

Barracuda NG Firewall Configuration

Contents

Barracuda NG Firewall Configuration	0
Barracuda NG VPN configuration for SMS PASSCODE®.....	1
Authentication	1
Configuration in SMS PASSCODE®.....	3



Barracuda NG VPN configuration for SMS PASSCODE®

This guide outlines the process of configuring a Barracuda NG for Authentication with SMS PASSCODE®. In order to protect the Barracuda NG the Firmware must be at least version 5.2.3. (SSLVPN has been supported since version 5.2.2).

Authentication

Log on to the Barracuda NG administration console, go to authentication service and create a RADIUS Server.

The Radius Server Address must be set to the IP-address of the NPS server as the SMS PASSCODE radius authentication client. Ensure that the Radius Server Key match the Shared secret on the NPS server's radius client.

RADIUS Authentication Settings

Activate Scheme	Yes
Method	RADIUS
Radius Server Address	10.10.10.10
Radius Server Port	1812
Radius Server Key	Current
Group Attribute	Login-LAT-Group
Group Attribute Delimiter	:
Group Attribute Usage	All
User Info Helper Scheme	
NAS-ID	
NAS IP Address	
NAS IP Port	
Number of Processes	5

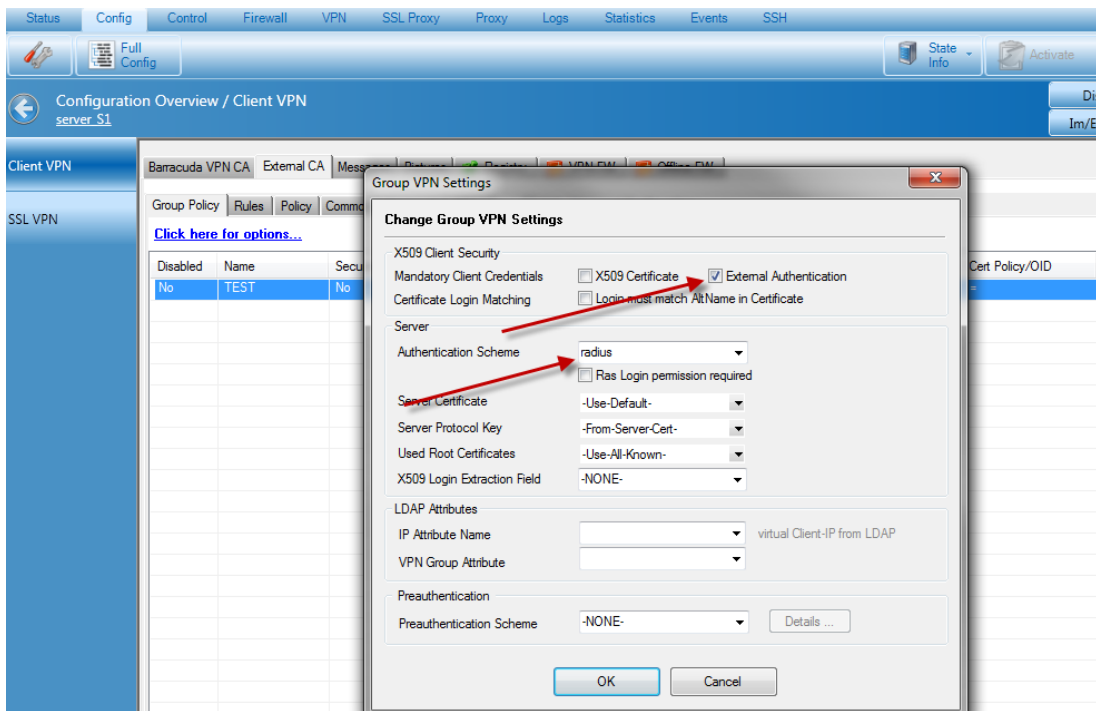
Activate Scheme

- Enable Radius as external directory service.
- Radius Server Address**
IP address of the Radius server
- Radius Server Key**
Note: Do not use backslashes!
- Group Attribute**
Radius attribute used as user group
- Group Attribute Delimiter**
Delimiter used to separate groups
- Group Attribute Usage**
Define the used group information.
All: Complete string.
First: Only the first group.
Last: Only the last group.
- User Info Helper Scheme**
Additional authentication scheme to determine additional group information.
- NAS-ID**
NAS identifier.
- NAS IP Address**
Some radius servers require NAS credentials to be set.
Define here the used IP address.
- NAS IP Port**
Some radius servers require NAS credentials to be set.
Define here the used port number.
- Number of Processes**
Number of authentication processes for handling requests.
Increase if slow authentication servers are present.

