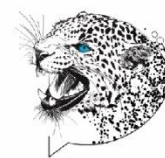


SMS Firewall Solution Description

Confidentiality, Information and Disclaimer

The information contained in this document is merely indicative. Broadnet Technologies will not be bound by any reference to a feature or other specific unless it is included in a contract properly drafted for the purpose and signed by a fully authorized person acting on behalf of the company.

Except for information that Broadnet Technologies has explicitly made public, all information contained in this paper regarding the Broadnet Technologies system and its future development should be regarded as confidential and should not be disclosed. Without prior written consent from Broadnet Technologies, no information may be shared with a third party.



Contents

Introduction	3
Overview	4
Broadnet Technologies SMS Firewall is an industry-recognized Tier 1 device that protects a mobile network from all SMS based messaging assaults and provides complete security and control over all network communications. The firewall is designed on the same engine/platform as the Broadnet Technologies Protect Unified Signalling Firewall suite and is an important part of it, therefore the SMS Firewall has access to the most recent technologies and capabilities.	
Purpose of an SMS Firewall.....	5
A2P Profitability	8
System Capabilities	9
Firewall Policies	10
Deployment.....	13
2.3 Features.....	13
2.4 Provisioning.....	13
<i>Rule Provisioning via Rest API</i>	13
Rule Provisioning via	14
Firewall Rules	14
DLT Templates.....	15
Block SMS Firewall Management.....	15
SMS Analysis.....	16
Message calcification	17
A2P Analysis Reports.....	18
SMS Anti-Phishing Capabilities.....	19
SMS Trap Analysis	20
The SMS Trap AnalysisProcess:	20
Benefits and Insights from SMS Trap Analysis: SMS Trap Analysis provides several benefits and valuable insights for operators in combating A2P SMS threats:	20
International Revenue Share Fraud detection	21
SMS Do-Not-Disturb (DND)	21
Pre-configured Rules	22
Network Implementation.....	23
Network Integration.....	23
Network architecture	23
SMS Firewall Redundancy	24
Traffic State	24
Description of Broadnet SMS Firewall Solution	25
Actions.....	26

Capture Module 27

Alert Module 28

Robust Backup Module 29

Data Retention and Deletion: 29

Vulnerability Management: 30

Employee Training and Awareness: 30

Third-Party Audits and Certifications: 30

Disaster Recovery and Business Continuity Plan: 30

Social Engineering and Phishing Mitigation: 30

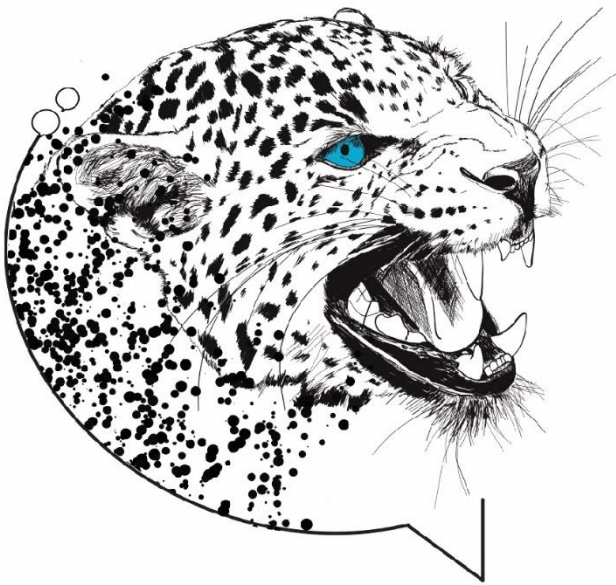
Incident Response Plan: 30

External Communication: 30

Risk Assessment: 30

Industry Compliance: 31

Non-Disclosure Agreements (NDAs): 31



Introduction

Overview

Broadnet Technologies SMS Firewall is an industry-recognized Tier 1 device that protects a mobile network from all SMS-based messaging assaults and provides complete security and control over all network communications. The firewall is designed on the same engine/platform as the Broadnet Technologies Protect Unified Signaling Firewall suite and is an important part of it, therefore the SMS Firewall has access to the most recent technologies and capabilities.

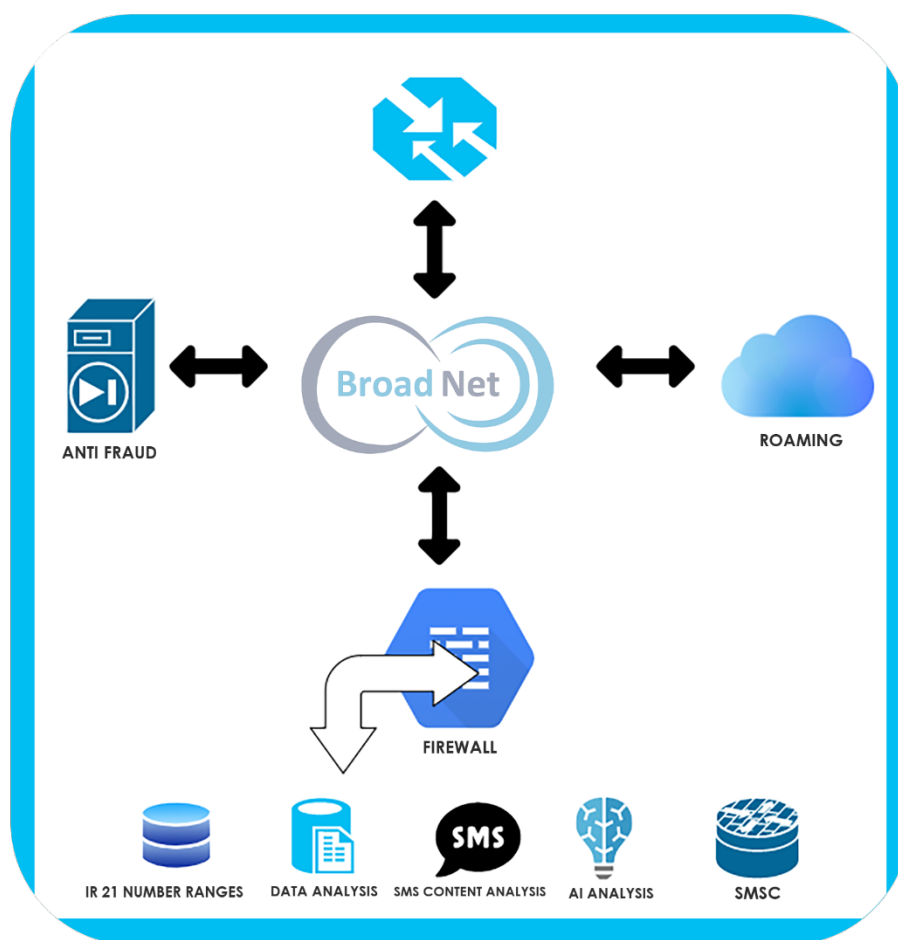


Figure 1--Broadnet Technologies products family tree, highlighting SMS Firewall and SMSC Home Router

SMS messages are terminated on a mobile network via the use of the following routes and technologies:

- International SMS are transmitted through means of international providers/gateways
- National off-net SMS messages originate from the national MNOs through SS7 interconnect trunks. This can be based on SIGTRAN.
- Corporate messaging is supplied over SMPP connections from the SMS Gateways
- Distributor of services (Service providers, they can send over HTTP/HTTPS Api's with easy tools to migrate from previous providers to our end in addition to SMPP connections that are available to both local and foreign businesses.
- SMS messages may both originate and terminated on the local network. This covers both valid person-to-person messages and messages from unauthorized SIMbox/SIMfarm sources.
- SMS Firewall is implemented at the network perimeter to intercept any interconnecting messages. Depending on client need, on-net messaging may also be protected by a firewall.

This can be seen in Figure 2.

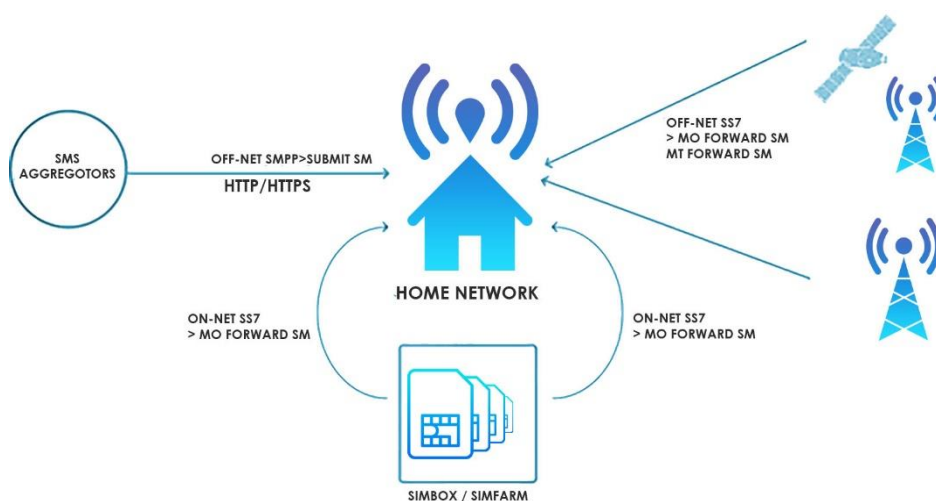


Figure 2--Broadnet Technologies SMS Firewall protects the network from illegitimate SMS from any source

Purpose of an SMS Firewall

1. **Security:** The primary purpose of an SMS firewall is to enhance the security of mobile networks by preventing unauthorized access, protecting against SMS-based threats such as spamming, spoofing, faking, smishing, and viruses. It helps maintain the integrity of network communications and safeguards user privacy.
2. **Threat Detection and Prevention:** An SMS firewall employs advanced technologies and algorithms to detect and prevent potential SMS-based threats in real-time. It analyzes SMS traffic, content, sender IDs, and other parameters to identify suspicious patterns or malicious activities, allowing timely intervention and mitigation.
3. **Content Validation and Filtering:** The firewall validates and filters SMS content based on predefined rules and policies. It ensures that only legitimate and authorized messages reach end-users while blocking or quarantining malicious or unauthorized content. Content filtering may include checking for specific keywords or URLs, enforcing compliance with regulatory guidelines, and identifying inappropriate or harmful content.
4. **Revenue Protection:** SMS firewalls play a crucial role in protecting revenue streams by preventing revenue leakage caused by SMS-related frauds, such as SMS spamming or SMS faking. By blocking fraudulent SMS traffic, the firewall ensures that legitimate A2P (Application-to-Person) messaging generates revenue for mobile network operators.
5. **Network Performance Optimization:** An SMS firewall helps optimize network performance by efficiently managing SMS traffic. It identifies and resolves issues related to network congestion, message routing, and delivery delays, ensuring a smooth and reliable messaging experience for end-users.
6. **Compliance with Regulatory Requirements:** SMS firewalls enable mobile network operators to comply with regulatory guidelines and standards related to SMS communications. They provide features for filtering and monitoring SMS content to ensure compliance with local regulations, industry guidelines, and privacy laws.
7. **Reporting and Analytics:** SMS firewalls offer comprehensive reporting and analytics capabilities, providing insights into SMS traffic patterns, security incidents, and network performance. Operators can leverage these reports to analyze trends, identify anomalies, and make informed decisions to improve operational efficiency and security measures.

