Networking Working Group
INTERNET-DRAFT
<draft-ietf-radext-filter-rules-00.txt>

Paul Congdon
Mauricio Sanchez
Hewlett-Packard Company
A. Lior
Bridgewater Systems
F. Adrangi
Intel
Bernard Aboba
Microsoft

24 February 2006

Filter Attributes

Copyright Notice

Abstract

In certain scenarios it is desirable to limit user access using filters or redirection. This document proposes additional attributes for this purpose, for use with the Remote Authentication Dial In User Server (RADIUS). The attributes described in this document are expected to be useful in a variety of environments, including enterprise and service provider scenarios.

Table of Contents

1. Introduction

Within the confines of RADIUS authentication, authorization, and accounting (AAA) environments, there is a requirement for standardized RADIUS attributes to limit user access using filters or redirection.

For example, in IEEE 802.1X [IEEE8021X] environments, which provides "network port authentication" for IEEE 802 [IEEE802] media, including Ethernet [IEEE8023] and 802.11 [IEEE80211i] wireless LANS, there exists a strong desire to control authorization beyond just the untagged VLAN parameter based on tunnel attributes in [RFC2868] and usage of these in [RFC3580].

This document describes filtering and redirection attributes that may prove useful in IEEE 802.1X and a variety of situations. The attributes defined in this document may be used with RADIUS dynamic authorization [RFC3576].

The Filter-ID attribute defined in [RFC2865] requires the NAS to be pre-populated with the desired filters. This may be difficult to deploy in roaming scenarios where the home realm may not know what filters have been pre-populated by the local operator. The filtering attributes specified in this document enable explicit description of layer 2 and layer 3 filters as well as redirection, and therefore extend the filter language described in [RFC3588].

User traffic redirection is supported with or without tunneling. Tunneling support is provided using the tunnel attributes defined in [RFC2868]. Redirection of traffic in mid-session may break applications.

1.1. Terminology

In this document when we refer to blocking of IP traffic we mean filtering of IP traffic. Additionally, this document uses the following terms:

Authenticator
: An authenticator is an entity that requires authentication from the supplicant. The authenticator may be connected to the supplicant at the other end of a point-to-point LAN segment or 802.11 wireless link.

Authentication server
: An authentication server is an entity that provides an authentication service to an authenticator. This service verifies from the credentials provided by the supplicant, the claim of identity made by the supplicant.

Hot-lining
: Blocking and redirection of users traffic is known as hot-lining of accounts. In this document, hot-lining is used as the motivation for these attributes and an illustration of how they would be used. However, the attributes may be used together or separately to provide other features.

Redirection
: Refers to an action taken by the NAS to redirect the user's traffic to an alternate location.

Supplicant
: A supplicant is an entity that is being authenticated by an authenticator. The supplicant may be connected to the authenticator at one end of a point-to-point LAN segment or 802.11 wireless link.

Terminal
: A terminal is an endpoint, such as an 802.1X supplicant, attached to the NAS port.

1.2. Requirements Language

In this document, several words are used to signify the requirements of the specification. 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].

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".

1.3. Capability Advertisement

RADIUS does not currently define a method by which a NAS can advertise its capabilities and in many instances, it would be desirable for the home network to know what capabilities are supported by the NAS to ensure proper operational behavior. The attributes defined in this document are intended to be used to enforce policy by the NAS. If a NAS does not recognize these attributes it will most likely ignore them and the desired policy will not be enforced. A method for the NAS advertising the capability to support these attributes would help the RADIUS server understand if the intended policies can be enforced. As a result, the attributes in this document, in particular NAS-Traffic-Rule(TBD), can benefit from capability advertisement, if available.

1.4 Attribute Interpretation

Unless otherwise noted in the individual description of an attribute contained herein, a NAS that conforms to this specification and receives an Access-Accept message that contains an attribute from this document that it cannot apply MUST interpret this though an Access-Reject had been sent and MUST terminate the session. If accounting is enabled on the NAS, it MUST generate an Accounting-Request(Stop) message upon session termination.

Similarly, if a NAS conforming to this specification and also conforming to RFC 3576 [RFC3576] receives a CoA-Request message that contains an attribute from this document that it cannot apply, it MUST NOT terminate the session and MUST generate a CoA-NAK packet with ERROR-CAUSE(101) set to "Unsupported Attribute"(401). If accounting is enabled on the NAS, it MUST NOT generate an Accounting-Request(Stop) message in such instances.

2. RADIUS Authentication

This specification introduces one new RADIUS authentication attributes.

