

# NPS FortiGate Captive Portal

**Autoren:** Morris Tichy, Lukas Freudensprung

## Inhaltsverzeichnis

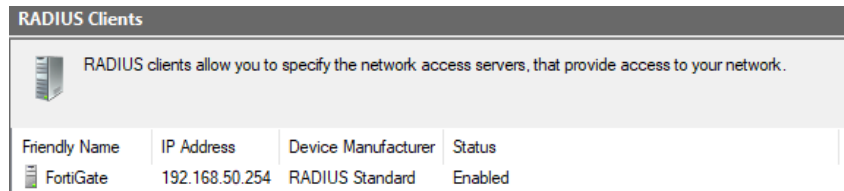
1. NPS FortiGate Captive Portal .....	2
1.1. NPS Konfiguration .....	2
1.1.1. Connection Request Policies .....	2
1.1.2. Network Policies .....	3
1.1.3. Vendor Specific Attributes .....	4
1.2. FortiGate Konfiguration .....	5
2. Test .....	6

## 1. NPS FortiGate Captive Portal

Mithilfe des NPS Dienstes unter Windows sollen sich die AD-User auf einer FortiGate oder um ins Internet zu gelangen authentifizieren. Diese Datei beschreibt die Konfiguration des NPS Dienstes und der FortiGate.

### 1.1. NPS Konfiguration

Nachdem der NPS Server grundkonfiguriert wurde und der Network Policy Server installiert ist, wird zuerst ein neuer Radius-Client erstellt. **NPS > Radius Client und Server > Radius Clients > Neu.** Hier wird die IP-Adresse der FortiGate und ein gemeinsames Passwort eingetragen.



Friendly Name	IP Address	Device Manufacturer	Status
FortiGate	192.168.50.254	RADIUS Standard	Enabled

Abbildung 1: Radius Client Konfiguration

1. Hinzufügen der FortiGate zu den ‚RADIUS Clients‘ in der MS NPS-Konfiguration (wählen Sie ‚RADIUS Clients‘ und wählen Sie ‚Neu‘).
2. Geben Sie die Details des FortiGate RADIUS-Clients ein:
  - Versichern Sie sich, dass das Kästchen ‚Enable this RADIUS client‘ aktiviert ist.
  - Geben Sie den ‚Friendly name‘, die IP-Adresse und das Passwort ein (das gleiche Passwort, das auf der FortiGate konfiguriert wurde).
  - Der Rest kann auf den Standardwerten belassen werden.

#### 1.1.1. Connection Request Policies

1. Erstellen Sie eine ‚Connection Request Policy‘ für die FortiGate (wählen Sie ‚Connection Request Policies‘ und wählen Sie ‚Neu‘).
2. Geben Sie den ‚Policy name‘ an und wählen Sie ‚Weiter‘.
3. Unter ‚Specify Conditions‘ wählen Sie ‚Add...‘ und wählen Sie ‚Client IPv4 Address‘ und geben Sie die IP-Adresse der FortiGate an.

