UNIVERSIDADE FEDERAL DO PARANÁ

# PARAMETRIZAÇÃO DO FRAMEWORK IPSEC PARA A SEGURANÇA NA INTEROPERABILIDADE EM SMART GRID

CURITIBA
2015

VICTOR RAUL NEUMANN SILVA

# PARAMETRIZAÇÃO DO FRAMEWORK IPSEC PARA A SEGURANÇA NA INTEROPERABILIDADE EM SMART GRID

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre, no Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Paraná.

Orientador: Prof. Dr. Clodomiro Unsihuay Vila
Co-orientadora: Prof.ª Dra. Keiko V. Fonseca

Curitiba
2015

Catalogação na publicação
Vivian Castro Ockner – CRB 9ª/1697
Biblioteca de Ciências Humanas e Educação - UFPR

Silva, Victor Raul Neumann
Parametrização do framework IPSEC para a segurança na interoperabilidade em *Smart Grid*. / Victor Raul Neumann. – Curitiba, 2015.
117f.

Orientador: Prof.º Dr.º Clodomiro Unsihuay Vila
Co-orientadora: Prof.ª Dr.ª Keiko V. Fonseca
Dissertação (Mestrado em Engenharia Elétrica) - Departamento de Engenharia Elétrica
Universidade Federal do Paraná.

1. Engenharia elétrica – energia elétrica – sistemas de energia elétrica. 2. Conservação de energia – redes elétricas inteligentes – distribuição. 3. *Smart power grids – data processing – power resources*. I. Título.

CDD 621.31

# TERMO DE APROVAÇÃO

Victor Raul Neumann Silva

## Parametrização do framework do protocolo IPsec para a Segurança na Interoperabilidade em Smart Grid

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre no Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Paraná.

Prof. Dr. Clodomiro Unsihuay Vila – Orientador
Universidade Federal do Paraná

Prof.ª Dra. Keiko V. Fonseca – Co-orientadora
Universidade Tecnologica Federal do Paraná

Prof. Dr. Evelio Martín García Fernández – Convidado
Universidade Federal do Paraná

Prof. Dr. Luís Henrique Assumpção Lolis – Convidado
Universidade Federal do Paraná

Dr. Rodrigo Jardim Riella – Convidado
LACTEC

Prof. Dr. Augusto Foronda – Convidado
Universidade Tecnologica Federal do Paraná

Curitiba, 09 de Julho de 2015

## AGRADECIMENTOS

Aos professores Clodomiro Unsihuay-Vila e Keiko Veronica Ono Fonseca pelo incansável apoio, com o ensino e orientação na pesquisa, e a confiança depositada.

Aos professores Thelma Solange Piazza, Elizete Maria Lourenço e Alexandre Rasi Aoki pela transmissão de conhecimento durante o período do mestrado.

Aos colegas do PPGEE/UFPR pelo apoio que prestaram durante o curso.

À Rede Nacional de Ensino e Pesquisa (RNP), sito no Centro Politécnico da UFPR, pela liberação do Laboratório e apoio de seus funcionários para a realização dos testes de campo desta pesquisa.

## RESUMO

Para gerenciar, armazenar e utilizar eficazmente os dados na *Smart Grid* ou Rede Inteligente, o sistema de energia e as tecnologias de informação e comunicação (TIC) devem ser coordenados por meio da abordagem de sistema-de-sistemas (*system-of-systems*) e de comunicações. A interoperabilidade entre sistemas permitirá que as empresas de energia, consumidores, e outros interessados, adquiram hardware e software no mercado para incorporá-los em diferentes áreas, mantendo a compatibilidade com outros componentes, fazendo a transição do legado para redes mais inteligentes e providas de segurança. O Modelo e Metodologia de Referência para Interoperabilidade em *Smart Grid* - SGIRM - apresentam alternativas de concepção e implementação da interoperabilidade para sistemas que facilitam o intercâmbio de dados entre seus elementos, cargas e aplicações para o consumidor. Sendo uma infraestrutura crítica, a Smart Grid requer soluções abrangentes para a segurança, que envolvem desde a Segurança Física das instalações elétricas à Segurança Cibernética das TIC. Uma solução de segurança de comunicação de redes inteligentes requer uma abordagem holística, incluindo métodos de criptografias de chaves, tecnologias PSK (Chaves Pré-compartilhadas) e PKI (Infraestrutura de Chaves Públicas), elementos de computação confiável, mecanismos de autenticação e o uso de protocolos de segurança baseados em padrões do estado da arte. Recentemente, muitos esforços têm sido feitos na comunidade de sistemas de potência para desenvolver protocolos de segurança para redes de energia, aproveitando suítes de protocolos existentes, tais como o IPsec, o Transport Layer Security (TLS), o Secure DNP3. Esta dissertação de mestrado propõe uma metodologia de parametrização do framework do protocolo de rede IPsec visando a segurança no fluxo de dados, de acordo aos níveis dos serviços de segurança: Integridade, Confidencialidade e Disponibilidade, recomendados pelo SGIRM. Nesta dissertação é proposta uma metodologia para implementação de uma VPN IPsec Site-a-Site, numa topologia básica da rede da Smart Grid, com programação em CLI (Interface de Linhas de Comando). A metodologia pode ser para implementações de VPNs IPsec Site-a-Site entre qualquer par dos sete domínios do SGIRM: Geração, Transmissão, Distribuição, Prestadores de Serviços, Mercados, Controle/Operações e Consumidores. Testes em laboratório que visaram demonstrar a aplicabilidade e viabilidade da metodologia proposta, são aqui apresentados.



Palavras-chave: *Smart Grid*. Rede inteligente. SGIRM. Segurança Cibernética. Protocolo IPsec. Serviços de Segurança. Integridade. Confidencialidade. Programação em CLI (Interface de Linhas de Comando). Latência. Taxa de Transferência.

## ABSTRACT

To manage effectively, store and use Smart Grid data, the power system and information and communication technologies (ICT) should be coordinated through the system-of-systems and interoperable communications. Interoperability will allow utilities, consumers and other interested parties, to acquire hardware and software on the market to incorporate them in different its areas in order to be compatible with other components, and will also facilitate the legacy transition of smarter power grid networks. The Methodology of the Smart Grid Interoperability Reference Model - SGIRM - presents alternative design and implementation of interoperability for systems that facilitate the exchange of data between its elements, loads and applications for the consumer. As a critical infrastructure, the Smart Grid requires comprehensive security solutions ranging from the Physical Security of electrical installations to ICT Cyber security. A Smart Grid communication security solution requires a holistic approach, including encryption methods keys, PSK technologies (Pre-shared keys) and PKI (Public Key Infrastructure), trusted computing elements, authentication mechanisms and the use of security protocols based on standards of the state of the art. Recently, many efforts have been made in the power systems community to develop security protocols for energy networks, taking advantage of existing protocols, such as IPsec, Transport Layer Security (TLS), Secure DNP3. This dissertation proposes a methodology of parameterization of the IPsec network protocol framework, aimed at security of data flow, according to the security services levels: Integrity, Confidentiality and Availability, recommended by the SGIRM. This dissertation proposes a methodology for implementing a VPN IPsec Site-to-Site, in a basic topology of the Smart Grid network, with programming in CLI (Command Line Interface). The methodology can be extended to VPN IPsec Site-to-Site implementations between any pair of the seven domains of the SGIRM: Generation, Transmission, Distribution, Service Providers, Markets, Control / Operations and Customers. Laboratory tests that aimed to demonstrate the applicability and feasibility of the proposed methodology are presented here.



Keywords: Smart Grid. SGIRM. Cyber security. IPsec protocol. Security Services. Integrity. Confidentiality. Programming CLI (Command Line Interface). Latency. Throughput.

## SUMARIO DE FIGURAS

## SUMARIO DE TABELAS

## LISTA DE SIGLAS

| | |
|---|---|
| 3DES | Triple Data Encryption |
| 3DESEDE | 3DES-Encrypt-Decrypt-Encrypt |
| ACL | Access Control List |
| AES | Advanced Encryption Standard |
| AH - ESP | Authentication Header - Encapsulating Security Payload |
| CBC | Cipher Block Chaining |
| CFB | Cipher Feedback |
| CLI | Command Line Interface |
| CT-IAP | Communication Technologies - Interoperability Architectural Perspective |
| DES | Data Encryption Standard |
| DH | Algoritmo Diffie-Helman |
| DNP3 | Distributed Network Protocol 3 |
| DoS / DDoS | Denial of Service / Distributed Denial of Service |
| ECB | Electronic Code Book |
| FIPS | Federal Information Processing Standard |
| GOOSE | Generic Object Oriented Substations Events |
| IAP | Interoperability Architectural Perspective |
| ICT / TIC | Information and Communication Technologies |
| IETF | Internet Engineering Task Force |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IKE | Internet Key Exchange |
| IP - IPsec | Internet Protocol - IP Security Protocol |
| IPS | Intrusion Prevention System |
| ISAKMP | Internet Security Association Key Management Protocol |
| LAN | Local Area Network |
| MPLS | Multiprotocol Label Switching |
| OFB | Output feedback |
| OSI | Open Systems Interconnection |
| PDU | Protocol Data Unit |
| PKI | Public Key Infrastructure |
| PSK | Pre-shared Keys |
| RTT | Round Trip Times |
| SA | Security Associations |
| SCADA | Supervisory Control and Data Acquisition |
| SEAL | Encryption Optimized-Software Algorithm |
| SG | Smart Grid |
| SGIRM | Smart Grid Interoperability Reference Model |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WiMAX | Worldwide Interoperability for Microwave Access |
| WPA / WPA2 | Wi-Fi Protected Access / Wi-Fi Protected Access Version 2 |

# SUMÁRIO

# 1. INTRODUÇÃO

Depois de quase um século de existência, os sistemas de energia elétrica estão prestes a sofrer uma mudança radical. Essa transformação consiste na modernização do conceito, projeto e operação dos sistemas de geração, transmissão, distribuição e uso final da energia elétrica, através do uso intensivo e integrado de sistemas de tecnologia de informação e comunicação. Essa nova concepção atende pelo nome genérico de *Smart Grid* ou redes elétricas inteligentes. As mudanças que estão acontecendo são particularmente significativas para as redes de distribuição de energia elétrica, em que a "cegueira" e operações manuais, juntamente com componentes eletromecânicos, precisarão se transformar em uma rede inteligente (FALCÃO, 2010).

Por se tratar de um conceito, e não de um produto, sua motivação, interpretação, abrangência e desafios são diferenciados entre os países, regiões do Brasil, entre concessionárias, ou mesmo, entre regiões de uma mesma área de concessão (MAIA, 2013).

A infraestrutura de geração de energia elétrica é tradicionalmente vista em termos de plantas de fornecimento de energia para consumidores, cujas cargas foram atendidas sem muita administração ou controle do consumo da energia elétrica. A Smart Grid*,* com os recursos distribuídos (geradores e sistemas de armazenamento) junto com os sistemas de informação e comunicação, possibilita um moderno e mais inteligente sistema de energia.

## 1.1. Contextualização

### O Modelo de Referência SGIRM

O Modelo e Metodologia de Referência para Interoperabilidade em *Smart Grid,* cujo acrônimo em inglês é SGIRM[1], apresenta alternativas de concepção e implementação de interoperabilidade para sistemas que facilitam o intercâmbio de dados entre elementos da *Smart Grid*, cargas e aplicações de usuário final. É uma

[1] Documento elaborado pelo SGIP (Smart Grid Interoperability Panel), (segue no próximo rodapé) uma parceria público-privada no âmbito dos grupos de trabalho em SG do IEEE. Tem uma estrutura organizacional permanente para apoiar a evolução contínua dos trabalhos no SG. O SGIP conta com mais de 400 organizações divididos entre 22 categorias de trabalhos por áreas do SG.

representação conceitual da sua arquitetura sob três perspectivas: 1) sistemas de energia; 2) tecnologia de comunicação; e 3) tecnologia da informação,
(IEEE STD 2030, 2011), conforme Figura 1-1.

O SGIRM contém as entidades e os relacionamentos dentro do ambiente da Smart Grid, e define as interfaces de uma forma agnóstica da tecnologia. As arquiteturas das tecnologias das três perspectivas são projetadas para acomodar a evolução de equipamentos de hoje para a implementação no futuro, sem obsolescência indevida.

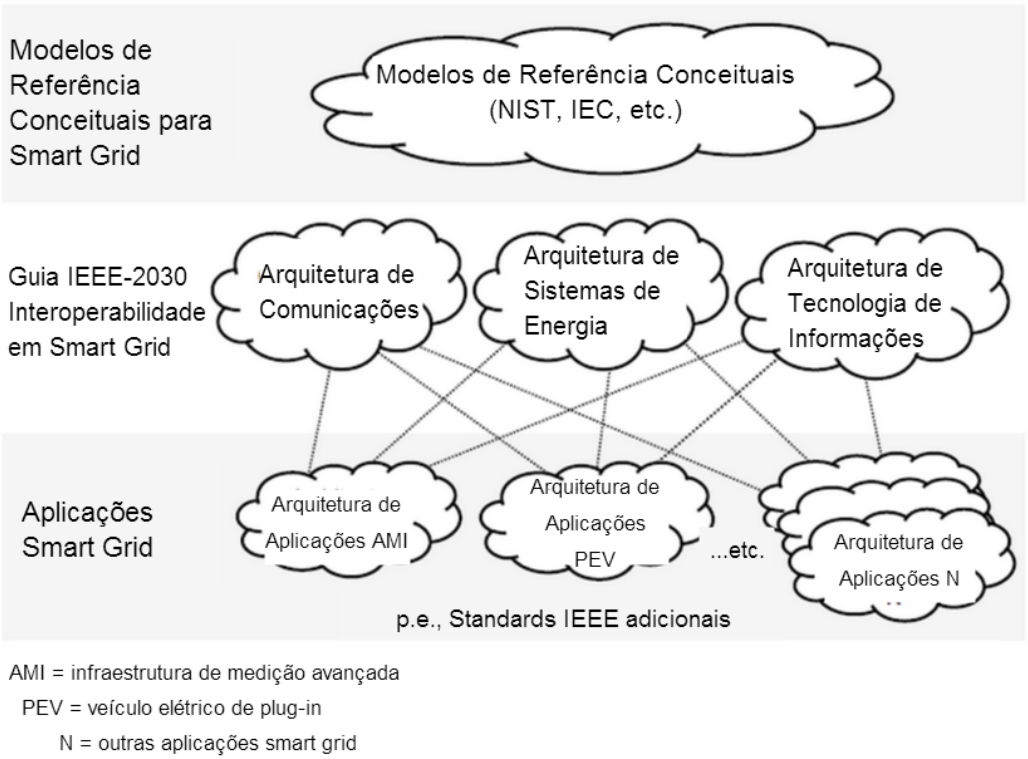


Figura 1-1 - Arquitetura Smart Grid - Fonte: Adaptado de IEEE STD 2030, 2011

O conceito da ferramenta de referência SGIRM é permitir extensibilidade, escalabilidade e capacidade de atualização. O SGIRM consiste de dois componentes: 1) Perspectivas Arquitetônicas de Interoperabilidade (IAPs) da *Smart Grid,* e 2) características do fluxo de dados entre as entidades dentro dessas perspectivas. O conceito de (IAPs) refere-se principalmente a considerações funcionais lógicas dos sistemas de energia, e das interfaces de tecnologia de informação e comunicação, sendo as três IAPs (IEEE STD 2030, 2011):

- Sistemas de energia IAP (PS-IAP): Sua ênfase é a produção, distribuição e consumo de energia elétrica, incluindo aparelhos, aplicativos e conceitos

operacionais. Essa perspectiva define sete domínios: Geração massiva, Transmissão, Distribuição, Prestadores de serviços, Mercados, Controle / Operações, e Consumidores.

- A tecnologia das comunicações IAP (CT-IAP): A ênfase é a comunicação para conectividade entre sistemas, dispositivos e aplicações no contexto da Smart Grid. A perspectiva inclui as redes de comunicação, mídia, desempenho e protocolos.
- A tecnologia da informação IAP (IT-IAP): A ênfase está no controle de processos e fluxo de dados de gestão. A perspectiva inclui tecnologias de informação que armazenam, gerenciam e controlam o fluxo de dados com segurança.

Cada uma das IAPs é composta de domínios, entidades e interfaces e/ou fluxos de dados, representado na Figura 1-2 (NIST, 2010). Os domínios comuns a todas as IAPs são:

- **Geração**. A geração de energia em grandes quantidades. Inclui-se aqui o armazenamento de energia para posterior distribuição.
- **Transmissão**. Os transportadores de grande quantidade de energia por longas distâncias.
- **Distribuição**. As distribuidoras de energia elétrica para e de Consumidores.
- **Prestadores de serviços**. As organizações que prestam serviços de infraestrutura aos Consumidores.
- **Mercados**. Os operadores e os participantes nos mercados da eletricidade.
- **Controle / operações**. A gestão do movimento de energia.
- **Consumidores**. Os usuários finais de energia elétrica.

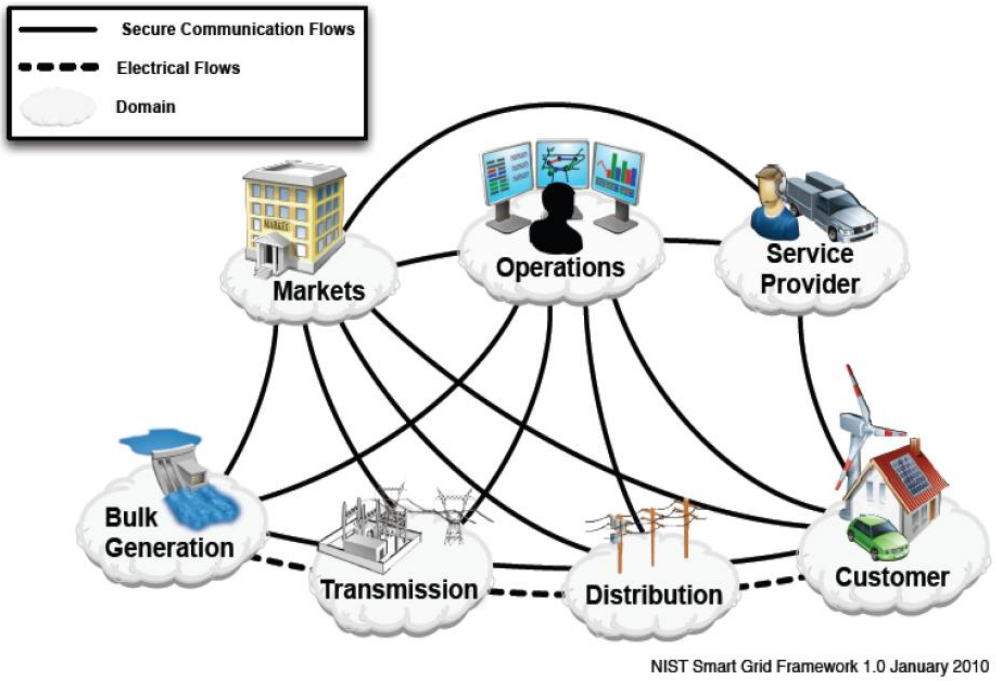


Figura 1-2 - Domínios e Interfaces do SGIRM - Fonte: NIST, 2010.

As Entidades (dispositivos, redes de comunicação, sistemas de computadores, programas de software, etc.) são geralmente localizadas no interior de um domínio e estão ligados entre si através de uma ou mais interfaces. As Interfaces são conexões lógicas de uma entidade para outra que suportam um ou mais fluxos de dados implementados com um ou mais enlaces de dados.

Os Fluxos de dados são usados em vez de interfaces na IT-IAP. Estes fluxos são comunicações de nível de aplicação das entidades que fornecem dados para entidades que os consomem. Cada perspectiva arquitetônica tem entidades que mais de perto mapeiam para sua tecnologia. No entanto, cada entidade pode mapear entidades de outra perspectiva arquitetônica.

### A Perspectiva Arquitetônica da CT-IAP e a Segurança

Na Perspectiva Arquitetônica de Interoperabilidade das Tecnologias de Comunicações (CT-IAP) a interoperabilidade é viabilizada pela adoção do modelo de referência OSI (ISO/IEC 7498-1:1994) de sete camadas, ou TCP/IP de quatro camadas, mostrada na Figura 1-3.


Figura 1-3 - Modelos OSI e TCP/IP - Fontes: Adaptado de Hubert (2003) e ISO/IEC 7498

Este modelo simplifica a tarefa de substituição de uma tecnologia de comunicação por uma tecnologia alternativa. Com a evolução dos protocolos e das aplicações existentes para uma arquitetura de comunicação em camadas, os implementadores poderão adaptar os protocolos legados para estar em conformidade com as camadas de rede (3) e transporte (4) (YAN *et al.,* 2012).

Recentemente, muitos esforços têm sido feitos pelos pesquisadores para desenvolver protocolos de segurança para redes de energia, a maioria dos quais estão aproveitando suítes de protocolos existentes para realizar comunicações seguras, tais como o IPsec (ZHANG; GUNTER, 2010) e o *Transport Layer Security* (TLS). Além de outros protocolos existentes como o DNP3[2], e sua extensão de segurança como o Secure DNP3[3] para comunicação em sistemas de energia também se tornaram um foco da padronização (WENYE; ZHUO, 2013).

A segurança atual de redes sem fios se baseia em tecnologias de padrões como o WPA2 (IEEE 802.11i, 2004) e o WiMAX (IEEE 802.16e, 2006). Os protocolos de redes sem fio têm diferentes graus de segurança. A segurança de redes cabeadas depende hoje de firewalls, redes privadas virtuais (VPNs) e tecnologias IPsec (IETF-RFC 6071, 2011). Mecanismos de segurança de camada

[2] DNP3 é um protocolo de sistema de controle mestre / escravo amplamente utilizado no setor elétrico para os sistemas SCADA de geração, transmissão e distribuição de energia elétrica.
[3] Secure DNP3 visa acrescentar autenticação de usuário e dispositivo, bem como proteger a integridade dos dados no protocolo DNP3. Secure DNP3 é um protocolo bidirecional que visa fornecer proteção entre as estações máster (HMI, servidores de controle) e estações de saída (PLC, RTU, IED).

superior, como o *Secure Shell* (SSH) e SSL / TLS também são usados (YAN *et al.,* 2012).

A segurança em *Smart Grid* envolve uma série de aspectos que vão desde a Segurança Cibernética a Segurança Física de instalações elétricas e das TIC (incluindo equipamentos). Vulnerabilidades e Ameaças são aspectos que precisam ser consideradas no início do processo de desenvolvimento de aplicações, bem como a privacidade. A privacidade é geralmente associada com a coleta, propriedade, controle de acesso, controle de integridade, distribuição, modificações, redefinição de objetivos, reconstrução e disposição de informações de identificação pessoal (PII), relativas a indivíduos e organizações.

A seguir, os termos em inglês security e safety são definidos para escopo deste trabalho. A Segurança (*Security*): Programas geralmente desenvolvidos em defesa da vida humana e dos próprios sistemas de energia. Já o termo *safety* se refere à seguridade e bem-estar das pessoas, e dos ativos tangíveis e intangíveis. Com um sistema que lida com a geração de energia, transmissão e distribuição, a responsabilidade da segurança se estende além dos muros do centro de dados. Um intruso pode, intencionalmente ou não, causar a energização de uma linha, o que colocaria em risco vidas.

Da mesma forma, uma linha pode ser desenergizada, de tal forma a causar apagões, danos aos sistemas de transmissão e de controle e, eventualmente, pôr em perigo a segurança dos trabalhadores e do público. A combinação de uma rede inteligente cada vez mais interligada e a crescente sofisticação das ameaças cibernéticas geram preocupações com a atual postura de lidar com a segurança na gestão da rede elétrica (HAHN; GOVINDARASU, 2011).

O sistema de energia tem necessidades específicas de desempenho e confiabilidade que variam de acordo com o sistema, e podem exigir medidas de segurança cibernéticas que diferem daquelas exigidas pela tecnologia da informação empresarial tradicional (TI). As soluções de segurança, como criptografia forte e infraestruturas de chaves públicas, que foram efetivamente implantadas para garantir a infraestrutura de TI de empresas e as aplicações de negócios, muitas vezes encontram limitações de desempenho e recursos quando aplicadas aos sistemas de energia. Muitos sistemas legados não foram projetados com a segurança como um recurso básico. As soluções devem implementar objetivos de

segurança consistentes que incluam acesso autorizado aos dados de mercado e de consumo, notificações confiáveis de status de equipamentos e auditoria.

## 1.2. Motivação

O NIST (*National Institute of Standards and Technology, USA*) e outras organizações estão avaliando as tecnologias de segurança existentes, tais como de controle de acesso, de autenticação e criptografia, que poderão ser usadas para proteger a Smart Grid. A evolução dos mecanismos de Segurança Cibernética foca o cumprimento dos denominados Objetivos de Segurança (NIST, 2009):

- Confidencialidade: preservar o acesso autorizado e restrições à informação e divulgação, incluindo os meios para proteção da privacidade pessoal e da propriedade das informações.
- Integridade: Proteção contra a modificação ou destruição inapropriada da informação.
- Disponibilidade: Garantir prontamente e de forma segura o acesso e uso das informações.

Confidencialidade, Integridade e Disponibilidade é da ordem de prioridade para um sistema de TI empresarial. No entanto, a Disponibilidade, Integridade e Confidencialidade é muitas vezes a ordem de prioridade para os sistemas de controle e proteção.

O modelo de referência SGIRM estabelece os níveis requeridos de Confidencialidade, Integridade e Disponibilidade nos fluxos de dados para cada uma das interfaces entre domínios, e entre entidades inter e intra domínios.

A comunidade internacional busca a padronização para permitir flexibilidade e versatilidade na configuração dos referidos níveis através da recomendação de adoção das Redes Privadas Virtuais (VPNs) e tecnologias IPsec (IETF-RFC 6071, 2011); a motivação foi pesquisar suas aplicações nos sistemas de energia e a discussão da diferença de prioridades quando aplicadas aos sistemas empresariais.

## 1.3. OBJETIVOS

### 1.3.1. Objetivo Geral

Esta dissertação de mestrado tem como objetivo geral desenvolver uma metodologia de implementação de Redes Privadas Virtuais (VPNs) e a parametrização do framework do protocolo IPsec, visando a segurança no fluxo de dados entre entidades que utilizam interfaces de comunicação entre gateways[4] de segurança dos domínios da Smart Grid, onde seja viável e recomendado o uso das VPNs e esse protocolo.

### 1.3.2. Objetivos Específicos

Como objetivos específicos que pretendem este trabalho são:

1. Implementar uma VPN IPsec entre os gateways de segurança dos domínios Distribuidor e Consumidor, na interface entre entidades destes domínios onde seja viável e recomendado o uso desse protocolo.
2. Verificar a aplicabilidade dos níveis de requerimento dos serviços de segurança: Integridade, Confidencialidade e Disponibilidade, recomendado pelo SGIRM.
3. Demonstrar a viabilidade e aplicabilidade da metodologia via simulações numa topologia básica de rede com equipamentos que simulem os gateways de segurança dos domínios.
4. Validar a metodologia com testes em Laboratório com a topologia básica de rede com equipamentos reais que representariam os gateways de segurança dos domínios.

## 1.4. Justificativa e Contribuição

Weerathunga *et al.* (2012), Yan *et al*. (2012) e Zhang; Gunter (2010), mencionam a necessidade de um estudo mais aprofundado para a aplicação das soluções das Redes Privadas Virtuais (VPNs) com a segurança do protocolo IPsec no fluxo de dados nos sistemas de energia*,* e que as soluções ou experiências

[4] Dispositivo destinado a interligar redes, separar domínios de colisão, traduzir protocolos de comunicação, executar criptografia e encapsulamento, e outras atividades relativas à segurança para o fluxo de dados.

existentes com essas tecnologias são de casos pontuais e não adotam as soluções do estado da arte que a segurança dos sistemas empresariais propicia atualmente.

Nesse sentido, contribuição desta pesquisa é uma metodologia de configuração ou parametrização dos componentes do framework do protocolo IPsec, para viabilizar sua adoção nas TIC da Smart Grid conforme recomendado pelo SGIRM.

### 1.5. Organização da dissertação

A dissertação está dividida em seis capítulos. No capítulo um, se incluem a Contextualização, Motivação, Objetivos e Contribuição pretendida da pesquisa e dissertação. O Capítulo dois aborda o estado da arte na Gestão e o estado da arte das Tecnologias de Segurança, com a fundamentação teórica e bibliográfica.

No capítulo três é apresentada a metodologia proposta de implementação de Redes Privadas Virtuais (VPNs) e parametrização do framework do protocolo de IPsec, o roteiro das tarefas para tal implementação, e as metodologias para as simulações e testes; no capítulo quatro são apresentadas as simulações e as respectivas análises dos processos e resultados.

No capítulo cinco são detalhados os testes em laboratório com equipamentos reais e também as respectivas análises dos resultados, visando a validação da metodologia proposta. O capítulo seis aborda as conclusões e trabalhos futuros.

# 2. ESTADO DA ARTE

Neste capítulo são apresentados o estado da arte da metodologia para gestão da segurança, estabelecida pelo SGIRM, e o estado da arte das tecnologias de segurança adotadas no âmbito empresarial, e adaptadas para sua aplicação nas infraestruturas da Smart Grid.

## 2.1. Gestão da Segurança

### 2.1.1. Princípios da Segurança da Informação

A gestão de segurança inclui a gestão de riscos, planos de segurança da informação e as políticas, procedimentos, normas, diretrizes, a classificação da informação, organização da segurança e educação em segurança. Uma abordagem sistemática para a concepção e implementação de um programa de Segurança Cibernética para a Smart Grid deve ser adaptado para atender às necessidades de negócios e de proteção da segurança de cada organização ou aplicação.

Cada organização deve desenvolver uma estratégia de Segurança Cibernética para a execução da sua parte do programa geral de segurança. As normas ISO/IEC 27000 e os padrões enumerados nas diretrizes da Smart Grid *Cyber Security* (NISTIR 7628, vol. 1) podem ser usadas como referências visando garantir a segurança.

### 2.1.2. O Processo da Segurança

Enquanto o processo da segurança aborda a Smart Grid em forma holística, a segurança da informação tem necessidades específicas. A segurança da informação consiste em medidas para prevenir o uso não autorizado, alteração ou recusa de utilização de dados. As principais atividades incluem o seguinte (IEEE STD 2030, 2011):

- **Avaliação de risco:** é usada para determinar o valor dos ativos de informação de uma organização, as ameaças a que estão expostos e as vulnerabilidades que oferecem, bem como a importância do risco total para a organização.

- **Políticas:** definem como a segurança deve ser implementada. Políticas definem os mecanismos de uso adequados para proteger as informações e sistemas, bem como a segurança física. Ele inclui vários aspectos, tais como as capacidades técnicas, melhores práticas, medidas preventivas, funcionários, resposta a incidentes, administração e gestão.
- **Implantação:** políticas de segurança, normas e medidas que sejam eficazes devem ser implementados por uma organização que pratica os devidos cuidados e diligências.
- **Treinamento:** a conscientização é o mecanismo apropriado para fornecer as informações necessárias aos empregados no que tange à segurança.
- **Auditoria:** esta função melhora a probabilidade de que os controles sejam configurados e monitorados corretamente em relação às políticas. As funções incluem a política de adesão das auditorias, avaliações periódicas e novas, e testes de penetração.

Essas atividades são uma extensão do processo de segurança de cinco etapas apresentadas na IEC 62351-1 TS, e são específicas para sistemas de energia e fornecem informações adicionais. A seguir se apresentam as principais atividades da Avaliação de Riscos e o conceitos da Política de Segurança:

**Avaliação de Riscos**

O risco é o potencial de perdas que requer proteção. Se não existe o risco, não há necessidade de segurança. Quando o risco é analisado, as vulnerabilidades e ameaças devem ser identificadas. A avaliação de riscos é essencial para a determinação dos controles necessários para a operação segura de um sistema de controle de potência que contém informações valiosas, sensíveis e críticas. É preciso identificar os riscos de segurança e modelar a dinâmica de sistemas de controle para encontrar uma solução ideal para monitorar ataques cibernéticos.

A avaliação de riscos, atividades realizadas por uma equipe de análise de riscos, inclui:

- Avaliação do valor dos ativos e da informação.
- Identificação de ameaças.
- Identificação de vulnerabilidades.

- Métodos de análise de riscos: Normas e metodologia definidas nos padrões ISO/IEC 27005.
- **Risco Total** = Em função das ameaças, vulnerabilidade e valor patrimonial.
- **Risco Residual** (se aceita conviver) = **Risco Total** menos **Contramedidas** (para reduzir riscos)
- Implementação da segurança: Identificar mecanismos de segurança atuais e avaliar a sua eficácia.
- Se uma organização decidir encerrar a atividade que está apresentando risco, isto é conhecido como a prevenção ou eliminação de riscos (*Risk Avoidance*). Exemplo: eliminação do uso do *Skype* nos terminais de controle do SCADA.
- **Mitigação de riscos** é uma abordagem em que o risco é reduzido para um nível considerado aceitável, a implementação de tecnologias de segurança (sistemas de firewalls, de intrusão/detecção e prevenção, criptografia, treinamento, etc.) representam uma forma de reduzir o risco.
- **Aceitação de Riscos** é uma abordagem utilizada quando a relação custo/benefício é superior a um, o que significa que o custo da medida preventiva supera o valor potencial de perda.

