



WatchGuard SSL VPN configuration

Contents

WatchGuard SSL VPN configuration.....	0
WatchGuard SSL VPN Configuration for SMS PASSCODE®	1
WatchGuard Configuration.....	1
NPS Configuration	3
Registry setting	5
Configuration in SMS PASSCODE®.....	5



WatchGuard SSL VPN Configuration for SMS PASSCODE®

This guide outlines the process of configuring a WatchGuard XTM Firewall for SSL VPN RADIUS Authentication with CensorNet MFA.

WatchGuard Configuration

From the XTM Web interface, navigate to 'Authentication' → 'Servers' → 'RADIUS'

Server	Status	
Firebox	0 Users	0 Groups
RADIUS	Primary	192.168.200.10
	Secondary	Disabled
SecurID	Primary	Disabled
	Secondary	Disabled
LDAP	Primary	Disabled

Enter the details of your SMS PASSCODE RADIUS server and click 'Save'. The 'Passphrase' is the Shared Secret key that must also be entered on the NPS.



WatchGuard Fireware XTM Web UI | User: admin | Help | Logout

Servers / RADIUS

Before you configure your XTM device to use a RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication requests.

Primary Server Settings

- Enable RADIUS Server

IP Address: 192.168.200.10

Port: 1812

Passphrase:

Confirm:

Timeout: 10 seconds

Retries: 1

Group Attribute: 11

Dead Time: 10 Minutes

Navigate to 'VPN' → 'Mobile VPN with SSL' → 'Authentication'
Enable Mobile SSL VPN and set RADIUS as the default Authentication Server and click 'Save'.

WatchGuard Fireware XTM Web UI | User: admin | Help | Logout

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

- Activate Mobile VPN with SSL

General | **Authentication** | Advanced

Authentication Server Settings

Select one or more authentication servers. The first server in the list is the default authentication server.

Select	Authentication Server
<input checked="" type="checkbox"/>	RADIUS (Default)
<input type="checkbox"/>	Firebox-DB

Default

- Auto reconnect after a connection is lost
- Force users to authenticate after a connection is lost
- Allow the Mobile VPN with SSL client to remember password

Define users and groups to authenticate with Mobile VPN with SSL. The users and groups you define are automatically included in the "SSLVPN-Users" group.

