Configuring RADIUS Authentication for VPN Client Authentication

Introduction

The use of AAA services (Authentication, Authorization, and Accounting) allows for several methods of controlling and recording access to AOS-based devices. The two methods of achieving this result involve either RADIUS or TACACS+ servers. This guide will specifically cover the use of controlling VPN client access using RADIUS authentication, using the Extended Authentication (XAUTH) function within IPSEC.

Command Line Configuration

Enabling the Service & Defining a Server

AOS-based devices require that the AAA process be enabled and that at least one RADIUS server is defined. The AOS device and the RADIUS server being accessed must agree on the Pre-Shared Key for the process to operate successfully; the key is used to encrypt the password portion of the RADIUS authentication request message. The configuration is as such:

```
aaa on
!
radius-server host <RADIUS Server IP> key <Pre-Shared Key>
```

NOTE: *Working with multiple AAA servers is covered under a different document.*

Define Authentication Methods

The next step is to define the desired VPN Client Authentication method. Currently only authentication to a RADIUS server or the Local-User List is supported.

The lists define the order of operations for authentication. The primary method will only fail over to the next defined method if the previous method is unavailable. For instance, if

the RADIUS server is specified first and then the Local-User List, the Local-User List will only be consulted if the RADIUS server does not respond to RADIUS request messages. If the RADIUS server rejects the user credentials, the user will be denied access and the Local-User List will not be consulted.

If there are no valid methods left in a given list, then the user will be denied access. An example is if only the RADIUS server is defined within the list, and the RADIUS server cannot be contacted for any reason; user login will not be possible because there are no longer any valid methods within the list. For this reason, it is always recommended to end every list with the Local-User List so the device can still be accessed if communication with the RADIUS server is interrupted because the Local-User List will never be unavailable.

The following example will apply to a named list the authentication method as RADIUS authentication first and the Local-User List second in the event RADIUS communication fails.

```
aaa authentication login LoginUseRadiusLocal group radius local
```

Apply Authentication Method to the VPN IKE Policy

The next step is to apply the defined named authentication method list to the VPN IKE policy. If this policy is used for non-client dynamic router-router VPN tunnels, it is important that the option *'no-xauth'* be applied to that neighbor's *'crypto ike remote-id'* statement. If this step is not taken, the router will request authentication from the peer router, which it most likely does not have the capability to provide, and that VPN tunnel could be rendered inoperable.

NOTE: *Unless a specific reasoning is merited, this configuration will be applied to the 'peer any' IKE policy, which is typically what the VPN clients will connect under.*

NOTE: *Only the AAA-relevant configuration is shown here. For the full VPN client configuration, please refer to other documents.*

```
crypto ike policy 100
  peer any
  client authentication server list LoginUseRadiusLocal
```

Enable XAUTH on the VPN Client Remote-IDs

To enable the use of the XAUTH process, it must not be disabled on the VPN client remote-ID command. It is stated "must not be disabled" rather than "must be enabled" because the relevant command to enable or disable it is only used when it is to be disabled. The sub-command in question is *'no-xauth'*, and it is appended at the end of the remote-ID statement when used. An example remote-ID statement with the XAUTH process both disabled and enabled, respectively, is:

```
crypto ike remote-id user-fqdn AdtranVPNClient preshared-key
     adtran ike-policy 100 crypto map VPN 10 no-xauth
!
crypto ike remote-id user-fqdn AdtranVPNClient preshared-key
     adtran ike-policy 100 crypto map VPN 10
```

NOTE: *In most cases, the VPN client configuration will already be in place, and the XAUTH portion is being added to enhance security. In these cases, the remote-ID statement needs to be removed and then re-added without the 'no-xauth' sub-command.*

Web Interface Configuration

This section will define the methods for configuring this functionality through the GUI. The technology definitions and explanations will not be repeated; please refer to the relevant command line configuration section for more information.

