FACULDADE – IDEZ
PÓS-GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

IMPACTO DA UTILIZAÇÃO DE CERTIFICADOS DIGITAIS EM SERVIDORES DE REDE : UM ESTUDO COMPARATIVO

JOÃO PESSOA PB
2009

FLÁVIO PEREIRA DA SILVA

IMPACTO DA UTILIZAÇÃO DE CERTIFICADOS DIGITAIS EM SERVIDORES DE REDE UM ESTUDO COMPARATIVO

Trabalho de Conclusão de Curso de Pós Graduação em segurança da Informação da faculdade IDEZ, como parte dos requisitos à obtenção do título de Pós-graduação em Segurança da Informação, orientado pelo professor Marcio Luiz Machado Nogueira.

JOÃO PESSOA PB

2009

IMPACTO DA UTILIZAÇÃO DE CERTIFICADOS DIGITAIS EM SERVIDORES DE REDE UM ESTUDO COMPARATIVO

DissertaçãoMonografia submetida ao corpo docente da Faculdade IDEZ, como parte dos requisitos necessários à obtenção do grau de especialista em Segurança da Informação.

Monografia aprovada em ____/____/____ para obtenção do título de Bacharel em Sistemas de Informação.

Banca Examinadora:

_____

Prof Márcio Nogueira

_____

Prof Marileuza Fernandes

_____

Prof Gerson Castro

JOÃO PESSOA PB

2009

JOÃO PESSOA PB

2009

AGRADECIMENTOS

Agradecemos ao professor Marcio Luiz Machado Nogueira, por sua orientação, que foi muito útil para o desenvolvimento deste trabalho.

À professora Marileuza, por sua importante revisão metodológica.

Aos professores e coordenadores do curso, que em muito contribuíram para nossa formação acadêmica.

Aos amigos acadêmicos, que ao longo de quatro anos, mostraram união, companheirismo e, principalmente, amizade uns com os outros.

A todos, que de alguma forma, contribuíram para a concretização deste objetivo.

JOÃO PESSOA PB

2009

RESUMO

Este trabalho tem por objetivo apresentar os conceitos envolvidos em Certificação Digital e operacionalização das ICPs (Infra estrutura de Chaves Públicas). O mesmo apresenta os conceitos envolvidos e descreve os passos para o planejamento e execução de uma infra-estrutura necessária a utilização de serviços com Certificação Digital. Utilizando a metodologia de experimentação é proposto um ambiente de testes, com utilização de Certificação Digital a fim de conferir autenticação e criptografia de dados e outro sem esses recursos. Nesse ambiente são realizados testes e feitas à coleta de resultados. Os testes visam mostrar fatores como desempenho, custo operacional, impacto no processo de autenticação. Por fim o trabalho é concluído traçando-se considerações sobre o uso de Certificação Digital e criptografia em redes corporativas buscando responder a seguinte questão: Qual o impacto na utilização de Certificação Digital, para conferir autenticação e criptografia de dados em redes de computadores locais?

Palavra chave: Criptografia. Assinatura Digital. Certificado Digital. EAP. TLS.

ABSTRACT

This paper aims to present the concepts involved in certification and operation of Digital ICPs (public key infrastructure). It presents the concepts involved and describes the steps for planning and implementing an infrastructure needed to use services with Digital Certification. Using the methodology of experimentation is proposed a test environment, the use of Digital Certificate in order to provide authentication and encryption of data and one without these features. In this environment are tested and made to collect the results. The tests aim to show factors such as performance, operational cost, impact on the authentication process. Finally the work is done by drawing up concerns about the use of digital certification and encryption in enterprise networks seeking to answer following question: What is the impact on the use of digital certification, to provide authentication and encryption of data on local networks of computers?

Keyword: Encryption. Digital Signature. Digital Certificate. EAP. TLS.

LISTAS DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AC - Autoridade Certificadora
AR - Autoridade de Registro
CHAP - Protocolo de autenticação de handshake de desafio
DES - Data Encryption Standard
DSS - Digital Signature Standard
EAP - protocolo de autenticação extensível
ICMP - Internet Control Message Protocol
ICP - infra-estruturas de chaves públicas
ITI - Instituto Nacional de Tecnologia da Informação
IP - Internet Protocol
MD-5 - Message Digest 5
PAP - Protocolo de autenticação de senha
PEAP - Protocolo de Autenticação Extensível Protegido
RSA - Rivest Shamir Adleman
SHA-1 - Secure Hash Algorithm 1
TCP - Transmission Control Protocol
TLS - Transport Layer Security
TCP/IP - Transmission Control Protocol / Internet Protocol
UDP - User Datagram Protocol
VM - Máquina virtual
X.509 - Padrão de Certificado Digital
ISAKMP - Internet Security Association e Key Management Protocol
3DES -Triple Data Encryption Standard

Sumário

1. INTRODUÇÃO

Segundo Monteiro (2002), as principais funções de segurança são: a autenticidade que verifica se a entidade com quem está se trocando informações sigilosas é realmente quem deveria ser; a confidencialidade que é a capacidade de limitar o acesso à informação apenas às entidades (pessoas, processos, máquinas) autorizadas; a integridade, assegurando que os dados não serão alterados durante uma transmissão; a disponibilidade mantém os recursos disponíveis; o não–repúdio que impede a uma entidade (computador, pessoa) envolvida em uma transação negue a sua participação no evento. Finalmente temos o controle de acesso que limita o acesso e a utilização de recursos apenas a pessoas autorizadas. (Monteiro, 2002)

Já na visão apresentada por Stalling (2008), a necessidade de aumentar a segurança dos serviços e o sigilo dos documentos que estão armazenados em servidores, fez da infra-estrutura de segurança da informação e em particular da criptografia com utilização de entidadesdades certificadoras, uma solução para atender esses requisitos de segurança citados no parágrafo anterior. Em uma Infra Estrutura De Chaves Públicas (ICP) o objeto central é o certificado digital. Ele é emitido por uma entidade confiável chamada de Autoridade Certificadora (C A) e seu conteúdo declara uma associ¬ação entre uma chave digital e um conjunto de informações que podem ser de identifica-ção de uma entidade como um indivíduo, por exemplo.

Em notícia publicada pelo governo federal podemos ler:

> Até o fim de 2009, metade das universidades federais do País deve disponibilizar para alunos, professores e demais servidores a Certificação Digital. Em solenidade realizada quinta-feira (13), foi lançada, em Brasília (DF), a chave pública da autoridade certificadora (AC) raiz da infra-estrutura de chaves públicas para a área de ensino e pesquisa (ICPEDU)". Certsign (2009).

Em outra notícia publicada pelo ITI (Instituto Nacional de Tecnologia da Informação) podemos ler:

> "O Instituto Nacional de Tecnologia da Informação (ITI) está em negociação com desenvolvedores dos navegadores de internet Firefox, Opera, Safari e Internet Explorer para incluir nesses programas os certificados da ICP-Brasi (Infra-Estrutura de Chaves Públicas Brasileira)". Infowester (2009).

A utilização de Certificação Digital por instituições de ensino e órgãos do governo vem crescendo conforme reportagens recentes. Diante desse panorama de segurança esse trabalho acadêmico vem de encontro à necessidade de compreensão do mecanismo de implantação dos requisitos de segurança se valendo da utilização de infra-estrutura de chaves publicas. Visando apresentar meios para tornar o tráfego de dados em redes locais mais seguros a criptografia fornece técnicas que permitem a codificação e decodificação dos dados, conferindo autenticação de usuário e criptografia de dados. Mas qual o impacto na utilização de Certificação Digital, para conferir autenticação e criptografia de dados em redes de computadores locais? Para tentar responder essa questão usaremos o experimento para estudar e compreender melhor o processo envolvido na utilização de certificados digitais.

1.1 OBJETIVOS

O principal objetivo deste trabalho monográfico é estudar o impacto causado na utilização de infra-estruturas de chaves públicas (ICPs) e mostrar a viabilidade de seu uso em um ambiente experimental no qual aplicativos que façam uso da Certificação Digital possam ser testados. Dessa forma esse trabalho monográfico tenta contribuir com estudos que possibilitem o entendimento e utilização de uma entidade certificadora para redes corporativas. Pretende-se também ao longo do trabalho experimental estudar o impacto na utilização de Certificação Digital, para conferir autenticação e criptografia de dados em uma rede LAN (*Local Area Networking*) corporativa.

1.2 JUSTIFICATIVA

A principal justificativa deste trabalho monográfico é fornecer material que contribua ao meio acadêmico, bem como ao meio corporativo, com informações relevantes sobre a utilização de infra-estruturas de chaves públicas (ICPs). O mesmo pretende levantar informações que revelem o impacto causado na utilização certificados digitais bem como a viabilidade de seu uso em redes locais. Desta forma o presente trabalho monográfico pretende fornecer a comunidade acadêmica e a quem necessitar informações relevantes que poderão contribuir para tomadas de decisão quando na utilização de aplicativos que façam uso da Certificação Digital.

2 METODOLOGIA

Por definição, experimentação é um método de pesquisa onde se manipulam uma ou mais variáveis independentes e posteriormente, analisam-se as conseqüências dessa manipulação; normalmente, os sujeitos de pesquisa são designados aleatoriamente a grupos chamados “experimentais”, conforme a afirmação de Kerlinger (1990).

Desta forma, este trabalho foi desenvolvido, visando apresentar meios para tornar o tráfego de dados em redes locais mais seguros, avaliando o impacto na rede quando da utilização de criptografia com uso de certificados digitais para conferir acesso, através de um servidor de domínio. Para esse fim foi desenvolvido um ambiente de testes com objetivo de verificação do impacto resultante da utilização de criptografia e autenticação utilizando certificados digitais em uma rede corporativa.

O método utilizado para o desenvolvimento desta pesquisa foi o experimental, tendo como objetivo descrever o tema, partindo dos conceitos básicos de Certificação Digital e os protocolos de autenticação mais usados, passando por construção do cenário de testes e avaliação dos resultados obtidos.

O plano de trabalho seguiu os tópicos abaixo: Introdução e metodologia, revisão de conceitos sobre Certificação Digital partindo dos conceitos iniciais até os mais específicos e desenvolvimento de um ambiente experimental de testes detalhado conforme mostrado na figura 1 a seguir.

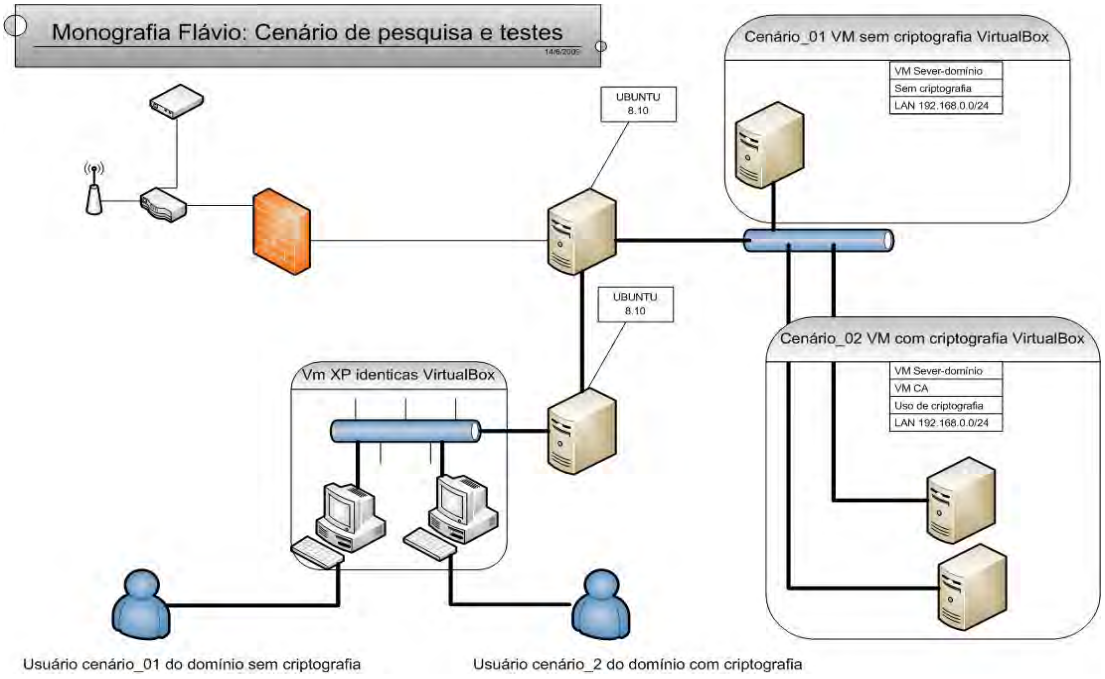


Figura 1 CENÁRIO DE TESTES

Conforme pode ser visualizado na figura acima no cenário foi usado como infra-estrutura para suportar as máquinas virtuais (VM´s) o linux Ubuntu.

Nesse cenário iremos medir o tempo gasto na configuração dos servidores com e sem a utilização de certificados, bem como o desempenho da rede, o tempo médio gasto com configuração dos serviços e principalmente a usabilidade por parte dos usuários.

No próximo capítulo iremos tratar do embasamento teórico começando pelo entendimento da Certificação Digital, Assinatura Digital, Infra Estrutura De Chaves Públicas bem como o processo de autenticação e os principais protocolos usados.

