

sipPROT 5.4

Fireline Communications Security Protection

sipPROT is Fireline Communications' advanced SIP security module designed to protect your PBX systems from brute-force attacks, unauthorized SIP registration attempts, SIP INVITE floods, and geographically targeted intrusion attempts. It provides automated firewall rule updates, dynamic blocking, permanent denylisting, GEO IP filtering, and detailed attack visibility.

Why sipPROT Is Critical

Brute-force SIP attacks are common and can lead to:

- PBX downtime or unreachability
- Unauthorized SIP registration attempts
- Financial loss due to fraudulent call activity

sipPROT actively monitors SIP traffic and blocks malicious IP addresses in real time, providing a security layer specifically optimized for VoIP environments.

How sipPROT Works

When sipPROT detects suspicious SIP activity, it immediately updates firewall rules to block the attacking IP address.

Unlike generic intrusion-prevention systems, sipPROT analyzes live SIP traffic and reacts instantly.

sipPROT also includes GEO IP protection. Incoming IP addresses are compared against a GEO database, and traffic from blocked countries is automatically denied.

Important Note Before Deleting Extensions

Before removing an extension from your PBX, always factory-reset the phone registered to that extension. Failure to do so may cause repeated failed SIP REGISTER attempts, triggering sipPROT blocks and email alerts.

Accessing sipPROT from Business or Contact Center Systems

- **PBX Admin Portal:** Admin Settings → sipPROT → Settings
-

sipPROT Dashboard Overview

The dashboard provides real-time visibility into system security:

- **Health Status** – Indicates whether sipPROT is running properly.
- **Attacks Per Endpoint** – Shows targeted IPs or PBX instances.

- **Most Blocked Countries** – Displays geographic origin of blocked IPs.
- **Heatmap** – Visual representation of attack density by region.

All widgets support date filtering and auto-refresh intervals.

sipPROT



[Dashboard](#) [Attack Logs](#) [Allowlist](#) [Denylist](#) [Dynamic Denylist](#) [Settings](#)

SIP Ports:

x 5060

x

SIP Blocking Rule:

10

bad registrations per minute

SIP Invite Rate Limit:

☒ Enabled

SIP Invite Rate Limit Value:

5

SIP Invite Rate Limit Unit:

per minute

SIP Invite Burst Limit:

10

Dynamic Block Time:

1 Hour

Block Threshold:

3

Permanent Block SIP Attacks

Block SIP Register Attacks:

☒ Enabled

Block SIP Invite Attacks:

☒ Enabled

Blocked User Agents:

x friendly-scanner x sipsak x Elite

x

Geo Protection:

☒ Enabled

Policy:

☐ Allow ☒ Deny

Countries:

x  Andorra x  Botswana x  Burundi x  Antigua & Barbuda

x

[IP Geolocation by DB-IP](#)

Version: 2025-03

Update DB

Additional Protection:

☒ TFTP Protection

Notifications:

☒ Enabled ☒ Send Daily Attack Summary ☒ Send Log For Every Attack

Mail Recipients:

x mail@provider.com

x

Save Settings

sipPROT Settings

Firewall Configuration

- **SIP Ports** – Define monitored SIP ports (e.g., 5060 or 5060–5062).
- **SIP Blocking Rule** – Maximum unauthorized registrations per minute.
- **Dynamic Block Time** – Duration of temporary blocks.
- **Block Threshold** – Number of dynamic blocks before permanent denylisting.
- **Blocked User Agents** – List of SIP user agents to reject.

GEO Protection

- **Allow Mode** – Only selected countries are permitted.
- **Deny Mode** – Selected countries are blocked entirely.

SIP INVITE Rate Limiting

- **Rate Limit** – Max INVITES per minute before blocking.
- **Burst Limit** – Allowed initial burst of INVITES.

Permanent Blocking

- **Register Attack Blocking** – Permanently blocks repeated SIP REGISTER attacks.
- **Invite Attack Blocking** – Permanently blocks repeated SIP INVITE attacks.