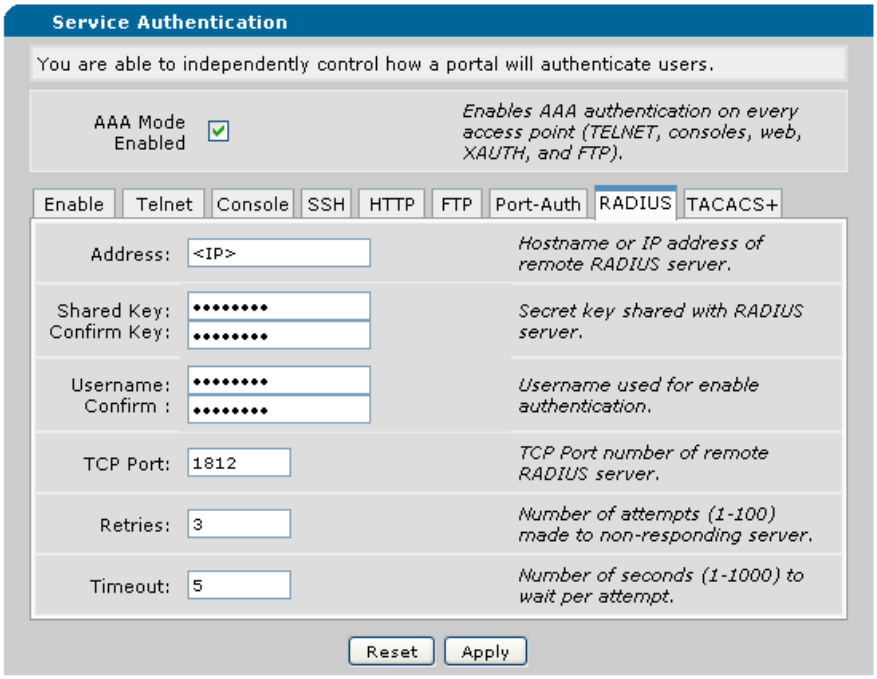
The AAA configuration is accomplished from the "System → Passwords" page, in the bottom section entitled "Service Authentication".

NOTE: *The functionality allowed by the GUI is limited in that it allows for only one method to be defined, and it uses pre-defined names for its authentication lists. This means that it is not possible to have the Local-User List as a fallback position should the RADIUS server be unavailable. For this reason, CLI configuration is recommended.*

Enabling the Service, Defining a Server, & the Enable Username

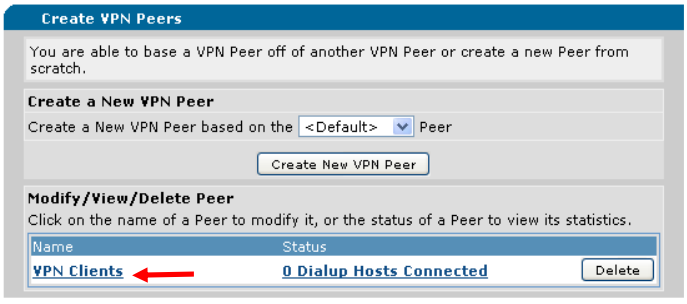
The “AAA Mode Enabled” checkbox must be checked and the RADIUS server defined with a Pre-Shared Key, as shown:

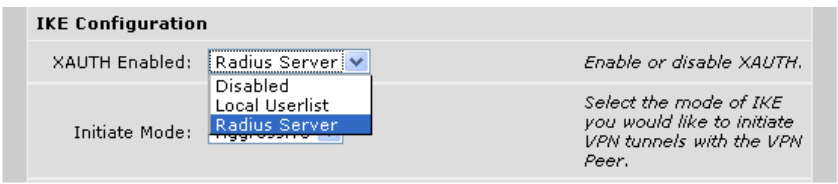
NOTE: *The Enable Username is not required for VPN Client Authentication.*



