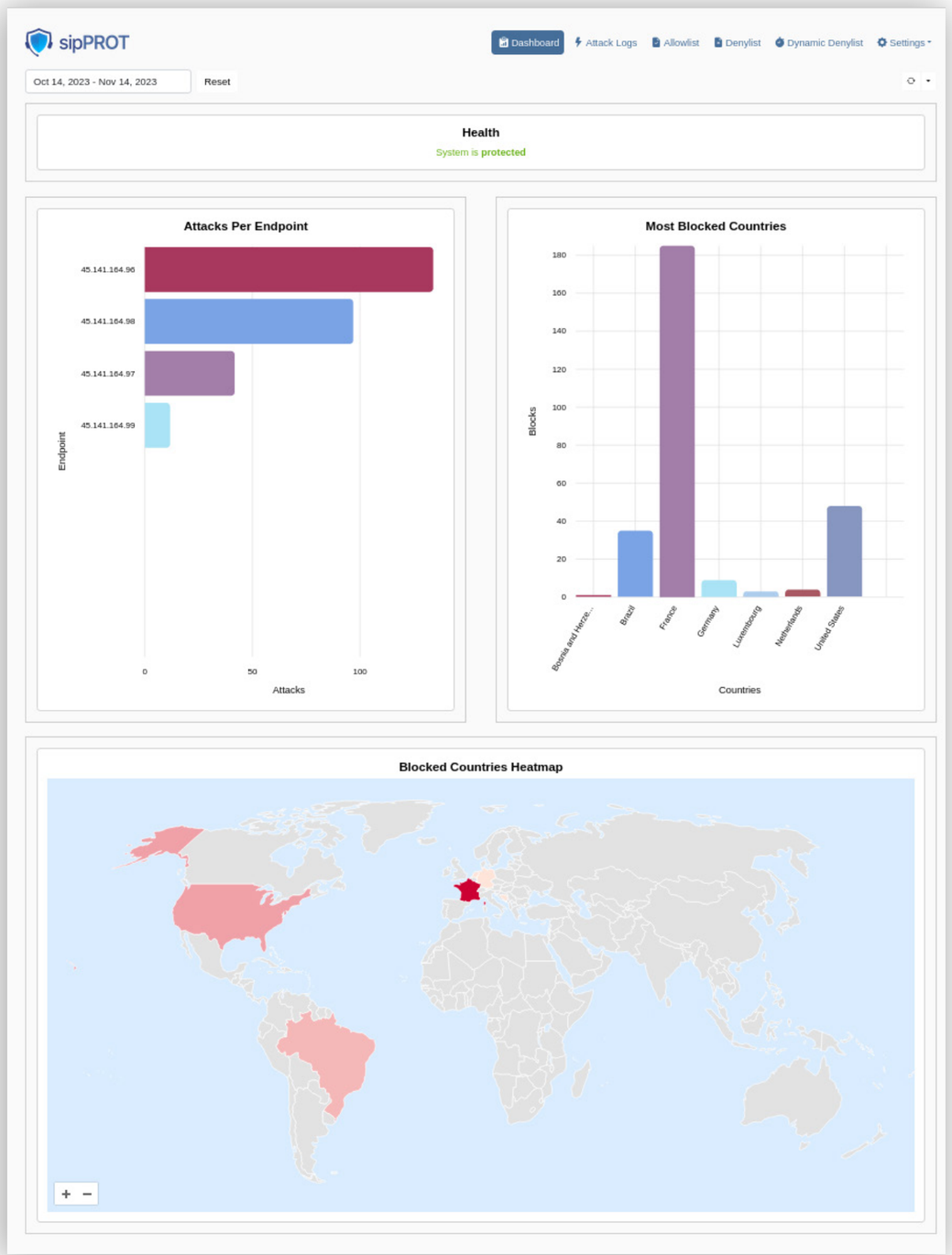
sipPROT Dashboard

The sipPROT Dashboard was added to provide a clear overview of blocked attacks, Geo-IP data and overall health status of the firewall.

The attacks per endpoint chart shows the number of attacks for each VPS on the system, or rather, their IPs that were under attack. Hovering on each bar will display the number of attacks which helps administrators see which VPS is most susceptible to them.

