Application Note

Using a Windows NT Domain / Active Directory for User Authentication NetScreen Devices

8/15/02
Jay Ratford
Version 1.0
Controlling Access to Large Numbers of Networks Devices to External Services

Today’s IT manager often finds himself managing large number of networks devices. While it certainly possible to control access to external services by administering the user database on each device, it is inefficient and prone to database divergence. Updating each network device’s user database each time a personnel change occurs in a network that has tens or hundreds of these devices becomes quite time consuming. Thankfully there are user authorization technologies such as RADIUS, which significantly reduce the overhead of administering access control. RADIUS, and Windows 2000 Active Directory provide services for user authentication through a centralized database of user information. NetScreen network security products utilize these technologies to provide efficient user authentication services. Additionally capitalization of costly hardware software components may be saved in that Windows 2000’s Active Directory provides services required to perform centralized authentication. Most important however is that most large enterprises already use NT Domain or Active Directory as the central user database, users change the passwords on their NT Domain which remains synchronized with other enterprise systems such as email, database and intranet logins. Integrating your NetScreen Device into an NT Domain or Active Directory user database allows you to leverage that database for authentication of VPN, Firewall and Administrative users.

This document will focus on configuring NetScreen ScreenOS 4.0 to authenticate usernames and passwords to an NT Domain or Active Directory via the RADIUS Protocol, using the Microsoft Internet Authentication Service (IAS), which comes standard on Windows 2000 Server. It will also explain how to use the NetScreen User-Group attribute, which enables all user change/adds/deletes to be performed from the NT Domain or Active Directory itself, as opposed to being done on the NetScreen Device. This allows you to effectively continue to manage users access, group membership, passwords and privileges through your existing NT Domain infrastructure, instead of doing so on each NetScreen Device.
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page #</th>
</tr>
</thead>
</table>

Section 1: Application Description…………………………………………………………………4
This section describes centralized authentication of access to external services, the roles of the Windows 2000 Server as a RADIUS server, the NetScreen Device running ScreenOS 4.0, and the user who will authenticate.

Section 2: Installing and Configuring Microsoft IAS RADIUS Server………………..5
This section describes the steps necessary to install Microsoft IAS and configure it for RADIUS authentication.

Section 3: Configuring Policies on Microsoft IAS with User-Group attribute……..9
This section describes the configuration steps necessary in Microsoft IAS server to create a Remote Access Policy using NetScreen attributes for User-Group membership.

Section 4: Configuring Authentication Servers and External User-Groups………16
This section describes the configuration steps necessary under ScreenOS 4.0 to configure RADIUS Servers and External User Groups.

Section 5: Setting up Policy Authentication using External User-Groups………18
This section describes the configuration steps necessary under ScreenOS 4.0 to enable policy authentication and restrict access to specific user groups on an external RADIUS Server.

Section 6: Setting up XAUTH using External User-Groups…………………………20
This section describes the configuration steps necessary under ScreenOS 4.0 to setup XAUTH VPN authentication and restrict access to specific user groups on an external RADIUS Server.

Conclusion…………………………………………………………………………………………25
Summary of RADIUS authentication with Microsoft IAS and the benefits it provides.

Appendix A: Other NetScreen Attributes and how to use them…………………..27
This section describes other less used NetScreen VSAs, what they are used for and how to set them up in the Microsoft IAS Server.
Section 1: Application Description

User Authentication for Access to External Services

Utilizing RADIUS authentication network connected devices can manage access to network services via centralized authentication. RADIUS authentication eliminates the need for user-by-user management of the access databases on each device. The access database resides on the RADIUS server. The NetScreen Device authenticates the user credentials, user-name, password and group-membership, from the RADIUS server. This greatly simplifies management of users and user access for large number of network devices.

Users or may authenticate to the NetScreen Device in plain-text with Policy Authentication or WebAuth. For VPN access with NetScreen-Remote XAUTH or L2TP is used for user authentication.
Section 2: Installing and Configuring Win2k for RADIUS Authentication

Microsoft Windows 2000, with its Active Directory Services, allows companies to develop large, centralized directories of network resources. Managing large numbers of users is easy due to its centralized directory architecture. NetScreen network security appliances can take advantage of a company's Active Directory infrastructure by authenticating users via Internet Authentication Service (IAS), Microsoft's implementation of a RADIUS.

