Oracle® Communications

Diameter Signaling Router

DSR Security App Using Mediation Example Procedure

Release 8.2

E88987-01

January 2018

ORACLE

Oracle Communications DSR Security Application Using Mediation Example Procedure User's Guide, Release 8.2

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (MOS) (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

See more information on My Oracle Support (MOS).

Disclaimer: This is just a reference to an example for creating security application using DSR Mediation functionality.

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose and Scope

This document provides a sample procedure required to build a security application using mediation.

No additional software installation is required before executing this procedure. The standard DSR installation procedure loads all required software. You do need to activate the Mediation feature before implementing the security application.

1.2 Overview of Security Application

- Most of the Diameter security vulnerabilities are for interconnect from roaming networks through IPX or directly from roaming partner networks.
- DEA is considered as the only point of contact into and out of an operator's network at the Diameter application level.
- Attacks are induced in operator's home network through Diameter messages passing through DEA.
- Security threats currently being discussed for SS7 are around below mentioned attacks:
  - Location tracking
  - Call intercept
  - Subscriber Denial of Service
  - Subscriber Account fraud
  - SMS SPAMS
- DSR based Diameter Security Countermeasures can be used to mitigate different diameter attacks.
- Diameter security countermeasures shall be implemented using ART or Mediation rules based screening.
- In this user guide, we use Mediation to configure and implement Diameter security countermeasures (Security Application).
- Diameter Security Countermeasures shall be applied on:
  - Ingress messages received from the peers of external foreign network
  - Egress messages sent from home network to external foreign network.
- For the purposes of applying countermeasures, subscribers are classified into one of following three types:
  - Inbound roaming subscribers: Security countermeasures are applicable for visited network subscribers roaming in home network
  - Outbound roaming subscribers: Security countermeasures are applicable for home network subscribers roaming in visited network
  - Non-Roaming home network subscribers: Security countermeasures are applicable for home network subscribers who are not roaming outside home network

2. Example Procedure

This section list the steps followed to build the sample security application using mediation. The security application uses various countermeasure checks. User may vary the templates (add/delete/modify) as per their needs.

Test Setup topology: DSR Setup with 1 NO + 1 SO + 1 MP. In the example (sample testing), DSR 80.14.1 is used with 1 NO + 1 SO + 1 MP, and taken as reference in this user guide.

2.1 Define Internal Variables

The internal variable provides inputs (i.e., Peer Type, Roamer Type, etc.) to templates, which implements countermeasures, generates alarms, and drops the vulnerable message.

To configure Internal Variables:

1. Launch an active SO GUI.
2. Navigate to **Main Menu -> Diameter -> Mediation -> Internal Variables Screen**.
3. Click **Insert** to insert each internal variable individually.
4. Define the internal variables as shown in Table 1 and shown in Figure 1 as reference. The templates set and read these internal variables.

Table 1: Internal Variables

Variable Name	Description	Type	Default Value
$msgDisallowed	If true, then message is not allowed further; false then message is allowed and it is still tracked by other templates.	Integer32	0
$foreignIngressPeer	If true, then message is from foreign network to home network.	Integer32	0
$foreignEgressPeer	If true, then message is from home network to foreign network.	Integer32	0
$inboundRoaming	If true, then subscriber is inbound subscriber.	Integer32	0
$outboundRoaming	If true, then subscriber is outbound subscriber.	Integer32	0
$index	Used as an index to delete the multiple occurrence of an AVP in one shot	Integer32	0

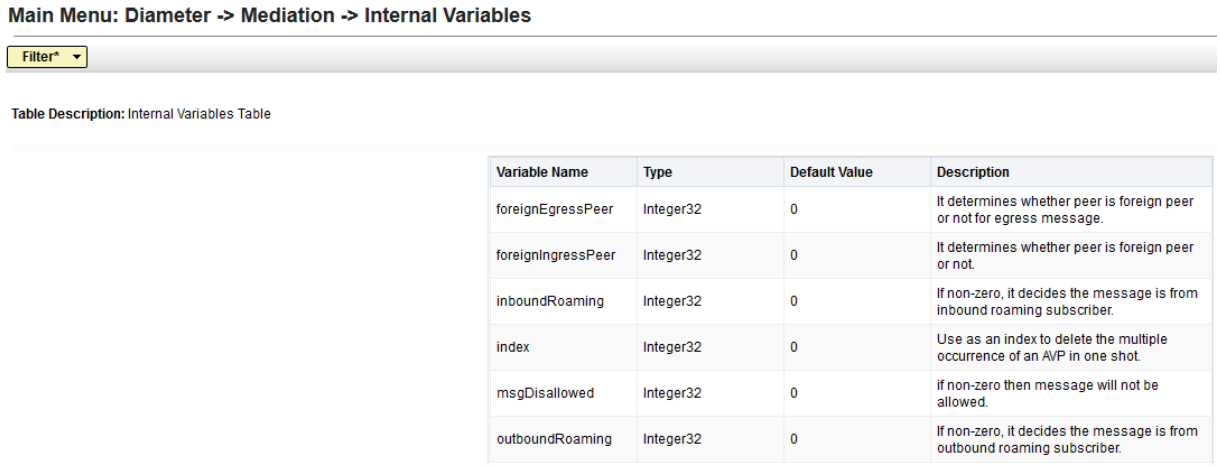


Figure 1: Define Internal Variables

2.2 Define Measurements

Measurements calculate the number of vulnerable messages dropped by the Security application. For each type of countermeasure, create an entry.

To configure Measurements,

1. Launch an active SO GUI.
2. Navigate to **Main Menu -> Diameter -> Mediation -> Measurements**.
3. Click **Insert** to insert each measurement individually.

Use the measurements from Table 2 and shown in Figure 2 as a reference for this example.

Table 2: Measurements

Measurement Name	Description
measurement_inbound_10	Application ID and CC whitelist for inbound roamers
measurement_outbound_20	Application ID and CC whitelist for outbound roamers
measurement_DRWhitelist_40	DR whitelist
measurement_DestRealm_ER_100	Destination Realm Egress Request
measurement_Handle_RRecordAVP_60	Handle Route Record AVP
measurement_OH_ends_with_OR_50	OH ends with OR
measurement_ORWhitelist_30	OR whitelist

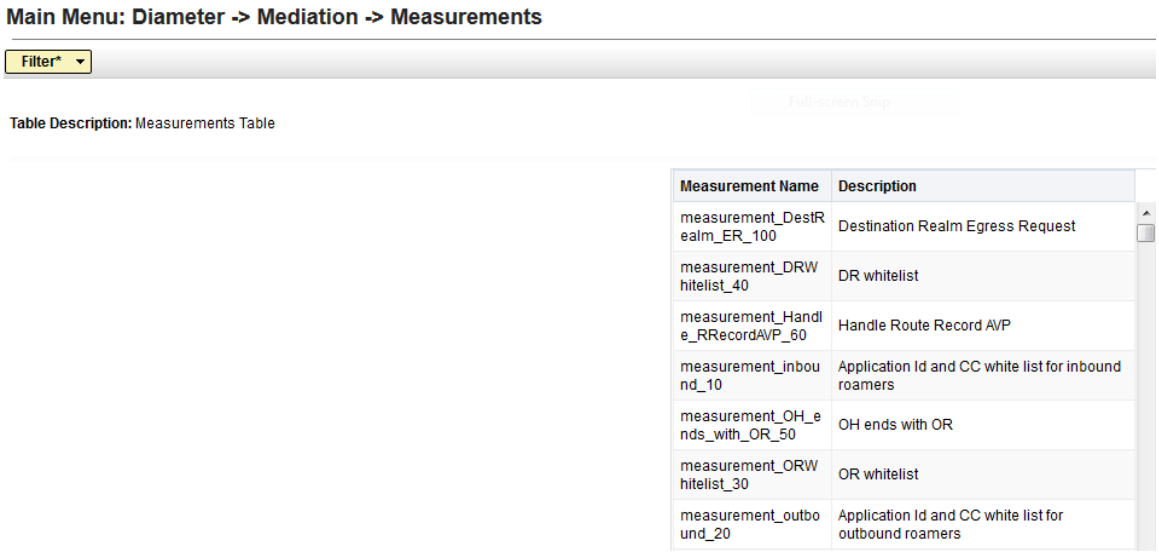


Figure 2: Sreenshot of Measurements

2.3 Add AVP to DSR Custom Dictionary

Add the following AVPs to the DSR custom dictionary:

2.3.1 OC-Supported-Features AVP

OC-Supported-Features ::= < AVP Header: 621 >
[OC-Feature-Vector]
* [AVP]

2.3.2 OC-OLR AVP

OC-OLR ::= < AVP Header: 623 >

< OC-Sequence-Number >

< OC-Report-Type >

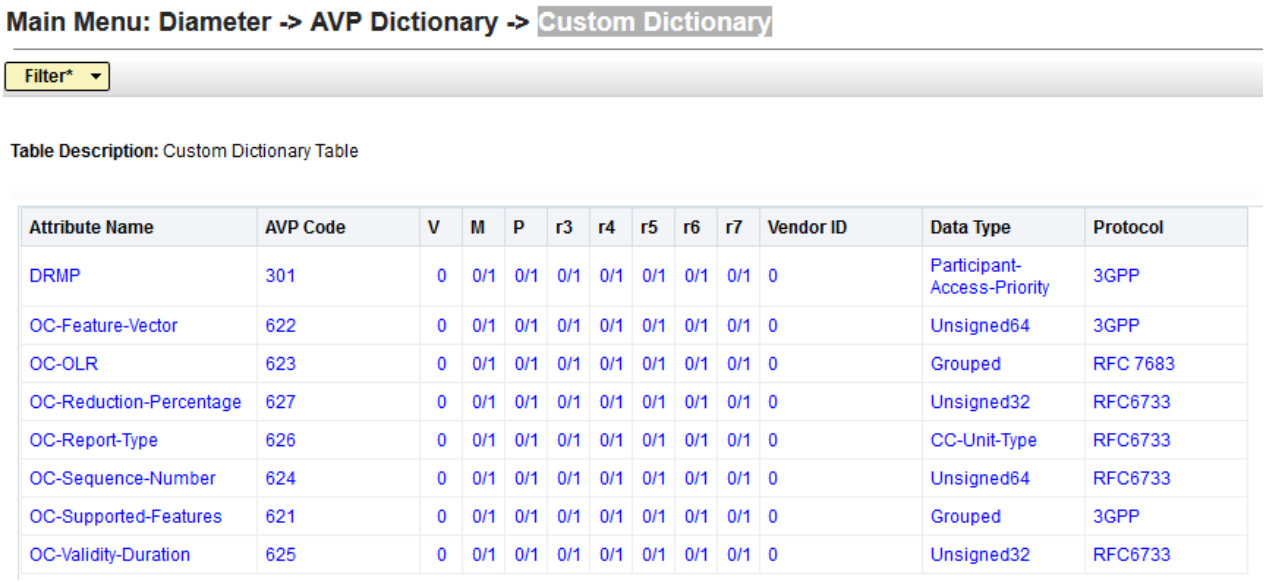
[OC-Reduction-Percentage]

[OC-Validity-Duration]

* [AVP]

2.3.3 DRMP AVP

The DRMP (AVP code 301) is an Enumerated type. Use Figure 3 as a reference.



Main Menu: Diameter -> AVP Dictionary -> Custom Dictionary

Filter*

Table Description: Custom Dictionary Table

Attribute Name	AVP Code	V	M	P	r3	r4	r5	r6	r7	Vendor ID	Data Type	Protocol
DRMP	301	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	Participant-Access-Priority	3GPP
OC-Feature-Vector	622	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	Unsigned64	3GPP
OC-OLR	623	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	Grouped	RFC 7683
OC-Reduction-Percentage	627	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	Unsigned32	RFC6733
OC-Report-Type	626	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	CC-Unit-Type	RFC6733
OC-Sequence-Number	624	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	Unsigned64	RFC6733
OC-Supported-Features	621	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	Grouped	3GPP
OC-Validity-Duration	625	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0	Unsigned32	RFC6733

Figure 3: Screenshot of DRMP AVP

2.4 Ruleset Configuration

To implement all six counter measures, configure the 14 Mediation templates. A few of these templates are common (i.e., not related to any specific counter measure), which performs generic actions like computing Peer Type/Roamer Type, generating alarms, pegging corresponding counters, and dropping the vulnerable messages. The remaining templates implement the counter measure specific business logic.