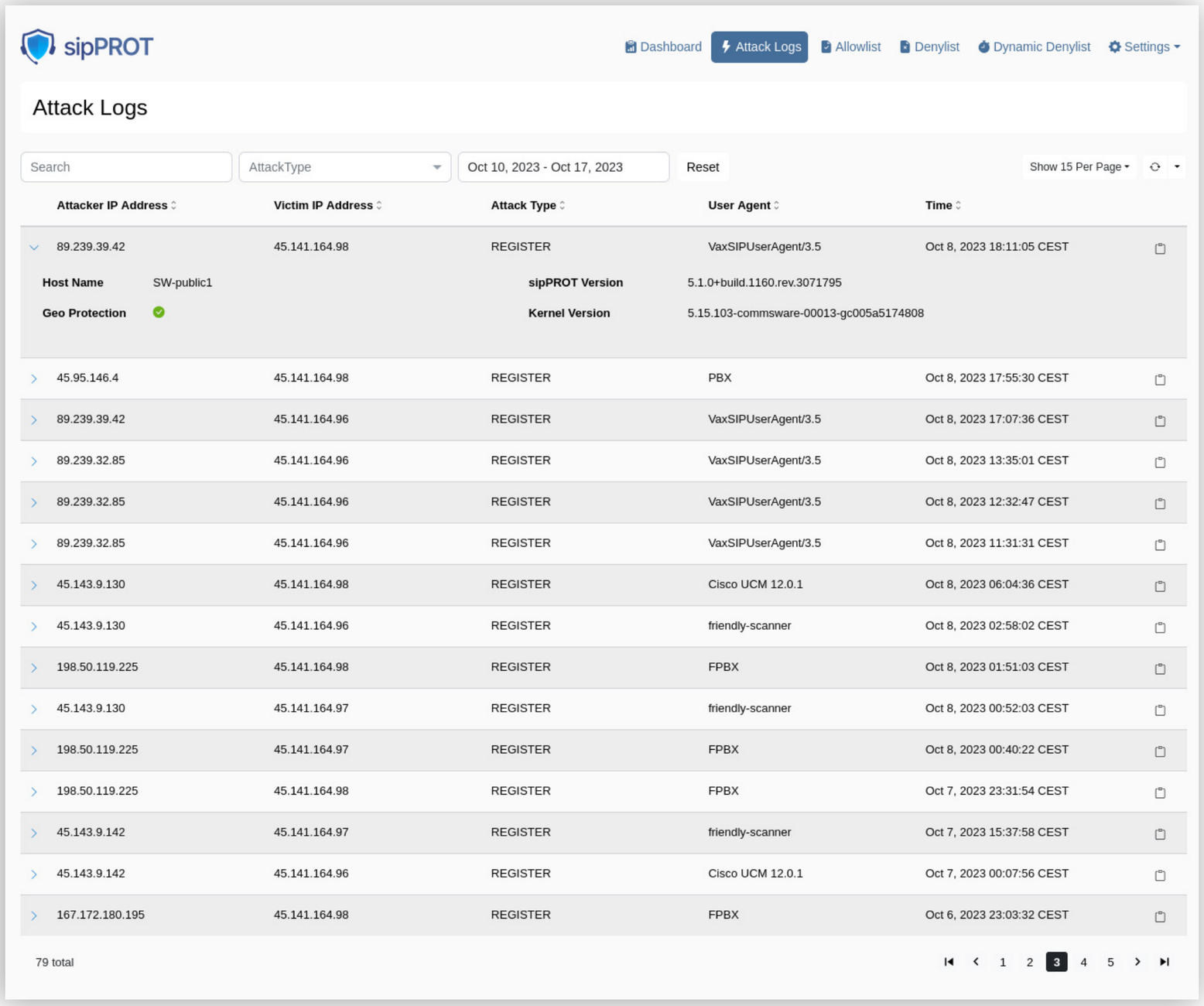
The Most Blocked Countries chart shows the number of IPs that were blocked from each country so that administrators can use the data to adjust geo-ip protection policies accordingly.

The Blocked Countries Heatmap visually illustrates the countries with the highest number of blocked IP addresses with the intensity of the color indicating the severity of IP address blocks. The darker the color, the greater the number of blocked IPs.