8. **Fraud Prevention and Revenue Assurance:** By detecting and blocking fraudulent SMS activities, an SMS firewall contributes to revenue assurance by minimizing revenue losses resulting from SMS frauds, such as SMS spoofing or unauthorized SMS routing. It helps protect the operator's brand reputation and maintain trust among end-users.
9. **Customer Experience Enhancement:** With its security measures and filtering capabilities, an SMS firewall enhances the overall customer experience by reducing the risk of receiving unsolicited or malicious messages. It ensures that legitimate SMS messages are delivered promptly, promoting customer satisfaction and trust in the network.
10. **Scalability and Adaptability:** SMS firewalls are designed to scale and adapt to the evolving needs of mobile networks. They can handle increasing SMS volumes, accommodate new messaging protocols, and integrate with existing network infrastructure seamlessly.

SMS Security is necessary for all networks to avoid network and subscriber abuse and fraud. SMS vulnerabilities are described in GSMA publications IR.70: SMS Fraud and IR.71: SMS Fraud Prevention.

Table 1 details the hazards identified in these papers.

Threat	What happens?	Operator risk
SMS spamming	Unwanted messages to subscribers	Irritated customers, degraded performance. MNO blamed for relay
SMS flooding	Remote network sends massive volumes of messages targeting subscribers and nodes	Overload of signaling network. MNO incurs relay and operator costs
SMS faking	Foreign system illegally uses the identity of home SMSC	MNO cannot collect termination fees
SMS spoofing	Messages sent illegally by simulating subscribers in a roaming situation	Subscribers wrongfully billed for unsent messages/content
SMS Smishing	Messages that appear to be from a valid source attempt to acquire subscriber personal information	Customer annoyance, billing issues. Potential to spread more viruses and increase spam
SMS viruses	Hacker engine launches message luring subscribers to a download site with viruses	Compromised terminals cause customer service problems and may send unwanted messages
SMS Smishing	Foreign system floods the target network with <i>MO ForwardSM</i> messages to find an unsecured SMSC.	SMSC is forced to send SMS from foreign systems and home operator cannot collect fees!

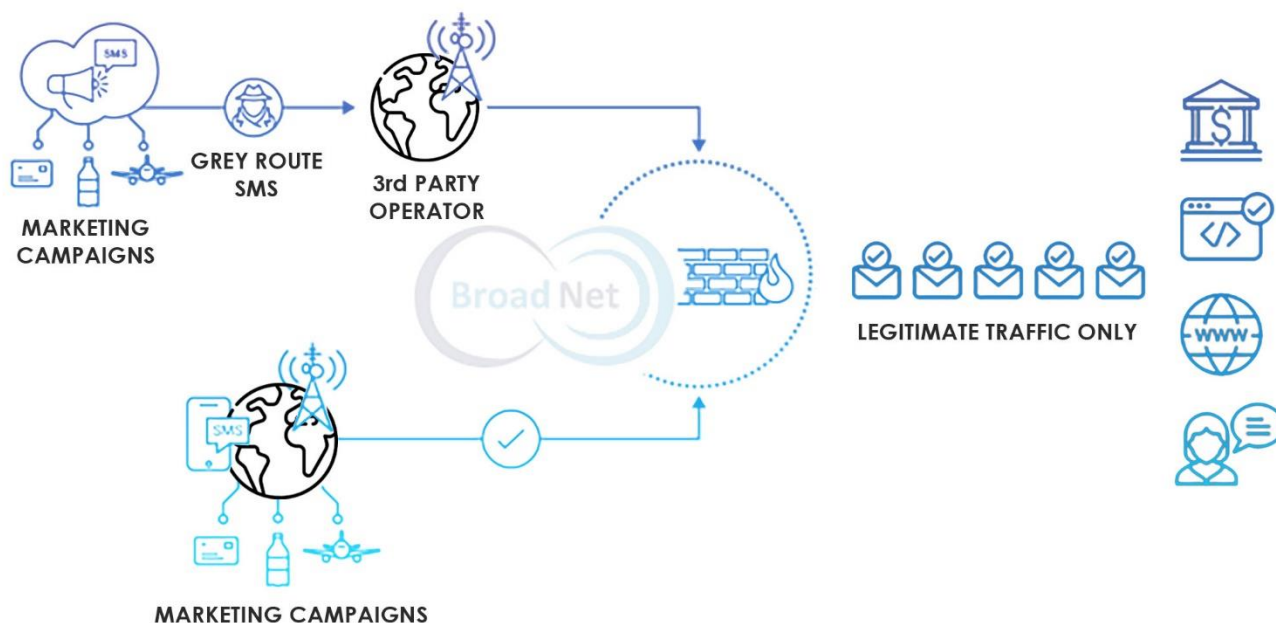
Broadnet Technologies SMS Firewall Solution Description

Table 1--Summary of SMS threats

In addition to the threat categories described before, the operator may be susceptible to risks associated with message characteristics, such as SMS content (e.g. viruses and smishing). The rising usage of SMS-based two-factor authentication (2FA, e.g. one-time passwords/OTPs) misleads users into believing they are protected, despite the reality that they are vulnerable to hackers through the SMS OTP threat vector.

A2P Profitability

A2P Monetization is the commercial approach of categorizing SMS into two distinct groups. P2P (Person-to-Person) and A2P (Application-to-Person) SMS. Enterprises must pay a higher fee for SMS termination when delivering traffic to Home Network customers (i.e. A2P SMS). The SMS Firewall's goal is to identify and stop A2P SMS traffic delivered into the Home network through a grey-route (i.e. a cheaper route designed for P2P traffic). Thus, guaranteeing that all A2P SMS are ended via official means.



System Capabilities

1. **Real-time Threat Detection:** Highlight the system's ability to detect and respond to SMS-based threats in real-time. Emphasize its capability to identify and block spam messages, malicious content, spoofed sender IDs, and other security risks.
2. **Advanced Filtering and Content Validation:** Discuss the system's advanced filtering mechanisms and content validation techniques. Explain how it can examine SMS content, keywords, URLs, attachments, and multimedia messages to ensure compliance, prevent fraud, and protect against malware.
3. **Granular Policy Management:** Highlight the system's flexibility in defining and managing granular policies. Explain how administrators can set up rules based on sender IDs, recipient numbers, content categories, and other criteria to customize the level of filtering and control.
4. **Intelligent Traffic Routing:** Describe the system's capability to intelligently route SMS traffic based on predefined rules. Explain how it can prioritize certain traffic types, apply specific routing based on sender reputation or volume behavior, and ensure efficient delivery and processing of messages.
5. **Reporting and Analytics:** Discuss the system's comprehensive reporting and analytics features. Explain how it provides detailed insights into SMS traffic patterns, security incidents, compliance violations, and network performance metrics. Highlight the value of these reports in identifying trends, optimizing operations, and making informed decisions.
6. **Integration with Network Elements:** Explain how the SMS firewall system seamlessly integrates with existing network infrastructure and interfaces with various network elements. Discuss its compatibility with SMSCs (Short Message Service Centers), MMSCs (Multimedia Messaging Service Centers), signaling networks, and other critical components.

2. Content Filtering Policy:
 - Establish policies to filter SMS messages based on content.
 - Define rules to block or flag messages containing specific keywords or phrases.
 - Implement policies to prevent the transmission of inappropriate or harmful content.
3. Keyword Filtering Policy:
 - Set up policies to filter SMS messages based on specific keywords.
 - Define rules to block or flag messages containing keywords associated with spam, fraud, or prohibited content.
 - Customize keyword filtering policies based on regulatory requirements or specific industry guidelines.
4. Traffic Volume Policy:
 - Establish policies to manage SMS traffic volume.
 - Define thresholds or limits for incoming or outgoing SMS messages.
 - Implement policies to prevent SMS flooding or abuse, ensuring fair usage of network resources.
5. Blacklisting/Whitelisting Policy:
 - Create policies to manage blacklisted or whitelisted sender IDs or phone numbers.
 - Specify rules to block or allow SMS messages from known spam sources or trusted senders.
 - Implement policies to maintain an updated list of blacklisted or whitelisted entities.
6. Compliance Policy:
 - Establish policies to ensure compliance with regulatory requirements.
 - Define rules to enforce privacy protection, consent management, or opt-in/opt-out processes.
 - Implement policies to adhere to local telecom regulations or industry-specific guidelines.
7. Routing Policy:
 - Define policies for SMS message routing.
 - Specify rules to route messages based on sender ID, recipient number, or other attributes.
 - Implement policies to optimize routing for cost efficiency or quality of service.
8. Reporting and Alerting Policy:
 - Establish policies for generating reports and alerts.
 - Define rules for capturing and analyzing SMS traffic, security incidents, or compliance violations.
 - Implement policies to trigger alerts based on predefined thresholds or suspicious activities.
9. Quarantine Policy:
 - Set up policies to quarantine suspicious or flagged SMS messages.
 - Define rules for holding messages that require further analysis or manual review.
 - Implement policies to ensure the integrity and security of the SMS communication channel.
10. Maintenance and Update Policy:
 - Establish policies for ongoing maintenance and updates of the SMS firewall.
 - Define rules for regular system updates, patches, and vulnerability management.

- Implement policies to ensure the firewall stays up-to-date with emerging threats and security best practices.

As part of the SMS firewall's capabilities, it supports various SS7 (Signaling System 7) and SMPP (Short Message Peer-to-Peer) messages for comprehensive protection and control. Here are the supported SS7 and SMPP messages:

1. SS7 MAP SRI-SM (Send Routing Information for Short Message):
 - The SMS firewall handles SS7 MAP SRI-SM messages, which are used to request routing information for a short message. This message is crucial for determining the correct routing path for SMS delivery.
2. SS7 MAP MO_ForwardSM (Mobile Originated Forward Short Message):
 - The SMS firewall processes SS7 MAP MO_ForwardSM messages, which are sent by a mobile device to initiate the delivery of a mobile-originated short message.
3. SS7 MAP MT_ForwardSM (Mobile Terminated Forward Short Message):
 - The SMS firewall handles SS7 MAP MT_ForwardSM messages, which are sent by the network to deliver a mobile-terminated short message to a mobile device.
4. SMPP SubmitSM (Submit Short Message):
 - The SMS firewall supports the SMPP SubmitSM message, which is used by external applications or systems to submit short messages for delivery through the SMPP protocol.
5. SMPP DeliverSM (Deliver Short Message):
 - The SMS firewall processes the SMPP DeliverSM message, which is used to deliver short messages to external applications or systems via the SMPP protocol.

In addition to supporting these specific SS7 and SMPP messages, the SMS firewall is fully compliant with SMPP v3.4 and MAP 3GPP TS 29.002-Rel12. It ensures compatibility with industry standards and protocols, allowing seamless integration with mobile network infrastructure. The SMS firewall's Anti-Fraud Engine operates between the core network of the Mobile Network Operator (MNO) and the rest of the network. It plays a crucial role in safeguarding the network's core and preventing it from becoming congested or overwhelmed by undesirable traffic.