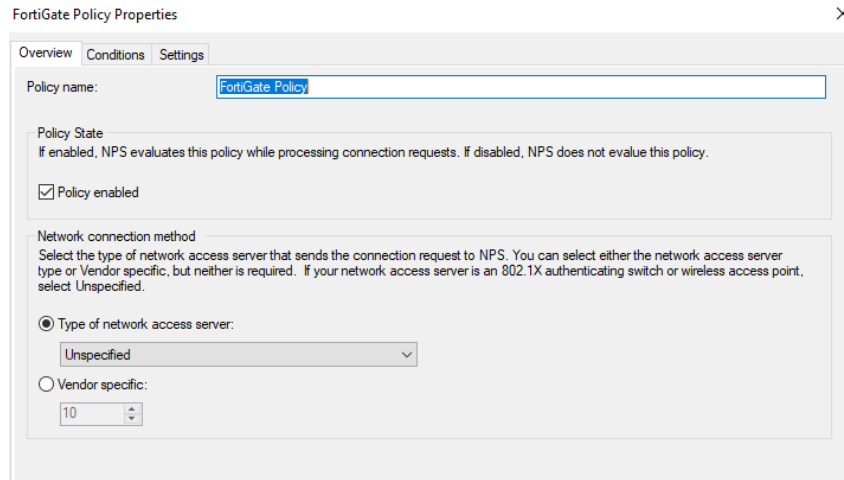


Abbildung 2: Connection Request Policy

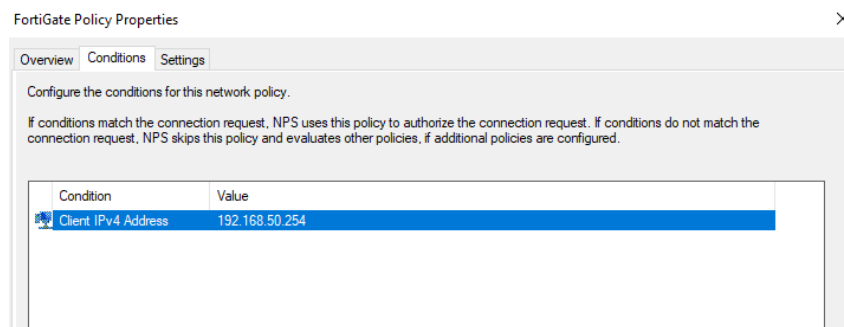


Abbildung 3: Connection Request Policy

### 1.1.2. Network Policies

1. Erstelle eine ‚Network Policy‘ für Zugriffsanfragen, die von der FortiGate kommen (wählen Sie ‚Network Policies‘ und wählen Sie ‚Neu‘). NPS -> Policies -> Network Policies.
2. Geben Sie den ‚Policy name‘ an und wählen Sie ‚Weiter‘.

Adding Network Policy with AD authentication.

Hinzufügen einer Netzwerkrichtlinie mit AD-Authentifizierung.

1. Unter ‚Specify Conditions‘ wählen Sie ‚Add...‘ und wählen Sie ‚Windows Groups‘ wählen Sie ‚Add Groups...‘ und geben Sie den AD-Gruppennamen ein.

Wenn Sie fertig sind, bestätigen Sie die Einstellungen mit ‚OK‘ und ‚Hinzufügen...‘.

- Geben Sie die Zugriffsberechtigung an und wählen Sie ‚Weiter‘

- Der Rest kann auf den Standardwerten belassen werden.

**Network Policies**

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
FortiGate Policy	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

**FortiGate Policy**

Conditions - If the following conditions are met:

Condition	Value
Windows Groups	AvangerHQ\Domain Users

Settings - Then the following settings are applied:

Setting	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False

Abbildung 4: Funktionsbereite Network Policy

### 1.1.3. Vendor Specific Attributes

**Configure Settings**

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

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

**Settings:**

- RADIUS Attributes**
  - Standard
  - Vendor Specific**
- Routing and Remote Access**
  - Multilink and Bandwidth Allocation Protocol (BAP)
  - IP Filters
  - Encryption
  - IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific 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.

Name	Vendor	Value
------	--------	-------

Buttons: Add, Edit, Remove

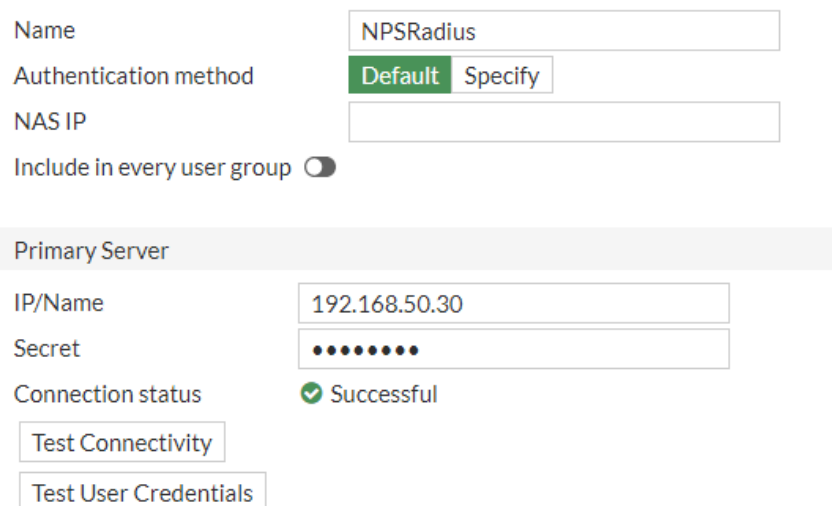
Navigation: Previous, Next, Finish, Cancel

Abbildung 5: Vendor Specific Attributes

1. Drücken Sie auf ‚Add...‘ und wählen Sie ‚Vendor-Specific‘
2. Wählen Sie ‚Add...‘ und geben Sie die Vendor Code ‚12356‘ ein und Yes. It conforms.
3. Drücken Sie nun auf Configure Attribute und geben Sie die Attribute ein. vendor: 12356, attribute: 1, as string: Domain\_User.
4. Überprüfen der Konfiguration und Finish