2.5. NAS-Traffic-Rule

Description

The NAS-Traffic-Rule attribute is derived from the Diameter IPFilterRule and enables provisioning of base encapsulation (Layer 2) rules, Internet Protocol (Layer 3-4) rules, and HTTP (Layer 5+) rules on the NAS by the RADIUS server. Compared to Diameter's IPFilterRule, NAS-Traffic-Rule is a superset in functionality, but is largely based on the same syntax foundations.

For each rule and depending on the rule type, the NAS can be instructed to take a single action as follows:

Rule Type	Allowable rule action
Base Encapsulation	filter, tunnel
Internet Protocol	filter, tunnel
HTTP	filter, redirect

When specifying a base encapsulation rule, NAS-Traffic-Rule processes packets based on the following information that is associated with it:

Direction	(in and/or out)
Base encapsulation type	
Source and destination MAC address	(possibly masked)

For a base encapsulation rule, the filter action entails having the NAS permit (i.e. forward) or deny (i.e. block) a user's traffic. The tunnel action entails having the NAS forward user traffic to or from a named tunnel that has been established per [RFC2868].

When specifying an Internet Protocol rule, NAS-Traffic-Rule processes packets based on the following information that is associated with it:

Direction	(in and/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

For an Internet Protocol rule, the filter action entails having the NAS permit (i.e. forward) or deny (i.e. block) a user's traffic. The tunnel action entails having the NAS forward user traffic to or from a named tunnel that has been established per [RFC2868].

When specifying an HTTP rule, NAS-Traffic-Rule processes packets based on the following information that is associated with it:

HTTP URL
Source and destination IP address (possibly masked)

For an HTTP rule, the filter action entails having the NAS permit (i.e. forward) or deny (i.e. block) a user's [RFC2616] request message. For a deny action, the NAS MAY respond to the request message with a code 403 (Forbidden) response in accordance with [RFC2616]. For a redirect action the NAS SHOULD respond to the user's request with a code 302 (Found) response in accordance with [RFC2616].

For the HTTP redirection action, it is also possible to have redirection automatically removed by including a redir-cnt count parameter along with the rule. The rule will be removed from the active rule set when the rule matches redir-cnt number of times. Upon removal from the active rule set, traffic is no longer evaluated against this rule.

It should be noted that an HTTP filter or redirect rule is only useful with plain-text HTTP and not [RFC2818] HTTPS. Redirection or filtering of HTTPS is outside the scope of this document.

As per the requirements of RFC 2865, Section 2.3, if multiple NAS-Traffic-Rule attributes are contained within an Access-Accept or CoA-Request packet, they MUST be maintained in order. The attributes MUST be consecutive attributes in the packet. RADIUS proxies MUST NOT reorder NAS-Traffic-Rule attributes.

The RADIUS server can return multiple NAS-Traffic-Rule attributes in an Access-Accept or CoA-Request packet. Where more than one NAS-Traffic-Rule attribute is included, it is assumed that the attributes are to be concatenated to form a single filter list. Furthermore, if the list contains different

types of rules, they MUST appear in the following order: flush

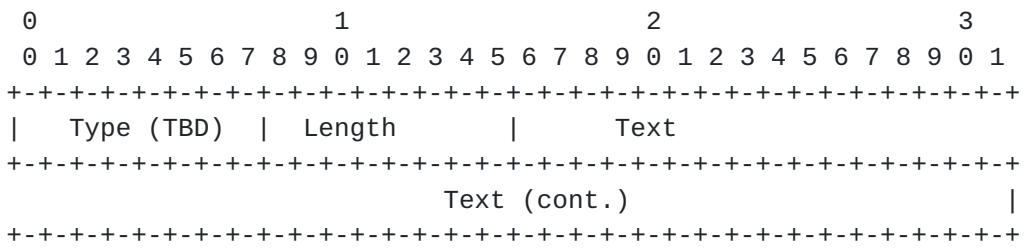
rules, base encapsulation tunnel rules, base encapsulation filter rules, IP tunnel rules, HTTP redirect rules, IP filter rules, and HTTP filter rules.

Rules are evaluated in order, with the first matched rule terminating the evaluation. Each packet is evaluated once. If no rule matches, then packet is dropped (implicit deny all).

When an HTTP redirect rule matches, the NAS shall reply to the HTTP request with an HTTP redirect in accordance with [RFC2616] redirecting traffic to specific URL.

Filter-ID (11) and NAS-Traffic-Rule both define how filters are to be applied in the NAS. These attributes are not intended to be used concurrently and SHOULD NOT appear in the same RADIUS message. Only one type of filtering attribute must be processed. If a Filter-ID (11) is present, then the NAS-Traffic-Rule MUST be ignored, if present.