Refer to Table 1 to see counter measures to template mapping.

Table 3: Mediation Templates

Counter Measure Name	Used Template
Application-ID Whitelist Screening	Template 2 & 3
Application-ID and Command Code Consistency Check	Template 2 & 3
Origin Realm and Destination Realm Whitelist Screening	Template 4, 5 & 11
Origin host and Origin Realm Consistency Check	Template 6
Route-Record Validation	Template 7
Removal of Blacklisted AVPs	Template 9a, 9b, 12a & 12b

2.4.1 Template 1: Roaming Scenario Identification

This template computes Peer Type [Foreign or Home Peer], Roamer Type [Inbound or Outbound roamer], which is used by remaining templates.

It is associated with trigger point RTP1.

Template Definition

If @dsr.ingress.peer equals list of foreign peers

Then

Set Internal Variable: $foreignIngressPeer = 1

Set Internal Variable $outboundRoaming = (@msg.avp["User-Name"][1].imsi.mccmnc == <LOCAL MCCMNC>)

Set Internal Variable: $inboundRoaming = !$outboundRoaming

This template sets internal variables if ingress peer is listed in a foreign peer list.

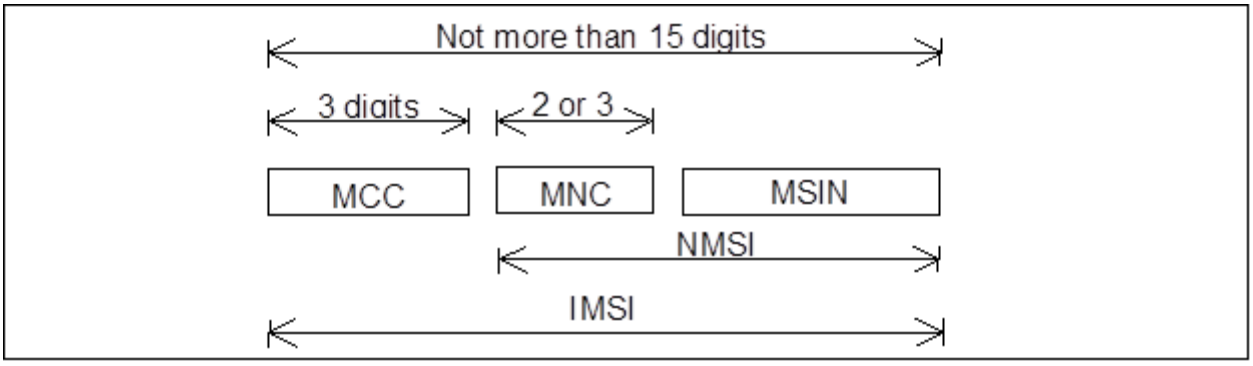
If the peer is in the whitelist then, check IMSI (International Mobile Subscriber Identity) from User-Name AVP to find out the home network of this user.

If the MCCMNC (extracted from IMSI) is equal to the local MCCMNC, then this subscriber is an **outbound** roaming subscriber.

If the MCCMC (extracted from IMSI) is not equal to the local MCCMNC, then this subscriber is an **inbound** roaming subscriber.

How to Extract MCC and MNC from IMSI Stored in USIM

The value of MNC (two or three digits) depends on the value of MCC.



In our sample testing, we used the following IMSIs:

Table 4: Sample IMSIs

MCC	MNC	Country	IMSI	Network
404	17	India	404179712345678	Home Network Subscriber
460	02	China	460022112345678	Foreign Network Subscriber

These IMSIs have been used for outbound and inbound subscriber in our sample testing and can be used as a reference.

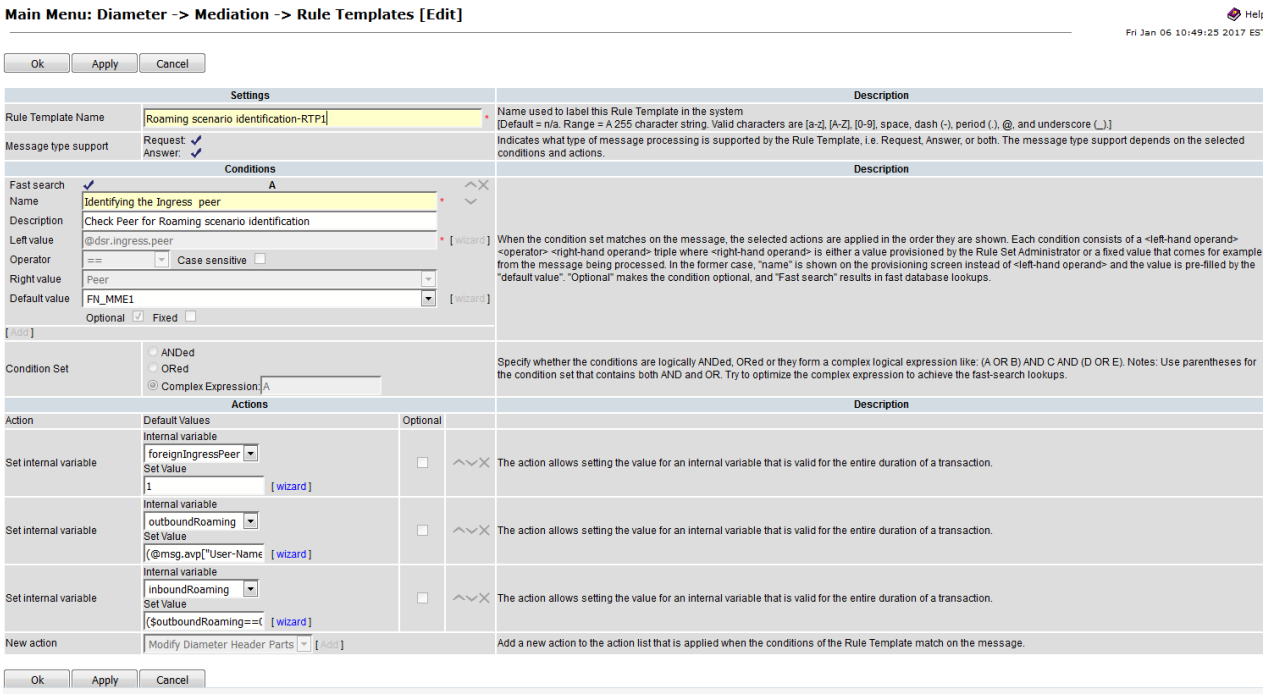


Figure 4: Screenshot of Roaming Scenario Identification Template

2.4.2 Template 2: Application ID and CC WhiteList for Inbound Roamers

This template is applicable for the subscriber marked as Valid Inbound Subscriber by Template 1 "Roaming Scenario Identification."

If the diameter message is for inbound subscriber, then this template is executed.

This template checks for $msgDisallowed (to allow this message or not), @msg.application_id (to check that application ID is in the whitelist or not) and @msg.command.code (to check that this command code is allowed or not).

If above conditions are satisfied, then it allows the message by setting $msgDisallowed = 0.

If not satisfied, then it abandons the message by setting $msgDisallowed = 10. 10 indicates "Application ID and CC whitelist for inbound roamers" template check fails for this message. Hence, every template sets a different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

Template Definition

IF	$inboundRoaming	is	true
AND	$msgDisallowed	is	false
AND	@msg.application_id	equals	list of application IDs
AND	@msg.command.code	equals	list of command-codes per application ID
THEN	Set Internal Variable:	$msgDisallowed = 0 for all the rules except the default rule: $msgDisallowed = 10	

Note: CC can be optional, i.e., App-ID can be put on the whitelist without setting any CC. If you decide not to put CC in the whitelist, then only the App-ID filters the messages irrespective of CC in messages.

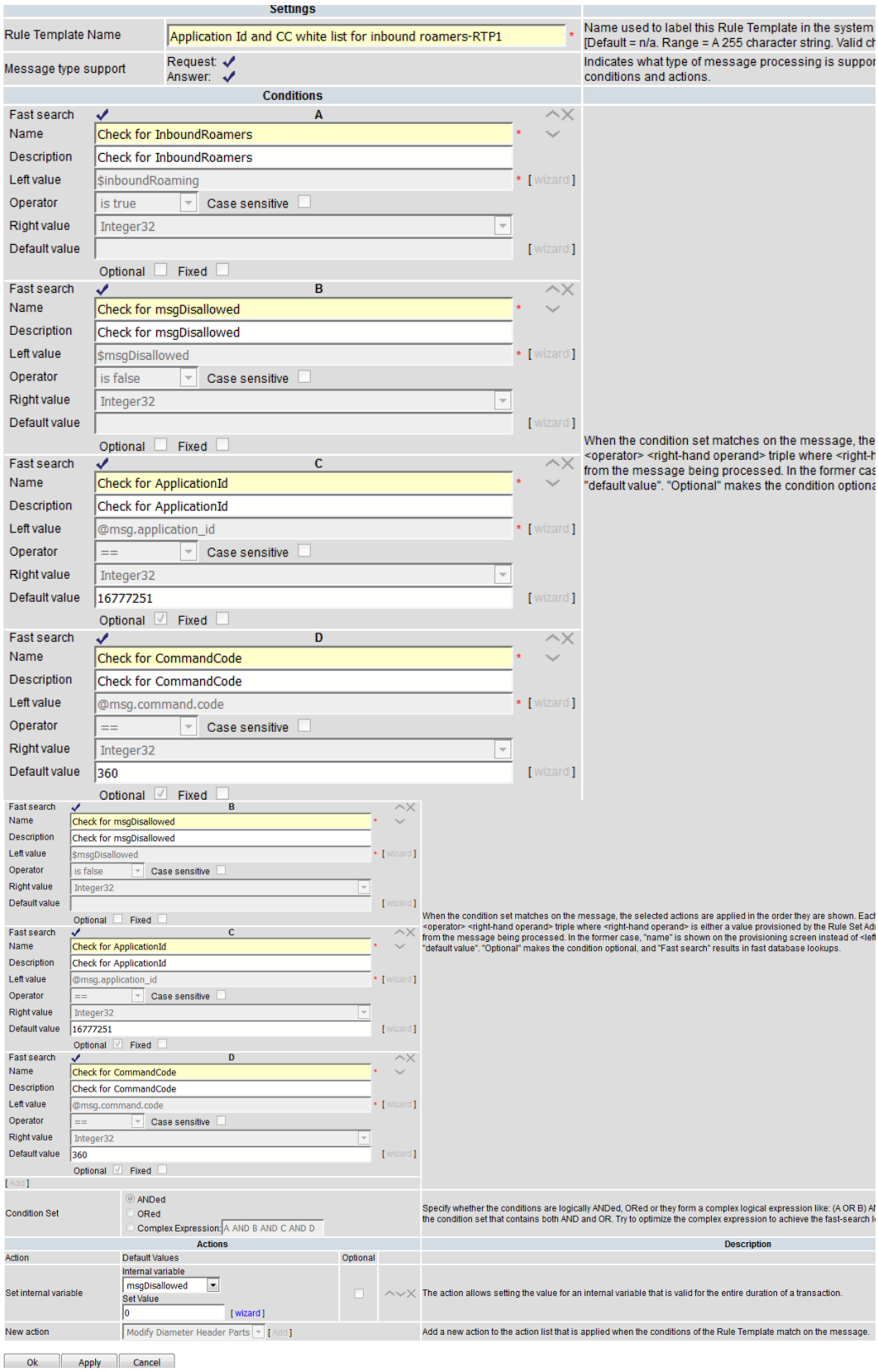


Figure 5: Screenshot of Application ID and CC Whitelist for Inbound Roamers Configured Template

2.4.3 Template 3: Application ID and CC Whitelist for Outbound Roamers

This template is applicable for the subscriber marked as Valid Outbound Subscriber by Template 1(i.e., roaming scenario identification).

If the diameter message is from outbound subscriber, then this template is executed.

This template checks for $msgDisallowed (to allow this message or not), @msg.application_id (to check that application ID is in the whitelist or not) and @msg.command.code (to check that this command code is allowed or not).

If above conditions satisfied, then it allows the message by setting $msgDisallowed = 0.