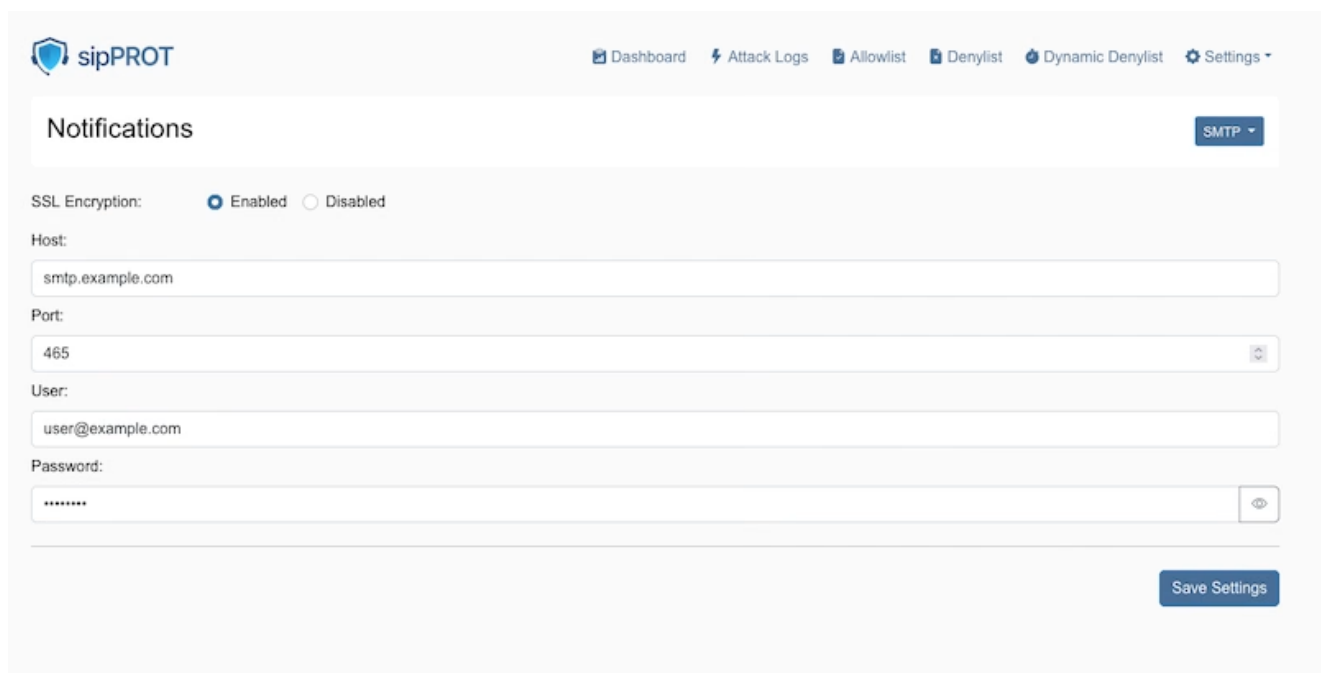
Additional Protections

- **TFTP Protection** – Rate-limits TFTP brute-force attempts.
- **DNS Protection** – Protects older systems from DNS resolver vulnerabilities.

Notifications

- **Daily Attack Summary**
- **Per-Attack Notifications**
- **Multiple Email Recipients**

SMTP settings must be configured correctly for notifications to function.



The screenshot shows the 'Notifications' settings page in the sipPROT interface. At the top, there is a navigation bar with links to Dashboard, Attack Logs, Allowlist, Denylist, Dynamic Denylist, and Settings. The 'Notifications' section is active, and a dropdown menu shows 'SMTP' selected. Below this, there are several configuration options: 'SSL Encryption' is set to 'Enabled' (radio button selected); 'Host' is 'smtp.example.com'; 'Port' is '465'; 'User' is 'user@example.com'; and 'Password' is masked with asterisks. A 'Save Settings' button is located at the bottom right of the form.

sipPROT

Dashboard Attack Logs Allowlist Denylist Dynamic Denylist Settings

Notifications SMTP

SSL Encryption: ☒ Enabled ☐ Disabled

Host: smtp.example.com

Port: 465

User: user@example.com

Password: *****

Save Settings

Attack Logs

The Attack Logs page displays:

- Attacker IP
- Victim IP
- Attack Type (REGISTER or OPTIONS)
- User Agent
- Timestamp

Logs can be filtered, searched, paginated, and inspected for detailed information.



