Using the Barracuda DC Agent With Microsoft Network Policy Server

https://campus.barracuda.com/doc/28966983/

Microsoft Network Policy Server (NPS) performs centralized authentication, authorization, and accounting for wireless, authenticating switch, remote access dial-up and virtual private network (VPN) connections. With the Barracuda DC Agent, you can also log the IP addresses and AD identities of wireless users in the organization by monitoring the NPS logs if the following requirements are met:

- The Barracuda DC Agent is installed locally on the NPS server.
- The wireless access points (WAPs) in the environment are configured to use RADIUS authentication against the NPS server on which the DC Agent is installed.
- The WAPs must be configured to send RADIUS *accounting* information, i.e. not merely RADIUS authentication information. The reason is that the framed IP address attribute of the RADIUS session contains the user's IP address, and that information is only contained in the accounting information.
  The NPS log must be in the default location (C:\Windows\system32\LogFiles) and in the default format ("ODBC (Legacy)"), with the log file rotation set to **Monthly**, or the Barracuda DC Agent will not be able to monitor the log. To change the logging properties, see **How to access configuration of the NPS log file properties** below.

Note that normal operation of the DC Agent allows for installation either locally or remotely, and this configuration requires local installation on the NPS server. The NPS server does not need to be a domain controller (DC). If you also want to pick up logins from workstations and other sources, you will need to either install the DC Agent on a DC or add a remote Active Directory (AD) connection to the instance of the DC Agent running on the NPS server.

Configure your Barracuda Networks appliances (e.g.Barracuda Web Security Agent, Barracuda CloudGen Firewall, etc.) as you normally would so that the device can collect the logins harvested from the NSP log by the DC Agent.

This feature is automatically enabled in the DC Agent – if it finds NPS logs, it automatically monitors them. Log entries for NPS-related events are prefixed with "NPS: ", and increasing the log verbosity (Debug Log Level) will log additional NPS-related information for troubleshooting purposes. The only necessary configuration to perform in the DC Agent interface is to configure the properties of the NPS log file in which you want to store the accounting data.

How to access configuration of the NPS log file properties

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. In the console tree, click **Accounting**.
3. In the details pane, in **Log File Properties**, click **Change Log File Properties**. The **Log File**

Properties dialog box opens. Barracuda Networks recommends using the default settings. See http://technet.microsoft.com/en-us/library/ee663944(v=ws.10).aspx for more information.

Due to limitations in the RADIUS protocol, the DC Agent does not track when a user "logs out" of the wireless environment, so the IP address associated with that wireless user will remain associated with them until it is re-used by a new AD user or until the appliance times out the session. This timeout interval is configurable on the appliance.

Note also that there may be a delay in between when a user authenticates to RADIUS and when a user's identity is available to their appliance(s) since many devices have a RADIUS accounting interval.