Global Information Assurance Certification Paper

Case Study in Implementing AAA Servers Using TACACS+

Steve Ingram

December 1, 2003

Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b

Option #2 – Case Study

Introduction

This case study covers the decision-making processes used to implement an Authentication, Authorization and Accounting (AAA) solution in an enterprise environment. The final AAA solution was to deploy Cisco Secure ACS 3.1 using Terminal Access Controller Access Control System Plus protocol (TACACS+). The business rationale to implement AAA started as a mitigation activity recommended in an internal security risk assessment. My responsibilities ranged from team member on the risk assessment team, member of the solution development team, team lead for the proof of concept testing team and to provide engineering support for implementation.

This paper will cover the steps taken before implementing the AAA server solution using TACACS+ into the networked environment. First I will describe AAA and TACACS+ to provide an understanding of how they work together. Secondly, I will describe the network prior to implementation and its vulnerabilities. After laying this foundation, I will describe the process used and alternatives considered to come to the conclusion that implementing AAA using TACACS+ would be the best security solution for the client's networking security needs. This will lead to the process of actually configuring and testing the AAA/TACACS+ product as well as the implementation/integration process.

AAA Server and TACACS+ Background

Authentication, Authorization and Accounting (AAA) Server

Prior to explaining the problem-solving process leading to the decision to use AAA and implement it, I think it is necessary to explain what AAA is to provide a basic understanding and foundation for this paper.

AAA stands for Authentication, Authorization and Accounting, which are three ways to control and monitor access to a network device. The following are generic definitions for the AAA components as derived from a variety of sources: (Cisco System Inc., Cisco AAA Case Study Overview, "AAA Technology Summary"; Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Server, "Overview of Cisco Secure ACS" and Steel-Belted Radius/Enterprise Edition).

- Authentication occurs when a user is identified before accessing a network device.

- Authorization is the process of granting or denying a user access to a network device. Authorization can include level of access configured for the user.

- The Accounting portion of the AAA security system is the logging of actions when a user accesses a network device.

To understand how AAA works, the relationship between the AAA client and server needs explanation. The explanation is derived from information gathered from the source referenced at the end of this paragraph. The AAA client is software that runs on a network device, such as a Cisco router. When a user attempts to connect to the router, the function of the client software is to pass authentication, authorization and accounting duties to the AAA server in order to complete the connection. It begins when the client sends the user's authentication request to the server using either the TACACS+ or the RADIUS protocols. The server can verify the username and password and then notifies the client when the authentication attempt has succeeded or failed. If the authentication is successful, the user is granted access to the network device. The server will provide authorization information to the client allowing the user to perform tasks based upon the assigned privilege level. At this point, the client communicates accounting information to the server so the user's actions can be clearly tracked. The AAA server provides a centralized location to configure and control these three important security functions described in the paragraph. (Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Server, "Overview of Cisco Secure ACS").

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a Cisco proprietary protocol used to deliver AAA security services. It is actually what separates AAA into the Authentication, Authorization and Accounting security functions. This feature of TACACS+ is the backbone behind the entire AAA server solution. Another important feature that is relevant to this case study is that TACACS+ will support 16 different privilege levels, which is used to limit a user's access to a network device. There are other features available when using TACACS+, however, the two mentioned is worth noting for this case study. Other useful TACACS+ features are listed in the "TACACS+ Overview" section of the "Cisco AAA Case Study Overview." (Cisco Systems, Inc., Cisco AAA Case Study Overview, "TACACS+ Overview" and Internet Next Generation, "TACACS+").

Network Description Prior to Implementation

Network Description

The network that is being described for the purpose of this paper is an IP routed wide area network (WAN) that provides enterprise routing services to users. This network includes 100 plus router nodes distributed throughout the country. The routing nodes consist of four different network component configurations, which are listed below:

1. Multiple NET PX-3 Card Router Based. A PX-3 is a router on a circuit card that is installed on a Bandwidth Manager node (a layer two transport device).

It is co-developed by Cisco (the IOS) and N.E.T (the hardware). See Figure A.

2. Dual Cisco 7500 Series Router Based. See Figure B.
3. Dual Cisco 2621 Router Based. See Figure C.
4. Single Cisco 2621 or 1720 Router Based. See Figure D.

The configuration diagrams are included below to provide a description of the entire network.

