NewNet Mobile Messaging SMS Firewall

User Guide

Revision A

October 2018

Table of Contents

List of Figures

Chapter 1

Introduction

Topics:

1.1 About this Document

This document describes the NewNet Mobile Messaging firewalling solution, which consists of the:

- Firewall (FWL) feature of the Router (RTR) component
- Firewall Advanced Filters (FAF) component

This document describes the configuration and operation of the FWL and the configuration of the FAF. Before reading this document, you should be familiar with SS7 message routing basics, the RTR's rule evaluation mechanisms, and the Mobile Messaging semi-static and dynamic configuration concepts.

The FWL, RTR, and FAF are part of the NewNet Mobile Messaging family of SS7 message routing and network querying products.

Because some functionalities are licensed and depend on your specific implementation, this document may describe functions and/or features that are not relevant to the system that you are working with.

1.2 Scope

This document describes the functionality of the NewNet Mobile Messaging FWL component and describes how the FAF component can be used to accomplish advanced message filtering and firewalling.

This document does not provide detailed information about the operation or configuration of the FAF software. For information about the FAF software, refer to the FAF Operator Manual.

1.3 Intended Audience

This document is mainly intended for:

- Implementation engineers who are responsible for the planning, on-site installation, and configuration of the FWL and/or FAF in the operator environment
- Maintenance and support engineers who are responsible for maintaining the environment of which the FWL and/or FAF is a part
- Network operators who are in charge of the daily operation of NewNet Mobile Messaging systems and infrastructure

1.4 Documentation Conventions

Typeface or Symbol	Meaning	Example
Bold	Refers to part of a graphical user interface.	Click **Cancel**.

Typeface or Symbol	Meaning	Example
`Courier`	Refers to a directory name, file name, command, or output.	The `billing` directory contains...
`<pointed brackets>`	Serves as a placeholder for text that the user will replace, as appropriate in context.	The file is called `MGRdata.xml.<ip>.gz`, where `<ip>` is the server's IP address.
`[square brackets]`	Indicates an optional command.	`[--validateonly]`
Note:	Indicates information alongside normal text, requiring extra attention.	**Note:** Ensure that the configuration...
\ (Unix)	Denotes line continuation; the character should be ignored as the user types the example, and ENTER should only be pressed after the last line.	`% grep searchkey \` `data/*.dat`

1.5 Locate Product Documentation on the Customer Support Site

Access to NewNet's Customer Support site is restricted to current NewNet customers only. This section describes how to log into the NewNet Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the NewNet Customer Support site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

Overview

Topics:

2.1 Introduction

Unsolicited messages (spam) and falsified originator information (spoofing) present operators with many issues:

- Higher network capacity requirements
- Reduced customer service for subscribers
- Threatened revenue from outbound-roaming subscribers
- Increased instances of billing fraud
- Damaged image and brand
- Reduced interconnect capacity and increased interconnect disputes

The NewNet Mobile Messaging Firewall (FWL) is a feature within the Router (RTR) component that uses patented techniques to detect unsolicited messages and messages containing false originator information, and to prevent these messages from affecting subscribers. The FWL can:

- Screen incoming messages from the home network and from foreign networks
- Provide statistical information about traffic originating outside the home network
- Protect subscribers from receiving unwanted messages
- Protect subscribers from fraudulent charges resulting from false originator information
- Prevent incorrect termination fees from other operators

This figure illustrates the position of the FWL in relation to other parts of the network.

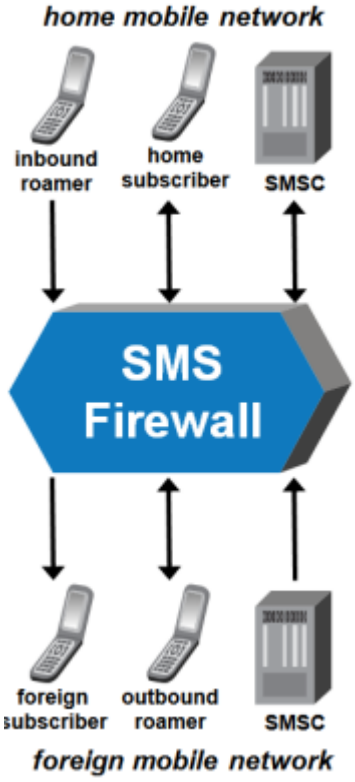


Figure 1: FWL in the network

2.2 Terminology

Before you use the FWL, it is important to understand the terminology that is commonly used when discussing SMS firewalling.

Term	Description
Destination point code (DPC)	Unique address of the destination signaling node
Foreign subscriber	A subscriber of a network other than the operator's home network
General Packet Radio Service (GPRS)	Packet-oriented mobile data service on GSM
Global System for Mobile Communications (GSM)	Popular standard for mobile telephony systems
Global title (GT)	Address used in the SCCP protocol for routing signaling messages
Home Location Register (HLR)	Database that contains information about the subscribers who are authorized to use the GSM core network
Home Public Land Mobile Network (HPLMN)	An operator's home network
Home Routing	A feature that allows an operator to route MT messages to outbound-roaming subscribers through the operator's own network
Home subscriber	A subscriber of the operator's home network
Inbound roamer	A subscriber of a foreign network, who is roaming in the operator's home network (that is, receiving service from the operator's home network)
Message Transfer Part (MTP)	Part of the SS7 protocol that is responsible for the transport of SS7 messages between communication partners
Mobile Application Part (MAP)	SS7 protocol that is used for MO and MT traffic in the core network
Mobile Application Part (MAP) Screening	A feature that enables an STP operator to set up routing based on the MAP operation type
Mobile-originating (MO) traffic	Traffic that is originated by a mobile communication subscriber who is using a mobile station (MS)
Mobile Switching Center (MSC)	The primary service delivery node for GSM networks
Mobile-terminating (MT) traffic	Traffic that reaches an MS and is accepted by it (such as calls and short messages)
MoForwardSm	MAP operation that an MSC uses to send an MO message to an SMSC
MO anti-spoofing	A feature that enables the FWL to detect and handle MO messages with spoofed originator information

Term	Description
MT anti-spoofing	A feature that enables the FWL to detect and handle MT messages with spoofed originating network information
MtForwardSm	MAP operation that an SMSC uses to send an MT message to an MSC
Off-net	Network elements that are outside the mobile operator's own network
On-net	Network elements that are within the mobile operator's own network (HPLMN)
Originating point code (OPC)	Unique address of the originating signaling node
Outbound roamer	A subscriber of the home network, who is roaming in a foreign network (that is, receiving service from a foreign network)
Point code (PC)	Unique address for a signaling node
Public Land Mobile Network (PLMN)	Generic term for a wireless network
Republishing	When, instead of relaying an SRI-SM response to an SMSC, the FWL reissues the original SRI-SM with the original SCCP addresses so the FWL is no longer involved
Routing Indicator (RI)	Indicates how an SCCP message should be routed (using global title or using point code/subsystem number)
SendRoutingInfoForSm (SRI-SM)	MAP operation that systems (such as an SMSC) use to request subscriber data from an HLR
Service center address	Address of the service center that will handle SMS; this is called the "common address" of the RTR
Serving GPRS Support Node (SGSN)	Part of the GPRS core network that is responsible for the delivery of data packets from and to the mobile stations within its geographical service area
Short message service center (SMSC)	Network element that provides the store-and-forward function for short messages
Short message entity (SME)	Any entity that can send and/or receive short messages
Spamming	The act of sending unsolicited and unwanted SMS messages to subscribers
Spoofing	The act of one short message entity (SME) impersonating another SME
Spoof check	General term for the actions that the FWL takes to determine whether the originator of a message is spoofed
SS7	The Signaling System No. 7 telephony protocol
Signal Transfer Point (STP)	Router that relays SS7 messages between signaling end-points (SEPs) and other STPs

Term	Description
Signaling Connection Control Part (SCCP)	Part of the SS7 protocol that provides extended routing, segmentation, and connection functions
Subsystem number (SSN)	Identifies an application within a network entity that uses SCCP signaling
Suspect messages	Messages that originate from non-trusted sources or sources that could have been spoofed
Transaction Capabilities Application Part (TCAP)	An SS7 protocol that facilitates multiple concurrent dialogs between the same subsystems on the same machines
Termination fees	Fees that a mobile operator pays to other mobile operators to compensate them for delivering messages to the originating operator's outbound-roaming subscribers
Trusted messages	Messages that originate from trusted sources that cannot be spoofed
Visitor Location Register (VLR)	Database that stores information about the mobile devices that are currently under the jurisdiction of the MSC that the VLR serves
Virtual point code (VPC)	A non-physical point code

2.3 Usage Scenarios

There are many scenarios in which the FWL can be used to combat fraud and to prevent unsolicited messages from reaching subscribers.

1. **Scenario: Subscribers are being billed for messages that they did not send.**

   This type of erroneous charging may be caused by mobile-originated (MO) spoofing, which is when a message originator impersonates a subscriber to avoid message charges. The FWL's anti-spoofing functionality can identify and block messages with spoofed originator information, which ensures that the subscribers being spoofed are not charged for the messages. Refer to *Figure 3: MO spoofing* for an illustration.

2. **Scenario: Network B registered more messages sent from Network C than Network C actually sent.**

   A network component in Network A can originate mobile-terminated (MT) traffic to network B while impersonating Network C. When Network B and Network C attempt to reconcile their SMS interconnect bill, they will find that Network C sent less messages than what was registered in Network B. These messages actually originated from network A, which will not be invoiced for the relevant messages. This is known as MT spoofing. Refer to *Figure 4: MT spoofing* for an illustration.

3. **Scenario: Subscribers are receiving unsolicited messages, such as advertisements, chain-mail messages, false emergency alerts, and other unwanted and disruptive messages.**

   Unsolicited messages, also called spam, can originate from SMS applications, national interconnect networks, international interconnect networks, or home-network subscribers. Spam negatively affects customer satisfaction and lower the level of trust associated with SMS as a communication medium.

4. **Scenario: Viruses on mobile devices (such as smartphones) are sending unsolicited messages without subscribers' knowledge.**

   While the FWL cannot determine whether a message was sent intentionally, it can, in combination with the Firewall Advanced Filters (FAF) component, block messages based on attributes such as submit time, frequency, and text patterns in the message content. It can also send an SMS to the subscriber to notify him or her of the issue and what actions to take, particularly if it is a known handset virus.

2.3.1 SMS Spam

SMS spam is any type of unsolicited, unwanted message. Typical spam content includes advertisements, invitations to premium services or contests, misleading or false emergency information, and other types of content that are generally intended to illicit a response from the receiver.

SMS spam does the most damage when it affects a large number of subscribers of one network in a country. These large-scale spam attacks, during which unsolicited messages are sent to thousands of subscribers, are usually highlighted by the national media, reflecting negatively on the operator's image. The handling of subscriber complaints usually requires significant administrative resources, increasing operational costs.

Although there are many entry points in the HPLMN that potentially allow unsolicited, unwanted messages, operators typically focus on preventing spam from the international SS7 network, because it is the most difficult to control and eliminate.

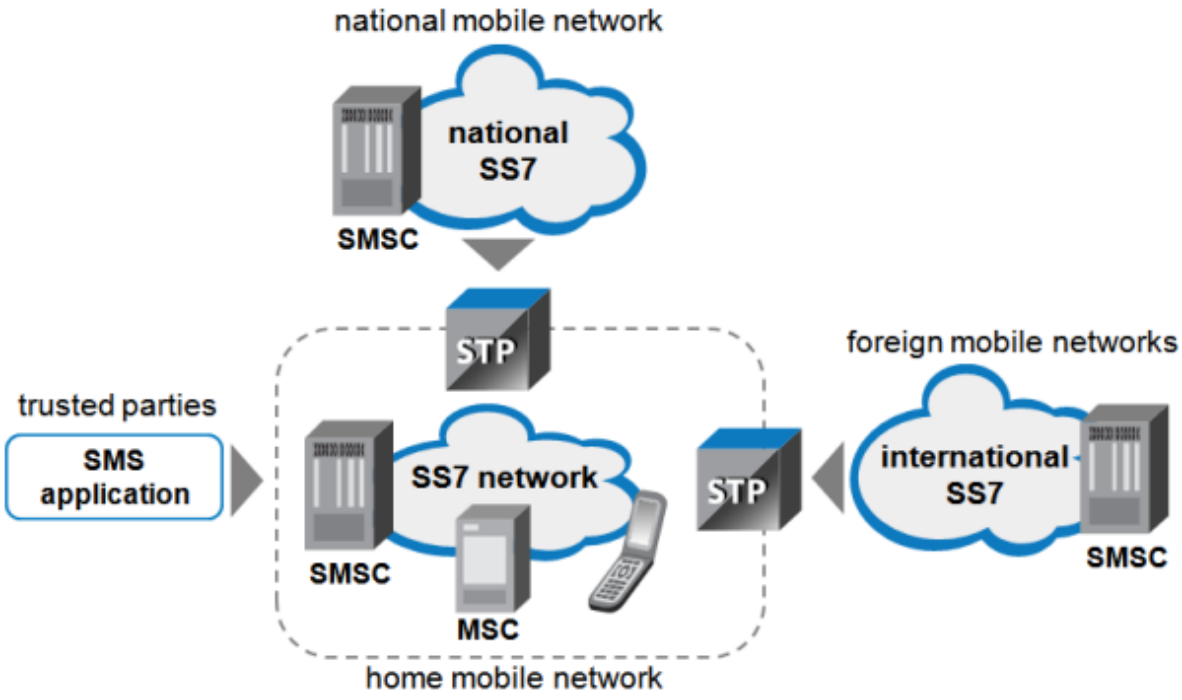


Figure 2: Potential spam entry points

2.3.2 SMS Spoofing

SMS spoofing is generally done by replacing the SCCP addresses with forged addresses, usually real addresses of different networks. In many cases, SMS spoofing techniques are applied to spam messages to attempt to avoid termination fees and circumvent basic originating network-based traffic blockades. Spoofed messages are harmful and undesired.

The FWL can be configured to detect SMS spoofing in incoming MO and incoming MT messages.

2.3.2.1 MO Spoofing

In the case of MO spoofing, the originator address of an MO message does not reflect the actual sender of the message. The sender impersonates the subscriber who is identified by the originator address, which causes the recipient to see the impersonated (spoofed) subscriber as the message originator. This usually results in the impersonated subscriber being charged for the message.

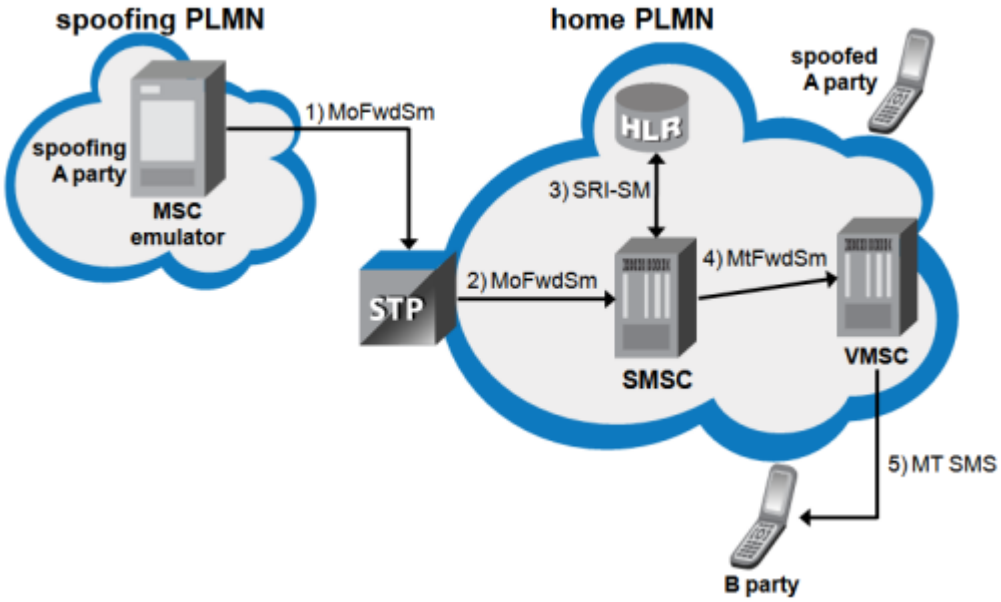


Figure 3: MO spoofing

2.3.2.2 MO Entry Points and Risks

These are the points at which MO messages originate and the spoofing risk profile associated with various origin/destination combinations.

Originating Network	Originating Subscriber	Destination SMSC	Risk Profile
HPLMN	Home subscriber	HPLMN	Low risk, low probability (origin is controlled by the operator)
HPLMN	Foreign subscriber (inbound roamer)	Foreign network (national or international)	Low risk, low probability (origin is controlled by the operator)

Originating Network	Originating Subscriber	Destination SMSC	Risk Profile
Foreign network (national or international)	Home subscriber (outbound roamer)	HPLMN	High risk, medium probability (operator cannot control the origin and subscriber is roaming in a foreign network)

The tracing and blocking mechanisms for MO messages that originate in foreign networks are limited when compared to the mechanisms for messages that originate in the HPLMN.

2.3.2.3 MT Spoofing

In the case of MT spoofing (also called "faking"), the SMSC address of an MT message does not reflect the actual originating network of the message. The spoofer impersonates another network, which causes the terminating network to charge the impersonated (spoofed) network for terminating fees. The MAP address, SCCP address, or both can be spoofed.

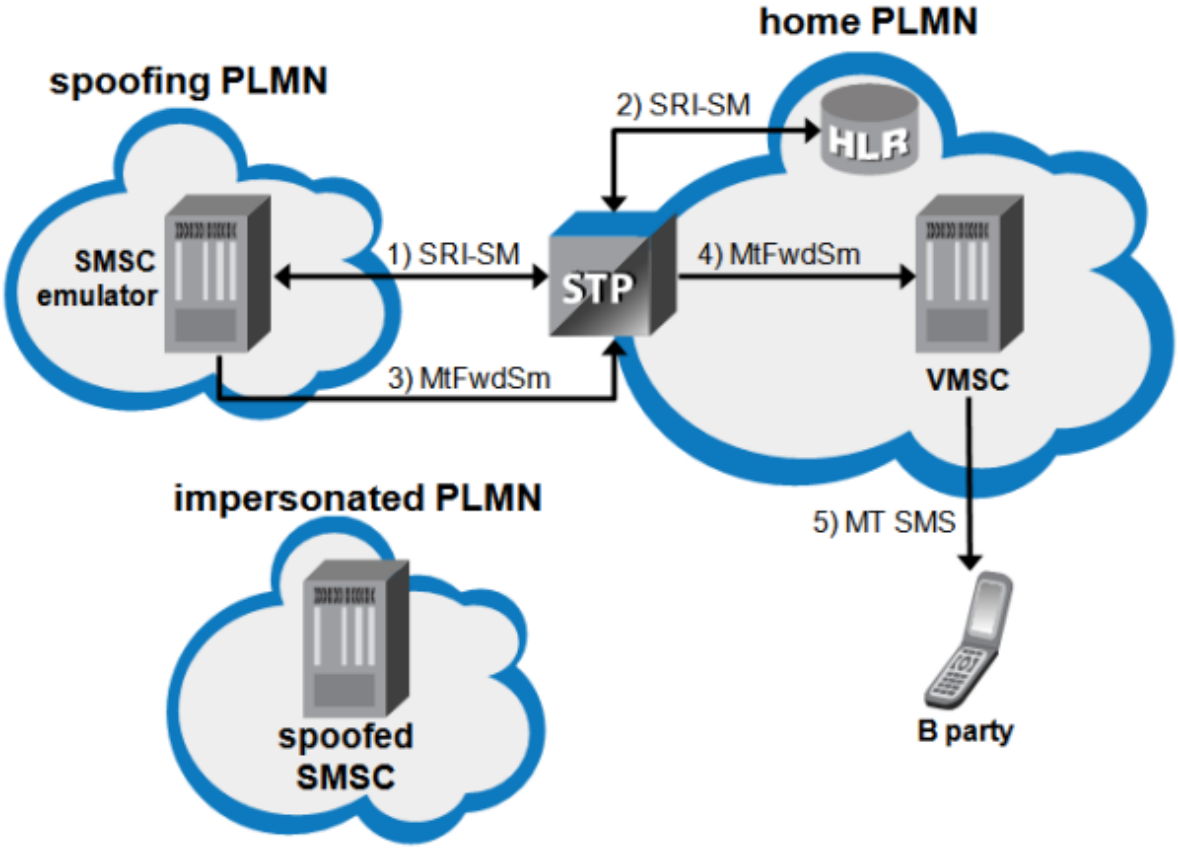


Figure 4: MT spoofing

2.3.2.4 MT Entry Points and Risks

These are the points at which MT messages originate and the spoofing risk profile associated with various origin/destination combinations.

Originating SMSC	Destination Subscriber	Terminating Network	Risk Profile
HPLMN	Home subscriber	HPLMN	Low risk, low probability (origin is controlled by the operator)
HPLMN	Foreign subscriber (inbound roamer)	HPLMN	Low risk, low probability (origin is controlled by the operator)
HPLMN	Home subscriber (outbound roamer)	Foreign network (national or international)	Low risk, low probability (origin is controlled by the operator)
HPLMN	Foreign subscriber	Foreign network (national or international)	Low risk, low probability (origin is controlled by the operator)
Foreign SMSC (national or international)	Home subscriber	HPLMN	Medium risk, high probability (origin cannot be controlled by the operator)
Foreign SMSC (national or international)	Home subscriber (outbound roamer)	Foreign network (national or international)	High risk, high probability (origin cannot be controlled by the operator and subscriber is roaming in a foreign network)

2.3.2.5 Indicators of MT Spoofing

There are scenarios in which your SMSCs may be spoofed: the MAP address may be spoofed, or the MAP address and the SCCP address may be spoofed.

If the MAP address is being spoofed, the SCCP and MAP addresses in the MtForwardSm operation will differ. In this scenario, the spoofing party is easily identified by the SCCP calling party address (CGPA) global title (GT).

A combination of MAP and SCCP address spoofing can be harder to detect. In this scenario, the MtForwardSm operation will appear to be valid. However, your SMSC will received a TCAP End operation without a corresponding TCAP Begin (an unsolicted, or unexpected, TCAP End). Normally, such operations are ignored. However, they are a strong indicator of MT spoofing.

This figure illustrates these MT spoofing scenarios.

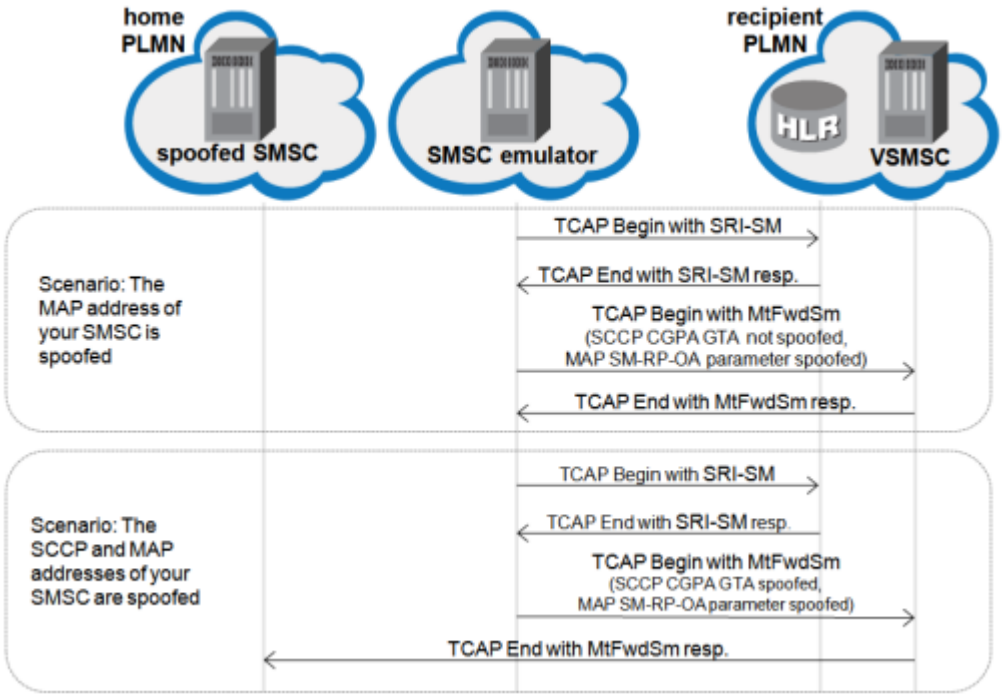


Figure 5: MT spoofing scenarios

2.3.3 Grey Routing of SMS

"Grey routing" of SMS refers to a situation in which an operator chooses to route messages that are originated from its own subscribers and destined for a partner operator's subscribers indirectly, i.e. via a third operator's network, instead of directly sending such messages to the destination network. This is done in order to avoid paying message termination charges, since the originating operator in this case would already be having interconnect agreements with its partner, i.e. the recipient operator. But if instead of routing the messages directly they are actually routed through the network of a third operator who does not have agreements with the recipient operator, then the originating operator would no longer have to pay any charges for the messages while there would be a substantial loss of revenue for the recipient operator.

Note that in the case of grey routing the message is always originated from a foreign subscriber and is routed via another foreign operator's SMSC. Hence the recipient operator can never control the origin or the routing point of a grey routed message; it can only try to detect such instances by comparing the network and country of the originator address (TP-OA) and the MAP layer SMSC address (SM-RP-OA) of an MtForwardSm. This is distinct from the MT spoofing or "faking" scenario described in the previous section.

Chapter 3

Firewalling MO Traffic

Topics:

3.1 Introduction

MO messages are always MAP messages originating from an MSC/SGSN and directed to an SMSC. This figure illustrates normal MO routing **without** the FWL.

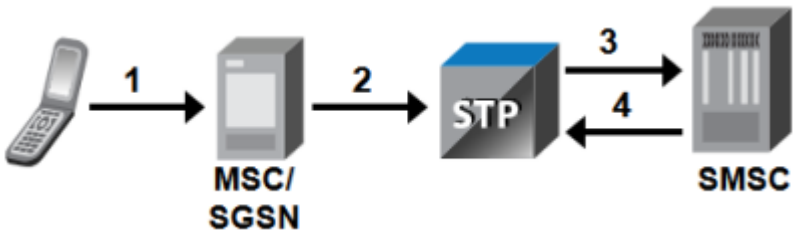


Figure 6: MO routing before FWL deployment

In this configuration:

1. The mobile submits the MO message to the HPLMN SMSC (destination service centre address).
2. The MSC/SGSN routes the message to the SMSC (MoForwardSm operation), normally via the STP (although it can be done without the STP). At this point, the originating global title (GT) is the MSC/SGSN and the destination GT is the SMSC.
3. The STP routes the message from the MSC/SGSN to the destination SMSC.
4. The SMSC acknowledges the MoForwardSm operation with an ACK.

In this configuration, MO spoofing cannot be detected.

This figure illustrates normal MO routing **with** the FWL:

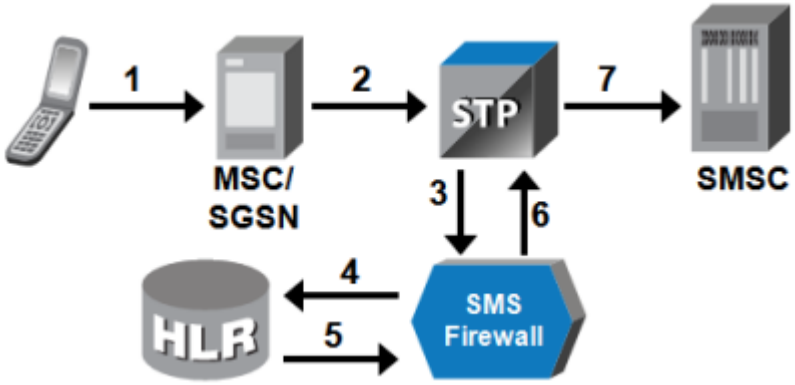


Figure 7: MO routing after FWL deployment

In this configuration:

1. The mobile submits the MO message (MoForwardSm operation) to the HPLMN SMSC (destination service centre address).
2. The MSC/SGSN routes the message to the SMSC (MoForwardSm operation), normally via the STP (although it can be done without the STP). At this point, the originating GT is the MSC/SGSN and the destination GT is the SMSC.
3. Based on the service centre address, the STP routes the MoForwardSm operation to the FWL (by default, no specific STP configuration is required).

Depending on the SS7 network and SMSC capabilities, MAP screening and/or translation types (TTs) may be required.

4. If the message is suspect, the FWL performs an MO spoofing check, which consists of an HLR query to the HPLMN.

   Messages are normally suspect, but it is possible to route an MO message from the HPLMN toward the FWL without an MO spoofing check.

5. Depending on the FWL configuration, the message is forwarded to the SMSC.
6. The SMSC acknowledges the MoForwardSm operation with an ACK to the FWL.
7. The FWL acknowledges the MoForwardSm operation with an ACK to the MSC/SGSN.

Note: When the FWL forwards the MoForwardSm to the SMSC, it changes the originating MSC/SGSN address to the FWL's GT. If this will impact billing (which is often the case), TTs must be used to preserve the originating MSC/SGSN address when forwarding the MoForwardSm.

3.2 Identifying Suspect MO Traffic

To determine whether an MO message is spoofed, the FWL compares the mobile's location (the originating MSC/SGSN address to the location that is indicated by the HLR (the serving MSC/SGSN address). The FWL considers an MO message to be spoofed when the first N digits of the originating MSC/SGSN in the MoForwardSm do not match the serving MSC/SGSN, where N is configurable (refer to *Set the Digits Considered for MO Spoofing*). The complete MSC/SGSN address is not used to allow for multi-address MSCs/SGSNs.

Some MSCs/SGSNs may include the IMSI in the MoForwardSm (MAP phase 2+ only); in this case, the FWL also compares the originator IMSI to the IMSI that is returned by the HLR. If the IMSIs do not exactly match, the FWL considers the MO message to be spoofed.

Therefore, the FWL must execute an HLR query for each MO message that it must check for spoofing. To avoid an excess of HLR queries, most operators prefer to deploy the FWL that originates from suspect sources.

In this type of FWL deployment, all MO messages from trusted MSCs/SGSNs are routed to the SMSC. MO messages from suspect MSCs/SGSNs flow through the FWL and are checked for spoofing, at which point they can be blocked, if necessary.

This diagram illustrates the preferred deployment.

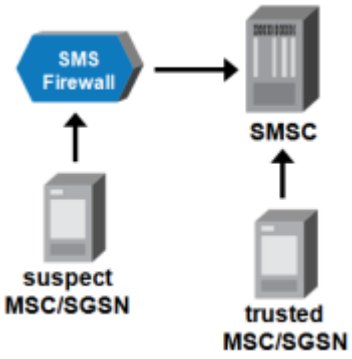


Figure 8: Preferred FWL deployment for MO spoofing checks

The FWL enables you to limit the overall number of MO spoofing checks that the FWL will perform each second. This can prevent the denial of HLR services during a spam attack. For information about configuring this feature, refer to *Limit the Number of MO Spoofing Checks*.

3.2.1 PC/SSN Routing versus GT Routing

An MSC/SGSN can use one of two types of SCCP routing to send signaling messages to the FWL:

Type of Routing	Applicable MSC	Description
Point code/subsystem number (PC/SSN) routing	On-net only	Only network elements within the same GSM network can use PC/SSN routing to address the FWL.
Global title (GT) routing	On-net or off-net	A network element can use GT routing to address any other element within the same GSM network or in a different GSM network.

Most networks use GT routing only, with the MSC/SGSN handling traffic from the HPLMN and from inbound roamers (roaming subscribers of other networks).

3.2.2 Point Code Comparison

The FWL determines whether a message's origin is suspect or trusted based on the originating point code (OPC) of a signaling message. If the OPC:

- Is equal to the STP's PC, then the message is suspect
- Is not equal to the STP's PC, then the message is trusted

This diagram shows the flow of a signaling message from a trusted MSC/SGSN to the FWL using PC/SSN routing. The destination point code (DPC) is the virtual point code (VPC) of the FWL.

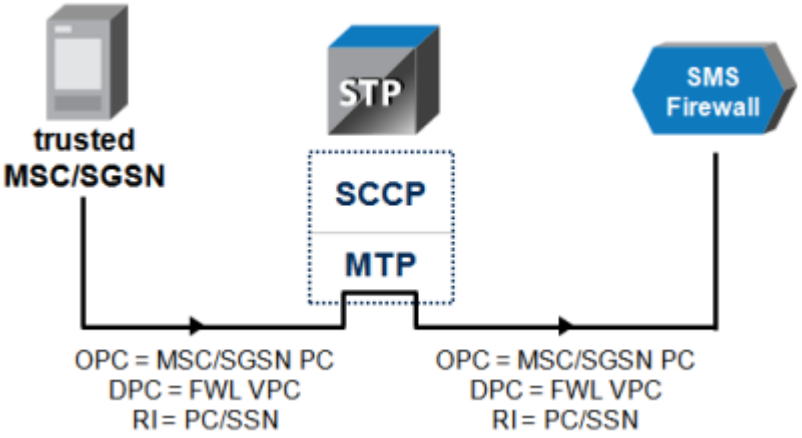


Figure 9: Trusted MSC/SGSN using PC/SSN routing

This diagram shows the flow of a signaling message from a suspect MSC/SGSN to the FWL using GT routing. Between the STP and the FWL, the routing indicator (RI) is normally set to GT.

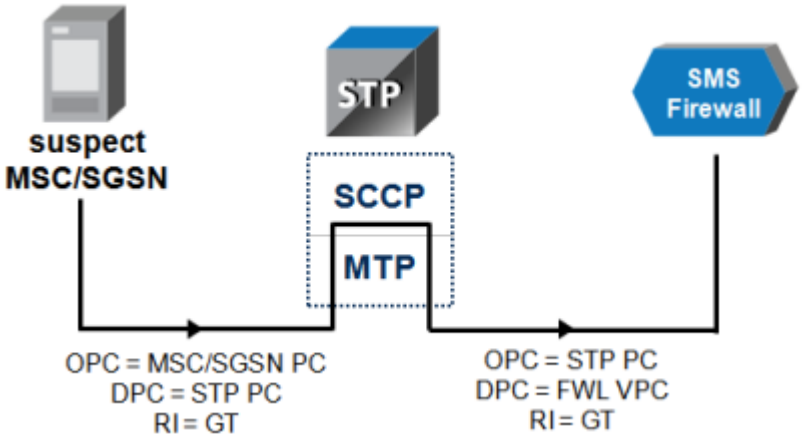


Figure 10: Suspect MSC/SGSN using GT routing

The SCCP calling party address (CGPA) contains the GT of the MSC/SGSN (even in the case of PC/SSN routing), and does not change. It must remain in a form that enables the network to route subsequent response messages back to the MSC/SGSN.

In the case of GT routing, when the message is sent from the MSC/SGSN to the STP, the SCCP called party address (CDPA) contains a GT. The STP may leave the GT unmodified, remove it, or replace it with a PC. In the case of PC/SSN routing, the CDPA only requires the SSN; the GT and PC are optional.

3.2.3 Controlling When the FWL Performs MO Spoofing Checks

The `tpconfig` attribute `firewallmospoofingcheckcondition` in the semi-static configuration file determines when the FWL will perform an MO spoofing check. Possible values are:

- always—The FWL will always perform an MO spoofing check. This is the default and most commonly used setting.
- whenmscsgsnaddressingsmscongt—The FWL will only perform an MO spoofing check when the MSC or SGSN addresses the SMSC using GT routing. This enables you to restrict MO spoofing checks to MO messages with suspect origins. It requires that all MSCs and SGSNs within your network have a GTT rule for the public SMSC address.
- never—The FWL will never perform an MO spoofing check.

3.3 Detecting MO Spoofing

In the MoForwardSm operation, the SCCP calling address (CGPA) contains a representation of the originator's MSC/SGSN address in the CGPA's global title (GT). The MoForwardSm operation may also contain the IMSI of the MO message originator.

To determine whether an MO message is spoofed, the FWL compares the mobile's location (the originating MSC/SGSN address) to the location that is indicated by the HLR (the serving MSC/SGSN address). To obtain the serving MSC/SGSN address, the FWL queries the HLR using the SendRoutingInfoForSm (SRI-SM) operation. This figure illustrates the process.

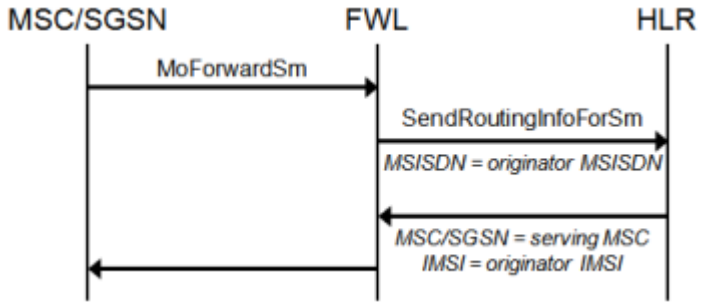


Figure 11: Checking an MO message for spoofing

The FWL considers an MO message to be spoofed when the first N digits of the originating MSC/SGSN in the MoForwardSm do not match the serving MSC/SGSN, where N is configurable (refer to *Set the Digits Considered for MO Spoofing*). The complete MSC/SGSN address is not used to allow for multi-address MSCs/SGSNs.

Some MSCs/SGSNs may include the IMSI in the MoForwardSm (MAP phase 2+ only); in this case, the FWL also compares the originator IMSI to the IMSI that is returned by the HLR. If the IMSIs do not exactly match, the FWL considers the MO message to be spoofed.

This figure illustrates the MO spoofing detecting process.