A gestão de segurança da informação inclui o processo de atribuição de prioridades, de acordo a um orçamento, para implementar e manter as medidas de redução de risco adequadas.

Após a quantidade de **Risco Total** ou **Risco Residual** ser determinada, a administração deve decidir como tratar e mitigar o risco, podendo: transferir, rejeitar, aceitar ou reduzir o risco.

**Política de Segurança**

Política de Segurança é um conjunto de princípios básicos para seguir, relacionados para estabelecer o que significa estar seguro para um sistema, organização ou outra entidade. Para uma organização, aborda as metas para o comportamento de seus membros, bem como as restrições impostas aos estranhos por mecanismos tais como portas, fechaduras, chaves e paredes. Um programa de segurança deve incluir políticas de segurança, normas, diretrizes, procedimentos, treinamento de conscientização de segurança, plano de resposta a incidentes, e um

programa de conformidade. Estes termos são descritos na série de padrões ISO/IEC 27000[5].

### 2.1.3. Segurança de Redes

Nesta seção inclui-se o conceito de Segurança de Redes, que especificamente se refere à segurança da rede de telecomunicações. Esta rede inclui todos os equipamentos ativos como roteadores, firewalls, switches, gateways, servidores, notebooks, desktops, etc., e os equipamentos passivos como enlaces físicos de cabeamento de cobre ou fibra ótica, e todas as tecnologias de redes sem fio, referenciadas nas interfaces lógicas que interconectam as entidades inter e intra domínios da perspectiva arquitetônica CT-IAP do SGIRM.

## 2.2. Tecnologias de Segurança

A seção 2.2.1 deste capítulo aborda as pesquisas e aplicações práticas que recomendam a utilização das Redes Privadas Virtuais (VPNs), tecnologias PKI (Infraestrutura de Chaves Públicas), IPsec e *Transport Layer Security* (TLS), como o estado da arte das tecnologias de segurança para o fluxo de dados na interoperabilidade da Smart Grid. As seções seguintes apresentam os conceitos e tecnologias sobre a Segurança das Redes Modernas, os serviços AAA *(Authentication, Authorization, and Accounting*), o IDS (*Intrusion Detection Systems)* e o IPS *(*Intrusion Prevention System), os *Firewalls*, os Sistemas de Criptografias devido à sua importância na configuração do framework IPsec, e por último as Redes Privadas Virtuais (VPNs) e a estrutura do protocolo de rede IPsec.

### 2.2.1. Fundamentação bibliográfica

Para a segurança cibernética na *Smart Grid* (YAN *et al.,* 2012) e (WENYE; ZHUO, 2013) recomendam a adoção de soluções abrangentes e uma arquitetura de comunicação integrada com a internet e com foco na segurança desde o início da

[5] A série da ISO 27000 mostra como uma organização pode implementar um Sistema de Gestão de Segurança da Informação (S.G.S.I.) baseado na norma ISO 27001. Num contexto amplo, a família da ISO 27000 é um conjunto de normas desenvolvidas que fornecem uma estrutura para gerenciamento de segurança da informação para qualquer organização, pública ou privada, de grande ou pequeno porte.

implementação, incluindo esquemas tradicionais como a tecnologia PKI (Infraestrutura de Chaves Públicas), mecanismos de Autenticação baseados em padrões da indústria, e o uso de protocolos de segurança baseados em padrões do estado da arte, e que as redes cabeadas estarão seguras com firewalls, Redes Privadas Virtuais (VPNs) e tecnologias IPsec (IETF-RFC 6071, 2011).

Os protocolos baseados na Internet como o IPv4 e IPv6, desenvolvidos ao longo de muitos anos e de uso generalizado, são uma referência de comunicação de baixo custo. Nivelando o conjunto de protocolos de segurança desenvolvido para IP [tais como o IPsec e o *Transport Layer Security* (TLS)] com esta referência de comunicação, se aproveita o vasto trabalho realizado nesta área por peritos em protocolos de comunicação.

Vários fornecedores que oferecem soluções SCADA e que têm diferentes capacidades e mecanismos de segurança, adotam protocolos como *Distributed Network Protocol 3* (DNP3), o *Generic Object Oriented Substations Events* (GOOSE), mas ainda há necessidade de tornar mais consistente as soluções de segurança aplicadas a tais implantações no SCADA. O *Federal Information Processing Standard* (FIPS) aprovou as soluções de criptografia *Advanced Encryption Standard* (AES) e *Triple Data Encryption* (3DES), que oferecem sólida segurança e desempenho. O NIST determinou que a solução 3DES provavelmente vai se tornar insegura até o ano de 2030. Considerando que os componentes de serviços públicos deverão ter vida longa, o AES seria a solução preferida para novos componentes (METKE; EKL, 2010).

A Segurança Cibernética na *Smart Grid* é vital para a confiabilidade das operações do sistema de energia. As aplicações das comunicações em sistemas de energia são diferentes das aplicações de sistemas empresariais (WEERATHUNGA *et al.,* 2012).

Ataques à confidencialidade dos comandos cibernéticos para o controle e operação do sistema energia poderão afetar sua integridade e disponibilidade. Porque com o conhecimento adequado da topologia do sistema, das configurações internas, e como a camada física responde aos comandos cibernéticos, o controle e operação ficam vulneráveis (GAMAGE *et al*., 2013).

Uma aplicação de túnel VPN IPsec, com solução de sistemas abertos, entre o gateway de uma subestação e o gateway do centro de controle do sistema de

energia, como mostrado na Figura 2-1, utilizou *o Encapsulating Security Payload* (ESP) como autenticador e os DES, 3DES, AES e outros, para criptografar o fluxo de dados. Vários testes de desempenho foram realizados no túnel VPN IPsec para determinar o equilíbrio entre segurança e o desempenho do túnel no gateway da subestação. A conclusão do trabalho recomenda o uso do túnel VPN IPsec para realizar comunicações seguras entre subestações e o centro de controle do sistema de energia.

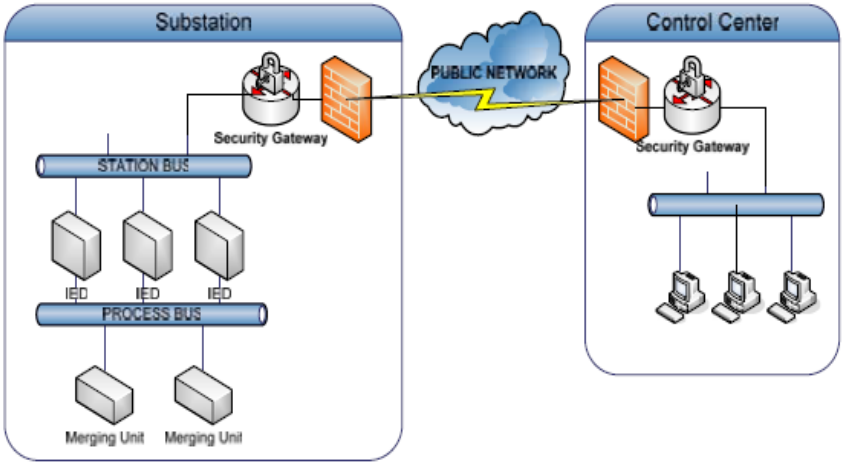


Figura 2-1 - Aplicação do Túnel IPsec - Fonte: Weerathunga *et al*. (2012).

Ericsson (2010) discute o papel de segurança cibernética em uma arquitetura de rede inteligente. Ericsson (2009) apresenta aplicações de segurança cibernética em redes dos sistemas de energia, e propôs uma estrutura funcional para a segurança da informação das concessionárias. Ramos (2012) realizou simulações com proteção de comunicação de dados através de criptografia obtendo resultados que não prejudicaram o tempo de resposta.

Naedele *et al.* (2001) investigaram as ameaças dos ataques baseados nas redes de subestações e propuseram um protocolo de comunicação segura para combater esses ataques. Horalek e Sobeslav (2010) propuseram as Redes Privadas Virtuais (VPNs) com IPsec para isolar a rede das salas de controle remotas da rede das subestações. Gungor e Lambert (2006) compararam a VPN baseada em *Multiprotocol Label Switching* (MPLS[6]) com a VPN baseada no IPsec para aplicações de automação do sistema elétrico, em termos de atributos de

[6] É um mecanismo de transporte de dados pertencente à família das redes de comutação de pacotes. O MPLS é padronizado pelo IETF através da RFC-3031.

desempenho, incluindo a qualidade do serviço (QoS), confiabilidade, escalabilidade, robustez, segurança e gestão de rede.

Projetistas de sistemas muitas vezes identificam a necessidade e especificam o uso de protocolos de segurança, como o *Secure Shell* (SSH) e o IPsec, mas não consideram os detalhes relacionados com o estabelecimento da segurança associada entre os *end-points* (dispositivos finais) das comunicações. Tal abordagem é provável que resulte num sistema em que sejam necessários procedimentos para o gerenciamento de chaves de segurança (*secure key management*) que pode rapidamente tornar-se um pesadelo operacional (METKE; EKL, 2010).

Com base nos requisitos de segurança para *Smart Grid*, bem como a escalabilidade e disponibilidade exigida para o sistema, acredita-se que a utilização das tecnologias de chave pública PKI, juntamente com elementos de computação confiáveis, apoiados por outros componentes, é a melhor solução global para a *Smart Grid* (METKE; EKL, 2010).

Mesmo que a tecnologia IPsec tenha sido completamente discutida na literatura acadêmica, uma discussão mais aprofundada sobre aplicações de IPsec em ambiente de subestações é necessária. Como a solidez da segurança de um túnel IPsec depende estritamente de seus algoritmos de criptografia e de seu gerenciamento de chaves, é importante para avaliar algoritmos de criptografia para túneis IPsec nos gateways de subestações (WEERATHUNGA *et al.,* 2012).

Esta dissertação segue as recomendações descritas nos parágrafos anteriores, ao aplicar os conceitos e tecnologias de Segurança de Redes com soluções PKI, incluindo a seleção dos algoritmos de autenticação de dispositivos, e encriptação e criptografia de chaves e dados, no processo de configuração das Redes Privadas Virtuais (VPNs) e do framework IPsec, visando adaptar tal processo aos requerimentos de segurança para a *Smart Grid* determinados no SGIRM.

### 2.2.2. Conceitos e Tecnologias

Apresentamos conceitos e tecnologias que compõem a solução holística para a segurança da Smart Grid. Estes incluem dispositivos, serviços, componentes, algoritmos do estado da arte para autenticação, encriptação e criptografias de

chaves e dados, e soluções PKI que devem fazer parte, direta ou indiretamente, das soluções IPsec VPN.

**Segurança de Redes e Ameaças Modernas**

A segurança da rede é uma parte integrante da rede de computadores, pois envolve protocolos, tecnologias, equipamentos, ferramentas e técnicas para proteger os dados e reduzir as ameaças.

A maioria das ameaças de dentro da rede está alavancada nos protocolos e tecnologias utilizadas na rede de área local (LAN) ou na infraestrutura de comutação. Estas ameaças internas se dividem em duas categorias: *Spoofing e Denial of Service (DoS)*. Os ataques de spoofing são ataques em que um dispositivo tenta se passar por outro através da falsificação de dados. Os ataques DoS tornam os recursos de computador indisponíveis para os usuários a quem se destinam.

- Vírus: software malicioso anexado a outro programa para executar ações indesejadas em um sistema final.
- Worm: executa um código arbitrário e instala cópias de si mesmo na memória de um computador infectado, que então infecta outros hospedeiros.
- Cavalo de Tróia: aplicativo que foi escrito para parecer outro aplicativo. Quando é baixado e aberto, ataca o computador do usuário final a partir de dentro.
- Ataques de Reconhecimento: envolvem a descoberta não autorizada e mapeamento de sistemas, serviços e vulnerabilidades.
- Ataques de Acesso: exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP, e serviços da Internet para conseguir a entrada às contas de web, bancos de dados confidenciais e outras informações sensíveis.
- Ataques DoS *(Denial of Service Attack*): enviam um número extremamente grande de pedidos através de uma rede ou da Internet. Essas solicitações excessivas sobrecarregam o dispositivo de destino causando degradação no desempenho.
- Ataques DDoS *(Distributed Denial of Service Attack):* semelhantes em intenção de um ataque *DoS*, exceto que um ataque *DDoS* se origina a partir de múltiplas fontes de coordenadas.

Ataques de Acesso, de Reconhecimento, DoS e DDoS são mitigados com técnicas, dispositivos e tecnologias específicas.

Os procedimentos de Autenticação, Autorização e Contabilidade (“O triplo A”, do inglês *Authentication, authorization, and accounting*) é uma maneira de controlar quem está autorizado a acessar redes (autenticação), o que pode ser feito quando estiverem lá (autorização) e observar as ações executadas ao acessá-la (contabilidade):

- **Autenticação:** Os usuários ou dispositivos finais e administradores devem provar quem são. Em sistemas e redes grandes, uma solução mais escalável é a autenticação externa. A autenticação externa permite que todos os usuários sejam autenticados por meio de um servidor de rede externa. As duas opções mais populares para a autenticação externa de usuários são RADIUS e TACACS+[7].
- **Autorização:** Após o usuário ser autenticado, os serviços de autorização determinam quais recursos o usuário pode acessar e quais operações o usuário tem permissão para executar.
- **Contabilidade:** A contabilidade ou contabilização registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo que o recurso é acessado e todas as alterações efetuadas. A contabilização rastreia como os recursos de sistemas e da rede são usados.

**Sistema de Detecção de Intrusão - IDS**

Uma das primeiras ferramentas de segurança de rede foi o Sistema de Detecção de Intrusão (*IDS-Intrusion Detection System*). Um IDS oferece detecção em tempo real de certos tipos de ataques, enquanto eles estão em andamento. Esta detecção permite que os professionais de segurança de rede reduzam mais rapidamente o impacto negativo desses ataques a dispositivos de rede e usuários.

**Sistema de Prevenção de Intrusão - IPS**

Sistema ou Sensor de Prevenção de Intrusão *(IPS-Intrusion Prevention System or sensor)* substitui a solução IDS. Dispositivos de IPS permitem a detecção

[7] Terminal Access Controller Access-Control System (TACACS) é um protocolo de autenticação remoto usado para comunicação com servidores de autenticação, comumente em redes UNIX. O TACACS permite que um servidor de acesso remoto se comunique com um servidor de autenticação para verificar se o usuário tem acesso à rede.

de atividade maliciosa e têm a capacidade de bloquear automaticamente o ataque em tempo real.

***Firewalls***

Foram desenvolvidos para evitar o tráfego indesejado entre em áreas prescritas dentro de uma rede, proporcionando assim a Segurança de Perímetro. Originalmente eram dispositivos de rede existentes às quais foram adicionados recursos de software, tais como os roteadores. Ao longo do tempo, desenvolveram-se firewalls autônomos, ou firewalls que permitem aos roteadores e switches efetuarem a atividade de descarregamento de memória e processamento intensivo de filtragem de pacotes dedicado.

### 2.2.3. Sistemas de Criptologia

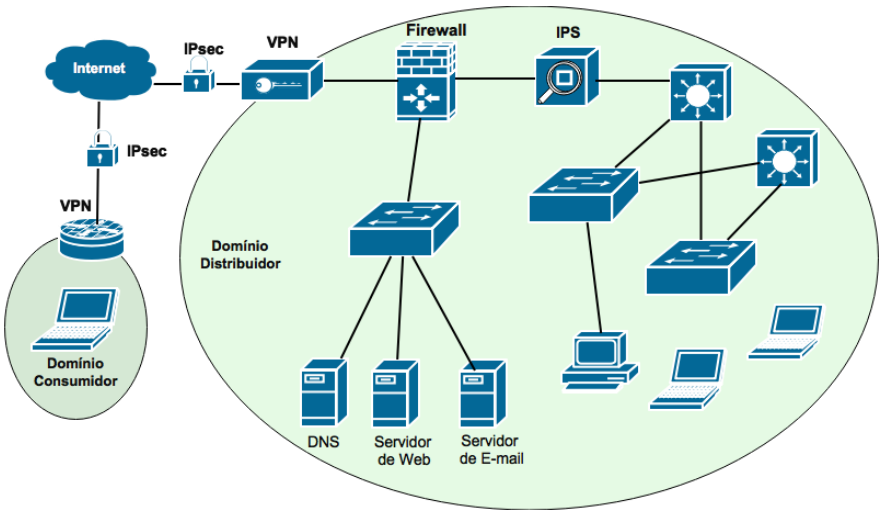


Figura 2-2 - Conjunto de Soluções para Segurança - Fonte: O Autor, 2015

Protegem-se os dispositivos da rede controlando os acessos via AAA, por meio dos recursos de firewall, e implementando IPSs, conforme arquitetura sugerida na Figura 2-2. Estas características combinadas protegem os dispositivos da infraestrutura, bem como os dispositivos finais dentro das redes locais. Os métodos de criptografia devem proteger os tráfegos dos dados quando atravessarem a Internet pública.

**Criptografia**

Muitas redes modernas garantem a Autenticação com protocolos como o HMAC (*Hash-based Message Authentication Code*), a Integridade é assegurada através da aplicação de protocolos MD5 (*Message Digest 5* ) ou SHA-1 (*Secure Hash Algorithm 1*) e a Confidencialidade dos dados por meio de algoritmos de criptografia simétrica, incluindo DES (*Data Encryption Standard)*, 3DES (*Triple Data Encryption Standard)* e AES (*Advanced Encryption Standard)*, ou algoritmos assimétricos, incluindo RSA (*Rivest, Shamir & Adleman*) e a infraestrutura de chave pública – PKI (METKE; EKL, 2010).

Algoritmos de criptografia simétrica são baseados na premissa de que cada uma das partes conhece a chave pré-compartilhada. Algoritmos de criptografia assimétrica baseiam-se no pressuposto de que as duas partes que se comunicam ainda não tenham compartilhado uma chave e devem estabelecer um método seguro para fazê-lo.

Autenticação, Integridade e Confidencialidade são componentes da criptografia. A criptografia é tanto a prática como o estudo de ocultar informações. Serviços de criptografia são a base para muitas implementações de segurança e são usados para garantir a proteção dos dados quando esses dados podem estar expostos a partes não confiáveis. Compreender as funções básicas de criptografia e como a criptografia fornece Confidencialidade e Integridade é importante na criação de uma política de segurança bem sucedida. Também é importante entender os problemas que estão envolvidos na gestão da chave de criptografia.

A criptografia utiliza um algoritmo específico, chamado de cifra, para criptografar e descriptografar mensagens. A cifra é uma série de etapas bem definidas que podem ser seguidas como um procedimento quando criptografar e descriptografar mensagens. Dentre os vários métodos de criação de texto cifrado, o DES e o 3DES usam a transposição como parte do algoritmo.

**Criptoanálise**

Desde que houve a criptografia, houve a criptoanálise. Criptoanálise é a prática e estudo para determinar o sentido das informações criptografadas (quebrar o código), sem acesso à chave do segredo compartilhado. Vários métodos são usados na criptoanálise: Ataque de Força Bruta, Ataque ao Texto

Cifrado, Ataque ao Texto Conhecido, Ataque ao Texto Escolhido, *Meet-in-the-Middle*, etc. Cada método tem sua força baseada no espaço de chaves (quantidade possível de chaves) e a porção dos dados cifrados, ou não, previamente conhecidos.

Uma máquina de decifrar o DES foi usada para recuperar uma chave DES de 56 bits em 22 horas usando Ataque de Força Bruta, e estima-se ser necessário 149 trilhões de anos para quebrar o AES usando o mesmo método.

### 2.2.4. As Redes Privadas Virtuais - VPNs

No sentido mais simples, uma VPN conecta dois pontos finais através de uma rede pública para formar uma conexão lógica. As ligações lógicas podem ser feitas na Camada 2 ou na Camada 3 do modelo OSI. Tecnologias VPNs podem ser classificadas em geral sobre estes modelos de conexão lógica como VPNs de Camada 2 ou VPNs de Camada 3. Exemplo de VPN Camada 3 é a VPN IPsec.

A segurança na VPNs é fornecida pelos serviços IPsec que permitem a autenticação, integridade, controle de acesso e confidencialidade. Com o IPsec, as informações trocadas entre locais remotos podem ser criptografadas e autenticadas. Tanto as VPNs de acesso remoto como as VPNs site-a-site podem ser implantadas usando IPsec.

Alguns dos benefícios das VPNs são:

- **Economia** - VPNs permitem que as organizações utilizem de forma econômica o transporte na Internet para conectar dispositivos, escritórios remotos e usuários remotos para a sede principal da empresa. As VPNs eliminam os caros links WAN dedicados e bancos de modem.
- **Segurança** - VPNs com IPsec proporcionam segurança usando criptografia e protocolos de autenticação avançados que protegem os dados contra acesso não autorizado.
- **Escalabilidade** - VPNs permitem que corporações usem a infraestrutura de Internet e dispositivos que estão dentro de provedores de serviços de Internet (ISPs). Isto torna mais fácil adicionar novos usuários e dispositivos, de modo que as empresas possam adicionar capacidade significativa sem adição de infraestrutura significativa.

## 2.3. Estrutura dos Protocolos IPsec

O IPsec é um padrão IETF (RFC 6071, 2011) que define como uma VPN pode ser configurada usando o protocolo de endereçamento IP. O IPsec é uma estrutura de padrões abertos que explicita as regras para comunicações seguras. Baseia-se em algoritmos existentes para implementar a criptografia, autenticação e intercâmbio de chaves.

O IPsec funciona na camada de rede, protegendo e autenticando os pacotes IP entre dispositivos IPsec (*peers*) participantes. Como resultado, o IPsec pode proteger praticamente todo o tráfego da aplicação, porque a proteção pode ser implementada a partir da camada 4 até a camada 7. Todas as implementações do IPsec têm um cabeçalho de texto simples da camada 3, para que não haja problemas com roteamento. O IPsec funciona sobre todos os protocolos da Camada 2. O quadro IPsec é composto por cinco blocos:

- O primeiro representa o protocolo IPsec. As opções incluem o ESP e AH.
- O segundo representa o tipo de confidencialidade implementado usando um algoritmo de criptografia, como o DES, 3DES, AES ou SEAL. A escolha depende do nível de segurança necessário.
- O terceiro representa o tipo de integridade que pode ser implementado usando MD5 ou SHA.
- O quarto representa como a chave secreta compartilhada é estabelecida. Os dois métodos são pré-compartilhado e assinado digitalmente usando RSA.
- O quinto representa o grupo de algoritmos DH. Há quatro algoritmos DH de intercâmbio de chaves separadas para escolher, incluindo DH Grupo 1 (DH1), DH Grupo 2 (DH2), DH Grupo 5 (DH5) e DH Grupo 7 (DH7). O tipo de grupo selecionado depende das necessidades específicas.

O IPsec fornece o framework (estrutura) e o administrador escolhe os algoritmos que serão utilizados para a execução dos serviços de segurança nessa estrutura. O fato do IPsec não ser vinculativo a algoritmos específicos, permite que algoritmos mais recentes e melhores sejam implementados sem remendar as normas IPsec existentes.

O IPsec pode garantir um caminho entre um par de gateways, um par de hosts, ou um gateway e host. E oferece as seguintes funções essenciais de segurança:

- **Confidencialidade** - usando criptografia.
- **Integridade** - usando um algoritmo de hash como o MD5 ou SHA.
- **Autenticação** - usando o IKE para autenticar usuários e dispositivos que poderão realizar a comunicação de forma independente. O IKE usa vários tipos de autenticações, incluindo nome de usuário e senha, senha de uso único, biometria, PSK - Pre-shared key (chaves pré-compartilhadas), e certificados digitais.
- ***Secure key exchange*** (Intercâmbio Seguro de Chaves) - usando o algoritmo DH (*Diffie Helman*) para fornecer um método de intercâmbio de chave pública para pares visando estabelecer uma chave secreta compartilhada.

### 2.3.1. Confidencialidade

A confidencialidade é conseguida através da criptografia do tráfego à medida que viaja pela VPN. O grau de segurança depende do comprimento da chave e do algoritmo de encriptação. A seguir estão alguns algoritmos de criptografia e comprimentos de chave que as VPNs usam (Figura 2-3):

- DES, 3DES, AES e SEAL (*Encryption Optimized-Software Algorithm*)

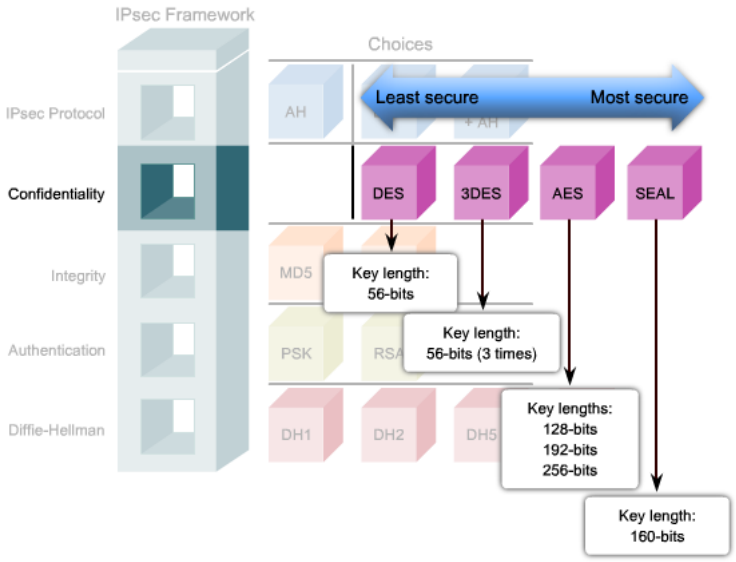


Figura 2-3 - Confidencialidade - Fonte: Adaptado de IETF- RFC 6071, 2011

### 2.3.2. Integridade

A integridade na VPN é provida por um método para garantir que o conteúdo não foi alterado. Um algoritmo de integridade de dados pode oferecer essa garantia. *Hashed Message Authentication Codes* (HMAC) é esse algoritmo, e os dois mais comuns são (Figura 2-4):

- HMAC-Message Digest 5 (HMAC-MD5)
- HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1)

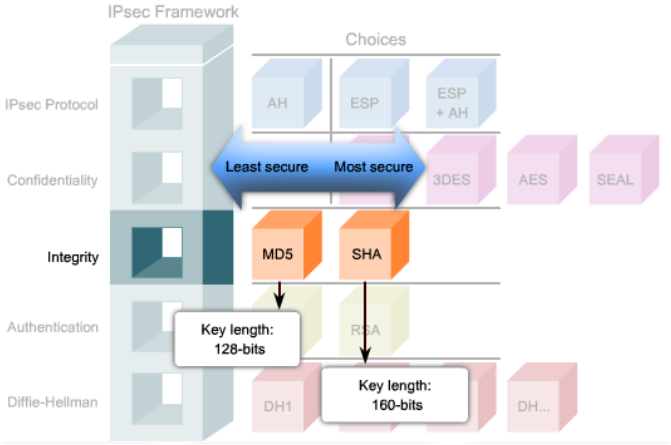


Figura 2-4 - Integridade - Fonte: Adaptado de IETF- RFC 6071, 2011

O HMAC-SHA-1 é considerada criptograficamente mais forte que o HMAC-MD5. Recomenda-se quando uma segurança de nível levemente superior é importante.

### 2.3.3. Autenticação

Existem dois métodos principais para configurar a autenticação de pares (Figura 2-5):

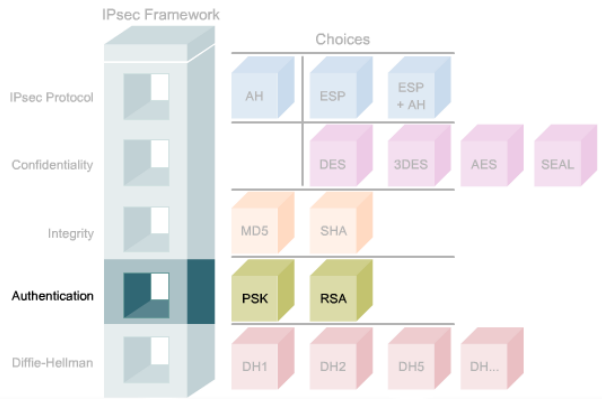


Figura 2-5 - Autenticação - Fonte: Adaptado de IETF- RFC 6071, 2011

**1. Chaves pré-compartilhadas** (*Pre-shared Keys - PSKs*) - Um valor de chave secreta pré-compartilhada é entrado em cada ponto manualmente e é usado para autenticar os pares. Em cada extremidade, a PSK é combinada com outras informações para formar a chave de autenticação. Cada ponto deve autenticar seu par oposto antes que o túnel seja considerado seguro. Chaves pré-compartilhadas são fáceis de configurar manualmente, mas não escalam bem porque cada ponto IPsec deve ser configurado com cada chave pré-compartilhada de todos os outros pares com os quais ele se comunica.

No dispositivo local, a chave de autenticação e a informação de identidade (informações específicas do dispositivo) são enviadas através de um algoritmo de Hash para formar o Hash_L. A Autenticação em uma via é estabelecida através do envio do Hash_L para o dispositivo remoto. Se o dispositivo remoto pode criar de forma independente o mesmo hash, o dispositivo local é autenticado. O processo de autenticação continua repetindo estes passos na direção inversa.

**2. Assinaturas RSA** - O intercâmbio de certificados digitais autentica os pares. O dispositivo local deriva um hash e criptografa com a sua chave privada. O hash criptografado está anexado à mensagem e é encaminhado para a outra extremidade e funciona como uma assinatura. Na extremidade remota, o hash encriptado é descriptografado usando a chave pública do local final. Se o hash descriptografado corresponde ao hash recalculado, a assinatura é verdadeira. Cada ponto deve autenticar seu par oposto antes que o túnel seja considerado seguro.

Uma forma menos comum de realizar a autenticação é através de *nonces* (valores aleatórios) RSA-criptografados. Um nonce é um número aleatório que é gerado pelo par. Nonces RSA criptografados usam o RSA para criptografar o valor de uso único e outros valores.

***Secure Key Exchange* -** Intercâmbio Seguro de Chaves: Os algoritmos de criptografia, como DES, 3DES e AES, bem como os algoritmos de hash o MD5 e SHA-1 requerem uma chave secreta simétrica compartilhada para executar a criptografia e descriptografia.

E-mail, correio, ou correio expresso pode ser usado para enviar as chaves secretas compartilhadas para os administradores dos dispositivos. Mas o método de troca de chaves mais simples é um método de troca de chave pública.

O acordo Diffie-Helman (DH) é um método de intercâmbio de chave pública que possibilita que pares estabeleçam uma chave secreta compartilhada que somente eles conheçam, mesmo que eles estejam se comunicando através de um canal inseguro. Variações do intercâmbio de chave DH são especificadas como grupos DH. Existem vários grupos DH (Figura 2-6):

- Grupos DH 1, 2 e 5 suportam exponenciação sobre um módulo principal com tamanhos de chaves de 768, 1024 e 1536 bits, respectivamente. Estes grupos já não são recomendados para uso depois de 2012.
- Grupos DH 14, 15 e 16 usam tamanhos de chaves maiores, com 2048, 3072 e 4096 bits, respectivamente, e são recomendado para uso até 2030.
- Grupos DH 19, 20 e 24 suportam Criptografia de Curva Elíptica (ECC), que reduz o tempo necessário para gerar chaves. Com tamanhos de chaves de 256, 384 e 2048 bits, respectivamente. O Grupo DH 24 é o preferido pela longevidade na utilização.

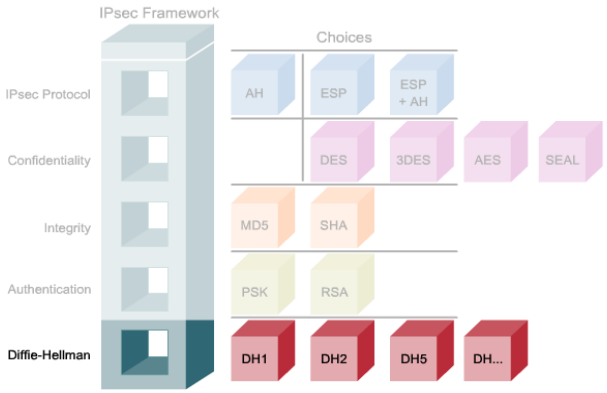


Figura 2-6 - Algoritmos Diffie-Helman - Fonte: Adaptado de IETF- RFC 6071, 2011

O grupo DH escolhido deve ser suficientemente forte (ter bits suficientes) para proteger as chaves IPsec durante a negociação. Por exemplo, o grupo DH 1 é forte o suficiente para suportar apenas DES e 3DES, mas não AES. Durante a configuração do túnel, pares VPN negociam que grupo DH utilizar.