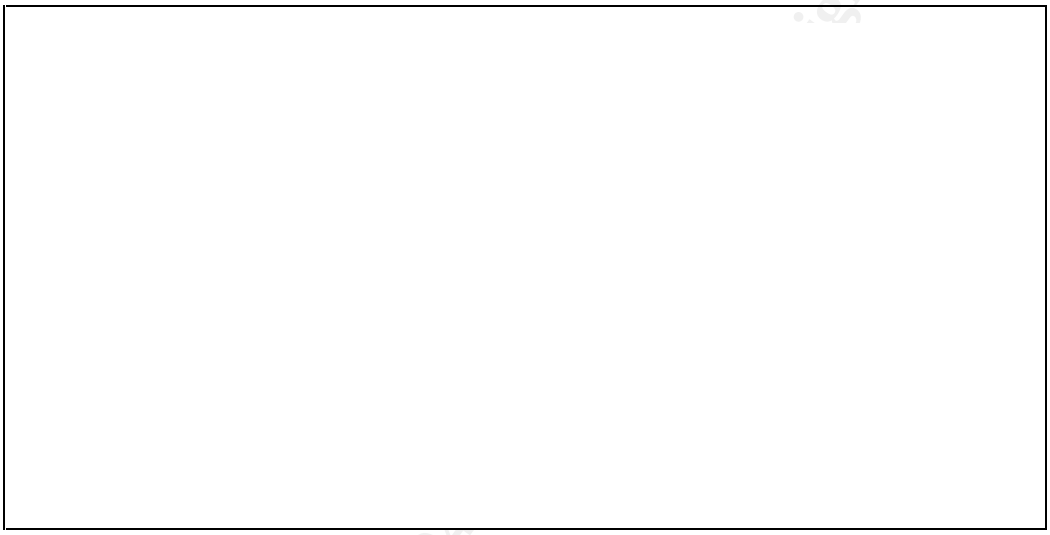

Figure A. Multiple NET PX-3 Card Router Based

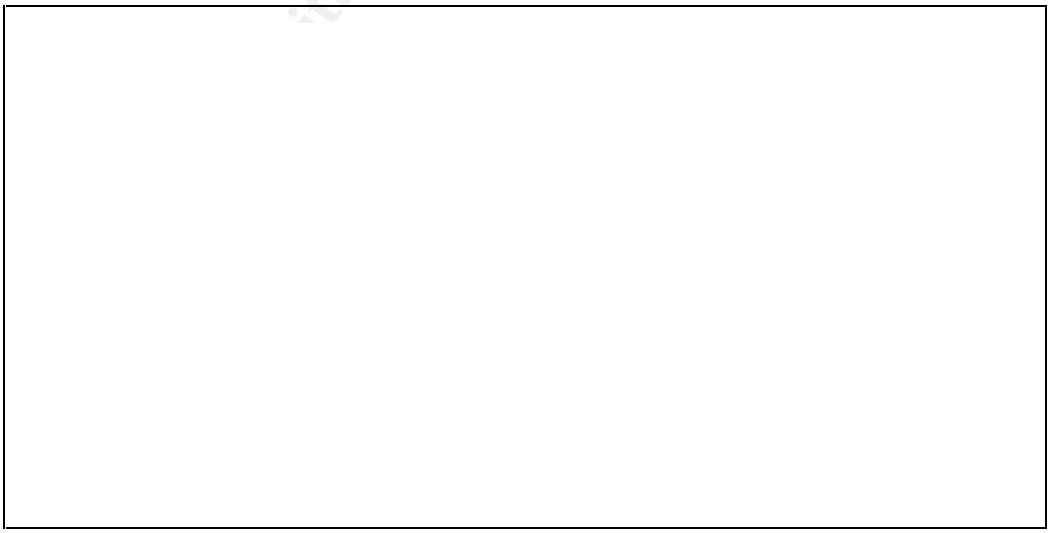

Figure B. Dual Cisco 7500 Series Router Based

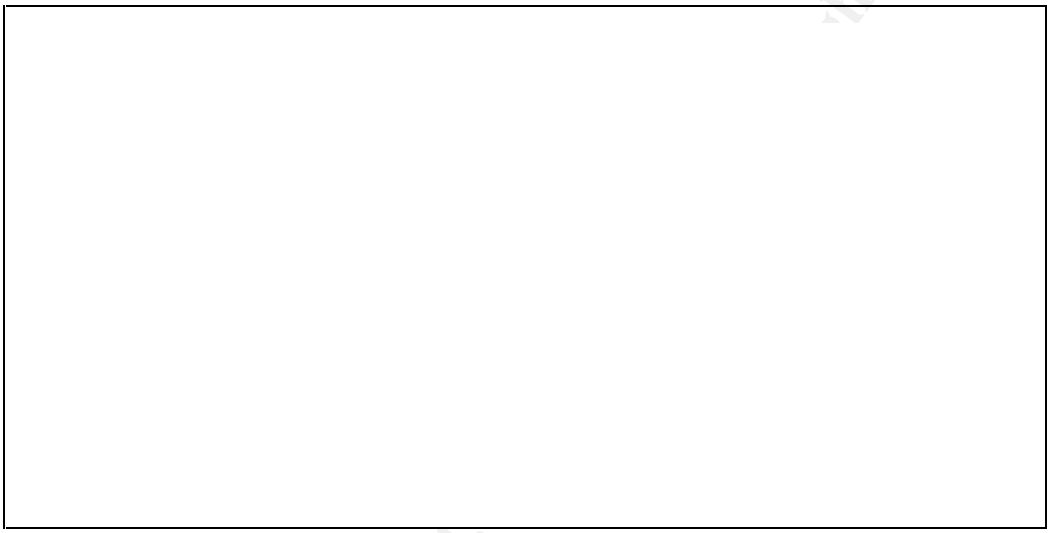

Figure C. Dual Cisco 2621 Router Based

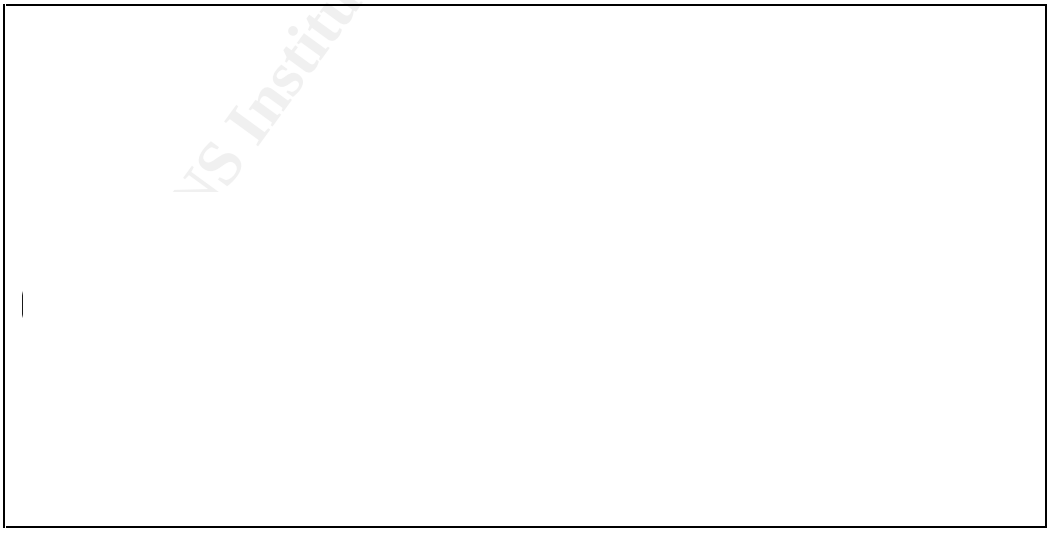

Figure D. Single Cisco 2621 or 1720 Router Based

Technicians at two Network Operations Centers (NOCs) located on the east and west coasts and second level support at a third facility had virtual terminal (vty) interface access to the router nodes to allow remote maintenance capabilities.

This method of performing remote maintenance had some weaknesses, as follows.

- They were unable to enforce password policies. Each router had its own user Identification (ID) and password controls.
- Failure to perform system audits would result in the inability to monitor security activities related to system users and maintenance activities.
- The lack of authorization controls placed on users would result in unnecessary access to the system. As a result, the system was vulnerable to abuse that could have degraded system performance and caused system failure.

The network itself did not change during the course of the project; only how remote maintenance was handled.

Decision Making Process and Testing

Risk Analysis

The whole decision-making process that lead to the conclusion that AAA servers using TACACS+ was the best security solution began when a risk assessment was done on the previously described IP router network.

Before completing the actual risk assessment analysis, samplings of sites were visited across the country. A visual inspection of the physical and network component's security was performed. Interviews with system subject experts were conducted using questionnaires to facilitate discussion about the security state of the IP router network.

