ESET

Plugin for Cisco NAC (Network Admission Control)

Installation Guide

contents

REV.20090810-003

1. Cisco Network Admission Control (NAC)

Cisco NAC is a technology that helps ensure a clean and secure network environment and, in connection with Cisco devices (switches, routers), helps increase the security level within the company network. The NAC system enables or blocks access to critical network resources based on the detected client security status, increasing overall network security.

1.1 Advantages of NAC

A computer running an antivirus program with an outdated virus signature database can pose a serious security risk The antivirus program may fail to detect the most recent malware threats in the network, resulting in infected client computers. Costs for malware intrusion prevention and implementation of NAC are considerably lower than the substantial costs incurred by repairing the damage caused by malware activities in the network. In this way, Cisco NAC helps secure client workstations even at network hardware level.

Cisco NAC cooperates with antivirus programs that submit security status reports (e.g., virus signature database version) from client workstations directly to the NAC server before they connect to the network.

1.2 How does NAC work?

CISCO NAC consists of the following components that communicate with each other:

1. Cisco Trust Agent (CTA) and its plugins
2. CTA plugin supplied by the antivirus program vendor
3. Cisco IOS device (NAD) supporting NAC
4. Cisco Secure Access Control Server (ACS), which collects and evaluates all security status data from client computers
5. Posture validation server(PVS), which validates data received from client computers with an antivirus program installed

The functionality of NAC is depicted schematically in Figure 1 – 1.

NAC consists of a client computer (Host), which is connected to a Cisco device (Network Access Device) configured for NAC. An AAA Server is connected to NAD (Network Access Device), where Cisco Secure Access Control Server (ACS) is running. The last component is Posture Validation Server (PVS) with an integrated HTTP server communicating back with ACS.

On the client computer (Host), Cisco Trust Agent (CTA) is installed. For CTA to submit current antivirus status data (along with data from other programs) via NAD to the AAA server, an antivirus plugin from the antivirus vendor must be installed on CTA. On the AAA Server, Cisco Secure Access Control (ACS) is running, which is a core component of NAC.

The configured ACS verifies client authentication data submitted by CTA. After verification, ACS sends a data validation request to the corresponding PVS (the request includes data from CTA, such as information from antivirus software). The PVS then compares the data submitted by CTA with the current version of the antivirus software. Based on the specified criteria, the PVS creates a report on the current posture status of the client computer.

CTA then sends the posture status to ACS, which evaluates posture statuses from other programs and creates an overall computer status. Finally, ACS sends the status to the client computer and sets the corresponding NAD interface to a group, where all other computers with the same status are located.

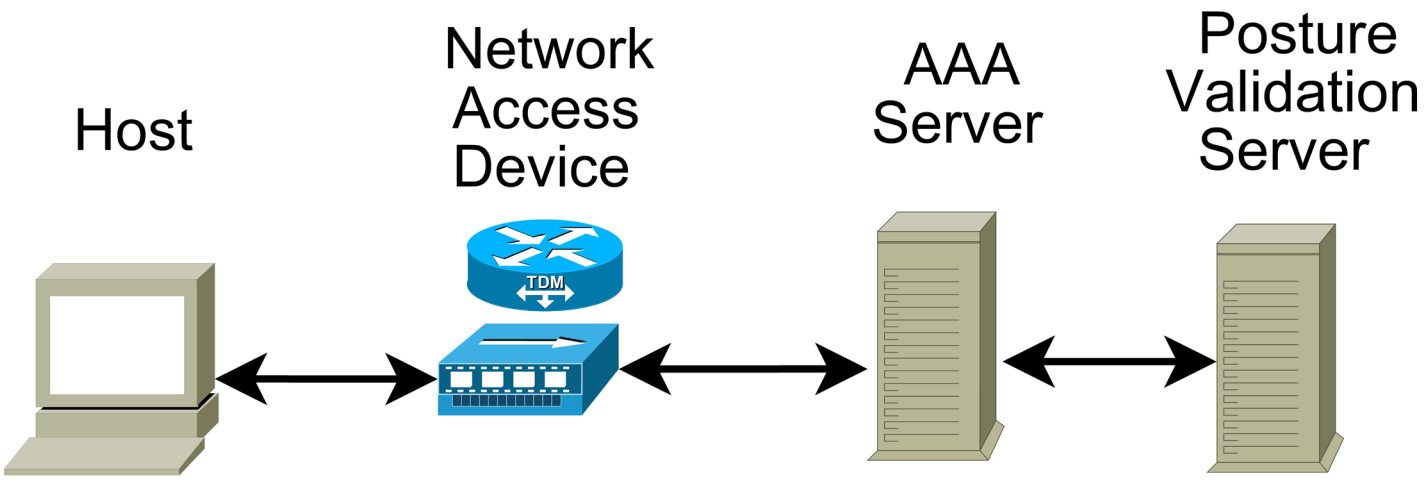

Figure 1 – 1. The 802.1x NAC functionality scheme

2. ESET NAC plugin requirements

Hardware

- Cisco router, or Cisco switch supporting Cisco NAC
- Cisco NAC device configured for Cisco NAC

