UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

ELTON ROBERTO GROCHOSKI VIEIRA
NEIDE CABRAL KREFER
WILLIAN PEREIRA VIEIRA DA CUNHA

# IMPLANTAÇÃO DE SERVIDOR DE AUTENTICAÇÃO TACACS + E RADIUS EM EMPRESA DE PEQUENO E MÉDIO PORTE

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2014

ELTON ROBERTO GROCHOSKI VIEIRA
NEIDE CABRAL KREFER
WILLIAN PEREIRA VIEIRA DA CUNHA

# IMPLANTAÇÃO DE SERVIDOR DE AUTENTICAÇÃO TACACS + E RADIUS EM EMPRESA DE PEQUENO E MÉDIO PORTE

Proposta para Trabalho de Conclusão de Curso do Curso Superior de Tecnologia em Sistemas de Telecomunicações da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA

2014

**TERMO DE APROVAÇÃO**

ELTON ROBERTO GROCHOSKI VIEIRA
NEIDE CABRAL KREFER
WILLIAN PEREIRA VIEIRA DA CUNHA

# IMPLANTAÇÃO DE SERVIDOR DE AUTENTICAÇÃO TACACS + E RADIUS EM EMPRESA DE PEQUENO E MÉDIO PORTE

Este trabalho de conclusão de curso foi apresentado no dia 21 de novembro 2013, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. PhD. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

**BANCA EXAMINADORA**

_____
Prof. MsC. Lincoln Herbert Teixeira
UTFPR

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
UTFPR

_____
Prof. Dr. Augusto Foronda
Orientador - UTFPR

“A Folha de Aprovação assinada encontra-se na Coordenação do Curso”

# RESUMO

VIEIRA, Elton Roberto Grochoski; KREFER, Neide Cabral; CUNHA, Willian Pereira Vieira da, **Implantação de servidor de autenticação tacacs + e radius em empresa de pequeno e médio porte .** 2013. 52 f. Trabalho de Conclusão de Curso (Graduação) – Curso Superior de Tecnologia em Sistemas de Telecomunicações, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Este trabalho apresenta tanto uma abordagem teórica quanto a implantação de um ambiente capaz de realizar a autenticação de usuários para garantir a segurança da informação, com foco na plataforma fornecida pela empresa americana Cisco Systems. Discute os conceitos referentes ao processo de autenticação e seus enfoques, bem como sua necessidade dentro de ambientes corporativos. Apresenta conceitos de diferentes protocolos responsáveis pelo processo de autenticação e seus funcionamentos. Complementado por uma implementação em campo, o estudo verificou, por meio de análises no ambiente criado, como ocorre a autenticação de um usuário e os possíveis resultados para estes processos. Traz como resultado do estudo um guia para futuras implementações na área de segurança da informação.

**Palavras-chave:** Segurança da informação. Autenticação. Autorização. Controle de acesso.

# ABSTRACT

VIEIRA, Elton Roberto Grochoski; KREFER, Neide Cabral; CUNHA, Willian Pereira Vieira da. **Deployment an authentication server radius and tacacs + in small and medium scale** . 2013. 52 f. Trabalho de Conclusão de Curso (Graduação) – Curso Superior de Tecnologia em Sistemas de Telecomunicações, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

This paper presents both a theoretical approach as the deployment of an environment able to perform user authentication to ensure security of information, focusing on the platform provided by the American company Cisco Systems. Discusses the concepts related to the authentication process and its approaches, as well as your need within corporate environments. Presents concepts of different protocols responsible for the authentication process and its workings. Supplemented by an implementation in the field, the study found, through analysis in the environment created, how does the authentication of a user and the possible outcomes for these processes. Brings as a result of the study a guide for future implementations in the area of information security.

**Keywords:** Information security. Authentication. Authorization. Access control.

## LISTA DE FIGURAS

Figura 1 - Como funciona a autenticação TACACS+.....17
Figura 2 - Processo de autorização de comando.....20
Figura 3 - Processo de autenticação via EAP.....28
Figura 4 - Visão geral de uma rede com ACS implementado.....30
Figura 5 - Tela inicial do Cisco ACS.....34
Figura 6 - Tela de criação dos *Network Device Groups* (*Location*).....35
Figura 7 - Tela de criação dos *Network Device Groups* (*Device Type*).....36
Figura 8 - Tela de criação dos *Network Devices and AAA Clients*.....37
Figura 9 - Tela de criação dos *Identity Groups*.....38
Figura 10 - Tela de criação dos *Users*.....39
Figura 11 - Tela de criação dos *Identity Store Sequences*.....40
Figura 12 - Tela de criação do *Shell Profile*.....41
Figura 13 - Tela de criação dos *Command Sets*.....42
Figura 14 - Tela de criação dos *Access Services*.....43
Figura 15 - Tela de criação da *Identity*.....44
Figura 1 - Tela de criação da *Authentication*.....45
Figura 17 - Logs de Autenticação.....46
Figura 18 - Detalhes de Autenticação com Sucesso.....47
Figura 19 - Detalhes de Autenticação sem Sucesso.....47

# LISTA DE TABELAS

Tabela 1 - Diferenças entre os protocolos RADIUS e TACACS +.....21

# LISTA DE SIGLAS

| | |
|---|---|
| AAA | Authentication, Authorization and Accounting |
| ACL | Access Control List |
| ACS SE | Access Controle Server Solution Engine |
| ACS | Access Control Server |
| CHAP | Challenge Handshake Authentication Protocol |
| CLI | Command Line |
| DOS | Denial of Service |
| EAP-FAST | Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling |
| EAP-GTC | Extensible Authentication Protocol – Generic Token Card |
| EAP-MD5 | Extensible Authentication Protocol - Message Digest Algorithm 5 |
| EAPOL | Extensible Authentication Protocol over LAN |
| EAP-SPEKE | Extensible Authentication Protocol - Simple Password-authenticated Exponential Key Exchange) |
| FTP | File Transfer Protocol |
| HTTP | Hyper-Text Transfer Protocol |
| IETF | Internet Engineering Task Force |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LEAP | Lightweight Extensible Authentication Protocol |
| MAR | Machine Access Restriction |
| MD5 | Message-Digest algorithm 5 |
| NAC | Network Access Control |
| NAF | Network Access Filter |
| NAP | Network Access Profile |
| NAS | Network Access Server |
| NDG | Network Device Group |
| ODBC | Open DataBase Connectivity |
| PAP | Password Authentication Protocol |
| PDP | Policy Decision Point |
| PEAP | Protected Extensible Authentication Protocol |
| PEP | Policy Enforcement Point |
| PIP | Policy Information Point |
| PPP | Point to Point Protocol |
| RADIUS | Remote Authentication Dial In User Service |
| SLA | Service Level Agreement |
| SSH | Secure Shell |
| TACACS | Terminal Access Controle Access-Control System |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAP | Wireless Application Protocol |
| WLAN | Wireless Local Area Network |

# SUMÁRIO

**1. INTRODUÇÃO ..... 9**
1.1 PROBLEMA ..... 9
1.2 JUSTIFICATIVA ..... 10
1.3 OBJETIVO ..... 10
1.3.1 Objetivo geral ..... 10
1.3.2 Objetivos específicos ..... 10
1.4 PROCEDIMENTOS METODOLÓGICOS ..... 11
**2. FUNDAMENTAÇÃO TEÓRICA ..... 12**
**3. IMPLEMENTAÇÃO ..... 30**
3.1 A REDE ..... 30
3.2 CONFIGURAÇÃO DOS EQUIPAMENTOS DE REDE ..... 31
3.2.1 Configuração do protocolo ssh ..... 31
3.2.2 Configuração do protocolo aaa ..... 32
3.3 CONFIGURAÇÃO DO SERVIDOR DE AUTENTICAÇÃO ..... 34
3.3.1 Criação dos *network device groups* ..... 34
3.3.2 Criação dos *network device and aaa clients* ..... 36
3.3.3 Criação dos *identity groups* ..... 37
3.3.4 Criação dos *users* ..... 38
3.3.5 Criação das *identity store sequences* ..... 39
3.3.6 Criação do *shell profile* ..... 40
3.3.7 Criação dos *command sets* ..... 41
3.3.8 Criação dos *access services* ..... 42
3.3.9 Criação da *identity* ..... 43
3.3.10 Criação de *authentication* ..... 44
3.4 TESTES ..... 46
**4. CONCLUSÃO ..... 49**
**REFERÊNCIAS ..... 50**

# 1. INTRODUÇÃO

Em um mundo cada vez mais interligado, a troca e transferência de informações são necessárias para o desenvolvimento de qualquer negócio. Por isso, é tão importante contar com uma rede segura para garantir a integridade e sigilo dos dados (METROBYTE, 2013).

Com o crescimento das conexões cliente-servidor, deverão também crescer as ameaças a esses dispositivos. O mercado de segurança especificamente voltado para redes deverá valer US$ 752 milhões até o final de 2017, o que inclui receitas com segurança de transmissão, de bens físicos e de acordos de nível de serviço (SLAs). Considerando uma empresa com múltiplos usuários, múltiplas unidades, múltiplos clientes e múltiplos fornecedores onde todos precisam de alguma forma acessar a rede da empresa, torna-se inviável montar políticas diferentes de acesso para cada tipo de usuário ou então ser mais radical e não permitir o acesso as redes (TELETIME, 2012).

Uma infraestrutura de rede pode ter segurança e integridade com os protocolos de autenticação RADIUS e TACACS +. Através destes protocolos é possível criar diferentes perfis de usuários dentro de uma rede e também negar o acesso para possíveis usuários maliciosos. Com esses diferentes perfis é possível determinar a qual segmento de cada usuário poderá ter acesso, preservando assim os dados sigilosos da empresa. Para monitorar e identificar problemas é possível visualizar se um usuário foi autenticado ou não. Em caso de erro, o motivo que houve falha na autenticação também é apresentado. Este projeto mostrará a implantação desta tecnologia e o seu funcionamento, em um ambiente empresarial de pequeno ou médio porte (HOOPER, 2012, p. 430).

## 1.1 PROBLEMA

- Configurar os equipamentos, *routers* e *switches*, para que a rede suporte a autenticação via TACACS + e RADIUS;
- Estudar o funcionamento e configuração do *Cisco Secure Access Control System (ACS);*

- Instalar o ACS em um servidor virtual e realizar a conexão entre este e a rede implantada no ambiente real;
- Demonstrar a instalação do ACS em um servidor físico (CSACS-1121);
- Simulação do ambiente funcionando como um todo e resolução de possíveis problemas que ocorram durante o mesmo.

## 1.2 JUSTIFICATIVA

Este projeto visa a implantação da tecnologia de autenticação via *TACACS* + e *RADIUS*, de padrão *Cisco Systems*, em uma empresa com sucursais dispersas em todo o território nacional. A implantação desta tecnologia viabilizará a utilização de um único servidor centralizado para autenticação de sites remotos e usuários dentro da rede de dados, possibilitando assim que a empresa reduza seus gastos com manutenção em dispositivos descentralizados; além de ter um controle de segurança para acesso a rede e criação de relatórios para fim de *troubleshooting*.

## 1.3 OBJETIVO

### 1.3.1 OBJETIVO GERAL

Implantar a tecnologia de autenticação TACACS + e RADIUS, proprietário da *Cisco Systems*, em uma rede de dados de uma empresa de pequeno e médio porte.

### 1.3.2 OBJETIVOS ESPECÍFICOS

- Pesquisar os equipamentos da família *Cisco Systems* compatíveis com a tecnologia TACACS + e RADIUS;
- Definir e desenhar a rede de dados da empresa, com todas as suas sucursais dispersas;
- Simular esta rede de dados no ambiente operacional real;
- Configurar os equipamentos, *routers* e *switches*, para que a rede suporte a autenticação via TACACS + e RADIUS;

- Estudar o funcionamento e configuração do *Cisco Secure Access Control System (ACS);*
- Instalar o servidor ACS e realizar a conexão entre este e a rede implantada;
- Demonstrar a instalação do ACS em um servidor físico (CSACS-1121);
- Verificação do ambiente funcionando como um todo e resolução de possíveis problemas que ocorram durante o mesmo.

## 1.4 PROCEDIMENTOS METODOLÓGICOS

Como a tecnologia de autenticação TACACS + e RADIUS a ser implementada neste projeto é proprietária da *Cisco Systems*, toda a pesquisa será realizada em cima de matérias publicadas pela própria empresa e parceiros.

