Analysis and Evaluation of Endpoint Security Solutions

SABRIA BOUGUETAIA

Master's Thesis
Computer Engineering
Nr: E3295D

2005
DEGREE PROJECT
Computer Engineering

<table>
<thead>
<tr>
<th>Programme</th>
<th>Reg number</th>
<th>Extent</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPUTER ENGINEERING</td>
<td>E3295D</td>
<td>30 ECTS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of student</th>
<th>Year-Month-Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sabria BOUGUETAIA</td>
<td>2005-09-14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supervisor</th>
<th>Examiner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marko Uusitalo</td>
<td>Pascal Rebreyend</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company/Department</th>
<th>Supervisor at the Company/Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helsinki Polytechnic Stadia</td>
<td>Marko Uusitalo</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis and Evaluation of Endpoint Security Solutions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key words in English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NAC, Microsoft NAP, endpoint security, AAA server, RADIUS</td>
</tr>
</tbody>
</table>

ABSTRACT

The main objective for this degree project was to analyze the Endpoint Security Solutions developed by Cisco, Microsoft and a third minor company solution represented by InfoExpress. The different solutions proposed are Cisco Network Admission Control, Microsoft Network Access Protection and InfoExpress CyberGatekeeper. An explanation of each solution functioning is proposed as well as an analysis of the differences between those solutions. This thesis work also proposes a tutorial for the installation of Cisco Network Admission Control for an easier implementation.

The research was done by reading articles on the internet and by experimenting the Cisco Network Admission Control solution. My background knowledge about Cisco routing and ACL was also used.

Based on the actual analysis done in this thesis, a conclusion was drawn that all existing solutions are not yet ready for large-scale use in corporate networks. Moreover all solutions are proprietary and incompatible. The future possible standard for Endpoint solution might be driven by Cisco and Microsoft and a rude competition begins between those two giants.
PREFACE

This master’s thesis was completed in the networking laboratory of Helsinki Polytechnic Stadia. I wish to thank Helsinki Polytechnic Stadia for offering me the opportunity to work on this Master’s thesis with a very topical subject of security systems.

I would like to give my best thanks to my instructor and supervisor Mr Marko Uusitalo, for guiding me through this graduate study. His advice has helped me to solve some difficulties during this thesis. I also want to thank some friends, Remko and Hossein, for their support and willingness to help me on some parts of the project.

Additionally, I would like to thank my family and friends for their supporting attitude throughout this thesis and during the school year.

Helsinki 14th September 2005

Sabria Bouguetaia
### ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ACS</td>
<td>Access Control Server</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface</td>
</tr>
<tr>
<td>AV</td>
<td>AntiVirus</td>
</tr>
<tr>
<td>CGPM</td>
<td>CyberGatekeeper Policy Manager</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CSAdmin</td>
<td>Cisco Secure Administration service</td>
</tr>
<tr>
<td>CSAuth</td>
<td>Cisco Secure Authentication and Authorization service</td>
</tr>
<tr>
<td>CSDBSync</td>
<td>Cisco Secure DataBase Synchronisation</td>
</tr>
<tr>
<td>CSLog</td>
<td>Cisco Secure Logging service</td>
</tr>
<tr>
<td>CSMon</td>
<td>Cisco Secure Monitoring</td>
</tr>
<tr>
<td>CSRadius</td>
<td>Cisco Secure RADIUS service</td>
</tr>
<tr>
<td>CSTacacs</td>
<td>Cisco Secure TACACS service</td>
</tr>
<tr>
<td>CTA</td>
<td>Cisco Trust Agent</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPoLAN</td>
<td>Extensible Authentication Protocol over Local Area Network</td>
</tr>
<tr>
<td>EAPoUDP</td>
<td>Extensible Authentication Protocol over User Datagram Protocol</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Extensible Authentication Protocol – Transport Layer Security</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>Extensible Authentication Protocol–Tunneled Transport Layer Security</td>
</tr>
<tr>
<td>EM</td>
<td>Enforcement Module</td>
</tr>
<tr>
<td>HIP</td>
<td>Cisco Security Agent</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HyperText Transfer Protocol over Secure Socket Layer</td>
</tr>
<tr>
<td>IAS</td>
<td>Internet Authentication Service</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IOS</td>
<td>Internetwork Operating System</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>Ipsec</td>
<td>IP secure</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MS-CHAP</td>
<td>Microsoft Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>NAD</td>
<td>Network Access Device</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Admission Control</td>
</tr>
<tr>
<td>NAP</td>
<td>Network Access Protection</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Access Server</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection</td>
</tr>
<tr>
<td>PA</td>
<td>Cisco Trust Agent</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PIX</td>
<td>Private Digital eXchange</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol 3</td>
</tr>
<tr>
<td>PPP</td>
<td>Point to Point Protocol</td>
</tr>
<tr>
<td>QA</td>
<td>Quarantine Agent</td>
</tr>
<tr>
<td>QEC</td>
<td>Quarantine Enforcement Client</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>SAM</td>
<td>Security Accounts Manager</td>
</tr>
<tr>
<td>SHV</td>
<td>System Health Validator</td>
</tr>
<tr>
<td>SoH</td>
<td>Statement of Health</td>
</tr>
<tr>
<td>TACACS</td>
<td>Terminal Access Controller Access Control System</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
6.2.2 Functionalities of NAC......................................................................................................37

7. MICROSOFT NETWORK ACCESS PROTECTION (NAP) ..................................................42

   7.1. NAP OVERVIEW ............................................................................................................42
   7.2. NAP PLATFORM ..........................................................................................................45
       7.2.1 The Client architecture ..........................................................................................46
       7.2.2 The Server architecture .......................................................................................47
   7.3. OPERATION OF NAP ..................................................................................................49

8. INFOEXPRESS CYBERGATEKEEPER .............................................................................51

   8.1 CYBERGATEKEEPER OVERVIEW ..............................................................................51
   8.2 CYBERGATEKEEPER PLATFORM ...............................................................................52
   8.3 FUNCTIONALITIES OF CYBERGATEKEEPER ...............................................................54

9. NAC CONFIGURATION TUTORIAL ..................................................................................58

   9.1 ACS CONFIGURATION ..................................................................................................58
       9.1.1 Administrators and administrative policy .............................................................59
       9.1.2 Interface configuration ..........................................................................................59
       9.1.3 Network configuration ..........................................................................................61
       9.1.4 System configuration ............................................................................................62
       9.1.5 Shared profile components ..................................................................................66
       9.1.6 Group Setup ..........................................................................................................68
       9.1.7 External User Database .........................................................................................71
       9.1.8 User Setup .............................................................................................................74
   9.2 CLIENT CONFIGURATION .............................................................................................75
   9.3 ROUTER CONFIGURATION ..........................................................................................76
       9.3.1 AAA server communication .................................................................................76
       9.3.2 EOU authentication method ..................................................................................76
       9.3.3 EOU timers and logging .......................................................................................77
       9.3.4 ACL and interface configuration ...........................................................................77
   9.4 TROUBLESHOOTING .....................................................................................................78
       9.4.1 ACS Installation troubleshooting ............................................................................78
       9.4.2 CTA configuration troubleshooting ......................................................................79
       9.4.3 NAC external database configuration troubleshooting .........................................79
       9.4.4 Passed authentication log ....................................................................................80

10. CONCLUSIONS ..................................................................................................................83
1. INTRODUCTION

The recent increase of viruses, worms and Internet attacks has caused significant IT infrastructure damages and a massive loss of productivity within enterprises. Businesses have been forced to spend more money and time to combat these evolving threats and still their networks are not secure. To help addressing new threats in today’s rapidly changing business environment, security updates are constantly being made available to both products and signatures. Devices that have been disconnected from the enterprise such as laptops used during travel and individuals who do not notice the enterprises’ update requirements are easy targets for malicious attacks. Consequently, the enterprise should proactively address these exposures by isolating these devices from the secure and production parts of the network until devices address the identified security exposures and policy violations.
Besides, with regard to external threats, monitoring the security vulnerabilities and policy violations of devices that connect to the network will become a “must” in the coming years. By establishing specific security compliance requirements for devices that connect to the network, the enterprise helps to limit the exposure to corrupted or infected devices. An enterprise can isolate clients that lack required components such as an operating system patch level or Antivirus protection. Additionally, the enterprise can establish remediation procedures that will help clients to meet the requirements for accessing the secure network. Uncontrollable devices pose a substantial security risk. In the everyday business, vendors are meeting clients for a demonstration and to do so, need to access to the Internet or their email for example. In such cases their laptops will be seen as illegitimate by the network as they will not meet the identity and security compliance, thus these devices should be given only limited network access. But are all new solutions developed enough to stop those existing external threats and which one of the existing one is the best?

To remedy these problems, some methods already exist and others will be available in a few months. This thesis shall give an overview of the many protocols used in those existing methods before going deeper into the new developed solutions and a tutorial of one of the solution. In the second section we will examine the standard 802.1x used by many networks nowadays. Then in the third section an overview of the Extensible Authentication Protocol (EAP) and PEAP protocols used with the 802.1x standard will be given. In the fourth section, we will understand the functioning of the two Authentication, Authorization and Accounting (AAA) protocols, RADIUS and TACACS+. The fifth section will describe the AAA server used in the Cisco NAC; the Cisco Secure Access Control Server (ACS). And the AAA server used in the Microsoft NAP will be explained in the sixth section. The following section will present the client agent used by Cisco NAC; the Cisco Trust Agent (CTA). Then an analysis of those different methods proposed by Cisco with its Cisco Network Admission Control (NAC) and the solution developed by Microsoft with its Network Access Protection (NAP) and a short overview of other existing solutions will be done. Finally, a tutorial about the Cisco NAC implementation will be given.
2. 802.1x STANDARD

802.1x is an Institute of Electrical and Electronic Engineers (IEEE) standard for EAP encapsulation over wired or wireless Ethernet drafted in 2001. 802.1x is also known as EAP over LAN (EAPoL). 802.1x uses RADIUS (Remote Authentication Dial-In User Service) for authenticating and giving network authorization to clients by verifying usernames and passwords. 802.1x works at the layer 2 of the OSI model (Local Area Network (LAN) switch and WLAN access point). The other role of this standard is to provide rotating keys for the WLAN encryption. 802.1x uses the EAP protocol as an envelope for the authentication negotiation between clients and servers of the network and to generate keys used to protect the traffic between clients and switches or access points. [1] 802.1x supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

2.1 802.1x overview

By using existing network infrastructure, such as EAP, RADIUS, LDAP, and Active Directory, 802.1x provides support for very large deployments at low cost. Furthermore, enterprises are able to use their active directories and databases to automatically authenticate employees. [2]

By using 802.1x to authenticate user’s access to the network, network administrators can be assured that no unauthorized access will take place, and all of the user authentication will take place on a centralized authentication server.

There are three basic components acting during the 802.1x authentication:

- Supplicant (Client) – Network access device requesting LAN services
- Authenticator – Switch ports
- Authentication Server - Server that performs the authentication, allowing or denying access to the network based on username and password. Usually a RADIUS server such as Cisco ACS, Funk Odyssey, Microsoft Internet Authentication Service (IAS) or FreeRadius. [3]
The following Figure illustrates those three basic components as well as the dialogue protocols used between them.

As said earlier, 802.1x happens at Layer 2 of the OSI model. To be able to communicate, the supplicant and the Authenticator use a protocol called EAPOL, which stands for EAP encapsulation over LANs. EAP is a separate protocol for authentication and will be presented in the following chapter. [1]

Initial 802.1x communication begins with an unauthenticated supplicant attempting to connect with an authenticator (switch). The switch responds by enabling a port for passing only EAP packets from the client to an authentication server. The switch blocks all other traffic, such as HyperText Transfer Protocol (HTTP), Dynamic Host Configuration Protocol (DHCP), and POP3 packets, until the router can verify the client’s identity using an authentication server (RADIUS). Once authenticated, the switch opens the client’s port for other types of traffic. So the switch acts only as a “forwarder” for 802.1x messages.[5] If the supplicant authentication is not successful, the access is denied. The authenticator denies access and places the unauthorized port into a held state, which
prevents transmission or reception of frames. After the first failed authentication, the supplicant triggers a quiet period on the authenticator. During the quiet period, the authenticator ignores all frames from the supplicant on that port. On the other hand, when a client is authenticated, details regarding the session, such as the switch port, client identity, and MAC address are sent to the RADIUS server. Now, we will go deeper in the authentication process in used with 802.1x.

### 2.2 802.1x authentication process

Figure 2-2 shows how the protocol works. It transports EAP information between supplicant and authenticator. The authenticator then uses a standard protocol, usually RADIUS, to relay information to and from the authentication server.