By utilizing a rule-based message screening mechanism, the SMS firewall enables the shaping of traffic. This capability allows for the filtering and prioritization of SMS messages based on predefined rules and policies, ensuring optimal network performance and protecting against fraudulent or malicious traffic.

Overall, the SMS firewall's support for SS7 and SMPP messages, along with its rule-based message screening and traffic shaping capabilities, provides comprehensive protection, efficient traffic management, and secure SMS communications within the mobile network infrastructure.

In addition to the support for SS7 and SMPP messages, the SMS firewall also extends its capabilities to handle HTTP/HTTPS communication protocols with various methods and data formats. Here are the supported HTTP/HTTPS methods and data formats:

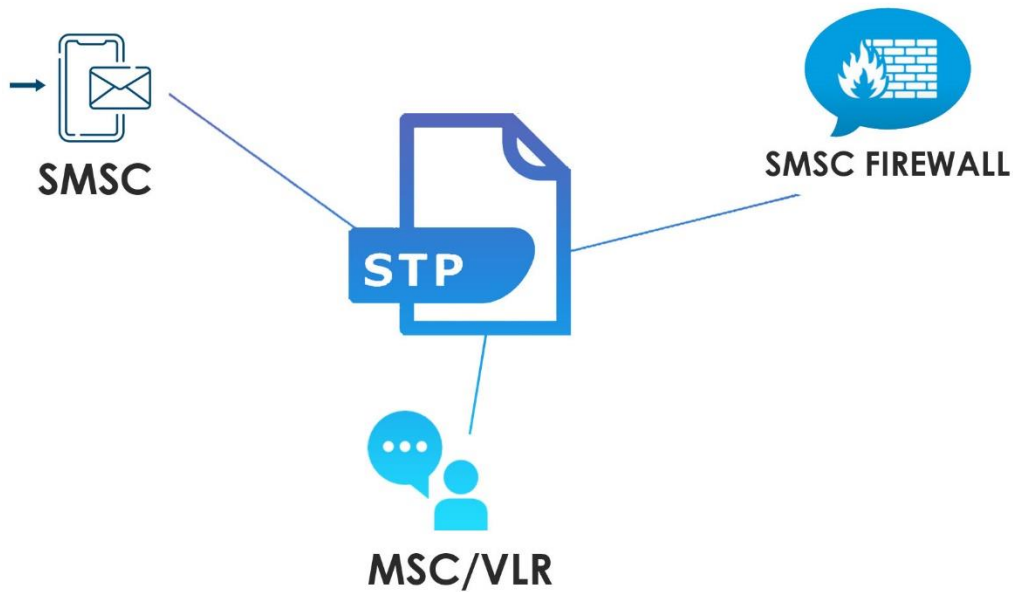
1. HTTP/HTTPS Methods:

- GET/POST: The SMS firewall supports the GET/POST methods, which allows retrieving data from a specified resource or URL. It can process incoming SMS requests and retrieve relevant information or trigger appropriate actions based on the provided parameters.
- 2. Data Formats:
 - XML: The SMS firewall handles XML data format, allowing the exchange of structured data in a standardized format. It can parse XML payloads, extract relevant information, and perform necessary actions based on the received XML data.
 - SOAP (Simple Object Access Protocol): The SMS firewall supports SOAP, which is a protocol for exchanging structured information in web services. It can process SOAP messages, extract relevant data elements, and perform actions based on the received SOAP requests.
 - JSON (JavaScript Object Notation): The SMS firewall handles JSON data format, which is widely used for lightweight data interchange. It can parse JSON payloads, extract relevant information, and trigger appropriate actions based on the received JSON data.
 - Text Method: The "text" method provides flexibility when dealing with SMS content that is not structured in XML, SOAP, JSON, or other specific formats. It ensures that the SMS firewall can effectively process and analyze the content regardless of the format in which it is received.

These capabilities enable the SMS firewall to seamlessly integrate with applications, systems, or services that utilize HTTP/HTTPS protocols and communicate using different methods and data formats. Whether it's receiving SMS-related requests or exchanging data with external entities, the SMS firewall ensures secure and reliable communication over HTTP/HTTPS, supporting various methods and data formats for enhanced interoperability and functionality.

Deployment

The firewall should be installed in the network of the service provider. It combines the signaling network via Sigtran (M3UA) .



2.3 Features

1. Calling Gt based filtering.
2. Called GT based filtering.
3. Sender Id based filtering.
4. Home Routing.
5. Keywords based filtering.
6. Calling GT validation

2.4 Provisioning

Rule Provisioning via Rest API

The firewall solution can be provisioned using Rest API or with the GUI interface. The network provision is file based while provision of rules is from APIs or GUI.

Rule Provisioning via API:

URL : <http://host:9000/firewall>

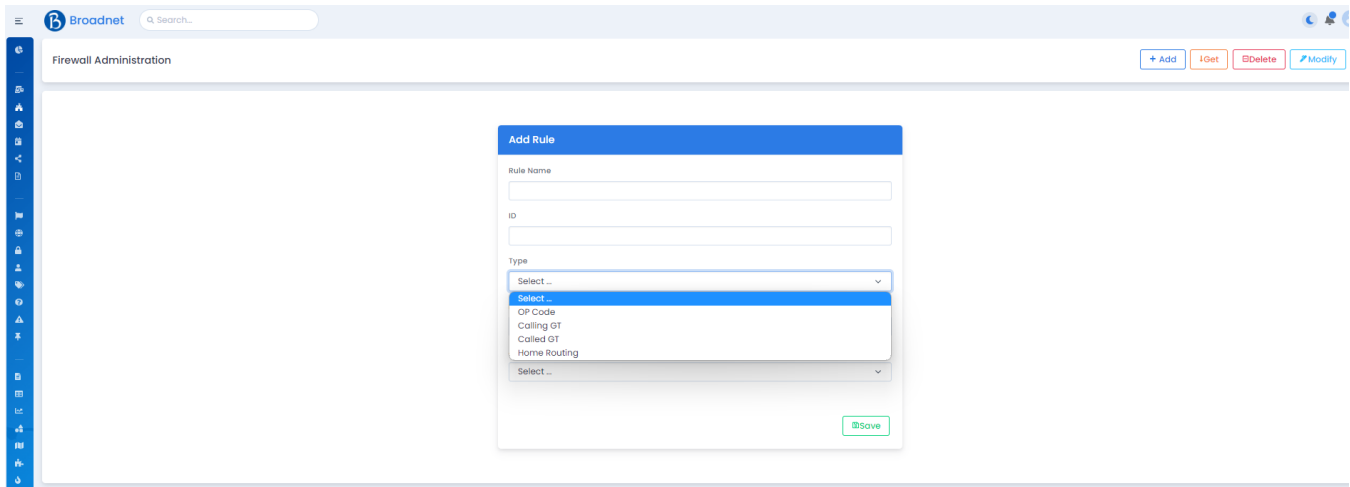
Json Body

```
{
  "ruleId" : "1",
  "type" : "2",
  "ruleName": "calledGtBlock",
  "op_code" : "0",
  "calling_gt" : "+878888888",
}
```

```
"called_gt" : "+92199999999",
"imsi" : "3456677777555",
"senderId" : "TESTSMS"
"text" : "Fraud Detection",
}
```

POST is for add rule, GET for getting the rule and DELETE for deleting an existing rule.

Rule Provisioning via *GUI*:



The screenshot shows the Broadnet Firewall Administration interface. A modal window titled 'Add Rule' is open, displaying fields for 'Rule Name', 'ID', and 'Type'. The 'Type' dropdown menu is expanded, showing options: 'OP Code', 'Calling GT', 'Called GT', and 'Home Routing'. A 'Save' button is visible at the bottom right of the modal.

Firewall Rules

Rule Criteria – A rule can include multiple criteria, and "AND" and "OR" logic are supported. In order for the message to comply with the rule, all evaluation criteria must be met. Cross-comparison of message parameters from separate or the same layers is supported.

The user can then specify a value to match after selecting a message parameter as a criterion.

This value may be an entire address, a prefix of an address, a range of numbers, or a list of values uploaded by the user.

Advanced matching cases also support regular expression matching.

The Broadnet Technologies SMS Firewall appends valuable parameters to each message (e.g., source country, source network, destination country, destination network, etc.)

All messaging layers are supported, and the rules system has access to every parameter.

All M3UA, MTP3, SCCP, TCAP, MAP, SM-TP, and SMPP messages are included.

Even though the list below (Figure 8) is not exhaustive, it does emphasize some of the most common criteria used in rule matching.

DLT Templates

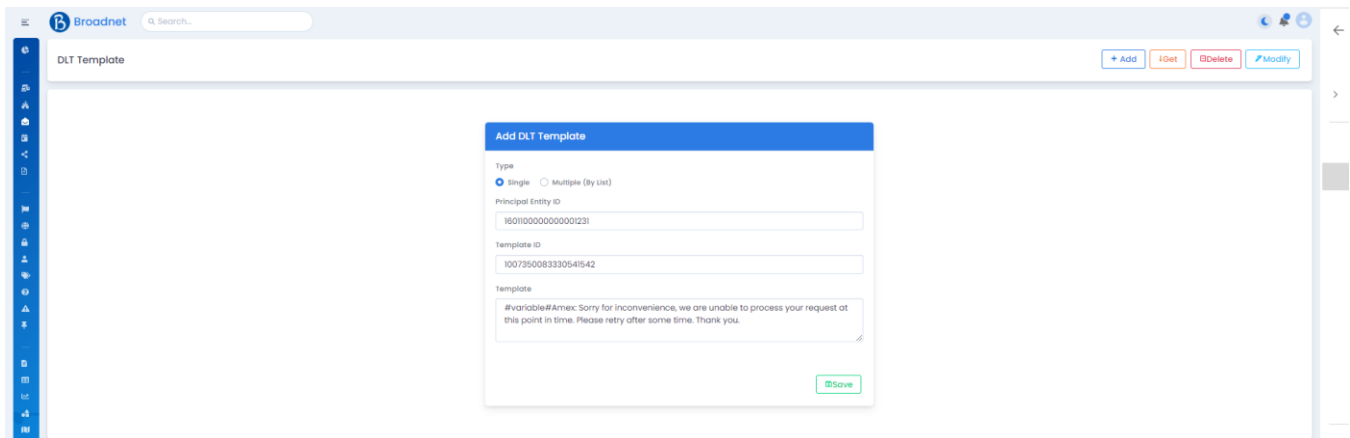
Distributed Ledger Technology (DLT) has revolutionized several sectors, including telecommunications.

DLT improves SMS firewall and server security, compliance, and message delivery. Decentralized and immutable DLT may be used in your SMS firewall. Secure and transparent Principal Entity ID and Template configurations enable comprehensive verification. Each SMS sender, receiver, and intermediary receives a unique, tamper-proof Principal Entity ID. This prevents spoofing and fraud by precisely tracing message sources.

DLT can also improve message template setting. DLT's decentralization allows templates to be saved and checked throughout the network, avoiding illegal changes and maintaining message integrity.

