



Title: Bi-Directional Netscreen Remote VPN using xAuth and Firewall Authentication with Microsoft Internet Authentication Service
Document Number: FW-400-002
Version: 1.1, October 1, 2004
OS Ver: Screen OS 4.0.2/above
HW Platforms this Paper Applies to: Netscreen 5xp, 5xt, 25, 50, 204, 208, 500, and 5200
Audience (Internal or External): Internal
Version: Ready for review

Bi-Directional Netscreen Remote VPN using xAuth and Firewall Authentication with Microsoft Internet Authentication Service (IAS)

Purpose

The purpose of this application note is to assist a user in setting up a Netscreen Firewall (ScreenOS 4.0.2 and above) and Netscreen Remote VPN Client (8.x and above) to use Xauth and Firewall Authentication with Microsoft IAS Service to establish a bi-directional remote VPN connection. This process will require the following:

1. Installing and configuring IAS (Internet Authentication Service) on Windows 2000 Server;
2. Configuring Netscreen Firewall for xAuth and Firewall Authentication; and
3. Configuring Netscreen Remote VPN for Dialup VPN connection.
4. Testing and verifying the Authentication and VPN Connection.

Overview

The use of RADIUS as the unified authentication server for user and device access has gained its popularity in the network security industry. RADIUS server provides a central repository of authentication and auditing information. Based on RFC 2165, 2865 and 2866, RADIUS is an open, flexible and scalable authentication mechanism.

It can be integrated with other existing authentication database such as Windows 2000 Active Directory or Novell Directory Services to provide access control and maintenance for enterprise wide network.

To take advantage of centralized authentication and simple user access management, Netscreen provides the feature for implementing RADIUS server to allow authentication of VPN, firewall, administrative user and external user groups.

This document is intended to provide a Step-by-Step instruction of utilizing Microsoft RADIUS Server (Internet Authentication Service) for Firewall and xAuth (external) Authentication to establish a bi-directional VPN connection.

The structure of this document includes the following sections:

Section 1: Application Description

Section 2: Lab Environment Diagram and Configuration Objective

Section 3: Installing and Configuring IAS to support Netscreen Device

Section 4: Configuring Remote Access Policy for Global User Group

Section 5: Configuring Netscreen for xAuth and Firewall Authentication
Section 6: Configuring Netscreen Remote Client for xAuth and Firewall Authentication
Section 7: Testing and Verifying Authentication and Bi-Directional VPN Connection

An appendix – CLI Example of Configuration is also included for reader's reference and review.

Section 1: Application Description

Firewall Authentication

Firewall authentication is a policy-based authentication method, which requires user to initiate an authentication request via HTTP, FTP or Telnet traffic. The authentication requests are initiated based on destination addresses defined in the policies. The authentication session are cached in the firewall for a specific interval (default timeout is 10 minutes; configurable up to 255 minutes) base on source IP address.

xAuth (Extended Authentication)

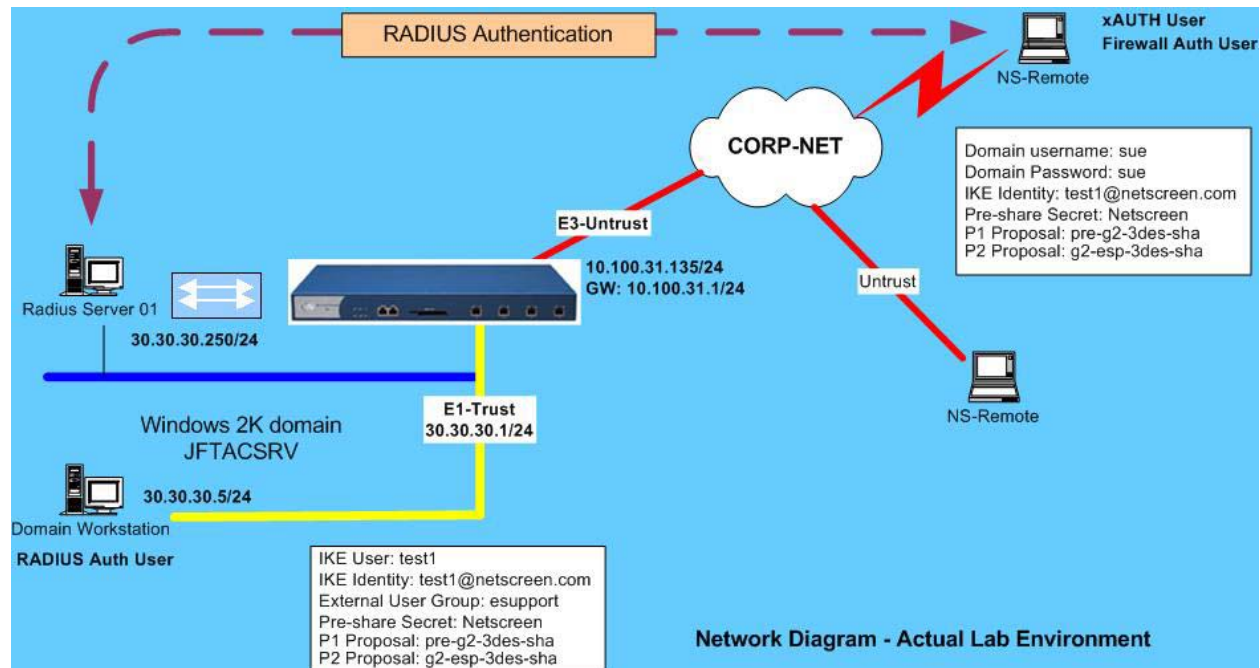
Netscreen's implementation of xAuth requires network user to provide the login credential when the VPN connection is initiated. It is configured on IKE gateway (Phase 1 configuration). The authentication request are made in between the IKE phase 1 and phase 2 negotiations. Unlike Firewall authentication, the User login credential is encrypted during the xAuth session. IP address assignment, DNS and WINS IP can be relayed to the xAuth client(s) upon successful authentication. The xAuth lifetime is 480 minutes.

Microsoft IAS (Internet Authentication Server)

Integrated with Microsoft Windows 2000 Active Directory infrastructure, Internet Authentication Service (IAS), a Microsoft's implementation of RADIUS, provides an efficient architecture of centralized user authentication, accounting and authorization. IAS incorporated the use of remote access or VPN equipment in a single or multiple vendor network environment. Advanced features of IAS can be used to secure the domain and user access. Please refer to Microsoft's IAS white paper for more information:

<http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remotearr/ias.asp>

Section 2: Lab Environment Diagram and Configuration Objective



The objective of this lab is to allow bi-directional VPN access between the Remote VPN user and the Window 2k Domain by using the double-layer of user authentication: xAuth and Firewall authentication.

The Proposed Traffic Flow

1. The Remote VPN user will initiate a Phase 1 negotiation from the Netscreen Remote Client by pinging the domain workstation (30.30.30.5) on JFTACSRV domain.
2. The Remote User will then enter the domain username and password to be authenticated by Microsoft IAS resides on Domain controller (30.30.30.250).
3. The Remote user will launch a HTTP session to access the domain workstation (30.30.30.5) therefore to invoke the Firewall Authentication. The Remote user will again use the domain username and password to login.
4. Upon successful authentication, the remote VPN user will process with ping request to reach Domain workstation. A successful ping reply should be returned.
5. The Domain Workstation will ping the IP (60.60.60.1) assigned to Remote VPN User and receive a successful reply. This will complete the bi-directional VPN Connection (required ScreenOS 4.0.2 and above).

Section 3: Installing and Configuration IAS to support Netscreen Device

This document assumed that IAS is installed on a Windows 2000 server (as a domain controller) and is configured to support Netscreen Device for xAuth and Firewall Authentication.

The following link provides a step-by-step installation instruction of IAS on a Windows 2000 server.

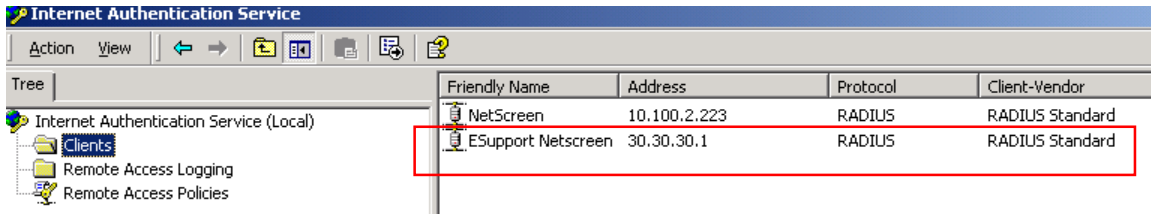
http://kb.juniper.net/kb/documents/public/ApplicationNotes/Technical/ScreenOS%204.0.0/400_config_screenos_ntdomain.pdf
(Section 2: Installing and Configuring Win2k for RADIUS Authentication. Page 5-8).

Section 4: Configuring Remote Access Policy for Global User Group

After configuring IAS to support Netscreen, you will see the available Clients on IAS Console.

Start- >Administrator Tools, select **Internet Authentication Service** to load the console.

Two RADIUS clients (“Netscreen – 10.100.2.223” and “Esupport Netscreen – 30.30.30.1”) are configured as illustrated. This documentation will use **Esupport Netscreen** as the example.

