



RELEASE NOTES
sipPROT 5.1

bicom
SYSTEMS

wiki.bicomsystems.com

Table of Contents

FEATURES	1
sipPROT Dashboard	1
Attack Logs	2
IP Addresses Lists - Improved Dynamic Denylist	4
Settings.....	5
Notifications	6
Reporting Service	7
Bug Fixes & Improvements	9

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.

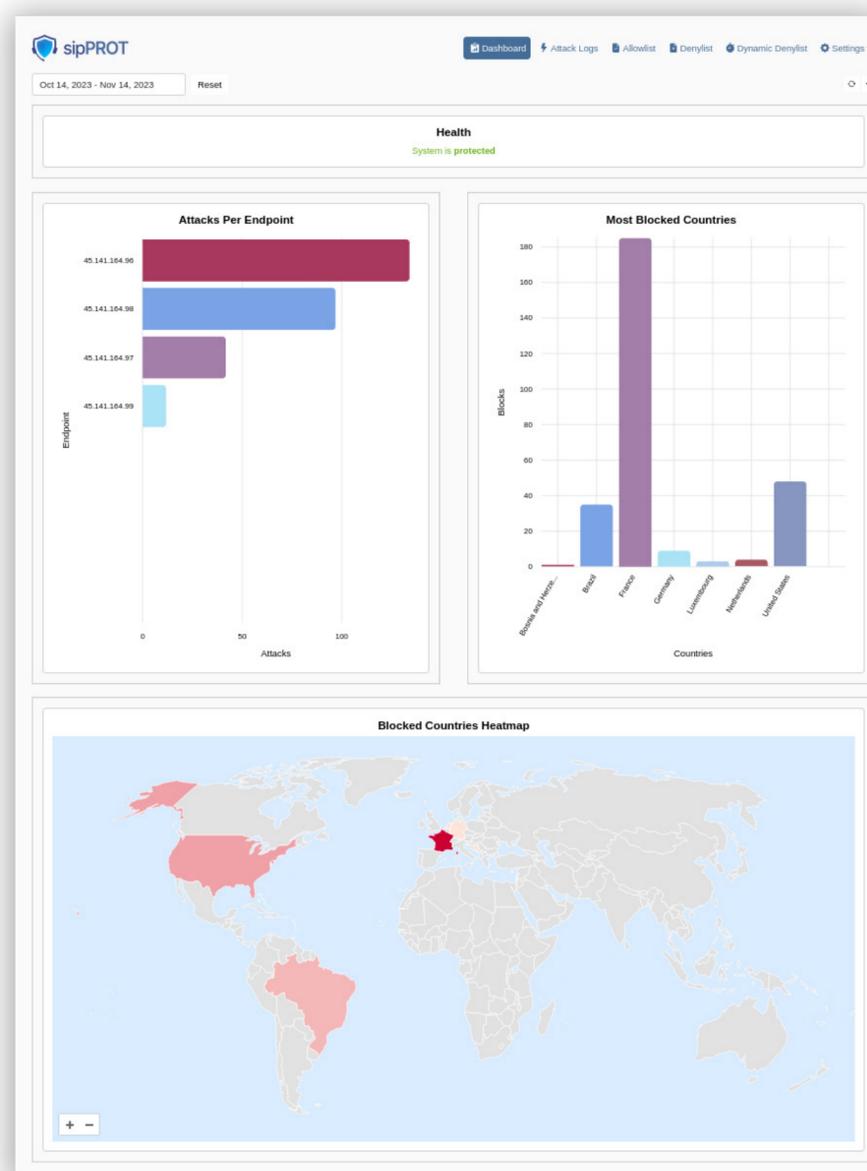
sipPROT Dashboard

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.