DLT improves SMS regulatory compliance. DLT lets you track message-related activity. This helps meet government and business regulations.

In conclusion, implementing DLT into your SMS firewall and server improves security, transparency, and compliance.



The screenshot shows the 'Add DLT Template' form in the Broadnet interface. The form includes the following fields and options:

- Type:** Radio buttons for 'Single' (selected) and 'Multiple (By List)'.
- Principal Entity ID:** A text input field containing '18010000000000231'.
- Template ID:** A text input field containing '1007350083330541542'.
- Template:** A text area containing the placeholder text: '#Variable#Amex: Sorry for inconvenience, we are unable to process your request at this point in time. Please retry after some time. Thank you.'
- Buttons:** '+ Add', 'Get', 'Delete', 'Modify' at the top right, and a 'Save' button at the bottom right of the form.

Block SMS Firewall Management

Our BSFM (Block SMS Firewall Management) firewall is equipped with advanced capabilities to ensure efficient SMS filtering and control. With our solution, you can effectively manage incoming and outgoing SMS messages by leveraging various parameters, including sender ID, prefix, client, routing, sender type group, content, profile activation, reroute group, force sender ID, message length, and schedule. By leveraging these parameters, our firewall can enforce specific rules and actions based on a hierarchical structure.

Our firewall system is designed to handle all incoming and outgoing SMS traffic, providing robust protection and control mechanisms. By analyzing the defined parameters, our solution can identify and categorize SMS messages accurately. This allows for effective decision-making and appropriate actions to be taken based on the predefined rules hierarchy.

With our BSFM firewall, you can ensure that your SMS ecosystem remains secure and compliant. By customizing rules and leveraging the parameters mentioned above, you can effectively block spam, phishing attempts, and other malicious SMS traffic. Additionally, the firewall enables efficient routing and management of legitimate messages, providing a seamless and reliable SMS experience for your users.

Our solution prioritizes flexibility and scalability, allowing you to adapt the rules hierarchy to meet your specific requirements. By fine-tuning the parameters and rules, you can ensure that the SMS firewall aligns perfectly with your organization's policies and objectives.

Profile Name			
Smsc	441827 44181 441810 4418100 441801 441802 441803 441804 441805 441806	>> <<	
Username	0018 440112 1004 1004 1004 1004 1004 1004 1004 1004 1004	>> <<	
SenderId (Comma Separated)			
SenderType		-NONE-	
Prefixes (Comma Separated)			
Contents (Comma Separated)			
ProfileActivation		Yes	
Reverse		No	
RerouteGroup		NONE	
Reroute			
ForceSenderId			
MessageLength		0	
MessageLengthOpr		NONE	
Schedule <input type="checkbox"/>			

SMS Analysis

This module incorporates advanced analytics and reporting capabilities, providing valuable insights into the SMS traffic entering the home network. It offers a comprehensive breakdown

of SMS messages based on factors such as enterprise sender, sender ID, country, network, and more.

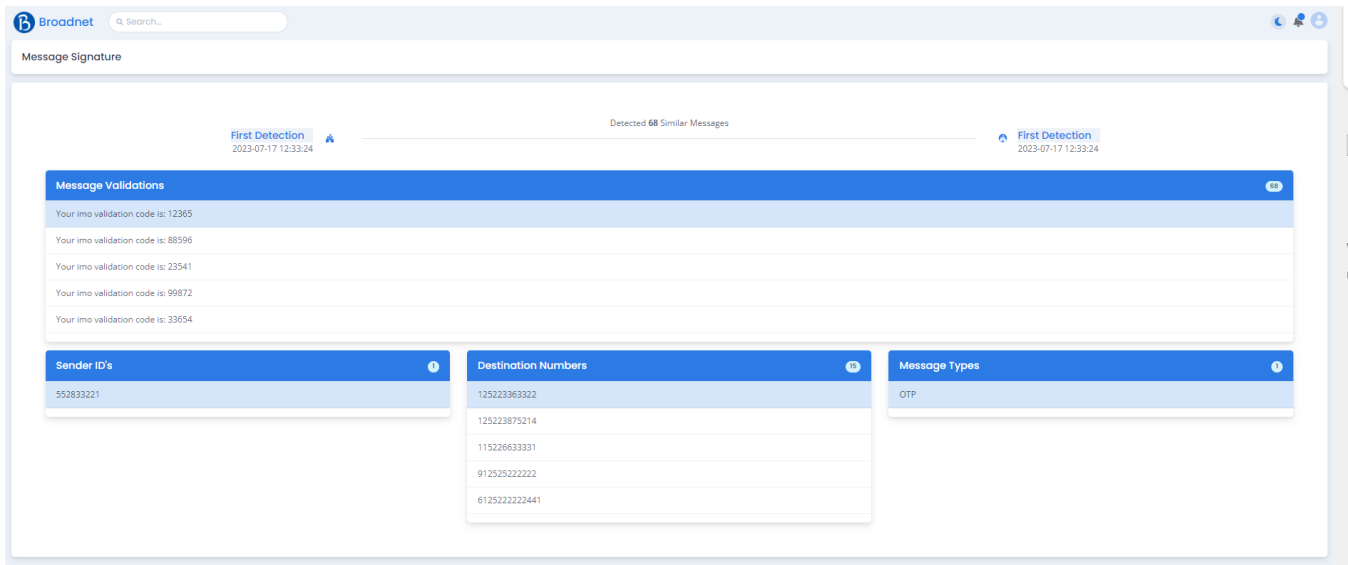
The A2P SMS Analysis module delivers two key capabilities:

1. **SMS Content Analysis:** This feature involves thorough scanning of the content of all SMS messages passing through the firewall. It generates message "Signatures" when multiple messages contain identical or highly similar content. The information included in each signature encompasses:
 - SMS message content, including any variations.
 - Count of SMS messages matching the identified content pattern.
 - Count and list of sender IDs associated with the content pattern.
 - Count and representative list of message receivers.
 - SMS message type, distinguishing between MO (Mobile Originated), MT (Mobile Terminated), or SMPP.
 -
- **Traffic Behavior,** provides detailed reports and notifications, highlighting any abnormal traffic behavior observed for specific sender IDs. This information allows network administrators to take proactive measures in addressing potential issues, such as blocking or rate-limiting suspicious sender IDs or applying additional security measures to mitigate risks.

The SMS Content Analysis capability ensures comprehensive monitoring and identification of recurring content patterns in SMS messages, facilitating effective detection and response to potential A2P or spam message threats.

Additionally, please note that the SMS Analysis module can be further enhanced with additional features such as:

- **Keyword Filtering:** Implementation of configurable keyword-based filtering rules to block or flag SMS messages containing specific keywords associated with spam, fraud, or prohibited content.
- **Real-time Reporting:** Provision of real-time reports and dashboards to visualize and analyze SMS traffic trends, identify potential security incidents, and make informed decisions based on the generated insights.



Broadnet Search...

Message Signature

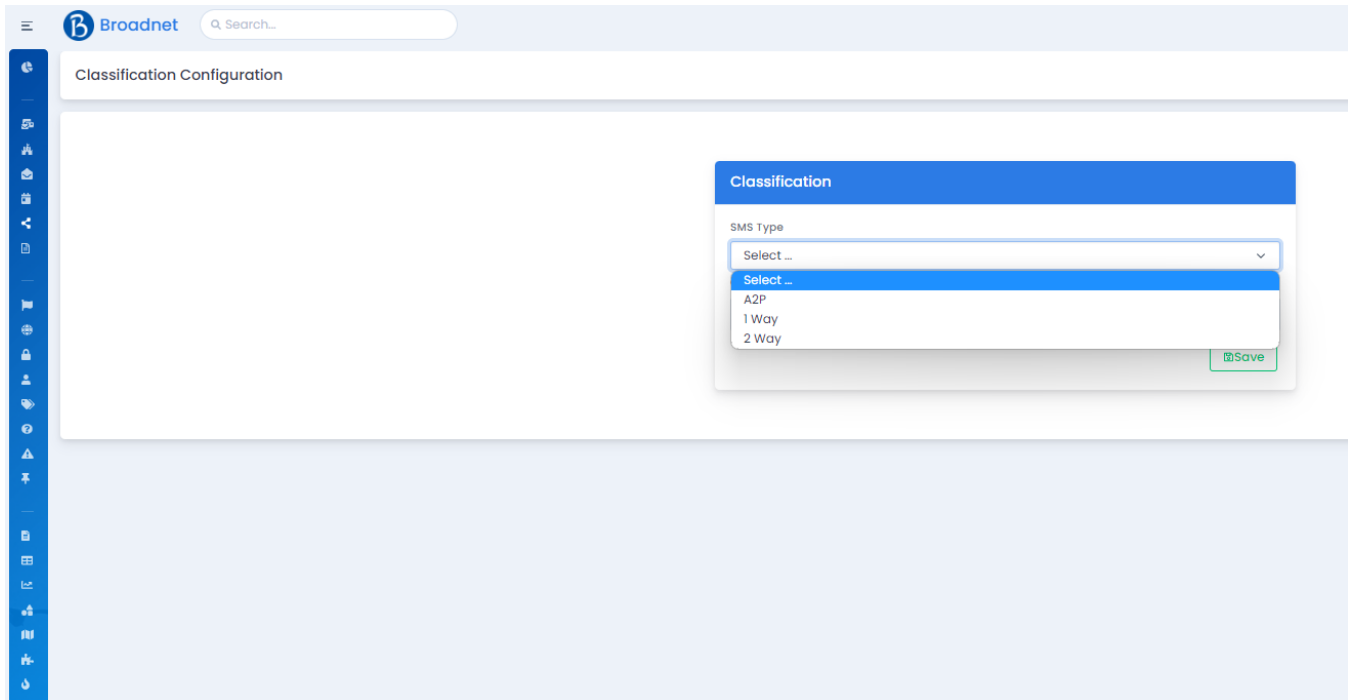
First Detection 2023-07-17 12:33:24 Detected 68 Similar Messages First Detection 2023-07-17 12:33:24

Message Validations	
Your imo validation code is:	12365
Your imo validation code is:	88396
Your imo validation code is:	23541
Your imo validation code is:	99872
Your imo validation code is:	33654

Sender ID's	Destination Numbers	Message Types
552833221	125223363322	OTP
	125223875214	
	115226633331	
	912525222222	
	6125222222441	

Message calcification

An "tag" of "A2P," "P2P," or "Spam" may be assigned to each signature. A tag is additional data appended to the signature. The tag is automatically applied whenever an SMS matching the stated signature is received by the firewall in the future. Whenever a message is received with an A2P tag (but over an unapproved route), the message might be ignored. Additional "tags" may be added to each signature to further categorize the communication. Facebook, Google, Onetimepassword, and many more are all examples.



Broadnet Search...

Classification Configuration

Classification

SMS Type

Select ...

Select ...