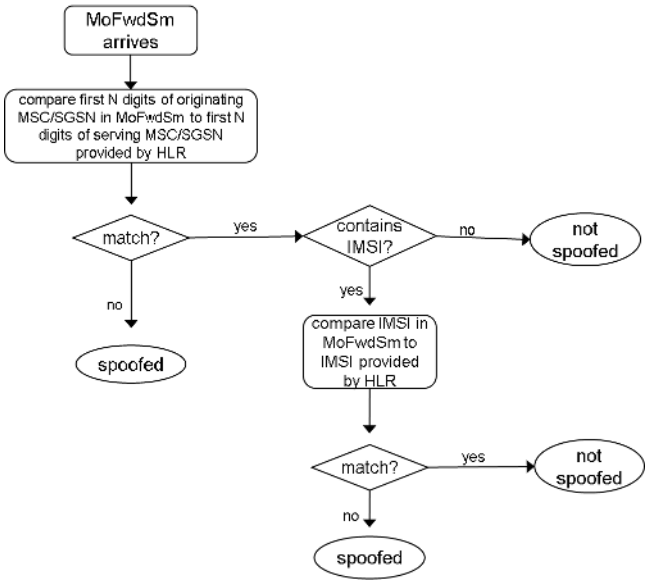


Figure 12: Detecting MO spoofing

3.3.1 MO Spoofing Example

In this example, the originating MSC/SGSN (identified by the CGPA GT) does not match the serving MSC/SGSN (identified by the HLR). However, the first four digits do match.

If the MO spoofing digits parameter is set to 4 or less, the FWL will not consider this MO message to be spoofed. If it is set to 5 or greater, the FWL will consider this MO message to be spoofed.

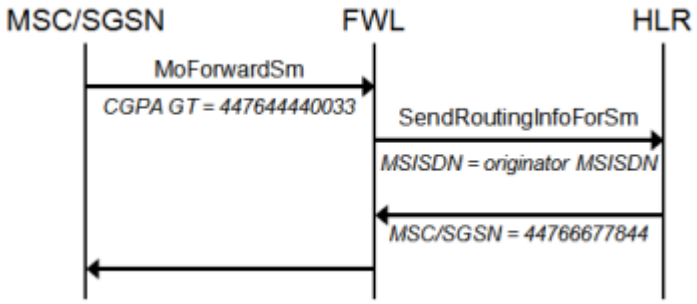


Figure 13: MO message with mismatched originating and serving MSCs/SGSNs

3.3.2 Detecting MO Spoofing with Multi-SIM

The Multi-SIM feature allows an operator to assign a public MSISDN to a subscriber who owns two or more mobile phones. The public MSISDN is in addition to the MSISDNs that are assigned to the subscriber's phones. Each phone uses the public MSISDN as the originator of MO messages and as calling line information (CLI) for outgoing calls. MT messages and incoming calls that are addressed to the public MSISDN terminate on the phone that the subscriber has chosen to receive them.

When the FWL issues a SendRoutingInfoForSm operation for MO spoofing detection, the HLR returns the serving MSC/SGSN for the phone that the subscriber designated to receive MT messages and incoming calls. If the subscriber is not using that phone to send the MO message, the serving MSC/SGSN will not match the originating MSC/SGSN, and the FWL will see the message as spoofed.

Therefore, the FWL must use different methods to detect MO spoofing. The method depends on the type of Multi-SIM solution that is in use. The FWL supports the Nokia solution.

3.3.2.1 Nokia Multi-SIM Support

The FWL supports Nokia's Multi-SIM solution, which maintains a list on the HLR of all MSISDNs that are in each Multi-SIM group. The FWL can use the USSD request operation to retrieve this list and use it to verify if an MO spoofing check failed because the MO message was sent from a group member that is not the member selected to receive MT messages. The FWL then performs an MO spoofing check for each member of the group. If none of these checks succeed, the MO message was spoofed.

This diagram illustrates the call flow beginning with an MO message sent from a Multi-SIM member that is not selected to receive MT messages.

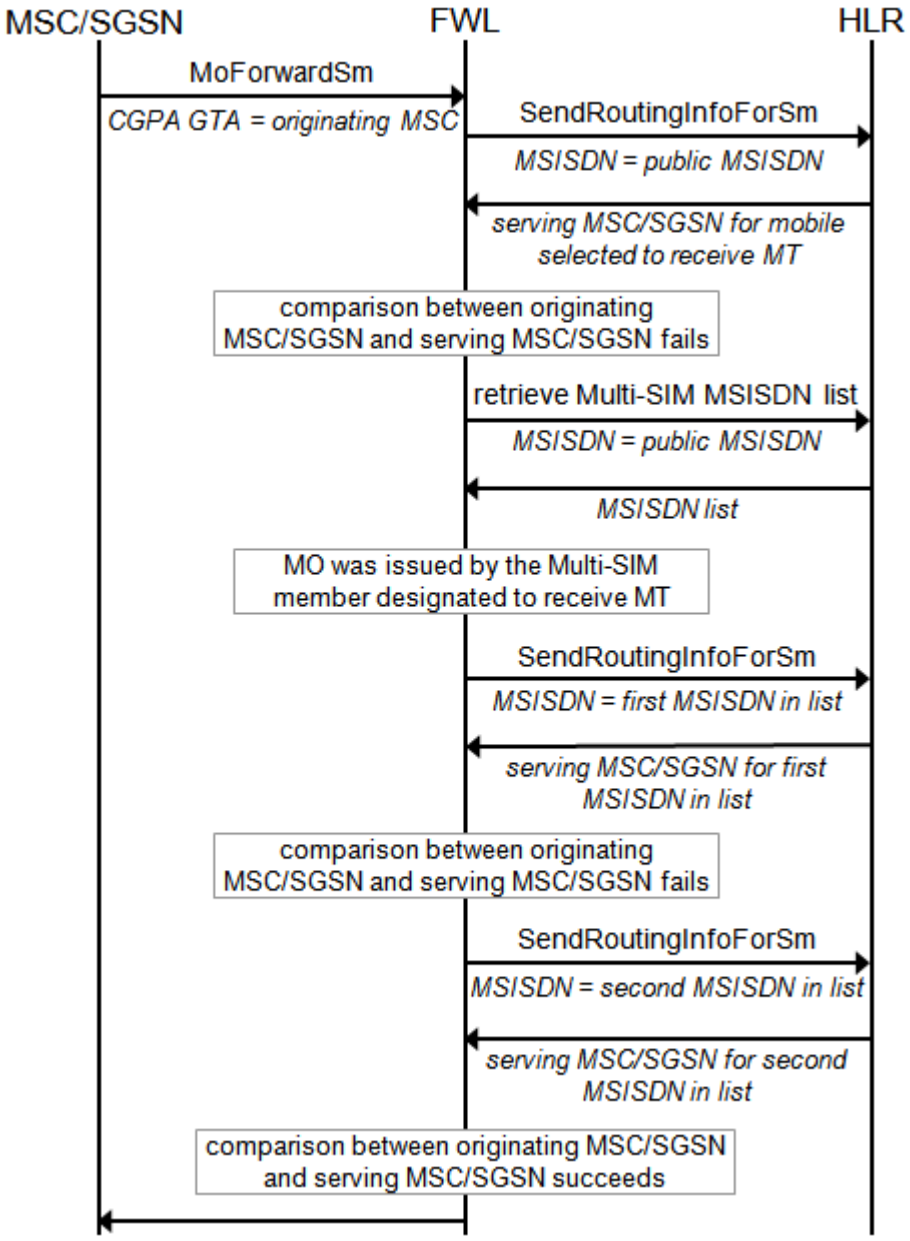


Figure 14: Nokia Multi-SIM example

Refer to *How To Configure the FWL for MO Traffic* for information about configuring Nokia Multi-SIM support.

3.4 Firewalling MO Traffic from Inbound Roamers

Inbound roamers are subscribers of foreign networks who are roaming in the HPLMN. You may want to intercept and possibly block MO traffic from inbound roamers; for example, if they are using virus-infected mobile devices that are overloading the HPLMN's international links with spam messages.

The FWL enables you to intercept MO traffic from inbound roamers and block it or pass it to external SMSCs that are not provisioned in your configuration ("unknown" SMSCs). This is a type of MO-MO routing that is also called CDPA-based forwarding.

This feature includes optional transparency on the SCCP and TCAP layers, so the receiving SMSC (or intermediate elements, such as another firewall) does not know that the message was intercepted. Transparency means that:

- There is only a single TCAP dialogue between the originating MSC/SGSN and the receiving SMSC
- The RTR/FWL preserves the protocol layers up to and including TCAP, with the exception of global title translation (GTT); however, the RTR/FWL may modify protocol layers above TCAP
- The external SMSC to which messages are forwarded is not aware that the messages have passed through the FWL
- When a message arrives at the external SMSC, the SCCP calling party address (CGPA) contains the global title (GT) of the originating MSC/SGSN, not the GT of the RTR

3.4.1 Sample Inbound Roaming Message Flow

The following is an example of the message flow when an MO message from an inbound roamer is routed to an external SMSC that is not provisioned:

1. The MSC/SGSN sends a TCAP Begin message and the Mobile Messaging network intercepts it.
2. The CdPA in the Begin message matches an address in a provisioned list.
3. The RTR transparently forwards the Begin message toward the external SMSC.
4. The SMSC responds to the Begin message by sending a Continue message toward the MSC/SGSN (the Mobile Messaging network does not intercept this message).
5. The MSC/SGSN responds with a Continue message with components.
6. The Mobile Messaging network intercepts the message and the RTR processes it. Standard mobile number portability (MNP) and anti-spoofing checks can be performed.
7. The MOX rules are evaluated and any resulting EC application actions (such as evaluation by the FAF and/or PBC).
8. If the evaluation is positive, the MOR rules are evaluated.
9. If the message matches the MOR rule, and the selected action is route to SMSC, and CdPA-based forwarding is enabled:
    - If transparent routing is enabled (the **Keep MSC/SGSN SCCP of CdPA** parameter is "true"), the RTR will reuse the existing TCAP dialogue to forward the message to the external SMSC
    - If transparent routing is disabled (the **Keep MSC/SGSN SCCP of CdPA** parameter is "false"), the RTR will start a new TCAP dialogue to forward the message to the external SMSC
    - If transparent routing is set to use the global setting, the RTR checks the `optimisedmorouting` parameter in the semi-static configuration file:
        - If it is "true", the RTR will reuse the existing TCAP dialogue to forward the message to the external SMSC

- If it is "false", the RTR will start a new TCAP dialogue to forward the message to the external SMSC

10. If transparent routing was used, the SMSC sends the End message directly to the MSC/SGSN (the Mobile Messaging network does not intercept this message). If transparent routing was not used, the SMSC sends the End message to the Mobile Messaging network.

3.4.2 Restrictions on Firewalling MO Traffic from Inbound Roamers

There are some restrictions on routing MO traffic from inbound roamers to unknown SMSCs:

- The RTR cannot send the messages to an SMSC other than the one identified by the CdPA of the TCAP Begin message.
- The RTR cannot load balance the messages over multiple SMSCs.
- The MAP phase cannot be changed between the incoming MO message and the outgoing MO message (except when required by the RTR's MAP phase negotiation functionality).
- If transparent routing is used, the message length cannot be increased such that it transforms from a TCAP non-segmented message to a TCAP-segmented message. Therefore:
  - The RTR's global title translation (GTT) functionality should not increase the address length
  - Text insertion (via the XS-TIE component) should not be used
  - The FAF should not be used in a way that increases the length of the user data (such as by masking or replacing text)

  If the message would require more than a single MTP PDU (because the address or the user data is too long), the RTR will refuse the message and return a "system failure" message to the originating MSC. The `smsCntMoRejectedDueToLengthChangeOnTransparentForwarding` counter indicates how many messages the RTR rejected for this reason.

Note: If transparent routing is used, the RTR will not know the result of the message submission nor the result of the message delivery. Online billing can be applied to this type of routing; however, for cases in which online billing depends on the delivery result, the RTR will assume that the message was submitted and delivered successfully. This could result in over-charging of the subscriber, so it is therefore not recommended.

3.5 Evaluating MO Messages

The RTR/FWL's default evaluation order for MO messages is:

1. MO spoofing check
2. MO external condition (MOX) rules
3. MO routing (MOR) rules
4. MO counting (MOC) rules

If the FWL detects that a message is spoofed and it is configured to discard spoofed messages (`tpconfig` attribute `firewallmoactionfororiginatingaddressspoofing` in the semi-static configuration file), the message will not be evaluated by the MOX, MOR, or MOC rules.

You can postpone the MO spoofing check until after the MOX rule evaluation. This functionality is required if you want an EC application to evaluate messages before the FWL performs the spoofing check. Refer to *How To Configure the FWL for MO Traffic* for information about changing the evaluation order.

3.6 Bypassing MO Spoofing Checks

You can create whitelists for messages with trusted origins; the FWL will bypass the MO spoofing check for messages from the numbers in the whitelist. You can also create whitelists for messages received from originating subscribers registered with trusted HLRs in the network; the FWL will bypass the MO spoofing check for messages whose originators are registered with HLRs having their GT addresses included in the whitelist. Refer to *How To Configure the FWL for MO Traffic* for information about the types of addresses that you can whitelist.

3.7 Responding to MO Spoofing

The FWL offers several ways to respond to MO spoofing.

When the FWL detects that the originator of a message was spoofed, it can discard the message and return a negative acknowledgment to the originator; this option means that the originator will know the message was blocked.

Alternatively, the FWL can block the message and return a positive acknowledgment, which will give the originator the impression that the message was accepted, or block the message and return no response to the originator, which prevents the originator from knowing the outcome of the spoofing attempt. These two options do not reveal the FWL to the originator, which can help prevent the originator from correctly guessing the network architecture.

The FWL can also allow the message to pass through the Mobile Messaging system; this option enables you to log information to use while planning your FWL configuration, without the risk of blocking legitimate messages because the configuration is not yet complete.

Refer to *How To Configure the FWL for MO Traffic* for information about configuring the response.

3.8 How To Configure the FWL for MO Traffic

This section describes procedures to configure the FWL for MO traffic.

3.8.1 Customize the Performance of MO Spoofing Checks

HPLMN MSCs should use PC/SSN routing to address the FWL; however, it is possible that they will use GT routing. Therefore, to enable the FWL to identify MSCs that use GT routing as being in the HPLMN:

1. Modify the MSC or SGSN configuration in the HPLMN to include a global title translation (GTT) rule that routes MoForwardSms to the FWL using PC/SSN routing.

This instructs the HPLMN to translate any GT-routed MoForwardSm operations to PC/SSN routing before they reach the FWL.

2. Set the `tpconfig` attribute `firewallmospoofingcheckcondition` in the semi-static configuration file to "whenmscsgsnaddressingsmscongt".

   This instructs the FWL to only perform an MO spoofing checks when the MSC or SGSN addresses the SMSC using GT routing. This enables you to restrict MO spoofing checks to MO messages with suspect origins. It requires that all MSCs and SGSNs within your network have a GTT rule for the public SMSC address.

`firewallmospoofingcheckcondition` also supports the value "always", which instructs the FWL to perform MO spoofing checks for all messages. This is the default and most commonly used setting for this attribute.

3.8.2 Configure the STP Point Code

The FWL distinguishes between on-net and off-net MSCs by comparing the originating point code (OPC) of a signaling message to the STP point code (PC).

1. In the semi-static configuration file, add a `destination` entity.
2. Set the `name` attribute to a unique name.
3. Set the `type` attribute to "stp".
4. Set the `pointcode` attribute to the STP PC.

For information about additional, optional attributes of the `destination` entity, refer to the RTR Operator Manual.

3.8.3 Set the Digits Considered for MO Spoofing

To set the number of MSC/SGSN address digits that the FWL considers when checking for MO spoofing:

1. In the left navigation bar of the MGR, select **Environment ➤ Networks**.

   The Network Table tab appears.
2. Select an existing network or click **Add New** to add a new network.
3. Set **Spoofing Check Digits** to the desired number of digits.

   If you are creating a new network, refer to the MGR Operator Manual for information about the other network parameters that are available.

3.8.4 Enable Nokia Multi-SIM Support

To enable support for the Nokia Multi-SIM solution, set the following `tpconfig` attributes in the semi-static configuration file:

1. Set `firewallenablemultisimservice` to "true".
2. Set `firewallussdrequestforretrievingmultisimstatus` to the string to use in the USSD request that checks if an MSISDN is subscribed to the Multi-SIM service (default "*137#").

3. Set `firewallussdresponseformultisimstatusdisabled` to the string that the HLR includes in the USSD response, indicating that an MSISDN is not subscribed to the Multi-SIM service (default "NOT SUCCESSFUL").

3.8.5 Evaluate MOX Rules Before MO Spoofing Check

To instruct the RTR to evaluate MOX rules before the FWL performs the MO spoofing check, set the `tpconfig` attribute `firewallcheckmospoofingafterextcondrules` to "true" in the semi-static configuration file.

In this case, the evaluation order is:

1. MOX rules
2. MO spoofing check
3. MOR rules
4. MOC rules

If the FWL detects that a message is spoofed and it is configured to block spoofed messages, the message will not be evaluated by the MOR and MOC rules.

3.8.6 Limit the Number of MO Spoofing Checks

To prevent the denial of important HLR services during a spam attack, you can limit the number of MO spoofing checks that the FWL will perform per second.

To limit the overall number of HLR queries that the FWL will perform for MO spoofing checks, in the semi-static configuration file, set the `tpconfig` attribute `firewallmospoofinghlrqueryceiling` to the maximum number of MO spoofing checks that the FWL can perform per second.

Note: This limit is on the number of MO spoofing checks, not on the number of HLR queries. In a scenario that requires multiple HLR queries for a single spoofing check, the spoofing check only counts as one. If theRTR is configured to perform a mobile number portability (MNP) check, it combines the HLR queries for the MNP check and for the MO spoofing check.

If the limit is exceeded, the FWL will not perform spoofing checks for the messages above the limit. Therefore, some messages will pass through the FWL unchecked.

3.8.7 Whitelist Originator MSISDNs

You can create up to 16 whitelists of MSISDNs that the FWL will compare to the originator MSISDN specified in the MoForwardSm operation. If the MSISDNs match, the FWL skips the MO spoofing check.

To whitelist originator MSISDNs:

1. In the MGR, go to **Routing ➤ Lists** and create lists of MSISDNs of the originators that the FWL should consider trusted. Each list can contain up to 10,000 addresses.
2. In the semi-static configuration file, set the `tpconfig` attribute `firewallmosmtrustedoriginatorlist[1..16]` to the name of the list, where `[1..16]` is a number between 1 and 16.

   Note: The number at the end of the attribute name is required, even if you implement only one list.

3.8.8 Whitelist MSCs

You can create a whitelist of MSC global titles (GTs) that the FWL will consider trusted. The FWL will not perform an MO spoofing check for messages from this MSC. For messages that are not from this MSC, the FWL will evaluate the rest of the configuration to determine if a spoofing check should be done. For example, if an MSC that is not on this list but it is on-net and the limit on the number of spoofing checks has not been reached, the FWL will not perform an MO spoofing check.

To whitelist MSCs:

1. In the MGR, go to **Routing ➤ Lists** and create a list of GTs of the MSCs that the FWL should consider trusted.
2. In the semi-static configuration file, set the `tpconfig` attribute `whitelistofmomscforspoofchecksuppression` to the name of the list.

3.8.9 Handle MO Spoofing Check Errors

If a SendRoutingInfoForSm (SRI-SM) query returns "teleservice not provisioned" or "call barred", the originator IMSI may not be available, which will cause the MO spoofing check to fail. To set the action that the FWL takes in these cases, set these `tpconfig` attributes in the semi-static configuration file:

- firewallmoactionforspoofingcheckfailureduetotsvcnotprov for "teleservice not provisioned"
- firewallmoactionforspoofingcheckfailureduetocallbarred for "call barred"

Each attribute can be set to:

Value	Description
pass	Do not consider the message to be spoofed.
treatasifspoofing	Consider the message to be spoofed (this is the default).
checkwithmapati	Use the MAP Any Time Interrogation (ATI) message to attempt to retrieve the originator IMSI from the HLR. This operation retrieves the serving Visitor Location Register (VLR) address, which the FWL compares to the address of the originating MSC. If the addresses do not match, the FWL considers the message to be spoofed. The IMSI is not part of the ATI response, so the FWL does not perform an IMSI check.

3.8.10 Configure the Response to MO Spoofing

To configure the way that the FWL responds when it detects MO spoofing, set the `tpconfig` attribute `firewallmoactionfororiginatingaddressspoofing` in the semi-static configuration file:

Value	Description
discardwithnak	Discard the message and return a negative acknowledgment (NACK) to the originator.
discardwithack	Discard the message and return a positive acknowledgment (ACK) to the originator.

Value	Description
discardwithnoresponse	Discard the message and do not return an acknowledgment to the originator (this is the default).
pass	Allow the Mobile Messaging system to continue processing the message.

3.8.11 Override MO Spoofing Check Results

You may want to ensure that messages from certain MSCs and/or SGSNs, certain HLRs or certain Originator IMSIs are never blocked by the FWL, even if the messages do not pass the MO spoofing check. The FWL allows you to whitelist up to 20,000 GTs, which the FWL will compare to the MSC or SGSN returned by the **SendRoutingInfoForSm** (SRI-SM) operation that it issued for the MO spoofing check. The FWL also allows you to whitelist up to 10,000 additional GTs, which it will compare to the HLR GT (SCCP CgPA) returned by the above SRI-SM operation. If the MSC or SGSN, or the HLR GT matches an MSISDN in the corresponding list, the FWL considers the message not to be spoofed.

Similarly, the FWL allows you to whitelist up to 10,000 IMSIs, which the FWL will compare to the Originator IMSI returned by the above SRI-SM operation. If the Originator IMSI matches an IMSI in the list, the FWL considers the message not to be spoofed.

To enable the whitelist of MSC/SGSN addresses, follow the below steps:

1. In the MGR, go to **Routing ➤ Lists** and create one or two lists of MSISDNs that the FWL should consider trusted. Each list can contain up to 10,000 addresses.
2. In the semi-static configuration file, set the `firewallmospoofingsrismmscorsgsnwhitelist1` attribute to the name of the first list. If you created a second list, set the `firewallmospoofingsrismmscorsgsnwhitelist2` attribute to its name.

Note: The number at the end of the attribute name is required, even if you implement only one list.

To enable the whitelist of Originator IMSIs, follow the below steps:

1. In the MGR, go to **Routing ➤ Lists** and create one list of IMSIs that the FWL should consider as trusted IMSIs. This list can contain up to 10,000 IMSIs.
2. In the semi-static configuration file, set the `firewallmospoofingsrismorigimsiwhitelist` attribute to the name of the list.

To enable the whitelist of HLR GT addresses, follow the below steps:

1. In the MGR, go to **Routing ➤ Lists** and create one list of MSISDNs that the FWL should consider as trusted MSISDNs. This list can contain up to 10,000 addresses.
2. In the semi-static configuration file, set the `firewallmospoofingsrismhlrgtwhitelist` attribute to the name of the list.

Note: The FWL overrides the MO spoofing check results if at least one of the following criteria is satisfied:

- The MSC/SGSN returned in the SRI-SM operation matches the configured whitelist of MSC/SGSN addresses,
- The Originator IMSI returned in the SRI-SM operation matches the configured whitelist of IMSIs,
- The HLR GT (SCCP CgPA) returned in the SRI-SM operation matches the configured whitelist of HLR GT addresses.

3.8.12 Preserve the MSC in the MoForwardSm Operation

Some SMSCs require that the MSC address is present in the calling party address (CGPA) field of the MoForwardSm operation, for billing purposes. However, you may not want the FWL to send the SMSC an MoForwardSm with a CGPA containing the original MSC address, because it would cause the SMSC to send the MoForwardSm response directly to the MSC, rather than to the FWL. Depending on your configuration, the FWL may need the MoForwardSm response for functions such as counting, logging, and billing.

Note: Please note the 'optimal MO routing' option, which manipulates the SCCP calling party address as well, can co-exist with this feature. The 'optimal MO routing' option always has precedence over this feature. The 'optimal MO routing' option only affects simple TCAP dialogues (i.e. a dialogue just comprising a TC-BEGIN and a TC-END), whilst this feature deals with simple TCAP dialogues and extended TCAP dialogues. So, when both functions are enabled, the SCCP calling party address of a simple TCAP dialogue is manipulated by the 'optimal MO routing' option and the SCCP calling party address of an extended TCAP dialogue is affected by this feature.

There are two methods to ensure that the CGPA contains an appropriate value.

3.8.12.1 Preserve the MSC Using PC/SSN Routing

This method of preserving the MSC address in the MoForwardSm operation does not require the SMSC to be able to perform SCCP routing based on a translation type (TT) value. To configure this method:

1. Set the `tpconfig` attribute `pcssnroutingwhenincludingmscaddrinmofwdsmtosmsc` to "true" in the semi-static configuration file. This instructs the FWL to send an MoForwardSm with the OPC set to the FWL's PC and a CGPA that contains:
   - A PC/SSN routing indication, and
   - A GT address equal to the MSC address
2. On the SMSC, add a GTT rule for every FWL point code (PC). This reverse-maps the PC of the FWL toward a GT address. This is required for the SMSC to return ACKs correctly.

3.8.12.2 Preserve the MSC Using Translation Type

One method of preserving the MSC address in the MoForwardSm operation requires the SMSC to be able to perform SCCP routing based on a translation type (TT) value. To configure this method:

1. Set the `tpconfig` attribute `ttwhenincludingmscaddrinmofwdsmtosmsc` in the semi-static configuration file to the value to use for the TT.

   For ITU-T, the default is 0; for ANSI, it is 10.
2. Set the `tpconfig` attribute `includemscaddrinmofwdsmtosmsc` to "always".

Note: A different TT is required for each FWL in the network, to ensure that the SMSC can route ACKs to the correct FWL server.

3.8.13 Route MO Traffic from Inbound Roamers

To enable the FWL to intercept MO traffic from inbound roamers, in the MGR:

1. In **Routing ➤ Lists**, create an MSISDN list. The addresses in this list will be matched against the CdPA of all empty Begin messages received for MO messages. You can use the list as a blacklist or as a whitelist.

   If the CdPA matches an entry in a whitelist or does not match an entry in a blacklist, the RTR/FWL will transparently forward the Begin message to the external SMSC.

   If the CdPA does not match an entry in a whitelist or does match an entry in a blacklist, the RTR/FWL will send a Continue back to the MSC/SGSN (this makes transparent routing impossible because it makes the MSC/SGSN aware of the RTR). Once the RTR/FWL has a Begin and a Continue with components, it will evaluate the MOR rules. If the RTR/FWL sees that the MOR rule is configured for transparent routing, the RTR/FWL will return a "system failure" error to the MSC/SGSN and increment the `smsCntTransparentForwardingOverriddenForSegmentedMo` counter.
2. In **Firewall ➤ MO ➤ Properties**, select the list that you created and set whether it will be a blacklist or a whitelist.
3. In **Routing ➤ Routing Rules ➤ MOR**, create an MOR rule that will handle MO traffic from inbound roamers. For the rule's action, select **Route to SMSC**. Set the **CdPA Based Forwarding** parameter to "true".

   If you want the RTR/FWL to route MO messages transparently, for the **Keep MSC/SGSN SCCP CdPA** parameter, select:

   - False—Start a new TCAP dialogue to forward the message to the external SMSC
   - True—Reuse the existing TCAP dialogue to forward the message to the external SMSC
   - Use global setting—Use the value of the `optimisedmorouting` parameter in its semi-static configuration file (which defaults to "false")

3.8.14 Limit MO Rules Evaluation to Certain SMSCs

You can create a list of SMSC global titles (GTs) that identify MoForwardSm operations that are destined for specific SMSCs. Only MoForwardSm operations with SCCP CDPAs that are in this list will be evaluated by the MO rules. If an MoForwardSm has a CDPA that does not match an entry in the list, the FWL will send the MoForwardSm transparently (without performing a spoofing check nor any rule-, logging-, or billing-related action).

To enable this functionality:

1. In the MGR, go to **Routing ➤ Lists** and create a list of GTs of the desired SMSCs.
2. In the semi-static configuration file, set the `firewallmofwdsmsccpcdpagtaiwhitelist` attribute to the name of the list.

If `firewallmofwdsmsccpcdpagtaiwhitelist` is not set, all MoForwardSm operations will be evaluated by the MO rules.

3.9 Billing for MO Spoofing

On rejection of the incoming MO message due to spoofing, the billing profile configured for the "Default Profile For MO Spoofing" in the Post-paid Billing Properties is used for creating the reject CDRs.

Only the FCDR format will be supported for reject CDR generated by the RTR.

On MO Spoofing, the reject CDRs can be created for the following actions:

1. Discard with No Response
2. Discard with Ack
3. Discard with Nack

Chapter 4

Firewalling MT Traffic

Topics:

4.1 Introduction

MT messages are always MAP messages originating from an SMSC and directed to an MSC. This figure illustrates normal MT routing without the FWL.

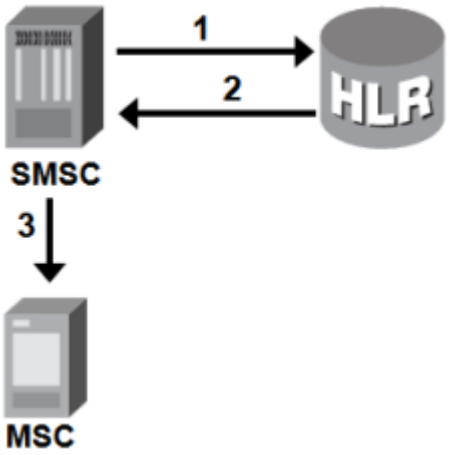


Figure 15: MT routing before FWL deployment

In this configuration:

1. The SMSC sends a SendRoutingInfoForSm (SRI-SM) request to the HLR to obtain the location of the subscriber (MSC or SGSN address) and the subscriber's IMSI.

   The SMSC must always execute this step because the location of the destination MSC may differ between two subsequent attempts to deliver the MT message.

   Note: Although a SendRoutingInfoForSm operation must be performed for an MT delivery, some SMSCs cache SendRoutingInfoForSm information and will perform retries based on the same data received for the first delivery attempt (FDA). Also, some SMSCs may perform multiple MT deliveries based on one SendRoutingInfoForSm operation using the MoreMessagesToSend flag in the MT delivery attempt. The FWL handles both cases, as long as the FWL's internal correlation record has not yet expired (see *Generating Correlation Records*).

2. The HLR sends a SendRoutingInfoForSm response that contains MSC or SGSN and IMSI of the subscriber to the SMSC.
3. The SMSC issues an MtForwardSm operation that contains the IMSI and GT of the destination MSC.

This figure illustrates normal MT routing with the FWL:

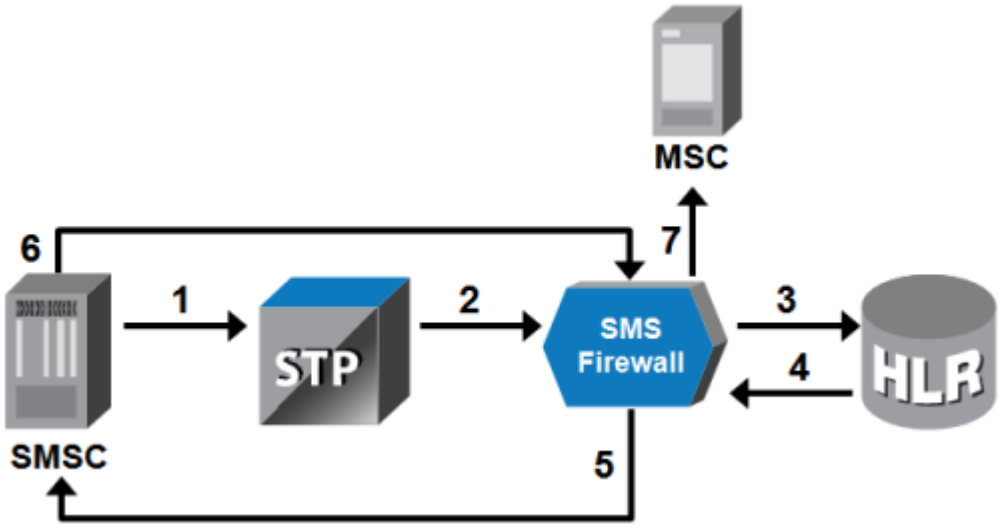


Figure 16: MT routing after FWL deployment

In this configuration:

1. The STP redirects intercepts a SendRoutingInfoForSm request and redirects it to the FWL; this could be a request from a suspect SMSC (which will be checked for MT spoofing) or from a trusted SMSC (which is being Home Routed).
2. If the SendRoutingInfoForSm request is suspect, the FWL performs address comparisons to check for MT spoofing (see *Detecting MT Spoofing*).
3. The FWL modifies the SendRoutingInfoForSm request to ensure that the HLR's response will be directed to the FWL (instead of to the SMSC).
4. The FWL sends the SendRoutingInfoForSm request to the HLR.
5. The HLR sends the SendRoutingInfoForSm response to the FWL, which modifies it to ensure that the SMSC will send the MtForwardSm to the FWL (rather than to the MSC). This is called Home Routing.
6. The SMSC sends the subsequent MtForwardSm operation to the FWL.
7. If the operation is suspect, the FWL again checks for spoofing; if it passes the spoofing check or if it was trusted to begin with, the FWL sends it to the MSC or SGSN.

The Home Routing rules determine if the FWL will transparently pass:

- The SendRoutingInfoForSm response from the HLR to the SMSC
- The MtForwardSm request from the SMSC to the MSC or SGSN

This functionality ensures that the trusted SMSC receives:

- The recipient's true IMSI instead of the scrambled IMSI that the FWL would pass to a suspect SMSC, and
- The genuine serving MSC instead of the FWL's GT

Refer to the RTR Operator Manual for information about the order in which routing rules are evaluated and the fields that are available at each stage in MT message processing.

4.2 Identifying Suspect MT Traffic

MT spoofing checks are limited to traffic that is suspect. Normally, this means MT traffic that originates from SMCSs in other GSM networks ("off-net" SMSCs). Traffic that originates within the HPLMN (from "on-net" SMSCs) is typically considered to be trusted.

The FWL differentiates between suspect and trusted SMSCs by examining the originating point code (OPC). If the OPC:

- Is equal to the STP PC, then the message is from an off-net SMSC (and is therefore suspect)
- Is not equal to the STP PC, then the message is from an on-net SMSC (and is therefore trusted)

There are several ways to route MT traffic so that the FWL can differentiate between trusted and suspect traffic:

- Configure the STP to use MTP3 route messages from trusted sources (routed on PC/SSN routing) to the FWL's VPC
- Configure the HPLMN SMSCs to send MT messages to the STP using PC/SSN routing
- Configure the HPLMN SMSCs to send MT messages to the STP using GT routing and add the SMSCs to the trusted SMSC list

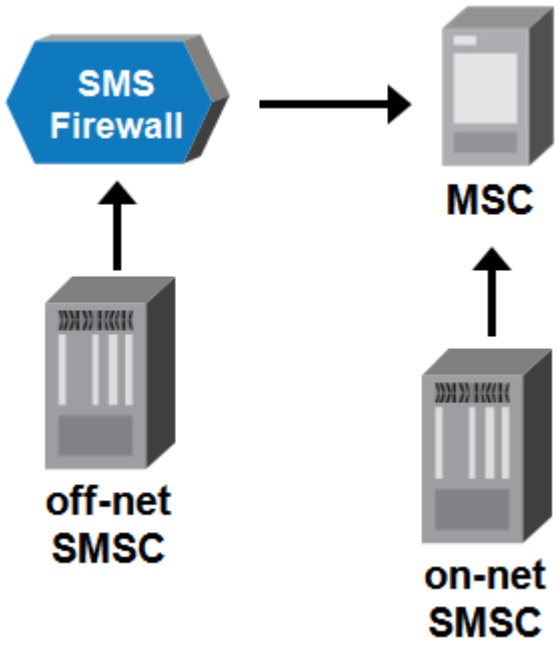


Figure 17: Preferred FWL deployment for MT spoofing checks

The FWL receives unsolicited MtForwardSm operations from the STP on the FWL's VPC. An unsolicited MtForwardSm may indicate that an originator is attempting to bypass firewalling measures. However, unsolicited MtForwardSms from inbound roamers are legitimate, and should not be blocked. Therefore, the FWL has a process to detect unsolicited MtForwardSms and determine if they are destined for inbound roamers. Refer to *Detecting Unsolicited MtForwardSm Operations* for information about this process.

You can use whitelists to further refine what the FWL considers to be trusted and suspect; refer to *How To Configure the FWL for MT Traffic*.

4.3 Detecting MT Spoofing

There are several types of MT spoofing:

Type of Spoofing	Description
Spoofing at the SCCP layer	The SMSC address at the SCCP layer differs between the SendRoutingInfoForSm request and the MtForwardSm request
Spoofing at the MAP layer	The SMSC address at the MAP layer differs between the SendRoutingInfoForSm request and the MtForwardSm request
Conflicting addresses in the SendRoutingInfoForSm request	In the SendRoutingInfoForSm request, the SMSC address at the SCCP layer differs from the SMSC address at the MAP layer
Conflicting addresses in the MtForwardSm request	In the MtForwardSm request, the SMSC address at the SCCP layer differs from the SMSC address at the MAP layer

This diagram illustrates the types of MT spoofing.

