

IKEv2 Remote Access VPN

IKEv2 Remote Access may be used to access resources on a local network remotely.

Server authentication occurs via a X.509 certificate and user authentication via username and password using a configured RADIUS server.

Server Certificate Requirements

A suitable X.509 server certificate must be provided. This may be the same as the one used for the web interface of the CyberHound Appliance. The server certificate will require the following fields:

- **Extended Key Usage (EKU):**
 - serverAuth, aka "TLS Web server authentication", OID: 1.3.6.1.5.5.7.3.1
 - For maximum interoperability set: ikeIntermediate, aka "IP Security IKE Intermediate", OID: 1.3.6.1.5.5.8.2.2
- **Subject:**
 - Set the common name to the server name, e.g. CN = gateway.mydomain.com
- **Subject Alternative Name** extension:
 - Set the subject alternative name (subjectAltName) to the server name. This will be the name required in the client-side configuration when specifying the remote server.

Note:

- Wild card certificates do not work. The server name needs to be unambiguous and must be specified in the Subject Alternative Name in the certificate.
- The certificate that was used to issue the server certificate will need to be trusted by the clients wanting to connect to the VPN.

Split Tunneling

During the connection handshake, the IKEv2 Remote Access service negotiates with the client to select what traffic will be sent over the VPN connection. This can be configured on the server end using the "Advertised Networks" field.

The most common configurations will either be for everything (i.e. connections to both LAN and internet) to be sent over the VPN connection, or just traffic to IP addresses on the LAN side of the CyberHound Appliance.

This latter configuration is sometimes called "split tunneling" because the client's traffic is split, only traffic to the LAN will go over the VPN, other connections will go directly via their normal internet connection.

CyberHound Appliance Configuration

Go to *Configuration > Remote Access (IKEv2)*:

- Check the **Enabled?** check box.
- Follow the **Edit...** link in the **Server Certificate** field:
 - Upload a suitable certificate (see above) if required.
 - Select the certificate in the **Certificate to use for IKEv2 remote access server** field.
 - If required, select any intermediate certificates used to sign the server certificate.
- IKEv2 Remote Access requires a RADIUS authentication plugin. Neither local user accounts nor accounts connected via an Active Directory plugin are supported for IKEv2 Remote Access. If this is not set up yet, follow the **Edit...** link in the **Authentication Plugin** field. Typically, the RADIUS plugin should connect to NPS running on a Windows Server. On the CyberHound Appliance, the RADIUS plugin should be configured with the IP address of the NPS server and the shared secret. If an Active Directory plugin is used as well, the RADIUS plugin should be placed below the Active Directory plugin in the plugins list.
- Enter a private subnet range (which must not be used by any of your LAN networks) for the VPN. To ensure the subnet is large enough for your number of clients, consult the following table:

Prefix length	Max number of clients
/24	254
/23	510
/22	1022
/21	2046
/20	4094

- Enter the DNS servers that clients will use. This should typically be one of the LAN IP addresses of the CyberHound Appliance.
- Configure what networks will be advertised to the client.

RADIUS Authentication Plugin

The CyberHound Appliance RADIUS plugin provides authentication services against an external RADIUS server.

This is needed primarily for VPN logins. The RADIUS plugin may be used alongside other plugins to provide VPN support; to do this please ensure the RADIUS plugin is below the other plugin in the list.

Settings	Notes
Enabled	Specifies if the plugin should be active. This setting is useful for temporarily disabling a plugin without deleting it and losing configuration settings.
Comment	Description for the plugin instance. This is optional but useful when reviewing configuration later. The description is shown in the CyberHound Appliance authentication logs to assist when troubleshooting.
RADIUS authentication host	External RADIUS server to make authentication requests to.
Shared secret	Password to use when communicating with RADIUS server. The password for the above username. This must be updated if the account password is changed on the RADIUS server.

Fallback group	CyberHound Appliance group to use for RADIUS users if a group cannot be determined.
Communication timeout	Seconds to wait before giving up on a RADIUS request.
Maximum number of retries	Number of times to retry a RADIUS request if errors occur.