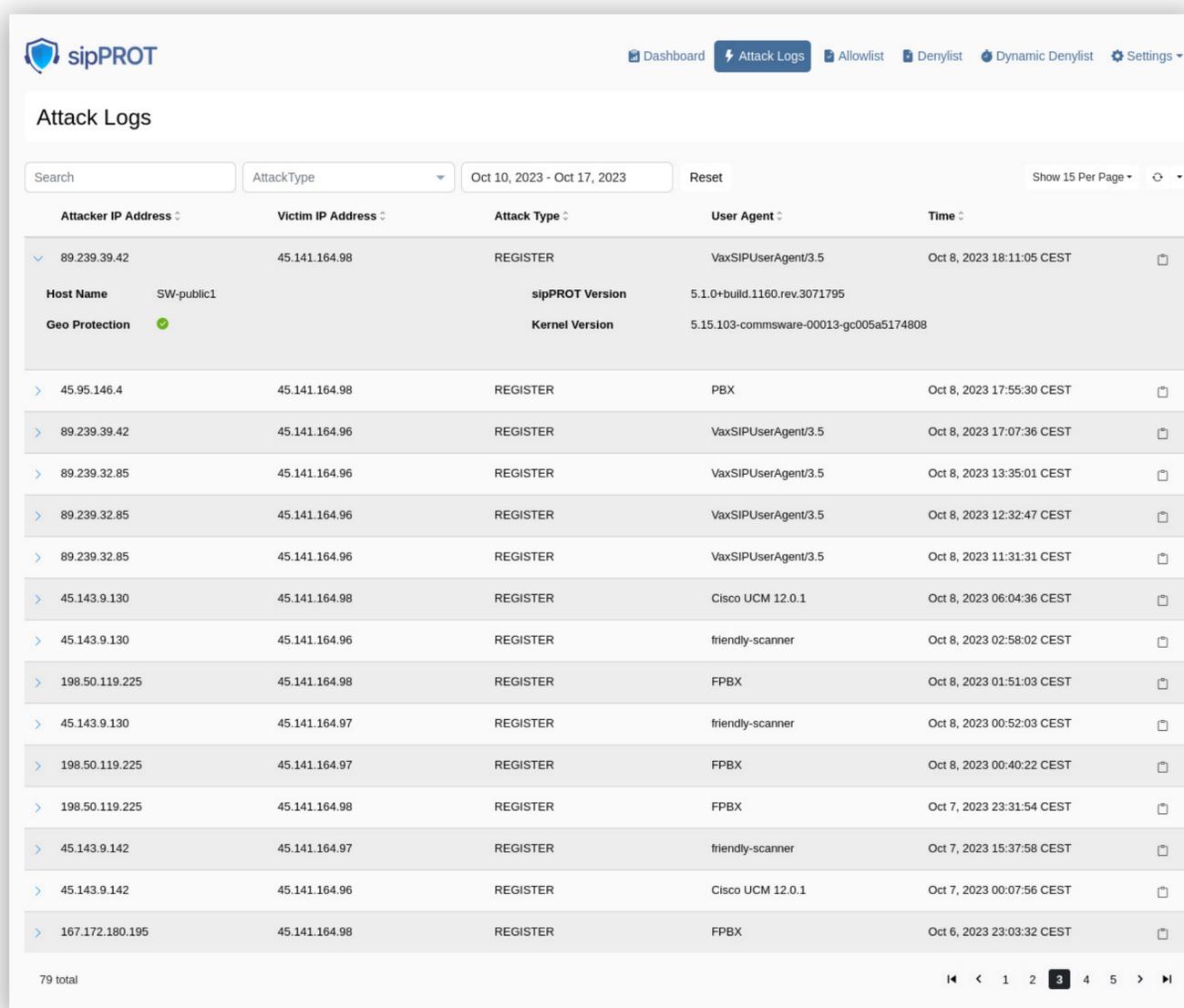
The Most Blocked Countries chart shows the number of IPs that were blocked from each country so that administrators can use the data to adjust geo-ip protection policies accordingly.

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.