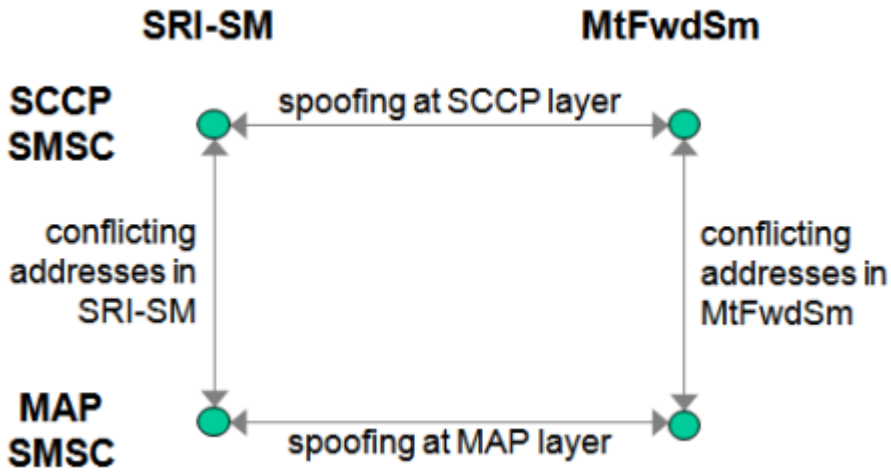


Figure 18: MT spoofing types

To detect MT spoofing, the FWL:

- Compares the SMSC addresses at the MAP and SCCP levels in SendRoutingInfoForSm requests from suspect SMSCs
- Compares the SMSC addresses at the MAP and SCCP levels in MtForwardSm requests from suspect SMSCs
- Correlates each SendRoutingInfoForSm request from a suspect SMSC with its corresponding MtForwardSm request from a suspect SMSC and compares their SMSC addresses at the MAP and SCCP levels

4.3.1 Comparing SMSC Addresses

After the FWL correlates a SendRoutingInfoForSm request from a suspect SMSC with its corresponding MtForwardSm request, it compares the requests' SMSC addresses at the MAP and SCCP levels. A conflict may indicate MT spoofing.

However, the SMSC addresses could differ between the SendRoutingInfoForSm and the MtForwardSm in non-spoofed messages. Therefore, to detect spoofing, the FWL compares the SMSC addresses to the country and network entities that are defined in the MGR. Countries are identified by their country code, while networks are identified by ranges of MSISDNs.

The following diagram illustrates the process of comparing the SMSC addresses in the SendRoutingInfoForSm and MtForwardSm operations to the defined country and network entities.

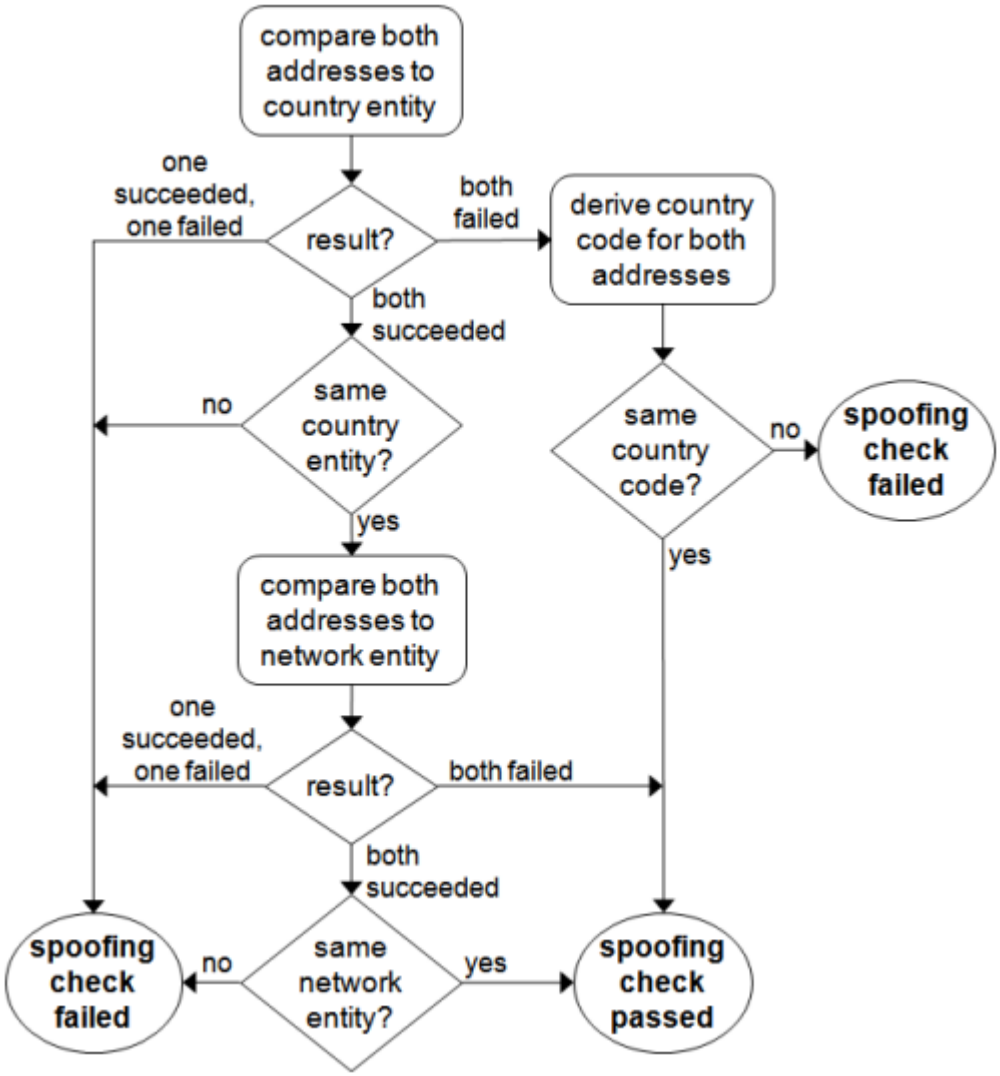


Figure 19: SRI-SM and MtForwardSm SMSC address comparison

4.3.1.1 Deriving the Country Code

The FWL compares SMSC addresses to both the country and mobile network entities that are provisioned in the MGR because it is possible that some networks in a particular country are not provisioned. This can happen as mobile operators acquire competitors and as authorities allocate new number ranges to operators. However, the more network entities you provision, the better the FWL can detect MT spoofing.

When the FWL encounters an SMSC address that does not match any provisioned country entity, it uses an internal table to derive the country code from the SMSC address. The result is:

SMSC address starts with...	**Results in a country code of length...**
1 or 7	1 digit
20, 27, 30, 31, 32, 33, 34, 36, 39, 40, 41, 43, 44, 45, 46, 47, 48, 49, 51, 52, 53, 54, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65, 66, 81, 82, 84, 90, 91, 92, 93, 94, 95, or 98	2 digits
Any other number	3 digits

4.3.2 MT Anti-Spoofing Process

The MT anti-spoofing process flows as follows:

1. The STP intercepts the SendRoutingInfoForSm operation from the SMSC to the HLR and redirects it to the FWL.
2. If the operation originates from an SMSC outside the operator's own network, the FWL compares:
   - The SMSC address at the SCCP layer against the mobile networks that are defined in the MGR
   - The SMSC address at the MAP layer against the mobile networks that are defined in the MGR
   - The country and network parts of the SMSC address at the SCCP layer against the country and network parts of the SMSC address at the MAP layer

   If any of these addresses do not match, the FWL generates an SNMP trap and increments one or more of the following counters:

   - `smsCntRecvSriSmUnknownSccpSmscAddressCounter`
   - `smsCntRecvSriSmUnknownMapSmscAddressCounter`
   - `smsCntRecvSriSmConflictingSmscAddressCounter`
3. The FWL modifies the SendRoutingInfoForSm request to ensure that the SendRoutingInfoForSM response will be sent back to the FWL.
4. The FWL passes the SendRoutingInfoForSm operation to the HLR.
5. When the FWL receives the SendRoutingInfoForSm response from the HLR, it:
   a. Stores information about the response in a correlation record with a randomly generated key (called a "scrambled IMSI")
   b. Modifies the response as follows:
      - Substitutes an address randomly selected from the list in `firewallmscsgsnaddressinsuspectsrismresponse` (or the FWL's GT, if a list is not provisioned) for the MSC and/or SGSN

- Substitutes the correlation key for the IMSI
- Removes the LMSI, if it is present

This is called Home Routing.

6. The FWL sends the modified SendRoutingInfoForSm response to the SMSC.
7. The SMSC sends an MtForwardSm operation that:
   a. Terminates at the FWL's specific PC (as a result of the MSC/SGSN substitution in the SendRoutingInfoForSm response)
   b. Passes the correlation key as the IMSI (as a result of the IMSI substitution)
   c. Specifies the IMSI as the reference for the destination mobile (as a result of the LMSI removal)
8. If the operation is suspect (as opposed to trusted), the FWL compares:
   - The SMSC address at the SCCP layer against the mobile networks that are defined in the MGR
   - The SMSC address at the MAP layer against the mobile networks that are defined in the MGR
   - The country and network parts of the SMSC address at the SCCP layer against the country and network parts of the SMSC address at the MAP layer

   If any of these addresses do not match, the FWL generates an SNMP trap and increments one or more of the following counters:
   - `smsCntRecvMtUnknownSccpSmscAddressCounter`
   - `smsCntRecvMtUnknownMapSmscAddressCounter`
   - `smsCntRecvMtConflictingSmscAddressCounter`
9. The FWL looks up the correlation record:
   - If the look-up succeeds, the FWL compares the:
     - The country and network parts of the SMSC address at the SCCP layer in the `SendRoutingInfoForSm` request against the country and network parts of the SMSC address at the SCCP layer in the `MtForwardSm` request.
     - If the **Enable MT Spoofing Address Match** configuration option is selected for the Network corresponding to the SMSC address at the SCCP layer in the `SendRoutingInfoForSm`, then the SMSC address at the SCCP layer in the `SendRoutingInfoForSm` against the SMSC address at the SCCP layer in the `MtForwardSm` request. Otherwise this comparison will be skipped.
     - The country and network parts of the SMSC address at the MAP layer in the `SendRoutingInfoForSm` request against the country and network parts of the SMSC address at the MAP layer in the `MtForwardSm` request.
     - If the **Enable MT Spoofing Address Match** configuration option is selected for the Network corresponding to the SMSC address at the MAP layer in the `SendRoutingInfoForSm`, then the SMSC address at the MAP layer in the `SendRoutingInfoForSm` against the SMSC address at the MAP layer in the `MtForwardSm` request. Otherwise this comparison will be skipped.

     If there are no conflicts, the FWL combines the information from the correlation record and the MtForwardSm operation and issues an MtForwardSm operation toward the MSC or SGSN using the actual IMSI. In this case, the originator address on the SCCP level contains the SCCP address of the FWL.
   - If the look-up fails, the FWL rejects the MT message.

4.3.3 Impact of MT Anti-Spoofing on Billing Records

MT anti-spoofing measures impact the content of the billing records (CDRs) that are generated by the SMSC and MSC:

- When a suspect SMSC sends an MT message to a subscriber of a network that includes the FWL, the SMSC will generate a billing record with:
  - The scrambled recipient IMSI (as provided by the FWL)
  - A destination GT equal to the GT of the FWL

  In the Mobile Messaging system, this type of CDR is called an inboundMtMtRecord.
- When a destination MSC receives an MT message from the FWL, the MSC will generate a billing record with:
  - The actual recipient IMSI (as provided by the HLR)
  - A MAP address equal to the originating SMSC address
  - An originating GT equal to the GT of the FWL

  In the Mobile Messaging system, this type of CDR is called an outboundMtMtRecord.

Note: The RTR only supports the formatted (FCDR), Ericsson (ECDR), and Logica (LCDR) billing record formats for MT-MT messages. Refer to the Billing Manual for more information about MT-MT billing.

4.3.4 Detecting Unsolicited MtForwardSm Operations

An unsolicited MtForwardSm operation is an MtForwardSm that the FWL cannot correlate with a preceding SendRoutingInfoForSm operation. The FWL receives unsolicited MtForwardSms from the STP, which should be configured to route operations that terminate on an MSC to the FWL.

An unsolicited MtForwardSm may indicate that an originator is attempting to bypass firewalling measures. However, unsolicited MtForwardSms to inbound roamers are legitimate, and should not be blocked. Therefore, the FWL has a process to detect unsolicited MtForwardSms and determine if they are destined for inbound roamers.

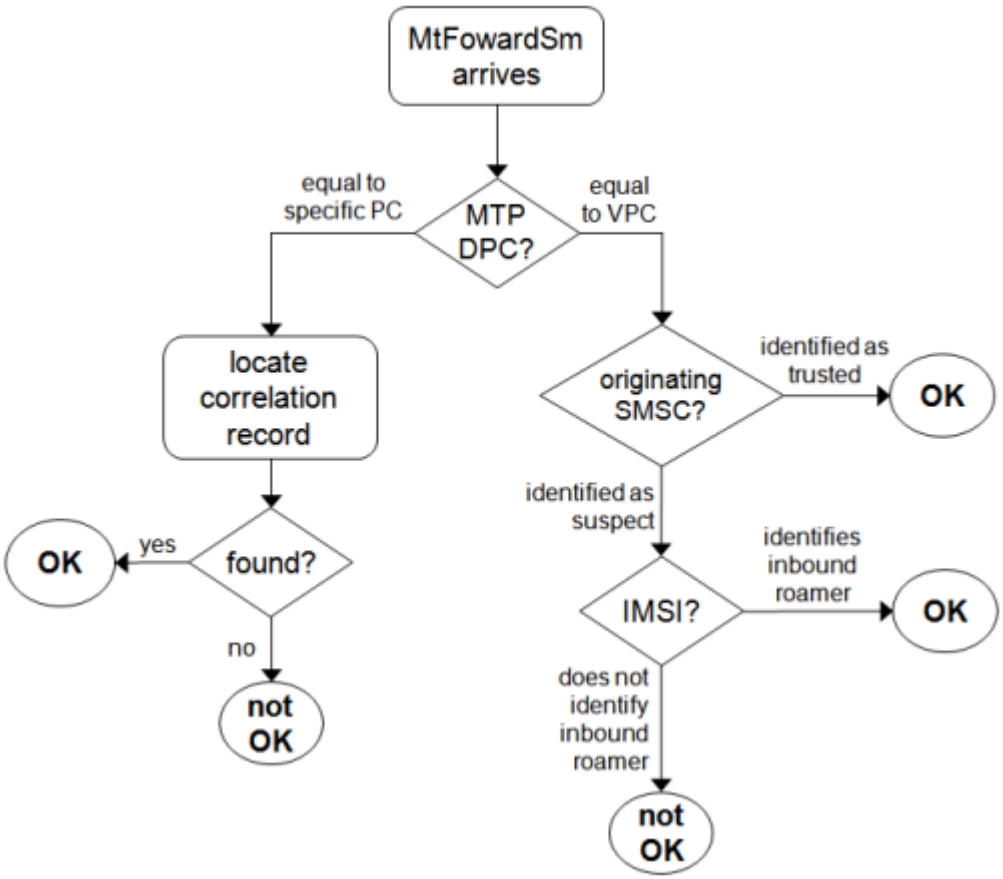


Figure 20: Detecting unsolicited MtForwardSms

To determine whether the recipient is a local subscriber or an inbound roamer, the FWL compares the recipient's IMSI to the IMSI prefixes that are provisioned in the Home Routing entries (at **Environment ➤ Own IMSI** in the MGR GUI). Please refer to MGR manual section "Provisioning Own IMSIs" in the chapter "Environment".

When the FWL receives an unsolicited MtForwardSm operation from a suspect SMSC, it rejects the message if the IMSI in the MtForwardSm matches any of the (non-empty) IMSI prefixes that are defined in the Home Routing entries for suspect traffic (entries in which the **Apply to Suspect** option is selected). Otherwise, the message must be destined for an inbound roamer and is therefore legitimate.

4.3.5 Detecting Unsolicited TCAP End Operations

An unsolicited TCAP End operation (also called an unexpected TCAP End or a rogue TCAP End) is a TCAP End without a corresponding TCAP Begin. Unsolicited TCAP End operations are a strong indicator that your SMSCs' MAP and SCCP addresses are being spoofed. Refer to *Indicators of MT Spoofing* for an illustration of this type of spoofing.

An unsolicited TCAP Continue operation is also an operation without a corresponding TCAP Begin. These operations are additional indicator of spoofing.

The Mobile Messaging system can log unsolicited TCAP End and TCAP Continue operations, alerting you to possible MT spoofing. This logging, viewable in the Log Viewer (LGV), includes information such as:

- Date and time of the operation
- MTP3 originating point code (OPC)
- SCCP calling party address (CGPA) (country and network)
- SCCP called party address (CDPA) (country and network)
- TCAP message type (End or Continue)
- TCAP transaction ID
- Application context name

Enable logging of unsolicited TCAP End and TCAP Continue operations in **Logging ➤ Events ➤ Properties** in the MGR. To create a log filter for viewing the results, go to **Logging ➤ Events ➤ Filters** and select "tcap".

You can view statistics about unsolicited TCAP End and TCAP Continue operations, per country and per network, in the Statistics Viewer (STV) at **Statistics ➤ Unexpected Traffic**.

4.4 SRI-SM Request Rule Set

The SRI-SM Request rule set determines how the RTR handles **inbound** SendRoutingInfoForSm requests, as emitted by an external SMSC. Use the SRI-SM request rule set to control the RTR's behavior regarding the following questions:

1. Should we process SRI-SM request, or reject it?
2. Should we immediately pass the SRI-SM request to the HLR, or not?

4.4.1 SRI-SM Request Rule Evaluation

When the RTR receives a SendRoutingInfoForSm request from an external SMSC, it first executes any applicable validation checks[1]. If the request successfully passes these tests, you may query the Subscriber Service Information (SSI) component for the recipient and the originator MSISDN, if it is present. Then, the RTR evaluates the SRI-SM Request rule set and applies the resulting routing action.

The SRI-SM Request rule set is **not** evaluated for outbound SRI-SM requests (that is, when the RTR plays the role of the SMSC).

The RTR evaluates the SRI-SM Request rule set in the same way that it evaluates the routing rule set; it evaluates individual rules in priority order, and the first matching rule is used, with any lower-priority rules being disregarded. If no rule matches the RTR behaves as if a rule with the routing action "query HLR" had matched.

4.4.2 SRI-SM Request Rule Conditions

The SRI-SM Request rule set supports conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received SRI-SM request, but is evaluated against the time at which the rule is evaluated.

[1] Depending on the installed licenses, this may include MT anti-spoofing checks.

Condition	Format	Description
Originator	General	This condition is evaluated against the address included in the SRI-SM request's optional RP-SMEA parameter. When the parameter is absent, but this condition is specified, the condition evaluates to false if not inverted and to true if inverted.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the normalised MSISDN, if the RP-SMEA address is categorized as MSISDN.
	Single short number, short number range, or short number prefix	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is categorized as a short number.
	Alphanumeric	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges, if the RP-SMEA address is categorized as MSISDN.[2]
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs, , if the RP-SMEA address is categorized as MSISDN. This enables logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a TON of "unknown"; otherwise, it evaluates to false.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a NPI of "unknown"; otherwise, it evaluates to false.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this

[2] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
		condition should not be specified. If the originator is not available, or if it is not categorized as MSISDN, the SSI will be empty (no services).
Recipient	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the MSISDN received at the MAP layer of the SRI-SM request. It refers to the recipient of the subsequent MT messages.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the received MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the MSISDN against the provisioned mobile network number ranges.[3]
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the received MSISDN against a list of MSISDNs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges.
	List	This condition evaluates the SMSC address received at the MAP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that issued the SRI-SM request. Refer to the Firewall Guide for information about how this categorization is done.

[3] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs. If there is a match, the recipient is considered to be a portable application.

4.4.3 SRI-SM Request Rule Routing Action

The sole effect of the evaluation of the SRI-SM Request rule set is that the RTR applies the resulting routing action to the SendRoutingInfoForSm operation. The possible actions are:

Action	Effect
Send to HLR	Send the SRI-SM request to the RTR's outbound SRI-SM request processing, with the intent to forward the SRI-SM to the HLR in such a way that the response will be routed back to the RTR (using a new TCAP dialogue).
Discard with temporary error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for temporary errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mttemporarydiscarderrorforhlr`. In this case, the SRI-SM Response rule set is not evaluated.
Discard with permanent error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for permanent errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mtpermanentdiscarderrorforhlr`. In this case, the SRI-SM Response rule set is not evaluated.
Discard with no response	Drop the SRI-SM request, without sending a response back to the external SMSC. In this case, the SRI-SM Response rule set is not evaluated.
Accept and respond to SMSC immediately	Do not send the SRI-SM request on to the RTR's outbound SRI-SM request processing, but proceed with the evaluation of the SRI-SM response rules.
Have HLR respond to SMSC directly	Send the SRI-SM request to the RTR's outbound SRI-SM request processing, with the intent to relay the SRI-SM to the HLR in such a way that the response will be routed directly back to the external SMSC (using the same TCAP dialogue). In this case, the SRI-SM Response rule set is not evaluated.

4.4.4 SRI-SM Request Rule Matching Ratio

The SRI-SM Request **Rule Matching Ratio** parameter enables you to provision a matching fraction. This is a fraction of two integers, M and N; N must be equal to or greater than M, and both integers must be between 1 and 9999. The matching fraction causes the rule to:

- Only match M out of N times
- Not match N minus M of N times

Non-matching due to the matching fraction only occurs if all other provisioned conditions evaluate to true.

4.5 SRI-SM Response Rule Set

The SRI-SM Response rule set determines how the RTR handles **inbound** SendRoutingInfoForSm requests, to be sent back to an external SMSC. Use the SRI-SM response rule set to control the RTR's behavior regarding the following questions:

1. Should we Home Route subsequent MT messages?
2. What IMSI should we return to the external SMSC?

Home Routing, as well as returning a real IMSI vs. a generated IMSI is described in more detail at the end of this section.

4.5.1 SRI-SM Response Rule Evaluation

If the SRI-SM Request rule set routed the inbound SendRoutingInfoForSm request such that the HLR was not contacted (routing action "accept and respond to SMSC immediately"), the RTR evaluates the SRI-SM Response rule set immediately after evaluating the SRI-SM Request rule set.

If the inbound SendRoutingInfoForSm request was forwarded to the HLR (routing action "send to HLR") and the outbound SendRoutingInfoForSm processing (MTO) resulted in the intent to neither reject nor release the SendRoutingInfoForSm request, the RTR also evaluates the SRI-SM Response rule set.

In all other situations, the SRI-SM Response rule set is ignored.

The RTR evaluates the SRI-SM Response rule set in the same way that it evaluates the routing rule set; it evaluates individual rules in priority order, and the first matching rule is used, with any lower-priority rules being disregarded. If no rule matches and the RTR successfully queried the HLR previously, the RTR behaves as if a rule with the routing action "no home routing" action had matched. If no rule matches and the RTR did not successfully query the HLR, the RTR behaves as if a rule with the routing action "discard with temporary error" action had matched.

4.5.2 SRI-SM Response Rule Conditions

The SRI-SM Response rule set supports conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received SRI-SM request or response, but is evaluated against the time at which the rule is evaluated.
Originator	General	This condition is evaluated against the address included in the SRI-SM request's optional RP-SMEA parameter. When the parameter is absent, but this condition is specified, the condition evaluates to false if not inverted and to true if inverted.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN.

Condition	Format	Description
	Single short number, short number range or short number prefix	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is categorized as a short number.
	Alphanumeric	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges, if the RP-SMEA address is categorized as MSISDN[4].
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs if the RP-SMEA address is categorized as MSISDN. This enables logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a TON of "unknown"; otherwise, it evaluates to false.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a NPI of "unknown"; otherwise, it evaluates to false.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified. If the originator is not available, or if it is not categorized as MSISDN, the SSI will be empty (no services).
Recipient	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the MSISDN received at the MAP layer of the SRI-SM request. It refers to the recipient of the subsequent MT messages.

[4] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the received MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the MSISDN against the provisioned mobile network number ranges[5].
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the "real" IMSI for the recipient of the subsequent MT messages, as returned by the HLR or retrieved from the portable application provisioning data. If no "real" IMSI is available, the condition evaluates to false if not inverted and to true if inverted.
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the received MSISDN against a list of MSISDNs or the recipient IMSI against a list of IMSIs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges.
	List	This condition evaluates the SMSC address received at the MAP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
Dest. MSC or SGSN	General	This condition is evaluated against the MSC or SGSN address as returned by the HLR. If the HLR returns both addresses, the rule set is evaluated against either

[5] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
		the MSC or the SGSN address, as selected by the semi-static attribute `preferredmtdestination`. If neither an MSC nor SGSN address is available when the SRI-SM Response rule set is evaluated, a non-inverted condition evaluates to false and an inverted condition evaluates to true. **Note:** If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), the '**Preferred MT Destination**' in the Network configuration overrides the semi-static attribute '`preferredmtdestination`' for the rules evaluation.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the selected MSC or SGSN address received at the MAP layer of the SRI-SM response from the HLR.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the selected MSC or SGSN address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the selected MSC or SGSN address against the provisioned mobile network number ranges.
	List	This condition evaluates the selected MSC or SGSN address against a list of E.164 numbers. This enables logical OR operation.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that issued the SRI-SM request. Refer to the Firewall Guide for information about how this categorization is done.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs. If there is a match, the recipient is considered to be a portable application.

4.5.3 SRI-SM Response Rule Routing Action

The primary effect of evaluating the SRI-SM Response rule set is that the RTR determines whether subsequent MT messages should be Home Routed or not, which is implemented through the matching SRI-SM rule's routing action. The possible actions are:

Action	Effect
Home Routing	Return a successful SRI-SM response to the external SMSC so that when the returned routing data is used, subsequent MT messages will be routed to the RTR. A rule with this action can only match if: • A real IMSI is available (from the HLR or the portable application provisioning data), or • The rule specifies a range of IMSIs from which an IMSI can be generated
Discard with temporary error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for temporary errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mttemporarydiscarderrorforhlr`.
Discard with permanent error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for permanent errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mtpermanentdiscarderrorforhlr`.
Discard with no response	Drop the SRI-SM request, without sending a response back to the external SMSC.
No Home Routing	Return a successful SRI-SM response to the external SMSC that includes the IMSI and MSC and/or SGSN address as returned by the HLR. This causes the SMSC to direct subsequent MT delivery attempts for that recipient directly to the MSC or SGSN. A rule with this action can only match if the RTR successfully queried the HLR previously, so there is real routing data to return to the external SMSC.

4.5.4 SRI-SM Response Rule Matching Ratio

The SRI-SM Response **Rule Matching Ratio** parameter enables you to provision a matching fraction. This is a fraction of two integers, M and N; N must be equal to or greater than M, and both integers must be between 1 and 9999. The matching fraction causes the rule to:

- Only match M out of N times
- Not match N-M of N times

Non-matching due to the matching fraction only occurs if all other provisioned conditions evaluate to true.

For example, to Home-Route only 30% of the Home-Routable messages, all SRI-SM Response rules with the "Home Route" action should have a **Rule Matching Ratio** of 3/10.

4.5.5 IMSI Generation

If an SRI-SM Response rule has a routing action of "home route", you can associate it with a range of IMSIs between 5 and 15 digits. The range is used to generate an IMSI for use in the RTR's SendRoutingInfoForSm response to the external SMSC in two cases:

- No "real" IMSI (that is, no IMSI provided by the HLR or portable application provisioning data) is available, so a "fake" IMSI must be generated to make Home Routing possible.

- A "real" IMSI is available, but the MT anti-spoofing license is enabled, and generated[6] IMSIs are used to generate a one-to-one mapping between the SendRoutingInfoForSm request and the subsequent MT messages on a per-SMSC basis.

Therefore, if the MT anti-spoofing license is disabled and a real IMSI is available, the RTR will return the real IMSI to the external SMSC. This is called "plain" Home Routing.

Note: When a generated IMSI is returned to the external SMSC instead of a real IMSI, you should be aware that the result is that all logging and billing done on the external SMSC will show the generated IMSI instead of the real IMSI.

IMSI Generation Range

The ranges for generating IMSIs must be large enough to supply sufficient IMSIs under high load conditions. If more IMSIs cannot be generated, the SRI-SM request is rejected with a temporary error. A guideline for calculating the appropriate size of an IMSI generation range is:

```
throughput * max_interval_between_srism_and_mt * 2.2 / number_of_rtr_nodes
```

Where:

- `throughput` is the expected number of MT messages that are supposed to be Home-Routed using this IMSI generation range under peak traffic load, in SMs per second.
- `max_interval_between_srism_and_mt` is the value of the semi-static configuration attribute `firewallmaxintervalbetweensrismandmtfwdsm`, which defaults to 60 seconds.
- `number_of_rtr_nodes` is the number of RTR nodes that perform the same task (that is, that share the message load as identified by (`throughput`)

For example, if a certain IMSI generation range is supposed to support a throughput of 1000 SM/s and four RTR nodes are deployed to share that load, the IMSI generation range should contain at least 33,000 IMSIs.

4.5.6 Home Routing

Home Routing is a RTR feature that causes an external SMSC to deliver MT messages to the RTR instead of to a real MSC or SGSN. You can use Home Routing to:

- Apply MT anti-spoofing checks
- Apply personalized services or services such as message forwarding, message copying, spam detection, or spam filtering to MT messages
- Take advantage of interconnect agreements that may exist between the foreign PLMN and the HPLMN or between the HPLMN and the visited PLMN

Home Routing requires the RTR to maintain a *correlation database* that contains *correlation records*. These records preserve message parameters that are available during SendRoutingInfoForSm processing, so they will be available during MT message processing. The database is stored in volatile memory[7],

[6] Generated IMSIs have also been called "scrambled" IMSIs. However, this term implies that there is a reverse-engineerable algorithm that translates a real IMSI into a scrambled IMSI, which is not the case. When an IMSI is generated, the RTR selects a random IMSI out of the configured range.

[7] This means that when the RTR is restarted, the database will be cleared. In this case, if the external SMSC attempts to delivery Home Routed MT messages, an "unsolicited MT message" event will occur on the RTR. By default, this event causes the RTR to drop the MT message with no response. The SMSC's delivery attempt will time out, and the next delivery attempt will begin with a SendRoutingInfoForSm operation again, re-installing the correlation record.

and the key for retrieving a record is the recipient IMSI[8] (as included in the Home Routed MT message issued by the external SMSC). A correlation record typically preserves the recipient MSISDN (as it is not available in an MT message) and the relevant routing data returned by the HLR. Each correlation record exists only on a single RTR instance; the instance that processed the SendRoutingInfoForSm request.

Home Routing works because the MSC and/or SGSN address returned to the external SMSC in the SendRoutingInfoForSm response is populated with an E.164 address that is uniquely assigned to that RTR instance. By default, that is the RTR's global title (GT) or one of the E.164 addresses specified in the list that is provisioned in the semi-static configuration attribute `firewallmscsgsnaddressinsuspectsrismresponse`. If, during the processing of the SendRoutingInfoForSm request, the HLR was queried successfully and the HLR returned both an MSC and an SGSN address, the RTR's SendRoutingInfoForSm response will include the same E.164 address in the MSC and SGSN fields. Therefore, the external SMSC can choose whether to deliver the MT message to the SGSN or to the MSC. That decision is conveyed to the RTR by means of the subsystem number (SSN) in the called party address (CDPA) of the subsequent MT delivery attempt.

4.6 MTI Rule Set

There are three types of MTI rules:

- MTI routing rules (MTIR)
- MTI external condition rules (MTIX)
- MTI counting rules (MTIC)

All rules are evaluated for **Home-Routed**, **inbound** MT traffic only; that is, when the RTR plays the role of a firewall. They are not evaluated for outbound MT traffic, and they are not evaluated for MT traffic that is rerouted to the RTR through MAP screening functionality.

All MTI rule sets support the same conditions.

Note: An MT message can be either a GSM 03.40 Deliver-SM (a normal message) or a phase 2 Status-Report.

4.6.1 MTI Rule Evaluation

When the RTR processes inbound MT traffic from an external SMSC, it begins by categorizing the SMSC as trusted or suspect. The originating external SMSC of an inbound MT message is categorized as trusted if:

- The SMSC address at the SCCP layer (and at the MAP layer, if present) matches the list of trusted SMSCs in the semi-static configuration attribute `firewalltrustedsmsclist`, or
- If the MT message was received with an originating point code (OPC) that is different from the provisioned STP's[9]

[8] If the HLR returned an LMSI, that LMSI is not returned to the SMSC when Home Routing, so that the recipient IMSI is always present in a Home-Routed MT message.

[9] This way of categorizing originating SMSCs means that operators must instruct their own SMSCs to directly route SRI-SMs (and MT messages) to the RTR; that is, GT translation rules on the SMSC would address the RTR, and any intermediate STP would not need to apply GTT rules, and therefore not

- If the SCCP CgPA GT address present in an incoming SendRoutingInfoForSm exists in the **Trusted SMSC SCCP CgPA List** configured in the MGR GUI (**Firewall ➤ MT ➤ Properties**), then the SMSC is considered trusted and the corresponding MT Forward SM received with the same IMSI as returned in the SendRoutingInfoForSm response is also considered trusted.

MT messages from suspect sources undergo stricter MT anti-spoofing checks (when the MT anti-spoofing license is present).

After the SMSC is categorized as trusted or suspect, the RTR validates the categorized MT message, which includes normalization of address parameters and performing MT anti-spoofing checks. During validation, the RTR retrieves the correlation record from the correlation database. If retrieval fails, the RTR rejects the MT message as unsolicited. If the retrieval succeeds, the message parameters contained in the correlation record (such as the recipient MSISDN and, possibly, the recipient's real IMSI and serving MSC) become available to be used in rule conditions.

If the message passes the validation phase successfully, the RTR can optionally retrieve the SSI data. Then, the RTR evaluates the MTIX rule set. After the message passes MTIX rule evaluation, the RTR evaluates the MTIR rule set, primarily to determine the routing path for the inbound MT message. The RTR then routes the MT message and sends a response back to the external SMSC. The RTR evaluates the MTIC rule set during the post-processing phase for the message, and increments MTIC counters according to the response sent back to the SMSC.

Note: The external SMSC may use a single TCAP dialogue to request the delivery of multiple MT messages. For Home-Routed MT traffic, the TCAP dialogue is always established between the SMSC and the RTR; it is never established between the SMSC and the real MSC or SGSN. If the RTR needs to forward the MT message to the real MSC or SGSN, the RTR initiates a second TCAP dialogue to do so. For each MT message received over the same TCAP dialogue, the same evaluation process is executed. Therefore, every message can potentially take a different route (even if this would be desirable only for rare scenarios). When routing the MT message to an application (MT-AT), to storage (MT-Store), or to another SMSC as AO (MT-AO), the RTR uses the TP-MMS field of the inbound MT message to determine if the inbound TCAP dialogue should be continued. When the MT message is routed to the real MSC or SGSN, that node's dialogue continuation behavior will be mirrored on the inbound TCAP dialogue.

4.6.2 MTI Rule Conditions

The MTI rule sets support conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received MT message, but is evaluated against the time at which the rule is evaluated.
Originator	General	By originator, we generally refer to the TP-OA parameter of a Deliver-SM message or the TP-RA parameter of a Status-Report message.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the originator address, if the originator address is categorized as MSISDN.

change the message's OPC. Therefore, any SRI-SM or MT message received on the RTR from an STP's OPC would not come from any of the operator's own SMSCs, but from a foreign, suspect SMSC.

Condition	Format	Description
	Single short number, short number range or short number prefix	This condition is evaluated against the originator address, if the originator address is categorized as a short number.
	Alphanumeric	This condition is evaluated against the originator address, if the originator address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized originator address, if the originator address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges, if the originator address is categorized as MSISDN.
	List	This condition evaluates the normalized address against a list of MSISDNs or short numbers, enabling logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the TP-OA or TP-RA parameter.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the TP-OA or TP-RA parameter.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the MTI rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified.
Recipient	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the recipient MSISDN retrieved from the correlation record.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the recipient MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the recipient MSISDN against the provisioned mobile network number ranges[10].
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the "real" IMSI for the recipient of the subsequent MT messages, as returned by the HLR or retrieved from the portable application

[10] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
		provisioning data. If no "real" IMSI is available, the condition evaluates to false if not inverted, and to true if inverted.
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the recipient MSISDN against a list of MSISDNs, or the "real" recipient IMSI against a list of IMSIs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the MTI rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
DCS		This condition is evaluated against the Deliver-SM's TP-DCS parameter. If the MT message is a Status Report, the condition evaluates as if the TP-DCS parameter were set to 0.
Message Type		This condition is evaluated against the MT message type, which is a Deliver-SM or a Status Report.
User Data		This condition is evaluated against the user data portion of the MT message. In the case of a Status Report, this condition behaves as if the user data portion were empty.
User Data Header		This condition is evaluated against the list of user data header information element identifiers that are present in the MT message.
Ext Att		This condition is evaluated against the external attributes as set and reset by the EC application consulted during the evaluation of the MTIX rules. This condition is not supported in the MTIX rule set.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the MT message.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges.
	List	This condition evaluates the SMSC address received at the MAP layer of the MT message against a list of E.164 numbers. This enables logical OR operation.

