Network Working Group
Internet-Draft
Expires: August 6, 2004

A. Lior
Bridgewater Systems
F. Adrangi
Intel
February 6, 2004

Remote Authentication Dial In User Service (RADIUS) Redirection
draft-lior-radius-redirection-00

Status of this Memo

Copyright Notice

Abstract

In certain scenarios there needs to be a method to force the users traffic to a specific location. This document describes several methods that are available to be used with Remote Authentication Dial In User Service (RADIUS) Protocol and defines three new RADIUS attributes: NAS-Filter-Rule, Redirect-Id and Redirect-Rule.

Table of Contents

1. Introduction

From time to time an Internet Service Provider (ISP) requires to restrict a user's access to the Internet and redirect their traffic to an alternate location. For example, the user maybe on a prepaid plan and all the resources have been used up. In this case the ISP would block the user's access to the Internet and redirect them to a portal where the user can replenish their account. Another example where the ISP would want to restrict access and redirect a user that was involved in some fraudulent behavior. Again the ISP would want to block the user's access to the Internet and redirect to a portal where they can inform the user as to their state and allow them to inform the user of their concerns and potentially rectify the situation.

In the examples above it is important to note that the ability to block and redirect user's traffic is required at service initiation and once service has been established. These capabilities must also be available across access technologies and various business scenarios. For example, the ability to block and redirect traffic is required for TCP users, cell phone users, WiFi users. As well, this capability must work whether the user is in their home network or roaming in a visited network which may or may not have a direct roaming relationship with the user's home network.

This document describes a protocol extension to the Remote Authentication Dial In User Service (RADIUS) Protocol RFC2865 [3] by which the aforementioned requirements can be addressed. To meet these needs three new RADIUS attributes are required. One option for providing these capabilities is to utilize RADIUS attributes for tunneling protocol specified in RFC2868 [5]. This document describes how to provide capabilities for users traffic redirection with or without using tunnels. Finally, the document describes how to provide for these capabilities dynamically (mid-service) using the RADIUS procotol extension described in RFC3576 [8].

Blocking and redirection of users traffic is known as hotlining of accounts. In this document, hotlining is used as the motivation for these attributes and an illustration of how they would be used. However, the NAS-Filter-Rule(TBD), Redirection-Id(TBD) and Redirection-Rule(TBD) may be used together or separately to provide other features.

1.1 Terminology

In this document when we refer to Blocking we mean Filtering.

1.2 Requirements Language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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 [2].

An implementation is not compliant if it fails to satisfy one or more of the must or must not requirements for the protocols it implements. An implementation that satisfies all the must, must not, should and should not requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the must and must not requirements but not all the should or should not requirements for its protocols is said to be "conditionally compliant".

2. Overview

As described in the Introduction section, from time to time an ISP requires to control users access to the Internet by blocking their access and/or redirecting them to a specific location. In this section we will examine these requirements in more detail.

Blocking access refers to setting up some rules at the NAS such that when the user initiates IP traffic, the NAS examines the set of rules associated with the Service granted to the subscriber. These rules determine what traffic is allowed to proceed through the NAS and what traffic will be blocked. Today this capability is supported in RADIUS and is configurable during service establishment and mid-service via the Filter-Id(11) attribute. To use Filter-Id to control access to the Internet the rules need to be configured at each NAS. Filter-Id(11) is used in an Access-Accept to specify the name of the filter rule(s) to apply to this session. To effect a change mid-service (dynamically) the Filter-Id(11) is included in a Change-of-Authorization (COA) packet. Upon receiving the Filter-Id(11) the NAS start to apply the rules specified by the Filter-Id(11).

As pointed out by NASREQ the use Filter-Id is not roaming friendly and it is recommended that instead one should use NAS-Filter-Rule(400) AVP. For this reason, this document introduces NAS-Filter-Rule(TBD) to RADIUS.

Redirection refers to an action taken by the NAS to redirect the user's traffic to an alternate location. Redirecting traffic in mid-session will most probably break some applications. However, Redirection at the start of a Service will most certainly work.