### 2.3.4. Protocolos de Enquadramento IPsec

O IPsec é uma estrutura de padrões abertos. O IPsec enuncia o sistema de mensagens para garantir as comunicações e se baseia em algoritmos existentes. Os dois principais protocolos de enquadramento IPsec são: AH e ESP. O protocolo IPsec é o primeiro bloco da construção do quadro. A escolha de AH ou ESP estabelece que outros blocos de construção estarão disponíveis.

***Authentication Header* (AH):** O AH (protocolo IP 51) é o protocolo apropriado para usar quando a confidencialidade não for exigida ou permitida. Fornece autenticação e integridade dos dados para pacotes IP que são passados entre dois sistemas. Assegura-se que a origem dos dados é R1 ou R2, (Figura 2-7), e verifica que os dados não foram alterados durante o trânsito. AH não fornece confidencialidade de dados. Todo o texto é transportado sem criptografia. Se o protocolo AH é usado sozinho, ele fornece uma proteção fraca.

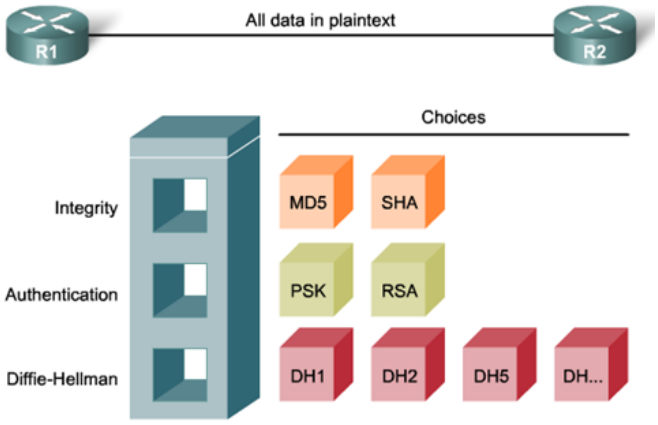


Figura 2-7 - Enquadramento AH - Fonte: Adaptado de IETF- RFC 6071, 2011

O AH consegue a autenticidade através da aplicação de uma função hash unidirecional com chave sobre o pacote para criar um hash ou *Message Digest* (síntese da mensagem). O hash é combinado com o texto e é transmitido. O receptor detecta alterações em qualquer parte do pacote que ocorrem durante o trânsito realizando a mesma função hash unidirecional no pacote recebido e compara o resultado com o valor da *Message Digest* (síntese da mensagem) que o remetente enviou. O hash unidirecional também envolve uma chave secreta compartilhada entre os dois sistemas a fim de preservar a autenticidade.

A função AH é aplicada a todo o pacote, com exceção do campo do cabeçalho IP mutável que mudam em trânsito. Por exemplo, os campos *Time to Live* (TTL), que são modificados pelos roteadores ao longo do caminho de transmissão, são campos mutáveis. O processo de AH ocorre nesta ordem:

1º. O cabeçalho IP e o *payload* (carga útil) de dados são misturados usando a chave secreta compartilhada.

2º. O *hash* constrói um novo cabeçalho AH, que é inserido no pacote original.

3º. O novo pacote é transmitido para o roteador par do IPsec.

4º. O roteador par mistura (*hashes*) o cabeçalho IP e o payload de dados usando a chave secreta compartilhada, extrai o *hash* transmitido a partir do cabeçalho AH, e compara os dois *hashes*.

Os *hashes* devem coincidir exatamente. Se um bit é alterado no pacote transmitido, a saída do *hash* sobre as alterações de pacotes recebidos e o cabeçalho AH não irá corresponder. AH suporta os algoritmos HMAC-MD5 e HMAC-SHA-1. AH pode ter problemas se o ambiente usa NAT (*Network Alocation Table*)[8].

***Encapsulating Security Payload*** **(ESP):** O ESP (protocolo IP 50) pode garantir a confidencialidade e autenticação. Fornece confidencialidade através da criptografia no pacote IP ao ocultar a carga de dados e as identidades de origem e de destino final. O ESP fornece autenticação para o pacote IP interno e o cabeçalho ESP. Autenticação fornece a autenticação da origem dos dados e a integridade dos dados. Embora tanto a criptografia como a autenticação sejam opcionais no ESP, no mínimo, um deles deve ser selecionado.

O ESP fornece confidencialidade, criptografando o *payload* (carga útil). Suporta uma variedade de algoritmos de criptografia simétrica. Se o ESP é selecionado como protocolo IPsec, um algoritmo de criptografia também deve ser selecionado. O algoritmo padrão para IPsec é o DES de 56 bits. Também podem ser usados o 3DES, AES, ou SEAL para criptografia mais forte (Figura 2-8).

O ESP também pode fornecer integridade e autenticação. Em primeiro lugar, o payload é criptografado. Em seguida, o payload criptografado é enviado através de

[8] A principal razão é que o AH aplica o hash no cabeçalho do IP e qualquer adulteração, mesmo pelo NAT, poderá ser detectada. Neste caso, os pacotes serão descartados silenciosamente. Então, a menos que haja um dispositivo (talvez o dispositivo de gateway de segurança), que faça a tradução do NAT ao original (um caso específico de duas vezes NAT), o AH não irá funcionar através de dispositivos NAT.

um algoritmo de hash, HMAC-MD5 ou HMAC-SHA-1. O hash fornece autenticação e integridade de dados para o payload. Opcionalmente, o ESP também pode reforçar a proteção anti repetição. A proteção verifica se cada pacote é único e não é duplicado. Esta proteção assegura que um hacker não poderá interceptar pacotes e inserir pacotes alterados no fluxo de dados. Anti repetição é normalmente usado no ESP, mas também é suportado no AH.

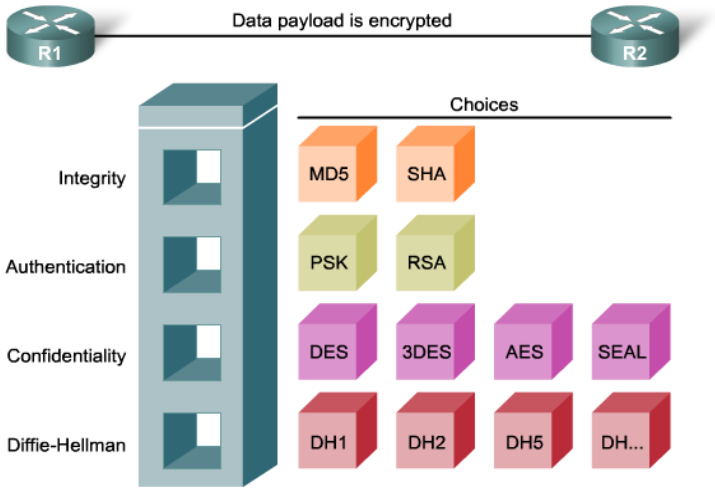


Figura 2-8 - Enquadramento ESP - Fonte: Adaptado de IETF- RFC 6071, 2011.

Os dados originais são protegidos pelo ESP, porque todo o datagrama IP original e trailer ESP são criptografados. Com a autenticação ESP, o datagrama IP e trailer criptografados, e o cabeçalho ESP, estão incluídos no processo de hashing. Por último, um novo cabeçalho de IP é anexado ao payload. O novo endereço IP é usado para encaminhar o pacote através da Internet.

Quando a autenticação e criptografia são selecionadas, a criptografia é efetuada em primeiro lugar. Uma razão para esta ordem de processamento é que facilita a rápida detecção e rejeição pelo dispositivo de recepção dos pacotes falsos ou repetidos. Antes de descriptografar o pacote, o receptor pode autenticar os pacotes de entrada. Ao fazer isso, ele pode detectar rapidamente os problemas e, potencialmente, reduzir o impacto dos ataques DoS.

O ESP e o AH podem ser aplicados a pacotes IP em dois modos diferentes, o modo de transporte e modo de túnel:

**1. Modo de transporte:** No modo de transporte, a segurança é fornecida apenas para a camada de transporte e acima, do modelo OSI. O modo de transporte protege a carga útil (payload) do pacote, mas deixa o endereço IP original em texto

simples. O endereço IP original é usado para encaminhar o pacote através da Internet. O modo de transporte ESP é usado entre hosts.

**2. Modo Túnel:** O modo túnel oferece segurança para o pacote IP original completo. O pacote IP original é encriptado e é então encapsulado em outro pacote IP. Isto é conhecido como criptografia de IP-em-IP. O endereço IP do pacote IP externo é usado para encaminhar o pacote através da Internet.

O modo de túnel ESP é usado entre um host e um gateway de segurança[9], ou entre dois gateways de segurança[10]. Para aplicações de gateway-para-gateway, em vez de carregar o IPsec em todos os computadores nos escritórios remotos e corporativos, é mais fácil ter os gateways de segurança executando a criptografia e encapsulamento IP-em-IP. O modo de túnel ESP é usado em aplicações de acesso remoto IPsec. Uma rede local pode não ter um roteador para realizar o encapsulamento e criptografia IPsec. Neste caso, um cliente IPsec rodando no PC executa o encapsulamento e criptografia IPsec IP-em-IP. No caso do gateway de segurança, o roteador descapsula e decifra o pacote. O processo de VPN envolve a seleção e aplicação de muitos parâmetros.

### 2.3.5. Intercâmbio de Chaves pela Internet (IKE)

A solução VPN IPsec negocia os parâmetros de troca de chaves, estabelece uma chave compartilhada, autentica o mesmo nível, e negocia os parâmetros de criptografia. Os parâmetros negociados entre dois dispositivos são conhecidos como uma Associação de Segurança (SA).

**Associações de Segurança** (*SA - Security Associations*)

Uma SA é um bloco de construção básico do IPsec. Associações de segurança são mantidas dentro de uma base de dados SA (SADB), que é estabelecida por cada dispositivo. A VPN tem entradas SA que definem os parâmetros de criptografia IPsec, bem como entradas SA que definem os parâmetros de troca de chaves.

---

[9] E este seria o caso da interface entre as entidades *Energy Services* e *Smart Meter* do domínio Consumidor (ver Figura 3-2).

[10] Este seria o caso da interface entre a entidade *Smart Meter* do domínio Consumidor com os domínios Distribuidor e Provedor de Serviços, via interfaces CT-12 e CT-29 (ver Figura 3-2).

Todos os sistemas de criptografia devem lidar com as questões da gestão de chaves. O DH é usado para criar a chave secreta compartilhada. No entanto, o IPsec usa o protocolo *Internet Key Exchange* (IKE) para estabelecer o processo de troca de chaves.

Em vez de transmitir as chaves diretamente através de uma rede, o IKE calcula as chaves compartilhadas com base na troca de uma série de pacotes de dados. O IKE é nivelado no UDP e usa a porta UDP 500 para trocar informações IKE entre os gateways de segurança. Pacotes Porta UDP 500 devem ser permitidas em qualquer interface IP envolvida para conectar um par de gateways de segurança.

O IKE é definido na IETF (RFC 6071, 2011). É um protocolo híbrido, combinando *o Internet Security Association* e o *Key Management Protocol* (ISAKMP[11]) e outros métodos de troca de chaves. O ISAKMP define o formato da mensagem, os mecanismos de um protocolo de troca de chave, e o processo de negociação para construir uma SA para o IPsec. O ISAKMP não define como as chaves são gerenciadas ou compartilhadas entre os dois pares IPsec.

O IKE combina estes protocolos para construir conexões IPsec seguras entre os dispositivos. Estabelece SAs que são mutuamente aceitáveis para cada par. Cada par deve ter o ISAKMP e os parâmetros IPsec idênticos para estabelecer uma VPN operacional e segura. Note-se que os termos ISAKMP e IKE são comumente usados pela indústria para se referir ao IKE. Uma alternativa à utilização do IKE é configurar manualmente todos os parâmetros necessários para estabelecer uma conexão segura o IPsec. Este processo é impraticável porque não escala.

Neste capítulo dois foi detalhada a gestão, os conceitos e as tecnologias de segurança, e foi abordada a estrutura dos protocolos IPsec, como fundamentações para propor, no capítulo a seguir, a metodologia de implementação da VPN e da parametrização do framework do IPsec.

[11] Textualmente pode ser: Protocolo de Gestão de Chaves para Associação de Segurança pela Internet.

# 3. METODOLOGIA

No capítulo um desta dissertação foi mencionada a necessidade de um estudo mais aprofundado para a aplicação das Redes Privadas Virtuais (VPNs) com o protocolo IPsec nos sistemas de energia. A fundamentação bibliográfica apresentada no capítulo dois recomenda aplicar os conceitos e tecnologias de Segurança de Redes com soluções PKI, algoritmos de autenticação de dispositivos, encriptação e criptografia de chaves e dados, no processo de configuração das Redes Privadas Virtuais (VPNs) e do framework IPsec.

Também no capítulo dois foram apresentadas as soluções de segurança, e detalhada a estrutura do protocolo IPsec para destacá-lo comparativamente com outros protocolos utilizados nos sistemas de energia.

Com base nestes argumentos, é proposta uma metodologia, que se detalha neste capitulo três, para sistematizar a implementação das Redes Privadas Virtuais (VPNs) com a adoção do protocolo IPsec para oferecer a segurança no fluxo de dados na interoperabilidade da *Smart Grid*.

Para ilustrar a metodologia, é apresentado na seção 3.1 um Diagrama de Fluxo de atividades, processos, decisões e seleção de opções para parametrização do framework IPsec, prévio à implementação da VPN IPsec, para operacionalizar os Serviços de Segurança para o fluxo de dados na interface a ser selecionada. Este Diagrama de Fluxo é complementado com as informações detalhadas nas distintas seções deste capitulo três.

Na seção 3.2 deste capítulo é apresentada a visão do SGIRM sobre os Objetivos de Segurança, para na seção 3.3 ser abordada a compatibilidade dos blocos do framework IPsec com tais objetivos. Na seção 3.4 é apresentada uma proposta de Tabela de opções de blocos IPsec para oferecer os Serviços de Segurança que visam atender esses objetivos. Na seção 3.5 é apresentada uma topologia básica da arquitetura de rede para representar a CT-IAP visando implementação da VPN IPsec Site-a-Site[12].

Na seção 3.6, o processo indicado no último bloco do Diagrama de Fluxo, é detalhado como um roteiro de tarefas com execução passo-a-passo para sua

[12] No contexto desta dissertação, Site-a-Site se aplica como DomÍnio-a-DomÍnio ou Entidade-a-Entidade ou, eventualmente, DomÍnio-a-Entidade, da CT-IAP do SGIRM.

programação em CLI (Interface de Linhas de Comando) para a implementação e operacionalização da VPN e componentes do framework do IPsec.

Nas seções 3.7 e 3.8 são descritas as metodologias das simulações e testes com equipamentos reais, respectivamente, visando demonstrar a viabilidade, aplicabilidade e validação da metodologia de parametrização.

Adota-se a arquitetura do modelo de referência CT-IAP (Perspectiva Arquitetônica de Interoperabilidade das Tecnologias de Comunicações) e se pretende aplicar as recomendações do SGIRM sobre os níveis de requerimento nos serviços de segurança para Integridade, Confidencialidade e Disponibilidade, exclusivamente para os fluxos de informações ou dados, sem visar a priori sua aplicação nas comunicações para interoperabilidade dos serviços de proteção, comando e controle do PS-IAP (Perspectiva Arquitetônica de Interoperabilidade do Sistema de Energia).

## 3.1. Diagrama de Fluxo da Metodologia Proposta de Parametrização IPsec

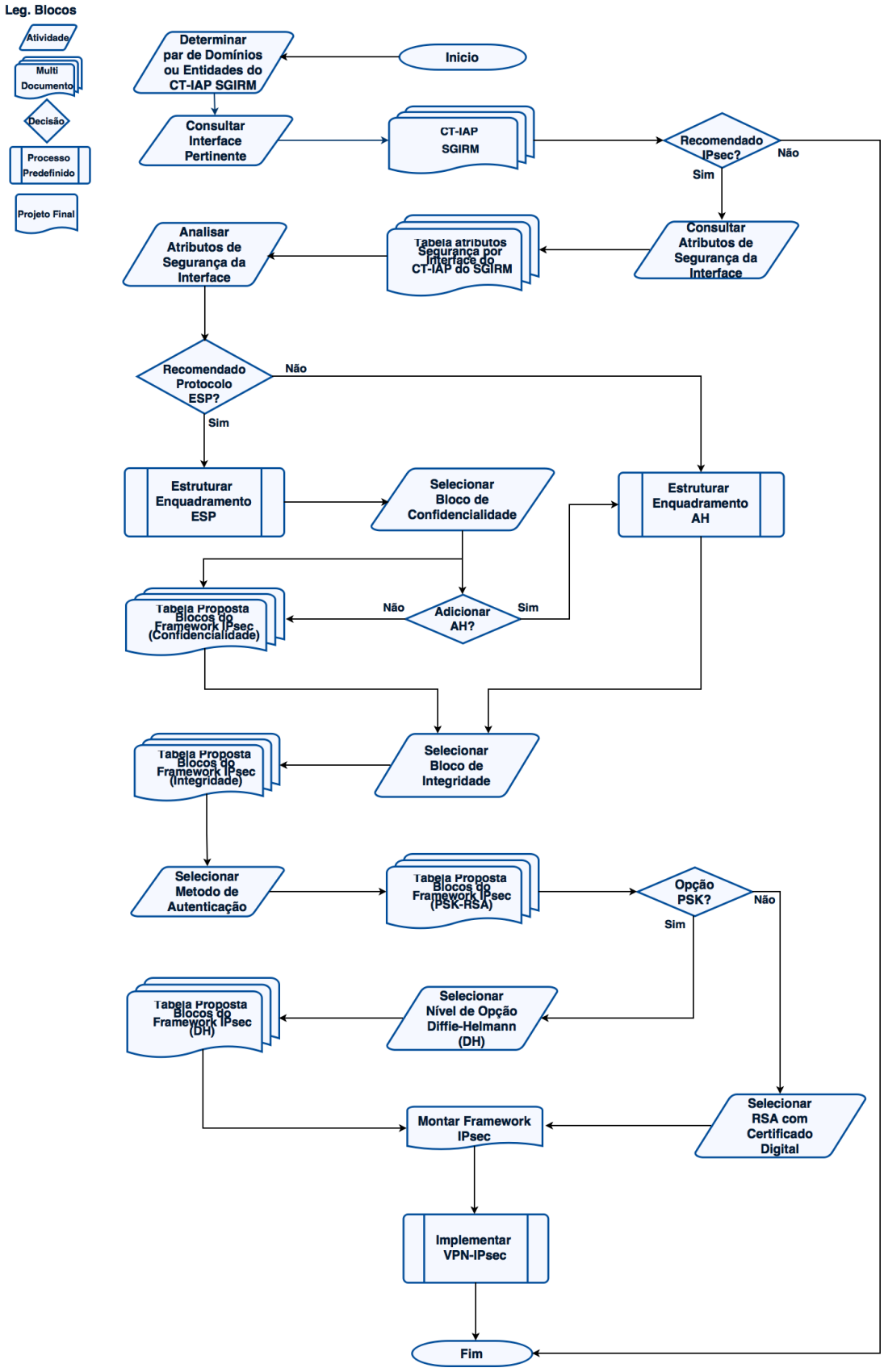


Figura 3-1 - Metodologia de Parametrização VPN IPsec. Fonte: O Autor, 2015

## 3.2. O SGIRM e os Objetivos de Segurança

A cada tipo de fluxo de informação ou dados dentro de um sistema de comunicação, ou no próprio sistema, deve ser atribuída uma categoria de segurança que considera o nível de impacto para uma interface ou para um sistema em particular em relação ao atendimento de cada um dos três objetivos de segurança: a Confidencialidade, a Integridade, e a Disponibilidade dos dados. Um nível baixo de impacto L (*Low*), moderado M (*Moderate*), ou elevado H (*High*) representa o impacto sobre as operações, ativos, ou indivíduos, caso haja uma violação nos sistemas (CIP STANDARDS, 2015).

As definições do SGIRM a respeito do impacto potencial sobre o atributo dos objetivos de segurança estão na Tabela 3-1, mas sua interpretação poderá depender da visão de cada empresa do setor de energia e suas prioridades respeito à segurança.

Atribuições da categoria de segurança podem ser feitas em diversas fases de desenvolvimento ou construção de arquiteturas de sistemas, incluindo durante a avaliação preliminar de produtos ou em processo de certificação, ou no reconhecimento dos requisitos de proteção para infraestruturas críticas (IEEE STD 2030, 2011).

Tabela 3-1 - Impacto nos Objetivos de Segurança – Fonte: IEEE STD 2030, 2011

| **Impacto Potencial** | | | |
|---|---|---|---|
| **Objetivo de Segurança** | **Baixo (L)** | **Moderado (M)** | **Alto (H)** |
| **Confidencialidade**<br>Preservar restrições autorizadas sobre acesso e divulgação às informações, incluindo os meios para proteção da privacidade pessoal e informações proprietárias. | A divulgação não autorizada de informações poderia ter um efeito adverso limitado nas operações e ativos da organização, ou em indivíduos. | A divulgação não autorizada de informações poderia ter um efeito adverso serio nas operações e ativos da organização, ou em indivíduos. | A divulgação não autorizada de informações poderia ter um efeito adverso severo ou catastrófico nas operações e ativos da organização, ou em indivíduos. |
| **Integridade**<br>Proteger da indevida modificação ou destruição de informações. | A modificação ou destruição não autorizada de informações poderia ter um efeito adverso limitado nas operações e ativos da organização, ou em indivíduos. | A modificação ou destruição não autorizada de informações poderia ter um efeito adverso serio nas operações e ativos da organização, ou em indivíduos. | A modificação ou destruição não autorizada de informações poderia ter um efeito adverso severo ou catastrófico nas operações e ativos da organização, ou em indivíduos. |

| | | | |
|---|---|---|---|
| **Disponibilidade**<br>Garantir prontamente o acesso seguro e uso de informações. | A interrupção do acesso ou do uso de informações, ou um sistema de informação, poderia ter um efeito adverso limitado nas operações e ativos da organização,<br>ou em indivíduos. | A interrupção do acesso ou do uso de informações, ou um sistema de informação, poderia ter um efeito adverso serio nas operações e ativos da organização,<br>ou em indivíduos. | A interrupção do acesso ou do uso de informações, ou um<br>sistema de informação, poderia ter um efeito adverso severo ou catastrófico nas operações e ativos da organização, ou em indivíduos. |

O SGIRM atribuiu as categorias de segurança para todas as interfaces de comunicação entre domínios, e entre entidades inter, e intra, domínios, da CT-IAP e estabeleceu os níveis de requerimento da *Integridade, Confidencialidade e Disponibilidade*, como objetivos de segurança. Uma parte é apresentada na Tabela 3-2. Conforme indicado na Tabela 3-2, por exemplo, a interface CT-12 entre a entidade *Smart Meter Energy Services* do domínio Consumidor e a entidade *Neighborhood Area Network* do domínio Distribuidor (interfaces e entidades mostradas na Figura 3-2) deverá ter alta (H) Confidencialidade, alta (H) Integridade e alta (H) Disponibilidade.

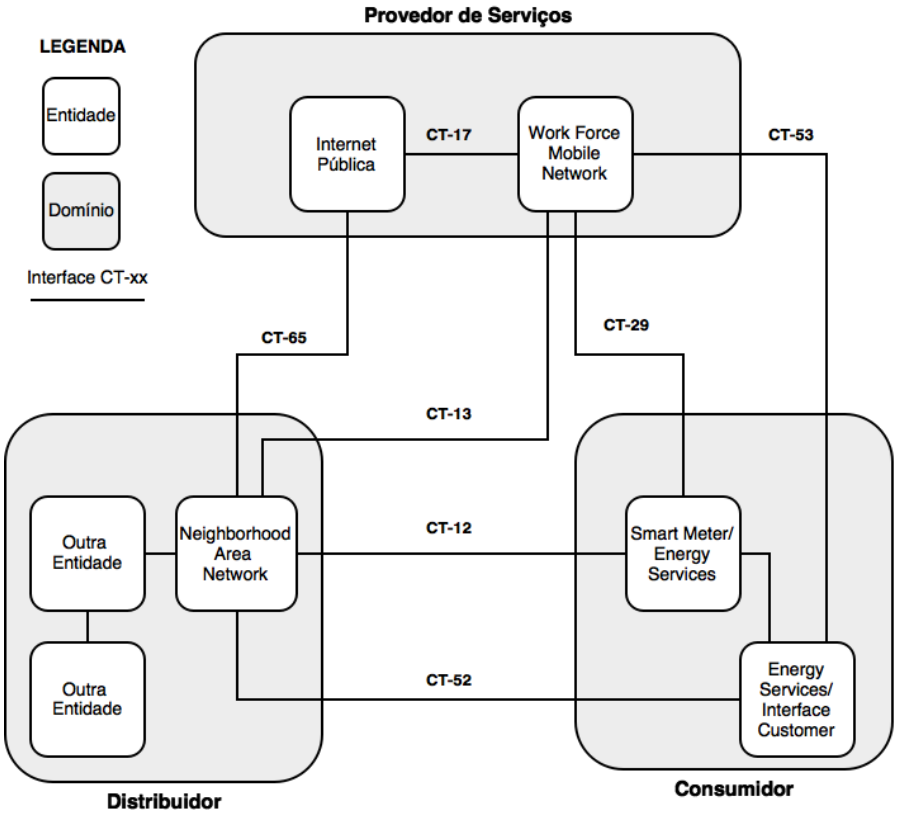


Figura 3-2 - Interfaces Smart Meter-NAN-WNM - Fonte: Adaptado de IEEE STD 2030, 2011

Tabela 3-2 - Níveis de Segurança por Interface - Fonte: IEEE STD 2030, 2011

| **Interface de Comunicação da *Smart Grid*** | **Requisitos dos Objetivos de Segurança** | | |
|---|---|---|---|
| | Confidencialidade | Integridade | Disponibilidade |
| CT-12 | H | H | H |
| CT-13 | L | H | M |
| CT-29 | H | H | M |
| CT-52 | H | M | L |

Para implementar os serviços que visem os objetivos de segurança, devem ser identificados seus mecanismos e avaliar suas eficácias antes selecioná-los, o que exige uma abordagem de análise de custo / benefício. O custo dos serviços incluem muitos itens de custo do produto, e é necessário procurá-los nos recentes documentos publicados (ISO/IEC 27000 a 27008, 27010 a 27011 e 27019), e especificamente o ISO/IEC 27033-1 que aborda a segurança de redes.

A Tabela 3-3 mostra a relação entre os serviços de segurança e tipos de ataques, e é usada para determinar os mecanismos de proteção necessários.

Tabela 3-3 - Serviços de Segurança por Ataque - Fonte: IEEE STD 2030, 2011

| **Ataques (Criptoanálise)** | **Serviços de Segurança** | | | |
|---|---|---|---|---|
| | Confidencialidade | Integridade | Disponibilidade | Contabilidade (Não Repúdio) |
| Acesso | X | | | X |
| Modificação | | X | | X |
| Negação de Serviço | | | X | |
| Repúdio | | X | | X |

Os tipos de Ataques, a Confidencialidade, a Integridade e a Contabilidade (ou Prestação de Contas) foram abordados no capítulo dois. O serviço de Contabilidade não protege contra ataques por si só. Deve ser utilizado em combinação com outros serviços para torná-los mais eficazes. Sem este serviço, alguns mecanismos de Integridade e Confidencialidade, como o de anti repetição falhariam. Mecanismos de proteção incluem a identificação e autenticação.

O serviço de Disponibilidade prevê que a informação seja útil. Backups é a forma mais simples de garantir a disponibilidade, mas em alguns contextos da *Smart Grid* não é o suficiente. É preciso tempo para recuperar informações de backups, especialmente quando os backups residem em um local remoto. Ao contrário dos backups, sistemas configurados com *fail-over*[13] tem a capacidade de poder detectar falhas e restabelecer a capacidade (processamento, acesso às informações, ou comunicações) por um processo automático, através da utilização de hardware redundante. No entanto, os mecanismos de disponibilidade podem ser os mecanismos de segurança mais caros em uma organização. O serviço de Disponibilidade é usado para reduzir os efeitos ou se recuperar de ataques de negação de serviço. A Disponibilidade não requer da Contabilidade.

### 3.3. A Compatibilidade do IPsec com os Serviços de Segurança

Dentre os quatro serviços de segurança, três deles: a Confidencialidade, a Integridade, e a Contabilidade (embutido nos processos de identificação e autenticação do serviço de Confidencialidade), compõem o framework (estrutura) do protocolo de segurança IPsec.

A parametrização do IPsec consiste na escolha apropriada de cada um dos cinco blocos do framework, conforme mostrado na Figura 3-3, em função ao tipo de protocolo IPsec a ser adotado, à complexidade dos algoritmos de criptografia, chaves e seu método de intercâmbio, e seu comprimento, necessários para atender o nível de requerimento dos serviços de segurança para o fluxo de dados (IETF-RFC 6071, 2011).

As variáveis linguísticas H (alta), M (moderada) e L (baixa) dos objetivos de segurança das tabelas do SGIRM, e em particular da Tabela 3-2, deverão ter uma escala de correspondência apropriada a cada um dos blocos na formatação do framework IPsec.

[13] Em computação, o conceito de tolerância a falhas (em Inglês: fail-over) refere-se à capacidade de um sistema acessar informações, mesmo se ocorrer um erro ou falha do sistema.

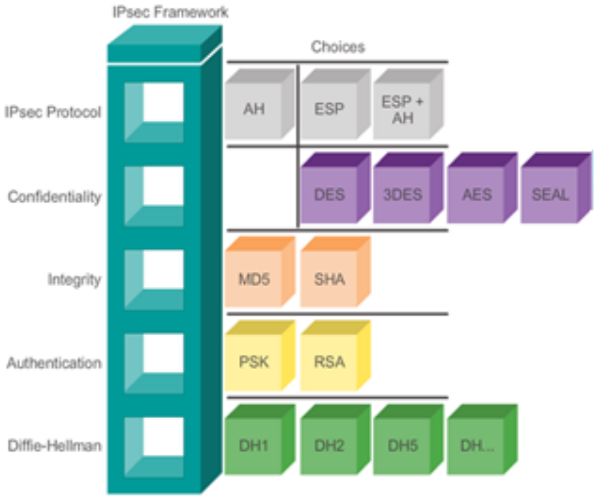


Figura 3-3 - Framework do IPsec - Fonte: Adaptado de IETF- RFC 6071, 2011

Uma abordagem apropriada para dar um tratamento matemático às variáveis linguísticas dos objetivos de segurança seria com as aplicações da Teoria de Conjuntos Nebulosos ou Fuzzy (ZADEH, 1973). Isto visaria obter uma interpretação menos imprecisa[14] e mais próxima de um centro de gravidade[15] do que se esperaria de um espaço de amostra de expectativas sobre os serviços de segurança.

### 3.4. Proposta de Tabela de Blocos IPsec x Serviços de Segurança

Conforme o diagrama de fluxo da Figura 3-1, a Tabela de Blocos Enquadramento IPsec é a primeira tabela a ser consultada a partir da atividade “Analisar Atributos de Segurança da Interface”. Esta análise definirá o tipo de Enquadramento que o protocolo IPsec utilizará: ESP, AH ou ESP+AH. Nos seguintes passos mostrados no diagrama, a cada atividade de seleção de opções de blocos IPsec, serão consultadas as tabelas de blocos de Confidencialidade, blocos Integridade, e blocos de Autenticação incluindo os grupos DH.

Em base a uma análise qualitativa fundamentada na complexidade dos algoritmos de criptografia, incluindo seu custo computacional (overhead), chaves e seu método de intercâmbio, vida útil, e seu comprimento, (p.e. AH, DES, 3DES, SHA, PSK, DH1, etc.) detalhadas nos capítulos dois, são propostas na Tabela 3-4, Tabela 3-5, Tabela 3-6 e Tabela 3-7, correspondências de cada opção de blocos do

[14] A Lógica Fuzzy é um paradigma efetivo para lidar com a imprecisão. Ele pode ser usado para tirar observações difusas e imprecisas das entradas e ainda chegar a valores nítidos e precisos para as saídas.
[15] Valor numérico que representa o centro de gravidade da distribuição de possibilidades de saída de um sistema Fuzzy.

framework IPsec necessárias para atender os níveis de requerimento dos serviços da Tabela 3-2.

Como o framework IPsec coloca a disposição várias opções para cada um dos blocos a serem parametrizados para a Confidencialidade e a Integridade dos dados que fluirão no túnel VPN IPsec a ser implementado, o critério adotado para a escolha das opções é atribuir cada opção (blocos: Protocolo IPsec, Confidencialidade, Integridade, Autenticação e Diffie-Helman) menos resistente à criptoanálise, ao nível de Serviços de Segurança L (baixo); e a opção mais resistente à criptoanálise, ao nível de Serviços de Segurança H (alto). Para o nível de Serviço M (moderado), as opções com resistência intermediária.

Esta metodologia de implementação, juntamente com as simulações, testes e resultados apresentados, visam validar esta proposta. Poderão ser feitas outras escolhas de opções de blocos IPsec de acordo às políticas de segurança ou à relação custo-benefício a serem adotadas por cada empresa do setor de energia.