Installing Microsoft IAS on Win2K

The following illustrates how to install and configure IAS on a Windows 2000 domain controller running Active Directory.

It is assumed the Windows 2000 server has been configured to be a domain controller and is already running Active Directory – although Active Directory is not required for IAS, a regular NT Domain will do the job. The illustrated steps will show a default configuration. It is recommended that advanced features of IAS be used in order to secure the IAS server. Please refer to Microsoft's IAS white paper for more information:


Click on Start->Settings->Control Panel
Double click on Add/Remove Programs
Click on Add/Remove Windows Components, located in the left menu bar
Highlight *Networking Services* and click on *Details*

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what’s included in a component, click *Details*.

**Components:**
- Message Queuing Services: 2.6 MB
- Networking Services: 3.6 MB
- Other Network File and Print Services: 0.0 MB
- Remote Installation Services: 1.7 MB
- Remote Storage: 3.5 MB

**Description:** Contains a variety of specialized, network-related services and protocols.

**Total disk space required:** 0.9 MB
**Space available on disk:** 7161.4 MB

Click *Next* to install IAS.

Check the *Internet Authentication Service* and click *OK* and then *Next* to install IAS.

**Subcomponents of Networking Services:**
- Dynamic Host Configuration Protocol (DHCP): 0.0 MB
- Internet Authentication Service: 0.0 MB
- QoS Admission Control Service: 0.0 MB
- Simple TCP/IP Services: 0.0 MB
- Site Server ILS Services: 1.5 MB
- Windows Internet Name Service (WINS): 0.9 MB

**Description:** Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.

**Total disk space required:** 0.9 MB
**Space available on disk:** 7161.3 MB
Configuring IAS to talk with NetScreen Devices

Click Start->Programs->Administrative Tools->Internet Authentication Service to start the IAS administrative tool.

Add the NetScreen Device as a client, right click on Clients and click on New Client Type in a name for the client and click Next.

Type in IP address of the NetScreen Device, in most cases this will be the trusted or internal interface IP Address. Leave the Client-Vendor as RADIUS Standard and make sure you uncheck the "Client must always send the signature attribute in the request" check box. Type in shared secret* that you will be using for this connection, you will
need to know the shared secret later on so make sure you remember it, it is case sensitive.

Note: The share secret allows for basic encryption of the RADIUS packets between the RADIUS Server and the NetScreen Device. If your RADIUS packets will be going across a public network such as the Internet you may also wish to establish a VPN for this connection to ensure greater security.

Once this setup has been complete, the RADIUS Server will permit the NetScreen Device to query it, however a Remote Access Policy is still required to permit or deny access to specific users, this is covered in Section 3
Section 3: Configuring Policies on Microsoft IAS with User-Group attribute

A Remote Access Policy tells the IAS Server to permit or deny access to a user based on a set of credentials. It also allows you to configure Vendor Specific Attributes (VSA’s) a form of RADIUS-Extensions, which allow you to send specific information to the NetScreen Device. Remote access policies can permit access based on a Users Group membership on the NT Domain, scheduled time or dates and many other parameters. Before any user can authenticate to the Microsoft IAS Server, a Remote Access Policy must be defined, we will create the following Remote Access Policy:

Policy 1: Permit Access to Sales users and return Sales User-Group attribute

This policy will permit users who are members of NT Domain User-Group “Sales” to authenticate to the RADIUS Server. This Policy will also return attributes the NetScreen Device if the is a member of the “Sales” Group, so access can be restricted to members of the Sales group only.

To define a remote access policy, first load the Microsoft IAS console from Start->Administrator Tools, select Internet Authentication Service to load the console. Right click on Remote Access Policy and click Add, a wizard will appear. First give this policy a name. In this example we used “Permit Access to Sales users and return Sales User-Group attribute”

Under conditions to match select Add and select Windows-Group
Select the Windows user-group you wish to restrict access to, in this example we will use “Sales”

A summary of conditions to match for this policy is shown: Windows-User Group matched “Sales” you may add additional user-groups here if desired, but users must be a member of all groups defined here for access to be permitted.