Attack Logs

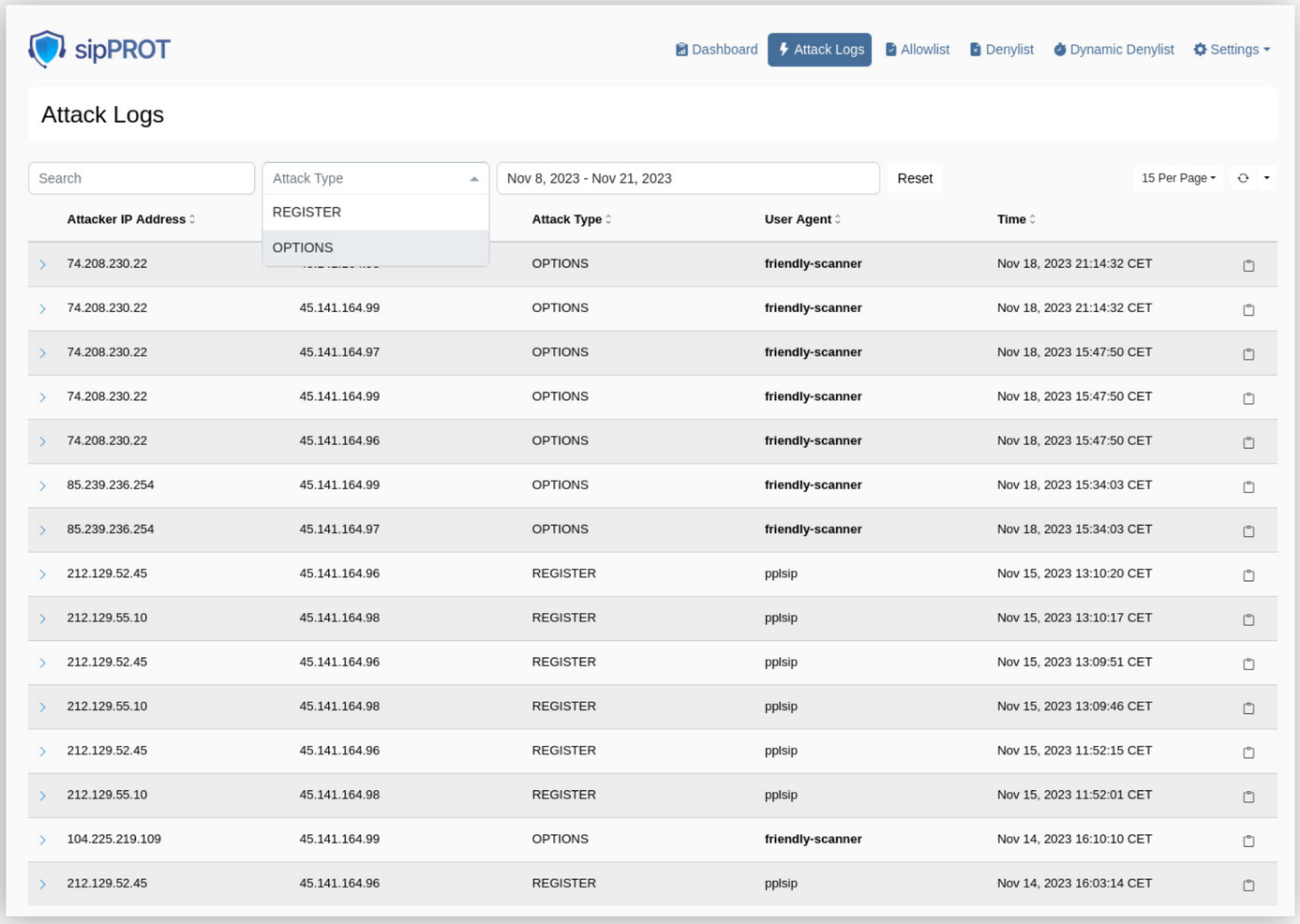
sipPROT's Attack Logs will display logs of all SIP attacks on the system with the intention to provide a better insight into the security of the entire system and allow administrators to apply additional measures if necessary.