If not satisfied, then it abandons the message by setting $msgDisallowed = 20. 20 indicates “Application ID and CC whitelist for outbound roamers” template check fails for this message. Hence, every template sets a different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

Template Definition

IF	$inboundRoaming	is	true
AND	$msgDisallowed	is	false
AND	@msg.application_id	equals	list of application IDs
AND	@msg.command.code	equals	list of command-codes per application ID
THEN	Set Internal Variable:	$msgDisallowed = 0 for all the rules except the default rule: $msgDisallowed = 20	

Note: CC can be optional, i.e., App-ID can be put on the whitelist without setting any CC. If you decide not to put CC in the whitelist, then only the App-ID filters the messages irrespective of CC in messages.

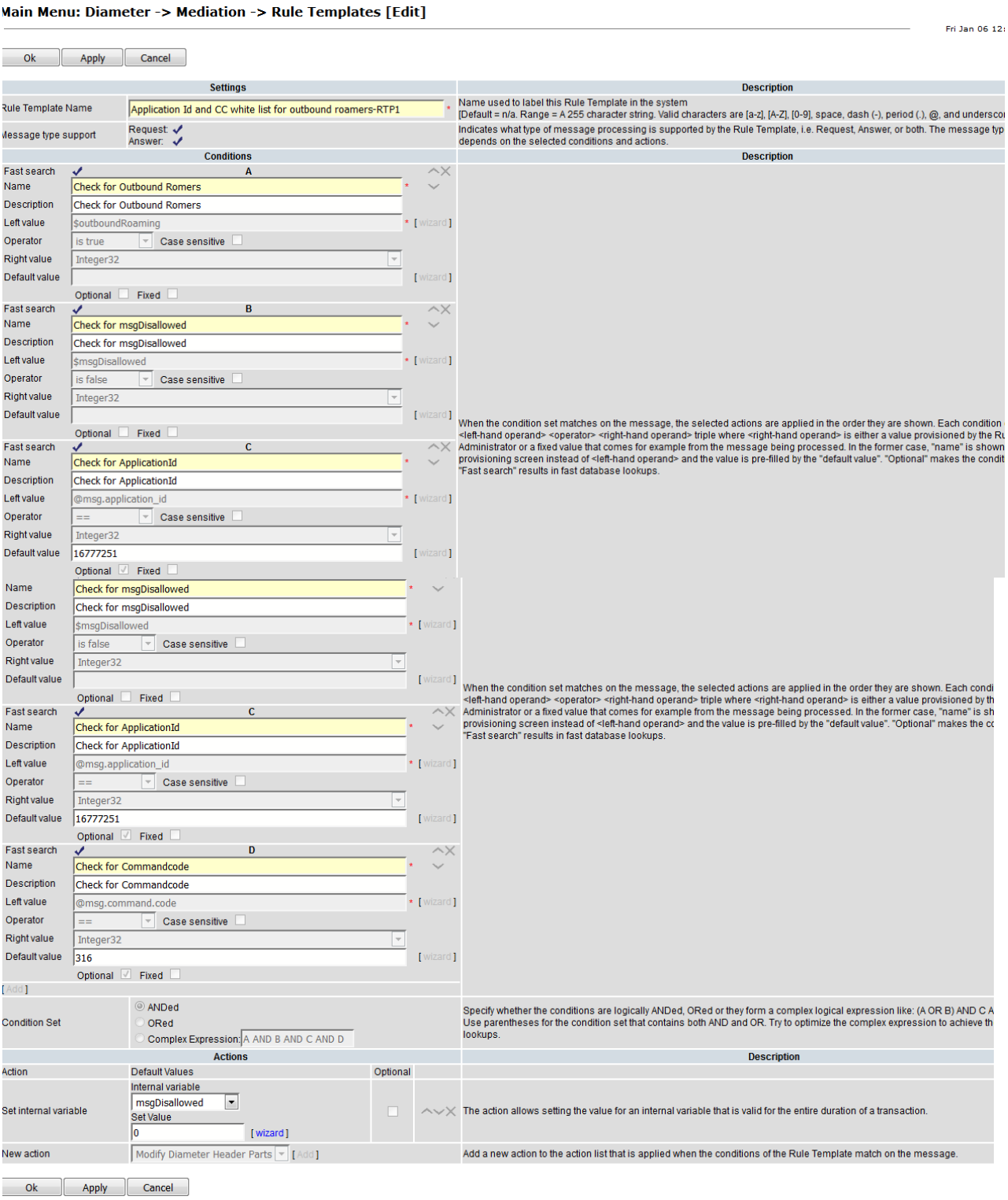


Figure 6: Screenshot of Application ID and CC Whitelist for Outbound Roamers Configured Template

2.4.4 Template 4: OR Whitelist

This template checks the Origin Realm of the incoming diameter message against the whitelist of Origin Realms. If the message's Origin Realm is in the whitelist, then the diameter message is allowed for further processing, otherwise it is not.

This template checks for $foreignIngressPeer (whitelisted foreign peer), $msgDisallowed (to allow this message or not), and @msg.avp["Origin-Realm"] (to check that message's Origin Realm is in the whitelist or not).

If above conditions are satisfied, then it allows the message by setting $msgDisallowed = 0.

If not satisfied, then it abandons the message by setting $msgDisallowed = 30. 30 indicates "OR whiltelist" template check fails for this message. Hence, every template sets a different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

Template Definition

IF	$foreignIngressPeer	is	true
AND	$msgDisallowed	is	false
AND	@msg.avp["Origin-Realm"]	equals	list of ORs
THEN	Set Internal Variable:	$msgDisallowed = 0 for all the rules except the default rule: $msgDisallowed = 30	

Note: The Origin-Realm is an optional condition. If you do not want to check origin realm, then use the empty value of origin realm or do not use this template.

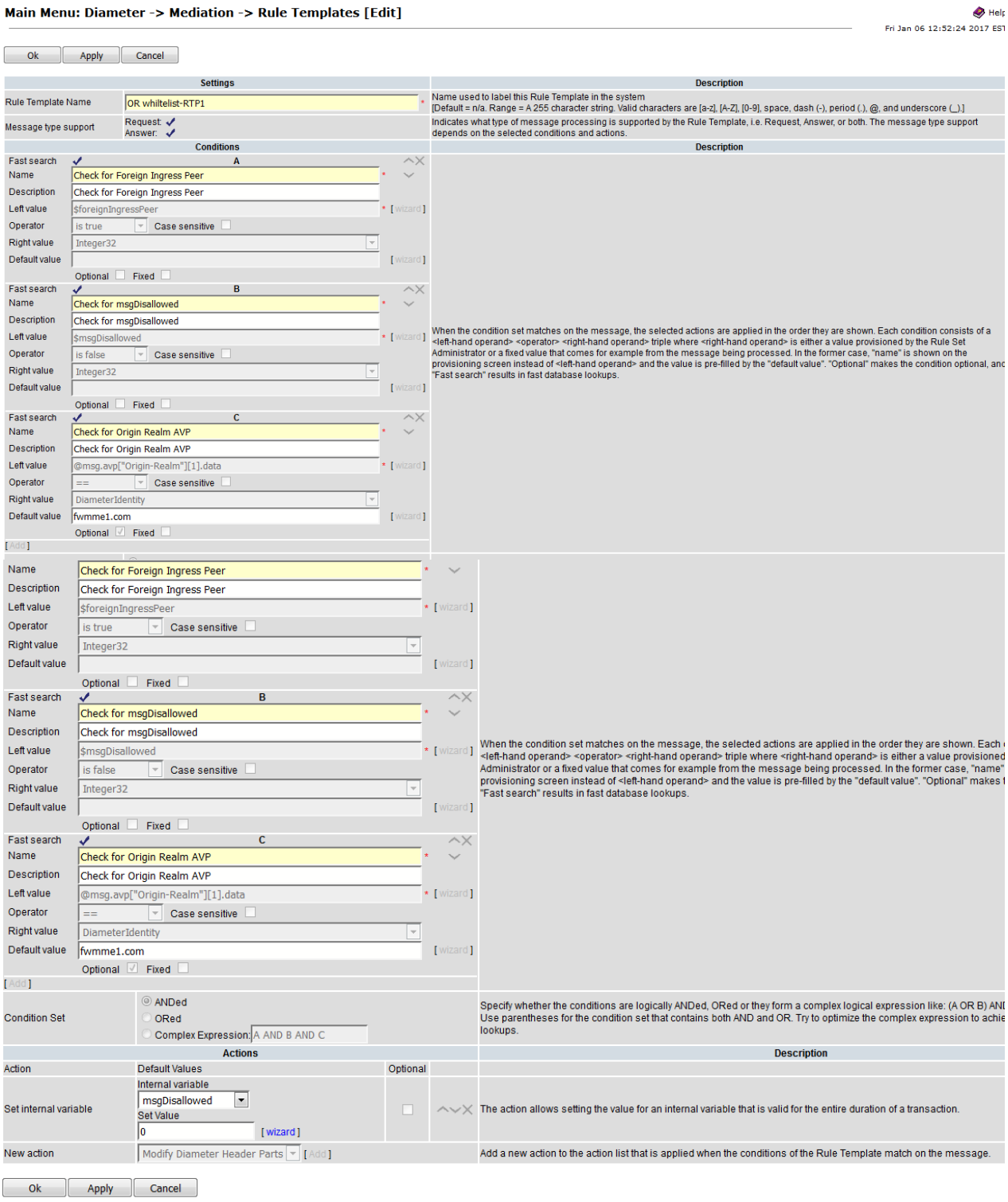


Figure 7: Screenshot of OR Whitelist Configured Template

2.4.5 Template 5: DR Whitelist

After successful execution of Template 4 “OR Whitelist,” if $msgDisallowed is 0 (message is still allowed for further processing), then Template 5 DR Whitelist is executed.

This template checks the Destination Realm of the incoming diameter message against the whitelist of Destination Realms. If the Destination Realm is in the whitelist, then the diameter message is allowed for further processing.

This template checks for $foreignIngressPeer (whitelisted foreign peer), $msgDisallowed (to allow this message or not), and @msg.avp["Destination-Realm"] (to check that Destination Realm is in the whitelist or not).

If above conditions are satisfied, then it allows the message by setting $msgDisallowed = 0.

If not satisfied, then it abandons the message by setting $msgDisallowed = 40. 40 indicates “DR whiltelist” template check fails for this message. Hence, every template sets different msgDisallowed value in case of failure.

It is associated with trigger point RTP1.

Template Definition

IF	$foreignIngressPeer	is	true
AND	$msgDisallowed	is	false
AND	@msg.avp["Destination-Realm"]	equals	list of DRs
THEN	Set Internal Variable:	$msgDisallowed = 0 for all the rules except the default rule: $msgDisallowed = 40	

Note: The Destination-Realm is an optional condition. If you do not want to check the destination realm, then use the empty value of destination realm or do not use this template.