O diagrama de fluxo da Figura 3-4 indicam as atividades e passos que correspondem ao processo de seleção das opções de enquadramento do IPsec:

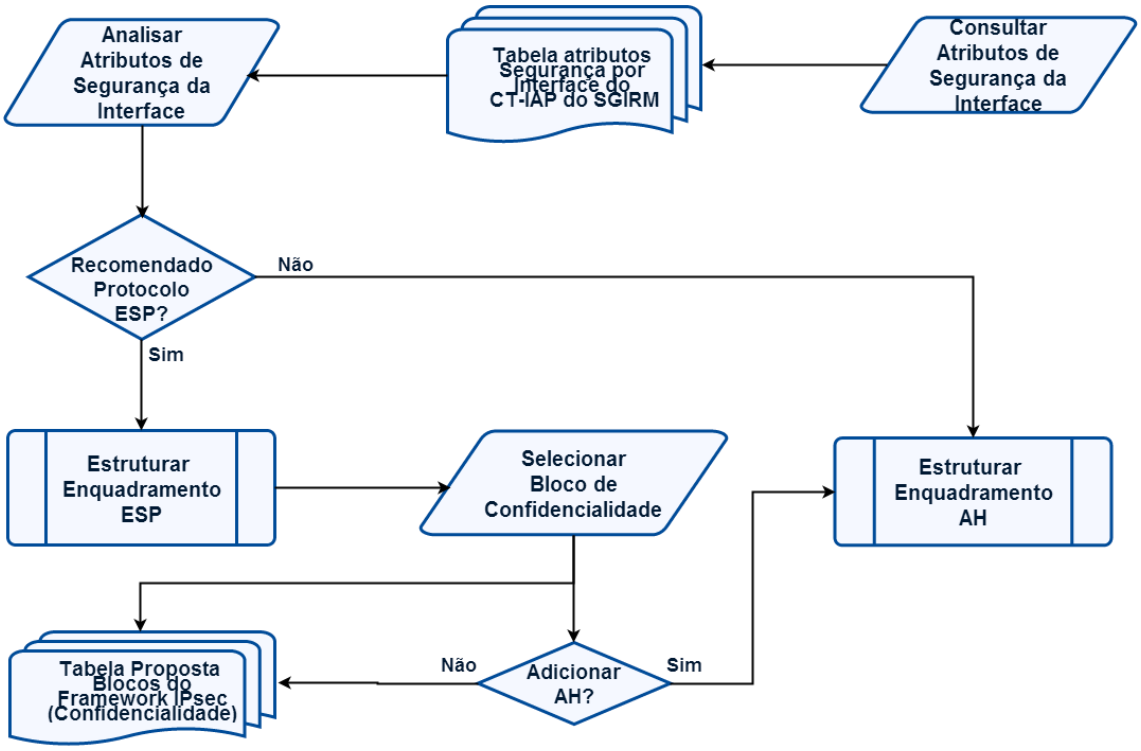


Figura 3-4 - Diagrama de Fluxo de Enquadramento IPsec - Fonte: O Autor, 2015

A proposta desta dissertação para o enquadramento IPsec por serviços de segurança são apresentadas na Tabela 3-4:

Tabela 3-4 - Tabela de Blocos Enquadramento IPsec – Fonte: O Autor, 2015

| **Framework IPsec** | | **Referências** | | **Serviços de Segurança** | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Vida útil (ano)**[16] | **Overhead (ms)**[17] | **Confidencialidade** | | | **Integridade** | | |
| **Bloco** | **Opções** | NIST, 2012. NIST, 2015. | Kuhurana, *et al,* 2007. Seibel, *et al,* 2011 Weerathunga, *et al*., 2012. | L | M | H | L | M | H |
| **Enquadramento** | AH | Ver Bloco Integridade | Ver Bloco Integridade | ✔[18] | | | ✔ | ✔ | ✔ |
| | ESP | Ver Bloco Confidencialidade | Ver Bloco Confidencialidade | | ✔ | | | ✔ | |
| | ESP+AH | Ver Blocos Integridade e Confidencialidade | Ver Blocos Integridade e Confidencialidade | | | ✔ | | | ✔ |

Na sequencia, é utilizado o diagrama de fluxo da Figura 3-5 que indicam as atividades e passos que correspondem ao processo de seleção das opções dos blocos de Confidencialidade:

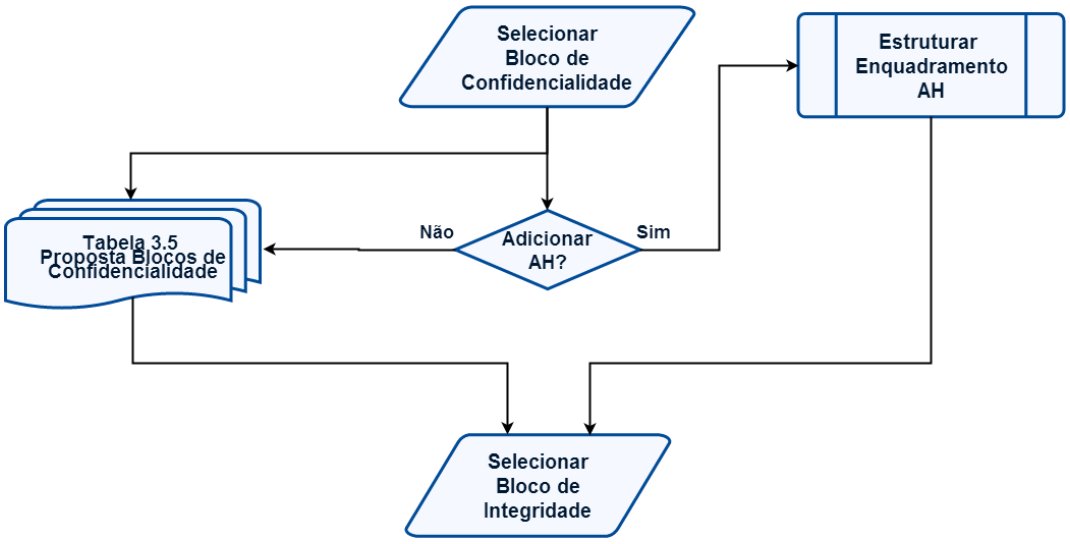


Figura 3-5 - Diagrama de Fluxo de Confidencialidade - Fonte: O Autor, 2015

[16] A vida útil varia também em função à magnitude dos números primos utilizados, junto com as chaves, nos cálculos de fatoração modular ou logaritmos discretos usados na criptografia.
[17] Diferença de latências, em milissegundos, em decorrência do custo computacional no desempenho dos protocolos de criptografias e tamanho das chaves, em payloads de 1500 bytes, em links de 100 e 1000 Mbps. Desktops usados pelas referências: Processador AMD Opteron 2.2 Ghz 248, SO Linux; Processador Intel Pentium III 863 MHz, Linux Ubuntu10.04.2, LTS(kernel 2.6.32).
[18] Indica a opção do framework sugerida pelo Autor para o serviço de segurança requerido.

Sendo a proposta desta dissertação para os blocos de Confidencialidade por serviços de segurança apresentadas na Tabela 3-5:

Tabela 3-5 - Tabela de Blocos Confidencialidade – Fonte: O Autor, 2015

| **Framework IPsec** | | **Referências** | | **Serviços de Segurança** | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Vida útil (ano)** | **Overhead (ms)** | **Confidencialidade** | | | **Integridade** | | |
| **Bloco** | **Opções** | NIST, 2012. NIST, 2015. | Kuhurana, *et al,* 2007. Seibel, *et al,* 2011 Weerathunga, *et al*., 2012. | L | M | H | L | M | H |
| **Confidencialidade** | DES 56 bits | 2015 | 0,70[19] | ✔ | | | NA[20] | NA | NA |
| | 3DES 168 | 2015-2030 | 1,02 | | ✔ | ✔ | NA | NA | NA |
| | AES 128 | >[21] 2030 | 0,53 | | ✔ | ✔ | NA | NA | NA |
| | AES 192 | >> 2030 | ND[22] | | | ✔ | NA | NA | NA |
| | AES 256 | >>> 2030 | 0,82 | | | ✔ | NA | NA | NA |
| | SEAL 160 | > 2030 | ND | | | ✔ | NA | NA | NA |

Seguidamente, o diagrama de fluxo da Figura 3-6 indicam as atividades e passos que correspondem ao processo de seleção dos blocos de Integridade:

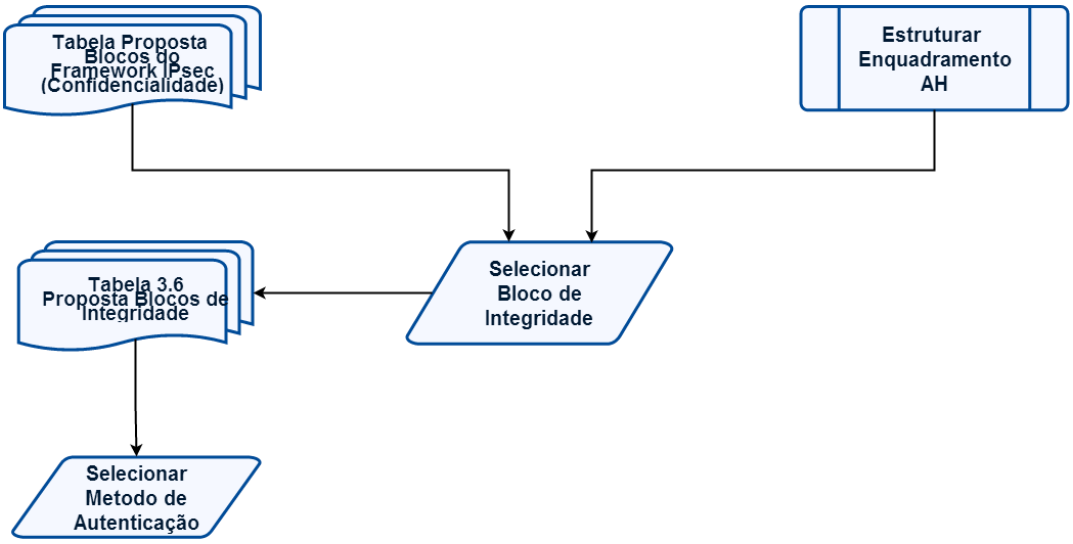


Figura 3-6 - Diagrama de Fluxo de Integridade - Fonte: O Autor, 2015

[19] Em conjunto com MD5. Idem para 3DES e AES 128.
[20] NA: Não aplicável.
[21] O NIST não é muito preciso para definr “>”, ”>>” e “>>>”. Mas, sugere que “>” é até 2050.
[22] ND: Dado preciso não disponível.

Sendo a proposta desta dissertação para os blocos de Integridade por serviços de segurança apresentadas na Tabela 3-6:

Tabela 3-6 - Tabela de Blocos Integridade – Fonte: O Autor, 2015

| **Framework IPsec** | | **Referências** | | **Serviços de Segurança** | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Vida útil (ano)** | **Overhead (ms)** | **Confidencialidade** | | | **Integridade** | | |
| **Bloco** | **Opções** | NIST, 2012. NIST, 2015. | Kuhurana, *et al,* 2007. Seibel, *et al,* 2011 Weerathunga, *et al*., 2012. | L | M | H | L | M | H |
| **Integridade** | MD5 128 | 2015 | 1,02[23] | NA | NA | NA | ✔ | ✔ | |
| | SHA-1 160 | 2015-2030 | 1,08 | NA | NA | NA | | ✔ | ✔ |
| | SHA-224 | 2030 | ND | NA | NA | NA | | ✔ | ✔ |
| | SHA-256 | > 2030 | 1,12 | NA | NA | NA | | | ✔ |
| | SHA-384 | >> 2030 | ND | NA | NA | NA | | | ✔ |
| | SHA-512 | >>> 2030 | ND | NA | NA | NA | | | ✔ |

E finalmente, o diagrama de fluxo da Figura 3-7 indicam as atividades e passos que correspondem ao processo de seleção das opções dos blocos de Autenticação:

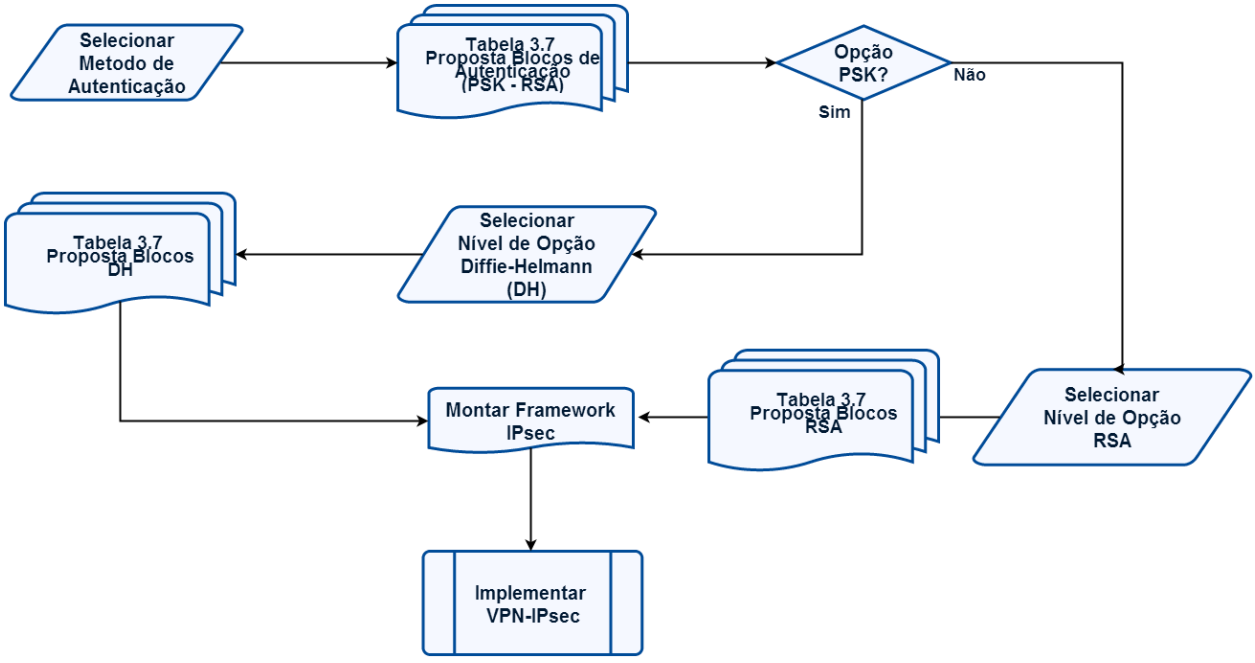


Figura 3-7 - Diagrama de Fluxo de Autenticação - Fonte: O Autor, 2015

[23] Em conjunto com 3DES. Idem para SHA-1 e SHA-256.

Sendo a proposta desta dissertação para os blocos de Autenticação por serviços de segurança são apresentadas na Tabela 3-7:

Tabela 3-7 - Tabela de Blocos Autenticação e DH – Fonte: O Autor, 2015

| **Framework IPsec** | | **Referências** | | **Serviços de Segurança** | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Vida útil (ano)** | **Overhead (ms)** | **Confidencialidade** | | | **Integridade** | | |
| **Bloco** | **Opções** | NIST, 2012. NIST, 2015. | Kuhurana, *et al,* 2007. Seibel, *et al,* 2011 Weerathunga, *et al*., 2012. | L | M | H | L | M | H |
| **Autenticação** | PKS | 2012 - >>2030 | DH1-24 | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| | RSA 512 | > 2030 | 13,09[24] | | ✔ | ✔ | | ✔ | ✔ |
| | RSA 1024 | > 2030 | 88,2 | | | ✔ | | | ✔ |
| | RSA 2048 | >>2030 | 798,25 | | | ✔ | | | ✔ |
| | RSA 4096 | >>>2030 | ND | | | ✔ | | | ✔ |
| | ECC 160 | 2015 | 3,36[25] | | ✔ | ✔ | | ✔ | ✔ |
| | ECC 224 | 2015-2030 | 7,05 | | ✔ | ✔ | | ✔ | ✔ |
| | ECC 256 | > 2030 | ND | | | ✔ | | | ✔ |
| | ECC 512 | >> 2030 | ND | | | ✔ | | | ✔ |
| **Diffie-Helman** | DH1 768 | 2012 | ND | ✔ | | | ✔ | | |
| | DH2 1024 | 2012 | ND | ✔ | | | ✔ | | |
| | DH5 1536 | 2012 | ND | ✔ | | | ✔ | | |
| | DH14 2048 | 2030 | ND | | ✔ | ✔ | | ✔ | ✔ |
| | DH15 3072 | 2030 | ND | | | ✔ | | | ✔ |
| | DH16 4096 | 2030 | ND | | | ✔ | | | ✔ |
| | DH19 [26] 256 | > 2030 | ND | | | ✔ | | | ✔ |
| | DH20 384 | > 2030 | ND | | | ✔ | | | ✔ |
| | DH24 2048 | >> 2030 | ND | | | ✔ | | | ✔ |

[24] Para o RSA inclui os tempos de encriptação, desencriptação, assinatura, geração e verificação de chaves, e exponenciação modular, no processo da criptografia.
[25] Para ECC (Criptografia de Curva Eliptica) inclui os tempos de computação DH, assinatura, geração e verificação de chaves, e multiplicação de ponto da curva, no processo da criptografia.
[26] DH 19 a DH 24 suportam ECC (Criptografia de Curva Eliptica)

## 3.5. Topologia Básica da Arquitetura de Redes da CT-IAP

Assume-se uma topologia básica com base na CT-IAP com uma arquitetura da rede que interconectam, através das interfaces principais, os sete domínios do SGIRM, representado na Figura 3-8, referência (WENYE; ZHUO, 2013), que adota o conceito de gateway de segurança para cada domínio.

Cada um dos domínios conta com um gateway de segurança que são os roteadores que suportam os recursos de VPN e IPsec compatíveis com os serviços de segurança requeridos pelo SGIRM.

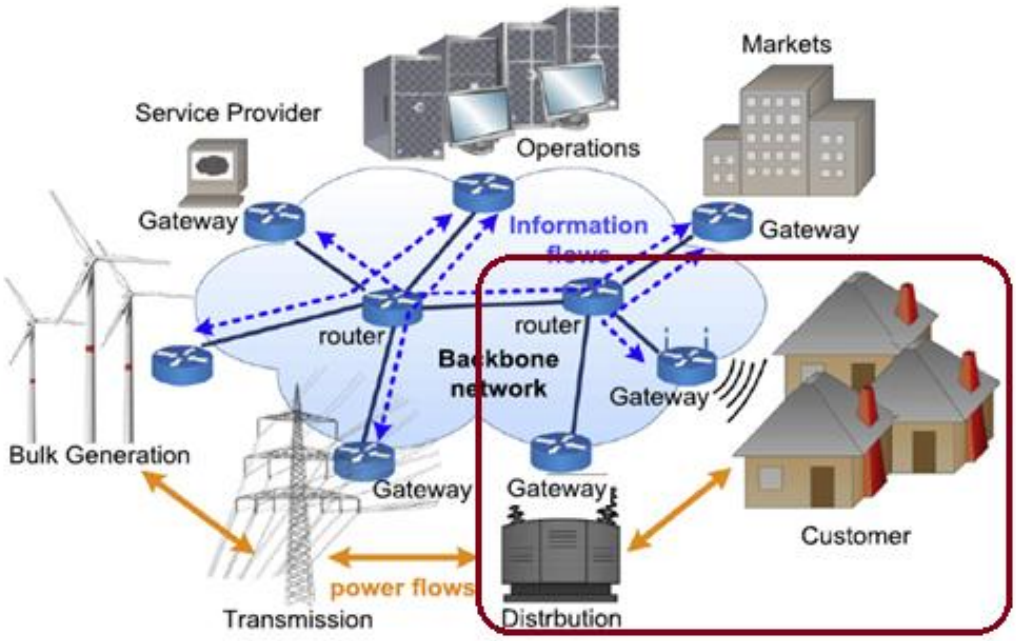


Figura 3-8 - Topologia Básica da Arquitetura de Redes - Fonte: (WENYE; ZHUO, 2013)

## 3.6. Roteiro de Implementação da VPN IPsec

Nesta seção se apresenta o roteiro completo de implementação da VPN IPsec Site-a-Site na topologia básica da rede de telecomunicação da CT-IAP.

Este roteiro, elaborado com explicações detalhadas das técnicas e conceitos adotados para a programação em CLI (Interface de Linhas de Comando), pode ser considerada entre dois domínios quaisquer[27] da CT-IAP e as interfaces entre eles, que representariam o par de sites[28] entre os quais será estabelecido o túnel VPN, passando pela Internet pública, e estruturado o IPsec. Para isto, é selecionada uma

[27] Exceto o domínio S*ervice Provider* que representará o provedor de acesso à Internet pública.
[28] Vem da nomenclatura padrão *Site-a-Site* e pode ser um domínio ou entidade do SGIRM.

seção da topologia básica da rede de telecomunicações da CT-IAP mostrada na Figura 3-8.

No entanto, para as simulações da VPN IPsec Site-a-Site, são selecionados três domínios específicos (Consumidor, Distribuidor e Provedor de Serviços) e duas interfaces (uma que conecta o Consumidor com o Provedor de Serviços e outra que conecta o Provedor de Serviços com o Distribuidor). Isto visa simular o caso onde o Provedor de Serviços é, efetivamente, o provedor da conexão entre dois domínios usando a Internet pública, por onde circularão os dados que se desejam proteger com o túnel VPN IPsec Site-a-Site.

A implementação da programação e simulações poderá ser replicada em qualquer outro conjunto de domínios e interfaces, adotando as recomendações do SGIRM sobre os níveis de requerimento dos objetivos de segurança na interfaces do conjunto selecionado. A implementação da VPN IPsec Site-a-Site considera que os dispositivos de rede suportam os recursos citados nos capítulos dois.

**Tarefas para Implementação da VPN IPsec Site-a-Site**

Para acompanhar plenamente a implementação dos comandos CLI é recomendado ter conhecimento básico sobre sistemas operacionais de roteadores e/ou switches. No entanto, não ter esse conhecimento básico não impede a compreensão do processo.

Todos os comandos CLI e rotinas de programação apresentadas nesta dissertação foram selecionados da referência (IOS SECURITY COMMAND, 2014) disponível na internet, com testes prévios no simulador Packet Tracer 6.2.

Para facilitar a representação gráfica do processo de implementação, adotamos o roteador R1 como sendo o gateway de segurança[29] de um dos domínios e o roteador R2 o gateway de segurança do outro domínio, sendo o Host A e o Host B os computadores onde serão implementados os programas computacionais, via CLI, dos roteadores R1 e R2, respectivamente (Figura 3-8 e Figura 3-9).

[29] O gateway de segurança é a porta de comunicação da rede local ou rede interna do domínio com os demais domínios, conforme mostrado na Figura 3-8. A segurança dos dados e aplicações da rede local ou interna do domínio deve ser feita pelos meios recomendados, como ser: Firewalls, IPS, Sistemas de Antivírus, etc. Também poderá ser adotado o IPsec na rede local.


Figura 3-9 - Topologia para Implementação. Fonte: Adaptado de Packet Tracer

Uma VPN (Rede Privada Virtual) é um canal de comunicações que é utilizada para formar uma conexão lógica entre duas extremidades através de uma rede pública. VPNs não incluem necessariamente criptografia ou autenticação. VPNs IPsec invocam o protocolo IKE para estabelecer comunicações seguras.

A implementação se inicia com a negociação IKE para a VPN IPsec que envolve várias etapas das Fase 1 e Fase 2.

1. Um túnel IPsec é iniciado quando o Host A envia tráfego interessante para o Host B. O tráfego é considerado interessante quando viaja entre os pares IPsec e satisfaz os critérios definidos na criptografia da Lista de Controle de Acesso - ACL[30] (*Access Control List*).
2. A Fase 1 do IKE começa. Os pares IPsec negociam a política SA IKE a ser estabelecida. Quando os pares são autenticados, um túnel seguro é criado usando o ISAKMP.
3. A Fase 2 do IKE começa. Os pares IPsec usam o túnel seguro autenticado para negociar a Transformação SA IPsec. A negociação da política compartilhada determina como o túnel IPsec é estabelecido.
4. O túnel IPsec é criado e os dados são transferidos entre os pares IPsec com base nos parâmetros IPsec configurados no conjunto Transformação IPsec.
5. O túnel IPsec termina quando as SAs IPsec são excluídas ou quando sua vida útil expira.

Tarefas necessárias para implementar uma VPN Site-a-Site e parametrizar os componentes do framework do IPsec:

[30] Access Control List ou Lista de Controle de Acesso (também conhecida pelo acrônimo ACL) é definida pela área de ciência da computação como uma lista que determina quem tem permissão de acesso a certos serviços.
Roteadores utilizam ACL para filtragem de pacotes, seja ele de entrada (Inbound traffic) ou de saída (Outbound traffic), TCP/UDP, entre outros protocolos. As ACLs não podem ser tratadas como um firewall, mas sim como um complemento para segurança da rede. Existem basicamente três tipos de ACLs: Padrão, Estendida e Nomeada.

**Tarefa 1: Configuração de ACLs Compatíveis**

O primeiro passo na configuração do ISAKMP é garantir que as ACLs existentes nos roteadores de perímetro (primeira linha de defesa da rede, pode ser o gateway de segurança), firewalls ou outros roteadores, não bloqueiem o tráfego IPsec. Roteadores de perímetro tipicamente implementam uma política de segurança restritiva com ACLs, onde é permitido apenas um tráfego específico, e todos os outros tráfegos são negados. Tal como uma política restritiva que possa bloquear o tráfego IPsec. Portanto, as sentenças de permissão específicas devem ser adicionadas à ACL.

Se certificar que as ACLs estão configurados para que o ISAKMP, o *Encapsulating Security Payload (ESP)* e o *Authentication Header (AH)* não tenham seus tráfegos bloqueados nas interfaces utilizadas pelo IPsec.

- Ao ESP é atribuído o número de protocolo IP 50.
- Ao AH é atribuído o número de protocolo IP 51.
- O ISAKMP usa a porta UDP 500.

A partir deste ponto é detalhada a programação CLI[31] a ser realizada a partir do computador (Host) conectado ao roteador R1[32]. Primeiramente, após acessar o sistema operacional do roteador, se deve acessar o modo privilegiado:

```
R1>enable
```
[33]

Ativar o modo de configuração global, com as senhas de acessos, se forem solicitados:

```
R1#config terminal
```

O prompt do roteador deverá apresentar:

```
R1(config)#
```

Para permitir os AH, ESP e ISAKMP numa interface IPsec negando qualquer outro tráfego desnecessário, uma ACL existente deve ser editada ou uma nova ACL criada.

Para permitir o tráfego AH, usar o comando[34]:

---

[31] As edições das linhas de programação são apresentadas na fonte Courier New 11 e negrita.
[32] Existem vários meios de acesso ou conexão de um host ao roteador: via console, via Telnet ou via vty.
[33] Adota-se uma fonte diferente para a programação de forma a diferencia-los do texto normal.

**access-list** acl **permit ahp** source **wildcard** destination **wildcard** (1)[35]

Para permitir o tráfego ESP, usar o comando:

**access-list** acl **permit esp** source **wildcard** destination **wildcard** (2)

Para permitir o tráfego ISAKMP, usar o comando:

**access-list** acl **permit udp** source **wildcard** destination **wildcard eq isakmp** (3)

Para verificar as entradas usar o comando:

**show access-lists** (4)

### Tarefa 2: Configuração do IKE

A segunda principal tarefa na configuração do suporte ISAKMP é definir os parâmetros dentro da política IKE. Uma tabela das opções de parâmetros é apresentado na Tabela 3-8. O IKE utiliza esses parâmetros durante a negociação para estabelecer o pareamento ISAKMP entre dois pontos IPSec.

Tabela 3-8 - Opções de Parametrização do ISAKMP – Fonte: O Autor, 2015

| **Parâmetros ISAKMP** | | | | |
|---|---|---|---|---|
| Parâmetro | Código | Valores Aceitos | Valor Default | Descrição |
| Encryption | des<br>3des<br>aes<br>aes 192<br>aes 256 | 56 bits (standard)<br>Triple DES<br>AES 128 bits<br>AES 192 bits<br>AES 256 bits | des | Message encryption algorithm |
| Hash | sha<br>md5 | SHA-1 (variante HMAC)<br>MD5 (variante HMAC) | sha | Message integrity (Hash) algorithm |
| Authentication | pre-share<br>rsa-encr<br>rsa-sig | Chaves pré-compartilhadas<br>Nonces RSA<br>Assinaturas RSA | rsa-sig | Peer authentication method |
| Group | 1<br>2<br>5 | 768-bit Diffie-Hellman (DH)<br>1024 bits DH<br>1536 bits DH | 1 | Key exchange parameters (DH group identifier) |
| Lifetime | seconds | Pode ser especificado qualquer numero de segundos | 86,400 sec (um dia) | ISAKMP-established SA lifetime |
| Os parâmetros podem variar de acordo à versão do sistema operacional | | | | |

[34] As palavras que não estão em negrita na linha de comando, indicam que são parâmetros a serem entrados. Esta é a razão de usarmos o nome “Parametrização” no título da dissertação e processo da configuração do IPsec.

[35] O número entre parêntesis é para numerar as linhas de comando caso seja necessária alguma referência.

Várias políticas ISAKMP podem ser configuradas em cada ponto participante do IPsec. Ao configurar políticas, a cada uma das políticas deve ser dado um número de prioridade único. Para configurar a prioridade de uma política usar o comando:

```
crypto isakmp policy priority          (5)
```

Onde a prioridade *(priority)* é um número que identifica exclusivamente a política do IKE e atribui uma prioridade para essa política. Usar um número inteiro de 1 a 10.000, sendo 1 a mais alta prioridade e 10.000 a mais baixa. Atribuir a política mais segura ao menor número disponível.

O comando *crypto isakmp policy* invoca o modo de comando de configuração da política do ISAKMP (Figura 3-10). Definem-se os parâmetros ISAKMP neste modo. Se os comandos não são explicitamente configurados, os valores padrões são usados. Por exemplo, se o comando hash não está explicitamente configurado, o IKE usa o valor SHA padrão.

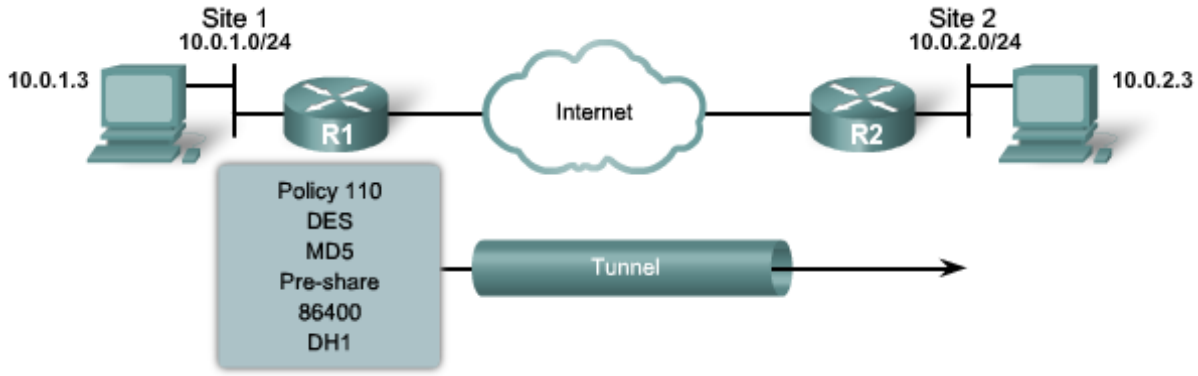


Figura 3-10 - Parâmetros de Políticas IKE. Adaptado de Packet Tracer

Dois terminais devem negociar as políticas ISAKMP antes que eles concordem uma SA a utilizar no IPSec. Quando a negociação ISAKMP começa na Fase 1 do IKE de modo principal, o ponto local inicia a negociação enviando todas suas políticas para o ponto remoto.

O ponto remoto tenta encontrar uma correspondência com suas próprias políticas, comparando a sua própria política de prioridade mais alta contra as políticas que recebeu do outro ponto. O ponto remoto verifica cada uma das suas políticas na ordem das suas prioridades (prioridade mais alta primeiro) até que seja encontrada uma correspondência.

A Figura 3-11 mostra os casos de correspondências das políticas de números 100 e 200, e a não correspondência da de número 300 (métodos de autenticação diferentes).