![Figure 2-2: 802.1x functioning](image)

Between the Supplicant and the Authenticator, 802.1x and EAPOL transport the EAP information. Then the authenticator re-encapsulates the EAP information within RADIUS to pass it to the authentication server. [1] Figure 2-3 shows and explains broader how the authentication process works.
Before the authentication, the switch port, with 802.1x authentication enabled, is set to an uncontrolled state and accepts only EAP messages which will be forwarded to the Authentication server. The client sends user credentials to the switch with EAP, and the switch forwards the request to the RADIUS server for approval. If the credentials are valid, the client will request credentials from the Authenticator via 802.1x and EAP.[3]

The authentication process begins when the supplicant attempts connection to the WLAN. The authenticator receives the request and opens a port for the 802.1x authentication session, closing off all other types of traffic. A negotiation is set in place:

1. The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client;
2. The switch replies with an EAP-request identity message. (Dialogue 1 of Figure 2-4)
3. The client sends an EAP-response packet containing its identity to the authentication server. (Dialogue 2 of Figure 2-4)
4. The switch encapsulates the EAP-response packet containing the identity of the client in a RADIUS request packet to the authentication server. (Dialogue 3 of Figure 2-4)
5. The authentication server will challenge the client and sends its credentials to authenticate the client. The switch forward this packet. (Dialogue 4 and 5 of Figure 2-4)

6. The client sends its credentials to the server to authenticate. The packet is forwarded by the switch to the authentication server which uses a specific authentication algorithm to verify the client's identity. (Dialogue 6 and 7 of Figure 2-4)

7. The authentication server will either send an accept or reject message to the switch. (Dialogue 8 of Figure 2-4)

8. The switch sends an EAP-success packet (or reject packet) to the client. (Dialogue 9 of Figure 2-4)

9. If the authentication server accepts the client, then the switch will transfer the client's port to an authorized state and forward additional traffic. [6] [7]

Figure 2-4 illustrates this negotiation:

![EAP/RADIUS Message Exchange](image)

**Figure 2-4: EAP/RADIUS Message Exchange [4]**

In Figure 2-4, the Authenticator (The router) initiates communication with an 802.1x enabled client. When the client responds, it is prompted for a username and password. The Authenticator passes this information to the Authentication Server, which determines whether the client can access services provided by the Authenticator. When the RADIUS server successfully authenticates the client, the port is placed in the authorized state. When the client will log off, the port will be placed
in the unauthorized state again. If the client does not support 802.1x, authentication cannot take place. By using 802.1x a successful authentication has to be achieved before any traffic is allow to transit into the network (including DHCP requests) regardless of whether a link is established between the client and authenticator (switch port).

An understanding of 802.1x was provided. The next section will present two of the existing authentication protocol used by 802.1x.
3. EAP AND PEAP PROTOCOLS

EAP is an Internet Engineering Task Force (IETF) authentication standard. EAP was originally designed for use over Point to Point Protocol (PPP). EAP is a protocol that is used between the client and the authenticator to authenticate the client. As seen in the previous section, the 802.1x standard specifies encapsulation methods for transmitting EAP messages so they can be carried over different media types. [1] The different type of EAP will be seen briefly in the following subsection. The EAP specification mandates support for only one type of authentication: a password, which is sent as a hash using the Message Digest 5 (MD5) algorithm.[8]

PEAP stands for Protected Extensible Authentication Protocol. It was developed jointly by Microsoft, RSA Security and Cisco. Nowadays, it is an open standard of the IEEE. In fact, PEAP was designed to use older authentication mechanisms while retaining the strong cryptographic foundation of TLS. [7] It provides a method to transport securely authentication data, including legacy password-based protocols. PEAP accomplishes this by using tunnelling between PEAP clients and the authentication server. The authentication data is transmitted after an encrypted tunnel is created. PEAP authenticates wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN. [9] PEAP can be found among the different EAP types as shown in the following paragraph.

3.1 The different types of EAP

As said before, many types of EAP exist. This section will give a short overview of two types of EAP; Extensible Authentication Protocol -Transport Layer Security (EAP-TLS) which is the other based for PEAP and the Extensible Authentication Protocol–Tunnelled Transport Layer Security (EAP-TTLS) which is the “old competitor” protocol of PEAP.

EAP-TLS is based on the IEEE and IETF standards. It was at first created by Microsoft and then accepted by the IETF. As for EAP, it needs an infrastructure with a RADIUS server and a centralized account database like Microsoft Active Directory. This protocol requires certificates to be distributed to users before they are granted network access.[10] EAP-TLS requires digital
certificates at both ends of a link, authenticating both the client and the server. It is seen as the most secure EAP type. It offers an authentication mechanism based on the computer as well as on the user. It prevents for example a non-authorized user connected to an authorized computer to access to the network. It also allows the computer to be identified on the network even when no users are connected.

EAP-TTLS is a proprietary protocol which was developed by Funk Software and Certicom. It is considered by the IETF as a standard. Like PEAP, it authenticates WLAN clients using only server certificates. Thus certificates do not have to be distributed to endpoint beforehand. It sets up a complete end-to-end tunnel to transfer the user’s credential and therefore do not need to encrypt the certificates. EAP-TTLS enables client authentication method to all of the EAP types.[10] The coming part presents the functioning of EAP and PEAP and therefore their differences.

### 3.2 The functioning of EAP and PEAP

#### 3.2.1 EAP (RFC 2284)

EAP does not select a specific authentication mechanism at Link Control Phase, but rather postpones this until the Authentication Phase. This allows the authenticator to request more information before determining the specific authentication mechanism. This also permits the use of a RADIUS server which actually implements the various mechanisms while the authenticator just passes through the authentication exchange. The taken actions are described:

1. After the Link Establishment phase is completed, the authenticator sends one or more requests to authenticate the Client.
2. The authentication server sends a Response packet in reply to each Request.
3. The authenticator ends the authentication phase with a Success or Failure packet.

The green dotted arrows in Figure 3-1 show the RADIUS messages the authenticator relays as already shown in the section 2.
The role of the authenticator is more than a relay agent. It does observe the EAP authentication exchange to recognize the Success or Failure message. Then it will take the appropriate action by flagging the port as authorized or do nothing. Once the authorization is established, the ordinary traffic will flow without EAP until it receives an EAPOL Logoff. In that case the authenticator returns the port state to unauthorized.

Next section will describe the second authentication protocol using 802.1x.

### 3.2.2 PEAP

802.1x uses two types of encryption keys, static and dynamic. Dynamic encryption keys make the encryption key more secure. EAP uses static encryption keys while PEAP uses a dynamic encryption key, which is why PEAP is more secure than EAP. [7] PEAP sets up an end-to-end
tunnel to transfer the user’s credentials, such as password. It selectively encrypts the client’s authentication credentials instead of setting up a complete tunnel. It is a two-stage protocol that establishes security in stage one and then exchanges authentication in stage two. Stage one establishes a TLS tunnel and authenticates the authentication server to the client with a certificate. Once that a secure channel has been established, client’s authentication credentials are exchanged in the second stage. [10] PEAP uses the TLS channel to protect an EAP exchange. Authentication must be performed using a protocol defined to be used with EAP. As for EAP-TLS, PEAP supports authentication of machines or users.

We have just seen the way both EAP and PEAP protocols are functioning; now their advantages and disadvantages will be seen.

3.3 Advantages and disadvantages of the two protocols

3.3.1 Advantages

The EAP protocol can support multiple authentication mechanisms without having to pre-negotiate a particular one during Link Control Phase. In EAP, the authenticator does not necessarily have to understand each request type and may be able to simply act as a pass-through agent for a RADIUS server. It only needs to look for the success/failure code to terminate the authentication phase.

Concerning PEAP, it does not need to request certificates from the client, which makes the solution more manageable since there is no need to distribute certificates to users before they are granted network access. PEAP is secure enough to be used in WLAN.

3.3.2 Disadvantages

EAP moves away from the PPP authentication model of negotiating a specific authentication mechanism during Link Control Phase. [12] PEAP is included with Windows XP. Therefore, it only
supports client authentication using Microsoft's own MS-CHAP v2 protocol, so it requires a Microsoft server running Active Directory.[8]

We have just seen two type of authentication protocol with their ways of being run and their advantages and disadvantages. Both protocols are good to work with depending on the existing architecture, one may be better to use than the other one. After seeing the authentication protocols, a part of the 802.1x authentication process is still missing, the AAA protocols. AAA provides the exchange messages to grant or deny access to the network. Two AAA protocols will be discussed in the next section.
4. RADIUS AND TACACS+ PROTOCOLS

There are two common protocols used for NAS authentication, RADIUS and TACACS. Those two protocols will be discussed in this section.

4.1 RADIUS Protocol (RFC 2865-2866-2867-2869-2139-2138)

With the emergence of 802.1x port security for wired and wireless LANs, Remote Authentication Dial-In-Use Service (RADIUS) has recently seen a greater usage. Microsoft has built 802.1x security into Windows XP and so in a relatively short time every corporate PC will require RADIUS authentication before getting access. [13]

Remote users of large companies are often authenticated to use the network through a RADIUS server. RADIUS is an Authorization, Authentication, and Accounting client-server protocol for applications such as network access or Internet Protocol (IP) mobility. RADIUS is the de facto industry standard for remote access AAA (Authentication, Authorization, Accounting), as well as an IETF standard. In general, it acts as a network daemon which performs authentication, authorization and accounting actions when someone login onto a Network Access Server (NAS) or logout from it. It is a system of distributed security that protects remote access to networks and network services against unauthorized access. RADIUS uses a challenge/response method for authentication. RADIUS is a UDP based protocol composed of three components: a protocol with a frame format that uses UDP/IP, a server and a client.

A router operates as a RADIUS client. The client is responsible for passing user’s information to the designated RADIUS server, and then acting on the returned response. RADIUS servers are responsible for receiving user’s connection requests, authenticating the user, and then returning all configuration information that are necessary for the RADIUS client to deliver service to the user. The RADIUS protocol provides also a strong network security. Transactions between the RADIUS client and the RADIUS server are authenticated using a shared secret key which is never sent over the network. In addition, any user passwords are sent encrypted between the RADIUS client and the RADIUS server but all other data are sent in plain text. To authenticate the user, the RADIUS
server supports a variety of methods such as PPP, PAP, Challenge-Handshake Authentication Protocol (CHAP), or MS-CHAP UNIX login, and other authentication mechanisms.

4.1.1 RADIUS tasks

RADIUS allows access to the network only to the approved users (via user name and password). The server verifies the user before access is given. Different levels of access can be set up as well.[10] RADIUS performs the 3 following tasks:

- **Authentication phase:** Verifies a user name and password against a local database. After the credentials are verified, the authorization process begins.
- **Authorization phase:** Determines whether a request will be allowed access. An IP address is assigned to the client.
- **Accounting phase:** Collects information on resource usage for the purpose of trend analysis, auditing, session time billing, or cost allocation. [7]

Now that the 3 different tasks performed by RADIUS have been seen, one can see how those tasks are performed.

4.1.2 RADIUS operation

RADIUS is a username and password scheme that enables only approved users to access the network; it does not affect or encrypt data. The first time a user wants to access to the network, he or she must input username and password and submit it over the network to the RADIUS server. The server then verifies that the individual has an account and, if so, ensures that the person uses the correct password before she or he can be granted to the network.

RADIUS can be set up to provide different access levels. For example, one level can provide just an access to the Internet; another can provide access to the Internet as well as to e-mail communications; yet another account can be provided access to the internet, email and the secure business file server.
RADIUS enables centralized management of authentication data, such as usernames and passwords. When a user attempts to login to a RADIUS client, such as a router, the router sends the authentication request to the RADIUS server. The communication between the RADIUS client and the RADIUS server are authenticated and encrypted through the use of a shared secret key which is not transmitted over the network. The RADIUS server may store the authentication data locally or externally. The RADIUS server checks that the information is correct using authentication schemes like PAP, CHAP or EAP. The RADIUS server will also be notified when the session starts and stops, so that the user can be recorded accordingly; or the data can be used for statistical purposes. An overview of the different RADIUS message types is explained:

- **Access-Request**: Sent by a RADIUS client to request authentication and authorization for a network access connection attempt.
- **Access-Accept**: Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is authenticated and authorized.
- **Access-Reject**: Sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is rejected. A RADIUS server sends this message if the credentials are not authentic or the connection attempt is not authorized. When the RADIUS server sends an Access-Reject message, it gives the information to the client about the type of connection that can be made.
- **Access-Challenge**: Sent by a RADIUS server in response to an Access-Request message. This message is a challenge to the RADIUS client that requires a response.
- **Accounting-Request**: Sent by a RADIUS client to specify accounting information for a connection that was accepted.
- **Accounting-Response**: Sent by the RADIUS server in response to the Accounting-Request message. This message acknowledges the successful receipt and processing of the Accounting-Request message.[15]

For PPP authentication (protocols such as Password Authentication Protocol (PAP), CHAP, Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), and MS-CHAP version 2 (MS-CHAP v2)), the results of the authentication negotiation between the access server and the access client are forwarded to the RADIUS server for verification. To provide security for RADIUS messages, the RADIUS client and the RADIUS server are configured with a common shared secret key. It is used to secure RADIUS traffic and is commonly configured as a text string on both the
RADIUS client and server.[15] Figure 4-1 shows how the authentication and authorization take place with RADIUS.