Serão utilizados os guias de estudos para certificações relacionados com a tecnologia de autenticação, como as certificações *CCNA Security* e *CCNP Security.* No caso da certificação *CCNP Security* existem quatro guias para estudo, dos quais serão utilizados principalmente o primeiro, que possui um grande foco em autenticações e configurações dos *devices,* o que será muito necessário para o desenvolvimento deste projeto.

Será utilizada também a página *web* da *Cisco Systems*, a qual possui uma vasta quantidade de material relacionado à seus produtos e as tecnologias suportadas. Este material contido no site são atualizações de assuntos e resoluções de problemas que foram encontrados na implantação ou funcionamento da tecnologia, e não foram incluídos nos guias de estudos.

Para realização da simulação da solução de autenticação TACACS + E RADIUS será utilizado um simulador de redes chamado GNS3. O estudo e pesquisa de seu funcionamento serão realizados em documentos dispostos na página *web* do próprio simulador, bem como a instalação de uma máquina virtual com o servidor Cisco ACS, os quais é possível analisar o funcionamento em seus manuais e no próprio site da Cisco.

# 2. FUNDAMENTAÇÃO TEÓRICA

A banda larga na sociedade de hoje representa muito mais que um acesso rápido à internet ela é o principal veículo de inclusão social, capaz de levar não apenas conhecimento aos cidadãos, mas também desenvolvimento econômico ao País. A banda larga no Brasil tem feito uma revolução ágil e silenciosa, com a conexão de mais de 94 milhões de acessos, sendo que mais da metade desse total foram acessos ativados muito recentemente, nos últimos 18 meses. (LEVY, 2013).

Até outubro de 2012, 26 milhões de novos acessos foram ativados, a um ritmo de uma nova conexão por segundo. Um grande contingente da população passou a ter acesso a novas aplicações, serviços e facilidades do dia a dia, apenas por estarem conectados. (LEVY, 2013).

Toda esta oferta oferece aos fraudadores um leque variado de novos meios para cometer fraudes ainda nem previstos, tais como as existentes atualmente na internet:

- *Hacking*;
- Cavalo de Tróia (*Trojan Horses*);
- DoS (*Denial of Service*);
- *Spoofing*.

No mundo IP novas ameaças se fazem presentes, ameaças essas que vão além das perdas financeiras, tais como (SALOMON, 2013):

- Falsificação de Identidade: onde o usuário esconde sua identidade através de um assinante real, funcionando como um disfarce ideal para o tráfico de drogas, o crime organizado, o terrorismo e a lavagem de dinheiro;
- Perda de Qualidade do Serviço: onde múltiplos usuários consumem todos os recursos de uma determinada rede: DoS, *Spam*, *Malware*;
- Violação de SLA: onde por meio da manipulação de indicadores de qualidade de serviço Provedores de Conteúdo cobram por qualidade de serviço não ofertado;

- Utilização imprópria de serviços e conteúdo: onde após roubar as informações, estas são revendidas de forma não autorizada;
- Deterioração da imagem da operadora, devido a Interrupção de Serviço, provocando perda (*Churn*) de assinantes lucrativos;
- Perda de conteúdo pelo usuário final (*ringtones*, filmes, etc.), quando da ocorrência de problemas no terminal celular e não existência de política (serviço) de backup oferecido pela operadora;
- Sabotagem de Serviços em geral;
- Responsabilidade Social e Política relacionada ao anonimato de atividades ilegais, tais como: Pedofilia, Pornografia, Terrorismo, Lavagem de Dinheiro.

A proteção de uma rede contra o acesso indevido é uma maneira eficiente para auxiliar na mitigação de diversos tipos de fraudes. Esta proteção pode ser feita através da restrição de acesso aos equipamentos. Sem acesso à infraestrutura de rede os atacantes terão muito mais dificuldade de cometer suas fraudes.

Os protocolos de autenticação são tecnologias que podem ser utilizadas para proteção de uma rede. Ambos fazem parte do processo de autenticação onde atuam protegendo o acesso remoto às redes e aos serviços. Este processo de autenticação possui três componentes (WATKINS; WALLACE, 2008, p. 234):

- Um servidor de autenticação;
- Um autenticador;
- Um cliente.

As transações entre o cliente e o servidor são autenticadas através do uso de um segredo compartilhado, que nunca é enviado através da rede. Além disso, todas as senhas do usuário são enviadas criptografadas entre o cliente e o servidor RADIUS, o que garante a integridade dos dados trafegados nestas transações (WATKINS; WALLACE, 2008, p. 141).

Os flexíveis mecanismos de autenticação do servidor suportam uma variedade de métodos para autenticar um usuário. Estes métodos são: PPP (*Point-to-Point Protocol*), PAP (*Password Authentication Protocol*), CHAP (*Challenge-Handshake Authentication Protocol*) ou UNIX *login*, e outros mecanismos de autenticação (RFC 2138).

A maneira mais eficiente de gerenciar acesso à rede é através dos protocolos AAA. O modelo de protocolos AAA (*authentication, authorization and accounting*) ajuda a gerenciar quem acessa a rede e quais segmentos da rede podem ser acessados, além de prover meios de determinar quando, onde e como esses acessos serão feitos. O AAA é composto de uma série de serviços de segurança na rede montados numa forma modular, provendo assim a estrutura básica para a configuração de um NAC (*Network Access Control*). Os protocolos TACACS + e RADIUS são baseados no modelo AAA, sendo assim é importante detalhar as principais características deste modelo (WATKINS; WALLACE, 2008, p. 111). Para ajudar a entender melhor o modelo AAA, é importante detalhar melhor as características deste modelo (WATKINS; WALLACE, 2008, p. 115);

- Autenticação é o processo em que os usuários e administradores provam que eles realmente são quem eles dizem ser. Há várias maneiras de isto ser implantado na rede, sendo alguns exemplos o uso de nome de usuário e senha, cartões token e uso de pergunta e resposta. Assim que o usuário ou administrador é autenticado, serviços de autorização decidem quais recursos o mesmo poderá usar dentro da rede.

- Já contabilidade ou auditoria, como também pode ser chamada, tem como característica gravar todos os acessos que o usuário fez dentro da rede. Informações pertinentes a esta função é o que o usuário acessou, quando, por quanto tempo, entre outras.

A Cisco disponibiliza três maneiras de implementar os serviços do modelo AAA: (WATKINS; WALLACE, 2008, p. 115):

- *Cisco Secure ACS Solution Engine*: nesta implementação temos que os serviços AAA contactam um ACS SE para autenticação tanto para usuários como para administradores. O ACS SE é usado para controlar quem pode acessar a rede, para autorizar que tipos de serviços de rede são disponíveis para os usuários ou grupos de usuários, e para manter um registro contábil de todas as ações dos usuários na rede. Suporta controle de acesso e

contabilidade para servidores de acesso *dial-up*, *firewalls* e VPNs (*Virtual Private Networks*), voz sobre IP, soluções de redes de conteúdo e comutação e redes locais sem fio (LANs e WLANs). Além disso, é usado o mesmo quadro AAA, via TACACS +, para gerir funções administrativas e para controle;

- *Cisco Secure Access Control Server* (ACS) *for Windows Server*: Este é um pacote de softwares que pode ser usado para autenticação usando usuário e senha. Os serviços AAA rodando num roteador ou NAS que contactam um *Cisco Secure* ACS rodando num sistema *Microsoft Windows*;
- *Self-Contained* AAA: Como o nome já diz, os serviços AAA já estão embutidos no roteador ou NAS, ganhando assim o nome de autenticação local.

O modelo AAA pode ser dividido nas seguintes categorias (CONVERY, 2013):

- *Client to Policy Enforcement Point* (PEP);
- *PEP to Policy Decision Point* (PDP);
- *Client to PDP*;
- *PDP to Policy Information Point* (PIP).

Os três principais protocolos de comunicação entre PEP e PDP são (CONVERY, 2013):

- RADIUS;
- TACACS+;
- *Diameter*.

Os protocolos AAA TACACS + e RADIUS são os mais utilizados, cada um com características diferentes que os tornam adequados para diferentes situações.

O protocolo RADIUS foi originalmente desenvolvido pela Livingston Enterprises Inc. e agora faz parte do padrão baseado em IETF *(Internet Engineering Task Force*) (RFC 2138). Um servidor RADIUS é executado como um serviço

(baseado em Windows ou Linux) e fornece serviços de autenticação e contabilidade para um ou mais dispositivos de rede que estão atuando como clientes RADIUS. O cliente envia solicitações de autenticação para um servidor central que contém toda a autenticação de usuário e informações de acesso aos serviços da rede. Tipicamente, um servidor RADIUS é implantado como uma máquina dedicada que está ligada à rede. Você pode ter vários servidores RADIUS para redundância. Estes servidores oferecem os seguintes recursos (DEVERIYA, 2006, p. 92):

- Controle de acesso centralizado: fornece uma gestão centralizada de serviços de controle de acesso através da rede;
- Criptografia: no RADIUS apenas a senha é criptografada. O cliente RADIUS usa o algoritmo *Message Digest* 5 (MD5) para enviar senha para o servidor. O algoritmo MD5 produz um *hash* da senha, que por sua vez é enviado ao servidor. Como apenas o *hash* é enviado (e não a senha), existe uma garantia de que ninguém pode saber a senha por espionagem na linha;
- Baseado no protocolo UDP: utiliza as portas 1812 e 1645 para autenticação e as portas 1813 e 1646 para a contabilidade. O uso de UDP fornece um desempenho mais rápido, pois o protocolo RADIUS inclui um mecanismo integrado para o tratamento de retransmissão e problemas de tempo limite, eliminando assim a necessidade de TCP.

O protocolo TACACS+ foi desenvolvido pela Cisco e trata-se de um conjunto de *software* e protocolos de cliente / servidor que fornece serviços de AAA, oferecendo os seguintes recursos (DEVERIYA, 2006, p. 91):

- Acesso centralizado de controle: fornece gerenciamento centralizado dos serviços de controle de acesso através da rede;
- Serviços modulares: fornece serviços modulares e separados de autenticação autorização e contabilidade. Esses serviços podem utilizar um único banco de dados, ou cada serviço pode ter seu próprio banco de dados;
- Criptografia: todas as informações transmitidas entre o cliente e um servidor TACACS+ são criptografadas; tanto o cliente como o servidor devem ser configurados com a mesma chave de criptografia;

- Confiabilidade: usa TCP (*Transmission Control Protocol*) para uma conexão confiável e robusta entre o cliente e o servidor. O número padrão da porta TCP é 49, embora isso possa ser alterado.

O protocolo TACACS+ será abordado com mais ênfase neste texto, por ser um protocolo mais atual e mais completo, além de mais flexível; ele permite por exemplo que uma conexão arbitrária seja realizada entre o servidor e o usuário até que o servidor receba informação suficiente para autenticar o usuário. Tipicamente, isto é realizado por solicitação de uma combinação de usuário e senha, mas isso pode incluir métodos adicionais também, como por exemplo pergunta e resposta (WATKINS; WALLACE, 2008, p. 138).

O processo de autenticação é baseado numa serie de troca de mensagens entre três elementos da rede. Os elementos envolvidos são (MALIK, 2003, p.122):

- *Supplicant* ou suplicante;
- *Authenticator* ou autenticador;
- *Authentication Server* ou Servidor de Autenticação.

A figura 1 ilustra o processo de autenticação com as trocas de mensagens entre os três elementos da rede:

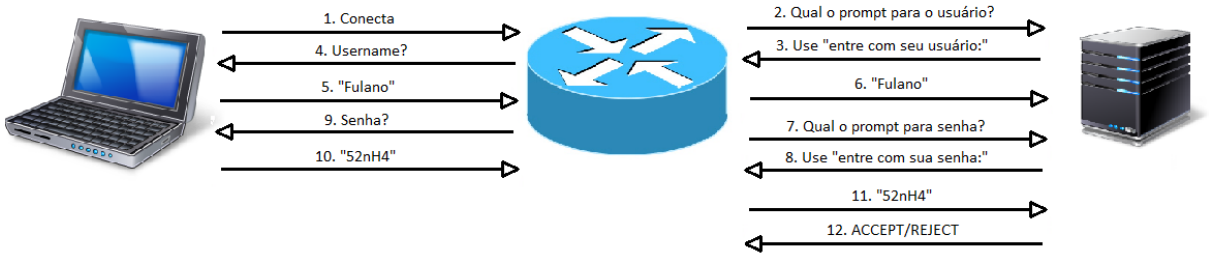


**Figura 2 - Como funciona a autenticação TACACS+**
**Fonte: WATKINS; WALLACE, 2008, p. 138**

1. O suplicante solicita acesso;
2. O autenticador solicita um *prompt* de nome de usuário para o servidor de autenticação;

3. O servidor de autenticação fornece um *prompt* de nome de usuário;
4. O autenticador repassa ao usuário o *prompt* fornecido pelo servidor;
5. O suplicante fornece um nome de usuário;
6. O autenticador encaminha o nome de usuário para o servidor de autenticação;
7. O autenticador solicita um *prompt* de senha para o servidor de autenticação;
8. O servidor de autenticação fornece um *prompt* de senha;
9. O autenticador repassa ao usuário o *prompt* de senha;
10. O suplicante envia a senha;
11. O autenticador encaminha a senha para o servidor de autenticação;
12. O servidor de autenticação aceita ou rejeita o usuário, baseado nas polícitas definidas pelo administrador.