Software

- On client computers, Cisco CTA (Cisco Trust Agent) must be installed (Cisco TrustAgent – Windows – Supplicant – 2.0.0.30 and higher)
- ESET Smart Security 4.0 or ESET NOD32 Antivirus 4.0 installed on client computers
- ACS 4.1 or 4.0 installed on NAC server
- Correctly configured ACS (users, groups, rights, policy, control rules)
- PVS for client validation (can be configured directly in NAC)

  Server must contain:

  – Microsoft IIS 5.1 or higher with. NET framework 2.0 or higher, or Apache server 2.2 or higher with PHP 5 installed

  – Internet connection for downloading referential update files

  – ESET Smart Security 4.0 (optional)

3. Implementing plugin ESET NAC

ESET NAC implementation consists of two phases:

1. Client phase

   a) installation of PPESET plugin for CTA on client computers

2. Server phase

   a) adding ESET ADF configuration to ACS

   b) configuration of HTTP server where PVS (posture validation serer) is running

   c) enabling communication of PVS with ACS

   d) configuration of validation rules in PVS

An HTTP server must be running with Microsoft IIS 5.1 or higher, or Apache 2.2 with PHP5 installed (also, other HTTP servers supporting CGI applications can be used). Please note that ESET is not liable for any problems caused by using those HTTP servers.

3.1 Client phase

3.1.2 Installation of PPESET plugin for CTA on client computers

Before installing the plugin, CTA (CiscoTrustAgent – Windows – Supplicant – 2.0.0.30 or higher) should be present on the computer. If you install ESET Smart Security 4.0 on the client, the plugin installs automatically. If you are using an earlier version of ESET security products (ESET Smart Security 3.0, ESET NOD32 Antivirus 3.0 or 2.7), then follow the steps below to install the plugin.

Required files:

`PPESET.dll – plugin`

`PPESET.inf – file containing the list of parameters transferred to ACS`

Installation:

Copy PPESET.dll and PPESET.inf to the Common files directory `(c:\Program Files\Common Files\Posture Agent\Plugins\Install\)`.

CTA will automatically install the plugin after it receives a request from ACS. Then CTA moves PPESET.dll and PPESET.inf to the following folder:

`c:\Program Files\Common Files\Posture Agent\Plugins\.`

Logging:

To enable logging of events related to the PPESET.dll plugin, modify the logging level in the ctalogd.ini configuration file `(c:\Program Files\Common Files\PostureAgent\Plugins\Logging\ctalogd.ini)` in the [loglevel]section. The following PPESET logging levels are available:

0 – no logging

1 – log includes only important events

2 – logging with a more detailed output

3 – records all events

The plugin log contains events in the PPESET.log file `(c:\Program Files\Cisco Systems\CiscoTrustAgent\Logging\Logs\PPESET.log)`.

3.2 Server phase

To perform the server installation more easily, use the epfnac.msi installer. This installer allows for automatic creation of the validation server with the configuration website running within the Microsoft IIS server. To test the configuration website, open your web browser and go to http://localhost/enacs/default.aspx. If the configuration website does not display, please check which version of ASP. NET Microsoft ISS you are using(to **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services**, click **Web Sites** > **Default Web Site > ENACS,** then right – click **Properties** in the **ASP. NET** tab). For the server to work correctly, you must install version 2 or higher. If the problem persists, please see section **3.2.2.1, „Configuring IIS 5.1 server to be used as PVS"**, and follow the instructions to set up your IIS server.

After installing Epfnac.msi, add new attributes for ESET NAC to the Cisco ACS Server.

3.2.1 How to install.adf file to Cisco ACS

1. copy the file <install dir>\adf\ESET.adf where CSUtil.exe is installed (<ACS Install_Dir>\bin\)

2. run **CSUtil.exe** – addAVP ESET.adf

3. restart ACS, i.e.:
```
net stop CSAdmin
net stop CSLog
net stop CSAuth
net start CSAdmin
net start CSLog
net start CSAuth
```

The following attributes are added to Cisco ACS:

`ESET:AV:Protection – Status`

The value here represents the protection status of ESS or EAV installed on the client computer.