The NAS-Traffic-Rule attribute is shown below. The fields are transmitted from left to right:



Type

TBD

Length

>= 3

Text

The text conforms to the following ABNF [RFC2234] formatted syntax specification:

```
; Start of ABNF description of NAS-Traffic-Rule

rule           =  (flush-rule / permit-all-rule
                  / l2-filter-rule / l2-tunnel-rule
```

```
                    / ip-filter-rule / ip-tunnel-rule
                    / http-filter-rule / http-redir-rule)
                    rule-delim

        ; Flush Rule
        flush-rule     =  "flush"

        ; Permit all rule
        permit-all-rule = "permit inout any from any to any"

        ; Base encapsulation filter rule
        l2-filter-rule =  ("permit" / "deny") " "
                          ("in" / "out" / "inout") " "
                          l2-filter-body [" " log-rule]
        l2-filter-body =  (l2-proto " from " l2-address " to "
                          l2-address) / l2-rmon-str
        l2-proto       =  "l2:ether2" [":0x" 1*4HEXDIG]
        l2-rmon-str    =  "l2:" 1*DIGIT *("." 1*DIGIT)
        l2-address     =  ["!"] (macaddr / (macaddr "/" macmask)
                          / "any")
        macaddr        =  2HEXDIG 5("-" 2HEXDIG)
        macmask        =  DIGIT                ; 0-9
                          / %x31-33 DIGIT      ; 10-39
                          / "4" %x30-38        ; 40-48

        ;Base encapsulation tunnel rule
        l2-tunnel-rule =  "tunnel " tunnel-id " "
                          ("in" / "out" / "inout") " "
                          l2-filter-body [" " log-rule]

        ;IP Filter Rule
        ip-filter-rule =  ("permit" / "deny") " "
                          ("in" / "out" / "inout") " "
                          ("ip" / ip-proto) filter-body
                          [" " ip-option] [" " log-rule]
        ip-proto       =  d8
        ip-address     =  ["!"] (ipv4-address ["/" ipv4mask] /
                                 ipv6-address ["/" ipv6mask] /
                                 "any" /
                                 "assigned")
        ipv4-address   =  d8 "." d8 "." d8 "." d8
        ipv4mask       =  DIGIT                  ; 0-9
                          / %x31-32 DIGIT        ; 10-29
                          / "3" %x30-32          ; 30-32
        ipv6-address   =  1*4HEXDIG 7(":" 1*4HEXDIG)
        ipv6mask       =  DIGIT                  ; 0-9
                          / %x31-39 DIGIT        ; 10-99
                          / "1" %x30-31 DIGIT    ; 100-119
                          / "1" %x32 %x30-38     ; 120-128
```

```
tcp-ports      =  tcp-port *("," tcp-port)
```

```
        tcp-port       =  d16 / d16 "-" d16
        ip-option      =  "frag" /
                          ["ipoptions " ["!"] ipopt *("," ["!"] ipopt)]
                          ["tcpoptions " ["!"] tcpopt
                           *("," ["!"] tcpopt)]
                          ["established"]
                          ["setup"]
                          ["tcpflags " ["!"] tcpflag
                           *("," ["!"] tcpflag)]
                          ["icmptypes " icmptype *("," icmptype)]
        ipopt          =  "ssrr" / "lsrr" / "rr" / "ts"
        tcpopt         =  "mss" / "window" / "sack" / "ts" / "cc"
        tcpflag        =  "fin" / "syn" / "rst" / "psh" / "ack" / "urg"

        icmptype       =  d8 / d8 "-" d8
                          / "echo reply" / "destination unreachable"
                          / "source quench" / "redirect"
                          / "echo request" / "router advertisement"
                          / "router solicit" / "time-to-live exceeded"
                          / "IP header bad" / "timestamp request"
                          / "timestamp reply" / "information request"
                          / "information reply"
                          / "address mask request"
                          / "address mask reply"

        ;IP Tunnel Rule
        ip-tunnel-rule =  "tunnel " tunnel-id " "
                          ("in" / "out" / "inout") " "
                          ("ip" / ip-proto) filter-body
                          [" " ip-option] [" " log-rule]

        ;HTTP Filter Rule
        http-filter-rule= ("permit" / "deny") org-url " "
                          ("in" / "out" / "inout") filter-body
                          [" " log-rule]


        ;HTTP Redirect Rule
        http-redir-rule=  "redirect " [redir-cnt " "] redir-url
                          filter-body [" " org-url]
                          [" " log-rule]
        redir-cnt      =  1*DIGIT
        org-url        =  http_URL
                          ;Note: Syntax for http_URL defined in
                          ;[RFC2616], section 3.2.2
        redir-url      =  http_URL

        ;Common
        filter-body    =  " from " ip-address [" " tcp-ports]
```

```
" to " ip-address [" " tcp-ports]
```

```
      tunnel-id      =  DQUOTE
                        1*(TEXTDATA / ("%" 2HEXDIG))
                        DQUOTE
      log-rule       =  "cnt"

      ;Primitives
      LF             =  %x0A                 ; linefeed
      DIGIT          =  %x30-39              ; 0-9
      DQUOTE         =  %x22                 ; " (Double Quote)
      HEXDIG         =  DIGIT / "A" / "B" / "C" / "D" / "E" / "F"
      rule-delim     =  LF
      d8             =  DIGIT                ; 0-9
                        / %x31-39 DIGIT      ; 10-99
                        / "1" 2DIGIT         ; 100-199
                        / "2" %x30-34 DIGIT  ; 200-249
                        / "25" %x30-35       ; 250-255
      d16            =  DIGIT                ; 0-9
                        / %x31-35 1*4DIGIT   ; 10-59999
                        / "6" "4" 3DIGIT     ; 60000-64999
                        / "6" "5" %x30-34 2DIGIT     ; 65000-65499
                        / "6" "5" "5" %x30-32 1DIGIT  ; 65500-65529
                        / "6" "5" "5" "3" %x30-36     ; 65530-65536
      TEXTDATA       =  %x20-21 / %x23-24 / %x26-7E

      ; End of ABNF description of NAS-Traffic-Rule
```