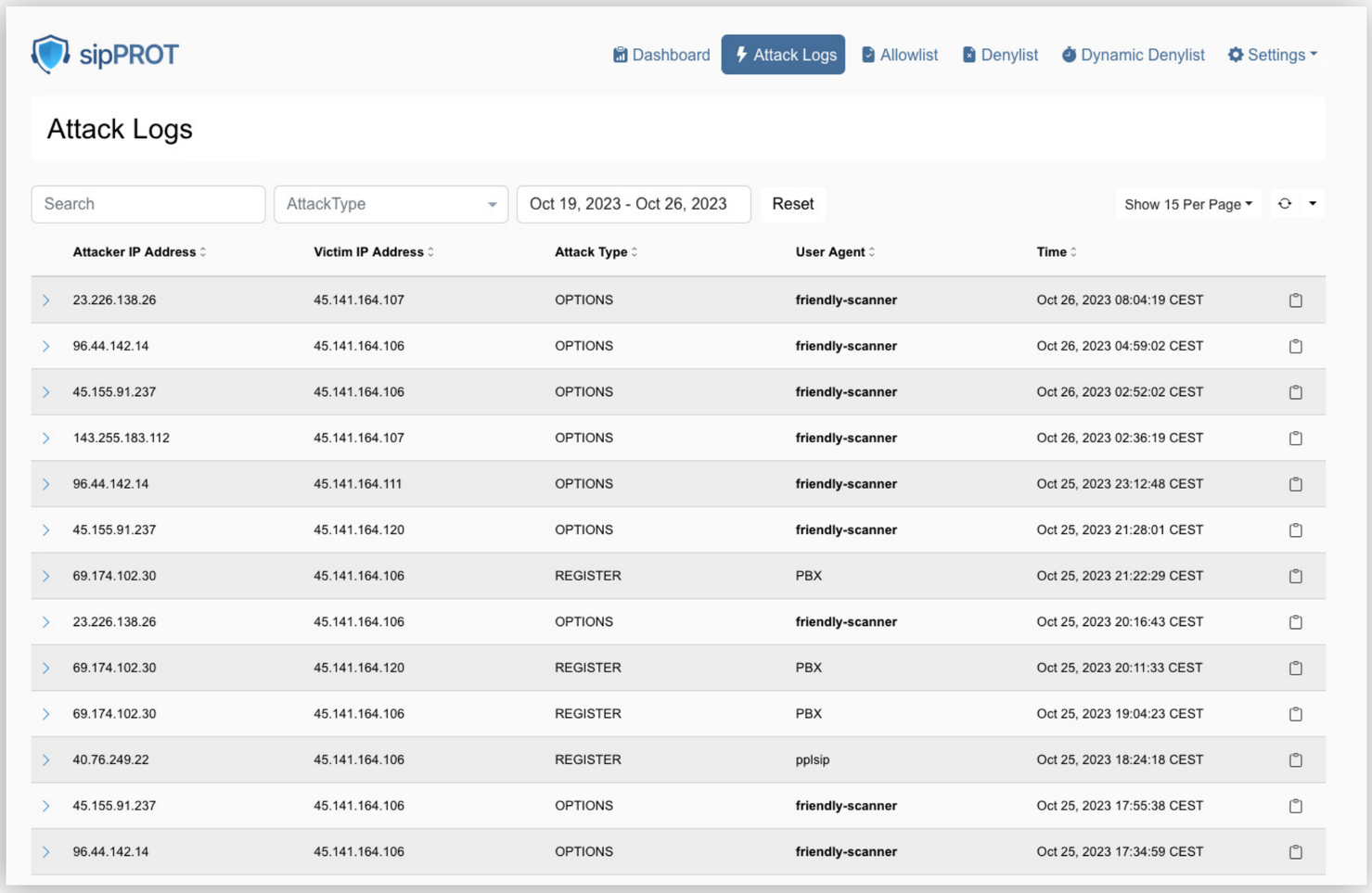
The logs will show the attacker's and the victim's IP addresses, the attack type, the user agent and the date and time of the attack. By clicking on the symbol in front of each log, administrators can find more information, namely on which host the attack was detected, whether Geo-IP protection is available on that host and the host's sipPROT and kernel versions.

The logs can be filtered either by utilizing the search bar or by choosing the attack type to be presented from the drop down menu next to the bar.

sipPROT's attack logs will differentiate between two types of attack, REGISTER and OPTIONS.



Known user agents will be singled out on the logs. Logs are kept for three months.

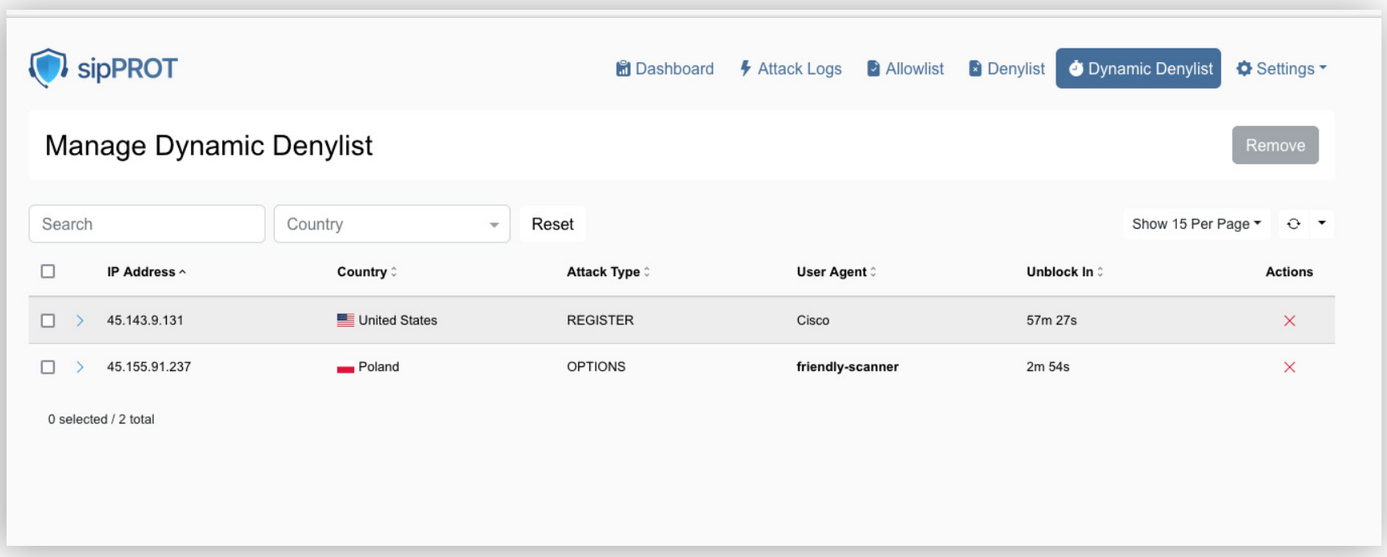


IP Addresses Lists - Improved Dynamic Denylist

The dynamic denylist functionality has been further enhanced so that when an address is dynamically blocked on one host, that information is shared among all hosts within the cluster.