3 CERTIFICAÇÃO DIGITAL

Um certificado digital ou identidade é um arquivo digital que, como os demais documentos tradicionais de identificação, além dos dados do indivíduo ou entidade, possuem uma chave pública do assinante. (Emiliano, 2007). Estes documentos eletrônicos são chancelados digitalmente pela entidade emissora, conhecida com autoridade certificadora, com o objetivo de interligar a chave pública a uma pessoa ou entidade, possuindo o mesmo valor do documento físico, como carteira de identidade, cartões de crédito, passaportes, que ao serem apresentados servem como prova de identificação, servindo também como mecanismo de divulgação da chave publica. (Stallings, 2008).

3.1 ASSINATURA DIGITAL

Uma Assinatura Digital é um algoritmo de autenticação, que possibilita ao criador de um objeto unir ao objeto criado, um código que irá agir como uma assinatura. Stallings (2008, p 272) afirma que: “a assinatura garante a origem e a integridade da mensagem”.

Já a função resumo recebe como entrada uma mensagem de qualquer tamanho e produz um resumo de tamanho fixo, que representa o conteúdo da mensagem. (Emiliano, 2007).

O resumo criptográfico é o resultado retornado por uma função de hash. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

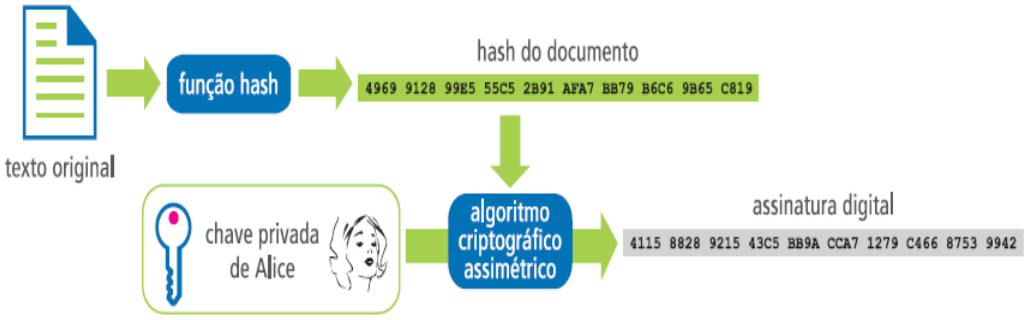


Figura 2 ASSINATURA DIGITAL USANDO ALGORITMO DE CHAVE PÚBLICA. FONTE: (ITI BRASIL, 2009).

A função de hash é uma função que recebe uma mensagem como um conjunto de bits de qualquer tamanho e a relaciona a um valor de tamanho fixo. A utilização de resumos criptográficos ao processo de ciframento reduz o tempo de operação para gerar uma assinatura por serem os resumos, em geral, muito menores que os documentos em si. Consumindo assim um tempo menor, independente do tamanho do documento a ser assinado. A grande vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, uma vez que os algoritmos de criptografia assimétrica são lentos. Na Assinatura Digital, o documento não sofre qualquer alteração e o hash cifrado com a chave privada é anexado ao documento. (Willian, 2008).

Assinaturas digitais não garantem a confidencialidade da mensagem. Porém elas podem ser combinadas com criptografia para garantir a confidencialidade, a integridade e a autenticidade de mensagens. Algoritmos comuns de Assinatura Digital são o RSA e o DSS (*Digital Signature Standard*). (RNP, 2007).

Tomando como referência uma rede TCP/IP. Caso (A) queira enviar uma mensagem assinada para (B), os seguintes passos são necessários:

(A) cria um par de chaves.

(A) distribui sua chave pública para (B).

(A) escreve uma mensagem para (B) e usa a mensagem como entrada para uma função Hash.

(A) cifra o resultado com uma chave privada, resultando na Assinatura Digital.

(A) envia o resultado para (B), que separa a assinatura da mensagem original.

(B) utiliza a chave pública de (A) para decifrar a assinatura.

(B) calcula o hash da mensagem original, utilizando a mesma função usada por (A).

Em sendo os dois hash iguais, a mensagem foi enviada por uma pessoa com a chave privada de (A) e não foi modificada na transmissão. Mas para que isso funcione de forma eficiente é necessário uma Infra-Estrutura De Chaves Públicas.

3.2 INFRA-ESTRUTURAS DE CHAVES PÚBLICAS (ICP)

As aplicações que se utilizam da ICP conseguem asseguras os cinco requisitos de segurança: autenticação, integridade, confidencialidade, não repúdio e autorização, fazendo uso de um sistema de certificados e chaves em conjunto com diversos algoritmos.

A natureza das aplicações abrangidas e a cobertura da ICP variam de acordo com os tipos de Autoridade Certificadora (AC), tornando-se o ponto mais crítico do processo de certificação. A Infra-Estrutura De Chaves Públicas (ICP) é uma série de padrões envolvendo componentes, tais como autoridades certificadoras (AC), autoridades de registro (AR), Diretório Público, estrutura entre múltiplas ACs. Definido como um conjunto de serviços necessários ao uso de tecnologias baseadas em Chave Pública. O nível de segurança oferecida pela ICP depende da infra-estrutura e do comprimento das chaves utilizadas assegurando os cinco requisitos de segurança já citado. (Emiliano, 2007).

3.3 HIERARQUIA DE UMA ICP

Os serviços de Certificação Digital pública atende a uma hierarquia de Infra-Estrutura De Chaves Públicas composta pelas seguintes entidades:

Autoridade Certificadora Raiz (AC-Raiz): mais alto nível na cadeia de certificação emitindo certificados para as ACs inferiores na hierarquia. Usa algoritmo RSA e chave de 4096 bits, possuindo validade de 8 anos.

Autoridade Certificadora (CA); Sendo cada CA subordinada a uma CA - Raiz podendo emitir, gerenciar e revogar certificados.

Autoridade de Registro (AR): Verifica e valida, aprova ou rejeita solicitações de certificados. Dependendo do resultado não enviam a solicitação para a AC.

Repositórios: Um repositório é um banco de dados mantido pela AC a disposição do público para armazenar, recuperar e consultar certificados e outras informações relacionadas aos certificados. (Emiliano, 2007).

3.4 AUTORIDADES CERTIFICADORAS

Uma AC é uma entidade, pública ou privada, que emite certificados digitais para outras entidades, empresas, indivíduos, que precisam se identificar e garantir as suas operações no mundo digital. No âmbito do Governo Federal, a AC, para ter seus certificados legalmente reconhecidos, o que é obrigatório para transações com órgãos públicos, tem de ter sido certificada pela AC Raiz, ou seja, pelo Instituto Nacional de Tecnologia da Informação (ITI), que é a autoridade responsável por credenciar as demais AC’s.

Segundo Emiliano (2007, 17) “cada certificado Digital emitido é certificado e garantido pela AC responsável pela sua emissão estabelecendo assim uma relação de confiança. A AC recebe a autentica a solicitação de certificados, emite e chancela digitalmente o certificado e gerencia os certificados emitidos”.

O solicitante, no ato do pedido do certificado, envia para AC informações pessoal, através de um formulário assegurado pela AC, junto com a chave Pública gerada pelo sistema local ou não. A AC verifica a veracidade das informações antes de emitir o certificado ao solicitante de acordo com a classe do certificado.

As ACs são divididas em três categorias:

Interna: Operacionalizada por uma instituição, para emissão de certificados digitais internos.

Terceirizada: Uma instituição ou empresa contrata uma AC de terceiros para emitir certificados internos e para clientes.

Autônoma: Privada ou do governo, que comercializa o serviço de certificações aos usuários finais.

Obrigações legais e regras da AC e dos usuários de certificados devem ser expressas em um termo conhecido como DPC (Declaração de práticas de Certificação). Neste documento estão definidos os métodos de trabalho, o grau de confiabilidade dos certificados e das CA´s envolvidas no processo de certificação. (Emiliano, 2007).

3.5 CERTIFICADO DIGITAL

O certificado digital ou identidade digital é um arquivo eletrônico que além de possuir dados de uma pessoa ou instituição, possuem também uma Chave Pública do assinante utilizada para comprovar sua identidade. Estes documentos eletrônicos são chancelados digitalmente pela entidade emissora CA com o objetivo de interligar a chave pública a uma pessoa ou entidade, possuindo o mesmo valor de um documento físico, como carteira de identidade, passaporte, cartões de créditos e utilizados da mesma forma na identificação do indivíduo ou entidades na rede. William (2008). Um certificado digital tem dois objetivos: estabelece a identidade do proprietário e torna disponível a chave pública do proprietário. (IBM, 2009).

Os certificados digitais foram inicialmente padronizados no padrão X.509. A especificação X.509 é um padrão internacional que especifica o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública. Na ICP-Brasil utiliza-se de certificados no padrão X.509 versão três. (Cert.BR, 2009).

Os certificados digitais possuem uma estrutura padronizada e estruturada como veremos a seguir.

3.6 ESTRUTURA DE UM CERTIFICADO DIGITAL

Um certificado digital normalmente apresenta as seguintes informações:
Nome da pessoa ou entidade a ser associada à chave pública;
Período de validade do certificado;
Chave pública;
Nome e assinatura da entidade que assinou o certificado e
Número de série. (Caixa, 2009).

A figura 03 apresenta a estrutura de um certificado digital:

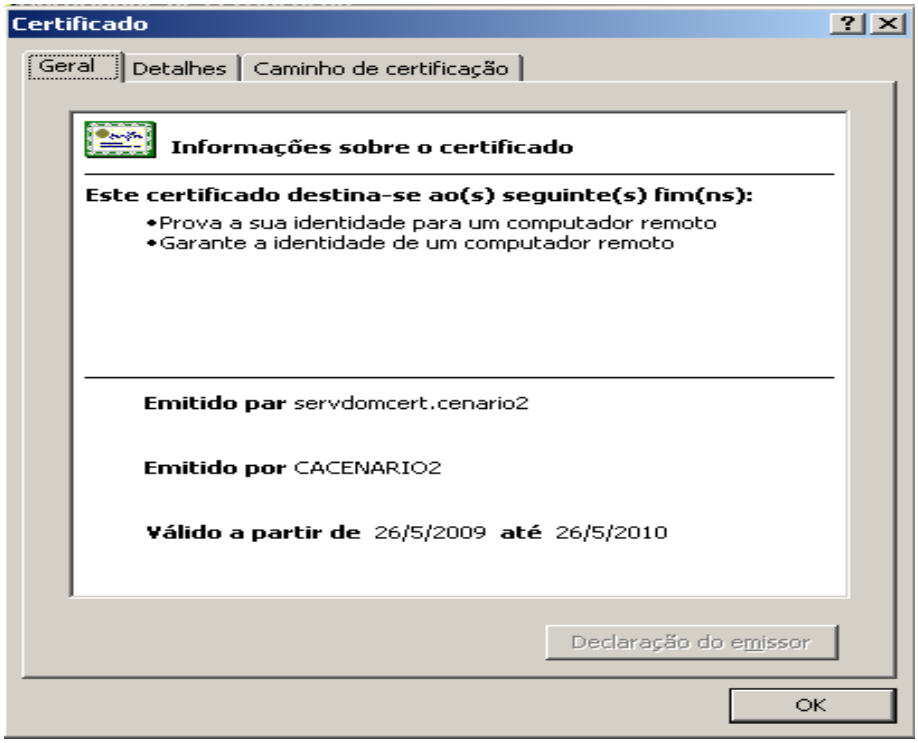


Figura 3 CERTIFICADO DIGITAL EMITIDO NO EXPERIMENTO CENARIO2. FONTE: O AUTOR.

No próximo item trataremos dos conceitos básicos envolvidos no processo de autenticação.

3.7 MÉTODOS DE AUTENTICAÇÃO

As autenticações dos clientes de acesso normalmente usam um protocolo de autenticação que é negociado durante o processo de estabelecimento da conexão. Aqui são apresentados alguns protocolos de autenticação básica utilizado pelo sistema operacional proprietário usado no experimento. Foge ao escopo deste trabalho detalhar esses métodos;

* EAP: Com o protocolo EAP (protocolo de autenticação extensível), um mecanismo de autenticação arbitrária autentica uma conexão de acesso remoto. O esquema exato de autenticação a ser usado é negociado pelo cliente de acesso remoto e o autenticador (o servidor de acesso remoto ou um servidor RADIUS [*Remote Authentication Dial-In User Service*]).

* EAP TLS : É um tipo EAP usado em ambientes de segurança baseados em certificado. A troca de mensagens EAP-TLS proporciona a autenticação mútua, negociação do método de criptografia e determinação de chave de criptografia entre o cliente de acesso remoto e o autenticador. O TLS (*Transport Layer Security*) é padrão IETF do SSL (*Secure Sockets Layer*). Permite que aplicações cliente-servidor comuniquem-se prevenindo: escuta de conversas privadas; modificação das mensagens sem permissão; e cópia ilegal de mensagens (Tecnet, 2009). O objetivo principal do protocolo TLS é prover integridade e privacidade dos dados na comunicação de aplicações. É um protocolo independente da aplicação, ou seja, outros níveis de protocolo podem estar acima do TLS de forma transparente. As decisões sobre como iniciar o TLS e como interpretar os certificados de autenticação trocados entre as partes da comunicação, ficando a cargo da aplicação que roda acima do TLS. (RFC 2246, 2009).

* PEAP: O Protocolo de Autenticação Extensível Protegido (PEAP) é um novo membro da família dos protocolos (EAP).

* CHAP: O protocolo CHAP (protocolo de autenticação de *handshake* de desafio) é um protocolo de autenticação de resposta de desafio que usa o esquema de hash padrão da indústria, o *Message Digest* 5 (MD5) para criptografar a resposta. O CHAP é usado por vários fornecedores de servidores e clientes de acesso a rede.