A2P

1 Way

2 Way

Save

A2P Analysis Reports

This section of the module is designed to identify enterprises engaged in transmitting A2P (Application-to-Person) SMS messages, such as popular platforms like WhatsApp, TikTok, Facebook, Google, PayPal, and more. Leveraging these additional identifiers, the A2P Analysis module generates comprehensive reports on A2P SMS messages entering the operator's network. Here's an overview of the report's key data:

1. **Separation of A2P and P2P Traffic:** The report distinguishes between A2P and P2P (Person-to-Person) traffic to provide a clear understanding of the SMS message types entering the network.
2. **Transmitting Enterprises:** It provides a breakdown of the transmitting enterprises involved in A2P traffic, including platforms like Viber, WhatsApp, and others. This information helps identify the entities responsible for A2P SMS messaging.
3. **Sender IDs:** The report highlights the specific sender IDs utilized in A2P SMS communications, allowing for better tracking and identification of message sources.
4. **Countries and Networks of Origin:** It provides insights into the countries and networks from which the A2P SMS messages originate, aiding in geographical analysis and identifying global traffic patterns.
5. **Source SCCP Calling GTs:** This data reveals the source SCCP (Signaling Connection Control Part) calling GTs, which are the sending SMSC (Short Message Service Center) addresses associated with the A2P communications.
6. **Timeline:** The report includes a timeline feature, indicating when the A2P messages entered the network, enabling time-based analysis and trend identification.
7. **Regulatory Tags:** Any specific tags specified in the regulatory section are captured, providing additional information and compliance-related insights.

The most valuable feature of this report lies in its ability to apply filters to the data. Users can interact with the report by clicking on various metrics, which dynamically applies filters and presents relevant information. Here are some examples of the data exposed through interaction:

- Clicking on "Facebook" reveals countries, networks, SMSCs, and sender IDs associated with Facebook's A2P traffic.
- Clicking on an SMSC address provides details of the companies and sender IDs utilizing that particular SMSC for SMS messaging.
- Clicking on a Sender ID, such as "Facebook," displays all businesses using this shortcode, including those employing local SMPP connections as a grey-route.

By offering interactive filtering and comprehensive data exposure, the A2P Analysis Reports provide valuable insights into A2P SMS traffic, facilitating accurate identification of transmitting enterprises, message sources, geographical patterns, and compliance-related information within the operator's network.

SMS Anti-Phishing Capabilities

SMS-based phishing, also known as smishing, has become a growing concern in the mobile communications landscape. Attackers exploit the widespread use of SMS messaging to trick users into clicking malicious links or sharing sensitive information.

SMS firewall, specifically designed to detect and prevent smishing attacks. It employs various techniques and intelligence databases to identify potentially harmful URLs within SMS messages and apply appropriate actions to protect users from falling victim to phishing attempts.

Key Actions to Combat SMS Phishing:

1. **Blocking Suspicious URLs:** The SMS firewall can analyze SMS content and block any messages containing URLs that are known to be associated with attack sites. By proactively preventing these messages from reaching users, the firewall significantly reduces the risk of users inadvertently accessing malicious websites.
2. **Allowing Safe URLs:** Conversely, the SMS firewall can allow SMS messages containing URLs that are recognized as safe and trusted. This ensures that legitimate messages with valuable links reach their intended recipients without disruption.
3. **Modifying SMS Content:** In cases where the SMS contains a URL of unknown reputation, the firewall can modify the content of the SMS to indicate the safety of the link to the user. This proactive approach informs users about potential risks associated with the URL and promotes cautious behavior.
4. **URL Redirection:** Another effective strategy is to modify the URL within the SMS content to redirect users to a warning or block page. This technique prevents users from accessing potentially malicious websites, redirecting them to a secure environment where they can be educated about the risks and advised on how to proceed safely.
5. **User Notifications:** To further enhance user awareness, the SMS firewall can send an additional SMS to inform users about the safety of the link. This real-time notification ensures that users are promptly informed about potential threats and encourages them to exercise caution when interacting with SMS messages.

The Broadnet Technologies Phishing Threat Intelligence Database: The SMS Anti-Phishing capabilities are bolstered by the Broadnet Technologies Phishing Threat Intelligence Database, which comprises two essential components: the Broadnet Technologies SMS Anti-Phishing Cloud and the 3rd Party URL reputation database.

The Broadnet Technologies SMS Anti-Phishing Cloud serves as a central repository for caching URL reputations from all Broadnet Technologies SMS Anti-Phishing deployments. This cloud-based architecture ensures fast processing of URLs within SMS messages and provides a global view of ongoing smishing attacks, enabling comprehensive protection for users across multiple networks.

Additionally, the integration of a 3rd Party URL reputation database enriches the SMS Anti-Phishing capabilities by leveraging external intelligence sources to identify known malicious URLs. This collaborative approach enhances the accuracy and effectiveness of the SMS firewall in detecting and mitigating smishing attacks.

Conclusion: SMS Anti-Phishing is a vital feature within an SMS firewall, dedicated to mitigating the risks associated with smishing attacks. By employing a combination of techniques, such as blocking suspicious URLs, allowing safe URLs, modifying SMS content, URL redirection, and user

notifications, the SMS firewall provides robust protection against SMS phishing attempts. With the support of the Broadnet Technologies Phishing Threat Intelligence Database, including the Broadnet Technologies SMS Anti-Phishing Cloud and 3rd Party URL reputation database, operators can ensure comprehensive security for their networks and users, defending against evolving smishing threats.

SMS Trap Analysis is a sophisticated technique employed by SMS firewalls to strengthen the security of mobile networks and protect against A2P (Application-to-Person) SMS attacks. By setting up virtual phone numbers within the firewall system, known as Trap Analysis numbers, operators can effectively intercept and analyze A2P SMS messages originating from popular enterprise platforms. This article delves into the process of SMS Trap Analysis, highlighting its significance in detecting and mitigating A2P SMS-based threats.

SMS Trap Analysis

The SMS Trap Analysis Process:

1. **Triggering A2P SMS from Enterprise Platforms:** A2P SMS messages are initiated from enterprise platforms such as Facebook, Google, or WhatsApp. These messages are sent to one of the virtual MSISDNs (Mobile Subscriber Integrated Services Digital Network Numbers) set up within the SMS firewall.
2. **Intercepting SRI-SM at the SMS Firewall:** Upon arrival of the SMS Routing Information-Short Message (SRI-SM) at the SMS firewall for the specific virtual MSISDN, the firewall responds with a fake IMSI (International Mobile Subscriber Identity) and a global title that is routed back to the originating enterprise platform. This interaction creates the illusion that the message has been successfully delivered to the intended recipient.
3. **Analyzing A2P MT-FSM Messages:** As a result, the subsequent A2P Mobile Terminated-Forward Short Message (MT-FSM) message is routed back to the SMS firewall. At this stage, the firewall drops the message to prevent it from reaching the actual recipient. The dropped message is logged and thoroughly analyzed to ensure that it arrived via the appropriate route and matches the expected behavior.

Benefits and Insights from SMS Trap Analysis: SMS Trap Analysis provides several benefits and valuable insights for operators in combating A2P SMS threats:

1. **Early Detection of A2P SMS:** By intercepting A2P SMS messages within the SMS firewall, operators gain early visibility into potential A2P SMS-based attacks. This allows them to promptly analyze and respond to emerging threats before they impact the network and its users.
2. **Improved Threat Intelligence:** The analysis of intercepted A2P MT-FSM messages provides valuable insights into the behavior, origin, and patterns associated with A2P SMS traffic. This information helps operators enhance their threat intelligence, refine SMS firewall policies, and develop proactive defense strategies against A2P SMS attacks.

3. Ensuring Proper Routing: Analyzing the dropped A2P MT-FSM messages ensures that messages arriving over the expected route are properly identified and handled. This verification process ensures the integrity and security of SMS traffic within the network.

Conclusion: SMS Trap Analysis is a crucial component of an SMS firewall, enabling operators to detect, intercept, and analyze A2P SMS messages originating from popular enterprise platforms. By simulating successful delivery to the enterprise platforms while dropping the messages within the firewall, operators gain valuable insights into A2P SMS behavior and enhance their overall security posture. SMS Trap Analysis, in conjunction with other advanced features, plays a pivotal role in safeguarding mobile networks from A2P SMS threats, ensuring secure and reliable communication for users.

Regenerate response

Simbox Detection

A2P simbox detection is one of SMS Sender Aggregation's primary use cases. When a standard SIM card is used to transmit A2P traffic. Typically, this is characterized by a single MSISDN transmitting messages to numerous recipients. The default configuration for identifying simbox MSISDNs would involve the transmission of over 20 messages per hour to 15 distinct recipients. This is deployed as the default configuration, and the results are then analyzed to determine if the matching MSISDNs can be confirmed as simboxes. This type of fraud identification will require network-specific tailoring based on the number of subscribers, the approved A2P SMS rate, and the prevalence of P2P SMS on the network.

IRSF Discovery

International Revenue Share Fraud detection

IRSF fraud involves subscribers who send SMS messages with a high termination rate to international destinations. These messages may not reach their intended recipient and may be intercepted by a fraudster so that they can retain the majority of their revenue. This fraud will be perpetrated in one of two ways: by fraudulently procuring a large number of post-paid SIM cards without the intent to pay, or by infecting normal subscriber handsets with malware. SMS Sender Aggregation can aid in combating this type of fraud by analyzing all MO traffic originating from domestic network subscribers destined for international destinations. Standard operating procedure would be to verify for more than ten international SMS transmissions per hour. Similar to simbox detection, this form of fraud will require fine-tuning based on subscriber characteristics.

SMS Do-Not-Disturb (DND)

The SMS do not disturb functionality enables subscribers to opt out of receiving A2P sms messages previously identified as marketing or originating from particular A2P sources. The subscriber can send an SMS message to a particular brief code, at which point they will be added to the block list. Various keywords can be included in the SMS message to determine

which services or sources the subscriber cannot receive traffic from. At any time, the subscriber may opt out of this service.