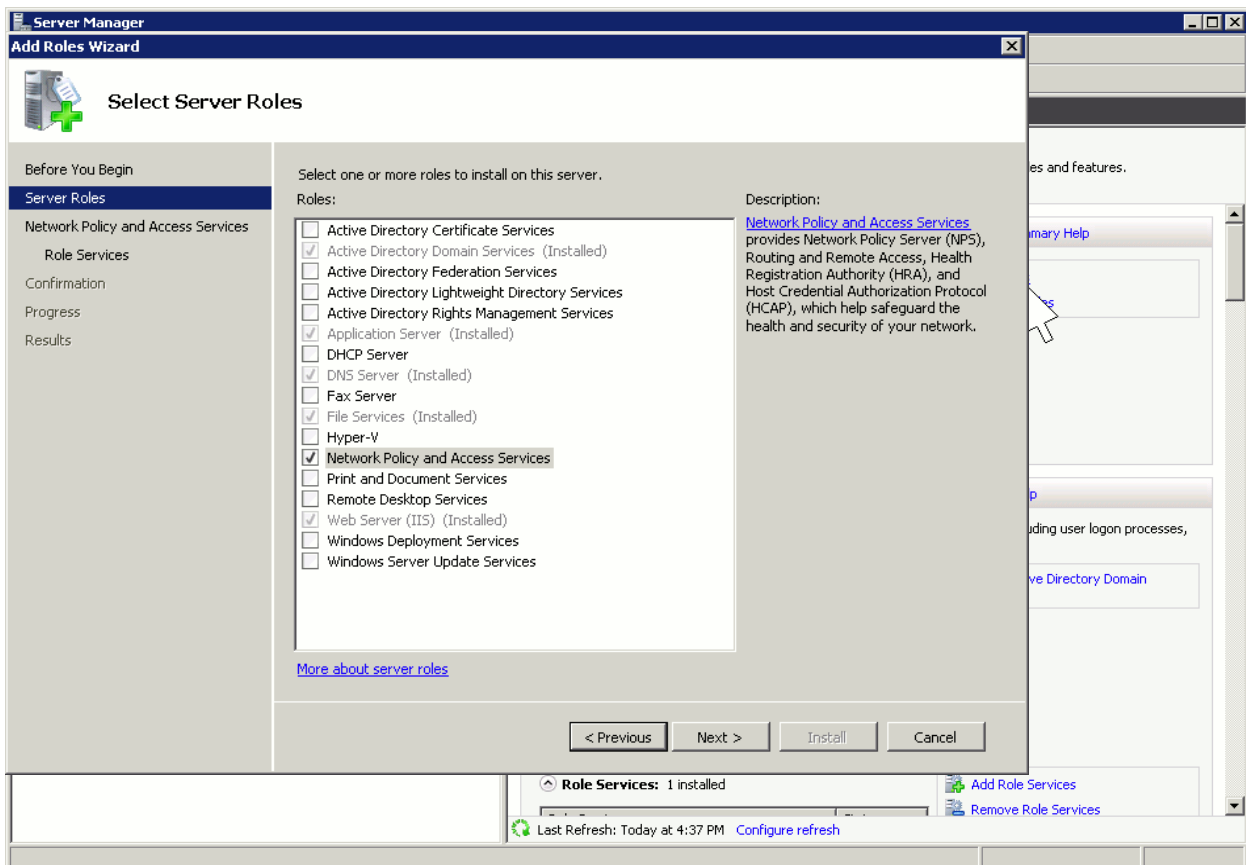
Setting up a RADIUS Server on a Windows 2009 Server

This section outlines a sample configuration of a Microsoft Windows Server to act as a RADIUS server for the CyberHound Appliance. You will need to login to the Windows server as an Administrator.

Installing NPS

The RADIUS server in Windows 2008 Server is provided as part of the Network Policy Service (NPS). To install NPS, follow these steps:

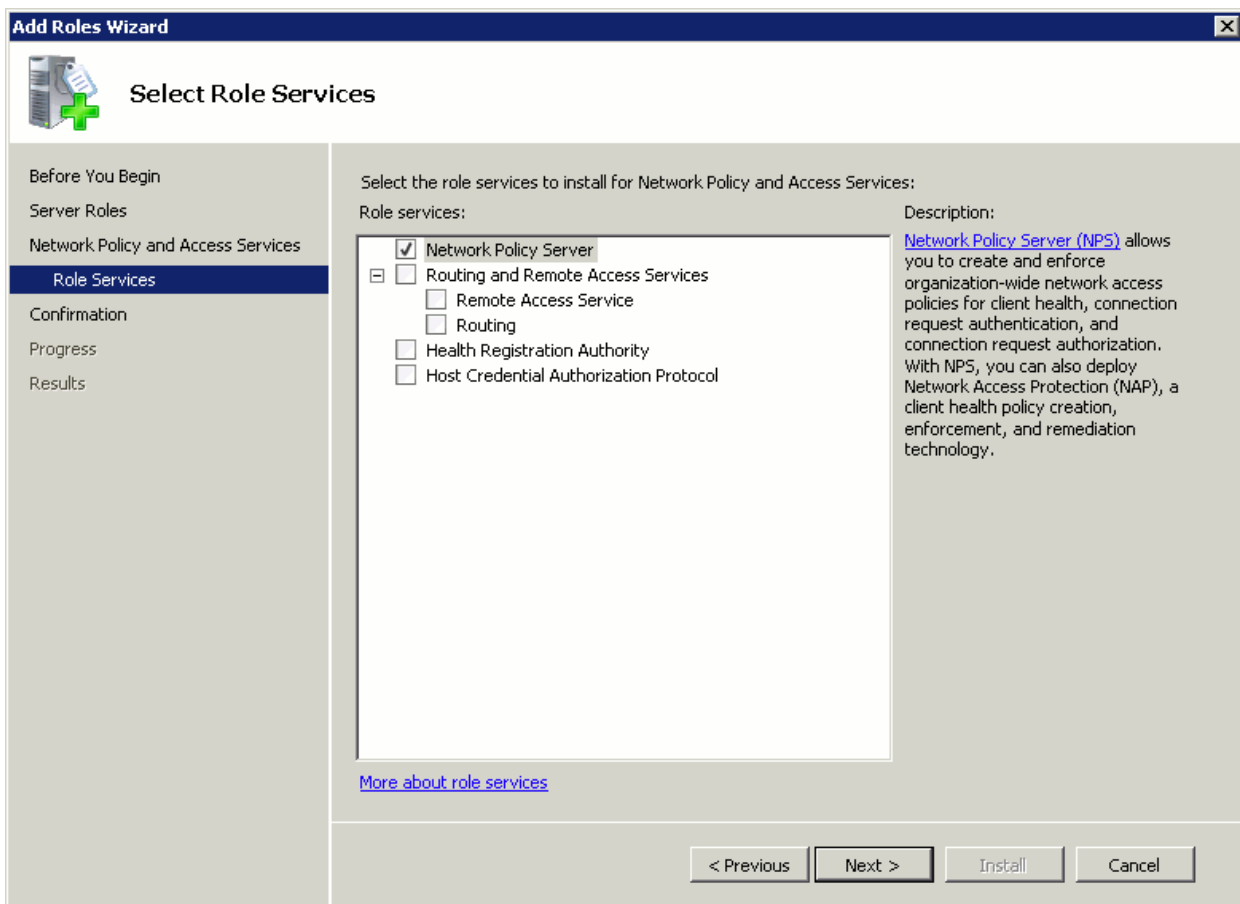
- Open the Control Panel
- Click Turn Windows features on or off
- Click Add Roles:

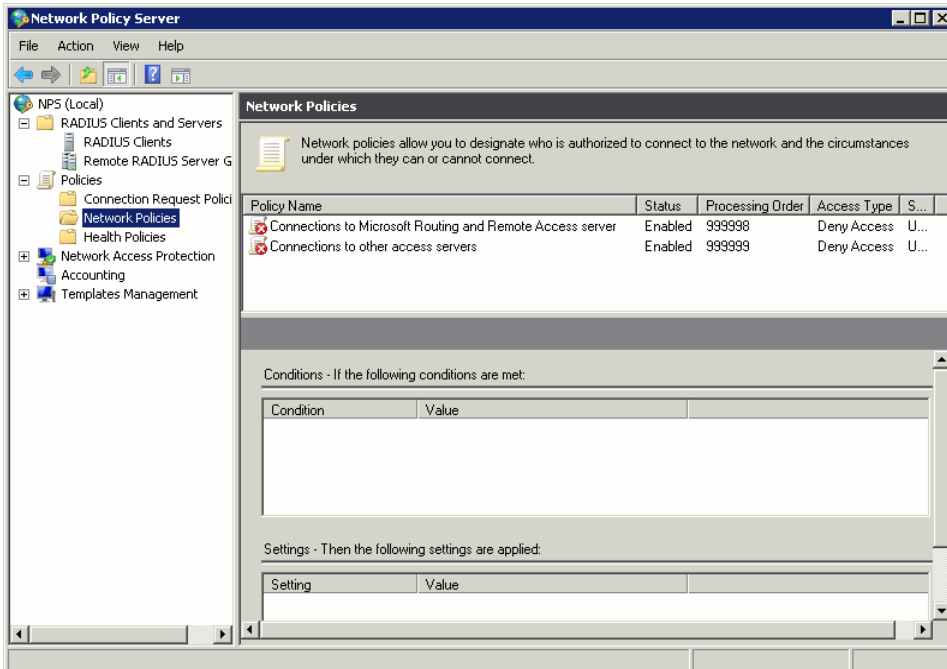


- Choose Network Policy and Access Service
- Select Network Policy Server

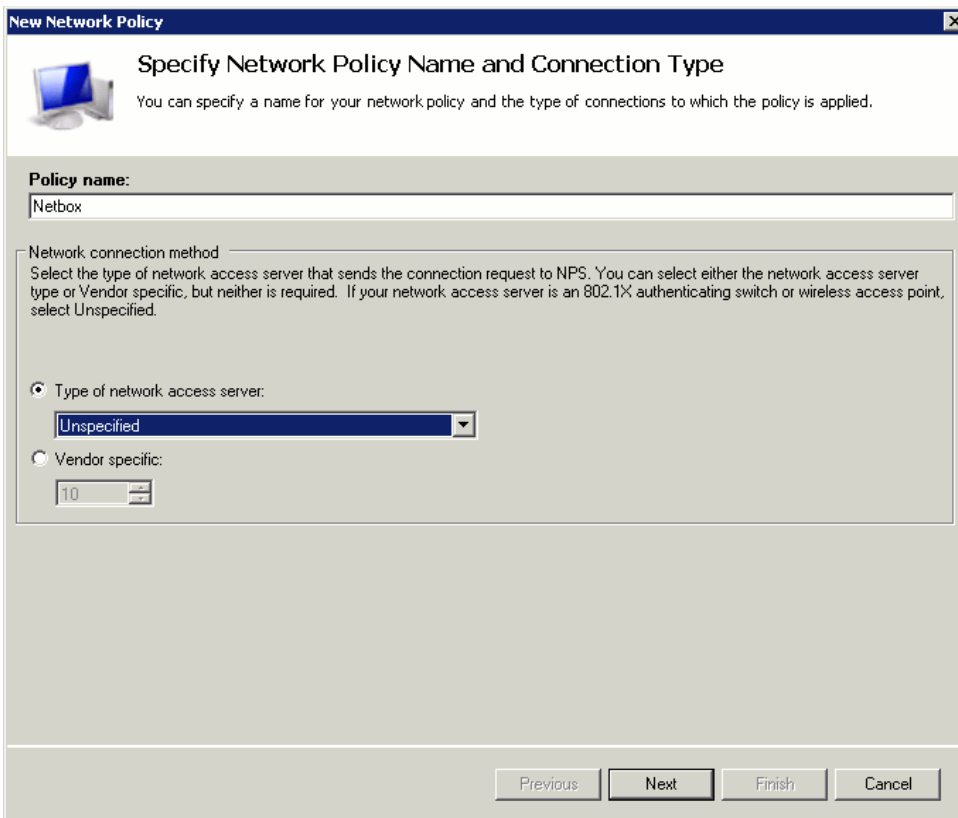
Configuring Network Policies

- Open Network Policy Server by going to Start > Administrative Tools > Network Policy Server.

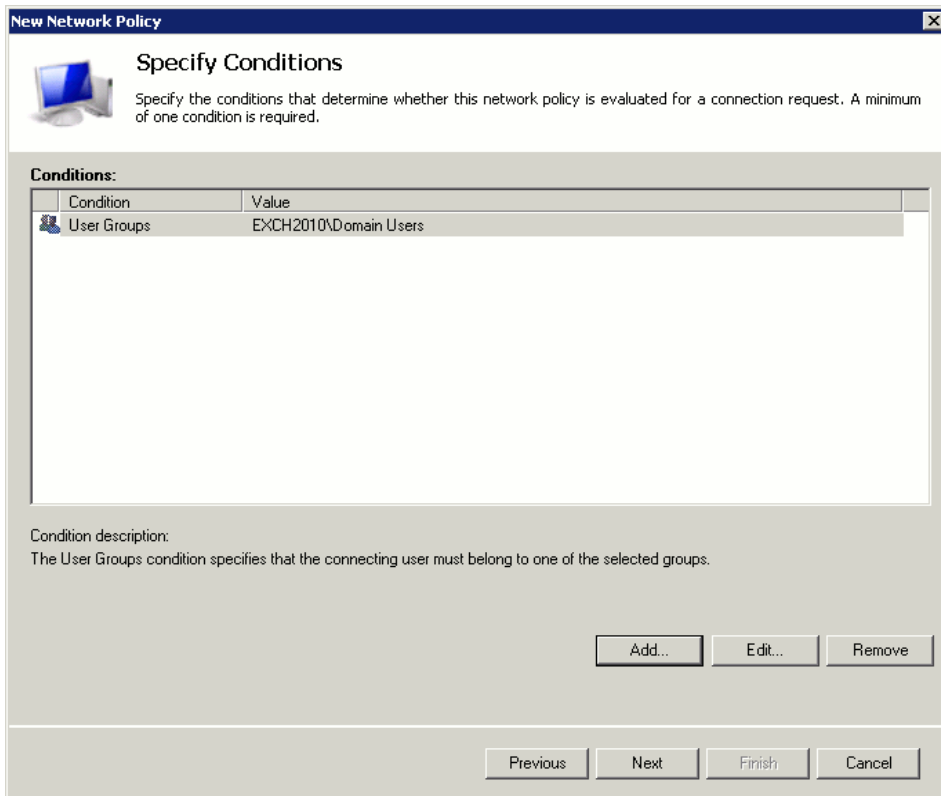
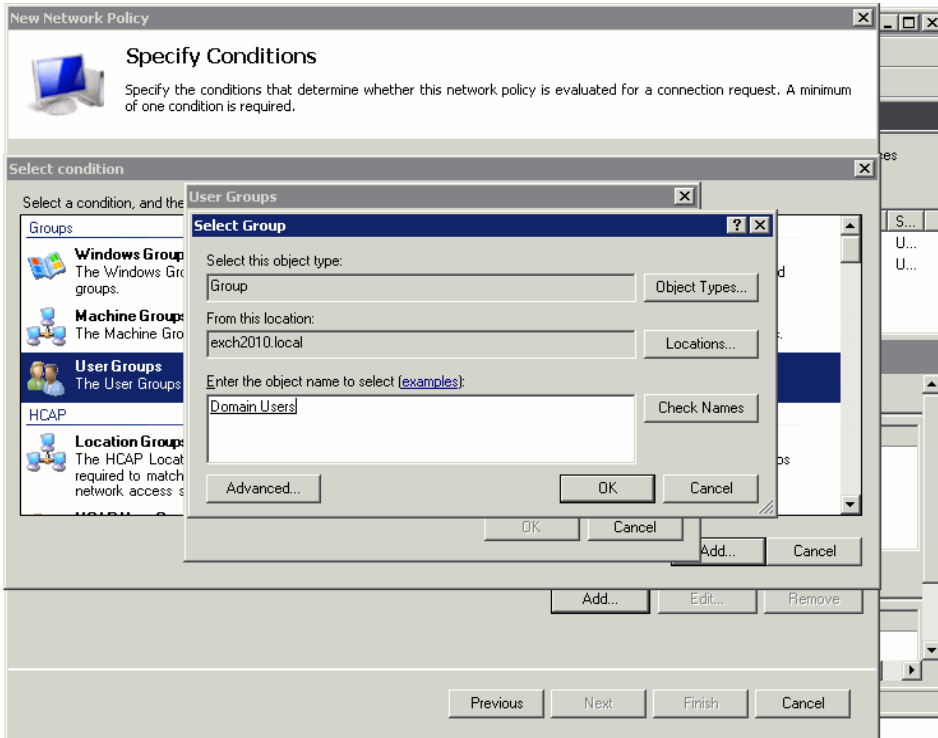