Define & Apply Authentication Methods

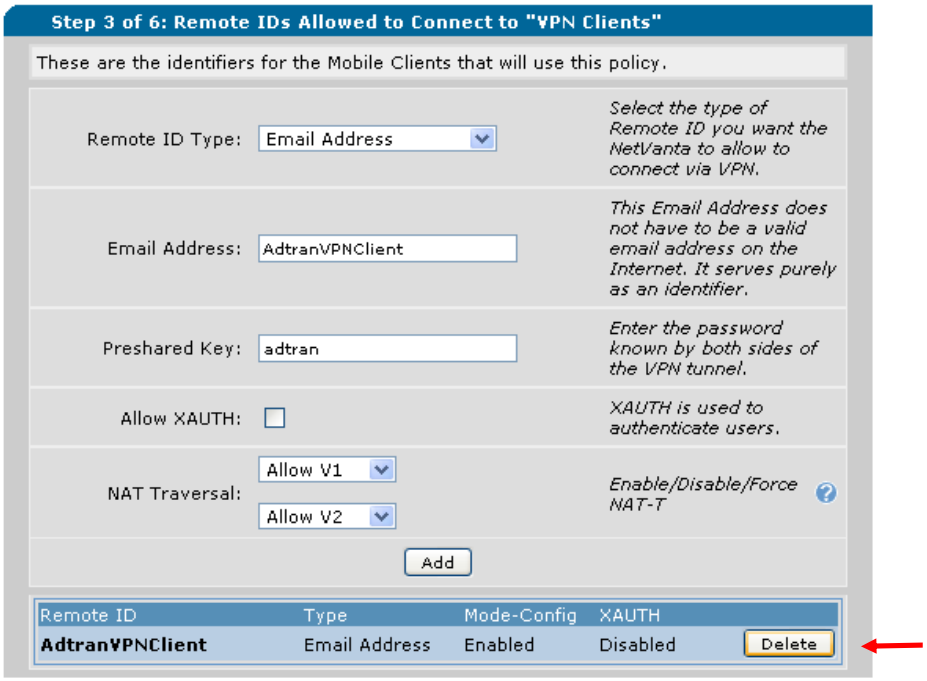
The Authentication method is applied under the “VPN Peers → <Peer Name>” page, as shown:



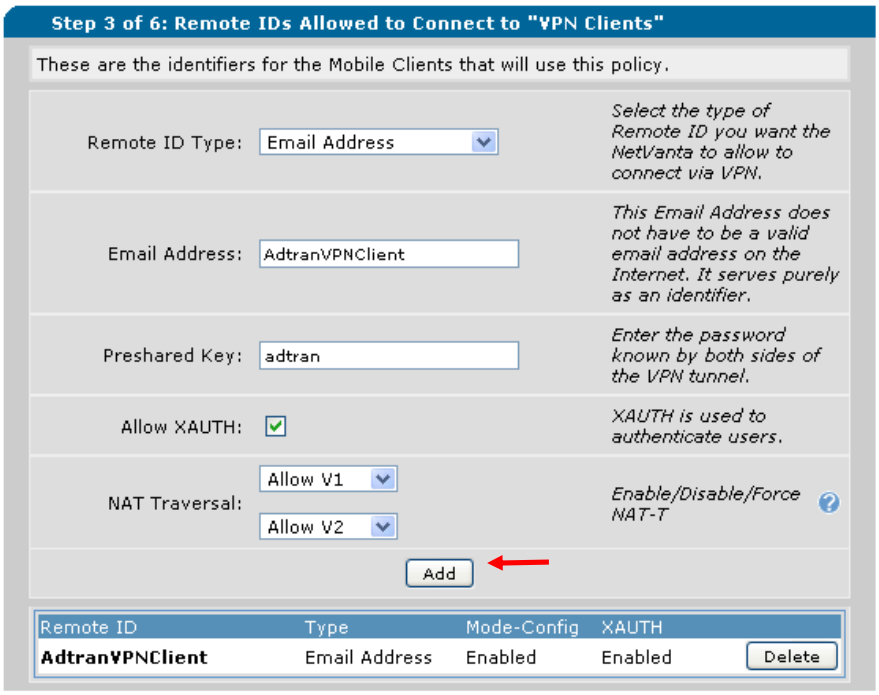


Enable XAUTH on the VPN Client Remote-IDs

The XAUTH parameter is also applied under the “VPN Peers → <Peer Name>” page. Existing remote-IDs can be removed using the following method:



New and replacement remote-IDs can be added using the following method:



Configuring the RADIUS Server

This section will define the relevant portions of the RADIUS message that the server should be looking for, and use the IAS function of a Windows 2003 Server as an example.