For hotlining, the purpose of redirection is not to continue to provide the service at this alternate location. Rather the purpose is to facilitate a mechanism whereby the user is informed of their state, and is provided for a way to rectify the situation. In some cases redirection could be used to redirect traffic to another location where service can continue.

The following illustrates the user's experience when being redirected. A valued prepaid user is roaming the net in their hotel room over WiFi is to be Hotlined (this is the term used by 3GPP2) because their account has no more funds. The user's Service Provider instructs the NAS to block all traffic, and redirect any port 80 traffic to the Service Provider's Prepaid Portal. Upon detecting that there is no service, the user launches his browser and regardless of which web site is being accessed the browser traffic will arrive at the Prepaid Portal which will then return a page back to the

subscriber indicating that he needs to replenish his account.

There are several ways to redirect the users traffic. Which method will be used depends on the capabilities available at the NAS and Service Provider's perferrence. User traffic can be redirected by tunneling the user's traffic to an alternate location. Tunneling can be used at layer-2 or layer-3. Tunneling will typically redirect all the users traffic for the Service. When tunneling is used to redirect all the traffic then blocking is not necessary.

Another method available for redirection is to have the NAS re-write the IP header in accordance with a redirection rule. We call this method Layer-3 Redirection. As the NAS receives packets from the user's device; if the packets match the redirection rule, the

destination address and (optionally) the port is re-written causing them to arrive at the alternate location. As packets from that location arrive back at the NAS, the NAS rewrites the source address with the original destination address. This is similar to what a NAT will do. This method of redirection provides more flexibility than tunneling in that we can control which layer-3 flows are to be redirected.

Another method of redirection is redirection in the application layer. In this method, the NAS is aware of application flows and redirects traffic based on an application specific method. For example, if the application is based on HTTP then an HTTP aware NAS would redirect traffic by issuing an HTTP Redirect response causing the users browser to navigate to an alternate Web Portal.

Finally, redirection can be achieved by utilizing the RADIUS Framed-Route(22) attribute. Using this attribute the NAS can be instructed to route the packet over a specific path. Due to the security risks associated with Framed-Routing, the use of this attribute for redirection is discouraged and hence we will not deal with this method in this document.

3. Operations

In this section we present the various methods used for redirecting user traffic, which are:

1) Tunneling;

2) Layer-3 Redirection; and

3) Application Redirection

For each method, we describe how redirection is done at service initiation and mid-sesssion. We also describe how redirection is removed when it is no longer desired.

3.1 Tunneling

When tunneling is used it will typically be used to redirect the entire traffic associated with the Service. Therefore, blocking (or filtering) will not be necessary at the NAS.

As discussed above, tunneling can be used to redirect traffic at either layer-2 or layer-3. Regardless, the message flows presented in the following sections are the same.

3.1.1 Service Initiation

Redirect using tunnels at service initiation requires that the RADIUS server send the appropriate tunnel attributes to the NAS. The tunnel attributes will describe the tunnel endpoint and the type of tunnel to construct. The operation is as specified in RFC2868 [5].

3.1.2 Mid-session Redirection

Redirection of traffic using tunnel mid-session involves sending the tunnel attributes as per RFC2868 [5] to the NAS using Change-of-Authorization (COA) packet. The operation is described in RFC3576 [8]. Careful attention should be paid to the security issues in RFC3576.

Note that if the session is already tunneled (eg. Mobile-IP) then the COA packet with a new tunnel specification can be sent to the NAS or alternatively the redirection can occur at the tunnel endpoint (the Home Agent) using any one of these methods.

3.1.3 Redirection Removal

If the normal mode for the session was to tunnel the session and

redirection was sent to the NAS, the RADIUS Server can send the original tunnel attributes to the NAS in a COA packet. The NAS will tear down the original tunnel and establish a connection back to the original tunnel endpoint.