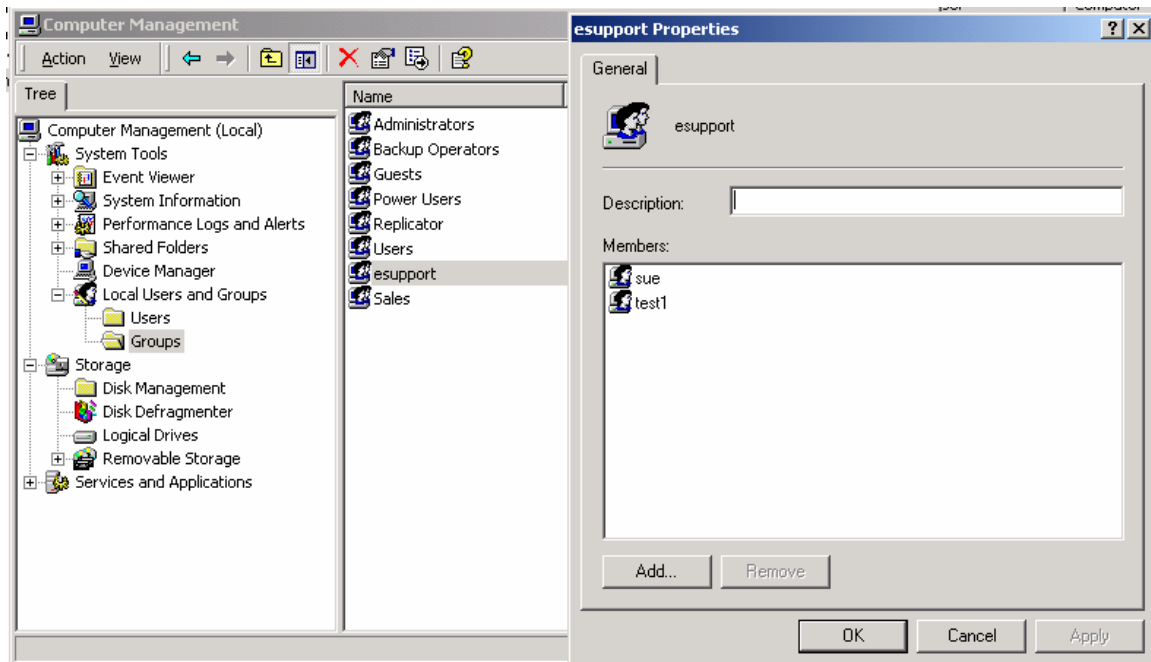


1. Creating Domain User Group

Prior to creating a Remote Access policy, User Groups need to be defined on Domain Computer Management.

Start- >Administrator Tools, select **Computer Management**.

Esupport Group is created and domain users “sue” and “test1” are added as group members.



2. Creating Remote Access Policy

A Remote Access Policy is a form of access lists created on IAS to permit or deny user access based on a set of credentials. Netscreen provides Vendor Specific Attributes (VSA's) to allow specific information to be forwarded to the NetScreen Device.

Parameters, such as Domain Users Group membership, scheduling and others can be implemented on Remote Access Policies. A Remote Access Policy must be created and defined prior to allowing user authentication to the IAS Server. In our lab, we will create the following Remote Access Policy:

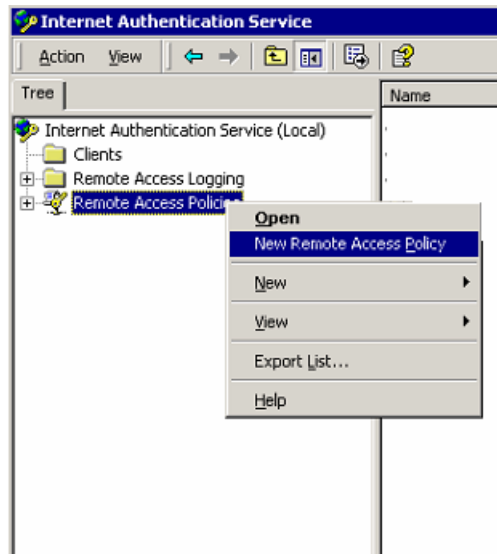
Policy 1: Permit access to esupport VPN to all users in “esupport” Group

This policy will permit domain users who are members of “esupport” Group to login with NetScreen-Remote to gain access to resources defined in esupport VPN with Policy manager.

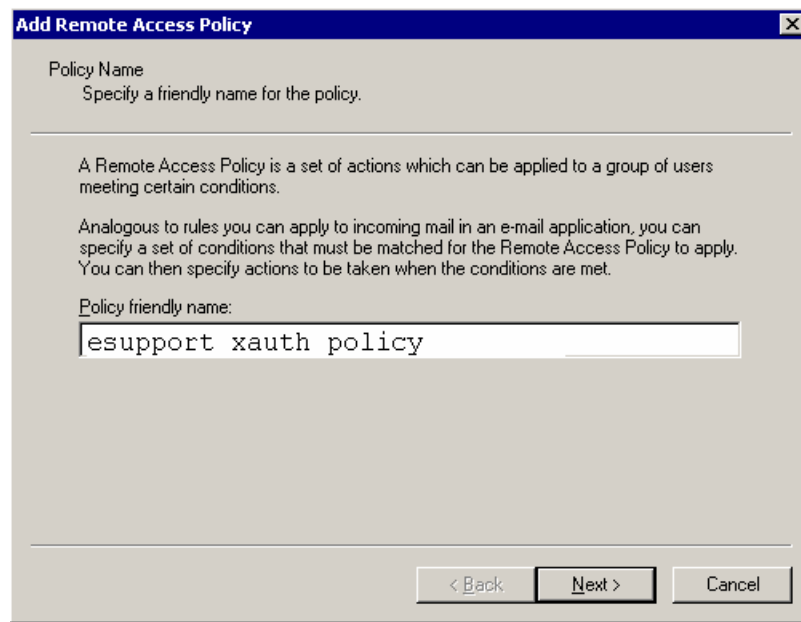
To create a remote access policy, start Microsoft IAS console.

Start- >Administrator Tools, select **Internet Authentication Service** to load the console.

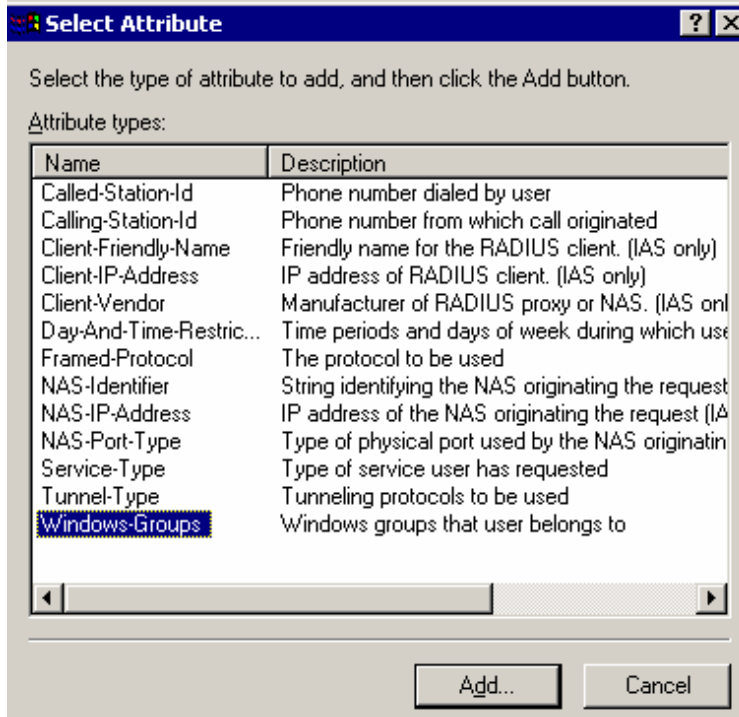
Right click on Remote Access Policy and click **Add**, a wizard will appear.



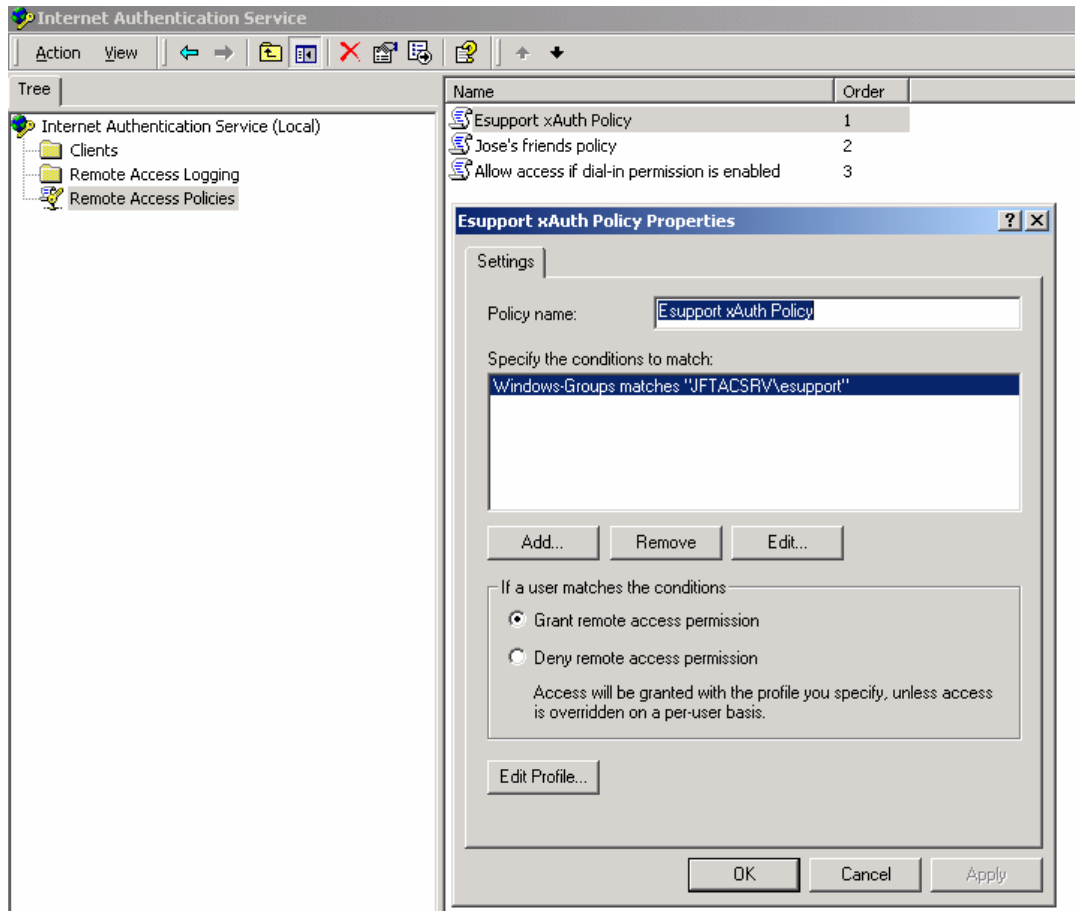
Enter a name of the new policy, for example “*Esupport xAuth policy*” and click on “*Next*”.