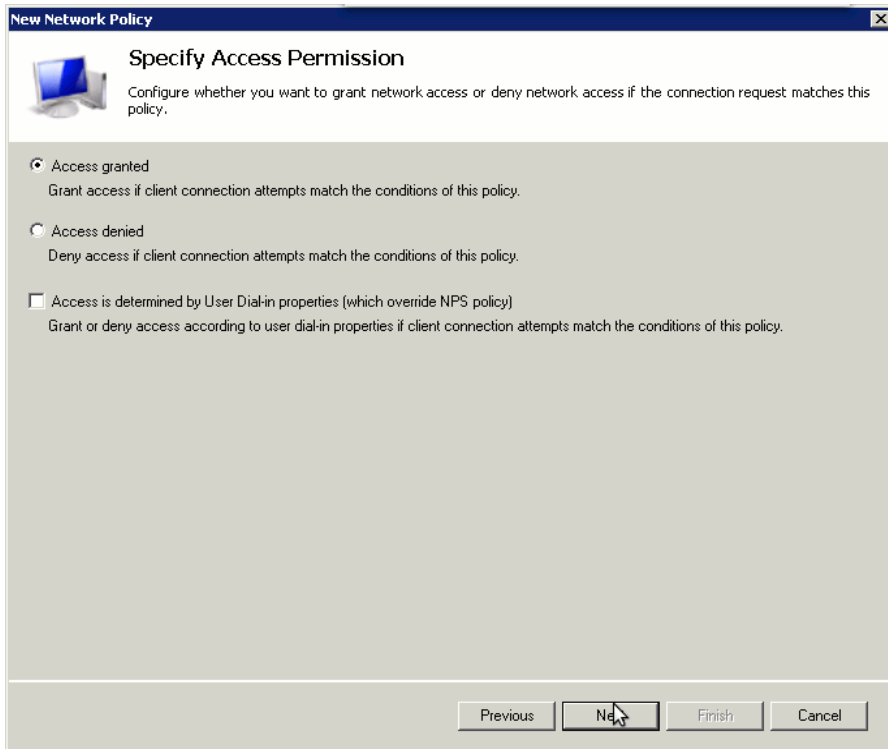
- Select NPS > Policies > Network Policies Go to Action -> New