However, if the normal mode for the session is not to use tunneling then we have a problem because RADIUS does not have a mechanism where by it can de-tunnel. Receiving a COA message without tunnel attributes should not cause an existing tunnel to be collapsed. In order to de-tunnel the session, the RADIUS server has to send the NAS a COA message requesting it to perform a re-Authorization. The RADIUS server will send an Access-Accept packet without the tunneling information. Upon receiving the corresponding Access-Accept packet the NAS MUST apply the new authorization attributes. If these do not contain tunnel attributes, then the NAS MUST tear down the tunnel.

3.2 Layer-3 Redirection

This document proposes two methods to convery redirection rules at layer-3. One is by using a Redirection-Id(TBD) attribute, the other to use Redirection-Rule(TBD) attribute. The message flows is the same regardless of which attribute is used. However, in order to use the Redirection-Id(TBD) attribute the RADIUS server and the NAS MUST have common knowledge as to the available Redirection Rules. When the administrative domains are not the same this could be a problem and hence the use of Redirection-Id(TBD) is not roaming friendly.

Layer-3 Redirection may require the use of blocking. If only some of the flows are redirected then the other flows will have to be blocked. In this case, the RADIUS server MUST communicate to the NAS the blocking rules. Blocking rules can be conveyed to the NAS using either Filter-Id(11) or NAS-Filter-Rule(TBD) attribute. These attributes will be carried along side the redirection attributes.

3.2.1 Service Initiation

If redirection is required during service initiation then the RADIUS server will send the redirection attributes and optionally the blocking attributes in the Access-Accept. The NAS will then start the service as usual with the traffic redirect and blocked as per the received redirection and blocking attributes.

If the NAS receives a Redirection-Id(TBD) attribute and or a Filter-Id(11) attribute that it does not recognize, the NAS should interpret the Access-Accept message as an Access-Reject message.

3.2.2 Mid-session Layer-3 Redirection

If Layer-3 redirection is required to be applied to a service that has already been started then the RADIUS server can push the redirection attributes and optionally the filter attributes to the NAS using a COA packets. The NAS will then commence to apply the redirecting rules and/or the filter rules.

If the NAS receives a COA message that contains a Redirection-Id(TBD) and or a Filter-Id(11) that it does not recognize it MUST generate a COA-NAK packet with ERROR-CAUSE(101) set to "Invalid Request"(404).

Alternatively, the RADIUS server can request that the NAS re-authorize the session using the procedures defined in RFC3576 [8]. The RADIUS server responds with an Access-Accept message (with Service-Type(6) set to "Authorize Only" that will contain the redirection and optionally filtering attributes.

If the NAS receives an Access-Accept message that contains a Redirection-Id(TBD) and or a Filter-Id(11) that it doesn't recognize it MUST treat the Access-Accept as an Access-Reject and terminate the session immediately generating an Accounting-Request(Stop) packet.

3.2.3 Layer-3 Redirection Removal

The RADIUS server can turn redirection off mid-session in two ways. It can push a new redirection attributes to the NAS using a COA packet; or it can send the NAS a COA packet requesting it to re-authorize.

If the NAS receives a Redirection-Id in the COA packet that it does not recognize then the NAS MUST respond with a COA-NAK with Error-Cause(101) set to "Invalid Request"(404). If the NAS receives an Access-Accept message sent in response to its Authorize-Only Access-Request, that contains an unrecognizable Redirection-Id(TBD), then the NAS MUST treat the Access-Accept as an Access-Reject and terminate the session immediately.

3.3 Application Redirection

The call flow associated with performing redirection at the application layer is very similar with the call flow associated with redirection done at the IP layer. What is different here is the number of different possible applications that must be considered. Fortunately, the most common application (and the one that we will

consider here) is HTTP based applications, or browser based application.

The redirection attributes described above are used to convey the redirection rules to use for Application Redirection. The

Redirection-Rule(TBD) attribute supports the encoding of a redirection URL to apply when a rule is matched.

3.3.1 Service Initiation

As with previous call flows. The RADIUS MAY send a Redirection-Id(TBD) or Redirection-Rule(TBD) attributes to the NAS in the Access-Accept message. If the NAS receives a Redirection-Id(TBD) attribute which it does not understand then the NAS MUST treat the Access-Accept as an Access-Reject packet.