![Figure 4-1: RADIUS Message Exchange](image)

The client creates an Access-Request RADIUS packet, including at least the User-Name and User-Password attributes. The Access-Request packet's identifier field is generated by the client. The generating process for the identifier field is not specified by the RADIUS protocol specification, but it is usually implemented as a simple counter that is incremented for each request. This packet is completely unprotected, except for the User-Password attribute. The server receives the RADIUS Access-Request packet and verifies that the server possesses a shared secret key for the client. If the server does not possess that key for the client, the request is silently dropped. If the server also possesses the shared secret key, it then uses its authentication database to validate the username and password. If the password is valid, the server creates an Access-Accept packet to send back to the client. If the password is invalid, the server creates an Access-Reject packet to send back to the client.

Both the Access-Accept packet and the Access-Reject packet use the same identifier value from the client's Access-Request packet, and put a Response Authenticator in the Authenticator field. The
Response Authenticator is the MD5 hash of the response packet with the associated request packet's Request Authenticator in the Authenticator field, joined with the shared secret.

When the client receives a response packet, it attempts to match it with an outstanding request using the identifier field. If the client does not have an outstanding request using the same identifier, the response is silently discarded. The client then verifies the Response Authenticator by performing the same Response Authenticator calculation the server performed, and then comparing the result with the Authenticator field. If the Response Authenticator does not match, the packet is silently discarded. If the client received a verified Access-Accept packet, the username and password are considered to be correct, and the user is authenticated. If the client received a verified Access-Reject message, the username and password are considered to be incorrect, and the user is not authenticated.

So now that RADIUS is known, the next section has the purpose of introducing TACACS+.

### 4.2 TACACS+ Protocol (RFC 1492)

TACACS+ (Terminal Access Controller Access Control System) was invented at the same time as RADIUS. The protocol was developed by Cisco to service similar needs. TACACS was primarily developed for use with its own routers and NAS systems. Therefore some of the definition of the protocol has been considered proprietary by Cisco. TACACS was proposed to the IETF as a standard but remains only in draft RFC form to this day. TACACS+ is mainly used with Cisco Routers and Switches. TACACS+ is a TCP based protocol that cleanly separates all three stages of the AAA process. TACACS+ is based on an older authentication protocol common to Unix networks called TACACS that allows a remote access server to forward a user's logon password to an authentication server to determine whether access could be allowed to a given system. TACACS is less secure than the later TACACS+ and RADIUS protocols because it was unencrypted. TACACS+ is not compatible with TACACS. As said before, TACACS+ uses the Transmission Control Protocol (TCP) which is more reliable than UDP. TACACS+ separates the two operations of authentication and authorization.
As for RADIUS, TACACS+ is composed by three components: a protocol with a frame format that uses TCP/IP (unlike RADIUS), a server and a client.

Figure 4-2 describes the topology of TACACS+ composed by those three components.

![Figure 4-2: TACACS+ Topology [14]](image)

A router operates as a TACACS+ client. The client is responsible for passing user’s information to the designated TACACS+ servers, and then acts on the returned response. TACACS+ servers are responsible for receiving user’s connection requests, authenticating the user, and then returning all configuration information that is needed for the client to deliver the service to the user. The TACACS+ protocol provides also a strong network security. Transactions between the TACACS+ client and TACACS+ server are authenticated using a shared secret key which is never sent over the network. In addition, TACACS+ forwards encrypted username and password information to a centralized security server. TACACS+ server provides AAA services independently. To authenticate the user, the TACACS+ server supports a variety of methods such as PAP, CHAP, or MS-CHAP authentication mechanisms.

4.2.1 Features of TACACS+

As for RADIUS, TACACS+ allows only approved users to access to the network. The server verifies the user before access is given. TACACS+ supports the following three required features:

- **Authentication**: The TACACS+ protocol forwards many types of username password information. This information is encrypted over the network with MD5, an encryption
algorithm. TACACS+ can forward the password types for ARA, SLIP, PAP, CHAP, and standard Telnet. This allows clients to use the same username password for different protocols.

- **Authorization**: TACACS+ provides a mechanism to tell the access server which access list a user connected to port X have to use. The TACACS+ server locates the username and password and then identifies the access list the user depends on. The access lists reside on the access server. The TACACS server responds to the user with an accept message and an access list number to apply the given list.

- **Accounting**: TACACS+ provides accounting information to a database through TCP to insure a more secure and complete accounting log. TACACS+ protocol gets the network address of the user, the username, the service attempted, protocol used, time and date, and the packet-filter module originating the log.

### 4.2.2 TACACS+ running

When a host attempts to authenticate using PAP or CHAP, a NAS using TACACS+ will contact an authentication server across the network and request verification. This verification may include not only the username and Password, but other parameters including the port number and request to use a specific IP address or host name. The TACACS+ server validates the request against a database on the server, logs the activity, and sends an approval or denial to the NAS. TACACS+ also allows the NAS to log information to the authentication server when the communications link is terminated. [16]

Fundamentally, TACACS+ provides the same services as RADIUS. Every authentication login attempt on an NAS is verified by a remote TACACS+ daemon. TACACS+ authentication uses three packet types:

- **Start packets** are always sent by the TACACS+ client. It starts the authentication process.

- **Continue packets** are always sent by the TACACS+ client. It is sent to the server to give the requested data and information.

- **Reply packets** are always sent by the TACACS+ server. It is sent to the client to request more information about the user and to grant or denied access to the user.
During the login authentication process only three login retries are allowed for normal users. Another kind of authentication process exists; it is the privilege authentication process which is determined whether a user is allowed to use commands at a particular privilege level. This authentication process is handled similarly to login authentication, except that the user is limited to one authentication attempt. An empty reply to the challenge forces an immediate access denial. [17] Figure 4-3 shows the conversation stack used between the TACACS+ server and the final user.

![TACACS+ Server, TACACS+ Client, Client]

**Figure 4-3: EAP/TACACS+ Message Exchange**

TACACS+ client sets up a TCP connection to the TACACS+ server and sends a Start packet (1 and 3). The TACACS+ server responds with a Reply packet, which grants or denies access, reports an error, or as in this example, challenges the user (4). TACACS+ client might challenge the user to provide username, password and other information (5). Once the requested information is entered, TACACS+ client sends a Continue packet over the existing connection (7). The TACACS+ server sends a Reply packet (8). Once the authentication is complete, the connection is closed (10).
The TACACS+ accounting service enables to create an audit trail of user sessions and commands that have been executed within these sessions. For example, the system can track users’ connections and disconnections, when configuration modes have been entered and exited, and which configuration and operational commands have been executed. [17] Now that RADIUS and TACACS+ have been introduced, the next section displays differences between the two protocols.

### 4.3 The differences between RADIUS and TACACS+

The following table presents the main differences between the two AAA protocols that one can deduced by reading and understanding the two protocols.

<table>
<thead>
<tr>
<th></th>
<th>RADIUS</th>
<th>TACACS+</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td>Omni-present support.</td>
<td>Cisco Proprietary protocol.</td>
</tr>
<tr>
<td><strong>Challenge/Response</strong></td>
<td>Supports unidirectional challenge and response from the RADIUS server to the RADIUS client.</td>
<td>Supports bi-directional challenge and response as used in CHAP between two routers.</td>
</tr>
<tr>
<td><strong>Data Privacy</strong></td>
<td>Only encrypts the shared-secret key password.</td>
<td>Encrypts the entire packets body of every packet. So it is more secure.</td>
</tr>
</tbody>
</table>
Functionality

Performs both authentication and authorization at the same and then performs the accounting separately.

Performs authentication, authorization and accounting separately. This allows a modularity of the security server implementation.

Authorization Process

All reply attributes in the user profile are sent to the router (NAS). The router accepts or rejects the authentication request based on the received attributes.

Server accepts or rejects the authentication request based on the contents of the user profile. The router (NAS) never knows the contents of the user profile.

Accounting

Large number of information fields. So it is nicer for a better understanding of the records.

Limited number of information fields.

Table 4-1: RADIUS and TACACS+ differences [22] [15]

One can conclude that RADIUS protocol is the most frequent protocol used for AAA even though the TACACS+ protocol seems to be better. TACACS+ is more secure and more reliable. The only thing that makes it not being widely used is the fact that it is not a standard protocol but a proprietary one.

Now that we have a better understanding of the two most known AAA protocols, the following section analyses the AAA servers using either RADIUS or TACACS+. It will provide an overview of Cisco Secure ACS which supports RADIUS and TACACS+ and the Microsoft IAS server which supports RADIUS.
5. AAA Server

AAA servers are responsible for receiving user’s connection requests, authenticating users, and then returning all the necessary configuration information for the client to deliver the service to the user. In our case, the AAA server is in charge of receiving the request from the router to connect a specific user. Then, the AAA server authenticates the user and if it is authorized, it returns the configuration information to the router in order to let the user access the network. During all the time the user is having its session, the AAA server performs an accounting task. The name of AAA server comes from the three different tasks the server performs; Authenticating, Authorizing and Accounting.

This section will describe two different products, the Cisco Secure ACS and the Microsoft IAS depending on which Access control end-point method will be used, the Cisco NAC or Microsoft NAP.

5.1 Cisco Secure ACS

Cisco Secure ACS is a network security software application that helps to control access to the enterprise network, dial-in access, and the Internet. Cisco Secure ACS operates as Windows NT, 2000 or 2003 services and controls authentication, authorization, and accounting (AAA) of users accessing the network.[18]

5.1.1 Overview

Cisco Secure ACS provides AAA services to network devices that function as AAA clients, such as routers. An AAA client is any device that provides AAA client functionality and uses one of the AAA protocols (TACACS+ and/or RADIUS) supported by Cisco Secure ACS. Cisco Secure ACS uses both TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment. The Figure 5-1 shows the network architecture.[18]
Cisco Secure ACS helps to centralize access control and accounting, in addition to router access management. With Cisco Secure ACS, network administrators can quickly administer accounts and change levels of services offered for entire groups of users. Cisco Secure ASC offers the use of an external user database which helps companies to use their existing user database.[18]

Cisco Secure ACS is an easy-to-use AAA server, simple to install and administer. The Cisco Secure ACS administration interface is viewed using supported web browsers, making it easy to administer. Figure 5-2 illustrates the Cisco Secure ACS interface.
Cisco Secure ACS v3.3

Cisco Secure ACS v3.3 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authentication, authorization, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit http://www.cisco.com.

Figure 5-2: Cisco Secure ACS web-interface

Cisco Secure ACS authenticates usernames and passwords against the Windows NT, 2000 or 2003 Active Directory, the Cisco Secure ACS database, a token server database, or Novell NetWare Directory Service.

Different levels of security can be used with Cisco Secure ACS. The basic user-to-network security level is PAP. Although it does not represent the highest form of encrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows NT, 2000 or 2003 database. With this configuration, users need to log in only a single time. CHAP allows a higher level of security for encrypting passwords when communicating from a client to the NAS.

CHAP can be used with the Cisco Secure ACS for Windows user database. Microsoft CHAP (MS-CHAP) is a version of CHAP that was developed by Microsoft to work more closely with the Microsoft Windows operating system. Then EAP is allowed with the used of smart cards, certificates and token card. It is done through the use of EAP-MD5.[18]
Multiple Cisco Secure ACS and AAA servers can be configured to communicate with each other as masters, clients, or peers. There are using replication in order to simplify the maintenance. The administrator has to configure the master Cisco Secure ACS and this configuration will be replicated automatically, if desired, on the other AAA servers.[18]

Regardless of which database is used to authenticate users, the Cisco Secure user database authorizes requested network services. Cisco Secure ACS for Windows communicates with the external user database. For Windows NT, 2000 or 2003, Generic LDAP, and Novell NDS authentication, the Application Program Interface (API) for the external authentication is local to the Cisco Secure ACS and is provided by the local operating system. So no further components are required.[18]

### 5.1.2 Internal Architecture of ACS

Cisco Secure ACS provides AAA services to multiple NAS. It includes seven service modules.

The following services are installed on your server:

- **Administration service (CSAdmin):** Cisco Secure ACS is equipped with its own internal web server. It is used for the Cisco Secure ACS configuration through the web interface.

- **Authentication and authorization service (CSAuth):** The primary task of Cisco Secure ACS is to authenticate and authorize requests from AAA clients to permit or deny access to a specified user. CSAuth is responsible for determining whether access should be granted and for defining the privileges associated with each user.

- **TACACS service (CSTacacs) and RADIUS service (CSRadius):** These services communicate between the CSAuth module and the NAS that request the authentication and authorization services. CSTacacs is used to communicate with TACACS+ devices and CSRadius is used to communicate with RADIUS devices. Both services can run simultaneously.

- **Logging service (CSLog):** CSLog is used to capture and place logging information. CSLog gathers data from the TACACS+ or RADIUS packet and CSAuth.

- **Cisco Secure DataBase Synchronisation (CSDBSync) service:** This service performs automated user and group account management services for Cisco Secure ACS. It is used to
synchronize the Cisco Secure ACS database with third-party Database Replication Management Systems.

- **Cisco Secure Monitoring (CSMon):** CSMon is the Cisco Secure ACS self-monitoring and self-correcting service. CSMon works for both TACACS+ and RADIUS and automatically detects which protocols are in use. [18]

Since each module can be started and stopped individually from within the Microsoft Service Control Panel or as a group from within the Cisco Secure ACS for Windows browser interface, one can choose whether or not a service is needed. Anyway, some of the services are compulsory to be started such as CSadmin, CSAuth, CSTacacs or CSRadius and the most important one CSMon.

