

**FACULDADE DE TECNOLOGIA DE JOÃO PESSOA – FATEC
CURSO DE PÓS-GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO**

FÁBIO FALCÃO DE FRANÇA

**ESTUDO DE CASO SOBRE A UTILIZAÇÃO DE VPNS
REDUNDANTES EM UM AMBIENTE CRÍTICO DE ALTA
DISPONIBILIDADE**

JOÃO PESSOA - PB

2010

FÁBIO FALCÃO DE FRANÇA

**ESTUDO DE CASO SOBRE A UTILIZAÇÃO DE VPNS
REDUNDANTES EM UM AMBIENTE CRÍTICO DE ALTA
DISPONIBILIDADE**

Estudo de caso apresentado ao Curso de Especialização em Segurança da Informação da Faculdade de Tecnologia de João Pessoa - FATEC, como pré-requisito para obtenção do grau de Especialista em Segurança da Informação. Orientador: Prof. Esp. Gerson Domingos de Castro Filho

JOÃO PESSOA - PB

2010

FICHA CATALOGRÁFICA
Dados de Acordo com AACR2, CDU e CUTTER
Biblioteca Central - FATEC

F814e FRANÇA, Fábio Falcão
Estudo de Caso Sobre a Utilização de VPNs
Redundantes em um Ambiente Crítico de Alta
Disponibilidade/Fábio Falcão de França – João Pessoa PB,
2010.
55 fls.

Orientador: Prof. Esp. Gerson Domingos de Castro Filho
Monografia Especialização em Segurança da Informação

1. Segurança da Informação. 2. VPN. 3. Transações
Financeiras.

I.Título II. Faculdade de Tecnologia de João Pessoa-
FATEC

FATEC/BC

CDU: 004

Ficha Catalográfica Elaborada pelo Setor de Processos
Técnicos da FATEC

FÁBIO FALCÃO DE FRANÇA

**ESTUDO DE CASO SOBRE A UTILIZAÇÃO DE VPNS
REDUNDANTES EM UM AMBIENTE CRÍTICO DE ALTA
DISPONIBILIDADE**

Estudo de caso apresentado ao Curso de Especialização em Segurança da Informação – Faculdade de Tecnologia de João Pessoa, como pré-requisito para obtenção do grau de Especialista em Segurança da Informação. Apreciada pela Banca Examinadora composta pelos seguintes membros:

- Aprovado
 Reprovado

Data / /

Prof. Esp. Gerson Domingos de Castro Filho
Orientador

Prof. Ms. Jorge Loureiro Dias
Examinador

Dedico este trabalho a Deus, ao meu pai e ao meu grande amigo Gerson de Castro, todos verdadeiros pais para mim. Dedico também a todos aqueles que me apoiaram durante mais essa etapa de minha vida, professores, amigos, vocês foram e sempre serão importantes.

AGRADECIMENTOS

Agradeço o apoio dos meus amigos, que por vários momentos demonstraram confiança e apoio no projeto, pois sem esta força, com certeza não obteria êxito no mesmo. Agradeço também ao apoio especial de Mariana Fernandes e Thaís Gaudêncio, ambas demonstraram bastante paciência e amizade no momento que eu mais precisei, saibam que hoje vocês simbolizam o termo amizade no sentido mais literal possível. Da mesma forma aos meus amigos mais próximos, Urias, Roosevelt, Vinícius, Fábio Nicácio, Evilásio, aquele abraço e obrigado por sempre participarem dos momentos bons e ruins da minha vida. Um agradecimento especial também ao meu pai, por ignorar o som alto durante a madrugada nos momentos de inspiração no projeto. Por fim, não menos importante, agradeço ao Prof. Cândido do Egypto pelo apoio, paciência e atenção com a minha pessoa, desde os tempos de Unipê até os dias de hoje, muito obrigado.

RESUMO

Esse trabalho possui como foco a realização de um estudo de caso sobre a construção de um ambiente utilizando VPNs redundantes em um ambiente crítico e de alta disponibilidade. Podemos descrever o ambiente citado como crítico por se tratar da captura e autorização de transações financeiras, operações estas que requerem um elevado nível de segurança e disponibilidade. Por conter essas características, este ambiente é propício à aplicação dos conceitos de segurança da informação, dada a criticidade e a necessidade de um mecanismo que garanta a alta disponibilidade do mesmo. Nesse estudo de caso, será demonstrado a implantação de túneis VPN redundantes, utilizados para realizar a transmissão de transações financeiras de maneira segura, por utilizar algoritmos de criptografia e autenticação das transações para prover a integridade e autenticidade dos dados ali trafegados. Esta estrutura será sempre referenciada aos pilares da segurança da informação, uma vez que a confidencialidade, integridade e disponibilidade das informações que trafegarão nesta estrutura serão cruciais para o estabelecimento da mesma em um ambiente de produção. Para isso foram utilizadas ferramentas *open source* capazes de implementar os conceitos da segurança da informação sempre referenciados neste estudo de caso, estabelecendo uma correlação entre eles. É de fundamental importância neste estudo, demonstrar como esses conceitos inferem sobre a implementação e o resultado final deste ambiente, especificando a relevância deles em um ambiente de produção corporativo. Por fim, serão demonstrados os resultados da utilização deste ambiente e o retorno sobre o investimento aqui aplicado.

Palavras chave: Segurança da informação, VPN, transações financeiras

ABSTRACT

This work has focused the achievement of a case study about the building of an environment using redundant VPNs in a critical and high availability. Because it contains these features, this environment is conducive to the implementation of security information concepts, given the critically and the need of a mechanism to ensure high availability of the same. In this case study, it will demonstrated the implementation of redundant VPN tunnels, used for transmission of secure financial transactions, by using one encryption algorithm of information and other to provide the authenticity of the data that travel over there. This structure will always be referenced to the pillars of the information security, once the confidentiality, integrity and availability of the information in which will travel in this structure, will be crucial for the establishment of such a production environment. To this, it was used open source tools capable of implementing the concepts referenced in this case study, establishing a correlation between them. It is of fundamental importance in this study, demonstrate how these inferred concepts about the implementation and the final result of this environment, specifying their relevance in a corporate production environment. Finally, the results of the utilization of this environment and the return on the investment here applied will be demonstrated.

Key words: Information Security; VPN; Financial transaction.

LISTA DE ILUSTRAÇÕES

Figura 1 – Pilares da segurança da informação	18
Figura 2 - Comparação entre o modelo OSI e TCP/IP.	21
Figura 3 - Formato do datagrama IPv4	21
Figura 4 - Representação do protocolo IPSec	22
Figura 5 - Exemplo da estrutura de VPN client-to-gateway	29
Figura 6 - Exemplo da estrutura de VPN gateway-to-gateway	30
Figura 7 - Estrutura do protocolo AH	31
Figura 8 - Estrutura do protocolo ESP	32
Figura 9 - Método Diffie-Hellman.....	35
Figura 10 - Visão geral do serviço prestado no cenário.....	36
Figura 11 - Caminho percorrido pelas transações	38
Figura 12 - Representação da estrutura entre autorizador e gateways VPN	42
Figura 13 - Caminho percorrido através do túnel VPN com as interfaces.....	50
Figura 14 - Tráfego na porta 4000 nas interfaces do túnel.....	51

LISTA DE TABELAS

Tabela 1 - Família SHA com suas variantes	34
Tabela 2 - Estrutura do estudo de caso	37
Tabela 3 - Requisitos especificados pelo cliente	40
Tabela 4 - Requisitos mínimos para estabelecimento das conexões	41

LISTA DE ABREVIATURAS E SIGLAS

VPN - *Virtual Private Network*

IP – *Internet Protocol*

IPSec – *IP Security Protocol*

OSI – *International Organization for Standardization*

IEC – *International Eletrotechnical Comission*

TCP – *Transmission Control Protocol*

OSI - *Open Systems Interconnection*

DNS – *Domain Name System*

UDP – *User Datagram Protocol*

IEEE – *Institute of Electrical and Electronics Engineering*

IETF – *Internet Engineering Task Force*

PDU – *Protocol Data Unit*

IPv4 – *Internet Protocol Version 4*

SQL – *Structured Query Language*

SSH – *Secure Shell*

SMTP – *Simple Mail Transfer Protocol*

HTTP – *HyperText Transfer Protocol*

POP3 – *Post Office Protocol Version 3*

IMAP – *Internet Message Access Protocol*

LDAP – *Lightweight Directory Access Protocol*

WAN – *Wide Area Network*

TEF – *Transferência Eletrônica de Fundos*

CC – *Compiler Collection*

GCC – *GNU Compiler Collection*

SUMÁRIO

1 INTRODUÇÃO.....	14
1.1 Objetivos.....	15
1.1.1 Objetivo Geral.....	15
1.1.2 Objetivos específicos.....	15
1.2 Estrutura do trabalho	15
1.3 Metodologia de pesquisa	16
2 FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO	17
2.1. Conceitos de segurança da informação	17
2.2 Pilares da segurança da informação	17
2.2.1 Confidencialidade	17
2.2.2 Integridade	17
2.2.3 Disponibilidade	18
2.3 Protocolos de rede.....	18
2.3.1 Modelo TCP/IP	18
2.3.2 Protocolo IP	21
2.4 Protocolo IPSec.....	22
2.4.1 Definição	22
2.4.2 Segurança.....	23
2.4.3 Associação de Segurança (SA).....	23
3 SOLUÇÕES DE ACESSO REMOTO	24
3.1 Características	24
3.1.1 Escalabilidade	24
3.1.2 Segurança.....	24
3.1.3 Retorno do investimento.....	26
3.2 Aplicações de acesso remoto corporativas	26
3.2.1 STunnel.....	26
3.2.2 OpenSwan.....	27
3.3 Redes virtuais privadas (VPN)	27
3.3.1 Conceitos básicos	27
3.3.2 Características	28
3.4 Tipos de VPN.....	29
3.4.1 <i>Client-to-gateway</i>	29
3.4.2 <i>Gateway-to-gateway</i>	29
3.5 Técnicas de criptografia e autenticidade	30
3.5.1 Authentication Header (AH).....	30
3.5.2 <i>Encapsulation Security Payload (ESP)</i>	31
3.6 Principais algoritmos de criptografia utilizados em VPN	32
3.6.1 <i>Triple Data Encryption Standard (3DES)</i>	32
3.6.2 <i>Advanced Encryption Standard (AES)</i>	33
3.7 Principais algoritmos de autenticidade utilizados em VPN	34
3.7.1 <i>Message-Digest algorithm (MD5)</i>	34
3.7.2 <i>Secure Hash Algorithm (SHA-1)</i>	34
3.8 Método para trocas de chaves <i>Diffie-Hellman</i>	35
4 ESTUDO DE CASO.....	36
4.1 Estrutura do estudo de caso	36
4.2 Motivação	37

4.3 Benefícios	39
4.4 Análise de requisitos da infra-estrutura.....	40
4.5 Implantação.....	41
4.5.1 Planejamento.....	41
4.5.2 Execução.....	47
4.5.3 Homologação e testes.....	50
4.6 Resultados obtidos	51
5 CONCLUSÃO.....	53
REFERÊNCIAS.....	55

1 INTRODUÇÃO

Na última década, têm-se percebido o aumento da preocupação das organizações de um modo geral com a informação, independentemente do segmento das mesmas. Ao se tratar do segmento financeiro, esta preocupação aumenta vertiginosamente, tendo em vista que quaisquer falhas podem representar uma queda eminente nas ações e faturamento da organização, além de afetar diretamente a imagem e integridade da mesma perante a sociedade e seus clientes. Uma pesquisa publicada pelo *Gartner Group* aponta uma tendência ao indicar que duas entre cinco organizações que enfrentam ataques ou danos em seus sistemas computacionais deixam de existir, entretanto, segundo a Academia Latino Americana de Segurança da Informação (BAUER, 2005), em um estudo publicado pela Universidade do Texas, apenas 6% das organizações que sofrem algum tipo de falha catastrófica de segurança em sistemas computacionais sobrevivem.