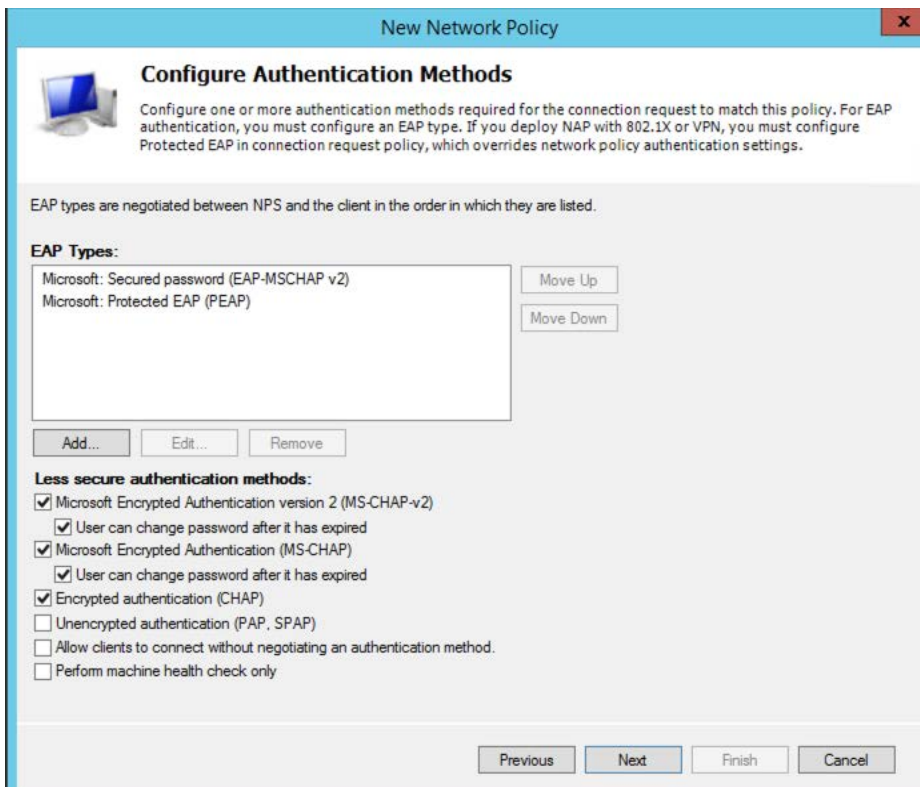
- Give the policy a name, then click next.
- Add a "User groups" condition, and specify the groups that you wish to have access



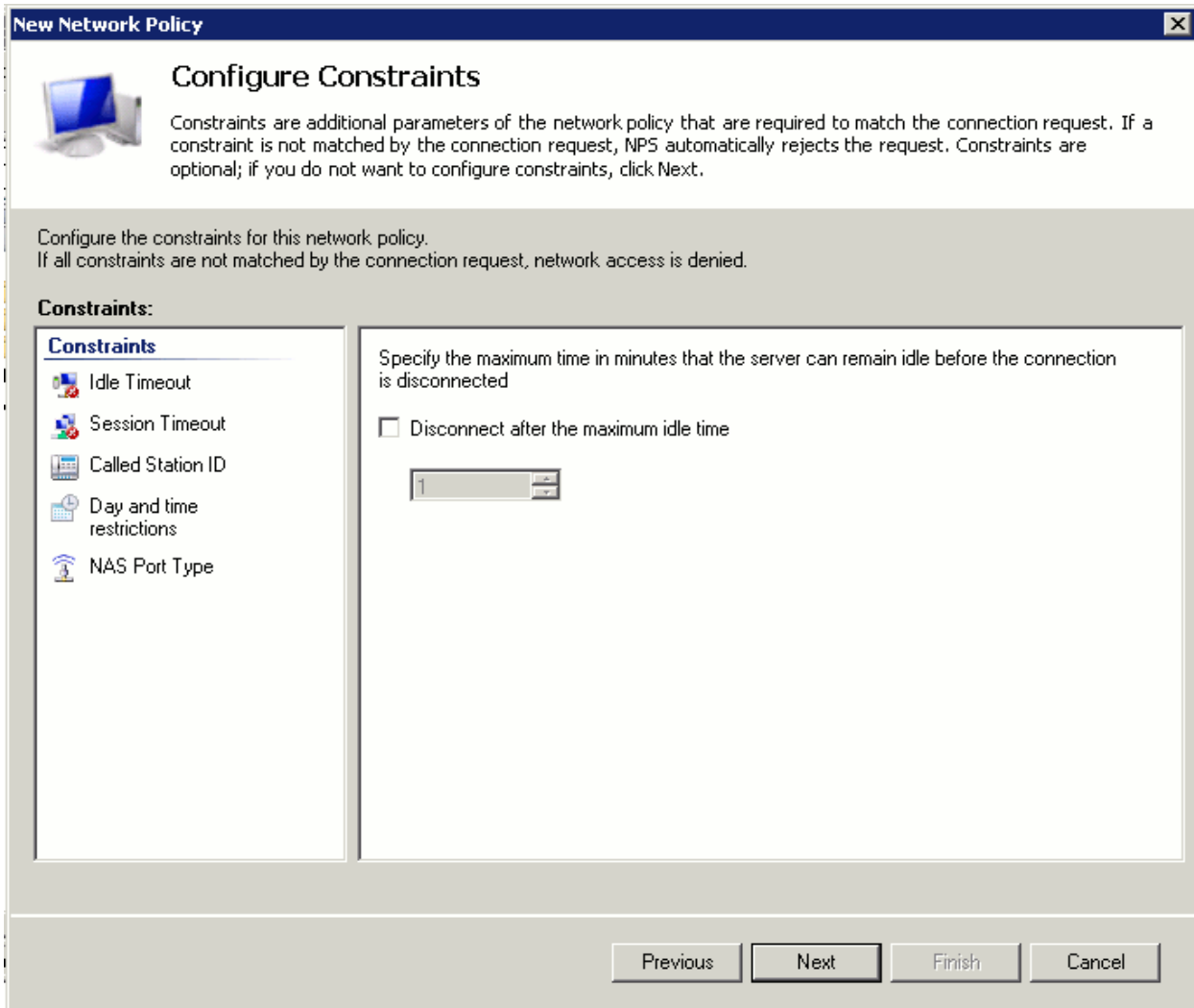
- Choose the permission "Access granted"