* PAP: O protocolo PAP (protocolo de autenticação de senha) utiliza senhas de texto sem formatação e é o protocolo de autenticação menos seguro. Normalmente, é negociado se o cliente de acesso remoto e o servidor

de acesso remoto não puderem negociar uma forma mais segura de validação. (Tecnet, 2009).

Cada método de autenticação tem vantagens e desvantagens em termos de segurança, uso e abrangência do suporte. A configuração do servidor de acesso ao cliente determina o método de autenticação a ser usado.

Alguns métodos de autenticação como PEAP e EAP, usam certificados para autenticação de computadores e usuários. Protocolo EAP-TLS e Protocolo PEAP sempre utilizam certificados na autenticação de servidores. Dependendo do tipo de autenticação configurado com o método de autenticação, podem ser utilizados certificados para autenticação de usuários e clientes. A latência na replicação do servidor de domínio pode afetar temporariamente a capacidade de um cliente ou servidor obter um certificado a partir de uma CA (autoridade de certificação). Se um computador configurado para usar certificados para autenticação não puder registrar um certificado, a autenticação falhará. (RFC 2246, 2009).

PAP-TLS com reconexão rápida: A reconexão rápida do PEAP reduz o tempo de resposta para autenticação entre o cliente e o autenticador, uma vez que a solicitação de autenticação é encaminhada do novo servidor para o servidor original. Uma vez que o autenticador e o cliente PEAP usam as propriedades de conexão por TLS armazenadas em cache anteriormente (a coleta a partir da qual o manipulador TLS é nomeado), o autenticador pode determinar rapidamente se a conexão do cliente deve ser reconectada (Tecnet, 2009).

Os Certificados são utilizados para autenticar o acesso à rede por oferecerem alta segurança na autenticação de usuários e computadores e eliminam a necessidade de métodos menos seguros, como os baseados em senha.

* ISAKMP: É um protocolo para o estabelecimento de associações de segurança (SA) e chaves criptográficas em um ambiente de rede. ISAKMP (*Internet Security Association e Key Management Protocol*) define os procedimentos de autenticação de uma comunicação entre colegas, a criação e a gestão das associações de segurança, criação de chaves técnicas de mitigação e de ameaça (por exemplo, negação de serviço e de ataques repetidos). ISAKMP normalmente utiliza IKE para a troca de chaves, embora

outros métodos podem ser implementados. ISAKMP está documentado na RFC 2048 (2009): *Internet Security Association e Key Management Protocol* (ISAKMP). ISAKMP em IP (*Internet Protocol*) é documentada no RFC 2407 (2009): *The Internet IP Security Domain* de Interpretação para ISAKMP.

* IKE: IKE é um modo de troca de chaves para ISAKMP. IKE é usado para troca segura encriptação chaves, como parte da construção de um túnel VPN.

Encriptação IKE suporta os seguintes algoritmos:

DES-CBC

IDEA-CBC

Blowfish-CBC

RC5-R16-B64-CBC

3DES-CBC

CAST-CBC

IKE suporta os seguintes algoritmos *hash*:

MD5

SHA

Tiger

IKE suporta os seguintes métodos de autenticação:

Pré-chave compartilhada

DSS assinaturas

Assinaturas RSA

Encryption com RSA

Revisto com criptografia RSA

O IKE utiliza o (Diffie-Hellman assimétrica) cifra para troca de chaves e pode ser conhecido com mais detalhe na RFC 2409 (2009).

Neste capítulo foi visto os conceitos básicos sobre Certificação Digital, infra-estrutura de chaves bem como conceitos de autoridade certificadora, mecanismos de autenticação e protocolos utilizados. No próximo capítulo será abordado o planejamento do ambiente de testes.

4 AMBIENTE DE TESTES COM INFRA ESTRUTURA DE CHAVE PÚBLICA

Ao decidirmos planejar uma rede local segura, devemos observar os seguintes critérios: Requisitos de segurança – Autenticação e autorização robusta de clientes; Controle de acesso de clientes; Criptografia de alta segurança; Gerenciamento seguro de chaves de criptografia; Suporte a várias plataformas – Oferecer suporte aos diversos clientes: Sistema operacional proprietário; Número de usuários; Número de máquinas na rede. (Tecnet, 2009).

Para o experimento proposto temos:

Configuração de um servidor de autoridade de certificação.

Configuração de um servidor autenticação de rede.

Realização dos testes e comparação dos resultados

Configuração de uma máquina cliente

O próximo capítulo detalha os recursos necessários para criação de um ambiente de testes controlado.

4.1 INFRA-ESTRUTURA NECESSÁRIA

Neste cenário utilizamos sistema operacional proprietário que vem com todos os produtos necessários no nível de serviço que suportam o padrão de infra-estrutura de chaves públicas e foi usado como elemento principal da infra-estrutura da LAN (*Local Area Networking*) objeto deste trabalho. Todas as VM´s criadas possuem 10GigaByts de espaço em disco, 256 MB Ram, 64 MB vídeo. Na figura 4 são mostradas as Máquinas virtuais (Vm´s) criadas com a utilização do software de virtualização de máquinas VirtualBox. O Linux Ubuntu 8.10 serviu de suporte para instalação do VirtualBox. Não é objetivo desse trabalho detalhar as funcionalidades do software de virtualização usado no cenário de testes.

Figura 4 CONFIGURAÇÃO DAS VM´S NO VIRTUALBOX-2.2. FONTE: O AUTOR.

Logo, os elementos necessários que compõem este cenário de testes são:

Cenário_01

Sistema operacional proprietário: Servidor de autenticação

Visualizar Eventos

Sistema operacional livre servindo de infra para as VM´s

Sistema operacional proprietário: Máquina cliente

Baseado nas informações descritas anteriormente pode-se propor o cenário da (figura 1) como ambiente LAN (*Local Area Networking*) para demonstração e o uso das tecnologias envolvidas.

Descrição sumária do ambiente cenário_01:

Instalação do Virtual-Box-2.2 em ambiente Linux para servir de infra estrutura para instalação das VM´s que compõem o cenário proposto.

VM - Sistema operacional proprietário: Servidor de autenticação. Nome do servidor; “SERVER_DOMINIO”, IP: 192.168.0.30/24

Grupos e usuários com acesso a LAN

Usuário: “TESTECENARIO1”.

VM - Sistema operacional proprietário: (estação cliente do domínio) Nome Clientecen1 IP: 192.168.0.20

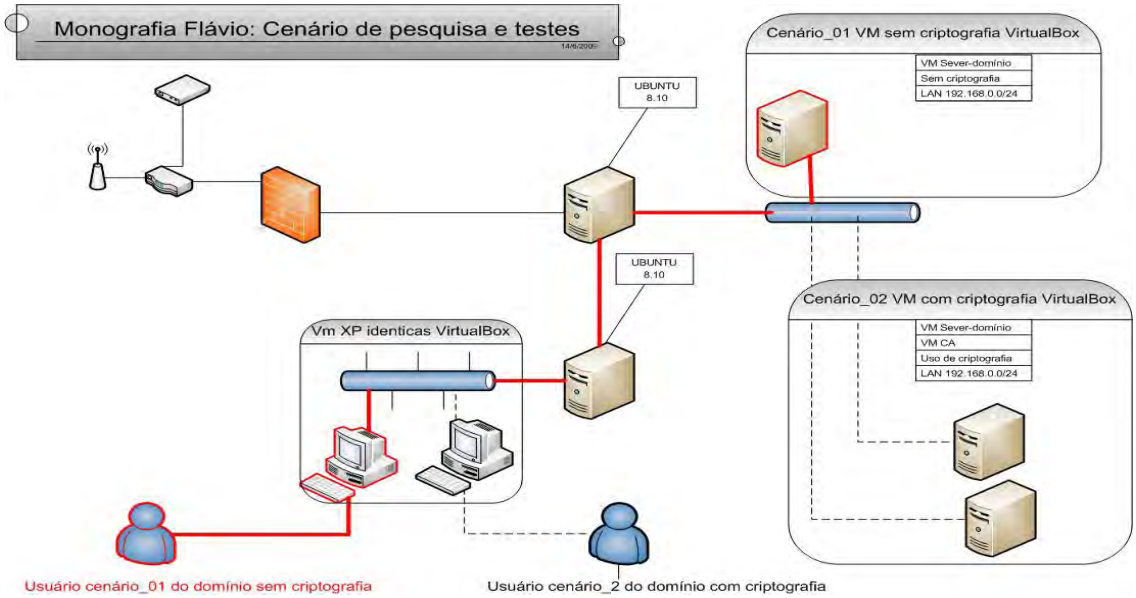


Figura 5 CENÁRIO_01 DE TESTES FONTE: O AUTOR.

Cenário_02

Sistema operacional proprietário: Servidor de autenticação

Sistema operacional proprietário: Serviço de Certificado (CA)

Visualizar Eventos

Sistema operacional livre servindo de infra para as VM´

Sistema operacional proprietário: Máquina cliente

Descrição sumária do ambiente cenário_02:

Instalação do Virtual-Box-2.2 em ambiente Linux Ubuntu para servir de infra estrutura para instalação das VM´s que compõem o cenário proposto.

VM - Sistema operacional proprietário: Servidor de autenticação, Nome do domínio; “SERVDOMCERT”, IP: 192.168.0.30/24

VM - Um servidor único com CA e IAS (*Internet Authentication Service*), Nome do servidor; “CACENARIO2”, IP: 192.168.0.40/24

Grupos e usuários com acesso a LAN

Usuário: “TESTECENARIO2”.

VM - Sistema operacional proprietário: (estação cliente do domínio). Nome Clientecen2 IP: 192.168.0.20

VM - Certificado da Autoridade Certificadora

Certificados de Computador e Usuário

Autenticação usando certificados.

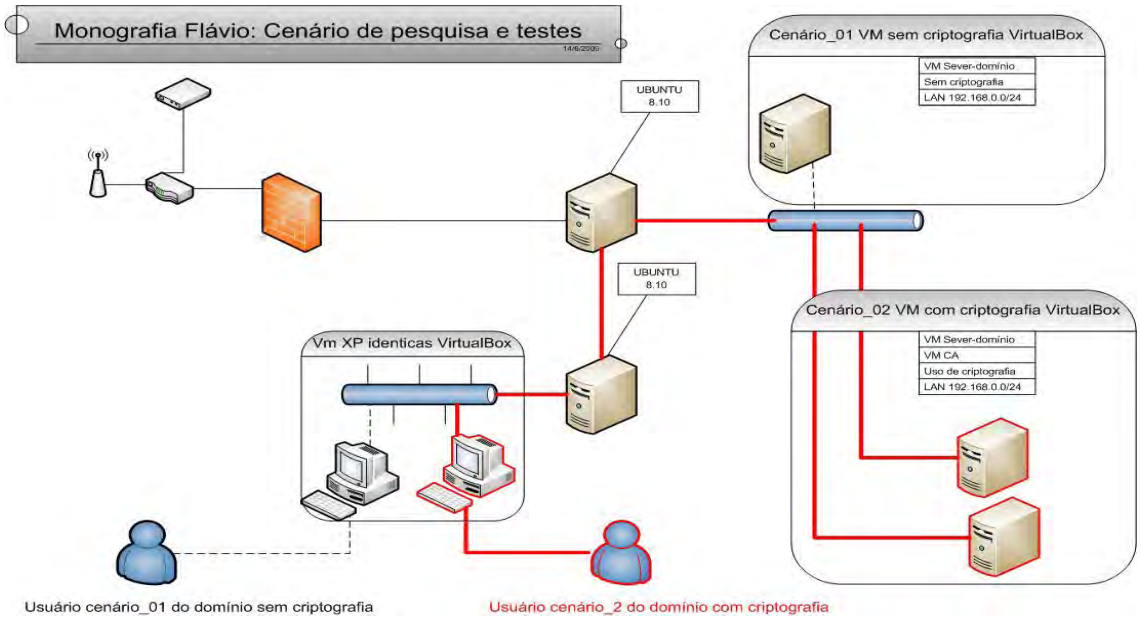


Figura 6 CENÁRIO_02 DE TESTES FONTE: O AUTOR.

Para implantar certificados para usuários e computadores será necessário:

Criar uma infra-estrutura de chave pública (PKI).

Implantar uma autoridade de certificação (CA) utilizando Serviços de Certificados.

Criar e publicar um ou mais certificados usando modelos de certificados, que são instalados com os Serviços de Certificados.

Selecionar um ou mais métodos de distribuição (também conhecidos como métodos de registro de certificados) para instalar os certificados em computadores e distribuí-los aos usuários. Todos os certificados que são utilizados para autenticação de acesso a redes devem atender aos requisitos de certificados X.509 e trabalhar para conexões que utilizem SSL/TLS (camada de soquetes de segurança – segurança no nível de transporte). (Tecnet, 2009).

5 DETALHES RELEVANTES NA PREPARAÇÃO DO EXPERIMENTO

O passo zero é montar o servidor de autenticação do ambiente proposto previamente instalado em Vm´s, não sendo objeto deste experimento descrever os passos para instalação de um controlador de domínio. O leitor poderá usar o “Assistente para instalação do Controlador de domínio” figura 7, executando o comando dcpromo e seguir suas orientações (Tecnet, 2009). Nesse experimento também não será abordado a criação de Vm´s para construção do cenário, mas em anexo será disponibilizado um tutorial do Virtual Box utilizado no experimento.

O ambiente proposto possui um servidor de autenticação sem utilização de certificados cenario_01, nomeado de SERVDOM e um servidor de autenticação com utilização de certificados cenario_02, nomeado de SERVDOMCERT.