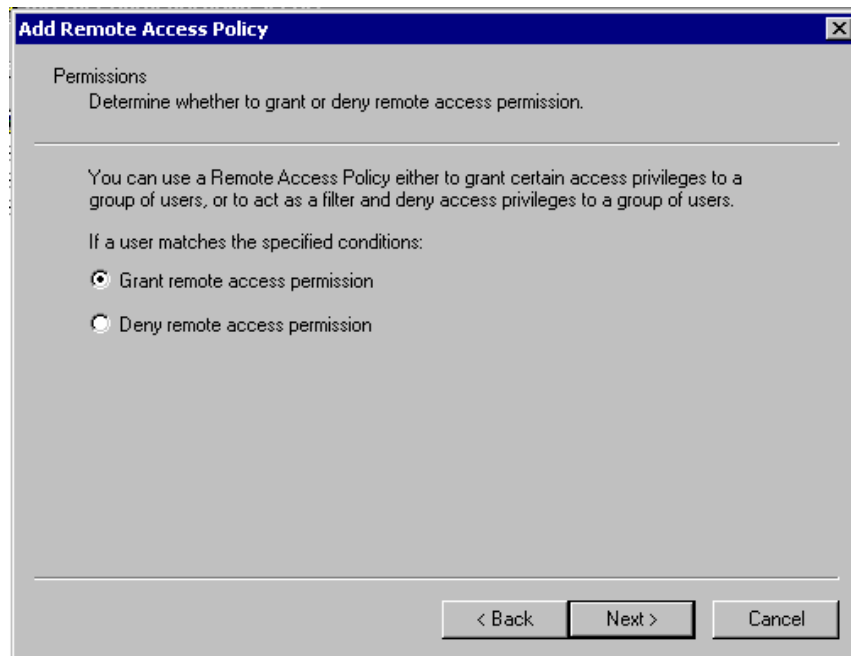
Select Attribute *Windows-Groups* and click on “Add” to continue.



Select appropriate Windows Group that will be bound to this access policy and be added under conditions to match. “*Windows-Groups matches “JFTACSRV\esupport”* is used in our lab. You may add additional User Group to permit the access in the Remote Access Policies.



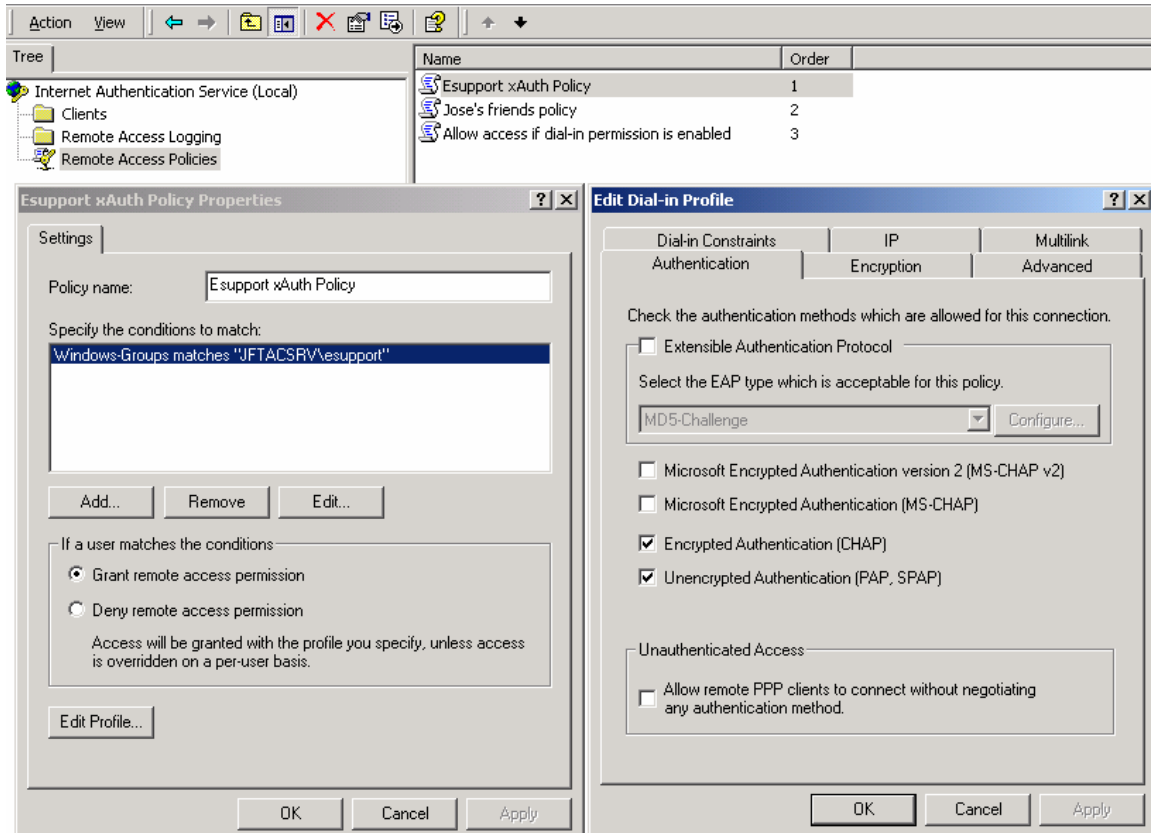
We have elected “Grant Remote Access Permission” to esupport group.



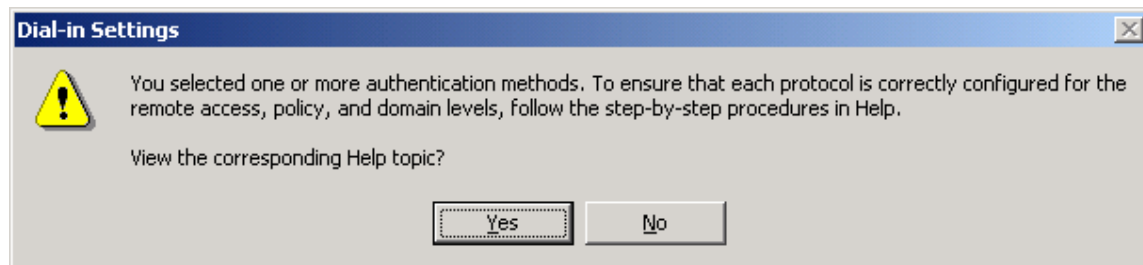
3. Defining Remote Access Profile

We will define PAP Authentication and NetScreen's Vendor Specific Attributes (VSAs) under Dial-in Properties of Remote Access Profile.

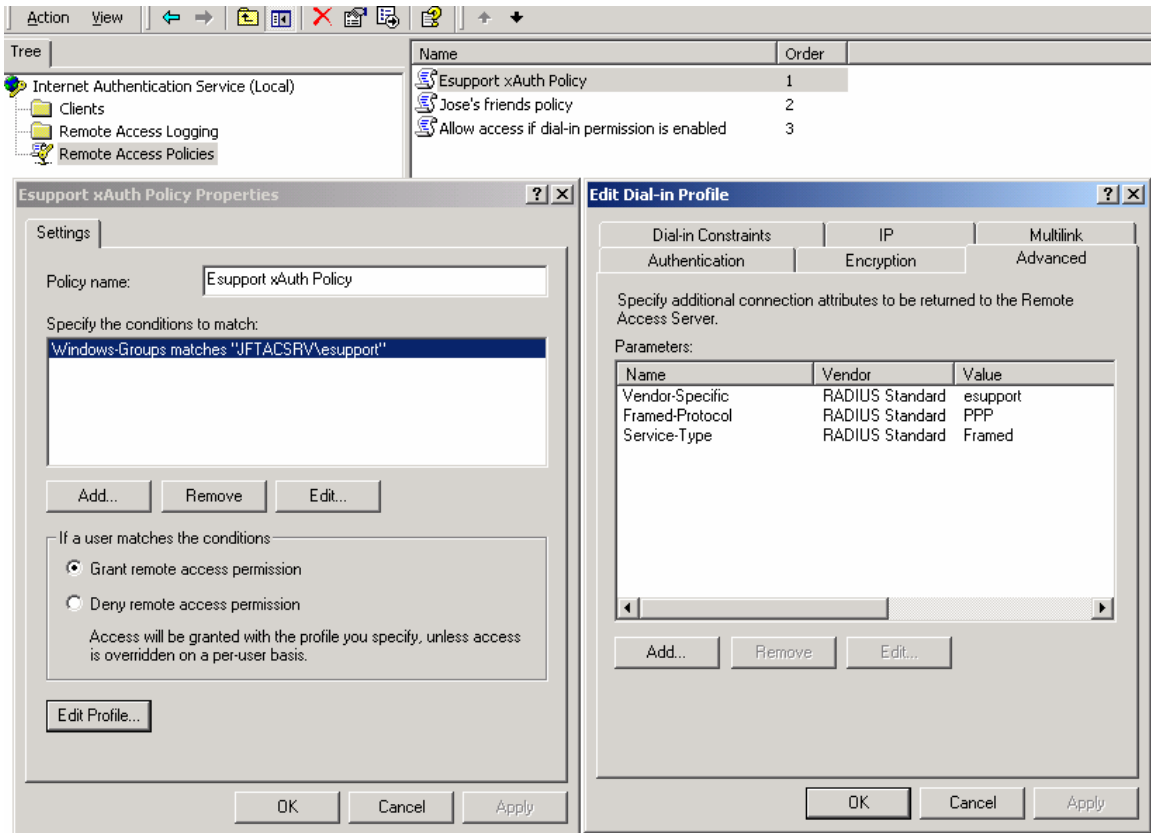
Click on Edit Profile, select "*Authentication*" tab. Uncheck both "*Microsoft Encrypted Authentication version 2*" and "*Microsoft Encrypted Authentication*" check boxes and check the *Unencrypted Authentication* check box.



A warning dialog box will pop up regarding the changed settings. Click on *No* to exit.