- Ensure "Unencrypted authentication (PAP, SPAP)" is enabled.



- Configure constraints if required:








New Network Policy [X]

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

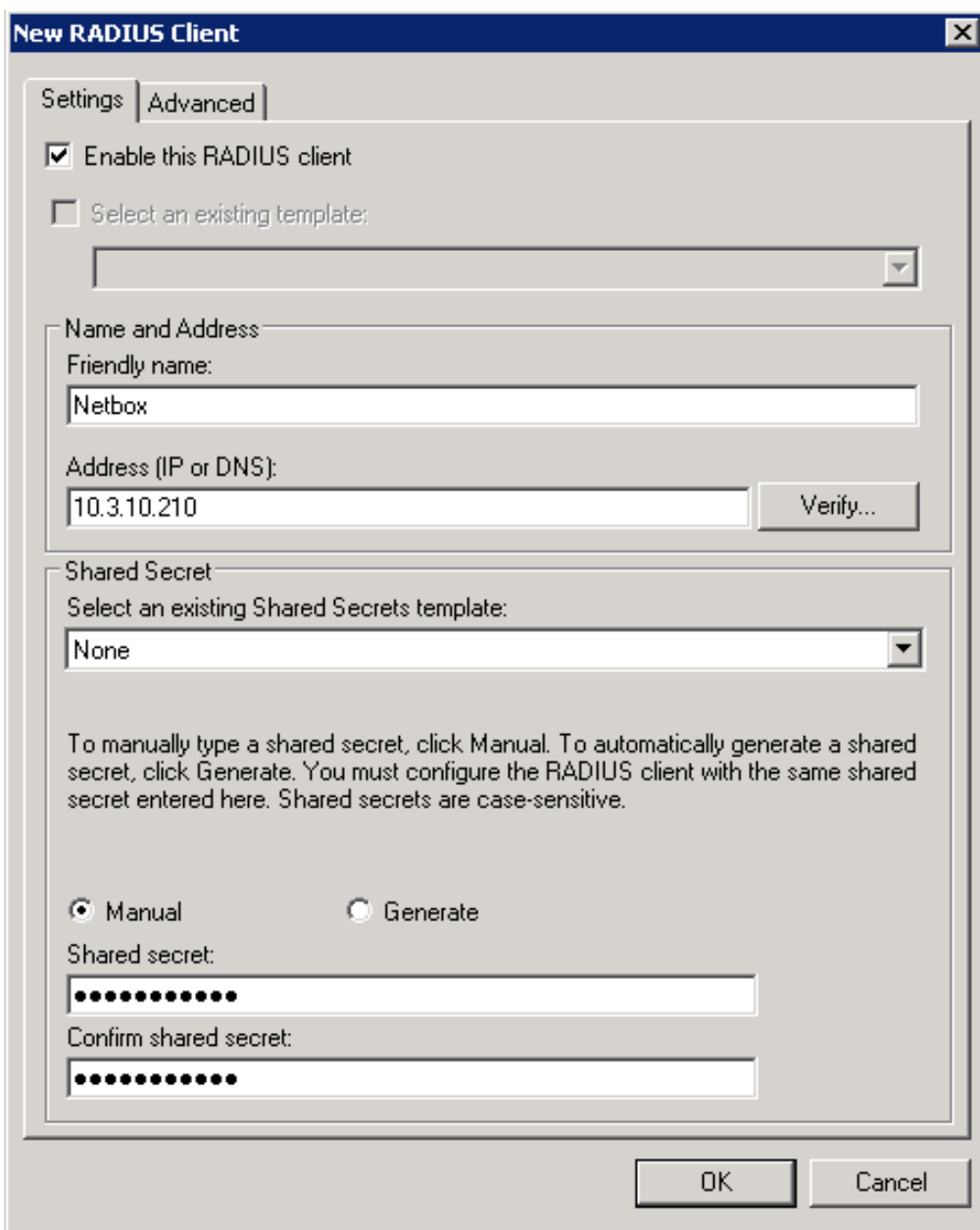
Constraints	
 Idle Timeout	<p>Specify the maximum time in minutes that the server can remain idle before the connection is disconnected</p> <p><input type="checkbox"/> Disconnect after the maximum idle time</p> <p><input type="text" value="1"/></p>
 Session Timeout	
 Called Station ID	
 Day and time restrictions	
 NAS Port Type	