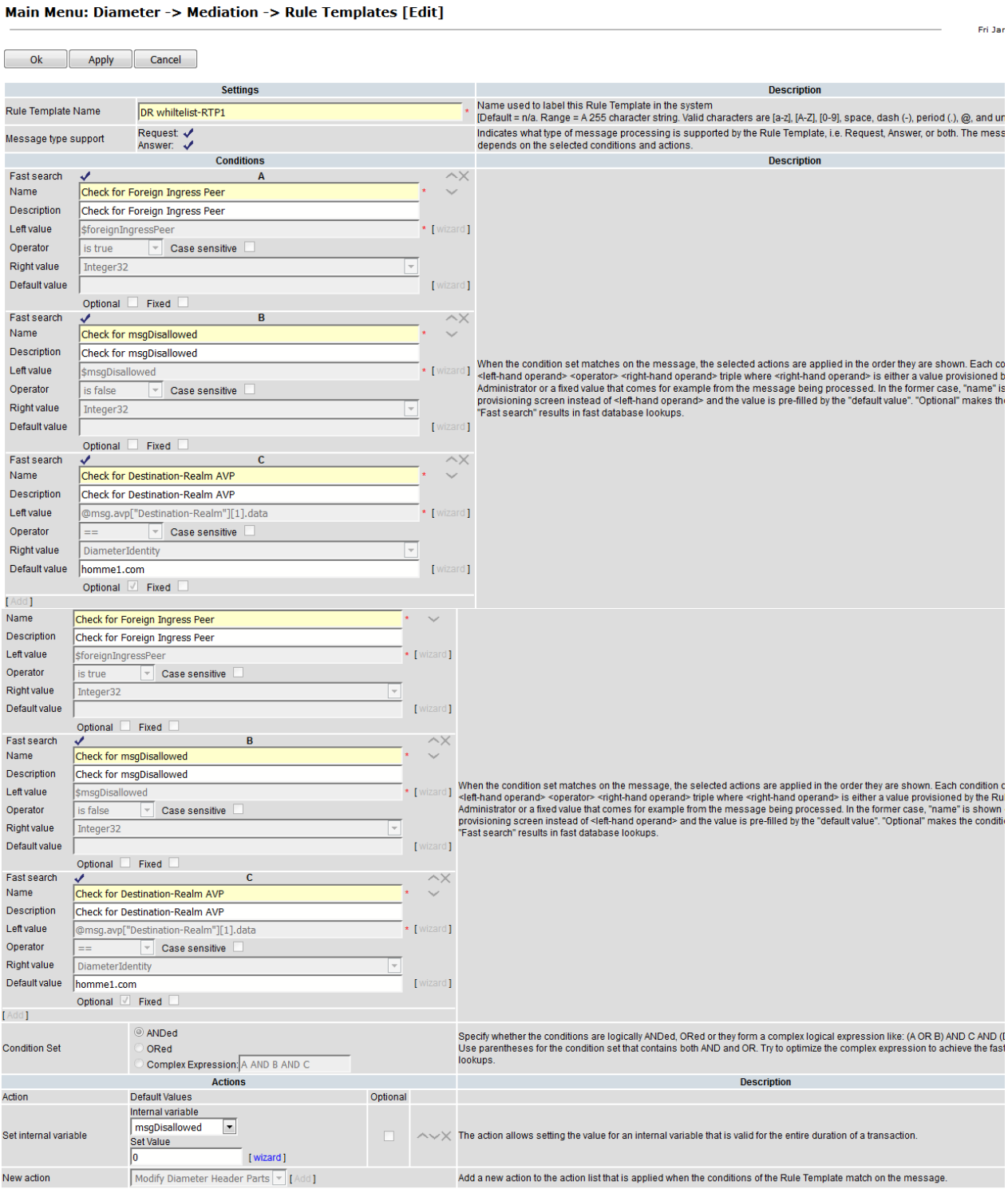


Figure 8: Screenshot of DR Whitelist Configured Template

2.4.6 Template 6: OH Ends with OR

After successful screening of the diameter message with Template 5 “DR whitelist,” if the internal variable $msgDisallowed is still false, then it means the diameter message is allowed for further processing and Template 6 “Origin Host Ends with Origin Realm” is executed.

This template picks the Origin-Host and Origin-Realm AVP from the diameter message and it checks that the Origin-Host is ending with Origin-Realm or not.

If not, then it abandons the diameter message and sets $msgDisallowed = 50.

It also checks for $foreignIngressPeer and $msgDisallowed in the same way as it has been tested by the previous template.

It is associated with trigger point RTP1.

Template Definition

IF	$foreignIngressPeer	is	true
AND	$msgDisallowed	is	false
AND	@msg.avp["Origin-Host"]	does not end with	"." + @msg.avp["Origin-Realm"]
THEN	Set Internal Variable:	$msgDisallowed = 50	

Below is the screen shot of configured template “OH ends with OR”:

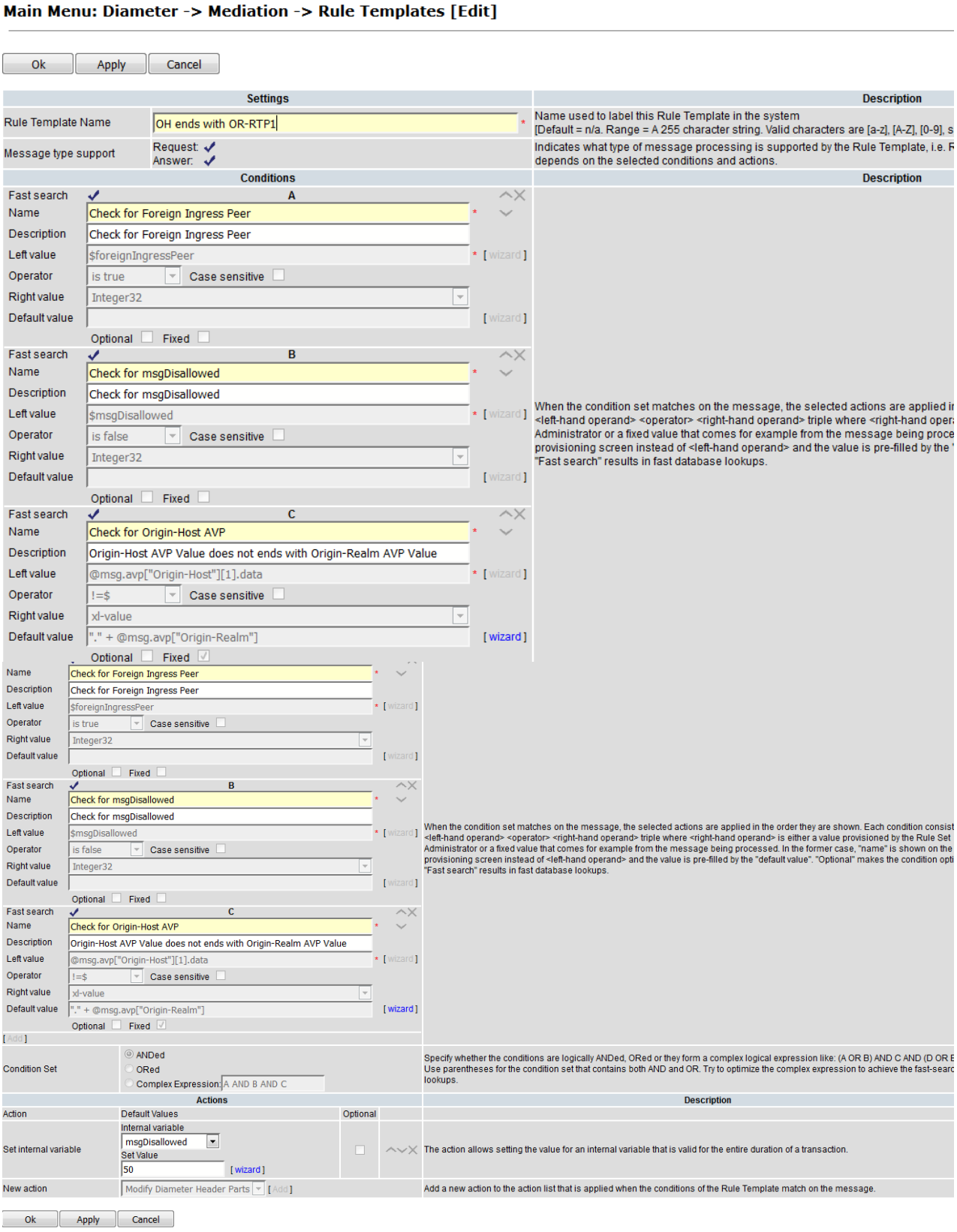


Figure 9: Screenshot of OH Ends with OR Configured Template

2.4.7 Template 7: Handle Route Record AVP

After successful screening of diameter message with Template 6 “OH Ends with OR,” if the internal variable $msgDisallowed is still false, it means the diameter message is allowed for further processing and Template 7 “Handle Route Record AVP” is executed.

This template basically iterated through all the route record AVPs which are present in the diameter message and will compare each rout record AVP with blacklist of Realms. If any Rout Record AVP from diameter message match with ANY realm from blacklisted realms then it will abandoned the message by setting $msgDisallowed = 60.

It is associated with trigger point RTP1.

Template Definition

IF	$foreignIngressPeer	is	true
AND	$msgDisallowed	is	false
AND	`@msg.avp["Route-Record"][any].data	ends with	list of realms
THEN	Set Internal Variable:	$msgDisallowed = 60	

Note: In this template, we are using ANY keyword, which acts as a loop and iterates through all the route record AVPs to find out blacklisted realms present in any of the route record AVPs. Create one rule for each blacklisted realm.

The right hand side type is set to xl-value to a force slow-search.

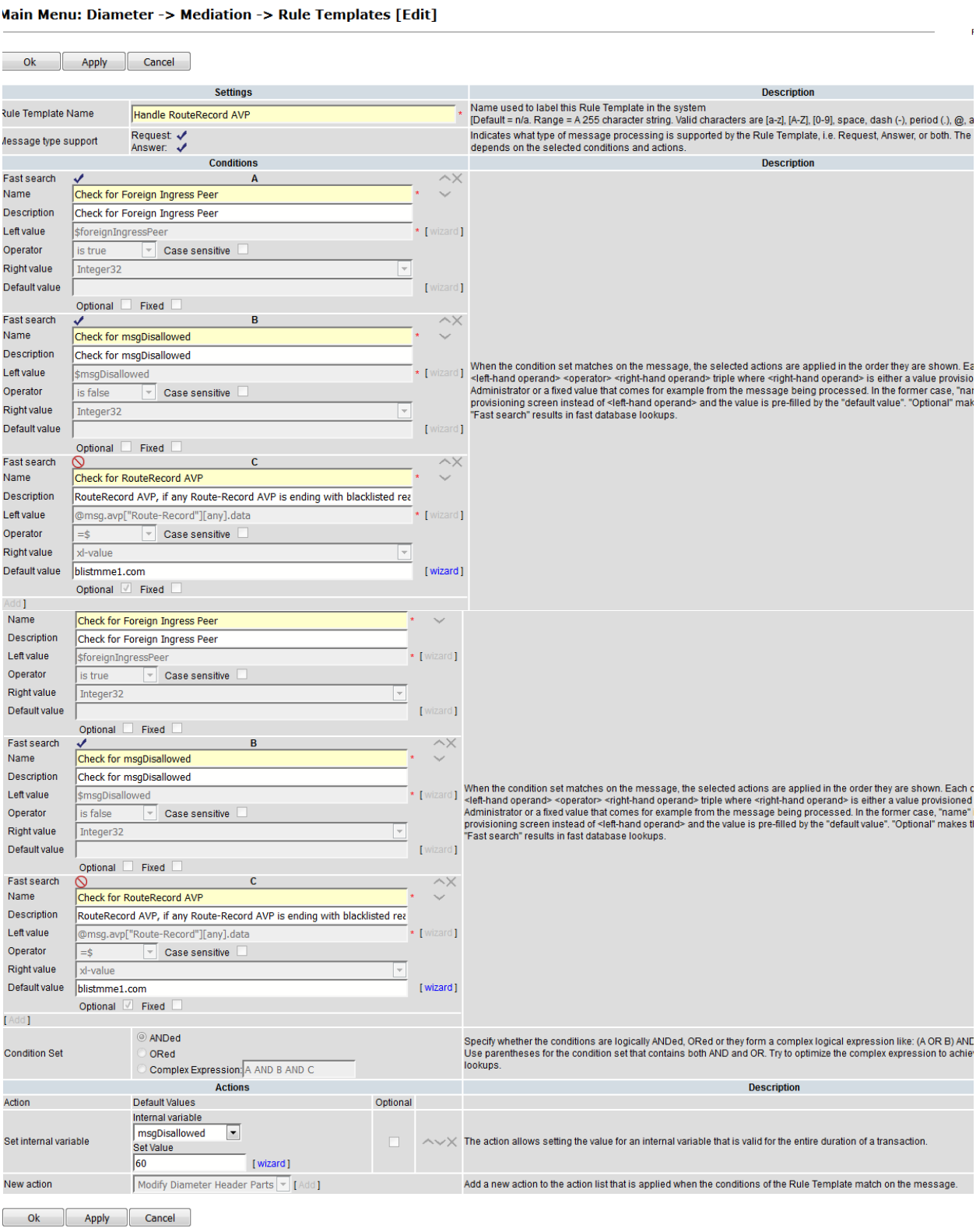


Figure 10: Screenshot of Handle Route Record AVP Configured Template

2.4.8 Template 8: Handle Disallowed Requests

Template 8 picks certain AVPs from the diameter message, and tests them again with certain countermeasure, which you configure.

If the diameter message fails at any countermeasure, then $msgDisallowed is set to a non-zero integer.

This template acts on the $msgDisallowed value.

Template 8 takes three types of action, but you can be modify the requirements.

- **Peg Counter**: Count the number of disallowed request.
- **Raise Alarm**: Include the value of $msgDisallowed in the alarm description.
- **Abandon** the diameter message.