Pre-configured Rules

Select	Profile ID	Name	Active	Reverse	Reroute	Schedule
<input type="radio"/>	142	TelcelKSA	true	false	GW997	false
<input type="radio"/>	3	UAE2	true	false		false
<input type="radio"/>	19	UAESenders	true	false	GWSERV169P	false
<input type="radio"/>	7	UAE6	true	false		false
<input type="radio"/>	2	UAE1	true	false		false
<input type="radio"/>	61	SMSMOB	true	false	GW166	false
<input type="radio"/>	141	Blocked 1879432675	true	false	GW997	false
<input type="radio"/>	136	URL_FILTER	false	false		false
<input type="radio"/>	42	IndiaBlock8	true	false		false
<input type="radio"/>	6	UAE5	true	false		false
<input type="radio"/>	26	IndiaBlock	true	false		false
<input type="radio"/>	18	India170	true	false		false
<input type="radio"/>	46	IndiaBlock12	true	false		false
<input type="radio"/>	5	UAE4	true	false		false
<input type="radio"/>	17	USERTOMOB	true	false	AMSERV285	false
<input type="radio"/>	16	USERTAIN	true	false	AMSG5120	false
<input type="radio"/>	25	USMOB12	true	false	GW997	false
<input type="radio"/>	24	DMSC777TOUAE	true	false	GW625	false
<input type="radio"/>	23	RANDHOSP	true	true	GW120	false
<input type="radio"/>	21	45444457	true	false	GW457	false
<input type="radio"/>	54	460792457	true	false	GW457	false
<input type="radio"/>	20	MOBmob128	true	false	GW128	false
<input type="radio"/>	4	UAE3	true	false		false
<input type="radio"/>	1	Alfa1	true	false		false
<input type="radio"/>	12	KSAZAIN	true	false	GW128	false
<input type="radio"/>	40	IndiaBlock6	true	false		false
<input type="radio"/>	9	Qatar content	true	true		false
<input type="radio"/>	8	45444438	true	false	SMSCMob	false
<input type="radio"/>	36	IndiaBlock2	true	false		false
<input type="radio"/>	37	IndiaBlock3	true	false		false
<input type="radio"/>	38	IndiaBlock4	true	false		false
<input type="radio"/>	39	IndiaBlock5	true	false		false
<input type="radio"/>	41	IndiaBlock7	true	false		false
<input type="radio"/>	43	IndiaBlock9	true	false		false

Profile Name

UAE1

UAE2

UAE3

UAE4

UAE5

UAE6

UAE7

UAE8

UAE9

UAE10

UAE11

UAE12

UAE13

UAE14

UAE15

UAE16

UAE17

UAE18

UAE19

UAE20

UAE21

UAE22

UAE23

UAE24

UAE25

UAE26

UAE27

UAE28

UAE29

UAE30

UAE31

UAE32

UAE33

UAE34

UAE35

UAE36

UAE37

UAE38

UAE39

UAE40

UAE41

UAE42

UAE43

UAE44

UAE45

UAE46

UAE47

UAE48

UAE49

UAE50

UAE51

UAE52

UAE53

UAE54

UAE55

UAE56

UAE57

UAE58

UAE59

UAE60

UAE61

UAE62

UAE63

UAE64

UAE65

UAE66

UAE67

UAE68

UAE69

UAE70

UAE71

UAE72

UAE73

UAE74

UAE75

UAE76

UAE77

UAE78

UAE79

UAE80

UAE81

UAE82

UAE83

UAE84

UAE85

UAE86

UAE87

UAE88

UAE89

UAE90

UAE91

UAE92

UAE93

UAE94

UAE95

UAE96

UAE97

UAE98

UAE99

UAE100

UAE101

UAE102

UAE103

UAE104

UAE105

UAE106

UAE107

UAE108

UAE109

UAE110

UAE111

UAE112

UAE113

UAE114

UAE115

UAE116

UAE117

UAE118

UAE119

UAE120

UAE121

UAE122

UAE123

UAE124

UAE125

UAE126

UAE127

UAE128

UAE129

UAE130

UAE131

UAE132

UAE133

UAE134

UAE135

UAE136

UAE137

UAE138

UAE139

UAE140

UAE141

UAE142

UAE143

UAE144

UAE145

UAE146

UAE147

UAE148

UAE149

UAE150

UAE151

UAE152

UAE153

UAE154

UAE155

UAE156

UAE157

UAE158

UAE159

UAE160

UAE161

UAE162

UAE163

UAE164

UAE165

UAE166

UAE167

UAE168

UAE169

UAE170

UAE171

UAE172

UAE173

UAE174

UAE175

UAE176

UAE177

UAE178

UAE179

UAE180

UAE181

UAE182

UAE183

UAE184

UAE185

UAE186

UAE187

UAE188

UAE189

UAE190

UAE191

UAE192

UAE193

UAE194

UAE195

UAE196

UAE197

UAE198

UAE199

UAE200

UAE201

UAE202

UAE203

UAE204

UAE205

UAE206

UAE207

UAE208

UAE209

UAE210

UAE211

UAE212

UAE213

UAE214

UAE215

UAE216

UAE217

UAE218

UAE219

UAE220

UAE221

UAE222

UAE223

UAE224

UAE225

UAE226

UAE227

UAE228

UAE229

UAE230

UAE231

UAE232

UAE233

UAE234

UAE235

UAE236

UAE237

UAE238

UAE239

UAE240

UAE241

UAE242

UAE243

UAE244

UAE245

UAE246

UAE247

UAE248

UAE249

UAE250

UAE251

UAE252

UAE253

UAE254

UAE255

UAE256

UAE257

UAE258

UAE259

UAE260

UAE261

UAE262

UAE263

UAE264

UAE265

UAE266

UAE267

UAE268

UAE269

UAE270

UAE271

UAE272

UAE273

UAE274

UAE275

UAE276

UAE277

UAE278

UAE279

UAE280

UAE281

UAE282

UAE283

UAE284

UAE285

UAE286

UAE287

UAE288

UAE289

UAE290

UAE291

UAE292

UAE293

UAE294

UAE295

UAE296

UAE297

UAE298

UAE299

UAE300

UAE301

UAE302

UAE303

UAE304

UAE305

UAE306

UAE307

UAE308

UAE309

UAE310

UAE311

UAE312

UAE313

UAE314

UAE315

UAE316

UAE317

UAE318

UAE319

UAE320

UAE321

UAE322

UAE323

UAE324

UAE325

UAE326

UAE327

UAE328

UAE329

UAE330

UAE331

UAE332

UAE333

UAE334

UAE335

UAE336

UAE337

UAE338

UAE339

UAE340

UAE341

UAE342

UAE343

UAE344

UAE345

UAE346

UAE347

UAE348

UAE349

UAE350

UAE351

UAE352

UAE353

UAE354

UAE355

UAE356

UAE357

UAE358

UAE359

UAE360

UAE361

UAE362

UAE363

UAE364

UAE365

UAE366

UAE367

UAE368

UAE369

UAE370

UAE371

UAE372

UAE373

UAE374

UAE375

UAE376

UAE377

UAE378

UAE379

UAE380

UAE381

UAE382

UAE383

UAE384

UAE385

UAE386

UAE387

UAE388

UAE389

UAE390

UAE391

UAE392

UAE393

UAE394

UAE395

UAE396

UAE397

UAE398

UAE399

UAE400

UAE401

UAE402

UAE403

UAE404

UAE405

UAE406

UAE407

UAE408

UAE409

UAE410

UAE411

UAE412

UAE413

UAE414

UAE415

UAE416

UAE417

UAE418

UAE419

UAE420

UAE421

UAE422

UAE423

UAE424

UAE425

UAE426

UAE427

UAE428

UAE429

UAE430

UAE431

UAE432

UAE433

UAE434

UAE435

UAE436

UAE437

UAE438

UAE439

UAE440

UAE441

UAE442

UAE443

UAE444

UAE445

UAE446

UAE447

UAE448

UAE449

UAE450

UAE451

UAE452

UAE453

UAE454

UAE455

UAE456

UAE457

UAE458

UAE459

UAE460

UAE461

UAE462

UAE463

UAE464

UAE465

UAE466

UAE467

UAE468

UAE469

UAE470

UAE471

UAE472

UAE473

UAE474

UAE475

UAE476

UAE477

UAE478

UAE479

UAE480

UAE481

UAE482

UAE483

UAE484

UAE485

UAE486

UAE487

UAE488

UAE489

UAE490

UAE491

UAE492

UAE493

UAE494

UAE495

UAE496

UAE497

UAE498

UAE499

UAE500

UAE501

UAE502

UAE503

UAE504

UAE505

UAE506

UAE507

UAE508

UAE509

UAE510

UAE511

UAE512

UAE513

UAE514

UAE515

UAE516

UAE517

UAE518

UAE519

UAE520

UAE521

UAE522

UAE523

UAE524

UAE525

UAE526

UAE527

UAE528

UAE529

UAE530

UAE531

UAE532

UAE533

UAE534

UAE535

UAE536

UAE537

UAE538

UAE539

UAE540

UAE541

UAE542

UAE543

UAE544

UAE545

UAE546

UAE547

UAE548

UAE549

UAE550

UAE551

UAE552

UAE553

UAE554

UAE555

UAE556

UAE557

UAE558

UAE559

UAE560

UAE561

UAE562

UAE563

UAE564

UAE565

UAE566

UAE567

UAE568

UAE569

UAE570

UAE571

UAE572

UAE573

UAE574

UAE575

UAE576

UAE577

UAE578

UAE579

UAE580

UAE581

UAE582

UAE583

UAE584

UAE585

UAE586

UAE587

UAE588

UAE589

UAE590

UAE591

UAE592

UAE593

UAE594

UAE595

UAE596

UAE597

UAE598

UAE599

UAE600

UAE601

UAE602

UAE603

UAE604

UAE605

UAE606

UAE607

UAE608

UAE609

UAE610

UAE611

UAE612

UAE613

UAE614

UAE615

UAE616

UAE617

UAE618

UAE619

UAE620

UAE621

UAE622

UAE623

UAE624

UAE625

UAE626

UAE627

UAE628

UAE629

UAE630

UAE631

UAE632

UAE633

UAE634

UAE635

UAE636

UAE637

UAE638

UAE639

UAE640

UAE641

UAE642

UAE643

UAE644

UAE645

UAE646

UAE647

UAE648

UAE649

UAE650

UAE651

UAE652

UAE653

UAE654

UAE655

UAE656

UAE657

UAE658

UAE659

UAE660

UAE661

UAE662

UAE663

UAE664

UAE665

UAE666

UAE667

UAE668

UAE669

UAE670

UAE671

UAE672

UAE673

UAE674

UAE675

UAE676

UAE677

UAE678

UAE679

UAE680

UAE681

UAE682

UAE683

UAE684

UAE685

UAE686

UAE687

UAE688

UAE689

UAE690

UAE691

UAE692

UAE693

UAE694

UAE695

UAE696

UAE697

UAE698

UAE699

UAE700

UAE701

UAE702

UAE703

UAE704

UAE705

UAE706

UAE707

UAE708

UAE709

UAE710

UAE711

UAE712

UAE713

UAE714

UAE715

UAE716

UAE717

UAE718

UAE719

UAE720

UAE721

UAE722

UAE723

UAE724

UAE725

UAE726

UAE727

UAE728

UAE729

UAE730

UAE731

UAE732

UAE733

UAE734

UAE735

UAE736

UAE737

UAE738

UAE739

UAE740

UAE741

UAE742

UAE743

UAE744

UAE745

UAE746

UAE747

UAE748

UAE749

UAE750

UAE751

UAE752

UAE753

UAE754

UAE755

UAE756

UAE757

UAE758

UAE759

UAE760

UAE761

UAE762

UAE763

UAE764

UAE765

UAE766

UAE767

UAE768

UAE769

UAE770

UAE771

UAE772

UAE773

UAE774

UAE775

UAE776

UAE777

UAE778

UAE779

UAE780

UAE781

UAE782

UAE783

UAE784

UAE785

UAE786

UAE787

UAE788

UAE789

UAE790

UAE791

UAE792

UAE793

UAE794

UAE795

UAE796

UAE797

UAE798

UAE799

UAE800

UAE801

UAE802

UAE803

UAE804

UAE805

UAE806

UAE807

UAE808

UAE809

UAE810

UAE811

UAE812

UAE813

UAE814

UAE815

UAE816

UAE817

UAE818

UAE819

UAE820

UAE821

UAE822

UAE823

UAE824

UAE825

UAE826

UAE827

UAE828

UAE829

UAE830

UAE831

UAE832

UAE833

UAE834

UAE835

UAE836

UAE837

UAE838

UAE839

UAE840

UAE841

UAE842

UAE843

UAE844

UAE845

UAE846

UAE847

UAE848

UAE849

UAE850

UAE851

UAE852

UAE853

UAE854

UAE855

UAE856

UAE857

UAE858

UAE859

UAE860

UAE861

UAE862

UAE863

UAE864

UAE865

UAE866

UAE867

UAE868

UAE869

UAE870

UAE871

UAE872

UAE873

UAE874

UAE875

UAE876

UAE877

UAE878

UAE879

UAE880

UAE881

UAE882

UAE883

UAE884

UAE885

UAE886

UAE887

UAE888

UAE889

UAE890

UAE891

UAE892

UAE893

UAE894

UAE895

UAE896

UAE897

UAE898

UAE899

UAE900

UAE901

UAE902

UAE903

UAE904

UAE905

UAE906

UAE907

UAE908

UAE909

UAE910

UAE911

UAE912

UAE913

UAE914

UAE915

UAE916

UAE917

UAE918

UAE919

UAE920

UAE921

UAE922

UAE923

UAE924

UAE925

UAE926

UAE927

UAE928

UAE929

UAE930

UAE931

UAE932

UAE933

UAE934

UAE935

UAE936

UAE937

UAE938

UAE939

UAE940

UAE941

U

Network Implementation

SMS Firewall is deployed on-site in customer data centers. Bare-metal machines deployments are supported.