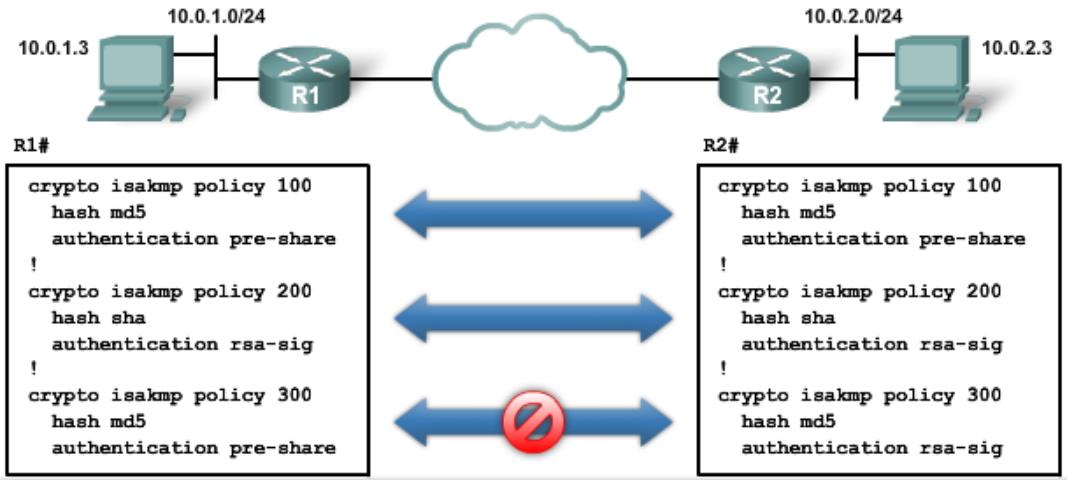


Figura 3-11 - Múltiplas Políticas ISAKMP – Fonte: Adaptado de Packet Tracer

A correspondência é feita quando ambas as políticas provenientes das duas pontas contenham a mesma criptografia, hash, autenticação, valores dos parâmetros DH, e quando a política do ponto remoto especifica uma vida menor ou igual ao tempo de vida da política que está sendo comparada. Se os tempos de vida não forem idênticos, o tempo de vida mais curto da política do ponto remoto é utilizado. Atribuir a política mais segura ao menor número de prioridade disponível para que a política mais segura encontre uma correspondência antes de quaisquer políticas menos seguras sejam configuradas.

Se uma correspondência aceitável não for encontrada, o ISAKMP recusa a negociação, e o IPsec não fica estabelecido. Se for encontrada uma correspondência, o ISAKMP completa a negociação de modo principal, e as SAs IPsec serão criadas durante a Fase 2 do IKE de modo rápido.

PSKs (Chaves pré-compartilhadas) são necessárias para a criptografia. Num dado ponto, a mesma chave pode ser configurada para ser compartilhada com múltiplos pontos remotos. A abordagem mais segura é especificar chaves diferentes para compartilhar entre diferentes pares de pontos. Para configurar uma PSK se usa o comando de configuração global:

**crypto isakmp key** (6)

Esta chave deve ser configurada se o comando de autenticação pré-compartilhada, ***authentication pre-share,*** foi configurado na política ISAKMP:

```
crypto isakmp key keystring[36] address peer-address[37]      (7)
crypto isakmp key keystring hostname hostname[38]             (8)
```

Por padrão, a identidade ISAKMP está configurada para usar o endereço IP. Para usar o parâmetro `hostname`, a identidade ISAKMP deve ser configurada para usar o nome do host com o comando no modo de configuração global:

```
crypto isakmp identity hostname       (9)
```

Além disso, o DNS deve ser acessível para resolver o nome do host.

**Tarefa 3: Parametrização do Conjunto de Transformadas IPsec**

Um conjunto de transformadas é uma combinação de transformadas IPsec individuais que é projetado para promulgar uma política de segurança específica para o tráfego. Durante a negociação ISAKMP da SA IPsec, que ocorre na Fase 2 do IKE, modo rápido, os pares concordam em usar uma transformada específica definida para proteger um fluxo de dados em particular.

Conjunto de transformadas consistem em uma combinação de uma transformada AH, uma transformada ESP, e o modo de IPsec (modo de túnel ou de transporte). Conjuntos de transformadas são limitados a uma transformada AH e uma ou duas transformadas ESP. Vários conjuntos de transformadas podem ser configurados. Uma ou mais deste conjunto de transformadas podem ser especificadas em uma entrada do mapa de criptografia (*crypto map*). A negociação SA IPsec utiliza o conjunto de transformadas definido na entrada do mapa de criptografia para proteger os fluxos de dados que são especificados pela ACL daquela entrada do mapa de criptografia.

Para definir um conjunto de transformadas, especificar um a quatro transformadas usando o comando de configuração global `crypto ipsec transform-set`. Este comando invoca o modo de configuração cripto-transformada:

---

[36] Este parâmetro especifica a chave pré-compartilhada PSK. Dever ser usado qualquer combinação de caracteres alfanuméricos até 128 bytes. Esta PSK deve ser idêntica em ambos os pontos do par.
[37] Este parâmetro especifica o endereço IP do ponto remoto.
[38] Este parâmetro especifica o nome do host do ponto remoto. Este nome deve estar concatenado com seu nome de domínio (por exemplo, meuhost.dominio.com).

**crypto ipsec transform-set** transform-set-name[39] transform1[40] [transform2] [transform3] [transform4] (10)

Cada transformada representa um protocolo de segurança IPsec (AH ou ESP) mais o algoritmo associado. Estes protocolos e algoritmos são especificados no âmbito do modo de configuração cripto-transformada. Em um conjunto de transformadas se especificam o protocolo AH, o protocolo ESP, ou ambos. Se um protocolo ESP é especificado em um conjunto de transformadas, um conjunto de transformada de criptografia ESP, ou um conjunto de transformada de criptografia ESP e um conjunto de transformada de autenticação ESP deve(m) ser especificado(s).

Durante a negociação, cada par procura por um conjunto de transformadas que tenha os mesmos critérios (a combinação de protocolos, algoritmos e outras configurações apresentadas na Tabela 3-9) para ambas.

Tabela 3-9 - Tabela de Transformações permitidas – Fonte: O Autor, 2015

| Tipo de Transformação | Transformada | Descrição |
|---|---|---|
| Transformação AH (escolher só uma) | ah-md5-hmac | AH com o algoritmo de autenticação MD5 (uma variante do HMAC) |
| | ah-sha-hmac | AH com o algoritmo de autenticação SHA (uma variante do HMAC) |
| Transformação de Criptografia ESP (escolher só uma) | esp-aes | ESP com algoritmo de criptografia AES de 128 bits |
| | esp-aes 192 | ESP com algoritmo de criptografia AES de 192 bits |
| | esp-aes 256 | ESP com algoritmo de criptografia AES de 256 bits |
| | esp-des | ESP com algoritmo de criptografia DES de 56 bits |
| | esp-3des | ESP com algoritmo de criptografia 3DES de 168 bits |
| | esp-seal | ESP com algoritmo de criptografia SEAL de 160 bits |
| | esp-null | Algoritmo de encriptação nulo[41] |
| Transformação de Autenticação ESP (escolher só uma) | esp-md5-hmac | ESP com algoritmo de autenticação MD5 (uma variante do HMAC) |
| | esp-sha-hmac | ESP com algoritmo de autenticação SHA (uma variante do HMAC) |
| Transformação de Compressão de IP | comp-lzs | Compressão de IP com o algoritmo Lempel-Ziv-Stac (LZS) |

[39] Este parâmetro especifica o nome do conjunto de transformada a ser criado (ou modificado).
[40] Tipos de Conjunto de transformadas: especificar até quatro *transformadas*: uma de AH, uma de criptografia ESP, uma de autenticação ESP, e opcionalmente uma de (segue no próximo rodapé...) compressão IP. Estas transformadas definem os protocolos de segurança IPsec e os algoritmos. Um Conjunto de transformadas é uma combinação de transformadas IPsec que promulgam uma política de segurança para o tráfego. Um conjunto de transformadas pode ter uma transformada AH e até duas transformadas ESP.
[41] NULL não altera os dados de texto pleno, fornecendo os meios ao ESP proporcionar autenticação e integridade sem confidencialidade.

Quando um conjunto de transformadas é encontrado, ele é selecionado e aplicado ao tráfego protegido como parte das SAs IPsec de cada par. Quando o ISAKMP não é utilizado para estabelecer as SAs, um único conjunto de transformadas deve ser usado. Neste caso, o conjunto de transformadas não é negociado.

Os conjuntos de transformadas são negociadas durante o IKE Fase 2 de modo rápido. Ao configurar múltiplos conjuntos de transformadas, selecione as transformadas do mais para o menos seguro, de acordo com a política de segurança de rede. Pares IPsec procuram por um conjunto de transformada que corresponda em ambas as extremidades e concordam com uma proposta de transformada unidirecional por SA.

**Tarefa 4: Configuração das ACLs de criptografia**

As ACLs (Listas de Controle de Acessos) de criptografia identificam os fluxos do tráfego a proteger. ACLs de criptografia de saída selecionam o tráfego de saída que o IPsec deve proteger. O tráfego que não for selecionado é enviado em texto simples. Se forem necessárias, ACLs de entrada podem ser criadas para filtrar e descartar o tráfego que deveria ter sido protegido pelo IPsec.

As ACLs de IP Estendida[42] (*Extended IP Access List*) selecionam o tráfego IP para criptografar com base no protocolo, endereço IP, rede, sub-rede, e porta. Embora a sintaxe das ACLs não seja alterada a partir das ACLs de IP Estendida, os significados são ligeiramente diferentes para as ACLs de criptografia. Por exemplo, a o comando **`permit`**[43] (permitir) especifica que os pacotes correspondentes devem ser criptografados, e **`deny`**[44] (negar) especifica que os pacotes correspondentes não serão criptografados. O tráfego não é necessariamente descartado por causa de uma declaração **`deny`**. As ACLs de criptografia são processadas de forma semelhante a uma ACLs de IP Estendida aplicada ao tráfego de saída de uma interface.

[42] ACLs numeradas de 1-99 ou 1300-1999 são ACLs padrão IPv4. Essas ACLs são usadas para filtrar pacotes com base unicamente na camada três do IP de origem. ACLs de IP Estendidas, numeradas de 100-199, filtram pacotes com base nas camadas três e quatro dos IP de origem e de destino. A camada quatro pode incluir informações TCP e UDP

[43] Esta opção faz com que todo tráfego IP que coincida com as condições especificadas deve ser protegido por criptografia, usando a política descrita pela entrada do mapa de criptografia correspondente.

[44] Esta opção instrui o roteador para rotear o tráfego em texto simples.

A sintaxe do comando para a forma básica de uma ACL de IP Estendida é:

**access-list** access-list-number {**permit | deny**} protocol[45] source[46] source-wildcard[47] destination[48] destination-wildcard (11)

As ACLs de criptografia de saída definem o tráfego interessante a ser criptografado. Todos os outros tipos de tráfego passam como texto simples. As ACLs de criptografia de entrada informarão ao roteador quais tráfegos devem ser recebidos como o tráfego criptografado. Quando o tráfego corresponde à declaração de permitida, o roteador espera que o tráfego seja criptografado. Se o tráfego de entrada recebido é texto simples que corresponde a uma instrução de permitida no ACL de criptografia, o tráfego será descartado. Esse descarte ocorre porque se esperava que o tráfego de texto simples devesse ter sido protegido pelo IPsec e criptografado, mas não foi, conforme apresentado no exemplo da Figura 3-12.

Um administrador poderia precisar que um tráfego específico tenha que receber uma combinação de proteção IPsec (autenticação somente), e outros tipos de tráfego receber uma combinação diferente (autenticação e criptografia). Para fazer isso, se deve criar duas ACLs de criptografia diferentes para definir os dois tipos diferentes de tráfego. Para diferentes entradas no mapa de criptografia devem ser usadas ACLs específicas para diferentes políticas IPsec.

[45] Esta opção especifica qual tráfego será protegido pela criptografia baseada no protocolo, como o TCP, UDP, ou ICMP. Se o protocolo é IP, então todo tráfego IP correspondente à declaração *permit* é criptografado.
[46] Se a declaração na ACL é uma declaração *permit*, são indicadas as redes, sub-redes ou hosts, entre os quais o tráfego deve ser protegido. Se a declaração na ACL é uma declaração *deny*, então o tráfego entre a origem e o destino especificado é enviado em texto simples.
[47] Máscara de rede curinga ou universal para ser aplicada ao intervalo de endereços de IP da rede de origem ou destino.
[48] Idem *source*.

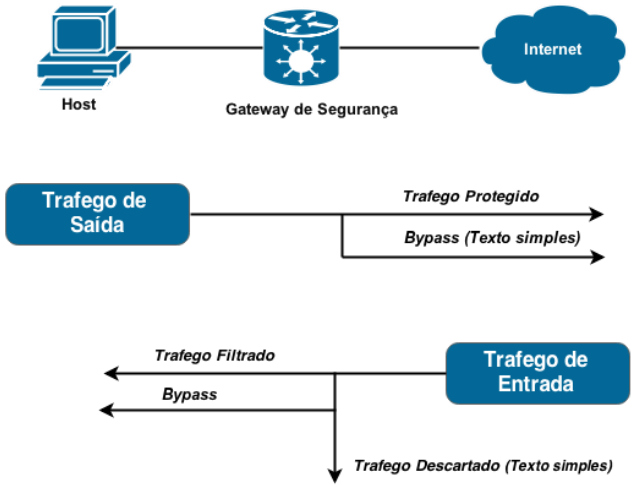


Figura 3-12 - Trafego Protegido[49], Descartado e Filtrado[50] - Fonte: O Autor, 2015

Deve-se ser o mais restritivo possível ao definir quais pacotes proteger em uma ACL de criptografia. Utilizar a palavra-chave **`any`** para especificar endereços de origem ou de destino não é recomendado. A declaração de permitir **`permit any any`** é fortemente desencorajada porque faz com que todo o tráfego de saída tem que ser protegido para ser enviado para o ponto que está especificado na entrada do mapa de criptografia correspondente. Assim, todos os pacotes de entrada que não possuam proteção IPsec são silenciosamente descartados, incluindo pacotes para protocolos de roteamento, NTP, Eco, resposta de Eco, e outros. Se a palavra-chave **`any`** deve ser utilizada em uma declaração de permitir, preceda a declaração com uma série de declarações de negar **`deny`** para filtrar o tráfego que não devem ser protegidos. A ACL de criptografia está associada a um mapa de criptografia, o qual por sua vez é atribuído a uma interface específica.

ACLs simétricas de criptografia devem ser configuradas para utilização pelo IPsec. Quando um roteador recebe pacotes criptografados de um ponto IPsec, ele usa a mesma ACL para determinar quais pacotes de entrada descriptografar, visualizando os endereços de origem e de destino na ACL em ordem inversa. Os critérios da ACL estão aplicados na direção para frente do tráfego que sai de um roteador, e na direção para trás para o tráfego que entra no roteador, de modo que a origem da ACL de saída torna-se o destino da ACL de entrada.

Por exemplo, supondo-se que para o Site 1 da topologia da Figura 3-13 (pag. 57) a proteção IPsec é aplicada ao tráfego entre os hosts da rede 10.0.1.0/24 a

[49] Outbound: indica o tráfego de saída de dados a ser protegido pelo IPsec. Exemplo: Dados do Consumidor.
[50] Inbound: indica o tráfego filtrado e descartado que deveria ter sido protegido por IPsec.

medida que os dados saem da interface S0/0/0 de R1 em rota para os hosts do Site 2 na rede 10.0.2.0/24. Para o tráfego desde os hosts da rede 10.0.1.0/24 do Site 1 para os hosts da rede 10.0.2.0/24 do Site 2, a entrada da ACL em R1 é avaliado da seguinte forma:

- *Source* (Origem) = hosts na rede 10.0.1.0/24
- *Destination* (Destino) = hosts na rede 10.0.2.0/24

Para o tráfego que provem dos hosts da rede 10.0.2.0/24 do Site 2 para os hosts da rede 10.0.1.0/24 do Site 1, essa mesma entrada ACL em R1 é avaliado da seguinte forma:

- *Source* (Origem) = hosts na rede 10.0.2.0/24
- *Destination* (Destino) = hosts na rede 10.0.1.0/24

**Tarefa 5: Aplicar o Mapa de Criptografia**

Entradas no mapa de criptografia que são criadas para o IPsec combinar os parâmetros de configuração necessários nas SAs IPsec, inclui os seguintes parâmetros:

- Tráfego que será protegido através de uma ACL de criptografia.
- Granularidade[51] do fluxo de dados a ser protegido por um conjunto de SAs.
- Ponto IPsec remoto, que determina onde o tráfego protegido pelo IPsec é enviado.
- Endereço local utilizado para o tráfego IPsec (opcional).
- Tipo de segurança IPsec aplicada ao tráfego, escolhendo de uma lista de um ou mais conjuntos de transformadas.

Entradas no mapa de criptografia com o mesmo nome do mapa de criptografia (conforme mostrado nas sentenças 12, 13 e 14 da pag. 56), mas com diferentes números de sequência do mapa, são agrupados em um conjunto de mapa de criptografia. Apenas um mapa de criptografia pode ser definido para uma única interface. O conjunto de mapa de criptografia pode incluir o IPsec usando IKE. Múltiplas interfaces podem compartilhar o mesmo mapa de criptografia definido, se a mesma política é aplicada às múltiplas interfaces.

Se mais de uma entrada no mapa de criptografia é criada para uma determinada interface, usar o número sequencial (seq-num) de cada entrada do

[51] A granularidade se refere ao numero e tamanho dos campos em que os dados são subdivididos.

mapa para classificar as entradas no mapa. Quanto menor o número de sequência, maior é a prioridade. Na interface que tem o conjunto de mapa de criptografia, o tráfego é avaliado contra as entradas no mapa de prioridade mais elevados em primeiro lugar.

Deve-se criar múltiplas entradas no mapa de criptografia para uma determinada interface se qualquer uma destas condições existir:

- Pares IPsec separados lidarem com diferentes fluxos de dados.
- Diferentes níveis de segurança IPsec devem ser aplicados a diferentes tipos de tráfego (para os mesmos pares IPsec ou separados). Por exemplo, se o tráfego entre um conjunto de sub-redes precisa ser autenticado, e o tráfego entre outro conjunto de sub-redes precisa ser autenticado e criptografado. Neste caso, definir os diferentes tipos de tráfego em duas ACLs separadas, e criar uma entrada do mapa de criptografia separado para cada ACL de criptografia.
- O IKE não é utilizado para estabelecer um conjunto particular de SAs, e múltiplas entradas ACL devem ser especificadas criando ACLs separadas (uma por entrada permitida) e especificando uma entrada no mapa de criptografia separada para cada ACL.

Usa-se o comando de configuração global **`crypto map`** para criar ou modificar uma entrada no mapa de criptografia entrando no modo de configuração do mapa de criptografia. Definem-se as entradas do mapa de criptografia que fazem referência a mapas dinâmicos, para a prioridade mais baixa num conjunto de mapa de criptografia (eles devem ter os maiores números de sequência). A sintaxe de comandos e definições de parâmetros são os seguintes:

**`crypto map`** map-name[52] seq-num[53] **`ipsec-manual`**[54] (12)
**`crypto map`** map-name seq-num **`ipsec-isakmp`**[55] [**`dynamic`**[56] dynamic-map-name[57]] (13)
**`no`**[58] **`crypto map`** map-name [seq-num] (14)

[52] Parâmetro de entrada do nome atribuído do mapa de criptografia a ser editado ou criado.
[53] O número atribuído à entrada do mapa de criptografia
[54] Indica que o ISAKMP não será usado para estabelecer as SAs IPsec.
[55] Indica que o ISAKMP será usado para estabelecer as SAs IPsec.
[56] (Opcional) Especifica que esta entrada do mapa de criptografia faz referência a um mapa de criptografia estático preexistente. Se esta palavra-chave é usada, nenhum dos comandos de configuração do mapa de criptografia estará disponíveis.
[57] (Opcional) Especifica o nome do conjunto de mapas de criptografia dinâmicas que deve ser usado como modelo de política.

Usando o comando **`crypto map`** no modo de configuração global, entra-se no modo de configuração do mapa de criptografia. A partir daqui, vários componentes do IPsec são parametrizados ou configurados, incluindo qual criptografia, ACL, endereços de pares, e conjunto de transformada serão usados. Na continuação são apresentados comandos de um exemplo de criação do mapa *MYMAP* e aplicado na à interface de saída do roteador R1 da topologia da Figura 3-13:


Figura 3-13 - Aplicação de Mapa MYMAP. Fonte: Adaptado de Packet Tracer

```
(config)#crypto map MYMAP 10 ipsec-isakmp
(config-crypto-map)#match address[59] 110
(config-crypto-map)#set[60] peer[61] 172.30.2.2 default
(config-crypto-map)#set peer 172.30.2.2
(config-crypto-map)#set pfs[62] group1
(config-crypto-map)#set transform-set[63] mine
(config-crypto-map)#set security-association lifetime[64] seconds 86400
(config-crypto-map)#exit[65]
```

ACLs para entradas no mapa de criptografia que estão marcados como *IPsec-manual* estão restritos a uma única entrada permitida, e as entradas posteriores são ignoradas. As SAs que sejam estabelecidas por essa determinada entrada no mapa de criptografia são apenas para um único fluxo de dados. Para suportar múltiplas SAs estabelecidas manualmente para diferentes tipos de tráfego, definem-se múltiplas ACLs de criptografia e depois se aplicam cada uma delas para

---

[58] Usado para excluir comandos digitados com o comando *set*.
[59] Identifica a ACL Estendida por seu nome ou número. O valor deve corresponder à lista de acesso, número ou nome do argumento da ACL de IP Estendida correspondente previamente definida.
[60] Usado com os comandos peer, pfs, transform-set, e security-association.
[61] Especifica o ponto IPsec permitido por endereço IP ou hostname. Múltiplos pares podem ser especificados para redundância.
[62] Especifica o grupo DH.
[63] Especifica o conjunto de listas de transformadas em ordem de prioridade. Quando o parâmetro *ipsec-manual* é usado com o comando *crypto map*, então apenas um conjunto de transformada pode ser definido. Quando o parâmetro *ipsec-isakmp* ou o parâmetro *dynamic* é usado com o comando *crypto map*, até seis conjuntos de transformadas podem ser especificados.
[64] Define os parâmetros da vida útil da SA em segundos ou quilo bytes.
[65] Sai do modo de configuração do *crypto map*.

cada entrada no mapa de criptografia do *IPsec-manual* em separado. Cada ACL inclui uma declaração de permissão que define o tráfego que deve proteger.

Dois pontos podem ser especificados num mapa de criptografia para redundância. Se o primeiro ponto não pode ser contatado, o segundo ponto é usado. Não há limite para o número de pontos redundantes que podem ser configurados.

Depois que os parâmetros do mapa de criptografia estão configurados, atribui-se o mapa de criptografia para as interfaces usando o comando de configuração **`crypto map`** na interface. O mapa de criptografia é aplicado à interface de saída do túnel VPN usando o comando **`crypto map`** no modo de configuração na interface:

**`crypto map`** `map-name` (15)

`map-name` é o nome do conjunto do mapa de criptografia para aplicar na interface. Certificar-se de que as informações de roteamento que são necessários para enviar pacotes pelo túnel também estão configuradas.

Todo o tráfego IP que passa através da interface onde o mapa de criptografia é aplicado é avaliado em relação ao conjunto de mapas de criptografia aplicado. Se uma entrada no mapa de criptografia vê tráfego IP de saída que deve ser protegido e o mapa de criptografia especifica o uso do IKE, uma SA é negociada com o ponto remoto de acordo com os parâmetros que estão incluídos na entrada do mapa de criptografia.

**Verificação e Resolução de Problemas da Configuração IPSec**

VPNs podem ser complexas e, por vezes, não operam como se esperava. Por esta razão, há uma variedade de comandos úteis para verificar o funcionamento das VPNs e solucionar problemas quando necessário. O melhor momento para se familiarizar com esses comandos, e sua saída, é quando a rede não está funcionando corretamente. Desta forma, as anomalias podem ser detectadas quando os comandos são utilizados para a solução de problemas.

Para ver todos os mapas de criptografia configurados, usa-se o comando **`show crypto map`** (17). Este comando verifica as configurações e mostra o tempo de vida da SA. O comando **`show running-config`** (18) também revela muitas dessas mesmas configurações. Usa-se o comando **`show crypto isakmp policy`** (19) para exibir as políticas IKE configuradas e as definições das políticas IKE

padrão. Este comando é útil porque revela todas as informações de configuração do ISAKMP (IKE).

Usa-se o comando **`show crypto ipsec transform-set`** (20) para mostrar todos os conjuntos de transformadas configurados. Os conjuntos de transformadas determinam o nível de proteção que os dados terão quando passam pelo túnel, isto é importante para verificar a fortaleza da política de proteção do IPSec.

Um dos comandos mais úteis é **`show crypto ipsec sa`** (21). Se a saída indica que uma SA é estabelecida, o resto da configuração é assumido como funcionando. Dentro da saída, os valores *pkts encrypt* (pacotes criptografados) *pkts decrypt* (pacotes descriptografados) indicam qual tráfego está fluindo através do túnel. Um comando útil semelhante é **`show crypto isakmp sa`** (22). Este comando exibe todas as SAs IKE correntes. O estatus *QM_IDLE* indica uma SA IKE ativa.

Para solucionar problemas de conectividade da VPN, usam-se os comandos de depuração. O comando **`debug crypto isakmp`** (23) exibe informações sobre os processos da negociação específica da Fase 1 e da Fase do IKE. O comando **`debug crypto ipsec`** (24) exibe informações detalhadas sobre os eventos IPsec.

Tal como acontece com outros comandos de depuração, o comando **`debug crypto isakmp`** deve ser usado com cautela, porque os processos de depuração podem interferir no desempenho no dispositivo. Deve ser usado o comando **`undebug all`** (25) para desligar a depuração, o mais rapidamente possível.

## 3.7. Metodologia de Simulações

As simulações com a ferramenta *Packet Tracer 6.2* são feitas num projeto de Topologia de Rede que reproduz a topologia básica da CT-IAP. São selecionados três domínios específicos (Consumidor, Distribuidor e Provedor de Serviços) e duas interfaces (uma que conecta o Consumidor com o Provedor de Serviços e outra que conecta o Provedor de Serviços com o Distribuidor).

Nas simulações são aplicadas as tarefas passo-a-passo da metodologia proposta de implementação da VPN e parametrização do framework IPsec, visando demonstrar com as análises das estruturas dos dados e resultados dos processos envolvidos, antes e depois da parametrização, a viabilidade e aplicabilidade da metodologia.

## 3.8. Metodologia de Testes em Laboratório

Os testes em laboratório realizados no Laboratório da Rede Nacional de Ensino e Pesquisa (RNP), sito no Centro Politécnico da UFPR, são feitos em equipamentos reais e também numa topologia de rede que reproduz parte da Topologia Básica da CT-IAP.

Nos testes também são aplicadas as tarefas passo-a-passo da metodologia proposta de implementação da VPN e parametrização do framework IPsec, para medir com as ferramentas IPERF e NetPIPE o jitter (variação da latência) e taxa de transferência do fluxo de dados decorrente do IPsec, para comparar os resultados com os limites estabelecidos no SGIRM.

Cada teste é repetido vinte vezes visando realizar com o MatLab uma análise dos dados e uma avaliação estatística dos resultados, com o objetivo de filtrar eventuais erros não sistemáticos e determinar padrões, se houverem.

## 3.9. Ferramentas e Materiais

Esta dissertação foi elaborada num notebook *Dell Inspiron 1525, 1,73 Ghz, 4 Gb de RAM*, onde foram instalados os seguintes programas visando a implementação, simulações, testes em Laboratório, medições e avaliações de dados, e testes de vulnerabilidade da VPN IPsec:

- Simulador *Packet Tracer 6.2.*
- MatLab R2014a, ferramenta da MathWorks, Inc.
- Software de Criptoanálise *Cain & Abel, v4.9.56*.

As ferramentas a seguir foram instaladas nos computadores Dell do Laboratório da Rede Nacional de Pesquisa para a realização dos testes com equipamentos reais:

- Ferramenta de Monitoramento de Desempenho de Redes *Iperf.*
- Ferramenta de desempenho de protocolos de rede *NetPIPE*.

No simulador Packet Tracer 6.2 foram simulados os seguintes equipamentos de rede:

4 (quatro) roteadores com a seguinte configuração:

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)

4 (quatro) roteadores com a seguinte configuração:
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

3 (três) switches com a seguinte configuração:
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
63488K bytes of flash-simulated non-volatile configuration memory.
Model number:  WS-C2960-24TT
System serial number:  FOC1033Z1EY

No Laboratório da Rede Nacional de Ensino e Pesquisa (RNP), na UFPR, a topologia para os testes em laboratório contou com os seguintes equipamentos reais:

Host 1  (Distribuidor):

Notebook Dell - Core i7 2.1Ghz- 8Gb Ram, placa de rede intel Gigabit. Sistema operacional Linux.

Host 2 (Consumidor)
Desktop Dell - Core 2 duo 2.9ghz - 2Gb Ram, placa de rede Broadcom Gigabit. Sistema operacional Linux.

Roteadores:
Nome do roteador: Distribuidor
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(12), RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 7.0) with 233472K/28672K bytes of memory.
Processor board ID FTX1426Y04F
2 FastEthernet interfaces
1 Serial(sync/async) interface
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.

Nome do roteador: Consumidor:
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(12), RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 6.0) with 115712K/15360K bytes of memory.
Processor board ID FTX1040Z06W
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity

Switch
Cisco WS-C2950-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
24 FastEthernet/IEEE 802.3 interface(s)
63488K bytes of flash-simulated non-volatile configuration memory.

# 4. VALIDAÇÃO DA VPN IPsec VIA SIMULAÇÕES

Neste capítulo são apresentados estudos de caso utilizando a metodologia proposta no capítulo anterior. Os estudos de caso considera os testes da VPN IPSec Site-a-Site via simulações com a ferramenta *Packet Tracer 6.2* implementando o roteiro detalhado na seção 3.6. Também são feitas análises dos processos e dos resultados obtidos, visando demonstrar a viabilidade e aplicabilidade da metodologia.

A implementação é feita selecionando três domínios específicos (Consumidor, Distribuidor e Provedor de Serviços) e duas interfaces (uma que conecta o Consumidor com o Provedor de Serviços e outra que conecta o Provedor de Serviços com o Distribuidor). Isto visa simular casos onde o Provedor de Serviços é, efetivamente, o provedor da conexão entre dois domínios usando a Internet pública, por onde circularão os dados que se desejam proteger com o túnel VPN IPSec Site-a-Site.

## 4.1. Simulações IPsec VPN via Packet Tracer 6.2

O modelo de implementação de VPN IPsec adotado propicia seus benefícios mais importantes que são a Segurança, a Economia e a Escalabilidade, descritos na seção 2.2.4 do capítulo dois. Estes benefícios podem ser obtidos com a parametrização adequada dos métodos de distribuição (protocolo ISAKMP), de intercâmbio de chaves, de autenticação de pares e dos algoritmos de hash e criptografia (estes parâmetros fazem parte da Política ISAKMP detalhada na Tarefa 2 da metodologia proposta). A implementação da VPN IPSec Site-a-Site é feita de acordo aos dados dos dispositivos de estado da arte da topologia da Figura 4-1, cenário que reproduz a Topologia Básica de Rede da CT-IAP da seção 3.5, com os domínios e as interfaces lógicas entre os domínios.

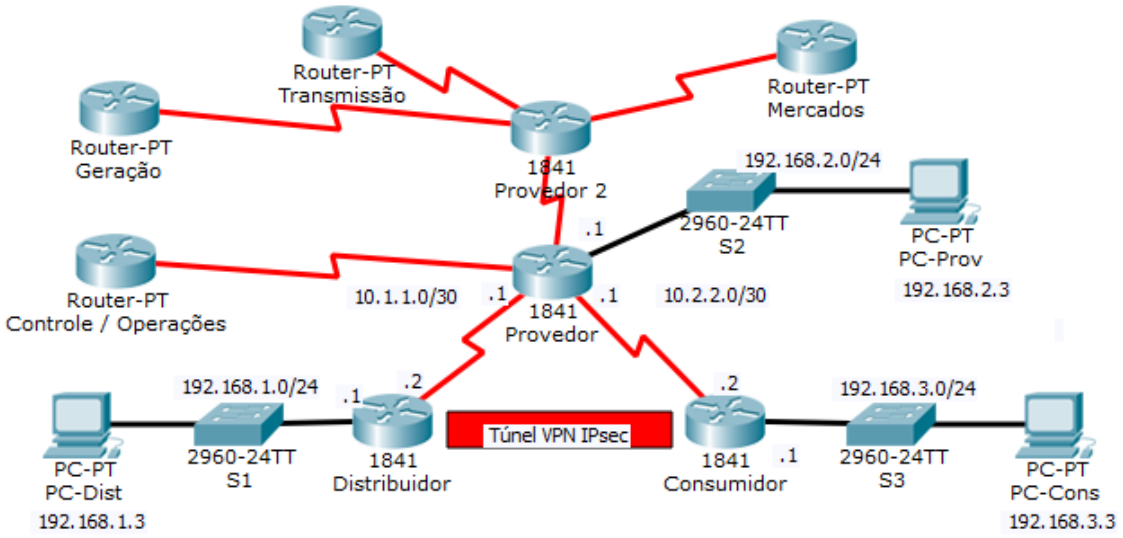


Figura 4-1 - Topologia para Simulações – Fonte: O Autor, 2015

A Tabela 4-1 detalha os dados dos dispositivos ativos e passivos da rede da Topologia de Testes, que inclui: nome dos dispositivos, suas interfaces físicas, seus endereços de IPs (sejam das redes, sub-redes, interfaces lógicas e físicas, e PCs dos domínios), seus gateways (por onde os roteadores, que representam os domínios, conectam suas interfaces lógicas com outros domínios).