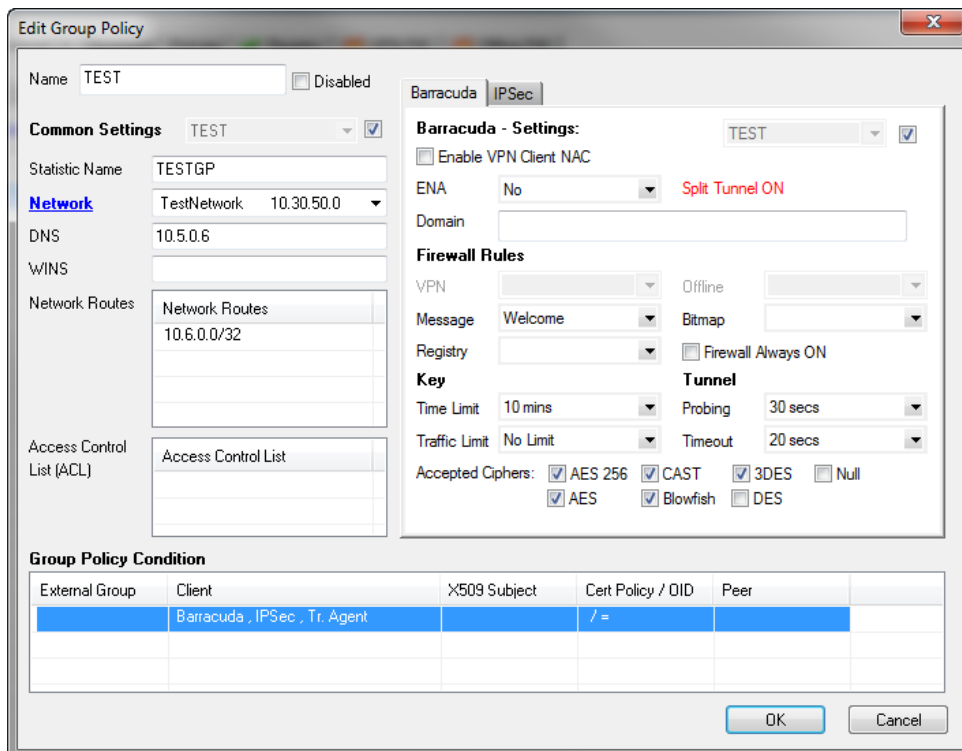
This scheme is referred to as radius/RADIUS in this and other config parts.



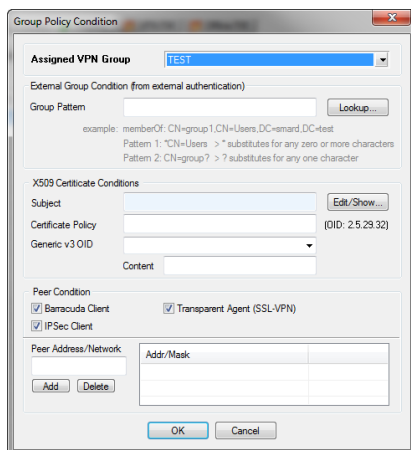
In Client VPN Go to External CA and press "Click here for options..." and make sure to check External Authentication and set the Authentication Scheme to radius



Create a Group Policy with corresponding Group Policy Condition to allow access from the client.



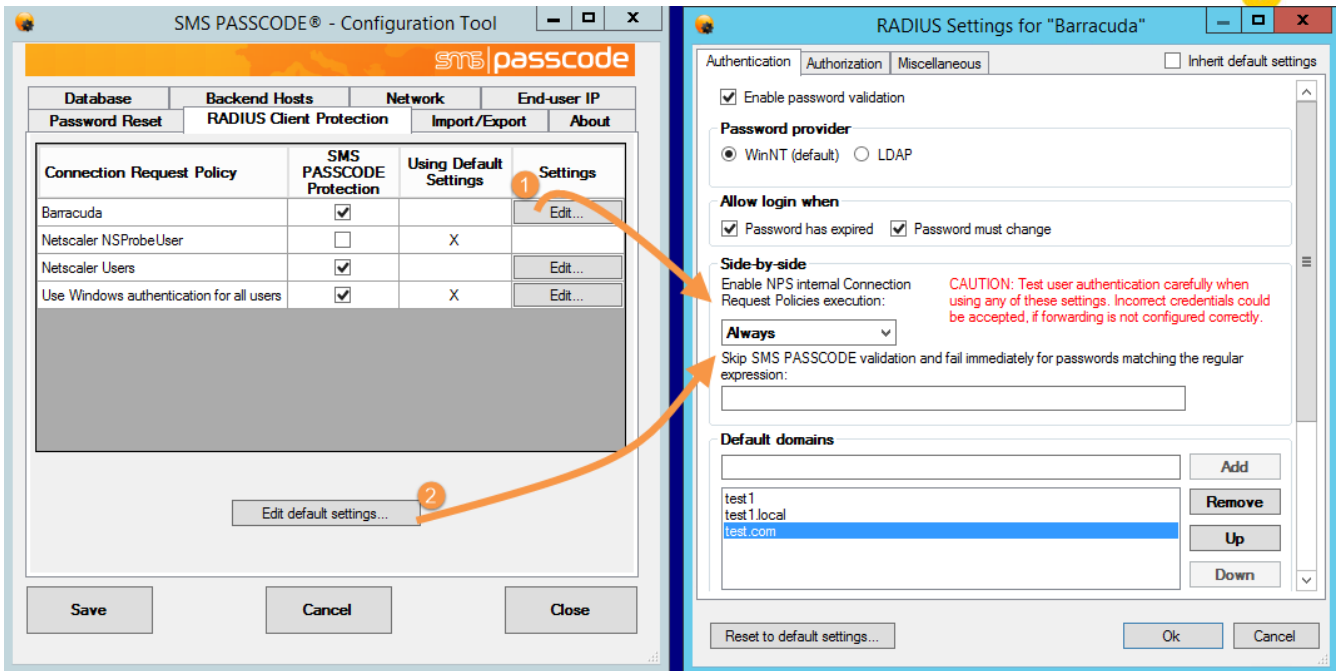
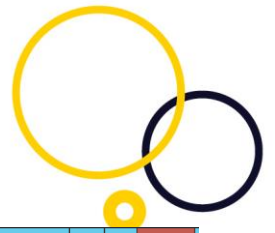
It is possible to limit to Group Pattern (Groups send in the Login-LAT-Group attribute)