The purpose of the risk assessment was to identify system vulnerabilities, threats and existing countermeasures by measuring the adverse impact to the information Confidentiality (C), Integrity (I) and Availability (A). Confidentiality is the expectation that data crossing the network will remain private. Integrity is the expectation that the data will be the same at the beginning as at the end. Availability is the expectation that the data will remain accessible to the end user. CIA definitions were derived from one source. (Stoneburner, Goguen and Feringa, p. 22)

In this risk assessment, vulnerabilities and threats were described in terms of vulnerability-threat pairs. The Likelihood (L) of a threat impacting the IP network was measured in qualitative terms of high, medium or low. Quantitative values were assigned to the qualitative terms (high=3, medium=2, low=1). The severity

of impact to the network was measured in terms of adverse impacts to information CIA, which were also assigned impact values of high (3), medium (2), and low (1). Risk ratings (R) were calculated as follows: R=L(C+I+A).

Based on the data gathered during the visual inspections and the interviews, the vulnerability-threat pair analysis described above was completed. The results gave an indication of the vulnerability findings and recommendations were made that provided solutions to correct them. These recommendations were meant to address the implementation of proposed security controls, procedures, and safeguards to reduce system vulnerabilities. The recommendations identified in this particular risk assessment report provided the foundation for developing the Risk Mitigation Plan. All of this will be discussed further in the following paragraphs.

Vulnerabilities are weaknesses that can be exploited to cause harm to a system or network (Stoneburner, Goguen and Feringa, p. E-2). Threats can be defined as an event that can cause harm to a system by exploiting a particular vulnerability (Stoneburner, Goguen and Feringa, p. E-2). In this case, after visiting sites, looking at all the data gathered and completing the analysis, four particular vulnerability (v)- threat (t) pairs stood out (there were more, but these are specific pairs related to this case study).

The first pair was System Access Control (v) – Intrusion or Unauthorized Access to System Resources (t). This included the following specific vulnerabilities:

- Minimal password makeup rules currently levied on the system
- No password aging rules currently levied by the system
- No password reuse rules currently levied by the system
- User ID and passwords are the same for all users.

The second pair was Session Control (v) - Intrusion or Unauthorized Access to System Resources (t). The specific vulnerability was though the router would automatically disconnect after three failed login attempts, the connection could be reestablished immediately.

The third pair was System Auditing (v) - Intrusion or Unauthorized Access to System Resources (t). The specific vulnerability was that the Syslog logged configuration changes and failed and successful logins, but no username is recorded when an individual logs into a router node.

Recommendations

At this point, recommendations were made to eliminate or reduce the risk of the vulnerabilities. The recommendations related to this case study were as follows:

- Implement an Authentication Authorization and Accounting (AAA) server to provide a central point of remote router access control that enforces password policies for:
    - Length
    - Character Makeup
    - Lifetime
    - Reuse
- Implement AAA server to provide logging for router nodes should include:
    - All Logon and Logoff Events (success or failure)
    - Account Management Events (success or failure)
    - Object Access (success only)
    - Security Policy Changes (success or failure)
    - Privilege Change Event (success or failure)
    - Restart, Shutdown and System (success or failure)

Other considerations

Another twist was added to the decision-making process. It was decided that the regular NOC users would need access to the router nodes and PX-3 routing cards to perform basic troubleshooting tasks. The NOC users needed to access the router to do the following:

- Run shutdown/no shutdown command
- Run debug commands
- View router configurations

The goal was to limit the regular NOC users to those three tasks and a few other non-intrusive commands on the router nodes. The solution would have to limit them to that level of granularity.

It didn't take long to come to the conclusion that a AAA server solution using TACACS+ could possibly allow the company to reduce the risk associated with the current management configuration. This conclusion was reached because:

- The AAA server allows the necessary control over the password makeup
- The Accounting portion of AAA handles the necessary logging
- TACACS+ provides password encryption
- AAA allows certain access restrictions to be enforced so regular NOC users could access routers without causing more security issues.

Alternatives

These recommendations did not come without considering alternatives. First of all, the hardware was researched. A Compaq ProLiant DL360 server and a Dell PowerEdge 2600 were considered. The Compaq was decided against due to the

fact that Dell is the vendor that is most widely used within the company and the Compaq was slightly more expensive.

The second decision to be made was which AAA software to use. The choices were Cisco ACS 3.1 and Steel-Belted Radius, which is a RADIUS/AAA Server. The decision to use Cisco ACS 3.1 was made when the protocols were considered, as discussed in the following paragraphs.

The third consideration was the protocol that was going to be used to deliver the AAA services. The choices were TACACS+ and RADIUS. The differences are listed below in Table A (Cisco Systems, Inc., Cisco AAA Case Study Overview, "Comparison of TACACS+ and RADIUS") and are discussed further in the following paragraphs:

Table A. TACACS+/Radius Comparison

TACACS+	RADIUS
Uses Transmission Control Protocol (TCP)	Uses User Datagram Protocol (UDP)
Encrypts the entire body of the packet; more secure	Encrypts only the password in the access-request packet; less secure
Uses the full AAA architecture	Combines Authentication and Authorization together
Cisco Proprietary	Industry Standard
Offers multi-protocol support	Does not support many protocols
RADIUS does not allow users to control which router commands can be executed	TACACS+ allows control of router commands on a per-user and per-group basis

(Cisco Systems, Inc., "Comparison of TACACS+ and RADIUS, Cisco AAA Case Study Overview)

TACACS+ uses TCP, which is a connection-oriented protocol and RADIUS uses UDP, which is connection-less and provides best effort delivery. Since RADIUS uses UDP, other variables need to be programmed, such as, retransmit attempts. This is not required with TCP. (Cisco Systems, Inc., Cisco AAA Case Study Overview, "Comparison of TACACS+ and RADIUS").

Some encryption is provided by both protocols; however, RADIUS just encrypts the password in the access-request packet, leaving the rest of the packet vulnerable if intercepted. TACACS+ encrypts the entire packet except for the header. However, this header only indicates whether the packet is encrypted or not. Keep in mind that this encryption only occurs between the AAA client and the AAA server. Prior to that, precautions need to be take to protect the password because it is transmitted in the clear. (Cisco Systems, Inc., Cisco AAA Case Study Overview, "Comparison of TACACS+ and RADIUS").

Another important difference is that TACACS+ uses the full AAA architecture and it allows the Authentication, Authorization and Accounting functions to be performed independently of each other. This was important for this company because this functionality allowed the granularity necessary to configure authorization on the Cisco router nodes down to the command level. This satisfied the need to limit the NOC users to certain commands. RADIUS combines Authentication and Authorization together, which does not allow the ability to limit the NOC user access down to the command level. (Cisco Systems, Inc., Cisco AAA Case Study Overview, "Comparison of TACACS+ and RADIUS").