Diferentemente do que se pode notar, o autenticador tem um papel importante durante a autenticação pois ele não atua apenas como meio de comunicação entre o suplicante e o servidor de autenticação. O autenticador também é responsável pela liberação da porta que o *supplicant* está tentando conectar. Está porta será devidamente liberada se o processo de autenticação for finalizado com sucesso (MALIK, 2003, p.122).

Há casos em que o servidor de autenticação não vai permitir o acesso solicitado pelo suplicante, para isto o servidor conta com os seguintes resultados para o processo de autenticação: (WATKINS; WALLACE, 2008, p. 139):

- ACCEPT: O suplicante é autenticado e recebe a permissão de acessar a porta solicitada;
- REJECT: A autenticação falhou para o suplicante. O suplicante é solicitado a repetir a seqüência de login ou todo o acesso é negado, dependendo das políticas aplicadas pelo administrador;
- ERROR: Um erro ocorreu em algum momento durante o processo de autenticação. Isso pode ter ocorrido tanto no servidor ou na conexão de rede entre o servidor e o autenticador. Se uma resposta de erro é recebida, o autenticados normalmente tenta usar um método alternativo para autenticar o usuário, como as senhas configuradas localmente no autenticado;

- CONTINUE: o processo ainda não é finalizado, sendo que mais informações de autenticação são solicitadas do suplicante.

Assim que a fase de autenticação é finalizada, o suplicante deve iniciar a fase de autorização. O servidor de autenticação é contatado novamente que retorna uma resposta (ACCEPT ou REJECT). Se retornar ACCEPT como resposta, é enviado junto informações que são usadas para direcionar a sessão de rede para o suplicante. Isso determina quais serviços o usuário pode acessar. O servidor de autenticação pode ser configurado para carregar um ACL por suplicante, assim como vários outros parâmetros (WATKINS; WALLACE, 2008, p. 139).

As etapas envolvidas no processo de autenticação são as seguintes (WATKINS; WALLACE, 2008, p. 140):

1. O autenticador envia um pedido de autorização para acesso à rede para o servidor de autenticação;
2. O pedido é aceito ou negado pelo servidor. Se o acesso for aceito, parâmetros de autorização são enviados para o autenticador e em seguida aplicados na conexão do usuário.

O servidor utiliza uma grande quantidade de atributos para autorização, isto permite um controle maior da rede e um acesso muito restrito aos suplicantes. Este acesso restrito permite aos suplicantes acessar apenas o necessário impedindo diversos tipos de fraldes na rede. Alguns dos parâmetros mais utilizados são (WATKINS; WALLACE, 2008, p. 140):

- ACL (autorização EXEC): Lista o número da classe de acesso que será aplicada a uma linha;
- ADDR (SLIP, PPP/autorização IP): Ao usar uma conexão SLIP ou PPP/ IP, este atributo é usado para especificar o endereço IP do host remoto;
- CMD (EXEC):Este atributo é usado para iniciar um pedido de autorização para um comando EXEC;

- Priv-lvl (autorização EXEC): Pode ser um número inteiro (*integer*) entre 0 e 15 e é usado para especificar o nível de privilégio atual de autorização de comando;
- Route (PPP/ IP, SLIP autorização): Usado para especificar uma rota a ser aplicada a uma interface;
- InACL (PPP/IP, SLIP autorização): Usado com SLIP ou PPP/ IP para listar o IP de entrada de uma ACL;
- OutACL: Usado com SLIP ou PPP/ IP para listar uma IPACL de saída;
- Addr.-pool: Usado para especificar o nome de um pool de endereços local, a partir do qual se obtém o endereço do host remoto;
- Autocmd: Usado para especificar um comando a ser executado automaticamente na inicialização EXEC.

Além destes atributos, há diversos outros atributos utilizados em diferentes aplicações de rede. Como o protocolo TACACS+ é um protocolo proprietário da Cisco. É o principal protocolo usado com implementações AAA em redes Cisco. Sendo assim compatível com roteadores, switches, IOS PIX Firewall da Cisco (WATKINS; WALLACE, 2008, p. 141).

A Figura 2 ilustra o processo de autorização envolvido quando um suplicante deseja executar o comando "configure terminal" no autenticador.


**Figura 3 - Processo de autorização de comando**
**Fonte: WATKINS; WALLACE, 2008, p. 138**

1. O suplicante solicita a autorização para executar o comando "*configure terminal*";
2. O autenticador encaminha ao servidor de autenticação a solicitação do suplicante informando qual usuário deseja executar o comando;

3. O servidor de autenticação permite o acesso encaminhando ao autenticador o resultado “*ACCEPT*”;
4. O autenticador permite a execução do comando “*configure terminal*”.

Neste exemplo, o autenticador consulta o servidor de autenticação sobre a permissão para executar o comando solicitado pelo suplicante. Durante este processo, o servidor e o autenticador estabelecem uma nova sessão TCP, esta no sessão ocorre a cada pedido de autorização. Desta maneira, quando há problemas de comunicação entre o servidor e o autenticador pode existir atrasos quando o suplicante tentar acessar difentes serviços (WATKINS; WALLACE, 2008, p. 140).

Desta forma ao utilizar sessões dedicadas é garantido uma melhor detecção de quebra na comunicação. Esta única sessão persiste enquanto o servidor ou o dispositivo de rede estiverem operacionais (WATKINS; WALLACE, 2008, p. 141).

Para auditar e guardar todas as atividades executadas pelos usuários contamos com o servidor de autenticação que armazena a informação de cada transação solicitada por todos os suplicantes (RILEY, 2003, p. 705).

Para ilustrar as principais diferenças entre estes dois principais protocolos abaixo tem-se uma tabela comparando os protocolos RADIUS e o TACACS+:

**Tabela 2 - Diferenças entre os protocolos RADIUS e TACACS +**
**Fonte: DEVERIYA, 2006, p. 93**

| | **TACACS+** | **RADIUS** |
|---|---|---|
| Desenvolvedor | Cisco. | Livingston; atualmente um protocolo de código aberto. |
| Implementadores | Cisco. | Várias empresas incluindo Cisco. |
| Portas | TCP 49. | UDP 1812, 1813, 1645, 1646. |
| RFC | IETF *draft-grant*-TACACS. | RFC 2865, 2139, 2138. |
| Encriptação | Todo o pacote é criptografado, exceto o cabeçalho. | Apenas a senha é criptografada; o resto do pacote está em texto legível (*clear text*). |
| Modularidade | Separa autenticação, | Autenticação e autorização |

| | **TACACS+** | **RADIUS** |
|---|---|---|
| | autorização e contabilidade, gerando assim um maior | estão juntos. controle. |
| Suporte a diferentes protocolos | Vários protocolos são suportados. | Não há suporte para os seguintes protocolos: AppleTalk Remote Access (ARA) *Protocol, NetBIOS Frame Protocol Control Protocol, Novell Asynchronous Services Interface* (NASI), e conexão X.25 PAD. |
| Comandos dos Roteadores | Fornece controle granular sobre cada comando em cada roteador, podendo ser executado tendo como base um usuário ou um grupo que pode ser executado em uma base por usuário ou por grupo. | Não há suporte para controlar os comandos de cada roteador. |

Embora ambos os protocolos RADIUS e TACACS+ forneçam funcionalidade AAA, os seus padrões de uso dentro da indústria são diferentes. TACACS+ é usado frequentemente para assegurar o acesso a dispositivos de rede como roteadores e switches. Enquanto o RADIUS é amplamente utilizado para controlar o acesso aos recursos da rede, tais como HTTP, FTP, e-mail e compartilhamento de arquivos e de impressão através de dial-up ou *Virtual Private Networks* (VPN). Em tais situações, os dispositivos de acesso (chamados de servidores de acesso à rede, ou NAS) são configurados para consultar os servidores RADIUS para verificar a solicitação do usuário de um determinado recurso. Exemplos de dispositivos que utilizam RADIUS são os seguintes (DEVERIYA, 2006, p. 93):

- Roteadores com uma lista de acesso por usuário;
- Switches com porta de segurança;
- Firewalls com proxies de autenticação;

- Concentradores VPN para usuários remotos;
- WLANs com autenticação de usuário 802.1X;
- Dispositivos compatíveis com WAP (*Wireless Application Protocol*).

A fim de fornecer as funcionalidades demandadas pelos protocolos AAA (*authentication*, *authorization* e *accounting*) a *Cisco Systems* conta com o *Cisco Secure ACS*, o qual provê serviços AAA para dispositivos de rede que atuam como clientes AAA (ROLAND, 2004, p. 53).

Esta ferramenta é um sistema de políticas de acesso centralizado, escalável e de alto desempenho, o qual através do protocolo TACACS + permite o gerenciamento e a administração dos acessos de usuários para os mais diferentes cenários, conforme descrito abaixo: (CISCO ACS DATASHEET, 2013):

- Administração do dispositivo: *Cisco Secure ACS* autentica os administradores de rede, autoriza comandos, além de fornecer *audit trail*;
- Acesso remoto: trabalha com VPN e outros dispositivos de acesso remoto à rede para aplicar políticas de acesso;
- Sem fio: *Cisco Secure ACS* autentica e autoriza usuários wireless e reforça as políticas específicas de wireless;
- 802.1xLAN: Suporte aprovisionamento dinâmico de VLANs e listas de controle de acesso (ACLs) em uma base por usuário e 802.1x com segurança baseada em porta;
- *Network Admission Control*: *Cisco Secure ACS* se comunica com servidores de postura e de auditoria para impor políticas de controle de admissão.

Abaixo tem-se algumas das funcionalidades suportadas pelo Cisco Secure ACS:

- Suporte a protocolos AAA: *Cisco Secure ACS* suporta dois protocolos AAA distintos, o RADIUS e TACACS+. RADIUS é suportado para o controle de acesso à rede; já o TACACS+ para controle de acesso aos dispositivos de rede. *Cisco Secure ACS* é um único sistema que consegue impor políticas de acesso à rede, além do gerenciamento e configuração dos dispositivos que formam esta rede.

Suporte para administração de equipamentos compatíveis com TACACS+ em redes rodando tanto IPv4 quanto IPv6 (CISCO ACS DATASHEET, 2013).

- Banco de dados: *Cisco Secure ACS* pode trabalhar tanto usando seu banco de dados interno, como tem suporte a integração com *Windows Active Directory, LightWeight Directory Access Protocol* (LDAP) e *Open Database Connectivity* (ODBC). Além disto, suporte para *RSA SecurID Authentication Manager* e *RADIUS-enabled token servers* garantem um sistema de autenticação robusto (CISCO ACS DATASHEET, 2013).

- Protocolos de autenticação: *Cisco Secure ACS* tem suporte a uma infinidade de protocolos de autenticação, incluindo *Password Authentication Protocol* (PAP), *Challenge Handshake Authentication Protocol* (CHAP), MS-CHAP, *Extensible Authentication Protocol* (EAP)-MD5, *EAP-Generic Token Card* (GTC), *Cisco LEAP*, *Protected EAP* (PEAP), *EAP-Flexible Authentication via SecureTunneling* (FAST), e *EAP-Transport Layer Security* (TLS) (CISCO ACS DATASHEET, 2013).

- Políticas de acesso à rede: *Cisco Secure ACS* disponibiliza a configuração de políticas de acesso à rede que incluem restrições baseadas em autenticação do usuário, data e hora, entre outras. É possível também aplicar listas de controle de acesso via download (dACLs), atribuição de VLAN, além de outros parâmetros de autorização (CISCO ACS DATASHEET, 2013).

- Gerenciamento centralizado: *Cisco Secure ACS* permite ao administrador replicar configurações para outros servidores ACS presentes na rede, criando assim flexibilidade e um fácil gerenciamento de redes mais complexas. Esta ferramenta de gerenciamento é disponibilizada tanto via interface web (*web-based* GUI), ou via interface de linha de comando (CLI) (CISCO ACS DATASHEET, 2013).