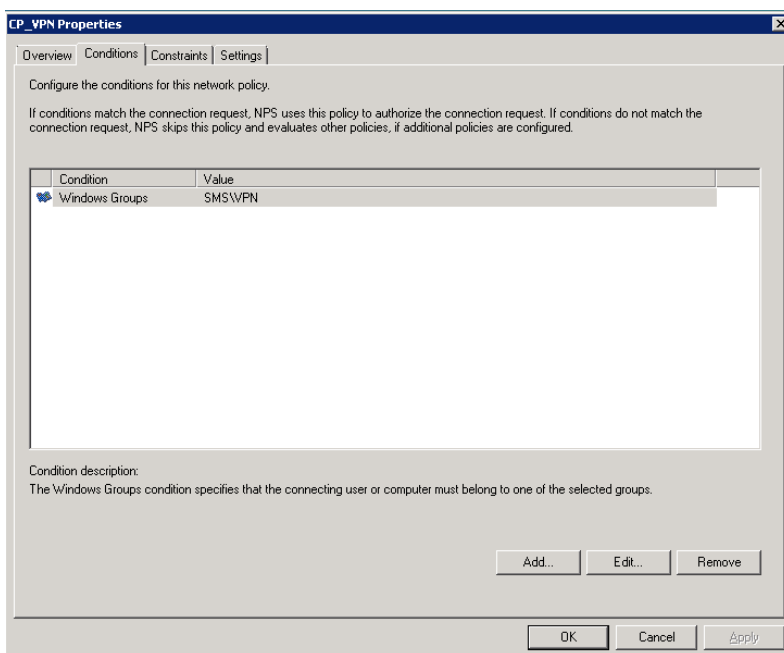
Configuration in SMS PASSCODE®

First, consult the SMS PASSCODE® Administrator Guide for configuration of the SMS PASSCODE Radius Client Protection.

Install the SMS PASSCODE radius protection and set side by side to Always in the SMS PASSCODE® configuration tool as illustrated below. You can configure this in the individual Connection Request Policy settings (1) or in the default settings (2).

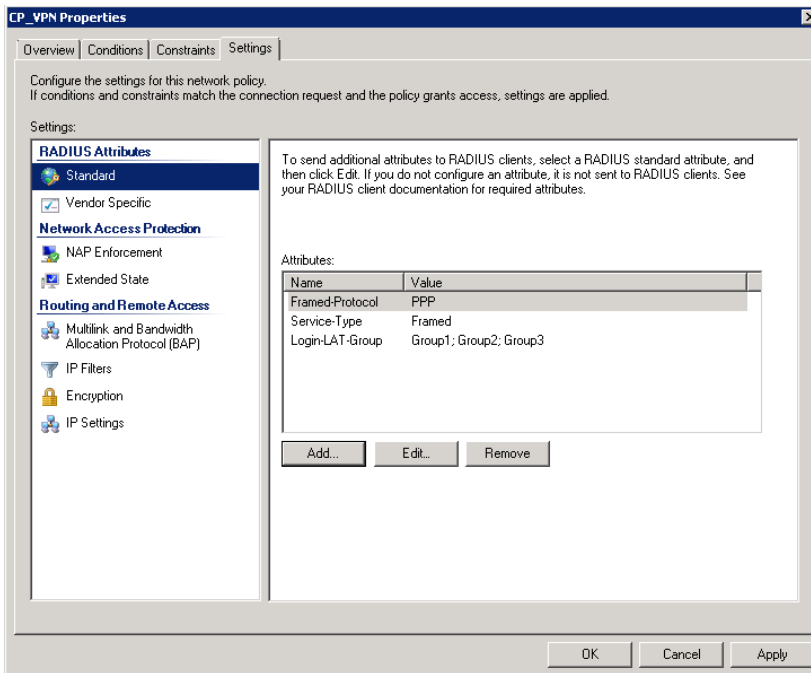


Open the Microsoft Windows Network Policy Server (NPS) and proceed to create a network policy. Once done, open the policy and choose the Windows group(s) that contains the users. Note the user must be a member of the group. For more details, please consult the SMS PASSCODE® Administrator Guide.





The Login-LAT-Group attribute can be used to send group name(s) to the Radius client.



This completes the setup of the integration.