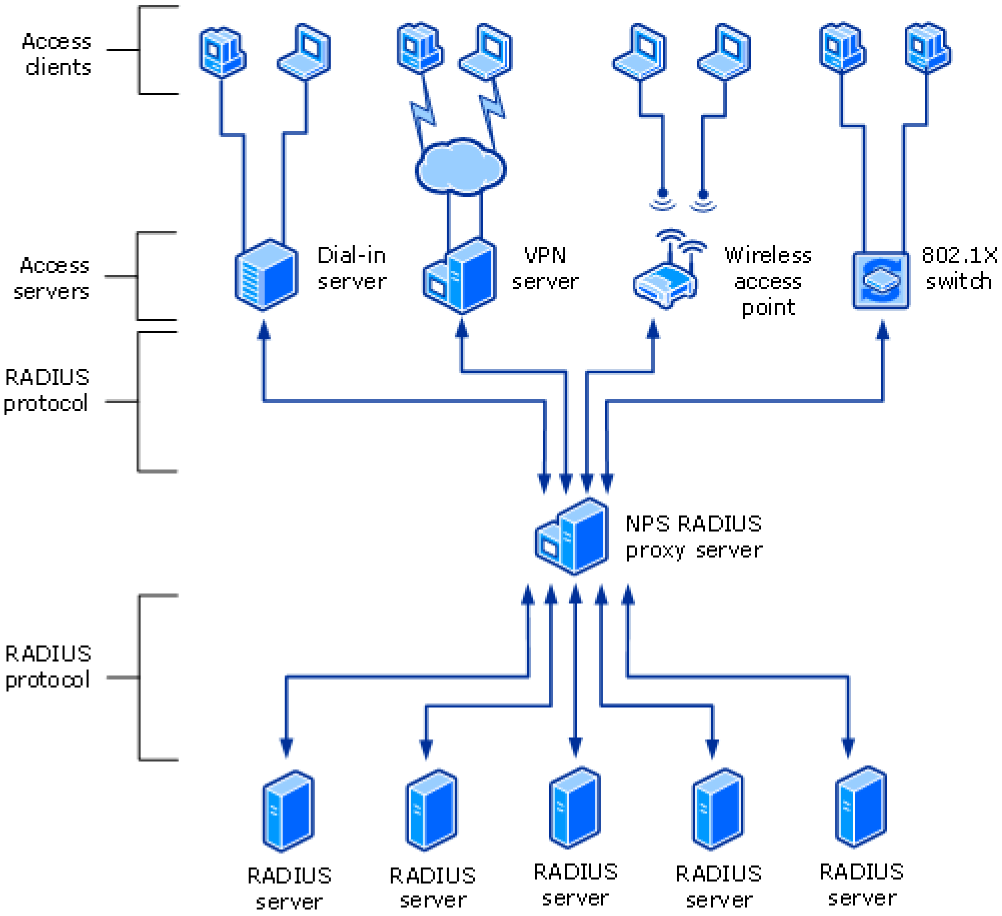
RADIUS Proxy

Updated: March 29, 2012

Applies To: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2

Network Policy Server (NPS) can be used as a RADIUS proxy to provide the routing of RADIUS messages between RADIUS clients access servers and RADIUS servers that perform user authentication, authorization, and accounting for the connection attempt. When used as a RADIUS proxy, NPS is a central switching or routing point through which RADIUS access and accounting messages flow. NPS records information in an accounting log about the messages that are forwarded.

The following illustration shows NPS as a RADIUS proxy between RADIUS clients (access servers) and either RADIUS servers or another RADIUS proxy.



When NPS is used as a RADIUS proxy between a RADIUS client and a RADIUS server, RADIUS messages for network access connection attempts are forwarded in the following way:

1. Access servers, such as dial-up network access servers, virtual private network (VPN) servers, and wireless access points, receive connection requests from access clients.

2. The access server, configured to use RADIUS as the authentication, authorization, and accounting protocol, creates an Access-Request message and sends it to the NPS server that is being used as the NPS RADIUS proxy.

3. The NPS RADIUS proxy receives the Access-Request message and, based on the locally configured connection request policies, determines where to forward the Access-Request message.

4. The NPS RADIUS proxy forwards the Access-Request message to the appropriate RADIUS server.

5. The RADIUS server evaluates the Access-Request message.

6. If required, the RADIUS server sends an Access-Challenge message to the NPS RADIUS proxy, where it is forwarded to the access server. The access server processes the challenge with the access client and sends an updated Access-Request to the NPS RADIUS proxy, where it is forwarded to the RADIUS server.

7. The RADIUS server authenticates and authorizes the connection attempt.

8. If the connection attempt is both authenticated and authorized, the RADIUS server sends an Access-Accept message to the NPS RADIUS proxy, where it is forwarded to the access server.

   If the connection attempt is either not authenticated or not authorized, the RADIUS server sends an Access-Reject message to the NPS RADIUS proxy, where it is forwarded to the access server.

9. The access server completes the connection process with the access client and sends an Accounting-Request message to the NPS RADIUS proxy. The NPS RADIUS proxy logs the accounting data and forwards the message to the RADIUS server.

10. The RADIUS server sends an Accounting-Response to the NPS RADIUS proxy, where it is forwarded to the access server.

You can use NPS as a RADIUS proxy when:

- You are a service provider who offers outsourced dial-up, VPN, or wireless network access services to multiple customers. Your NASs send connection requests to the NPS RADIUS proxy. Based on the realm portion of the user name in the connection request, the NPS RADIUS proxy forwards the connection request to a RADIUS server that is maintained by the customer and can authenticate and authorize the connection attempt.

- You want to provide authentication and authorization for user accounts that are not members of either the domain in which the NPS server is a member or another domain that has a two-way trust with the domain in which the NPS server is a member. This includes accounts in untrusted domains, one-way trusted domains, and other forests. Instead of configuring your access servers to send their connection requests to an NPS RADIUS server, you can configure them to send their connection requests to an NPS RADIUS proxy. The NPS RADIUS proxy uses the realm name portion of the user name and forwards the request to an NPS server in the correct domain or forest. Connection attempts for user accounts in one domain or forest can be authenticated for NASs in another domain or forest.

- You want to perform authentication and authorization by using a database that is not a Windows account database. In this case, connection requests that match a specified realm name are forwarded to a RADIUS server, which has access to a different database of user accounts and authorization data. Examples of other user databases include Novell Directory Services (NDS) and Structured Query Language (SQL) databases.

- You want to process a large number of connection requests. In this case, instead of configuring your RADIUS clients to attempt to balance their connection and accounting requests across multiple RADIUS servers, you can configure them to send their connection and accounting requests to an NPS RADIUS proxy. The NPS RADIUS proxy dynamically balances the load of connection and accounting requests across multiple RADIUS servers and increases the processing of large numbers of RADIUS clients and authentications per second.

- You want to provide RADIUS authentication and authorization for outsourced service providers and minimize intranet firewall configuration. An intranet firewall is between your perimeter network (the network between your intranet and the Internet) and intranet. By placing an NPS server on your perimeter network, the firewall between your perimeter network and intranet must allow traffic to flow between the NPS server and multiple domain controllers. By replacing the NPS server with an NPS proxy, the firewall must allow only RADIUS traffic to flow between the NPS proxy and one or multiple NPS servers within your intranet.