Descriptions of notable fields and keywords follow:

"permit" Allow packets that match the rule.

"deny" Drop packets that match the rule.

"redirect" Redirect packets that match the rule.

"tunnel" Tunnel packets that match the rule.

"flush" A flush rule removes all previously assigned filter rules. When flush is specified, it can be followed by other NAS-Traffic-Rule attributes. This allows for an atomic change of authorization with a single RADIUS message.

"permit inout any from any to any"
Special rule that matches against all traffic. This allows the implicit deny at the end of a filter list to be overridden.

"in" Is from the terminal.

"out" Is to the terminal.

"inout" Is from and to the terminal.

ipv4-address An IPv4 number in dotted-quad form. Only this exact IP number will match the rule.
ipv6-address An IPv6 number in canonical IPv6 form. Only this exact IP number will match the rule.
ipv4-address/ipv4mask
An IP number with a mask width of the form 192.0.2.0/24. In this case, all IP numbers from 192.0.2.0 to 192.0.2.255 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.

"any" Keyword for 0.0.0.0/0 or the IPv6 equivalent.

"assigned" Keyword for 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.

tcp-port With the TCP, UDP and SCTP protocols, this field specifies ports to match.

Note: 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" keyword for details on matching fragmented packets.

log-rule Increments rule hit counter by one every time a packet matches on rule. Counters start with a zero value at session start and are reset back to a zero value every time a successful authorization change occurs due to a CoA message being received by the NAS.

For base encapsulation rules:

"l2:" Prefix to designate a rule as a base encapsulation rule.

"l2:ether2" keyword means any Ethernet-II (DIX Ethernet) will match.

ether2:val Used to specify an Ethernet-II type by hexadecimal number, whereby "val" is replaced by desired number. Example: "l2:ether2:0x800" for IP ethertype (0x0800).

l2-rmon-str Used to specify base encapsulation per the octet string format defined in [RFC2895], section 4.2. Example: "l2:0.0.0.2.0.0.0.240" for Netbios over LLC.

macaddr For base encapsulation filter rules of "l2:ether2" type, the Ethernet MAC address with octet values separated by a "-". Example: "00-10-A4-23-19-C0".

macaddr/mask An Ethernet number as above with a mask width of the form "00-10-A4-23-00-00/32". In this case, all MAC addresses from 00-10-A4-23-00-00 to 00-10-A4-23-FF-FF will match. The MAC address MUST NOT have bits set beyond the mask. The keyword "any" is 00-00-00-00-00-00/0.

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

Note: macaddr nor macaddr/mask argument is not used for "l2:rmon" type rules.

For IP rules:

"ip" Keyword means any IP protocol will match.

ip-proto An IP protocol specified by number.

"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" 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" 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" 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" 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).