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	☐
Host Name SW-public1 Geo Protection ✔ sipPROT Version 5.1.0+build.1160.rev.3071795 Kernel Version 5.15.103-commsware-00013-gc005a5174808					
> 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	☐

79 total

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.

Attack Logs

Search: [] Attack Type: [] Nov 8, 2023 - Nov 21, 2023 Reset 15 Per Page []

Attacker IP Address	Attack Type	User Agent	Time
74.208.230.22	OPTIONS	friendly-scanner	Nov 18, 2023 21:14:32 CET
74.208.230.22	OPTIONS	friendly-scanner	Nov 18, 2023 21:14:32 CET
74.208.230.22	OPTIONS	friendly-scanner	Nov 18, 2023 15:47:50 CET
74.208.230.22	OPTIONS	friendly-scanner	Nov 18, 2023 15:47:50 CET
74.208.230.22	OPTIONS	friendly-scanner	Nov 18, 2023 15:47:50 CET
85.239.236.254	OPTIONS	friendly-scanner	Nov 18, 2023 15:34:03 CET
85.239.236.254	OPTIONS	friendly-scanner	Nov 18, 2023 15:34:03 CET
212.129.52.45	REGISTER	pplsip	Nov 15, 2023 13:10:20 CET
212.129.55.10	REGISTER	pplsip	Nov 15, 2023 13:10:17 CET
212.129.52.45	REGISTER	pplsip	Nov 15, 2023 13:09:51 CET
212.129.55.10	REGISTER	pplsip	Nov 15, 2023 13:09:46 CET
212.129.52.45	REGISTER	pplsip	Nov 15, 2023 11:52:15 CET
212.129.55.10	REGISTER	pplsip	Nov 15, 2023 11:52:01 CET
104.225.219.109	OPTIONS	friendly-scanner	Nov 14, 2023 16:10:10 CET
212.129.52.45	REGISTER	pplsip	Nov 14, 2023 16:03:14 CET

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

Attack Logs

Search: [] AttackType: [] Oct 19, 2023 - Oct 26, 2023 Reset Show 15 Per Page []

Attacker IP Address	Victim IP Address	Attack Type	User Agent	Time
23.226.138.26	45.141.164.107	OPTIONS	friendly-scanner	Oct 26, 2023 08:04:19 CEST
96.44.142.14	45.141.164.106	OPTIONS	friendly-scanner	Oct 26, 2023 04:59:02 CEST
45.155.91.237	45.141.164.106	OPTIONS	friendly-scanner	Oct 26, 2023 02:52:02 CEST
143.255.183.112	45.141.164.107	OPTIONS	friendly-scanner	Oct 26, 2023 02:36:19 CEST
96.44.142.14	45.141.164.111	OPTIONS	friendly-scanner	Oct 25, 2023 23:12:48 CEST
45.155.91.237	45.141.164.120	OPTIONS	friendly-scanner	Oct 25, 2023 21:28:01 CEST
69.174.102.30	45.141.164.106	REGISTER	PBX	Oct 25, 2023 21:22:29 CEST
23.226.138.26	45.141.164.106	OPTIONS	friendly-scanner	Oct 25, 2023 20:16:43 CEST
69.174.102.30	45.141.164.120	REGISTER	PBX	Oct 25, 2023 20:11:33 CEST
69.174.102.30	45.141.164.106	REGISTER	PBX	Oct 25, 2023 19:04:23 CEST
40.76.249.22	45.141.164.106	REGISTER	pplsip	Oct 25, 2023 18:24:18 CEST
45.155.91.237	45.141.164.106	OPTIONS	friendly-scanner	Oct 25, 2023 17:55:38 CEST
96.44.142.14	45.141.164.106	OPTIONS	friendly-scanner	Oct 25, 2023 17:34:59 CEST

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.