Com o controlador de domínio cenário_01 e cenário_02 em Vm´s distintas, conforme figura 01. Usando o comando mmc é possível criar Usuários e Computadores do Controlador de domínio.

5.1 INSTALANDO E CONFIGURANDO UM SERVIDOR DE CERTIFICADO DIGITAL

Esta seção descreve os passos para instalação e configuração do Serviço de Certificado. Na distribuição utilizada o serviço de certificado é um componente opcional e por padrão não é instalado.

Uma instalação do serviço de certificado é chamada de CA (autoridade de certificação). Para este nosso experimento, somente uma CA é necessária e será usada para emitir certificado para o servidor cenário_02 e para os usuários, que serão usados no modelo de autenticação EAP-TLS, que usa certificados para comprovar a identidade do usuário.

O objetivo desta seção é apenas fornecer uma CA muito simples, não se aprofundando em nenhum dos conceitos específicos de uma arquitetura PKI (infra-estrutura de chave pública), apenas o processo de instalação e os passos básicos de uso da CA para emissão dos certificados necessários ao nosso experimento.

5.2 INSTALANDO A CA

Vamos agora instalar e configurar a CA como uma autoridade de certificação raiz corporativa. A mesma necessita estar conectado com uma conta no servidor de domínio proposto no cenario2, que seja membro do grupo de administradores corporativos e grupo de administradores do domínio raiz. (Tecnet, 2009).

Clique em Iniciar, clique em Painel de Controle e, em seguida em Adicionar e remover programas para iniciar a instalação. Clique em Adicionar/Remover componentes do Sistema operacional proprietário. Na lista de componentes, selecione Serviços de certificado figura 8. Clique em Avançar para continuar.

Figura 7 ASSISTENTE DE COMPONENTES DO SISTEMA OPERACIONAL PROPRIETÁRIO – SERVIÇOS DE CERTIFICADO FONTE: O AUTOR.

Na lista de tipo de autoridade, selecione Autoridade de certificação raiz corporativa. Clique em Avançar para continuar. Nomeie a autoridade como CACENARIO2. Clique em Avançar em continuar.

Clique em Avançar para continuar. Clique em Sim em Serviços de certificados na pergunta sobre ativação de páginas ASP. Feche o “Assistente de componentes.

Após instalação da CA torna-se necessário a instalação dos modelos de certificados mostrado na figura 10, para tanto foi usado o comando certtmpl.msc.

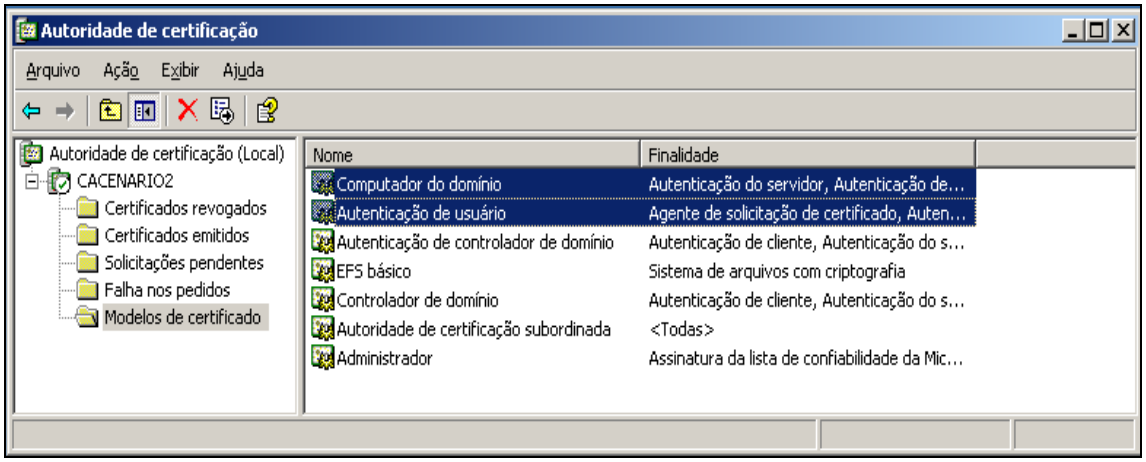


Figura 8 VISUALIZAÇÃO DOS MODELOS DE CERTIFICADOS DISPONÍVEIS FONTE: O AUTOR.

Para que os clientes se registrem automaticamente e a CA emita automaticamente um certificado, foi configurado um modelo padrão descrito em “Configurando um modelo de certificado para registro automático do cliente” (Tecnet, 2009). Uma CA pode ser administrada remotamente por meio de páginas web, no próximo item será mostrado como instalar esse recurso.

5.3 INSTALANDO O SERVIDOR DE APLICAÇÃO WEB

O serviço de certificado opcionalmente pode ser administrado através de uma página web, para isso, é necessária a instalação do IIS. Execute o procedimento a seguir para instalar o IIS: Clique em Iniciar, clique em Painel de

Controle e, em seguida em adicionar e remover programas para iniciar a instalação. Clique em Adicionar/Remover componentes do Sistema operacional proprietário. Na lista de componentes, selecione Servidor de aplicativo. Clique em Avançar para continuar.

Feche o “Assistente de componentes do Sistema operacional proprietário”.

5.4 EMITINDO UM CERTIFICADO

Uma vez que criamos um modelo de certificado automático tanto para o computador e para cliente em uma CA que faz parte do domínio cenário2, será necessário habilitar no controlador de domínio a diretiva (Diretiva de chave pública) para solicitação automática de certificados, conforme figura 10.

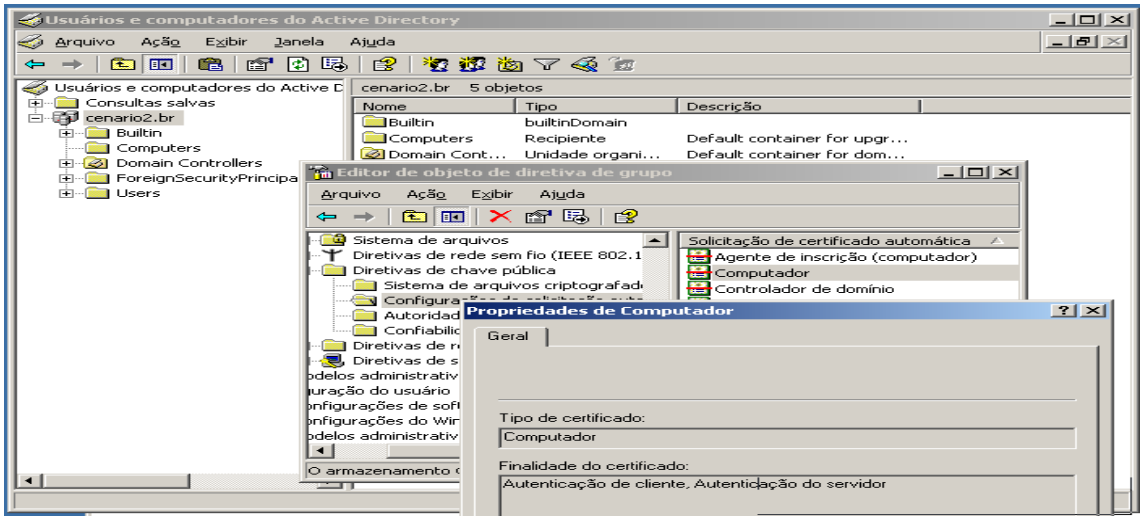


Figura 9 SOLICITAÇÃO DE CERTIFICADOS AUTOMÁTICA: O AUTOR.

Será necessário habilitar também no controlador de domínio a diretiva de chave pública de configuração de usuário para obtenção de registro automático. Uma vez que os clientes façam novamente sua autenticação no controlador de domínio usando a senha de administrador de domínio o servidor CA automaticamente emitirá os certificados correspondentes conforme visto na figura 10 abaixo.

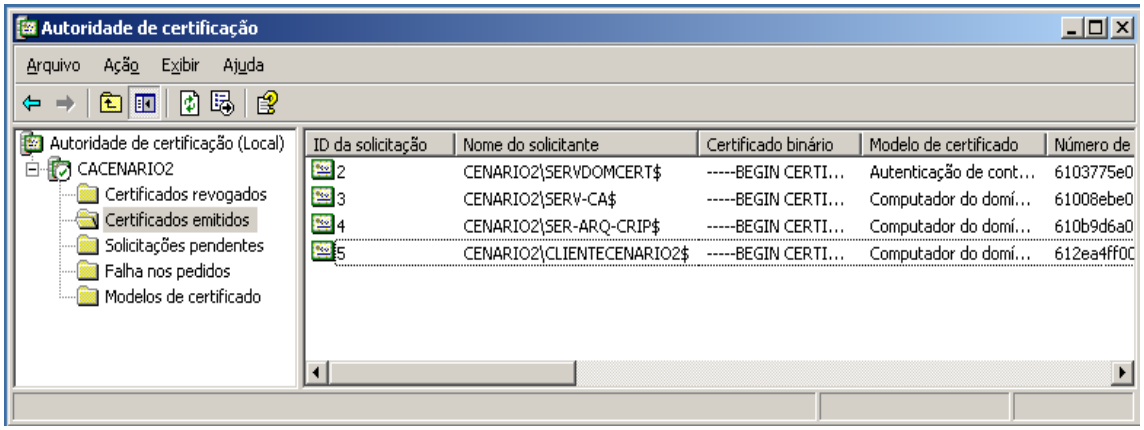


Figura 10 SOLICITAÇÃO DE CERTIFICADOS AUTOMÁTICA: O AUTOR.

Esta seção descreveu o processo de instalação de uma CA e a emissão dos certificados. Uma configuração simples e quer requer pouca manutenção e, portanto, deverá exigir um gerenciamento mínimo. Uma outra opção será solicitar um certificado via comando MMC, configurando incluindo um snap-in de certificados ou utilizar o serviço web para solicitar o certificado. Abaixo o resultado da solicitação de um certificado via web no endereço HTTP:/cacenario2/certsrv/.

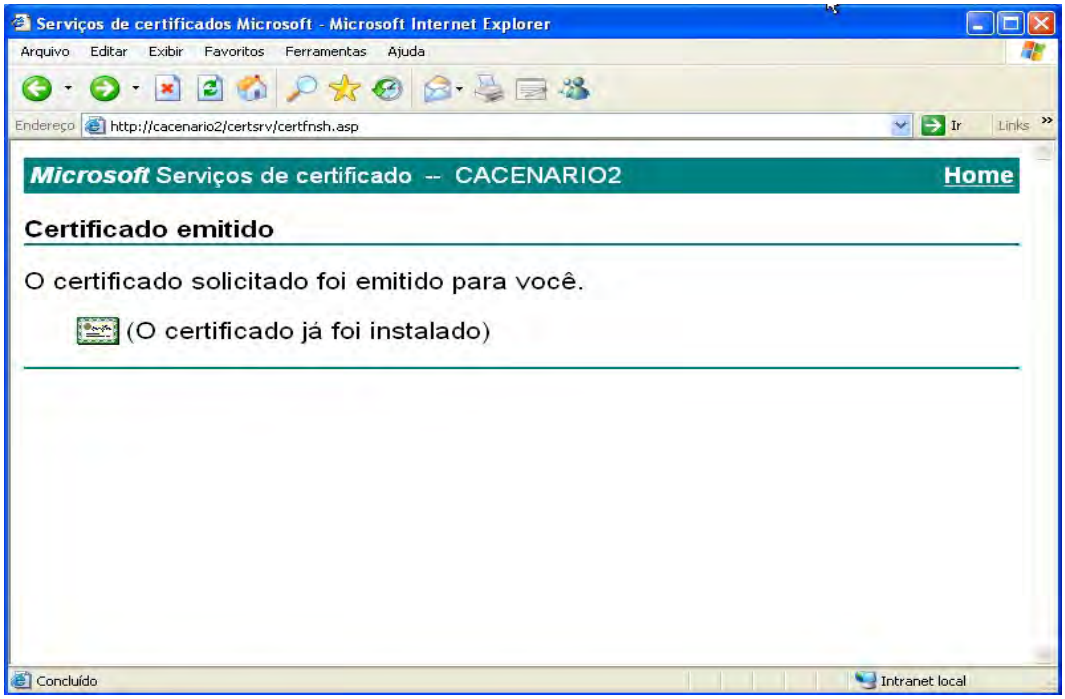


Figura 11 EMISSÃO DE CERTIFICADO VIA SERVIÇO WEB FONTE: O AUTOR.

5.5 CONFIGURANDO O SISTEMA OPERACIONAL CLIENTE COM EAP-TLS

Será necessário configurar manualmente o sistema operacional cliente e para tanto abra no sistema operacional cliente item iniciar, configurações e configurações de rede local. Na aba autenticação escolha a opção ativar a autenticação IEEE 802.1x para esta rede. No combo escolha EAP protegido (PEAP) e click em propriedades. Já no combo propriedades, marque a opção (validar certificado do servidor). Na mesma tela selecione a autoridade certificadora que no nosso experimento é CACENARIO2 conforme figura abaixo.

Figura 12 PROPRIEDADES DO EAP PROTEGIDAS FONTE: O AUTOR.

Uma vez o sistema operacional estando corretamente configurado o processo de negociação de autenticação por certificados pode ser visto conforme mostrado na figura abaixo. Para realizar a captura do pacote foi utilizado um analisador de protocolos chamado wireshark escutando na interface de rede eth1 do ubuntu que fornece infra estrutura para as Vm´s envolvidas no cenário de testes figura 13.

