

VPN 3000 Network Access Device 4.7.1 NAC Administration and Configuration

Document ID: 65114

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure NAC

- Task 1: Configure AAA Server Communication
- Task 2: Configure Global EAP Over UDP
- Task 3: Create a Filter Rule to Allow EAP over UDP Communication
- Task 4: Configure the NAC Exception List
- Task 5: Configure NAC for the Base Group and User Defined Groups

Monitor and Administer NAC Sessions

Enable EAP, EAPoUDP, and NAC Logging

Sample VPN 3000 Debug Logs

- Typical Successful Posture Validation Log
- Typical Clientless Log

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

Network Admission Control (NAC) provides a method you can use to validate a peer based on its state, a function referred to as *posture validation*. Posture validation can include the verification that the peer runs applications with the latest patches. Posture validation can also ensure that the anti-virus files, personal firewall rules, or intrusion protection software are up-to-date. NAC supplements the identity-based validation that PPP, IPsec, and other access methods provide.

The VPN Concentrator functions as both a NAC authenticator and a Cisco Secure Access Control Server (ACS) client.

As a NAC authenticator, the VPN Concentrator performs these tasks:

- Initiates the initial exchange of credentials based on IPsec session establishment and periodically thereafter.
- Relays credential requests and responses between the peer and the authentication (ACS) server with the use of Protected Extensible Authentication Protocol (PEAP).
- Enforces network access policy for an IPsec session based on results from the ACS server.
- Implements the configured EAP Status Query method.
- Supports a local exception list based on the peer operating system.
- Requests access policies from the ACS server for a clientless host.

As an ACS client, the VPN Concentrator supports:

- EAP/RADIUS

- RADIUS attributes required for NAC

NAC on the VPN 3000 Concentrator differs from that on Cisco IOS® Layer 3 devices such as routers. Whereas routers trigger posture validation (PV) based on routed traffic, the VPN 3000 Concentrator configured with NAC uses the establishment of an IPsec VPN session as the trigger for PV. Cisco IOS routers configured with NAC use an Intercept access control list (ACL) in order to trigger PV based on traffic destined for certain networks. Because external devices cannot access the network behind the VPN 3000 Concentrator without starting a VPN session, the VPN 3000 Concentrator does not need an intercept ACL as a PV trigger. While posture validation occurs, all IPsec traffic from the peer is subject to the Default ACL configured for the peer's group on the **Base Group > NAC** tab or the **Groups > NAC** tab.

Configure NAC on the **Configuration > Policy Management > NAC** window and the **Configuration > User Management > Base Group/Groups > NAC** tab.

This document supplements instructions in these guides:

- VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7
- VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring, Release 4.7

Prerequisites

Requirements

Because the VPN 3000 Network Access Device is the enforcement device in NAC, it is recommended that you configure it last, especially if some hosts do not have Cisco Trust Agent (CTA) installed. This causes less disruption to network operations.

You can disable NAC on the VPN 3000 Concentrator if problems occur. In order to access the Enable NAC parameter, select **Configuration > User Management > Base Group/Group > NAC**.

Components Used

Ensure that the VPN 3000 Concentrator runs release 4.7 or later before you attempt to configure NAC.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

System error messages from Cisco devices are displayed in a different font. For example, a router restarted with the **reload** command displays the `System returned to ROM by reload` message, whereas a router restarted by power-cycle displays the `System returned to ROM by power-on` message.

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure NAC

These sections describe the NAC configuration tasks:

- Task 1: Configure AAA Server Communication
- Task 2: Configure Global EAP Over UDP

- Task 3: Create a Filter Rule to Allow EAP over UDP Communication
- Task 4: Configure the NAC Exception List
- Task 5: Configure NAC for the Base Group and User Defined Groups