Manage Dynamic Denylist

Search Country Reset Show 15 Per Page

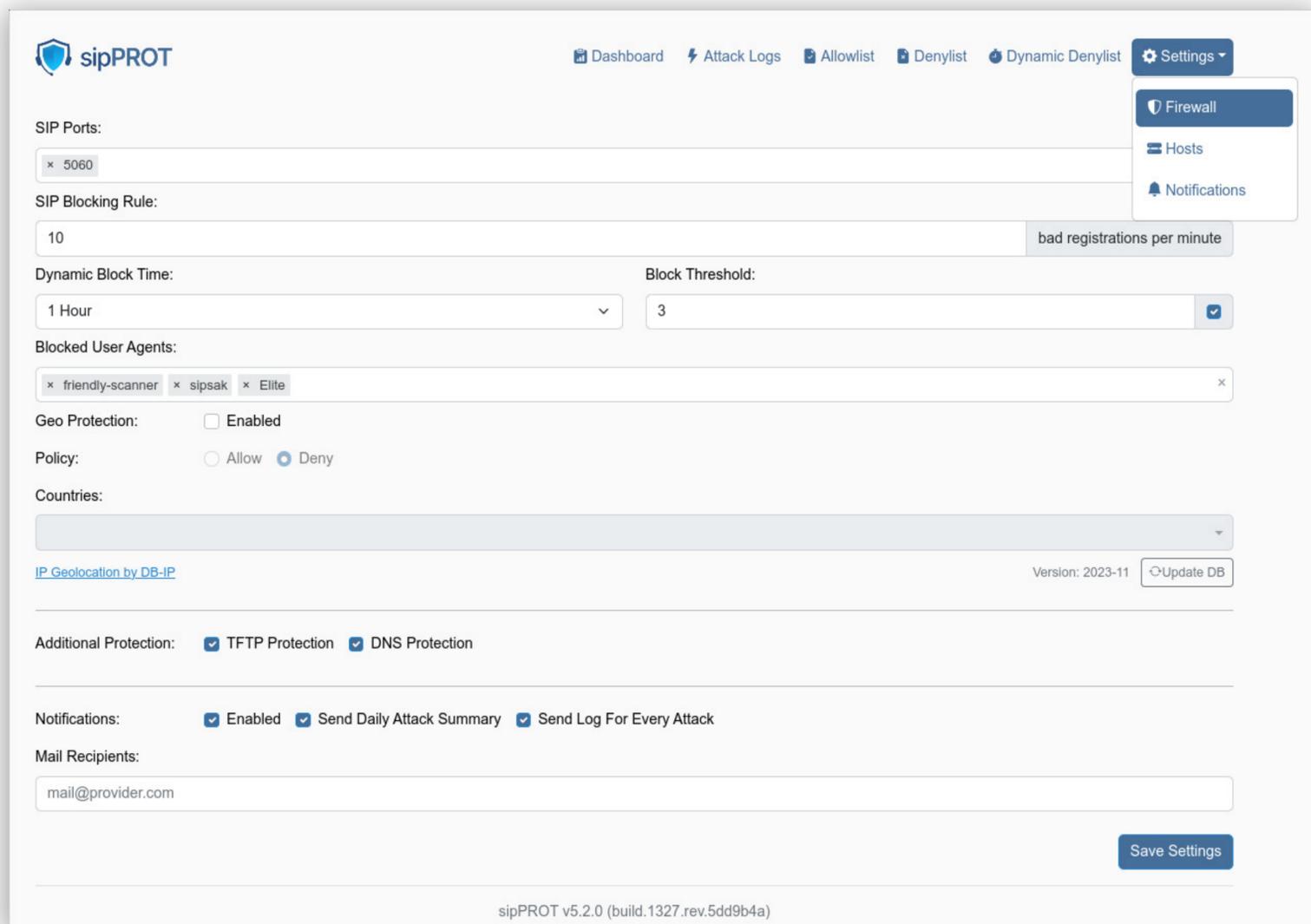
IP Address	Country	Attack Type	User Agent	Unblock In	Actions
45.143.9.131	United States	REGISTER	Cisco	57m 27s	✕
45.155.91.237	Poland	OPTIONS	friendly-scanner	2m 54s	✕

0 selected / 2 total

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.