Addresses that end up permanently blocked through the dynamic denylist functionality (by exceeding the block threshold) will appear in the denylist.

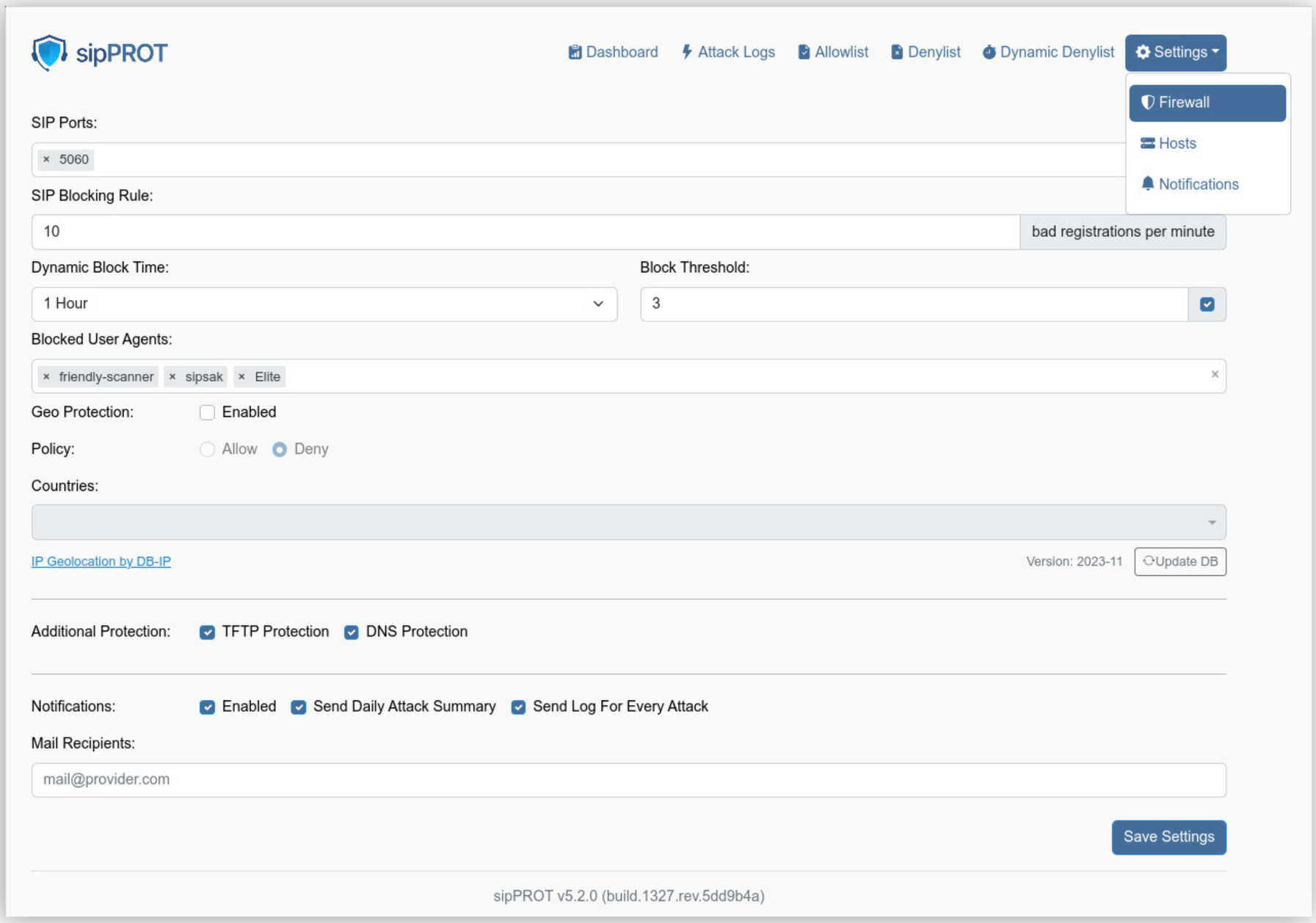
The dynamic denylist has been further enhanced so it shows the user agent device of the blocked address. If it’s a known user agent device, it will appear in bold letters.