Condition	Format	Description
Originator - SMSC Addr. Match		This condition is evaluated by comparing the Originator address and the SMSC Address on the basis of their country and network parameters. The respective country is derived by extracting the E.164 country code from the Originator and the SMSC address and matching the same against the provisioned countries. Similarly, the respective network is derived by matching the Originator and the SMSC address against the provisioned mobile network number ranges/prefixes. In case no provisioned country or network number range/prefix is matched, then the corresponding country or network is considered as “unknown”. The comparison of the Originator and the SMSC address is based on the following criteria, which are configurable on the MGR: • 0 - Originator Country equals SMSC • 1 - Originator Country strictly equals SMSC • 2 - Originator Network equals SMSC • 3 - Originator Network strictly equals SMSC The 'strictly equals' criterion requires an exact match of the two values being compared, and it is a special case of the 'equals' criterion which can be satisfied even if one (or both) of the values being compared is (are) 'unknown'. Note that only one criterion can be configured at a time. In case none of the criteria is configured, the non-inverted condition always evaluates to FALSE and the inverted condition always evaluates to TRUE.
Dest. MSC or SGSN	General	This condition is evaluated against the real MSC or SGSN address as retrieved from the correlation record. If addresses are available, the rule set is evaluated against either the MSC or the SGSN address, as selected by the SSN included in the SCCP CDPA. If neither an MSC nor SGSN address is available in the correlation record, a non-inverted condition evaluates to FALSE, and an inverted condition evaluates to TRUE.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the selected MSC or SGSN address retrieved from the correlation record.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the selected MSC or SGSN address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the selected MSC or SGSN

Condition	Format	Description
		address against the provisioned mobile network number ranges.
	List	This condition evaluates the selected MSC or SGSN address against a list of E.164 numbers. This enables logical OR operation.
Reply Path		This condition is evaluated against the MT message's TP-RP flag.
Status Report		This condition is evaluated against the MT message's TP-SRI flag.
PID		This condition is evaluated against the Deliver-SM's TP-PID parameter. If the MT message is a Status Report, the condition evaluates as if the TP-PID parameter were set to 0.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that which issued the MT message.
Message Segments		This condition is evaluated against the interpreted user data header information element, indicating that the message is segmented. **Note:** A condition with neither the first, nor the last, nor the intermediate segment flags turned on will evaluate to false if the MT message is not segmented. To match on unsegmented messages only, turn on all three flags and invert the condition.
Recipient RN Group		During the processing of the preceding SRI-SM request, the HLR may have returned an IMSI that was prefixed with a provisioned routing number. If a routing number was recognized, it was stripped off the real IMSI, associated with a routing number group, and added to the correlation record. This condition is evaluated against that routing number group.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs during the processing of the SRI-SM request. If there was a match, the recipient is considered to be a portable application.

4.6.3 MTIR Rule Set

The RTR evaluates the MTIR rule set to determine how inbound, Home-Routed MT messages will be routed. An MT message can be Deliver-SM (a normal message) or a Status Report. For information about the circumstances in which the MTIR rule set is evaluated, refer to *MTI Rule Evaluation*.

4.6.3.1 MTIR Routing Action

The primary effect of the evaluation of the MTIR rule set is that the RTR determines where the MT message will be routed, which is implemented through the matching MTIR rule's routing action. The possible actions are:

Action	Effect
Discard with temporary error	Reject the MT message by sending a ReturnError response that contains the configurable error code for temporary errors of the MSC/SGSN back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mttemporarydiscarderrorformscorsgsn`.
Discard with permanent error	Reject the MT message by sending a ReturnError response that contains the configurable error code for permanent errors of the MSC/SGSN back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mtpermanentdiscarderrorformscorsgsn`.
Discard with no response	Drop the MT message without sending a response back to the external SMSC.
Discard with acknowledgment	Discard the MT message after sending a response to the external SMSC that indicates delivery success. The external SMSC will proceed as if the MT messages was delivered successfully.
Store for delivery to MS	Store the MT message in the specified AMS queue and return a response depending only on the storage result. At a later point in time, the AMS will request that the RTR deliver the MT message, which may lead to multiple retries. You must specify the AMS queue in which to temporarily store the MT message in the MTIR rule. A rule with this routing action only matches if, at the time of the rule evaluation, at least one AMS is available, which indicates the capability for storing messages (as opposed to Icache functionality only).
Route to mobile	Directly send the inbound MT message on to the MSC or SGSN with which the recipient is currently registered. If no routing data is available from the correlation record (because the HLR was not queried during the preceding SRI-SM processing), the HLR query is executed before the MT message is sent to the MSC or SGSN. **Note:** In this case of a "late" HLR query, the transparent nature of MT-MT forwarding is lost, the RTR recreates the outbound MT message, and the RTR typically uses its own global title (GT) to identify the SMSC toward the terminating MSC or SGSN. Likewise, the transparent nature of the MT response forwarding toward the external SMSC is lost. Depending on the categorization of the MT response from the MSC or SGSN, the error code that is sent back to the SMSC is determined in the same way as for the "discard with temporary error" or "discard with permanent error" action. In the case of a late HLR query, the MTO rules are evaluated during the outbound SRI-SM processing in the same way as they are evaluated for an outbound SRI-SM during the inbound SRI-SM processing, with one exception: the MTOR rule set does not follow the

Action	Effect
	`firewallenablemtrtgruleevaluationforsrismresponse` attribute, but rather is never evaluated for SRI-SM responses.
Route to application	Route the inbound MT message as an AT message to an application. The target application can be determined in three ways: • By the rule. The MTIR rule explicitly refers to a provisioned application. All MT messages matching this rule are delivered as AT messages to that application. Such MTIR rules only match if, at the time of the rule evaluation, the target application is available for receiving AT messages. • By recipient address. The recipient address can refer to a provisioned application by means of the provisioned portable applications. If that is the case of the inbound MT message, such an MTIR rule can only match if at the time of the rule evaluation, the application associated with the recipient address is available for receiving AT messages. • By load balancing group. Refer to the description of AT load balancing groups. The MTIR rule explicitly refers to a provisioned load balancing group. All MT messages matching this rule are delivered as AT messages to one of the applications in that load balancing group. Such MTIR rules only match if at the time of the rule evaluation, at least one of the applications in the load balancing group is available for receiving AT messages. When an temporary/permanent error is returned, the error code can be configured using the semi-static configuration attributes: • `mttemporarydiscarderrorformscorsgsn` • `mtpermanentdiscarderrorformscorsgsn`
Route to SMSC as AO	Route the inbound MT message as an AO message to an external SMSC so that the SMSC will take care of the (further) delivery of the message. The rule explicitly specifies: • Which application should be used to submit the AO message to the SMSC • Which SMSC group the AO message should be forwarded to For such an MTIR rule to match, the following additional conditions must be met: • The MT message must be a Deliver-SM (it is not possible to route Status Report messages as AO) • At the time of the rule evaluation, at least one of the SMSCs in the SMSC group must be available to receive AO messages from the designated application When an temporary/permanent error is returned, the error code can be configured using the semi-static configuration attributes: • `mttemporarydiscarderrorformscorsgsn`

Action	Effect
	• mtpermanentdiscarderrorformscorsgsn

If no MTIR rule matches, the RTR applies the following logic:

```
If the recipient MSISDN is associated with an application by means of the portable
application provisioning data, then
     If that application is available to receive AT messages
          Route the MT message as AT to that application
     Else
          Behave as if a MTIR rule with action "discard with temporary error" had
          matched
Else
     Behave as if a MTIR rule with action "route to MS" had matched
```

4.6.3.2 MTIR Rule Modifier

MTIR rules can refer to an MTI modifier. The MTI modifier only supports the **Defer Period** parameter, which enables you to defer the delivery of an MT message that matches an MTIR rule that refers to the modifier. The modification is applied to the inbound message after MTIR rule evaluation, along with any modifications requested by EC applications that were contacted during evaluation of the MTIX rules. The defer period only has an effect if the routing action is "store for delivery to MS" or "route to SMSC as AO".

4.6.3.3 MTIR Rule Billing

MTIR rules can refer to a billing profile that will trigger the generation of CDRs representing the processing of the inbound MT messages. When processing inbound MT traffic, the RTR creates CDRs that represent the fact that the inbound MT message was accepted (that is, a positive acknowledgment is sent back to the SMSC). When generating CDRs for inbound MT traffic, the RTR also considers any billing profiles that were assigned to the message during the evaluation of the MTOR or ATOR rule sets.

For more information about the CDR formats that the RTR supports, refer to the Billing Manual.

4.6.4 MTIX Rule Set

The RTR evaluates the MTIX rule set so that EC applications can process the inbound MT message. EC processing may include providing extra personalized services, filtering messages, and/or performing real-time charging. For information about the circumstances in which the MTIX rule set is evaluated, refer to *MTI Rule Evaluation*.

4.6.4.1 MTIX Rule Failure Action

If the ECI evaluation produces a result of false (after the optional inversion of the corresponding MTIX rule's external condition), then the processing of the sorted list of matching MTIX rules stops and the failure action of the MTIX rule is applied.

The possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching MTIX rules, or assume that the message "passed" the MTIX rule evaluation if there are no more matching rules in the list.
Discard With Temporary Error	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with temporary error" had matched.
Discard With Permanent Error	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with permanent error" had matched.
Discard With No Response	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with no response" had matched.
Discard With Ack	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with ACK" had matched.

4.6.5 MTIC Rule Set

The MTIC rule set is evaluated to generate statistics about the handling of inbound, Home-Routed MT messages. Each MTIC rule has a set of per-result counters in addition to the "total" counter. The result counters pertain to the result as the external SMSC would see it (coming from the RTR).

4.6.6 Portable Application Support for Inbound MT Traffic

The portable applications feature enables you to associate certain MSISDNs with an application. Messages addressing one of these MSISDNs can be routed as AT messages to the associated application. To use the portable applications feature for home-routed inbound MT messages, you must have the MT-AT routing path license, and you must enable the feature for inbound MT traffic in **Routing ➤ Properties ➤ Enable Portable Application for MT**).

The RTR will match the recipient MSISDN of the inbound SendRoutingInfoForSm request against the portable application provisioning data. If there is a match, the RTR associates the recipient address with the corresponding application and flags the message as making use of the portable application feature. The flag and the association of the recipient address with an application can be used during the evaluation of the SRI-SM and MTI rule sets.

By default, the portable application feature works in the absence of SRI-SM Request and MTI rules. However, it is recommended to explicitly express the fact that the portable application feature is in use for inbound MT traffic by defining rules.

Sample Portable Application Configuration

This is a sample of a recommended configuration for the portable application feature:

1. Create an SRI-SM response rule that Home Routes all MT traffic that is destined for a portable application. Enable the portable application condition. Set the routing action of the rule to "home route". The specification of an IMSI range is not necessary.

2. Create an SRI-SM Request rule with the appropriate priority and the portable application condition enabled. Set the routing action to "Accept and Respond to SMSC immediately."
3. Create an MTIR rule of appropriate priority with the portable application condition enabled. Set the routing action to "route to application" and set the Application to "by recipient".

This configuration implements rule-based MT-AT routing for inbound MT traffic toward portable applications. The RTR will automatically select the appropriate destination application based on the portable application provisioning data.

4.7 Generating Correlation Records

MT anti-spoofing and Home Routing both require a correlation record to associate each MtForwardSm operation with its preceding SendRoutingInfoForSm operation. In the case of MT anti-spoofing and "scrambled" Home Routing, the key that the FWL uses to look up the correlation record is a unique, scrambled version of the recipient's IMSI (as provided by the HLR).

In the case of "plain" Home Routing, the key is the recipient's real IMSI; it is, therefore, not unique. During the lifetime of the correlation record, MT messages from different trusted SMSCs can be correlated with it.

Note: When the scrambled IMSI is used, the SMSC will not receive the real IMSI of the short message recipient.

This diagram shows the SendRoutingInfoForSm and MtForwardSm phases of the MT delivery proces. The FWL generates the correlation record at step 4 of the SendRoutingInfoForSm phase, after it has received a SendRoutingInfoForSm response from the HLR (step 3). This record contains the correlation key (scrambled IMSI) and information that the FWL received from the HLR. In step 5, the FWL sends the SendRoutingInfoForSm response to the SMSC with the correlation key in place of the recipient's IMSI.

In the MtForwardSm phase, the MtForwardSm request from the SMSC (step 6) contains the correlation key. In step 7, the FWL uses the key to look up the correlation record and compare the SMSC addresses. If the FWL does not detect spoofing, it uses the HLR information in the record to compose the MtForwardSm to the MSC.

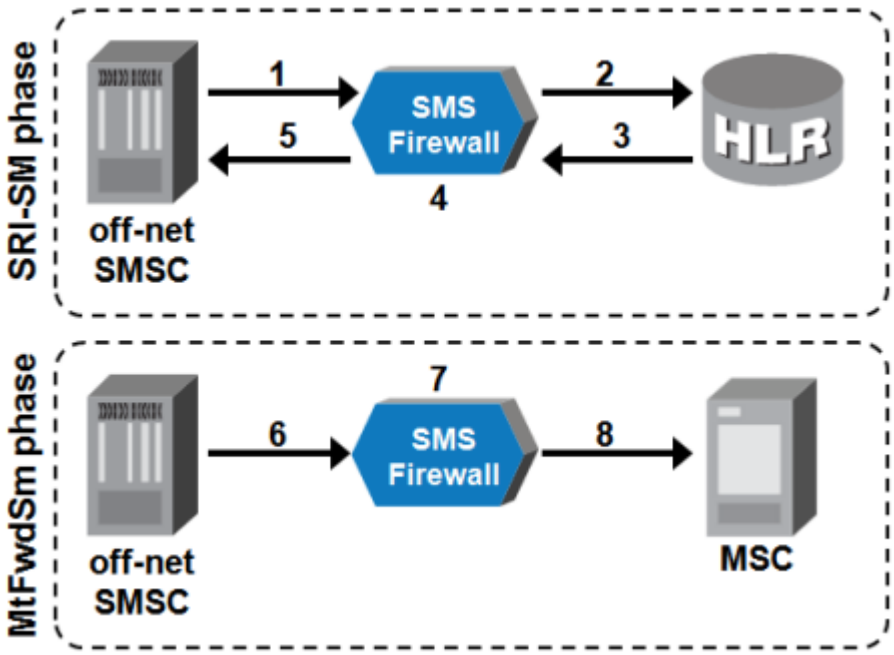


Figure 21: Correlation record creation and look-up

Note: If the MtForwardSm arrives at the FWL after the number of seconds specified in the `tpconfig` attribute *firewallmaxintervalbetweensrismandmtfwdsm* in the semi-static configuration file, the correlation record look-up will fail.

Typically, an operator only modifies SendRoutingInfoForSm responses that pertain to its own subscribers. The FWL identifies the operator's own subscribers by comparing the recipient's real IMSI to a list of IMSI prefixes that the operator has configured. If the real IMSI matches a prefix, the FWL randomly selects a scrambled IMSI from the IMSI range that corresponds to that prefix.

To avoid confusion and erroneous charging, the range of scrambled IMSIs must not overlap the range of IMSIs that are in use for subscribers.

The `mtScramblingCount` counter indicates the number of times that IMSI scrambling has been applied.

4.8 Handling Mobile Number Portability

Typically, mobile number portability (MNP) is configured such that, when an SMSC sends a SendRoutingInfoForSm requests for a ported-out number, the request is routed to the FWL. The FWL can then send the request back to the STP for further handling.

The FWL can distinguish ported-out MSISDNs from HPLMN MSISDNs if a routing number (RN) is inserted in the SCCP called party address (CDPA) between the country code and the nationally significant part of the GT (a common practise for ported-out numbers). For example, if the RN is 015, the number 44123456789 becomes 44015123456789.

Refer to *How To Configure the FWL for MT Traffic* for information about configuring MNP.

4.8.1 Republishing SRI-SM Requests

The FWL's republishing functionality handles a scenario in which multiple networks within a country have deployed a FWL, and at least one of the networks deployed its FWL before deploying the signaling relay function for mobile number portability (MNP/SRF).

Republishing means that, instead of relaying a SendRoutingInfoForSm response from the HLR to the SMSC, the FWL reissues the SendRoutingInfoForSm request to the HLR with some changes to the SCCP address.

When the FWL receives a SendRoutingInfoForSm response from the HLR for a request from a suspect SMSC, it inspects the IMSI. If the IMSI does not identify a subscriber of the HPLMN, the FWL concludes that it represents a ported-out subscriber. If the subscriber is a member of the FWL's list of networks to which republishing applies, the FWL republishes the SendRoutingInfoForSm request.

The FWL modifies the SCCP of the republished request as follows:

SCCP Address	Initial SRI-SM from FWL	Republished SRI-SM Request
Calling party address (CGPA)	GT equal to the FWL GT	Equal to CGPA from SRI-SM request (as received from SMSC)
Called party address (CDPA)	GT equal to MSISDN to be queried	Equal to CGPA from response to first SRI-SM request

Note: When republishing the SendRoutingInfoForSm, the FWL always uses the TCAP transaction ID that the SMSC supplied in the original SendRoutingInfoForSm. This enables the SMSC to correlate the response.

The following figures illustrate the republishing process. In the first phase, the SMSC sends a SendRoutingInfoForSm request, which the FWL of Net 1 intercepts and then forwards toward the HLR, to retrieve the IMSI.

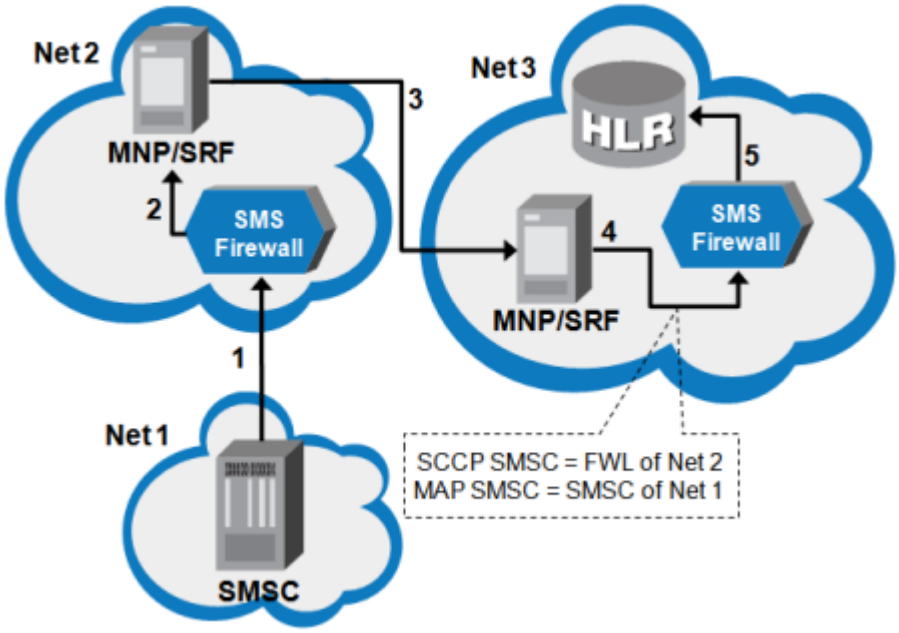


Figure 22: Republishing phase 1, SendRoutingInfoForSm request

In the second phase, the FWL of Net 2 inspects the IMSI and determines that the query concerns a ported-out subscriber.

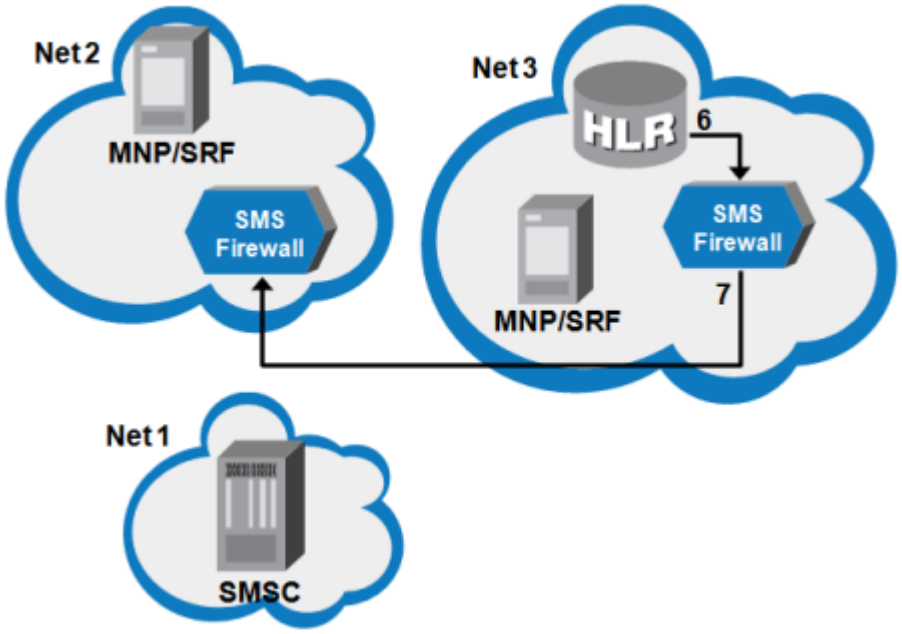


Figure 23: Republishing phase 2, SendRoutingInfoForSm response

In the third phase, the FWL of Net 2 republishes the SendRoutingInfoForSm request with the CGPA of the SMSC.

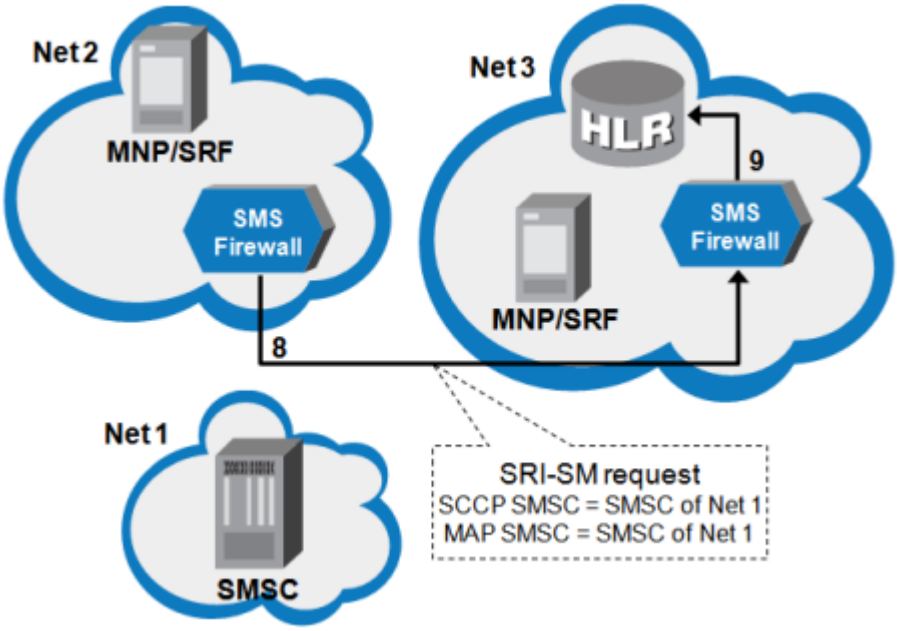


Figure 24: Republishing phase 3, republished SendRoutingInfoForSm request

In the fourth phase, the HLR responds to the republished SendRoutingInfoForSm request.

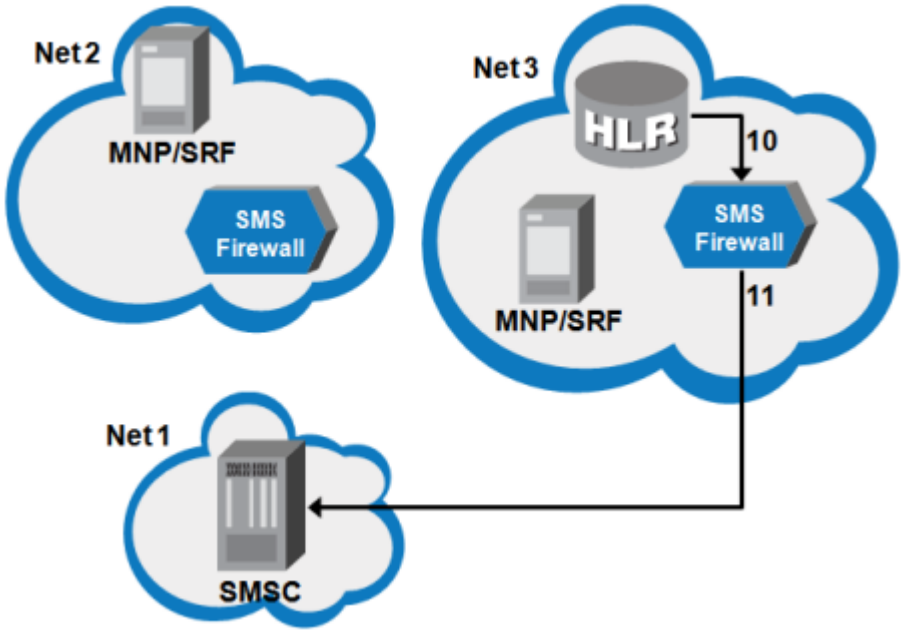


Figure 25: Republishing phase 4, republished SendRoutingInfoForSm response

In the fifth phase, the SMSC of Net 1 sends the subsequent MtForwardSm request toward the FWL of Net 3.

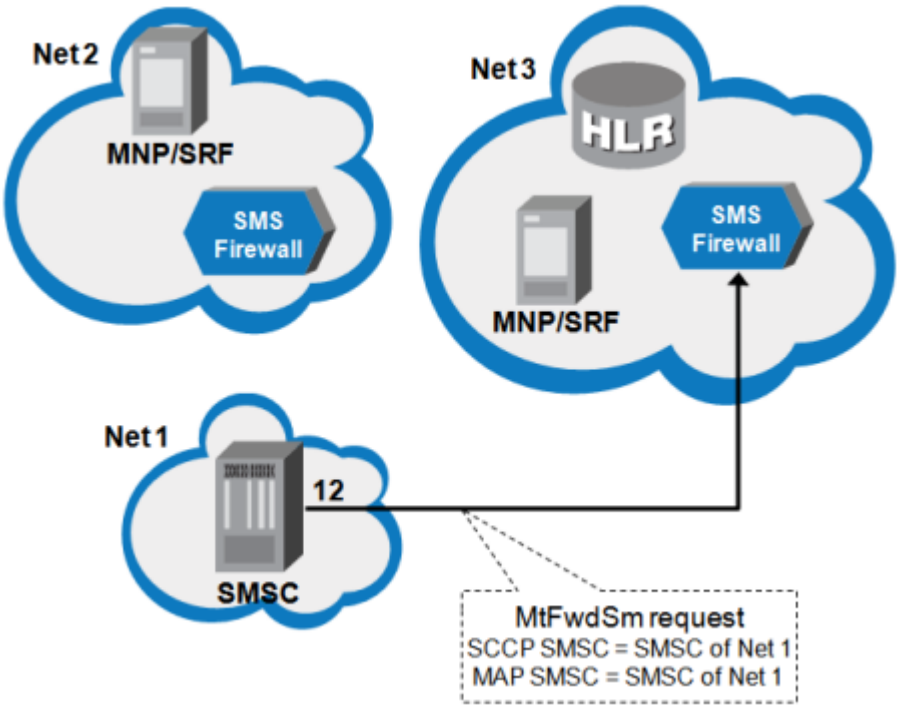


Figure 26: Republishing phase 5, MtForwardSm request

Refer to *How To Configure the FWL for MT Traffic* for information about configuring republishing.

4.9 Responding to MT Spoofing

The FWL enables you to customize the way it responds to each MT spoofing condition.

When the FWL detects MT spoofing in a message, it can discard the message and return a temporary or a permanent error to the originator; both of these options mean that the originator will know the message was blocked.

Alternatively, the FWL can block the message and return no error to the originator, which prevents the originator from knowing the outcome of the spoofing attempt. This option does not reveal the FWL to the originator, which can help prevent the originator from correctly guessing the network architecture.

The FWL can also allow the message to pass through the Mobile Messaging system; this mode enables you to log information to use while planning your FWL configuration, without the risk of blocking legitimate messages because the configuration is not yet complete.

Refer to *How To Configure the FWL for MT Traffic* for information about configuring the FWL's response.

4.10 Monitoring MT Spoofing

Counters provide information about the number of times the FWL has detected different types of MT spoofing.

Spoofing detected...	Counters
At the SCCP layer	• smsCntRecvMtSpoofedSccpSmscAddressCounter • countryRecvMtSpoofedSccpSmscAddressCounter • mobNetworkRecvMtSpoofedSccpSmscAddressCounter
At the MAP layer	• smsCntRecvMtSpoofedMapSmscAddressCounter • countryRecvMtSpoofedMapSmscAddressCounter • mobNetworkRecvMtSpoofedMapSmscAddressCounter
In the SRI-SM request	• smsCntRecvSriSmConflictingSmscAddressCounter • countryRecvSriSmConflictingSmscAddressCounter • mobNetworkRecvSriSmConflictingSmscAddressCounter
In the MtForwardSm request	• smsCntRecvMtConflictingSmscAddressCounter • countryRecvMtConflictingSmscAddressCounter • mobNetworkRecvMtConflictingSmscAddressCounter

To view the current value of a counter, execute the following command at a command prompt:

```
tp_walk <counter name>
```

4.11 How To Configure the FWL for MT Traffic

This section describes procedures to configure the FWL for MT traffic.

4.11.1 Customize Blocking of Unsolicited MtForwardSm Operations

The FWL will block unsolicited MtForwardSm operations that are not destined for inbound roamers. To customize the way the FWL blocks these operations, set the `tpconfig` attribute `firewallmtactionforunsolicitedmtfwdsm` in the semi-static configuration file:

Value	Description
blockwithtemporaryerror	Block and return a temporary error to the SMSC (by default, MAP error "absent subscriber")
blockwithpermanenterror	Block and return a permanent error to the SMSC (by default, MAP error "unknown subscriber")
blockwithnoresponse	Block and do not return a response to the SMSC (this is the default)
blockwithack	Block and return an ACK to the SMSC

To customize the temporary or permanent MAP error that the FWL returns to the SMSC, set the `tpconfig` attribute `mttemporarydiscarderrorformscorsgsn` or `mtpermanentdiscarderrorformscorsgsn` (respectively) to one of the following:

- unknownsubscriber
- absentsubscriber
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror
- unknownservicecentre
- sccongestion
- invalidsmeaddress
- subscribernotscsubscriber

4.11.2 Apply SRI-SM Response Rules to HLR Responses

The SRI-SM Response Rules should be used to process SendRoutingInfoForSm responses from the HLR. For information about the SRI-SM Response rule conditions and actions, refer to *SRI-SM Response Rule Set*.

4.11.3 Identify Ported-Out MSISDNs

To handle MNP, the FWL must identify ported-out MSISDNs and send SendRoutingInfoForSm requests for them back to the STP. To enable the FWL to identify these numbers, set the `tpconfig` attribute `firewallmnproutingnumberforownnetwork` to the routing number (RN) of the HPLMN in the semi-static configuration file. The RN is typically three digits, but can be up to 15 digits.

If a request does not contain an RN or contains an RN that is equal to the HPLMN's RN, the MSISDN belongs to the HPLMN. If a request contains an RN that is not equal to the HPLMN's RN, the MSISDN is a ported-out number.

The Mobile Messaging system only accepts RNs that start with zero. It assumes that:

- An RN is present if the SCCP CDPA contains a zero after the country code
- The MSISDN is ported-out if the SCCP CDPA starts with the local country code, followed by a zero, followed by digits that do not match the RN of the HPLMN (where the zero is considered to be part of the RN)

If `firewallmnproutingnumberforownnetwork` is not specified, the FWL will not send SendRoutingInfoForSm requests for ported-out numbers back to the STP.

4.11.4 Configure Republishing

Republishing is the act of reissuing a SendRoutingInfoForSm request to the HLR with some changes to the SCCP address (refer to *Republishing SRI-SM Requests*). The `tpconfig` attribute `firewallrepublishsrismnetworks` in the semi-static configuration file indicates the list of networks to which republishing applies. Set this attribute to a list of up to 10 networks, separated by commas and formatted as:

1. Two-letter country code (according to ISO 3166)
2. A hyphen
3. The name of a network defined in the MGR

> **Sample Republishing Configuration**
>
> If the country is the Netherlands and the KPN and Vodafone networks have been defined in the MGR, `firewallrepublishsrismnetworks` can be set to:
>
> ```
> nl-kpn,nl-vodafone
> ```

If `firewallrepublishsrismnetworks` is defined, the FWL:

- Assumes that all SendRoutingInfoForSm requests that are classified as suspect are possible candidates for republishing
- Republishes requests for SendRoutingInfoForSm responses that contain an IMSI that is associated with one of the networks in the list

If `firewallrepublishsrismnetworks` is not defined, the FWL does not republish SendRoutingInfoForSm requests.

4.11.4.1 Customize SCCP Address Modification

When the FWL is configured to republish SendRoutingInfoForSm requests, you can customize the way that the FWL modifies the SCCP address in the republished request using the `tpconfig` attribute `firewallrepublishsrismcdpasetsameasinitialsrism` in the semi-static configuration file. The value of this attribute determines the behavior as follows:

Value	CDPA of Initial SRI-SM from FWL	CDPA of Republished SRI-SM Request
false (default)	GT equal to MSISDN to be queried	Equal to CGPA from response to first SRI-SM request

Value	CDPA of Initial SRI-SM from FWL	CDPA of Republished SRI-SM Request
true	GT equal to MSISDN to be queried	GT equal to MSISDN to be queried

4.11.4.2 Enable Republishing for Trusted SMSCs

In addition to republishing for suspect SMSCs, the FWL can republish SendRoutingInfoForSm requests for trusted SMSCs. To enable this functionality, set the `tpconfig` attribute `firewallenablesrismrepublishingfortrustedsmsclist` to "true" in the semi-static configuration file.

In this case, the FWL will republish SendRoutingInfoForSm requests if:

- The SMSC that sent the original request is on the trusted SMSC list (`firewalltrustedsmsclist` attribute), and
- The MSISDN was ported from the HPLMN to a network that is on the republishing list (`firewallrepublishsrismnetworks` attribute)

The FWL will not republish requests from SMSCs that are trusted for an reason other than being on the trusted SMSC list (for example, if the OPC of the SendRoutingInfoForSm request was not the OPC of an STP).

4.11.5 Customize the Calling Party Address

You can configure the FWL to replace the SCCP calling party address (CGPA) in a suspect SendRoutingInfoForSm response to the originating SMSC with the GT of the HLR that sent the SendRoutingInfoForSm response to the FWL. This functionality makes the FWL's handling of suspect messages more transparent, because it makes the response seem as if it comes directly from the HLR.

To modify the CGPA, set the semi-static configuration attribute `firewallusehlraddressassccpcgpainsuspectsrismresponse` to "true". The FWL will replace the CGPA in the SendRoutingInfoForSm response with the GT of the HLR.

If `firewallusehlraddressassccpcgpainsuspectsrismresponse` is set to "false" (this is the default), the FWL will put its own GT in the CGPA of the SendRoutingInfoForSm response.

4.11.6 Customize the SMSC Address

You can configure the FWL to replace the SMSC address at the MAP layer of suspect MtForwardSm requests with its common address. This functionality prevents terminating firewalls from rejecting the MtForwardSm request sent by the FWL.

To modify the address, set the `tpconfig` attribute `firewallusecommonaddressinsuspectmtforwardsm` to "true" in the semi-static configuration file. The FWL will replace the SMSC address at the MAP layer with the value of the semi-static configuration attribute `commonaddress`.

If `firewallusecommonaddressinsuspectmtforwardsm` is set to "false" (which is the default), the FWL will not change the SMSC address at the MAP layer.

Note: For suspect MtForwardSm operations, the FWL always changes the SMSC address at the SCCP layer.

4.11.7 Customize the MSC Address

You can configure the FWL to replace the MSC and/or SGSN in a suspect SendRoutingInfoForSm response to the originating SMSC with a randomly selected GT. This functionality allows the FWL to be addressed on its PC with its own GT, as well as with a GT from a list that you specify.

Random selection of the address helps reduce the visibility of the FWL in the network and helps obscure the presence of Home Routing.

To modify the address, set the semi-static configuration attribute `firewallmscsgsnaddressinsuspectsrismresponse` to up to ten E164 addresses in international format (maximum 15 digits), separated by spaces. For example:

```
firewallmscsgsnaddressinsuspectsrismresponse="495800000099 495810000000 495820000000
 495830000000 495840000000 495850000000 495860000000"
```

The FWL will randomly select one of these addresses to replace the MSC and/or SGSN in the suspect response. To randomly select the GT, the FWL generates a random number, computes the modulus of the number of configured addresses, and uses the result to select the replacement address.

The addresses must be unique among all RTR/FWLs in the system. For example, if there are two RTR/FWLs, they cannot use any of the same addresses.

If `firewallmscsgsnaddressinsuspectsrismresponse` is not specified, the FWL uses its own GT for the MSC and/or SGSN. In this case, the FWL can only be addressed on its PC with its own GT.

The STP that is responsible for translating the GT to the FWL's PC must be configured to translate all addresses listed in `firewallmscsgsnaddressinsuspectsrismresponse` to the FWL's PC. This is also the case if there are multiple FWL instances in the system. For example, if the SCCP called party address (CDPA) GT of an MtForwardSm is equal to the fifth address listed in `firewallmscsgsnaddressinsuspectsrismresponse` on FWL instance 3, the GTT rule must translate the GT to the PC of FWL instance 3.

4.11.8 Whitelist SMSC GTs

You can create a whitelist of SMSC GTs for which the FWL will skip the MT spoofing check. This functionality enables you to fine-tune the MT traffic that the FWL considers to be trusted.

To enable this functionality:

1. In the MGR, go to **Routing ➤ Lists** and create a list of the GTs of the SMSCs for which the FWL should skip the spoofing check.
2. In the semi-static configuration file, set the `tpconfig` attribute `firewalltrustedsmsclist` to the name of the list.
3. In the MGR, go to **Firewall ➤ MT ➤ Properties**, select the name of the list created in the first step in the dropdown for **Trusted SMSC SCCP CgPA List**.

   If the SCCP CgPA GT address of an incoming SendRoutingInfoForSm exists in this **Trusted SMSC SCCP CgPA List**, then the SMSC is considered trusted and the corresponding MT Forward SM received with the same IMSI as returned in SendRoutingInfoForSm response is also considered trusted.