After weighing these alternatives, it was recommended that Cisco ACS using TACACS+ and running on a Dell server should be implemented to provide the desired security that included the granular control required, accounting, connection-based transmissions and full data encryption.

Costs

Now that a probable solution was found, it was necessary to estimate the cost of this project to make sure it was financially feasible. The costs of four server units and the Cisco Secure ACS 3.1 software were considered. The four servers were for the test lab, the two NOCs and the second level support facility that was responsible for configuring and implementing this security solution. The cost data was gathered from www.dell.com and www.cdw.com. Fortunately, the total cost of the project was well within budget constraints for the company so we were allowed to proceed with the initial testing phase.

Initial Testing

Now that the analysis was completed and alternatives and costs were considered, it was time to test this solution to see if it actually provided the necessary security. A test bed with a minimal amount of equipment was created using a Dell server running Windows 2000 and a Cisco 2621 router running 12.1(18) IOS. The Cisco ACS 3.1 software was loaded onto the Dell Server. At this point, the IP addresses were configured on the server and the router and connectivity was verified using the ping command. A password was then configured on the router so it could be accessed in case the server did not function properly. This is an important step because if the server goes down or the configuration is incorrect, the AAA feature could lock an individual out of the Cisco router. When this was completed the server and the router were ready to be configured to use the AAA and TACACS+ functionality.

ACS Server Configuration

The ACS software was easy to load and provided a user-friendly Graphical User Interface (GUI) interface to make configuring the server an easy process. After

the ACS software was loaded, an icon appeared on the desktop. The GUI interface can be accessed when clicking on the icon. To properly test the AAA functionality, it was decided to create two user groups; a group for administrators and a group for regular users. The administrators would have full access to the routers while the regular user group would have the same limited access that was planned for the NOC users in the company. Tables B-K list the configurations entered on the server to test the AAA concept. These tables (B-K) were created to package the configuration and function explanations that came from Cisco Systems, Inc. (Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software). The configurations are included in the case study to give an individual the basis to configure the AAA server and to show how the server was configured to help eliminate risks identified in the risk assessment.

Table B. Administrative Group Configurations

Administrative Group Configuration		
Item	**Configuration**	**Function**
Max Sessions	5	Maximum number of simultaneous connections for the group
Sessions available to users of this group	5	Maximum number of simultaneous connections available for each user in the group
Enable Options	• Highlight "Max Privilege for any AAA client" • Select 15	Assigns maximum privilege levels for the user
Password Aging Rules	• Check "Apply age-by-date" rules box • Active period was configured to be 75 days, Warning period is 14 days and Grace period is 1 day	Configures AAA to warn a user about password expiration after 75 days. The warning period is 14 days and the grace period is 1 day. This allows a total of 90 days.
Apply Password Change Rule	This should be checked	Prompts the user to change their password after the first login
TACACS+ Settings	• Check "Shell (exec)" • Check "Privilege level" and type 15 in the box	Users assigned to this group will have the highest privilege level and will defer to the

Administrative Group Configuration		
Item	**Configuration**	**Function**
Shell Command Authorization Set	• Highlight "Assign a Shell Command Authorization Set for any network devices" • Choose "Router Admin"	command authorization settings created in the Router Admin group.

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table C. Regular User Group Configurations

Regular User Group Configuration		
Item	**Configuration**	**Function**
Max Sessions	3	Maximum number of simultaneous connections for the group
Sessions available to users of this group	3	Maximum number of simultaneous connections available for each user in the group
Enable Options	• Highlight "Max Privilege for any AAA Client" • Type 15 in the box	Assigns maximum privilege level for user.
Password Aging Rules	• Check "Apply age-by-date" rules box • Active period was configured to be 75 days, Warning period is 14 days and Grace period is 1 day.	Configures AAA to warn a user about password expiration after 75 days. The warning period is 14 days and the grace period is 1 day. This allows 90 total days.
Apply Password Change Rule	This should be checked	Prompts the user to change their password after the first login
TACACS+ Settings	• Check "Shell (exec)" • Check "Privilege level" and type 15 in the box	Users assigned to this group will have the highest privilege level and will defer to the command authorization settings created in the Users group.
Shell Command Authorization Set	• Highlight "Assign a Shell Command Authorization Set for any network devices" • Choose "Users"	

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers

and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table D. Administrator User Configurations

Administrator User Configuration		
Item	**Configuration**	**Function**
Supplementary User Information	Type a Real Name for the user and a user description	A name will appear in the logs which will allow them to be held accountable for any configurations changes.
User Setup	Select "Cisco Secure Database" and choose a password	Configures a password for the Administrative User.
Group to which the user is assigned	Select "Administrative Group"	Assigns the user to a particular group.
Max Sessions	Highlight "Use Group Setting"	Defers to the Maximum Sessions setting for the group the user is assigned to.
Account Disable	• Check "Failed attempts exceed:" • Type 3 in the box	The user's account will be disabled after 3 failed login attempts and can only be restored by the administrator.
TACACS+ Enable Control	Highlight "Use Group Setting"	Defers to the TACACS+ Enable Control setting for the group the user is assigned to.
TACACS+ Enable Password	Highlight "Use Cisco Secure PAP" password	Choose this to use the password configured in the password authentication section.

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table E. Regular User Configurations

Regular User Configuration		
Item	**Configuration**	**Function**
Supplementary User Information	Type a Real Name for the user and a user description	A name will appear in logs which will allow them to be held accountable for any configurations changes.
User Setup	Select "Cisco Secure Database" and choose a password	Configures a password for the Regular User.

Regular User Configuration		
Item	**Configuration**	**Function**
Group to which the user is assigned	Select "Regular User Group"	Assigns the user to a particular group.
Max Sessions	Highlight "Use Group Setting"	Defers to the Maximum Sessions setting for the group the user is assigned to.
Account Disable	• Check "Failed attempts exceed:" • Type 3 in the box	The user's account will be disabled after 3 failed login attempts.
TACACS+ Enable Control	Highlight "Use Group Setting"	Defers to the TACACS+ Enable Control setting for the group the user is assigned to.
TACACS+ Enable Password	Highlight "Use Cisco Secure PAP" password	Choose this to use the password configured in the password authentication section.