Previous **Next** Finish Cancel

Configuring RADIUS Clients

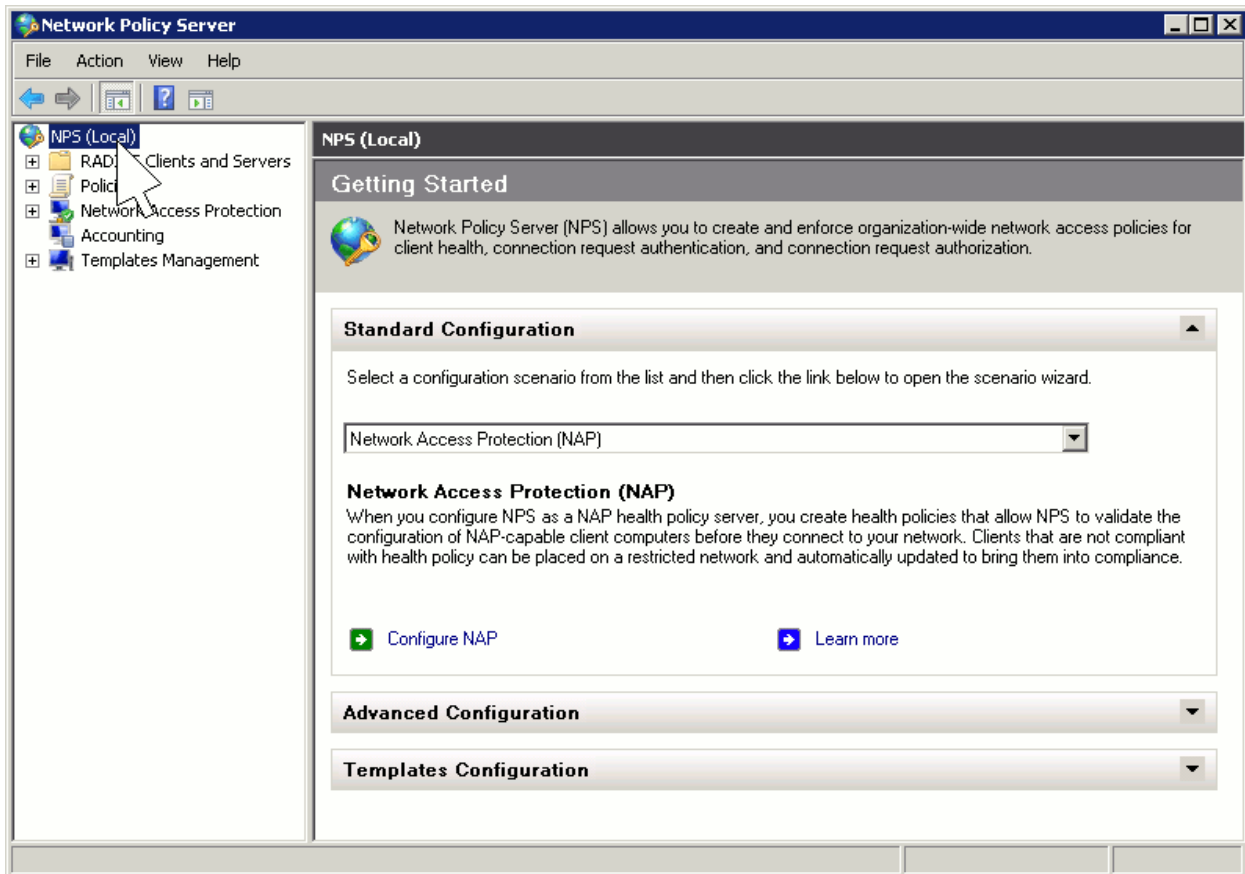
You will need to configure the RADIUS server to allow access from the CyberHound Appliance.

- Go to RADIUS Clients and Servers > RADIUS Clients and click Action > New.
- Enter a name (e.g. " CyberHound Appliance"), the IP address of the CyberHound Appliance and a shared secret:



Restarting the NPS Service

To ensure the changes take effect it is sometimes necessary to restart the NPS service. To do this, select NPS(local):



- Click on Action > Stop
- Click on Action > Start

And that is it! If you have experienced any difficulties or require some assistance with the configuration please contact us at support@cyberhound.com on 07 3020 3330 or log a Support Ticket [here](#).