RADIUS Attribute Value Pairs (AVPs)

The RADIUS authentication request will contain several Attribute Value Pairs (AVPs) that facilitate the required functions of authentication. They allow the authentication method defined within the RADIUS server to be specific enough to match only on traffic from this client (or class of clients). If the RADIUS server supports logging at high level of verbosity, they contain information about where the client is originating from for logging purposes. The AVPs that the device will send are:

- Username
  - Contains the unencrypted username attempting to authenticate.
- User-Password
  - Contains the encrypted password associated with this authentication attempt.
  - Encrypted using the Pre-Shared Key
- NAS-Port
  - Set to "0".
- Calling-Station-Id
  - Set to "XAUTH 100".
- Service-Type
  - Set to "Login-User"
- NAS-IP-Address
  - Indicates the primary IP of the interface that the RADIUS request packet is sourced from.

Configuring the RADIUS Server

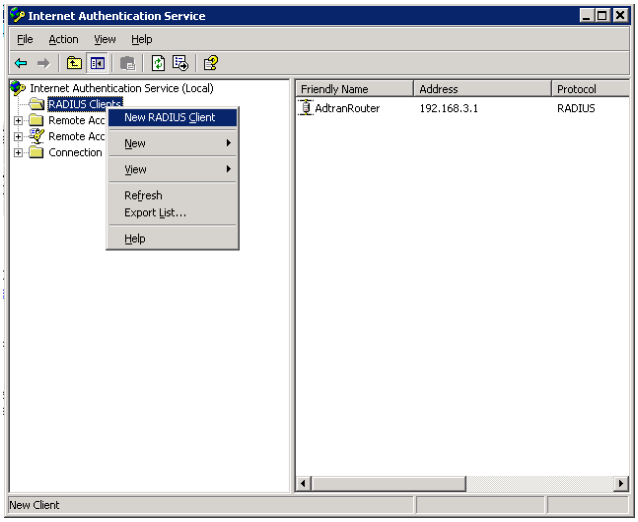
The RADIUS server, using Windows Server 2003's IAS as an example, can specify multiple dependencies that must match before a particular policy is allowed to be used to authenticate a request. It is recommended that these be used to protect the RADIUS server from client authentication requests from unauthorized sources, or to ensure that each RADIUS client has the correct policy applied to it if there are multiple devices sending authentication requests. Examples of such client groups are Device Administrators, Wireless Clients, Port-Authentication, and VPN Clients.

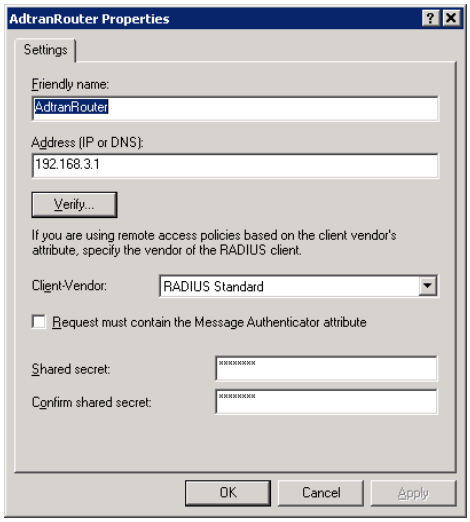
NOTE: *Windows IAS functionality and configuration style may change. The procedures described within this document are only used as an example. ADTRAN is not responsible for configuring the RADIUS server, and will not support the RADIUS server should it be found to be the source of any errors in the authentication process. This article will only*

cover the Netvanta-specific configuration options within IAS; there may be further configuration on the server required to utilize IAS in this manner.