Dashboard

Attack Logs

Allowlist

Denylist

Dynamic Denylist

Settings

Attack Logs

Search

Attack Type

Nov 20, 2023 - Nov 27, 2023

Reset

15 Per Page

Attacker IP Address	Victim IP Address	Attack Type	User Agent	Time	
107.189.5.180	45.141.164.96	OPTIONS	friendly-scanner	Nov 25, 2023 04:16:46 CET	
Host NameSW-public1					
Geo Protection					
sipPROT Version5.2.0+build.1380.rev.5640ab2					
Kernel Version5.15.103-commware-00013-gc005a5174808					
> 96.44.143.190	45.141.164.96	OPTIONS	friendly-scanner	Nov 25, 2023 00:49:20 CET	
> 96.44.142.190	45.141.164.99	OPTIONS	friendly-scanner	Nov 25, 2023 00:45:27 CET	
> 96.44.142.190	45.141.164.97	OPTIONS	friendly-scanner	Nov 25, 2023 00:45:27 CET	
> 96.44.142.186	45.141.164.100	OPTIONS	friendly-scanner	Nov 25, 2023 00:45:17 CET	
> 96.44.142.186	45.141.164.96	OPTIONS	friendly-scanner	Nov 25, 2023 00:45:17 CET	
> 104.225.219.109	45.141.164.96	OPTIONS	friendly-scanner	Nov 25, 2023 00:45:13 CET	
> 91.92.249.49	45.141.164.97	OPTIONS	friendly-scanner	Nov 24, 2023 16:06:40 CET	
> 91.92.249.49	45.141.164.96	OPTIONS	friendly-scanner	Nov 24, 2023 16:06:40 CET	
> 96.44.143.62	45.141.164.96	OPTIONS	friendly-scanner	Nov 23, 2023 22:07:58 CET	
> 96.44.143.62	45.141.164.96	OPTIONS	friendly-scanner	Nov 23, 2023 16:40:33 CET	
> 172.208.120.104	45.141.164.99	OPTIONS	friendly-scanner	Nov 23, 2023 14:45:24 CET	
> 172.208.120.104	45.141.164.98	OPTIONS	friendly-scanner	Nov 23, 2023 14:45:24 CET	
> 172.208.120.104	45.141.164.97	OPTIONS	friendly-scanner	Nov 23, 2023 14:45:24 CET	
> 172.208.120.104	45.141.164.96	OPTIONS	friendly-scanner	Nov 23, 2023 14:45:24 CET	

359 total

<

1

2

3

4

5

>

Allow & Deny Lists

Allowlist

IP addresses in the allowlist always bypass sipPR0T blocking.

- Add single IPs
- Import/export CSV
- Bulk delete
- Country-based search

Manage Allowlist					Add	Export	Import	Remove
Search		Country	Reset		Show 15 Per Page			
☐	IP Address ^	Country	Note	Actions				
☐	> 5.5.5.5	Germany						
☐	> 50.31.151.127	United States	local network backup					
☐	> 54.99.67.149	United States						
☐	> 60.158.27.62	Japan						
☐	> 65.148.109.35	United States						
☐	> 77.14.5.5	Germany	my test deskphone					
☐	> 78.8.31.95	Poland						
☐	> 86.150.131.175	United Kingdom						
☐	> 92.146.208.168	France						
☐	> 100.129.184.164	United States						
☐	> 100.137.140.192	United States						
☐	> 100.154.178.244	United States						
☐	> 100.210.114.249	United States						
☐	> 100.227.196.107	United States						
☐	> 100.245.112.237	United States						
0 selected / 1,045 total					1 2 3 4 5			

Denylist

IP addresses in the denylist are permanently blocked unless also present in the allowlist.