Task 1: Configure AAA Server Communication

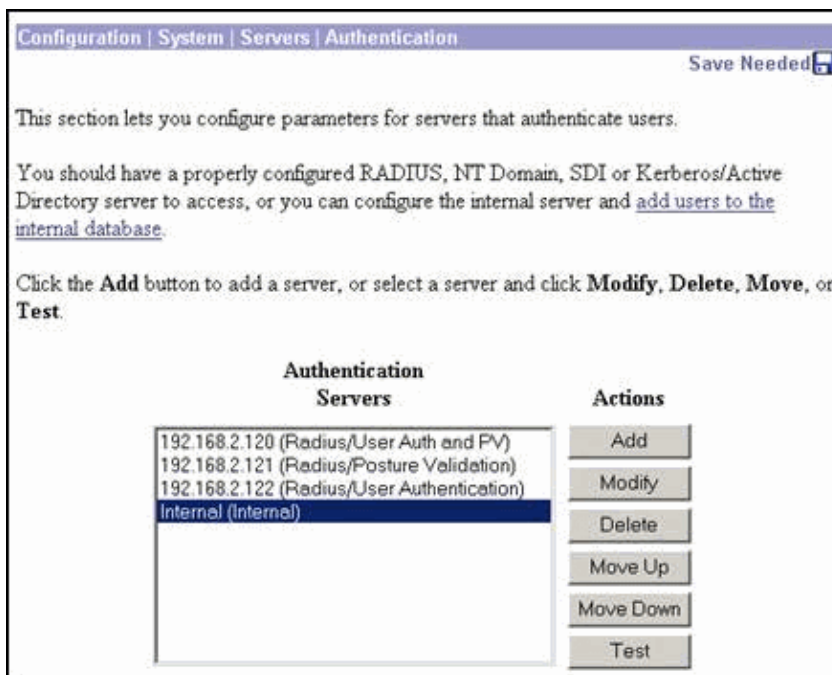
NAC requires an ACS server for posture validation. The "Used For" parameter specifies how to use the ACS server in its role as a RADIUS server. The choices are user authentication only, posture validation only, or both user authentication and posture validation.

Complete these steps in order to configure ACS as an authentication server and access the "Used For" parameter.

1. Use one of these paths in order to configure ACS as an authentication server:

- ◆ In order to configure ACS as the global authentication server, select **Configuration > System > Servers > Authentication**.
- ◆ In order to configure ACS as a group-specific authentication server, select **Configuration > User Management > Groups > Authentication Servers > Add**.

This illustration shows the global authentication server window through which you can access the "Used For" parameter.



The Authentication Servers box displays the configured usage of each RADIUS server.

2. Click **Add** or **Modify**.

The Add or Modify window opens. This illustration shows the global authentication add server configuration window that contains the "Used For" parameter.

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.

Authentication Server Enter IP address or hostname.

Used For Select the operation(s) for which this RADIUS server will be used.

Server Port Enter 0 for default port (1645).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the secret.

3. Set the parameters in this window as this list shows:

- ◆ **Server Type** The type of server used for posture validation. For NAC, it must be RADIUS.
- ◆ **Authentication Server** The IP address or hostname of the ACS.
- ◆ **Used For** The operation(s) for which to use the RADIUS server. Set this parameter to **Posture Validation** or **User Auth and PV** in order to use the RADIUS server for NAC. This list shows the options:
 - ◇ **User Authentication** Choose this option for user authentication only.
 - ◇ **Posture Validation** Choose this option for posture validation only.
 - ◇ **User Auth and PV** Choose this option for both user authentication and posture validation.
- ◆ **Server Port** The port number of the ACS server.
- ◆ **Timeout** The number of seconds for ACS server communication to time out.
- ◆ **Retries** The maximum number of retries to attempt communication with the ACS server.
- ◆ **Server Secret** The RADIUS server secret to match the ACS configuration.
- ◆ **Verify** The value of the "Server Secret" parameter repeated.

4. Click **Add** or **Apply**.

The authentication server appears as an entry in the Authentication Servers box.

5. Click **Save Needed**.

A confirmation window opens.

6. Click **OK**.

Task 2: Configure Global EAP Over UDP

The global NAC configuration applies to all NAC sessions on the VPN 3000. Complete these steps in order to configure the global NAC settings:

1. Select **Configuration > Policy Management > Network Admission Control > Global Parameters**.

The Global Parameters window opens.