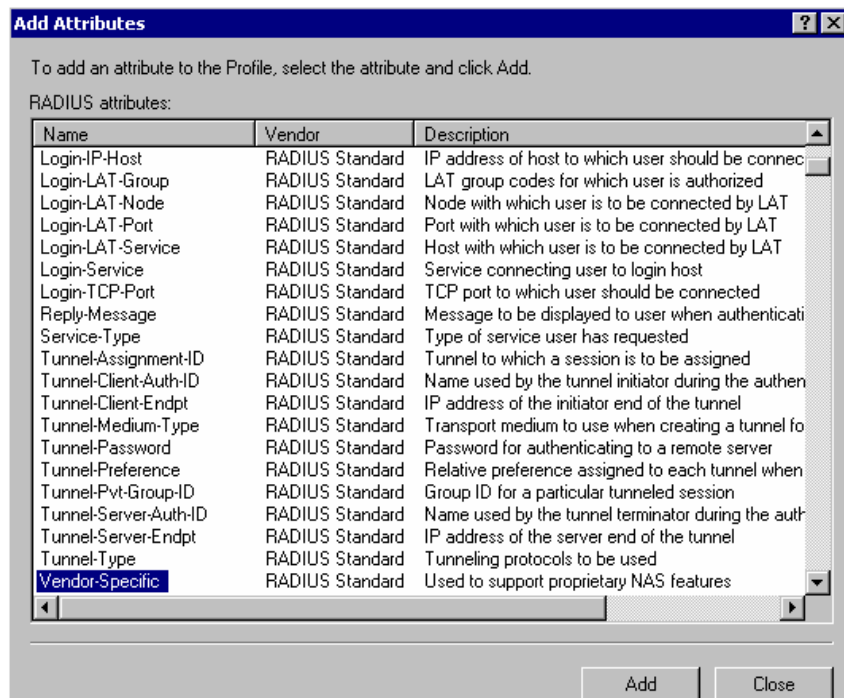


Click *OK* to acknowledge. Select "*Advanced*" tab of Dial-In Properties

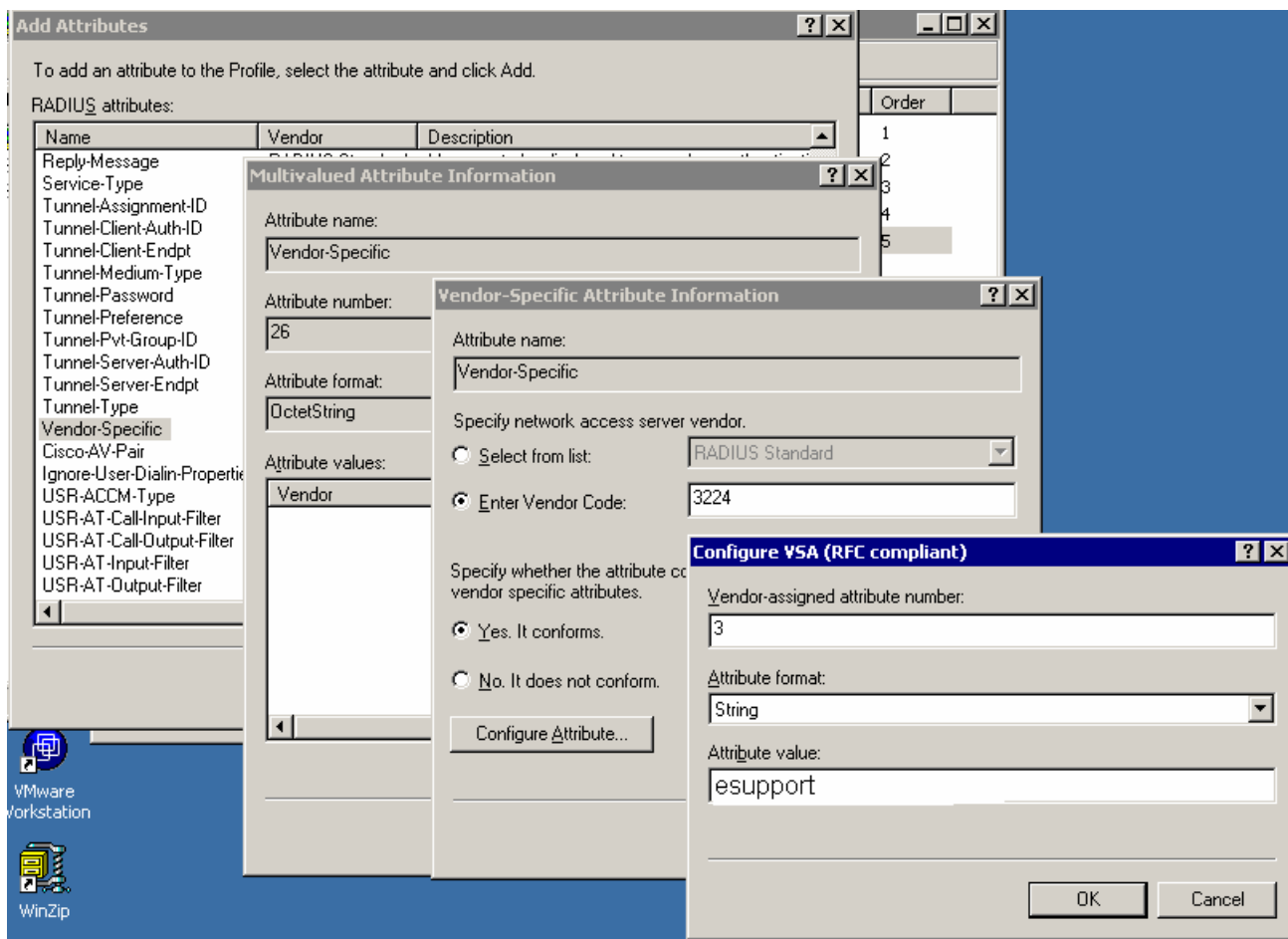


NOTE: For Framed-Protocol and Service-Type as shown on the *Advanced Dial-in Profile* property are not required.

Click the *Add* button to add the NetScreen VSA's. A list will appear, select *Vendor Specific* and click *Add*

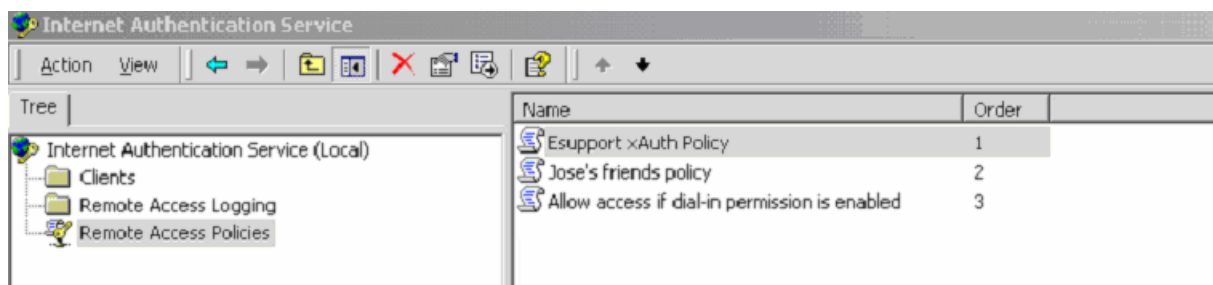


Select *Enter Vendor Code* and input 3224 (NetScreen's IETF Code) and make sure you select *Yes, it does confirm* and click *Configure Attribute*.



Enter the appropriate attribute value. The objective of this application is to use User group for xAuth and Firewall Authentication. Enter “3” for user group definition. The attribute value must match the external group definition on Netscreen Firewall. In this case is “**esupport**.” Continue to Click on OK and Finished.

Like all Access lists, ordering of the Remote Access Policies are extremely important. An access policy can contain multiple Netscreen specific attributes. To add additional access policies, simply repeat the above steps to create desired policies. In this case, Esupport xAuth Policy is in first order position, which takes precedence above all other access policies.



Section 5: Configuring Netscreen for xAuth and Firewall Authentication

1. Adding Authentication Server

On Netscreen WebUI, click on **Configuration > Auth > Servers > New**, enter name for new auth server. Enter the IP address of the Radius servers (Microsoft IAS). Select “Auth” and “xAuth” for account type. Enter Radius shared secret and click OK to complete adding new auth server.

The screenshot shows the 'Edit' configuration page for an authentication server in the Netscreen WebUI. The breadcrumb trail is 'Configuration > Auth > Auth Servers > Edit'. The page title is 'ns50'. The left sidebar shows the navigation menu with 'Auth' selected. The main content area contains the following fields and options:

- Name:** Microsoft
- IP/Domain Name:** 30.30.30.250
- Backup1:** (empty)
- Backup2:** (empty)
- Timeout:** 10 (0 to disable)
- Account Type:** Auth, L2TP, Admin, XAuth
- RADIUS:** RADIUS. Fields: Radius port (1645), Shared Secret (*****)
- SecurID:** SecurID. Fields: Client Retries (3), Client Timeout (5) seconds, Authentication Port (5500). Encryption Type: DES, SDI. Use Duress: Yes, No
- LDAP:** LDAP. Fields: LDAP Port (389), Common Name Identifier (cn), Distinguished Name(dn) (empty)

Buttons for 'OK' and 'Cancel' are at the bottom right.