For further information, please refer to the Microsoft KB article on IAS, which can be accessed here: http://technet.microsoft.com/en-us/library/cc738432(WS.10).aspx

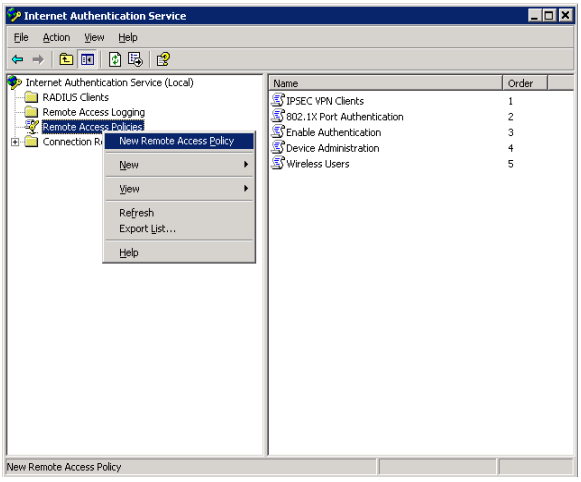
The first step to be completed in most RADIUS servers is to define the RADIUS client device, which involves specifying the Pre-Shared Key and the IP address it will be coming from. This will allow the RADIUS server to receive messages from this RADIUS client. In IAS, it is done in the following manner:

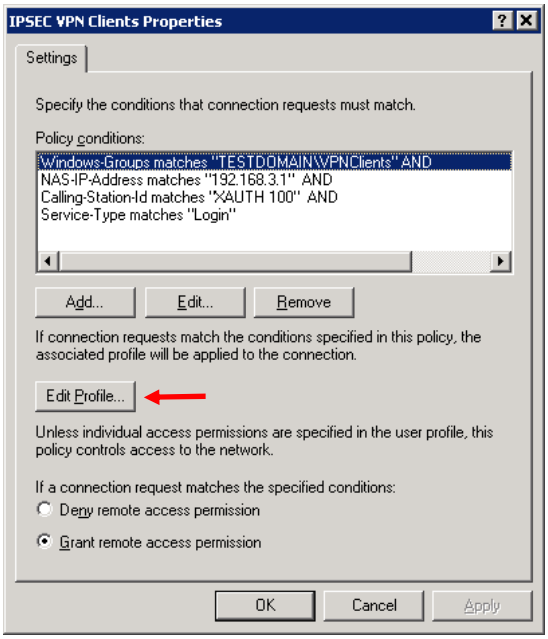


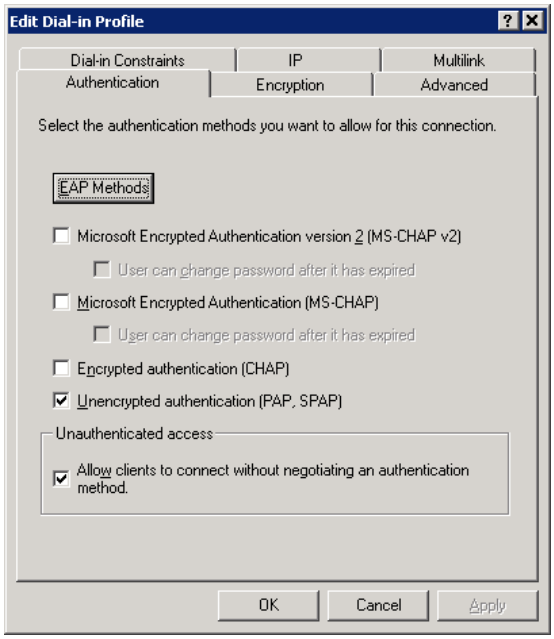


The next step is to create the policy that will process the request, ensure that it matches the required AVPs for this connection type, and permit or deny the request.