It is associated with trigger point RTP1.

Template Definition

IF	$msgDisallowed	is true
THEN	Peg counter	Count the number of disallowed ingress requests
	Raise alarm	Include the value of $msgDisallowed in the alarm description
	Abandon message	

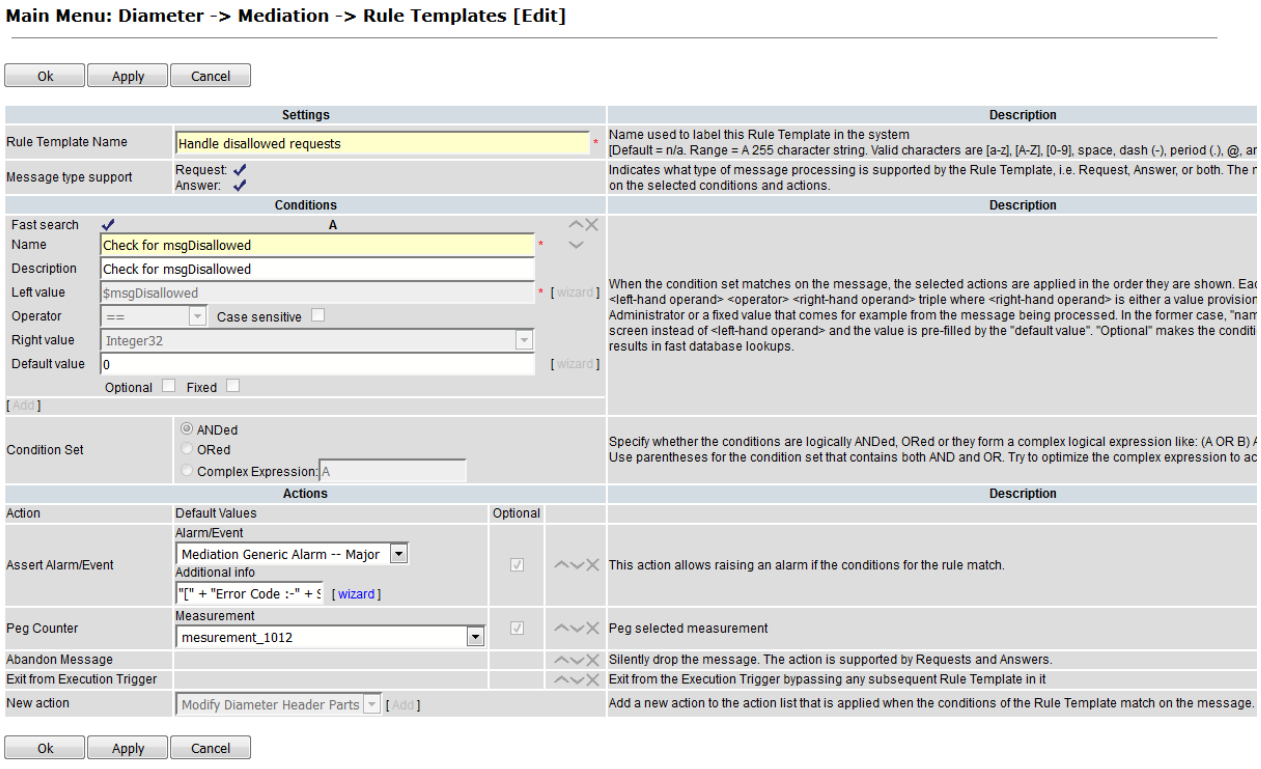


Figure 11: Screenshot of Handle Disallowed Requests Configured Template

2.4.9 Template 9a: Remove DOIC AVP

After successful execution of Template 8 “Handle Disallowed Requests,” if the message has failed at any countermeasure check, then the “Handle Disallowed Requests” template abandons the message (As per current configuration).

Once the diameter message passes all the above countermeasure checks ($msgDisallowed is still 0), then Template 9a “Remove DOIC AVP” is executed.

It checks for DOIC AVP (OC-Supported-Features and OC-OLR AVPs). If it is present in the diameter message, then it deletes the DOIC AVPs and forwards the message for further processing.

It is associated with trigger point RTP1.

Template Definition

IF	$foreignIngressPeer	is	true
AND	@msg.avp[“OC-Supported-Features”]	exists	
OR	@msg.avp[“OC-OLR”]	exists	
THEN	Delete AVP	OC-Supported-Features	
	Delete AVP	OC-OLR	

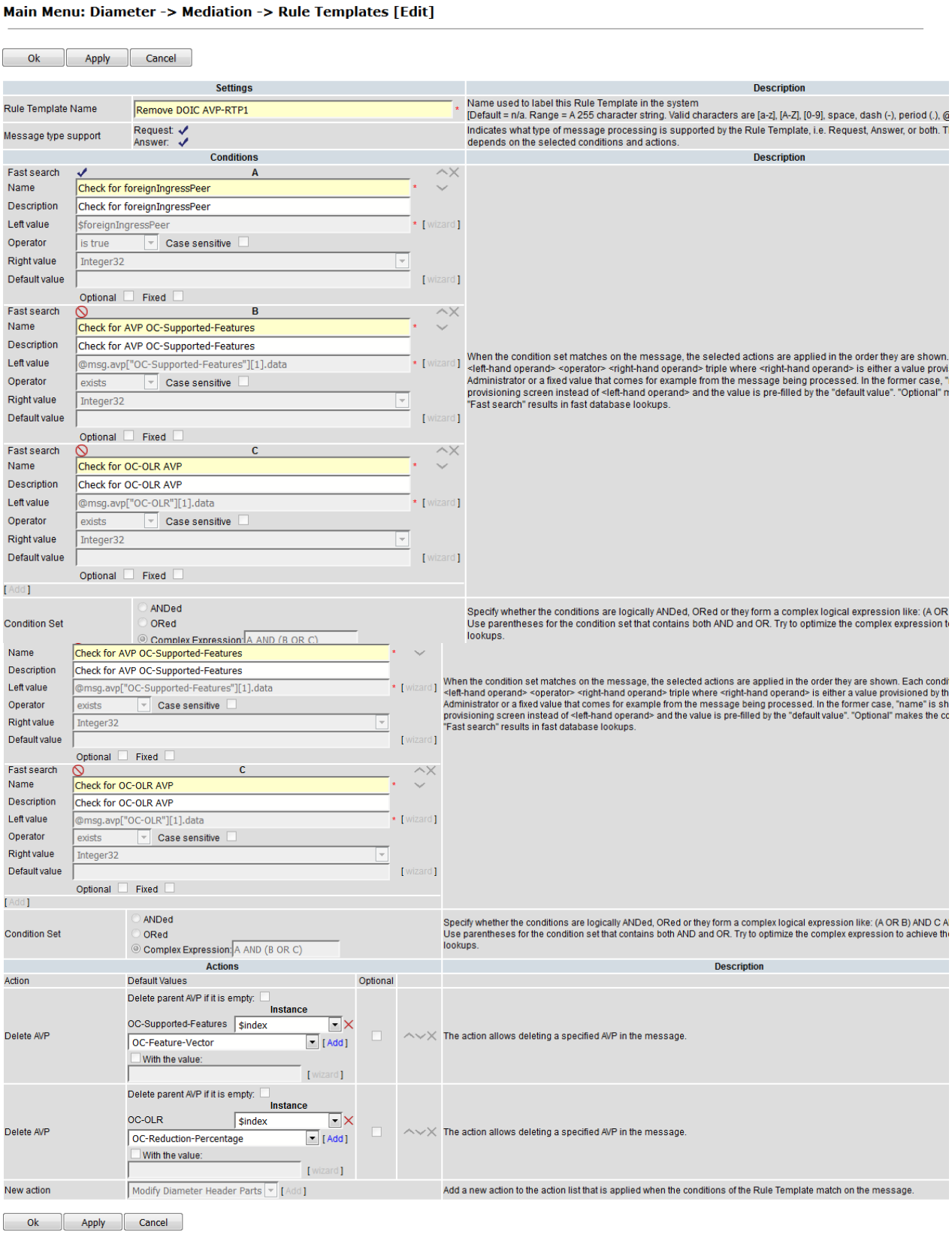


Figure 12: Screenshot of Remove DOIC AVP Configured Template

2.4.10 Template 9b: Remove DRMP AVP

After successful execution of Template 8 “Handle Disallowed Requests,” if the message has failed at any countermeasure check, then the “Handle Disallowed Requests” template abandons the message (As per current configuration).

Once the diameter message passes all the above countermeasure checks ($msgDisallowed is still 0), then Template 9b “Remove DRMP AVP” is executed.

It checks for DRMP AVP. If it is present in the diameter message, then it deletes the DRMP AVP and forwards the message for further processing.

It is associated with trigger point RTP1.

Template Definition

IF	$foreignIngressPeer	is	true
AND	@msg.avp[“DRMP”]	exists	
THEN	Delete AVP	DRMP	

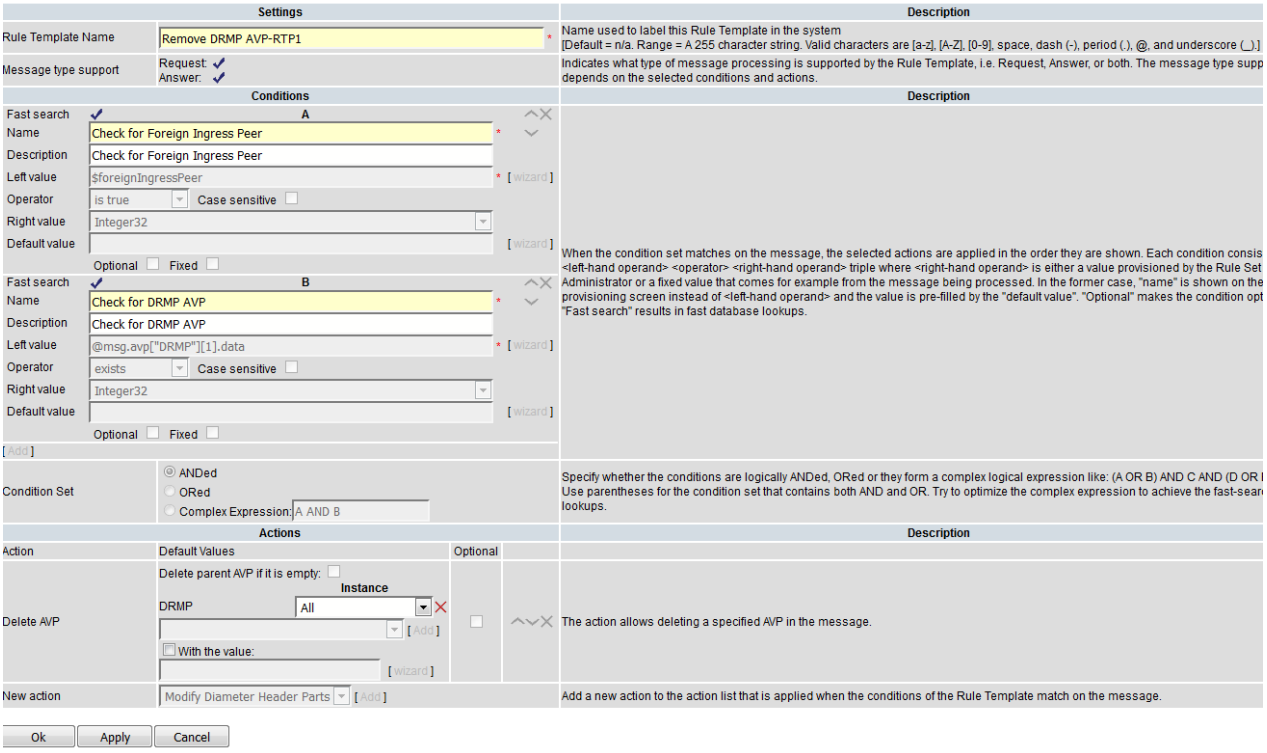


Figure 13: Screenshot of Remove DRMP AVP Configured Template

2.4.11 Template 10: Roaming Scenario Identification

Template 10 checks for an egress peer before sending the diameter message to the connection.

It checks for application ID s6a, which is fixed in the current configuration; egress peer (check for egress foreign peer); and command code. In the sample configuration, only two commands are allowed: AIR and ULR.

If the condition is satisfied, then the diameter message is marked for keeping track by setting $foreignEgressPeer = 1.