3.3.2 Mid-session Application Redirection

Mid-session initiated Application Based Redirection is similar to the call flows of IP based redirection method discussed above.

3.3.3 Application Redirection Removal

Redirection removal based on Application Based Redirection is similar to the call flows of IP based redirection method discussed above.

3.4 Accounting

Every time a session is redirected and every time the redirection is reverted back a new session is created and the old one is terminated. Therefore the NAS MUST generate and Accounting-Request(Stop) for the old session and an Accounting-Request(Start) for the new session.

As described above, when the NAS receives redirection attributes that it does not understand in an Access-Accept packet it MUST terminate the session and MUST generate an Accounting-Request(Stop) packet. Note, in the case where it receives redirection/filtering attributes in a COA packet that it does not understand, then it responds with a COA-NAK packet and does not terminate the session and therefore it MUST NOT generate an Accounting-Request(Stop) packet.

4. Attributes

This specification introduces three new RADIUS attributes.

NAS-Filter-Rule(TBD)

Redirection-ID(TBD)

Redirection-Rule(TBD)

4.1 NAS-Filter-Rule Attribute

The NAS-Filter-Rule(TBD) matches its Diameter counter part (that is its of type IPFilterRule), and provides filter rules that need to be configured on the NAS for the user. One or more such AVPs MAY be present in an Access-Accept packet or Change-of-Authorization packet.

NAS-Filter-Rule(TBD) can be used to filter packets based on the following information that is associated with it:

Direction	(in or out)
Source and destination IP address	(possibly masked)
Protocol	
Source and destination port	(lists or ranges)

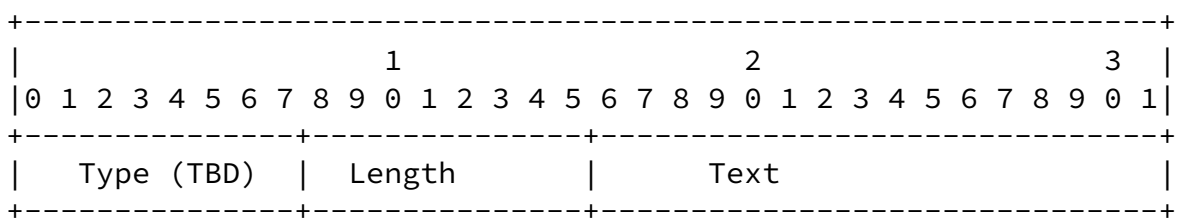
TCP flags

IP fragment flag

IP options

ICMP types

Rules for the appropriate direction are evaluated in order, with the first matched rule terminating the evaluation. Each packet is evaluated once. If no rule matches, the packet is dropped if the last rule evaluated was a permit, and passed if the last rule was a deny.



| Text

Type TBD for NAS-Filter-Rule.

Length >= 3

Text

The text conforms to the following specification (taken from Diameter IPFilterRule Type):

NAS-Filter-Rule MUST follow the format:

action dir proto from src to dst [options]

action

permit - Allow packets that match the rule.

deny - Drop packets that match the rule.

dir "in" is from the terminal, "out" is to the terminal.

proto An IP protocol specified by number. The "ip" keyword means any protocol will match.

src and dst <address/mask> [ports]

The <address/mask> may be specified as:

ipno An IPv4 or IPv6 number in dotted-quad or canonical IPv6 form. Only this exact IP number will match the rule.

ipno/bits An IP number as above with a mask width of the form 1.2.3.4/24. In this case, all IP numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width MUST be valid for the IP version and the IP number MUST NOT have bits set beyond the mask. For a match to occur, the same IP version MUST be present in the packet that was used in describing the IP address. To test for a particular IP version, the bits part can be set to zero. The keyword "any" is 0.0.0.0/0 or the IPv6

equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. For IPv4, a typical first rule is often "deny in ip! assigned"

The sense of the match can be inverted by preceding an address with the not modifier (!), causing all other addresses to be matched instead. This does not affect the selection of port numbers.