4.11.9 Whitelist Recipient IMSIs

You can create a whitelist of recipient IMSI ranges for which the FWL will skip the MT spoofing check. This type of whitelist is useful for subscribers who, through the use of Multi-SIM, have multiple IMSIs associated with one MSISDN. Whitelisting the IMSIs prevents blocking of the messages that these subscribers originate. However, because these messages will not be checked for MT spoofing, the whitelist should be used with care.

Note: The ranges specified in the recipient IMSI whitelist must not overlap with the ranges specified for IMSI scrambling.

4.11.10 Configure Rule-Based Release for MT-MT

To instruct the FWL to bypass the MT spoofing check for the SendRoutingInfoForSm operations of messages that are on the MT-MT routing path, use the SRI-SM Request and SRI-SM Response rules. For information about their conditions and routing actions, refer to *SRI-SM Request Rule Set* and *SRI-SM Response Rule Set*.

4.11.11 Configure the Response to MT Spoofing

Configure the ways that the FWL responds to various types of MT spoofing conditions in the following `tpcofig` attributes in the semi-static configuration file:

Spoofing condition	Description	Configure the response in...
Unknown SMSC address	The FWL received an SRI-SM or MtForwardSm with an SMSC address at the SCCP level that did not match any configured SMSC	firewallmtactionforunknownsccpaddress
Unknown MAP address	The FWL received an SRI-SM or MtForwardSm with an SMSC address at the MAP level that did not match any configured SMSC	firewallmtactionforunknownmapaddress
Conflicting addresses	The FWL received an SRI-SM or MtForwardSm with an SMSC address at the SCCP level that belongs to a different network from the SMSC address at the MAP level	firewallmtactionforconflictingaddress
Unsolicited MtForwardSm	The FWL received an MtForwardSm that could not be correlated to a previously received SRI-SM	firewallmtactionforunsolicitedmtfwdsm
MAP SMSC address spoofing detected	The FWL received an MtForwardSm with an SMSC address on the MAP level that belongs to a different network or country than the SMSC address on	firewallmtactionformapsmscaddressspoofing

Spoofing condition	Description	Configure the response in...
	the MAP level of the corresponding SendRoutingInfoForSm operation	
SCCP SMSC address spoofing detected	The FWL received an MtForwardSm with an SMSC address on the SCCP level that belongs to a different network or country than the SMSC address on the SCCP level of the corresponding SendRoutingInfoForSm operation	firewallmtactionforsccpsmscaddressspoofing

You can set each attribute to:

- discardwithtemporaryerror: Discard the message and return a temporary error to the originator
- discardwithpermanenterror: Discard the message and return a permanent error to the originator
- discardwithnoresponse: Discard the message and do not return an error to the originator (this is the default)
- pass: Allow the Mobile Messaging system to continue processing the message

Note: "Pass" is not supported for `firewallmtactionforunsolicitedmtfwdsm`.

4.11.12 Redirect TCAP Messages

When the STP intercepts an MtForwardSm operation that addresses an MSC rather than the FWL, it should redirect the operation to the FWL's virtual point code (VPC). To enable the STP to redirect complex TC-BEGIN, TC-CONTINUE, and TC-END dialogues to the same FWL instance in the network:

1. Set the `tpconfig` attribute `tcaprelaytccontinueonvpc` to "true" in the semi-static configuration file on each FWL instance.
2. On each FWL instance, define the MTP destinations for all other FWL instances in the `destination` entity.

If an inbound, non-home-routed MT message addresses the FWL itself, the FWL may transparently forward this message, potentially leading to a looping message in the SS7 network. Typically, non-home-routed MT messages never address the FWL, as they address the terminating MSC or SGSN (in the SCCP CdPA). Non-home-routed MT messages addressing the FWL would most likely be spoofed messages, from a spoofer (mis-)guessing the recipient's IMSI and MSC address. The potentially looping message can be discarded using one of the following solutions:

1. Route the message to a non-existent destination, using GTT rule(s) on the FWL.
2. Ensure that the STP recognizes the loop and discards the message (if possible).

Note: Defining an MTOR rule blocking messages addressing the MSC with one of the FWL's own GTs is not an option, because it does not cover the case of a CONTINUE'd TCAP dialogue, where the initial "empty" BEGIN message does *not* trigger the evaluation of the MTOR rules.

4.11.13 Configure Roaming Partners

To improve the granularity of FWL filtering, you should provision the countries, networks, and number ranges of operators with which you have a roaming agreement. Failure to do so reduces the FWL's ability to associate SMSC addresses with countries and/or operators, reducing the quality of spoofing checks.

To provision network number ranges:

1. In the MGR, go to **Environment ➤ Networks** and create a network entity.
2. Enter the E164 addresses of the SMSCs in the **Network Number Ranges** field.

4.11.14 Configure the Detection of Grey Routing

In order to detect and block grey routed MT messages, the Originator - SMSC Addr. Match condition in MTI rules should be used (refer section 4.6.2 for details about this rule condition).

For example, you can configure the option “Originator Country equals SMSC” or “Originator Network equals SMSC” as appropriate, and then negate the condition in a MTIR rule for which the routing action is set to either “Discard with no response” or “Discard with permanent error”. In this case the above MTIR rule will match any incoming MT message for which the Originator country/network does not equal the country/network of the corresponding SMSC address, i.e. a potentially grey routed message; as a result the message would be discarded either silently or with a NACK indicating a permanent error.

You can also use the options “Originator Country strictly equals SMSC” or “Originator Network strictly equals SMSC” along with a negated rule condition, in order to perform more stringent checking for grey routed MT messages.

4.11.15 Configure the GPRS Support Indicator

In case of the Home Routing scenario, if the '`GPRS support indicator`' is present in the incoming SRI-SM request, the RTR perform the following action for the outbound SRI-SM Request:

- If the SRI-SM request rule routing action is configured with "`Send to HLR`" and the MT Modifier is applied, where the SRI-SM Request can be modified, the RTR includes/excludes the GPRS support indicator in the MAP phase 2+ SRI-SM Request based on the semi static variable `gprssupportindicator`.
- The semi-static parameter `gprssupportindicator` does not have any impact on the outbound SRI-SM request which is transparently forwarded to the HLR. So, in this case the '`GPRS support indicator`' will be present in the outbound SRI-SM request.

4.12 Billing for MT Spoofing

On rejection of the incoming MT message due to spoofing, billing profile configured for the "Default Profile For MT Spoofing" in the Post-paid Billing Properties is used for creating the reject CDRs.

Only the FCDR format will be supported for reject CDR generated by the RTR.

On MT Spoofing, the reject CDRs can be created for the following actions:

1. Block with No Response
2. Block with Ack
3. Block Permanent

4.13 MAP Phase Translation in Home Routing

In home-routed scenario, the external SMSC does not have the actual MSC/SGSN address and hence it cannot determine the MAP Phase of Terminating MSC/SGSN which leads to more dialogues if there are "Application-Context-Name-Not-Supported" responses for the delivered MtForwardSm operation.

The FWL can be configured with the parameter **MAP Phase Translation** under the **Firewall ➤ MT ➤ Properties** in the MGR GUI to determine whether the MAP phase translation is to be supported or not for home routing scenarios.

This configuration provides the following three options:

S. No.	MAP Phase Translation option	FWL behavior
1.	No translation	With this configuration: **1.** FWL sends the outgoing MtForwardSm using incoming MAP Phase. **2.** Any error including Abort due to "Application-Context-Name-Not-Supported" received by the FWL is sent back to the external SMSC. **3.** External SMSC has the responsibility of retrying with lower MAP version.
2.	Translation based on App Context Not Supported Error	With this configuration: **1.** In Case the FWL receives the TCAP Abort due to "Application-Context-Name-Not-Supported" in response to MtForwardSm request, the FWL will try forwarding the outbound MtForwardSm using the supported map phase value received in the response from the other entity. **2.** If the message is not delivered, then the error received for outgoing MtForwardSm is converted to incoming MtForwardSm MAP phase format while sending the response back to the external SMSC. **3.** This is the default behavior of the FWL. **Note:** The RTR will perform the map-phase translation irrespective of whether the incoming message is received from a Japanese Operator or an Oversea Operator.
3.	Translation based on Destination MAP Phase and App Context Not Supported Error	With this configuration: **1.** FWL will check the MAP phase of the incoming MtForwardSm message. **2.** If the MAP phase is 1 or 2, then FWL will behave as defined for "No translation" operation.

S. No.	MAP Phase Translation option	FWL behavior
		3. If the MAP phase is 2+, FWL will convert and send the outgoing MtForwardSm using MAP Phase configured in Destination network (determined based on MSC/SGSN address). **4.** If the destination network is unknown, FWL uses the incoming MAP phase version. **5.** In case FWL received TCAP Abort due to "Application-Context-Name-Not-Supported" in response to MtForwardSm request, FWL tries to forward outbound MtFowardSm in decreasing order of map phase i.e. either 3>2 or 3>1. **6.** If the message is not delivered, then the error received for outgoing MtForwardSm is converted to incoming MtForwardSm MAP phase format while sending the response back to the external SMSC. **Note:** The RTR will perform the map-phase translation irrespective of whether the incoming message is received from a Japanese Operator or an Oversea Operator.

The following table specifies how the MAP phase translation is performed when the outgoing MtForwardSm is a success, failure or receives the TCAP abort with "Application-Context-Name-Not-Supported".

Incoming MAP Phase	Configured Destination Network MAP Phase	1st MtForwardSm delivery attempt	2nd MtForwardSm delivery attempt	3rd MtForwardSm delivery attempt	MAP-Phase translations	Response translation (while sending the response to the External SMSC)
3	3	Success				
3	3	Error				
3	3	App context not sup	Success		3 -> 2	
3	3	App context not sup	Error		3 -> 2	2 -> 3
3	3	App context not sup	App context not sup	Success	3 -> 2, 3 -> 1	
3	3	App context not sup	App context not sup	Error	3 -> 2, 3 -> 1	1 -> 3
3	2	Success			3 -> 2	
3	2	Error			3 -> 2	2 -> 3
3	2	App context not sup	Success		3 -> 2, 3 -> 1	

Incoming MAP Phase	Configured Destination Network MAP Phase	1st MtForwardSm delivery attempt	2nd MtForwardSm delivery attempt	3rd MtForwardSm delivery attempt	MAP-Phase translations	Response translation (while sending the response to the External SMSC)
3	2	App context not sup	Error		3 -> 2, 3 -> 1	1 -> 3
3	1	Success			3 -> 1	
3	1	Error			3 -> 1	1 -> 3
2	Don't care	Success			No translation, phase 2 used	No translation
2	Don't care	Error			No translation, phase 2 used	No translation
2	Don't care	App context not sup			No translation, required for 29.002 compliant behavior phase 2 used.	No translation required, application context error send towards SMSC.
1	Don't care	Success			No translation	No translation
1	Don't care	Error			No translation, phase 1 used	No translation

4.14 Preferred MT Destination in the Firewall

The **SRISM GPRS Support Indicator** in the **Firewall ➤ MT ➤ Properties** configuration, provides a finer control over the usage of the configuration parameter `enablegprssupportindicator` in the home routed scenario. The **SRISM GPRS Support Indicator** supports the following options:

- **Default**: With this configuration, the RTR transparently forwards the received value of the GPRS support indicator in the incoming SRI-SM request. When the SRI-SM request is being modified due to modifier or TCAP User Info addition then the inclusion/absence of the GPRS support indicator field is governed using `smsPropEnableGprsSupportIndicatorForSriSmRequest` parameter.
- **Off**: With this configuration, the RTR will not set the "GPRS support indicator" in SRI-SM request regardless of the inclusion/absence of GPRS support indicator in incoming SRI-SM. This behavior is only applicable when the MTOR action is configured as "Pass". However, in case the MTOR action is set as "Release", then the SRI-SM request is forwarded transparently.
- **On**: With this configurations, the RTR will set the "GPRS support indicator" in SRI-SM request regardless of the inclusion/absence of GPRS support indicator in incoming SRI-SM. This behavior is only applicable when the MTOR action is configured as "Pass". However, in case the MTOR action is set as "Release", then the SRI-SM request is forwarded transparently.

Note:

1. This parameter is only applicable when the Japanese MNP functionality is enabled in the RTR and the country determined from SCCP CDPA / MSISDN is same as the home country. If any of the mentioned conditions fail then RTR will behave as if the configured value of **SRISM GPRS Support Indicator** as **Default**.
2. In case of Japanese MNP if MNP action for first SRI-SM is forward, then second SRI-SM is sent. This second SRI-SM will never have the GPRS support indicator enabled.

By default, the RTR's preferred MT destination is the MSC. To change the preferred destination to the SGSN, set the `preferredmtdestination` parameter in the semi-static configuration file to "`sgsn`".

If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), the **Preferred MT Destination** in the Network configuration overrides the `preferredmtdestination` semi-static parameter. The **Preferred MT Destination** supports the following options (go to **MGR ➤ Environment ➤ Networks**):

- **MSC**
- **SGSN**
- **Use Global Setting**

If the **Preferred MT Destination** is set to **Use Global Setting**, the RTR's preferred MT destination is determined based on the `preferredmtdestination` semi-static parameter.

The RTR will always issue an MT message through the preferred path first. If delivery through this path fails, the RTR attempts to delivery through the alternative path (provided this is a valid option; refer to 3GPP TS 29.002 for more information).

The semi-static configuration parameter *firewallallowfallbacktosecdest* allows the fallback to secondary destination functionality to be applicable on the home-routed scenarios as well.

If the `firewallallowfallbacktosecdest` is set to true, on receiving both MSC and SGSN address in the SRISM response from the HLR, the RTR will return only one address in SRISM response to the external SMSC which is RTR's own GT address. On receiving the MtForwardSm, RTR will attempt delivery on preferred destination as configured in the terminating network (If the network is not configured preferred MT destination is determined based on the `preferredmtdestination` semi-static parameter). In case of failure, if **Enable Fallback to Secondary Dest** is set then RTR will re-attempt delivery on secondary destination.

In case of the following MtForwardSm errors only, re-attempt on secondary destinations is triggered:

- **FacilityNotSupported**
- **SystemFailure**
- **DataMissing**
- **UnexpectedDataValue**
- **UnidentifiedSubscriber**
- **SubscriberBusyForMT-SMS**
- **AbsentSubscriberSM**
- **MT FSM Timeout**

If **Enable Fallback to Secondary Dest** option is not set, then RTR will not attempt delivery to secondary destination and sends back error to the SMSC.

If **Preferred MT Destination** is configured as either MSC or SGSN in RTR, but in SRI-SM Response message RTR received only one destination address which is not same as the **Preferred MT Destination**,

then RTR will attempt delivery on secondary destination irrespective of the value configured for **Enable Fallback to Secondary Dest** in the recipient network settings.

In case of Home-Routing scenario, if the `firewallallowfallbacktosecdest` is set to false (this is the default behaviour), on receiving both MSC and SGSN address in the SRISM response from HLR, RTR will include its own GT address in both the MSC and SGSN addresses in the SRISM response towards external SMSC.

Chapter 5

Advanced Firewalling

Topics:

5.1 Introduction

The Mobile Messaging Firewall Advanced Filters (FAF) component enables you to block unsolicited messages that do not necessarily have a spoofed originator (MO spoofing) or a spoofed originating network (MT spoofing). FAF allows you to perform advanced message filtering such as:

- Detecting unsolicited messages based on their content, even when originators attempt to circumvent text filters (for example, by substituting "ca$h" for "cash")
- Detecting when a large number of messages with very similar content (called duplicates) are sent in a very short period of time
- Filtering messages that have specific Information Element IDs (IEIs) in their user data headers
- Filtering messages by matching regular expressions against message fields
- Detecting sudden increases in traffic from a single originator or from a range of originators (flooding)
- Detecting less sudden increases in traffic from a single originator, recipient, or SMSC (bulk sending)

5.2 Filter on Message Content

FAF can filter messages based on their content (user data). The filter conditions that operate on message content are:

- Content condition—Detects words or phrases that you provision in a filter list
- Duplicates condition—Detects messages that are very similar to a relatively large number of recent messages

5.2.1 Pre-Processing Message Content

Before FAF compares a message to the provisioned content and duplicates conditions, FAF pre-processes the content (user data) of the message and any filter lists that are used with the content conditions. Pre-processing reduces the resources that FAF's algorithms require to evaluate each message by reducing the amount of information contained in the message.

Pre-processing consists of three consecutive steps:

Name	Description	Input	Output	Used By
Tokenisation	Map similar characters to strings of "tokens" that you define in the normalisation table	The message content or an entry in a content condition list	A string of tokens that FAF generates based on the normalisation table	The content condition when its accuracy is set to "tokenise"
Normalisation	Collapse consecutive identical tokens into a single token	The output of the tokenisation step	A normalised string of tokens	The content condition when its accuracy is set to "normalise"

Name	Description	Input	Output	Used By
Featurisation	Group four consecutive tokens into a "feature"	The output of the normalisation step	The "signature" of the message	The duplicates condition

5.2.1.1 Tokenisation

During tokenisation, similar characters are mapped to the same token. The characters that are mapped to each token can be set using the semi-static configuration attribute `normalisationmap`.

Tokenisation automatically removes all of the following:

- Any character that is not in the mapping table
- Any character that is mapped to 0 (zero)
- White space

5.2.1.1.1 Format of the Tokenisation Map

The format of the `normalisationmap` attribute is a list of character groups separated by the new line character (`
`).

All characters of the first character group map to token 1, all characters of the second character group map to token 2, and so on. All characters that are not specified in the map are dropped during tokenisation.

Specify international characters using the decimal HTML encoding of the Unicode character. Refer to *http://www.utf8-chartable.de/unicode-utf8-table.pl?unicodeinhtml=dec* for character codes.

For example, assume that:

- Characters `a`, `A`, and a-umlaut (`ä`) should be mapped to token 1
- Characters `b`, `B`, and `6` should be mapped to token 2
- Character `C` should be mapped to token 3

The character code for a-umlaut is 228. Therefore, the configuration file should contain:

```
normalisationmap="aA&#228;&#10;bB6&#10;C"
```

Note: Changes to the tokenisation mapping will overwrite the FAF's default mapping. If you want to append to the default mapping table, ensure that you preserve it when you modify the `normalisationmap` attribute.

To view the current tokenisation mapping on a FAF system, execute:

```
tp_walk fafPropertiesNormalise
```

5.2.1.1.2 Default Tokenisation Map

The FAF's default mapping of characters to tokens is:

```
normalisationmap="0oO&#246;&#214;&#10;1iIlL!\/&#10;2zZ&#10;3eE&#10;4aA&#228;&#196;
&#10;5sS&#223;&#10;6&#10;7tT&#10;8bB&#10;9gG&#10;cC&#10;dD&#10;fF&#10;hH&#10;
jJ&#10;kK&#10;mM&#10;nN&#10;pP&#10;Q&#10;rR&#10;uU&#252;&#220;&#10;vV&#10;
wW&#10;xX&#10;yY"
```

This translates to:

Token	Characters
1	0, o, O, ö, Ö
2	1, i, I, l, L, !, \, /
3	2, z, Z
4	3, e, E
5	4, a, A, ä, Ä
6	5, s, S, $, ß
7	6
8	7, t, T
9	8, b, B
10	9, g, G
11	c, C
12	d, D
13	f, F
14	h, H
15	j, J
16	k, K
17	m, M
18	n, N
19	p, P
20	q, Q
21	r, R
22	u, U, ü, Ü
23	v, V
24	w, W
25	x, X
26	y, Y

5.2.1.1.3 Sample Tokenisation Maps

A sample tokenisation map that includes French characters is:

```
normalisationmap="0oO&#246;&#214;&#244;&#212;&#10;1iIlL!\/&#238;&#206;&#239;
&#207;&#10;2zZ&#10;3eE&#233;&#201;&#232;&#200;&#234;&#202;&#235;&#203;
&#10;4aA&#228;&#196;&#226;&#194;&#10;5sS&#223;&#10;6&#10;7tT&#10;8bB&#10;
9gG&#10;cC&#231;&#199;&#10;dD&#10;fF&#10;hH&#10;jJ&#10;kK&#10;mM&#10;nN&#10;
pP&#10;qQ&#10;rR&#10;uU&#252;&#220;&#250;&#218;&#251;&#219;&#10;vV&#10;wW&#10;
xX&#10;yY&#255;&#159;"
```

A sample tokenisation map that includes Arabic characters is:

```
normalisationmap="0oO&#246;&#214;&#1569;&#10;1iIlL!\/&#1575;&#1573;
&#1571;&#1570;&#10;2zZ&#1572;&#10;3eE&#1574;&#10;4aA&#228;&#196;&#1576;&#10;
5sS&#223;&#1578;&#1577;&#10;6&#1579;&#10;7tT&#1580;&#10;8bB&#1581;&#10;9gG&#1582;
&#10;cC&#1583;&#10;dD&#1584;&#10;fF&#1585;&#10;hH&#1586;&#10;jJ&#1587;&#10;
kK&#1588;&#10;mM&#1589;&#10;nN&#1590;&#10;pP&#1591;&#10;qQ&#1592;&#10;rR&#1593;
&#10;uU&#252;&#220;&#1594;&#10;vV&#1601;&#10;wW&#1633;&#1602;&#10;xX&#1634;
&#1603;&#10;yY&#1635;&#1604;"
```

A sample tokenisation map that includes Russian (Cyrillic) characters is:

```
normalisationmap="&#x410;&#x430;&#10;0Oo&#246;&#214;&#10;6&#x411;&#x431;
&#10;1IiLl!\/&#10;&#x412;&#x432;&#10;2Zz&#10;&#x413;&#x433;&#10;&#x414;&#x434;
4Aa&#228;&#196;&#10;3Ee&#x415;&#x435;&#x417;&#x437;&#10;5Ss&#223;&#10;&#x416;
&#x436;6&#10;7Tt&#10;&#x418;&#x438;8Bb&#10;&#x419;&#x439;9Gg&#10;&#x41a;&#x43a;
Cc&#10;&#x41b;&#x43b;Dd&#10;&#x41c;&#x43c;Ff&#10;&#x41d;&#x43d;Hh&#10;&#x41e;
&#x43e;Jj&#10;&#x41f;&#x43f;Kk&#10;&#x420;&#x440;Mm&#10;&#x421;&#x441;Nn&#10;
&#x422;&#x442;Pp&#10;&#x423;&#x443;Qq&#10;&#x424;&#x444;Rr&#10;&#x425;&#x445;
Uu&#252;&#220;&#10;&#x426;&#x446;Vv&#10;&#x427;&#x447;Ww&#10;&#x428;&#x448;
Xx&#10;&#x429;&#x449;Yy&#10;&#x42a;&#x44a;&#10;&#x42b;&#x44b;&#10;&#x42c;
&#x44c;&#10;&#x42d;&#x44d;&#10;&#x42e;&#x44e;&#10;&#x42f;&#x44f;"
```

5.2.1.1.4 Tokenisation Examples

These examples of tokenisation are based on the default tokenisation map:

1. The string `many dollars` is tokenised into:

   ```
   17,5,18,26,12,1,2,2,5,21,6
   ```

   After tokenisation, the following strings are equal:

   ```
   many dollars
   M4NyD011Ar5
   ```

2. The string `E l l e n` is tokenised into:

   ```
   4,2,2,4,18
   ```

   After tokenisation (and removal of white spaces), the following strings are equal:

   ```
   E l l e n
   Ellen
    E llen
   ```

5.2.1.2 Normalisation

After tokenisation, FAF applies normalisation, which collapses multiple identical tokens into a single token.

5.2.1.2.1 Normalisation Examples

Some examples:

1. In the first example in *Tokenisation*, two token 2s appear consecutively (representing the two letter Ls in dollar). During normalisation, they are collapsed into a single token 2, so the string becomes:

   ```
   17,5,18,26,12,1,2,5,21,6
   ```

   After normalisation, the following strings are equal:

   ```
   many dollars
   maany dolar$s
   ```

2. In the second example in *Tokenisation*, the normalised result is:

   ```
   4, 2, 4, 18
   ```

The following strings are all mapped to the same token:

```
elen
elllen
e llen
 e l l e n n
```

5.2.1.3 Featurisation

After normalisation, the FAF applies featurisation to the normalised string of tokens to create features. A feature is a combination of four consecutive tokens.

During featurisation, the FAF translates a string of tokens into a set of features by considering each substring of four tokens as one feature. A feature can occur multiple times in a string.

While the order of tokens in a string is important, a set of features has no "order". Therefore, featurisation helps the FAF's algorithms match text fragments, independent of their order.

5.2.1.3.1 Featurisation Example

The example string `"many dollars"` is tokenised into:

```
17,5,18,26,12,1,2,2,5,21,6
```

Then, the tokens are featurised as follows:

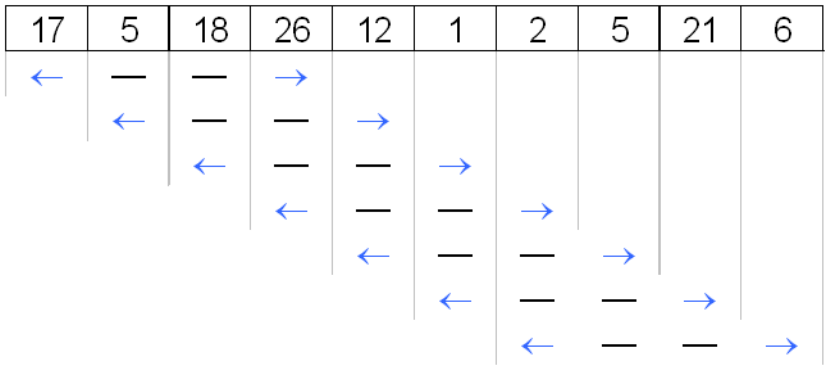


Figure 27: Featurisation example

The example string contains seven features, which are in an arbitrary order:

```
17-5-18-26
2-5-21-6
26-12-1-2
1-2-5-21
12-1-2-5
5-18-26-12
18-26-12-1
```

5.2.2 Content Filtering

The FAF's content condition detects whether the content of a configured message field matches a word, phrase, or regular expression in a provisioned list. If the content of the field matches at least one of the items in the list, the condition returns "true" for the message being evaluated. The accuracy of word or phrase detection is configurable, ranging from an exact match to a match after normalisation.

The content condition is most commonly used to evaluate the content of the user data (message content) field.

After the FAF identifies a match, it can modify the content of the field. For example, the FAF can replace a word or words in the user data with `'X'` characters. Note that the **Modify** option is relevant only for the user data field and should be set to “None” for all other message fields.

The FAF supports up to **100** instances of the content condition.

Note: In the FAF MIB and license file, the content filter is referred to as the string filter.

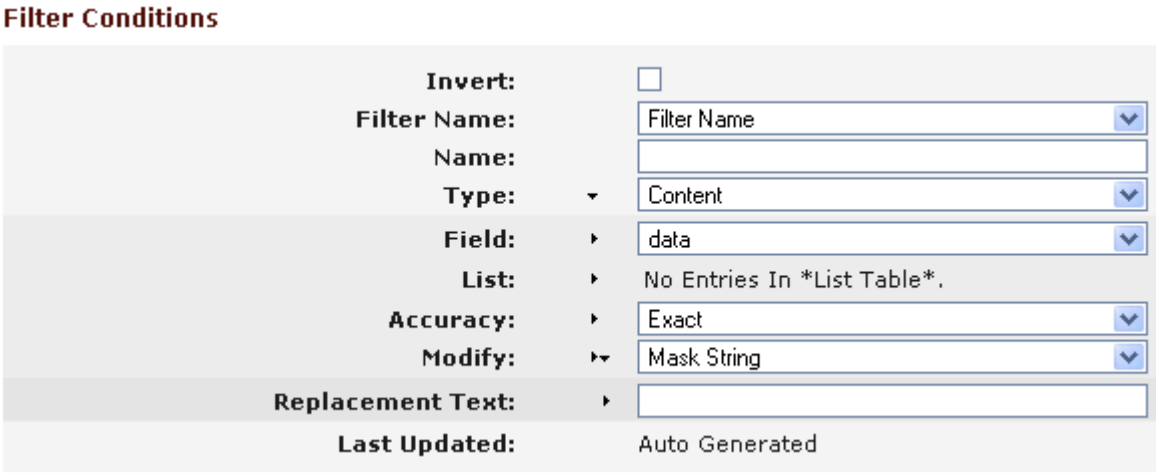


Figure 28: Content condition MGR configuration

5.2.2.1 Content Condition Examples

Detect Combinations of Words

You can use two or more content conditions to detect combinations of words. For example, assume you want to detect and block messages that contain the words "free" and "money". However, you do not want to block messages that contain only "free" or only "money". To accomplish this:

1. Ensure the EC application for the FAF is configured to send the data message field to the FAF
2. Create two lists: one containing "free", the other containing "money"
3. Create two filters
4. Open one filter and add a content condition
5. For the **Field** parameter, select data
6. For the **List** parameter, select one of the lists that you created
7. Open the other filter and add a content condition
8. For the **List** parameter, select the other list that you created
9. Ensure that the filter with the higher priority has an **Action** of "continue"

If both filters return "true", then both words are present in the message.

Detect Numeric Originators

To use the content condition to detect numeric originators:

1. Ensure the EC application for the FAF is configured to send the originator address message field to the FAF
2. To detect numeric originators with international numbers, create a list that contains the following regular expression:

   ```
   ^[+][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]$
   ```

   To detect numeric originators with national numbers, create a list that contains the following regular expression:

   ```
   ^[N|U][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]$
   ```

3. Create a filter
4. Add content condition to the filter
5. For the **Field** parameter, select "originator address"
6. For the **List** parameter, select the list that you created
7. For the **Accuracy** parameter, select "regular expression"

Detect Short Code Originators

To use the content condition to detect short code originators:

1. Ensure the EC application for the FAF is configured to send the "originator address" message field to the FAF
2. Create a list that contains the following regular expression:

   ```
   ^[N|U][1-9][0-9][0-9][0-9][0-9][0-9]$
   ```

3. Create a filter
4. Add a content condition to the filter
5. For the **Field** parameter, select "originator application"
6. For the **List** parameter, select the list that you created
7. For the **Accuracy** parameter, select "regular expression"

Detect protocol ID field

To use the content condition to detect the message having configured protocol id. Assume you want to detect messages that contain protocol id 50.

To accomplish this:

1. Ensure the EC application for the FAF is configured to send the message field (protocolId) to the FAF
2. Create list with either a single specific value (50) or a set of possible values including the desired value (50) of protocol id.
3. Create one filter ‘F’.
4. Open filter ‘F’ and add a content condition.
5. For the **Field** parameter, select “protocolId”.
6. For the **List** parameter, select one of the lists that you created.

7. For the **Accuracy** parameter, select "Exact" and for the **Modify** parameter, select "None".
8. Select the **Whole Words Match** option.

5.2.2.2 Content Condition Required Message Fields

The message field that you specify in the content condition's **Field** parameter must be sent to the FAF. To ensure that it is, select this message field in the EC application that you create for the FAF.

5.2.2.3 Content Condition Traps

The content condition does not generate SNMP traps.

5.2.3 Duplicates Filtering

The FAF's duplicates condition detects messages that are very similar to a relatively large number of recent messages. Positive detection returns true.

The duplicates condition measures similarity by comparing a number of features (see *Pre-Processing Message Content*). If the similarity is set to 100%, exact matching is performed.

The duplicates condition performs cluster detection, through which it attempts to detect groups of similar messages that are large enough to be worthy of tracking. If it detects such a group, the duplicates condition creates a cluster for this group of messages and starts to track them accurately (called cluster matching).

The FAF supports up to **10** instances of the duplicates condition.

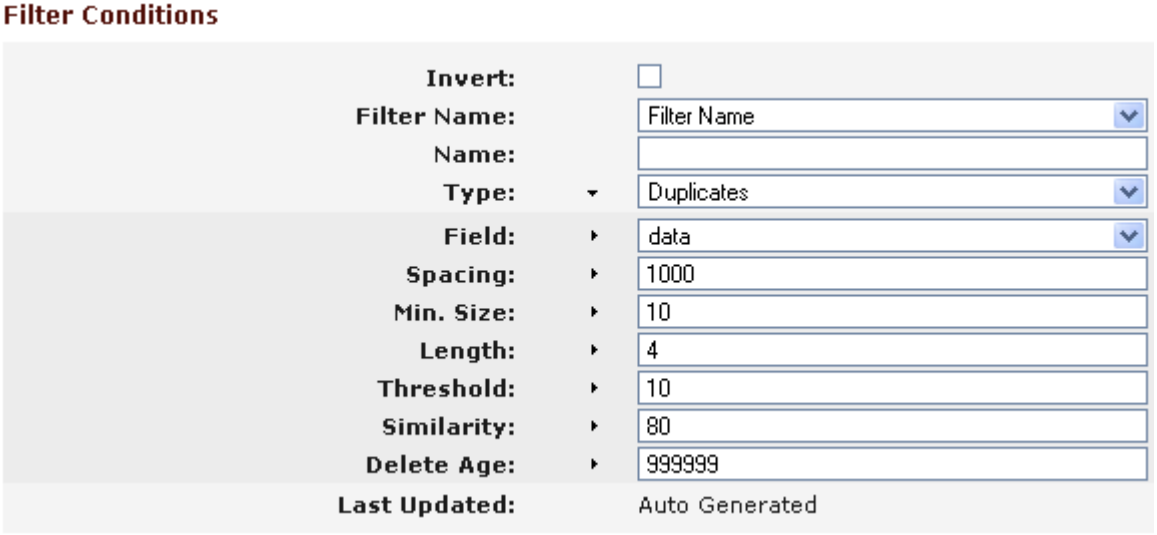


Figure 29: Duplicates condition MGR configuration

5.2.3.1 Detecting Duplicates Clusters

The duplicate condition considers the entire history of features that are recorded. A cluster is created when enough features in the message have been recorded in the history and the appearance frequency exceeds the configuration.

The creation of clusters is related to the configuration, the traffic load, and the traffic pattern. The configuration impacts clusters as follows:

- **Similarity**—The lower the similarity, the more clusters can be created. The similarity is calculated based on how many features in a new incoming message were previously seen in a different message. For example, assume the new incoming message contains 10 features, and 8 of the 10 features are found in the old message; this means the similarity is 8/10 = 80%.

  Note: If the similarity is set to 100%, the **Length** parameter will be ignored and it will detect duplicate messages with any length.

- **Length**—Total number of features in the message. If the message is short, less features can be generated from the message. The length should be big enough to avoid matching commonly used short messages like `"Hello!"`.
- **Minimum Size**—Number of messages that satisfy the similarity, before a cluster is created for these group of similar messages. The smaller the minimum size is, the more clusters can be created.
- **Spacing**—Number of messages between similar messages. If more messages than the spacing are found between two messages, the messages are not considered duplicates. For example, if a user sends `"hello"` twice and there are many other messages in between, it is not a duplicate attack. Set this field to a value that is big enough if your traffic is high and a duplicate attack is likely to happen.
- **Delete Age** (duration of a cluster being stored in the FAF)—The longer the delete age, the more clusters can be created.

The more messages there are, the more patterns can be found; consequently, there will be more clusters. Some common patterns, such as very frequently used words like `"where"`, increase the chance of cluster creation.

5.2.3.2 Duplicates Cluster Matching

The process of matching duplicates clusters is:

1. When the duplicates condition evaluates a message, it compares the message to all existing clusters.
2. If the message matches one cluster, the process is finished and the condition returns "true".
3. If the message does not match any cluster, the condition compares the message against the feature pool and the message history.
4. The condition adds the message and its features to the history.
5. If a match is found or if the number of duplicates has not yet reached the limit, the process is finished and the condition returns "false".
6. If a match is found and the number of duplicates has reached the limit, the condition creates a new cluster, the process is finished, and the condition returns "true".

Clusters expire (that is, are forgotten) if no new duplicates of the messages in the cluster are found during a configurable period of time.

5.2.3.2.1 Duplicates Cluster Alerts

When the number of clusters that the FAF is currently tracking exceeds a configurable threshold (by default, 300), the FAF will issue the `clustersInUseAlert` SNMP trap. The trap will indicate the number of clusters being tracked and the warning level:

- `warningThreshold`—The number of clusters is above the configured threshold
- `limitationReached`—The number of clusters has reached the maximum that the FAF supports (500)

The FAF issues the `clustersInUseAlertClean` trap when the number of clusters is 50 less than it was when the `clustersInUseAlert` trap was issued.

To check the number of clusters being tracked at any given time, execute the following at a command prompt on a FAF system:

```
tp_walk fafPropertiesDupsClustersInUse
```

To check whether the number of clusters is below or above the configured threshold, or at the maximum limit, by executing:

```
tp_walk fafPropertiesDupsClusterStatus
```

5.2.3.3 Limitations of Duplicates Cluster Tracking

The FAF stores historic information using memory and evaluates the history using CPU. Therefore, to prevent the FAF from using too much memory and CPU, there is a 500-cluster limitation. The more clusters that are created, the slower the FAF becomes and the more memory and CPU it will use.

Each duplicates condition can track up to 65,536 messages at one time. Each new message will overwrite an old message in this count.

The FAF determines message similarity by processing each message into features (refer to *Pre-Processing Message Content*), which are stored in the FAF's feature pool. The feature pool only remembers the message ID of the last match; therefore, if more than one message contains the same feature, the duplicates condition only remembers the last message that contained that feature. In some cases, this may prevent duplicates matching.

5.2.3.3.1 Troubleshooting Duplicates Cluster Tracking

There are several considerations to note when you are troubleshooting the duplicates condition.