- Registro de eventos: Os registros de eventos (também chamado de *logs*) do *Cisco Secure ACS* podem ser visualizados e exportados para outros sistemas. Estes registros ajudam o administrador na manutenção do sistema, diagnóstico,

auditoria, criação de relatório, entre outras atividades (CISCO ACS DATASHEET, 2013).

- Opções de plataforma: *Cisco Secure ACS* está disponível como uma plataforma física ou como *software* para *Windows Server*. Para clientes que irão trabalhar com servidores virtuais, *Cisco Secure ACS for Windows* pode ser usado em conjunto com a solução *VMWare ESX Server* (CISCO ACS DATASHEET, 2013).

- Serviço *Proxy*: *Cisco Secure ACS* pode funcionar como um *proxy* RADIUS ou TACACS+ para um servidor AAA externo, direcionando pedidos AAA entre um dispositivo da rede e este um servidor externo.

- Suporte a Cisco NAC (*Network Admission Control*): é uma iniciativa patrocinada pela Cisco Systems e se baseia no Cisco Secure ACS. A solução utiliza a infra-estrutura de rede para garantir o cumprimento da política de segurança em todos os dispositivos que buscam acessar os recursos de computação em rede. Em implementações NAC, *Cisco Secure ACS* para Windows fornece políticas configuráveis que usa para avaliar e validar as credenciais recebidas do *Cisco Trust Agent*. Com estas credenciais é determinado o estado da máquina e enviada uma autorização para o NAD: ACLs, uma ACL baseada em políticas, ou uma atribuição de VLAN privada. Esta avaliação das credenciais da máquina pode impor uma variedade de políticas específicas, tais como nível de *patch* do OS e versão do arquivo digital de antivírus. Cisco Secure ACS também salva os registros dos resultados desta avaliação de políticas para uso com sistemas de monitoramento. Para *hosts* que não contam com o agente adequado, *Cisco Secure ACS* para Windows torna possível que estas máquinas sejam auditadas por fornecedores de terceiros antes de conceder acesso à rede. Servidores de política externa também tornam possível estender as políticas do *Cisco Secure ACS* (WATKINS; WALLACE, 2008, p. 130).
- Perfis de acesso à rede (NAP): Com o uso de perfis de acesso à rede, os administradores podem classificar solicitações de acesso com base na localização na rede, a participação em um grupo de dispositivos de rede (*Network Device Group*), tipo de protocolo, ou outros valores de atributos RADIUS enviados pelo NAD usado pelo usuário para se conectar. Além disto,

diferentes políticas AAA podem ser mapeadas para perfis específicos (WATKINS; WALLACE, 2008, p. 131).

- Componentes de replicação extendidos: os administradores podem replicar NAPs e todas as configurações relacionadas, incluindo (WATKINS; WALLACE, 2008, p. 131):
    - Configurações de validação de Postura
    - Clientes AAA e hosts
    - Configuração de banco de dados externo
    - Configuração de autenticação global
    - NDGs
    - Dicionários
    - Componentes dos perfis compartilhados
    - Atributos de *logging* adicionais

- Suporte a EAP-FAST: Cisco desenvolveu EAP-FAST como um tipo IEEE 802.1x EAP de fácil acesso ao público para dar suporte a clientes e usuários que não podem impor uma forte política de senha. EAP-FAST é também para aqueles que querem implantar um tipo de EAP 802.1x que tenha as seguintes características (WATKINS; WALLACE, 2008, p. 131):
    - Nenhum certificado digital é necessário
    - Suporte versátil para diferentes tipos de banco de dados de usuário e senha
    - Suporte para mudança e expiração de senha
    - Flexível e fácil de implantar e gerenciar

- Restrições de acesso da máquina (MARs): MARs funciona como uma melhoria da autenticação presente no Microsoft Windows. Os administradores podem usar MARs para controlar autorização de EAP-TLS, EAP-FASTv1a e usuários do Microsoft PEAP que são autenticados com um usuário de banco de dados Microsoft Windows externo. Com esse recurso, se um usuário acessar a rede com um computador que não tenha passado na autenticação (dentro de um período de tempo configurável) recebe as permissões de acesso que foi pré-configurado. É possível configurar isso para limitar a autorização, conforme

necessário, ou você pode optar por negar o acesso à rede (WATKINS; WALLACE, 2008, p. 131).

- NAFs: Filtros de acesso à rede (NAF) que permitem uma maneira fácil e flexível de aplicar restrições de acesso à rede e download de ACLs em nomes de rede de dispositivos, NDGs, ou qualquer outro endereço IP (podendo usar ainda um intervalo de endereços IP e wildcards). Esta funcionalidade permite uma aplicação granular de restrições de acesso à rede (NAR) e download de ACLs (WATKINS; WALLACE, 2008, p. 132).

- IP ACLs aplicadas via *download*: suporte a ACL-por-usuário é estendido a qualquer dispositivo de rede camada 3 (deste que o dispositivo tenha suporte a ACLs via download, como Cisco ASA, *firewalls* Cisco PIX, Soluções VPN Cisco e roteadores Cisco IOS) (WATKINS; WALLACE, 2008, p. 132).
- Protocolos de autenticação: suporte a diversos protocolos de autenticação utilizados pelos suplicantes para efetuar as transações necessárias para o processo de autenticação. Alguns destes protocolos são: ASCII/PAP, CHAP, MS-CHAP, LEAP, EAP-CHAP, EAP TLS, ARAP (ROLAND, 2004, p. 54).

O principal protocolo de autenticação é o EAP (*Extensible Authentication Protocol*), que é um método que concede permissão para a autenticação de um usuário a um servidor específico, a fim de permitir a recepção de dados de outro ponto de acesso. Este servidor trabalhará com o uso do protocolo RADIUS ou TACACS + e tanto pode ser representado pelo ponto de acesso quanto por uma outra máquina dedicada a este fim (PAIM, 2013).

A figura 3 apresenta cada passo da transação de autenticação, ilustrando assim o funcionamento do EAP em conjunto com os protocolos AAA Radius e TACACS+:

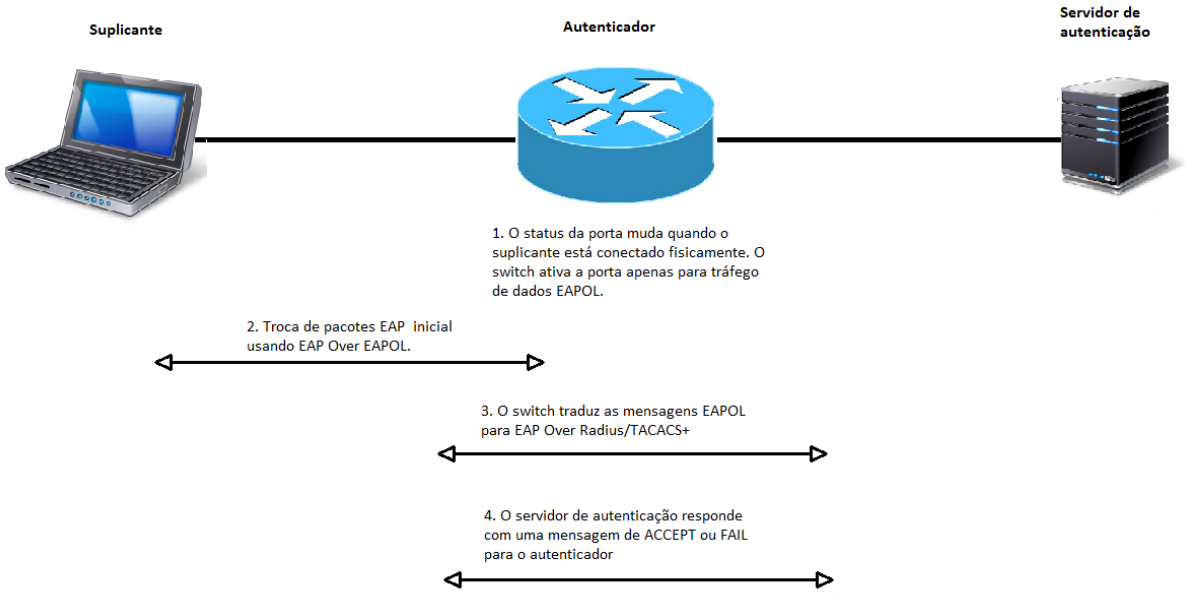


**Figura 4 - Processo de autenticação via EAP**

**Fonte: MALIK, 2003, pg 123**

1. A interface do autenticador alterará o *status* quando o suplicante conecta fisicamente, desta maneira o autenticador habilita a interface para o tráfego EAPOL;
2. O suplicante encaminha o pacote inicial utilizando EAPOL;
3. O autenticador traduz as mensagens EAPOL para EAP Over Radius/TACACS +;
4. O servidor de autenticação responde com uma mensagem de "*ACCEPT*" ou "*FAIL*" para o autenticador.

O EAP permite conversação ilimitada entre o cliente de acesso remoto e o autenticador. A conversação consiste no autenticador solicitando informações de autenticação e nas respostas do cliente de acesso remoto. Por exemplo, quando o EAP é usado com cartões de *token* de segurança, o autenticador pode solicitar separadamente ao cliente de acesso remoto o seu nome, PIN e valor do *token* do cartão. À medida que cada consulta é feita e respondida, o cliente de acesso remoto passa para outro nível de autenticação. Quando todas as perguntas forem respondidas satisfatoriamente, o cliente de acesso remoto será autenticado (TECHNET, 2013).

Este modelo apresenta uma característica muito interessante que é o isolamento do servidor RADIUS: em nenhum momento o suplicante envia uma mensagem diretamente para ele (PAIM, 2013).

Conforme descrito acima a ferramenta Cisco ACS suporta diversas variações do protocolo base EAP. A seguir, um breve comentário sobre as mais utilizadas.

EAP-MD5 é um protocolo baseado no EAP. Este tipo EAP utiliza uma mensagem MD5–*Challenge* para que o servidor de autenticação possa autenticar a mensagem vinda do cliente. Este é muito parecido com a mensagem utilizada no PPP CHAP (*Point-to-Point Protocolo Challenge Handshake Authentication Protocol*), que usa MD5 (*Message Digest 5*) como algoritmo de *hashing* (WATKINS; WALLACE, 2008, p. 236).

O EAP-MD5 permite que o servidor autentique uma solicitação de conexão, verificando o *hash* MD5 de uma senha de usuário. Entretanto, o cliente não efetua nenhuma ação a fim de autenticar o servidor (RFC 2284).

Já o protocolo EAP-TLS (*Transport Layer Security*) exige que o usuário e o servidor de autenticação passem por um processo de autenticação mútua utilizando certificados digitais. Embora este protocolo seja muito forte mais seguro, sua implantação exige e uma infraestrutura de certificados para todos os seus usuários (WATKINS; WALLACE, 2008, p. 238).

O protocolo EAP-TTLS é similar ao EAP-TLS porém o certificado digital é instalado somente no servidor o que permite a autenticação do servidor por parte do cliente e não do cliente por parte do servidor. A autenticação do cliente por parte do servidor faz-se após estabelecer uma sessão TLS utilizando outro método (OFICINA DA NET, 2013).

O protocolo EAP-SPEKE (*Simple Password-authenticated Exponential Key Exchange*) permite ao cliente e servidor compartilhar uma senha secreta o que proporciona um serviço de autenticação mútua sem o uso de certificados de segurança (OFICINA DA NET, 2013).

# 3. IMPLEMENTAÇÃO

## 3.1 A REDE

O experimento a seguir foi realizado com equipamentos reais para simular uma empresa de pequeno porte, onde foram configurados todos os equipamentos, desde *switches*, roteadores e o servidor de autenticação.

Esta empresa possui sua matriz na cidade de São Paulo e outros dois escritórios em Curitiba e em Porto Alegre. Cada localidade está em uma rede diferente e todas as redes estão interligadas por uma WAN que é fornecida por uma Operadora de Telecomunicações.