Settings

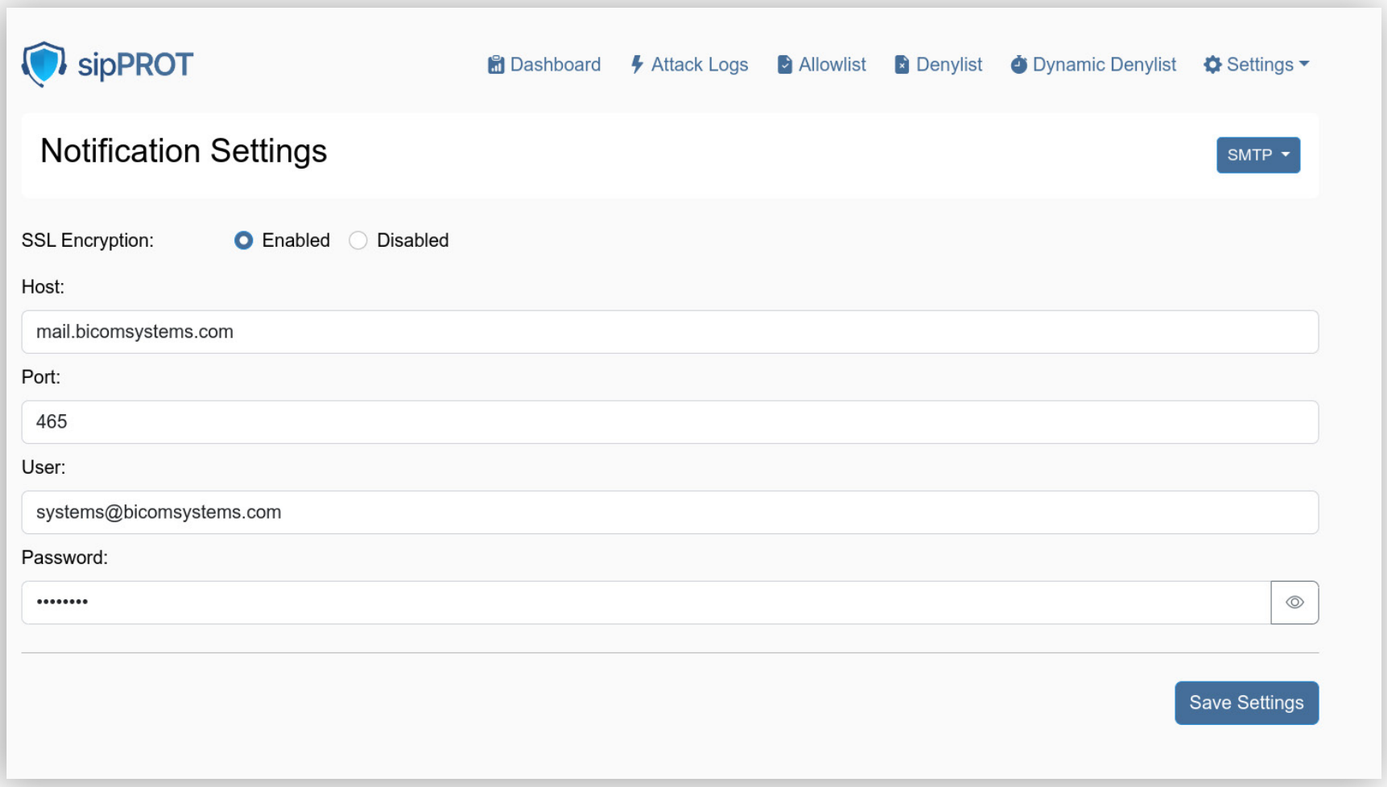
General sipPROT settings can be found under Settings → Firewall.

The Host menu provides sipPROT with information for each host in the cluster. Administrators will be able to monitor the health of sipPROT and the Geo-IP service on each host. They will be able to exclude a host from sipPROT with a single click.