Attribute	Value	Description
Retransmission Timer	3	Time period allowed for an EAPoUDP response to be received from the peer. Enter the value in seconds. Range is 1 - 60 seconds. Default value is 3.
Hold Timer	180	Time period between a failed EAPoUDP association and next attempt to start a new EAPoUDP association. Enter the value in seconds. Range is 60 - 86400 seconds. Default value is 180.
EAPoUDP Retries	3	Enter the number of EAP over UDP message retries. Range is 1 - 3 retries. Default value is 3.
EAPoUDP Port	21862	Enter the EAPoUDP port number. Default value is 21862.
Clientless Authentication	Enable <input checked="" type="checkbox"/> Username <input type="text" value="clientless"/> Password <input type="password"/> Verify <input type="password"/>	Check to allow authentication of clientless hosts (hosts without an active Cisco Trust Agent) and to set the clientless username and password. This is used to get an access policy from ACS for clientless hosts.

Apply Cancel

2. Set the parameters in this window as this list shows:

- ◆ **Retransmission Timer** The wait time allowed for an EAP over UDP response to be received from the host. This timer starts when the VPN 3000 sends an EAP over UDP message to a host. The timer terminates when the VPN 3000 receives a response. If this timer expires before the VPN 3000 receives a response, the VPN 3000 resends the message. The setting is in seconds.
- ◆ **Hold Timer** The interval between a failed EAP over UDP association and the next attempt to initiate a new EAP over UDP association. The setting is in seconds.
- ◆ **EAPoUDP Retries** The number of times the VPN 3000 resends an EAP over UDP message. This parameter limits the number of consecutive retries sent in response to Retransmission Timer expirations. If the VPN 3000 does not receive a response after the maximum number of retries, the NAC session of the host on the VPN 3000 enters the Hold state, at which time the Hold Timer starts.
- ◆ **EAPoUDP Port** The port number used for EAP over UDP communication with the Cisco Trust Agent (CTA) on the host. This number must match the port number configured on the CTA.
- ◆ **Clientless Authentication Enable** Enables or disables clientless authentication. If this parameter is disabled, non-responsive hosts (for example, because CTA is not present or runs) are subject to the NAC Default ACL (if defined). If this parameter is enabled, ACS requests the access policy for non-responsive hosts. The access policy configured on ACS for this user determines the access policy for non-responsive hosts.
- ◆ **Clientless Authentication Username** The username configured on the ACS.
- ◆ **Clientless Authentication Password** The ACS password assigned to "Clientless Authentication Username."
- ◆ **Clientless Authentication Verify** The value of "Clientless Authentication Password" repeated.

3. Click **Apply**.

4. Click **Save Needed**.

A confirmation window opens.

5. Click **OK**.

Task 3: Create a Filter Rule to Allow EAP over UDP Communication

Filters on the VPN 3000 determine which network traffic to forward and which to drop. These filters consist of one or more rules. If a filter configured on the public interface of the VPN 3000 causes the VPN 3000 to

drop EAP over UDP traffic, posture validation cannot proceed, and all hosts are then considered clientless. Similarly, if a filter configured for a particular user or group causes the VPN 3000 to drop EAP over UDP traffic, posture validation cannot proceed and all hosts connected by the affected users are then considered clientless. The same applies to an ACL sent from the ACS. Filters applied to a user session, whether configured locally on the VPN 3000 or downloaded from the ACS, must forward EAP over UDP traffic in order for NAC to work properly. ACLs from the ACS must allow UDP traffic on the configured EAP over UDP port (by default, port 21862). This table lists the settings used to create two rules in the VPN 3000 configuration. One rule forwards incoming EAP over UDP packets and one rule forwards outgoing EAP over UDP packets.

