

Abuse Contact Policy Update

AFPUB-2018-GEN-001-DRAFT03



@JordiPalet

(jordi.palet@theipv6company.com)

Summary of the problem (I)

- The current policy **doesn't imply the obligation** to register an abuse contact and specifies a format for personal communication and for “automatic reporting”, which compared to other RIRs becomes confusing, as a single email will be more efficient, as at the end, reports get copied to both emails.
- As a result, **some LIRs may not have this contact information registered and up to date** for their resources. In fact, there are even cases of LIRs that use a non-existent mailbox or one that is not actively monitored.
- In practice, **this contact becomes ineffective** to report abuses and generally gives rise to security issues and costs for the victims.
- This proposal aims to solve this problem and ensure the existence of a proper abuse-c contact and the process for its utilization, which is more uniform across all the RIRs, in order to facilitate cross-region abuse reporting.

Summary of the problem (II)

- Existing policy references to a **“Best Practice Paper”**, which is **not deemed as mandatory** and in fact, **is not being used by the community**. This proposal doesn't change the scope of that document, and in fact, a link between the few existing IRT objects and the new one, should be automatically established.
- At this way, AfriNIC abuse contact will be in line with other RIRs. APNIC is now using the IRT, but since an equivalent proposal has been accepted, an automated “link” with the existing IRT will be created, so abuse-c and abuse-mailbox prevail.
- There is no need to delete the other optional data today included in the IRT. This policy just ensures that the abuse-mailbox is available and verified periodically.

Addressing the problem

- The Internet community is based on **collaboration**. However, in many cases this is not enough and we all need to be able to contact those LIRs that may be experiencing a problem in their networks and are unaware of the situation.
- This proposal creates a new section in the Policy Manual to solve this problem by means of a simple, **periodic verification**, and establishes the basic rules for performing such verification and thus avoids unnecessary costs to third parties that need to contact the persons responsible for solving the abuses of a specific network.
- The proposal guarantees that the cost of processing the abuse falls on the LIR whose client is causing the abuse (and from whom they receive financial compensation for the service), instead of falling on the victim, as would be the case if they had to resort to the courts, thus avoiding costs (lawyers, solicitors, etc.) and saving time for both parties.
- For this, the **abuse-c attribute becomes mandatory** in the "aut-num", "inetnum" and "inet6num" objects, as well as in any others that may be used in the future. This attribute is an abuse contact, which must contain at least the "abuse-mailbox" attribute.
- The proposal is expected to be implemented in 90 days, to be confirmed by AfriNIC, a reasonable time frame to allow both the staff to develop the tool and the LIRs to update their abuse-c contacts.

Changes from Previous Version

- Addressed inputs from staff assessment
- Inputs from the list
- Follow up and actions of failed validations by staff in accordance to existing policies/procedures
- Escalation methods determined by staff

Proposed Changes (I)

8.1 Introduction

This policy specifies a dedicated object that shall be used as the preferred place to publish abuse public contact information within the AFRINIC service region.

The mentioned object can be referenced in the inetnum, inet6num and aut-num objects in the AFRINIC whois Database. It provides a more accurate and efficient way for abuse reports to reach the correct network contact

8.1 Introduction

This policy specifies a **mandatory** object that must be used to publish abuse public contact information within the AFRINIC service region.

The mentioned object **must be** referenced in the inetnum, inet6num and aut-num objects in the AFRINIC whois Database. It provides a more accurate and efficient way for abuse reports to reach the correct contact.

Proposed Changes (II)

8.2 Policy details

(all replaced)

8.2 Description of “abuse-c” and “abuse-mailbox”

Resources allocated/assigned by AFRINIC must include a mandatory "abuse-c" contact attribute (abuse contact) in their corresponding WHOIS entry, with at least one valid, monitored and actively managed email inbox (abuse-mailbox) intended for receiving manual or automatic reports regarding abusive behavior, security issues, and the like.

The "abuse-mailbox" attribute must be available in an unrestricted way via whois, APIs and future techniques.

Considering the hierarchical nature of IP address objects, child objects of those directly distributed by AFRINIC may be covered by parent objects or they may have their own "abuse-c" attribute.

Following usual practices, other "e-mail" attributes may be included for other purposes.

Proposed Changes (III)

8.3 Advantages and disadvantages of the policy

(all replaced)

8.3 About the "abuse-mailbox"

Emails sent to "abuse-mailbox" must require manual intervention by the recipient at some point, and may not be filtered, because in certain cases this might prevent receiving the abuse reports. For example, in a spam case where the abuse report could include the spam message itself or URLs or content usually classified as spam.

The "abuse-mailbox" may initially send an automatic reply, for example, assigning a ticket number, applying classification procedures, requesting further information, etc. However, it should not require that the abuse reporter fills a form, as this will imply that each company that needs to report abuse cases (a task that is typically automated), would be forced to develop a specific interface for each ISP in the world that mandates filling forms, which is neither feasible nor logical, as it would place the cost of processing the abuse on those who submit the claim and are therefore victims of the abuse, instead of being paid for by the those whose client causes the abuse (and from whom they obtain income).

By way of information, it is worth noting that it is reasonable to expect that the abuse reporting procedure sends, with the initial abuse report, the logs, a copy of the spam message (attaching an example of the spam email or its full headers), or equivalent evidence (depending on the abuse type).