We now must edit the Dial-In Properties for this Remote Access Profile. This is where we will enable PAP or CHAP Authentication and NetScreen’s Vendor Specific Attributes
Under Dial-In Properties “Authentication” tab ensure that Password Authentication Protocol (PAP) or CHAP Encrypted Authentication is enabled. PAP is an authentication protocol that allows PPP peers to authenticate one another. The remote host attempting to connect to the local host is required to send an authentication request. Unlike CHAP, PAP passes the password and the host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access but merely identifies the remote end. The server then determines whether that user is allowed access. **Note:** CHAP is only supported when used with XAUTH on the NetScreen Device.

Also uncheck the two *Microsoft Encrypted Authentication* check boxes and check the *Unencrypted Authentication* check box and then click *OK*.

A dialog box will pop up, warning that you have changed settings. Just click on *No*. Click *OK* to acknowledge.
The RADIUS Server must tell the NetScreen Device that users matching this policy are a member of the Sales group, this is done through sending *Vendor Specific Attributes* (VSAs) to the NetScreen Device as part of this remote access policy. In the Advanced tab of the profile, Click the *Add* button to add the NetScreen VSA’s. A list will appear, select *Vendor Specific* and click *Add*.
From the list of attributes scroll down to **Vendor-Specific** and press **Add**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Vendor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login-IP-Host</td>
<td>RADIUS</td>
<td>IP address of host to which user should be connected</td>
</tr>
<tr>
<td>Login-LAT Group</td>
<td>RADIUS</td>
<td>LAT group codes for which user is authorized</td>
</tr>
<tr>
<td>Login-LAT-Node</td>
<td>RADIUS</td>
<td>Nodes with which user is to be connected by LAT</td>
</tr>
<tr>
<td>Login-LAT-Port</td>
<td>RADIUS</td>
<td>Port with which user is to be connected by LAT</td>
</tr>
<tr>
<td>Login-LAT-Service</td>
<td>RADIUS</td>
<td>Host with which user is to be connected by LAT</td>
</tr>
<tr>
<td>Login-Service</td>
<td>RADIUS</td>
<td>Service connecting user to login host</td>
</tr>
<tr>
<td>Login-TCP-Port</td>
<td>RADIUS</td>
<td>TCP port to which user should be connected</td>
</tr>
<tr>
<td>Reply-Message</td>
<td>RADIUS</td>
<td>Message to be displayed to user when authenticating</td>
</tr>
<tr>
<td>Service-Type</td>
<td>RADIUS</td>
<td>Type of service user has requested</td>
</tr>
<tr>
<td>Tunnel-Assigment-ID</td>
<td>RADIUS</td>
<td>Tunnel to which a session is to be assigned</td>
</tr>
<tr>
<td>Tunnel-Client-Auth-ID</td>
<td>RADIUS</td>
<td>Name used by the tunnel initiator during the authentication</td>
</tr>
<tr>
<td>Tunnel-Client-Endpt</td>
<td>RADIUS</td>
<td>IP address of the initiator end of the tunnel</td>
</tr>
<tr>
<td>Tunnel-Medium-Type</td>
<td>RADIUS</td>
<td>Transport medium to use when creating a tunnel for a particular session</td>
</tr>
<tr>
<td>Tunnel-Password</td>
<td>RADIUS</td>
<td>Password for authenticating to a remote server</td>
</tr>
<tr>
<td>Tunnel-Preference</td>
<td>RADIUS</td>
<td>Relative preference assigned to each tunnel when a session is created</td>
</tr>
<tr>
<td>Tunnel-Pti-Group-ID</td>
<td>RADIUS</td>
<td>Group ID for a particular tunneled session</td>
</tr>
<tr>
<td>Tunnel-Server-Auth-ID</td>
<td>RADIUS</td>
<td>Name used by the tunnel terminator during the authentication</td>
</tr>
<tr>
<td>Tunnel-Server-Endpt</td>
<td>RADIUS</td>
<td>IP address of the server end of the tunnel</td>
</tr>
<tr>
<td>Tunnel-Type</td>
<td>RADIUS</td>
<td>Tunneling protocols to be used</td>
</tr>
<tr>
<td><strong>Vendor-Specific</strong></td>
<td>RADIUS</td>
<td>Used to support proprietary NAS features</td>
</tr>
</tbody>
</table>
Select *Enter Vendor Code* and input 3224 (NetScreen’s IETF Code) and ensure you select *Yes, it does confirm* and click *Configure Attribute*

![Vendor-Specific Attribute Information](image)

Under *Vendor-assigned attribute number* enter 3. This is the assigned number for the NetScreen User-Group attribute, the attribute is in *string* format. In this example we will use *Sales* as the value for this attribute.