It is associated with trigger point RTP10.

Template Definition

IF	@msg.application_id	equals	S6a	
AND	@dsr.egress.peer	equals	list of	foreign peers
AND	@msg.command.code	equals	AIR	
OR	@msg.command.code	equals	ULR	
THEN	Set Internal Variable:	$foreignEgressPeer = 1		

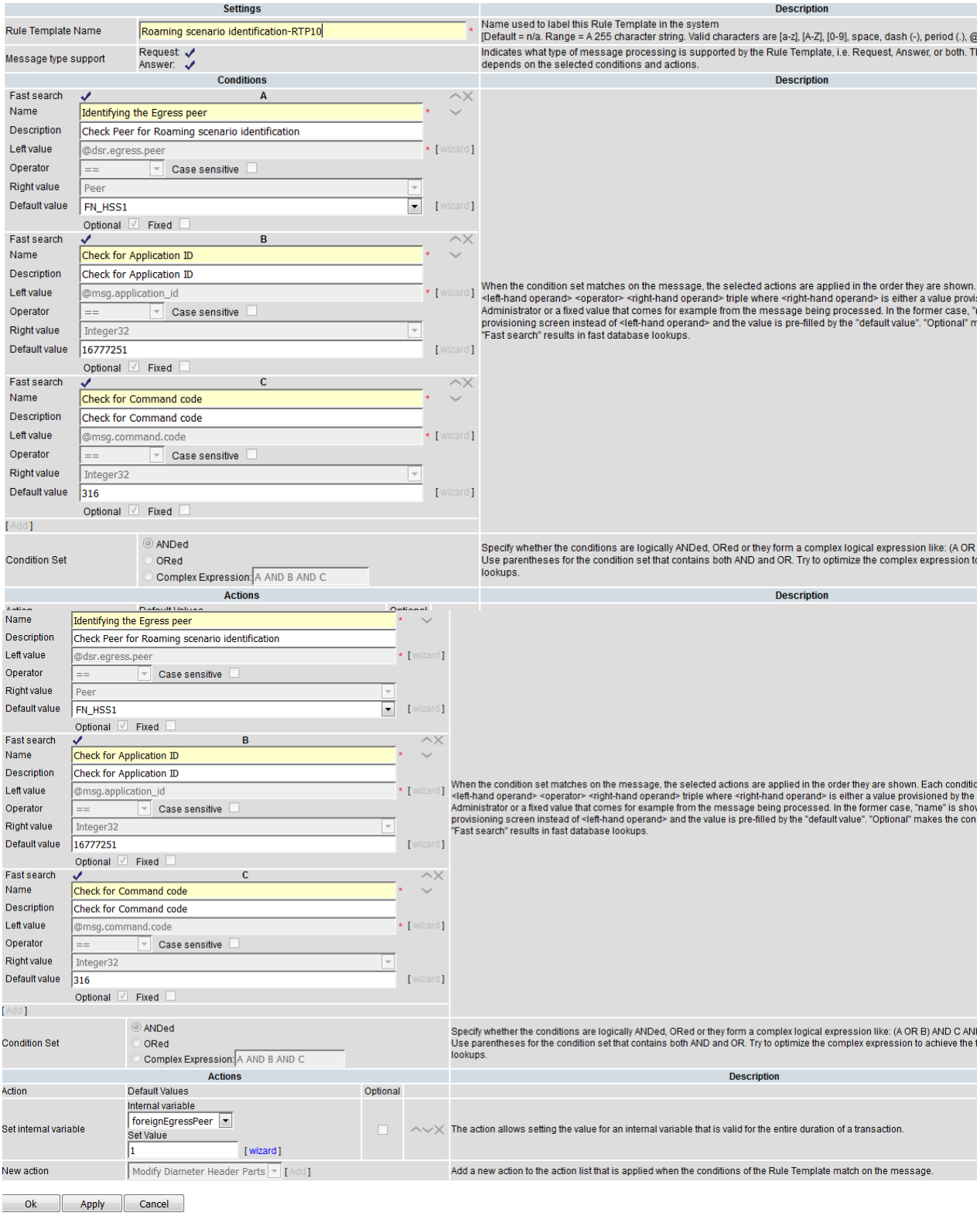


Figure 14: Screenshot of Roaming Scenario Identification Configured Template

2.4.12 Template 11: Destination-Realm Whitelist

Once the Template 10 “Roaming Scenario Identification” successfully executes, and $foreignEgressPeer is set to 1, Template 11 checks for Destination Realm AVP.

If the Destination Realm of the current diameter message is in the Destination Realm whitelist, then the $msgDisallowed is set to 0; otherwise, $msgDisallowed is 100, where 100 indicates the “Destination-Realm Whitelist” template check failed.

It is associated with trigger point RTP10.

Template Definition

IF	$foreignEgressPeer	is	true
AND	$msgDisallowed	is	false
AND	@msg.avp["Destination-Realm"]	equals	list of DRs
THEN	Set Internal Variable:	$msgDisallowed = 0 for all the rules except the default rule: $msgDisallowed = 100	

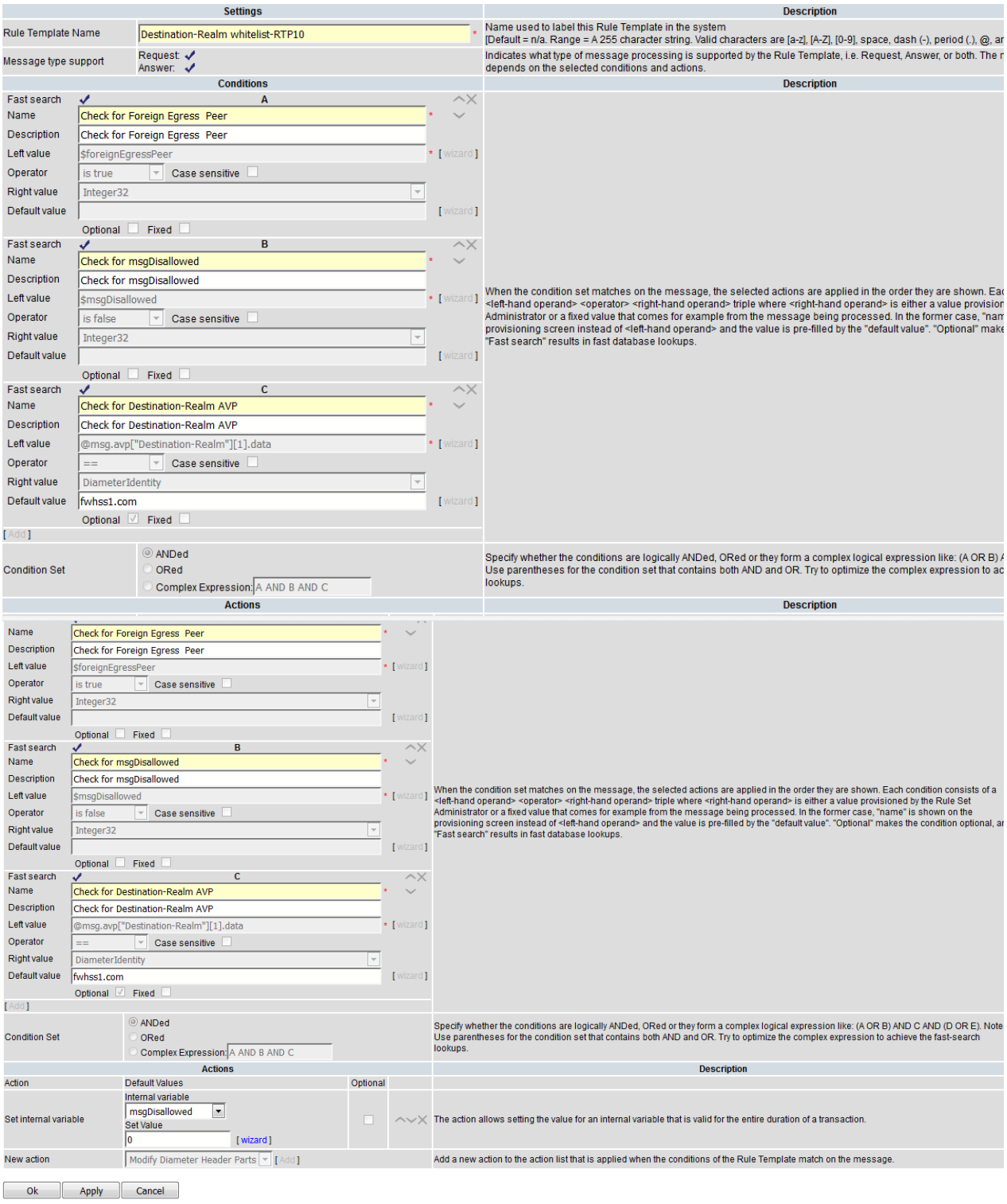


Figure 15: Screenshot of Destination-Realm Whitelist Configured Template

2.4.13 Template 12a: Remove DOIC AVP

This template's behavior is same as Template 9a, but association to trigger point is different and this works for egress peer.

It checks for DOIC AVP (OC-Supported-Features and OC-OLR AVPs). If it is present in the diameter message, then it deletes the AVPs and forwards the message for further processing.

It is associated with trigger point RTP10.

Template Definition

IF	$foreignEgressPeer	is	true
AND	@msg.avp[“OC-Supported-Features”]	exists	
OR	@msg.avp[“OC-OLR”]	exists	
THEN	Delete AVP	OC-Supported-Features	
	Delete AVP	OC-OLR	

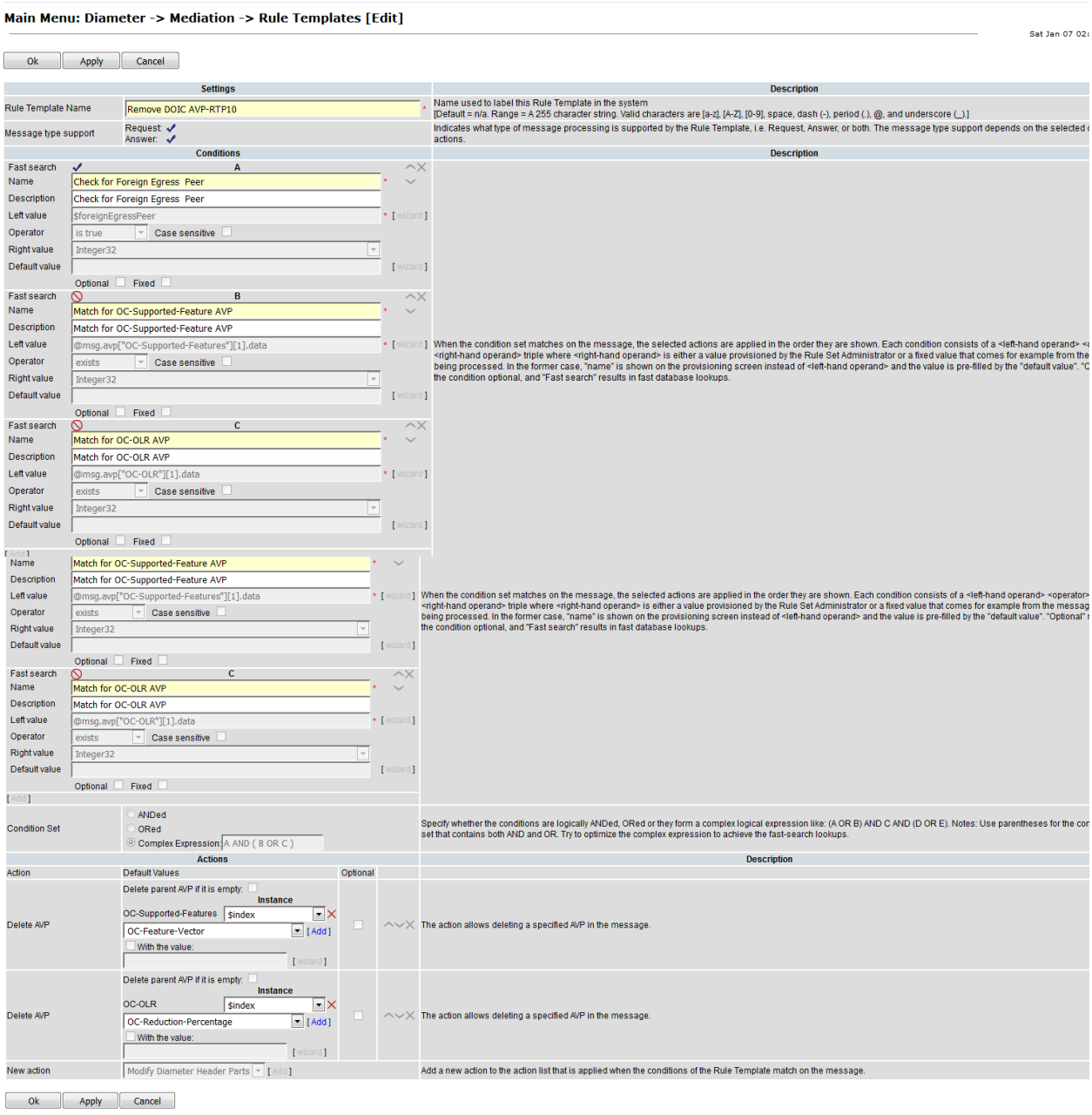


Figure 16: Screenshot of Remove DOIC AVP Configured Template

2.4.14 Template 12b: Remove DRMP AVP

This template behavior is same as template 9b but association to trigger point is different and this will work for egress peer.