Foram utilizados roteadores Cisco 2921 e *switches* Cisco 3560. O servidor Cisco ACS foi instalado na localidade de São Paulo por esta possuir o principal Datacenter. A figura 4 mostra a topologia usada:

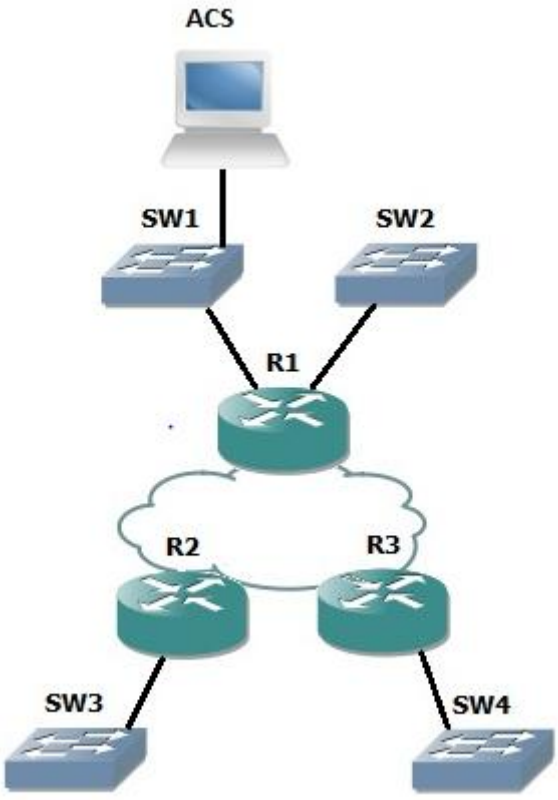


**Figura 5 - Visão geral de uma rede com ACS implementado**

**Fonte: Autoria própria**

O processo de autentição será iniciado ao conectar remotamente à qualquer disposivo de rede, seja este um *switch* ou um roteador. Onde após iniciar a conexão remota, o equipamento de rede irá solicitar as credenciais do usuário e encaminhará para o servidor de autenticação que verificará se estas credenciais são válidas baseado nas políticas configuradas no mesmo.

Desta maneira, o primeiro passo na configuração dos equipamentos será a ativação do serviço de SSH (*Secure Shell*), possibilitando assim o acesso remoto de maneira segura. Neste protocolo os dados da sessão de acesso remoto são criptografados e os dispositivos que participam da sessão são autenticados através da troca de chaves assimétricas. (BARRETT; SILVERMAN, 2001, p. 9)

A autenticação, controle de acesso e a contabilidade serão realizados através do protocolo AAA. Estes serviços serão ativados nos equipamentos de rede, permitindo estes equipamentos participarem do processo de autenticação como autenticadores, encaminhando as solicitações para o servidor de autenticação. A ativação deste serviço é exibida a seguir como o segundo passo na configuração dos equipamentos.

Por fim, há necessidade da configuração do servidor de autenticação onde serão configuradas todas as políticas de acessos para os usuários que iniciarão os acessos remotos.

## 3.2 CONFIGURAÇÃO DOS EQUIPAMENTOS DE REDE

### 3.2.1 CONFIGURAÇÃO DO PROTOCOLO SSH

O gerenciamento dos equipamentos pode ser realizado através dos protocolos TELNET ou SSH. O *Secure Shell* (SSH) é a solução mais segura para gerenciar dispositivos, este criptografa todo o tráfego da interface virtual dos equipamentos. (ODOM; HEALY; DONOHUE, pag 759)

Para realizar a configuração de um servidor SSH nos dispositivos Cisco é necessário realizar os seguintes passos (ODOM; HEALY; DONOHUE, pag 760):

- Configurar o *hostname*;

- Configurar o *domain name*;
- Configurar um *username* e um *password*;
- Gerar um par de chaves RSA (Rivest, Shamir e Adelman);
- Desabilitar Telnet nas interfaces virtuais (VTY);
- Habilitar SSH nas interfaces virtuais.

Estes passos consistem em aplicar os comandos abaixo (TETZ, 2011, p. 249):

```
router(config)# hostname TCC
TCC(config)# ip domain-name TCCSISTEL
TCC(config)# username cisco password sistel
TCC(config)# crypto key generate rsa
TCC(config)# line vty 0 4
TCC(config-line)# transport input none
TCC(config-line)# transport input ssh
```

O resultado do comando pode ser verificado através do comando ***show ip ssh***, o qual apresenta o status do protocolo SSH. O resultado esperado é (CISCO, 2013):

```
Router# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

### 3.2.2 CONFIGURAÇÃO DO PROTOCOLO AAA

O acesso ao ambiente Cisco da empresa é controlado por um protocolo AAA. O protocolo em questão é o TACACS +.

Para realizar a configuração dos equipamentos para atuarem como autenticador dentro do processo de autenticação utilizando o protocolo TACACS + é necessário realizar os seguintes passos (WATKINS; WALLACE, 2008, p. 117):

- Acesso seguro aos equipamentos, conforme descrito no item 3.2

- Habilitar os serviços AAA
- Configurar o serviço de autenticação
- Configurar o serviço de autorização
- Configurar o serviço de contabilidade
- Configurar os servidores TACACS +

Estes passos consistem em aplicar os comandos abaixo (AKIN, 2002, p. 158):