The RADIUS server will need to define the AVPs that will remain static within all authentication attempts from this RADIUS client & change the authentication process to allow PAP authentication without negotiation. In IAS, it is done in the following manner:







Troubleshooting

This section will describe the relevant debug procedures involved when determining any issues with the AAA, RADIUS, or XAUTH configuration. The commands that will be used are:

- debug aaa
- debug radius
- debug crypto ike client authentication

A successful authentication attempt would be similar to the following:

```
AAA: New Session on portal 'XAUTH 100'.
AAA: Session using AUTHENTICATION list 'LoginUseRadiusLocal'.

2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XauthEDStartVpnMutexPath:
     Before State machine Fun execution  State: 0x0  Event : 0x0
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH    Attribs in
     ISAKMP_CFG_REQUEST:
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH  XAUTH_TYPE
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH    XAUTH_USER_NAME
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH    XAUTH_USER_PASSWORD
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     AttribSize= 12
```

```
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     GenHdrSize= 4
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     Attrib Payload Size:= 20
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     HashPayload Size: 24
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     Total Msg Size(before Encrypt):44
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     Total Msg Size(After Encrypt):48
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     Total Length of the packet with ISAKMP HDR:76
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH
     XauthSendMsgVpnMutexPath:Total Packet Length:76
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XauthTransactionStart: SENT
     OUT ISAKMP_CFG_REQUEST MESSAGE ....
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XauthEDStartVpnMutexPath:
     After State machine Fun execution State:  0x1  Event : 0x0
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
     Host Identifier : 10
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
     Peer Identifier: 10
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
     Before State machine Fun execution  State:  0x1  Event :
     0x1
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH    Attribs in
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH  ISAKMP_CFG_REPLY:
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XAUTH_TYPE
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XAUTH_USER_NAME
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XAUTH_PASSWORD
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH
2010.02.16 15:45:29 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
     After State machine Fun execution  State:  0x2  Event : 0x1

RADIUS AUTHENTICATION: Sending packet to <Server IP> (1812).
RADIUS AUTHENTICATION: Waiting on response from server
RADIUS AUTHENTICATION: Receiving from RADIUS socket
RADIUS AUTHENTICATION: Response received from server (<Server
     IP>)
RADIUS AUTHENTICATION: Received response from <Server IP>.
AAA: RADIUS authentication passed.

2010.02.16 15:45:30 CRYPTO_IKE.XAUTH
     XauthSessionValidationSucceeded: Validation Succeeded
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH XauthLBProcessData: Before
     State machine Fun execution  State: 0x2 Event : 0x2
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH    Attribs in
     ISAKMP_CFG_SET:
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH    XAUTH_STATUS
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
```

```
      AttribSize= 4
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      GenHdrSize= 4
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Attrib Payload Size:= 12
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      HashPayload Size: 24
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Total Msg Size(before Encrypt):36
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      ISAKMP_CFG_SET Message
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 0e
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 18
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 7a
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 9f
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 50
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 86
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 2a
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 55
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH f9
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 29
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH c7
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH d8
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 1c
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 9e
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 98
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 42
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH ae
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH d2
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 78
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 46
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 05
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH c6
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 0c
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 03
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 0a
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH c0
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 8f
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 00
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH 01
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Total Msg Size(After Encrypt):48
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
```

```
      Total Length of the packet with ISAKMP HDR:76
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH
      XauthSendMsgVpnMutexPath:Total Packet Length:76
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH SENT OUT ISAKMP_CFG_SET
      MESSAGE ....
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH XauthLBProcessData: After
      State machine Fun execution  State:  0x3  Event : 0x2
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      Host Identifier : 10
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      Peer Identifier: 10
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      Before State machine Fun execution  State:  0x3  Event :
      0x3
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH    Attribs in
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH  ISAKMP_CFG_ACK:
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH EDCallBackFun: Xauth
      succeeded
2010.02.16 15:45:30 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      After State machine Fun execution  State:  0x3  Event : 0x3
```