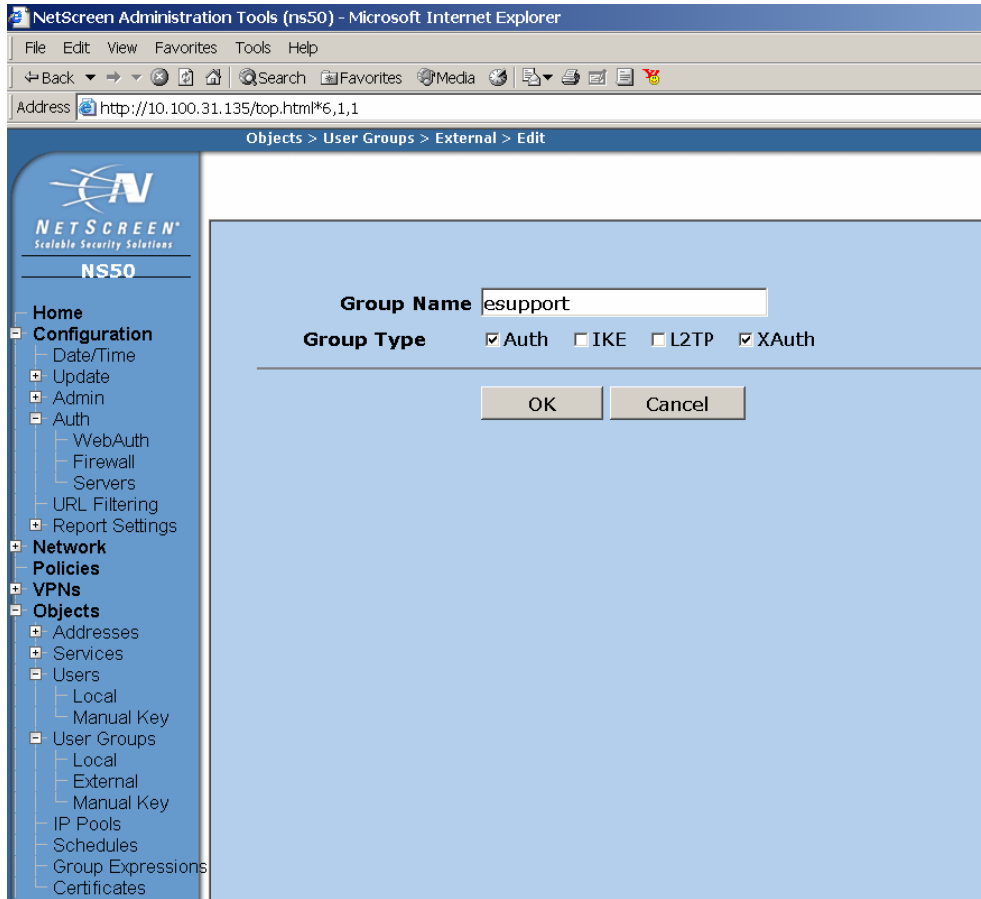
The illustration below shows the newly added Microsoft Radius Server.

	ID	Name	Server IP/Name	Type	Acct Type	Configure
	0	Local	Local	Local	admin auth l2tp xauth	Edit -
*	1	Microsoft	30.30.30.250	RADIUS	auth xauth	- -

* - Auth server is in use

2. Adding External User Group

On Netscreen WebUI, click on **Object > User Groups > External > New**, enter Group name “esupport” and select **Auth** and **xAuth** as Group type.



Group Name	Group Type	Configure	
esupport	Auth XAuth	Edit	Remove

3. Adding IP Pool

Select **Objects > IP Pools > New**, enter IP Pool Name "ippool." Input Start IP and End IP. Note that the IP Pool must be different from the subnet of trust and untrust networks. In our lab, we have defined a range of 10 IPs, starting from 60.60.60.1 to 60.60.60.10. This IP Pool will be used to assign to the Remote Dialup VPN user upon successful xAuth Authentication.

4. Defining xAuth Settings

Click on **VPNs > Autokey Advanced > xAuth settings**. Select "**Microsoft**" as the *Default Authentication Server* and "**ippool**" as *xAuth IP Pool*. Enter *DNS Primary/Secondary Server IP* and *WINS Primary/Secondary IP* if need to relay to Remote VPN Users.

The screenshot shows the configuration page for xAuth Settings in the Netscreen NS50 management console. The breadcrumb trail at the top reads "VPNs > Autokey Advanced > XAuth Settings". On the left is a navigation tree with categories: Auth, Network, Policies, VPNs, Manual Key, L2TP, Objects, and Certificates. The main content area is divided into sections:

- Reserve Private IP for XAuth User:** A text input field containing "5" followed by "Minutes".
- Default Authentication Server:** A dropdown menu set to "Microsoft".
- Query Client Settings on Default Server:** A checkbox that is unchecked.
- CHAP:** A checkbox that is unchecked.
- IP Pool Name:** A dropdown menu set to "ippool".
- DNS Primary Server IP:** A text input field containing "198.6.1.146".
- DNS Secondary Server IP:** A text input field containing "0.0.0.0".
- WINS Primary Server IP:** A text input field containing "0.0.0.0".
- WINS Secondary Server IP:** A text input field containing "0.0.0.0".

At the bottom right of the configuration area are two buttons: "Apply" and "Cancel".

5. Adding IKE User

Click on **Objects > Users > Local > New**, Enter *test1*. Select **IKE User** and **Simple Identity**. On the *IKE Identity*, enter test1@netscreen.com as the identity. The following steps are not required since the purpose of IKE User creation is for Phase 1 Negotiation only.

Select "**Authentication User**" and "**xAuth User**" and enter password. Choose "**ippool**" from the drop-down list of IP Pool on L2TP/xAUTH Remote Settings. Click **OK** to complete the user creation.

Objects > Users > Local > Edit

Auth/IKE/L2TP/XAuth User

User Name: test1 User Group: xauth user

Status: Enable Disable

IKE User Number of Multiple Logins with Same ID: 1

Simple Identity

IKE ID Type: AUTO IKE Identity: test1@netscreen.com

Use Distinguished Name For ID

Authentication User User Password: ****

XAuth User Confirm Password: ****

L2TP User

L2TP/XAuth Remote Settings (Remote IP: 0.0.0.0)

IP Pool: ippool Static IP: 0.0.0.0

Primary DNS IP: 0.0.0.0 Primary WINS IP: 0.0.0.0

Secondary DNS IP: 0.0.0.0 Secondary WINS IP: 0.0.0.0

OK Cancel

Name	Type	Group	Status	Identity	Configure
test1	Auth,IKE,XAuth	xauth user	Enabled	test1@netscreen.com	In Use

6. Adding IKE User Group

Click on **Objects > User Groups > Local > New**, enter a New Group Name "xauth user" and elect test1 as the member of the user group. This user group will be used for Remote Dialup VPN.

Objects > User Groups > Local > Edit

Group Name xauth user

<-- Group Members -->

test1

<-- Available Members -->

<< >>

OK Cancel

Group Name	Group type	Members	Configure
xauth user	auth ike xauth	test1	Edit

7. Creating Phase 1 IKE Gateway

Click on **VPNs > Autokey Advanced > Gateway > New**, enter Gateway Name “P1 xAuth.” Select “Dialup User Group – xauth user” and input “Preshared Key.” In our example, we used **Netscreen**. Click on “Advanced” to continue with Phase 1 Proposal Setting.

The screenshot shows a configuration dialog for creating a new IKE gateway. The 'Gateway Name' field contains 'P1 xAuth'. Under 'Security Level', the 'Custom' radio button is selected. The 'Remote Gateway Type' section has 'Dialup User Group' selected, with 'IP Address/Hostname', 'Peer ID', 'User' (set to 'None'), and 'Group' (set to 'xauth user') fields. The 'Preshared Key' field is filled with asterisks. The 'Local ID' field is empty with '(optional)' text. The 'Outgoing Interface' is set to 'ethernet3'. At the bottom are 'OK', 'Cancel', and 'Advanced' buttons.

In this lab, we use **pre-g2-3des-sha** as our Phase 1 Proposal. Make sure to select “Aggressive” mode. Check “Enable xAuth” and select “External Authentication” to use with “User Group – esupport.” If you are behind a NAT device, select Enable NAT-Traversal. Press *Return* and click on **OK** to complete the Phase 1 creation.

The screenshot shows the 'Phase 1 Proposal' configuration dialog. Under 'Security Level', 'Predefined' is selected with 'Standard', 'Compatible', and 'Basic' options. Under 'User Defined', 'Custom' is selected. The 'Phase 1 Proposal' section has two dropdown menus: the first is set to 'pre-g2-3des-sha' and the second to 'none'. The 'Mode (Initiator)' section has 'Aggressive' selected. There are checkboxes for 'Enable NAT-Traversal' and 'Enable XAuth'. The 'UDP Checksum' checkbox is unchecked. The 'Keepalive Frequency' is set to '0' seconds. The 'Heartbeat' section has 'Hello' set to '0' seconds, 'Reconnect' set to '0' seconds, and 'Threshold' set to '5'. Under 'Enable XAuth', 'Local Authentication' is selected with 'Allow Any' chosen. Under 'External Authentication', 'Microsoft' is selected in the dropdown, and 'Query Remote Setting' is unchecked. The 'Name' field is set to 'esupport'. There is also a 'CHAP' checkbox at the bottom.

Use Distinguished Name for Peer ID

CN

OU

Organization

Location

State

Country

8. Adding Phase 2 VPN

Click on **VPNs > Autokey IKE > New**, enter VPN name “*P2 xAuth*.”
 Select “*P1 xAuth*” as the Predefined Remote Gateway and click on *Advanced* to continue on Phase 2 Proposal Configuration.

VPN Name

Security Level Standard Compatible Basic Custom

Remote Gateway Predefined Create a Simple Gateway

Gateway Name

Type Static IP Dynamic IP Dialup User Dialup Group

Address/Hostname

Peer ID

User

Group

Local ID (optional)

Preshared Key

Security Level Standard Compatible Basic

Outgoing Interface

OK Cancel Advanced

G2-esp-3des-sha is used as Phase 2 Proposal in our example. Press *Return* to the previous page and Click on “*OK*” to complete the Phase 2 creation.

Security Level

Predefined
 Standard
 Compatible
 Basic
 User Defined
 Custom

Phase 2 Proposal

g2-esp-3des-sha	none
none	none

Replay Protection
 Transport Mode (For L2TP-over-IPSec only)

Bind to
 None
 Tunnel Interface none
 Tunnel Zone Untrust-Tun

Proxy-ID
Local IP / Netmask 0.0.0.0 /
Remote IP / Netmask 0.0.0.0 /
Service ANY

VPN Group None Weight 0

VPN Monitor
Source Interface default
Destination IP 0.0.0.0
 Rekey

9. **Creating Bi-Directional Remote Dialup VPN Policies** (Required ScreenOS 4.0.2 and above)

Click on **Policies > Select "From Untrust to Trust" > New**.