- Manual add
- CSV import/export
- Bulk removal

Manage Denylist

AddExportImportRemove

SearchCountryReset

Show 15 Per Page

☐	IP Address ^	Country	Note	Actions
☐	> 217.119.13.239	Netherlands		
☐	> 217.123.228.162	Netherlands		
☐	▼ 217.146.168.190	Switzerland	IP address has been added by Damir du...	
Time		Apr 24, 2023 11:37:46 CEST	Added By	Administrator ()
Note: IP address has been added by Damir due to suspicious activity. The IP had made 15 unauthorized registration attempts within a minute, exceeding the blocking rule threshold of 10.				
☐	> 217.152.243.67	Finland		
☐	> 217.153.51.76	Poland		
☐	> 217.159.254.73	Estonia		
☐	> 217.166.151.115	Netherlands		
☐	> 217.180.143.10	France		
☐	> 217.193.84.238	Switzerland		
☐	> 217.193.237.214	Switzerland		
☐	> 217.195.56.42	Latvia		
☐	> 217.196.1.143	United Kingdom		
☐	> 217.225.152.121	Germany		
☐	> 217.228.179.112	Germany		
☐	> 217.231.5.116	Germany		

0 selected / 10,045 total

◀ < 571 572 573 574 575 > ▶

Dynamic Denylist

Automatically populated with IPs that violate sipPR0T rules. Temporary blocks reset if attacks continue, and repeated offenders become permanently blocked.

Manage Dynamic Denylist

Remove

Search

Country

Reset

Show 15 Per Page

☐	IP Address ^	Country ^	Attack Type ^	Unblock In ^	Actions
☐	> 1.2.3.4	Australia	Sipsak	1h 59m 15s	
☐	> 15.6.63.44	United States	UNKNOWN	1h 59m 56s	
☐	> 25.6.63.44	United Kingdom	UNKNOWN	1h 59m 52s	
☐	> 45.6.63.4	Mexico	Telephone	1h 59m 38s	
☒	> 45.6.63.44	Mexico	Telephone	1h 59m 45s	

1 selected / 5 total

Manage Denylist

Add

Export

Import

Remove

Search

Country

Reset

Show 15 Per Page

☐	IP Address ^	Country	Note	Actions
☐	> 217.119.13.239	Netherlands		☒ ☐
☐	> 217.123.228.162	Netherlands		☒ ☐
☐	> 217.146.168.190	Switzerland	IP address has been added by Damir du...	☒ ☐
☐	> 217.152.243.67			☒ ☐
☐	> 217.153.51.76			☒ ☐
☐	> 217.159.254.73			☒ ☐
☐	> 217.166.151.115			☒ ☐
☐	> 217.180.143.10			☒ ☐
☐	> 217.193.84.238			☒ ☐
☐	> 217.193.237.214			☒ ☐
☐	> 217.195.56.42	Latvia		☒ ☐
☐	> 217.196.1.143	United Kingdom		☒ ☐
☐	> 217.225.152.121	Germany		☒ ☐
☐	> 217.228.179.112	Germany		☒ ☐
☐	> 217.231.5.116	Germany		☒ ☐

0 selected / 10,045 total

571

572

573

574

575

573

sipPROT v5.1.0 (build.788.rev.40990e9)

Add New IP Record

IP Address

217.146.168.190

Switzerland

✓

Note

Note

✓

Cancel

Add

Notifications & SMTP Configuration

Configure secure email delivery using SSL/TLS:

- SMTP host
- Port
- Username
- Password



[Dashboard](#) [Attack Logs](#) [Allowlist](#) [Denylist](#) [Dynamic Denylist](#) [Settings](#)

Notifications

SMTP

SSL Encryption: ☒ Enabled ☐ Disabled

Host:

Port:

User:

Password:

Save Settings

sipPROT CLI

sipPROT includes a command-line interface with autocomplete support.

```
sipprot status  
sipprot version  
sipprot list  
sipprot settings
```

Use flags such as --allow, --deny, --dynamic for detailed list output.

Summary

sipPROT is a critical security component for Fireline Communications PBX deployments, providing real-time SIP attack protection, GEO filtering, dynamic blocking, permanent denylisting, and comprehensive monitoring tools.