For HTTP redirection rules:

redir-cnt Specifies the number of HTTP redirect rule matches that should transpire before removing this rule from the active rule set. Upon removal from the

active rule set, traffic is no longer evaluated against this rule.

redir-url An HTTP URL. When the 'redirect' rule matches (src/dst and/or org_URL), HTTP requests are redirected to redir_URL address in accordance with [RFC2616] redirection traffic to specific URL.

org-url An HTTP URL. Specifies the HTTP URL against which user HTTP requests will be evaluated. If user HTTP request matches org_URL, then redirection action is taken.

For base encapsulation and IP tunnel rules:

tunnel_id A tunnel id. When the 'tunnel' rule matches, traffic is redirected over the tunnel with the specified tunnel_id. Traffic can only be redirected to or from named tunnels that have been established per [RFC2868] and named using the Tunnel-Assignment-ID attribute described therein.

The tunnel id MUST be encapsulated in double quotes and follow the labeling convention defined by the TEXTDATA.
Example: A tunnel with the name of tunnel "ppp%1" would be specified as "%22ppp%251%22"

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

3. RADIUS Accounting

This specification introduces one new RADIUS accounting attribute.

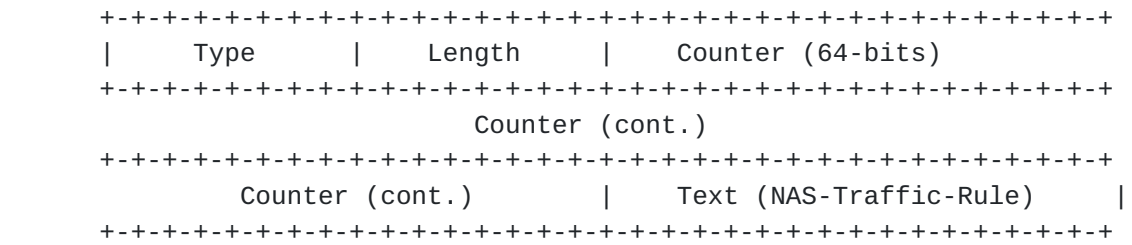
3.1. Acct-NAS-Traffic-Rule

Description

Acct-NAS-Traffic-Rule enables a RADIUS client to include NAS-Traffic-Rule[TBD] rule match counters as part of the accounting message.

The Acct-NAS-Traffic-Rule attribute is shown below. The fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```



Type
TBD

Length
>=3

String

The first eight octets of this string are used for a 64-bit value of the rule counter. The remaining octets are used to specify for which filter rule the counter is for a value. The rule specification MUST conform to the syntax rules specified for NAS-Traffic-Rule[TBD].

4. 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	#	Attribute
0	0+	0	0	0+	TBD	NAS-Traffic-Rule

Actng-Request	Actng-Response	#	Attribute
0-1	0	TBD	Acct-NAS-Traffic-Rule

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

0	This attribute MUST NOT be present in 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.

5. Diameter Considerations

Diameter needs to define identical attributes with the same Type values. The attributes should be available as part of the NASREQ

application [RFC4005], as well as the Diameter EAP application [RFC4072].

6. IANA Considerations

This document uses the RADIUS [RFC2865] namespace, see <http://www.iana.org/assignments/radius-types>. Allocation of six updates for the section "RADIUS Attribute Types" is requested. The RADIUS attributes for which values are requested are:

TBD - NAS-Traffic-Rule
TBD - Acct-NAS-Traffic-Rule

7. Security Considerations

Since this document describes the use of RADIUS for purposes of authentication, authorization, and accounting in [IEEE8021X] enabled networks, it is vulnerable to all of the threats that are present in other RADIUS applications. For a discussion of these threats, see [RFC2607], [RFC3162], [RFC3579], and [RFC3580].

This document specifies new attributes that can be included in existing RADIUS messages. These messages are protected using existing security mechanisms; see [RFC2865] and [RFC3576] for a more detailed description and related security considerations.

The security mechanisms in [RFC2865] and [RFC3576] are primarily concerned with an outside attacker who modifies messages in transit or inserts new messages. They do not prevent an authorized RADIUS server or proxy from inserting or deleting attributes with a malicious purpose in messages it sends.

An attacker who compromises an authorized RADIUS server or proxy can use the attributes defined in this document to influence the behavior of the NAS in ways that previously may not have been possible. For example, modifications to the VLAN-related attributes may cause the NAS to permit access to other VLANs that were intended. To give another example, inserting suitable redirection rules to the NAS-Traffic-Rule attribute may allow the attacker to eavesdrop or modify packets sent by a legitimate client.