Select "Dialup VPN" as the *Source address* and "Sue 30.30.30.0/24" as the *Destination Address*. Choose "Tunnel" as Action and Select "P2 xAuth" as Tunnel VPN. Make sure to Check on "**Modify matching bidirectional VPN Policy**". This will allow two-way VPN traffic between Remote Dialup VPN user and the trust network. Click on *Advanced* to continue on next window.

Name (optional)

Source Address

New Address /

Address Book

Destination Address

New Address /

Address Book

Service

Action

Tunnel VPN

Modify matching bidirectional VPN policy

L2TP

10. Configuring Firewall Authentication

On Advanced Policy Settings, Check on **"Authentication."** Select *Microsoft* as the Auth Server. On User Group, select **External Auth Group – esupport**. Click on **"Return"** and **OK** to complete the policy configuration.

Advanced Policy Settings

NAT

DIP Off Fix-Port

DIP On

Authentication

Auth Server Use Default

WebAuth Use

User Group

User External User

Group Expression

HA Session Backup

Logging

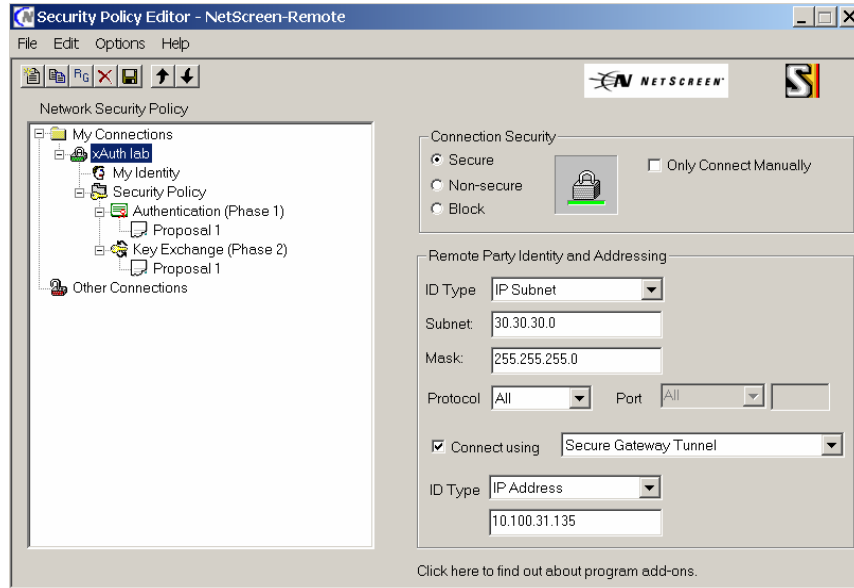
Counting

Alarm Threshold Bytes/Sec KBytes/Min

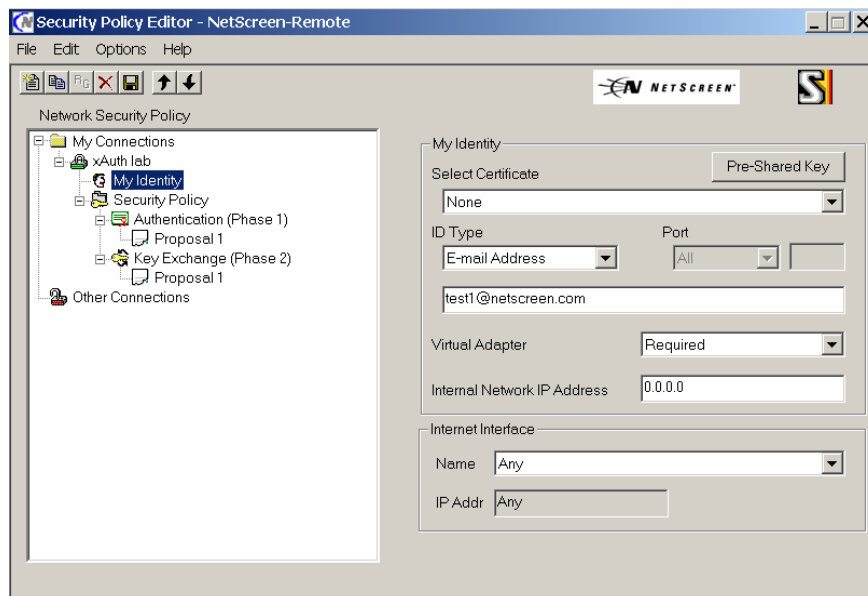
Schedule

Section 6: Configuring Netscreen Remote Client for xAuth and Firewall Authentication

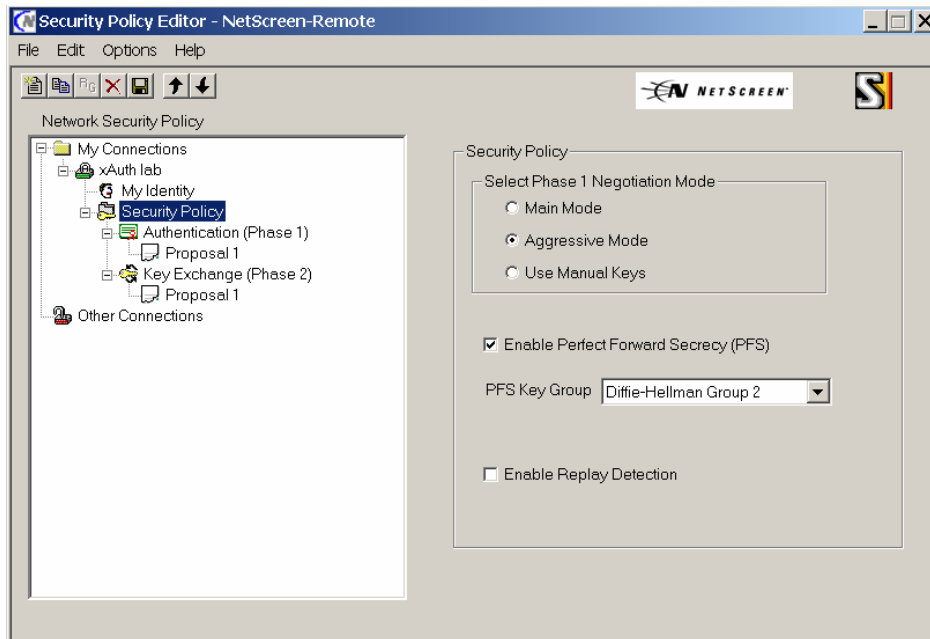
- Create a new connection. In this lab, we named it “xAuth lab.” Select “Secure” for the Connection Security.
- Choose “IP Subnet” for **Remote Party Identity and Addressing**. Enter the IP subnet of the Remote Trust Network; for example, subnet: 30.30.30.0; Mask: 255.255.255.0.
- Click on **Connect using Secure Gateway Tunnel** and use “IP Address” as ID type.
- Enter IP of **Remote IKE Gateway** – “10.100.31.135.”



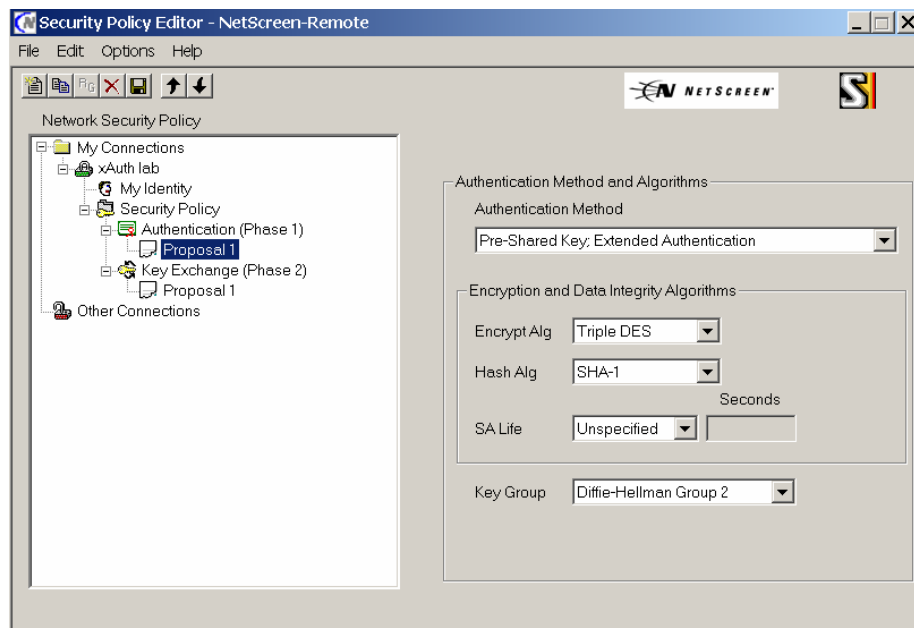
- Under “My Identity,” enter “Netscreen” as the **Pre-Shared Key**.
- Select “**Email Address**” as the local ID Type and enter IKE ID “test1@netscreen.com.”
- Make sure to select “**Required**” for Virtual Adapter. This will enable the Remote Client to receive an IP assignment from the xAuth IP Pool.