## 1.2. FortiGate Konfiguration

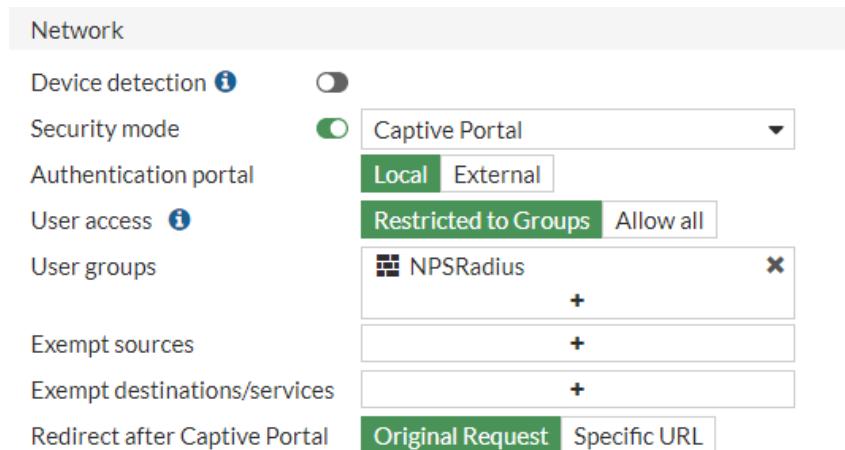
Nachdem der NPS Server konfiguriert wurde, wird die FortiGate konfiguriert. Dazu wird ein neuer Radius-Server erstellt. **User & Device > Radius Servers > Neu.** Hier wird die IP-Adresse des NPS Servers und das gemeinsame Passwort eingetragen. Unter Test Connectivity kann die Verbindung getestet werden und mit Test Credentials kann ein Anmeldevorgang simuliert werden.




The screenshot shows the FortiGate configuration interface for a Radius Server. The 'Name' field is set to 'NPSRadius'. The 'Authentication method' is set to 'Default'. The 'NAS IP' field is empty. The 'Include in every user group' checkbox is checked. Below this, the 'Primary Server' section is expanded, showing the 'IP/Name' field set to '192.168.50.30' and the 'Secret' field filled with dots. The 'Connection status' is 'Successful' with a green checkmark. At the bottom, there are buttons for 'Test Connectivity' and 'Test User Credentials'.

Abbildung 6: Radius Server Konfiguration in der FortiGate

Anschließend wird eine neue User Group erstellt die als Remote Server den NPS Server eingetragen hat. **User & Device > User Groups > Neu.** Hier wird der Name der Gruppe und der NPS Server eingetragen. Daraufhin wird unter dem jeweiligen Port ein neues Captive Portal erstellt.






Network


Device detection  ☐


Security mode ☒ Captive Portal

Authentication portal **Local** External

User access  **Restricted to Groups** Allow all

User groups  NPSRadius   
+

Exempt sources 

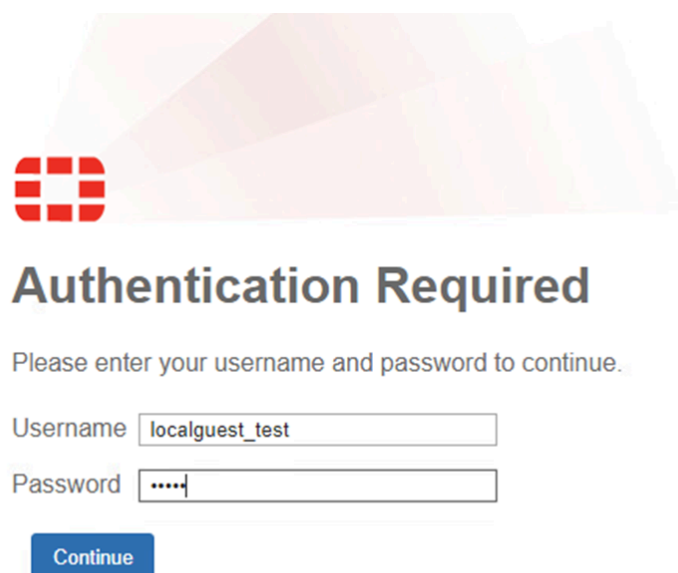
Exempt destinations/services 


Redirect after Captive Portal **Original Request** Specific URL

Abbildung 7: Captive Portal Konfiguration

## 2. Test

Wenn alle Konfigurationsschritte durchgeführt wurden, sollte sich ein AD-User auf der FortiGate oder im Internet authentifizieren können. Folgendes sollte passieren:





## Authentication Required

Please enter your username and password to continue.

Username

Password

**Continue**

Abbildung 8: Login Screen