Seguindo este panorama, não seria exagero indicar a Segurança da Informação como um dos pontos cruciais para a existência de quaisquer organizações, uma vez que o repúdio a esta cultura dentro da organização pode trazer danos financeiros irreversíveis.

Quando esta preocupação abrange organizações que possuem parceiros fisicamente afastados, que participam e interferem ativamente nas informações utilizadas pelo negócio principal da organização, esta preocupação se torna ainda maior, uma vez que os pontos de possíveis falhas não estão apenas no escopo físico da mesma. É importante atentar para o fato de nenhum padrão ou modelo de segurança ser totalmente seguro, entretanto, eles devem existir exatamente para garantir a minimização dos impactos causados por possíveis falhas encontradas.

O presente estudo trata, especificamente, da realização de um estudo de caso que tem como enfoque principal a interconexão de duas organizações, utilizando a Internet como meio de comunicação para o transporte de transações financeiras, porém, utilizando protocolos seguros para roteamento e transporte das informações. Baseando-se nos pilares da segurança da informação, o objeto desse estudo foi construído a fim de prover a confidencialidade, integridade e disponibilidade das informações.

1.1 Objetivos

1.1.1 Objetivo Geral

Apresentar a implantação e validação da utilização de redes virtuais privadas (VPN) em um cenário de transações financeiras eletrônicas, através do desenvolvimento de um estudo de caso baseando-se nos pilares da segurança da informação: integridade, confiabilidade e disponibilidade.

1.1.2 Objetivos específicos

- Realizar um estudo sobre alguns dos principais algoritmos de criptografia e de autenticação;
- Descrever os fundamentos e evidenciar a utilização do método *Diffie-Hellman* para troca segura de chaves de criptografia;
- Apresentar o conceito de redes virtuais privadas (VPN), destacando a necessidade da utilização do protocolo *IPSec*, em substituição ao protocolo IP nesta tecnologia;
- Demonstrar os passos necessários para implantação de uma VPN usando o protocolo *IPSec*, através de um estudo de caso real;
- Apresentar um paralelo entre a utilização das conexões de redes virtuais privadas e os pilares da segurança da informação, citando os ganhos advindos da utilização das mesmas.

1.2 Estrutura do trabalho

Este trabalho será organizado em cinco capítulos. No capítulo introdutório, podemos encontrar um panorama geral da segurança da informação nas organizações, assim como a sua importância para a sobrevivência da mesma nos dias de hoje.

Com base no objetivo geral deste trabalho, no capítulo 2, descreveremos os fundamentos de segurança da informação que dão embasamento para os conceitos de segurança ali aplicados.

Por estarmos utilizando a criação de redes virtuais privadas como objeto principal deste trabalho, o capítulo 3 menciona e detalha as soluções de acesso remoto, seus princípios, conceitos e principais características.

No capítulo 4, já embasados sobre as tecnologias e métodos utilizados, descrevemos a construção do estudo de caso, objeto principal deste trabalho. Este capítulo está dividido em seis partes, que nos leva desde a motivação, benefícios, análise de requisitos para a implantação e os resultados obtidos a partir da homologação destas conexões no ambiente que fora apresentado.

1.3 Metodologia de pesquisa

Fora realizada para este trabalho uma pesquisa aplicada e exploratória sobre a utilização de redes virtuais privadas redundantes em um ambiente crítico de alta disponibilidade. Do ponto de vista dos procedimentos técnicos aqui apresentados, fora realizado um estudo de caso a fim de apresentar um estudo aprofundado sobre redes virtuais privadas, explicitando os benefícios advindos de sua utilização para aplicação dos conceitos e pilares da segurança da informação no ambiente aqui apresentado.

2 FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

Este capítulo tem por objetivo definir os fundamentos relacionados à segurança da informação necessários para o entendimento das atividades desenvolvidas neste estudo de caso.

2.1. Conceitos de segurança da informação

O conceito de segurança da informação está diretamente ligado ao manutenção do bem mais importante e fundamental de qualquer organização existente, que é como o próprio nome já diz a informação.

Partindo deste ponto de vista, tal conceito visa de maneira prioritária a proteção à confidencialidade, autenticidade e disponibilidade das informações.

Segurança da Informação, segundo a própria norma ISO/IEC 17799:2005, é caracterizada como um conjunto de princípios considerados críticos, com o intuito de preservar a proteção da informação. Princípios estes, essenciais e fundamentais para o estabelecimento de padrões de segurança.

2.2 Pilares da segurança da informação

2.2.1 Confidencialidade

Este é um princípio que descreve a garantia de que, uma informação será acessível apenas para os indivíduos autorizados. Em outras palavras, descreve que apenas as pessoas que devem acessar determinadas informações irão, de fato, acessá-las.

2.2.2 Integridade

Este princípio preza pela garantia da exatidão das informações a serem acessadas, assim como o acesso da mesma de forma íntegra e completa. Este conceito está diretamente ligado aos métodos de processamento e garantias que a mesma irá submeter-se. Em linhas gerais, trata-se de ter a certeza que a informação que fora gerada, será a mesma a ser acessada e utilizada.

2.2.3 Disponibilidade

Este princípio trata a garantia que o indivíduo terá de acessar as informações no momento em que necessitar, ou seja, garantirá que os mesmos estejam disponíveis sempre que necessário. Tal princípio também é largamente utilizado como indicador de nível de serviços de tecnologia em geral, uma vez que a sua porcentagem permite a medida do tempo disponível do serviço.

A **figura 1** exibe uma representação gráfica dos pilares da segurança da informação:



Figura 1 – Pilares da segurança da informação
Fonte: Adaptado de ALVES, Gustavo Alberto.

2.3 Protocolos de rede

2.3.1 Modelo TCP/IP

O modelo TCP/IP se baseia em uma pilha de protocolos que garantem a interoperabilidade de comunicação entre todos os tipos de hardware e de sistemas operacionais, aumentando assim o número de tipos de computadores que podem participar de uma determinada rede de computadores. Ele é constituído por quatro camadas que por sua vez possuem uma co-relação com o modelo OSI. São elas: aplicação, transporte, inter-rede e física. Porém, alguns autores costumam chamar a camada física, que de certa maneira contém a camada de enlace, apenas de tecnologias de transmissão, pois a junção dessas camadas tem por finalidade fazer a movimentação dos dados no meio físico, utilizando para isto dos

serviços prestados nas mesmas. [TANEBAUM, 1997]

- Aplicação: esta camada é a que está representada como a mais alta deste modelo, e por consequência apresenta os protocolos de níveis mais altos.
Segundo TANENBAUM, o modelo TCP/IP não possui as camadas de apresentação e de sessão, pois não foi percebida a necessidade de inclusão das mesmas. A prova disso foi a experiência com o modelo OSI, que demonstrou o pouco uso das mesmas pelas aplicações. Dentre os seus protocolos podemos citar o antigo protocolo de terminal virtual (TELNET), hoje já em desuso por não oferecer melhorias em segurança, o servidor de nomes de domínio (DNS), responsável pela tradução de nomes de *hosts* em seus respectivos endereços de rede e o Protocolo de Transferência de Hiper Texto, ou HTTP, responsável pela requisição/respostas de páginas na Internet. [TANEBAUM, 1997]
- Transporte: esta camada é responsável pelo estabelecimento da conversação entre dois *hosts* de uma rede. Assim como no modelo de referência OSI, esta também possui as funções de controle de congestionamento e controle de fluxo. Dois protocolos fim a fim foram aqui definidos, o primeiro deles é o protocolo de controle de transmissão (TCP). Este é um protocolo confiável e orientado a conexão, ou seja, ele se baseia na necessidade de um *handshake*¹ entre as partes para estabelecimento da conexão.. O segundo protocolo desta camada é o protocolo de datagrama de usuário (UDP), que ao contrário do TCP não é confiável, do ponto de vista de não necessitar do *handshake* para estabelecer uma conversação entre os *hosts* interessados. Este protocolo é bastante utilizado para aplicações que não necessitam do controle de fluxo e de congestionamento, como as aplicações de *streaming*, utilizadas hoje em larga escala na Internet para transmissão de vídeo e áudio em tempo real, ou sob demanda (*video on demand*²). [TANEBAUM, 1997]
- Inter-rede: sua principal função é garantir que os *hosts* enviem pacotes em qualquer rede e garantir que eles venham a ser transmitidos independentes até o destino, que pode ser a mesma rede, ou outra rede. Tais pacotes poderão até ser transmitidos em uma ordem diferente das que foram enviados, obrigando as camadas superiores a

¹ Espécie de acordo entre as partes envolvidas, tradução da expressão “aperto de mão” da língua inglesa.

² Solução de vídeo sobre xDSL, por meio de uma página web em um TV digital.

organizá-los a fim de um entendimento ao chegar à camada de aplicação. Assim como no modelo OSI é nesta camada que o processo de roteamento é estabelecido, porém naquele modelo ela é chamada apenas de camada de rede. A camada de inter-rede define um formato de pacote universal e um protocolo chamado IP (*Internet Protocol*). Este protocolo define o endereçamento lógico de *hosts* em uma rede de computadores. [TANEBAUM, 1997]

- Tecnologias de transmissão: alguns autores chamam a fusão destas duas camadas (enlace e física) apenas de física, outros preferem denominá-la de tecnologias de transmissão. O porquê dessa denominação está no simples fato destas duas camadas ao se fundirem, terem a função principal de receber os pacotes enviados pela camada de rede, encapsulá-los em um quadro seja ele de qualquer tecnologia e enviá-los usando o meio definido por esta tecnologia. Algumas tecnologias de transmissão utilizam o ar como meio físico, como o padrão IEEE 802.11³, outras utilizam cabeamento, como a *Ethernet*, *Token Ring*, ATM e X.25. O X.25 é uma tecnologia de transmissão que opera por comutação de pacotes e é largamente utilizada para transmissão de transações financeiras, pelo fato do baixo valor da contratação deste serviço junto às operadoras de telefonia. Esta tecnologia de transmissão é utilizada no percurso das transações financeiras evidenciadas neste trabalho, entretanto, não será amplamente detalhada. Cada tecnologia de transmissão tem um quadro que utiliza cabeçalhos diferentes para envio e recepção dos dados em seu meio. A explicação para isso é que diferentes variáveis são utilizadas pelas tecnologias para organizar, classificar, transmitir e receber seus dados. [TANEBAUM, 1997]

³ Padrão utilizado como base para descrever a tecnologia Wi-Fi.

A seguir, na **Figura 2**, é apresentada uma comparação entre o modelo OSI e o modelo TCP/IP, relacionando suas camadas equivalentes.