With the TCP, UDP and SCTP protocols, optional ports may be specified as:

{port/port-port}[,ports[,...]]

The '-' notation specifies a range of ports (including boundaries).

Fragmented packets that have a non-zero offset (i.e., not the first fragment) will never match a rule that has one or more port specifications. See the frag option for details on matching fragmented packets.

options:

frag Match if the packet is a fragment and this is not the first fragment of the datagram. frag may not be used in conjunction with either tcpflags or TCP/UDP port specifications.

ipoptions spec

Match if the IP header contains the comma separated list of options specified in spec. The supported IP options are:

ssrr (strict source route), lsrr (loose source route), rr (record packet route) and ts (timestamp). The absence of a particular option may be denoted with a '!'.

tcpoptions spec

Match if the TCP header contains the comma separated list of options specified in spec. The supported TCP options are:

mss (maximum segment size), window (tcp window

advertisement), sack (selective ack), ts (rfc1323 timestamp) and cc (rfc1644 t/tcp connection count). The absence of a particular option may be denoted with a '!'.

established

TCP packets only. Match packets that have the RST or ACK bits set.

setup TCP packets only. Match packets that have the SYN bit set but no ACK bit.

tcpflags spec
TCP packets only. Match if the TCP header contains the comma separated list of flags specified in spec. The supported TCP flags are:

fin, syn, rst, psh, ack and urg. The absence of a particular flag may be denoted with a '!'. A rule that contains a tcpflags specification can never match a fragmented packet that has a non-zero offset. See the frag option for details on matching fragmented packets.

icmptypes types
ICMP packets only. Match if the ICMP type is in the list types. The list may be specified as any combination of ranges or individual types separated by commas. Both the numeric values and the symbolic values listed below can be used. The supported ICMP types are:

echo reply (0), destination unreachable (3), source quench (4), redirect (5), echo request (8), router advertisement (9), router solicitation (10), time-to-live exceeded (11), IP header bad (12), timestamp request (13), timestamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18)

There is one kind of packet that the access device MUST always discard, that is an IP fragment with a fragment offset of one. This is a valid packet, but it only has one use, to try to circumvent firewalls.

A NAS that is unable to interpret or apply a deny rule MUST terminate the session. A NAS that is unable to interpret or apply a permit rule

MAY apply a more restrictive rule. A NAS MAY apply deny rules of its

own before the supplied rules, for example to protect the access device owner's infrastructure.

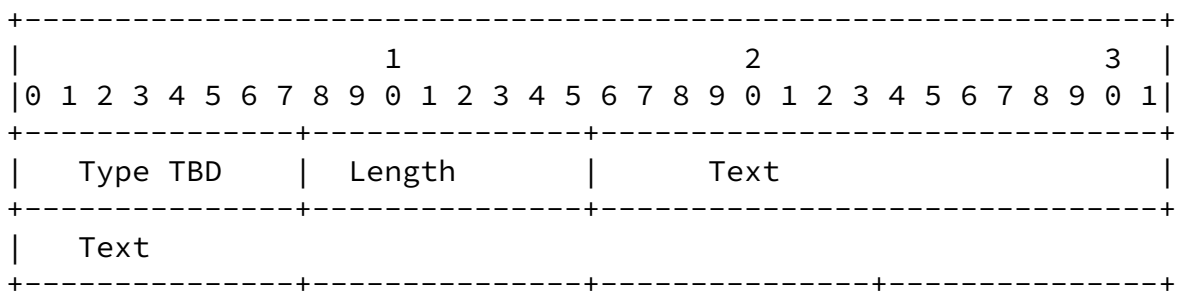
The rule syntax is a modified subset of ipfw(8) from FreeBSD, and the ipfw.c code may provide a useful base for implementations.

4.2 Redirection-Id

The Redirection-Id(TBD) attribute indicates the name of the redirection list to apply to this session. Zero or more Redirection-Id attributes MAY be sent in an Access-Accept packet or an COA packet.