Network Integration

The integration of the SMS Firewall into the network involves establishing connectivity with the customer's Signaling Transfer Points (STPs) using SIGTRAN M3UA protocol.

The deployment of the firewall takes into consideration factors such as traffic volumes, link dimensioning, and redundancy requirements to determine the number and location of the message processor (MP) machines.

To ensure seamless integration, the firewall nodes are connected to dedicated M3UA links positioned behind the customer STPs. Since the firewall does not directly support interception of TDM links, any TDM connections originating from external sources and terminating at the customer STP are forwarded to the firewall through the SIGTRAN M3UA interface. This is accomplished by configuring the firewall as an M3UA endpoint and configuring the customer STPs to direct the traffic towards the firewall for analysis and policy enforcement. For a visual representation of this network integration, please refer to the architecture diagram.

Network architecture

The SMS Firewall architecture consists of two types of servers: the SS7 Signalling Server (SS) and the Message Processing Server (MP). It is recommended to deploy these servers on bare-metal hardware for optimal performance.

Within the network core, the Message Processors play a vital role and offer various functionalities, including:

1. Platform for network-based message transmission and reception.
2. SMS Firewall application for screening SMS messages.
3. SMS routing capabilities.
4. Web interface for system administration.
5. Threat assessment to identify and mitigate potential risks.
6. System monitoring to ensure the firewall's smooth operation.
7. Database and reporting functionalities to store and analyze SMS-related data.

All incoming messages from the SS7/SIGTRAN and/or SMPP network are relayed through the IP network to the message processing servers for further processing. The firewall intercepts all SMS-related MAP messages such as MO, SRI-SM, and MT at the access platform and forwards them to the Firewall Filter SMSC component on the message processing servers for screening.

The system's capacity and efficiency can be easily enhanced by adding more message processors as the system scales linearly. Additionally, the message processors establish communication with external sources to gather information. This includes connecting to a remote Phishing Threat Intelligence Provider Database used by the SMS Anti-Phishing module. The message processors interact with this remote location to verify the safety of links within SMS messages.

SMS Firewall Redundancy

The SMS Firewall incorporates various levels of redundancy to ensure system reliability and uninterrupted operation. These redundancy measures are implemented at both the hardware and software levels, as described below:

Hardware Level:

- Dual power supplies are utilized to provide backup power in case of a failure in one power supply unit.
- Dual network interface cards (NICs) are employed to maintain network connectivity even if one NIC encounters a malfunction.
- Dual Ethernet cables are used specifically for handling signaling traffic, ensuring redundancy in case of cable failure or disruption.
- Multiple HDDs are deployed in a RAID (Redundant Array of Independent Disks) configuration, which enhances -data redundancy and provides fault tolerance. This safeguards against data loss in the event of a single HDD failure.
- These hardware-level redundancies help mitigate the impact of potential hardware failures, ensuring uninterrupted operation and minimizing downtime for the SMS Firewall.

Traffic State

For more precise analysis, the Firewalls Report can be filtered by firewall and proxy connection.

Message Counts displays the number of messages received from and sent to the source and target proxy connections.

Origin and Final Destination Displays the SYSTEM, P95, and maximal message latencies. originating refers to the proxy connection's originating side. Destination refers to the endpoint of the proxy connection that will be accessed.

-Max latency indicates that all messages at that time were processed within the displayed value.

-The system latency indicates that 95% of communications were processed within the time period displayed.

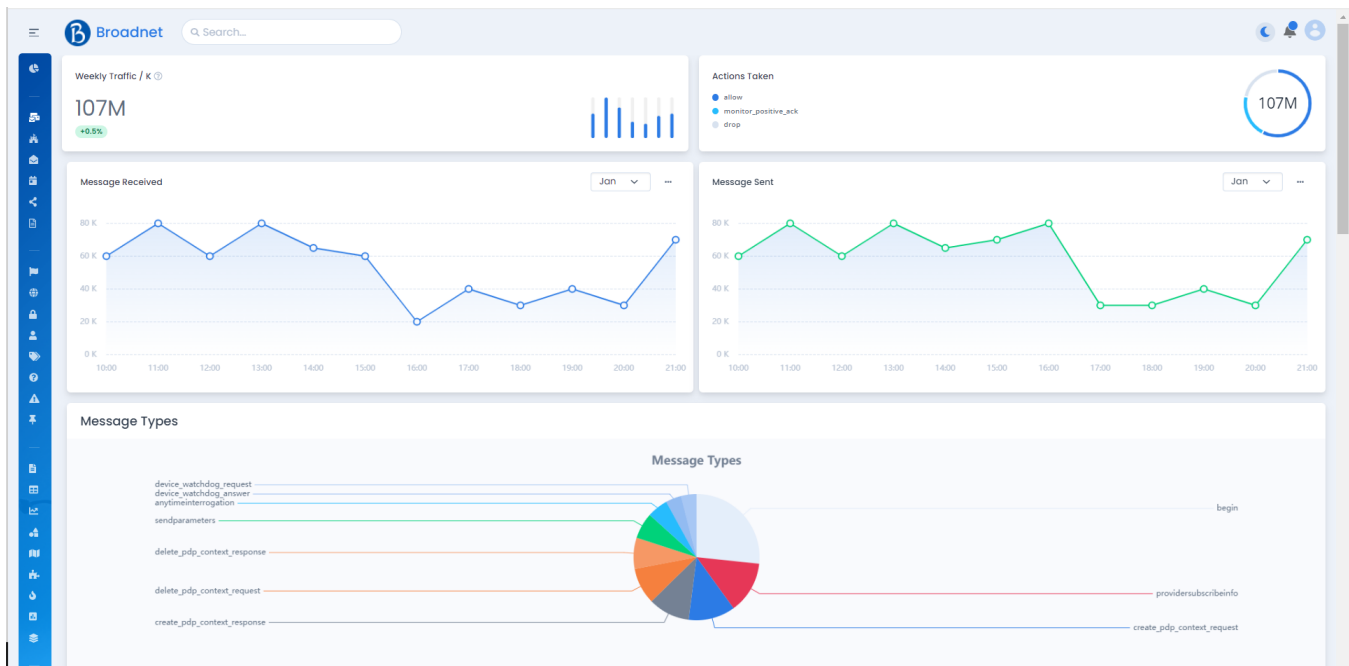
-The SYSTEM latency indicates that fifty percent of communications at that time were processed within the displayed time period.

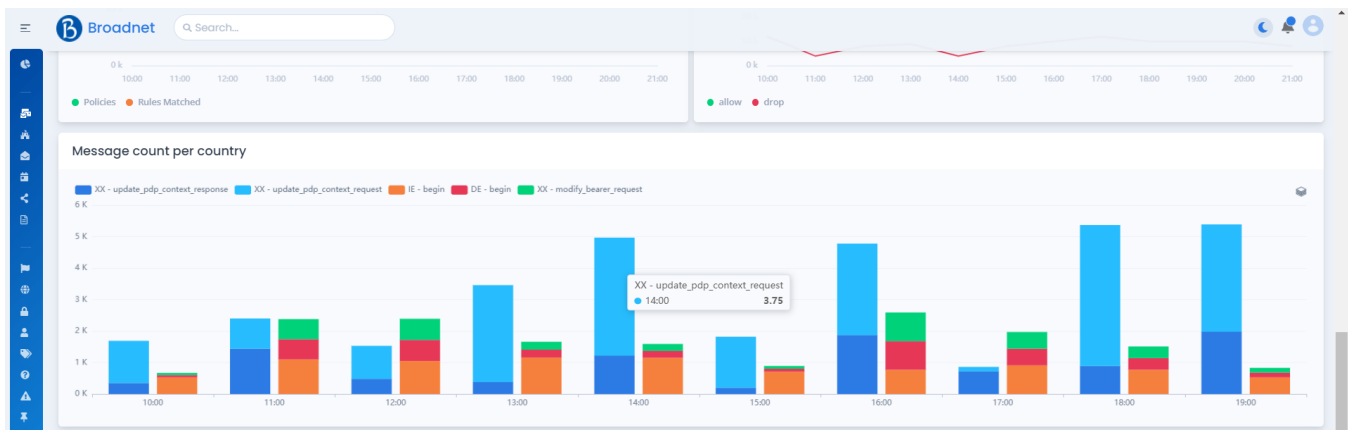
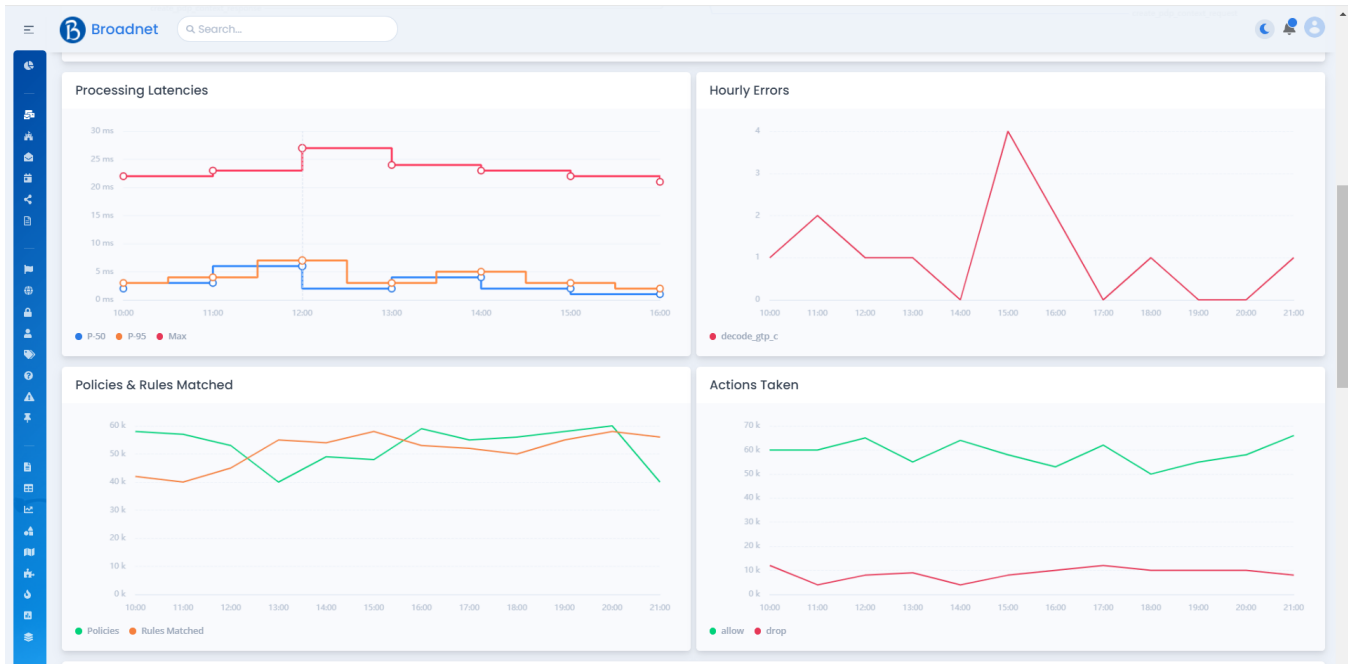
Description of Broadnet SMS Firewall Solution