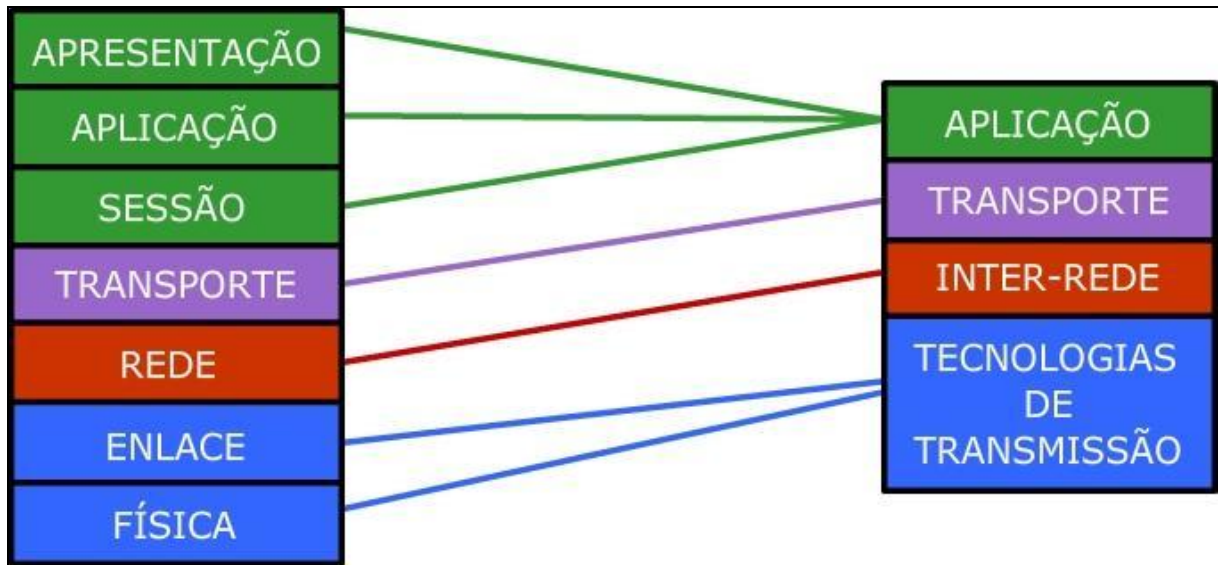


Figura 2 - Comparação entre o modelo OSI e TCP/IP

Fonte: Adaptada de TANENBAUM, Andrew S., Redes de Computadores, 1997.

2.3.2 Protocolo IP

Segundo a própria definição do IP (*Internet Protocol*), escrita em setembro de 1971 pelo Departamento de Defesa Americano (DoD) e padronizada pelo IETF, o protocolo IP foi escrito para o uso em sistemas de interconexão baseados redes de comunicação computacionais. O protocolo IP, segundo TANENBAUM(2003), é o ponto de partida apropriado para o estudo da camada de rede da Internet.

Na camada de rede, a *PDU* correspondente é o datagrama ou pacote IP. Nosso objeto de estudo aqui é o datagrama IPv4 apenas, por ter sido utilizado no estudo de caso de maneira plena.

O formato do datagrama IPv4 é exibido na figura 3:

VERSÃO	COMPRIMENTO DO CABEÇALHO	TIPO DE SERVIÇO	COMPRIMENTO DO DATAGRAMA	
IDENTIFICADOR DE 16 BITS		FLAGS	DESLOCAMENTO DE FRAGMENTAÇÃO (13 BITS)	
TEMPO DE VIDA	PROTOCOLO DA CAMADA SUPERIOR	SOMA DE VERIFICAÇÃO DO CABEÇALHO		
ENDEREÇO IP DE 32 BITS DA FONTE				
ENDEREÇO IP DE 32 BITS DO DESTINO				
OPÇÕES				
DADOS				

Figura 3 - Formato do datagrama IPv4

Fonte: James F. Kurose e Keith W. Ross. Redes de Computadores e a Internet (2005)

O protocolo IP executa o papel para o qual foi feito até hoje com perfeição, entretanto, ao passar do tempo e a medida que a necessidade de segurança foi crescendo, percebeu-se que estava cada vez mais difícil e dispendioso utilizar mecanismos de autenticação e criptografia em outras camadas para suprir a ausência da capacidade de utilização de controle de segurança nestes datagramas. Esta preocupação surgiu em 1992, dentro do IETF, órgão criado para definir padrões de segurança na área de Internet, que criou um subgrupo composto de engenheiros de segurança do IETF e representantes das maiores empresas de tecnologia e serviços de rede. [SILVA,2005]

2.4 Protocolo IPSec

2.4.1 Definição

O objetivo do grupo criado no IETF era criar um padrão para a conexão TCP/IP, que implementasse conceitos de integridade, autenticidade e privacidade, transparente e utilizando a estrutura de rede disponível, que até outrora não existira. Foi ai que surgiu o IPSec. Os documentos IPSec criados por este grupo, trazem três conceitos fundamentais para VPN, algoritmos de criptografia, algoritmos de autenticidade e gerência de chaves.

Segundo SILVA(2005), “o protocolo IPSec é um protocolo padrão para se estabelecer uma VPN entre dois pontos, independentemente do fabricante ou da aplicação envolvida.”. Em resumo, quaisquer softwares que implementem o protocolo IPSec são capazes de se comunicar e fechar conexões VPN com outros softwares que também façam uso do mesmo protocolo, sem a necessidade de quaisquer alterações em suas estruturas.

A **figura 4**, exibe a representação gráfica do protocolo IPSec:

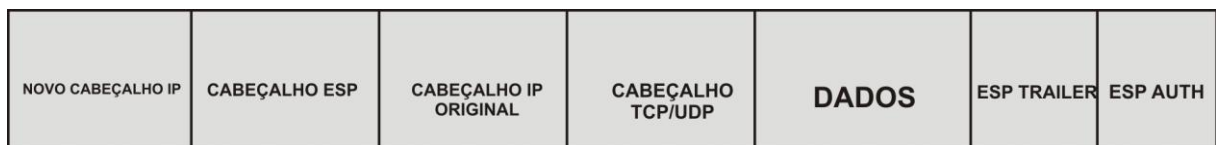


Figura 4 - Representação do protocolo IPSec

Fonte: Adaptada de James F. Kurose e Keith W. Ross. *Redes de Computadores e a Internet*(2005)

Com a criação do protocolo IPSec, cada servidor que tenha um software que implemente o protocolo é de fato, um gateway ou ponto de ligação de uma rede virtual privada (VPN). [SILVA, 2005]

2.4.2 Segurança

A segurança no protocolo IPSec é oferecida através de dois protocolos de segurança, o *Authentication Header* (Autenticação de cabeçalho – AH) e o *Encapsulation Security Payload* (Encapsulamento Seguro do Dado – ESP). Ambos serão detalhados de maneira aprofundada decorrer deste trabalho. [SILVA, 2005]

2.4.3 Associação de Segurança (SA)

Segundo SILVA (2005), *Security Association* é um dos conceitos fundamentais do IPSec, pois uma SA define os tipos de medidas de segurança nos quais a origem de envio dos pacotes deve se basear, além de definir o destino e o tipo de dado que está sendo transportado. Os serviços de segurança oferecidos pela associação de segurança vai depender do protocolo de segurança utilizado, assim como suas opções e o modo no qual a SA irá trabalhar.

Uma SA é identificada pelo endereço ip de destino, da identificação do protocolo de segurança usado, neste caso dois códigos são estabelecidos (51 se for utilizado o AH e 50 se for utilizado o ESP) e o Índice do parâmetro de segurança (*Security Parameter Index – SPI*).

O Índice SPI identifica uma SA e o mesmo é definido no momento em que ocorre a negociação que antecede o estabelecimento da SA em questão. Uma SA define apenas o endereço IP de destino, pois se trata de uma conexão unilateral. Caso ambos os lados desejem trocar informações, duas SA's deverão ser estabelecidas, uma para cada lado da conexão. Também durante este processo é definido quais serão as chaves e algoritmos de criptografia e autenticação que serão utilizados para realizar o estabelecimento da conexão VPN.

3 SOLUÇÕES DE ACESSO REMOTO

Uma solução de acesso remoto pode ser definida como um software, capaz de prover acesso a serviços entre dois ou mais hosts, separados fisicamente, fazendo com que os mesmos possam compartilhar serviços. Neste capítulo não abordaremos todas as soluções de acesso remoto disponíveis, mas sim, apenas as que serão relevantes como referências ao estudo de caso que será apresentado no capítulo 4.

3.1 Características

3.1.1 Escalabilidade

Uma solução de acesso remoto deverá garantir a escalabilidade da infra-estrutura na qual será implantada, uma vez que, a adição de novos pontos de expansão como filiais, escritórios ou mesmos *hosts*, deve ser tratada como um procedimento esperado e não deve apresentar grandes dificuldades. Esta característica está diretamente ligada ao retorno do investimento apresentado neste capítulo, pois, de acordo com a facilidade de escalar a infra-estrutura o custo irá subir consideravelmente, trazendo assim uma grande disparidade com o benefício que a mesma trará à instituição. [ALVES, 2006]

3.1.2 Segurança

Esta característica é a mais óbvia e trivial de todas, porém, devemos ter em mente a real importância da segurança em uma solução de acesso remoto. Dentro do contexto de segurança, podemos citar diversos elementos que compõem o cenário de segurança:

- **Ativo:** Um ativo pode ser definido como um elemento qualquer que representa valor para o negócio da empresa, ou seja, qualquer elemento que agrega algum peso para a atividade principal da empresa. Podemos citar como exemplos de ativos os próprios humanos, ou seja, funcionários da instituição que de alguma forma colaboram para o negócio no qual a mesma está inserida; Ativos tecnológicos, como por exemplo, um software ou hardware, usados de forma a agregar funções que lidem com o negócio principal da empresa; Ativos físicos, como por exemplo, os escritórios, filiais, setores, etc. [ALVES, 2006]

- Ameaça: Uma ameaça pode ser definida como uma causa potencial, capaz de ser responsável por um incidente qualquer de segurança, uma vez que as mesmas exploram possíveis falhas existentes, falhas estas chamadas de vulnerabilidades. [ALVES, 2006]

Uma ameaça pode ser apresentada de diversas maneiras, como por exemplo:

Hackers: segundo o site *linhade defensiva.org*, o termo hacker vem desde a década de 50, onde o mesmo era designado às pessoas que se interessavam pela era da informática. A palavra *hacker* vem do verbo em inglês “*to hack*”, ou seja, o ato de alterar algo pronto, funcional e torná-lo melhor.

Crackers: segundo o site *linhade defensiva.org*, o termo *cracker* designa as pessoas que usam seus conhecimentos avançados em informática, para corromper sistemas e conseguir de alguma forma usar essas informações em benefício próprio.