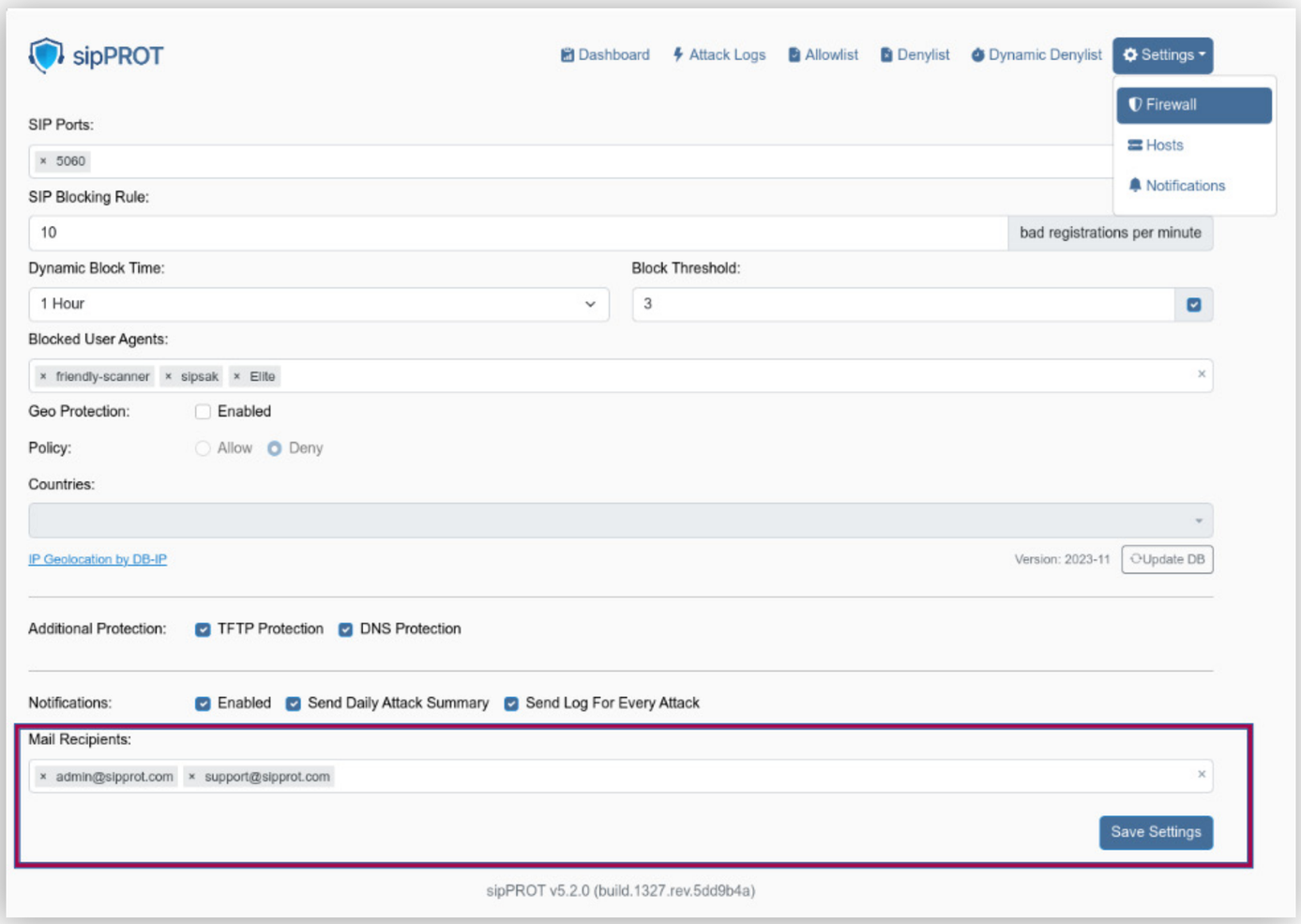
Notifications

sipPROT administrators will be able to configure SMTP settings for notifications sent out by sipPROT.



Under Firewall settings administrators can enter the email addresses of all sipPROT notification recipients.

At the moment, sipPROT only supports SMTP for sending out notifications.



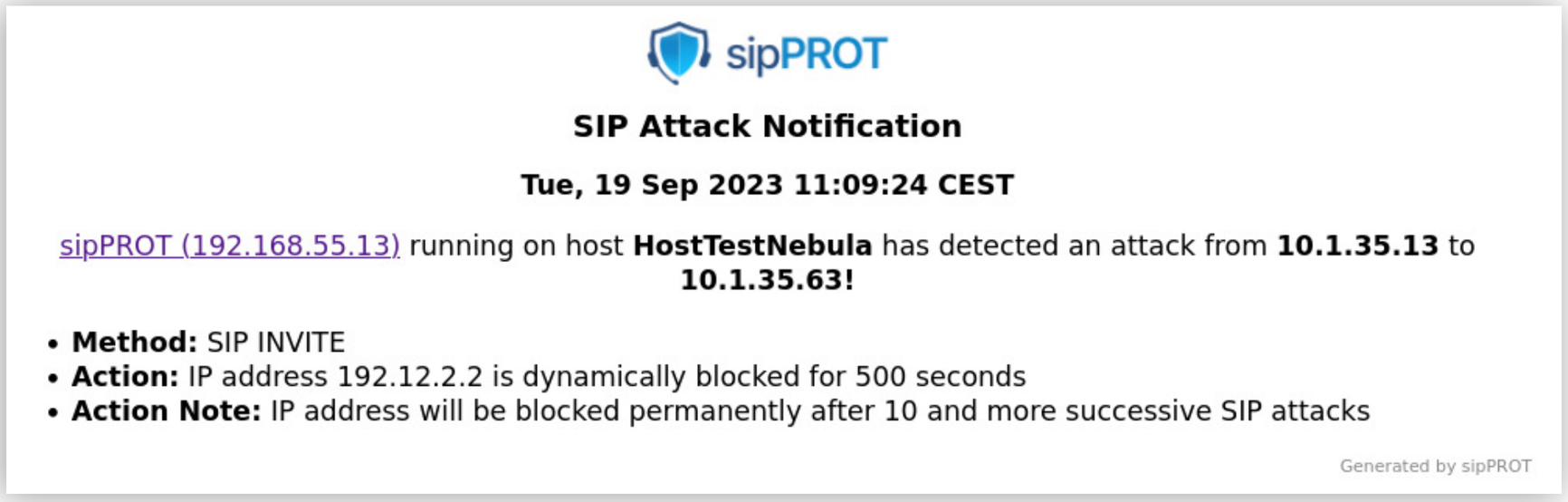
Reporting Service

Administrators can choose the type of reports they want to receive from sipPROT.