Tabela 4-1 - Tabela de Dispositivos com Endereços IPs - O Autor, 2015

| Dispositivo (Domínio) | Interface Física | Endereço IP | Mascara | Gateway (Interface Logica) | Porta do Switch |
|---|---|---|---|---|---|
| Distribuidor | Fa0/0 | 192.168.1.1 | 255.255.255.0 | N/A | S1 Fa0/1 |
| | S0/0/0 (DCE) | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| Provedor de Serviços | Fa0/0 | 192.168.2.1 | 255.255.255.0 | N/A | S2 Fa0/2 |
| | S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| | S0/0/1 (DCE) | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| Consumidor | Fa0/0 | 192.168.3.1 | 255.255.255.0 | N/A | S3 Fa0/5 |
| | S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| PC-Dist | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 Fa0/2 |
| PC-Prov | NIC | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | S2 Fa0/1 |
| PC-Cons | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 Fa0/18 |

### Objetivos das simulações

- Verificar a conectividade da rede de telecomunicações.

- Configurar o roteador de gateway de segurança do domínio Distribuidor para suportar uma VPN IPsec Site-a-Site com o roteador do domínio Consumidor.
- Configurar o roteador de gateway de segurança do domínio Consumidor para suportar uma VPN IPsec Site-a-Site com o roteador do domínio Distribuidor.
- Analisar os resultados das simulações e datagramas dos dados que fluem na VPN IPsec.

**Antecedentes e Cenário**

A Topologia para Simulações da rede de telecomunicação inclui ao menos um roteador por domínio, mas para as simulações serão configurados os roteadores Distribuidor e Consumidor para suportar uma VPN IPsec Site-a-Site quando o tráfego flua de um domínio a outro. O túnel VPN IPsec se dá a partir roteador do Distribuidor para o roteador do Consumidor via o roteador do Provedor de Serviços de Internet pública. O roteador do Provedor atua para passagem do fluxo de dados e não tem conhecimento da VPN. O IPsec fornece a transmissão segura de informações confidenciais através de redes desprotegidas, como a Internet, entre dispositivos IPsec (pares), tais como roteadores dos domínios Distribuidor e Consumidor.

Adota-se, para esta simulação, um cenário particular da CT-IAP do SGIRM, onde a interface CT12 entre a entidade *Smart Meter Energy Services* do domínio Consumidor e a entidade *Neighborhood Area Network* do domínio Distribuidor (interfaces e entidades mostradas na Figura 3-2) deverá contar com serviços de segurança de alta (H) Confidencialidade e alta (H) Integridade para o fluxo de dados entre tais domínios (mostradas na Tabela 3-2). Assim, a parametrização da VPN IPsec deverá contar com esses níveis de serviços.

É reproduzido um resumo da Tabela 3-4, Tabela 3-5, Tabela 3-6 e Tabela 3-7 de Propostas de Blocos Framework IPSec, na Tabela 4-2 a seguir, para uma alta (H) Confidencialidade e alta (H) Integridade, cujas opções para cada bloco do framework IPsec deverão ser selecionados como parâmetros da VPN IPSec a ser simulada.

Tabela 4-2 - Parâmetros para os Blocos IPsec - O Autor, 2015

| **Framework IPsec** | | **Serviços de Segurança** | | | |
|---|---|---|---|---|---|
| | | **Confidencialidade** | | **Integridade** | |
| **Bloco** | **Opções** | | (H) | | (H) |
| **Protocolo IPsec** | AH-ESP-ESP+AH | | *ESP+ AH* | | *AH* |
| **Confidencialidade** | DES-3DES-AES-SEAL | | *AES-SEAL* | | - |
| **Integridade** | MD5-SHA | | - | | *SHA* |
| **Autenticação** | PKS-RSA | | PKS-RSA | | PKS-RSA |
| **Diffie-Helman** | DH1-DH2-DH5-DH7 | | *DH2*[66] | | *DH2* |

A seguir são selecionados os parâmetros para cada uma das fases e implementadas as tarefas para as simulações:

Fase 1 - Parametrização da Política ISAKMP:

Tabela 4-3 - Tabela de Parâmetros da Política ISAKMP - O Autor, 2015

| **Parâmetros**[67] | | **Distribuidor** | **Consumidor** |
|---|---|---|---|
| **Método de distribuição de chave** | Manual ou **ISAKMP** | **ISAKMP** | **ISAKMP** |
| **Algoritmo de encriptação** | **DES**, 3DES, or AES | AES | AES |
| **Algoritmo de hash** | MD5 or **SHA-1** | **SHA-1** | **SHA-1** |
| **Método de Autenticação** | Chave pré-compartilhada ou **RSA** | pré-compartilhada | pré-compartilhada |
| **Método de intercâmbio** | DH, Grupos 1, 2, ou 5 | DH 2 | DH 2 |
| **Tempo de vida da SA IKE** | 86400 seconds or less | **86400** | **86400** |
| **Chave ISAKMP** | | vpnpa55 | vpnpa55 |

[66] É utilizado o Grupo 2 do DH devido à limitação do roteador simulado. O recomendado é DH5.
[67] Os parâmetros em negrito são defaults. Somente os parâmetros sem negrito devem ser configurados de forma explícita.

Fase 2 - Parametrização da Política IPsec:

Tabela 4-4 - Tabela de Parâmetros da Política IPsec - O Autor, 2015

| Parâmetros | Distribuidor | Consumidor |
|---|---|---|
| **Conjunto de Transformada** | VPN-SET | VPN-SET |
| **Nome do Dispositivo Par** | **Consumidor** | **Distribuidor** |
| **Endereço IP do Par** | 10.2.2.2 | 10.1.1.2 |
| **Rede a ser criptografada** | 192.168.1.0/24 | 192.168.3.0/24 |
| **Nome do Mapa de Criptografia (***Crypto Map name***)** | VPN-MAP | VPN-MAP |
| **SA Estabelecida** | ipsec-isakmp | ipsec-isakmp |

Os roteadores foram pré-configurados com o protocolo de roteamento RIP[68] *(Routing Information Protocol)* versão 2.

### Parte 1. Configurar os Parâmetros IPsec no roteador *Distribuidor*

Teste conectividade:

Ping desde o computador Distribuidor (PC-Dist) para o computador Consumidor (PC-Cons)

```
PC-Dist>ping 192.168.3.3
```
[69]

### Passo 1: Identificar tráfego interessante[70] no roteador Distribuidor.

Configurar a ACL 110 para identificar o tráfego como interessante a partir da rede do domínio Distribuidor para a rede do domínio Consumidor. Este tráfego interessante irá acionar a VPN IPsec a ser implementada sempre que haja tráfego entre as redes dos domínios Distribuidor e Consumidor. Todos os outros tráfegos provenientes de ambos os domínios não serão criptografados. Por causa negação implícita (*deny all*), não há necessidade de configurar uma declaração *deny any any*.

```
Distribuidor>enable
Distribuidor#config terminal
Distribuidor(config)#access-list 110 permit ip 192.168.1.0
0.0.0.255 192.168.3.0 0.0.0.255
```

[68] É um dos mais antigos protocolos de vetor distancia e um padrão amplamente utilizado.
[69] As edições das linhas de programação são apresentadas na fonte Courier New 11.
[70] Palavra utilizada para indicar que um fluxo de dados será protegido com o IPsec.

**Passo 2: Configurar as propriedades do ISAKMP Fase 1 no Distribuidor**

Configurar as propriedades da política de criptografia ISAKMP de número 10 no Distribuidor, juntamente com chave de criptografia compartilhada *vpnpa55*. Consultar a tabela da Fase 1 ISAKMP para ter os parâmetros específicos para configurar. Os valores default não precisam ser configurados; portanto, apenas a criptografia, o método de troca de chaves, e o método de DH devem ser configurados.

```
Distribuidor(config)#crypto isakmp policy 10
Distribuidor(config-isakmp)#encryption aes
Distribuidor(config-isakmp)#authentication pre-share
Distribuidor(config-isakmp)#group 2
Distribuidor(config-isakmp)#exit
Distribuidor(config)#crypto isakmp key vpnpa55 address 10.2.2.2
```

**Passo 3: Configurar as propriedades do ISAKMP Fase 2 no Distribuidor**

Parte a: Criar o conjunto de transformadas *VPN-SET* para ser utilizada a transformada de encriptação *esp-3des* e a transformada de autenticação *esp-sha-hmac*.

```
Distribuidor(config)#crypto ipsec transform-set VPN-SET esp-
3des esp-sha-hmac
```

Parte b: Criar o mapa de criptografia *VPN-MAP* que unam todos os parâmetros da Fase 2. Usar o número de sequência 10 e identificá-lo como um mapa *ipsec-isakmp*.

```
Distribuidor(config)#crypto map VPN-MAP 10 ipsec-isakmp
Distribuidor(config-crypto-map)#description VPN connection to
Consumidor
Distribuidor(config-crypto-map)#set peer 10.2.2.2
Distribuidor(config-crypto-map)#set transform-set VPN-SET
Distribuidor(config-crypto-map)#match address 110
Distribuidor(config-crypto-map)#exit
```

**Passo 4: Configurar o mapa de criptografia na interface de saída**

Vincular o mapa de criptografia VPN-MAP à interface *Serial 0/0/0* de saída.

```
Distribuidor(config)#interface S0/0/0
Distribuidor(config-if)#crypto map VPN-MAP
*March 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

**Parte 2: Configurar os Parâmetros IPsec no roteador Consumidor**

**Passo 1: Configurar o roteador Consumidor para suportar uma VPN Site-a-Site VPN com o roteador Distribuidor.**

Configurar reciprocamente os parâmetros no Consumidor. Configurar a ACL 110 para identificar como interessante o tráfego da rede do domínio Consumidor à rede do domínio Distribuidor.

```
Consumidor> enable
Consumidor# config terminal
Consumidor(config)#access-list 110 permit ip 192.168.3.0
0.0.0.255 192.168.1.0 0.0.0.255
```

**Passo 2: Configurar as propriedades do ISAKMP Fase 1 no Consumidor.**

Configurar as propriedades da política de criptografia ISAKMP de número 10 no roteador Consumidor com a chave criptografada *vpnpa55* compartilhada.

```
Consumidor(config)#crypto isakmp policy 10
Consumidor(config-isakmp)#encryption aes
Consumidor(config-isakmp)#authentication pre-share
Consumidor(config-isakmp)#group 2
Consumidor(config-isakmp)#exit
Consumidor(config)#crypto isakmp key vpnpa55 address 10.1.1.2
```

**Passo 3: Configurar as propriedades do ISAKMP Fase 2 no Consumidor**

Parte a: Como foi feito no roteador do Distribuidor, criar o conjunto de transformadas *VPN-SET* para serem utilizadas a transformada de encriptação *esp-3des* e a transformada de autenticação *esp-sha-hmac*.

```
Consumidor(config)#crypto ipsec transform-set VPN-SET esp-3des
esp-sha-hmac
```

Parte b: Criar o mapa de criptografia *VPN-MAP* que une todos os parâmetros da Fase 2. Use o número de sequência de 10 e identificá-lo como um mapa *ipsec-isakmp*.

```
Consumidor(config-crypto-map)#crypto map VPN-MAP 10 ipsec-
isakmp
Consumidor(config-crypto-map)#description VPN connection to
Distribuidor
Consumidor(config-crypto-map)#set peer 10.1.1.2
Consumidor(config-crypto-map)#set transform-set VPN-SET
Consumidor(config-crypto-map)#match address 110
Consumidor(config-crypto-map)#exit
```

**Passo 4: Configurar o mapa de criptografia na interface de saída**

Vincular o mapa de criptografia VPN-MAP à interface *Serial 0/0/1* de saída.

```
Consumidor(config)#interface S0/0/1
Consumidor(config-if)#crypto map VPN-MAP
*Mar 13 17:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

## 4.2. Análises de Resultados das Simulações

**Parte 1: Análise da VPN IPsec**

**Passo 1: Analisar o túnel antes do tráfego interessante.**

Ao usar o comando `show crypto ipsec sa` no roteador Distribuidor antes de tráfego interessante, observa-se que o número de pacotes encapsulados, criptografados, descapsulados e descriptografados são todos 0 (linhas sublinhadas), indicando que, mesmo com a VPN IPsec parametrizada, ainda não foi requerido seus serviços porque não houve fluxo de dados.

```
Distribuidor#show crypto ipsec sa
```

As seguintes informações são mostradas:

```
interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 10.1.1.2
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

**Passo 2: Criar um trafego interessante.**

No PC-Dist, ping PC-Cons

```
PC-Dist>ping 192.168.3.3
```

As seguintes informações são mostradas:

```
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=13ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 13ms, Average = 7ms
```

**Passo 3: Verificar o túnel depois do tráfego interessante.**

Ao usar de novo o comando `show crypto ipsec sa` no roteador Distribuidor, depois do tráfego interessante observa-se que o número de pacotes encapsulados, criptografados, descapsulados e descriptografados são diferentes de zero, indicando que a VPN IPsec está funcionando com o encapsulamento e autenticação ESP-3DES-SHA (linhas sublinhadas) e usando os conjuntos de transformadas parametrizados e negociados:

```
Distribuidor#show crypto ipsec sa
```

As seguintes informações são mostradas:

```
interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 10.1.1.2
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0D7F4EA8(226447016)
inbound esp sas:
spi: 0x790E10F3(2030964979)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2006, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/3579)
```

**Parte 2: Análise dos Datagramas dos processos AH/ESP e ISAKMP**

Nesta parte, é gerado um trafego TFTP (Protocolo de Transferência de Arquivos Triviais) de 1 Kbyte a partir do PC-Distribuidor com destino ao PC-Consumidor para analisar os datagramas (PDUs) e processos IPsec nos dispositivos. A Figura 4-2 mostra uma serie de atividades realizadas pelo roteador Distribuidor para o tratamento e encaminhamento das unidades de dados de protocolos (PDUs), dentre as quais se destacam:

- A atividade nº 5 indica que os pacotes de dados estão sendo criptografados e encapsulados em PDUs IPsec.
- A atividade nº 6 indica que o protocolo ESP encriptou os pacotes.

- A atividade nº 13 indica que uma mensagem IPsec (AH/ESP) está sendo enviada pela interface.

As atividades acima demonstram o funcionamento da criptografia, encapsulamento e encriptação de pacotes de dados previstas no processo IPsec de Autenticação de dispositivos pares prévio ao envio de dados.

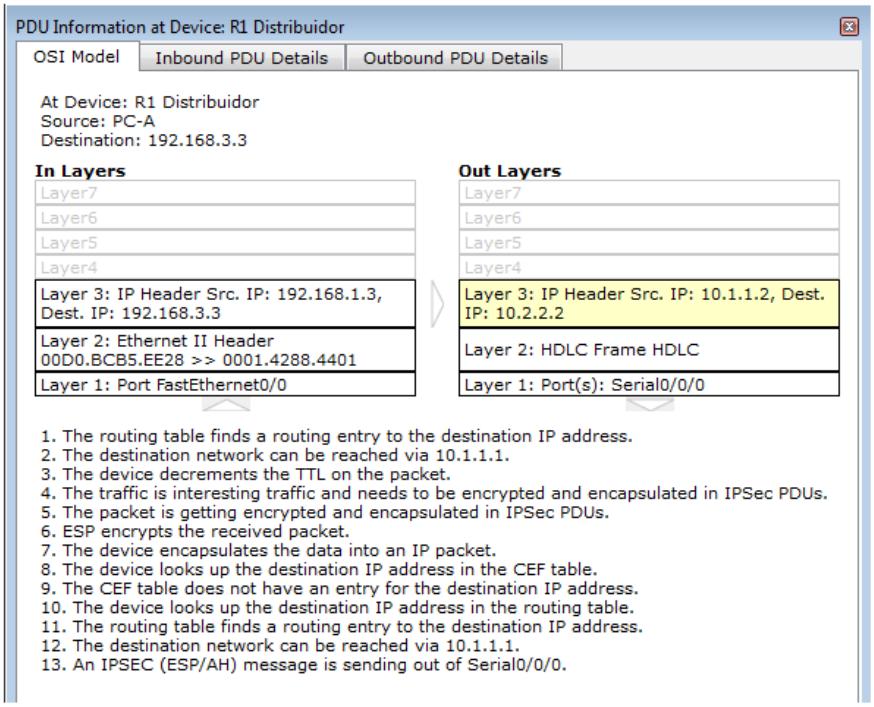


Figura 4-2 - Informações das PDU no Distribuidor. Fonte: Packet Tracer

A Figura 4-3, à esquerda, mostra os detalhes das PDUs dos dados de entrada no roteador Distribuidor, provindo do PC-Distribuidor. Se pode observar que os formatos das PDUs são *Ethernet II, IP e TCP*. No entanto, na Figura 4-3, à direita, mostra os detalhes das PDUs dos dados de saída do roteador Distribuidor, e fluindo pela interface na direção do roteador Provedor para depois seguir até roteador Consumidor, já inclui o formato *Encapsulate Security Payload* (ESP). Sendo que os dados ESP são encriptados com 3DES e autenticados com SHA-1. Assim, fica demonstrado que o processo AH/ESP utiliza o 3DES e o SHA-1 para estabelecer um túnel seguro.

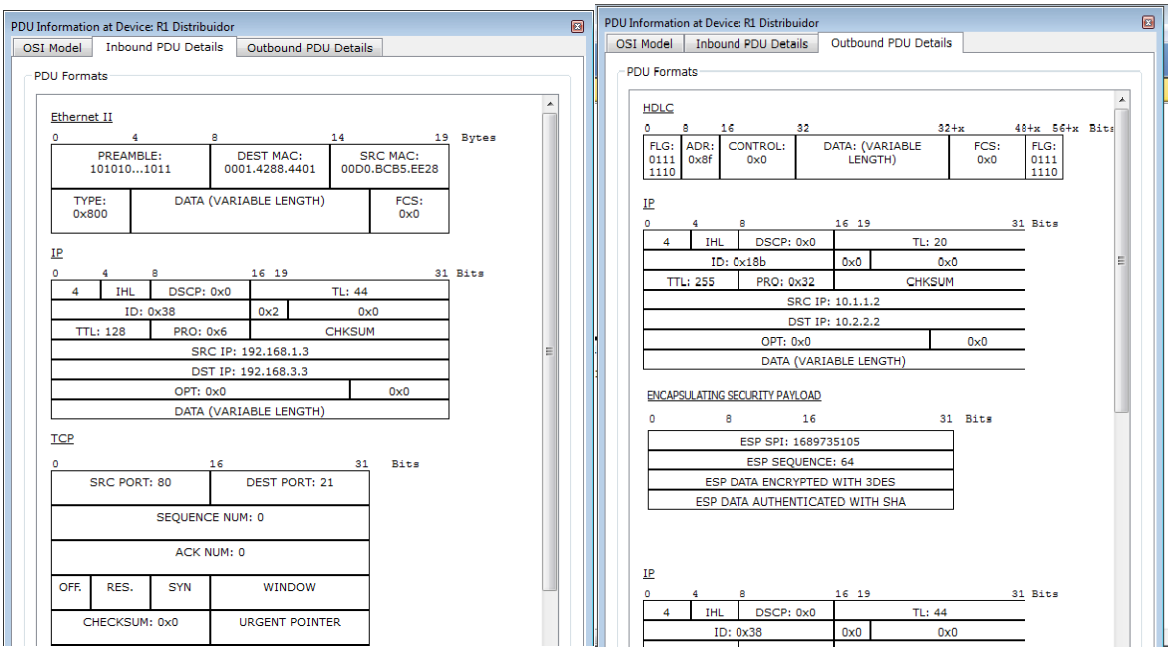


Figura 4-3 - Estrutura das PDUs de Entrada e Saída - Fonte: Packet Tracer

Já a Figura 4-4, à esquerda, mostra que o processo ISAKMP encripta a mensagem quando sai do Distribuidor (pela interface 10.1.1.2) para fluir através do Provedor (entrando na interface 10.2.2.2). E na Figura 4-4, à direita, mostra os detalhes do datagrama do Payload # 1 da Transformada ISAKMP n: º 10, dentre os que podemos comprovar o uso do algoritmo de encriptação AES no modo CBC (*Cipher Block Chaining*) para fornecer Confidencialidade, o uso do algoritmo de hash SHA para fornecer Integridade aos dados, e o uso do DF Grupo 2 para o PSK.

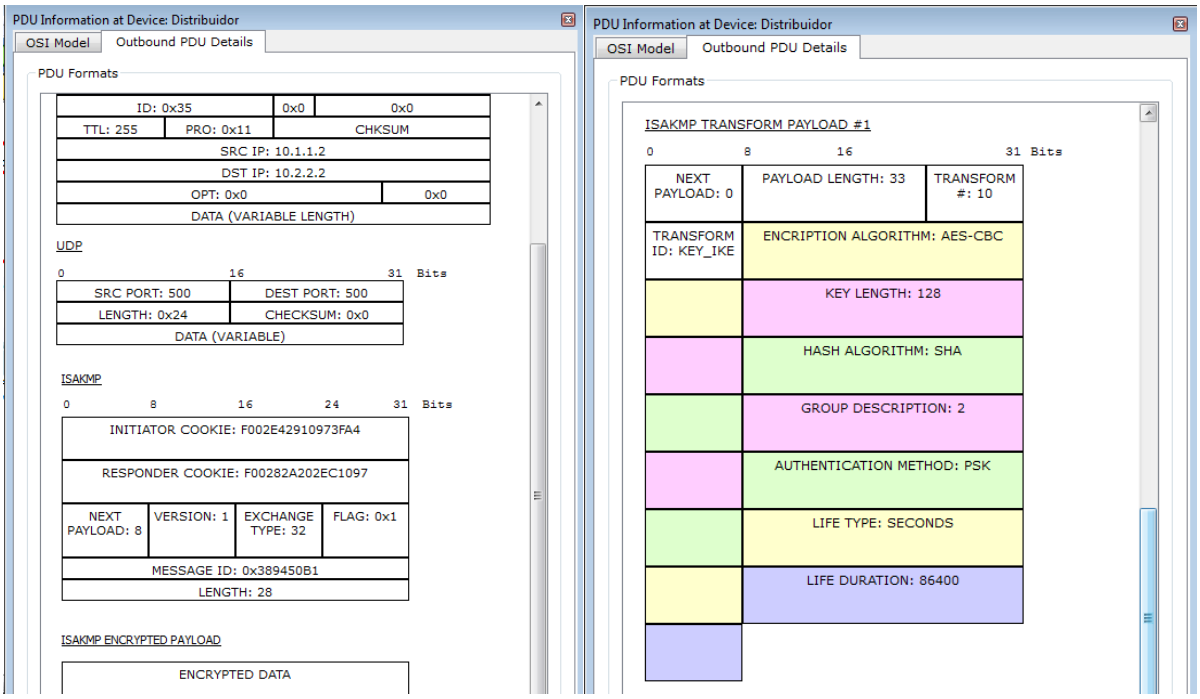


Figura 4-4 - Payloads Encriptado e Transformada ISAKMP - Fonte: Packet Tracer

# 5. TESTES EM LABORATÓRIO COM EQUIPAMENTOS REAIS

Nos testes em laboratório com equipamentos reais, também são aplicadas as tarefas passo-a-passo da metodologia proposta de implementação da VPN, para medir com as ferramentas IPERF e NetPIPE o *jitter* (variação da latência) e a taxa de transferência do fluxo de dados decorrente da parametrização do IPsec, para comparar os resultados com os limites estabelecidos no SGIRM, visando validar a metodologia proposta nesta dissertação.

Cada teste, feito com todos os conjuntos de pares de blocos IPsec de Confidencialidade e Integridade suportados pelos gateways de segurança utilizados para representar os domínios Distribuidor e Consumidor, é repetido vinte vezes visando a análise dos dados e avaliações estatísticas dos resultados com a ferramenta MatLab, com o objetivo de filtrar eventuais erros sistemáticos e identificar padrões, se houverem.

## 5.1. Topologia e Configurações do Sistema de Testes

Os testes, realizados com o apoio do pessoal técnico da Rede Nacional de Ensino e Pesquisa (RNP), Centro Politécnico da UFPR, foram feitos em equipamentos listados na seção 3.9, com uma topologia de rede que reproduz parte da Topologia Básica da CT-IAP, conforme mostrada na Figura 5-1. Esta topologia é similar à que foi utilizada nas simulações apresentadas no capítulo quatro, quando se selecionaram os domínios Distribuidor e Consumidor para estabelecer entre eles uma VPN IPsec.

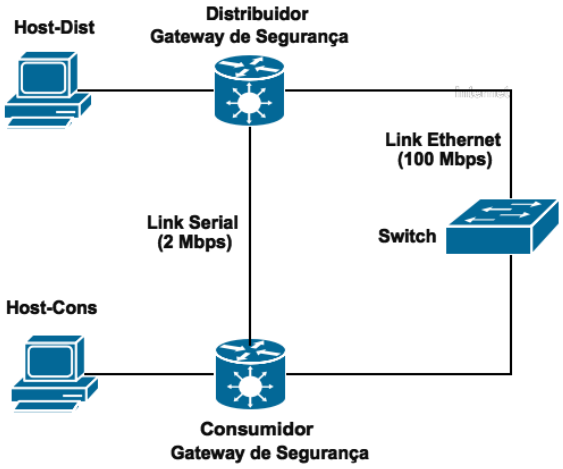


Figura 5-1 - Topologia de Testes - Fonte: O Autor, 2015

Para se visualizar como a Topologia de Testes seria aplicada aos dispositivos da *Smart Grid*, tais como o medidor inteligente (*Smart Meter Energy Services),* instalado na infraestrutura do domínio Consumidor, e a entidade *Neighborhood Area Network* do domínio Distribuidor, que presta serviços de conectividade aos medidores inteligentes para a obtenção das medições das distintas grandezas elétricas e de consumo, na Figura 5-2 superpõem-se as figuras da Topologia de Testes com um zoom da CT-IAP na interface CT-12.

Nesta figura, os links serial de 2 Mbps e ethernet de 100 Mbps representariam a interface lógica CT-12.

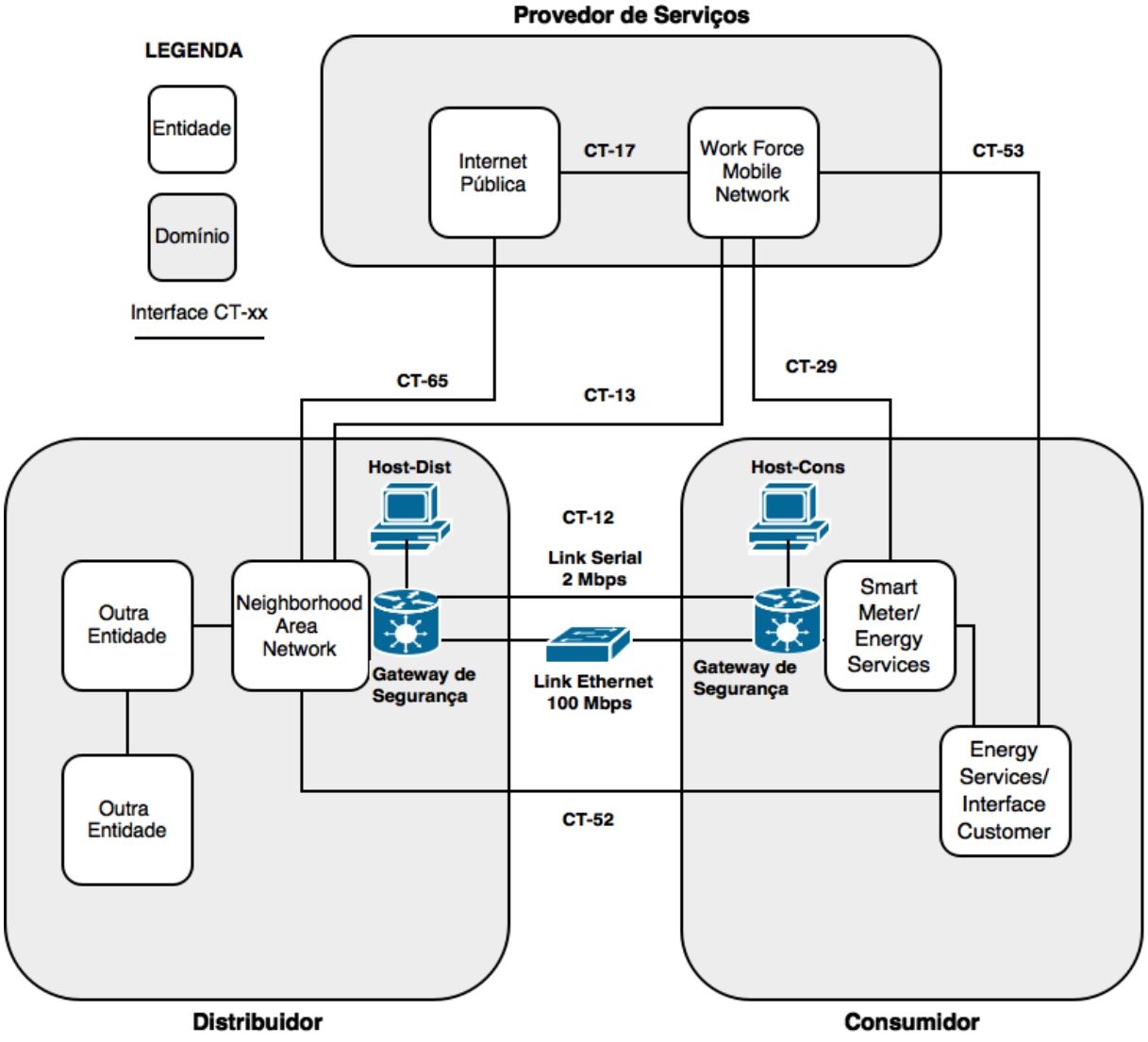


Figura 5-2 - Superposição de Topologia de Testes e a CT-12. Fonte: O Autor

Para se proteger o fluxo de dados na interface CT-12 com o IPsec, é esperado um impacto na latência e banda disponível devido ao overhead gerado pelo protocolo. Para avaliar esse impacto, foi implementado o ambiente de testes com roteadores reais (representados pelos gateways de segurança) e computadores onde foram realizadas uma série de testes de banda e latência utilizando diferentes parâmetros de configuração do IPsec em dois cenários de conectividade de rede entre os domínios Distribuidor e Consumidor: link serial de 2 Mbps e link ethernet de 100 Mbps. Todos os dados e resultados destes testes estão disponíveis no seguinte link da RNP: http://www.pop-pr.rnp.br/noticias/pop-colaboracao-ppgee2/

Destaca-se que os roteadores utilizados nos testes são equipamentos com desempenho médio, existindo outros com melhor ou pior desempenho que ofereceriam resultados com melhor ou pior latência e banda disponível. A Figura 5-3 mostra os equipamentos utilizados:


Figura 5-3 - Equipamentos de Testes em Laboratório – Fonte: O Autor, 2015

**Objetivos dos Testes em Laboratório**

- Verificar a conectividade da rede real de testes.
- Configurar o roteador de gateway de segurança Distribuidor para suportar VPNs-IPsec Site-a-Site com o roteador do domínio Consumidor.

- Configurar o roteador de gateway de segurança do Consumidor para suportar VPNs-IPsec Site-a-Site com o roteador do domínio Distribuidor.
- Implementar um série de testes de desempenho das VPNs-IPsec Site-a-Site visando medir as latências de acesso e de recepção, e taxa de transferência de dados, devido ao overhead adicional introduzidos pela segurança do IPsec nos gateways, no dois cenários de conectividade de rede: link serial de 2 Mbps e link ethernet de 100 Mbps.
- Identificar as ferramentas mais apropriadas e os testes mais confiáveis para as medições pretendidas no item anterior.
- Comparar as medições de latência com as métricas de desempenho estabelecidas pelo SGIRM, visando validar a aplicação da metodologia proposta nesta dissertação.

**Cenário e Antecedentes**

Em vista a subestações (entidades de domínios como Distribuidor, Consumidor, etc.) usam redes ethernet de 100 Mbps e a maior parte dos dispositivos atuais suportam 100 Mbps de tráfego de rede, mesmo que possam usar links de gigabit (1000 Mbps) para suas comunicações externas, na prática as comunicações podem estar limitadas a 2 Mbps (interface serial) ou 100 Mbps (interface ethernet).

Assim, as topologias utilizadas para os testes, composta por dois gateways de segurança interligados por meio de um switch e pelas suas interfaces ethernet, suportam um rendimento máximo teórico de 100 Mbps de tráfego de rede, e também são interligados pelas interfaces seriais de 2 Mbps, tal como mostrado nas Figura 5-1 a Figura 5-3.

Como se deseja medir a latência de acesso e recepção, não é considerada a latência de propagação que na pratica seria própria do link ou interface de comunicação entre quaisquer dois hosts de qualquer rede ou de dois domínios da CT-IAP. Ou seja, a priori a latência de propagação não seria influenciada pelas alterações nas configurações do protocolo IPsec, podendo apenas haver alterações no nível do tráfego de rede em tal link ou interface.

Testes de latência de propagação não podem ser realizados nos links em operação da RNP porque poderão interferir no trafego normal da rede.

## 5.1 O SGIRM e a Latência

Na avaliação de um protocolo de comunicação de um link ou interface, o atraso de acesso de canal inclui qualquer tempo necessário até que a transmissão possa começar. Também inclui quaisquer atrasos na lógica de mover os dados através da interface de comunicação com o meio (codificação dos dados, a adição de correção de erros, etc.). Se o atraso de acesso é medido na aplicação, seriam os atrasos provocados pelo sistema operacional, atrasos de processamento de protocolo (por exemplo, protocolos IP, TCP, IPsec, etc.) e atrasos incorridos da transferência de dados para a interface de comunicação. A combinação dos atrasos de propagação, serialização, filas, e processamento, muitas vezes produz um perfil complexo e variável de latência da rede.

O SGIRM, na tabela 6.3 da referência IEEE STD 2030, 2011, determinou as seguintes referências para os níveis de latência por serviço de interoperabilidade da *Smart Grid*:

- Proteção: < 3 ms (milissegundos)
- Monitoramento: > 160 ms
- Controle: < 3 ms
- Telefonia: > 160 ms

Para o fluxo de dados em determinadas interfaces da CT-IAP, os níveis latências permitidos variam muito em função às aplicações previstas para o Smart Grid, mas as faixas são:

- CT-12: < 1 ms a 1500 ms e 1ms a 15s
- CT-14: < 1 ms a 1500 ms
- CT-15: < 1500 ms
- CT-16: < 1 ms a 1500 ms e 4ms a 15s
- CT-29: < 1 ms a 1500 ms e 1ms a 15s
- CT-52: < 1 ms a 1500 ms e 4ms a 15s
- CT-53: < 10 ms a 5000 ms e 10ms a 15min
- CT-68: < 1 ms a 1500 ms e 4ms a 15s

Para o *payload* (carga útil), a faixa está entre 10 e 1500 bytes, e o *bit rate* (taxa de transferência) entre 1 Kbps e 75 Mbps, nessas interfaces.

## 5.2 Implementação dos Testes em Laboratório

Conforme descrito no roteiro de tarefas (seção 3.6) para a implementação da VPN IPsec Site-a-Site, são criadas duas associações de segurança (SAs), uma SA para IKE (Fase 1 - IKE SA) e outra para a SA IPsec (Fase 2 - IPsec SA), que são implementadas em ambos os gateways de segurança. A Fase 1 intercambia os atributos dos algoritmos de criptografia e hashing para proteger os intercâmbios de parâmetros IPsec da Fase 2.

Assim, para realizar os testes das parametrizações dos blocos de algoritmos de criptografia e autenticação, as mudanças dos parâmetros são feitas na Fase 2 para diferentes configurações de IPsec SA, especificamente conforme detalhado no Passo 3 – Parte A da seção 4.1, para criar 11 (onze) conjuntos VPN-SET.

Estas mudanças de parâmetros foram automatizadas via scrips (rotinas), no ambiente Linux dos hosts dos domínios Distribuidor e Consumidor, para interagir diretamente com seus gateways de segurança, conforme detalhado nos arquivos incluídos nas pastas Scripts no link na RNP. Foram elaboradas 11 (onze) Associações de Segurança (SAs) que representam os 11 (onze) conjuntos de níveis de Confidencialidade e Integridade do framework IPsec que são suportados pelo modelo dos roteadores utilizados como gateways de segurança.

Estes conjuntos de SA IPsec são denominados de VPN-SET0 a VPN-SET10, sendo a VPN-SET0 correspondente ao conjunto SA com Texto-Simples ou *Clear-Text* (VPN sem proteção de criptografia e hashing). Os scripts das implementações destas SAs estão na pasta Scripts no link da RNP: http://www.pop-pr.rnp.br/noticias/pop-colaboracao-ppgee2/. Estes conjuntos VPN-SET0 a 10 foram previamente codificados e armazenados, via CLI, como parâmetros nos sistemas operacionais dos gateways de segurança Distribuidor e Consumidor.

A seguir é apresentado um dos scripts (/testes-ethernet/sripts/distribuidor-VPN-SET1.txt) elaborados para automatizar, via CLI, a mudança da SA do gateway de segurança do domínio Distribuidor:

```
spawn telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
User Access Verification
```

```
Password:
Distribuidor#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Distribuidor(config)#crypto map VPN-MAP 10 ipsec-isakmp
Distribuidor(config-crypto-map)#set transform-set VPN-SET1
Distribuidor(config-crypto-map)#end
Distribuidor#write memory
Building configuration...
[OK]
Distribuidor#dormindo 10s
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.774 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.773 ms
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 2006ms
rtt min/avg/max/mdev = 0.773/0.773/0.774/0.027 ms
```

Cada uma das subpastas VPN-SET contêm arquivos tipo texto, por tipo de teste (Iperf, TCP, UDP), enumerados de 1 a 20, que representam as 20 repetições de cada teste, com exceção do teste NetPipe que apresenta um arquivo por pasta devido a que o próprio teste já realiza 20 (vinte) repetições.

Inicialmente, foram realizados os Testes de Banda (TCP), transferindo um arquivo de 300 MB (para os testes com o link Ethernet de 100 Mbps) e de 30 MB (para os testes com o link serial de 2 Mbps), utilizando a ferramenta IPERF, a partir do Host-Dist (conectado ao gateway de segurança Distribuidor) com destino ao Host-Cons (conectado ao gateway de segurança Consumidor) usando o protocolo TCP/IP para medir a taxa de transferência e latência do tráfego de dados com e sem a segurança IPsec, visando medir a variação provocada pelas distintas opções de blocos de Confidencialidade e Integridade (incluindo Autenticação) do framework IPsec.

Comando e parâmetros aplicados:

***ipterf -c 192.168.1.1 -n 300m*** (testes com link ethernet de 100 Mbps)

***ipterf -c 192.168.1.1 -n 30m*** (testes com link serial de 2 Mbps)

Seguidamente, foram transferidas as mesmas quantidades de dados utilizando a ferramenta NetPipe, mas em diferentes tamanhos de payloads para determinar o efeito do tamanho dos pacotes na comunicação (500 mensagens

variando de 1 a 1536 bytes). Este tipo de teste foi repetido 20 (vinte) vezes para cada tamanho de payload.

Comandos e parâmetros aplicados:

***NPtcp -l 1 -u 1600 -n 500 -p0 –r***

Ping (64 bytes / 1500 bytes):

***ping -A -c 100 192.168.1.1***

***ping -A -c 100 -s 1472 192.168.1.1***

Também foram realizados vários testes de largura de banda usando a ferramenta IPERF. O teste de banda (protocolo UDP) foi com pacotes 64/1500 bytes, por 30 segundos.

Comandos e parâmetros aplicados:

***iperf -c 192.168.1.1 -u -l 36[71] -t 30 -b 100m***

***iperf -c 192.168.1.1 -u -l 1472[72] -t 30 -b 100m***

Todos os dados brutos dos resultados de todos os testes para cada SA estão nas pastas VPN-SET0 a VPN-SET10, subpastas das pastas Testes-Serial e Testes-Ethernet, estão no mesmo link da RNP: http://www.pop-pr.rnp.br/noticias/pop-colaboracao-ppgee2/.

## 5.3 Análise e coleta dos dados dos Testes em Laboratório

Como podem ser verificados no link anterior, os testes geraram uma quantidade considerável de dados (em torno a 7 MB em 4.400 arquivos). Após análises dos dados de cada tipo de arquivo gerado pelos testes, foram determinados os tipos de testes e os dados relevantes para realizar a importação apenas de tais dados. Devido ao volume de arquivos e dados, a importação foi automatizada via funções e scripts codificados na ferramenta MatLab R2014a.

A seguir são apresentados um dos scripts e uma das funções codificadas para a importação seletiva e estatísticas dos dados relevantes. Na pasta MATLAB do link da RNP estão todos os scripts e funções codificadas e utilizadas para a

[71] 20 bytes ip + 8 udp + 36 = 64

[72] 20 bytes ip + 8 udp + 1472 = 1500 - Se desconsidera os cabeçalhos ethernets

importação, cálculos estatísticos e plotagem dos dados relevantes. Caso se deseje executar os scripts e funções, deverá ser copiada a pasta MATLAB, com suas subpastas e arquivos, para o diretório raiz do MatLab do computador. Preferentemente, deve ser utilizada a versão R2014a da ferramenta.

**Script para Cálculo de Estatísticas do Teste Iperf Ping 64 Ethernet**

```
% Script para coleta de dados de Latência RTT(Round Trip Times) %
RTTsaidaPing64Ethernet = zeros(11,28);
for j=1:11
for i=1:20
    RTTsaidaPing64Ethernet(j,i) = importfile15(strcat('testes-ethernet\vpn-
set',int2str(j-1),'\saida_ping64-',int2str(i),'.txt'));
end;

% Estatísticas %
% Cálculo da média %
RTTsaidaPing64Ethernet(j,21) = mean(RTTsaidaPing64Ethernet(j,1:20));
% Identificação do valor mínimo %
RTTsaidaPing64Ethernet(j,22) = min(RTTsaidaPing64Ethernet(j,1:20));
% Identificação do valor máximo %
RTTsaidaPing64Ethernet(j,23) = max(RTTsaidaPing64Ethernet(j,1:20));
Cálculo do Desvío Padrão %
RTTsaidaPing64Ethernet(j,24) = std(RTTsaidaPing64Ethernet(j,1:20));

% Create a normal distribution object by fitting it to the data %
pd = fitdist(RTTsaidaPing64Ethernet(j,1:20).','Normal');
% CI = paramci(PD) returns CI, a 2-by-N array containing 95% ...
% confidence intervals for the parameters of the Prob Dist object PD.
% ci = paramci(pd) returns the array ci containing the lower and upper
% boundaries of the 95% confidence interval for each parameter in
% probability distribution pd.

% Cálculo dos Parâmetros para Intervalo de Confiança de 95%
ci = paramci(pd);
% Identificação do μ Inf
RTTsaidaPing64Ethernet(j,25)= ci(1,1);
% Identificação do μ Sup
RTTsaidaPing64Ethernet(j,26)= ci(2,1);
% Identificação do σ Inf
RTTsaidaPing64Ethernet(j,27)= ci(1,2);
% Identificação do σ Sup
RTTsaidaPing64Ethernet(j,28)= ci(2,2);
end;

% Identificação dos VPN-SETs
for j=2:11
   Cellu = importfile19(strcat('testes-ethernet\scripts\consumidor-VPN-
SET',int2str(j-1),'.txt'));
   VPNSETT(j)=strcat(Cellu(1),'-',Cellu(2));
end;
VPNSET = transpose(VPNSETT);
clear VPNSETT Cellu i j pd ci;
```

**Função de Importação de dados revelantes do Teste Iperf Ping 64**

```
function saidaping641 = importfile15(filename, startRow, endRow)
%IMPORTFILE15 Import numeric data from a text file as a matrix.
%   SAIDAPING641 = IMPORTFILE15(FILENAME) Reads data from text file
%   FILENAME for the default selection.
%
%   SAIDAPING641 = IMPORTFILE15(FILENAME, STARTROW, ENDROW) Reads
data from
%   rows STARTROW through ENDROW of text file FILENAME.
%
% Example:
%   saidaping641 = importfile15('saida_ping64-1.txt', 104, 104);
%
%    See also TEXTSCAN.
% Auto-generated by MATLAB on 2015/07/28 19:32:34
%% Initialize variables.
delimiter = {' ','/'};
if nargin<=2
    startRow = 104;
    endRow = inf;
end
%% Format string for each line of text:
%   column8: double (%f)
% For more information, see the TEXTSCAN documentation.
formatSpec =
'%*s%*s%*s%*s%*s%*s%*s%f%*s%*s%*s%*s%*s%*s%*s%*s%[^\n\r]';
%% Open the text file.
fileID = fopen(filename,'r');
%% Read columns of data according to format string.
% This call is based on the structure of the file used to generate
this
% code. If an error occurs for a different file, try regenerating
the code
% from the Import Tool.
textscan(fileID, '%[^\n\r]', startRow(1)-1, 'ReturnOnError', false);
dataArray = textscan(fileID, formatSpec, endRow(1)-startRow(1)+1,
'Delimiter', delimiter, 'MultipleDelimsAsOne', true,
'ReturnOnError', false);
for block=2:length(startRow)
    frewind(fileID);
    textscan(fileID, '%[^\n\r]', startRow(block)-1, 'ReturnOnError',
false);
    dataArrayBlock = textscan(fileID, formatSpec, endRow(block)-
startRow(block)+1, 'Delimiter', delimiter, 'MultipleDelimsAsOne',
true, 'ReturnOnError', false);
    dataArray{1} = [dataArray{1};dataArrayBlock{1}];
end
%% Close the text file.
fclose(fileID);
%% Post processing for unimportable data.
% No unimportable data rules were applied during the import, so no
post
% processing code is included. To generate code which works for
```