Agentes naturais: pode ser considerado um agente natural, quaisquer tipos de eventos que independam da ação natural do homem e que representem uma ameaça, como por exemplo, uma enchente, terremoto ou incêndio. [ALVES, 2006]

Vândalos: o termo vândalo, segundo a definição, pode ser designado àquelas pessoas que promovem ações motivadas pela hostilidade, contra uma arte, cultura, ou destruição intencional de bens ou propriedades alheias. [ALVES, 2006]

- Vulnerabilidades: Uma vulnerabilidade pode ser definida como uma/ou um conjunto de falhas capazes de serem exploradas por quaisquer tipos de ameaças. Em outras palavras, uma vulnerabilidade é um produto da exploração de uma ameaça qualquer, passível de causar danos a integridade da informação. Podemos citar alguns exemplos de vulnerabilidades:
 - a. Contas de usuário sem senha
 Esta vulnerabilidade parece ser aparentemente boba, porém, é comumente encontrada nas organizações, que resulta em prover acesso a terceiros, comumente não-autorizados nas

mesmas.[ALVES,2006]

b. Falhas no código do software

Esta vulnerabilidade permite inúmeras formas de exploração e apresentam um grande risco para a organização, porém, explorar tais vulnerabilidades não é trivial e requer um conhecimento avançado em programação e sistemas operacionais. Alguns exemplos de falhas no código podem gerar os famosos Buffer Overflow e Stack Overflow. [ALVES, 2006]

c. Injeção de código SQL

Esta vulnerabilidade é especificamente explorada em cima da linguagem SQL. Ela ocorre quando um código SQL é inserido em um sistema qualquer, onde este código inserido irá compor parâmetros de outra consulta SQL, previamente criada pelo programador. Esta vulnerabilidade poderá tanto afetar dados como até mesmo a estrutura do banco de dados em questão. [ALVES, 2006]

3.1.3 Retorno do investimento

Esta característica é de longe a mais importante no fim das contas, pois a mesma é influenciada por todas as outras características aqui citadas. Uma vez que o tipo de informação a utilizar a solução de acesso remoto de uma organização é apresentado e que, sua importância para o negócio é definida de maneira clara para os envolvidos, o retorno do investimento é indispensável para a decisão sobre a solução a ser utilizada na mesma. De uma forma literal, o retorno do investimento simboliza em curto, médio ou longo prazo, o quanto que a empresa transformará o que gastou em lucro. Em linhas gerais, o que a empresa ganhará em decorrência da solução escolhida a ser utilizada. [SANTOS, 2008]

3.2 Aplicações de acesso remoto corporativas

3.2.1 STunnel

STunnel é um software que permite encriptar arbitrariamente conexões TCP usando SSL (*Secure Socket Layer*).

SSL ou na sua tradução literal, camada de *sockets* segura, pode ser definida como um protocolo que provê segurança na comunicação pela Internet para serviços da camada de aplicação como SSH, SMTP e HTTP, entre outros. Este protocolo disponibiliza a integridade e privacidade de informações entre dois *hosts* através da autenticação dos mesmos e criptografia dos dados transmitidos entre eles.

O STunnel permite que *daemons* de serviços de protocolos normalmente não-criptados como POP3, IMAP, LDAP utilizem SSL para autenticação dos hosts envolvidos e encriptação dos dados trafegados entre os *hosts*. O STunnel está sob a licença GNU Public License, permitindo o seu uso para aplicações comerciais e não-comerciais.

3.2.2 OpenSwan

OpenSwan é uma aplicação *opensource* que implementa o protocolo IPSec, para estabelecimento de conexões VPN entre duas ou mais pontas, utilizando o sistema operacional Linux. O mesmo foi desenvolvido a partir do projeto FreeS/WAN, por desenvolvedores que trabalharam até o fim do projeto anterior. O protocolo IPSec, originalmente desenvolvido pela Microsoft, foi implementado em uma aplicação *opensource* inicialmente no projeto FreeS/WAN, porém este projeto foi descontinuado em 2003, por motivos políticos, uma vez que nos EUA algoritmos de encriptação com chaves fortes como o 3DES são proibidos de ser exportados por lei, por se tratar de algoritmos militares. Outra razão para o término do mesmo foi o fato de não ter sido escolhido como o software padrão do Linux para estabelecimento de conexões VPN.

O OpenSwan permite a utilização inúmeros algoritmos de integridade dos pacotes, como MD5, SHA-1, etc. assim como inúmeros algoritmos de criptografia, como 3DES, AES, Blowfish, Serpent, etc. Ele foi o software escolhido para o estabelecimento das conexões VPN, objeto desse estudo de caso.

3.3 Redes virtuais privadas (VPN)

3.3.1 Conceitos básicos

Segundo TANENBAUM(2003), VPNs (Virtual Private Network) são redes sobrepostas às redes públicas, mas com grande parte das características e propriedades de redes privadas. O fato de serem chamadas de virtuais se explica pelo fato de não serem

ligadas fisicamente, ou seja, depende de uma conexão virtual, temporária e sem presença física no meio.

Uma rede virtual privada (VPN) é uma das principais formas de unir diferentes redes de uma ou várias corporações, agregando propriedades de redes locais e utilizando um meio público para o estabelecimento da conexão e tráfego das informações, como a Internet. [CYCLADES,2000]

3.3.2 Características

As características desejáveis em uma VPN seguem as já definidas neste documento, características das soluções de acesso remoto em geral.

A escalabilidade de uma VPN é uma característica imprescindível e de certa forma sempre presente nas mesmas, pois permite que um host ou rede, se conecte a outra, trazendo um acréscimo significativo no tamanho de sua estrutura. Este acréscimo na infraestrutura é acompanhado da ausência de injeção financeira em infra-estrutura extra e ainda permite que usuários móveis sejam agregados à rede sem a necessidade de utilização de banco de modems e/ou servidores de acesso remoto. [SCRIMGER, 2002]

A segurança é uma característica intrínseca ao conceito de uma VPN, pois segundo a sua própria definição, utilizamos de um meio inseguro, porém, utilizando protocolos de segurança para prover um ambiente seguro em um meio que inicialmente não fora projetado para este fim. O *IPSec*, protocolo que encapsula o IP como uma camada de segurança, é o principal envolvido nessa característica no estabelecimento das conexões VPN. Ele provê a possibilidade de utilização de algoritmos de autenticação e criptografia sobre o protocolo IP, inicialmente desprovido dessa funcionalidade. [SILVA,2003]

O baixo custo e o alto índice de retorno do investimento fazem da utilização da VPN a principal alternativa para interligação de corporações fisicamente distantes, superando até mesmo o uso de conexões dedicadas, contratadas junto às empresas de telefonia. Segundo Cyclades (2000, p.167) “A principal motivação para a implementação de VPNs é financeira [...]”, além do mais, com o aumento progressivo da largura de banda da Internet comercial, este tipo de decisão tem se tornado cada vez mais unânime entre as organizações.

3.4 Tipos de VPN

Basicamente, existem dois tipos de VPNs: *client-to-gateway* e *gateway-to-gateway*.

3.4.1 *Client-to-gateway*

Neste tipo de VPN, um usuário móvel conecta a VPN, por intermédio de uma conexão de Internet qualquer, adsl, cabo, dsl, etc. e tem acesso a toda a infra-estrutura da rede interna da matriz na qual ele se conecta.

A **Figura 5** exibe um exemplo da estrutura utilizada por este tipo de VPN:

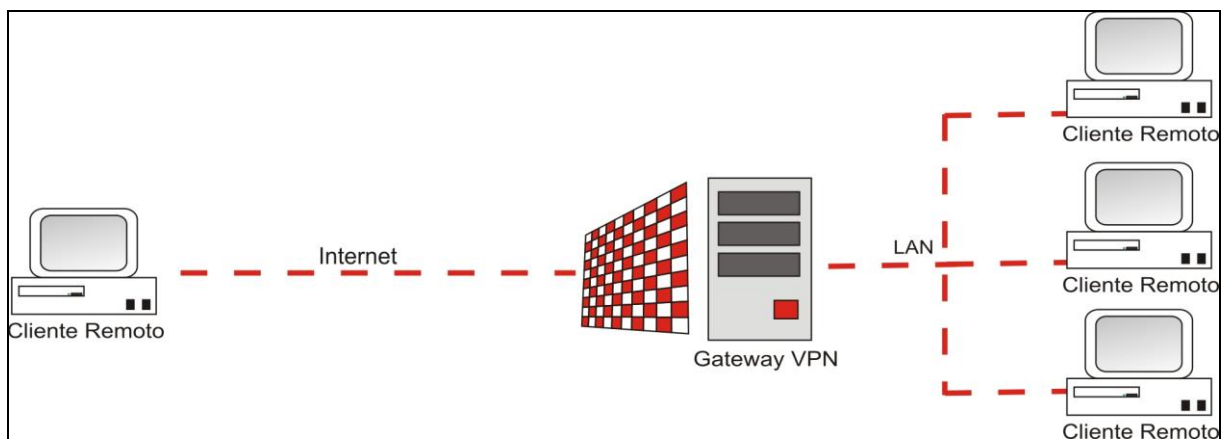


Figura 5 - Exemplo da estrutura de VPN client-to-gateway

Fonte: Adaptada de RESENDE & GEUS (2004)

3.4.2 *Gateway-to-gateway*

Neste tipo de VPN, uma rede de uma organização se interliga a outra rede, da mesma organização (como uma filial, por exemplo) ou de outra organização (como um parceiro, por exemplo), fazendo com que mais de um host de uma rede tenha acesso a mais de um host da outra rede. Desta forma, as redes irão trabalhar de forma virtual como se fosse apenas uma rede local e não duas fisicamente separadas.

A **Figura 6** demonstra um exemplo da estrutura *gateway-to-gateway*:

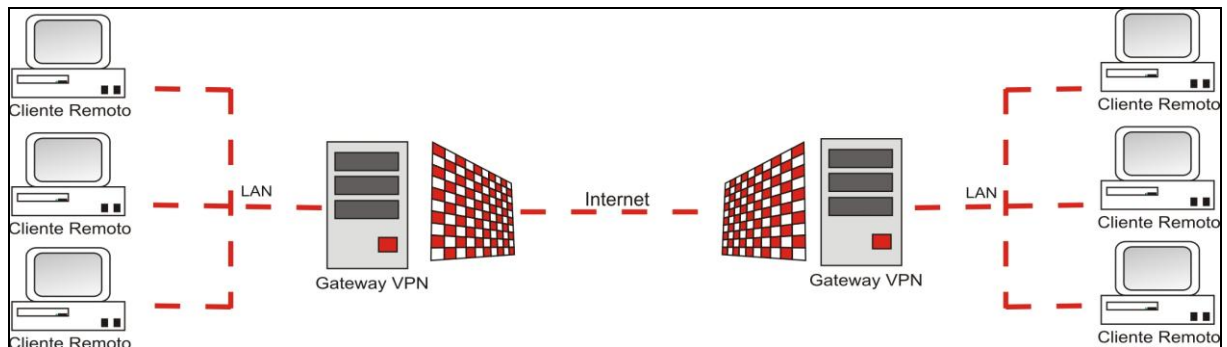


Figura 6 - Exemplo da estrutura de VPN gateway-to-gateway

Fonte: Adaptada de RESENDE & GEUS (2004)

3.5 Técnicas de criptografia e autenticidade

Os protocolos *Authentication Header(AH)* e *Encapsulation Security Payload(ESP)* fazem parte da arquitetura do IPSec e por questões de interoperabilidade, os mesmos estabelecem que quaisquer implementações do protocolo IPSec devem suportar um número mínimo de algoritmos predefinidos. No período referente a proposta do IPSec (1992), os algoritmos estabelecidos eram o DES e o 3-DES para criptografia dos pacotes e HMAC, MD5 e SHA-1 para autenticação das conexões. Essa lista continua obrigatória, porém, as várias implementações do IPSec ao redor do mundo, hoje implementam também vários outros algoritmos:

Criptografia: DES, 3-DES, Blowfish, CAST, AES, SERPENT, TWOFISH, etc.

Autenticação: HMAC, MD5, SHA-1, SHA-2

Tal lista poderá sofrer alterações ao longo do tempo, devido a quebra de algoritmos obsoletos e/ou criação de algoritmos mais seguros.