	Rule for Incoming Traffic	Rule for Outgoing Traffic
Rule Name	EAPoUDP In	EAPoUDP Out
Direction	Inbound	Outbound
Action	Forward	Forward
Protocol	UDP	UDP
TCP Connection	Do not care	Do not care
Source Address	0.0.0.0/255.255.255.255	PRIVATE *
Destination Address	PRIVATE *	0.0.0.0/255.255.255.255
TCP/UDP Source Port	21862 **	All
TCP/UDP Destination Port	All	21862 **

* The IP address of Private Interface a.b.c.d/0.0.0.0. This is optional and can be set to 0.0.0.0/255.255.255.255 or to a network list such as VPN Client Local LAN (Default).

** Set to the port number in the NAC Global configuration. The default is 21862.

For example, the factory configured filter Firewall Filter for VPN Client (Default) allows all outgoing traffic but drops all incoming traffic. If the VPN 3000 applies this filter to a user session, posture validation does not take place. You can correct this problem when you add the EAPoUDP In rule (defined in the table) to this filter. There is no need to explicitly allow EAPoUDP Out since this filter already allows all outgoing traffic.

In order to create rules, select **Configuration > Policy Management > Traffic Management > Rules Add**. Refer to the VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7 for detailed instructions about filters and rules.

After you create rules, you must add them to a filter before they take effect.

Task 4: Configure the NAC Exception List

The NAC Exception List excludes hosts from posture validation and gives them a static access policy. The entries in the NAC Exception List specify the operating system (OS) of hosts to be filtered. The Cisco VPN Client identifies the host OS to the VPN 3000. If the OS matches an entry in the NAC Exception List, the

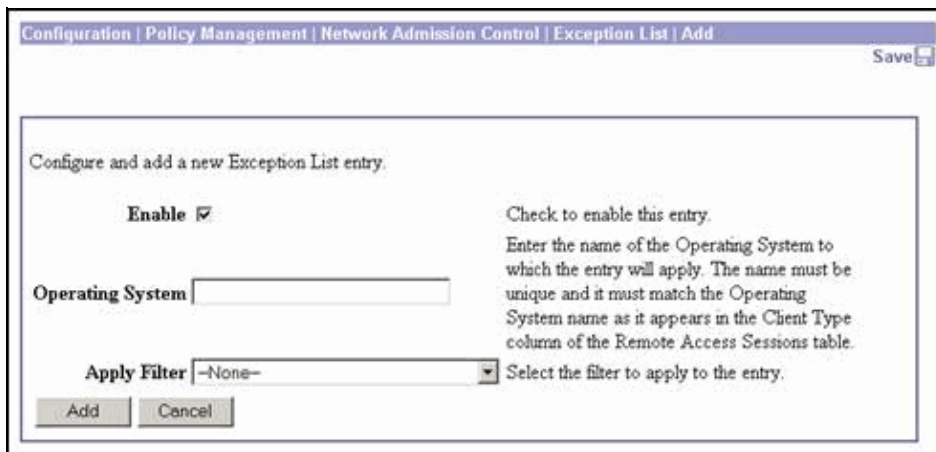
VPN 3000 applies the corresponding filter (if any) and stops further NAC processing for the host, for the duration of the VPN session.

The VPN 3000 uses the NAC Exception List only if NAC is enabled for the user's group. In order to access the Enable NAC parameter, select **Configuration > User Management > Base Group/Groups > NAC**.

Complete these steps in order to configure the NAC exception list:

1. Connect the hosts that run the operating systems to be specified in the NAC Exception List, to the VPN 3000 with the use of the Cisco VPN Client.
2. Select **Administration > Administer Sessions or Monitoring > Sessions** and copy the strings that identify the operating systems to appear in the NAC Exception List from the Client Type column in the Remote Access Sessions table.
3. Select **Configuration > Policy Management > Network Admission Control > Exception List > Add**.

The Add window opens.



4. Set the parameters in this window as this list shows:

- ◆ **Enable** Check this box in order to enable Exception List functionality for this entry.
- ◆ **Operating System** The name of the operating system. The string must exactly match the operating system reported by the Cisco VPN Client. Copy one of the strings noted in step 2.
- ◆ **Apply Filter** Select the filter to apply to the user session.