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table F. Shared Profile Components

Shared Profile Components Configuration		
Item	**Configuration**	**Function**
Create a Profile called "Router Admin" (As referred to in the "Shell Command Authorization Set" in the Administrative Group Configuration)	• Name: Router Admin • Description: Command Set for Administrative Group • Next to "Unmatched Commands:," highlight "Permit" No other configurations should be made	This would give users assigned to the Administrative Group authorization to run any command on the router nodes.
Create a Profile called "Users" (As referred to in the "Shell Command Authorization Set" in the Regular User Group Configuration)	• Name: Users • Description: Regular Users • Next to "Unmatched Commands:," highlight "deny" • Leave "Permit Unmatched Args" unchecked	This configuration will limit the regular NOC users to only the necessary commands they need to perform their job duties. Since "Permit Unmatched Args" remained unchecked, the NOC users will not be authorized to run any

Shared Profile Components Configuration		
Item	**Configuration**	**Function**
	• In the box to the left, type: - clear - configure - exit - interface - no - show - shutdown - write - debug • In the box to the right, type - permit memory - permit network - deny erase	other commands.

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table G. Network Configuration

Network Configuration		
Item	**Configuration**	**Function**
Create a Network Device Group called “Group A” and assign AAA clients to it	• In the box, IP addresses of network devices that will be assigned to the group. • Type a secret key • Choose the group • Next to “Authenticate Using Select” select “TACACS+ (Cisco IOS)” • Check “Single Connect TACACS+ AAA Client (Record stop in accounting on failure)”	The configurations (e.g. secret key) will be applied to all network devices included in the IP address box. This will allow the administrator to make one configuration change for all the nodes (e.g. Authentication method and secret key).

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table H. System Configuration

System Configuration		
Item	**Configuration**	**Function**
Service Control:	Service Log File	Controls the parameters

System Configuration		
Item	**Configuration**	**Function**
Service Log File Configuration	Configuration - • Under “Level of Detail” highlight “Full” • Under “Generate New File” highlight “Every day” • “Manage Directory” should remain unchecked	for the Service Log File configuration.
Logging:	Log Target: Choose to log - • CSV Failed Attempts • CSV Passed Authentications • CSV TACACS+ Accounting • CSV TACACS+ Administration Enable Logging – • Check the appropriate log report • Under “Generate New File” highlight “Every Day” Select Columns to Log – • Everything to be logged should be in “Logged Attributes” column Directory – • Select the directory, “C: (or other drive used)\Program Files\Cisco Secure ACS v3.1\Logs\ TACACS+ Administration” • “Manage Directory” remains unchecked	This is where logging is configured. CSV log files can be imported into many spreadsheet applications.
Date Format Control	Under “Date Format	Formats date

System Configuration		
Item	**Configuration**	**Function**
	Selection" highlight "Use Month/Day/Year Format"	
Local Password Management	Under "Password Validation Options" set the following: • Password length should be between 8 and 32 characters • Check "Password may not contain usernames • Check "Password is different from the previous value • Check "Password must be alphanumeric • Under "Remote Change Password," check "Upon remote user password change immediately propagate the change to selected replication partners • Under Password Change Log File Management, Generate a New File Every day	Sets password rules, allows the primary server to replicate password changes to the backup servers and configures logging of password changes.
Database Replication Setup	ON THE PRIMARY SERVER: • Highlight "Send" for all Replication components • Under "Outbound Replication," set schedule for replication (e.g. 15 minutes) • Choose the servers the primary is replicating to • Under "Inbound	Sets up replication. Any user configuration changes made on the primary AAA server will be replicated to any backup servers configured.

System Configuration		
Item	**Configuration**	**Function**
	Replication," choose "Any Known Cisco Secure ACS Server" ON THE BACKUP SERVERS: • Highlight "Receive" for all Replication components • Under "Inbound Replication," choose "Any Known Cisco Secure ACS Server"	
ACS Backup	• Under "ACS Backup Scheduling," highlight "Manual" • Under "Backup Location," the directory should be C: (or drive used)\Program Files\Cisco Secure ACS v3.1\CSAuth\ System Backups • "Manage Directory" should be select and highlight "Keep only last 7 files"	The ACS can only be backed up manually to the directory and keeps only the last 7 files. This can be configured to back up automatically as well.
ACS Service Management	ACS Active Service Management Setup – • Under "System Monitoring," "Test login process every 1 minute if no successful authentications are recorded choose "Restart All" • "Generate event when an attempt is made to log in to a disabled account" should be	Enables monitoring of all Cisco Secure ACS services.

System Configuration		
Item	**Configuration**	**Function**
	checked. Event Logging – "Log all events to the NT event log" should be checked.	

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table I. Interface Configuration

Interface Configuration		
Item	**Configuration**	**Function**
Interface Configuration	Configure as necessary based on ACS configuration needs.	Used to configure the ACS gui interface.

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table J. Administration Control Configuration

Administration Control Configuration		
Item	**Configuration**	**Function**
Administration Control	• Add an Administrator for the ACS • Type in a password under "Administrator Details" Administrator Privileges – • Under "User & Group Setup…," check "Add/Edit users in these groups" and "Setup of these groups." • Put all groups in the "Editable groups" list • Check everything else	Configures an Administrator for the AAA server.

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

Table K. Reports and Activity Section

Reports and Activity		
Item	**Configuration**	**Function**

Reports and Activity		
Item	**Configuration**	**Function**
Reports and Activity	No configuration necessary	This is where the logging files can be viewed.

(Cisco Systems, Inc., User Guide for Cisco Secure ACS 3.1 for Windows Servers and On-line documentation provided with the Cisco Secure ACS 3.1 software)

These are configurations specific to this company's needs. Additional configurations are possible for different scenarios and more information is in the Cisco Secure ACS 3.1 for Windows 2000/NT Servers User Guide available on the Cisco website.

Cisco Router Configuration

For the initial testing, a Cisco 2621 router was used. Accessing the router through the console port, the following commands were configured to enable the AAA and TACACS+ functionality. These commands were researched in the Cisco Systems, Inc. website and the table was created to summarize the commands used. (Cisco Systems, Inc., "Cisco IOS Software Release 12.1, Commands Summaries, CS1: Part 6: Security" and Cisco Systems, Inc., "Configuring Basic AAA on an Access Server"). To access "Configuring Basic AAA on an Access Server," requires a Cisco, Inc. CCO account. Since it requires a user ID and password, I did not include it in the reference section of this paper because Administrivia rules on the GIAC website state not to include references requiring passwords.

Table L. Router Configurations

Router Commands
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
tacacs-server host <*IP address*>
tacacs-server key <*secret key #*>

(Cisco Systems, Inc., "Cisco IOS Software Release 12.1, Commands

Summaries, CS1: Part 6: Security" and Cisco Systems, Inc., "Configuring Basic AAA on an Access Server")

Notice that a secret key is configured on a router. A corresponding secret key was also configured on the ACS server (See Table G, Network Configuration). In regards to the configuration, it is worth pointing out that the commands "aaa authorization config-commands" and "aaa authorization commands 15 default group tacacs+ none" are necessary to allow control over the user's authorization level.