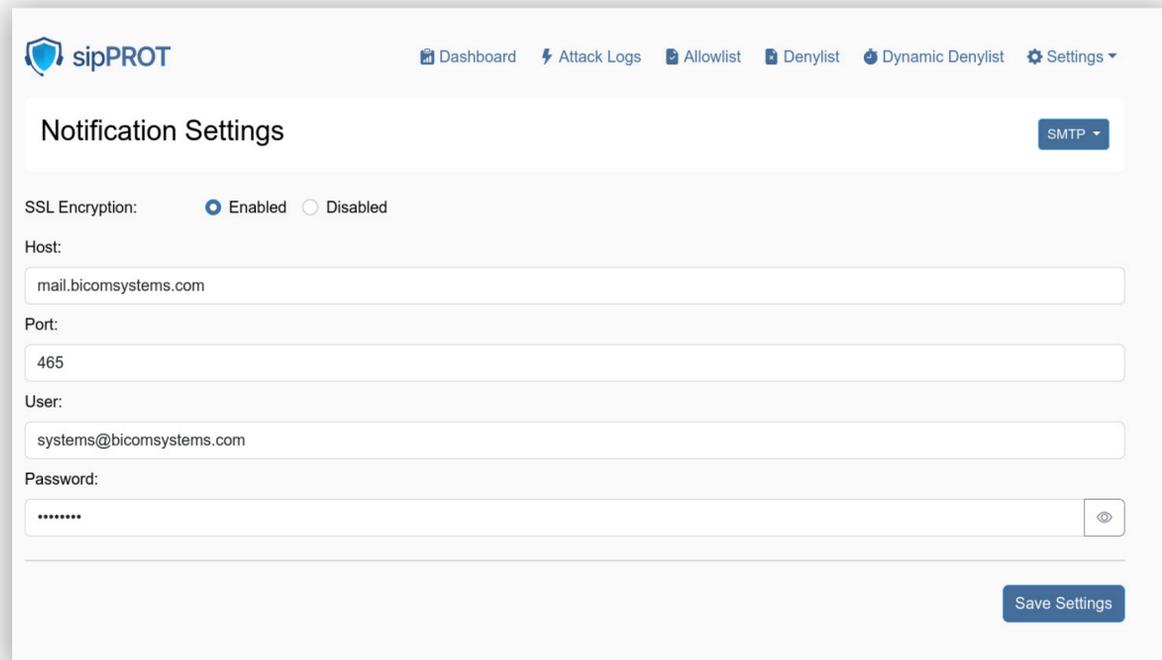
The screenshot shows the sipPROT Settings page, specifically the Firewall section. The page has a navigation bar at the top with links for Dashboard, Attack Logs, Allowlist, Denylist, Dynamic Denylist, and Settings. The Settings dropdown menu is open, showing options for Firewall, Hosts, and Notifications. The Firewall settings include:

- SIP Ports:** A text input field containing "5060".
- SIP Blocking Rule:** A text input field containing "10" and a label "bad registrations per minute".
- Dynamic Block Time:** A dropdown menu set to "1 Hour".
- Block Threshold:** A text input field containing "3" with a checkmark icon.
- Blocked User Agents:** A list of user agents: "friendly-scanner", "sipsak", and "Elite".
- Geo Protection:** A checkbox labeled "Enabled" which is unchecked.
- Policy:** Radio buttons for "Allow" and "Deny", with "Deny" selected.
- Countries:** A dropdown menu.
- IP Geolocation by DB-IP:** A link and a "Version: 2023-11" label with an "Update DB" button.
- Additional Protection:** Checkboxes for "TFTP Protection" and "DNS Protection", both checked.
- Notifications:** Checkboxes for "Enabled", "Send Daily Attack Summary", and "Send Log For Every Attack", all checked.
- Mail Recipients:** A text input field containing "mail@provider.com".