Likewise, it is reasonable to expect that the initial auto-reply email could specify that the claim will not be processed unless such evidence has been submitted, thus allowing the sender an opportunity to repeat the submission and include relevant evidence. This allows automatic reporting, for example, via fail2ban, SpamCop or others, keeping costs at a minimum for both parties involved.

Commonly, if a ticket number has been generated, it should be kept (typically as part of the subject) through successive communications.

Proposed Changes (IV)

8.4 Objectives of "abuse-c"/"abuse-mailbox" validation

The procedure, which will be developed by AFRINIC, must meet the following objectives:

1. A simple process that guarantees its functionality and allows the helpdesks that deal with abuse reports to verify that validation requests actually come from AFRINIC and not from third parties (which might involve security risks), avoiding, for example, a single "direct" URL for validation.
2. Avoid exclusively automated processing.
3. Confirm that the person performing the validation understands the procedure and the policy, that they regularly monitor the "abuse-mailbox", that measures are taken, and that the abuse report receives a response.
4. Validation period of no longer than 15 days.
5. If validation fails, escalate to the LIR and set a new validation period not to exceed 15 days.

The “initial” and “escalation” validation periods may be modified by AFRINIC, if deemed appropriate, informing the community about the motivation. For example, it could be longer for the first validation, once this policy is implemented, and shortened afterwards once the percentage of failures decreases, so the quality of the contacts increases and consequently a decrease in the average abuse response times could be expected.

(By way of example, a detailed procedure is included in this policy proposal under "Additional Information").

Proposed Changes (V)

8.5 Validation of "abuse-c"/"abuse-mailbox"

AFRINIC will validate compliance with the items above, both when the "abuse-c" and/or "abuse-mailbox" attributes are created or updated, as well as periodically, not less than once every 6 months, and whenever AFRINIC sees fit.

Lack of compliance will lead to a more exhaustive follow-up, warnings and blocking of certain services, at AFRINIC discretion, in accordance with the relevant policies/procedures.

The frequency of the periodic validation could be modified if the AFRINIC deems this appropriate and informs the community of its reasons. For example, a single validation could be done in the first year, to facilitate adherence to the policy, and then the number of annual validations could progressively increase, reaching even quarterly ones, with the aim of improving the quality of the contacts.

Proposed Changes (VI)

8.6 Escalation to AfriNIC

In order to allow escalation of fraudulent behavior (for example, an "abuse-mailbox" that only replies to AFRINIC's emails, or to messages with a specific subject or content), or failure to comply with the remaining aspects of this policy (incorrect or lack of response to cases of abuse), an escalation method should be provided, thus allowing for a re-validation (according to section 8.5 above).

Additional Information

Since this proposal is implemented, AFRINIC will publish the IRT as an alias to the abuse-c, in order to facilitate the search in whois for the same information, regardless if looking for abuse-c or IRT. The rest of the actual information in the IRT, can be kept as per the actual guidelines (which will need to be updated AFRINIC). This is done in order to assimilate the IRT to the majority of the RIRs where it is abuse-c.

Example of the validation procedure.

1. AFRINIC initiates the validation automatically, sending TWO consecutive emails to the "abuse-mailbox".
2. These emails will be sent containing plain text only.
3. At the discretion of AFRINIC, in general or in specific cases (for example, for confirmation in cases of escalation under 8.6), AFRINIC may use domains other than afrinic.*, and even modify the subject and body of the message, in order to perform said validations more effectively.
4. The first email will contain the URL where the validation is to be performed ("validacion.afrinic.net") and may contain information about the procedure, a brief summary of this policy, etc.
5. The second email will contain a unique alphanumeric validation code.
6. The person in charge of the "abuse-mailbox" must go to the URL and paste the code received in the second email in the form.
7. This URL must be designed in such a way that it prevents the use of an automated process (for example, "captcha"). In addition, it must contain a text that confirms that the person performing the validation understands the procedure and the policy, that they regularly monitor the "abuse-mailbox", that measures are taken to solve reported cases of abuse, and that the abuse report receives a response, with a "checkbox" that must be accepted in order to proceed.
8. The alphanumeric code will only be valid for a maximum of 15 working days.
9. If the code is not entered within that time, the system will mark the "abuse-c" as "temporarily invalid" and will alert AFRINIC staff so that they can initiate a personalized follow-up with the resource-holder.
10. If no reply is received confirming that the situation has been corrected, after an additional period of 15 business days, the "abuse-c" will be permanently marked as "invalid".
11. AFRINIC must ensure that all possible means of "warning" the resource-holder are put in place, such as periodic emails to other email boxes, alert pop-ups, etc. All those must contain the policy text and reminders about consequences in case of continued policy violation. Means of blocking access to certain services should be also considered.
12. The validation process will be repeated automatically (items 1 to 8 above). If satisfactory, the "abuse-c" will be marked as "valid"; otherwise it will be considered in breach of the policy.
13. There must be tools such as a form, mailbox (for example, a mailbox such as "abuse-escalation@afrinic.net"), or others in the future, to escalate lack of compliance with this policy and even the intermediation by AFRINIC and, where appropriate, the application of the relevant policies/procedures, especially those related to revocation of resources.

References

- An equivalent proposal has been accepted in APNIC and is under discussion in the ARIN, LACNIC and RIPE regions.