5. Click **Add**.

6. Repeat steps 3 through 5 for each additional operating system to appear in the NAC Exception List.

7. Click **Save Needed**.

A confirmation window opens.

8. Click **OK**.

Task 5: Configure NAC for the Base Group and User Defined Groups

Complete these steps in order to configure the group specific NAC settings:

1. Choose the path that defines the scope of the group settings:

- ◆ Select **Configuration > User Management > Base Group**.
- ◆ Select **Configuration > User Management > Groups > Modify <group-name>**.

2. Click on the NAC tab.

The Network Access Control Parameters window opens.

Attribute	Value	Description
Enable NAC	<input checked="" type="checkbox"/>	Check to enable Network Admission Control. NAC is supported only for IPSec and L2TP over IPSec tunnels.
Status Query Timer	300	Time period between sending status queries to the peer. A Status Query response from the peer indicates whether or not the peer's Posture has changed. Enter the value in seconds. Range is 30 - 1800 seconds. Default value is 300.
Revalidation Timer	36000	Time period between a successful posture validation and the unconditional commencement of the next posture validation. Enter the value in seconds. Range is 300 - 86400 seconds. Default value is 36000.
Default ACL (filter)	Public for NAC	Choose the filter that defines the Default Access Control List. If NAC is enabled and the user's session is not subject to the Exception List, the Default ACL is applied to the user's session during the initial posture validation. It is also applied if the EAPoUDP association is reinitialized via failed EAPoUDP communication or administrative action on the VPN concentrator.

The only difference between the user defined group NAC configuration window and Base Group NAC configuration window is that the NAC configuration window includes an Inherit checkbox for each item to allow the user defined groups to get their NAC configuration from the base group.

- Use these descriptions to set the parameters in this window, and click the **Inherit** box as needed:
 - ◆ **Enable NAC** Enables or disables NAC for the group. No NAC processing takes place for users in the group if you uncheck this box.
 - ◆ **Status Query Timer** Determines the number of seconds between NAC Status Queries for NAC sessions in the group. The Status Query timer starts after PV successfully completes.
 - ◆ **Revalidation Timer** The interval between unconditional, full posture validations for NAC sessions in the group. The Revalidation timer starts after PV successfully completes. The interval is in seconds.
 - ◆ **Default ACL (filter)** Choose the filter for the VPN 3000 in to apply to the user session during the initial PV. The VPN 3000 also applies the ACL (or filter in VPN 3000 terminology) to the user session if a previously successful EAPoUDP association fails. The VPN 3000 replaces the default ACL with a dynamic ACL if it obtains one from the ACS as a result of PV or Clientless Authentication.

If an IPsec session is configured to accept a per-user downloadable ACL (ACL A) during the completion of IKE negotiation, this downloadable ACL (ACL A) is overridden by the downloadable ACL (ACL B) passed down during posture validation. The two downloadable ACLs (A and B) are not merged. The user's access policy abides by the ACL passed down during posture validation (ACL B).

- Click **Apply**.
- Click **Save Needed**.

A confirmation window opens.

- Click **OK**.

Monitor and Administer NAC Sessions

In order to view NAC session data, select **Monitoring > Sessions**.

The Monitoring Sessions window opens.

Monitoring | Sessions Thursday, 17 February 2005 16:53:51
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group:

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Weighted Active Load	Percent Session Load	Concurrent Sessions Limit	Total Cumulative Sessions
0	1	1	2	2	1	0.13%	750	2

NAC Session Summary

Accepted		Rejected		Exempted		Non-responsive		Hold-off		N/A	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
1	1	0	0	0	0	0	0	0	0	0	0

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
user1	192.168.2.68 10.86.5.16	bxbvprlab	IPSec 3DES-168	Feb 17 16:53:31 0:00:19	WinNT 4.0.1 (Ref)	2192 4184	Accepted Healthy

Management Sessions [LAN-to-LAN Sessions | Remote Access Sessions]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	161.44.173.232	HTTP	None	Feb 17 16:53:48	0:00:03

The NAC Session Summary table (also shown in the next illustration) shows the number of active and total NAC sessions categorized by the outcome of posture validation.