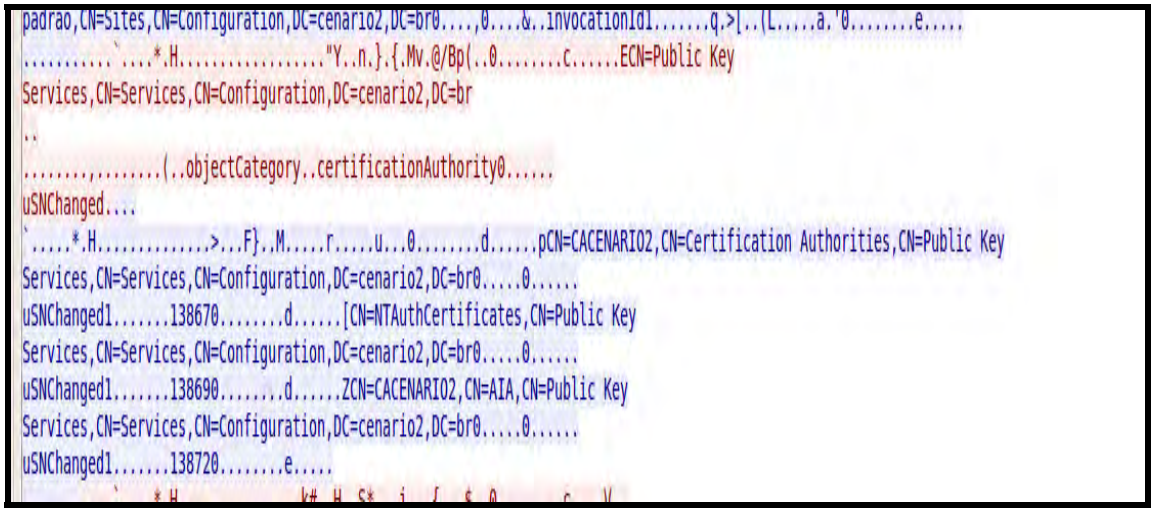


Figura 13 PROPRIEDADES DO EAP PROTEGIDAS FONTE: O AUTOR.

Neste capítulo foi visto detalhes relevantes na implantação do cenário experimental. No próximo capítulo será descrito a coleta de resultados do experimento realizado.

6 MEDIDAS DE DESEMPENHO

O objetivo principal é estudar qual a efetivo impacto na implantação e no desempenho (performance) das redes LAN (*Local área Networking*) devido à utilização de mecanismos de segurança, tais como, sistemas de autenticação utilizando certificados digitais e criptografia estudados no capítulo 2, em comparação a serviços de autenticação sem utilização de certificados e criptografia. Para isso, este trabalho propõe-se realizar uma simulação da operação de uma rede LAN (*Local área Networking*) definida em um cenário de testes e com seus aspectos relevantes mostrado no capítulo 3. A partir desse experimento poderemos quantificar o real impacto da utilização das técnicas descritas, seja no desempenho, seja no custo para implantar o cenário proposto.

Segundo Tanenbaum (2003, p 595) “uma quantidade útil que se deve ter em mente ao se analisar o desempenho das redes é o produto da largura de banda pelo retardo. Esse produto é obtido multiplicando-se a largura de banda (em bits/segundo) pelo tempo de retardo da viagem de ida e volta (em segundos)”.

O tempo de resposta e a vazão (*throughput*) são os parâmetros de interesse para avaliação e medição do desempenho.

Eles são definidos neste trabalho como se segue:

Tempo gasto na configuração dos servidores.

Tempo para autenticação: tempo medido no processo de autenticação.

Vazão/Taxa (*Throughput*):Taxa na qual os pedidos são atendidos (servidos) pelo sistema.

Tempo de Resposta: tempo total de transmissão da mensagem entre dois pontos. O tempo de resposta total inclui o tempo de negociação entre o cliente e o servidor, o tempo de efetiva transferência dos dados e o tempo de desconexão.

6.1 PROCEDIMENTOS PARA MEDIÇÃO

Neste capítulo serão mostrados os procedimentos de testes e os resultados obtidos comparando os dois cenários propostos. Para cada cenário, com exceção da medida de tempo gasto na instalação e configuração dos servidores, o experimento foi repetido 10 vezes, sendo que os três primeiros resultados foram desconsiderados, de forma a se evitar a influência de fatores dos sistemas operacionais e das máquinas, como por exemplo, o processo de armazenamento de dados das páginas em memória *cache*.

6.1.2 TEMPO GASTO NA INSTALAÇÃO E CONFIGURAÇÃO DOS SERVIDORES

O tempo gasto na instalação e configuração dos servidores do cenario1 e cenário2 foi medido tomando como referência apenas a instalação dos sistemas operacionais nas respectivas VM´s do VirtualBox. Neste experimento não foi considerado para efeito de testes o tempo gasto na instalação do VirtualBox. A medição foi cronometrada a partir do boot do sistema operacional. Já a medição do tempo de configuração foi medida a partir da tela de logon no sistema operacional até a completa configuração do servidor e máquinas clientes. Os resultados obtidos para o cenário1 foram:

Instalação do SO SERV-DOM: 83 minutos.

Instalação do SO Cliente1: 58 minutos.

Configuração do SERV-DOM: 20 minutos.

Configuração do SO Cliente para entrada no domínio: 10 minutos

Tempo Total: 171 minutos foi o tempo total medido desde a instalação até a completa configuração do cenario1.

A figura a seguir mostra o gráfico resultante.

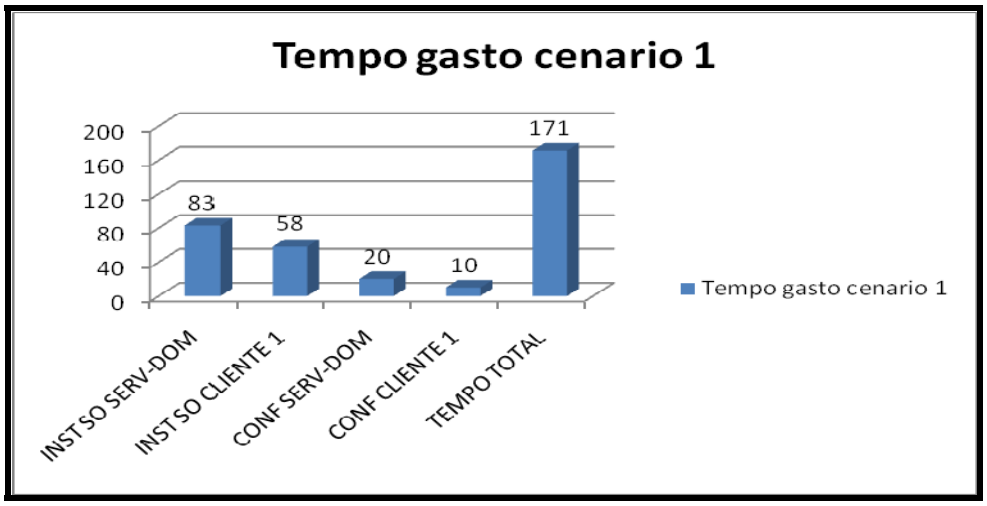


Figura 14 TEMPO EM MINUTOS GASTO NA INSTALAÇÃO E CONFIGURAÇÃO DO SENÁRIO 1 Senario? Ou cenário? FONTE: O AUTOR.

Os resultados obtidos para o cenário2 foram:

Instalação do SO SERV-DOM-CERT: 82 minutos.

Instalação do SO SERV-CA: 82 minutos.

Configuração do SERV-DOM-CERT: 30 minutos.

Instalação do SO Cliente2: 60 minutos.

Configuração do SO Cliente para entrada no domínio: 11 minutos

Configuração do SERV-CA: 20 minutos.

Tempo Total: 285 minutos foi o tempo total medido desde a instalação até a completa configuração do cenario2.

A figura abaixo mostra o gráfico resultante.

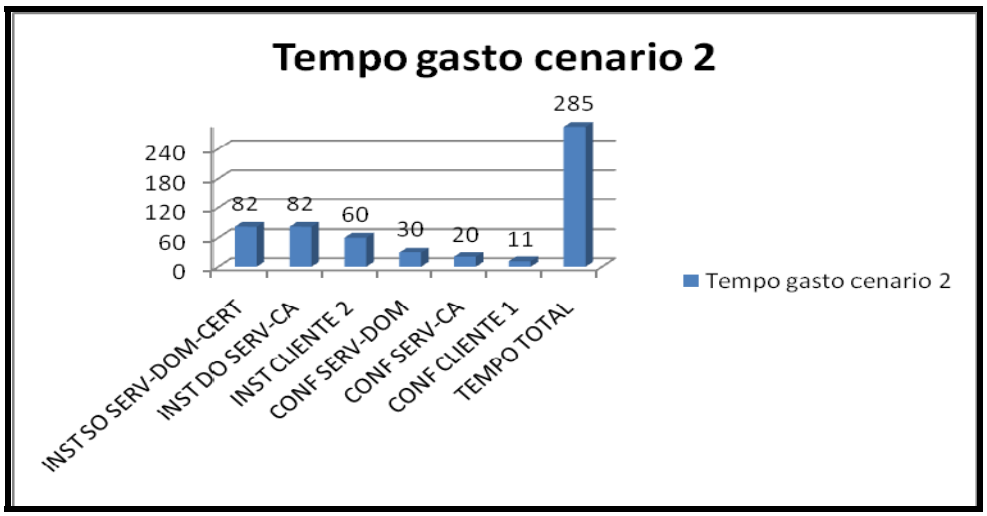


Figura 15 TEMPO EM MINUTOS GASTO NA INSTALAÇÃO E CONFIGURAÇÃO DO CENÁRIO 2 FONTE: O AUTOR.

Podemos ver que o tempo de configuração e instalação do cenário2 foi superior em 114 minutos, ou seja, uma hora e 54 minutos. A principal causa deste valor é o fato de o cenario2 possuir um servidor a mais nomeado de SERV-CA. A figura a seguir o ilustra os dois cenários.

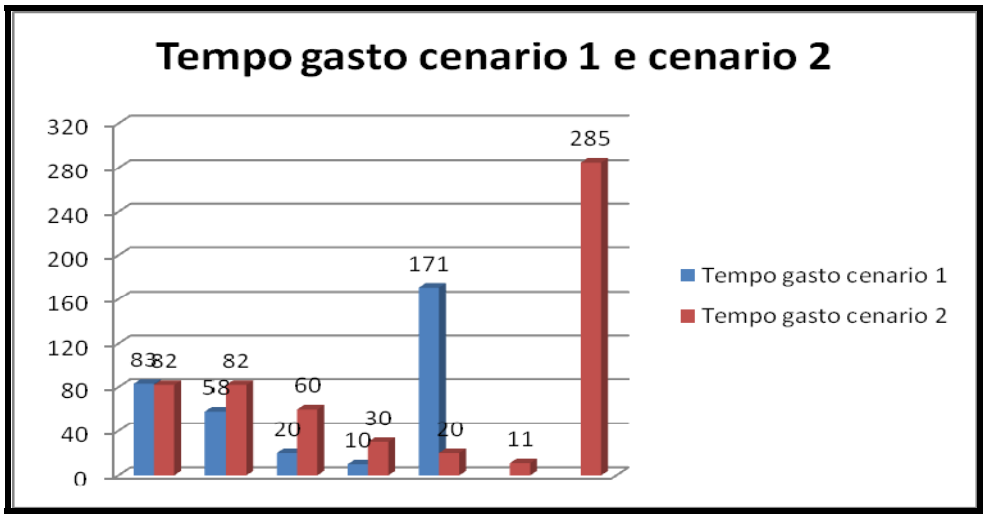


Figura 16TEMPO EM MINUTOS GASTO NA INSTALAÇÃO E CONFIGURAÇÃO DO CENÁRIO DE TESTES FONTE: O AUTOR.

Podemos aferir pelos tempos de instalação e configuração coletada que a montagem de uma infra estrutura de chaves públicas com o objetivo de aferir autenticação e criptografia de dados, necessita de mais recursos computacionais bem como de um maior tempo desprendido em sua montagem. Pode-se deduzir desse teste que em um cenário real envolvendo muitas máquinas esse fato se torna por si só um fator relevante de tomada de decisão.

6.1.3 TEMPO DE AUTENTICAÇÃO:

O tempo de autenticação foi medido com o software Wireshark escutando na interface de rede eth1 do Ubuntu que fornece infra estrutura para as Vm´s envolvidas. Foi considerado o tempo gasto até o recebimento do último pacote de dados envolvido no processo de autenticação. Nos testes não foi considerado o tempo gasto para a 1º autenticação do cliente após ingresso no domínio. Quando o computador ingressa em um domínio, é criada uma conta de computador.

Depois disso, quando o sistema é iniciado, ele usa a senha de conta do computador para criar um canal seguro com um controlador de domínio para o seu domínio. Esse canal seguro é usado para executar operações como autenticação de passagem consulta de nome, etc. (Tecnet, 2009).

A figura a seguir ilustra o processo de autenticação de forma auto-explicativa.