In general, the NAS cannot know whether the attribute values it receives from an authenticated and authorized server are well-intentioned or malicious, and thus it is not possible to completely protect against attacks by compromised nodes. In some cases, the extent of the possible attacks can be limited by performing more fine-grained authorization checks at the NAS.

For instance, a NAS could be configured to accept only certain VLAN IDs from a certain RADIUS server/proxy, or not to accept any redirection rules if it is known they are not used in this environment.

8. References

8.1. Normative references

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

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach P., Berners-Lee T., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

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

[RFC2895] Bierman, A., Bucci, C., Iddon, R., "Remote Network Monitoring MIB Protocol Identifier Reference", RFC 2895, August 2000

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

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

[IEEE802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[IEEE8021X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, August 2004.

8.2. Informative references

[RFC2234] Croker, E., Overell, P., "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

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

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC2818, May 2000.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol

Support", RFC 2868, June 2000.

[RFC3162] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[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.

[RFC4072] Eronen, P., Hiller, T., Zorn G., "Diameter Extensible Authentication Protocol (EAP) Application", RFC4072, August 2005.

[IEEE8023]
ISO/IEC 8802-3 Information technology - Telecommunications And information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, (also ANSI/IEEE Std 802.3- 1996), 1996.

[IEEE80211]
Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-1999, 1999.

[IEEE80211i]
Institute of Electrical and Electronics Engineers, "Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer
(PHY) Specifications: Specification for Enhanced Security", June 2004.

Appendix A - Traffic Redirection

There are several ways to redirect the user's traffic. Which method will be used depends on the capabilities available at the NAS and Service Provider's preference. This Appendix describes

various methods to redirect user traffic by using the new attributes outlined in this document in conjunction with existing attributes, which are:

1) Tunneling; and
2) HTTP Redirection;

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

A.1 Tunneling

User traffic can be redirected by tunneling the user's traffic to an alternate location. Tunneling will typically redirect all of the user's traffic for the Service. When tunneling is used to redirect all the traffic, then filtering may not be necessary.

A.1.1 Service Initiation

Redirect using tunnels at service initiation requires that the RADIUS server send the appropriate [RFC2868] tunnel attributes and NAS-Traffic-Rule attributes to the NAS. The [RFC2868] tunnel attributes describe the tunnel endpoint and the type of tunnel to construct. The 'tunnel <tunnel_id>' option for the NAS-Traffic-Rule allows the specification of a traffic rule for which to redirect traffic to a named tunnel.

A.1.2 Mid-session Tunnel Redirection

Redirection of traffic using tunnels mid-session involves sending the tunnel attributes as per [RFC2868] to the NAS using Change-of-Authorization (CoA) message. The operation is described in [RFC3576]. 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 message 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.

A.1.3 Tunnel 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 message. The NAS will tear down the 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 there is a problem because RADIUS does not have a mechanism whereby it can de-tunnel. Receiving a CoA message without tunnel attributes would not have an effect on an existing tunnel. In order to de-tunnel the session, the RADIUS server has to send the NAS a CoA message with Service-Type(6) set to "Authorize-Only" causing the NAS to perform a re-Authorization. In response to the 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.

A.1.4 Tunnel Redirection Examples

The following examples illustrate how traffic flows when subjected to a NAS-Traffic-Rule using tunnel redirection. In these scenarios, the following notation is used to represent traffic flows:

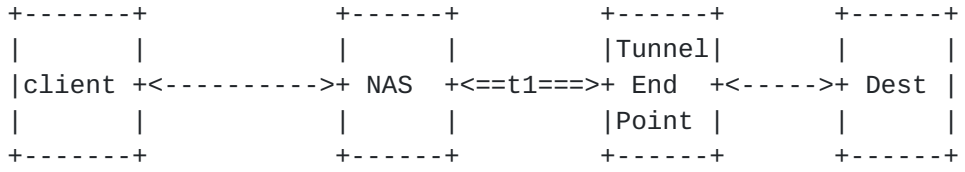
```
------>  Flow in one direction
<----->  Flow in two directions
======>  Flow in a tunnel in one direction
<=====>  Flow in a tunnel in two directions
```

A RADIUS server that wishes all IP traffic to flow between the client and a selected redirection destination will issue an Access-Accept that contains the specification for the tunnel using the attributes defined by RFC 2868 and a NAS-Traffic-Rule attribute using the tunnel action and arguments.