The meanings of the headings in the NAC Session Summary table are:

- **Accepted** PV completed successfully.
- **Rejected** PV failed (ACS problem).
- **Exempted** Host OS is on the NAC exception list.
- **Non-responsive** The host is clientless.
- **Hold-off** EAPoUDP associations lost.
- **N/A** The NAC is disabled for a host.

The NAC Result Posture Token column in the Remote Access Sessions table shows the result of posture validation and the state of the host as determined by the ACS server during posture validation. Although these are configurable on ACS, typical ACS posture token values are Healthy, Checkup, Quarantine, Infected, and Unknown.

In order to administer NAC sessions, select **Administration > Administer Sessions**. The Administer Sessions window opens.

Administration | Administer Sessions Thursday, 17 February 2005 16:45:16
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Group:

Logout All: [PPTP User](#) | [L2TP User](#) | [IPSec User](#) | [IPSec LAN-to-LAN](#) | [E-mail](#) | [WebVPN](#) | [SSL Tunnel](#)
 NAC: [Revalidate All](#) | [Reinitialize All](#)

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Weighted Active Load	Percent Session Load	Concurrent Sessions Limit	Total Cumulative Sessions
0	1	1	2	2	1	0.13%	750	6

NAC Session Summary

Accepted		Rejected		Exempted		Non-responsive		Hold-off		N/A	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
1	9	0	0	0	0	0	0	0	0	0	0

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions
No LAN-to-LAN Sessions								

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
user1	192.168.2.68 10.86.5.16	bxbvprlab	IPSec 3DES-168	Feb 17 16:44:58 0:00:17	WinNT 4.0.1 (Rel)	2192 4168	Accepted Healthy [Reval Reinit]	[Logout Ping]

Management Sessions [LAN-to-LAN Sessions | Remote Access Sessions]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions
admin	161.44.173.232	HTTP	None	Feb 17 16:45:12	0:00:03	[Logout Ping]

This window adds administrative commands to the data present in the Monitoring Sessions window. For example, you can click the **Revalidate All** or **Reinitialize All** link to revalidate or reinitialize all active NAC sessions. Both links force posture validation for all NAC sessions. The difference between the two links is that revalidation does not change the active access policy currently in place for the NAC session before PV is initiated. Reinitialization applies the NAC Default ACL (if defined) before PV is initiated.

The **Reval** and **Reinit** links in the NAC Result Posture Token column in the Administer Sessions window allow revalidation and reinitialization of an individual session.

The Actions column in the Remote Access Sessions and Management Sessions tables in the Administer Sessions window also adds administrative access to the respective session.

Click an entry in the Username column to display the session details. The **Administration > Administer Sessions > Detail** window also contains information about NAC-enabled sessions. This illustration shows the Network Admission Control section of the session details table.

Administration Administer Sessions Detail				Tuesday, 25 January 2005 10:13:16				
				Reset Refresh				
Back to Sessions								
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
dbrownli	10.86.5.16	192.168.2.68	IPSec	3DES-168	Jan 25 10:13:07	0:00:09	2192	2352
IKE Sessions: 1								
IPSec Sessions: 1								
IKE Session								
Session ID	1			Encryption Algorithm	3DES-168			
Hashing Algorithm	MD5			Diffie-Hellman Group	Group 2 (1024-bit)			
Authentication Mode	Pre-Shared Keys (XAUTH)			IKE Negotiation Mode	Aggressive			
Rekey Time Interval	86400 seconds							
IPSec Session								
Session ID	2			Remote Address	192.168.2.68			
Local Address	0.0.0.0/255.255.255.255			Encryption Algorithm	3DES-168			
Hashing Algorithm	MD5			SEP	1			
Encapsulation Mode	Tunnel			Rekey Time Interval	28800 seconds			
Bytes Received	2352			Bytes Transmitted	2192			
Network Admission Control								
Revalidation Time Interval	300 seconds			Time Until Next Revalidation	299 seconds			
Status Query Time Interval	60 seconds			EAPoUDP Session Age	1 seconds			
Hold-Off Time Remaining	0 seconds			Posture Token	Healthy			
Redirect URL	www.cisco.com							