Each message layer's decoding errors are graphed over time.

Message actions can also be graphed and segmented by firewall and proxy connection using filters.

A breakdown of the various communication types traversing the firewalls





Actions

Firewalls, policies, rules, and sources may all be used to narrow down the Actions Report. It provides a more granular investigation of how different policies affect the messages that go over proxy connections.

For the chosen time period, the total number of messages allowed and dropped is shown.

- Actions Both cumulative and cumulative percentage data are shown throughout time.

Policy, Rule, and Check message counts are also shown.

Firewalls, policies, rulesets, rules, actions, and external queries are just some of the filtering options available across all panels.

Backup & restore

The SMS Firewall employs a robust backup and restore mechanism to ensure the preservation of critical and essential database tables. This process is carried out at regular intervals of every 30 minutes. During the backup procedure, the relevant configuration files and tables are extracted from the database and securely stored in an encrypted format.

To enhance data security and resilience, the encrypted backups are stored either in dedicated storage infrastructure or on a separate server known as the cross server. By storing the backups in an encrypted state, the sensitive information within the database tables remains protected and inaccessible to unauthorized individuals.

The backup files serve as a reliable source for restoring the system in case of unforeseen events or data loss incidents. With these regular backups, the SMS Firewall can effectively recover and restore the database tables to their previous state, ensuring the continuity of operations and minimizing any potential disruption or loss of critical data.

Overall, this backup and restore process guarantees the integrity and availability of the essential tables within the SMS Firewall's database, providing a robust data protection mechanism to safeguard against data loss and enable efficient recovery when needed.

Capture Module

The Broadnet Firewall has a safe and efficient mechanism for capturing and storing all SMPP (Short Message Peer-to-Peer) packets. This one-of-a-kind function guarantees that all SMPP communication data is logged and archived in a specific database, where it can be easily retrieved and analyzed for further study at any time. With the Broadnet Firewall, enterprises may keep detailed records for compliance, troubleshooting, and performance assessment reasons. This state-of-the-art system captures and stores SMPP packets without disrupting network performance, allowing businesses to make educated choices and obtain insights about their SMS messaging infrastructure to enhance the efficiency of their communication channels.

Broadnet Search...

PCAP Files

Filter

Select Time Range: 2023-07-17 00:00:0 to 2023-07-17 11:59:0

Message ID:

Sender ID:

System ID:

Destination:

SMPP Commands: All

Bind Mode: All

Submit

Date	Message ID	Destination	Sender ID	Command	System ID	Bind	Download
2023-07-17 10:22:23	93aa0a33-9d49-446a	+12523358xx	Broadnet	submit_sm	User1	Transceiver	Download
2023-07-17 10:22:21	93aa0a33-9d49-8897	+25363322xx	Broadnet	deliver_sm	User1	Transceiver	Download
2023-07-17 10:20:12	N/A	N/A	N/A	enquire_link	User3	Transmitter	Download
2023-07-17 10:20:09	N/A	N/A	N/A	unbind	N/A	N/A	Download
2023-07-17 10:20:05	93aa0a33-9d49-1242	+92352125xx	Broadnet	submit_sm	User2	Transceiver	Download
2023-07-17 10:19:06	93aa0a33-9d49-1163	+12536958xx	Broadnet	submit_sm	User1	Transceiver	Download

< 1 2 3 >

Alert Module

The Alert Management System integrated into Broadnet SMS Firewall represents a powerful and comprehensive solution that ensures proactive monitoring of all SMPP bindings and SMS traffic flowing through the system. This sophisticated feature encompasses Dynamic Link Real-time (DLR) reporting, enabling real-time tracking of message delivery status and identifying any potential delays in message receipt. In the event of an issue, such as message delivery failure or latency, the Alert Management System promptly triggers alerts to relevant stakeholders, enabling swift and targeted responses to rectify the situation and maintain seamless communication.

Additionally, the Alert Management System extends its monitoring capabilities beyond SMS traffic to encompass hardware health monitoring. This vital aspect of the system continuously monitors the health and performance of the underlying hardware infrastructure. It detects potential hardware failures, anomalies, or capacity-related issues, ensuring that any impending problems are promptly detected and addressed before they can escalate into critical incidents.

By effectively monitoring SMPP bindings, SMS traffic with DLR reporting, and hardware health, the Alert Management System not only ensures optimal SMS delivery and performance but also enhances the overall reliability and stability of the Broadnet SMS Firewall. With timely and actionable alerts, the system administrators can proactively manage and maintain the SMS infrastructure, thereby fostering a secure and seamless messaging environment for users and businesses alike.

Robust Backup Module

The Backup Module in Broadnet SMS Firewall is a comprehensive and efficient solution designed to safeguard vital data and files required for swift recovery in the event of hardware failure or system corruption. The module's core functionality lies in automatically creating regular backups of essential files and databases, providing an added layer of security and peace of mind for both service providers and end-users.

Key Features and Benefits:

1. **Frequent Backup Intervals:** The Backup Module conducts periodic backups, typically every one hour, capturing any changes made during that time frame. This high-frequency approach ensures that the latest data is consistently protected and readily available for recovery.
2. **Customizable Backup Intervals:** Recognizing that different businesses may have varying data protection requirements, the Broadnet SMS Firewall offers the flexibility to adjust backup intervals to as frequent as every 30 minutes. This tailored approach empowers organizations to align data protection strategies with their specific needs and risk tolerance.
3. **Comprehensive Data Protection:** The Backup Module encompasses both databases and essential files needed for system restoration. It diligently copies SMS traffic records, configuration settings, user preferences, and other critical data to safeguard the SMS infrastructure's integrity.
4. **Seamless Restore Process:** In the unfortunate event of hardware damage or data loss, the Backup Module facilitates a smooth and rapid restore process. The system administrators can effortlessly access the backed-up data, initiate the restoration procedure, and bring the SMS infrastructure back to its fully operational state with minimal downtime.
5. **Redundant Storage:** The backed-up data is stored in redundant and secure locations, reducing the risk of single points of failure. Broadnet SMS Firewall's Backup Module employs advanced storage technologies to ensure data availability even during catastrophic events.
6. **Disaster Recovery Preparedness:** By adopting a proactive approach to data backup and restoration, Broadnet SMS Firewall empowers organizations to be well-prepared for any unforeseen hardware disruptions. This readiness significantly enhances business continuity and customer satisfaction.
7. **Compliance and Legal Requirements:** In sectors where compliance and data retention regulations are stringent, the Backup Module plays a crucial role in meeting the necessary requirements. Organizations can confidently demonstrate their commitment to data security and integrity to regulatory bodies and stakeholders.

Data Retention and Deletion:

At Broadnet, we have well-defined policies and procedures for data retention and deletion concerning our SMSC and firewall systems.

We retain user data and message logs for the required duration, and when data is no longer needed, we securely delete it in accordance with legal and regulatory requirements.

Vulnerability Management:

Broadnet is committed to maintaining a secure SMS Firewall system. We proactively identify and address vulnerabilities through regular security assessments and penetration testing. Our team promptly handles any identified vulnerabilities to ensure the utmost security for our services.

Employee Training and Awareness:

At Broadnet, we understand the critical role of our employees in ensuring security. We conduct comprehensive training programs and awareness initiatives for our staff with access to the SMSC Firewall system. Our employees are well-informed about security best practices, data handling, and compliance requirements.

Third-Party Audits and Certifications:

Broadnet values the trust our customers and partners place in us. To validate the effectiveness of our security measures, we undergo third-party audits and hold relevant security certifications.

These audits and certifications contribute to building trust and confidence in our SMS Firewall and SMSC systems.

Disaster Recovery and Business Continuity Plan:

Ensuring uninterrupted SMS Firewall services is of utmost importance at Broadnet. We have a comprehensive disaster recovery and business continuity plan in place. This plan includes data backup procedures, system redundancy measures, and continuity strategies to address unforeseen circumstances effectively.

Social Engineering and Phishing Mitigation:

At Broadnet, we take proactive measures to prevent social engineering attacks and phishing attempts on our SMS Firewall system.

We implement a combination of employee training, security awareness initiatives, and technical controls to safeguard against these threats.

Incident Response Plan:

Broadnet has a well-defined incident response plan for our Firewall SMS services.

We have established a step-by-step process for identifying, managing, and resolving security incidents. Our incident response team is highly trained and equipped to handle any security-related events promptly.

External Communication:

Transparent and timely Broadnet. In the event of security our Firewall and SMSC services, we maintain open channels of customers, partners, and regulatory stakeholders are informed



communication is a priority at incidents or breaches related to

communication with our authorities to ensure all appropriately.

Risk Assessment:

Broadnet conducts thorough risk assessments on our Firewall SMSC system. We identify potential security risks, assess their impact and likelihood, and prioritize risk mitigation efforts to enhance the security and transparency of our services.

Industry Compliance:

At Broadnet, we strictly adhere to industry compliance standards and guidelines relevant to our SMS services.

Our commitment to compliance ensures that we meet all regulatory requirements, providing our customers with reliable and compliant A2P SMS solutions.

Non-Disclosure Agreements (NDAs):

Broadnet recognizes the significance of safeguarding sensitive information.

We use Non-Disclosure Agreements (NDAs) with our employees and third-party partners to ensure confidentiality and protect proprietary data.

Our NDAs underscore our commitment to maintaining the privacy and security of all parties involved.

Thank You For Your
Attention