Identifying a redirection list by name allows the redirection to be used on different NASes without regard to redirection implementation details. On the other hand, using Redirection-Id is not roaming friendly.

If the NAS does not recognize the Redirection-Id(TBD) then it MUST reject the request.



Type TBD for Redirection-Id.

Length >= 3

Text:

The Text field is one or more octets, and its contents are implementation dependent. It is intended to be human readable and MUST NOT affect operation of the protocol. It is recommended that the message contain UTF-8 encoded 10646 [7] characters.

4.3 Redirection-Rule

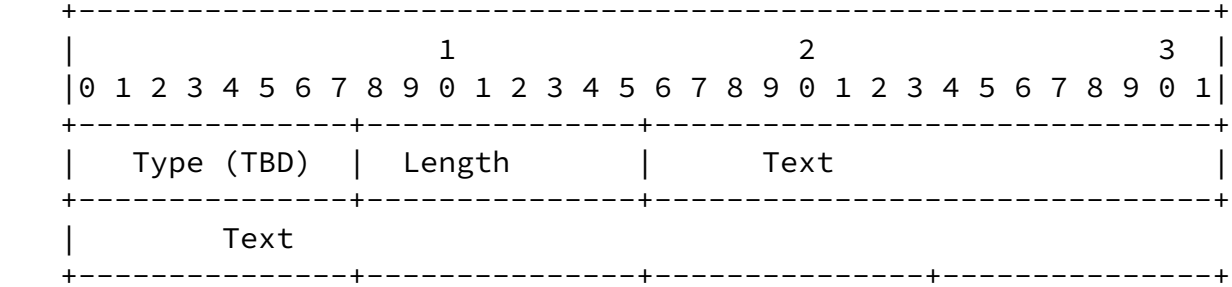
The Redirection-Rule(TBD) is very similar to the NAS-Filter-Rule and its Diameter counter part (that is its of type IPFilterRule), and provides redirection rules that need to be configured on the NAS for the user. One or more such attribute MAY be present in an

Access-Accept packet or Change-of-Authorization packet.

Redirection-Rule(TBD) can be used to redirect IP packets based on the following information that is associated with it:

- Direction (in or out)
- Source and destination IP address (possibly masked)
- Protocol
- Source and destination port (lists or ranges)
- TCP flags
- IP fragment flag
- IP options
- ICMP types

Rules for the appropriate direction are evaluated in order, with the first matched rule terminating the evaluation. Each packet is evaluated once. If no rule matches, the packet is dropped if the last rule evaluated was a permit, and passed if the last rule was a deny.



Type TBD for Redirection-Rule.

Length >= 3

Text

The text conforms to the following specification (taken from Diameter IPFilterRule Type) and modified to introduce redirection:

Redirect-Filter-Rule MUST follow the format:

action [redir | url] dir proto from src to dst [options]

action:

redirect - redirect packets that match the rule to either the specified redir ip address or the specified url.

redirectoff - turn the matching redirection rule of. The matching redirection rule has to match exactly in every parameter.

dir "in" is from the terminal, "out" is to the terminal.

proto An IP protocol specified by number. The "ip" keyword means any protocol will match.

redir, src and dst <address/mask> [ports]

The <address/mask> may be specified as:

ipno An IPv4 or IPv6 number in dotted-quad or canonical IPv6 form. Only this exact IP number will match the rule.

ipno/bits An IP number as above with a mask width of the form 1.2.3.4/24. In this case, all IP numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width MUST be valid for the IP version and the IP number MUST NOT have bits set beyond the mask. For a match to occur, the same IP version MUST be present in the packet that was used in describing the IP address. To test for a particular IP version, the bits part can be set to zero. The keyword "any" is 0.0.0.0/0 or the IPv6 equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. For IPv4, a typical first rule is often "deny in ip! assigned"

The sense of the match can be inverted by preceding an address with the not modifier (!), causing all other addresses to be matched instead. This does not affect the selection of port numbers.

With the TCP, UDP and SCTP protocols, optional ports may be specified as:

{port/port-port}[,ports[,...]]