Also, a list of basic test requirements was developed to be used during initial testing as follows:

- AAA shall be used to authenticate all access to routing nodes using unique usernames and passwords
- AAA services shall require passwords to have a minimum length of 8 characters
- AAA service shall require that new passwords use alphanumeric characters
- AAA services shall allow the ability to lock a user account after three failed login attempts, requiring administrator intervention to reset the account
- AAA services shall provide authorization for user access to routing nodes at the router command level
- AAA services shall provide for logging of routing node logon events (success or failure)

The purpose of the initial testing was to work out any problems prior to performing more extensive testing at the second level support facility. These requirements just covered the basics to prove that the AAA features were working properly. Fortunately, we were able to meet all of the requirements for testing. The configuration used was successful, but there may be other ways of configuring the server to get the same results. When this was completed, more testing at the second level support facility was scheduled.

Final Testing

For the final testing, test procedures were written, which included additional requirements and success criteria for the test. The entire list of requirements was written with the input of the second level support group since they were going to support the AAA servers and the network devices. The final test procedures are listed in Table N (created by me) and are included to show the steps that were taken to ensure that the solution would satisfy our security needs. The testing took place at the second level support facility and was witnessed by members of the support group. The test bed was set up to replicate the Network Management System (NMS) connectivity to the routing nodes and was used to verify the access controls provided by AAA services supported by the Cisco ACS software running on a Windows 2000 server. There were other recommendations being tested at the same time, but this will focus on

AAA and TACACS+ only. The test bed consisted of the AAA server, which was a Dell PowerEdge Server running Windows 2000, a Cisco 7206 router, a Cisco 2621 router, a Cisco 7513 router, a NET PX3 IP routing card, a Cisco Catalyst 2950 Ethernet switch and a Netgear Hub. Figure E shows the test bed configuration for this test. The IP addresses are not sanitized because it was an isolated test bed and the addresses were made up for this purpose only.

Prior to the testing, the routers and PX3 card had to be configured for AAA services using TACACS+. The router configurations were all the same (See Table L), however, the PX3 card's configuration was slightly different than the other routing nodes because the IOS on the PX3 was version 11.2. Both configurations provided the same results. No research was done to configure the PX3 card. The help feature was used to complete the configuration. Table M shows the PX3 card configuration and was created to summarize the PX3 card configurations.

Table M. PX3 Commands

PX3 Commands
aaa new-model
aaa authentication login default tacacs+ local
aaa authentication enable default tacacs+ enable
aaa authorization exec tacacs+ local none
aaa authorization commands 15 tacacs+ local none
aaa authorization config-commands
aaa accounting exec start
aaa accounting commands 15 start
tacacs-server host <*IP address*>
tacacs-server key <*secret key #*>

Once the PX3 card was configured, the test procedures listed below were followed on each routing node to prove that the AAA server using TACACS+ was able to satisfy the security needs of the company.

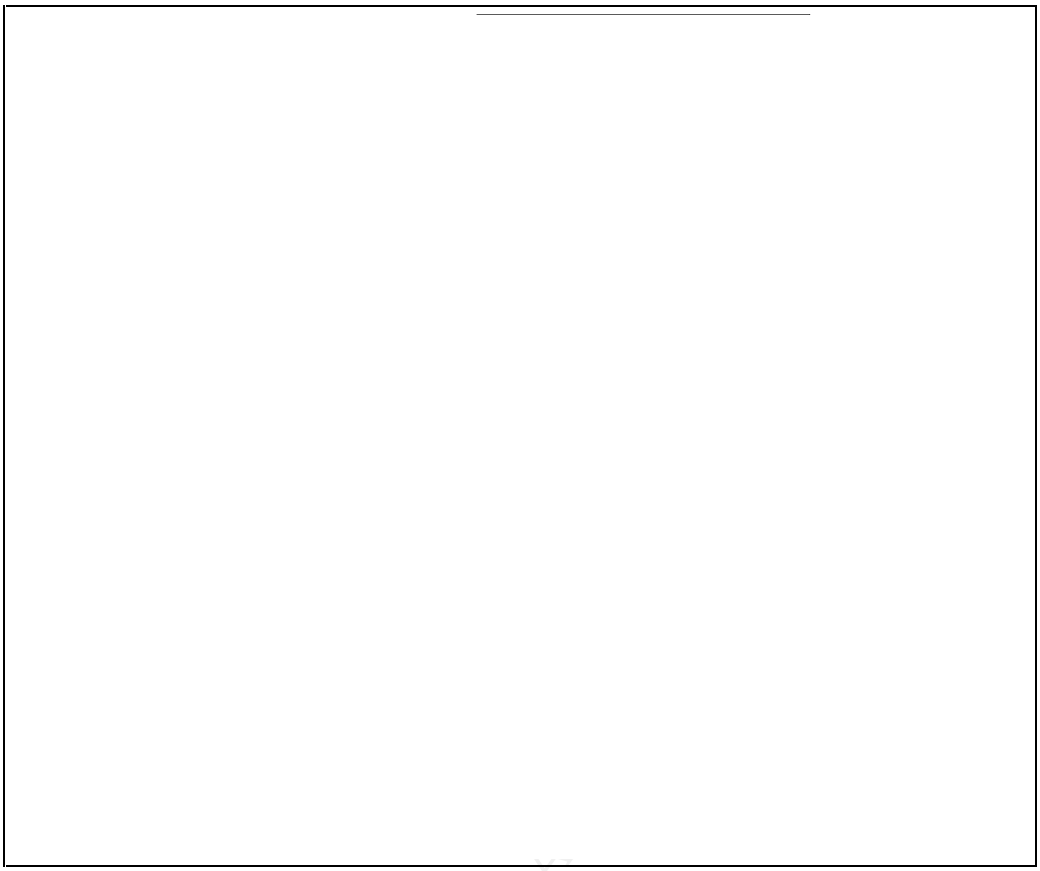

Figure E. Test Bed Configuration

Table N. Test Procedures

Requirement	Success Criteria	Procedure
AAA shall be used to authenticate all access to routing nodes using unique usernames and passwords.	A valid username and password will allow user access to the routing node and an invalid username and password will be rejected.	• Within the ACS web interface, create a group with two users and assign unique usernames and passwords to them. • From the administrators workstation, telnet to the routing node. Logon to each routing node using those usernames and passwords. • Exit the telnet session. • Again telnet to each routing node. Attempt to logon to each routing node using a valid username, but invalid password. • Attempt to logon to each routing node using an invalid username, but a valid password. • Attempt to logon to each routing node using an invalid username and an invalid password.
AAA services shall require the router node to authenticate using TACACS+ (Cisco IOS).	The router authenticates using TACACS+.	• From the administrator workstation, console into the routing node and logon as administrator. • At router prompt type, *enable*. At the prompt type, *debug aaa authentication*. • From the administrator workstation, telnet and logon to each routing node as any user. • Check the debug feedback in the console window to see if the authentication method is TACACS+.