### 5.1.3 Operations of Cisco Secure ACS

Using either the TACACS+ or the RADIUS protocol, the NAS directs all user’s access requests to Cisco Secure ACS for authentication and authorization of privileges, for example verifying the username and password. Cisco Secure ACS then returns a success or failure response to the NAS, which permits or denies user access. When the user has been authenticated, Cisco Secure ACS sends a set of authorization attributes to the NAS, and the accounting functions begins.[18]

Figure 5-3 shows the step involved when a user try to access the network. The numbers and arrows in green refer to the use of the Cisco Secure ACS user database to access the network while the numbers and arrows in red refer to the use of the Windows NT, 2000 or 2003 user database to access the network.

Referring to the numbers shown in Figure 5-3, when the Cisco Secure ACS user database is selected, the following service and database interactions occur (green numbers and arrows):

1. TACACS+ or RADIUS service directs the request to the Cisco Secure ACS Authentication and Authorization Windows NT, 2000 or 2003 service.
2. The request is authenticated against the Cisco Secure ACS for Windows user database, associated authorizations are assigned and accounting information is logged to the Cisco Secure ACS Logging service.
3. The Windows NT, 2000 or 2003 user database does not authenticate the user.
Referring to the numbers shown in Figure 5-3, when the Windows NT, 2000 or 2003 user database is selected, the following service and database interactions occur (red numbers and arrows):

1. TACACS+ or RADIUS service directs the request to the Cisco Secure ACS Authentication and Authorization service.
2. The username and password are sent to the Windows NT or Windows 2000 user database for authentication.
3. If approved, Windows NT, 2000 or 2003 grants dial permission as a local user.
4. A response is returned to Cisco Secure ACS and authorizations are assigned.
5. Confirmation and associated authorizations assigned in Cisco Secure ACS for that user are sent to the NAS. Accounting information is logged.

Using the Cisco Secure ACS user database requires to manually enter the usernames. However, after the usernames exist in the Cisco Secure ACS user database, administration is easier than using the Windows NT, 2000 or 2003 user database.

An added benefit of using the Windows NT, 2000 or 2003 user database is that the username and password that are used for authentication are the same than the ones used for network login. [18]
5.2 Microsoft IAS server

IAS is the Microsoft implementation of a RADIUS server. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless LAN and virtual private network (VPN) connections. IAS enables to centrally manage user’s authentication, authorization, and accounting, and to authenticate users in databases in the Windows NT, 2000 or 2003 domain controller. It supports a variety of NAS, including Routers. [19]

5.2.1 Overview

Microsoft IAS server provides authentication, authorization, and accounting for many type of network access (LAN, WLAN, VPN, etc…). The router is seen as an AAA client which uses the AAA protocol (RADIUS) supported by the IAS server. [19]

IAS helps to centralize access control and accounting. When an IAS server is a member of an Active Directory domain, IAS uses the directory service as its user account database. The same set
of credentials is used for network access control (authenticating and authorizing access to a network) and to log on to an Active Directory domain. With IAS, network administrators can quickly administer remote access by defining Remote access policies which provide a more powerful and flexible way to manage remote access permission. Microsoft IAS server is easy-to-use since it provides an administration tool named the IAS snap-in. You can run IAS from Administrative Tools on a local computer. To authenticate a connection request, IAS validates the connection credentials against user accounts in the local Security Accounts Manager (SAM), a Microsoft Windows NT Server 4.0 domain, or an Active Directory domain. To authorize a connection request, IAS uses the dial-in properties of the user account that correspond to both the connection credentials and remote access policies.[19]

Different authentication methods can be used with IAS. The basic password-based Point-to-Point Protocol with the basic user-to-network security level is PAP. Although it does not represent the highest form of encrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows NT, 2000 or 2003 database. With this configuration, users need to log in only a single time. CHAP allows a higher level of security for encrypting passwords during the communication between the client and the NAS. Microsoft CHAP (MS-CHAP) and MS-CHAP version 2 are also supported. Then EAP is allowed with the used of smart cards, certificates and token card. It is done through the use of EAP-MD5.[19]

You can use IAS in a variety of network configurations of varying size, from stand-alone servers for small networks to large organization. Multiple IAS servers can be configured with the used of replication if wanted. The synchronisation of the configuration of multiple IAS servers can be performed with the Netsh command-line tool.[19]

IAS collects, at a central location, the accounting records sent by all access servers. IAS also stores audit information (authentication accepts and rejects) and usage information (connect and disconnect records) in log files.[19]

**5.2.2 IAS tasks**
Using the RADIUS protocol, the NAS directs all users’ access requests to Microsoft IAS for authentication and authorization of privileges, which verifies the username and password. IAS then returns a success or failure response to the NAS, which permits or denies user’s access. When the user has been authenticated, IAS sends a set of authorization attributes to the NAS, and the accounting functions begins.[19] Figure 5-5 shows the process encounter when a user tries to access the network.

Figure 5-5: IAS authentication

1. RADIUS service directs the request to the IAS.
2. The IAS server checks the user credentials and the user’s dial-in-properties against the active directory. Does the user’s attempt to connect matches condition of at least one policy? A response is returned to IAS and authorizations are assigned.
3. Confirmation and associated authorizations assigned in IAS for that user are sent to the NAS. Accounting information is logged.[19]

As we have seen in this section, two proprietary AAA servers have been designed in order to support the end-point access control. Both present advantages and disadvantages. The Cisco Secure ACS presents the advantage of running with both TACACS+ and RADIUS as authentication.
protocol while Microsoft IAS proposes only the second one. In the next section, we will have an understanding of the CTA which collects and sends the client’s credentials to the server during the authentication.
6. CISCO TRUST AGENT AND CISCO NAC

6.1 Cisco Trust Agent

Cisco Trust Agent (CTA) is a proprietary Cisco software tool that resides on an endpoint system and collects security state information. It communicates the client’s state to the NAD by using Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP). It is an indispensable agent to be able to use Cisco NAC. Cisco has developed this trust agent software in order to gather and report security state levels to the network policy server. It provides endpoint security information such as operating system version, patch level, CTA version, antivirus presence and version. Figure 6-1 illustrates the CTA Architecture.

![CTA Architecture Diagram]

Figure 6-1: CTA architecture [20]

CTA is for the moment available to install on Windows NT, 2000 and XP SP1. In the coming phase, its availability will be extended to Windows XP SP2, 2003, Linux, Solaris and MAC OS. [20]
6.2 Cisco Network Admission Control (NAC)

Cisco developed its NAC solution to help enterprises define and enforce security criteria that protect them from devices connecting to the network. NAC is a cooperation program where different participants share their technology to provide a new solution. This solution allows organizations to enforce host policies and to regulate noncompliant and potentially vulnerable systems by assigning them to quarantined environments for remediation. By combining information about endpoint security status with network admission enforcement, NAC enables organizations to dramatically improve the security of their computing infrastructures and limits damage due to viruses and worms. The mechanism Cisco has developed extends the EAP protocol at the OSI layers two (EAP over 802.1x) and three (EAP over UDP) to transport the characteristics of a device and facilitate decisions about whether the device should be allowed or not. In turn, the NAD interrogates devices about their current state and forwards decisions about whether to allow individual devices onto the network. Additionally, the process leverages the Cisco Secure ACS to define the access rights.

6.2.1 NAC platform

The process of permitting or denying network hosts access to the network based on the state of their software is called posture validation. The four main components of the posture validation process are illustrated in Figure 6-2.
Figure 6-2: The main NAC components [22]

- **Cisco Trust Agent (seen in Section 6):** A software tool that resides on an endpoint system and collects security state information from security software solutions, such as antivirus and conveys them to the NAD. Cisco Systems has licensed its trust agent technology to the NAC cosponsors security software developers in order to gather and report security state levels to the network policy server.

- **Network access devices (NAD):** Network devices that enforce admission control policy include routers, switches, wireless access points, and security appliances. These devices demand host security "credentials" and relay this information to policy servers, where NAC decisions are made. Based on customer-defined policy, the network will enforce the appropriate admission control decision (permit, deny, quarantine, or restrict). For the moment, only routers are used as NAD in NAC, the use of switches will be released in phase 2 which should be available in a short time.

- **Policy server (discussed in Section 5):** Evaluates the endpoint security information relayed from the NAD and determines the appropriate access policy to be applied. Cisco Secure ACS, the authentication, authorization, and accounting (AAA) RADIUS server, is the
foundation of the policy server system. It works in concert with NAC cosponsor application servers, such as security policy servers that are able to provide deeper credential validation.

- **Management system:** A computer which provides monitoring and reporting tools. NAC cosponsors provide management solutions for their endpoint security software.

- **Remediation server (optional):** When an endpoint does not comply with the enterprise’s policies or does not respond to its challenges, Cisco NAD (in conjunction with Cisco Secure ACS) moves the endpoint to an isolated part of the network. The isolated endpoint might be badly configured or lack some required software updates or security products. Alternatively, enterprises may place additional requirements on users to maintain a certain level of security, such as password strength or power-on passwords. [21]

### 6.2.2 Functionalities of NAC

When a new client tries to log into the corporation network the NAD requests applications and operating system credentials from hosts with EAP request and response packets for authentication. There will be different types of hosts regarding whether they have the CTA installed or not. The first type will be seen as a responsive host and will go through the posture validation process, while the second one will be seen as non-responsive host. This second type is therefore unable to forward any requested credentials so the admission policy will have to be based on other information such as IP address or MAC address (e.g. for printers).

On the NAD, an access control list (ACL) is applied in order to restrict the access to all clients as long as they are not authorized by the ACS server. When the NAD obtains the client credentials, it forwards them to the ACS server. The server will then authenticate and authorize the client. The ACS server may also forward the version data to the vendor’s antivirus server for evaluation. Once the credentials are evaluated, Cisco Secure ACS selects the appropriate enforcement policy for the network device and sends an ACL to the NAD to enforce a specific policy for that host.

Depending on the token compliance defined by the Cisco ACS, the host will be granted access or placed into a quarantine zone or denied access. In the case of quarantine, the host is redirected to a remediation server. Thus the endpoint can update its missing application software in order to meet the required compliance level. Thus after few minutes (depending on what has been defined by the
administrator) the host will go through the posture validation process once more to see if after its updates it can access the network and so on until it meets the compliance policy. [22] Figure 6-3 goes into more details about the posture validation process.
Figure 6-3: The posture validation process
The posture validation process as shown in Figure 6-3:

1. The network client sends IP traffic on the network.
2. If this is the first packet the NAD has received from the client and if the traffic is designated on the NAD as requiring posture validation, the NAD initiates the posture validation process. The NAD applies a default access policy to the client and initiates an EAP over UDP (EAPoUDP) session with the client.
3. The NAD sends an EAP identity request to the network client and then forwards the EAP identity response to Cisco Secure ACS.
4. Cisco Secure ACS establishes a secure PEAP session with the network client and requests the network client security posture credentials.
5. CTA receives the security posture credential request and then requests security posture credentials from the applications on the client. CTA collects all of the security posture information and returns the information to Cisco Secure ACS.
6. Cisco Secure ACS evaluates the security posture credentials for each application on the client. Cisco Secure ACS then performs the credential’s evaluation using rules entered by the network administrator in the ACS database.
7. Cisco Secure ACS consolidates the application posture token into an overall system posture token. The system posture token can have one of the following values:

   - Healthy
   - Checkup
   - Quarantine
   - Infected
   - Unknown
8. Cisco Secure ACS maps the system posture token to a network access policy.
9. Cisco Secure ACS sends the result of the security posture validation and the user notification to CTA on the client. The results of the posture validation are logged and any user notifications are displayed on the screen in a dialog box.
10. Cisco Secure ACS closes the PEAP session with the client and downloads the appropriate enforcement policy to the NAD. The NAD enforces the policy and closes the EAP session with the network client. Based on the access policy, the network client is either permitted on the network, denied access to the network, or quarantined to a remediation network until the client security applications have been updated to the required levels. [21]
At the moment Cisco does not provide the NAC for wireless connections, VPN connections and IPsec connections. It will be provided in the coming development phase of the Cisco NAC. In the next section, we will discuss about another proprietary endpoint security solution provided by Microsoft; the NAP.
7. MICROSOFT NETWORK ACCESS PROTECTION (NAP)

As for Cisco NAC, NAP is a cooperation program where different participants share their technology. NAP also limits damage due to viruses and worms and controls network access by interrogating devices connecting to the network to see if they comply with the network security policy setup by administrators. To be able to use this method, you would need to have the Windows Server “Longhorn” which is planned to be release in 2007. The NAP platform provides enforcement for DHCP address configuration, VPN connections and IPsec connection. Then as in the previous method it will check if the client matches the security policies and then grant, quarantine or restrict the access to the network.