3.5.1 Authentication Header (AH)

Segundo SILVA(2005), o protocolo AH provê autenticação e integridade dos pacotes, garantindo assim a autenticidade do pacote e que o mesmo não fora modificado durante a transmissão. O protocolo AH previne três tipos de ataques clássicos, o *Replay*, *Spoofing* e o *Hijacking*. O ataque do tipo *Replay* acontece quando uma pessoa captura pacotes válidos e autenticados, replica-os e retransmite-os, se fazendo passar pela pessoa que enviou o pacote anteriormente. O *Spoofing* acontece quando o invasor assume o papel do destino dos pacotes, recebendo assim pacotes que não deveriam ser entregues nesse destino. O *Hijacking*

captura um pacote interceptando o contexto de uma conexão e passa a participar da conexão assim como a origem e destino anteriores.

A **Figura 7** exibe a estrutura do protocolo AH:

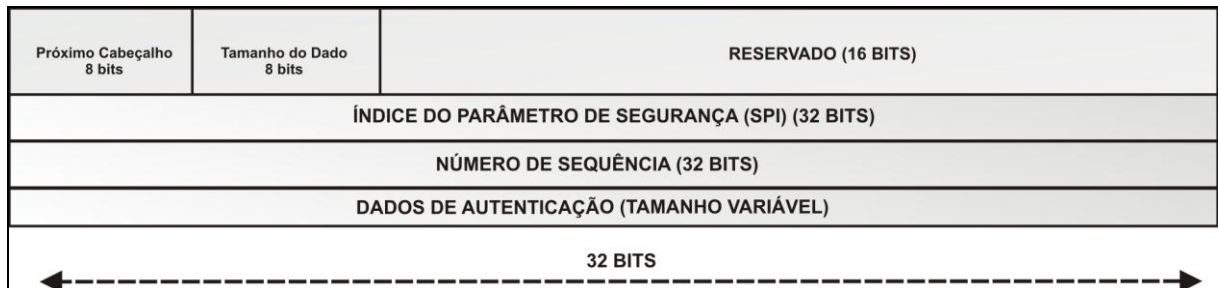


Figura 7 - Estrutura do protocolo AH

Fonte: Adaptada de SILVA, Lino Sarlo da. Virtual Private Network (2005)

Próximo Cabeçalho: este campo contém o identificador do próximo cabeçalho. É o mesmo valor inserido no campo “protocolo” no cabeçalho IP original;

Tamanho do dado: este campo contém o comprimento do cabeçalho de autenticação;

Reservado: este campo contém 16 bits dedicados para a extensão do protocolo;

SPI (*Security Parameter Index*): O protocolo AH, o endereço fonte descrito no protocolo IP e este índice, identificam uma SA para um determinado pacote;

Número de sequência: A utilização deste campo previne ataques do tipo *replay*, pois identificam os pacotes pertencentes a uma determinada SA, numerando os pacotes que trafegam dentro dela;

Dados de autenticação: Campo de tamanho variável que contém o ICV (*Integrity Check Value*), calculado seguindo o algoritmo de autenticação utilizado.

O mecanismo de autenticação utilizado pelo AH é feito utilizando uma função de *hash* usando a chave negociada durante o estabelecimento da SA. O resultado deste *hash* é exatamente o ICV, contido no campo Dados de autenticação.

3.5.2 Encapsulation Security Payload (ESP)

Segundo SILVA (2005), o protocolo de encapsulamento seguro do dado fornece autenticação, confidencialidade das informações por meio da criptografia e proteção de ataques do tipo *replay*. O protocolo de criptografia a ser utilizado no transporte de pacotes é definido na própria SA e estes pacotes deverão conter controles de sincronismo para que o processo de criptografia/descriptografia seja realizado.

3.6.2 *Advanced Encryption Standard (AES)*

O *AES* ou *Advanced Encryption Standard*, é um algoritmo de criptografia que sucedeu o DES, é baseado no algoritmo Rijndael (DAEMEN & RIJMEN, 2005). Ao contrário do DES, que implementa uma rede de Feistel, o Rijndael é uma rede de permutação-substituição, o que o torna rápido tanto em software quanto em hardware. Diferentemente do Rijndael, os mecanismos de criptografia do AES usam um tamanho de bloco fixo em 128 bits, enquanto as chaves podem ter tamanhos de 128, 192 ou 256 bits.

A criptografia do AES atravessa quatro estágios:

1) *AddRoundKey*

É gerada uma subchave a partir da chave principal usando o algoritmo de agendamento de chaves;

2) *SubBytes*

Cada byte é substituído por outro de acordo com uma tabela de referência;

3) *ShiftRows*

Nesta etapa cada fileira dessa fase é transposta uma determinada quantidade de posições;

4) *MixColumns*

Nesta etapa as os quatro bytes de cada uma das colunas dessa fase são mescladas usando uma transformação linear;

3.7 Principais algoritmos de autenticidade utilizados em VPN

3.7.1 Message-Digest algorithm (MD5)

MD5 é um algoritmo de *hash* de 128 bits desenvolvido pela RSA Data Security Inc. e bastante utilizado para verificação de integridade de arquivos e autenticação de conexões VPN. Este algoritmo também é largamente utilizado em ambientes *Unix* para autenticação de *login*.

O MD5 apresenta uma vulnerabilidade por realizar apenas uma passagem sobre os dados nos quais se pretendem executar a função de *hash*. Há uma possibilidade que duas *strings* gerem o mesmo *hash*, permitindo assim uma provável colisão.

3.7.2 Secure Hash Algorithm (SHA-1)

O algoritmo de autenticação *SHA-1* foi criado pela *National Security Agency* (NSA) e publicado como um padrão para geração de *hash* de autenticidade para o governo americano. Dentre a família SHA, o SHA-1 é o mais utilizado para geração de *hash*, sendo inclusive utilizada no *Emule* para controle de arquivos duplicados na rede e no OpenSwan como um padrão de algoritmo de autenticidade ao realizar a geração de SAs.

Embora o suporte a elas não sejam totalmente acessíveis ainda, as novas variantes da família SHA são bem mais poderosas do que o SHA-1, trazendo um maior número de blocos e gerando um *hash* de saída ainda maior, o que previne a ocorrência de colisões:

Algoritmo	Tamanho da saída	Tamanho dos blocos	Comprimento
SHA-0	160	160	64
SHA-1	160	160	64
SHA-256	256	512	64
SHA-512	512	1024	128

Tabela 1 - Família SHA com suas variantes

Fonte: NIST. Secure Hash Algorithm – FIPS 180

3.8 Método para trocas de chaves *Diffie-Hellman*

Este algoritmo não tem o objetivo de criptografar dados, nem de prover autenticação para as conexões VPN. Ele foi criado por *Whitfield Diffie* e *Martin Hellman* com o intuito de realizar uma troca rápida de chaves de criptografia, entre os envolvidos na conexão. O usuário A gera uma chave a partir da chave privada dele e a pública do usuário B. O usuário B gera uma chave a partir da chave privada dele e a pública do usuário A. Este algoritmo assim como os outros algoritmos de criptografia, oferece uma grande desvantagem, pois, ao capturar a chave pública do usuário B, esta transferência é feita de maneira insegura, permitindo assim possíveis ataques do tipo *man-in-the-middle*.

A **Figura 9** exibe o funcionamento do método *Diffie-Hellman*:

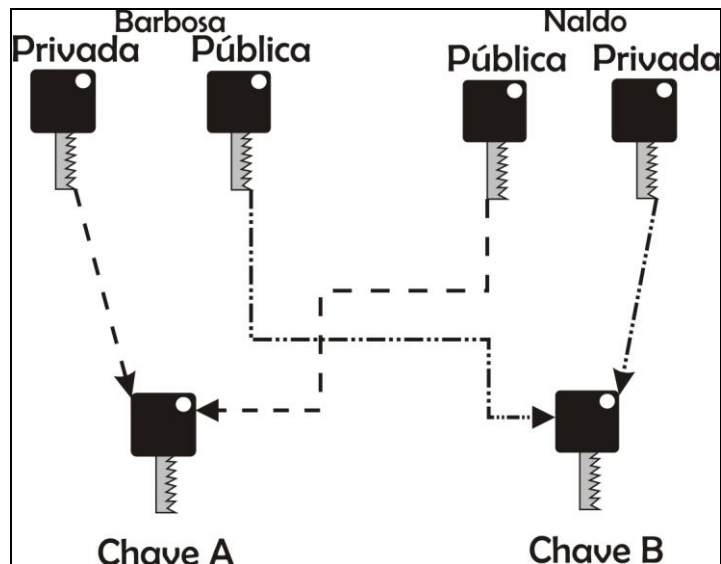


Figura 9 - Método Diffie-Hellman

Fonte: Adaptada de SILVA, Lino Sarlo da. Virtual Private Network (2005)

4 ESTUDO DE CASO

Este estudo de caso foi desenvolvido em um ambiente de uma corporação que tem como negócio principal a autorização de transações financeiras, advindas de cartões de crédito ou débito. Todas as informações específicas de configuração, endereçamento e/ou outras quaisquer que poderiam de alguma forma afetar a segurança e integridade dos dados da corporação em questão foram citadas de forma fictícias. Esta instituição possui clientes em todo o Brasil, principalmente do eixo Rio-São Paulo, lugar de maior concentração de transações financeiras utilizando cartões.

Alguns anos atrás, a empresa passou a operar também com cartões de crédito para pagamento nos seguintes segmentos: alimentação, combustível, refeição, presente, farmácia e gestão de frotas de veículos. Este fato proporcionou um grande crescimento das operações da mesma em todo o Brasil, ocasionando a assinatura de um contrato com duas das maiores redes de hipermercados existentes no território brasileiro.

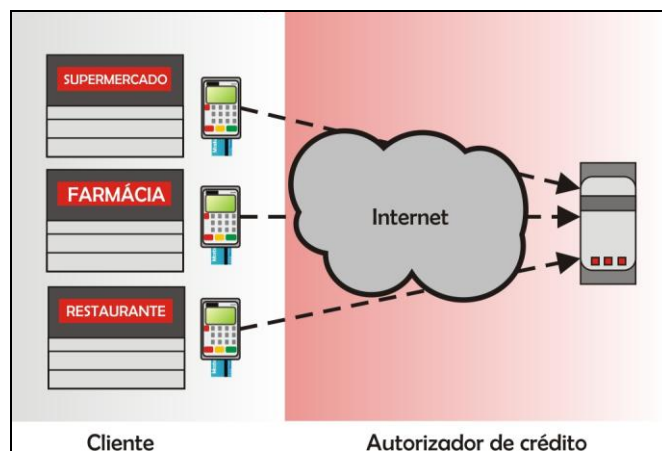


Figura 10 - Visão geral do serviço prestado no cenário
Fonte: Arquivo Pessoal (2010)

4.1 Estrutura do estudo de caso

Esse estudo de caso foi dividido em cinco partes, conforme descrito na tabela 1:

Etapas	Descrição
Motivação	Serão descritas as circunstâncias que levaram à implantação destas VPNs no ambiente que será estudado, bem como o problema que levou a criação das mesmas
Benefícios	Serão descritos os benefícios que podem ser adquiridos em virtude da utilização das VPNs no ambiente em estudo e como tais benefícios podem influenciar o negócio principal da instituição
Análise de Requisitos	Será descrita uma análise de requisitos, onde a mesma deverá conter todos e quaisquer elementos que de alguma forma influenciam no ambiente de modo a proporcionar a implantação destas VPNs
Implantação	Será descrito todo o processo de implantação, desde a troca de documentos entre os envolvidos, até a fase final de homologação e testes no ambiente
Resultados obtidos	Serão descritos os resultados obtidos a partir da utilização destas VPNs no ambiente, assim como as possíveis melhorias e impactos no negócio principal da instituição

Tabela 2 - Estrutura do estudo de caso

Fonte: Arquivo pessoal

4.2 Motivação

A motivação desse estudo de caso está relacionada à assinatura do contrato dos novos clientes supracitada neste estudo de caso. Durante a homologação destes novos clientes, uma das principais exigências dos mesmos, foi a criação de um canal exclusivo de comunicação com os estabelecimentos que passariam a utilizar este cartão. Este canal exclusivo deveria ter um sistema de autenticação e criptografia de pacotes específico, além de utilizar servidores de maior poder computacional, exclusivos para processar as transações destes clientes. Devido ao alto custo de um link dedicado para realizar estas operações, foi então cogitado a possibilidade da implantação de uma VPN entre o gateway X.25 terceirizado e a instituição de autorização de crédito, objeto desse estudo de caso, tendo em vista que as

conexões de Internet dos servidores de autorização têm uma largura de banda bem acima do necessário para o tipo de operação realizada. Este fato foi crucial para o amadurecimento da idéia de se utilizar VPNs redundantes para este fim, uma vez que esta tecnologia está presente hoje nas grandes corporações como uma forma de eliminar distâncias de forma segura, barata e de fácil escalabilidade, uma vez que estas estruturas tendem a crescer e sofrerem alterações. Após análise realizada na estrutura de comunicação da empresa autorizadora de crédito, levando em consideração características da organização, disponibilidade financeira, conclui-se que a melhor alternativa é a utilização de uma conexão com o Gateway X.25 terceirizado através de uma solução VPN.