The Network Admission Control section of the session details table shows these items:

- **Revalidation Time Interval** The interval (in seconds) between revalidation processes. You can configure the interval on the **Configuration > User Management > Base Group/Groups > NAC** tab. However, the ACS can override this configuration.
- **Time Until Next Revalidation** The number of seconds that remain until revalidation takes place.
- **Status Query Time Interval** The interval (in seconds) between status queries. You can configure the interval on the **Configuration > User Management > Group/Groups > NAC** tab. However, the ACS can override this configuration.
- **EAPoUDP Session Age** The number of seconds that the EAP over UDP session is up.
- **Hold-off Time Remaining** The number of seconds that remain before the VPN 3000 removes the host EAPoUDP session from the hold-off state and retries posture validation. Hold-off state is entered when EAPoUDP communication is lost to a host with an established EAPoUDP session.
- **Posture Token** The state of the host as determined by the ACS server during posture validation.
- **Redirect URL** The optional URL to which the VPN Concentrator redirects HTTP sessions of the hosts. The ACS downloads this URL as a result of posture validation or clientless authentication.

Refer to the VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring, Release 4.7 for more information about the Administration and Monitoring windows.

Enable EAP, EAPoUDP, and NAC Logging

The EAP, EAPoUDP, and NAC software modules log events on the VPN 3000 that can be useful for when you debug NAC. Select **Configuration > System > Events > Classes > Add** in order to enable event logging.

The Severities 1–3 NAC, EAP, and EAPoUDP events are the ones most relevant for debugging NAC. Refer to the VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7 for more information

about event logging.

Sample VPN 3000 Debug Logs

These sections show example logs for which Severities 1-5 NAC, EAP, and EAPoUDP event logging are enabled:

Refer to Important Information on Debug Commands before you issue **debug** commands.

- Typical Successful Posture Validation Log
- Typical Clientless Log

Typical Successful Posture Validation Log

These event messages indicate a typical successful posture validation. Most of the event messages show a public IP address (PUB_IP), private (assigned by VPN 3000) IP address (PRV_IP), or both as a way to associate the events with each other. The last event in this log, EAPoUDP association successfully established, signals the end of a successful posture validation.

```
296 03/21/2005 15:38:40.930 SEV=4 NAC/2 RPT=6 NAC session
initialized - PUB_IP:10.86.5.114 PRV_IP:192.168.2.68

297 03/21/2005 15:38:40.930 SEV=7 NAC/31 RPT=8 NAC Default ACL not
configured - PUB_IP:10.86.5.114, PRV_IP:192.168.2.68

298 03/21/2005 15:38:40.930 SEV=4 EAPoUDP/2 RPT=9 EAPoUDP association
initiated - PRV_IP:192.168.2.68

299 03/21/2005 15:38:46.930 SEV=6 EAPoUDP/20 RPT=21 EAPoUDP response
timer expiry - PRV_IP:192.168.2.68

300 03/21/2005 15:38:46.940 SEV=7 EAPoUDP/4 RPT=1 NAC EAP association
initiated - PRV_IP:192.168.2.68, EAP context:0x0658b594

301 03/21/2005 15:38:46.940 SEV=4 EAP/2 RPT=3 EAP association
initiated - context:0x0658b594

302 03/21/2005 15:38:47.010 SEV=7 NAC/22 RPT=3 NAC auth type:0 -
PRV_IP:10.86.5.114

303 03/21/2005 15:38:47.590 SEV=7 NAC/22 RPT=4 NAC auth type:0 -
PRV_IP:10.86.5.114

304 03/21/2005 15:38:47.710 SEV=7 NAC/22 RPT=5 NAC auth type:0 -
PRV_IP:10.86.5.114

305 03/21/2005 15:38:47.920 SEV=7 NAC/22 RPT=6 NAC auth type:0 -
PRV_IP:10.86.5.114

306 03/21/2005 15:38:48.050 SEV=7 NAC/22 RPT=7 NAC auth type:0 -
PRV_IP:10.86.5.114

307 03/21/2005 15:38:48.220 SEV=7 NAC/22 RPT=8 NAC auth type:0 -
PRV_IP:10.86.5.114

308 03/21/2005 15:38:50.650 SEV=7 NAC/22 RPT=9 NAC auth type:0 -
PRV_IP:10.86.5.114

309 03/21/2005 15:38:51.070 SEV=7 NAC/22 RPT=10 NAC auth type:0 -
PRV_IP:10.86.5.114
```

```
310 03/21/2005 15:38:51.470 SEV=6 EAP/5 RPT=3 EAP received Access
Accept - context:0x0658b594

311 03/21/2005 15:38:51.470 SEV=7 NAC/22 RPT=11 NAC auth type:1 -
PRV_IP:10.86.5.114

312 03/21/2005 15:38:51.470 SEV=4 NAC/29 RPT=4 NAC Applying filter -
PUB_IP:10.86.5.114, PRV_IP:192.168.2.68, Name:Fred-41c30abf, ID:5

314 03/21/2005 15:38:51.470 SEV=6 NAC/7 RPT=4 NAC Access Accept -
PUB_IP:10.86.5.114,PRV_IP:192.168.2.68

315 03/21/2005 15:38:51.470 SEV=4 EAPOUDP/5 RPT=3 EAPOUDP association
successfully established - PRV_IP:192.168.2.68
```