An example NAS-Traffic-Rule will look like:

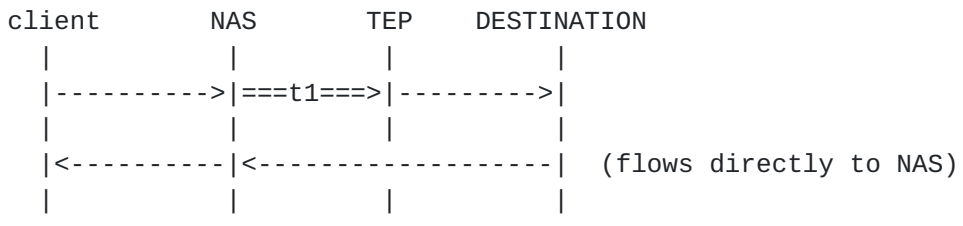
tunnel "t1" in ip from assigned to any

This will cause all traffic that flows from the client to any destination to be tunneled over the named tunnel "t1" to the tunnel endpoint (TEP).



The direction argument takes the values of "in", "out" or "inout" and is important because it controls how information is routed. The following diagram demonstrates how traffic is routed. In all these diagrams time is increasing as we proceed down the page.

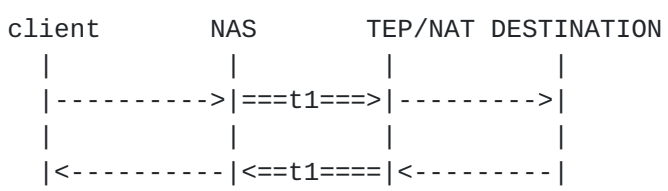
When rule direction is "in":



The inbound traffic from the client matches the specified filter rule and the IP packet is placed in the tunnel to the TEP. The TEP forwards the packet to the Destination using the destination IP address in the packet header. Note that the source address of the packet is the address assigned at the NAS. Therefore if the destination were to reply to the packet it would use the NAS source address and the packet would flow directly to the NAS and to the client bypassing the TEP. The Home network would use this capability if it was only interested in metering or seeing the inbound traffic from the client.

However, if the home network wanted to see the traffic in both directions it could deploy a NAT function at the TEP.

Here is the flow when the TEP is acting like a NAT:



The client establishes a connection to the Destination, but the TEP acting as NAT, changes the source address of the IP packet (as NATs do) to that of the TEP/NAT. Now any replies from the Destination are sent to the TEP/NAT. The TEP/NAT then forwards these packets to the client through the NAS.

When the TEP is acting as a NAT, using the direction argument "in" is important. The direction argument set to "out" will have no effect on traffic coming from the tunnel since all traffic to the client should come from the TEP/NAT inside the tunnel. The direction argument set to "inout" will have the same effect as if it were set to "in".

The TEP/NAT forwards all traffic for the client into the tunnel to the NAS. The NAS always forwards any egressing traffic from the tunnel to the client. It does not apply any redirection rules on

traffic egressing a tunnel. The NAS does not care whether the TEP is transparent or is acting as a NAT.

A.2 HTTP Redirection

Another method of redirection is at the application layer, specifically the HTTP layer. An HTTP aware NAS redirects traffic by issuing an HTTP Redirect response causing the user's browser to navigate to an alternate Web Portal.

The call flow associated with performing redirection at the HTTP layer is very similar with the call flow associated with redirection done at the IP layer.

The same NAS-Traffic-Rule(TBD) attribute described above is used to convey the redirection rules to use for HTTP redirection. HTTP redirection rules within the NAS-Traffic-Rule attribute supports the encoding of a redirection URL to apply when a rule is matched.

A.2.1 Service Initiation

As with previous call flows, the RADIUS server MAY send multiple HTTP redirect or filtering rules within a NAS-Traffic-Rule(TBD) attribute to the NAS in the Access-Accept message.

A.2.2 Mid-session HTTP Redirection

If HTTP redirection is required to be applied to a service that has already been started then the RADIUS server can push the redirection rules, and optionally the filter rules, to the NAS within a NAS-Traffic-Rule(TBD) attribute using a CoA-Request message. The NAS will then commence to apply the redirection rules and/or the filter rules.

Alternatively, the RADIUS server can request that the NAS re-authorize the session using the procedures defined in [RFC3576]. 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 rules within a NAS-Traffic-Rule(TBD) attribute.

A.2.3 HTTP Redirection Removal

HTTP Redirection rules can be automatically removed mid-session from the NAS using the redir-cnt parameter or explicitly removed from the RADIUS server. The RADIUS server can explicitly turn HTTP redirection off mid-session in two ways. It can push new redirection rules within a NAS-Traffic-Rule(TBD) attribute using a CoA-Request message or it can send the NAS a CoA-Request message requesting it to re-authorize.