Na **figura 11**, observe todo o caminho a ser percorrido pelas transações, desde o cliente final, de posse do cartão, até o autorizador de crédito e aprovação da venda:

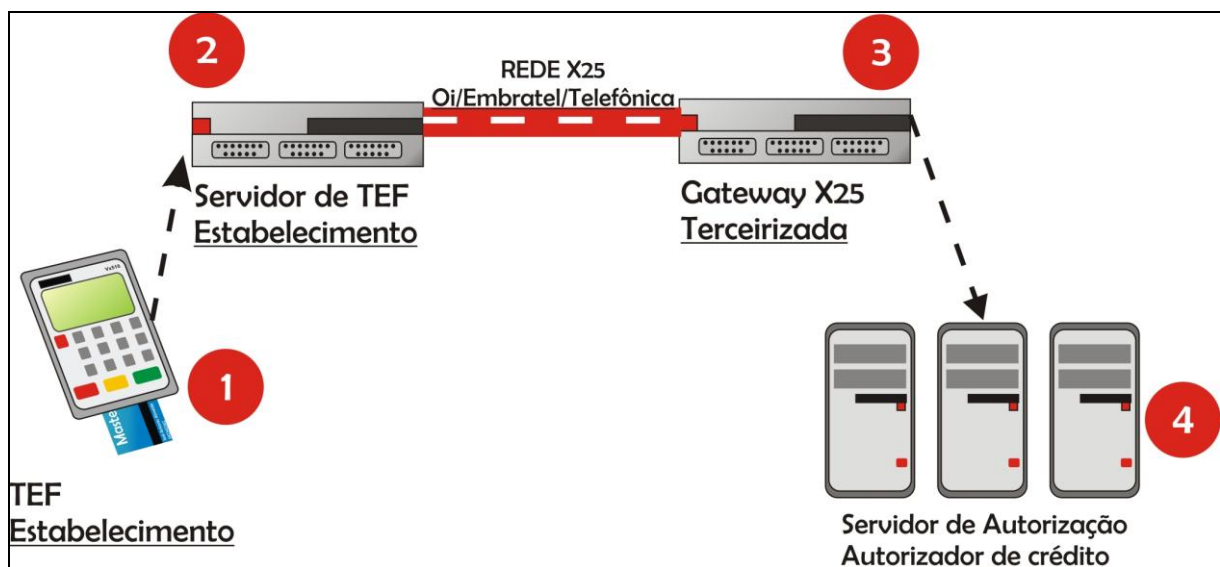


Figura 11 - Caminho percorrido pelas transações

Fonte: Arquivo Pessoal (2010)

No passo 1, o usuário realiza a transação no *pinpad* ligado ao TEF do estabelecimento.

No passo 2, a transação chega ao servidor de TEF do estabelecimento, que por sua vez estará ligado a um modem X.25 conectado ao canal do *gateway* X.25 da empresa terceirizada.

No passo 3, o *gateway* X.25 recebe a transação, remove o cabeçalho X.25 da mesma e envia o pacote para o servidor de autorização usando a Internet.

No passo 4, as transações chegam ao servidor de autorização, que processam as mesmas, autorizam ou não a mesma e respondem para o estabelecimento usando o mesmo caminho.

4.3 Benefícios

Os benefícios esperados advindos da implantação destas conexões VPN dizem respeito à economia mensal do preço do aluguel de um link dedicado, contratado junto à operadora de telefonia. Além disso, devido à redundância dos gateways X.25 terceirizados (um em SP e outro no RJ), a economia que será feita na contratação de novas conexões será ainda maior, aumentando assim o retorno do investimento realizado (ROI). Este valor está próximo dos R\$ 1.200 mensais para cada conexão de 1Mbit, ou seja, para se manter dois links dedicados de forma redundante, o gasto mensal sairia próximos aos R\$ 2.500 mensais o que faria o retorno do investimento cair, consideravelmente, uma vez iríamos arcar com mais um custo, fazendo com que as conexões de internet já existentes no ambiente ficassem sub-utilizadas.

Além disso, os ganhos com segurança são significativos, tendo em vista que mesmo contratando um link dedicado, os pilares da segurança da informação não estariam 100% assegurados, uma vez que ainda assim seria necessário implementar a autenticação da conexão para evitar possíveis ataques do tipo *man-in-the-middle*.

Entretanto, usando esta solução a confidencialidade dos dados estaria assegurada (ou maximizada) com o uso de protocolos de autenticação como o MD5; a integridade dos dados, pelo fato de utilizar um algoritmo de criptografia dos pacotes trafegados como o 3DES; e a disponibilidade, por utilizarmos conexões de Internet redundantes tanto na origem, como no destino dos túneis VPNs redundantes (RJ e SP).

Outro detalhe que deve ser lembrado, é que por essa estrutura necessitar ser construída nos meses de Novembro/Dezembro e o prazo mínimo para implantação de uma conexão dedicada junto a uma operadora de telefonia é de no mínimo 45 dias, a mesma teria que ser realizada em um tempo extremamente reduzido para que a empresa não perdesse de lucrar com estas transações, uma vez que este período é o mais rentável devido ao grande volume de transações.

4.4 Análise de requisitos da infra-estrutura

A análise dos requisitos para implantação destas VPNs fora realizada em cima da estrutura já existente no ambiente de produção dos servidores de autenticação, uma vez que os servidores e as conexões de Internet já operavam normalmente.

Na **tabela 3**, podemos observar os requisitos especificados pelo cliente para homologação das operações. Os status possíveis são: Disponível ou Não disponível:

Item	Descrição	Status
Servidor de Produção	Configuração mínima: Quatro processadores com quatro núcleos cada, 64 GB de memória RAM com ECC, 2 conexões de rede gigabit, 500 GB de disco rígido	Disponível
Conexão de Internet	Configuração mínima: Duas conexões de Internet de 1Mbit. OBS: O cenário atual já possuía conexões de Internet de 8Mbits redundantes.	Disponível
Criptografia do tráfego	Criptografar o tráfego realizado no transporte dos dados entre o cliente.	Disponível

Tabela 3 - Requisitos especificados pelo cliente

Fonte: Arquivo pessoal (2010)

Tendo em vista que os requisitos mínimos especificados pelo cliente já estavam disponíveis para a homologação das transações entre o mesmo e o autorizador de crédito, o foco passou a ser o estabelecimento das conexões VPN.

A **Tabela 4** exibe os requisitos para o estabelecimento destas conexões:

Item	Descrição	Obs.
Software de conexão VPN	OpenSwan Versão: 2.6.23	Disponível em http://www.openswan.org
Conexão de Internet	O cenário atual já possuía conexões de Internet de oito Mbits redundantes.	Disponível
Sistema Operacional Linux	Sistema operacional Linux, com os compiladores cc e gcc instalados; Kernel 2.6.x ou mais atual.	Disponível

Tabela 4 - Requisitos mínimos para estabelecimento das conexões

Fonte: Arquivo pessoal (2010)

4.5 Implantação

A implantação destas conexões foi dividida em três fases distintas: Planejamento, Execução e Testes.

Baseando-se no conceito de um ciclo de vida de um projeto, segundo o Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos – PMBOK, escrita pelo Instituto de Gerenciamento de Projetos (PMI), cada uma destas fases devem apresentar marcos específicos, que delimitam o início e o fim de cada uma delas. (PMI, 2004)

4.5.1 Planejamento

A fase de planejamento envolveu a troca de documentos entre as instituições envolvidas no estabelecimento das conexões VPN, ou seja, entre a empresa responsável pelo gateway X.25/IP e a empresa responsável pelos servidores de autorização de crédito, objeto deste estudo de caso. Os documentos trocados entre as partes descrevem e definem uma configuração comum entre as mesmas, para estabelecimento das conexões VPN. Além disso, também foi negociado o esquema de endereçamento IP que fora utilizado no tunelamento. As conexões VPN que foram estabelecidas são do tipo *client-to-gateway*, ou seja, um *host* do autorizador de crédito se conecta a um gateway VPN e este por sua vez, permitirá a conectividade do *host* do autorizador a LAN do gateway VPN.

A **Figura 12**, mostra uma representação do cenário que foi estabelecido entre o autorizador de crédito os estabelecimentos e o autorizador de crédito:

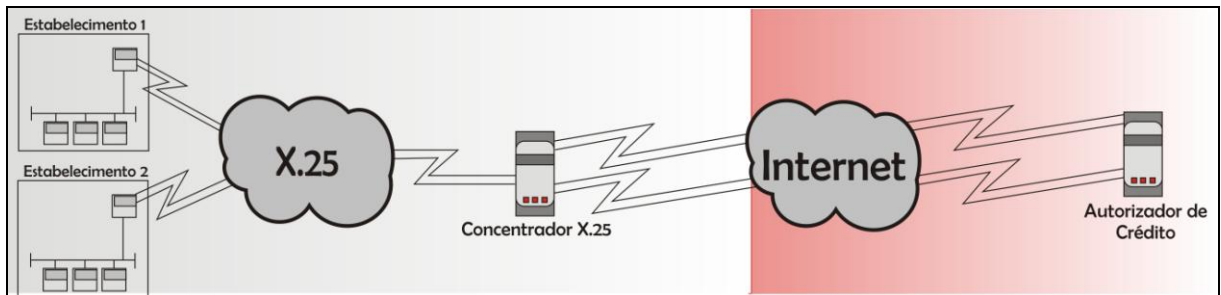


Figura 12 - Representação da estrutura entre autorizador e gateways VPN

Fonte: Arquivo pessoal (2010)

Os parâmetros negociados entre as partes envolvidas no processo de implantação das VPNs são de vital importância para a configuração do software OpenSwan neste ambiente, conforme seguem abaixo. Posteriormente, foi realizado o detalhamento de cada opção possível e as opções escolhidas para o desenvolvimento destas conexões:

```
# /etc/ipsec.conf - Arquivo de configuração Openswan IPsec
#
#
#
version 2.0      # Utilizando a especificação 2.0 do ipsec.conf
# Configuração OpenSwan
config setup
    protostack=netkey
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
conn SP
    left=188.88.88.48
    leftsubnet=192.168.168.1/32
    right=202.202.202.1
    rightsubnet=192.168.102.0/24
    auto=add
    type=tunnel
    authby=secret
    pfs=yes
conn RJ
    left=188.88.88.48
    leftsubnet=192.168.168.1/32
    right=200.200.200.1
    rightsubnet=192.168.101.0/24
    auto=add
    type=tunnel
    authby=secret
    pfs=yes
conn %default
    esp=3des-md5-192
    keyexchange=ike
    ikelifetime=28800s
    keylife=14400s
```