It checks for DRMP AVP. If it is present in the diameter message, then it deletes the DFRMP AVP and forwards the message for further processing.

It is associated with trigger point RTP10.

Template Definition

IF	$foreignEgressPeer	is	true
AND	@msg.avp[“DRMP”]	exists	
THEN	Delete AVP	DRMP	

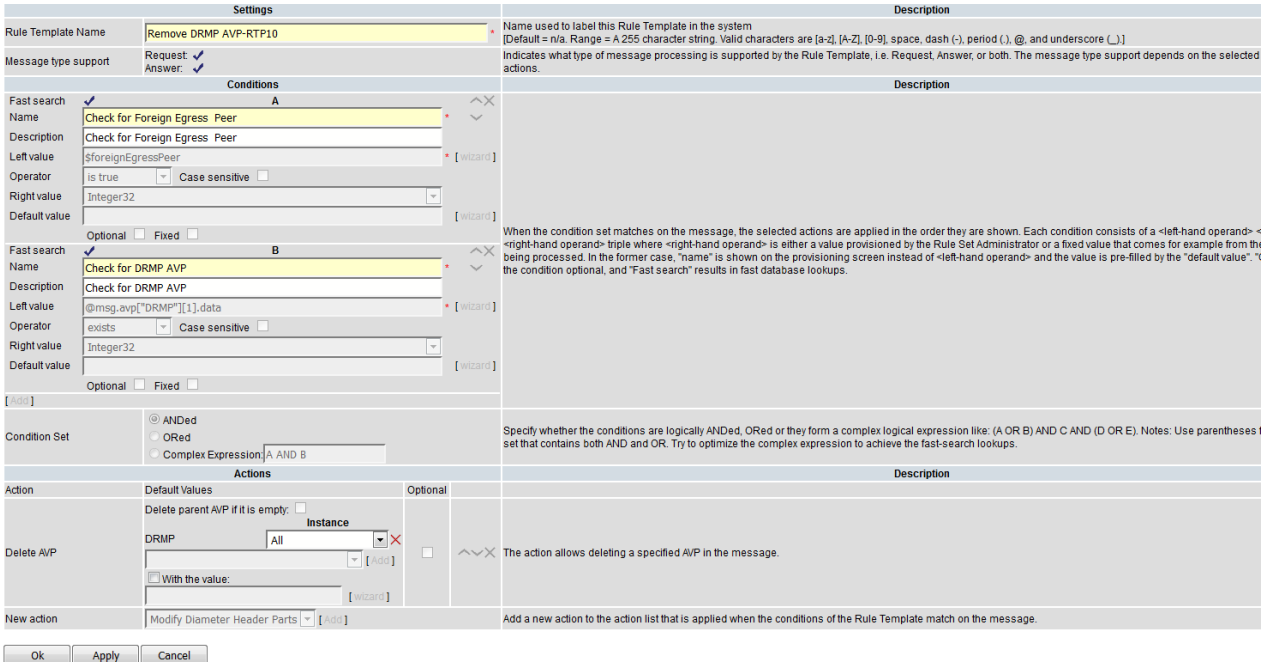


Figure 17: Screenshot of Configured Template

2.5 Insert Rules within a Rule Set

Insert rules within each rule set according to configuration. The condition value within each rule can be customized according to requirements.

In this sample application testing, templates are created (see screenshots of each of the Templates in Figure 4 though Figure 17) and rules are added accordingly in each template.

To insert a rule into the rule set:

1. Navigate to **Main Menu -> Diameter -> Mediation -> Rule Sets**.
2. Select a rule set and click Insert.

The following screenshots display each rule set with rules that can be used as a reference.

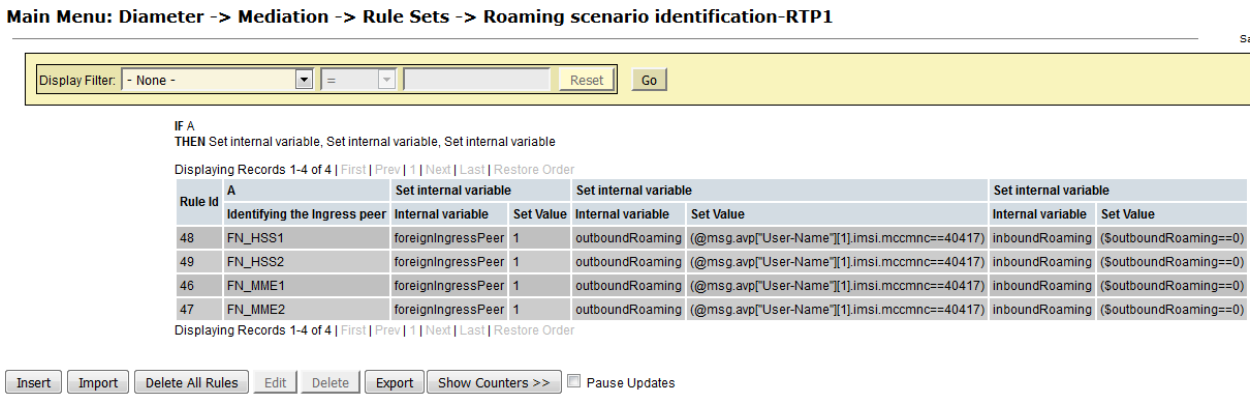


Figure 18: Template 1: Roaming Scenario Identification

IF A AND B AND C AND D
THEN Set internal variable

Displaying Records 1-6 of 6 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	C	D	Set internal variable	
	Check for InboundRoamers	Check for msgDisallowed	Check for ApplicationId	Check for CommandCode	Internal variable	Set Value
169	IS TRUE	IS FALSE	16777251	317	msgDisallowed	0
170	IS TRUE	IS FALSE	16777251	319	msgDisallowed	0
171	IS TRUE	IS FALSE	16777251	320	msgDisallowed	0
172	IS TRUE	IS FALSE	16777251	322	msgDisallowed	0
173	IS TRUE	IS FALSE	16777252		msgDisallowed	0
174	IS TRUE	IS FALSE			msgDisallowed	10

Displaying Records 1-6 of 6 | First | Prev | 1 | Next | Last | Restore Order

Figure 19: Template 2: Application ID and CC Whitelist for Inbound Roamers

Displaying Records 1-6 of 6 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	C	D	Set internal variable	
	Check for Outbound Romers	Check for msgDisallowed	Check for ApplicationId	Check for Commandcode	Internal variable	Set Value
175	IS TRUE	IS FALSE	16777251	316	msgDisallowed	0
176	IS TRUE	IS FALSE	16777251	318	msgDisallowed	0
177	IS TRUE	IS FALSE	16777251	321	msgDisallowed	0
178	IS TRUE	IS FALSE	16777251	323	msgDisallowed	0
179	IS TRUE	IS FALSE	16777252		msgDisallowed	0
180	IS TRUE	IS FALSE			msgDisallowed	20

Displaying Records 1-6 of 6 | First | Prev | 1 | Next | Last | Restore Order

Figure 20: Template 3: Application ID and CC Whitelist for Outbound Roamers

IF A AND B AND C
THEN Set internal variable

Displaying Records 1-5 of 5 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	C	Set internal variable	
	Check for Foreign Ingress Peer	Check for msgDisallowed	Check for Origin Realm AVP	Internal variable	Set Value
183	IS TRUE	IS FALSE	fwhss1.com	msgDisallowed	0
184	IS TRUE	IS FALSE	fwhss2.com	msgDisallowed	0
181	IS TRUE	IS FALSE	fwmme1.com	msgDisallowed	0
182	IS TRUE	IS FALSE	fwmme2.com	msgDisallowed	0
185	IS TRUE	IS FALSE		msgDisallowed	30

Displaying Records 1-5 of 5 | First | Prev | 1 | Next | Last | Restore Order

Figure 21: Template 4: OR Whitelist

IF A AND B AND C
THEN Set internal variable

Displaying Records 1-5 of 5 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	C	Set internal variable	
	Check for Foreign Ingress Peer	Check for msgDisallowed	Check for Destination-Realm AVP	Internal variable	Set Value
188	IS TRUE	IS FALSE	hohss1.com	msgDisallowed	0
189	IS TRUE	IS FALSE	hohss2.com	msgDisallowed	0
186	IS TRUE	IS FALSE	homme1.com	msgDisallowed	0
187	IS TRUE	IS FALSE	homme2.com	msgDisallowed	0
190	IS TRUE	IS FALSE		msgDisallowed	40

Displaying Records 1-5 of 5 | First | Prev | 1 | Next | Last | Restore Order

Figure 22: Template 5: DR Whitelist

THEN Set internal variable

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	C	Set internal variable	
	Check for Foreign Ingress Peer	Check for msgDisallowed	Check for Origin-Host AVP	Internal variable	Set Value
211	IS TRUE	IS FALSE	"." + @msg.avp["Origin-Realm"]	msgDisallowed	50

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Figure 23: Template 6: OH Ends with OR

THEN Set internal variable

Displaying Records 1-2 of 2 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	Move the rule		A	B	C	Set internal variable		Move the rule	
			Check for Foreign Ingress Peer	Check for msgDisallowed	Check for RouteRecord AVP	Internal variable	Set Value		
148	Up	Down	IS TRUE	IS FALSE	blistmme2.com	msgDisallowed	60	Up	Down
147	Up	Down	IS TRUE	IS FALSE	blistmme1.com	msgDisallowed	60	Up	Down

Displaying Records 1-2 of 2 | First | Prev | 1 | Next | Last | Restore Order

Figure 24: Template 7: Handle RouteRecord AVP

IF A
THEN Assert Alarm/Event, Peg Counter, Abandon Message, Exit from Execution Trigger

Displaying Records 1-7 of 7 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	Assert Alarm/Event		Measurement
	Check for msgDisallowed	Alarm/Event	Additional info	
213	10	Mediation Generic Alarm -- Major	"[" + "Error Code :-" + String($msgDisallowed) + "." + "Error Description :-" + " Application Id and CC white list for inbound roamers check failed. Abandoned the message"	measurement_inbound_10
219	100	Mediation Generic Alarm -- Major	"[" + "Error Code :-" + String($msgDisallowed) + "." + "Error Description :-" + " Destination-Realm whitelist check failed. Abandoned the message"	measurement_DestRealm_ER_100
214	20	Mediation Generic Alarm -- Major	"[" + "Error Code :-" + String($msgDisallowed) + "." + "Error Description :-" + " Application Id and CC white list for outbound roamers check failed. Abandoned the message"	measurement_outbound_20
215	30	Mediation Generic Alarm -- Major	"[" + "Error Code :-" + String($msgDisallowed) + "." + "Error Description :-" + " OR whiltelist check failed. Abandoned the message"	measurement_ORWhitelist_30
216	40	Mediation Generic Alarm -- Major	"[" + "Error Code :-" + String($msgDisallowed) + "." + "Error Description :-" + " DR whiltelist check failed. Abandoned the message"	measurement_DRWhitelist_40
217	50	Mediation Generic Alarm -- Major	"[" + "Error Code :-" + String($msgDisallowed) + "." + "Error Description :-" + " OH ends with OR check failed. Abandoned the message"	measurement_OH_ends_with_OR_50
218	60	Mediation Generic Alarm -- Major	"[" + "Error Code :-" + String($msgDisallowed) + "." + "Error Description :-" + " Handle RouteRecord AVP check failed. Abandoned the message"	measurement_Handle_RRecordAVP_60