When using CoA-Request message to return the redirection and filtering back to "normal," there needs to be either a filter rule (or filter-id) or redirection rule that corresponds to the "normal" state. If normally the session did not have any filter and or redirection rules applied, the RADIUS server can send a NAS-Traffic-Rule(TBD) with the action of "flush" in the CoA-Request message. This action will cause all the filter rules and redirection rules previously assigned to the session to be removed.

A.3 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.

A.4 Example Scenarios

The following two examples illustrate the user's experience when being redirected.

For the first example assume an [IEEE8021X] environment, whereby a user connects to the enterprise LAN and initiates an authentication handshake. As part of the overall authentication process, it is also possible to pass endpoint state such as patch level, virus signature status, etc., all of which can be verified by a back-end server for policy compliancy and alter the authentication and authorization decision. In instances that an end-host is not in compliancy, the NAS may be instructed to limit network access in some fashion (i.e. quarantine) and limit network access to remediation services and a web-based information site. A user may sense degraded network performance and open a web session, which the NAS would redirect to the web-based information site for compliancy status, remediation actions, etc.

For the second example assume an ISP environment, whereby a prepaid user is roaming the net in their hotel room over WiFi and is to be Hot-lined 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.

Appendix B - NAS-Traffic-Rule Filter Examples

This appendix presents a variety of filter examples utilizing the syntax definition described in section 3.5

Example #1: Permit all user traffic, regardless of type.

```
permit inout any from any to any
```

Example #2: Permit only L2 traffic coming from and going to a user's Ethernet MAC address. Block all other traffic. Assume user's MAC address is 00-10-A4-23-19-C0.

```
permit in l2:ether2 from 00-10-A4-23-19-C0 to any
permit out l2:ether2 from any to 00-10-A4-23-19-C0
```

Example #3: Tunnel all L2 traffic coming from and going to a user. Assume tunnel name is: tunnel "1234".

```
permit tunnel "tunnel \"1234\"" inout l2:ether2 from any to any
```

Example #4: Permit only L3 traffic coming and going to from a user's IP address. Block all other traffic. Assume user's IP address is 192.0.2.128.

```
permit in ip from 192.0.2.128 to any
permit out ip from any to 192.0.2.128
```

Example #5: Permit only L3 traffic coming and going to the user's assigned IP address. Block all other traffic.

```
permit in ip from assigned to any
permit out ip from any to assigned
```

Example #6: Allow user to generate ARP requests, DNS requests, and HTTP (port 80) requests. Assume user's MAC address is 00-10-A4-23-19-C0 and IP address is 192.0.2.128.

```
permit in l2:ether:0x0806 from 00-10-A4-23-19-C0 to any
permit out l2:ether:0x806 from any to 00-10-A4-23-19-C0
permit in 17 from 192.0.2.168 to any 53
permit out 17 from any 53 to 192.0.2.168
permit in 6 from 192.0.2.168 80 to any
permit out 6 from any 80 to 192.0.2.168
```

Example #7: Allow user to generate ARP requests, DNS requests, and HTTP (port 80) requests, any of which are redirected to http://www.goo.org. Assume user's MAC address is 00-10-A4-23-19-C0 and IP address is 192.0.2.128.

```
        permit in l2:ether:0x0806 from 00-10-A4-23-19-C0 to any
        permit out l2:ether:0x806 from any to 00-10-A4-23-19-C0
        permit in 17 from 192.0.2.168 to any 53
        permit out 17 from any 53 to 192.0.2.168
        redirect http://www.goo.org in from 192.0.2.168 to any 80
```

Example #8: Allow user to generate ARP requests, DNS requests, and HTTP (port 80) requests, of which only requests to http://www.goo.org are redirected to http://www.goo.org. Assume user's MAC address is 00-10-A4-23-19-C0 and IP address is 192.0.2.128

```
        permit in l2:ether:0x0806 from 00-10-A4-23-19-C0 to any
        permit out l2:ether:0x806 from any to 00-10-A4-23-19-C0
        permit in 17 from 192.0.2.168 to any 53
        permit out 17 from any 53 to 192.0.2.168
        redirect http://www.goo.org in from 192.0.2.168 to any 80
           http://www.goo.org
```

Acknowledgments

The authors would like to acknowledge Joseph Salowey of Cisco, David Nelson of Enterasys, Chuck Black of Hewlett Packard, and Ashwin Palekar of Microsoft.

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 (editor)
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

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

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

Disclaimer of Validity

Copyright Statement