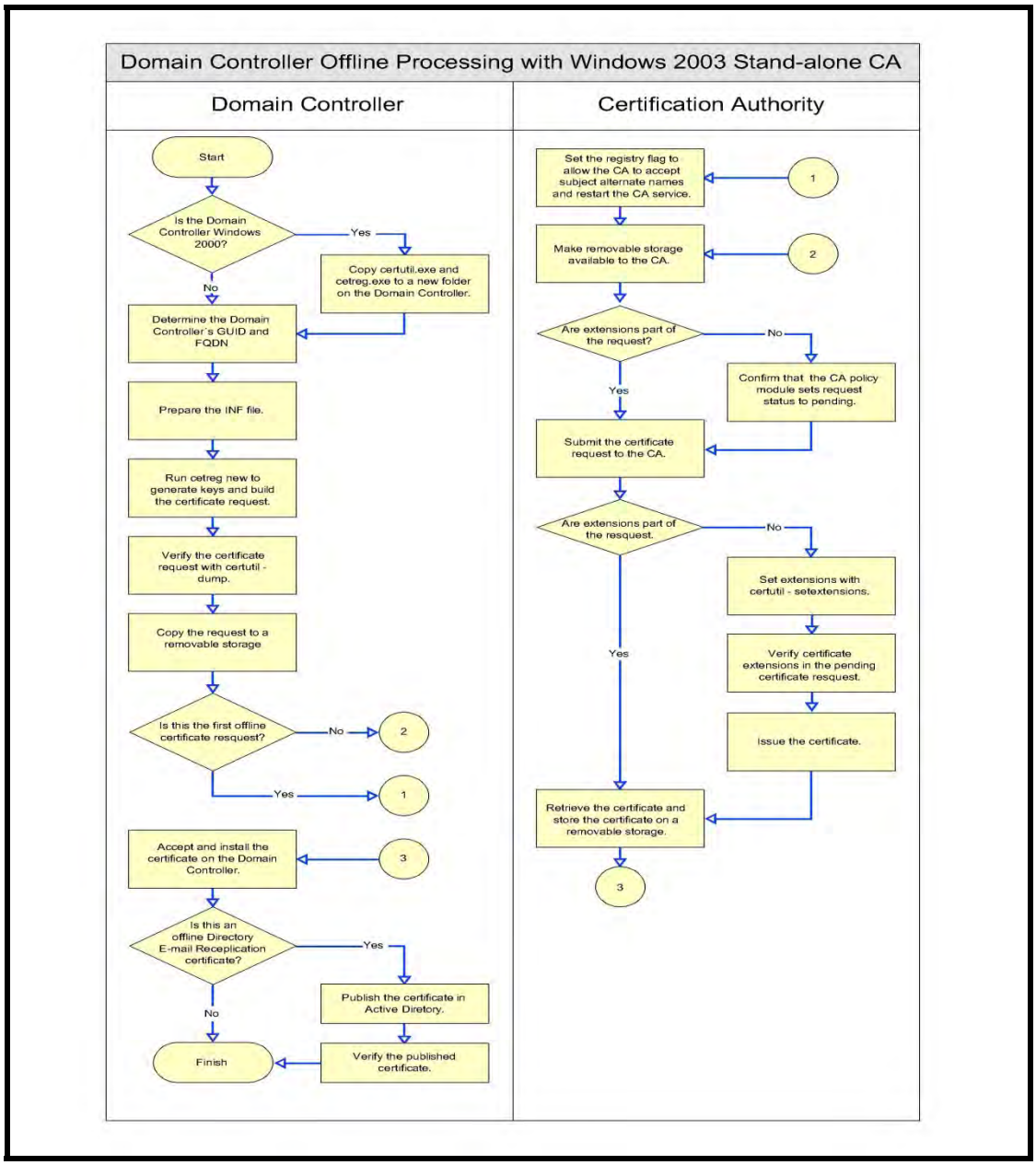
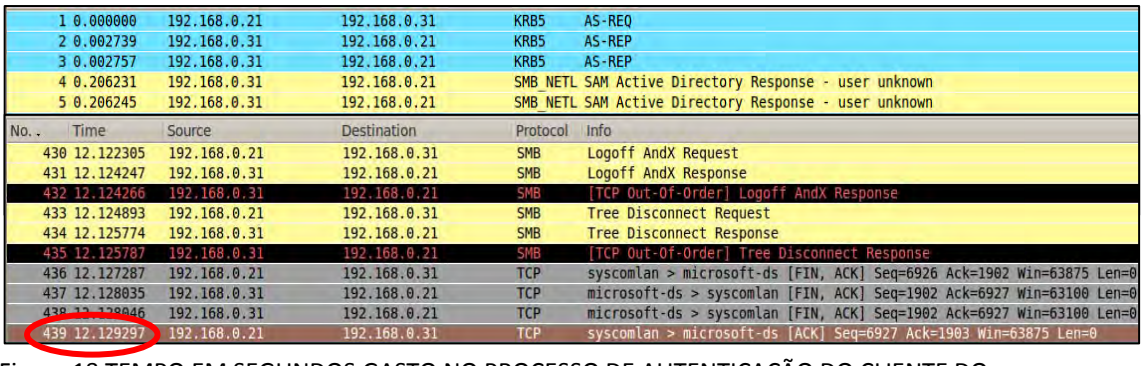


Figura 17 PROCESSO DE AUTENTICAÇÃO FONTE: (TECNET, 2009).

6.1.3.1 MEDIDA REFERENTE AO CENARIO1

O critério de medida seguiu a seqüência natural dos pacotes de dados registrado após a autenticação. O resultado de teste do cenário1 é mostrado a seguir: Na figura abaixo é mostrado o início do envio do primeiro pacote e logo abaixo o último pacote totalizando um tempo de 12,129 segundos.

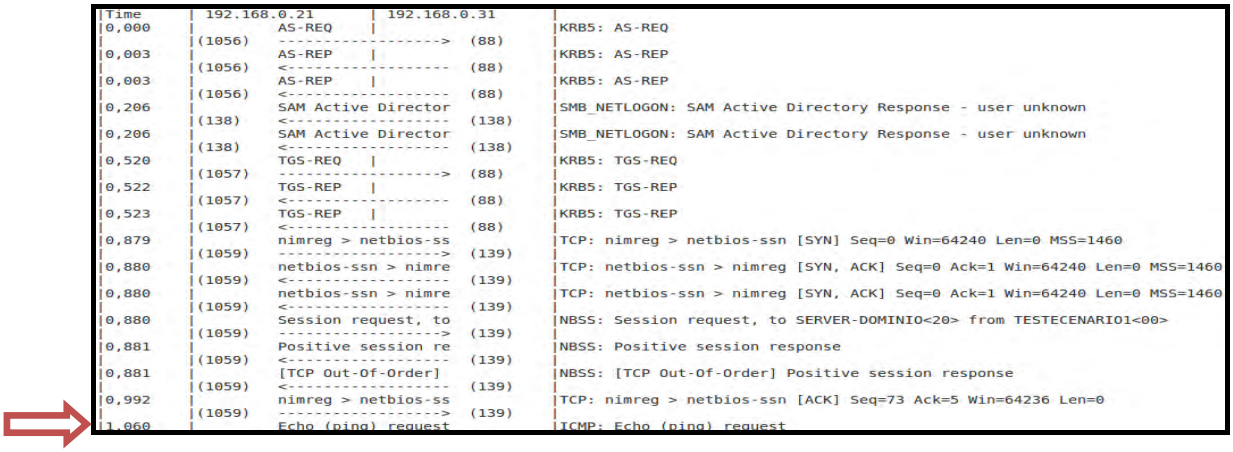


1	0.000000	192.168.0.21	192.168.0.31	KRB5	AS-REQ
2	0.002739	192.168.0.31	192.168.0.21	KRB5	AS-REP
3	0.002757	192.168.0.31	192.168.0.21	KRB5	AS-REP
4	0.206231	192.168.0.31	192.168.0.21	SMB_NETL	SAM Active Directory Response - user unknown
5	0.206245	192.168.0.31	192.168.0.21	SMB_NETL	SAM Active Directory Response - user unknown

No.	Time	Source	Destination	Protocol	Info
430	12.122305	192.168.0.21	192.168.0.31	SMB	Logoff AndX Request
431	12.124247	192.168.0.31	192.168.0.21	SMB	Logoff AndX Response
432	12.124266	192.168.0.31	192.168.0.21	SMB	[TCP Out-Of-Order] Logoff AndX Response
433	12.124893	192.168.0.21	192.168.0.31	SMB	Tree Disconnect Request
434	12.125774	192.168.0.31	192.168.0.21	SMB	Tree Disconnect Response
435	12.125787	192.168.0.31	192.168.0.21	SMB	[TCP Out-Of-Order] Tree Disconnect Response
436	12.127287	192.168.0.21	192.168.0.31	TCP	syscomlan > microsoft-ds [FIN, ACK] Seq=6926 Ack=1902 Win=63875 Len=0
437	12.128035	192.168.0.31	192.168.0.21	TCP	microsoft-ds > syscomlan [FIN, ACK] Seq=1902 Ack=6927 Win=63100 Len=0
438	12.128046	192.168.0.31	192.168.0.21	TCP	microsoft-ds > syscomlan [FIN, ACK] Seq=1902 Ack=6927 Win=63100 Len=0
439	12.129297	192.168.0.21	192.168.0.31	TCP	syscomlan > microsoft-ds [ACK] Seq=6927 Ack=1903 Win=63875 Len=0

Figura 18 TEMPO EM SEGUNDOS GASTO NO PROCESSO DE AUTENTICAÇÃO DO CLIENTE DO CENARIO1 FONTE: O AUTOR.

Na figura abaixo podemos ver mais detalhes do primeiro segundo, de troca de informações, do protocolo de autenticação utilizando o Kerberos.



Time	192.168.0.21		192.168.0.31	
0,000		AS-REQ		KRB5: AS-REQ
	(1056)	---------->	(88)	
0,003		AS-REP		KRB5: AS-REP
	(1056)	<----------	(88)	
0,003		AS-REP		KRB5: AS-REP
	(1056)	<----------	(88)	
0,206		SAM Active Director		SMB_NETLOGON: SAM Active Directory Response - user unknown
	(138)	<----------	(138)	
0,206		SAM Active Director		SMB_NETLOGON: SAM Active Directory Response - user unknown
	(138)	<----------	(138)	
0,520		TGS-REQ		KRB5: TGS-REQ
	(1057)	---------->	(88)	
0,522		TGS-REP		KRB5: TGS-REP
	(1057)	<----------	(88)	
0,523		TGS-REP		KRB5: TGS-REP
	(1057)	<----------	(88)	
0,879		nimreg > netbios-ss		TCP: nimreg > netbios-ssn [SYN] Seq=0 Win=64240 Len=0 MSS=1460
	(1059)	---------->	(139)	
0,880		netbios-ssn > nimre		TCP: netbios-ssn > nimreg [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
	(1059)	<----------	(139)	
0,880		netbios-ssn > nimre		TCP: netbios-ssn > nimreg [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
	(1059)	<----------	(139)	
0,880		Session request, to		NBSS: Session request, to SERVER-DOMINIO<20> from TESTECENARIO1<00>
	(1059)	---------->	(139)	
0,881		Positive session re		NBSS: Positive session response
	(1059)	<----------	(139)	
0,881		[TCP Out-Of-Order]		NBSS: [TCP Out-Of-Order] Positive session response
	(1059)	<----------	(139)	
0,992		nimreg > netbios-ss		TCP: nimreg > netbios-ssn [ACK] Seq=73 Ack=5 Win=64236 Len=0
	(1059)	---------->	(139)	
1,060		Echo (ping) request		ICMP: Echo (ping) request

Figura 19 O PRIMEIRO SEGUNDO REGISTRADO NO PROCESSO DE AUTENTICAÇÃO DO USUÁRIO DE TESTE DO CENARIO1 FONTE: O AUTOR.

Foram realizadas 10 tentativas sendo que as três primeiras foram descartadas conforme mostrado na tabela abaixo

Medidas CENARIO1	1	2	3	4	5	6	7	Média
Tempo autenticação em segundos	12,52	13	12.43	12.12	12.13	12.20	12.5	12,76

Figura 20 TEMPO MÉDIO DE AUTENTICAÇÃO CENARIO1 FONTE: AUTOR.

Foram consideradas as sete tentativas válidas conforme tabela. O resultado do experimento resultou em uma média de 12,76 segundos. Essa média representa o tempo gasto no experimento para ocorrer à autenticação do usuário.

6.1.3.2 MEDIDA REFERENTE AO CENARIO2

O critério de medida seguiu a seqüência natural dos pacotes de dados, começando pelo primeiro pacote até o último registrado com informações de certificados digitais. Foi realizado medidas de tempo para autenticação usando o protocolo EAP protegido bem como medida de tempo para autenticação usando TLS.

O resultado do teste cenário2 com autenticação EAP protegido é mostrado a seguir: Na figura abaixo podemos ver o início do envio do primeiro pacote ip.

