

Using Radius for PE-Based VPN Discovery
<[draft-heinanen-radius-pe-discovery-02.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

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>.

Abstract

This document describes how in PE-based VPNs a PE of a VPN can use Radius to authenticate its CEs and discover the other PEs of the VPN.

1. Introduction

This document describes how in PE-based VPNs a PE of a VPN can use Radius [1-2] to authenticate its CEs and discover the other PEs of the VPN. In Radius terms, the CEs are users and PEs are Network Access Servers (NAS) implementing Radius client function.

A VPN can span multiple Autonomous Systems (AS) and multiple providers. Each PE, however, only needs to be a Radius client to Radius of the "local" provider. In case of a CE belongs to a "foreign" VPN, Radius of the local provider acts as a proxy client to Radius of the foreign provider.

It is envisioned that a similar Radius based mechanism can be used by CEs of a CE-based VPN to discover the other CEs of the VPN.

2. Site Identification

Each CE (a VPN site) is identified by a "user name" of the form

[realm/]user@domain

"realm", if present, denotes a provider that is the administrative owner of the VPN. It is needed only if a CE connects to a VPN at a PE that does not belong to the owner of the VPN and is then used by Radius of the PE to proxy requests to Radius of the owner of the VPN.

"user" identifies a site in a VPN identified by "domain". As an example,

providerX/atlanta@vpnY.domainZ.net

could denote a CE called "atlanta" in a VPN identified by "vpnY.domainZ.net", which is owned by providerX.

3. Radius Configuration

Each realm has a single Radius that stores all information regarding VPNs that belong to the realm. For reliable operation of this protocol, each Radius should consist of more than one physical Radius server. For correct operation of this protocol, all these physical servers MUST at all times share the same database content.

For each VPN, Radius of the realm to which the VPN belongs to MUST at all times be configured with a set of "users" that correspond to the potential CEs of the VPN, i.e., CEs that are currently allowed to be connected to the VPN at some PE. User information includes user name, password, and VPN identifier:

<CE user name, password, VPN identifier>

User information MAY also include other information, such as a list of PEs to which the CE is allowed to connect to and QoS information regarding the CE's connection to the VPN.

In addition to the above manually configured information, Radius keeps dynamically track of the PEs of the VPN as described below (Protocol Operation). The PEs MAY also have pre-configured attributes telling, for example, that a PE is a hub of a VPN.

If dynamic PE discovery capability of this protocol is not used,

Radius MUST be configured for each VPN with a list of its PEs. Such a degenerate use of this protocol is not discussed further in this memo.

In order to allow local PEs and Radius servers in foreign realms to make CE related queries to Radius of the local realm, potential local PEs and Radius servers of foreign realms MUST be configured in local Radius as clients.

4. PE Configuration

Each PE MUST be configured with the information about the Radius servers of local Radius to which to send requests to. For reliability reasons, each PE SHOULD have available more than one physical Radius server.

5. Protocol Operation

5.1 Radius Database

Radius keeps track of the PEs and CEs of a VPN in a database table that has the following fields:

<VPN identifier, PE IP address, CE user name>

In addition, Radius records for each active PE the time when it has last received from the PE any Radius request:

<PE IP address, timestamp>

This information is used by Radius to detect if a PE has failed for a longer period of time or has been taken improperly out of use, and if so, to clean up its database.

5.2 Connecting a CE to a VPN at a PE

When a CE is to be connected to a VPN at a PE, the PE issues a Radius Access-Request using the user name and password of the CE. The PE has either learned this information from the CE via an authentication protocol, for example, 802.1x/EAP, or it has been configured in the PE.

If (a) authentication succeeds, (b) possible other preconditions are met, e.g., the CE is allowed to connect to the particular PE, and (c) a record

<VPN identifier, *, CE user name>

does not already exist in Radius database with some other PE IP address, Radius inserts the

<VPN identifier, PE IP address, CE user name>

record in its database (if not already there) and responds with an Access-Accept. Access-Accept includes as reply items the identifier of the VPN to which the CE belongs, a list of all unique PE IP addresses in the set

<VPN identifier, *, *>

and possibly other CE specific information, e.g., QoS parameters. After receiving the Access-Accept, the PE considers the CE as connected to the VPN and issues a Start Accounting-Request.

If some of the conditions (a) - (c) listed above are not met, Radius responds with Access-Reject.

If a PE wants for some reason to get from Radius an up-to-date list of PEs in a particular VPN, it can at any time issue a new Access-Request for any one of its CEs that belongs to the VPN.

[5.3](#) Disconnecting a CE from a VPN at a PE

When a CE is to be disconnected from the VPN at a PE, the PE issues a Stop Accounting-Request. After receiving the request, Radius removes the

<VPN identifier, PE IP address, CE user name>

record from its database and responds with an Accounting-Response. The PE considers the CE as disconnected from the VPN at the PE when it has received the Accounting-Response.

[5.4](#) PE Failure Detection and Recovery

Whenever N minutes has elapsed from the last Radius request that the PE has sent for any CE in a realm, it issues an Interim-Update Accounting-Request for any one of its CEs that belong to the realm.

If Radius doesn't receive from a PE any request during a period of M * N minutes, Radius considers the PE un-operational and removes from its database all

<*, PE IP address, *>

records and the

<PE IP address, timestamp>

record. No matter how long the failure has lasted, upon recovery, the PE re-authenticates all CEs connected to it in all VPNs and thus re-discovers all other PEs in all those VPNs.

6. Scaling Limits

Since Radius protocol operates over UDP, the maximum UDP payload size available for Radius attributes is limited to about $1500 - 40 = 1460$ octets assuming that UDP fragmentation is not supported. The most space consuming message is Access-Accept response, which contains a list of IP addresses of the PEs of a VPN. This limits the number of PEs in a VPN to about 350, which is large enough for a fully meshed VPN.

Larger VPNs can be easily supported by configuring some of the PEs as hubs, since only the hubs of a VPN need to be advertised in the Access-Accept response. This provides a scalable way to increase the maximum number of PEs in a VPN to thousands.

Besides the packet size, another factor limiting scalability of this protocol might be the keep-alive mechanism implemented by Interim-Update Accounting-Request. However, since a PE needs to send only one keep-alive message per N minutes per realm in which it has at least one VPN site, scalability of keep-alives it is not an issue.

9. Security Considerations

Security of Radius based VPN discovery depends on the security of Radius, that is covered in [[1](#)] and [[2](#)].

9. Further Work

Protocol details of Radius based VPN discovery will be specified in a future version of this memo, provided that there is enough IETF interest in Radius based discovery.

Acknowledgements

I would like to thank Mark Duffy, Joel Halpern, and Mark Townsley for their constructive comments on earlier versions of this memo.

References

[1] C. Rigney, et al., "Remote Authentication Dial In User Service (RADIUS)". [RFC 2865](#), June 2000.

[2] C. Rigney, "RADIUS Accounting". [RFC 2866](#), June 2000.

Author's Address

Juha Heinanen
Song Networks, Inc.
Hallituskatu 16
33200 Tampere, Finland
Email: jh@song.fi

Full Copyright

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.