Requirement	Success Criteria	Procedure
AAA services shall allow user defined minimum password length; the minimum length is 8 characters.	Valid passwords with a minimum length of 8 characters will allow access to the routing node, otherwise the password will not be allowed.	• Open the ACS web interface. Create a new user account, Regular User. Give this user limited privileges. Configure the AAA server to allow a minimum password length of 8 characters. • Enter a password that is less than 8 characters in length to see if the password is rejected. • Enter a password that is 8 characters or more in length. Confirm the password is accepted and is not visible during entry.
AAA services shall not allow passwords to contain the username.	Passwords containing the username will not be allowed.	• Using the new account created in the previous test. • Change the password. • Enter a password containing the username to see if it is accepted as a valid password.
AAA services shall require new passwords to be different from previous passwords.	Passwords changed to the previously used password will not be allowed.	• Using the same user account from previous test scenarios. • Change the password. • Enter the same password as the current password and see if it is accepted as a valid password.
AAA services shall require that new passwords use alphanumeric characters (AAA does not allow configuration of character types).	Passwords not containing alphanumeric characters will not be allowed.	• Using the same user account from previous test scenarios. • Change the password. • Enter a password that is at least 8 characters in length and contains only letters to see if it accepted as a valid password.

Requirement	Success Criteria	Procedure
AAA server will log when user try to login using expired accounts.	After the specified period of time the users account will expire and the account will remain locked until the administrator changes the password or moves the user to another group.	• Within the ACS web interface select “Group Setup,” select “Password Aging Rules” section, check the “Age-by-date rules” box. • Enter 0 in the 3 boxes and restart the service. • From the administrator workstation, establish a telnet session and try to login into the routing node. • On the ACS web interface, check the user status under “User Setup” to see if it indicates the user account has expired. Check log files for failed attempts.
User will be forced to change passwords after the first time a new user logs in.	The AAA server will request the password be changed the first time a user logs in.	• Open the ACS web interface, select “Group Setup,” select “Password Aging Rules” section, select the “Apply Password Change Rule”. • From the administrator workstation, establish a telnet session to the routing node. • Confirm that a new password is required.

Requirement	Success Criteria	Procedure
User passwords will expire after 90 days	The AAA server will require that the user change their password after 90 days.	• Open the ACS web interface, select “Group Setup”, select “Password Aging Rules” section. • Set the password to expire in 90 days. • On the administrator workstation, telnet to the routing node using the user/password. Log off the routing node. • On the AAA server reset the system clock for 90 days in advance. Reboot AAA server. • From the administrator workstation, telnet to the routing node. Confirm that the password has expired.
AAA services shall allow the ability to lock a user account after three failed login attempts, requiring administrator intervention to reset the account.	After a third failed login attempt, the user’s account will be disabled until the administrator resets the account.	• From the administrator’s workstation, establish a telnet session to each of the routing nodes. • Try and login to each of the routing nodes. Enter in a valid user name, but type the incorrect password three times when prompted. • Try logging in using the valid password. Verify that the login fails. • On the ACS web interface, check the user’s account under “User Setup” to see if the account is disabled.

Requirement	Success Criteria	Procedure
AAA services shall provide authorization for user access to routing nodes at the router command level.	Users attempting to run unauthorized commands will see a “command” authorization failed” message in the telnet window.	• From the administrator’s workstation, establish a telnet session and logon to each of the routing nodes as the Regular User. • Run show and debug commands to make sure these are allowed. • Enter into an unused interface for example Ethernet 0/1, *type int fa0/1.* • Type *no shut* and *shut.* Confirm these commands work. • Type *ip address 200.50.100.250 255.255.255.0.* Confirm that the system will not change the IP address.
AAA services shall provide for logging of routing node logon events (success or failure).	• Successful attempts will be logged in the “Passed Authentications” file (*.csv) for that day. • Failed logon attempts will be logged in the “Failed Attempts” file (*csv) for that day.	• From the administrator’s workstation, logon to each of the routing nodes using a valid username/password. • Through the ACS web interface, check the current file under “Passed Authentications” in the “Reports and Activity” section to see if the successful logon is recorded. • Attempt to logon to the routing node using an invalid username/password. • Check under “Failed Attempts” in the “Reports and Activity” section to see if the failed logon is recorded.
AAA services shall provide for logging of all administrative changes to the Cisco Secure ACS.	All administrative changes and activities will be logged to the “Administrative Audit” file (*csv) for the current day.	• Make a configuration change to any section of the ACS web interface. • Check under “Administration Audit” in the “Reports and Activity” section to see if the change is recorded.

Requirement	Success Criteria	Procedure
AAA services shall provide for logging of attempts to access router nodes outside of a user's AAA privilege settings (success or failure).	Any attempts to run unauthorized commands will be logged to the "Failed Attempts" file (*.csv) for the current day.	• On the administrator's workstation, telnet to each of the routing nodes. • Logon as the Regular User and enter an unauthorized command while in configuration mode. • On the ACS web interface, check under "Failed Attempts" in the "Reports and Activity" section to see if the attempt is recorded.
AAA services shall provide for logging of router node configuration changes.	Commands entered on the routing node will be logged in the "TACACS+ Administration" file (*csv) for the current day.	• From the administrator's workstation, logon to each of the routing nodes as the administrator and enter a command while in configuration mode. • On the ACS web interface, check the current "TACACS+ Administration" file to see if the router command was recorded. • Exit configuration mode on the routing node and run any authorized command. Check to see if it was recorded in the same file on the ACS web interface.
AAA services shall provide for backup of user and group databases and Cisco Secure ACS system configuration information at specified times.	User and Group databases will be backed up in the c:\Program Files\Cisco Secure ACS v3.1\CSAuth\System Backups directory on the AAA server at specified times.	• On the ACS web interface, under "ACS Backup" in the "System Configuration" section, configure the database to be backed up in 15 minute intervals. • At the end of 15 minutes, check under "ACS Backup and Restore" in the "Reports and Activity" section to see if the backup database file is created.