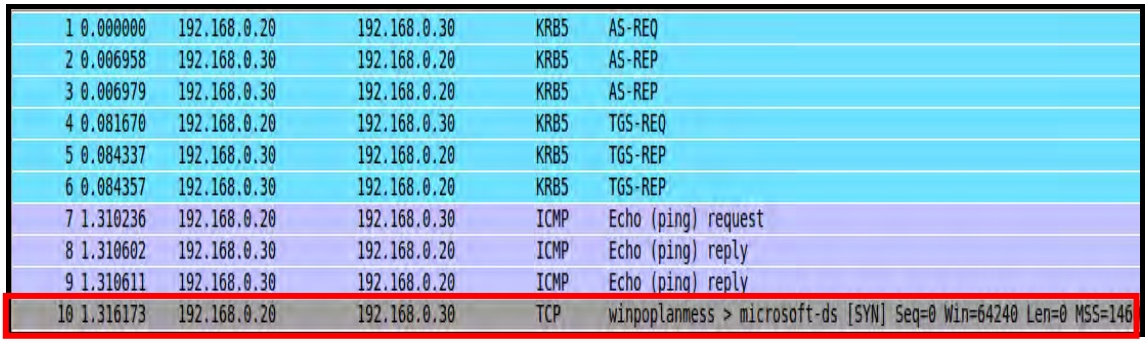
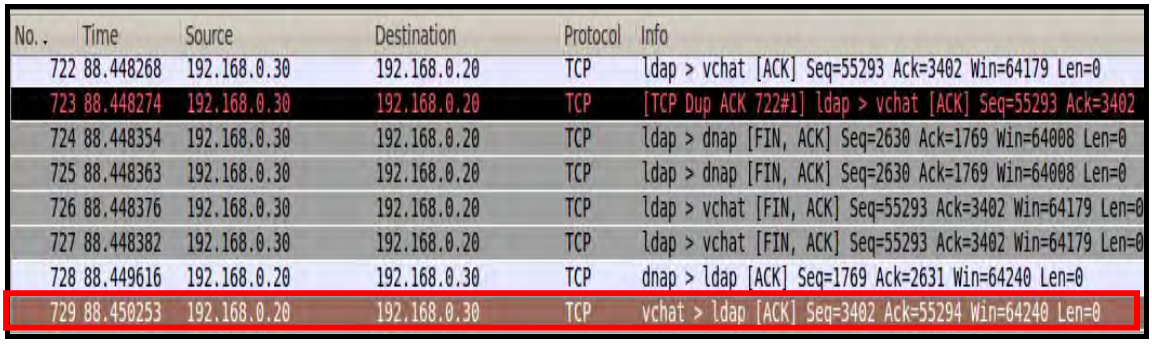


Figura 21 INÍCIO DE AUTENTICAÇÃO DO CLIENTE CENARIO2 FONTE: O AUTO.

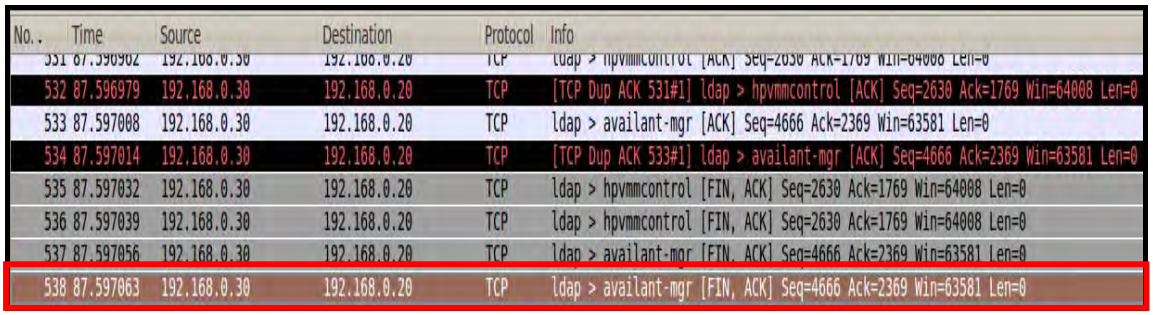
Na próxima figura podemos ver o tempo exato da finalização dos pacotes envolvidos na autenticação.



No.	Time	Source	Destination	Protocol	Info
722	88.448268	192.168.0.30	192.168.0.20	TCP	ldap > vchat [ACK] Seq=55293 Ack=3402 Win=64179 Len=0
723	88.448274	192.168.0.30	192.168.0.20	TCP	[TCP Dup ACK 722#1] ldap > vchat [ACK] Seq=55293 Ack=3402
724	88.448354	192.168.0.30	192.168.0.20	TCP	ldap > dnap [FIN, ACK] Seq=2630 Ack=1769 Win=64008 Len=0
725	88.448363	192.168.0.30	192.168.0.20	TCP	ldap > dnap [FIN, ACK] Seq=2630 Ack=1769 Win=64008 Len=0
726	88.448376	192.168.0.30	192.168.0.20	TCP	ldap > vchat [FIN, ACK] Seq=55293 Ack=3402 Win=64179 Len=0
727	88.448382	192.168.0.30	192.168.0.20	TCP	ldap > vchat [FIN, ACK] Seq=55293 Ack=3402 Win=64179 Len=0
728	88.449616	192.168.0.20	192.168.0.30	TCP	dnap > ldap [ACK] Seq=1769 Ack=2631 Win=64240 Len=0
729	88.450253	192.168.0.20	192.168.0.30	TCP	vchat > ldap [ACK] Seq=3402 Ack=55294 Win=64240 Len=0

Figura 22 TEMPO EM SEGUNDOS GASTO NO PROCESSO DE AUTENTICAÇÃO EAP DO CLIENTE DO CENNARIO2 FONTE: O AUTOR.

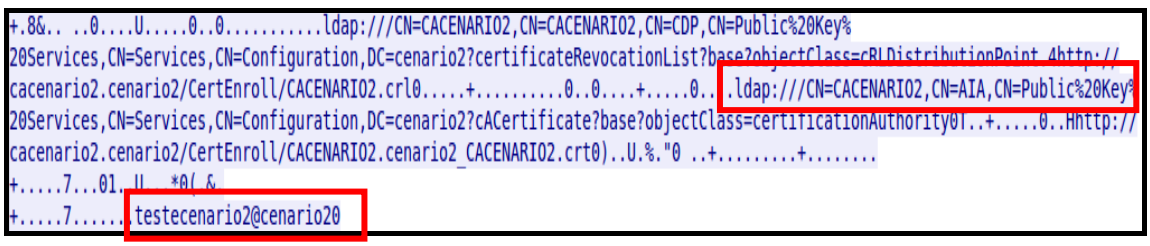
O resultado do teste cenário2 com autenticação TLS é mostrado a seguir: podemos ver o tempo exato da finalização dos pacotes envolvidos na autenticação.



No.	Time	Source	Destination	Protocol	Info
532	87.596979	192.168.0.30	192.168.0.20	TCP	[TCP Dup ACK 531#1] ldap > hpvmmcontrol [ACK] Seq=2630 Ack=1769 Win=64008 Len=0
533	87.597008	192.168.0.30	192.168.0.20	TCP	ldap > availant-mgr [ACK] Seq=4666 Ack=2369 Win=63581 Len=0
534	87.597014	192.168.0.30	192.168.0.20	TCP	[TCP Dup ACK 533#1] ldap > availant-mgr [ACK] Seq=4666 Ack=2369 Win=63581 Len=0
535	87.597032	192.168.0.30	192.168.0.20	TCP	ldap > hpvmmcontrol [FIN, ACK] Seq=2630 Ack=1769 Win=64008 Len=0
536	87.597039	192.168.0.30	192.168.0.20	TCP	ldap > hpvmmcontrol [FIN, ACK] Seq=2630 Ack=1769 Win=64008 Len=0
537	87.597056	192.168.0.30	192.168.0.20	TCP	ldap > availant-mgr [FIN, ACK] Seq=4666 Ack=2369 Win=63581 Len=0
538	87.597063	192.168.0.30	192.168.0.20	TCP	ldap > availant-mgr [FIN, ACK] Seq=4666 Ack=2369 Win=63581 Len=0

Figura 23 TEMPO EM SEGUNDOS GASTO NO PROCESSO DE AUTENTICAÇÃO EAP DO CLIENTE DO CENNARIO2 FONTE: O AUTOR.

Na próxima figura é mostrado um fragmento do pacote 538 envolvido no processo de autenticação com certificado digital.



```
+.8&.. ..0....U.....0..0..........ldap:///CN=CACENARIO2,CN=CACENARIO2,CN=CDP,CN=Public%20Key%
20Services,CN=Services,CN=Configuration,DC=cenario2?certificateRevocationList?base?objectClass=cRLDistributionPoint.4http://
cacenario2.cenario2/CertEnroll/CACENARIO2.crl0.....+.........0..0....+.....0..ldap:///CN=CACENARIO2,CN=AIA,CN=Public%20Key%
20Services,CN=Services,CN=Configuration,DC=cenario2?cACertificate?base?objectClass=certificationAuthority0I..+.....0..Hhttp://
cacenario2.cenario2/CertEnroll/CACENARIO2.cenario2_CACENARIO2.crt0)..U.%."0 ..+.........+........
+.....7...01..U...*0( &
+.....7.....testecenario2@cenario20
```

Figura 24 FRAGMENTO DO PACOTE 538 ENVOLVIDO NO PROCESSO DE AUTENTICAÇÃO TLS CLIENTE DO CENARIO2 FONTE: O AUTOR

Foram realizadas 10 tentativas sendo que as três primeiras foram descartadas conforme mostrado na tabela abaixo:

Medidas CENARIO2	1	2	3	4	5	6	7	Média
Tempo autenticação em segundos com EAP protegido	87,81	88,20	88,11	88,45	88.61	87.90	88.14	88,14
Tempo autenticação em segundos com TLS	87,31	87,22	87,44	87.23	87.89	87.59	87.55	87,32

Figura 25 TEMPO MÉDIO DE AUTENTICAÇÃO CENARIO2 FONTE: AUTOR

Podemos verificar nos testes realizados no cenario2 que o tempo gasto no processo de autenticação utilizando certificação digital tanto para EAP protegido como para TLS se mostrou bem maior que o tempo para autenticação sem uso desta técnica. No próximo item veremos a taxa (*throughput*) na qual os pedidos de autenticação são atendidos.

6.1.4 VAZÃO/TAXA (*THROUGHPUT*):TAXA NA QUAL OS PEDIDOS DE AUTENTICAÇÃO SÃO ATENDIDOS (SERVIDOS) PELO SISTEMA.

Para essa medida foi utilizado o software Wireshark escutando na interface de rede eth1 do Ubuntu que fornece infra estrutura para as Vm´s. Também foi gerado gráficos de ocupação de banda utilizando o software NTOP. Os resultados são mostrados em seqüência. As medidas dos cenários1 e cenario2 tomou como referência o tempo médio dotal envolvido no processo de autenticação colhido no experimento anterior. Dessa forma foi adicionada uma margem de erro de 2 segundos em cima do valor médio colhido no experimento anterior. Portanto o tempo destinado ao teste cenário1, para medida de taxa efetiva de dados durante o processo de autenticação, foi 15 segundos. Já o tempo de medida para o cenario2 foi de 90 segundos para o teste usando TLS. Como os tempos de autenticação EAP e TLS são muito

próximos o teste de vazão foi realizado apenas com autenticação utilizando EAP para o cenario2.

6.1.4.1 MEDIDA REFERENTE AO CENARIO1

No cenário1 foram capturados 433 pacotes em um tempo de 12 segundos. No total foram 8434.199 bytes por segundo conforme figura abaixo.

Traffic	Captured	Displayed
Packets	433	433
Between first and last packet	12,912 sec	
Avg. packets/sec	33,536	
Avg. packet size	251,499 bytes	
Bytes	108899	
Avg. bytes/sec	8434,199	
Avg. MBit/sec	0,067	

Figura 26 TRÁFEGO DE DADOS CAPTURADO NO PROCESSO DE AUTENTICAÇÃO CENARIO1 FONTE: AUTOR.

Com ajuda do software NTOP, podemos ver na figura abaixo a taxa de transmissão e recepção de pacotes envolvidos na autenticação.

Network Throughput: Local Hosts - Data Sent+Received

Host	Domain	Data			Packets		
		Current	Avg	Peak	Current	Avg	Peak
server-dominio.cenario1.com		20.1 Kbit/s	0.0 bit/s	20.1 Kbit/s	10.1 Pkt/s	0.0 Pkt/s	10.1 Pkt/s
testecenario1 [NetBIOS]		20.1 Kbit/s	0.0 bit/s	20.1 Kbit/s	10.1 Pkt/s	0.0 Pkt/s	10.1 Pkt/s
192.168.0.1		0.0 bit/s	0.0 bit/s	0.0 bit/s	0.0 Pkt/s	0.0 Pkt/s	0.0 Pkt/s

Figura 27 TAXA DE TRANSMISSÃO E RECEPÇÃO CENARIO1 FONTE: AUTOR.

O resultado da taxa de vazão local ficou em torno de 20.1kbits/s. Já a taxa de vazão da interface eth1 do Ubuntu que dá suporte ao cenário1 foi de 21,8k conforme figura abaixo.

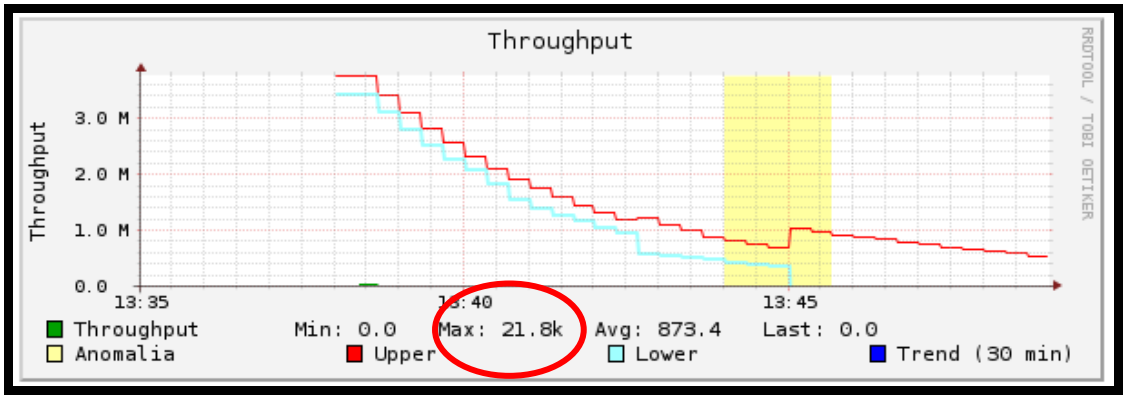


Figura 28 TAXA DE TRANSMISSÃO E RECEPÇÃO GERAL DA INTERFACE ETH1 DO UBUNTU QUE DÁ SUPORTE AO CENARIO1 FONTE: AUTOR.