One is that when MSCs receive duplicate messages from a single originator, they load share the traffic over STPs, which in turn load share the traffic over the RTRs that communicate with individual FAF servers in the Mobile Messaging system. This load sharing enlarges the average time between each duplicate message, and can therefore cause the FAF to not recognize duplicates because, by the time a potentially matching message reaches the FAF, the FAF has already overwritten the message history of the oldest matching message.

Another consideration is that because the duplicates condition only remembers the last message that contained a given feature, duplicates may not match because other messages in between them have updated the feature history. For example, duplicate messages D1 and D2, and non-duplicate message N1, all contain feature F1. If the messages arrive in the order D1, N1, D2, then D2 will not match D1 because the last instance of F1 that the FAF remembers was in N1.

5.2.3.3.2 Duplicates Condition and Inaccuracy

The duplicates condition is a statistical condition and therefore introduces a certain degree of inaccuracy that may rarely cause the following behaviour:

- Detection of duplicates that are not exact matches (unless a similarity of 100% is configured)
- Delayed detection of a cluster due to overlapping features of non-duplicate messages between duplicated messages
- Failure to detect exact duplicates because the cluster is started with a similar, but not identical, message (the duplicate message will not cluster-match)

5.2.3.4 Duplicates Condition Required Message Fields

For the duplicates condition, the external condition (EC) application must be configured to send the following message fields to the FAF:

- Originator address
- Originator IMSI
- User data
- SMSC address
- MSC address

5.2.3.5 Duplicates Condition Traps

The duplicates condition may issue the following SNMP traps:

- `clusterStarted`—A new cluster was started/created.
- `clusterThreshold`—A cluster has grown beyond the configured size threshold; depending on the configuration, further duplicate messages may be blocked.
- `clusterExpired`—A cluster expired (the cluster is not matched for longer than the delete age).
- `clustersInUseAlert`—The number of clusters that the FAF is tracking (`fafPropertiesDupsClustersInUse`) crossed the configured threshold (`dupsclustertrapwarningthreshold` in the semi-static configuration file).
- `clustersInUseAlertClean`—The number of clusters that the FAF is tracking is 50 less than when the `clustersInUseAlert` was issued.

Refer to the NewNet Mobile Messaging SNMP Trap Reference Guide for more information about these traps.

5.2.3.6 Troubleshooting the Duplicates Condition

Duplicates conditions can increase the complexity of the FAF's internal state. To investigate an instance of the duplicates condition, monitor the SNMP table `FAFDupsCountTable`. Consult the FAF MIB for a description of the columns of this table.

The following table describes some symptoms that a duplicates condition instance can show and some possible remedies.

Symptom	**Action**
No cluster created.	Reduce the **Similarity** value and/or increase the **Spacing** value.
Cluster created too late.	Reduce the **Min. Size** value.
Cluster created, but no action is taken.	Reduce the **Threshold** value.
Cluster expires too quickly.	Increase the **Delete Age** value.

Symptom	Action
Too many clusters.	• Increase the **Similarity** value. • Increase the **Length** value. • Increase the **Min. Size** value. • Reduce the **Delete Age** value. • Reduce the **Spacing** value.

5.3 Filter on Message Fields

FAF can filter messages based on the value of message fields. FAF uses regular expressions to evaluate the field values.

FAF can also filter messages based on specific Information Element IDs (IEIs) that are present in their user data header field.

5.3.1 Enhanced Messaging (EMS) Filtering

The FAF's enhanced messaging (EMS) condition detects messages that contain specific Information Element IDs (IEIs) in the user data header (UDH) or specific protocol id values. If the UDH of a message contains the selected IEI(s) or if the message contains a protocol id that matches with any of the configured **Protocol Id Values**, the filter condition will return "true". If the **Protocol Id Values** parameter is left blank, then the filter condition will match any message protocol id value.

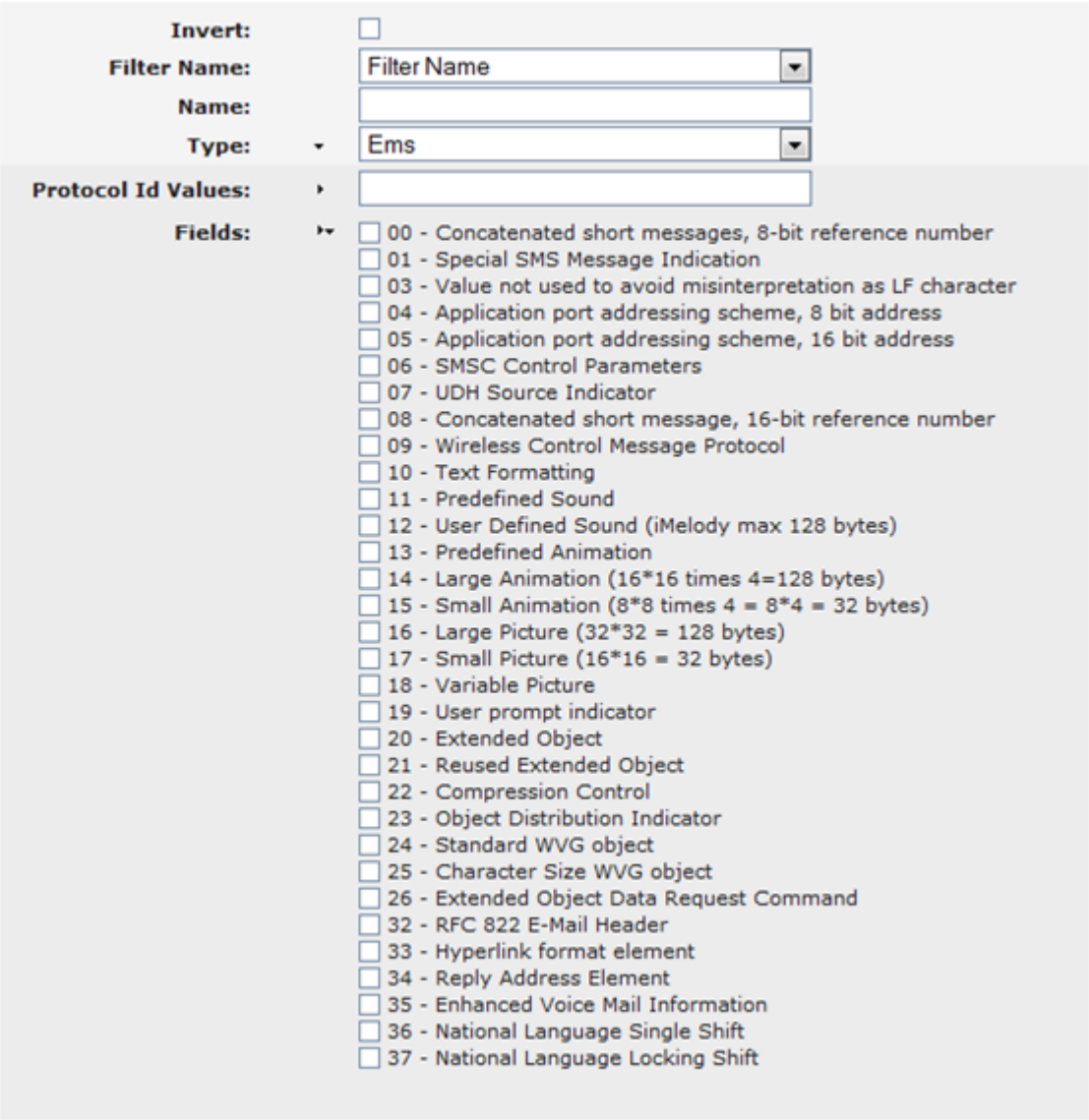
The EMS condition uses a logical OR operation; therefore, if you select multiple IEIs and also configure certain protocol id values for one EMS condition and the message contains any of the selected IEIs OR any of the configured protocol ids, the condition will return "true".

In the case of the application port addressing scheme IEIs, FAF can also verify that the source and destination ports in these IEIs match provisioned ports. This functionality can be used, for example, to detect and block WAP push messages, which use 16-bit source port 9200 (decimal) and destination port 2948 (decimal).

Refer to chapter 9.2.3.24 of the 3GPP 23.040 specification for a description of EMS IEIs.

The FAF supports up to **100** instances of the EMS condition.

Figure 30: EMS condition MGR configuration



5.3.1.1 EMS Condition Required Message Fields

For the EMS condition, the external condition (EC) application must be configured to send the user data header message field and, if the **Protocol Id Values** parameter is not blank, the "protocolId" message field as well, to the FAF.

5.3.1.2 EMS Condition Traps

The EMS condition does not generate SNMP traps.

5.3.2 Expression Filtering

The FAF's expression condition can evaluate message fields according to a regular expression. A single expression can contain nested expressions, enclosed in parentheses.

For example:

```
(messagetype > 1 && messagetype < 4)
```

or

```
(messagetype == 0 && totalsegments >= 4)
```

You can use the expression condition to assign values to external attributes on the ECI interface (using `eciattribute` fields).

FAF's test expression condition can be used to:

- apply filter on messages of certain message type
- have conditional evaluation based on set ECI attributes
- set a limit on the number of segments of a concatenated SMS

The FAF supports up to **100** instances of the expression condition.

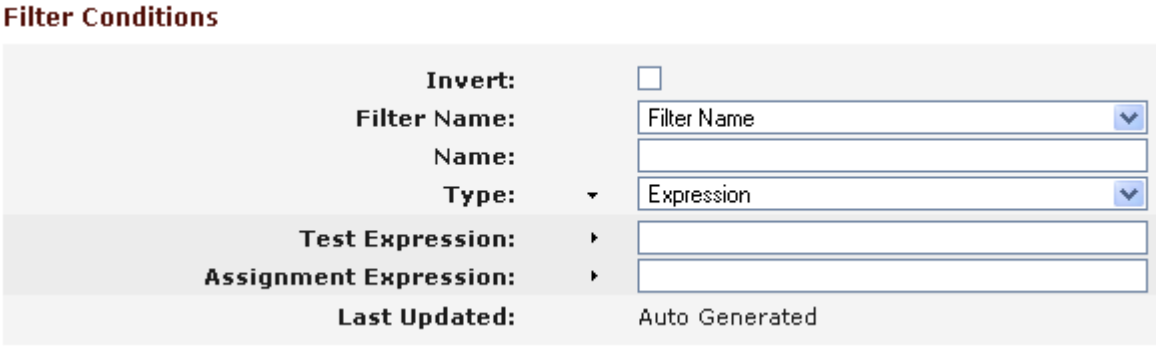


Figure 31: Expression condition MGR configuration

5.3.2.1 Expression Condition Required Message Fields

If the expression condition includes `messagetype` and/or `totalsegments`, then the external condition (EC) application must be configured to send the ECI message type and/or `cmTotalSegments` message field to the FAF.

5.3.2.2 Expression Condition Traps

The expression condition does not generate SNMP traps.

5.4 Filter on Traffic Volume

FAF can filter messages based on trends in traffic volume that may indicate spamming and/or cause network congestion.

5.4.1 Flooding Filtering

The FAF's flooding condition detects sudden increases in traffic from the same originator(s). Positive detection returns the result "true".

The flooding condition continuously monitors the short-term and long-term traffic averages (in messages per second) per originator (or range of originators). If the short-term traffic average exceeds the long-term traffic average by a configured margin for a configured period of time, flooding is detected and the condition returns "true".

The flooding condition remains in effect until the short-term traffic average drops below the level at which flooding was initially detected. While the flooding condition is in effect, the FAF does not update the long-term traffic average.

The FAF supports up to **10** instances of the flooding condition.

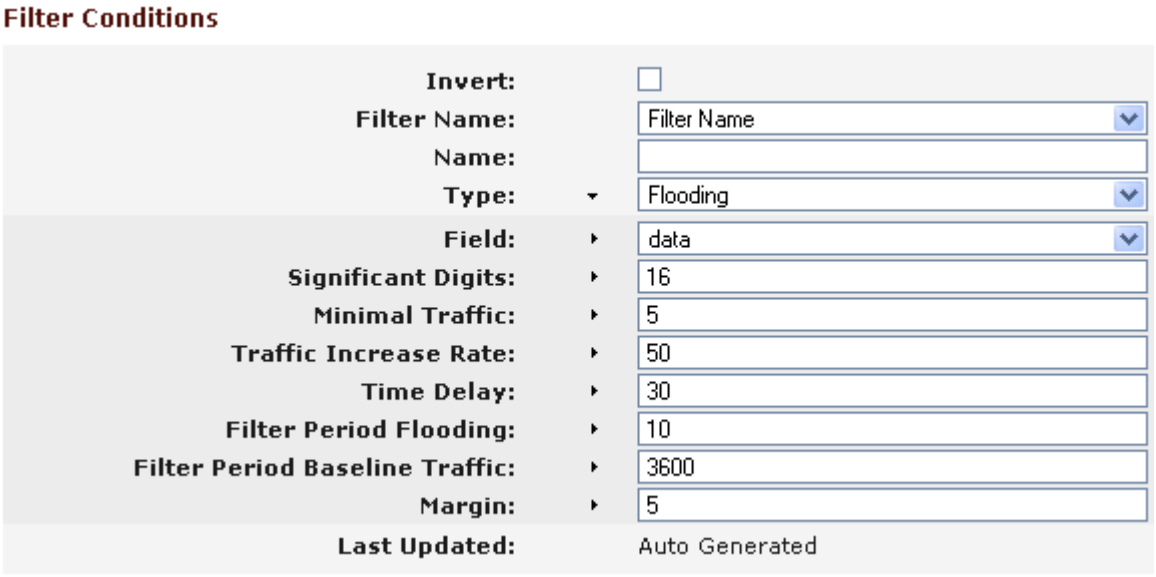


Figure 32: Flooding condition MGR configuration

5.4.1.1 Detecting Flooding

The short-term traffic average (`stta`) and long-term traffic average (`ltta`) are calculated as follows:

```
stta = number of messages received in the last X seconds / X seconds
ltta = number of messages received in the last Y seconds / Y seconds
```

Where `X` is the value of the **Filter Period Flooding** parameter and `Y` is the value of the **Filter Period Baseline Traffic** parameter.

The FAF detects flooding if the following condition evaluates to true for the configured period of time:

```
stta > ltta * (1 + rate/100) + threshold
```

Where `rate` is the value of the **Traffic Increase Rate** parameter and `threshold` is the value of the **Minimal Traffic** parameter.

The short-term and long-term traffic averages are first-order conditions; both have a configurable response time.

The FAF creates a tracking record for each encountered group of significant digits (**Significant Digits** parameter), if the record does not already exist. A maximum of 10,000 simultaneous tracking records can exist at one time. Every second, the FAF checks each tracked group to evaluate if both the long-term and short-term traffic are below margin/100 messages per second. If they are, the FAF deletes the tracking record for that number group.

Note: To prevent spurious flooding detection after the FAF is started or restarted, the FAF disables flooding detection for a time period (the long-term filter range plus the short-term filter range) after the first message has been received. This method allows the condition parameters to settle on stable values.

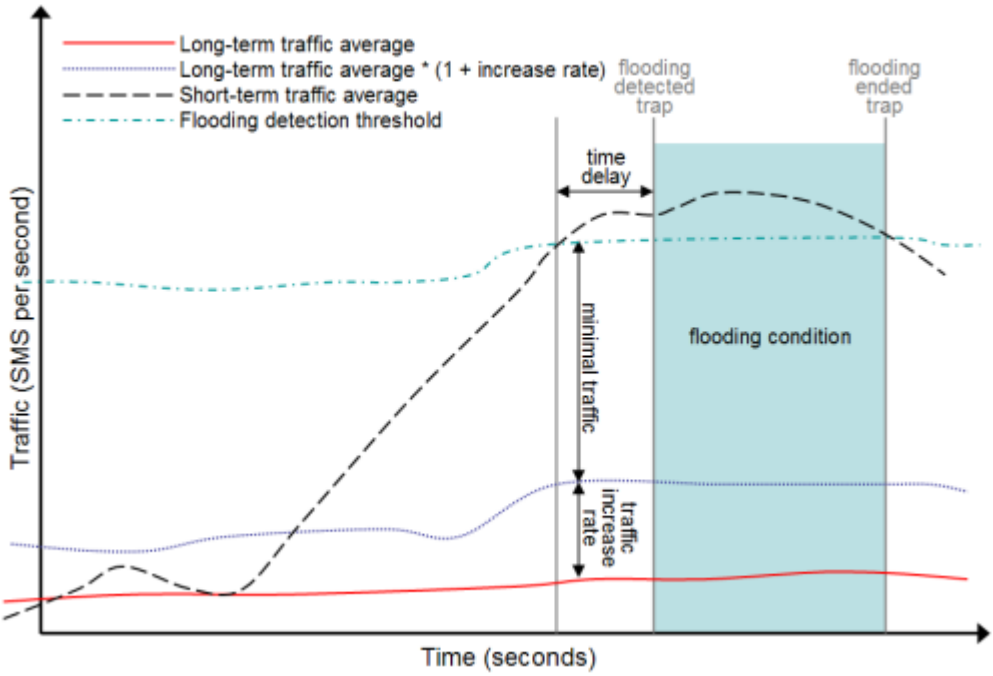


Figure 33: Flooding detection

5.4.1.2 Flooding Condition Example

In this example, the FAF flooding condition parameters are set as follows:

- Type—Flooding
- Field—orig
- Significant Digits—10
- Minimal Traffic—5 messages per second
- Traffic Increase Rate—100%
- Time Delay—5 seconds
- Filter Period Flooding—10 seconds
- Filter Period Baseline Traffic—120 seconds
- Margin—5 messages per 1000 seconds

A single originator sends 1 message per second for 150 seconds. Then, the originator starts sending 10 messages per second.

Until the 150th second afterward, the short-term and long-term traffic average are both 1 message per second. Flooding is not detected because the resulting condition is false:

```
1 > 1 * (1 + 100 / 100) + 5
```

At the 155th second:

```
stta = (5 * 1 + 5 * 10) / 10 = 5.5
ltta = (115 * 1 + 5 * 10) / 120 = 1.375
```

Flooding is still not detected because the resulting condition is false:

```
5.5 > 1.375 * (1 + 100 / 100) + 5
```

At the 158th second:

```
stta = (2 * 1 + 8 * 10) / 10 = 8.2
ltta = (112 * 1 + 8 * 10) / 120 = 1.6
```

Flooding is detected at this second because the resulting condition is true:

```
8.2 > 1.6 * (1 + 100 / 100) + 5
```

FAF waits 5 seconds (because the time delay is set to 5); if the the flooding condition persists, then FAF starts blocking all messages from the originator.

FAF continues to calculate the short-term traffic average; when it falls below 8.2, the flooding condition becomes false and traffic from the originator is allowed again. The long-term traffic average (1.6) remains constant while the flooding condition is true.

5.4.1.3 Flooding Condition Required Message Fields

For the flooding condition, the external condition (EC) application must be configured to send the message field specified in the flooding condition's **Field** parameter to the FAF.

5.4.1.4 Flooding Condition Traps

The flooding condition may issue the following SNMP traps:

- `floodingStartDetected`—Traffic from a foreign network has increased significantly.
- `floodingEndDetected`—Traffic from a foreign network has normalised (clears the `floodingStartDetected` trap).

Refer to the NewNet Mobile Messaging SNMP Trap Reference Guide for more information about these traps.

5.4.1.5 Troubleshooting the Flooding Condition

Flooding conditions can increase the complexity of the FAF's internal state. To investigate an instance of the flooding condition, monitor the SNMP `FAFFloodCountTable`. Consult the FAF MIB for a description of the columns of this table.

The following table describes some symptoms that a flooding condition instance can show and some possible remedies.

Symptom	**Action**
Flooding detection is too sensitive.	Increase the **Traffic Increase Rate**.
Flooding detection is not sensitive enough.	Reduce the **Traffic Increase Rate**.
Flooding detection is too sensitive to short term traffic fluctuations.	Increase the **Filter Period Flooding** or increase the **Time Delay**.
Flooding detection is too slow.	Reduce the **Time Delay**.

Symptom	Action
Flooding detection is not sensitive enough to slow traffic increases.	Increase the **Filter Period Baseline Traffic** or reduce the **Traffic Increase Rate**.
Flooding detection affects unrelated originators.	Increase the **Significant Digits** or try a different message **Field**.
Flooding detection is too sensitive during low traffic periods.	Increase the **Minimal Traffic**.

5.4.2 Bulk Filtering

The FAF's bulk condition detects messages with matching fields that FAF receives during a relatively short timespan; for example, several seconds or several minutes. The field that the FAF checks for matching can be a message field such as originator, recipient, SMSC, and so on.

You can use the bulk condition to detect that a single originator is sending messages in bulk, even if the originator is not sending messages at a regular rate, and/or is sending messages more slowly than what the flooding condition will detect.

You can also use one or more bulk conditions to reduce the load on the duplicates condition. The FAF has a limited buffer for tracking duplicates clusters, so reducing the number of messages that it must evaluate improves its performance.

Note: For best results, a flooding condition should be provisioned with a higher priority than the bulk condition.

Because the message rate may vary, FAF calculates the average timespan between each message and the message that came before it. When the average timespan crosses a configured threshold, FAF considers this to be bulk messaging, and returns "true" for the condition.

FAF uses internal records to track the messages that match the bulk condition. To prevent spurious marking of bulk messages, FAF expires its internal records after a configured time period.

The FAF can track 2^{19} (524288) bulk records. This equals to 145 message per second for 3600 seconds. Either reducing the validation period or reducing message per second can avoid overflow.

You can use the `tp_walk` command-line tool to view up to 500 of the records that the FAF generates during bulk detection in the `fafBulkCountTable` SNMP table. Although the FAF can trace up to 524,288 records at once, it only stores 500 of the records in the SNMP table. This preserves resources and prevents significant delays when `tp_walk` is used.

The FAF supports up to **100** instances of the bulk condition.

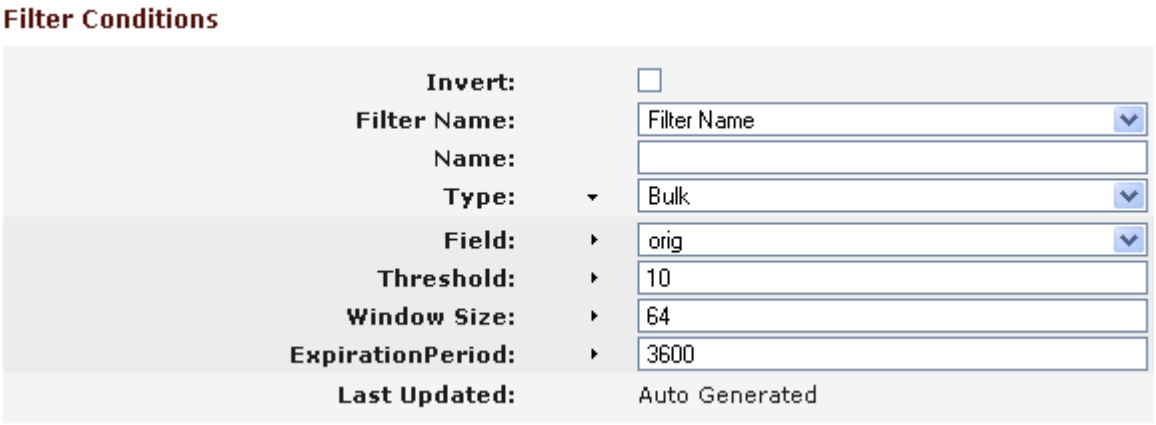


Figure 34: Bulk condition MGR configuration

5.4.2.1 Bulk Condition Calculation

The bulk condition uses the autoregressive moving average model (ARMA) to calculate the average time between messages. This section explains the calculation.

This figure illustrates a timeline during which FAF is receiving messages with matching fields (for example, messages from the same originator).

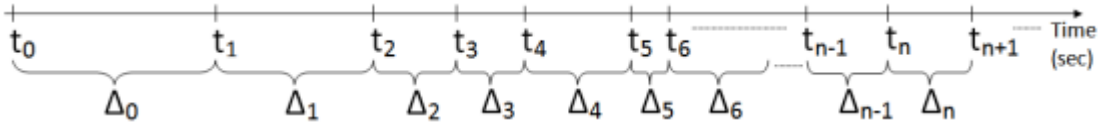


Figure 35: Bulk condition calculation

To determine the average timespan between each message, FAF calculates:

Variable	Represents...
t_n	The moment that FAF receives a message with matching fields, expressed in seconds. As soon as the filter containing the bulk condition is activated, the timeline starts at 0. For example, if a message arrives 10 seconds after filter activation, t_0 is equal to 10. If a second message with matching information then arrives 25 seconds after filter activation, t_1 is equal to 25.
$\Delta_n = t_n+1 - t_n$	The timespan between two messages with matching fields. This value changes dynamically because it is recalculated every time a new message with matching fields is received. For example, if t_0 is 10 and t_1 is 25, then this value is: $\Delta_0 = t_1 - t_0 = 25 - 10 = 15$
$A_0 = 2 *$ threshold	The initial average value when the first message is received. This value is always two times the configured threshold.

The formula to calculate the average at a specific moment when a message with matching information is received is:

$A_n = A_n - 1 * C + \Delta_n * (1 - C)$

Which can also be written as:

new_value = old_value * C + timespan * (1 - C)

Where:

Variable	Represents...
A_n	The average time at n
$C = \exp(-timespan/window) = e^{(-\Delta_n / window)} = [0 \ldots 1]$	The autoregressive moving average model, where *e* is the mathematical constant (approximately 2.71)

A message is marked as bulk when:

$A_n < threshold$

C is recalculated every time a new message with matching information is received. The value of C is heavily influenced by the timespan between two messages with matching information.

If C is close to 1, FAF is less likely to mark messages as bulk, or it will take some time until messages are marked as bulk. As C decreases in value, the chance that messages are marked as bulk increases.

5.4.2.1.1 Bulk Condition Calculation Example

This section provides an example of the bulk condition calculation. This example uses the default bulk condition values:

- Field is originator
- Threshold is 10
- Window size is 64
- Expiration is 3600 seconds

Assume messages from a single originator are arriving at the following times:

$t_0 = 0$

$t_1 = 20$

$t_2 = 30$

$t_3 = 40$

$t_4 = 45$

$t_5 = 50$

$t_6 = 60$

The initial average value is:

$A_0 = 2 * threshold = 2 * 10 = 20$

The timespan between each message is:

$\Delta_0 = t_1 - t_0 = 20 - 0 = 20$

$\Delta_1 = t_2 - t_1 = 30 - 20 = 10$

$\Delta_2 = t_3 - t_2 = 40 - 30 = 10$

$\Delta_3 = t_4 - t_3 = 45 - 40 = 5$

$\Delta_4 = t_5 - t_4 = 50 - 45 = 5$

$\Delta_5 = t_6 - t_5 = 60 - 50 = 10$

The average value calculations are:

Message	Formula	Calculation	Marked as bulk?
1	$A_1 = A_0 * C + \Delta_0 * (1 - C)$, where $C = \exp(-20/64) = e^{(-20/64)} \approx 0.73$	$A_1 = A_0 * C + \Delta_0 * (1 - C) = 20 * 0.73 + 20 * (1 - 0.73) = 14.6 + 5.4 = 20$	No, because A_1 is greater than the threshold (20 > 10)
2	$A_2 = A_1 * C + \Delta_1 * (1 - C)$, where $C = \exp(-10/64) = e^{(-10/64)} \approx 0.86$	$A_2 = A_1 * C + \Delta_1 * (1 - C) = 20 * 0.86 + 10 * (1 - 0.86) = 17.2 + 1.4 = 18.6$	No, because A_2 is greater than the threshold (18.6 > 10)
3	$A_3 = A_2 * C + \Delta_2 * (1 - C)$, where $C = \exp(-10/64) = e^{(-10/64)} \approx 0.86$	$A_3 = A_2 * C + \Delta_2 * (1 - C) = 18.6 * 0.86 + 10 * (1 - 0.86) = 15.99 + 1.4 = 17.3$	No, because A_3 is greater than the threshold (17.3 > 10)
4	$A_4 = A_3 * C + \Delta_3 * (1 - C)$, where $C = \exp(-5/64) = e^{(-5/64)} \approx 0.93$	$A_4 = A_3 * C + \Delta_3 * (1 - C) = 17.3 * 0.93 + 5 * (1 - 0.93) = 16.08 + 0.35 = 16.53$	No, because A_4 is greater than the threshold (16.53 > 10)
5	$A_5 = A_4 * C + \Delta_4 * (1 - C)$, where $C = \exp(-5/64) = e^{(-5/64)} \approx 0.93$	$A_5 = A_4 * C + \Delta_4 * (1 - C) = 16.53 * 0.93 + 5 * (1 - 0.93) = 15.37 + 0.35 = 15.72$	No, because A_5 is greater than the threshold (15.72 > 10)
6	$A_6 = A_5 * C + \Delta_5 * (1 - C)$, where $C = \exp(-10/64) = e^{(-10/64)} \approx 0.86$	$A_6 = A_5 * C + \Delta_5 * (1 - C) = 15.72 * 0.86 + 1 * (1 - 0.86) = 13.51 + 0.02 = 13.53$	No, because A_6 is greater than the threshold (13.53 > 10)

As of t_6, no message has been marked as bulk, so the recommendation is to increase the threshold. Assuming the threshold is increased to 50, the average value calculations are:

Message	Formula	Calculation	Marked as bulk?
1	$A_1 = A_0 * C + \Delta_0 * (1 - C)$, where $C = \exp(-20/64) = e^{(-20/64)} \approx 0.73$	$A_1 = A_0 * C + \Delta_0 * (1 - C) = 100 * 0.73 + 20 * (1 - 0.73) = 73 + 5.4 = 78.4$	No, because A_1 is greater than the threshold (78.4 > 50)
2	$A_2 = A_1 * C + \Delta_1 * (1 - C)$, where $C = \exp(-10/64) = e^{(-10/64)} \approx 0.86$	$A_2 = A_1 * C + \Delta_1 * (1 - C) = 78.4 * 0.86 + 10 * (1 - 0.86) = 67.4 + 1.4 = 68.8$	No, because A_2 is greater than the threshold (68.8 > 50)
3	$A_3 = A_2 * C + \Delta_2 * (1 - C)$, where $C = \exp(-10/64) = e^{(-10/64)} \approx 0.86$	$A_3 = A_2 * C + \Delta_2 * (1 - C) = 68.8 * 0.86 + 10 * (1 - 0.86) = 59.1 + 1.4 = 60.5$	No, because A_3 is greater than the threshold (60.5 > 50)
4	$A_4 = A_3 * C + \Delta_3 * (1 - C)$, where $C = \exp(-5/64) = e^{(-5/64)} \approx 0.93$	$A_4 = A_3 * C + \Delta_3 * (1 - C) = 60.5 * 0.93 + 5 * (1 - 0.93) = 56.2 + 0.35 = 56.6$	No, because A_4 is greater than the threshold (56.6 > 50)

Message	Formula	Calculation	Marked as bulk?
5	$A_5 = A_4 * C + \Delta_4 * (1 - C)$, where $C = \exp(-5/64) = e^{(-5/64)} \approx 0.93$	$A_5 = A_4 * C + \Delta_4 * (1 - C) = 56.6 * 0.93 + 5 * (1 - 0.93) = 52.6 + 0.35 = 52.9$	No, because A_5 is greater than the threshold (52.9 > 50)
6	$A_6 = A_5 * C + \Delta_5 * (1 - C)$, where $C = \exp(-10/64) = e^{(-10/64)} \approx 0.86$	$A_6 = A_5 * C + \Delta_5 * (1 - C) = 52.9 * 0.86 + 10 * (1 - 0.86) = 45.49 + 1.4 = 46.8$	Yes, because A_6 is smaller than the threshold (46.8 < 50)

5.4.2.2 Bulk Condition Use Case

This section describes a use case in which the bulk condition is used to reduce the load on the duplicates condition.

When using the bulk condition to reduce the load on the duplicates condition, you assume that:

- An originator who is not sending a large number of messages in a short period of time is not sending duplicate messages, so the FAF does not need to track those messages as part of a duplicates cluster
- A recipient who is not receiving a large number of messages in a short period of time is not receiving duplicate messages, so the FAF also does not need to track those messages as part of a duplicates cluster

For example, this use case assumes that:

- An originator who is not sending more than one message per minute (on average) is not sending duplicate messages
- A recipient who is not receiving more than one message every 30 seconds (on average) is not receiving duplicate messages

This figure illustrates how two filters can be used to check the originator's rate of sending, check the recipient's rate of receiving, and check for duplicates. The first filter has a higher priority.

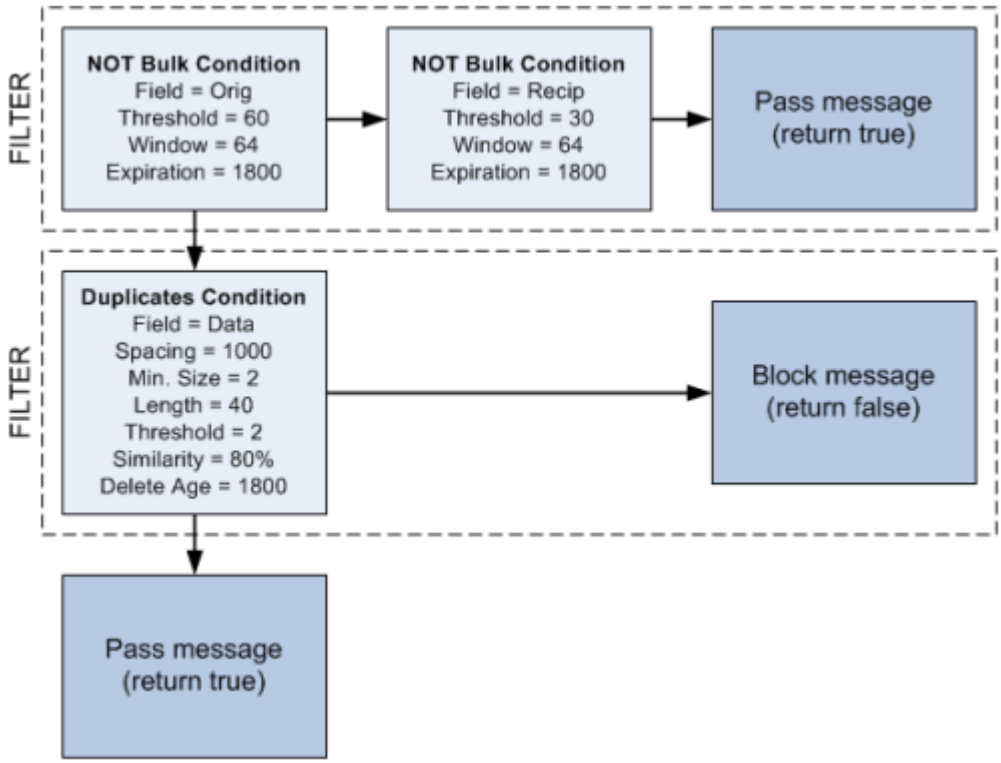


Figure 36: Sample filters with bulk and duplicates conditions

The filters operate as follows:

Filter	Description
First filter	The filter with the highest priority contains two bulk conditions: **1.** The first condition checks if the message originator is not sending messages less than 60 seconds apart (on average) **2.** The second condition checks if the message recipient is not receiving messages less than 30 seconds apart (on average) If: • Either condition is true, pass the message that is being evaluated (FAF returns "true" to the RTR) • Both conditions are true, pass the message that is being evaluated (FAF returns "true" to the RTR) • Neither condition is true, proceed to the filter with the next-lowest priority
Second filter	The filter with the next-lowest priority contains one duplicates condition, which checks for a duplicates cluster that contains messages with similar content. If the message:

Filter	Description
	• Is a duplicate, block the message that is being evaluated (FAF returns "false" to the RTR) • Is not a duplicate, proceed to the next filter with the next-lowest priority

Combining Bulk and Duplicates Filtering with Content Filtering

You can combine the bulk and duplicates filtering illustrated above with a content condition that checks messages for words or phrases that should be blocked. This figure illustrates how a content condition can be added to the bulk and duplicates conditions.