An unsuccessful authentication attempt would be similar to the following:

```
AAA: New Session on portal 'XAUTH 100'.
AAA: Session using AUTHENTICATION list 'LoginUseRadiusLocal'.

2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XauthEDStartVpnMutexPath:
      Before State machine Fun execution  State: 0x0  Event : 0x0
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH    Attribs in
      ISAKMP_CFG_REQUEST:
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH  XAUTH_TYPE
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH    XAUTH_USER_NAME
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH    XAUTH_USER_PASSWORD
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      AttribSize= 12
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      GenHdrSize= 4
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Attrib Payload Size:= 20
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      HashPayload Size: 24
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Total Msg Size(before Encrypt):44
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Total Msg Size(After Encrypt):48
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
```

```
      Total Length of the packet with ISAKMP HDR:76
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH
      XauthSendMsgVpnMutexPath:Total Packet Length:76
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XauthTransactionStart: SENT
      OUT ISAKMP_CFG_REQUEST MESSAGE ....
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XauthEDStartVpnMutexPath:
      After State machine Fun execution State:  0x1  Event : 0x0
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      Host Identifier : 7
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      Peer Identifier: 7
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      Before State machine Fun execution  State:  0x1  Event :
      0x1
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH    Attribs in
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH  ISAKMP_CFG_REPLY:
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XAUTH_TYPE
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XAUTH_USER_NAME
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XAUTH_PASSWORD
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH
2010.02.16 15:42:07 CRYPTO_IKE.XAUTH XauthProcessVpnMutexPath:
      After State machine Fun execution  State:  0x2  Event : 0x1

RADIUS AUTHENTICATION: Sending packet to <Server IP> (1812).
RADIUS AUTHENTICATION: Waiting on response from server
RADIUS AUTHENTICATION: Receiving from RADIUS socket
RADIUS AUTHENTICATION: Response received from server (<Server
      IP>)
RADIUS AUTHENTICATION: Received response from <Server IP>.
AAA: RADIUS authentication failed.

2010.02.16 15:42:08 CRYPTO_IKE.XAUTH XauthSessionPasswordFailed:
      Password Failed
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH XauthLBProcessData: Before
      State machine Fun execution  State: 0x2 Event : 0x2
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH    Attribs in
      ISAKMP_CFG_SET:
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH    XAUTH_STATUS
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      AttribSize= 4
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      GenHdrSize= 4
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Attrib Payload Size:= 12
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      HashPayload Size: 24
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      Total Msg Size(before Encrypt):36
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
      ISAKMP_CFG_SET Message
```

```
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 0e
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 18
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 24
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH ab
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH b8
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 80
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH ec
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 5c
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH c5
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 82
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH e2
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH a0
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 4f
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH fb
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 15
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 28
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH fb
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH a9
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH d4
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 1d
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH fc
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH fa
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 0c
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 03
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00

AAA: Closing Session on portal 'XAUTH 100'.

2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 07
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH c0
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 8f
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH 00
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     Total Msg Size(After Encrypt):48
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH IkeOutTransXchgProcess:
     Total Length of the packet with ISAKMP HDR:76
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH
     XauthSendMsgVpnMutexPath:Total Packet Length:76
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH SENT OUT ISAKMP_CFG_SET
     MESSAGE ....
2010.02.16 15:42:08 CRYPTO_IKE.XAUTH XauthLBProcessData: After
     State machine Fun execution  State:  0x3  Event : 0x2
```

DISCLAIMER

ADTRAN provides the foregoing application description solely for the reader's consideration and study, and without any representation or suggestion that the foregoing application is or may be free from claims of third parties for infringement of intellectual property rights, including but not limited to, direct and contributory infringement as well as for active inducement to infringe. In addition, the reader's attention is drawn to the following disclaimer with regard to the reader's use of the foregoing material in products and/or systems. That is:

ADTRAN SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ADTRAN BE LIABLE FOR ANY LOSS OR DAMAGE, AND FOR PERSONAL INJURY, INCLUDING BUT NOT LIMITED TO, COMPENSATORY, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.