Like NAC, NAP begins with a host client known as a Quarantine Agent (QA) that collects health and security information from third-party software. The QA will ran on Windows XP SP2. Microsoft has also released an API for software vendors to communicate with the QA. When a PC requests an IP address from the DHCP server, the server will ask the QA on the PC to report its system status. The DHCP server then reports this information to the IAS server run on the Windows Longhorn OS using RADIUS messages. The IAS compares the status information with policies stored in various System Health Validators (SHVs). SHV is the policy server that manages and updates each third-party agent, such as an antivirus program. Based on responses from the SHVs, the IAS server will instruct the DHCP server to allocate the PC with an IP address that allows full network access or restricts the PC to a quarantine or remediation area on a network segment.

7.1. NAP overview

NAP for Windows Server "Longhorn" is a new set of operating system components and protocols which provides an interactive platform for protecting networks access. The NAP platform provides an integrated way of detecting the state of a network client that is attempting to connect to the network and restrict the access to this client until the policy requirements for the connection to the network have been met. Figure 7-1 illustrates the different components used by the NAP application.
Figure 7-1: NAP platform components

- **NAP clients** are computers that try to access the network using DHCP configuration, remote access VPN connections, or secure communication with IPsec.
- **NAP servers** are computers running Windows Server "Longhorn" that support network access enforcement for NAP clients. It can be a **VPN server** that allows VPN-based remote access connection or a **DHCP server** that provides automatic address configuration.
- **IAS servers** are computers running Windows Server "Longhorn" that support system policy configuration for NAP clients.
- **Health certificate servers** are computers running Windows Server “Longhorn” that issue health certificates to IPsec-based clients.
- **Active Directory** stores user credentials for VPN connections.
- **Remediation resources** are servers that allow quarantined clients to update their states so that they can comply with network policy requirements.

Now the following Figure shows the interaction between those different components.
The two first set of communications concern the existing interaction when we are in presence of a DHCP client.

1. The DHCP client uses DHCP messages to obtain a valid IP address and to indicate its current system health state using a Statement of Health (SoH). The DHCP server uses DHCP messages to either allocate an IP address for the restricted network with the remediation instructions or an IP address for normal access to the intranet.

2. The DHCP server sends RADIUS messages to the IAS server that contains the settings of the DHCP client's system health state. The IAS server sends RADIUS messages to the DHCP server to indicate that the DHCP client is granted normal access or that the DHCP client should be placed on the restricted network until it becomes compliant.

The two next set of interactions regard the connections of VPN clients.

3. The VPN client uses PPP messages to establish a VPN connection and PEAP messages over the PPP connection to indicate its current system health state, using a SoH. The VPN server uses PEAP messages to follow IAS server messages that indicate remediation instructions or granted access.
4. The VPN server sends RADIUS messages to transfer PEAP messages sent by the VPN client. The IAS server sends RADIUS messages to indicate that the VPN client is granted normal access or that the VPN client should be placed on the restricted network.

The two coming set of interactions show the protocol used when an IPsec client tries to access the network.

5. The IPsec-based NAP client uses HyperText Transfer Protocol over Secure Socket Layer (HTTPS) to create a secure session with the health certificate server to indicate its current system health state using a SoH. The health certificate server uses the HTTPS session to send remediation instructions or to send a health certificate to authenticate communications initiated.

6. The health certificate server sends RADIUS messages containing the settings of the IPsec-based NAP client's system health state to the IAS server. The IAS server sends RADIUS messages to indicate if access is granted or if remediation should be performed.

Finally, the last set of interactions are those in relation to the policy server which contains resources to keep network clients policy-compliant and provides remediation for NAP clients that are not policy-compliant.

7. When the NAP client has normal access to the network, it accesses the policy server to ensure that it remains healthy and updates itself. If the NAP client is connected to the restricted network, it accesses the policy server to become network policy-compliant, based on given instructions from the IAS server.

8. When performing network access validation for a NAP client, the IAS server might have to contact a policy server to obtain information about the current requirements for system health.

7.2. NAP Platform

In reality NAP is more complex than what is explained in the previous section. Each client includes a System Health Agent (SHA); provided by the third party vendors; which performs the health updates and publishes its status as a SoH to the QA. The QA is an agent that maintains the system restricted state and has the role of interface between the SHA and the Quarantine Enforcement
Client (QEC). The QEC play the role of interface between the client and the server. In fact it will pass the computer’s health status to the NAP server. However as seen before, each type of connection is defined by the use of a specific server. The QEC also requests the type of network access the client wants. So the QEC will decide what sort of packets to use to send the SoH to the server. Those QEC matches with Quarantine Enforcement Server (QES) on the NAP server. The QES passes client’s health status to the IAS server for evaluation. Once the SoH arrives in the IAS server, a SHV verifies that the system health information contained in the SoH complies with the required system health state. The SHV returns a SoH response which is passed to the SHA on the client and indicates how the SHA can become policy compliant. As for the SHA, the SHV are provided by the third party vendors and often matches with the policy server. For example, the SHV for checking antivirus signature will be matched to the server which contains the latest signature file.

7.2.1 The Client architecture

The client is composed of three elements:

- System Health Agents (SHAs)
- Quarantine Enforcement Clients (QECs)
- Quarantine Agent (QA)

Figure 7-3 presents the client architecture.

The first software to consider is the System Health Agent (SHA) which updates the system state and publishes the state as a SoH to the QA. This SoH contains all the client information needed by the IAS server to decide whether the client will be granted or denied access. As you can see on the Figure 7-3, SHA communicates with the policy server which is a computer that contains resources to keep clients healthy and to provide remediation for clients that are not healthy.

The second software to describe is the QEC which is the one requesting the access to the network. It also passes on the decided client status for the network access to other client software. There are three types of QEC, one for each type of connection: DHCP QEC, VPN QEC and IPsec QEC. They can be seen in the Figure 7-3 as QEC_A, QEC_B and QEC_C.
Finally, the QA coordinates information between the System Health Agents (SHAs) and QECs as for example the collection of SoH from the SHA to pass them to the QEC when requested. It also takes care of maintaining an updated list on the current health state of the client, meaning for example that if the connection is refused the QA will update the health state to remediation.

7.2.2 The Server architecture

The server is composed of four elements:

- System Health Validator (SHV)
- Quarantine Server
- Quarantine Enforcement Server (QES)
- IAS

Figure 7-4 illustrates the server architecture.
The first element we can see on the Figure 7-4 is the SHV which is software placed on the server. It validates the information provided from the corresponding system health agent (SHA) on the client to verify whether the SoH complies with policy or not. In the initial release of the NAP platform, SHVs run on the IAS server. SHV communicates with the policy server to be able to verify if the information contains in the SoH are up to date or not.

Then, as for the QA on the client, the Quarantine Server is in charge of coordinating the values returned by all the system health validators (SHVs) and determines whether Quarantine Enforcement Server (QES) components should isolate the client or not from the network based on their policy compliance status.

Then, like in the client, we have quarantine enforcement software called Quarantine Enforcement Server (QES). It is responsible for passing the client health status to the IAS server for evaluation. As for the client, there are three types of QES, one for each type of connection: DHCP QES, VPN
QES and IPsec QES. They can be seen on the Figure 7-4 as QES_A, QES_B and QES_C. They will be placed respectively on DHCP server, VPN server and Health Certificate Server.

7.3. Operation of NAP

In the previous section, the architecture of the client and the server were described. This section will explain the way they communicate together. The figure 7-5 shows the communications between clients and servers.

![Figure 7-5: Communication between client and server NAP components](image)

When a client requests access to the network, the QEC sends a request to the corresponding QES. In more details, the QEC will request the QA to provide the SoH. The QA will forward this request to the SHA. The SoH returned by SHA will be gathered with other information in a form called SoH that will be passed on to the QEC via the QA. The SoH will be transported to the QES via DHCP messages, PEAP or HTTPS regarding the type of connection the client is attempting (see Figure 7-
1). The DHCP server, VPN server or Health Certificate server will forward this message via RADIUS to the IAS server. At that stage, the Quarantine Server pass the SoH to the SHV for evaluation. The SHV will contact the needed policy server to see if the information contained in SoH are up to date and compliant with the network requirement. Then the SHV returns a SoH response that will be forwarded by the Quarantine Server using a RADIUS message to the QES in the NAP server. The QES will send the SoH response to the corresponding QEC which will forward it to the QA. This one will now update the state of the client regarding the answer given by the SHV. Now two cases can appear for each connection either the client is granted the access, or it is placed in the remediation network. In case of DHCP client, if the client is placed into the restricted network the DHCP server assigns the quarantine subnet mask and the quarantine route addresses, as the network administrator has defined. Then the QA of this DHCP client reports its status to the SHA, which forwards it to the policy server and requests updates. As soon as the SoH is updated, the normal authorization procedure takes place. In case of a VPN client, the client is isolated to the restricted network and the same steps as for DHCP client take place. In case of a IPsec client, the Health Certificate server tells the client how to correct its health status and does not deliver a health certificate for that client. Therefore, the client cannot initiate any communication with computers other than the policy server in order to update its state to healthy. Then the client sends its updated SoH to the health certificate server. When the IAS server validates the updated SoH, the health certificate server issues a health certificate to the client.

Depending on network needs, an administrator might choose to define some computers, devices, and users exempt from network access requirements. For example, some versions of Windows do not support NAP, so computers running these versions of Windows are always isolated by default. However, the network administrator can configure an exception for these computers. If an exception is configured, these computers are not checked for compliance, and they will have normal access to the network.[23]
8. INFOEXPRESS CYBERGATEKEEPER

As for the method seen earlier, the CyberGatekeeper product separates non-compliant systems on the network from compliant ones, placing the non-compliant systems into quarantined networks.

8.1 CyberGatekeeper overview

As for the previously discussed method, this solution also uses an agent on the endpoint machine that will collect the system information and pass them on to the CyberGatekeeper server for access analysis. This agent could be CTA since InfoExpress is one of the Cisco NAC partner. The client platforms are for the moment the same as for Cisco NAC and potentially the same as for other Network Admission existing solutions. It also looks similar in the fact that administrators create policies defining compliance requirements. Those policies are then loaded into the CyberGatekeeper server. Using these policies and information obtained from the endpoint system, CyberGatekeeper server assesses the endpoint compliance state. Only compliant endpoints are granted access the network, while non-compliant endpoints are left on the restricted network until they become compliant. Figure 8-1 illustrates the CyberGatekeeper solution.
As you can see in Figure 8-1, the CyberGatekeeper offers two solutions: The CyberGatekeeper LAN Appliance to control endpoint access in LAN/WAN and WLAN environments, and the CyberGatekeeper Remote Appliance that enforces security with remote endpoints attempting to access network through VPN connections. This solution differs from both previous solutions since as soon as the host tries to access the network it is placed in the restricted network until access is granted. This will be examined further in the following sections.

8.2 CyberGatekeeper platform

The platform is composed of three main components. CyberGatekeeper solution consists of end user software and back end components. CyberGatekeeper Agent (CGAgent) obtains information from the endpoint system; CyberGatekeeper Server (CGServer) evaluates whether or not the end user machine complies with policy, and then grants or denies network access based on that result; CyberGatekeeper Policy Manager (CGPM) also lets administrators define what applications and
configurations are required or prohibited on end systems. Figure 8-2 gives an overview of the components interaction. Then a detailed description is provided below the figure.

![Diagram of CyberGatekeeper components](image)

**Figure 8-2: Interaction of the components**

- **The CyberGatekeeper Policy Manager.** It allows administrators to create policies that contain criteria that determine whether clients are compliant or not with the policies. Administrators are also able to create the installation files of the Agent run on endpoint machines. So several Agent can be used. And finally, it distributes the policies to the CyberGatekeeper Servers.

- **The CyberGatekeeper Server.** It evaluates endpoint compliance to the defined policies and permits or prohibits access to the network. The endpoint CyberGatekeeper Agent sends audit information to the CyberGatekeeper Server, which decides whether or not the client should be allowed to connect to the company network. The requirements for the network access are created, managed and distributed by the CGPM. The location of the CyberGatekeeper in the network will be different regarding the type of connection. In case of VPN access, it is placed between the remote access entry point and the company network.
For LAN access, it has to be placed in order to communicate with the switches. Figure 8-1 illustrates the different placement of the CyberGatekeeper Server.

- **The CyberGatekeeper Agent.** It is installed on the clients and collects information about their status and passes it on to the CyberGatekeeper Server. There are two different type of agent available: a desktop agent and a Web-based agent. The CyberGatekeeper Agent is distributed to users by the CGPM as a self-extracting installer.

As you can see in Figure 8-2, the CyberGatekeeper Server gives the access response to the Network Access Point which will then apply the policies and deal with the client. The following part explains the functioning of the solution.

### 8.3 Functionalities of Cybergatekeeper

Administrators first create policies on the CGPM, build agents, and distribute policies to CyberGatekeeper Servers; CyberGatekeeper LAN Appliance and CyberGatekeeper Remote Appliance who enforce the enforce policies. The designed policies contain validation criteria that determine whether endpoints are in compliance with policies or not. When an endpoint user wants to access the network, the DHCP server will first place that host on the restricted network by distributing a determined IP address. The CyberGatekeeper Agent present on the user’s machine will collect the system information such as the OS name, patch level or Antivirus protection level and send them to the CyberGatekeeper Server when requested. The CyberGatekeeper Server will determine what information to request depending on the appliance of the server. Then this CyberGatekeeper Server LAN appliance or Remote Appliance will assess the endpoint compliance state regarding whether it fulfils its policies. Only compliant endpoints are granted access the network, while non-compliant endpoints are left on the restricted network until they become compliant. The access is controlled through the three step process described below and shown on Figure 8-3.
1. CyberGatekeeper Server audits end systems requesting access to the corporate network.
2. CyberGatekeeper Server checks endpoint compliance.
3. CyberGatekeeper Server allows compliant endpoints to access the corporate network and blocks non-compliant endpoints in the restricted area until they are remediate.