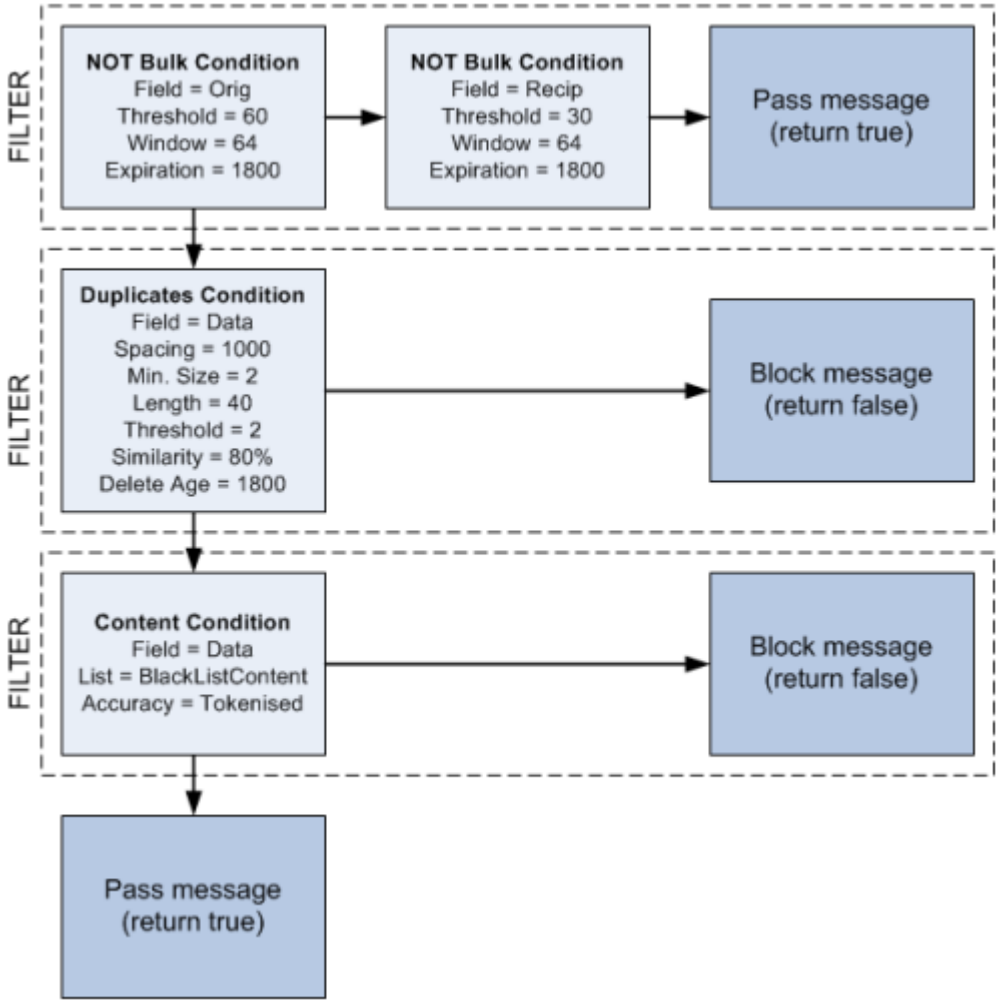


Figure 37: Sample filters with bulk, duplicates, and content conditions

The filters operate as follows:

Filter	Description
First filter	The filter with the highest priority contains two bulk conditions:

Filter	Description
	1. The first condition checks if the message originator is not sending messages less than 60 seconds apart (on average) **2.** The second condition checks if the message recipient is not receiving messages less than 30 seconds apart (on average) If: • Either condition is true, pass the message that is being evaluated (FAF returns "true" to the RTR) • Both conditions are true, pass the message that is being evaluated (FAF returns "true" to the RTR) • Neither condition is true, proceed to the filter with the next-lowest priority
Second filter	The filter with the next-lowest priority contains one duplicates condition, which checks for a duplicates cluster that contains messages with similar content. If the message: • Is a duplicate, block the message that is being evaluated (FAF returns "false" to the RTR) • Is not a duplicate, proceed to the next filter with the next-lowest priority
Third filter	The filter with the lowest priority contains one content condition, which checks the message content (user data) for words or phrases that the operator wants to block. If the message: • Contains blacklisted content, block the message that is being evaluated (FAF returns "false" to the RTR) • Does not contain blacklisted content, pass the message that is being evaluated (FAF returns "true" to the RTR)

5.4.2.3 Bulk Condition Required Message Fields

For the bulk condition, the external condition (EC) application must be configured to send the message field specified in the bulk condition's **Field** parameter to the FAF.

5.4.2.4 Bulk Condition Traps

The bulk condition may issue the following SNMP traps:

- `bulkStartDetected`—A new bulk record has been detected.
- `bulkEndDetected`—No more bulk messages have been detected for this value of the filter variable.

Refer to the NewNet Mobile Messaging SNMP Trap Reference Guide for more information on the traps.

5.4.3 Volume Filtering

The FAF's volume condition allows blocking of short messages (SMs) with certain characteristics, if their number exceeds a certain threshold in a limited period of time.

For example, the operator can use the volume filter condition to:

- Block traffic exceeding 50 SMS/day from the same originator
- Block traffic exceeding 30 SMS/12 hours where both the originator and message content are the same
- Block traffic exceeding 50 SMS/6 hours where the message content is the same.

The volume condition detects and counts SMs with the same *key fields* over a configurable tracking period. All SMs with the same key fields are counted in a *counting group*. A counting group is automatically created when a SM with a new set of key fields hits the condition. When a new SM with the same key fields hits the condition, the counter of the counting group is incremented. A certain period after the creation of the counting group, the counter is reset and the group is cleaned up. Whenever the counter exceeds a certain threshold, the volume condition returns 'true'.

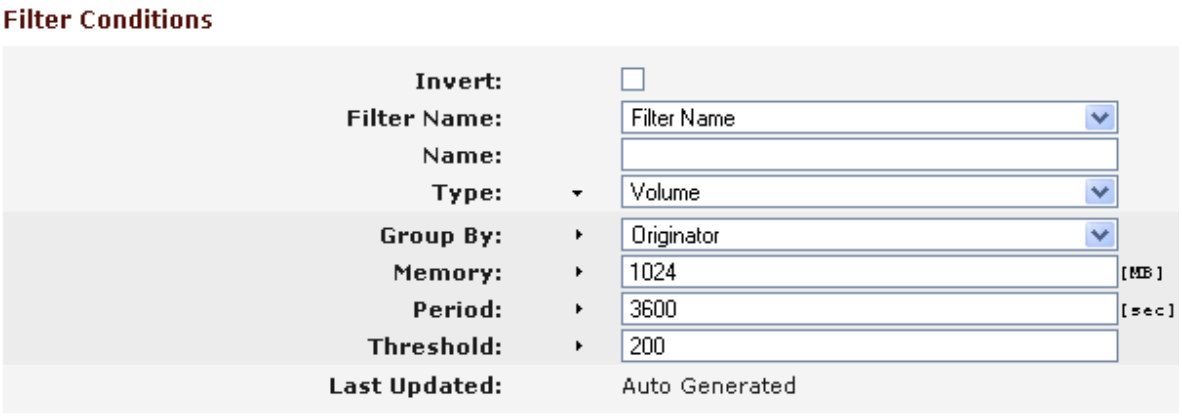


Figure 38: Volume condition MGR configuration

For the volume condition, you can configure the following parameters in the MGR:

- **Group By**—Defines the key fields[11] to group messages by:

Group By	Description	ECI Fields
Nothing	All messages are grouped in a single counting group.	Not applicable
Originator	Messages with the same originator, as specified in the TP-Originating-Address (TP-OA) field of the SM, are grouped and counted.	originatorAddress alphanumericOriginator
Content	Messages with the same content, as specified in the TP-User Data (TP-UD) field of the SM, are grouped and counted. The	userData

[11] These fields must be included in the ECI evaluation requests that the RTR sends to this FAF.

Group By	Description	ECI Fields
	content is based on raw SMS user data; the user data header is **not** taken into account.	
Originator + Content	Messages with both the same originator and content are grouped and counted.	originatorAddress alphanumericOriginator userData

- **Memory**—The amount of memory in megabytes (MB) to dedicate for the tracking of counting groups in the filter. Valid values range from 256 to 65,536 MB. Refer to *Volume Filtering* for more information.

  Note: Given the current maximum dimensioning of a FAF (750 SM/s) and current physical memory available in the current shipping baseline servers (maximum 24 GB RAM), this parameter should not exceed ~19,440 MB.

- **Period**—The tracking period is configurable in seconds, ranging from one minute (60 seconds) up to one day (86,400 seconds). Whenever a message with a new combination of key fields arrives, a new counting group is created, and the tracking period starts for that counting group. At the end of the period, the counting group is reset (discarded from memory).
- **Threshold**—The number of messages in each counting group after which the condition shall apply (return true). Valid values range from 0 to 2,147,483,647 messages.

Possible errors on filter condition activation are:

- Misconfigured parameters—The filter will return an SNMP error and will refuse to activate.
- License check failure—The filter will return an SNMP error and will refuse to activate.

The FAF supports up to **10** instances of the volume condition.

5.4.3.1 Memory Dimensioning

In certain situations, the volume condition requires a large amount of memory in order to operate accurately.

The memory available to a single volume condition is limited by:

- The amount of free physical memory on the system
- The memory requirements of other processes running on the same system
- The memory requirements of other conditions of the same FAF process, including other volume conditions.

To prevent the volume condition from consuming an undesirably high amount of memory, the volume condition provides a configurable memory limit. Generally speaking, the lower the memory limit is set, the less accurate the volume condition will work. Therefore, it is important to determine and configure a sensible value for this parameter.

Important: Each individual volume condition has its own memory limit parameter.

The formula for determining a value that provides accurate condition evaluation is:

```
Memory [MB] = input_volume * weight (key_fields)
```

The `input_volume` is the number of times the condition is expected to be evaluated in the configured period. If the period is one day, and 1 million messages hit the condition each day, then `input_volume` would be 1 million. The `input_volume` may depend on the applied load distribution (see *Volume Condition Load Distribution*).

The `weight` is a constant value, depending on the key fields setting:

Key Fields	Weight
Nothing	Not applicable [12]
Originator	0.00022
Content	0.00025
Originator + Content	0.0003

If the sum of all memory limits of all volume conditions of one FAF instance exceed the amount of available memory:

- Memory can be traded for accuracy (scale back the **Memory** parameter to fit the available memory), or
- The **Period** and **Threshold** values can be scaled down to reduce the memory requirements, or
- Additional traffic elements can be added to the network to make more memory available.

Example

Using the following input data:

- `input_volume` = 10,000,000 (10 million messages per day)
- `weight` = 0.0003 (Originator + Content)

The memory to be configured is calculated as follows:

```
Memory [MB] = input_volume * weight (key_fields)
            = 10,000,000 * 0.0003
            = 3000 MB
```

Note: The memory value can only be changed when the filter is disabled. Re-enabling the filter again causes the internal data structures to re-dimension according to the newly set parameter for optimal performance and causes all current counting groups to be removed from memory.

When memory is changed from a high value to a low value, the FAF must relocate the current in-use memory from the big memory block to a newly allocated small memory block. This CPU and memory load operation can take more than 3 seconds. This could possibly cause the watchdog to kill the FAF. Therefore, it is highly recommended to stop the FAF first, and then change the memory size from a high value to a low value.

5.4.3.2 Volume Condition Examples

This section provides some configuration examples for the volume filter condition.

[12] Because the volume condition with key field "Nothing" requires little memory, it is recommended to set the memory limit to the minimum of 256 MB for these conditions.

Example: Group by Originator

To block traffic exceeding 50 SMS/day from the same originator, the FAF volume condition parameters are set as follows:

- **Type:** Volume
- **Group By:** Originator
- **Memory:** 2200 MB (assuming `input_volume` = 10,000,000)
- **Period:** 86400 seconds (one day)
- **Threshold:** 50 messages

Example: Group by Originator + Content

To block traffic exceeding 30 SMS/12 hours where both the originator and message content are the same, the FAF volume condition parameters are set as follows:

- **Type:** Volume
- **Group By:** Originator + Content
- **Memory:** 1500 MB (assuming `input_volume` = 5,000,000)
- **Period:** 43200 seconds (12 hours)
- **Threshold:** 30 messages

Example: Group by Content

To block traffic exceeding 50 SMS/6 hours where the message content is the same, the FAF volume condition parameters are set as follows:

- **Type:** Volume
- **Group By:** Content
- **Memory:** 625 MB (assuming `input_volume` = 2,500,000)
- **Period:** 21600 seconds (6 hours)
- **Threshold:** 50 messages

Example: Group by Nothing

To block traffic exceeding 1,200,000 SMS/day from a specific country regardless of originator or message content, the FAF volume condition should be triggered by a MTOX rule with:

- **Originator [cond]:** Country + specified country
- **Message Type [cond]:** Bit String + 0 - Short Message
- **EC Application:** External Condition + specified FAF application
- **Failure Action:** Discard with temporary error

The FAF volume condition parameters are set as follows:

- **Type:** Volume
- **Group By:** Nothing
- **Memory:** 256 MB

- **Period:** 86400 seconds (one day)
- **Threshold:** 1200000 messages

5.4.3.3 Volume Condition Load Distribution

The volume condition counts SMs with the same key fields. For accurate operation, it is important that SMs with the same key fields get processed by the same FAF instance. This can be achieved by controlling the load distribution as applied by the RTR.

Key Fields	Load Distribution
Nothing	Any [13]
Originator	Key-based by originator address
Content	None [14]
Originator + Content	Key-based by originator address

Each FAF instance tracks its own set of counting groups. Whenever load distribution causes counting groups for the same key fields to be created on multiple FAF instances, the threshold applying to the whole network needs to be divided by the number of FAF instances. Also, in such situations, the accuracy of the volume condition degrades. Degradation gets stronger, the lower the threshold.

Important: In case FAF instances are chained to achieve the configuration as mentioned in *Volume Condition Examples*, threshold levels of the condition with key fields "nothing" may need revision. Note that statistically, when given high traffic volumes the traffic will be most likely equally spread, given high thresholds (for example, greater than 10,000) and an accepted accuracy margin, a volume condition with key fields "content" can produce acceptable results also when handled across multiple FAF instances. Please take into account that traffic characteristics may vary per network and per country.

5.4.3.4 Volume Condition Required Message Fields

The FAF receives evaluation requests via the ECI interface, through which it connects to a RTR.

For the volume condition, the external condition (EC) application must be configured to send the message fields specified in the volume condition's **Group By** parameter to the FAF. The following message fields apply (refer to the table in *Volume Filtering*):

- Originator Address
- Alphanumeric Originator
- User Data

5.4.3.5 Volume Condition Traps

The volume condition may issue the following SNMP traps:

[13] When the SMs are distributed over *N* FAF instances, the configured volume condition threshold should calculated by dividing the threshold to be applied to the total amount of SMs by *N*.

[14] Currently, the RTR is not able to distribute the load in such a way that messages with equal content end up on the same FAF instance. Therefore, a volume condition with key fields "content" can only work accurately if configured such that (also) a single instance of the FAF handles all SMs.

- `volumeStartDetected`—The volume condition starts to apply action on the matched counting group.
- `volumeEndDetected`—The volume condition stops to apply action on the matched counting group.
- `volumeMemoryInUseAlert`—Alerts the operator that the memory in use for a volume condition reaches the memory limit as configured in the **Memory** field of the volume filter condition.
- `volumeMemoryInUseAlertClean`—Informs the operator that the memory in use for a volume condition has dropped 50 MB below the configured memory limit.

Refer to the NewNet Mobile Messaging SNMP Trap Reference Guide for more information about these traps.

5.5 How To Configure Advanced Filters

This section describes procedures to configure advanced filters using FAF.

5.5.1 Create an Advanced Filter

To create an advanced filter:

1. In the left navigation bar, select **Advanced Filters ➤ Filters**.
   The Advanced Filters tab appears.
2. Click **Add New**.
   A new Advanced Filters tab appears.
3. Enter a unique name for the filter in the **Name** box (up to 31 characters).
4. Optionally enter a description of the filter in the **Description** box.
5. Enter a filter priority between 0 and 99 in the **Priority** box (defaults to 50).
   Filters with a higher priority are evaluated first.
6. From the **Action** list, select the action that the RTR should take if a message meets all conditions when the FAF processes the filter:
   - Return True—The FAF returns true for the message fields
   - Return False—The FAF returns false for the message fields
   - Continue—The FAF should continue to process the next filter

   When first creating the filter, select "Return True". Then, after you create and activate the desired conditions for the filter, change the filter action to "Return False". If you create a filter with no conditions and a "Return False" action, the FAF will immediately return "false" to the RTR and will therefore block messages.
7. In the **Append** box, optionally enter any text that the FAF should append to the message. The FAF will append this text if the message meets all conditions of the filter and if the Data message field was provided to the FAF.

   CAUTION: Do not use text replacement/append functions that may make the user data longer than the original user data. When applied to a "full segment" this will lead to an undeliverable message.

8. Click **Save**.
   The MGR saves the filter and closes the tab.
9. Activate the filter.

5.5.2 Add Conditions to an Advanced Filter

Prerequisites:

- Filter
- Filter list (if adding a content condition)

Combine advanced filters and conditions of different types to create filter conditions.

To add a filter condition to a filter:

1. In the left navigation bar, select **Advanced Filters ➤ Filters**.
   The Advanced Filters tab appears.
2. Click the name of an existing filter.
3. In the Filter Conditions section, click **Add New**. A Filter Conditions tab appears.
4. If the filter condition should be inverted if the condition is true, select **Invert**.
5. From the **Filter Name** list, select the filter to use (defaults to the filter that you clicked in the Advanced Filters tab).
6. In the **Name** box, enter the name of the filter condition.
7. From the **Type** list, select the condition type.
8. Click **Save**.

   The MGR creates the filter condition and closes the tab.
9. Activate the filter condition.

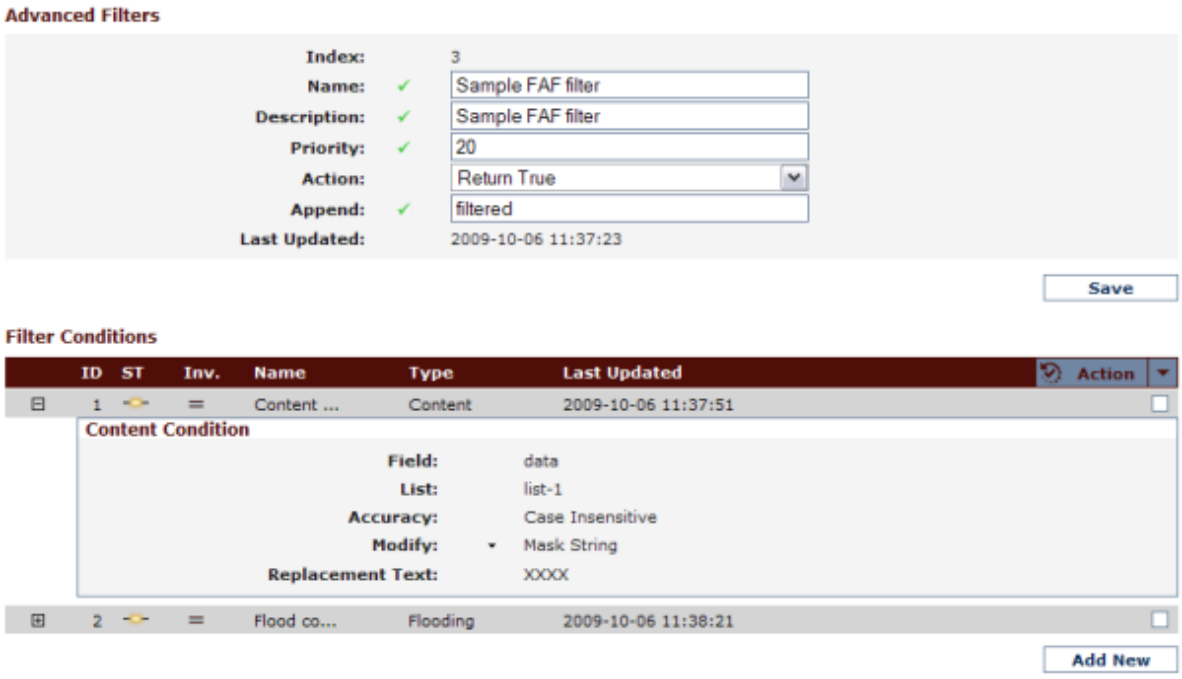


Figure 39: Sample filter with conditions

5.5.2.1 Add a Content Condition

When adding a content condition:

1. From the **Field** list, select the message field to which the condition should be applied; the default and most commonly used field is Data (message content).

   Refer to *Message Field Options* for a complete list of available message fields and descriptions.

2. From the **List** list, select the advanced filter list to use.
3. From the **Accuracy** list, select the accuracy level for matching:

   - Exact
   - Case-insensitive (can only be used with the ASCII character set)
   - Tokenised
   - Normalised
   - Regular Expression

   The accuracy indicates an implicit transformation that the FAF performs on all text involved in the match before the match is calculated.

4. From the **Modify** list, select how the target text should be modified:

   - None
   - Mask string (will not increase the length of the target string)
   - Replace string (may affect the length of the target string)
   - Replace message

5. If you select a content modification option other than **None**, enter the text that should mask or replace the target text in the **Replacement Text** box.

5.5.2.1.1 Message Field Options

The message fields that can be selected in **Field** list for the content, duplicates, flooding, and bulk conditions:

Field (number)	ECI Field	Description	Additional Information
path (1)	routingPath	Routing path	Integer format. Supported values are: • moMo (0) • moMt (1) • moMtMo (2) • moMtAt (3) • moAt (4) • moDiscardWithNack (5) • moDiscardWithAck (6) • moDiscardSilently (7) • mtMt (10) • mtBlockWithTemporaryError (11) • mtBlockWithPermantError (12) • mtBlockWithNoResponse (13) • mtBlockWithAck (14) • aoAo (20) • aoMt (21) • aoMtAo (22) • aoAt (23) • aoDiscardWithAck (24) • aoDiscardWithNak (25) • atAt (30) • atBlockWithTemporaryError (31) • atBlockWithPermanentError (32) • atBlockWithAck (33)
submit (3)	originalSubmitTime	Not adjusted submit time	Original submission time, in Unix time format.
uniq (4)	uniqueSubmitTime	Adjusted (made unique) submit time	Time the message was submitted to the RTR. Note that this field contains the potentially adjusted submission time as described in the RTR Operator Manual chapter on Service Center Time Stamps.
deliv (5)	deliveryTime	Delivery time	Time the RTR delivered or deleted the message. In Unix time format.
orig (6)	originatorAddress	Originator address	Self explanatory. In ASCII string format with prefix. A national number has the

Field (number)	ECI Field	Description	Additional Information
			prefix "N", an international has the prefix "+", an unknown has the prefix "U", and an alphanumeric has the prefix "A". For example, `N12345678`, `Aalphanumer`.
origImsi (7)	originatorImsi	Originator IMSI	Self explanatory. In ASCII string format.
smsc (8)	smscAddress	SMSC address	Self explanatory. In ASCII string format.
msc (9)	mscAddress	MSC address	Self explanatory. In ASCII string format.
recip (10)	recipientAddress	Recipient address	Self explanatory. An ASCII string format with the same prefix as "orig".
recipImsi (11)	recipientImsi	Recipient IMSI	Self explanatory. In ASCII string format.
segTotal (12)	cmTotalSegments	Total number of segments	Total number (0-255) that indicates the total number of pieces in a concatenated message (only present in case of a concatenated message when received as a part of SMPP `sar_total_segments` or as a part of 8 bit reference or 16 bit reference number UDH IEI).
segId (13)	cmCurrentSegment	Segment number	Current segment number (0-255) of the concatenated message. A running number for each part of a concatenated message (only present in case of a concatenated message when received as a part of SMPP `sar_segment_seqnum` or as a part of 8 bit reference or 16 bit reference number UDH IEI).
len (15)	lengthOfMessage	Length of message	Number of characters in septets or octets, depending on the data coding scheme (DCS).
header (17)	userDataHeader	User data header	Value specified in one of the information element identifiers (IEIs) of the user data header (UDH) of the message. Only evaluates positively if there is an exact match with the information element identifier (00-FF, hexadecimal) of the UDH.

Field (number)	ECI Field	Description	Additional Information
			Refer to technical specification 3GPP 23.040 for more information. Most common IEI values: • 00: Concatenated short message • 01: Special SMS message indication • 04: Application port addressing scheme, 8-bit address • 05: Application port addressing scheme, 16-bit address • 06: SMSC control parameters • 07: UDH Source Indicator
encoding (18)	dataCodingScheme	Data Coding Scheme (DCS)	Data coding scheme (DCS) specified in the message. Byte value (value between 00 and FF, hexadecimal)
data (19)	userData	Message data	The content can be already modified by other filters. Decoded into UTF-8 format.
statrepinfo (20)	statusReportInfo	Status report information	Opaque value containing the reference for the SS7 Status Report assigned by the TPR.
smppMsgId (21)	smppMessageId	SMPP message ID	In string format.
dataorg (22)	userData	User data	This is the original message content from ECI. Decoded into UTF-8 format.
segRef (23)	cmReferenceNr	Segment reference	Same for all segments in a concatenated SMS (received as a part of SMPP `sar_msg_ref_num` or as a part of 8 bit reference or 16 bit reference number UDH IEI).
notifreq (24)	notificationRequest	Notification request	Indicates whether notification or status report was requested for this message (true) or not (false).
callingGt (25)	callingPartyAddress	Calling global title	GT of the SCCP Calling Party Address in the message. In ASCII string format.
calledGt (26)	calledPartyAddress	Called global title	GT of the SCCP Called Party Address in the message. In ASCII string format.

Field (number)	ECI Field	Description	Additional Information
delstat (42)	deliveryStatus	Delivery status	Result of a delivery attempt as reported in a notification on an AO/SM. In integer format. Supported values are: • noStatusAvailable (0) • inProgress (1) • validityPeriodExpired (2) • deliveryFailed (3) • deliverySuccessful (4) • noResponse (5) • lastNoResponse (6) • cancelled (7) • deleted (8) • deletedByCancel (9) • scheduled (10) • accepted (11) • rejected (12) • skipped (13) • replaced (14)
exconrule (55)	selectedExternalConditionRule	Name of external condition rule	Name of the external condition rule used to forward the message to the FAF.
protocolId message (60)	protocol Id	protocol identifier	Indicates the value of the TP-PID field (included in the MAP header), if the message was MO or MT. Otherwise (i.e. for AO or AT messages) it indicates the value of the protocol id parameter included (if any) in the message. This field is not applicable for status reports and notifications. Valid values are in the range 0-255.

Note: The 'protocolId' message field should not be selected while configuring a duplicates, flooding or bulk filter condition, because it has no relevant use case for these filters.

5.5.2.1.2 Accuracy Options

The message text is matched with other text with a particular "accuracy". The accuracy indicates an implicit transformation that is performed on all text involved in the match, before the match is calculated.

The following options are available for the **Accuracy** parameter.

Option (Short Name)	Description
Exact (exact)	The target text must contain an exact match to an entry in the specified list. No transformation is done. For example: • `hello` matches `hello` • `hEllo` does not match `hello`
Case Insensitive (case)	The FAF removes the case from all characters (all characters are effectively lowercased) of the target text before attempting to match it to an entry in the specified list. For example: • `Hello` matches `hello` • `H3llo` does not match `hello` The FAF only supports case removal for the ASCII character set. Therefore, it is not recommended to use this option in combination with non-ASCII characters.
Tokenised (token)	The target text and all entries in the specified list are tokenised before the FAF attempts to match the text to an entry in the list. For example (assuming the default normalisation map is in use): • `H3ll0` matches `hello` • `HH3ll0` does not match `hello`
Normalised (repeat)	The target text and all entries in the specified list are normalised before the FAF attempts to match the text to an entry in the list. For example (assuming the default normalisation map is in use): • `H33ll1000` matches `hello` • `hollo` does not match `hello`
Regular Expression (regexp)	The target text is matched using regular expression statements that are provisioned by a list. Any non-regular expression strings from the list are ignored. For example: • `hello` matches `/(hello|hi|hoi)/` • `hello` does not match `/\d/` • `hello1234` matches `/\d+/` The regular expression conforms to the POSIX Extended Regular Expression standard. The FAF uses the POSIX regular expression library. Therefore, the limitation of the library also applies to the FAF. It is recommended to use basic regular expression grammar. **Note:** To support regular expressions, the FAF requires that the `en_US.UTF-8` locale is installed when using Red Hat Linux 5 and the

Option (Short Name)	Description
	`en_US.UTF-8` locale is installed when using Solaris 10. Refer to the Traffic Element Installation Manual for more information.

5.5.2.1.3 Modify Options

The following options are available for the **Modify** parameter. Note that this parameter is relevant only for the user data field and should be set to "None" for all other message fields.

Option	Description
None	The FAF does not modify the target text.

Mask String	The **Mask String** functionality ensures that the replacement of the text does not increase the length of the original message. This prevents truncation of the message.
	For example, there is a content filter for the word `website` and the **Replacement Text** is `CENSORED`. If the message is:
	`This website is good`
	The message will be modified to:
	`This CENSORE is good`
	In this example, the message length remains the same.
	If the **Replacement Text** is `***`, the message will be modified to:
	`This *** is good`
	In this example, the message length decreases.

Replace String	The matching string of the target text is replaced by the text in the **Replacement Text** box. As a result, the modified target text may increase or decrease in length.
Replace Message	The entire target text is replaced by the text in the **Replacement Text** box.

5.5.2.2 Add a Duplicates Condition

When adding a duplicates condition:

Note: Certain parameter changes in the duplicates filter condition may take a long time to effect due to the large state that is kept in the filters. Especially when the filter is full (has the maximum amount of memory state), it can take quite some time for the changes to take effect (sometimes 30 minutes or more).

1. From the **Field** list, select the message field to evaluate; the default and most commonly used field is Data.

   Refer to *Message Field Options* for a complete list of available message fields and descriptions.

2. In the **Spacing** box, enter the number of allowed dissimilar messages (2-99,999) between two similar messages (default 1,000).

   If more messages than this are found between two similar messages, the similar messages are not considered duplicates.

3. In the **Min. Size** box, enter the minimum number of messages (2-1,000) required to start a duplicates cluster (defaults to 10).
4. In the **Length** box, enter the minimum number of features (4-160) required for to start duplicates clustering (defaults to 4).
5. In the **Threshold** box, enter the minimum number of messages (2-999,999) that must be in the cluster for the duplicates condition to return true (defaults to 10).
6. In the **Similarity** box, enter the percentage (0-100) that messages must be similar to be placed in the same cluster (defaults to 80%).

   100% means the messages must match exactly.

7. In the **Delete Age** box, enter the number of seconds (0-999,999) that a never-matched cluster is allowed to exist before it is deleted (0 means clusters are never deleted).

   If the cluster is matched, the timer restarts for the cluster.

5.5.2.3 Add a Flooding Condition

When adding a flooding condition:

1. From the **Field** list, select the message field to evaluate.

   The field should depend on the type of traffic that is being evaluated for flooding. For example, for MO traffic, the MSC should be used; for MT traffic, the SMSC should be used.

   Refer to *Message Field Options* for a complete list of available message fields and descriptions.

2. In the **Significant Digits** box, enter the number of digits (0-16) of the specified field that are taken into account when tracking originators (defaults to 16, which is recommended).

   The first digits of the number are used; for example, for a setting of `6`, the originator numbers `15562235` and `155622234` map to the same trackable originator.

   More digits may be taken into account if the FAF detects higher traffic.

3. In the **Minimal Traffic** box, enter the minimum number of messages per second (1-1,000,000) required for the filter to become active (defaults to 5, which is recommended).

   This is the constant threshold used to compute the flooding detection threshold. Use this setting to prevent spurious flooding detection at low traffic levels. Higher values make flooding detection less likely.

4. In the **Traffic Increase Rate** box, enter a relative increase in traffic (1-10,000%) used to compute the flooding detection threshold.

   This is the traffic increase that is required to trigger the filter. The value is relative to the long-term traffic average. Higher values make flooding detection less likely.

5. In the **Time Delay** box, enter the number of seconds (1-10,000) that the short-term traffic average must exceed the flooding detection threshold before the filter becomes active (defaults to 30).

   The condition only yields true this number of seconds after the flooding detection threshold has been exceeded. Higher values make flooding detection less likely.

6. In the **Filter Period Flooding** box, enter the number of seconds (1-10,000) to use to calculate the short-term traffic average (default 10).

   This is the response time used to compute the short-term traffic average. Fluctuations shorter than this period are filtered out. Higher values make flooding detection less likely.

7. In the **Filter Period Baseline Traffic** box, enter the number of seconds (1-10,000) to use when calculating the long-term traffic average (defaults to 3600).

   Fluctuations slower than this are not considered flooding. This value should be significantly higher than the **Time Delay**; a factor of at least 20 is recommended. Higher values make flooding detection less likely.

8. In the **Margin** box, enter the threshold, in messages per 1000 seconds (1-100,000), below which traffic from a trackable originator is not tracked (default 5).

   For example, for a value of 10, originators sending less than 10 messages per 1000 seconds are not tracked. Use this parameter to avoid using FAF processing performance for message originators for which the traffic lies below a level of interest. Higher values make flooding detection less likely.

5.5.2.4 Add a Volume Condition

When adding a volume condition:

1. From the **Group By** list, select a value that determines on which fields to group and count messages for the Volume filter condition.

   Possible options are:

   - `Nothing` — Count all messages
   - `Originator` — Group and count messages based on originator address (as specified in the TP-Originating-Address (TP-OA) field of the SMS Message).
   - `Content` — Group and count messages based on raw SMS user data content (as specified in the TP-User Data (TP-UD) field of the SMS Message).
   - `Originator + Content` — Group and count messages based on originator address and raw SMS user data content

2. In the **Memory** field, enter the amount of memory in Megabytes (MB) to dedicate for the tracking of elements in the filter. Valid values range from 256 to 65,536 MB. Default is 1024 MB.

   This value is a hard memory limit on the amount of memory dedicated for storing data for this filter. When the memory limit is reached, a trap is generated.

   Refer to the FAF Operator Manual, Volume Condition for more information on memory dimensioning.

3. In the **Period** field, enter the tracked period of time in seconds. Valid values range from 60 seconds (one minute) to 86,400 seconds (one day) . Default is 3600 seconds (one hour).
4. In the **Threshold** field, enter the number of messages in each grouping after which the condition shall apply (return 'true'). Valid values range from 0 to 2,147,483,647 messages. Default is 200 messages.

5.5.2.5 Add a Bulk Condition

When adding a bulk condition:

Note: Certain parameter changes in the bulk filter condition may take a long time to effect due to the large state that is kept in the filters. Especially when the filter is full (has the maximum amount of memory state), it can take quite some time for the changes to take effect (sometimes 30 minutes or more).

1. From the **Field** list, select the message field to evaluate; the default and most commonly used field is Orig.

   Refer to *Message Field Options* for a complete list of available message fields and descriptions.

2. In the **Threshold** box, enter the minimum number of seconds (0-999,999) to mark a message as bulk (defaults to 10).

   When the average time span between messages is lower than this threshold, the message is regarded as bulk and the condition returns false.

3. In the **Window Size** box, enter the window size (0-999,999) used to calculate the average timespan (defaults to 64).

   This is the filter constant for the auto-regressive low-pass filter, which is based on the following algorithm:

   ```
   new_value = old_value * C + window_size * (1 - C)
   ```

   Where:

   - `window_size` is the timepan between two subsequent messages
   - `window` is this parameter
   - `C = exp(-timespan/window)`

   The larger the window size, the slower the low-pass filter becomes; that is, the less responsive the filter becomes to quick changes in value.

4. In the **Expiration Period** box number of seconds (0-999,999) before a record expires (default 3600).

   When a record matches, the FAF updates the record's timestamp. When the timestamp is older than the expiration time, the FAF deletes the record.

5.5.2.6 Add an Enhanced Messaging (EMS) Condition

When adding an enhanced messaging (EMS) condition:

1. In the **Protocol Id Values** box, enter the desired protocol id value(s) against which the EMS filter condition should compare the protocol id of a message. If no protocol id value is entered, then the filter condition will match any message protocol id.
2. Select one of more Information Element IDs (IEIs) on which to filter:

   - 00 - Concatenated short messages, 8-bit reference number
   - 01 - Special SMS Message Indication
   - 03 - Value not used to avoid misinterpretation as LF character
   - 04 - Application port addressing scheme, 8 bit address
   - 05 - Application port addressing scheme, 16 bit address
   - 06 - SMSC Control Parameters
   - 07 - UDH Source Indicator
   - 08 - Concatenated short message, 16-bit reference number
   - 09 - Wireless Control Message Protocol
   - 10 - Text Formatting

- 11 - Predefined Sound
- 12 - User Defined Sound (iMelody max 128 bytes)
- 13 - Predefined Animation
- 14 - Large Animation (16*16 times 4=128 bytes)
- 15 - Small Animation (8*8 times 4 = 8*4 = 32 bytes)
- 16 - Large Picture (32*32 = 128 bytes)
- 17 - Small Picture (16*16 = 32 bytes)
- 18 - Variable Picture
- 19 - User prompt indicator
- 20 - Extended Object
- 21 - Reused Extended Object
- 22 - Compression Control
- 23 - Object Distribution Indicator
- 24 - Standard WVG Object
- 25 - Character Size WVG Object
- 26 - Extended Object Data Request Command
- 32 - RFC 822 E-Mail Header
- 33 - Hyperlink format element
- 34 - Reply Address Element
- 35 - Enhanced Voice Mail Information
- 36 - National Language Single Shift
- 37 - National Language Locking Shift

If the user data header (UDH) of a message contains the selected IEI(s), FAF will return "true" for the condition. The EMS condition uses a logical OR operation; therefore, if you select multiple IEIs and also configure certain protocol id values for one EMS condition and the message contains any of the selected IEIs OR any of the configured protocol ids, the condition will return "true". Refer to the 3GPP 23.040-920 specification for a description of EMS IEIs.

3. If you selected "04 - Application port addressing scheme, 8 bit address":

   a. Enter an 8-bit source port number in the **8 Bit Source Port** box.
   b. Enter an 8-bit destination port number in the **8 Bit Destination Port** box.

   If the source port and/or destination port in the UDH of a message matches the provisioned port, FAF will return "true" for the condition. If you do not provision port numbers, FAF simply checks for the presence of the IEI, and returns "true" if it is present.

4. If you selected "05 - Application port addressing scheme, 16 bit address":

   a. Enter a 16-bit source port number in the **16 Bit Source Port** box.
   b. Enter a 16-bit destination port number in the **16 Bit Destination Port** box.

   If the source port and/or destination port in the UDH of a message matches the provisioned port, FAF will return "true" for the condition. If you do not provision port numbers, FAF simply checks for the presence of the IEI, and returns "true" if it is present.

5.5.2.7 Add an Expression Condition

When adding an expression condition:

1. In the **Text Expression** box, enter the regular expression containing the variable to test. Examples are as follows:

   ```
   messagetype == 4
   ```

   ```
   totalsegments >= 4
   ```

   ```
   messagetype == 0 && totalsegments >= 4
   ```

2. In the **Assignment Expression** box, enter the value to assign to the variable. For example:

   ```
   eciattribute2 = 1
   ```

5.5.2.7.1 Expression Variables

The variables in this section can be used for expression conditions. "Testable" indicates whether the variable can be used in a test expression and "Assignable" indicates whether the variable can be used in an assignment expression.