	Name	Type	Authentication Server
<input type="checkbox"/>	SSLVPN-Users	Group	Any

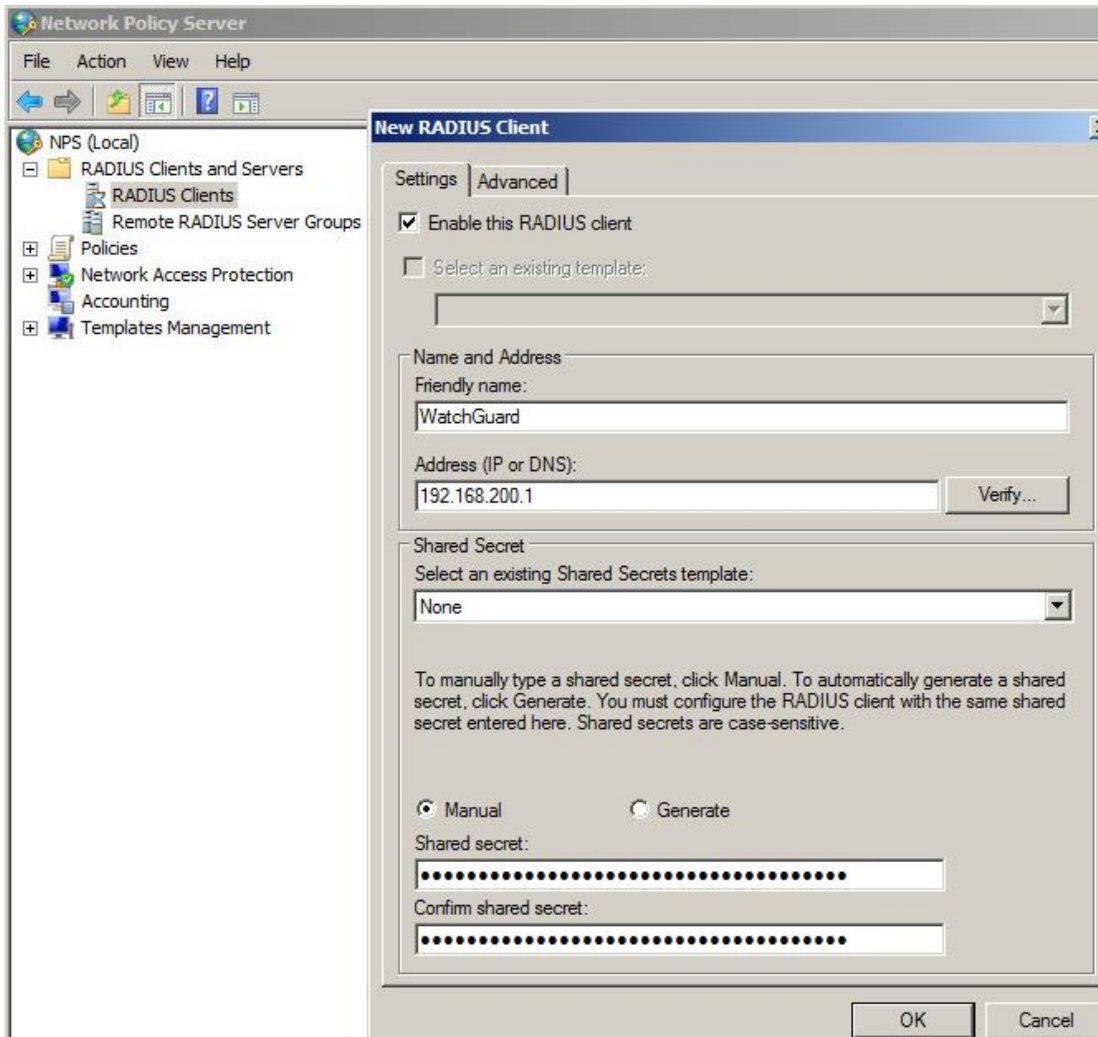
Add Remove

Save



NPS Configuration

On the NPS server with the SMS PASSCODE Radius client protection, open the Network Policy Server management console. Navigate to 'RADIUS Clients' and create a new client.





Navigate to 'Policies' → 'Connection Request Policies' and modify or create a new policy matching incoming RADIUS requests. Ensure that the RADIUS Attribute 11 – Filter-Id is set to 'SSLVPN-Users'. Make sure you have a condition, in example a day and time restriction.

Overview | Conditions | Settings

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Required Authentication Methods

- Authentication Methods

Forwarding Connection Request

- Authentication
- Accounting

Specify a Realm Name

- Attribute

RADIUS Attributes

- Standard
- Vendor Specific

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Filter-Id	SSLVPN-Users

Add... Edit... Remove

OK Cancel Apply

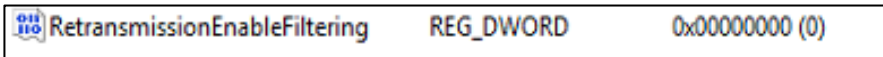
Note: For detailed instructions on how to configure the NPS, consult the SMS PASSCODE Administrator's Guide.

Make sure that you have a matching Network policy.



Registry setting

Open Registry Editor and navigate to HKLM\Software\SMS PASSCODE\RADIUS\[Connection Request Policy]\RetransmissionEnableFiltering
The DWORD must have a value of "0"



Please note that you might have more than one Connection request policy. The registry key name reflects the name of the Connection Request Policy in the NPS manager.

For SMS PASSCODE 7.2 and earlier versions of SMS PASSCODE:
HKLM\Software\SMS PASSCODE\RADIUS\RetransmissionEnableFiltering
Create a new DWORD, name it 'RetransmissionEnableFiltering' and give it a value of "0"

Configuration in SMS PASSCODE®

Open the SMS PASSCODE Configuration Tool and navigate to the 'RADIUS Client Protection' tab.

Set side by side to 'Always' and click 'Ok'. In the main "Radius Client Protection" pane click 'Save'. The NPS service will restart after this configuration.