```
TCC(config)# aaa new-model
TCC(config)# aaa authentication login default group tacacs+ local
TCC(config)# aaa authentication login console local
TCC(config)# aaa authentication enable default group tacacs+ enable
TCC(config)# aaa authorization exec default group tacacs+ local
TCC(config)# aaa authorization commands 1 default group tacacs+ local
TCC(config)# aaa authorization commands 15 default group tacacs+ local
TCC(config)# aaa accounting exec default
TCC(config)# action-type start-stop
TCC(config)# group tacacs+
TCC(config)# aaa accounting commands 1 default
TCC(config)# action-type start-stop
TCC(config)# group tacacs+
TCC(config)# aaa accounting commands 15 default
TCC(config)# action-type start-stop
TCC(config)# group tacacs+
TCC(config)# ip tacacs source-interface Loopback1
TCC(config)# tacacs-server host  192.168.1.7
TCC(config)# tacacs-server timeout 2
TCC(config)# tacacs-server key cisco
```

## 3.3 CONFIGURAÇÃO DO SERVIDOR DE AUTENTICAÇÃO

A figura 5 mostra como é a interface gráfica do Cisco ACS; existe um menu no lado esquerdo com várias opções para configuração do sistema, o qual será utilizado como referência na implementação dos itens a seguir:


**Figura 6 - Tela inicial do Cisco ACS**

**Fonte: Autoria própria**

### 3.3.1 Criação dos *Network Device Groups*

O primeiro passo para a configuração do servidor é a criação do grupo de equipamentos. Para este projeto serão configurados dois grupos. O primeiro grupo baseado na localização e o segundo grupo baseado no tipo de equipamento.

Para a criação do primeiro grupo, no menu principal do servidor Cisco ACS seleciona-se *Network Resources -> Network Device Groups -> Location.* Em seguida clica-se em *Create* (conforme mostra a figura 6):

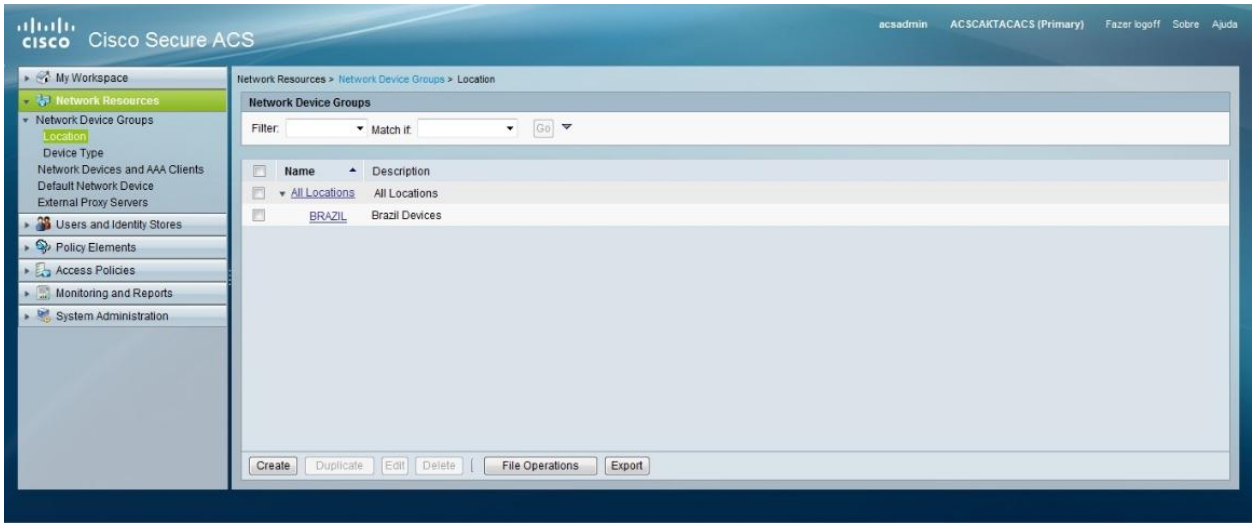


**Figura 7 - Tela de criação dos Network Device Groups (Location)**
**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome do grupo a ser criado;
- *Description*: referente à uma possível descrição para o grupo;
- *Parent*: utilizado para indicar se o grupo é ou não um subgrupo de algum grupo existente.

Na figura 7 tem-se instruções de como criar o primeiro grupo: no menu principal do servidor Cisco ACS seleciona-se *Network Resources -> Network Device Groups -> Device Type*. Em seguida clica-se em *Create*.

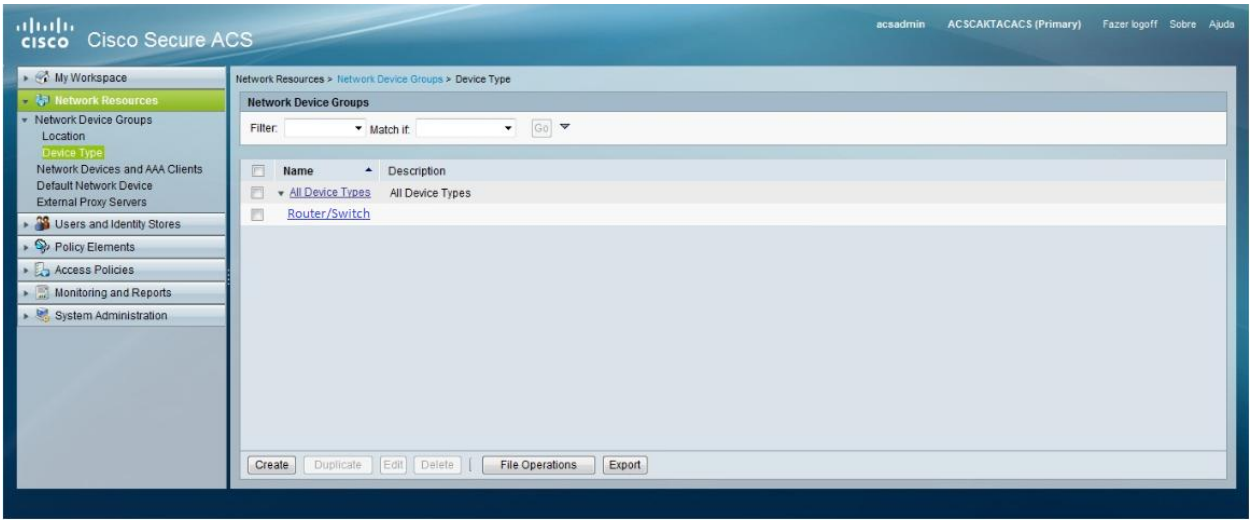


**Figura 8 - Tela de criação dos Network Device Groups (Device Type)**
**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome do grupo a ser criado;
- *Description*: referente à uma possível descrição para o grupo;
- *Parent*: utilizado para indicar se o grupo e ou não um subgrupo de algum grupo existente.

### 3.3.2 Criação dos *Network Device and AAA Clients*

Como parte do processo de autenticação é necessário cadastrar os equipamentos que serão clientes do servidor em questão, ou seja, os equipamentos que atuam como autenticadores no processo de autenticação.

Conforme mostrado na figura 8, no menu principal do servidor Cisco ACS seleciona-se *Network Resources -> Network Device and AAA Clients*. Em seguida clica-se em *Create*.

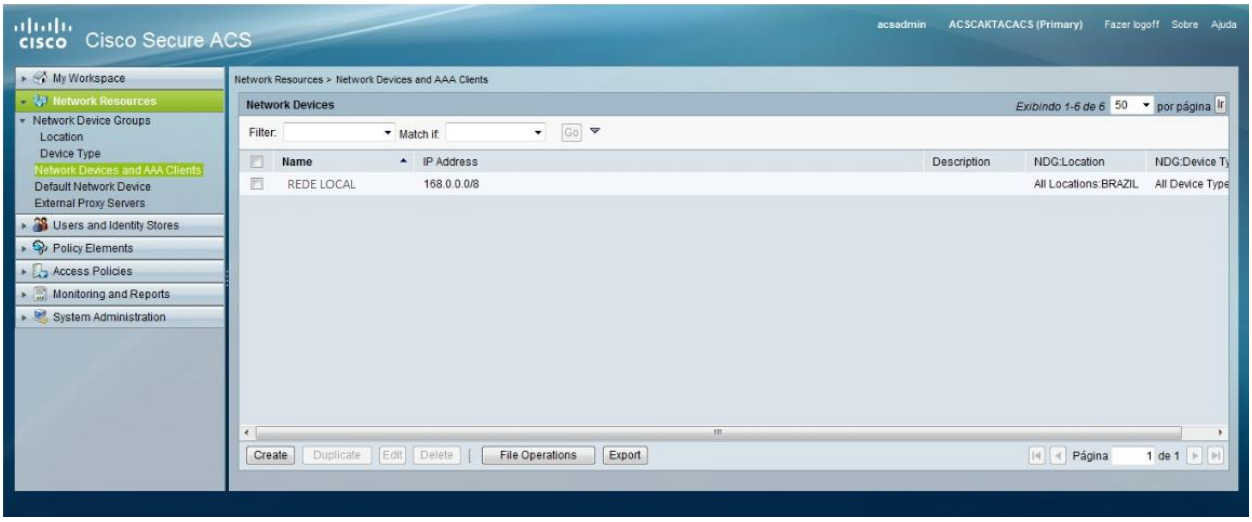


**Figura 9 - Tela de criação dos Network Devices and AAA Clients**

**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome do *device* ou grupo de *devices*;
- *Description*: referente à uma possível descrição;
- *Network Device Groups*: utilizado para indicar quais grupos estes equipamentos pertencem;
- IP *Address*: referente ao endereço IP do equipamento cadastrado. Neste campo é possível indicar uma rede englobando diversos endereços IP;
- *Authentication Options*: indicar qual protocolo será utilizado e a respectiva senha para autenticar os equipamentos dos clientes e o servidor. Esta senha deve ser a mesma no servidor e nos equipamentos.

### 3.3.3 Criação dos *Identity Groups*

Outro grupo necessário para a solução é o grupo de usuários. Este grupo pode ser criado acessando no menu principal do servidor Cisco ACS o *User and Identity Stores -> Identity Groups*. Em seguida clica-se em *Create* (conforme figura 9):

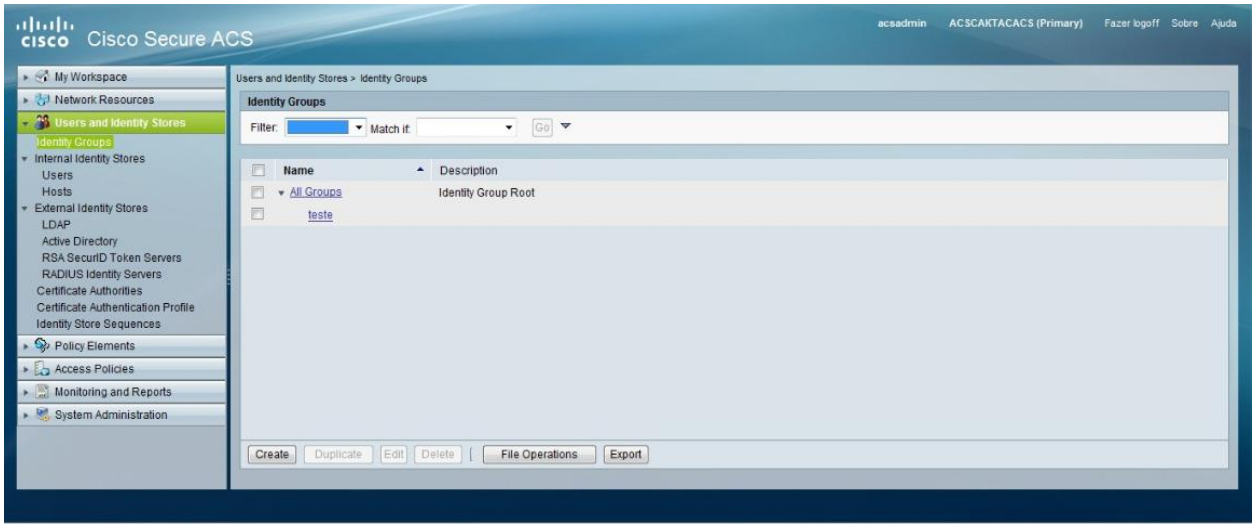


**Figura 10 - Tela de criação dos Identity Groups**

**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome do grupo a ser criado;
- *Description*: referente à uma possível descrição para o grupo;
- *Parent*: utilizado para indicar se o grupo e ou não um subgrupo de algum grupo existente.

### 3.3.4 Criação dos *Users*

Os usuários devem ser criados neste momento da configuração. Estes serão os usuários que terão permissão de acessar os equipamentos clientes AAA.

Para criar os *users,* conforme a figura 10, seleciona-se *User and Identity Stores -> Internal Identity Stores -> Users*. Em seguida clica-se em *Create*.

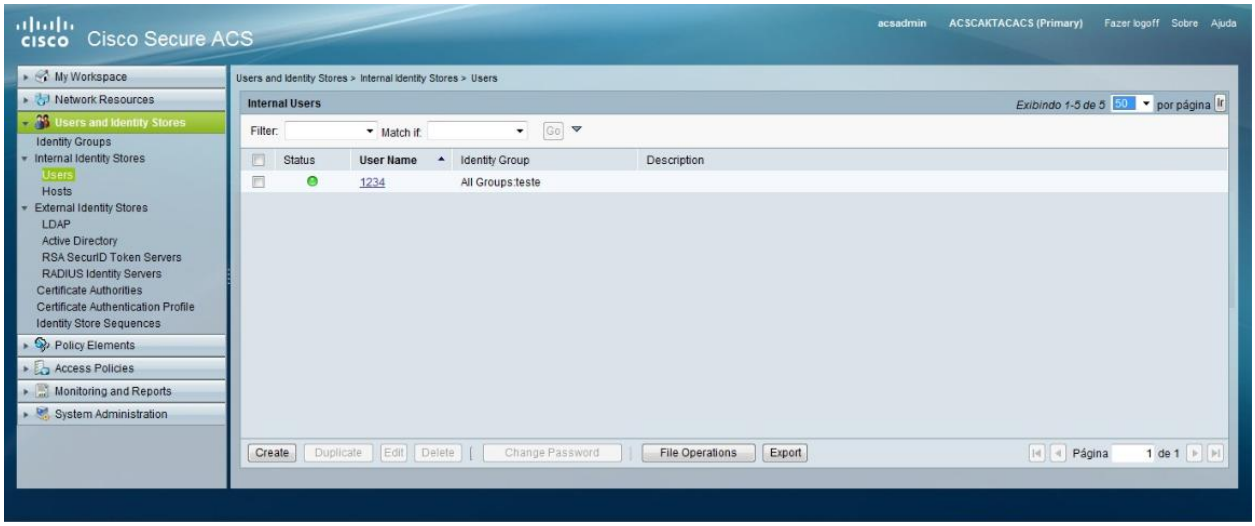


**Figura 11 - Tela de criação dos Users**

**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *User Name*: referente ao nome do usuário;
- *Description*: referente à uma possível descrição;
- *Identity Group*: utilizado para indicar qual grupo este usuário pertence;
- *Password Type*: indicar o tipo de senha que o usuário ira utilizar;
- *Password*: indicar a senha de acesso a ser utilizada pelo usuário;
- *Confirm Password*: confirmar a *Password;*
- *Enable Password*: indicar a senha para acesso ao nível privilegiado dos equipamentos;
- *Confirm Password*: confirmar a *Enable Password.*

### 3.3.5 Criação das Identity Store Sequences

Esta configuração é necessária para indicar ao servidor aonde e qual a sequência serão consultadas as informações dos usuários. Também é utilizado para indicar se a autenticação será baseada em certificados digitais ou *password*.