Na configuração detalhada acima, podemos observar os vários parâmetros que dizem respeito à configuração do software *OpenSwan*. Segue abaixo um detalhamento sobre a função de cada parâmetro citado:

protostack=auto

Esta opção define a pilha de protocolos que será utilizada, as opções possíveis são: *auto*, *klips*, *netkey* e *mast*. A opção *klips/mast*(versão mais recente) requer a aplicação de um patch, o que representa a necessidade de re-compilação do *kernel* em questão. A opção *netkey* não requer nenhum tipo de aplicação de patch ou correção no *kernel*, entretanto, esta opção não tem suporte a interfaces IPSec exclusivas para o tráfego pelo túnel, ou seja, não permitem a separação do tráfego existente no túnel.

interfaces=%defaultroute

Este parâmetro define qual interface de rede será utilizada para transportar os dados advindos do túnel VPN. A opção *%defaultroute* utiliza a interface de rede associada a rota padrão do sistema operacional para o tráfego das informações.

klipsdebug=none

Este parâmetro define o log do *klips* em modo *debug*, ou seja, exibe as informações das ações realizadas pelo *klips* no log do *OpenSwan*. A opção *none* desabilita a exibição destas informações.

plutodebug=none

Este parâmetro define o log do *pluto* em modo debug, ou seja, exibe as informações do *daemon* do *OpenSwan* de forma detalhada no arquivo de *log*.

conn SP

Este parâmetro define o nome da conexão VPN a ser criada.

left= 188.88.88.48

Este parâmetro define o endereço IP válido do servidor do autorizador de crédito, ou seja, o lado esquerdo da conexão VPN.

leftsubnet=192.168.168.1/32

Este parâmetro define o endereço da subrede associada ao túnel VPN no servidor do autorizador de crédito. Neste caso específico, apenas um endereço de IP fora definido, pois apenas o *host* do autorizador de crédito terá conectividade ao túnel VPN.

right=202.202.202.1

Este parâmetro define o endereço IP válido do concentrador VPN da empresa responsável pelo *gateway* X.25.

rightsubnet=192.168.102.0/24

Este parâmetro define o endereço da subrede associada ao túnel VPN na empresa responsável pelo *gateway* X.25. Neste caso específico, o *host* do servidor de autorização realizará uma conexão VPN *client-to-gateway* com a rede da empresa responsável pelo *gateway* X.25.

auto=add

Este parâmetro define a forma de inicialização da conexão e a criação do túnel VPN. As opções possíveis são:

i. *auto=start*

Cria o túnel VPN e inicia automaticamente a conexão VPN.

ii. *auto=add*

Apenas adiciona o túnel VPN, porém, não inicia a conexão VPN automaticamente. Esta opção será utilizada nesta conexão pelo fato do pedido de conexão vir do *gateway* VPN da empresa responsável pelo *gateway* X.25.

iii. *auto=route*

Esta opção apenas adiciona o roteamento para a criação do túnel, embora não execute a criação do mesmo, nem carregue as configurações, nem mesmo crie as conexões.

iv. *auto=manual*

Esta opção permite a inicialização de forma manual do túnel e conexão VPN.

type=tunnel

Este parâmetro define o tipo de conexão a ser estabelecida pelo *OpenSwan*. As opções possíveis são as seguintes:

i. *tunnel*

É utilizada para definir uma conexão *client-to-client*, *client-to-gateway* e *gateway-to-gateway*. É utilizada como padrão pelo *OpenSwan*.

ii. *passthrough*

Esta opção é utilizada para definir que o *IPSec* não deverá ser utilizada para estabelecer a conexão.

iii. *drop*

Esta opção define que todos os pacotes deverão ser descartados.

iv. *reject*

Esta opção permite a definição de quais pacotes deverão ser descartados.

authby=secret

Este parâmetro define como os gateways VPN irão autenticar-se. As opções possíveis são as seguintes:

i. *secret*

Esta opção é utilizada quando a autenticação se dá por meio de uma senha, compartilhada entre os *gateways VPN*.

ii. *rsasig*

Esta opção é utilizada quando a autenticação acontece utilizando certificados RSA.

pfs=yes

Este parâmetro habilita o método de renegociação de chaves, utilizado para prover segurança, uma vez que a chave é renegociada constantemente para que a nova chave nunca seja igual à chave anteriormente utilizada. Ao habilitar esta opção, o grupo *Diffie-Hellman* (*dhgroup*) deverá ser especificado.

conn %default

Este parâmetro inicia as configurações comuns as conexões criadas no arquivo ipsec.conf.

esp=3des-md5-192-modp1024

Este parâmetro define os algoritmos de autenticação, criptografia e o grupo Diffie-Hellman que a conexão irá utilizar no cabeçalho ESP. No caso específico, utilizamos o algoritmo de criptografia *3DES*, de autenticação *MD5* com chaves de 192 *bits* e o grupo *Diffie-Hellman Group2*.

keyexchange=ike

Este parâmetro define o protocolo de troca de chaves que será utilizado. No nosso caso em específico, utilizamos o *ike*, um protocolo de gerenciamento de chaves utilizado em conjunto com o IPsec e baseado em três protocolos; ISAKMP, que proporciona uma estrutura de autenticação e troca de chaves; Oakley, que define uma série de trocas de chaves chamadas de modos; SKEMI, que define uma troca dinâmica de troca de chaves que garante confidencialidade, não-repúdio e atualização rápida das chaves.

ikelifetime=28800s

Este parâmetro define o tempo de vida do protocolo IKE na conexão estabelecida, ou seja, após este tempo será executado novamente o protocolo de gerenciamento de chaves, forçando assim a atualização das chaves utilizadas.

keylife=14400s

Este parâmetro define o tempo de vida da chave negociada durante o estabelecimento do protocolo IKE. Observe que após 14.400 segundos ela será renegociada, e após 28.800 segundos, o IKE será reiniciado, fazendo assim com que tais chaves sejam novamente renegociadas. Estes parâmetros garantem a troca de chaves em intervalos fixos de tempo, isto permite melhorar a segurança do IPsec, pois aumenta o número de chaves que um possível atacante teria que “quebrar”.

De posse destas configurações, acertadas entre as duas corporações envolvidas no processo de estabelecimento das conexões VPN, podemos assim passar a fase de execução. O próximo passo que fora executado foi, de fato, o estabelecimento da conexão VPN e o

acompanhamento do tráfego entre o Gateway VPN SP e o servidor de autorização de crédito, pois inicialmente apenas a conexão com o gateway de São Paulo fora estabelecida. Só após os testes no ambiente junto à conexão com o gateway VPN SP é que fora estabelecida a conexão do autorizador de crédito com o Gateway VPN RJ.

4.5.2 Execução

O início da fase de execução tem como marco principal, o acordo entre as partes envolvidas no estabelecimento das conexões, onde ficou especificado quais as configurações que seriam utilizadas em ambos os lados, de maneira a permitir a conectividade entre as mesmas. Estas configurações e métodos a serem utilizados, foram documentadas através de comunicações formais e aprovadas por ambas as diretorias, definindo então o início da fase de execução do projeto de estabelecimento das conexões VPNs.

O primeiro passo da fase de execução trata-se da instalação do OpenSwan no ambiente de produção do servidor do autorizador de crédito, objeto desse estudo de caso. Não entraremos em detalhes sobre a instalação e configuração da VPN no ambiente da empresa responsável pelo *Gateway X.25*, uma vez que trata-se de uma empresa terceirizada e assumindo que a mesma esteja utilizando as configurações acertadas nos documentos trocados durante a fase de planejamento do projeto.

Segue abaixo os passos para efetuar o download do arquivo fonte do OpenSwan e realizar a compilação do mesmo, assim como a definição dos arquivos a serem alterados na configuração do OpenSwan:

```
[user@server ~]$ wget http://www.openswan.org/download/openswan-2.6.23.tar.gz
[user@server ~]$ tar -zxvf openswan-2.6.23.tar.gz
[user@server ~]$ cd openswan-2.6.23
[user@server openswan-2.6.23]$ ./configure
[user@server openswan-2.6.23]$ make
[user@server openswan-2.6.23]$ make install
[user@server openswan-2.6.23]$ /etc/init.d/ipsec start
```

Após estes comandos, o OpenSwan estava instalado e pronto para ser configurado. Para efetuar esta verificação, utilizamos o seguinte comando e obtivemos a seguinte resposta:

```
[user@server openswan-2.6.23]$ /etc/init.d/ipsec status
```

```
IPsec running - pluto pid: xxxx
pluto pid xxxx
0 tunnels up
```

Após a conclusão da instalação do *OpenSwan*, passamos então para a configuração dos arquivos do mesmo. Basicamente, realizamos as alterações em dois arquivos de configuração:

```
/etc/ipsec.secrets
/etc/ipsec.conf
```

No */etc/ipsec.secrets*, realizamos a configuração da *passkey* que foi negociada com a empresa responsável pela configuração do outro lado da VPN. Segue a configuração utilizada abaixo:

```
# Configuração /etc/ipsec.secrets

: PSK "chave@123"
```

Após a definição do arquivo de chave *PSK*, *ipsec.secrets*, utilizamos as configurações do arquivo *ipsec.conf*, já previamente definido neste documento, a fim de configurar os túneis com os gateways VPNs RJ e SP. Para isto, executamos os seguintes comandos:

```
[user@server openswan-2.6.23]$ /etc/init.d/ipsec restart
```

```
[user@server openswan-2.6.23]$ /etc/init.d/ipsec status
```

```
IPsec running - pluto pid: xxxx
pluto pid xxxx
2 tunnels up
```

Após a exibição desta mensagem, percebemos que os túneis VPN RJ e SP estavam configurados e ativos, então realizamos um teste de conectividade entre os *hosts* que realizaram a conexão VPN, utilizando o comando *ping* para trafegar pela interface do túnel:

```
[user@server openswan-2.6.23]$ ping -I 192.168.168.1 192.168.101.1
```

Disparando 192.168.101.1 de 192.168.168.1 com 64 bytes de dados:

Resposta de 192.168.101.1: bytes=64 tempo<1ms TTL=255

Resposta de 192.168.101.1: bytes=64 tempo<1ms TTL=255

Resposta de 192.168.101.1: bytes=64 tempo<1ms TTL=255

```
[user@server openswan-2.6.23]$ ping -I 192.168.168.1 192.168.102.1
```

Disparando 192.168.102.1 de 192.168.168.1 com 64 bytes de dados:

Resposta de 192.168.102.1: bytes=64 tempo<1ms TTL=255

Resposta de 192.168.102.1: bytes=64 tempo<1ms TTL=255

Resposta de 192.168.102.1: bytes=64 tempo<1ms TTL=255

Fora comprovado pelo comando *ping* acima, que há conectividade entre as pontas pelo endereço de rede do túnel, o que significa que para ambos os túneis, tanto *gateway* VPN RJ (192.168.102.1) como o *gateway* VPN SP (192.168.101.1) estavam ativos e operantes.