![Configure VSA (RFC compliant)](image)
Click OK and you will return to the advanced properties screen. You should now see the NetScreen VSA for User-Group Sales listed under advanced.

![Edit Dial-in Profile](image)

You should remove ALL other VSAs, as only this one is required. Then click OK to save the changed you made. You may come back and modify the VSA or Constraints at a later time if desired.

You are now done configuring your Remote Access Policy, it will appear on the list in the Microsoft IAS Server console. This policy will permit access and return the Sales attribute to the NetScreen Device when users who match these conditions authenticate.

![Internet Authentication Service](image)

**Note:** If you will be using Microsoft IAS Server for other applications, it may be necessary that you move the NetScreen Remote Access Policy to the top of the list. Just like firewall policies remote access policies are read in top-down order.
Section 4: Configuring Authentication Servers and External User-Groups

This section describes the NetScreen ScreenOS configuration for creating authentication servers and external user-groups. These steps must be done prior to creating policies or VPN tunnels that will use external RADIUS Servers or user-groups.

First you must define a RADIUS Server on the NetScreen-Device, to do that select Configuration -> Auth -> Auth Servers from the WebUI.

Click on the New button to add a new Authentication Server. The following window will appear asking for a name, IP Address and Account-Type. Fill in the IP Address of your Microsoft IAS Server, and select Account Type of XAUTH.

Select the RADIUS Radio button and fill in the shared secret you configured earlier on the RADIUS Server.

Note: Test communication from your NetScreen Device to the RADIUS Server by using the PING Command, if you cannot ping your RADIUS Server you may have to add routes to the NetScreen Device before continuing.
The new authentication server will now appear on the list

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Server IP/Name</th>
<th>Type</th>
<th>Acct Type</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Local</td>
<td>Local</td>
<td>Local</td>
<td>admin auth l2tp xauth</td>
<td>Edit</td>
</tr>
<tr>
<td>1</td>
<td>Def2TPAuthServer</td>
<td>Radius</td>
<td>l2tp</td>
<td></td>
<td>Edit</td>
</tr>
<tr>
<td>2</td>
<td>Microsoft\NAS</td>
<td>172.16.4.169</td>
<td>Radius</td>
<td>xauth</td>
<td>Edit</td>
</tr>
</tbody>
</table>

* - Auth server is in use

Once authentication servers have been defined, they may be used in policies or VPN tunnels to authenticate a subset of users against specific authentication server. Depending on the NetScreen device, up to 10 authentication servers may be defined.

If you wish to restrict access to a subset of users on that authentication server, you may create an external user-group. This also requires that the RADIUS Server be configured to return the NetScreen User-Group attribute, outlined in section 3 above.

We must now define external user-group Sales this is done from the WebUI under Objects->User Groups->External

The **Group Name** will be Sales, this must match exactly to the value defined for the NetScreen User-Group attribute (attribute number 3) in the RADIUS Servers Remote Access Policy, which we defined in section 3 above. For **Group Type** select the type of authentication that this user-group will be used for. In this example we will use this user group to authenticate Xauth users, so we will select Xauth.

Once we have defined RADIUS Servers and External User-Groups these may be selected in Policies and Tunnels on the NetScreen Device. The steps to do this are outlined in sections 5 and 6 below.

Copyright © 2002 NetScreen Technologies, Inc.
Section 5: Setting up Policy Authentication using External User-Groups

If enabled, Policy Authentication (also known as “Firewall Authentication”) requires users to authenticate in plain-text with either HTTP, FTP or Telnet prior to accessing resources. WebAuth is also a form of policy authentication which requires users to authenticate with their web-browser before access to a specific policy will be permitted.

Both forms of authentication allow you to select specific authentication servers and user-groups to restrict access. In this example we will restrict access to users on the Microsoft RADIUS Server who belong to the Sales user-group.

Since we previously defined the Authentication Server and External User Group in section 4, we simply enable authentication for a new policy, first define the parameters of your policy, then select the Advanced button, the authentication settings will appear.

Select the MicrosoftIAS server from the popup menu, to restrict access to the Sales group also select Sales from the user-group popup menu.

Note: To permit access to all users on the RADIUS Server, simply leave the user group popup menu set to the default setting: Allow Any
Access may also be restricted to specific usernames, by selecting the User radio button and entering the username in the field provided – However if a large number of users will be permitted access, an External User Group is likely the best approach.