We have to be more precise about the step used to grant or deny access to the network. After auditing an endpoint, CyberGatekeeper Server should determine that the endpoint system complies with policy and should gain access to the network. To allow endpoint access, CyberGatekeeper Server must notify network access devices that the endpoint traffic should be allowed. Network access devices will support various methods of achieving this.

The methods to control access to the network are embedded into enforcement modules (EMs). Enforcement modules provide the means to control different types of network infrastructure devices and components. The administrator must select the proper enforcement module to allow CyberGatekeeper Server to control network access for a given network access point. Specific
policies are defined in each enforcement module and are applied by the NAD to the endpoint user when they are fulfilled.

For example, some switches and wireless access points may be 802.1x compliant, so they can use the RADIUS EAP enforcement module. Another portion of the network may have an IPSec VPN, which is only supported by the Bridge enforcement module. Some other switches on the network may only support basic VLAN assignments (non 802.1x), so these may need to use the LAN enforcement module. The following figure shows which enforcement module deal with which network access devices

![Enforcement Modules and Network Access Devices](image)

**Figure 8-4: Enforcement Modules and Network Access Devices correspondences**

With many enforcement modules available on CyberGatekeeper Server, companies have the flexibility to use policy based access for a large portion of the network infrastructure. Many network access devices are supported by more than one enforcement module, so administrators can choose the enforcement module which best matches their specific requirements; such as uniformity, response time and/or flexibility.
Therefore in order to sum up the way CyberGatekeeper works, administrators will define policies for each enforcement modules. Those policies will be distributed on each enforcement modules on each CyberGatekeeper Server. When an endpoint requests access to the network, the CyberGatekeeper will determine which enforcement module to use regarding the requested type of connection and the preference defined by administrators. Then the chosen enforcement module will request the CyberGatekeeper Agent to send some specific credentials regarding its policy enforcement. Once the enforcement module analyses compliance, it will contact the corresponding Network Access Device (NAD) with the access response; granted or not; and with the access right to apply to the client. If the endpoint is compliant, they will be granted access to the company network with some restriction or not depending on the type of connection and if it does not comply with the policy, it will remain in a restricted area and be able to contact a remediation server to update its status and therefore try again to access the network.
9. NAC configuration tutorial

This section explains all the steps that an administrator has to take in order to configure different elements for Cisco NAC. First, a description of the Cisco Secure ACS configuration step is given, then the step to take on each network client for installing and configuring the CTA is explained. After that, the router configuration example is given and explained. Finally, some troubleshooting are provided based on my own experience.

9.1 ACS configuration

A 90 days trial version of Cisco Secure ACS version 3.3 can be found on Cisco web site. After installing it, open your browser and type the following address: http://127.0.0.1:2002 or http://server_ip_address:2002. The following page will appears.
9.1.1 Administrators and administrative policy

The first thing to do is to create an administrator account for the use of ACS. It is useful if you want to access to the AAA server interface remotely. Click on the Administration control button, then create the administrator user name and password and finally tick the “Grant all” box. Then push the submit button. The following figure shows those steps.

**Figure 9-2: Administrator account setup**

9.1.2 Interface configuration
The first thing to perform before any configuration is to define the needed option to configure ACS. Click on the interface configuration button on the left hand menu and then click on advanced option. Once in this menu, tick the options circled on Figure 9-3.

![Figure 9-3: Selected interface option](image)

Then select the RADIUS (Cisco PIX/IOS) and thick the cisco-av-pair option as shown in the following figure.

![Figure 9-4: Selected RADIUS configuration option](image)
And finally, select the RADIUS (IETF) and tick this following option: [027] Session-Timeout.

### 9.1.3 Network configuration

Now the different AAA server existing in the network as well as all the existing routers have to be configured. Click on the add new AAA client to create a new router, and then you have to define all the properties of this router as shown in Figure 9-5. You have to be very careful with the key which have to be the same as the one defined in the router configuration and on the server setup. Then select RADIUS (Cisco IOS/PIX) in the “authenticate using” field. At the moment NAC is working only by using the RADIUS protocol with Cisco Internetwork Operating System (IOS) routers. After that, in order to be taken into account, click the “submit + restart” button.

![AAA Client Setup For NACRouter](image)

**Figure 9-5 : AAA client setup example**
As for the AAA client, to configure the AAA server click on the add new AAA server button, write the name of your server and fill up the setup form as shown in the following figure. Once it is done, click on the “submit + restart” button. Once it is done, the configuration will continue with the server certificate installation. On the left menu click on the “System configuration button”.

![Figure 9-6 : AAA server setup example](image)

**9.1.4 System configuration**

The menu page is as shown in Figure 9-7. We will mostly talk about the steps to take to install the certificate as well as how to configure the authentication. The “Service Control” button permits us to manually restart the services of the Cisco ACS and to define the option concerning the Service log file. The “Logging” button allows us to choose which logging we want among Failed attempt logging, Passed authentication logging, and others. The following attributes: Message-Type, Reason, Application Posture-Token, System Posture-Token and Authen-Failure-Code were found very useful. Then with the “ACS Backup” button a manual backup of your existing ACS configuration or an automatic one if you wish to can be perform. The “ACS Restore” button permit to load an existing saved configuration.
By clicking on the “ACS Certificate Setup” the certificate installation will be performed. Figure 9-8 illustrates the certificate menu.

In case no certificate exists on the ACS server, a self-signed certificate has to be generated. First a subject for your certificate need to be given such as the name of your server for example by writing CN=Name_of_your_server. Then write the path where the certificate and the private key should be store by giving a understandable name that one knows what is that certificate for. For example the
name of your server followed by the letters ACS could be used. The certificate file is a .cer file while the private key file is a .pkv file. The key length and the Digest to sign with have to be as shown in Figure 9-9. Then the installation of the certificate can be done manually or automatically as done in the following figure.

**Generate Self-Signed Certificate**

| Certificate subject        | cn=CISCO1 |
| Certificate file           | C:\Certificate\CISCO1.cer |
| Private key file           | C:\Certificate\CISCO1.pvk |
| Private key password       | ********** |
| Retype private key password| ********** |
| Key length                 | 2048 bits |
| Digest to sign with        | SHA1       |
| Install generated certificate| ✔ |

*Figure 9-9: How to generate a self-signed certificate*

Once the installation is done, go to “Install ACS certificate” as displayed in Figure 9-8 earlier and the page that appears should look like Figure 9-10.

**Install ACS Certificate**

| Issued to:        | CISCO1     |
| Issued by:        | CISCO1     |
| Valid from:       | elokuu 02 2005 at 19:05:29 |
| Valid to:         | elokuu 02 2006 at 19:05:29 |
| Validity:         | OK         |

*Figure 9-10: Installation of the ACS certificate*

Now if there are some replication ACS servers in the network, the certificate file and the private key file of you main ACS server should be copied to other ACS servers. The installation of those files...
can be done by clicking on “Install ACS certificate” in the Certificate Setup menu and then by clicking on the “Install New Certificate” button as shown in Figure 9-10 and by filling up the path where the certificate was pasted and by writing the private key password when requested. The last thing to do is to click on “ACS Certification Authority Setup” in the Certificate Setup menu and enter the location of the certificate just installed. Then go to “Edit Certificate Trust List” in the Certificate Setup menu and then tick the certificate just installed. The certificate installation is then done on all the existing network servers. Now a definition of the type of authentication that will be used need to be done.

To do so, click on the “Global Authentication Setup” link on the System Configuration menu. The only compulsory box to tick is “Allow CNAC”. Then submit and restart the ACS services as shown in Figure 9-10. Now that some basic components of the NAC system are configured, the ACL that will be used when NAC will be operating have to be set up. In order to configure the ACL, click on the “Shared profile components” button on the left menu.
9.1.5 Shared profile components

The first thing to do is to decide if a dedicated server for remediation will be used. If a dedicated server for remediation is used and there is more than one NAD in the network, then click on the “Network Access Filtering” link. In the name field, give a clear name for this filtered access. Then, select to which devices the filter will take place as shown in red on the Figure 9-12. This is useful for the ACL configuration.
In order to enter the ACL in the ASC server click on the “Downloadable IP ACL” link. Five different ACLs have to be created. Each one will correspond to the different state our client could take once authenticated. Those names are Healthy, Checkup, Quarantine, Infected and Unknown. For each ACL created, one has to define the content. Figure 9-13 present as a table the configures downloadable access list content on the left side and the content of each of the ACL on the right side.

As you can see in Figure 9-13, in the “Quarantine” downloadable IP ACL, the “Network Access Filtering” box select “u206srv1”. It means that when a client is defined in Quarantine, the router will apply the Network access Filtering defined by “u206srv1”. In this case it would be to forward all the client requests to “NACRouter” which is in charge of establishing the connection between the client and the remediation server. The next things that will be done is to configure the groups that will be used by Cisco NAC during authentication by clicking on the “Group Setup” button on the left menu.
### Figure 9-13: Downloadable IP ACL configuration example

<table>
<thead>
<tr>
<th>ACL Contents</th>
<th>Network Access Filtering</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit_all</td>
<td></td>
<td>permit_all</td>
<td>ACL for healthy MAC group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>client_Checkup</td>
<td>ACL for MAC client in checkup condition</td>
</tr>
<tr>
<td>u206send</td>
<td>u206send</td>
<td>u206send_quarantine</td>
<td>Then compliance not find, redirect client to remediation server</td>
</tr>
<tr>
<td>Client_infected</td>
<td>Client_infected</td>
<td></td>
<td>ACL for infected MAC clients</td>
</tr>
<tr>
<td>Client_unknown</td>
<td>Client_unknown</td>
<td></td>
<td>ACL for unknown MAC clients</td>
</tr>
</tbody>
</table>

#### 9.1.6 Group Setup

- **permit_all**
  - ACL for healthy MAC group
- **client_Checkup**
  - ACL for MAC client in checkup condition
- **u206send**
  - Then compliance not find, redirect client to remediation server
- **Client_infected**
  - ACL for infected MAC clients
- **Client_unknown**
  - ACL for unknown MAC clients
When the Group Setup window appear, click on “add a group”. Then enter the name of the group. Repeat this step until all the following groups have been created. Those groups correspond to all the state the client can take: Healthy, Checkup, Quarantine, Infected and Unknown. Figure 9-14 shows the window display by the system when you have created all those groups.

![Group Setup](image)

**Figure 9-14: The compulsory groups to create**

For each group, one needs to edit it and fill up the settings as shown in Figure 9-15. For each group, the downloadable IP ACL to be used needs to be define by choosing the correspondent one and then ticking the “[009001] cisco av-pair” box when a value for posture-token and status query timeout have be written. Those values are the one send by ACS to the router when authentication is accepted. Be careful to not make any mistake in the spelling of the posture-token value and to write it in lower case letter. The router knows only the five following posture-token: Healthy, Checkup, Quarantine, Infected and Unknown. Then the value given to the status query timeout is the time (in seconds) the client will stay in that posture until it requests reauthentication. As it can be understood, it is important this time being short for quarantine status for example. If the requesting computer need to be redirect to the remediation server and this redirection has not been mentioned earlier in the ACL, then the following string need to be written as well: url-redirect=http://ip_address/. It will ensure that the client can only access this specific IP address. Finally, by ticking the “[027 Session-Timeout] box, the time entered in seconds is the time after which a revalidation process take place.
Figure 9-15: NAC Groups settings
Now the ACL and the group settings have been configured. The next step to perform is the definition of the external user database. An unknown user policy will be defined and the database against which authentication will be done will be configured. The policies used to authenticate users will also be entered.

### 9.1.7 External User Database

In the external user database menu click on the “database configuration” link. Then another menu appears with different database. By selecting the “windows database” link, the database the client will authenticate it’s login and password with will be defined. Once it is done, click on the “configure” button and select to which domain(s) the client have to authenticate. Then click on the “submit” button.

Now the NAC will be configured by clicking on the first link of the list. Once more, click to the “configure” button, give a name to the NAC database and then click on the “edit list” button to configure the mandatory credential types. Choose which credential types are needed and click on “submit”. There are four credential types: PA stands for CTA, Host and HIP stand for Cisco Security Agent and finally AV stands for Antivirus Vendor Attributes. Now that the mandatory credentials have been chosen, click on the “local policy” button or “external policy” button to configure the database policies. The external policy has to be validated by an external server; it is the case for Antivirus policy for example. Of course, once the database is configured, click on the “save configuration” button. Figure 9-16 shows an example of a NAC database configuration with one mandatory credential type and two local policies.