Displaying Records 1-7 of 7 | First | Prev | 1 | Next | Last | Restore Order

Insert | Import | Delete All Rules | Edit | Delete | Export | Show Counters >> | Pause Updates

Figure 25: Template 8: Handle Disallowed Requests

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	Move the rule		A	B	C	Delete AVP	Delete AVP	Move the rule	
			Check for foreignIngressPeer	Check for AVP OC-Supported-Features	Check for OC-OLR AVP				
192	Up	Down	IS TRUE	EXISTS	EXISTS	OC-Supported-Features[$index]	OC-OLR[$index]	Up	Down

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Figure 26: Template 9a: Remove DOIC AVP

THEN Delete AVP

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	Delete AVP	Rule Counters
	Check for Foreign Ingress Peer	Check for DRMP AVP		Total Pegs
193	IS TRUE	EXISTS	DRMP[0]	0

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Figure 27: Template 9b: Remove DRMP AVP

THEN Set internal variable

Displaying Records 1-4 of 4 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	C	Set internal variable		Rule Counters
	Identifying the Egress peer	Check for Application ID	Check for Command code	Internal variable	Set Value	Total Pegs
74	FN_HSS1	16777251	316	foreignEgressPeer	1	0
76	FN_HSS1	16777251	318	foreignEgressPeer	1	0
77	FN_HSS2	16777251	316	foreignEgressPeer	1	0
75	FN_HSS2	16777251	318	foreignEgressPeer	1	0

Displaying Records 1-4 of 4 | First | Prev | 1 | Next | Last | Restore Order

All Rules | Edit | Delete | Export | << Hide Counters | Expand Counters | Pause Updates

Figure 28: Template 10. Roaming Scenario Identification

IF A AND B AND C
THEN Set internal variable

Displaying Records 1-3 of 3 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	C	Set internal variable	
	Check for Foreign Egress Peer	Check for msgDisallowed	Check for Destination-Realm AVP	Internal variable	Set Value
195	IS TRUE	IS FALSE	fwhss1.com	msgDisallowed	0
196	IS TRUE	IS FALSE	fwhss2.com	msgDisallowed	0
197	IS TRUE	IS FALSE		msgDisallowed	100

Displaying Records 1-3 of 3 | First | Prev | 1 | Next | Last | Restore Order

Figure 29: Template 11. Destination-Realm Whitelist

IF A AND (B OR C)
THEN Delete AVP, Delete AVP

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	Move the rule		A	B	C	Delete AVP	Delete AVP	Move the rule	
			Check for Foreign Egress Peer	Match for OC-Supported-Feature AVP	Match for OC-OLR AVP				
194			IS TRUE	EXISTS	EXISTS	OC-Supported-Features[$index]	OC-OLR[$index]		

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Figure 30: Template 12a. Remove DOIC AVP

IF A AND B
THEN Delete AVP

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Rule Id	A	B	Delete AVP
	Check for Foreign Egress Peer	Check for DRMP AVP	
198	IS TRUE	EXISTS	DRMP[0]

Displaying Records 1-1 of 1 | First | Prev | 1 | Next | Last | Restore Order

Figure 31: Template 12b. Remove DRMP AVP

2.6 State and Properties of Ruleset

After injecting rules within a rule set, change the state of the template to Active.

1. Navigate to **Main Menu -> Diameter -> Mediation -> State & Properties**.
2. Select a template and click **Edit**.
3. Change the State to **Active**.
4. You can change the Action Error Handling: Ignore the error depending on your requirements.
5. You can change the Status of Rule Counters: Checked. If checked, then you can see the peg counter for each rule.

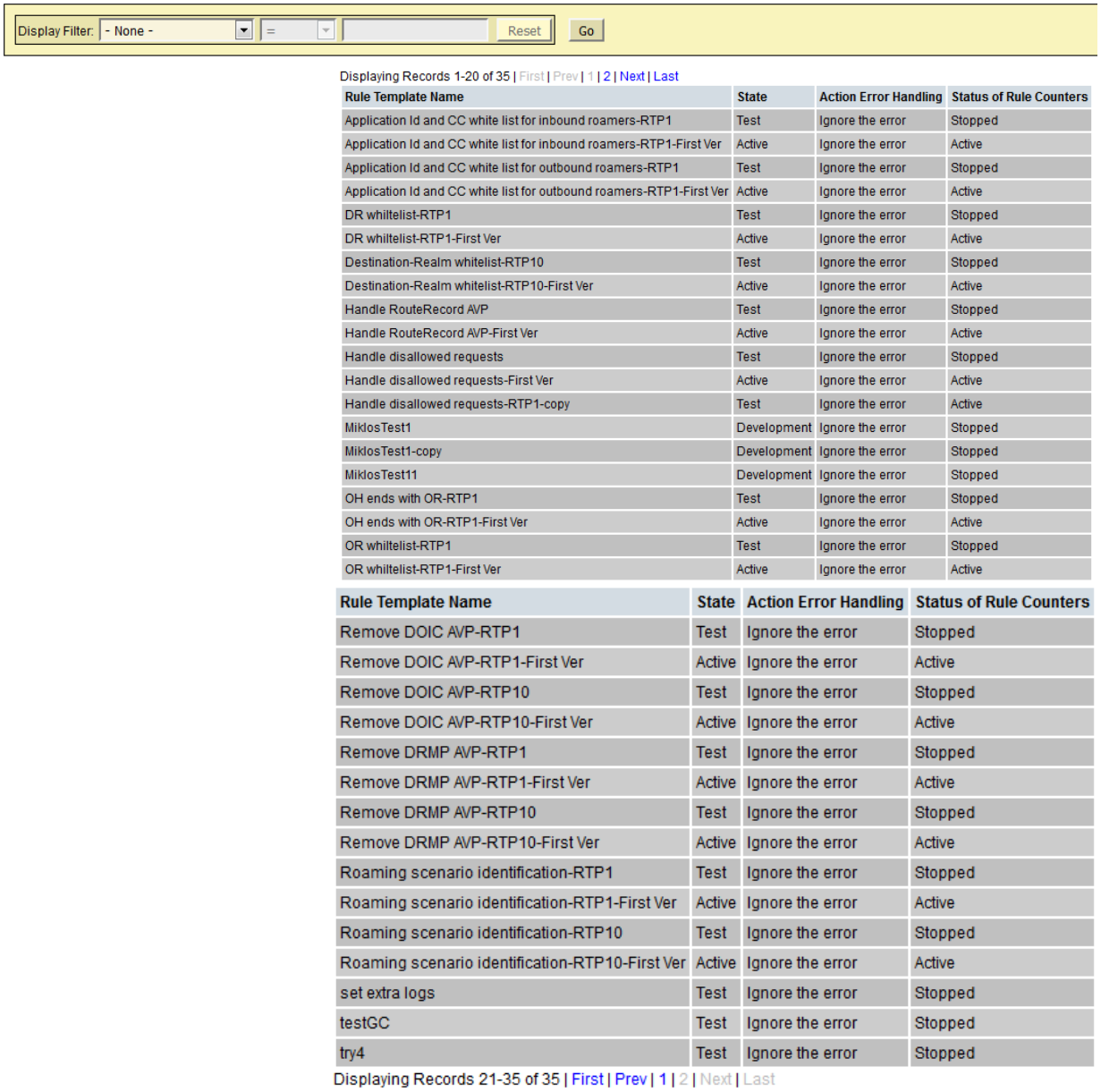


Figure 32: Active Templates Used as Reference

2.7 Association of Ruleset to a Trigger Point

This procedure associates the templates to a trigger point.

Associate Template 1 to Template 9b on trigger point RTP1 in increasing order. Associate Template 10, Template 11, Template 8, Template 12a, and Template 12b on trigger point RTP 10 in given sequence.

Associate Template 12a and 12b for the answer message on trigger point ATP10.

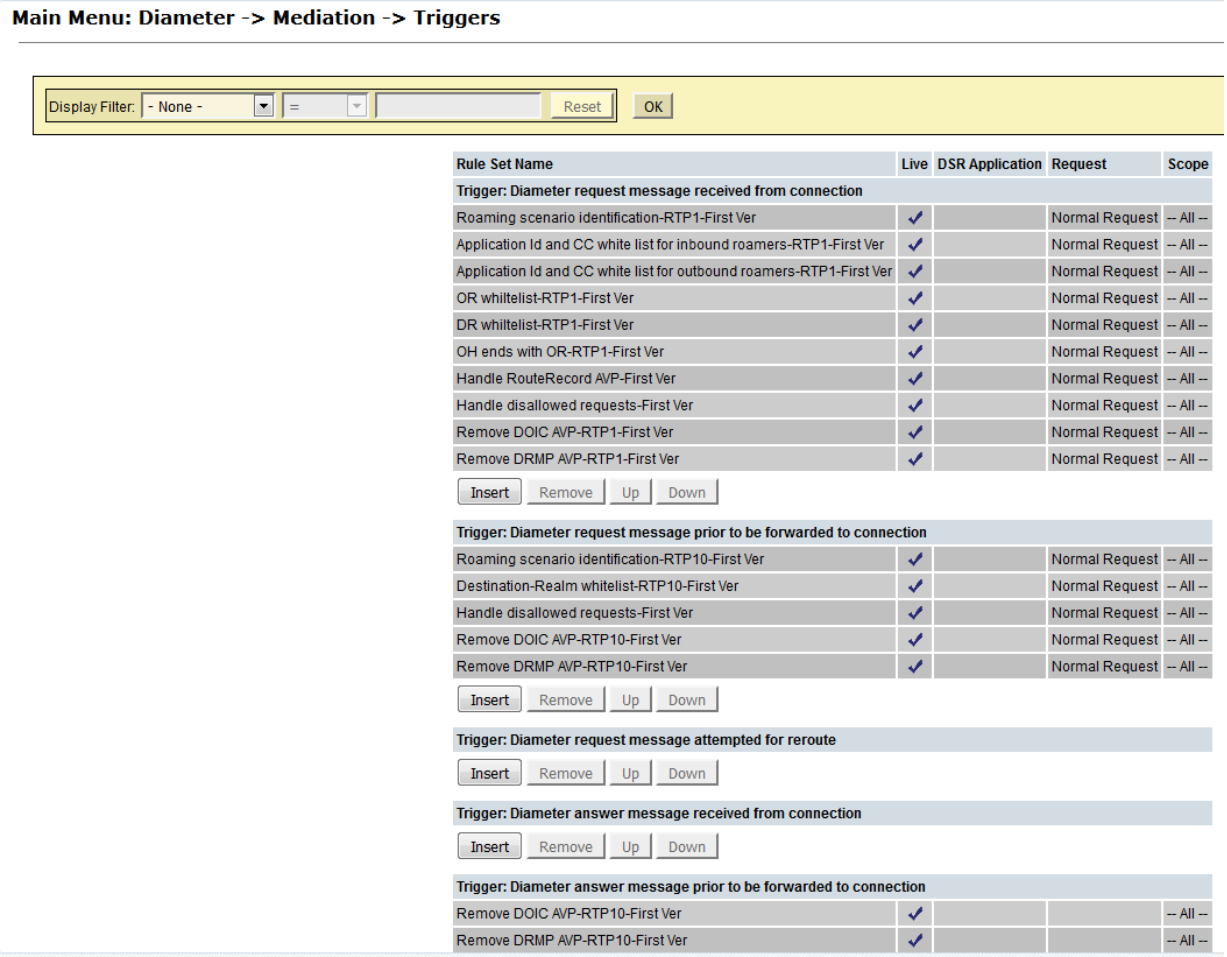


Figure 33: Screenshot of Rule Set Attached to its Trigger Points

Appendix A. My Oracle Support (MOS)

My Oracle Support

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown on the Support telephone menu:

1. Select 2 for New Service Request.
1. Select 3 for Hardware, Networking and Solaris Operating System Support.
2. Select one of the following options:

For technical issues such as creating a new Service Request (SR), select 1.

For non-technical issues such as registration or assistance with MOS, select 2.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at `1-800-223-1711` (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or "**Platforms**."
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select `Save target as` (or similar command based on your browser), and save to a local folder.