The '-' notation specifies a range of ports (including boundaries).

Fragmented packets that have a non-zero offset (i.e., not the first fragment) will never match a rule that has one or more port specifications. See the frag option for details on matching fragmented packets.

options:

frag Match if the packet is a fragment and this is not the first fragment of the datagram. frag may not be used in conjunction with either tcpflags or TCP/UDP port specifications.

ipoptions spec

Match if the IP header contains the comma separated list of options specified in spec. The supported IP options are:

ssrr (strict source route), lsrr (loose source route), rr (record packet route) and ts (timestamp). The absence of a particular option may be denoted with a '!'.

tcpoptions spec

Match if the TCP header contains the comma separated list of options specified in spec. The supported TCP options are:

mss (maximum segment size), window (tcp window advertisement), sack (selective ack), ts (rfc1323 timestamp) and cc (rfc1644 t/tcp connection count). The absence of a particular option may be denoted with a '!'.

established
TCP packets only. Match packets that have the RST or ACK bits set.

setup TCP packets only. Match packets that have the SYN bit set but no ACK bit.

tcpflags spec
TCP packets only. Match if the TCP header contains the comma separated list of flags

specified in spec. The supported TCP flags are:

fin, syn, rst, psh, ack and urg. The absence of a particular flag may be denoted with a '!'. A rule that contains a tcpflags specification can never match a fragmented packet that has a non-zero offset. See the frag option for details on matching fragmented packets.

icmptypes types
ICMP packets only. Match if the ICMP type is in the list types. The list may be specified as any combination of ranges or individual types separated by commas. Both the numeric values and the symbolic values listed below can be used. The supported ICMP types are:

echo reply (0), destination unreachable (3), source quench (4), redirect (5), echo request (8), router advertisement (9), router solicitation (10), time-to-live exceeded (11), IP header bad (12), timestamp request (13), timestamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18)

An NAS that is unable to interpret or apply a deny rule MUST terminate the session. A NAS that is unable to interpret or apply a permit rule MAY apply a more restrictive rule. A NAS MAY apply deny rules of its own before the supplied rules, for example to protect the NAS owner's infrastructure.

The rule syntax is a modified subset of ipfw(8) from FreeBSD, and the ipfw.c code may provide a useful base for implementations.

5. Table of Attributes

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

Access packets:

Request	Accept	Reject	Challenge	#	Attribute
0	0+	0	0	TBD	NAS-Filter-Rule
0	0+	0	0	TBD	Redirection-Id
0	0+	0	0	TBD	Redirection-Rule

Change-of-Authorization packet:

Request	ACK	NAK	#	Attribute
0+	0	0	TBD	NAS-Filter-Rule [note 1]
0+	0	0	TBD	Redirection-Id [note 1]
0+	0	0	TBD	Redirection-Rule[note 1]

[note 1] When included within a CoA-Request, these attributes represent an authorization change request. When one of these attributes is omitted from a CoA-Request, the NAS assumes that the attribute value is to remain unchanged. Attributes included in a CoA-Request replace all existing value(s) of the same attribute(s).

6. Security Considerations

TBD

7. IANA Considerations

This document uses the RADIUS [RFC2865] namespace, see <http://www.iana.org/assignments/radius-types>. There are three updates for

the section: RADIUS Packet Type Codes. These Packet Types are allocated in [RADIANA]:

TBD - NAS-Filter-Rule

TBD - Redirection-Id

TBD - Redirection-Rule

8. Open Issues

Normative References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[4] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[5] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[6] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.

Informative References

[7] Calhoun, P., "Diameter Network Access Server Application".

[8] 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.

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

Authors' Addresses

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Suite 100
Ottawa, Ontario K2K 3J1
Canada

Phone: (613) 591-6655
EMail: avi@bridgewatersystems.com
URI: TCP://.bridgewatersystems.com/

Farid Adrangi
Intel Corporation
2111 North East 25th
Hillsboro, Oregon 97124
United States

Phone: (503) 712-1791

EMail: farid.adrangi@intel.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

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