Network Working Group
INTERNET-DRAFT
Category: Proposed Standard
<draft-ietf-radext-filter-03.txt>
4 October 2006

Paul Congdon
Mauricio Sanchez
Hewlett-Packard Company
Bernard Aboba
Microsoft Corporation

RADIUS Filter Rule Attribute

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 10, 2007.

Copyright Notice

Copyright (C) The Internet Society 2006.

Abstract

This document defines the NAS-Filter-Rule attribute within the Remote Authentication Dial In User Service (RADIUS), equivalent to the Diameter NAS-Filter-Rule AVP described in RFC 4005.

Table of Contents

1. Introduction

This document defines the NAS-Filter-Rule attribute within the Remote Authentication Dialin User Service (RADIUS) which has the same functionality as the Diameter NAS-Filter-Rule AVP (400) defined in [RFC4005] Section 6.6. This attribute may prove useful for provisioning of filter rules.

While [RFC2865] Section 5.11 defines the Filter-Id attribute (11), this requires that the NAS be pre-populated with the desired filters. However, in situations where the server operator does not know which filters have been pre-populated, it useful to specify filter rules explicitly.

1.1. Terminology

This document uses the following terms:

Network Access Server (NAS)
: A device that provides an access service for a user to a network.

RADIUS server
: A RADIUS authentication server is an entity that provides an authentication service to a NAS.

RADIUS proxy
: A RADIUS proxy acts as an authentication server to the NAS, and a RADIUS client to the RADIUS server.

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.3. Attribute Interpretation

If a NAS conforming to this specification receives an Access-Accept packet containing a NAS-Filter-Rule attribute which it cannot apply, it MUST act as though it had received an Access-Reject. [RFC3576] requires that a NAS receiving a Change of Authorization Request (CoA-Request) reply with a CoA-NAK if the Request contains an unsupported attribute. It is recommended that an Error-Cause attribute with value set to "Unsupported Attribute" (401) be included in the CoA-NAK. As noted in [RFC3576], authorization changes are atomic so that this situation does not result in session termination and the pre-existing configuration remains unchanged. As a result, no accounting packets should be generated.

2. NAS-Filter-Rule Attribute

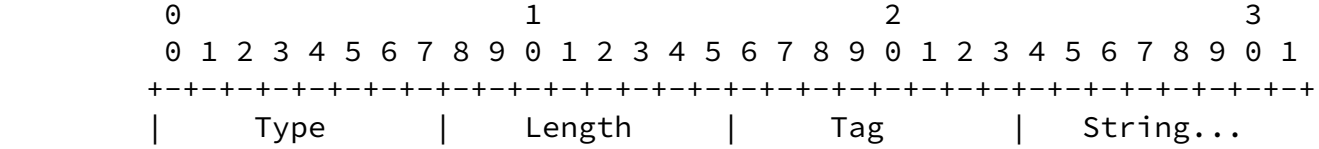
Description

This attribute indicates filter rules to be applied for this user. Zero or more NAS-Filter-Rule attributes MAY be sent in Access-Accept, CoA-Request, or Accounting-Request packets.

The NAS-Filter-Rule attribute is not intended to be used concurrently with any other filter rule attribute, including Filter-Id (11) and NAS-Traffic-Rule [Traffic] attributes, and SHOULD NOT appear in the same RADIUS packet. If a Filter-Id attribute is present, then implementations of this specification MUST silently discard NAS-Filter-Rule attributes, if present.

Where adjacent NAS-Filter-Rule attributes with the same non-zero Tag field value are included in a RADIUS packet, the String field of the attributes are to be concatenated to form a single filter. As noted in [RFC2865] Section 2.3, "the forwarding server MUST NOT change the order of any attributes of the same type", so that RADIUS proxies will not reorder NAS-Filter-Rule attributes.

A summary of the NAS-Filter-Rule Attribute format is shown below. The fields are transmitted from left to right.



Type

TBD

Length

>=4

Tag

The Tag field is used to identify the filter rule that is represented; the length of the Tag field is one octet and it MUST always be present.

Where a single filter rule is less than or equal to 252 octets in length, it MUST be encoded with a Tag field value of zero (0) and MUST NOT be split between multiple NAS-Filter-Rule attributes. On

receipt, attributes with a Tag field value of zero (0) MUST NOT be concatenated to form a single filter rule.

Where a single filter rule exceeds 252 octets in length, the rule MUST be encoded across multiple NAS-Filter-Rule attributes, each with the same Tag value which MUST be in the range 0x01 - 0x3F.

NAS-Filter-Rule attributes comprising a single filter rule MUST be sent consecutively, without intervening attributes with another Tag field value. The Tag field value of 0xFF is reserved and NAS-Filter-Rule attributes containing this Tag field value should be ignored upon receipt.