Variable	Testable	Assignable
`messagetype`	Yes	No
`failuremessagekey`	Yes	Yes
`eciattribute1`	Yes	Yes
`eciattribute2`	Yes	Yes
`eciattribute3`	Yes	Yes
`eciattribute4`	Yes	Yes
`eciattribute5`	Yes	Yes
`eciattribute6`	Yes	Yes
`eciattribute7`	Yes	Yes
`eciattribute8`	Yes	Yes
`eciattribute9`	Yes	Yes
`eciattribute10`	Yes	Yes
`eciattribute11`	Yes	Yes
`eciattribute12`	Yes	Yes
`eciattribute13`	Yes	Yes
`eciattribute14`	Yes	Yes
`eciattribute15`	Yes	Yes
`eciattribute16`	Yes	Yes
`eciattribute17`	Yes	Yes
`eciattribute18`	Yes	Yes
`eciattribute19`	Yes	Yes

Variable	Testable	Assignable
eciattribute20	Yes	Yes
eciattribute21	Yes	Yes
eciattribute22	Yes	Yes
eciattribute23	Yes	Yes
eciattribute24	Yes	Yes
eciattribute25	Yes	Yes
eciattribute26	Yes	Yes
eciattribute27	Yes	Yes
eciattribute28	Yes	Yes
eciattribute29	Yes	Yes
eciattribute30	Yes	Yes
eciattribute31	Yes	Yes
eciattribute32	Yes	Yes
testnumber	Yes	Yes
totalsegments	Yes	No

5.5.3 Create an Advanced Filter List

Use filter lists with the FAF's content condition type to filter certain words or phrases.

To create a filter list:

1. In the left navigation bar, select **Advanced Filters ➤ Lists**.
   The Filter List tab appears.
2. Click **Add New**.
   A new Filter List tab appears.
3. Enter a unique name for the list in the **Name** box (up to 31 characters).
4. Optionally enter a description of the list in the **Description** box.
5. In the **Text** box, enter the word(s) and/or phrase(s) the FAF should detect, each on a separate line.

   Note: If this list will be used on an originator field with the **Accuracy** setting "regular expression", it is important to consider the prefix. In the case of a numeric or short code originator, an international number is prefixed with a plus sign (+), a national number is prefixed with an N, and an unknown number is prefixed with a U. In the case of an alphanumeric originator, the originator is prefixed with an A.
6. Click **Save**.
   The MGR creates the filter list and closes the tab.
7. Activate the list.

Chapter 6

Analysing Firewalled Traffic

Topics:

6.1 Introduction

This section discusses different ways you can monitor the FWL's activities.

6.2 Using Traps

The FWL can generate many SNMP traps based on firewalled traffic. Some examples are:

Trap	Description
fwSriSmWithUnknownSccpSmscAddress	The FWL received an inbound SRI-SM operation with an SMSC address at the SCCP layer that could not be associated with any defined mobile network.
fwSriSmWithConflictingSmscAddress	The FWL received an inbound SRI-SM operation with conflicting SMSC addresses at the SCCP and MAP layers.
fwTrapImsiInMoFwdSm	The IMSI specified in an MoForwardSm operation conflicts with the IMSI provided by the HLR.
fwMoFwdSmWithSpoofedOriginatorAddress	The FWL received an MoForwardSm operation with a spoofed originator address.

The FAF also generates SNMP traps. Some examples are:

Trap	Description
eciLoginFailed	The FAF could not log in to the RTR.
floodingStartDetected	The FAF has detected flooding.
clusterExpired	A duplicates cluster expired because no duplicate messages were found during the configured duration.

For a complete list and description of all traps, refer to the SNMP Trap Reference Guide.

6.2.1 Spoofing Threshold Traps

When:

- The FWL detects a number of spoofing attempts that is greater than or equal to the configured threshold during the configured period, and
- The detected number of spoofing attempts was less in the previous period

Then the FWL will generate:

- `fwMoFwdSmWithSpoofingExceedThresholdAlarmTrap` for MO spoofing attempts
- `fwMtFwdSmWithSpoofingExceedThresholdAlarmTrap` for MT spoofing attempts

When:

- The FWL detects a number of spoofing attempts that is less than the configured threshold during the configured period, and
- The detected number of spoofing attempts was greater than or equal in the previous period

Then the FWL will generate:

- `fwMoFwdSmWithSpoofingExceedThresholdAlarmClearedTrap` for MO spoofing attempts
- `fwMtFwdSmWithSpoofingExceedThresholdAlarmClearedTrap` for MT spoofing attempts

Refer to the Mobile Messaging SNMP Trap Reference Guide for more information about these traps.

Note: The FWL's count of MT spoofing attempts only includes spoofed MtForwardSm operations. It does not include spoofed SendRoutingInfoForSm operations.

6.2.1.1 Configuring Spoofing Threshold Traps

To configure the MO and MT spoofing threshold traps, set the following `tpconfig` attributes in the semi-static configuration file:

- For MO spoofing:
  - `firewallmofwdsmwithspoofingthreshold` (range 0-1,000,000, default 0, which disables the functionality)
  - `firewallmofwdsmwithspoofingperiod` (range 1-86,400, default 3600)
- For MT spoofing:
  - `firewallmtfwdsmwithspoofingthreshold` (range 0-1,000,000, default 0, which disables the functionality)
  - `firewallmtfwdsmwithspoofingperiod` (range 1-86,400, default 3600)

6.2.1.2 Sample Spoofing Threshold Traps

This example illustrates the spoofing threshold traps.

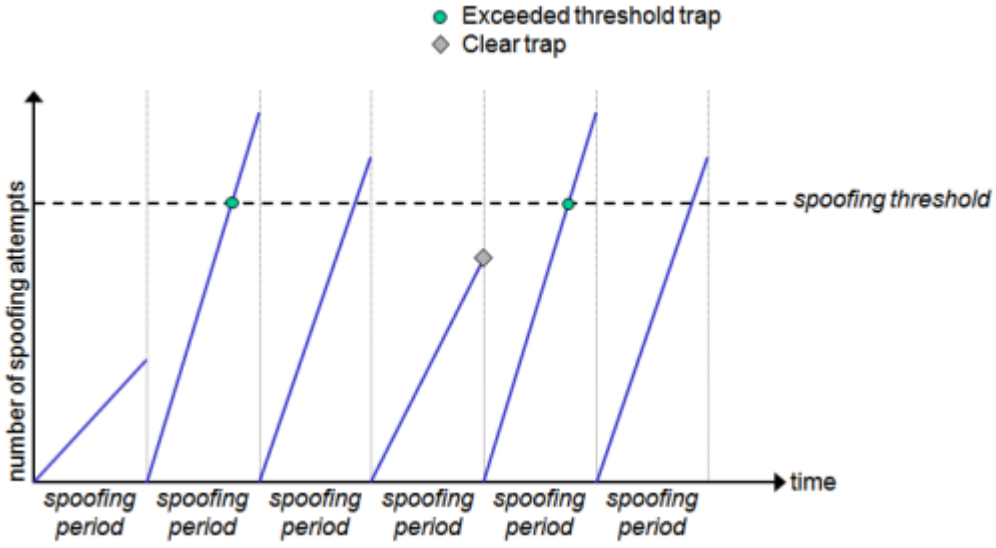


Figure 40: Spoofing threshold traps

In this example, the FWL does not generate a trap when the number of spoofing attempts exceeds the threshold in the third spoofing period because the trap was already generated for the preceding spoofing period. The trap is "cleared" by the trap generated in the fourth spoofing period.

6.3 Using Counters

The FWL and FAF offer many counters that track firewalled traffic and advanced filters. To retrieve the current value of a specific counter or a group of counters, execute the following command at a command prompt:

```
tp_walk <counter or group name>
```

6.3.1 FWL Counters

The `smsCounters` group provides information about firewalled traffic. Specific counters that are associated with firewalled traffic are:

Counter	Description
smsCntRecvSriSmInvalidSccpSmscAddressCounter	Number of times that the RTR received an inbound SRI-SM with an invalid SMSC address at the SCCP layer
smsCntRecvSriSmInvalidMapSmscAddressCounter	Number of times that the RTR received an inbound SRI-SM with an invalid SMSC address at the MAP layer
smsCntRecvSriSmInvalidRecipientAddressCounter	Number of times that the RTR received an inbound SRI-SM with an invalid recipient address
smsCntRecvSriSmInvalidOriginatorAddressCounter	Number of times that the RTR received an inbound SRI-SM with an invalid originator address
smsCntRecvSriSmUnknownSccpSmscAddressCounter	Number of times that the RTR received an inbound SRI-SM with an SMSC address at the SCCP layer that could not be associated with any defined mobile network
smsCntRecvSriSmUnknownMapSmscAddressCounter	Number of times that the RTR received an inbound SRI-SM with an SMSC address at the MAP layer that could not be associated with any defined mobile network
smsCntRecvSriSmConflictingSmscAddressCounter	Number of times that the RTR received an inbound SRI-SM with conflicting SMSC addresses at the SCCP and MAP layers

Counter	Description
smsCntRecvMtInvalidSccpSmscAddressCounter	Number of times that the RTR received an inbound MtForwardSm with an invalid SMSC address at the SCCP layer
smsCntRecvMtInvalidMapSmscAddressCounter	Number of times that the RTR received an inbound MtForwardSm with an invalid SMSC address at the MAP layer
smsCntRecvMtInvalidOriginatorAddressCounter	Number of times that the RTR received an inbound MtForwardSm with an invalid originator address
smsCntRecvMtInvalidImsiCounter	Number of times that the RTR received an inbound MtForwardSm with an invalid IMSI
smsCntRecvMtInvalidMscOrSgsnAddressCounter	Number of times that the RTR received an inbound MtForwardSm with an invalid MSC or SGSN address
smsCntRecvMtUnknownSccpSmscAddressCounter	Number of times that the RTR received an inbound MtForwardSm with an SMSC address at the SCCP layer that could not be associated with any defined mobile network
smsCntRecvMtUnknownMapSmscAddressCounter	Number of times that the RTR received an inbound MtForwardSm with an SMSC address at the MAP layer that could not be associated with any defined mobile network
smsCntRecvMtConflictingSmscAddressCounter	Number of times that the RTR received an inbound MtForwardSm with conflicting SMSC addresses at the SCCP and MAP layers or with different addresses at the SCCP layer among the TCAP messages of a segmented TCAP dialogue
smsCntRecvMtSpoofedSccpSmscAddressCounter	Number of times that the RTR received an inbound MtForwardSm with spoofing of the SMSC address at the SCCP layer
smsCntRecvMtSpoofedMapSmscAddressCounter	Number of times that the RTR received an inbound MtForwardSm with spoofing of the SMSC address at the MAP layer
smsCntRecvMtWithoutPrecedingSriSmCounter	Number of times that the RTR received an inbound MtForwardSm (pertaining to a home subscriber) with no preceding SRI-SM

Counter	Description
smsCntRecvMtForgedMscOrSgsnAddressCounter	Number of times that the RTR received an inbound MtForwardSm with spoofing of the MSC or SGSN address
smsCntRecvMtForgedImsiCounter	Number of times that the RTR received an inbound MtForwardSm with spoofing of the IMSI
smsCntRecvMtForgedLmsiCounter	Number of times that the RTR received an inbound MtForwardSm with spoofing of the LIMSI
smsCntRecvMtMatchingWhiteListedImsiCounter	Number of times that the RTR received an inbound MtForwardSm that matched a prefix that is whitelisted in the recipient IMSI whitelist
smsCntRecvMtHomeRoutedSuspectPlainCounter	Number of times that the RTR received an inbound MtForwardSm from a suspect source via plain Home Routing
smsCntRecvMtHomeRoutedTrustedPlainCounter	Number of times that the RTR received an inbound MtForwardSm from a trusted source via plain Home Routing
smsCntRecvMtHomeRoutedSuspectScrambledCounter	Number of times that the RTR received an inbound MtForwardSm from a suspect source via Home Routing with IMSI scrambling
smsCntRecvMtHomeRoutedTrustedScrambledCounter	Number of times that the RTR received an inbound MtForwardSm from a trusted source via Home Routing with IMSI scrambling
smsCntRecvMoSpoofedOriginatorAddressCounter	Number of times that the RTR received an inbound MtForwardSm with spoofing of the originator address
smsCntRecvRogueTcapContinueCounter	Number of times that the RTR received a TCAP Continue message that had no preceding dialogue and that contained components other than Invoke
smsCntRecvRogueTcapEndCounter	Number of times that the RTR received a TCAP End message with no preceding dialogue
smsCntRecvRogueTcapContinueUnknownCountryCounter	Number of times that the RTR received a TCAP Continue message that had no preceding dialogue, that contained components other than Invoke, and that originated from a country that could not be identified

Counter	Description
smsCntRecvRogueTcapEndUnknownCountryCounter	Number of times that the RTR received a TCAP End message with no preceding dialogue and that originated from a country that could not be identified
smsCntRecvRogueTcapContinueUnknownNetworkCounter	Number of times that the RTR received a TCAP Continue message that had no preceding dialogue, that contained components other than Invoke, and that originated from a network that could not be identified
smsCntRecvRogueTcapEndUnknownNetworkCounter	Number of times that the RTR received a TCAP End message with no preceding dialogue and that originated from a network that could not be identified

6.3.2 FAF Counters

In the MIB, FAF filters are called "chains" and filter conditions are called "blocks". The available FAF counters are:

Counter	Description
fafChainsCounter	Number of times this action was applied
fafChainsTrue	Number of time this filter returned "true"
fafChainsFalse	Number of times this filter returned "false"
fafChainsRet	Number of times this filter caused an immediate return
fafBlocksTrue	Number of times this filter condition returned "true"
fafBlockFalse	Number of times this filter condition returned "false"
fafBlocksRet	Number of times this filter condition caused an immediate return
fafEciSentConnects	Number of connection requests sent
fafEciRcvdConnects	Number of connection requests received
fafEciGotConnects	Number of successful connections
fafEciSentClose	Number of close requests sent
fafEciRcvdClose	Number of close requests received
fafEciSentBytes	Number of bytes sent
fafEciRcvdBytes	Number of bytes received
fafEciSentMsgs	Number of packages sent
fafEciRcvdMsgs	Number of packages received

Counter	Description
fafEciSentPartial	Number of congestions
fafEciRcvdPartial	Number of partial receives
fafEciTimeDisconnected	Duration spent disconnected, in seconds
fafEciTimeConnecting	Duration spent connecting, in seconds
fafEciTimeConnected	Duration spent connected, in seconds
fafEciTimeCongested	Duration spent in congestion, in seconds (this time is also counted as connected)
fafEciRcvdRequests	Number of received evaluation requests
fafEciSentResponses	Number of sent evaluation responses
fafEciReqdNotifications	Number of requested notification indications
fafEciRcvdNotifications	Number of received notification indications
fafEciMissNotifications	Number of missed notification indications
fafEciSentLogin	Number of sent log-in requests
fafEciRcvdLogin	Number of received log-in confirmations
fafEciRefusedLogin	Number of received negative log-in responses
fafEciGrantedLogin	Number of received positive log-in responses
fafEciSentLifecheck	Number of sent life checks
fafEciRcvdLifecheck	Number of received life check confirmations
fafEciSentLogout	Number of sent logout requests
fafEciRcvdLogout	Number of received logout confirmations
fafEciLostSync	Number of disconnections due to lost synchronization
fafEciSentConfirmations	Number of sent notification confirmations
fafEciRcvdErrors	Number of received error messages
fafEciUnknownTags	Number of unknown ASN.1 tags received
fafEvalCountTestExpressionErrors	Number of malformed test expressions evaluated
fafEvalCountAssignmentExpressionErrors	Number of malformed assignment expressions evaluated
fafStringMatches	Total number of matched strings
fafDupsCountMsgs	Total number of messages that have matched this cluster
fafBulkCountMessages	Amount of messages that have been filtered out for this particular variable value

6.4 Using Statistics Viewer

The Statistics Viewer (STV) component provides statistics about SMS traffic in general, as well as organized by country and network. For the FWL, STV provides statistics about:

- Incoming traffic
- Outgoing traffic
- Through traffic
- Blocked traffic
- Unexpected traffic

For the FAF, STV provides statistics about:

- The number of evaluation requests the FAF has received from the RTR
- The number of times each advanced filter was applied
- The number of times each advanced filter returned "true" or "false"

Access STV using the MGR's **Statistics** menu. To see statistics related to blocked MO, MT, and SendRoutingInfoForSm traffic, go to **Statistics ➤ Blocked Traffic**. To see statistics related to the FAF, go to **Statistics ➤ Advanced Filters**.

6.5 Using Log Viewer

The Log Viewer (LGV) component enables you to:

- Configure the log profiles that the RTR/FWL uses to log events and messages
- Query the database in which the Log Processor (LGP) stores logged events and messages

LGV is an essential tool when planning your FWL configuration. If you create log profiles that track suspect traffic, you can observe what origins the FWL considers to be suspect and adjust your configuration accordingly.

Access LGV using the MGR's **Logging ➤ Messages** menu. To create a log profile that tracks suspect traffic, add a new profile and select "both legitimate and violated" from the **Legitimate/Violated Messages** list.

Refer to the MGR Operator Manual for information about creating and using log profiles, and to the LGP Operator Manual for information about the way LGP works.

Chapter 7

Configuration Parameter Reference

Topics:

7.1 Introduction

This section provides a reference of `tpconfig` attributes that are related to the FWL. These are configured in the RTR semi-static configuration file.

For a complete reference of RTR semi-static configuration entities and attributes, refer to the RTR Operator Manual. For a reference of entities and attributes that are related to the FAF, refer to the FAF Operator Manual.

7.2 firewallacceptnonnumericmtoriginatormsisdn

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR/FWL should accept numeric originator MSISDNs that contain the digits a-f in incoming MT messages.

If this attribute is set to "true", the format of the originator must not be changed by means of an MTO modifier. Doing so will lead to misformatted outgoing MT traffic. This attribute does not affect the handling of alphanumeric MSISDNs.

Valid Values

- false: Non-numeric originator MSISDNs are rejected
- true: Non-numeric originator MSISDNs are allowed

Default

false

7.3 firewallallowfallbacktosecdest

Mandatory/Optional

Optional

Location

Common configuration file

Description

This parameter indicates if fallback to secondary destination should be performed in Home-Routed scenario. If TRUE, fallback to secondary destination is performed based on the terminating mobile network configuration (mobNetworkPreferredMTDestination, mobNetworkEnableFallbackToSecondaryDestination).

Valid Values

- true
- false

Default

false

7.4 firewallassumepropertimezonegeneratingbysmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the FWL should assume that the time zone of an inbound MT message is correct, which impacts the time zone that the RTR uses as a base when applying MT modifiers.

Valid Values

- false: Use the time zone of the RTR/FWL as a base
- true: Use the time zone of the message as a base

Default

false

7.5 firewallcheckmospoofingafterextcondrules

Mandatory/Optional

Optional

Location

Common configuration file

Description

Changes the order in which the FWL performs the MO spoofing check and the MO rule evaluation.

Valid Values

- false: Execute the MO spoofing check first
- true: Evaluate the MOX rules first

Default

false

7.6 firewallenablemtrtgruleevaluationforsrismresponse

Mandatory/Optional

Optional

Location

Common configuration file

Description

Determines whether SRI-SM responses are subject to MTOR rules.

Valid Values

- false: Only MtForwardSm requests are subject to MTOR rules
- true: MtForwardSm requests and SRI-SM responses are subject to MTOR rules

Default

false

7.7 firewallenablemultisimservice

Mandatory/Optional

Optional

Location

Common configuration file

Description

Determines whether Nokia Multi-SIM support is enabled.

Valid Values

- false: Multi-SIM support is disabled
- true: Multi-SIM support is enabled

Default

false

7.8 firewallenablesrismrepublishingfortrustedsmsclist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Enables SRI-SM republishing for SMSCs on the trusted list.

Valid Values

- false: Do not republish SRI-SM requests from trusted SMSCs
- true: Republish SRI-SM requests from SMSCs on the trusted list

Default

false

7.9 firewallfollowmaplayermmsformtforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Controls how the More-Messages-to-Send (MMS) field of the MAP layer MtForwardSm operation (phase 2 and 2+) should be set in forwarded MT messages:

- false— the 3GPP TS 23.040 layer's TP-MMS field is followed
- true—the value as received at the MAP layer of the inbound operation is reproduced.

For intercepted MT traffic (TCAP CONTINUE messages) this flag is ignored as the outgoing MT/SM only indicates MMS if text insertion causes extra segments.

Valid Values

- false
- true

Default

false

7.10 firewallmaxintervalbetweensrismandmtfwdsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of seconds allowed between a SendRoutingInfoForSm (SRI-SM) and an MtForwardSm operation. This value is the lifetime of a correlation record.

In case multiple MtForwardSm messages (correlated to this record) are received within the set timer, the interval gets reset at every MtForwardSm received. If the MtForwardSm arrives at the FWL after the number of seconds specified in this parameter, the correlation record look-up will fail.

Valid Values

1-3600 seconds

Default

60 seconds

7.11 firewallmnproutingnumberforownnetwork

Mandatory/Optional

Optional

Location

Common configuration file

Description

MNP routing number of the HPLMN, which enables the FWL to identify MSISDNs that have been ported out. This value must start with zero.

7.12 firewallmoactionfororiginatingaddressspoofing

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when MO spoofing is detected.

Valid Values

- discardwithnoresponse: Discard the message and do not return an acknowledgement to the originator
- discardwithack: Discard the message and return an ACK to the originator
- discardwithnak: Discard the message and return a NACK to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

discardwithnoresponse

7.13 firewallmoactionforspoofingcheckfailureduetocallbarred

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take if the SendRoutingInfoForSm (SRI-SM) operation for the MO spoofing check returns "call barred".

Valid Values

- pass: Do not consider the message to be spoofed
- treatasifspoofing: Consider the message to be spoofed
- checkwithmapati: Use MAP ATI to attempt to retrieve the IMSI from the HLR, then compare the VLR address to the originating MSC address

Default

treatasifspoofing

7.14 firewallmoactionforspoofingcheckfailureduetotsvcnotprov

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take if the SRI-SM for the MO spoofing check returns "teleservice not provisioned".

Valid Values

- pass: Do not consider the message to be spoofed
- treatasifspoofing: Consider the message to be spoofed
- checkwithmapati: Use MAP ATI to attempt to retrieve the IMSI from the HLR, then compare the VLR address to the originating MSC address

Default

treatasifspoofing

7.15 firewallmofwdsmsccpcdpagtaiwhitelist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list of SMSC GTs that identify MoForwardSm operations that are destined for specific SMSCs. Only MoForwardSm operations with SCCP CDPAs that are in this list will be evaluated by the MO rules.

7.16 firewallmofwdsmwithspoofingperiod

Mandatory/Optional

Optional

Location

Common configuration file

Description

Period during which the MO spoofing threshold is calculated.

Valid Values

1-86,400 seconds

Default

3600 seconds

7.17 firewallmofwdsmwithspoofingthreshold

Mandatory/Optional

Optional

Location

Common configuration file

Description

Number of detected MO spoofing attempts within the spoofing period, beyond which the FWL will generate a trap.

Valid Values

0-1,000,000

Default

0 (disable functionality)

7.18 firewallmospoofingdigits

Mandatory/Optional

Optional

Location

Common configuration file

Description

Number of digits used to compare the MAP layer and SCCP layer MSC/SGSN global title (GT) as part of the MO spoofing check. Digits after this prefix can differ, and spoofing will not be detected. You can override this value per-network using the **Spoofing Check Digits** parameter in the MGR.

Default

4

7.19 firewallmospoofingcheckcondition

Mandatory/Optional

Optional

Location

Common configuration file

Description

Determines when the FWL performs the MO spoofing check.

Valid Values

- always: Always check
- whenmscsgsnaddressingsmscongt: Only check when the MSC or SGSN addresses the FWL using GT
- never: Never check

Default

always

7.20 firewallmospoofinghlrqueryceiling

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of HLR queries per second that the FWL may issue for MO spoofing checks.

Default

65,535

7.21 firewallmosmtrustedoriginatorlist[1..16]

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list (created in the MGR) containing MSISDNs that should be matched against the originator MSISDN in the MoForwardSm operation. If there is a match, the MO message is considered to be trusted.

The attribute must be specified as `firewallmosmtrustedoriginatorlist#`, where # is a number between 1 and 16.

Valid Values

Each list can contain up to 10,000 addresses.

7.22 firewallmospoofingsrismhlrgtwhitelist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list (created in the MGR) containing MSISDNs that should be matched against the HLR GT address received in the **SendRoutingInfoForSm** (SRI-SM) operation which was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

If this parameter is not configured, then, by default, it is considered to be an empty string and hence the RTR/FWL does not attempt to match any list of MSISDNs against the HLR GT address received.

7.23 firewallmospoofingsrismmscorsgsnwhitelist1

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a first list (created in the MGR) containing MSISDNs that should be matched against the MSC or SGSN in the SendRoutingInfoForSm (SRI-SM) operation that was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

7.24 firewallmospoofingsrismmscorsgsnwhitelist2

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a second list (created in the MGR) containing MSISDNs that should be matched against the MSC or SGSN in the SendRoutingInfoForSm (SRI-SM) operation that was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

7.25 firewallmospoofingsrismorigimsiwhitelist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list (created in the MGR) containing IMSIs that should be matched against the Originator IMSI received in the **SendRoutingInfoForSm** (SRI-SM) operation which was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

If this parameter is not configured, then, by default, it is considered to be an empty string and hence the RTR/FWL does not attempt to match any list of IMSIs against the Originator IMSI received.

7.26 firewallmscsgsnaddressinsuspectsrismresponse

Mandatory/Optional

Optional

Location

Host-specific configuration file

Description

Addresses from which the FWL will randomly select an address to replace the MSC and/or SGSN in a suspect SRI-SM response (to an SMSC). If no addresses are specified, the FWL uses its own GT.

Valid Values

Up to 10 E164 addresses, in international format, separated by spaces.

7.27 firewallmtactionforconflictingaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an SRI-SM or MtForwardSm with an SMSC address at the SCCP level that belongs to a different network from the SMSC address at the MAP level.

Valid Values

- discardwithtemporaryerror: Discard the message and return a temporary error to the originator
- discardwithpermanenterror: Discard the message and return a permanent error to the originator
- discardwithnoresponse: Discard the message and do not return an error to the originator

- pass: Allow the Mobile Messaging system to continue processing the message

Default

discardwithnoresponse

7.28 firewallmtactionformapsmscaddressspoofing

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an MtForwardSm with an SMSC address on the MAP level that belongs to a different network or country than the SMSC address on the MAP level of the corresponding SRI-SM operation.

Valid Values

- discardwithtemporaryerror: Discard the message and return a temporary error to the originator
- discardwithpermanenterror: Discard the message and return a permanent error to the originator
- discardwithnoresponse: Discard the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

discardwithnoresponse

7.29 firewallmtactionforsccpsmscaddressspoofing

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an MtForwardSm with an SMSC address on the SCCP level that belongs to a different network or country than the SMSC address on the SCCP level of the corresponding SRI-SM operation.

Valid Values

- discardwithtemporaryerror: Discard the message and return a temporary error to the originator
- discardwithpermanenterror: Discard the message and return a permanent error to the originator
- discardwithnoresponse: Discard the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

discardwithnoresponse

7.30 firewallmtactionforunknownmapaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an SRI-SM or MtForwardSm with an SMSC address at the MAP level that does not match any configured SMSC.

Valid Vaues

- discardwithtemporaryerror: Discard the message and return a temporary error to the originator
- discardwithpermanenterror: Discard the message and return a permanent error to the originator
- discardwithnoresponse: Discard the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

discardwithnoresponse

7.31 firewallmtactionforunknownsccpaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an SRI-SM or MtForwardSm with an SMSC address at the SCCP level that does not match any configured SMSC.

Valid Values

- discardwithtemporaryerror: Discard the message and return a temporary error to the originator
- discardwithpermanenterror: Discard the message and return a permanent error to the originator
- discardwithnoresponse: Discard the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

discardwithnoresponse

7.32 firewallmtactionforunsolicitedmtfwdsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the RTR/FWL receives an MtForwardSm that cannot be correlated to a previously received SendRoutingInfoForSm (SRI-SM).

Valid Values

- blockwithtemporaryerror: Block and return a temporary error to the SMSC
- blockwithpermanenterror: Block and return a permanent error to the SMSC
- blockwithnoresponse: Block and do not return a response to the SMSC
- blockwithack: Block and return an ACK to the SMSC

Default

blockwithnoresponse

7.33 firewallmtfwdsmwithspoofingperiod

Mandatory/Optional

Optional

Location

Common configuration file

Description

Period during which the MT spoofing threshold is calculated.

Valid Values

1-86,400 seconds

Default

3600 seconds

7.34 firewallmtfwdsmwithspoofingthreshold

Mandatory/Optional

Optional

Location

Common configuration file

Description

Number of detected MT spoofing attempts beyond which the FWL will generate a trap.

Valid Values

0-1,000,000

Default

0 (disables functionality)

7.35 firewallreportunknownsmscaddressnotifications

Mandatory/Optional

Optional

Location

Common configuration file

Description
Indicator specifying how to report that a SendRoutingForSm or MtForwardSm operation is received with an unknown SCCP or MAP address for the SMSC.

Valid Values

- astrap: Generate SNMP traps.
- aslogmessage: Write warnings to syslog instead.
- ignore

Default

astrap

7.36 firewallreportunknownsmscaddressnotificationstosyslog

Mandatory/Optional

Optional

Location

Common configuration file

Description
Changes the way the FWL reports a SendRoutingInfoForSm (SRI-SM) or MtForwardSm request containing an unknown SCCP or MAP SMSC address.

Valid Values

- false: Generate SNMP traps
- true: Do not generate SNMP traps; write warnings to syslog instead

Default

false

7.37 firewallrepublishsrismcdpasetsameasinitialsrism

Mandatory/Optional

Optional

Location

Common configuration file

Description

Changes the RTR/FWL's SCCP address modification for republished SendRoutingInfoForSm (SRI-SM) requests.

Valid Values

- false: Set the CDPA equal to the CDPA of the response to the original SRI-SM request
- true: Set the CDPA equal to the GT of the MSISDN to be queried

Default

false

7.38 firewallrepublishsrismnetworks

Mandatory/Optional

Optional

Location

Common configuration file

Description

List of networks to which SRI-SM republishing applies. When `firewallrepublishsrismnetworks` is assigned a value, the FWL assumes that republishing applies to all SRI-SM requests that are classified as suspect. For suspect SRI-SM requests, republishing is done whenever the network (as associated with the IMSI) is equal to one of the specified networks.

Valid Values

List of up to 10 networks in the format:

1. Two-letter country code (according to ISO 3166)
2. A hyphen
3. The name of a network defined in the MGR

For example:

```
nl-kpn,nl-vodafone
```

7.39 firewalltrustedsmsclist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list containing the GTs of SMSCs for which the FWL should skip the MT spoofing check.

7.40 firewallusecommonaddressinsuspectmtforwardsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if the SMSC address at the MAP layer of suspect MtForwardSm requests should be replaced with the common address of the RTR/FWL.

Valid Values

- false: Do not replace the SMSC address
- true: Replace the SMSC address with the value specified in the commonaddress attribute

Default

false

7.41 firewallusehlraddressassccpcgpainsuspectsrismresponse

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if the SCCP CGPA in a suspect SendRoutingInfoForSm (SRI-SM) response (to an SMSC) should be replaced with the GT of the HLR.

Valid Values

- false: Use the GT of the RTR
- true: Use the GT of the HLR

Default

false

7.42 firewallussdrequestforretrievingmultisimstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

String to use in the USSD request that checks if an MSISDN is subscribed to the Nokia multi-SIM service.

Default

*137#

7.43 firewallussdresponseformultisimstatusdisabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

String that the HLR includes in the USSD response, indicating that an MSISDN is not subscribed to the Nokia multi-SIM service.

Default

NOT SUCCESSFUL

7.44 includemscaddrinmofwdsmtosmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies when the MSC address shoud be included in the CGPA of the MoForwardSm operation toward the SMSC.

Valid Values

- never: Never include the MSC address
- always: Always include the MSC address
- foreignonly: Only include the MSC address when the MSC is located in another country

Default

never

7.45 mtpermanentdiscarderrorformscorsgsn

Mandatory/Optional

Optional

Location

Common configuration file

Description

MAP error that the FWL returns to the SMSC when `firewallmtactionforunsolicitedmtfwdsm` is set to "blockwithpermanenterror".

Valid Values

- unknownsubscriber
- absentsubscriber
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror
- unknownservicecentre
- sccongestion
- invalidsmeaddress
- subscribernotscsubscriber

Default

unknownsubscriber

7.46 mttemporarydiscarderrorformscorsgsn

Mandatory/Optional

Optional

Location

Common configuration file

Description

MAP error that the FWL returns to the SMSC when `firewallmtactionforunsolicitedmtfwdsm` is set to "blockwithtemporaryerror".

Valid Values

- unknownsubscriber
- absentsubscriber
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror
- unknownservicecentre
- sccongestion
- invalidsmeaddress
- subscribernotscsubscriber

Default

absentsubscriber

7.47 pcssnroutingwhenincludingmscaddrinmofwdsmtosmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if the SCCP CGPA routing indicator should be set to PC/SSN when the MSC address is included in the CGPA of the MoForwardSm operation toward the SMSC.

Valid Values

- false: Do not set the routing indicator to PC/SSN
- true: Set the routing indicator to PC/SSN

Default

false

7.48 tcapmaxapplicationguardtime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining maximum time span allowed between receiving Invoke and response from higher layer for Invoke. Expressed in units of seconds.

Valid Values

1 - 100 (value in seconds)

Default

30 seconds

7.49 tcapmaxlongresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for long MAP operations defining maximum time span allowed between a TCAP request message (TC-BEGIN, TC-CONTINUE) and a TCAP response (TC-END, TC-CONTINUE), expressed in seconds. This timer applies to the MAP MtForwardSm operation.

The value of this timer will be applicable when:

1. No network is configured for the recipient or
2. Value of the **MTFSM max response time** field for the recipient network is configured to 0 (default value).

Valid Values

1 - 100 seconds

Default

30 seconds

7.50 tcapmaxnegotiationestablishresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining maximum time span allowed between a TC-Begin sent by RTR without component to initiate a Dialogue and subsequent TC-Continue received without component on the same TCAP session, expressed in units of seconds.

Valid Values

1 - 100 (value in seconds)

Default

5 seconds

7.51 tcapmaxnextmessagewaitingresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining maximum time span allowed between a TC-CONTINUE sent and subsequent TC-Continue received on the same TCAP session, expressed in units of seconds. This timer is applicable only for the scenario where RTR is a TCAP transaction receiver.

Valid Values

1 - 100 (value in seconds)

Default

5 seconds

7.52 tcapmaxreportsmresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for Report SM Delivery Status operation defining maximum time span allowed between a 'Report SM delivery status' request from the RTR and its response, expressed in units of seconds.

The default value is 0, which indicates that the system-wide timer value *tcapmaxresponsetime* will be used.

Valid Values

0 - 100 (value in seconds)

Default

0 seconds

7.53 tcapmaxresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for regular MAP operations defining maximum time span allowed between a TCAP request message (TC-BEGIN, TC-CONTINUE) and a TCAP response (TC-END, TC-CONTINUE), expressed in seconds. This timer applies to any MAP operation other than MtForwardSm.

If the following timers are configured with a non-zero value, then they override the `tcapmaxreponsetime` value:

1. *tcapmaxsrismresponsetime*
2. *tcapmaxreportsmresponsetime*

Note: If the value of the semi-static parameter *tcapmaxresponsetime* is changed from its default value of 5 seconds, consider changing the values of the semi-static parameters *tcapmaxnegotiationestablishresponsetime* and *tcapmaxnextmessagewaitingresponsetime* as well.

Valid Values

1 - 100 (value in seconds)

Default

5 seconds

7.54 tcapmaxsrismresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for SRISM operation defining the maximum time span allowed between a SRISM Request from the RTR and its Response. This value is expressed in seconds.

The default value is 0, which indicates that the system-wide timer value *tcapmaxresponsetime* will be used.

Valid Values

0 - 100 (value in seconds)

Default

0 seconds

7.55 tcaprelaytccontinueonvpc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies how the FWL should handle a TC-CONTINUE that it receives on a VPC (only supported for an ITU-T SS7 stack)

Valid Values

- false: Pass TC-CONTINUE to the MAP layer for further processing
- true: Derive the TC-CONTINUE destination
  - If the destination is the FWL, the FWL treats the TC-CONTINUE as if it were received on that PC
  - If the destination is another firewall, the FWL relays the TC-CONTINUE to that firewall (if an MTP destination exists for it)

Default

false

7.56 ttwhenincludingmscaddrinmofwdsmtosmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TT when the MSC address is included in the SCCP CGPA of an MoForwardSm operation toward an SMSC.

Default

The default for ITU-T is 0. The default for ANSI is 10.

7.57 whitelistofmomscforspoofchecksuppression

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list of MSC GTs that should be matched against the originator of an MO message. If there is match, the FWL does not perform an MO spoofing check for the message.

Appendix A

References

Topics:

A.1 References

1. 3GPP TS 23.040 v6.2.0
2. NewNet Mobile Messaging RTR Operator Manual
3. NewNet Mobile Messaging FAF Operator Manual
4. NewNet Mobile Messaging MGR Operator Manual
5. NewNet Mobile Messaging Billing Manual
6. NewNet Mobile Messaging SNMP Trap Reference Guide
7. NewNet Mobile Messaging LGP Operator Manual

Glossary