Internet Engineering Task Force
INTERNET DRAFT
Expires December 2003

Juha Heinanen
TutPro Inc.
June, 2003

Using Radius for PE-Based VPN Discovery
<draft-heinanen-radius-pe-discovery-04.txt>

Status of this Memo

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.

2. Site Identification

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

    [provider/]site@vpn

"provider" identifier, 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.

"site" identifier denotes a site in a VPN identified by "vpn". 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 "provider" has a single Radius that stores all information regarding VPNs that belong to the provider. 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 provider 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 site identifier, password, and VPN identifier:

    <site, password, vpn>

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 and CEs of a VPN in a database table that has the following fields:

    <vpn, PE IP address, site, timestamp>

received from the PE any Radius request:

<PE IP address, timestamp>

Timestamp tells the most recent time when the PE has authenticated the site to the VPN. It 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 the site and PE from its database.

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 queries about CEs that are connected PEs of a "foreign" provider, the Radius servers of this foreign provider MUST be configured as clients in the Radius of the VPN owner.

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 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.

Service-Type of the Access-Request is VPN-Login (value TBD).

If authentication succeeds and possible other (VPN or provider) specific preconditions are met (for example, the CE is allowed to connect to the particular PE and it is not already connected to some other PE), Radius inserts a

<vpn, PE IP address, site, timestamp>

record in its database (replacing a possible earlier record that only

differs by the timestamp value) and responds with an Access-Accept. Access-Accept includes as reply items a Session-Timeout attribute and one or more PE-List attributes that contain all unique PE IP addresses in the set

<vpn, *, *>

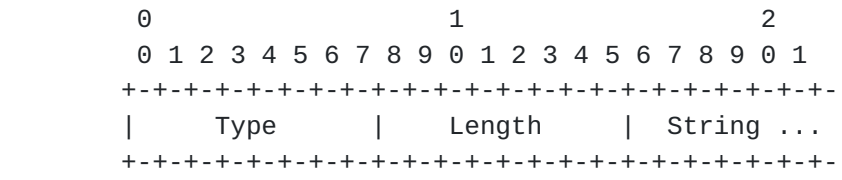
and possibly other CE specific information, e.g., QoS parameters.

Session-Timeout attribute tells to the PE for how long time Radius considers the CE as connected to the VPN at the PE unless the PE re-authenticates the CE. The value of the timestamp in

<vpn, PE IP address, site, timestamp>

record is the time of the Access-Accept plus the number of seconds in the Session-Timeout attribute.

PE-List attribute contains a list of PE IP addresses. It is only used in Access-Accept packets and has the following format:



Type

TBD for PE-List

Length

16 + N * 4 bytes, where 1 <= N <= 63.

String

N IP Addresses of PEs (the most significant octet first in each address).

After receiving the Access-Accept, the PE considers the CE as connected to the VPN and issues a Start Accounting-Request.

If authentication fails or some pre-conditions 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. In order to keep the CE connected to the VPN at the PE, the PE MUST issue a new Access-Request before the number of seconds returned by Radius in Session-Timeout attribute of the most recent Access-Accept has elapsed.

Note that this document does not define any protocol mechanisms by which the other PEs of the VPN would be notified that a new CE was connected to the VPN at the PE or that a new PE became associated with the VPN. Such mechanisms belong to the VPN solution documents that utilize the discovery protocol defined in this memo.

5.2 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, PE IP address, site>

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.

Note that this document does not define any protocol mechanisms by which the other PEs of the VPN would be notified that a CE was disconnected from the VPN at the PE or that the PE is not anymore associated with the VPN. Such mechanisms belong to the VPN solution documents that utilize the PE discovery protocol defined in this memo.

5.3 PE Failure Detection and Recovery

When a PE recovers from a failure, it 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.

Besides the packet size, another factor limiting scalability of this protocol might be the periodic re-authentication of CEs as required

by the Session-Timeout reply attribute. For example, if a provider has 3600 VPN sites and uses a Session-Timeout value of 1 hour, then Radius will get on the average of 1 Access-Requests per second.

7. Security Considerations

Security of Radius based VPN discovery depends on the security of Radius that is covered in [1] and [2]. In multi-provider operation, secure tunnels SHOULD be used to carry Radius traffic between providers.

8. Compliance with PPVPN L2 Requirements

This document covers a PE discovery and CE authentication solution for provider based VPNs. Thus only a small subset of the complete PPVPN L2 requirements listed in [3] are applicable to this document.

The solution described in this document fulfills all the requirements of section 6.3 of [3] on "Discovering L2VPN Related Information". In particular:

(1) Radius based discovery allows PEs to dynamically discover information about other PEs of a VPN with minimal or even with no configuration in the PEs.

(2) Unauthorized access to the VPN can be prevented by authentication that is an integral part of Radius.

(3) VPN membership information is only distributed to the PEs that have sites that are members of the VPN.

Other aspects mentioned on section 6.3 of [3], such as propagation of membership changes in a "timely manner" and no manual reconfiguration of the other PEs, are not directly covered in this document. They belong to VPN solution specifications that apply Radius based PE discovery and CE authentication, such as the one described in [4].

The Radius based solution described in this document also complies with all applicable generic requirements listed in [3]. In particular:

(1) The PEs of a VPN can be associated with topology and tunneling protocol information.

(2) VPN sites can be associated with QoS and access control information.

(3) Radius has been widely implemented by existing PEs and has

very good interoperability record.

(4) Multi-provider/multi-AS VPNs are readily supported without any extra complications.

(5) CEs of a VPN require either no configuration or minimal configuration (user name/password).

(6) There is no practical limit on the number of VPNs and, with hierarchical implementation, each VPN can have a very large number of PEs and CEs.

(7) Radius based provisioning systems are readily available and are easily adaptable to PE discovery.

In summary, Radius provides a good directory based alternative to PPVPN PE discovery and a natural means to authenticate VPN CEs.

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.

[3] W. Augustun, Y. Serbest, "Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks". draft-augustyn-ppvpn-l2vpn-requirements-02.txt, February 2003.

[4] J. Heinanen, "Radius/L2TP Based VPLS". draft-heinanen-radius-l2tp-vpls-00.txt, February 2003.

Author's Address

Juha Heinanen
TutPro Inc.
Utsjoki, Finland
Email: jh@tutpro.com

Full Copyright