Tais testes de conectividade entre os gateways VPN e o servidor de autorização (192.168.168.1) especifica um marco e encerra a fase de execução do projeto de implantação das conexões VPN, uma vez que o software responsável pela conexão foi compilado, instalado, configurado, mostrou-se ativo e respondendo as requisições advindas do túnel VPN estabelecido entre as partes envolvidas.

Vale salientar, que normalmente tais túneis com endereços de redes internas diferentes não poderiam trafegar diretamente, entretanto, neste servidor de autorização existem regras de roteamento específicas para este fim, que roteiam as transações para a interface do túnel, caso elas tenham como endereço destino a faixa de endereço IP 192.168.168.x.

Na **figura 13**, o caminho percorrido através do túnel VPN com as interfaces estabelecidas:

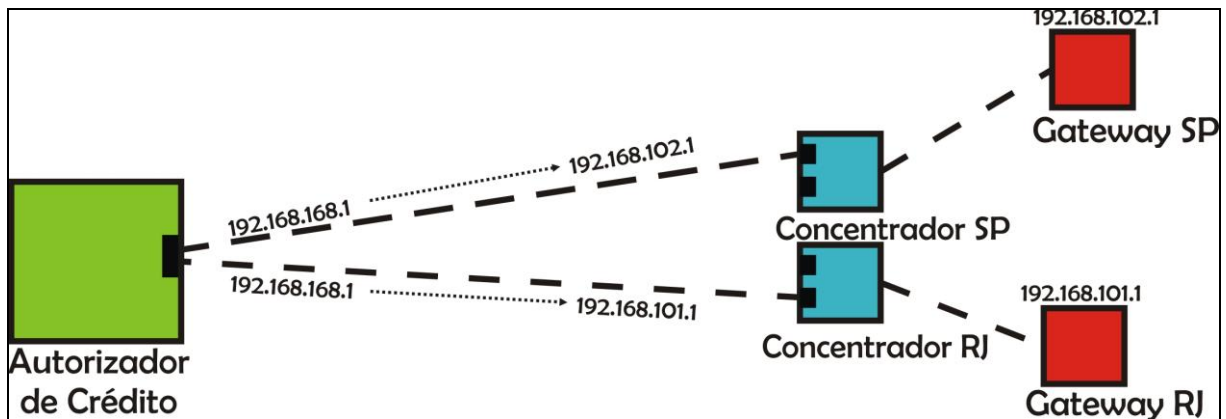


Figura 13 - Caminho percorrido através do túnel VPN com as interfaces

Fonte: Arquivo Pessoal (2010)

4.5.3 Homologação e testes

Após os testes de conectividade da fase de execução, a mesma se mostrou operante e ativa. Com este marco, podemos dar início à fase de homologação e testes junto ao cliente, uma vez que toda a estrutura necessária para o tráfego das transações financeiras entre a empresa responsável pelo *gateway* X.25 e o autorizador de crédito se mostrou pronta para operar em produção.

Foi instalada uma aplicação capaz de receber uma solicitação de abertura de *socket* e respondê-la, abrindo o *socket* em uma porta específica informada para o cliente. Após a definição da porta a ser transmitida tais transações, o cliente passou a enviar testes durante o período de 48hrs, enviando transações de abertura de terminal, venda, cancelamento de venda, desbloqueio de cartão, pagamento de faturas, entre outros tipos. Tais transações estavam sendo enviadas usando uma porta específica que definiremos de maneira fictícia como porta 4000. Ao verificar o tráfego da banda nesta porta, verificamos que todo o tráfego estava sendo enviado utilizando o endereçamento interno do túnel IPSec.

A **Figura 14** exibe um exemplo deste tráfego:

```
[root@decode ~]# tcpdump -X -ni any port 4000 -s 1500
03:43:42.684815 IP 192.168.102.1.58527 > 192.168.168.1.s
46 <nop,nop,timestamp 3335104956 3821496383>
    0x0000:  4500 0034 17bb 4000 3f06 9eb5 c0a8 6601
    0x0010:  c0a8 9e01 e49f 2694 2646 91d1 8e3d a064
    0x0020:  8010 002e 42c0 0000 0101 080a c6c9 a9bc
    0x0030:  e3c7 683f
03:43:47.455026 IP 192.168.102.1.51855 > 192.168.168.1.s
    0x0000:  4500 0034 8211 4000 3f06 345f c0a8 6601
    0x0010:  c0a8 9e01 ca8f 2694 e28e 4bc5 4acd f4d6
    0x0020:  8010 002e b04d 0000 0101 080a c6c9 bc5e
    0x0030:  e3c7 7ae1
03:43:52.689601 IP 192.168.168.1.58527 > 192.168.102.1 .s
    0x0000:  4500 0034 17bc 4000 3f06 9eb4 c0a8 6601
    0x0010:  c0a8 9e01 e49f 2694 2646 91d1 8e3d a064
    0x0020:  8010 002e f497 0000 0101 080a c6c9 d0d0
    0x0030:  e3c7 8f53
```

Figura 14 - Tráfego na porta 4000 nas interfaces do túnel

Fonte: Arquivo Pessoal (2010)

4.6 Resultados obtidos

Os resultados obtidos a partir da implantação destas conexões VPN, observados a partir do estabelecimento das conexões junto à empresa responsável de gateway X.25 foram extremamente satisfatórios e cumpriram plenamente o objetivo inicial do projeto, assim como o objetivo principal desse trabalho. As transações que estão sendo enviadas pela empresa responsável pelo gateway X.25 estão sendo criptografadas, utilizando o algoritmo 3DES (*Triple DES*) e as SAs autenticadas a partir do algoritmo MD5. O ambiente não apresentou grandes picos de processamento em virtude da adição dessas conexões, o que poderia significar grande poder computacional para criptografar/descriptografar cada transação em tempo real e devolver para o destino. Do ponto de vista dos pilares da segurança da informação, tais resultados obtidos serviram como alicerces para a aplicação dos pilares da segurança da informação: Confidencialidade, Integridade e Disponibilidade. Confidencialidade pelo fato das transações que irão trafegar, são antes autenticadas no momento do estabelecimento do túnel, ou seja, na criação da SA. A integridade também fora evidenciada, uma vez que os dados que trafegam pelo túnel sofreram um processo de

criptação e de geração de uma chave *hash* a fim de validar as informações trafegadas e por fim, não menos importante, a disponibilidade, tendo em vista que para estabelecimento de tais conexões foram utilizadas duas conexões de Internet, redundantes, assim como a criação de dois túneis apontando para servidores fisicamente separados, trazendo assim características inerentes aos pilares da segurança da informação.

Estes resultados nos embasam acerca do cumprimento de um dos objetivos específicos deste trabalho, o de prover os pilares da segurança da informação, utilizando para isto ferramentas e protocolos de rede, capazes de prover autenticidade (através da utilização do protocolo MD5), integridade (através do uso de criptografia e protocolo de autenticação juntos, gerando um *hash* do pacote e encriptando o mesmo para evitar possíveis alterações da informação) e gerando disponibilidade da infra-estrutura aplicada no estudo de caso, por conter conexões de internet e servidores de roteamento de transações redundantes.

5 CONCLUSÃO

Neste trabalho foi construído um estudo de caso para o estabelecimento de conexões virtuais privadas (VPNs), para trafegar transações financeiras em um ambiente crítico e de alta disponibilidade, onde quaisquer tipos de falhas de acesso a estas informações podem ocasionar grandes perdas financeiras e enormes danos a imagem da empresa provedora destes serviços. Foram avaliadas algumas soluções empresariais do mercado e após ser feito um levantamento de requisitos para implantação da mesma, o projeto foi então iniciado. O embasamento teórico referente ao estabelecimento dessas conexões foi descrito a fim de prover um melhor entendimento sobre as mesmas.

A estrutura criada serve até hoje como base de transporte para as transações financeiras advindas da empresa responsável pelo gateway X.25, parceira do autorizador de crédito. Tais pacotes de transações são enviados utilizando as SAs negociadas e passam por um processo de autenticidade utilizando MD5 e criptografia/descriptografia, usando o protocolo *Triple DES*. Uma SA, conforme foi citado na seção 2.3.3.3, define os tipos de medidas de segurança nos quais a origem de envio de pacotes deve se basear, definindo o destino e o tipo de dado a trafegar. A implantação destas conexões trouxe um retorno financeiro extremamente considerável para a empresa, principalmente pelo fato de economizar o valor de aluguel de um link dedicado, que é bastante dispendioso (algo em torno de R\$ 1.200 mensais para cada conexão de internet) quando comparado a esta solução.

Deve-se lembrar também, que além dos custos reduzidos com a não-necessidade de alocação de uma conexão de Internet dedicada, existe também o fato do prazo para implantação do ambiente, tendo em vista a demora para instalar tais links dedicados durante o final do ano, conforme no capítulo do estudo de caso.

Uma perspectiva futura para o aprimoramento deste trabalho seria a necessidade de aumentar a estrutura atual, em detrimento do crescimento da empresa, criando mais túneis de comunicação junto à empresas de terceiros. Não se deve esquecer que ao passar do tempo, a criação de novos e melhores algoritmos de criptografia e autenticação não significaria em grandes custos para migração, o que pode acarretar em melhorias em segurança e desempenho no tráfego de transações ao longo dos túneis entre as duas empresas.

Conforme citado no estudo de caso, esta solução nos fornece o suporte necessário aos pilares da segurança da informação: confidencialidade, integridade e disponibilidade, por oferecer ferramentas e algoritmos capazes de prover tais propriedades.

REFERÊNCIAS

- KUROSE, James F. & ROSS, Keith W. Ross. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. Editora Pearson 3ª Edição.
- TANENBAUM, Andrew S.. **Redes de Computadores**. 3ª ed. Rio de Janeiro: Campus, 1997.
- SILVA, Lino Sarlo da. **Virtual Private Network - VPN**. São Paulo: 2ª Ed. Novatec, 2005.
- VPN Consortium. **Artigos referentes a redes virtuais privadas** - disponível em: <http://www.vpnc.org> – Acessado em 19/02/2010
- Project Management Institute. **A Guide to the Project Management Body of Knowledge (PMBOK Guide)**. Third Edition.ed., 2004.
- SANTOS, Felipe. **IPSec Utilizando Openswan**. Openswan-BR Group, 2008.
- Cyclades. **Guia Internet de Conectividade**. São Paulo, Editora Senac, 2000.
- SCRIMGER, Rob et al. **TCP/IP: a bíblia**. Tradução Edson Furmankiewicz. Rio de Janeiro: Editora Elsevier, 2002. 642p..
- BAUER, César Adriano. **Política de segurança da informação para redes corporativas**. Novo Hamburgo, 2006.
- RESENDE, Edmar Roberto Santana de. & GEUS, Paulo Lício de. **Uma solução segura e escalável para Acesso Remoto VPN**. Campinas, 2004.
- Internet Engineering Task Force - IETF. **Internet Protocol (RFC 791)** – Disponível em: <http://www.ietf.org/rfc/rfc791.txt> - Acessado em 19/02/2010
- DAEMEN,Joan. BORG, Steve. RIJMEN, Vincent. **The Design of Rijndael: AES - The Advanced Encryption Standard**, Springer-Verlag, 2002
- CEDET. **3DES – Triple Data Encryption Standard**
Disponível em: <http://www.cedet.com.br/index.php?O-que-e/Seguranca-de-Redes/3des-triple-data-encryption-standard.html> - Acessado em 19/02/2010
- Internet Engineering Task Force - IETF. **The MD5 Message-Digest Algorithm (RFC 1321)** - Disponível em: <http://tools.ietf.org/html/rfc1321> - Acessado em: 19/02/2010