6.1.4.2 MEDIDA REFERENTE AO CENARIO2

No cenário2 foram capturados 679 pacotes em um tempo de 88,454 segundos. No total foram 3117,859 bytes por segundo conforme figura abaixo.

Traffic	Captured	Displayed	Marked
Packets	679	679	0
Between first and last packet	88,454 sec		
Avg. packets/sec	7,676		
Avg. packet size	406,165 bytes		
Bytes	275786		
Avg. bytes/sec	3117,859		
Avg. MBit/sec	0,025		

Figura 29 TRÁFEGO DE DADOS CAPTURADO NO PROCESSO DE AUTENTICAÇÃO CENARIO2 FONTE: AUTOR.

Com ajuda do software NTOP, podemos ver na figura abaixo a taxa de transmissão e recepção de pacotes envolvidos na autenticação.

Network Throughput: Local Hosts - Data Sent+Received

Host	Domain	Data			Packets		
		Current	Avg	Peak	Current	Avg	Peak
servdomcert.cenario2		4.5 Kbit/s	9.5 Kbit/s	4.5 Kbit/s	1.7 Pkt/s	4.6 Pkt/s	1.7 Pkt/s
192.168.0.1		0.0 bit/s	9.8 bit/s	0.0 bit/s	0.0 Pkt/s	0.0 Pkt/s	0.0 Pkt/s
192.168.0.20		3.7 Kbit/s	9.1 Kbit/s	3.7 Kbit/s	1.2 Pkt/s	4.4 Pkt/s	1.2 Pkt/s
192.168.0.40		813.3 bit/s	403.3 bit/s	813.3 bit/s	0.5 Pkt/s	0.3 Pkt/s	0.5 Pkt/s

Figura 30 TAXA DE TRANSMISSÃO E RECEPÇÃO CENARIO2 FONTE: AUTOR.

O resultado da taxa de vazão local ficou em torno de 4.5kbits/s. Já a taxa de vazão da interface eth1 do Ubuntu que dá suporte ao cenário1 foi de 10,3k conforme figura abaixo.

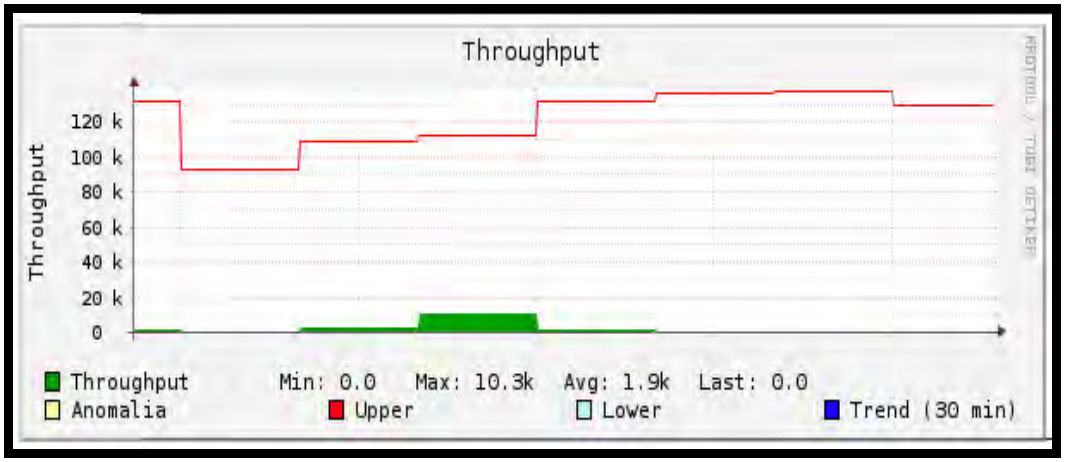


Figura 31 TAXA DE TRANSMISSÃO E RECEPÇÃO GERAL DA INTERFACE ETH1 DO UBUNTU QUE DÁ SUPORTE AO CENARIO2 FONTE: AUTOR.

Como o tempo total de autenticação utilizando certificados é da ordem de 88 segundos a distribuição dos bits nesse tempo cai bastante em relação ao cenario1 onde o tempo médio de autenticação é de aproximadamente 12 segundos.

CONCLUSÃO

Com os resultados obtidos pode-se concluir que mesmo utilizando autenticação EAP TLS com reconexão rápida, houve uma elevada diferença entre o total de dados enviados, aproximadamente 60% a mais do que o cenário 1 sem utilização de certificados.

Foi verificado na prática que a adoção de autenticação usando certificados como um mecanismo de segurança gera uma sobrecarga de pacotes, devido à inserção de tráfego extra para autenticação dos usuários. É possível inferir que em um ambiente com dezenas de máquinas se autenticando ao mesmo tempo consumiria muita banda da rede impactando de forma contundente o desempenho da rede. Os resultados apresentados mostram que esta sobrecarga é considerável, dependente do mecanismo adotado e deve ser levada em conta na decisão de qual modelo de autenticação a ser adotado. Outra consideração importante na implementação de serviço de autenticação, usando certificados, é que as máquinas clientes necessitam ser configuradas manualmente uma a uma, trazendo com isso um custo operacional considerável se a rede corporativa possuir muitas máquinas cliente. No planejamento de uma rede corporativa LAN (*Local área Networking*) deve-se avaliar o quanto o mecanismo adotado irá influenciar e comprometer a performance da rede. Caberá ao projetista e administrador da rede decidir pela utilização ou não de uma infra estrutura de chaves públicas para conferir autenticação e ou criptografia de dados.

SUGESTÃO DE TRABALHOS FUTUROS

Ainda tem-se uma ampla gama de testes que devem ser feitos que possam contribuir ainda mais com as conclusões chegadas com este trabalho, entre eles:

Realizar um estudo estatístico em um cenário com mais máquinas envolvidas a fim de determinar com precisão a quantidade de máquinas suportada em uma determinada infra-estrutura de rede.

Confrontar os dados obtidos comparando com cenários utilizando outros sistemas operacionais.

REFERÊNCIAS BIBLIOGRÁFICA

ANTÔNIO, Pedro. D, Resende. **Criptografia e segurança na Informática**: Copy Market, 1998.

WILLIAM, Stalling. **Criptografia e segurança de rede** 4º : PEARSON Printece Hall. São Paulo, 2008

EMILIANO, S.Monteiro, Maria Eloisang. **Certificados Digitais** 1º : BRASPORT. Rio de Janeiro, 2007.

ITI BRASIL. Instituto Nacional de Tecnologia da Informação – ITI. **O que é Certificação Digital?** Disponível em: http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf Acesso em: 03 março. 2009.

RNP . Escola superior de redes RNP. **Curso de Introdução a segurança de Redes Módulo I,** 2007.

IBM. **Certificados digitais**. Disponível em: <http://publib.boulder.ibm. com/tividd/td/TRM/GC32-1323-00/pt_BR/HTML/admin230.htm>. Acesso em: 15 Abril. 2009.

CERT.BR. **Cartilha de Segurança para Internet**. Disponível em: <http://cartilha.cert.br>. Acesso em: 10 Abril. 2009.

CAIXA.**Certificado digital** :< http://www.iti.gov.br/twiki/pub/ Certificacao/CartilhasCd/brochura01.pdf >. Acesso em: 19 Março. 2009.

TECNET. http://technet.microsoft.com/pt-br/library/cc759575.aspx . Acesso em: 19 Março. 2009.

INFOWESTER. http://www.infowester.com/noticias/iti-negocia-inclusao-da-icp-brasil-em-navegadores-de-internet/. Acesso em: 9 Maio. 2009.

CERTSIGN. https://www.certisign.com.br/certinews/banco_noticias/2008 /11/metade-das-universidades-do-pais-podera-ter-certificado-digital-em-2009. Acesso em: 30 Março. 2009.

WILLEY & CASAD, Joe. **Aprenda em 24 Horas TCP/IP**: Rio de Janeiro, Campus, 1999.

BURNETT, Steve & Paine Stephen. **Criptografia e segurança** – O guia oficial RSA: Rio de Janeiro, Campus, 2002.

CASAD, Joe. Sams **Teach Yourself TCP/IP in 24 Hours**.Third edition: Sams Publishing 800 East 96th Street Indianapolis, IN 46240 USA, 2003

CLARK, David & al.**Computers at Ris**k: Safe Computing in the Information National Academy Press 2101 Constitution Avenue, N.W. Washington, D.C. 20418 ,1991

KERLINGER. Fred N. **Metodologia da Pesquisa em Ciências Sociais**: um Tratamento Conceitual. São Paulo: EPU, 1980. 386 p. il.

HOPPEN, Norberto; LAPOINTE, Liette; MOREAU, Eliane. **Um Guia para Avaliação de Artigos de Pesquisa em Sistemas de Informação**. Porto Alegre: PPGA-UFRGS, 1996. 18 p. Série Documentos para estudo.

TANENBAUM, Andrew S. **Redes de Computadores**: Rio de Janeiro, Campus, 2003.

STALLING, WILLIAM. **Criptografia e segurança de redes** – Princípios e Práticas. 4º Edição. São Paulo. PEARSON, 2008.

BERKOVITS, S., CHOKHANI, S., FURNLONG, J. A., GEITER, J. A. and GUID, J. C. **Public Key Infrastructure Study**: Final Report, MITRE Corporation, abril de 1994

RFC 2246 –The TLS Protocol Version 1.0: Disponível em: http://www.ietf.org/rfc/rfc2246.txt 01/01/2009 a 30/04/2009

RFC 2401 – Security Architecture for Internet Protocol :Disponível em: http://www.ietf.org/rfc/rfc2401. tx, 01/01/2009 a 30/04/2009

RFC 2402 – IP Authentication Header: Disponível em: <http://www.ietf.org/rfc/rfc2402.txt>, 01/01/2009 a 30/04/2009

RFC 2403 – The Use of HMAC–MD5 within ESP and AH: Disponível em: <http://www.ietf.org/rfc/rfc2403.txt> 01/01/2009 a 30/04/2009

RFC 2404 – The Use of HMAC–SHA–1 within ESP and AH: Disponível em: <http://www.ietf.org/rfc/rfc2404.txt> 01/01/2009 a 30/04/2009

RFC 2406 – IP Encapsulating Security Payload: Disponível em: <http://www.ietf.org/rfc/rfc2406.txt> 01/01/2009 a 30/04/2009

RFC 2409 – The Intenet Key Exchange (IKE) : Disponível em: <http://www.ietf.org/rfc/rfc2409.txt> 01/01/2009 a 30/04/2009

RFC 2460 – Internet Protocol, Version 6 (IPv6) Specification: Disponível em: http://www.ietf.org/rfc/rfc2460.txt> 01/01/2009 a 30/04/2009

RFC 2818 – HTTPOverTLS: Disponível em: http://www.ietf.org/rfc/rfc2818.txt 01/01/2009 a 30/04/2009

RFC 826 – An Ethernet Address Resolution Protocol: Disponível em: <http://www.ietf.org/rfc/rfc826.txt> 01/01/2009 a 30/04/2009

RFC 903 – Bootstrap Loading using TFTP: Disponível em: <http://www.ietf.org/rfc/rfc903.txt> 01/01/2009 a 30/04/2009

GLOSSÁRIO

A

ALGORITMO – Operações elementares ordenadas em seqüência que devem ser efetuadas para se obter um resultado desejado. Por exemplo, uma receita de bolo é um algoritmo.

AUTENTICAÇÃO – O processo de determinar a identidade de uma entidade que esteja tentando se comunicar com outra entidade.

AUTENTICAR – Verificação da identidade de um usuário, de dispositivo, ou de outra entidade em um sistema computadorizado.

AUTORIDADE CERTIFICADORA – Entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

B

BLOWFISH - É uma cifra simétrica de blocos que pode ser usado em substituição ao DES ou IDEA. RC5-R16-B64-CBC

C

CHAVE – Em um sistema de encriptação, corresponde a um nome, uma palavra, uma frase, que permite, mediante o algoritmo de encriptação, cifrar ou decifrar uma mensagem.

CHAVE PRIVADA – Uma chave criptográfica secreta.

CHAVE PÚBLICA – Uma chave criptográfica disponível publicamente.

CERTIFICADO DIGITAL – Arquivo eletrônico, assinado digitalmente, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade.

CRIPTOGRAFIA – Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade

de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

I

INTEGRIDADE – A condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas. Garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.

IKE - É um modo de troca de chaves para ISAKMP

M

MD5 – Algoritmo seguro de hash criado por Ron Rivest. Message Digest Algorithm.

N

NÃO REPÚDIO – Não poder negar a autenticidade de um documento, a sua assinatura ou o seu envio.

P

PASSWORD – Veja "Senha".

R

REPÚDIO – Veja "Não Repúdio".

RSA – Algoritmo de cifragem por chave pública utilizado principalmente na cifragem da assinatura, permitindo a identificação do documento. Permite criptografar dados, criar e verificar assinaturas digitais.

S

SENHA – Uma única palavra ou seqüência de caracteres usada para autenticar uma identidade.

SIGILO – Somente os usuários autorizados têm acesso à informação.

SIMÉTRICO – Algoritmo de criptografia que usa somente uma chave, tanto para criptografar como para decriptografar.

SSL (Secure Sockets Layer) – Protocolo que possibilita realizar comunicações seguras através de criptografia e autenticação.