No menu principal do servidor Cisco ACS seleciona-se *User and Identity Stores -> Identity Store Sequences*. Em seguida clica-se em *Create*, conforme a figura 11:

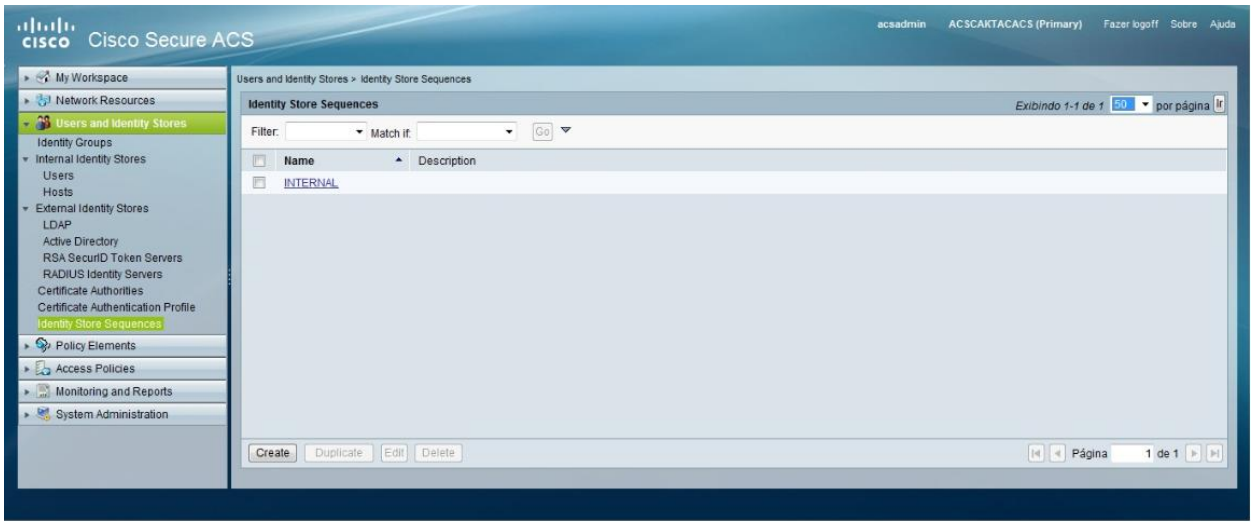


**Figura 12 - Tela de criação dos Identity Store Sequences**
**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome da *Identity Store Sequences*;
- *Description*: referente à uma possível descrição;
- *Authentication Method List*: referente ao tipo de autenticação (por certificado digital ou senha);
- *Additional Attribute Retrieval Search List*: indicar qual lista de usuários será utilizada.

### 3.3.6 Criação do *Shell Profile*

O *Shell Profile* é utilizado para fornecer atributos customizados no processo de autenticação, como por exemplo a necessidade de alguma variável adicional para algum serviço específico.

Na figura 12 é mostrado como criar os *Shell Profiles*. No menu principal do servidor Cisco ACS seleciona-se *Policy Elements -> Autorization and Permissions -> Device Administration -> Shell Profiles*. Em seguida clica-se em *Create*.

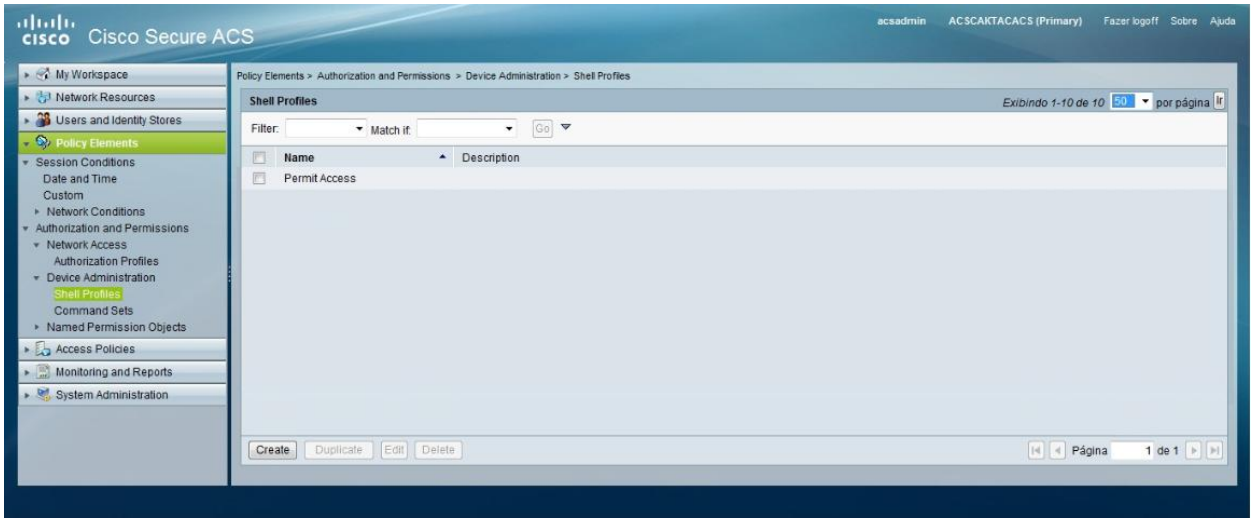


**Figura 13 - Tela de criação do Shell Profile**

**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome do Shell Profile;
- *Description*: referente à uma possível descrição;
- *Custom Attributes*: utilizados para definir atributos customizados para a autenticação.

### 3.3.7 Criação dos *Command Sets*

Neste item de configuração é indicado quais comandos podem ser executados nos dispositivos que estão utilizando o serviço de TACACS + para autenticação, autorização e contabilidade.

No menu principal do servidor Cisco ACS seleciona-se *Policy Elements -> Autorization and Permissions -> Device Administration -> Command Sets*. Em seguida clica-se em *Create* (conforme mostra a figura 13):

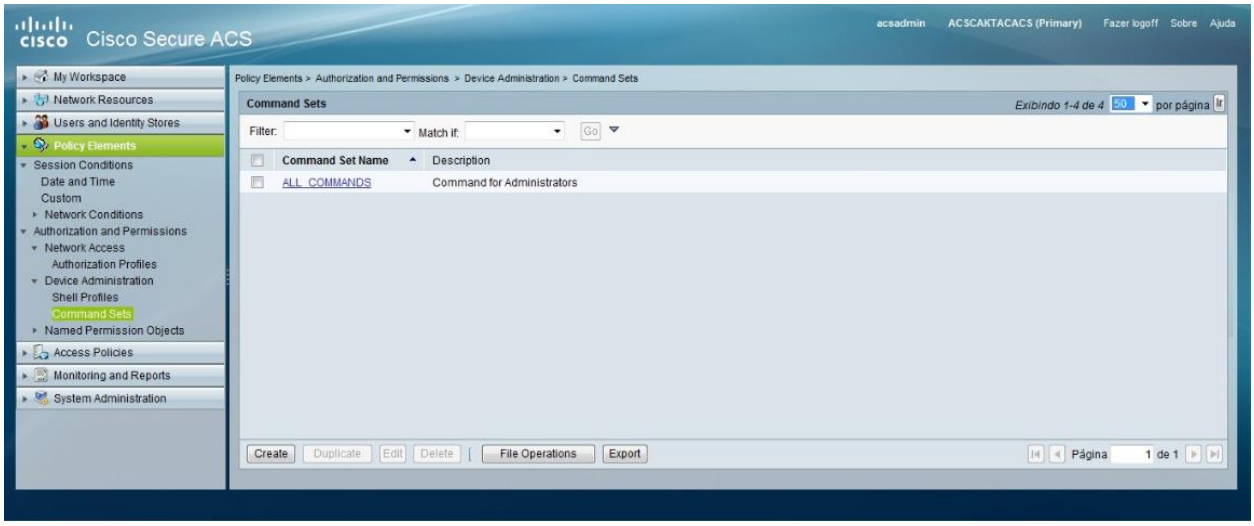


**Figura 14 - Tela de criação dos Command Sets**

**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome do *Command Set*;
- *Description*: referente à uma possível descrição;
- *Command*: utilizados para definir os comandos autorizados.

### 3.3.8 Criação dos *Access Services*

O *Access Service* é uma regra que direciona a política baseada pelo protocolo AAA.

No menu principal do servidor Cisco ACS seleciona-se *Access Policies -> Access Services-> Service Selection Rules*. Em seguida clica-se em *Create*. A figura 14 mostra a tela onde são criados os *Access Services:*

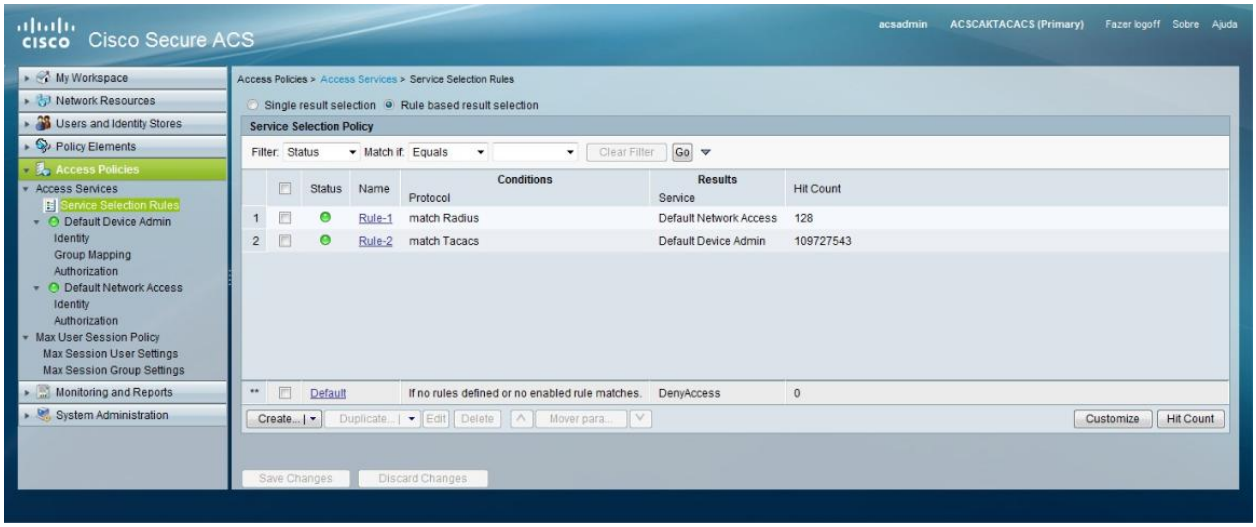


**Figura 15 - Tela de criação dos Access Services**

**Fonte: Autoria própria**

As seguintes informações serão solicitadas:

- *Name*: referente ao nome do *Access Services*;
- *Status*: referente ao status (ativo ou inativo);
- *Protocol*: selecionar qual protocolo AAA será direcionado para a política;
- *Service*: selecionar qual política será aplicada ao protocolo selecionado.

### 3.3.9 Criação da *Identity*

O *Identity* é necessário para indicar em qual base de usuários o ACS irá fazer a busca pelo usuário que poder dar uma resposta no processo de autenticação e quais as ações que deverão ser tomadas quando o processo de autenticação falhar.

No menu principal do servidor Cisco ACS seleciona-se *Access Policies -> Default Device Admin-> Identity*.

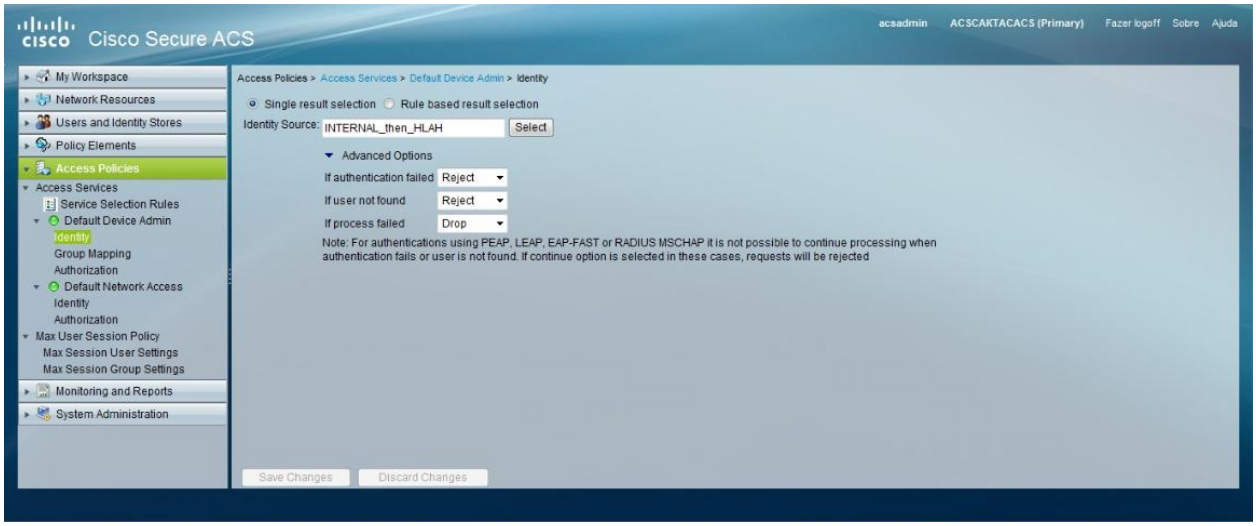


**Figura 16 - Tela de criação da Identity**

**Fonte: Autoria própria**

As seguintes informações serão solicitadas, conforme mostrado na figura 15:

- *Indentity Source*: referente a qual base de dados serão pesquisadas o usuário;
- *Advanced Options*: referente às ações que o ACS irá tomar para cada tipo de falha. As opções disponíveis são *Reject* e *Drop*. A diferença entre as opções é que o *Reject* informa ao usuário que a operação falhou. Na opção *Drop* o usuário não recebe nenhum retorno.

### 3.3.10 CRIAÇÃO DE *AUTHENTICATION*

Esta é a última etapa da configuração do servidor Cisco ACS. Através deste passo ligam-se todos os elementos criados nas etapas anteriores para criar a política de acesso.

No menu principal do servidor Cisco ACS seleciona-se *Access Policies -> Default Device Admin-> Authentication*.

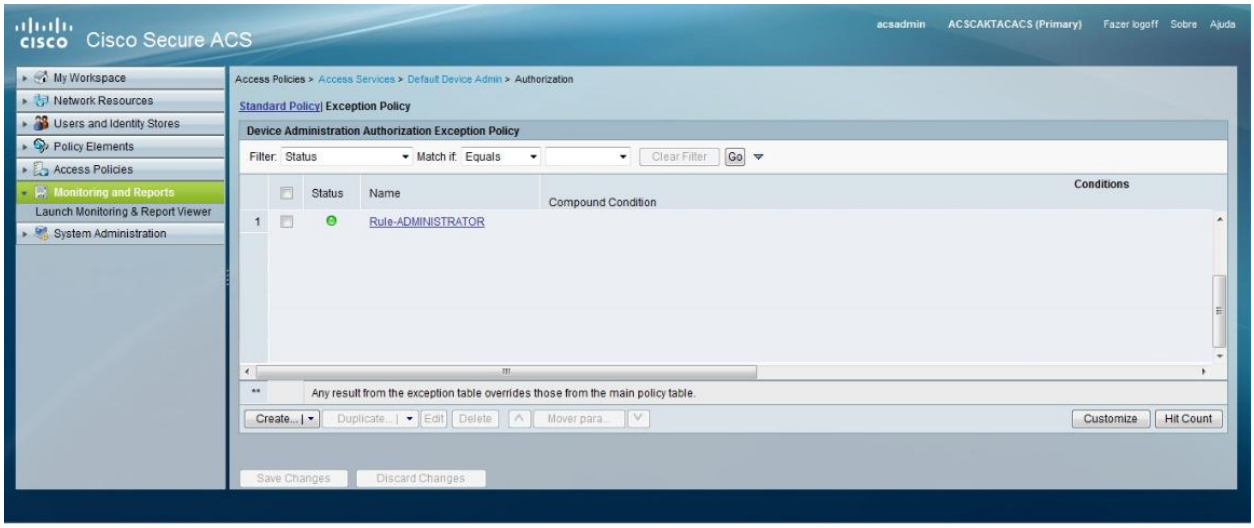


**Figura 17 - Tela de criação da Authentication**

**Fonte: Autoria própria**

A figura 16 mostra as informações que serão solicitadas:

- *Name*: referente ao nome da política;
- *Status*: referente ao *status* (ativo ou inativo);
- NDG:*Device Type*: selecionar em qual grupo de equipamentos será aplicada está política;
- NDG:*Location*: selecionar em qual grupo de equipamentos será aplicada esta política;
- *Identity Grupo*: selecionar em qual grupo de usuários será aplicada esta política;
- *Device* IP *Address*: selecionar em quais equipamentos serão aplicados esta política;
- Protocolo: selecionar para qual protocolo será aplicada esta política;
- *Shell Profile*: selecionar qual será o resultado do processo de autenticação, caso o usuário tenha sucesso no processo de autenticação;
- *Command Sets*: selecionar quais os comandos podem ser executados nos equipamentos.

## 3.4 TESTES

Os testes realizados na estrutura de rede podem ser observados através das *logs* do servidor de autenticação o qual recebe todas as solicitações de autenticação da rede e define se o processo de autenticação é válido ou não de acorod com as políticas configuradas.

No menu principal do servidor Cisco ACS deverá ser selecionado *Monitoring and Reports -> Launch Monitoring & Report Viewer.* Será exibida uma nova janela. Nesta nova janela deverá ser selecionado *Reports -> Catalog -> AAA Protocol*. Nesta opção é possível visualizar diversos tipos de *reports*. Para checar os testes realizados com autenticação dos usuários deverá ser clicado em TACACS *Authentication*.