A "Save Settings" button is located at the bottom right of the settings area. The footer of the page indicates the version: "sipPROT v5.2.0 (build.1327.rev.5dd9b4a)".

Notifications

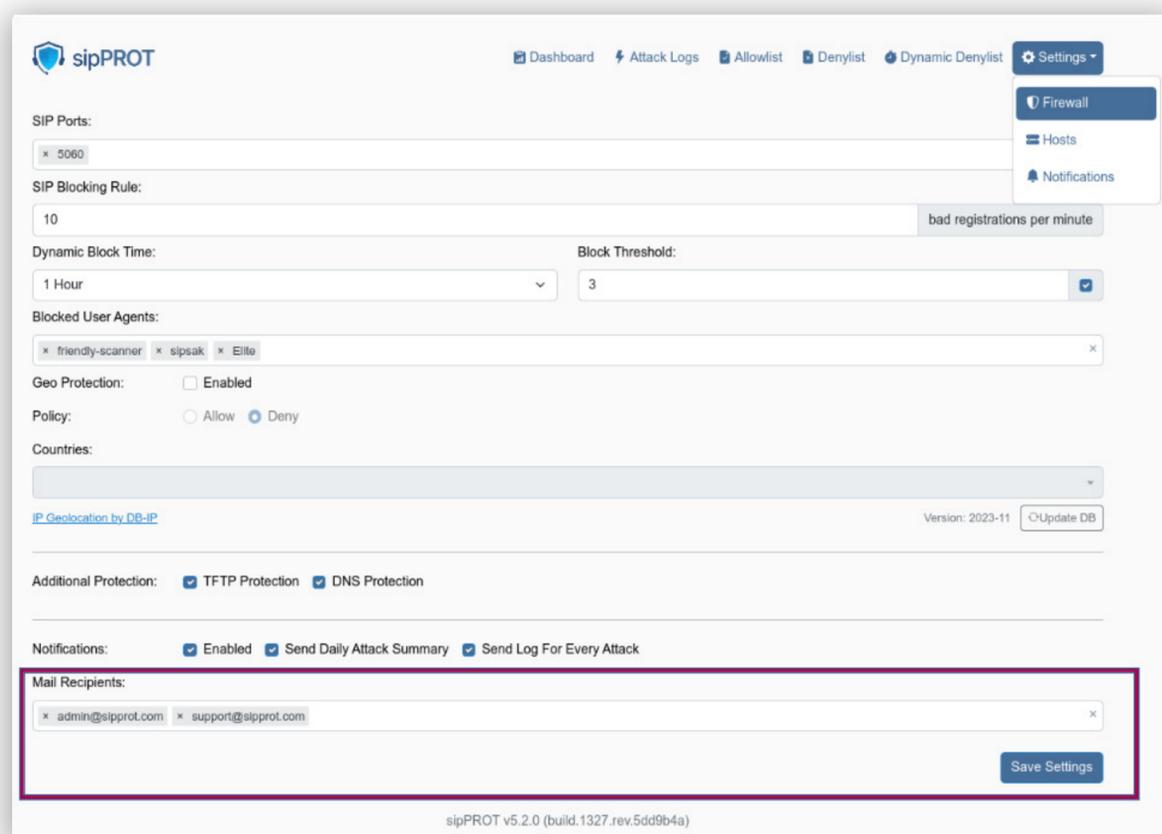
sipPROT administrators will be able to configure SMTP settings for notifications sent out by sipPROT.



The screenshot shows the 'Notification Settings' page in the sipPROT interface. At the top, there is a navigation bar with links for Dashboard, Attack Logs, Allowlist, Denylist, Dynamic Denylist, and Settings. The main heading is 'Notification Settings' with a dropdown menu set to 'SMTP'. Below this, there are several configuration options: 'SSL Encryption' is set to 'Enabled'; 'Host' is 'mail.bicomsystems.com'; 'Port' is '465'; 'User' is 'systems@bicomsystems.com'; and 'Password' is masked with dots. A 'Save Settings' button is located at the bottom right of the form.