Adjacent filter rules exceeding 252 octets in length MUST be encoded with different non-zero Tag field values; however, the Tag field value used for a given filter rule need not be unique within the entire RADIUS packet.

String

The String field is one or more octets. It contains filter rules in the IPFilterRule syntax defined in [RFC3588] Section 4.3. A

robust implementation SHOULD support the field as undistinguished octets.

3. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.

Access-Request	Access-Accept	Access-Reject	Access-Challenge	CoA-Req	Acct-Req	#	Attribute
0	0+	0	0	0+	0+	TBD	NAS-Filter-Rule

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present in the packet.
0+	Zero or more instances of this attribute MAY be present in the packet.
0-1	Zero or one instance of this attribute MAY be present in the packet.

4. Diameter Considerations

[RFC4005] Section 6.6 defines the NAS-Filter-Rule AVP (400) with the same functionality as the RADIUS NAS-Filter-Rule attribute. In order to support interoperability, Diameter/RADIUS gateways will need to be configured to translate RADIUS attribute TBD to Diameter AVP 400 and

vice-versa. Where a Diameter NAS-Filter-Rule AVP contains a filter rule larger than 252 octets, Diameter/RADIUS gateways translate the AVP to multiple RADIUS NAS-Filter-Rule attributes, each with the same Tag field value not equal to '0' (0x30). Similarly, when multiple RADIUS NAS-Filter-Rule attributes are received with the same Tag field value not equal to '0' (0x30), the String fields of the attributes are concatenated together and encoded as the value in a single Diameter NAS-Filter-Rule AVP. RADIUS NAS-Filter-Rule attributes with a Tag field of '0' (0x30) are encoded as distinct Diameter NAS-Filter-Rule AVPs.

Note that a translated Diameter message can be larger than the maximum RADIUS packet size (4096). Where a Diameter/RADIUS gateway receives a Diameter message containing a NAS-Filter-Rule AVP that is too large to fit into a RADIUS packet, the Diameter/RADIUS gateway

will respond to the originating Diameter peer with the DIAMETER_INVALID_AVP_LENGTH error (5014), and with a Failed-AVP AVP containing the NAS-Filter-Rule AVP. Since repairing the error will probably require re-working the filter rules, the originating peer should treat the combination of a DIAMETER_INVALID_AVP_LENGTH error and a Failed-AVP AVP containing a NAS-Filter-Rule AVP as a terminal error.

5. IANA Considerations

This specification does not create any new registries.

This document uses the RADIUS [RFC2865] namespace, see <http://www.iana.org/assignments/radius-types>. Allocation of one update for the section "RADIUS Attribute Types" is requested. The RADIUS attribute for which a value is requested is:

TBD - NAS-Filter-Rule

6. Security Considerations

This specification describes the use of RADIUS for purposes of authentication, authorization and accounting. Threats and security issues for this application are described in [RFC3579] and [RFC3580]; security issues encountered in roaming are described in [RFC2607].

This document specifies a new attribute that can be included in existing RADIUS packets, which are protected as described in [RFC3579] and [RFC3576]. See those documents for a more detailed description.

A NAS-Filter-Rule attribute sent by a RADIUS server may not be understood by the NAS which receives it. A legacy NAS not compliant

with this specification may silently discard the NAS-Filter-Rule attribute while permitting the user to access the network. This can lead to users improperly receiving unfiltered access to the network. As a result, the NAS-Filter-Rule attribute SHOULD only be sent to a NAS that is known to support it.

7. References

7.1. Normative references

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

[RFC2865] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation of ISO 10646", RFC 3629, November 2003.

[RFC4005] Calhoun, P., Zorn, G., Spence, D. and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

7.2. Informative references

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J., "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC3580, September 2003.

[Traffic] Congdon, P., Sanchez, M., Lior, A., Adrangi, F. and B. Aboba, "Filter Attributes", Internet draft (work in progress), draft-ietf-radext-filter-rules-00.txt, February 2006.

Acknowledgments

The authors would like to acknowledge Greg Weber of Cisco and David

Nelson of Enterasys.

Authors' Addresses

Paul Congdon
Hewlett Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5662
Roseville, CA 95747

EMail: paul.congdon@hp.com
Phone: +1 916 785 5753
Fax: +1 916 785 8478

Mauricio Sanchez
Hewlett Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5559
Roseville, CA 95747

EMail: mauricio.sanchez@hp.com
Phone: +1 916 785 1910
Fax: +1 916 785 1815

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

EMail: bernarda@microsoft.com
Phone: +1 425 706 6605
Fax: +1 425 936 7329

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Open issues

Open issues relating to this specification are tracked on the following web site:

http://www.drizzle.com/~aboba/RADEXT/

./