To configure correctly the local and external policies, administrators have to think of all the existing computers onto the network and all possible configuration they may find in the network to configure the policies’ rules. Once all the existing configuration have been determined, click on “new rule” button. Figure 9-17 gives an idea about how to build rules. The logical rule operator is OR while the logical policy operator is AND. That means that from the moment a rule is true, the returned token will be the one written in the token box. If the client does not match any of the rules, then it will be allocated to the default rules. Then each token of each policy is returned and goes
through the AND operator to determined the final system status. The worst token among the list of policy token will always be the one returned.

**Network Admission Control Expected Host Configuration**

![Network Admission Control Expected Host Configuration](image)

**Figure 9-16: Network Admission Control example configuration**
The following step to perform is to map the databases and their policies to the groups created earlier. To do so, click on the “Database group mapping” link. The list of all databases created earlier are listed. In our example, Windows database and NAC. For NAC, all the different tokens have to be matched with an existing group created earlier as shown in Figure 9-18. The PA user message is the status notification which appear on the client screen. In our Quarantine example, the procedure the user should follow to update its system is described.
### 9.1.8 User Setup

In the case the CTA is not available on the client, it should be placed to the unknown group in order not to be placed in quarantined area. To do so, click on the “user setup” on the main menu. Add a user named “Clientless”. Click the “add/edit” button and select to passed the authentication through Cisco Secure Database, then type the password “cisco123” in the CiscoSecure PAP password field.
and finally select unknown group to be assigned to. Figure 9-19 illustrates the step to take to configure the unknown user. Now the configuration of the ACS for NAC is finish, but few steps remained to be done on all clients.

![Clientless user configuration](image)

**User: Clientless**

**User Setup**

Password Authentication:

- CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked)
  - Password
  - Confirm Password
- Separate (CHAP/MS-CHAP/ARAP)
  - Password
  - Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

**Group to which the user is assigned**

- Unknown

Submit Cancel

---

**9.2 Client configuration**

For each client of the network the CTA software need to be installed. it can be download for free on the Cisco website. Then unzip the file which contains the posture plug-in files for the Cisco:PA credential. In that same folder, import a copy of the ACS server certificate. Then an installation of the imported certificate need to be performed, so open a command windows, place yourself under the folder where CTA has just been installed and type the following command: `ctacert /add C:certificate_file_location\certificate.cer /store root`. A message will appear telling that the certificate has been installed. Two ini file written with their default values have been installed and they can be changed. Those two files, ctad.ini and ctalogd.ini are given with an explanation in the appendix 1. Now, the last configuration that has to be done is the Cisco IOS router configuration.
9.3 **Router configuration**

The router configuration should look like the one display in appendix 2. The following paragraphs explain more in details the step to take to configure the Router as a NAC enforcement device.

### 9.3.1 AAA server communication

Enter the following command to define a new AAA configuration model:

```plaintext
aaa new-model
da auth default group radius
aaa session-id common
```

Then an indication of who is the RADIUS server and what is the shared key need to be done. The IP address interface from which ACS receives RADIUS packets has also to be specified. Then the http server for URL redirection has to be enabled. And finally non-standard attributes to be sent to RADIUS can be optionally allowed.

```plaintext
radius-server host 192.168.1.202 auth-port 1645 acct-port 1646
radius-server key sabria
ip radius source-interface FastEthernet0/0.50
ip http server
ip http authentication aaa
radius-server vsa send authentication
```

### 9.3.2 EOU authentication method

The following command enables the EOU (EAP over UDP) posture validation process. The Admission Control will be done on each interface the policy is applied.

```plaintext
ip admission name ENTREE eapoudp
```

By using the following command, the host (192.168.59.10) is allowed to communicate with another host (192.168.59.1). It is useful for printers or host that do not have the CTA install and to redirect them to the remediation server (192.168.1.51) using the URL redirection command. It can be used only if the determined host has a static IP address.

```plaintext
identify profile eapoudp
device authorize ip-address 192.168.59.10 policy NACclientless
identity policy NACclientless
access-group clientException
redirect url http://192.168.1.51/update
ip access-list extended clientException
```
Another solution for client without CTA is to configure a clientless user policy. The router inserts the clientless username during the authentication process. Then the ACS returns the token according to the group in which the user clientless is placed; usually the unknown group. This is used mainly when DHCP is used.

eou clientless username clientless
eou clientless password cisco123
eou allow clientless

### 9.3.3 EOU timers and logging

The following commands configure the EOU posturing processes timers. The first command will ignore packets from a host that has failed its authentication for a period of 60 seconds. Then the second command set the revalidation period for all clients. Here 600 seconds but it may be overwritten by the RADIUS av-pair command defined in the different group in Cisco ACS. The last command enable syslog messages from the posturing process. It is really useful to understand what is happening. Appendix 3 presents a part of a syslog message and its explanation.

eou timeout hold-period 60
eou timeout revalidation 600
eou logging

### 9.3.4 ACL and interface configuration

On every interfaces of the router where client can be connected, an ACL has to be defined to allow only UDP packet. By defining the ACL that way the endpoint cannot access to the company network neither to the internet but can request access and authenticate. The `ip admission ENTREE` command applies the previously configured NAC policy to the interface once the endpoint has been authenticated and given a token. Now the NAC configuration is done! The next section will discussed some troubleshooting that have been met for the NAC configuration during this thesis work.

interface FastEthernet0/0.51
   ip address 192.168.58.254 255.255.255.0
   ip access-group 101 in
   ip admission ENTREE
access-list 101 permit udp any any

9.4 Troubleshooting

9.4.1 ACS Installation troubleshooting

If a proxy server is used in the network, add the address of the ACS server in the proxy table. Else the administrator will not be able to log into ACS to configure the server. The main page request for a login and a password as shown in Figure 9-20. The problem is that if the ACS server IP address is not add to the proxy address, the ACS server sees any connection attempt as a remote connection and therefore ask for administrator login and password that do not exist yet.

![Cisco Secure ACS v3.3](image)

Figure 9-20 : Remote access to Cisco Secure ACS through the client
9.4.2 CTA configuration troubleshooting

The NAC configuration does not seem to work and when a look on “report and activity” and “Failed Attempts” on ACS is done the following table and message appear:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Reason</th>
<th>Application-Posture-Token</th>
<th>System-Posture-Token</th>
<th>AAA Server</th>
<th>NAS-TP-Address</th>
<th>User-Name</th>
<th>Authentication-Failure-Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/31/2005</td>
<td>23:52:13 ..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>CISCO1</td>
<td>192.168.1.1</td>
<td>00d0.b753.07aa</td>
<td>EAP-TLS or PEAP authentication failed during SSL handshake</td>
</tr>
<tr>
<td>07/31/2005</td>
<td>23:36:47 ..</td>
<td>..</td>
<td>..</td>
<td>..</td>
<td>CISCO1</td>
<td>192.168.1.1</td>
<td>00d0.b753.07aa</td>
<td>EAP-TLS or PEAP authentication failed during SSL handshake</td>
</tr>
</tbody>
</table>

Figure 9-21: SSL handshake Authentication failed attempt

The problem is that the server and the client cannot even begin to “discuss”, they don’t recognize each other. This problem was caused by a mistake in the cta.ini file on the client. The server was not able to satisfy the following rules because CN="abc” corresponding to the server certificate was not written. Another solution would be to erase those commands from the file since they are optional.

[ServerCertDNVerification]
TotalRules=1
Rule1=CN="CISCO1"

9.4.3 NAC external database configuration troubleshooting

In the Failed Attempts log the following table is obtained:
This time, NAC seams to function but fails all the client access trials. The Authen-Failure-Code column displays the following message “External DB account restriction” while the given reason is “No matched mandatory credential types in any external host configuration”. The problem was coming from an incorrect configuration of the mandatory credential type in the Network Access Control database. While the policies rules were using Cisco:PA credential type, the used and needed mandatory credential was not selected. By adding the used credential in the list, the problem was solved.

9.4.4 Passed authentication log

Now that we have seen the problem that had to be solved in this thesis work, a look at a passed authentication log should also be done. Figure 9-23 illustrates this log file.
By examining this log file, a better understanding on how the policies really function can be given. When there is only one policy with one rule, the application posture token and the system posture token will always return the same token (cf violet Quarantine and green Healthy). Then when the authentication is against two or more policies containing at least two rules plus the default policy, it is harder to see how it exactly functions. This log file shows that first a rule will be select in each policies; all policies will return their corresponding token (as seen in blue, red and pink) in the application posture-token column. The posture-token that will actually take the client is defined by the logic operation of all those return token and will return the worst token (red and pink).

The next figure was taken on the client during a quarantine status to confirm that the defined ACL was applied. As you can see, the client could access neither Internet nor ACS server. On the contrary, it could access the remediation server as defined in the ACL.

### Passed Authentications active.csv

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Message-Type</th>
<th>Reason</th>
<th>Application Posture-Token</th>
<th>System Posture-Token</th>
<th>AAA Server</th>
<th>Source-NAS</th>
<th>NAS IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/16/2005</td>
<td>14:57:23</td>
<td>Authen OK</td>
<td>Database-configuration=NAC, Rule=Default Rule</td>
<td>PA Cisco=Checkup, PA Cisco=Healthy</td>
<td>Checkup</td>
<td>CISCO1</td>
<td></td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>08/16/2005</td>
<td>14:47:04</td>
<td>Authen OK</td>
<td>Database-configuration=NAC, Rule=Default Rule</td>
<td>PA Cisco=Healthy, PA Cisco=Unknown</td>
<td>Unknown</td>
<td>CISCO1</td>
<td></td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>08/16/2005</td>
<td>14:44:55</td>
<td>Authen OK</td>
<td>Database-configuration=NAC, Rule=Default Rule</td>
<td>PA Cisco=Healthy, PA Cisco=Healthy</td>
<td>Healthy</td>
<td>CISCO1</td>
<td></td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>08/16/2005</td>
<td>14:42:42</td>
<td>Authen OK</td>
<td>Database-configuration=NAC, Rule=Default Rule</td>
<td>PA Cisco=Healthy, PA Cisco=Healthy</td>
<td>Healthy</td>
<td>CISCO1</td>
<td></td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>08/15/2005</td>
<td>16:24:34</td>
<td>Authen OK</td>
<td>Database-configuration=NAC, Rule=Default Rule</td>
<td>PA Cisco=Quarantine</td>
<td>Quarantine</td>
<td>CISCO1</td>
<td></td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>

**Figure 9-23: Different passed authentication**
The Appendix 4 illustrates the capture of packets taking place between the different element of the network during the authentication process. You can clearly see the RADIUS messages in light blue in the communication between the ACS server and the AAA client (router).
10. Conclusions

This thesis gave an overview of three different endpoint security solutions, Cisco NAC, Microsoft NAP, and InfoExpress CyberGatekeeper. We have seen that all those solutions use the same principle. An agent on the host collects other software status such as Antivirus, OS version. Then the agent communicates that information to a policy server, which compares the host’s credentials to the predefined policy. So the principle is the same but the execution is different for each solution.

It is known that Cisco is dominating market share in the networking production while Microsoft leads in desktop operating system. Therefore, it is logical for the Cisco NAC solution to be based on hardware while Microsoft NAP is based on software. The solution proposed by InfoExpress is based on hardware as Cisco NAC. But in the case of Cisco NAC, only Cisco NADs can be used while InfoExpress CyberGatekeeper does not make any differences between a Cisco and a Juniper NAD. The solution is proprietary but the network does not have to be. Besides, Cisco NAC relies heavily on 802.1x while CyberGatekeeper relies on 802.1x and non-802.1x which makes the system compatible with old NAD and client using operating systems older than Windows NT, 2000 and XP as long as an agent can collect their status.

Now if we take a closer look at the execution, we can see that Cisco NAC enforces the network access or quarantine of non-compliant hosts while CyberGatekeeper also enforces the network access and authorize compliant hosts to be moved from outside the quarantined area. Concerning Microsoft NAP, it builds a policy enforcement client directly into the operating system. For the moment, Cisco NAC work with LAN connection only. DHCP, VPN, WLAN and IP secure (Ipsec) are planned to be available with the phase 2 which is promised to also support Switches and Access Point. Microsoft already gives a large choice of connection; VPN, Ipsec and DHCP which relies on controlling IP address allocation to host via DHCP. But at the time the solution giving the largest choice of connection is CyberGatekeeper with VPN, Ipsec, LAN and WLAN.

When we look at the operating system where the agent can be ran we can see a lot of differences between all the solutions. For the moment CTA can be run only on Windows NT, 2000 and XP service pack 1. Microsoft NAP Quarantine agent is integrated with windows XP service pack 2 and will be in the new desktop operating system released in 2007. CTA should be compatible with
Windows 2003, XP service pack 2, Linux, Solaris and Mac OS as soon as phase 2 will be released. CyberGatekeeper is still the solution offering the largest possible client operating system since the solution can use several agents for all type of clients.