The daily reports will provide a list of blocked attacks for the day along with some additional information. The administrators can navigate to the SERVERware GUI by clicking on the link in the report.

In case no attacks occurred that day, a notification like the one below will be sent out.

In the event of an ongoing attack on the system, sipPROT will notify the administrators immediately together with the attacker's and the victim's IP addresses, method of attack, as well as what actions were taken.


sipPROT

SIP Attack Notification

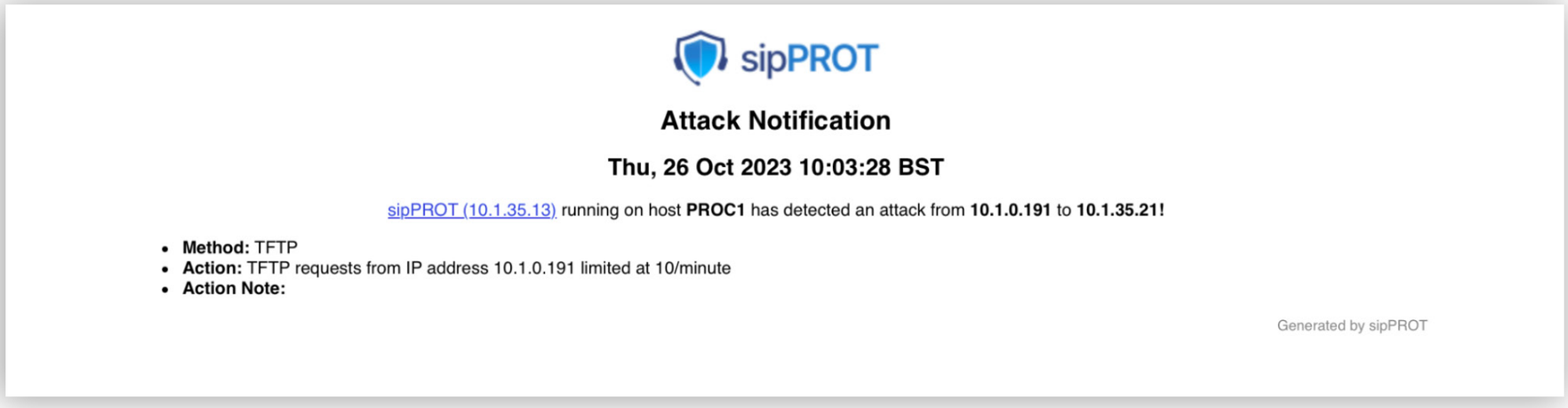
Tue, 19 Sep 2023 11:09:24 CEST

sipPROT (192.168.55.13) running on host **HostTestNebula** has detected an attack from **10.1.35.13** to **10.1.35.63!**

- **Method:** SIP INVITE
- **Action:** IP address 192.12.2.2 is dynamically blocked for 500 seconds
- **Action Note:** IP address will be blocked permanently after 10 and more successive SIP attacks

Generated by sipPROT

TFTP attacks will also prompt an email notification from sipPROT.


sipPROT

Attack Notification

Thu, 26 Oct 2023 10:03:28 BST

sipPROT (10.1.35.13) running on host **PROC1** has detected an attack from **10.1.0.191** to **10.1.35.21!**

- **Method:** TFTP
- **Action:** TFTP requests from IP address 10.1.0.191 limited at 10/minute
- **Action Note:**

Generated by sipPROT

Bug Fixes & Improvements:

- Fixed a bug where sipPROT would block the country that the IP was accessing from.

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

Bicom Systems (CAN)
Hilyard Place
B-125
Saint John, New Brunswick
E2K 1J5
Canada
Tel: +1 (647) 313 1515
Tel: +1 (506) 635 1135

Bicom Systems (UK)
Unit 5 Rockware BC
5 Rockware Avenue
Greenford
UB6 0AA
United Kingdom
Tel: +44 (0) 20 33 99 88 00

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
Email: sales@bicomsystems.it

Bicom Systems (RSA)
12 Houtkapper Street
Magaliessig
2067
South Africa
Tel: +27 (10) 0011390

email: sales@bicomsystems.com

Follow us

bicom SYSTEMS