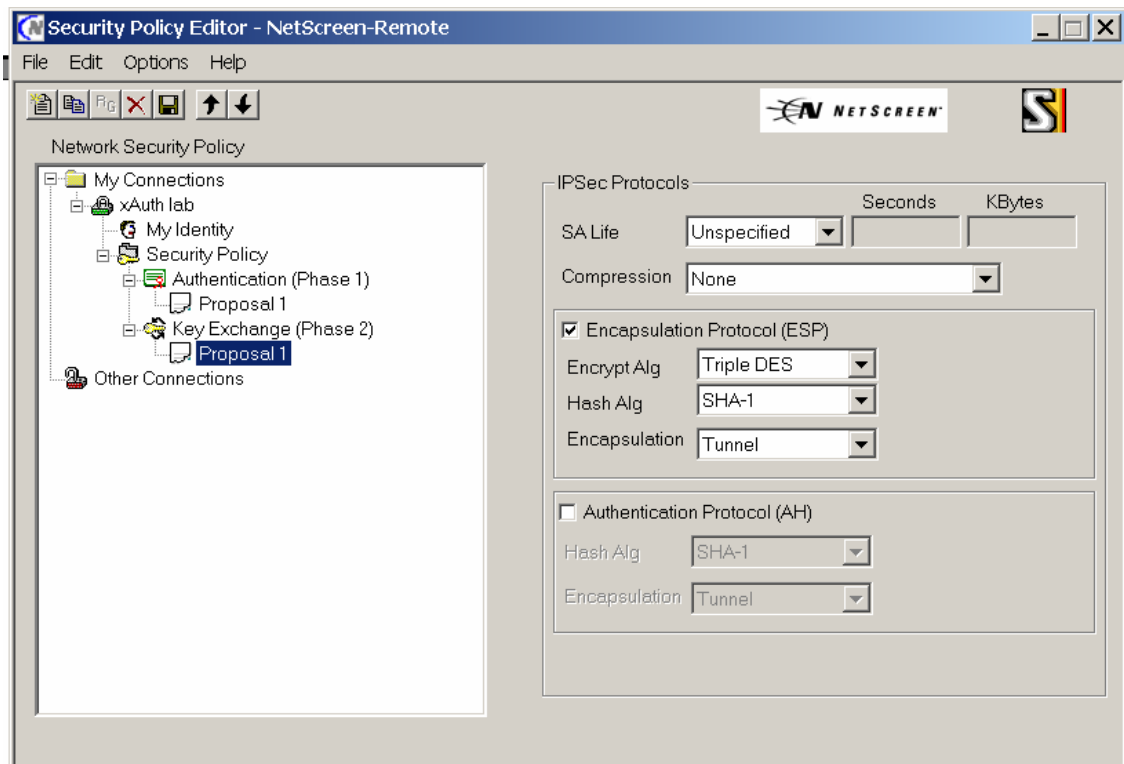
- Select “**Aggressive mode**” for *Phase 1 Negotiation mode*.
- Check on “**Enable Perfect Forward Secrecy (PFS)**” and select “**Diffie-Hellman Group 2**” as the PFS Key Group to correspond with Phase 1 Proposal configured on Netscreen Device.
- Uncheck “**Enable Replay Detection.**”



- Since xAuth is key objective we have emphasized on this lab, *Extended Authentication* needs to be enabled on the NS Remote Client.
- Select “**Pre-Shared Key, Extended Authentication**” as the *Authentication Method*.
- Chose “**Triple DES – SHA-1 and Diffie-Hellman Group2**” for Phase 1 *Encryption and Data Integrity Algorithms*.



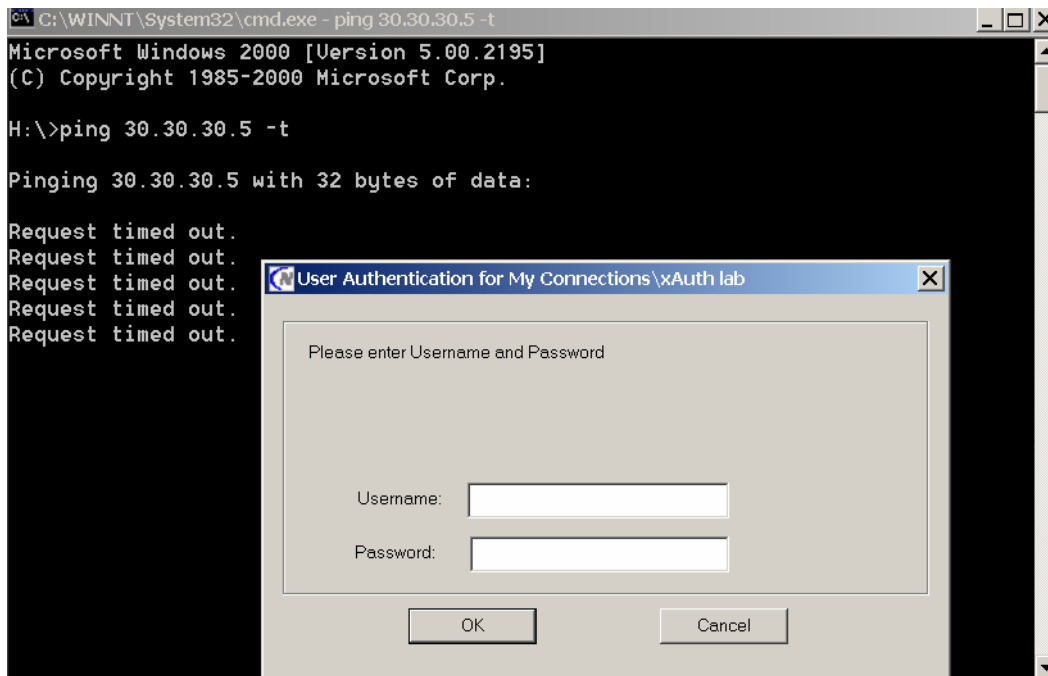
- Under Key Exchange (Phase 2) Proposal 1, check “**Encapsulation Protocol (ESP) and select “Triple DES – SHA-1 – Tunnel.**
- Make sure “*Authentication Protocol (AH)* is not checked.
- Click on File > Save to save the new configuration.



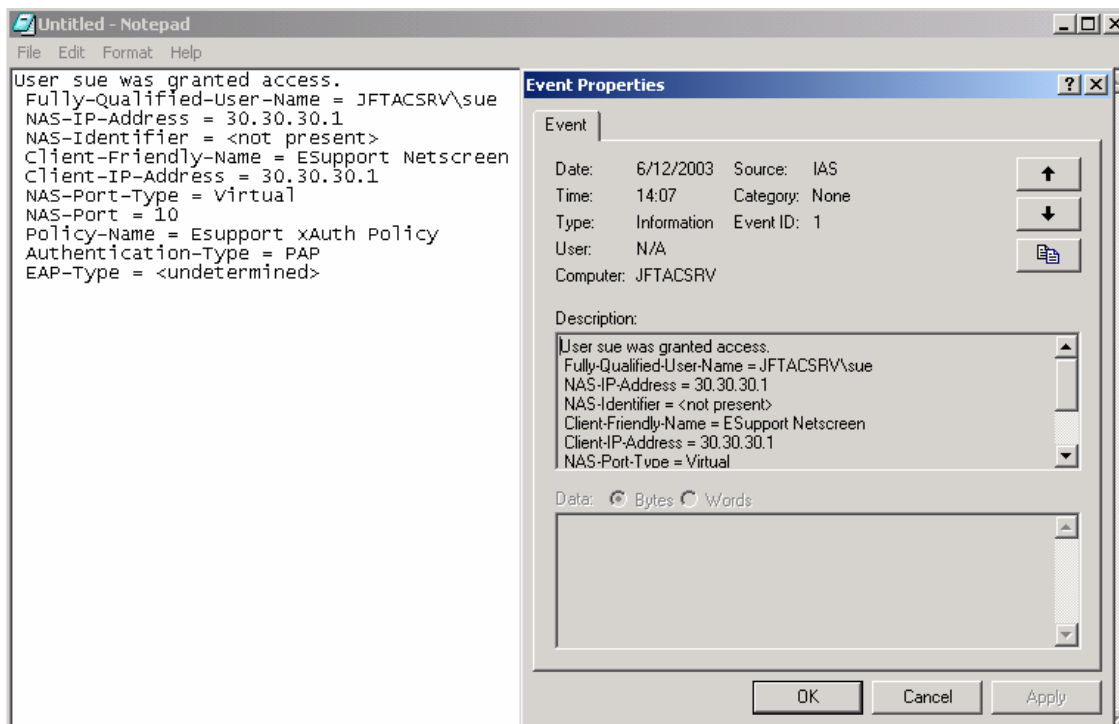
Section 7: Testing and Verifying Authentication and Bi-Directional VPN Connection

As proposed on Section 2, the Phase 1 negotiation is initiated by a ping request from the Netscreen Remote to the domain workstation (30.30.30.5) on JFTACSRV domain.

A login window will pop up for the xAuth user Authentication. The Remote User needs to enter the domain username and password to be authenticated by Microsoft IAS resides on Domain controller (30.30.30.250).

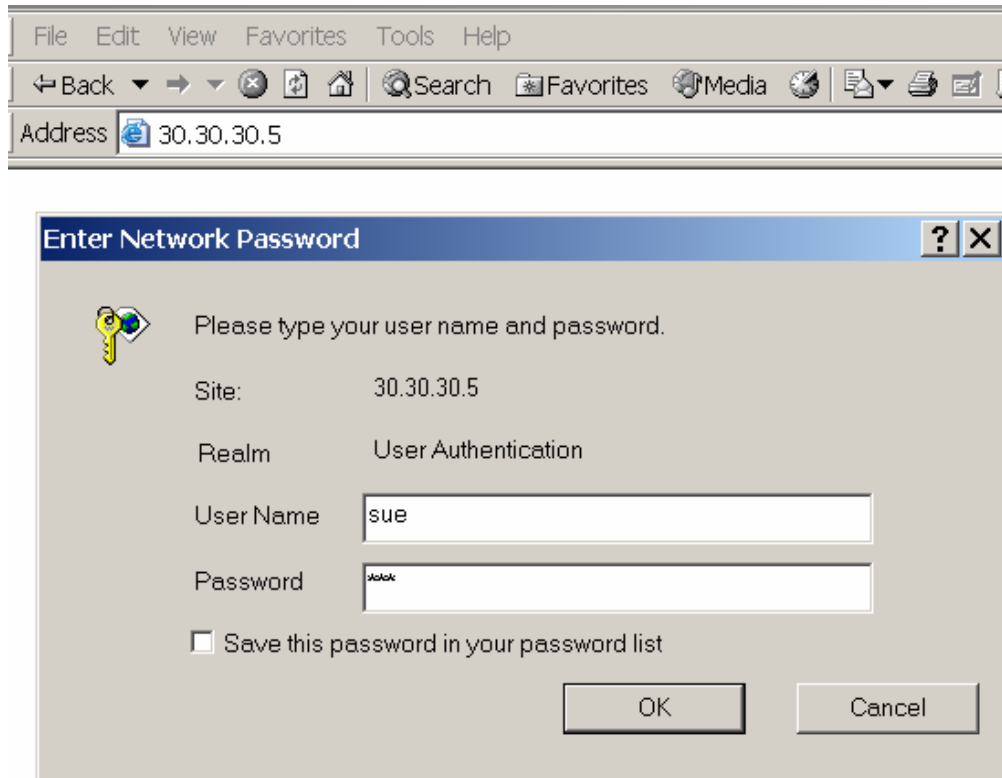


The authentication attempt can be observed from the Windows Event View as illustrated. The following Event Log showed that Domain User “sue,” a member of esupport group, is successfully authenticated by the Microsoft IAS Server and was granted access by matching the Windows Remote Access Policy of “*Esupport xAuth policy.*” The Authentication type is *PAP.*



The Firewall Authentication is implemented to reinforce an extra layer of network security. Upon the successful xAuth authentication, the Remote user needs to launch a HTTP session to access the domain workstation (30.30.30.5) in order to invoke the Firewall Authentication.