**Testing the authentication**

To test, we will authenticate to the resource and login as user Joe, who belongs to the NT User Group *Sales*.

Open your browser and point to destination address defined in the policy, in this case [http://172.16.4.251](http://172.16.4.251)

When prompted for a username and password, enter Joe’s username and Windows password.

![Enter Network Password dialog](image)

You are now authenticated as Sales user Joe and your access to that policy will be permitted.

All user logins both successful and failed are logged the event log on the Microsoft IAS System. You can verify that a user was successfully validated by RADIUS by checking the Windows event log on that system.
Section 6: Setting up XAUTH using External User-Groups

XAUTH is a form of authentication for IPSec VPN tunnels, when used with NetScreen-Remote XAUTH prompt the user for a username/password prior to establishing Phase II of a IPSec Connection. XAUTH also provides additional functionality via ModeConfig which assigns the user a Virtual IP Address, as well as virtual DNS and WINS addresses for use with VPN traffic.

The first step in configuring XAUTH, is to configure the IP Pool for the XAUTH users. You must select Objects>IP Pools. You must then enter an IP pool that is different than any other assigned address on the Netscreen device.

You must configure the IKE Identity in the internal user database. You may either use individual IKE Identities where each user is input into the NetScreen Device, or Group IKE Identities if you wish to define only single user identity and allow multiple users to share. For more information on Group IKE Identity please see the ScreenOS 4.0 Concepts & Examples guide.
To add a local IKE User from the WebUI select Objects->Users->Local and click New to add a new user. You need only select the IKE User checkbox and fill in an IKE Identity, usually in the form of an email address.

<table>
<thead>
<tr>
<th>User Name</th>
<th>User Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lisa</td>
<td>SalesIKE</td>
</tr>
</tbody>
</table>

Status: Enable

- **IKE User**
  - Simple Identity
    - IKE ID Type: AUTO
    - IKE Identity: lisa@netscreen.com

If using Group-IKE Identity you must add this user to a user-group as well, this is done from the WebUI under Objects->User-Groups->Local. Simply create a new user-group and add the appropriate users to that group.

Next we can define the Global XAUTH Settings for this device, XAUTH may also be used to provide Virtual IP Address, WINS and DNS Information to NetScreen-Remote Users after successful authentication. From the WebUI select VPNs->XAUTH Settings.

Define your internal WINS and DNS Servers here, if you wish to enable CHAP do so here, also select your default IP Pool from the IP Pool Name popup menu, click Apply to save these settings.
Once any local IKE Users, IP Pools and default XAUTH Settings have been defined, we can define the VPN connection.

Next we define an AutoKey IKE VPN using XAUTH, from the WebUI select VPNs->AutoKey IKE and click New to create a new entry.

Give the VPN a name, select DialUp Group Sales and enter a preshared key. We will use the default ethernet3 (untrust) interface to terminate traffic.

Once the VPN has been defined, press OK, it will appear on the list.

<table>
<thead>
<tr>
<th>Name</th>
<th>Gateway</th>
<th>Security</th>
<th>Monitor</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>SalesVPN</td>
<td>SalesVPN</td>
<td>Standard</td>
<td>Off</td>
<td>Edit, Remove</td>
</tr>
</tbody>
</table>

From the WebUI Select VPNs->AutoKey IKE Advanced->Gateway and click edit for the SalesVPN Gateway previously defined, click on the Advanced button and scroll down to Enable XAUTH section.

XAUTH is enabled on a Per VPN-basis, so to enable XAUTH for this VPN you must select the checkbox. Once enabled you may choose to authenticate users via the local database or an external server. In this example we will choose External Authentication and select the previously-defined MicrosoftIAS as our server. To limit access to a specific user-group we will select User Group and input Sales. You may also enable CHAP authentication here.
If only a specific user is to be permitted access, you may select the User ratio button and enter the username in the field provided; however for a scalable solution involving many users, External User Groups is the preferred method.

**Note:** The name of the User Group defined must be an exact match to the External User Group previously defined, and must match exactly to the NetScreen User-Group VSA defined on the Microsoft IAS Server in section 3 of this document.

Next define appropriate Policies for the VPN traffic, this will usually consist of permitting access to a specific subnet from DialUp Any, depending on your environment your policy may vary.