Requirement	Success Criteria	Procedure
AAA services shall provide at a minimum the date, time and username for each logged event.	The username, date and time will be logged every time a user logs into the routing node.	• On the ACS web interface, check under "TACACS+ Accounting" and "TACACS+ Administration" in the "Reports and Activity" section to see if the activities recorded include the username, date and time.

Implementation

Once all of the testing was completed, the implementation was planned and carried out. The AAA server was deployed to the two NOCs and to the second level support facility. The server at the second level support facility was configured as the primary AAA server and the two NOCs were the backup AAA servers. This provided redundancy in case the primary server was not able to function. The primary AAA server was configured to replicate user configurations to the backup AAA servers as well. See Table H, System Configuration, for the necessary configurations on the ACS server to enable replication. After the servers were set up, technicians at the second level support facility accessed each node individually via a telnet session and copied and pasted the AAA and TACACS+ router configurations into the routers. Once this was done, the AAA process began as the nodes started sending authentication requests to the AAA server when a user attempted to login.

Though this study concentrated on the router nodes, the Cisco switches were also configured for AAA, though TACACS+ services were not configured.

Figure F shows a basic network configuration of the final solution (keep in mind there are 100+ router nodes in the network).

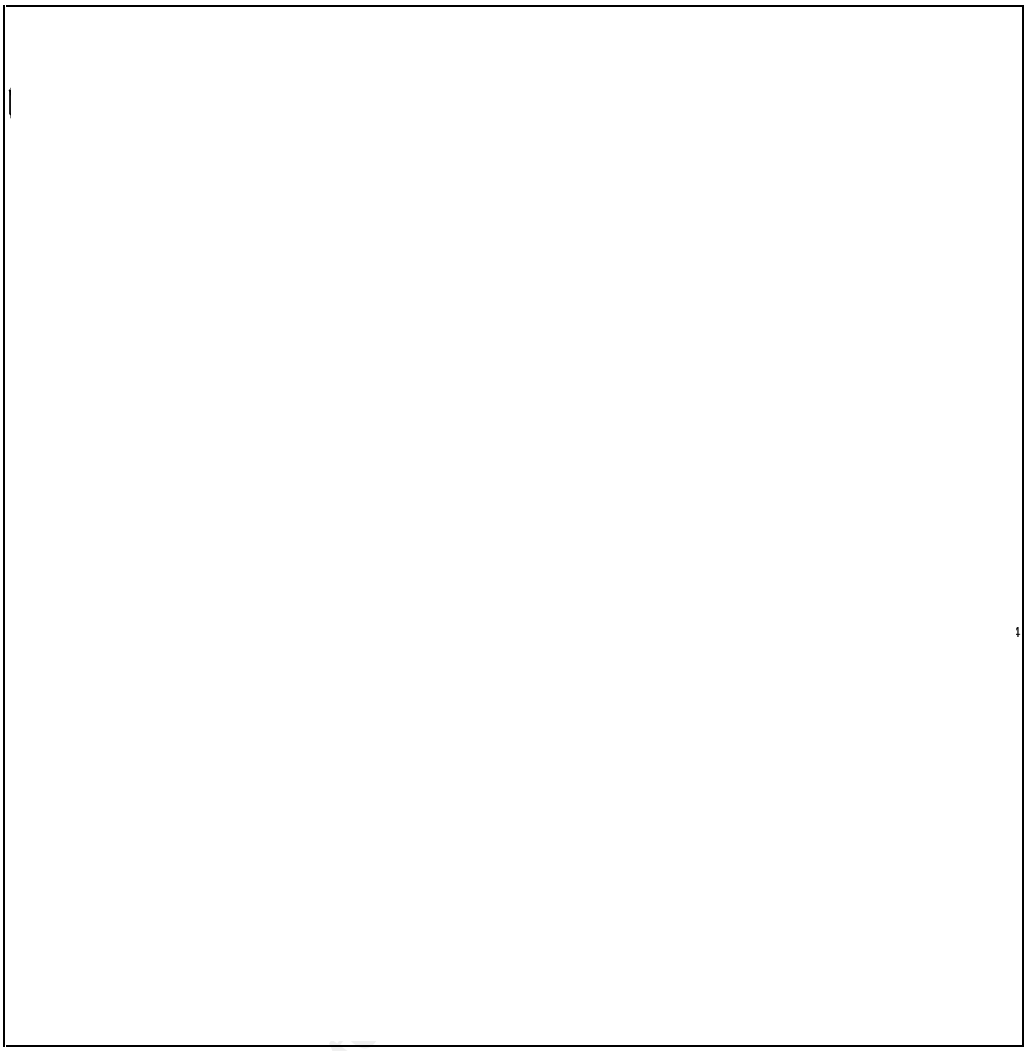

Figure F. Basic Configuration of Final Solution

Conclusion

In conclusion, the implementation of AAA servers using TACACS+ had a positive impact on the company's network. The solution reduced the risks identified in the original risk assessment, such as, lack of password policy controls, minimal logging of user actions and lack of user authorization control. Satisfying the recommendations of the risk assessment provided the extra security needed to help make this company's network less likely to be disrupted due to malicious or unintentional actions.

References

Gary Stoneburner, Alice Goguen and Alexis Feringa. NIST Special Publication 800-30. Risk Management Guide for Information Technology, Recommendations of the National Institute of Standards and Technology. October 2001. U.S. Government Printing Office, Washington, DC.

Cisco Systems, Inc. "AAA Technology Summary," "Comparison of TACACS+ and RADIUS" and "TACACS+ Overview." Cisco AAA Case Study Overview. URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/secsols/aaasols/c262c1.htm

"RADIUS/AAA Server for Managing and Securing Remote WLAN Access." Steel-Belted Radius/Enterprise Edition. URL: http://www.funk.com/radius/enterprise/sbr_ds.asp

Cisco Systems, Inc. User Guide for Cisco Secure ACS 3.1 for Windows Server. URL: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_book09186a0080102166.html

Cisco Systems, Inc. "Authentication Commands", "Authorization Commands", "Accounting Commands", "TACACS+ commands." Cisco IOS Software Release 12.1, Command Summaries, CS1: Part 6: Security. URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_summary_book09186a008008809d.html

"TACACS+." Internet Next Generation. 1 November 1999. URL: http://ing.ctit.utwente.nl/WU5/D5.1/Technology/tacacs+

Dell, Inc. URL: www.dell.com

CDW Corporation. URL: www.CDW.com

Cisco Systems, Inc. Online documentation for Cisco Secure ACS 3.1 for Windows software.