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.



The screenshot shows the 'Firewall' settings page in the sipPROT interface. The 'Settings' dropdown menu is open, showing 'Firewall', 'Hosts', and 'Notifications'. The 'Firewall' section includes: 'SIP Ports' with a tag '5060'; 'SIP Blocking Rule' with a value of '10' and a label 'bad registrations per minute'; 'Dynamic Block Time' set to '1 Hour' and 'Block Threshold' set to '3'; 'Blocked User Agents' with tags 'friendly-scanner', 'sipsak', and 'Elite'; 'Geo Protection' set to 'Enabled'; 'Policy' set to 'Deny'; 'Countries' with a dropdown menu; 'IP Geolocation by DB-IP' with 'Version: 2023-11' and an 'Update DB' button; 'Additional Protection' with 'TFTP Protection' and 'DNS Protection' checked; and 'Notifications' with 'Enabled', 'Send Daily Attack Summary', and 'Send Log For Every Attack' checked. The 'Mail Recipients' section is highlighted with a red box and contains tags for 'admin@sipprot.com' and 'support@sipprot.com'. A 'Save Settings' button is at the bottom right. The footer shows 'sipPROT v5.2.0 (build.1327.rev.5dd9b4a)'.

Reporting Service

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

Notifications: Enabled Send Daily Attack Summary Send Log For Every Attack

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.



sipPROT (192.168.55.13) Daily Firewall Report
Mon, 18 Sep 2023

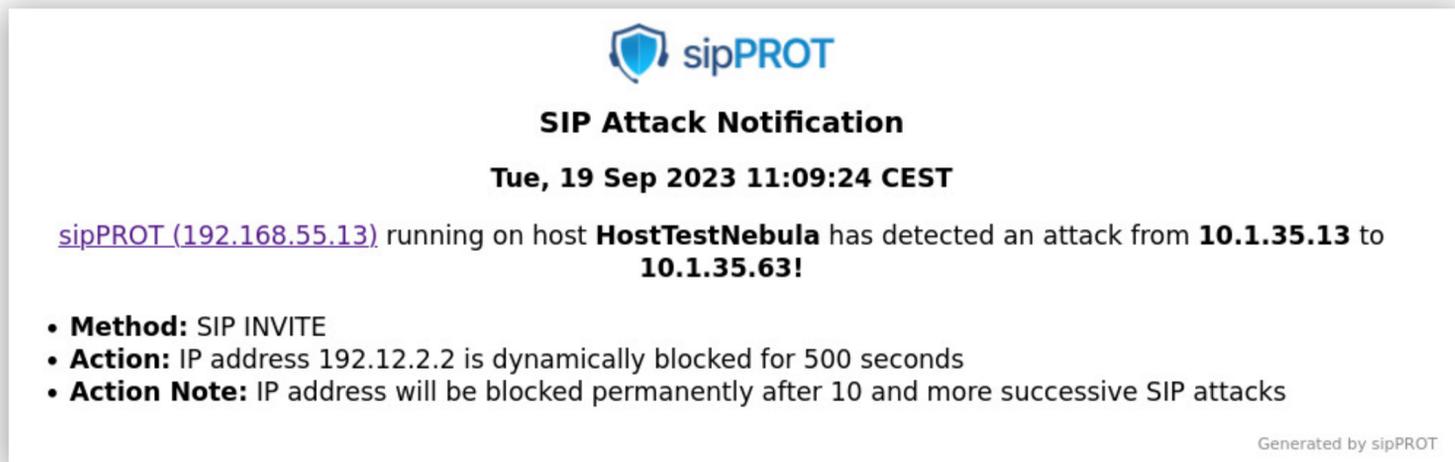
Attacker IP	Country	Method	Victim IP	Blocks
192.168.1.1	United States	SIP Scanner	10.0.0.1	50
192.168.1.5	Australia	SIP Scanner	10.0.0.5	25
192.168.1.7	India	SIP Scanner	10.0.0.7	45
192.168.1.9	Russia	SIP Scanner	10.0.0.9	55
10.0.0.2	Canada	SIP Scanner	192.168.1.2	30
172.16.0.1	Germany	SIP Scanner	192.168.1.3	20
10.0.0.4	United Kingdom	SIP Scanner	192.168.1.4	40
10.0.0.6	France	SIP Scanner	192.168.1.6	35
10.0.0.8	Brazil	SIP Scanner	192.168.1.8	15
192.168.1.1	China	SIP Scanner	192.168.1.10	60