Value types:

`0 = "Green"`
All security requirements in ESET Smart Security or ESET NOD32 Antivirus are met and the program is up-to-date.

`1 = "Orange"`
ESET Smart Security or ESET NOD32 Antivirus has not been updated for a short time.

`2 = "Red"`
None of the security requirements are met, or the program has not been updated for a long time.

`ESET:AV:Software – Name`

This value represents the name of the product installed.

Value types (value type – value string):
```
"NOD32V2"NOD version 2
"ESET NOD32 Antivirus"
"ESET Smart Security"
```

`ESET:AV:Software – Version`

This value represents the product version of ESS or EAV.

Value type:

`Example: 4.0.0.0`

If no external validation server with a built – in installer is used, then you must create your own validation rules in Cisco ACS. For more information, see documentation for Cisco ACS.

3.2.2 Configuring HTTP server, where PVS is running (if you select manual install)

3.2.2.1 Configuring IIS 5.1 server to be used as PVS

IIS PVS server consists of the following three files:

- `<install dir>\Validator\IIS\ISAPIValidator.dll`
  ISAPI validation server

- `<Common Application Data>\ESET\NAC\conf.ini`
  PVS server configuration file

- `<install dir>\Validator\IIS\ASP. NET\*.*`
  `<install dir>\Validator\IIS\ASP. NET\default.aspx`
  Configuration website dedication for modifying conf.ini

Proceed as follows:

1. Copy the contents of the folder (`<Install dir>\validator\IIS`) to a newly created folder on the disk, which will later be converted into a web service folder `(E.g. /server/NAC/)`.

2. Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** and run **Internet Information Services**.

3. Go to **local computer** > **Web Sites** > **Default Web Site** > and select **Default Web Site** > **New** > **Virtual Directory**.

4. In **Virtual Directory Alias** name the website, e.g. „ENAC".

5. In the **Web Site Content Directory** section find the folder created in step 1.

6. In the **Virtual Directory Access Permissions** section, select the **Read, Run script, and Execute** option.

7. In the **ASP. NET** item set ASP. NET version to **2 and higher**.

8. Click **Finish** to save changes.

9. Check properties of the **conf.ini** (`<Common Application Data>\ESET\NAC\conf.ini`) file to see if the user **Everyone** has the **Write** option selected. If it does not, then select it.

10. Launch or restart the web server.

11. To test the functionality of your ISAPI web server, use the `ISAPITest.dll` file `(<install dir>\Validator\IIS\ISAPITest.dll). Open your web browser and go to http://localhost/<nac>/ISAPITest.dll` (`<NAC>` match to web site name).

12. If you selected a different alias for the website, then change **<nac>** and **<localhost>** to match the correct IP address or computer name.

13. Now test the functionality of the ASP and. NET server. Open your browser and go to http://localhost/<nac>/ASP.NET/default.aspx. The configuration website should be displayed. You can set the desired client computer parameters and configure security groups based on the protection status of client computers.

14. If the configuration website does not load, then you must register ASPNET in IIS.

    Find the file

    `aspnet_regiis.exe` (it should be located in:
    `c:\WINDOWS\Microsoft. NET\Framework\v2.0.50 727\`

```
aspnet_regiis.exe)
```

and run

```
aspnet_regiis.exe – i
```

15. Restart IIS server.

16. Try to display the default.aspx website again.

Note: This configuration is suitable only for a general web server setup and does not include configuration of access rights for the website. The installer will not configure access rights either. It is up to the user how unauthorized access to the configuration website should be treated.

3.2.2.2 Apache server configuration

If you are using an Apache web server, follow the steps below:

IIS PVS server consists of the following three files:

- `CGIValidator.exe` – `CGI` validation server
- `<Common Application Data>\ESET\NAC\conf.ini` PVS server configuration file
- `index.php` Configuration website dedicated for modifying `conf.ini`

For ESET plugin for Cisco NAC to run correctly, configure your Apache server to run CGI scripts and applications using a PHP module. A sample configuration can be found in the **httpd.conf** file, which is included in the install package. Copy the contents of the `<install_dir>\validator\CGI\\server\apache\` folder to the web home directory (DocumentRoot) or another directory. The **CGIValidator.exe** file must run as a CGI application, therefore you must create ScriptAlias in the **httpd.conf** file. The folder where **CGIValidator.exe** is located is used as a parameter of the script. That folder must be assigned parameters similar to the following:

```
ScriptAlias /enacs/validator/ "C:/Epfnac/validator/
   CGI/"
<Directory "C:/Epfnac/validator/CGI/C:/bin">
AllowOverride None
Options ExecCGI
AddHandler cgi – script.exe
Order allow, deny
Allow from all
</Directory>
```

For the /validator/CGI/Php/nac/ directory you must create an alias with attributes necessary for launching PHP scripts.