In this lab, we delegated Microsoft IAS for both xAuth and Firewall User Authentication. The Remote user will enter domain username and password to login for Firewall Authentication.



To further exam the IP Configuration on the Remote VPN Client, use Windows DOS Command: ipconfig /all to check the IP assignment

```
Windows 2000 IP Configuration

Host Name . . . . . : 5B0F321-2333
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . :
    Description . . . . . : 3Com 3C920 Integrated Fast Ethernet
Controller (3C905C-TX Compatible) #2
    Physical Address. . . . . : 00-B0-D0-10-FA-EE
    DHCP Enabled. . . . . : No
    IP Address. . . . . : 10.100.31.131
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.100.31.1
    DNS Servers . . . . . : 10.100.3.140
                            198.6.1.4
    Primary WINS Server . . . . . : 10.100.3.110
    Secondary WINS Server . . . . . : 10.100.3.100

Ethernet adapter Local Area Connection:

    Media State . . . . . : Cable Disconnected
    Description . . . . . : 3Com 3C920 Integrated Fast Ethernet
Controller (3C905C-TX Compatible)
    Physical Address. . . . . : 00-08-74-96-D3-CE

PPP adapter SafeNet Virtual Adapter Interface:

    Connection-specific DNS Suffix  . :
    Description . . . . . : WAN (PPP/SLIP) Interface
    Physical Address. . . . . : 00-53-45-00-00-00
    DHCP Enabled. . . . . : No
    IP Address. . . . . : 60.60.60.1
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :
    DNS Servers . . . . . : 198.6.1.146
```

As shown above, IP address of 60.60.60.1, the first IP address of the xAuth IP Pool was assigned to the Remote VPN user. DNS Servers IP 198.6.1.146 was also relayed to this client.

From the CLI, we can verify the active xAuth user by using “get xauth active” command. The Gateway Name, login username, Authentication Server, Remote Gateway IP, IP assignment and Login time can be reviewed with this command.

```
Select C:\WINNT\System32\telnet.exe
Remote Management Console
login: netscreen
password:
ns50-> get xauth active

GW Name      Login      Auth By    GW IP      Private IP  Last Login
P1 xAuth     sue       Microsoft  10.100.31.131  60.60.60.1  2003-06-12 14:27:18
```

The bi-directional VPN is enabled on the Remote Dialup VPN. The domain workstation can also ping the Remote VPN User by using the private IP address assigned from the xAuth IP Pool.

```
C:\WINNT\System32\cmd.exe - ping 60.60.60.1 -t
H:\>ping 60.60.60.1

Pinging 60.60.60.1 with 32 bytes of data:

Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128

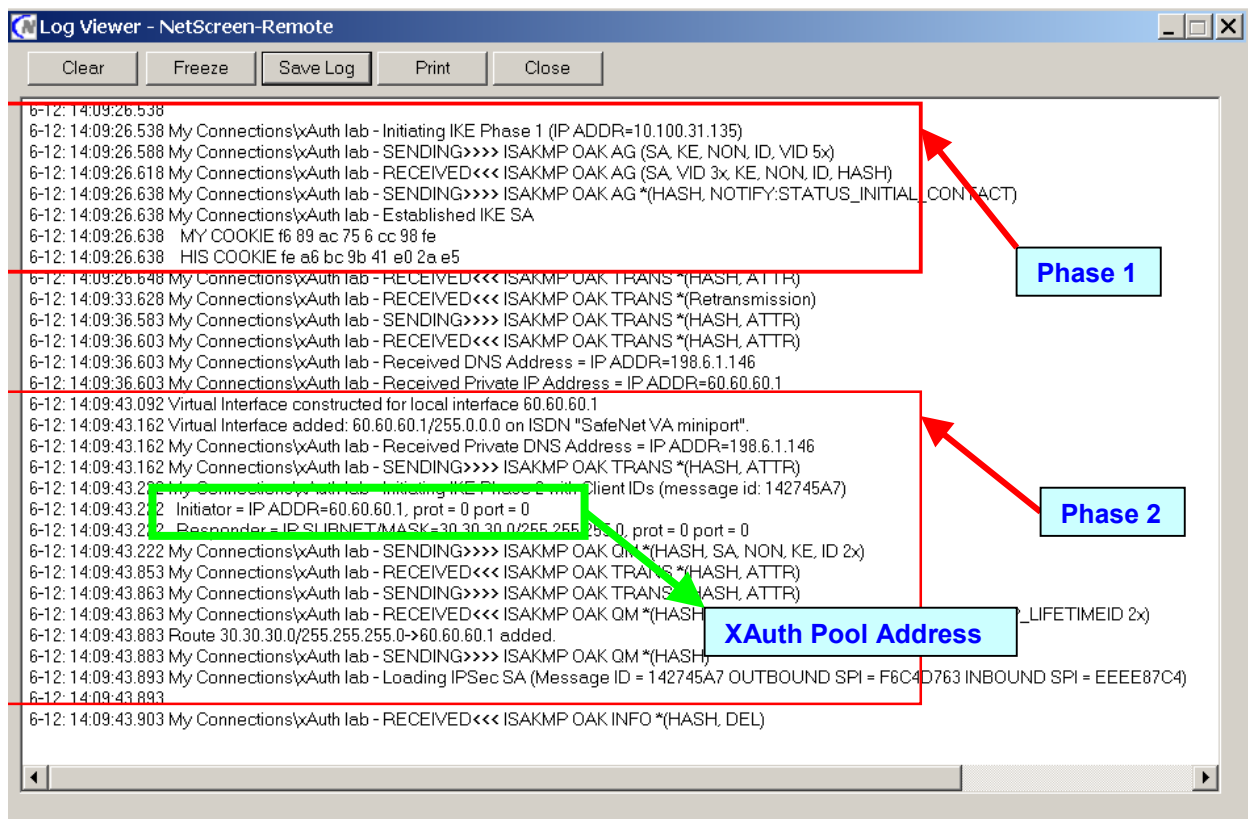
Ping statistics for 60.60.60.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

H:\>ping 60.60.60.1 -t

Pinging 60.60.60.1 with 32 bytes of data:

Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
Reply from 60.60.60.1: bytes=32 time<10ms TTL=128
```

Log Viewer on the Netscreen-Remote provides a source of VPN connection status verification. As highlighted below, the Phase 1 and Phase 2 were successfully negotiated and IP Address was received from the xAuth IP Pool.



Conclusion

Integration of Microsoft's Internet Authentication Service (IAS) and NetScreen network security appliances has provided a powerful user and device authentication. The centralized user database and access control allow Network Managers and administrators to manage network resources and security more efficiently and effectively. Saving on the man-hours of manual user configuration and database management is significantly improved by utilizing RADIUS as a primary authentication vehicle. Netscreen provides RADIUS feature support to meet with modern Network and Security professionals' needs. The use of xAuth and Firewall Authentication together with RADIUS provide a double-layer of network security solution to corporate enterprise at an optimal operational efforts and costs.

Appendix – CLI Example of Configuration

```

set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth-server "Microsoft" id 1
set auth-server "Microsoft" server-name "30.30.30.250"
set auth-server "Microsoft" account-type auth xauth
set auth-server "Microsoft" secret "netscreen"
set auth default auth server "Local"
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface ethernet1 ip 30.30.30.1/24
  
```

```

set interface ethernet1 nat
set interface ethernet3 ip 10.100.31.135/24
set interface ethernet3 route
set address "Trust" "Sue 30.30.30.0/24" 30.30.30.0 255.255.255.0
set ippool "ippool" 60.60.60.1 60.60.60.10
set user "test1" uid 1
set user "test1" ike-id u-fqdn "test1@netscreen.com" share-limit 10
set user "test1" type auth ike xauth
set user "test1" remote ippool "ippool"
set user "test1" password "test"
set user "test1" "enable"
set user-group "esupport" id 2
set user-group "esupport" location external
set user-group "esupport" type auth xauth
set user-group "xauth user" id 3
set user-group "xauth user" user "test1"
set ike gateway "P1 xAuth" dialup "xauth user" Aggr outgoing-interface
"ethernet3" preshare "netscreen" proposal "pre-g2-3des-sha"
unset ike gateway "P1 xAuth" nat-traversal
set ike gateway "P1 xAuth" xauth server "Microsoft" user-group "esupport"
set ike policy-checking
set vpn "P2 xAuth" id 7 gateway "P1 xAuth" no-replay tunnel idletime 0
proposal "g2-esp-3des-sha"
set ike id-mode subnet
set xauth lifetime 5
set xauth default ippool "ippool"
set xauth default dns1 198.6.1.146
set xauth default auth server Microsoft
set policy id 3 from "Trust" to "Untrust" "Sue 30.30.30.0/24" "Dial-Up VPN"
"ANY" Tunnel vpn "P2 xAuth" id 11 pair-policy 2 Auth server "Microsoft" user-
group "esupport"
set policy id 2 from "Untrust" to "Trust" "Dial-Up VPN" "Sue 30.30.30.0/24"
"ANY" Tunnel vpn "P2 xAuth" id 11 pair-policy 3 Auth server "Microsoft" user-
group "esupport"

```