As you can understand, all these solutions are still work in progress. Microsoft is still in the theory phase. The Network Admission Protection should not be released before 2007 when the new Windows Server Longhorn platform is released. Even if Cisco NAC and InfoExpress CyberGatekeeper are deployable today, they are not interoperable with all the existing network topologies. Cisco NAC can be installed today only on IOS router platforms and only with certain client operating systems as it is for InfoExpress CyberGatekeeper. The following example illustrates the problem. A company has all its clients using windows XP but only half of them using Service Pack 1 while the other half uses Service Pack 2. By implementing Cisco NAC, the solution can be applied only to half of the client and the clients with SP2 should theoretically be placed on quarantined. But a company needs those workers to work as well. Therefore as long as Cisco do not develop its solution for all type of operating system, no company networks are totally secure.

At last but not least, all the network admission solutions today are proprietary. Therefore buyers have to decide now in which direction their security should be based in the future, Cisco or Microsoft or another solution? They also should consider the cost for the future development of their network based on the chosen network admission solution. As Cisco and Microsoft are the main players in this competition, they promise not to lock in users in one or the other solution and assure to develop their solutions in order to be interoperable. The only remaining question is when it will be effective. But we can still wonder which one of the two big players Cisco and Microsoft will win this “network admission war” in the future. The answer is not clear. In one hand Cisco’s start presents a clear advantage, but in another hand Microsoft owns most of the PC operating system. Therefore Microsoft could catch up its delay faster than one could expect. One could think that Microsoft dominance on the client operating system will win this competition. But it is without thinking of the new devices that do not run Windows, such as IP phones, PDAs. So Microsoft would have to provide an agent form such devices. To try to balance the hegemony of Cisco and Microsoft, the Trusted Network Connect group, composed by Juniper networks and Foundry networks for example, work on standard specification to promote interoperability. Since Cisco and Microsoft already have proposed solutions, the standard will likely be driven by those two companies and solutions.
REFERENCES

[1] Peter J. Welcher (May 2004), *Examining 802.1x and EAP*, [WWW document],  


[20] Cisco System Inc, *Cisco Trust Agent 1.0*, [WWW document],
(accessed February 2005)


[22] Cisco System Inc, *Network Admission Control Q&A*, [WWW document],

APPENDIX 1: CTA INI FILES

ct.ini File

//communication settings: listening port number, max allowed ; sessions, session
time out value
[EAPoUDP](can be omitted, default values)
LocalPort=21862
MaxSession=8
SessionIdleTimeout=600
//user notification settings: ; notification enabled, how ; ; notification
appear, message timeout
[UserNotifies]
SysModal=0 // Prevent user to do anything else when status
message displayed if value is 1 (0/1)
EnableNotifies=1 // The user sees the status notifying
message (0/1)
MsgTimeout=300
EnableLogonNotifies=1 // The message do not appear on the logon desktop,
// it appears on the user desktop when log in. If
// value is 0, then message appear on the logon
// desktop (0/1)
LogonMsgTimeout=0
//certification filtering rules (Optional)
[ServerCertDNVerification]
TotalRules=1
Rule1=CN="CISCO1" // The server certificate have to satisfy that
rule

catalogd.ini File

[main]
EnableLog=0 // logging is disable (0/1)
LogDir="c:\Documents and Settings\All Users\Application Data\Cisco
Systems\CiscoTrustAgent\logs"
MaxFileSize=4

[loglevel] // 1=Low log, 2=medium log, 3=high
log,
// 15=everything
PADaemon=15 // high CTA service log level
NetTrans=15 // high Ntk transport specific log
level
CTAMsg=15 // high CTA posture plug-in log level
PEAP=15 // high CTA user notification module
EAPTLV=15 // high logging level for CTA PEAP module
EAPSQ=15 // high logging level for CTA TLV module
PPMgr=3 // high logging level for CTA query log
Plugin=3 // High logging level for all 3rd party plug-in
APPENDIX 2: ROUTER CONFIGURATION

NACrouter#sh run
Building configuration...

Current configuration : 2530 bytes
!
! Last configuration change at 10:25:02 eet Mon Aug 8 2005
! NVRAM config last updated at 16:02:23 eet Tue Aug 2 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname NACrouter
!
boot-start-marker
boot-end-marker
!
logging buffered 64000 debugging
enable password mikko#5
!
username administrator password 0 mikko#5
memory-size iomem 15
clock timezone eet 2
clock summer-time eet recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
!
!
ip cef
ip admission name ENTREE eapoudp
ip ips po max-events 100
aaa new-model
!
aaa authentication eou default group radius
aaa session-id common
no ftp-server write-enable
!
!
eou clientless username clientless
eou clientless password cisco123
eou allow clientless
eou timeout hold-period 60
eou timeout revalidation 600
eou logging
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.50
  encapsulation dot1Q 50 native
  ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0.51
  encapsulation dot1Q 51
  ip address 192.168.58.254 255.255.255.0
  ip access-group 101 in
  ip helper-address 192.168.1.51
  ip admission ENTREE
!
interface FastEthernet0/0.52
  encapsulation dot1Q 52
  ip address 192.168.59.254 255.255.255.0
  ip access-group 102 in
  ip helper-address 192.168.1.51
  ip admission ENTREE
!
interface Serial0/0
  no ip address
  shutdown
!
interface BRI0/0
  no ip address
  shutdown
!
interface Serial0/1
  no ip address
  shutdown
!
router eigrp 1234
  network 192.168.1.0
  network 192.168.58.0
  network 192.168.59.0
  auto-summary
!
ip classless
!
!
ip http server
ip http authentication aaa
no ip http secure-server
!
! ip radius source-interface FastEthernet0/0.50
access-list 101 permit udp any any
access-list 102 permit udp any any
!
! radius-server local
!
radius-server host 192.168.1.202 auth-port 1645 acct-port 1646
radius-server timeout 60
radius-server key sabria
radius-server vsa send authentication
! control-plane
! line con 0
    login authentication no_radius
line aux 0
line vty 0 4
    password mikko#5
! ntp server 192.168.1.202
! end
APPENDIX 3: SYSLOG MESSAGES FROM THE POSTURING PROCESS

Two different syslog are shown. One describing the Healthy posturing process and the other one for quarantine. Message beginning with eou_auth show the eou events the while message beginning with EOU-6 corresponds to the eou logging and describe the host validation step.

Healthy posture Token

Aug 8 13:29:36: %EOU-6-SESSION: IP=192.168.59.1| HOST=REMOVED|
Interface=FastEthernet0/0.52.52
Aug 8 13:29:45: eou_auth 192.168.59.1: initial state eou_initialize has enter
Aug 8 13:29:45: %EOU-6-SESSION: IP=192.168.59.1| HOST=DETECTED|
Interface=FastEthernet0/0.52
Aug 8 13:29:45: eou_auth 192.168.59.1: during state eou_initialize, got event1(eouCheckProfile)
Aug 8 13:29:45: %EOU-6-CTA: IP=192.168.59.1| CiscoTrustAgent=DETECTED
ACSACL#-IP=healthy-40a00ae9
Aug 8 13:29:47: %EOU-6-POSTURE: IP=192.168.59.1| HOST=AUTHORIZED|
Interface=FastEthernet0/0.52
Aug 8 13:29:47: %EOU-6-AUTHTYPE: IP=192.168.59.1| AuthType=EAP
.Aug 8 08:42:00.365: eou-ev:Starting Revalidate timer 500(192.168.59.1)
.Aug 8 08:42:00.669: EAPoUDP (rx) Flags:128 Ver=1 opcode=4 Len=0
MsgId=1883609088 Assoc ID=2566467561
.Aug 8 08:42:00.669: eou_auth 192.168.59.1: during state eou_authenticated, got event 7(eouResultAck)
.Aug 8 08:42:00.669: eou-ev:Starting Status Query timer 150(192.168.59.1)

Quarantine posture Token

(956098085:956098086)
*Aug 10 06:06:30.683: EAPoUDP (rx) Flags:128 Ver=1 opcode=3 Len=47
MsgId=956098086 Assoc ID=928736612
*Aug 10 06:06:30.683: Dumping TLV contents
*Aug 10 06:06:30.683: TLV M:1 R:0 Type=EAP Payload Length=43
*Aug 10 06:06:30.683: EAP code: 0x2  id: 0x41 length: 0x002B type: 0x19
06D03940:          0241002B 19010703 010020FB      .A.+...... {
06D03950: A010EC23 7FF9A2F7 942C717D 1E50B543   .l#.y"w,.g),P5C
06D03960: DCBCB2D9 42DD3AA7 FAACEF29 6C59B7    \<2YB":"z,oLY7
*Aug 10 06:06:30.687: eou_auth 192.168.59.1: during state eou_client, got event 14(eouEapResponse)
*Aug 10 06:06:30.687: eou-ev:Starting AAA timer 60(192.168.59.1)
*Aug 10 06:06:30.779: %EOU-6-POLICY: IP=192.168.59.1| TOKEN=Quarantine
*Aug 10 06:06:30.787: %EOU-6-POLICY: IP=192.168.59.1| ACLNAME=#ACSACL#-IP-quarantine-42e87875
*Aug 10 06:06:30.787: %EOU-6-POLICY: IP=192.168.59.1| ACLNAME=#ACSACL#-IP-quarantine-42e87875
*Aug 10 06:06:30.787: eou-packets:192.168.59.1: Received MPPE_RECV_KEY (32)
84C4DB70: 0BFCFE BD9C5B79 35277A9C 5FE5C255   \.|~...{y'z_eBU
84C4DB80: DE10C1EC 6BD8488A B35D1474 400D2EFD  ^.AlkXH.3}.t0.
84C4DB90: 4E     N
*Aug 10 06:06:30.787: eou-packets:192.168.59.1: ACL Name=#ACSACL#-IP-quarantine-42e87875
*Aug 10 06:06:30.787: %EOU-6-POLICY: IP=192.168.59.1| ACLNAME=#ACSACL#-IP-quarantine-42e87875
*Aug 10 06:06:30.787: %EOU-6-POSTURE: IP=192.168.59.1| HOST=AUTHORIZED
*Aug 10 06:06:30.787: Interface=FastEthernet0/0.52
*Aug 10 06:06:30.787: eou-ev:Starting Revalidate timer 3(192.168.59.1)
*Aug 10 06:06:30.787: EAPoUDP (tx) Flags:0 Ver=1 opcode=4 Len=8 MsgId=956098087
Assoc ID=2745972794
*Aug 10 06:06:30.791: Dumping TLV contents
*Aug 10 06:06:30.791: TLV M:1 R:0 Type=EAP Payload Length=4
*Aug 10 06:06:30.791: %EOU-6-AUTHTYPE: IP=192.168.59.1| AuthType=EAP
*Aug 10 06:06:31.259: EAPoUDP (rx) Flags:128 Ver=1 opcode=4 Len=0
MsgId=956098087 Assoc ID=928736612
*Aug 10 06:06:31.259: eou_auth 192.168.59.1: during state eou_authenticated, got event 7(eouResultAck)
*Aug 10 06:06:31.263: eou-ev:Starting Status Query timer 300(192.168.59.1)
APPENDIX 4: AUTHENTICATION CAPTURE PACKETS

Communication between the Client and the ACS server
### Communication between the ACS server and the DNS server

<table>
<thead>
<tr>
<th>Packet Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>38 9.66316 192.168.1.202 192.168.1.11 TCP 1926 &gt; 1674 [SYN, ACK] seq=0 ack=1 win=7520 Len=0 M=1450</td>
<td>Communication between the ACS server and the DNS server</td>
</tr>
<tr>
<td>39 9.66435 192.168.1.202 192.168.1.11 TCP 1926 &gt; 1674 [SYN, ACK] seq=0 ack=1 win=7520 Len=0 M=1450</td>
<td></td>
</tr>
<tr>
<td>40 9.66439 192.168.1.202 192.168.1.11 TCP 1926 &gt; 1674 [ACK] seq=1 Ack=1 win=7520 Len=0</td>
<td></td>
</tr>
<tr>
<td>41 9.66510 192.168.1.202 192.168.1.11 ICMP Echo Reply: ID=124060000001226234</td>
<td></td>
</tr>
<tr>
<td>42 9.66970 192.168.1.202 192.168.1.11 ICMP Echo Request: ID=124060000001226234 Max-Mss=1460</td>
<td></td>
</tr>
</tbody>
</table>

### Communication between the AAA client (Router) and the ACS server

<table>
<thead>
<tr>
<th>Packet Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>342 78.398801 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td>Communication between the AAA client (Router) and the ACS server</td>
</tr>
<tr>
<td>343 78.398802 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>344 78.398803 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>345 79.777476 192.168.1.11 192.168.1.202 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>346 79.790093 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>347 79.790098 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>348 80.081347 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>349 80.081348 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>350 80.225776 192.168.1.11 192.168.1.202 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>351 80.225777 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>352 80.253347 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>353 80.253348 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>354 80.260165 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>355 80.260166 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>356 80.392075 192.168.1.11 192.168.1.202 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>357 80.400723 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>358 80.400724 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>359 80.400725 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>360 81.890555 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>361 81.890556 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>362 81.890557 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>363 81.890558 192.168.1.202 192.168.1.11 RADIUS Access-Challenge [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>364 82.892910 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>365 82.892911 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
<tr>
<td>366 82.892912 192.168.1.202 192.168.1.11 RADIUS Access-Request [125, 1679]</td>
<td></td>
</tr>
</tbody>
</table>

---

Sabria Bouguetaia  
Degree Project  
E3161D  
June 2006