Example:

```
Alias /enacs/configuration "C:/Epfnac/validator/
   CGI/Php/"
<Directory " C:/Epfnac/validator/CGI/Php/">
    Options None
AllowOverride None
Order allow, deny
Allow from all
</Directory>
```

To start the PVS configuration website, restart your Apache server and go to http://localhost/<nac>/index.php (where <nac> is your web directory name, e.g. enacs/validator).

To test the functionality of the CGI interface, run **CGITest.exe**, e.g. http://localhost/enacs/validator/CGITest.exe.

This configuration does not include configuration of access rights for the website.

3.2.3 Enabling communication between PVS and ACS

To enable communication between PVS and ACS, configure your ACS server and the validation server according to section 3.3, „Configuration of the validation server". If you want to use all features of ESET NAC, then PVS must be installed externally. To do so, go to **Posture Validation** > **External Posture Validation Setup** > **ACS** and find the PVS address. If you are using an IIS server, then enter the URL for the **ISAPIValidator.dll** file (e.g. http://localhost/<nac>/ISAPITest.dll; where <nac> is your right web directory). For Apache servers, enter the URL for the **CGIValidator.exe** file (e.g. http://localhost/enacs/validator/CGITest.exe). Then restart the ACS configuration. After the client logs in, a security status report will be displayed on the client computer.

3.3 Configuration of the validation server

First, create a referential source for verifying virus signature databases in the **Select reference database source** item. You can use one of the following:

Use Installed ESET Antivirus – sets the installation of ESET Smart Security or ESET NOD32 Antivirus installed as a referential source.

Use NAC Internal Downloader – select this option to use the internal update module for NAC. Please note that the internal downloader is not capable of detecting the version of the client software. You must also enter the name (or URL) of the update server. We recommend selecting the default update server (**Autoselect**). In the **User Name** and **Password** text fields, enter the authentication data you received from ESET.

Click **Write** to save changes. To check the configuration, click **Read**.

3.3.1 Configuration of validation rules in PVS

Validation rules are divided into several profiles (Default, Soft, Hard, and Own). Values assigned to rules are specified to meet the criteria for everyday use.

Profile description:

Default – The most common rule status

Soft – Soft protection (client computers are checked with a security fall – back)

Hard – Strict protection (strict rules are used to check client computers)

Own – Custom rule setup

If you want to use your own rules, please see section 3.3.2, „Validation rule principles for client computers".

3.3.2 Validation rule principles for client computers

Columns in the validation rule table set the status, which is assigned to a client after it meets the required criteria (healthy, checkup, etc.). If the client meets the criteria for more than one column, then it is assigned the value of the worst status with one exception: if there are similar conditions in a row, then the first status is considered to be the worst and is assigned, all other similar conditions in that row are ignored. Rows in the tab are independent of each other. Between rows, the OR operator is applied.

Description of table rows

In the **Virus database age** row you can see differences between the current virus signature database version (the referential database on the PVS) and the client's version.

In the **Software version** row, you can see differences between program versions. You can set changes in the minor, major, or maintenance version, or require the client status to be completely up-to-date. To disable the Software version section, set all fields to **Major changed**. By default, Software version check is not performed and therefore all items are set to **Major Changed**.

In the **Protection status** row you can see the client's protection status. For ESET NOD32 v2.7, the Green protection status means that the resident module is enabled and the Red status means that the residential shield is turned off.

Click **Check** to check the rule configuration. To save changes in your configuration, click the **Write** button. To view the current configuration, click **Read**.

Description of security statuses available for client computers

Healthy – client computer is fully protected. All components are up-to-date and no network restrictions are required.

Checkup – client computer has not received the latest updates, updating is required. This status indicates that you should pay increased attention but does not indicate a serious security risk.

Transition – this status is applicable if some devices cannot be accessed (e.g. when booting). The Transition status can also be used for evaluation of disabling firewall protection or antispam. It is rarely used.

Quarantine – indicates that full protection is not provided. The virus signature database must be updated, the program version is out of date, the personal firewall is not running, or the real – time file system protection is disabled. The client should be moved into the group of users with limited access to the network.

Infected – the client computer poses a security risk to other computers in the network. The client should be moved into the group of users with limited access to the network.

Unknown – the client is not submitting its protection status. For such a client special conditions are created.

Note: Configuration of Cisco NAC components (CTA, ACS, NAD) is not included in this document. For more information about configuration of CTA, ACS, AND NAD, please contact your Cisco representative.