Typical Clientless Log

These event messages indicate a typical posture validation attempt with a clientless (or non-responsive) host. After three attempts to get a response to the EAPOUDP-Hello message, the VPN 3000 deems the host as clientless and requests the clientless access policy from ACS.

```
258 03/21/2005 15:36:16.870 SEV=4 NAC/2 RPT=5 NAC session
initialized - PUB_IP:10.86.5.114 PRV_IP:192.168.2.68

259 03/21/2005 15:36:16.870 SEV=7 NAC/31 RPT=7 NAC Default ACL not
configured - PUB_IP:10.86.5.114, PRV_IP:192.168.2.68

260 03/21/2005 15:36:16.870 SEV=4 EAPOUDP/2 RPT=8 EAPOUDP association
initiated - PRV_IP:192.168.2.68

261 03/21/2005 15:36:22.870 SEV=6 EAPOUDP/20 RPT=18 EAPOUDP response
timer expiry - PRV_IP:192.168.2.68

262 03/21/2005 15:36:28.870 SEV=6 EAPOUDP/20 RPT=19 EAPOUDP response
timer expiry - PRV_IP:192.168.2.68

263 03/21/2005 15:36:34.870 SEV=6 EAPOUDP/20 RPT=20 EAPOUDP response
timer expiry - PRV_IP:192.168.2.68

264 03/21/2005 15:36:34.870 SEV=7 NAC/22 RPT=1 NAC auth type:3 - PRV_IP:10.86.5.114

265 03/21/2005 15:36:34.870 SEV=7 EAPOUDP/7 RPT=1 AUTH request for
NAC Clientless host - PRV_IP:192.168.2.68

266 03/21/2005 15:36:35.270 SEV=7 NAC/22 RPT=2 NAC auth type:4 - PRV_IP:10.86.5.114

267 03/21/2005 15:36:35.410 SEV=4 NAC/29 RPT=3 NAC Applying
filter - PUB_IP:10.86.5.114, PRV_IP:192.168.2.68, Name:Allow HTTP-4 207d917, ID:5

269 03/21/2005 15:36:35.410 SEV=6 NAC/7 RPT=3 NAC Access
Accept - PUB_IP:10.86.5.114, PRV_IP:192.168.2.68
```

Verify

See the Typical Successful Posture Validation Log section of this document for verification information.

Troubleshoot

See the Typical Clientless Log section of this document for information you can use to troubleshoot.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7](#)
- [VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring, Release 4.7](#)
- [Implementing Network Admission Control: Phase One Configuration and Deployment](#)
- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPsec Negotiation/IKE Protocol Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 01, 2006

Document ID: 65114