Na figura 17 tem-se um exemplo de *log,* onde pode-se observar tanto as autenticações que foram realizadas com sucesso, apresentadas em verde, quanto os processos que foram negados pelo servidor, apresentados em vermelho.

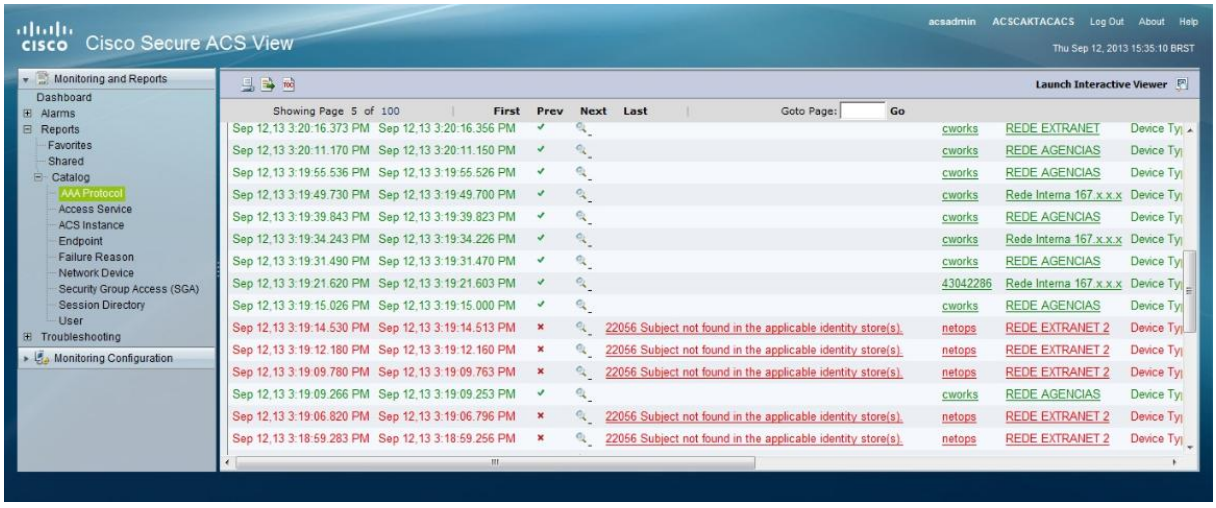


**Figura 17 - Logs de Autenticação**

**Fonte: Autoria própria**

Neste exemplo pode-se observar diversos exemplos de autenticação, onde cada linha representa uma requisição de autenticação ao servidor. Para obter detalhes sobre cada processo individualmente, pode-se clicar na lupa referente a linha que deseja obter mais detalhes.

Na figura 18 tem-se um exemplo dos detalhes de uma transação que foi realizada com sucesso:

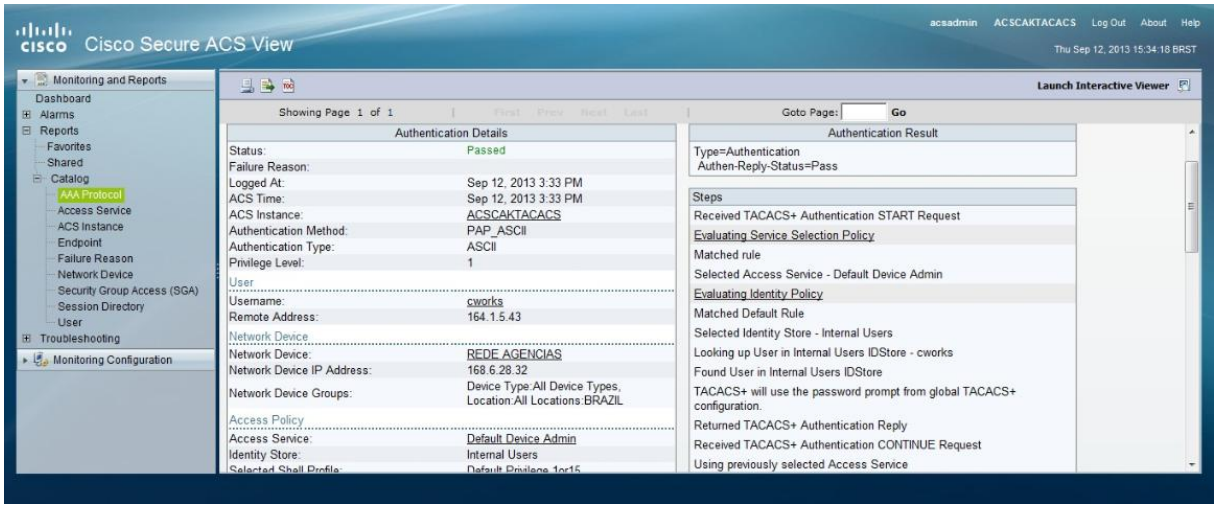


**Figura 18 - Detalhes de Autenticação com Sucesso**

**Fonte: Autoria própria**

E na figura 19 é mostrado outro exemplo dos detalhes de uma transação que foi realizada sem sucesso:

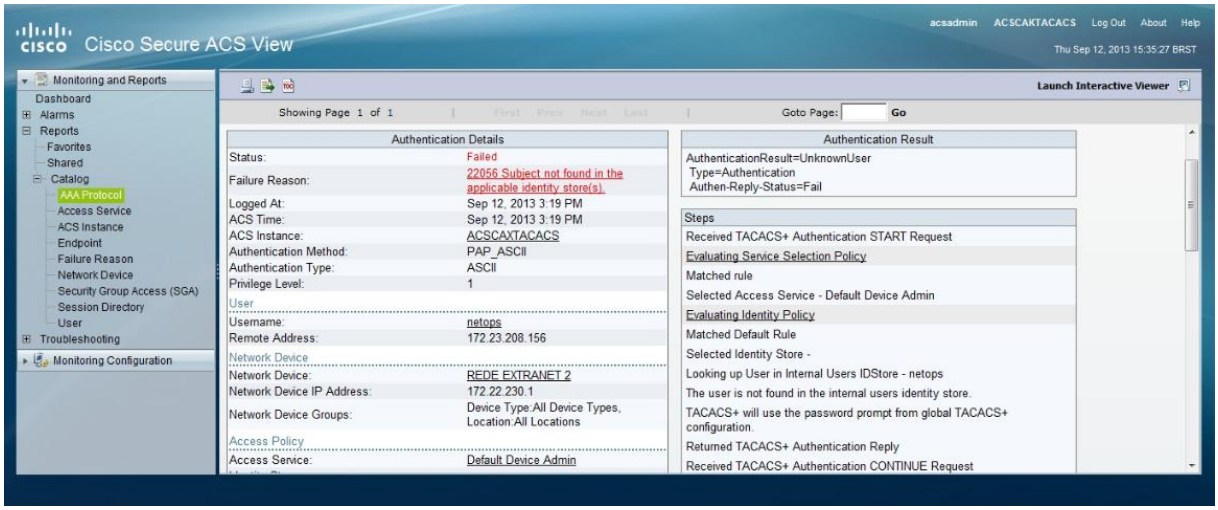


**Figura 19 - Detalhes de Autenticação sem Sucesso**

**Fonte: Autoria própria**

Dentre diversas informações é possível observar o motivo da falha do processo de autenticação (*Failure Reason)*. Neste caso, a autenticação não foi autorizada pois o usuário não foi encontrado na base de dados dos usuários. Para corrigir e permitir o acesso deste usuário, o mesmo deveria ser criado dentro da

*Internal Identity Stores.* Este processo este exemplificado no item 3.3.4 deste documento.

# CONCLUSÃO

Atualmente o principal problema das redes é a segurança, devido a diversas formas de vulnerabilidades encontradas. A utilização do TACACS+ provê autenticação, autorização e contabilidade fornecendo aos engenheiros de rede um nível a mais de proteção para suas redes. Isto permite que os acessos tenham controle, impedindo acessos indevidos. Isto é feito através da pesquisa em banco de dados de usuários e na aplicação de políticas para controle de acesso.

Em certos casos há a possibilidade de existir credenciais comprometidas, as quais podem ser desabilitadas assim que forem comprometidas. Em casos onde as credenciais comprometidas foram utilizadas, a contabilidade pode ser utilizada para rastrear as ações realizadas com estas credenciais.

Com o número de trabalhadores remoto aumentando diariamente, TACACS+ pode definitivamente administrar contas de usuários de uma maneira mais eficiente e segura.

A segurança da rede e dos dados contidos no servidor de autenticação está diretamente relacionada à segurança do servidor propriamente dito. Caso algum atacante comprometa o servidor de autenticação, este atacante terá acesso ao banco de dados com os dados de todos os usuários e as políticas existentes no servidor. Para minimizar este risco, nenhuma outra aplicação deve estar habilitada no servidor. Desta maneira, algum atacante não tem possibilidades de comprometer por alguma vulnerabilidade em outras aplicações.

# REFERÊNCIAS

_____. **RFC 2138**: remote authentication dial in user service (RADIUS). Livingston, 1997.

_____. **RFC 2139**: RADIUS Accounting. Livingston, 1997.

_____. **RFC 2284**: PPP Extensible Authentication Protocol (EAP). Livingston, 1998.

AKIN, Thomas. **Hardening Cisco Routers.** Sebastopol, O'Reilly, 2002.

BARRET, Daniel; SILVERMAN, Richard, **SSH, the Secure Shell: The Definitive Guide.** Sebastopol, O'Reilly, 2001.

CISCO, **Cisco IOS Security Command Reference, Release 12.2.** Disponível em <http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfssh.html #wp1023782>. Acesso em: 16.out. 2013

CONVERY, Sean, **Protocols, Applications, and the Future of AAA**. Disponível em: <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-2/102_aaa-part2.html>. Acesso em 15 out. 2013.

DEVERIYA, Anand. **Network Administrators Survival Guide.** Indianapolis, Cisco Press, 2006.

HOOPER, Howard. **CCNP Security VPN 642-648 Official Cert Guide**. Indianapolis, Cisco Press, 2012.

MALIK, Saadat. **Network Security Principles and Practices.** Indianapolis, Cisco Press, 2003.

METROBYTE, **Segurança de rede.** Disponível em: <http://www.metrobyte.com.br/servicos-de-ti/seguranca-de-rede/>. Acesso em 29 jul. 2013.

ODOM, Wendell; HEALY, Rus; DONOHUE, Denise. **CCIE Routing and Switching Certification Guide.** Indianapolis, Cisco Press, 2010.

OFICINA DA NET, **Segurança em Redes Sem Fio**. Disponível em <www.oficinadanet.com.br/artigo/1756/seguranca_em_redes_sem_fio>. Acesso em: 16 out. 2013

PAIM, Rodrigo R. **WEP, WPA e EAP.** Disponível em <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/index.html>. Acesso em: 16 out. 2013.

RILEY, Charles. **The Best Damn Cisco Internetworking Book Period.** Rockland, Syngress, 2003.

ROLAND, John. **CCSP Self-Study: Securing Cisco IOS Networks.** Indianapolis, Cisco Press, 2004.

TECHNET, **Visão geral do EAP.** Disponível em <http://technet.microsoft.com/pt-br/library/cc770622.aspx>. Acesso em: 16 out. 2013.

SALOMON, Marcos Vinicius Pinto. **Fraude no mundo IP e redes de nova geração celular.** Disponível em: <http://www.teleco.com.br/tutoriais/tutorialfraudeip/>. Acesso em 25 jul. 2013.

LEVY, Eduardo. **Os principais desafios do setor de telecom no Brasil.** Disponível em: <http://www.teleco.com.br/emdebate/elevy01.asp>. Acesso em 25 jul. 2013.

TELETIME, **Segurança para redes M2M será fundamental, diz ABI.** Disponível em: <http://www.teletime.com.br/25/10/2012/seguranca-para-redes-m2m-sera-fundamental-diz-abi/tt/307861/news.aspx>. Acesso em 25 jul. 2013.

TETZ, Edward. **Cisco Networking All-in-One for Dummies.** Indianapolis, John Wiley & Sons, 2011.

WATKINS, Michael; WALLACE, Kevin. **CCNA Security Official Exam Certification Guide.** Indianapolis, Cisco Press, 2008.