You must also setup NetScreen-Remote to make a VPN Connection to this device. If your not familiar with this process please see the NetScreen-Remote Administrator
Guide or the Application Note available from NetScreen TAC entitled *Configuring XAUTH VPN with NetScreen-Remote*.

When defining the Security Policy for NetScreen-Remote, be sure to enable Extended Authentication (XAUTH). To do so click on the “Authentication (Phase 1)” then click on “Proposal 1”, under the “Authentication Method” Select “Pre-Shared Key; Extended Authentication”.

![Security Policy Editor - NetScreen-Remote](image)

**Testing the authentication**

Once NetScreen-Remote has been setup you may now test your XAUTH Authentication and VPN Configuration. From the NetScreen-Remote machine simply ping the VPN network from the command-prompt.

```
C:\WINNT\System32\cmd.exe - ping 172.16.4.251 -t
G:\>ping 172.16.4.251 -t
Pinging 172.16.4.251 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```
XAUTH will prompt you for a username and password, enter the Windows username and password of a user in the Sales Group and press OK.

If authentication was successful, you should see replies to the PING packets and a green light in the NetScreen-Remote taskbar, indicating an active VPN tunnel.

The above procedure may be repeated for additional user-groups with separate access policies, giving very granular control over users VPN access rights.

All user logins both successful and failed are logged the event log on the Microsoft IAS System. You can verify that a user was successfully validated by RADIUS by checking the Windows event log on that system.

**Conclusion**

Powerful authentication of users can be realized using Microsoft’s Internal Authentication Service (IAS) and NetScreen network security appliances. NetScreen supports both RADIUS to suit the network managers needs. Network managers can take
advantage of centralized user databases provided by Active Directory to restrict access for
VPNs and Administration purposes for NetScreen products. Utilizing equipment and
software they may already exist in the network will save significant capital expense.
Authentication from a centralized source saves many man-hours of configuration time
and prevents database divergence which is likely to happen using locally administered
user databases. Together NetScreen’s authentication and Windows 2000 provide an
additional layer of security to the network at an optimize operational and capital expense.
Appendix A: Other NetScreen Attributes and how to use them

NetScreen Devices running ScreenOS 4.0 can make use of other NetScreen Attributes (VSAs) besides the User-Group attribute that are not covered in this document. The following is a list of VSAs supported in ScreenOS 4.0 at the time this document was produced. You can always retrieve the latest NetScreen RADIUS “Dictionary” Files from the NetScreen TAC Website http://support.netscreen.com

<table>
<thead>
<tr>
<th>VSA#</th>
<th>NetScreen VSA</th>
<th>VSA Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NS-Admin-Privilege</td>
<td>Integer</td>
<td>Device Admin Access Rights (see table 1)</td>
</tr>
<tr>
<td>2</td>
<td>NS-VSYS-Name</td>
<td>String</td>
<td>Name of VSYS, used for Admin Privilege</td>
</tr>
<tr>
<td>3</td>
<td>NS-User-Group</td>
<td>String</td>
<td>Matches External User Group definitions</td>
</tr>
<tr>
<td>4</td>
<td>NS-Primary-DNS</td>
<td>IP Addr</td>
<td>Used for XAUTH / L2TP DNS Only*</td>
</tr>
<tr>
<td>5</td>
<td>NS-Secondary-DNS</td>
<td>IP Addr</td>
<td>Used for XAUTH / L2TP DNS Only*</td>
</tr>
<tr>
<td>6</td>
<td>NS-Primary-WINS</td>
<td>IP Addr</td>
<td>Used for XAUTH / L2TP WINS Only*</td>
</tr>
<tr>
<td>7</td>
<td>NS-Secondary-WINS</td>
<td>IP Addr</td>
<td>Used for XAUTH / L2TP WINS Only*</td>
</tr>
</tbody>
</table>

* These values are used to assign client Virtual DNS/WINS Addresses when Query Client Settings on Server is enabled for a particular XAUTH or L2TP Connection.

Table 1:
Integer Values are used for Device Admin Access Privileges, enter a number between 1 and 5 to define the admin privilege for device admins.

1 – Root Admin Admin
2 – All VSYS Root Admin
3 – VSYS Admin Admin (Requires VSA#2 VSYS Name be entered)
4 – Read-Only Admin
5 – Read-Only VSYS Admin (Requires VSA#2 VSYS Name be entered)