Generated by sipPROT

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.



The screenshot shows an email notification from sipPROT. At the top is the sipPROT logo. Below it is the title "SIP Attack Notification" and the timestamp "Tue, 19 Sep 2023 11:09:24 CEST". The main body of the email states: "sipPROT (192.168.55.13) running on host HostTestNebula has detected an attack from 10.1.35.13 to 10.1.35.63!". Below this is a bulleted list of details: "Method: SIP INVITE", "Action: IP address 192.12.2.2 is dynamically blocked for 500 seconds", and "Action Note: IP address will be blocked permanently after 10 and more successive SIP attacks". The footer of the email reads "Generated by sipPROT".

 sipPROT

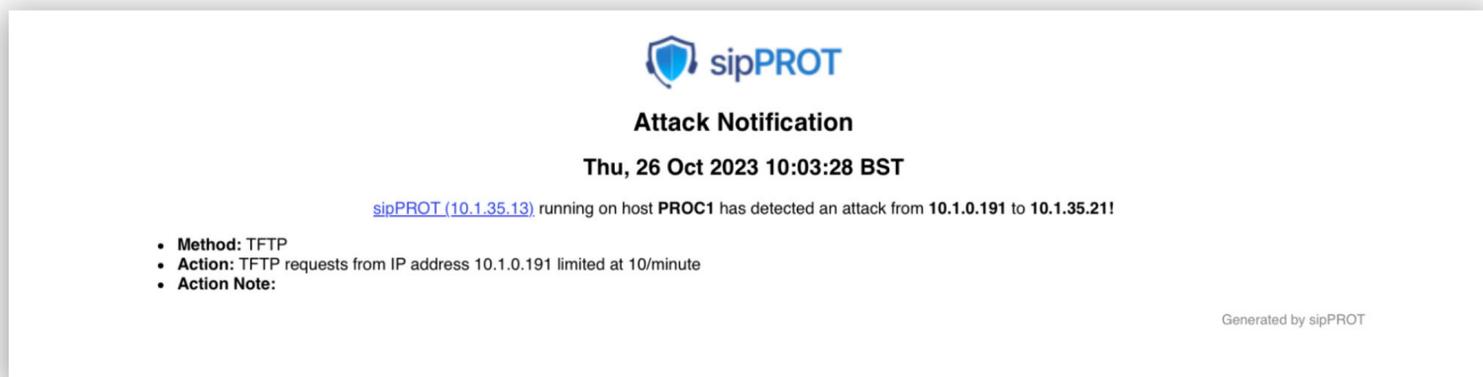
SIP Attack Notification
Tue, 19 Sep 2023 11:09:24 CEST

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.



The screenshot shows an email notification from sipPROT. At the top is the sipPROT logo. Below it is the title "Attack Notification" and the timestamp "Thu, 26 Oct 2023 10:03:28 BST". The main body of the email states: "sipPROT (10.1.35.13) running on host PROC1 has detected an attack from 10.1.0.191 to 10.1.35.21!". Below this is a bulleted list of details: "Method: TFTP", "Action: TFTP requests from IP address 10.1.0.191 limited at 10/minute", and "Action Note:". The footer of the email reads "Generated by 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
S Y S T E M S



Copyright Bicom Systems 2024