```
% unimportable data, select unimportable cells in a file and
regenerate the
% script.
%% Create output variable
saidaping641 = [dataArray{1:end-1}];
```

## 5.4 Análises de Resultados dos Testes em Laboratório

Os resultados dos testes realizados são apresentados com as médias, mínimas e máximas das métricas de RTT[73] *(Round Trip Times)* em ms (milissegundos) para a latência, e em Mbps (Mega bits por segundo) para o teste de banda *(throughput),* contabilizadas para as 20 (vinte) repetições dos testes para cada VPN-SET, visando as comparações dos desempenhos e o descarte dos erros não sistemáticos. Também, visando identificar distorções significativas nas medições, são incluídos o Desvio Padrão (S) das 20 (vinte) repetições de testes por VPN-SET, calculados diretamente no MatLab pela formula:

$$s = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \overline{x})^2}$$

**Latência**

A Tabela 5-1 (para os testes com o link ethernet de 100 Mbps) e a Tabela 5-2 (para os testes com o link Serial de 2 Mbps), apresentam os valores de latências para fluxo de dados em Texto Simples (sem a segurança do IPsec) e os valores de latência quando são aplicadas os distintos níveis de Confidencialidade e Integridade da segurança do IPsec (criptografias, funções de hashing e tamanhos de chaves). Os mesmos testes foram aplicados em dois tamanhos de payloads (64 e 1500 bytes) devido ao impacto que também causa o processamento da fragmentação dos pacotes de dados no desempenho. Como valores de referência, também são inseridos nessas tabelas os limites de latência estabelecidos pelo SGIRM para a interface CT-12.

[73] É medido a partir do momento em que a informação é colocada na rede até o momento que a confirmação de recebimento é entregue ao remetente.

Tabela 5-1 - Link Ethernet: Latências por overhead do IPsec - Fonte: O Autor, 2015

| Tamanho do Pacote | VPN SET | Criptografia (Bloco Confidencialidade) | Função de Hashing (Bloco Integridade + Autenticação) | | | | | | | | Interface CT-12 SGIRM |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Latência (ms) | | | | | | | | |
| | | | Med | Min | Max | S (%) | Med | Min | Max | S (%) | |
| 64 bytes | 0 | Texto Simples | 0,457 | 0,424 | 0,489 | 2,0 | 0,457 | 0,424 | 0,489 | 2,0 | <1,0 a 1500 |
| | | | MD5 | | | | SHA1 | | | | |
| | 1/2 | DES | 1,726 | 1,698 | 1,746 | 1,2 | 1,727 | 1,693 | 1,741 | 1,2 | < 1,0 a 1500 |
| | 3/4 | 3DES | 1,753 | 1,731 | 1,768 | 0,9 | 1,733 | 1,716 | 1,755 | 1,0 | < 1,0 a 1500 |
| | 5/8 | AES 128 | 1,762 | 1,746 | 1,782 | 1,0 | 1,743 | 1,723 | 1,756 | 1,0 | < 1,0 a 1500 |
| | 6/9 | AES 192 | 1,759 | 1,738 | 1,777 | 1,2 | 1,744 | 1,729 | 1,763 | 0,9 | < 1,0 a 1500 |
| | 7/10 | AES 256 | 1,763 | 1,742 | 1,779 | 0,9 | 1,759 | 1,737 | 1,773 | 1,1 | < 1,0 a 1500 |
| 1500 bytes | 0 | Texto Simples | 1,618 | 1,595 | 1,630 | 1,0 | 1,618 | 1,595 | 1,630 | 1,0 | <1,0 a 1500 |
| | | | MD5 | | | | SHA1 | | | | |
| | 1/2 | DES | 3,569 | 3,534 | 3,602 | 1,9 | 3,571 | 3,539 | 3,600 | 1,7 | < 1,0 a 1500 |
| | 3/4 | 3DES | 3,680 | 3,650 | 3,713 | 1,8 | 3,666 | 3,634 | 3,697 | 1,5 | < 1,0 a 1500 |
| | 5/8 | AES 128 | 3,581 | 3,555 | 3,605 | 1,9 | 3,586 | 3,554 | 3,608 | 1,3 | < 1,0 a 1500 |
| | 6/9 | AES 192 | 3,596 | 3,562 | 3,634 | 2,0 | 3,585 | 3,557 | 3,641 | 2,3 | < 1,0 a 1500 |
| | 7/10 | AES 256 | 3,633 | 3,602 | 3,659 | 1,9 | 3,627 | 3,590 | 3,669 | 2,4 | < 1,0 a 1500 |

Observa-se na Tabela 5-1 que para os testes com pacotes de 64 bytes a variação relativa da latência média, entre o fluxo em Texto Simples e o fluxo com as distintas criptografias (DES, 3DES, AES 128, AES 192 e AES 256) juntamente com as funções de hashing (MD5 e SHA), é próximo a 400%. No entanto, em termos absolutos o aumento na latência média é em torno a 1,3 ms.

Assim também, para os testes com pacotes de 1500 bytes, a variação relativa da latência média, entre o fluxo em Texto Simples e o fluxo com as distintas criptografias (DES, 3DES, AES 128, AES 192 e AES 256) juntamente com as funções de hashing (MD5 e SHA1), é em torno a 220%. No entanto, em termos absolutos o aumento na latência média é em torno a 2,0 ms.

Também se observa que a variação da latência média com as trocas das criptografias do nível de Confidencialidade mais fraco (DES) ao mais forte (AES 256) é de 0,037 ms quando é utilizada a função de hashing MD5 (para pacotes de 64 bytes) e 0,064 ms (para pacotes de 1500 bytes). As variações da latência média estão na mesma ordem de grandeza quando é utilizada a função de hashing SHA1. Esta variação ínfima pode decorrer da capacidade dos gateways de segurança no processamento dos distintos algoritmos de criptografia e hashing.

Assim, a escolha apropriada dos blocos de criptografia e função de hashing estaria na longevidade dos algoritmos e chaves. Exemplo: AES de 256 bits teria

uma vida útil muito além de 2030, no entanto o 3DES não além de 2030, conforme referências na Tabela 3-5. Também, as referências de overhead na Latência apresentadas indicam que os resultados das medições estão próximos dos valores de referência.

Os Desvios Padrão (S), tanto para os testes com 64 e 1500 bytes, permaneceram na faixa de 0,9 a 2,4 %, o qual indica a ausência de distorções significativas nos resultados das medições.

Para aprofundar a análise estatística dos resultados, também foram tabulados os cálculos, feitos via codificação no MatLab, dos Intervalos de Confiança (CI no MatLab) para os parâmetros da Distribuição Normal (PD no MatLab) das medições para cada VPN-SET (rotina detalhada na seção 5.3). Na Tabela 5-2 são apresentados os limites inferior e superior para o parâmetro μ (mu ou média), e os limites inferior e superior para o parâmetro σ (sigma ou desvio padrão), todos para o Intervalo de Confiança de 95 % das medições de latências para os testes com o link ethernet.

Os Intervalos de Confiança da Tabela 5-2 corroboram a ausência de distorções significativas nos resultados, e a presença de um padrão de Distribuição Normal dessas medições.

Tabela 5-2 - Link Ethernet: Intervalo de Confiança - Fonte: O Autor, 2015

| **Tamanho do Pacote** | **VPN SET** | **Criptografia (Bloco Confidencialidade)** | **Função de Hashing (Bloco Integridade + Autenticação)** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Intervalo de Confiança (μ em ms e σ em %) das Latências (95 %) | | | | | | | |
| | | | μ Inf | μ Sup | σ Inf | σ Sup | μ Inf | μ Sup | σ Inf | σ Sup |
| 64 bytes | **0** | **Texto Simples** | 0,4480 | 0,4667 | 1,53 | 2,93 | 0,4480 | 0,4667 | 1,53 | 2,93 |
| | | | **MD5** | | | | **SHA1** | | | |
| | **1/2** | **DES** | 1,7207 | 1,7316 | 0,89 | 1,70 | 1,7216 | 1,7323 | 0,88 | 1,68 |
| | **3/4** | **3DES** | 1,7492 | 1,7575 | 0,68 | 1,30 | 1,7286 | 1,7380 | 0,76 | 1,46 |
| | **5/8** | **AES 128** | 1,7579 | 1,7669 | 0,73 | 1,39 | 1,7380 | 1,7471 | 0,74 | 1,43 |
| | **6/9** | **AES 192** | 1,7538 | 1,7649 | 0,91 | 1,75 | 1,7396 | 1,7485 | 0,72 | 1,37 |
| | **7/10** | **AES 256** | 1,7588 | 1,7672 | 0,69 | 1,32 | 1,7536 | 1,7638 | 0,82 | 1,58 |
| 1500 bytes | **0** | **Texto Simples** | 1,6131 | 1,6221 | 0,73 | 1,40 | 1,6131 | 1,6221 | 0,73 | 1,40 |
| | | | **MD5** | | | | **SHA1** | | | |
| | **1/2** | **DES** | 3,5607 | 3,5780 | 1,41 | 2,71 | 3,5629 | 3,5787 | 1,29 | 2,47 |
| | **3/4** | **3DES** | 3,6710 | 3,6881 | 1,40 | 2,68 | 3,6587 | 3,6732 | 1,17 | 2,25 |
| | **5/8** | **AES 128** | 3,5723 | 3,5897 | 1,41 | 2,71 | 3,5798 | 3,5924 | 1,02 | 1,96 |
| | **6/9** | **AES 192** | 3,5870 | 3,6056 | 1,51 | 2,90 | 3,5741 | 3,5960 | 1,78 | 3,42 |
| | **7/10** | **AES 256** | 3,6237 | 3,6415 | 1,45 | 2,78 | 3,6154 | 3,6380 | 1,84 | 3,54 |

Por outro lado, para os testes com o link serial de 2 Mbps, observa-se na Tabela 5-3 que para os testes com pacotes de 64 bytes a latência média do fluxo em

Texto Simples é de 1,98 ms e as latências médias do fluxo com as distintas criptografias (DES, 3DES, AES 128, AES 192 e AES 256) juntamente com as funções de hashing (MD5 e SHA), está em torno a 4,20 ms.

Já para os testes com pacotes de 1500 bytes, a latência média do fluxo em Texto Simples é de 25,11 ms e as latências médias do fluxo com as distintas criptografias (DES, 3DES, AES 128, AES 192 e AES 256) juntamente com as funções de hashing (MD5 e SHA), está em torno a 29,0 ms. Como era esperado, o uso de links com taxa de transferência baixa como o de 2 Mbps tem um impacto significativo nas latências. Assim, o uso destes links nas interfaces do CT-IAP deve ser bem avaliado em função dos requisitos de latência.

Também se observa na Tabela 5-3 que a variação da latência média com as trocas das criptografias do nível de Confidencialidade mais fraco (DES) ao mais forte (AES 256), é de 0,3 ms quando é utilizada a função de hashing MD5 (para pacotes de 64 bytes) e 0,67 ms (para pacotes de 1500 bytes). As variações da latência média estão na mesma ordem de grandeza quando é utilizada a função de hashing SHA1.

Tabela 5-3 - Link Serial: Latências por overhead do IPsec - Fonte: O Autor, 2015

| **Tamanho do Pacote** | **VPN SET** | **Criptografia (Bloco Confidencialidade)** | **Função de Hashing (Bloco Integridade + Autenticação)** | | | | | | | | **Interface CT-12 SGIRM** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Latência (ms) | | | | | | | | |
| | | | Med | Min | Max | S (%) | Med | Min | Max | S (%) | |
| 64 bytes | **0** | **Texto Simples** | 1,980 | 1,946 | 2,002 | 1,5 | 1,980 | 1,946 | 2,002 | 1,5 | <1,0 a 1500 |
| | | | **MD5** | | | | **SHA1** | | | | |
| | **1/2** | **DES** | 4,028 | 4,008 | 4,044 | 1,2 | 4,039 | 4,020 | 4,053 | 1,0 | < 1,0 a 1500 |
| | **3/4** | **3DES** | 4,056 | 4,037 | 4,073 | 0,9 | 4,043 | 4,025 | 4,059 | 1,1 | < 1,0 a 1500 |
| | **5/8** | **AES 128** | 4,376 | 4,292 | 5,568 | 28,1 | 4,427 | 4,276 | 6,930 | 59,0 | < 1,0 a 1500 |
| | **6/9** | **AES 192** | 4,317 | 4,300 | 4,330 | 0,9 | 4,433 | 4,289 | 6,724 | 53,9 | < 1,0 a 1500 |
| | **7/10** | **AES 256** | 4,328 | 4,309 | 4,345 | 0,9 | 7,437 | 4,299 | 66,737 | 1395 | < 1,0 a 1500 |
| 1500 bytes | **0** | **Texto Simples** | 25,11 | 25,09 | 25,15 | 1,7 | 25,11 | 25,09 | 25,15 | 1,7 | <1,0 a 1500 |
| | | | **MD5** | | | | **SHA1** | | | | |
| | **1/2** | **DES** | 28,55 | 28,54 | 28,56 | 0,8 | 29,61 | 28,55 | 49,27 | 462,7 | < 1,0 a 1500 |
| | **3/4** | **3DES** | 28,61 | 28,56 | 29,07 | 10,8 | 28,57 | 28,55 | 28,59 | 0,9 | < 1,0 a 1500 |
| | **5/8** | **AES 128** | 28,95 | 28,93 | 28,97 | 0,9 | 30,55 | 28,93 | 61,08 | 718,6 | < 1,0 a 1500 |
| | **6/9** | **AES 192** | 28,96 | 28,95 | 28,97 | 0,6 | 28,96 | 28,95 | 28,98 | 0,7 | < 1,0 a 1500 |
| | **7/10** | **AES 256** | 29,20 | 28,95 | 32,03 | 76,4 | 28,96 | 28,95 | 28,97 | 0,7 | < 1,0 a 1500 |

No caso dos testes com o link serial de 2 Mbps, os Desvios Padrão (S), tanto para os testes com 64 e 1500 bytes, apresentam casos com distorções significativas nos resultados das medições (>>2%), conforme mostrado na Tabela 5-3. Estas

distorções podem decorrer da sobrecarga no processamento da taxa de transferência de dados mais o processamento dos algoritmos de criptografia e hashing, quando da utilização do link de baixa velocidade como o de 2 Mbps, pois uma baixa distorção (1,5 a 1,7%) é observada quando o fluxo é em Texto Simples.

Do link na RNP pode ser baixada a planilha Dados_Relevantes_dos_Resultados_dos_20_Testes.xlsx que inclui a tabulação de todos os dados das medições e os cálculos dos limites inferior e superior para o parâmetro μ (mu ou média), e os limites inferior e superior para o parâmetro σ (sigma ou desvio padrão), para o Intervalo de Confiança de 95 % das medições de latências para todos os testes com o link serial. Os parâmetros μ e σ para tal Intervalo de Confiança apresentam distorções significativas em algumas das medições com o link serial.

Na Figura 5-4 é mostrado o gráfico dos resultados de testes NetPipe com link ethernet de 100 Mbps, específicos de variação de latência de acordo ao tamanho dos pacotes de dados (payloads) de 1 a 1560 bytes, para os distintos conjuntos de blocos de Confidencialidade e Integridade (VPN-SET 0 a 10, conjuntos enumerados na Tabela 5-1). As superposições da plotagem no gráfico corroboram a diferença ínfima na latência devido à troca dos algoritmos e tamanho de chaves. Neste teste, a métrica de latência da ferramenta NetPipe é a metade do RTT, ou seja só o tempo de ida dos dados entre o remetente e receptor. A Figura 5-5 é um zoom nas curvas de latência para visualizar as diferenças para o ponto 1500 bytes (em torno a 0,07 ms entre a VPN1 e VPN10).

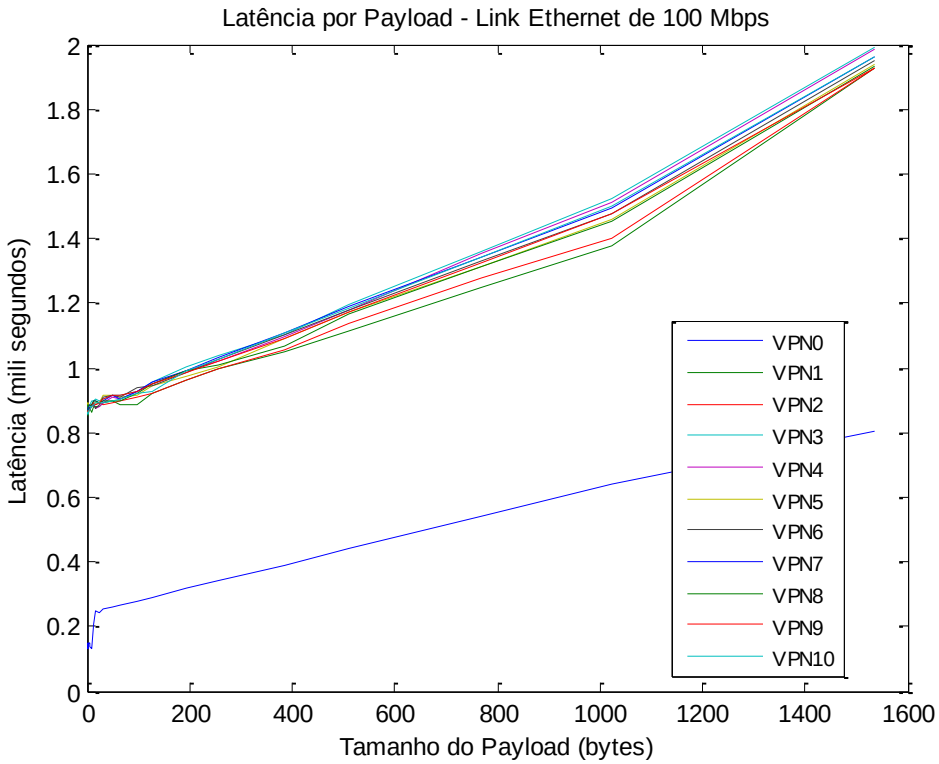


Figura 5-4 - Latência por Payload, Link Ethernet - Fonte: O Autor, 2015

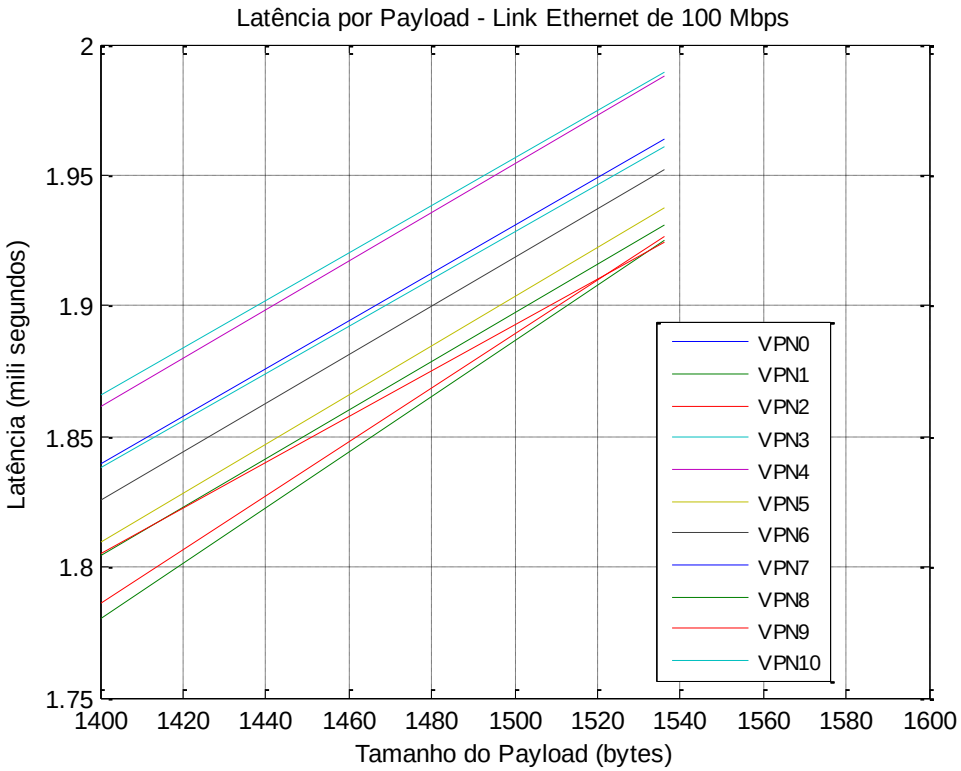


Figura 5-5 - Zoom em 1500 bytes - Fonte: O Autor, 2015

Analogamente aos testes NetPipe feitos com o link ethernet, a Figura 5-6 e a Figura 5-7 mostram os gráficos dos testes NetPipe feitos com o link serial:

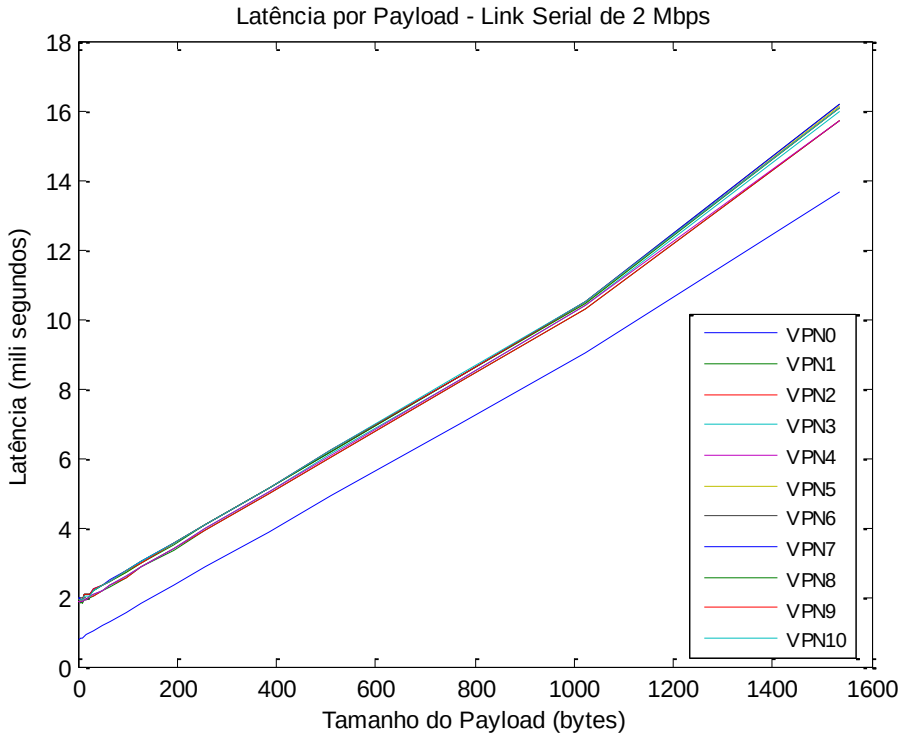


Figura 5-6 - Latência por Payload, Link Serial - Fonte: O Autor, 2015

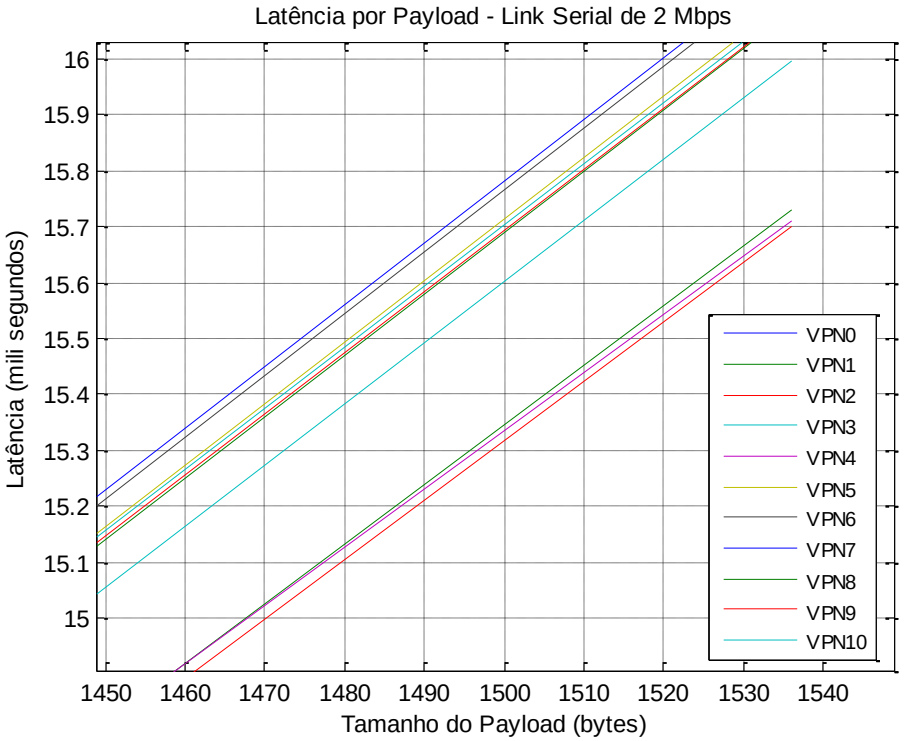


Figura 5-7 - Zoom em 1500 bytes - Fonte: O Autor, 2015

**Considerações finais sobre as latências nos links ethernet e serial**

Como o impacto do overhead da segurança do IPsec na latência está numa faixa de 1,8 a 3,6 ms para os testes com o link ethernet, esta faixa está próximo do limite de tolerância fixado pelo SGIRM para as comunicações de Proteção e Controle (< 3 ms). Em contrapartida, para os testes com o link serial a latência está na faixa de 4,0 a 29,2 ms, o que extrapola a tolerância de latência para as comunicações para Proteção e Controle (< 3 ms).

No entanto, para algumas interfaces de comunicação da CT-IAP, listadas no final da seção 5.1, as faixas acima estariam dentro dos intervalos de faixa de latências permitidas (p.e. CT-12 < 1 ms a 1500 ms; CT-53 < 10 ms a 5000 ms).

De qualquer maneira, deverá ser sempre levado em consideração, e medido quando possível, o nível de latência de propagação do link que será agregado à latência provocada pelo overhead de segurança do IPsec.

Também, como foi identificado nos testes com o link serial, há um incremento importante na latência quando o tamanho do payload é de 1500 bytes, o que deve ser considerado quando determinadas aplicações no Smart Grid exijam esse tamanho de payload e baixas latências nas interfaces do CT-IAP.

**Throughput**

A Tabela 5-4 apresentam os resultados dos testes de *throughput* com o protocolo TCP e arquivo de 300 MB, feitos com o link ethernet de 100 Mbps, para fluxo de dados em Texto Simples (sem a segurança do IPsec) e os valores quando são aplicados os distintos níveis de Confidencialidade e Integridade da segurança do IPsec (criptografias, funções de hashing e tamanhos de chaves).

Observa-se um significativo impacto do overhead de segurança do IPsec reduzindo o throughput médio de 94,15 Mbps a próximo de 29 Mbps, redução a 30%. Neste caso, entenderia-se que o uso dos recursos computacionais para o processamento dos algoritmos de criptografia e hashing reduzem consideravelmente a taxa de transferência dos dados. Como valores de referência, também são inseridos na Tabela 5-4 os limites de throughput estabelecidos pelo SGIRM para a interface CT-12.

Tabela 5-4 - Link Ethernet: Throughput - Fonte: O Autor, 2015

| Tamanho do Arquivo de teste | VPN SET | Criptografia (Bloco Confidencialidade) | Função de Hashing (Bloco Integridade + Autenticação) | | | | | | | | Interface CT-12 SGIRM |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Throughput (Mbps) | | | | | | | | |
| | | | Med | Min | Max | S (%) | Med | Min | Max | S (%) | |
| 300 MB (TCP) | 0 | Texto Simples | 94,15 | 94,10 | 94,20 | 5,1 | 94,15 | 94,10 | 94,20 | 5,1 | 0,001 a 30,0 |
| | | | MD5 | | | | SHA1 | | | | |
| | 1/2 | DES | 29,28 | 28,70 | 29,40 | 16,5 | 29,16 | 28,90 | 29,40 | 13,9 | 0,001 a 30,0 |
| | 3/4 | 3DES | 29,07 | 28,50 | 29,20 | 15,0 | 29,07 | 28,50 | 29,20 | 16,6 | 0,001 a 30,0 |
| | 5/8 | AES 128 | 28,61 | 28,00 | 29,00 | 22,2 | 28,49 | 28,10 | 28,60 | 11,2 | 0,001 a 30,0 |
| | 6/9 | AES 192 | 28,60 | 28,00 | 28,70 | 15,9 | 28,82 | 28,50 | 28,90 | 9,3 | 0,001 a 30,0 |
| | 7/10 | AES 256 | 28,68 | 28,60 | 28,70 | 4,4 | 28,78 | 28,10 | 28,90 | 16,8 | 0,001 a 30,0 |

Os Desvios Padrão (S), para os testes TCP com 300 MB com o link ethernet, apresentam distorções consideráveis nos resultados das medições (>15% na maioria das VPN-SET), conforme mostrado na Tabela 5-4. Estas distorções também podem decorrer da sobrecarga no processamento da taxa de transferência de dados mais o processamento dos algoritmos de criptografia e hashing, mas a distorção observada de 5,1% quando o fluxo é em Texto Simples já é um indicativo que o próprio processamento da taxa de transferência e/ou o protocolo TCP tem um peso importante no desempenho do link ethernet para o volume do arquivo de teste (300MB). Os parâmetros μ e σ calculados para o Intervalo de Confiança de 95 % também corroboram as distorções significativas nestas medições.

A Tabela 5-5 apresenta os resultados dos testes de throughput com o protocolo TCP e arquivo de 30 MB, feitos com o link serial de 2 Mbps, também para fluxo de dados em Texto Simples e os valores quando são aplicados os distintos níveis de Confidencialidade e Integridade da segurança do IPsec.

Tabela 5-5 - Link Serial: Throughput - Fonte: O Autor, 2015

| Tamanho do Arquivo de teste | VPN SET | Criptografia (Bloco Confidencialidade) | Função de Hashing (Bloco Integridade + Autenticação) | | | | | | | | Interface CT-12 SGIRM |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Throughput (Mbps) | | | | | | | | |
| | | | Med | Min | Max | S (%) | Med | Min | Max | S (%) | |
| 30 MB (TCP) | 0 | Texto Simples | 1,019 | 1,010 | 1,020 | 0,31 | 1,019 | 1,010 | 1,020 | 0,31 | 0,001 a 30,0 |
| | | | MD5 | | | | SHA1 | | | | |
| | 1/2 | DES | 0,963 | 0,953 | 0,973 | 0,60 | 0,961 | 0,955 | 0,973 | 0,51 | 0,001 a 30,0 |
| | 3/4 | 3DES | 0,963 | 0,954 | 0,975 | 0,67 | 0,965 | 0,956 | 0,975 | 0,57 | 0,001 a 30,0 |
| | 5/8 | AES 128 | 0,955 | 0,944 | 0,961 | 0,42 | 0,955 | 0,951 | 0,959 | 0,26 | 0,001 a 30,0 |
| | 6/9 | AES 192 | 0,955 | 0,945 | 0,963 | 0,48 | 0,955 | 0,948 | 0,962 | 0,36 | 0,001 a 30,0 |
| | 7/10 | AES 256 | 0,954 | 0,947 | 0,961 | 0,35 | 0,955 | 0,948 | 0,963 | 0,34 | 0,001 a 30,0 |

Os resultados dos testes com o link serial de 2 Mbps apresentam dados que demonstram uma média de baixa redução relativa do throughput devido ao overhead do IPsec (em torno a 6 %). Também, os Desvios Padrão (S) permaneceram baixos, na faixa de 0,31 a 0,67 %, o qual indica a ausência de distorções significativas nos resultados das medições. Os parâmetros μ e σ calculados para o Intervalo de Confiança de 95 % também corroboram a ausência de distorções significativas nos resultados, e a presença de um padrão de Distribuição Normal dessas medições.

Estes resultados indicam que o link serial tem um desempenho uniforme mesmo com a troca das VPN-SETs, e estável para as 20 (vinte) repetições de cada teste.

**Considerações finais sobre o Throughput**

Nos testes com o link ethernet de 100 Mbps, o impacto do overhead da segurança do IPsec na taxa de transferência o reduz a em torno de 30 Mbps, e a faixa de operação para algumas interfaces de comunicação da CT-IAP, listadas no final da seção 5.1, segundo o SGIRM deve estar entre 1 Kbps e 75 Mbps, e em particular entre 1 Kbps e 30 Mbps para a CT-12. Deverá ser levado em conta este impacto quando da necessidade de transferências de volumes de dados consideráveis que requeiram Confidencialidade e Integridade (mais Autenticação) e seja necessário o uso do link ethernet de 100 Mbps.

Por outro lado, quando é desejável um nível baixo, e constante, da incidência do overhead do IPsec na taxa de transferência do link de comunicação, os testes com o link serial demonstram que seu uso é o mais indicado.

Os resultados das simulações e testes em laboratório demonstram a aplicabilidade e viabilidade da metodologia proposta para implementação da VPN e a parametrização do framework do IPsec. Tal metodologia pode ser aplicada a qualquer par de domínios ou entidades da topologia da arquitetura de rede da CT-IAP do SGIRM de acordo aos níveis de serviços exigidos para a Confidencialidade e Integridade dos dados para cada interface entre domínios e entre entidades.

Também, os resultados dos testes com as repetições exaustivas sugerem que a metodologia de medições do overhead do IPsec na latência e throughput, pode ser aplicada a qualquer par de domínios ou entidades da CT-IAP.

## 5.5 Vulnerabilidades, Ameaças, Ataques e Mitigação de Riscos

É importante analisar o impacto de possíveis ataques cibernéticos à rede elétrica. Atualmente, se dispõe de simuladores como o *Real-time Digital Simulator* (RTDS), que pode simular distintos tipos de ciber ataques reais, como o ataque de inundação de TCP SYN e o *Man-in-the-Middle*. Estas simulações podem ser realizadas nos modelos *IEEE Standard Power System Test* para analisar o impacto dos ciber ataques na *Smart Grid* (LIU, R.; SRIVASTAVA, A., 2015).

Não é objetivo desta pesquisa a aplicação da Avaliação de Riscos da Política de Segurança, previstas no conjunto de atividades das cinco etapas do Processo da Segurança do item 2.1.2 (IEC 62351-1 TS), no entanto, como exemplo de Avaliação de Riscos, algumas das suas atividades previstas são aqui discutidas:

- Identificação de vulnerabilidades.
- Identificação de ameaças.
- Mitigação dos Riscos

Estas atividades são implementadas no roteador de segurança do domínio Distribuidor, identificando as ameaças a que está exposta esse dispositivo durante a programação CLI, em consequência às vulnerabilidades que oferece, e procurar mitigar os riscos.

### Vulnerabilidades e Ameaças

Resumidamente, as atividades específicas aplicadas no roteador Distribuidor são:

- Identificação da vulnerabilidade: Acesso físico local via console, ou remotamente via Telnet, tomando o controle do dispositivo.
- Identificação das ameaças: Manipulação do dispositivo via acesso a seus dados de configuração, incluindo acesso direto às senhas, quebra de senhas criptografadas e da chave de hashing via ataques de Força Bruta.

**Ataque de Força Bruta**

Os casos simulados foram quando o atacante, que tem habilidades em CLI, toma o controle de acesso do roteador Distribuidor, independente do meio de acesso ser local ou remoto, e realiza tentativas de manipulação da configuração do dispositivo, considerando que tal atacante conta com um dos softwares de criptoanálise disponíveis para ser baixado da internet como o *Cain & Abel, v4.9.56*.

**Caso 1:** Tentativa de quebra da senha de acesso ao modo privilegiado do roteador, utilizando o ataque de Força Bruta do software *Cain & Abel, v4.9.56*.

**Resultado:** O atacante teve sucesso imediato, conforme mostrado no campo *Decrypted password* da Figura 5-8:

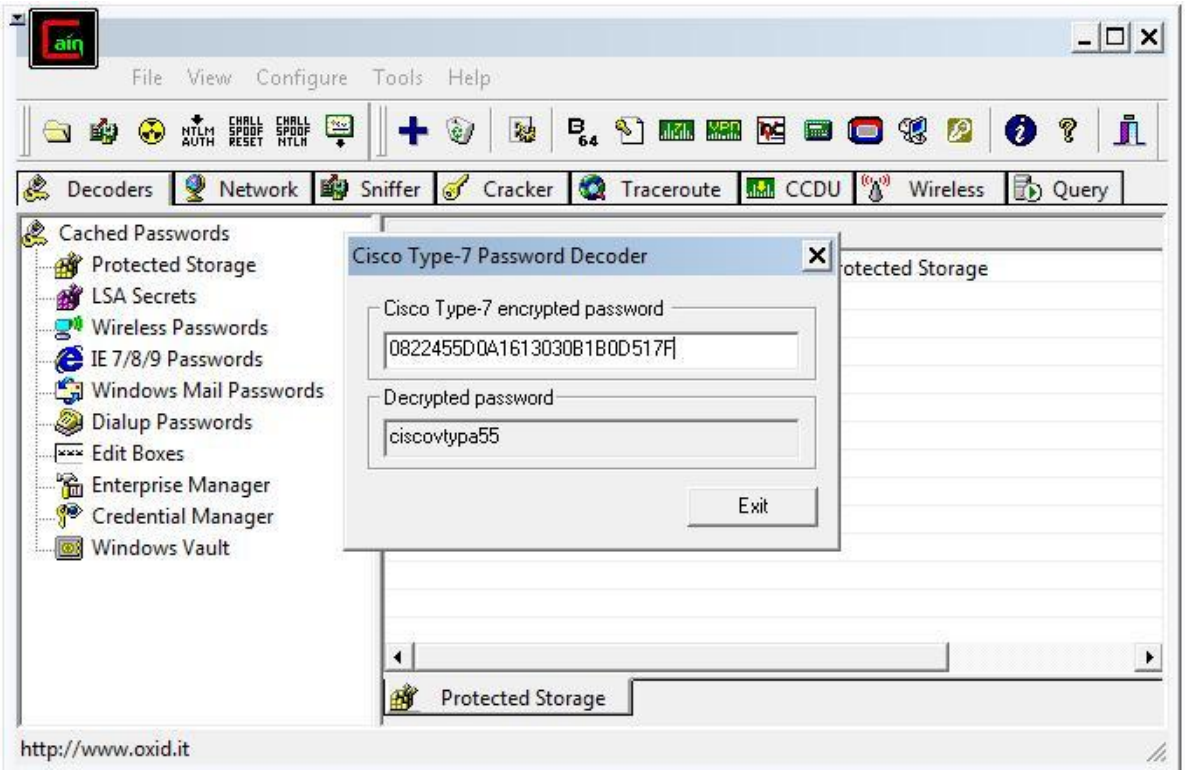


Figura 5-8 - Caso 1, Ataque de Força Bruta - Fonte: Cain & Abel

**Caso 2:** Tentativa de quebra da chave de hashing encriptada em MD5 do roteador, utilizando o ataque de Força Bruta do software *Cain & Abel, v4.9.56*.

**Resultado:** O atacante levará em media 1.16 x $10^{14}$ anos para ter sucesso (tempo em função aos recursos computacionais, neste caso o software foi rodado no notebook *Dell Inspiron 1525*), conforme mostrado no campo *Time Left* da Figura 5-9,

sendo esse tempo compatível com a ordem de grandeza prevista para quebra do MD5.

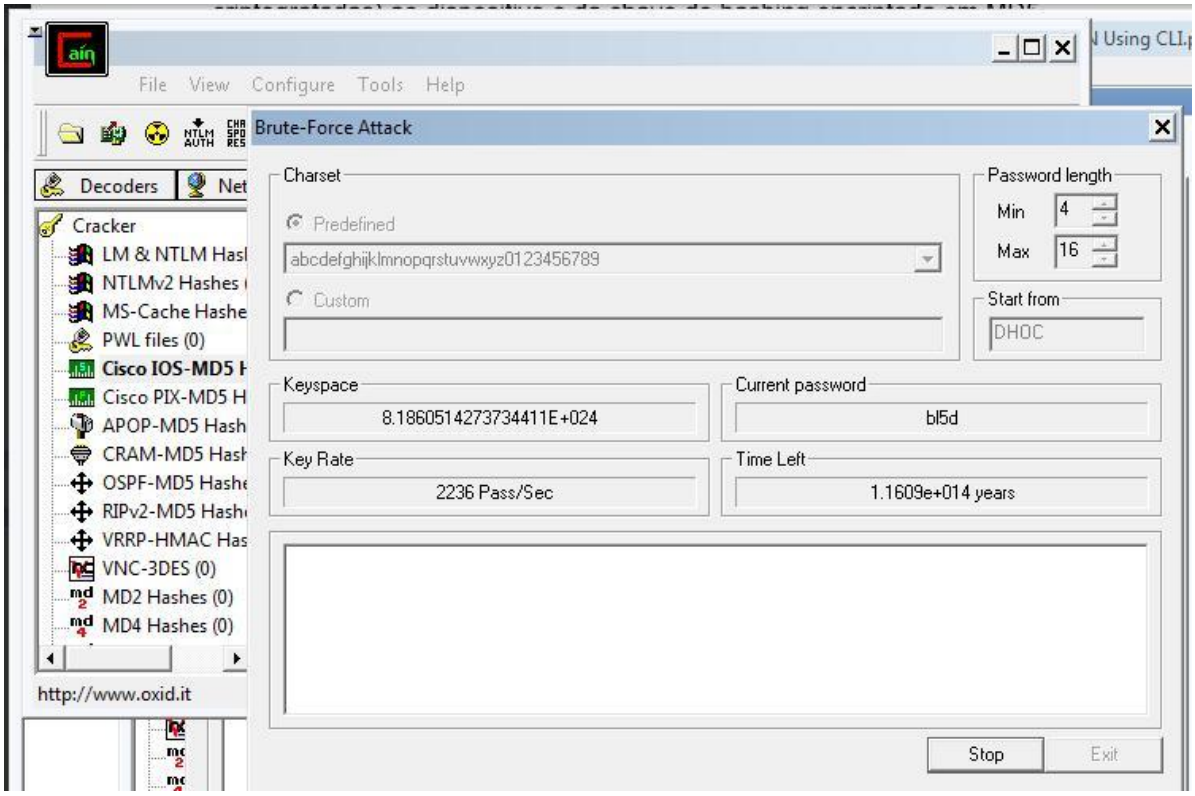


Figura 5-9 - Caso 2, Ataque de Força Bruta - Fonte: Cain & Abel

**Mitigação de Riscos**

Obviamente, a primeira contramedida para mitigar a ameaça de acesso ao dispositivo é a Segurança Física do acesso ao local, além de desabilitar a opção de acesso via *Telnet*.

E em relação à quebra da senha do Caso 1, conclui-se que a versão 12.4 do sistema operacional do roteador é vulnerável aos ataques de Força Bruta, sendo recomendado como contramedida o upgrade uma versão que não apresente a mesma vulnerabilidade.

# 6. CONCLUSÕES E TRABALHOS FUTUROS

Considerando o objetivo geral e específicos propostos no início desta dissertação, entende-se que os objetivos foram alcançados, porem sugere-se que outras pesquisas complementares sejam desenvolvidas no futuro.

## 6.1. Conclusões

Uma metodologia de implementação da VPN com a parametrização do framework do protocolo de rede IPsec, visando a segurança no fluxo de dados nas interfaces de comunicação entre domínios, e entre entidades inter e intra domínios do SGIRM, se entende que foi validada pelas simulações e testes em laboratório nas condições da infraestrutura disponíveis.

O objetivo específico da parametrização do framework do protocolo de rede IPsec entre os domínios Distribuidor e Consumidor, também se entende que foi validado pelas simulações e testes em equipamentos reais com as análises dos processos, latência, taxa de transferência e datagramas dos dados, com a implementação da VPN IPsec Site-a-Site, para a topologia de rede da Figura 4-1, detalhados na seções 4.1, 5.1 e 5.2 e respaldada nas análises dos resultados apresentadas nas seção 4.2 e 5.3.

Pode-se concluir que o método adotado para a parametrização do framework do protocolo de rede IPsec, visando a segurança no fluxo de dados nas demais interfaces da *Smart Grid*, pode ser aplicado se o protocolo for recomendado.

Em relação à aplicabilidade dos diferentes níveis de requerimento dos objetivos de segurança Integridade, Confidencialidade e Disponibilidade, recomendados pelo SGIRM, ficou comprovada a compatibilidade de dois dos três objetivos: a Integridade e a Confidencialidade com a parametrização dos serviços do protocolo IPsec, como observada nas simulações, testes e análises de resultados.

Como o objetivo Disponibilidade visa reduzir os efeitos, ou se recuperar de ataques de negação de serviço DoS, ele pode ser garantido por mecanismos ou dispositivos de proteção da rede como IPSs, Firewalls, sistemas de *fail-over* e sistemas de backup. Funcionalmente, o serviço de segurança Disponibilidade fica além do escopo do framework do IPsec, e pode ser relacionado com um eventual fora de serviço do túnel VPN que resulte de ataques, mas esta contingência não

envolve o protocolo IPsec em si e sim os dispositivos e sistemas de proteção da rede.

Finalmente, pode-se concluir que o método de implementação de VPN IPsec e parametrização do framework do IPsec, adotado e apresentado neste trabalho, pode ser aplicado nas demais interfaces de comunicação entre domínios, e entre entidades inter e intra domínios do SGIRM.

Esta dissertação foi submetida e aceita em formato de artigo (*paper*), em dois eventos internacionais patrocinados pelo IEEE: o Intercon 2015 em Lima, Peru (http://intercon2015.org/) e o ISGT-LA 2015 em Montevidéu, Uruguai (http://isgtla.org/).

## 6.2. Trabalhos futuros

Os trabalhos futuros previstos para complementar ou estender o escopo desta pesquisa seriam:

- Verificar a compatibilidade das TIC da rede elétrica para implementação do uso do protocolo IPsec.
- Validar a implementação do protocolo IPsec em instalações reais entre os domínios Distribuidor e Consumidor locais.

Para viabilizar estes trabalhos futuros, deverá se contar com as tecnologias requeridas, além de ter o acesso a esses recursos para realizar as parametrizações do IPsec para testar sua compatibilidade, funcionalidade e analisar seus resultados.

Entre os outros trabalhos futuros sugerem-se:

- Testar a funcionalidade da aplicação do protocolo IPsec integrada nos seis domínios mais importantes do modelo SGIRM: Geração, Transmissão, Controle/Operações, Provedor de Serviços, Distribuição e Consumidor.
- Testar o desempenho do túnel VPN IPsec em links de 1 Gbps com os mais novos algoritmos de criptografia e de hashing (últimas versões do AES e do SHS), com equipamentos cujos sistemas operacionais os suportem (TANVER, A. *et al*, 2015).
- Desenvolver uma abordagem para dar um tratamento matemático às variáveis linguísticas dos objetivos de segurança com as aplicações da Teoria de Conjuntos Nebulosos ou Fuzzy (ZADEH, L., 1973). Isto visaria obter uma

interpretação menos imprecisa do que se esperaria de um espaço de amostra de expectativas sobre os serviços de segurança do SGIRM.

## REFERÊNCIAS

CIP Standards - Reliability Standards section of NERC's Reliability Standards for the Bulk Electric Systems in North America**. Standards, Critical Infrastructure Protection (CIP)**, p. 135-848. June 2015. Disponível em: http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

DIFFIE, W.; HELLMAN, M. New directions in cryptography. **Information Theory, IEEE Transactions on,** v. 22, n. 6, p. 644–654, 1976. ISSN 0018-9448.

ERICSSON, G.N. Cyber Security and Power System Communication - Essential Parts of a Smart Grid Infrastructure. **Power Delivery, IEEE Transactions on,** v. 25, n. 3, p. 1501–1507, July 2010. ISSN: 0885-8977.

ERICSSON, G.N. Information security for Electric Power Utilities (EPUs): CIGRÉ Developments on Frameworks, Risk Assessment, and Technology. **Power Delivery, IEEE Transactions on**, vol. 24, n. 3, p. 1174 - 1181, July 2009. ISSN: 0885-8977.

FALCÃO, D. M. Integração de Tecnologias para Viabilização da Smart Grid. **Anais do III Simpósio Brasileiro de Sistemas Elétricos (SBSE)**, 18-21 Maio. 2010. Belém, PA.

GAMAGE, T.T.; ROTH, T.P.; MCMILLIN, B.M.; CROW, M.L. Mitigating Event Confidentiality Violations in Smart Grids: An Information Flow Security-Based Approach. **Smart Grid, IEEE Transactions on**, v. 4, n. 3, p. 1227 - 1234. Sept. 2013. ISSN: 1949-3053.

GUNGOR, V. C.; LAMBERT, F. C. A survey on communication networks for electric system automation," **Computer Networks:** The International Journal of Computer and Telecommunications Networking, v. 50, n. 7, p. 877–897. May 2006. Disponível em: Https://smartech.gatech.edu/bitstream/handle/1853/27879/electric_system_automation.pdf

HAHN, A.; GOVINDARASU, M. Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and test bed evaluation. **Smart Grid, IEEE Transactions on**, vol. 2, n. 4, p. 835 – 843. Dec. 2011. ISSN: 1949-3053.

HORALEK, J.; SOBESLAV, V. Data networking aspects of power substation automation. **COMATIA'10 Proceedings of the 2010 international conference on Communication and management in technological innovation and academic globalization**, Tenerife, Spain, 2010, pp. 147–153.

HUBERT, Z. OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. **Communications, IEEE Transactions on**, v. 28 n. 4, p. 425–432. January 2003. ISSN: 0090-6778.

IEC 62351-1 TS - Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues. **Technical Especification**, First Edition, p. 6-34. May 2007.

IEEE STD 2030. Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads. **IEEE Standard,** p. 1-126, Sept 2011. E-ISBN: 978-0-7381-6727-5.

IEEE Std 802.11i. IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. **IEEE Standard,** p. 1-175, July 2004. E-ISBN: 0-7381-4074-0.

IEEE Std 802.16e. IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1. **IEEE Standard,** p. 1-822, March 2006. E-ISBN: 0-7381-4857-1.

IETF-RFC 6071. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. Internet Engineering Task Force (IETF). **Request for Comments**, p. 1-63, February 2011. Disponível em: http://tools.ietf.org/html/rfc6071**.** ISSN: 2070-1721.

IOS Security Command. IOS Security Command Reference**. Commands A to C**. Cisco Systems, Inc. 2014. Disponível em: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book.pdf

ISO/IEC 10116:2006. Information technology - Security techniques -- Modes of operation for an n-bit block cipher. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-44, April 2013 (Stage). ICS: 35.040.

ISO/IEC 27000:2014. Information technology - Security techniques - Information security management systems – Overview and vocabulary. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-31, April 2014 (Stage). ICS: 01.040.35; 35.040.

ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-23, Sept 2013 (Stage). ICS: 35.040.

ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-80, Sept 2013 (Stage). ICS: 35.040.

ISO/IEC 27003:2010. Information technology - Security techniques - Information security management system implementation guidance. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-68, Jan 2013 (Stage). ICS: 35.040.

ISO/IEC 27004:2009. Information technology - Security techniques - Information security management – Measurement. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-55, June 2013 (Stage). ICS: 35.040.

ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management. **Standards, ISO/IEC JTC 1/SC 27**, p. 1-68, June 2013 (Stage). ICS: 35.040.

ISO/IEC 27006:2011. Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems. **Standards, ISO/IEC JTC 1/SC 27**, p. 1-37, June 2012 (Stage). ICS: 35.040.

ISO/IEC 27007:2011 Information technology - Security techniques - Guidelines for information security management systems auditing. **Standards, ISO/IEC JTC 1/SC 27**, p. 1-27, Aug 2014 (Stage). ICS: 35.040.

ISO/IEC 27008:2011 Information technology - Security techniques - Guidelines for auditors on information security controls. **Standards, ISO/IEC JTC 1/SC 27**, p. 1-36, Aug 2014 (Stage). ICS: 35.040.

ISO/IEC 27010:2012 Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications. **Standards, ISO/IEC JTC 1/SC 27**, p. 1-34, Jan 2015 (Stage). ICS: 35.040.

ISO/IEC 27011:2008. Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-44, June 2013 (Stage). ICS: 35.040.

ISO/IEC 27033-1:2009. Information technology - Security techniques - Network security - Part 1: Overview and concepts. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-73, Jan 2013 (Stage). ICS: 35.040.

ISO/IEC 7498-1:1994. Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model. **Standards, ISO/IEC JTC 1,** p. 1-59, June 2000 (Stage). ICS: 35.100.01.

ISO/IEC TR 27019:2013. Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. **Standards, ISO/IEC JTC 1/SC 27,** p. 1-37, Nov 2014 (Stage). ICS: 35.040.

SEIBEL, J., PLAKOSH, D., SIMANTA, S., MORRIS, E. Experimentation in the Use of Service Orientation in Resource-Constrained Environments. **Software Engineering Institute**, Carnegie Mellon University. May 2011. Pittsburgh. Disponivel em: http://resources.sei.cmu.edu/asset_files/Presentation/2011_017_001_24129.pdf

KHURANA, H.; KOLEVA, R.; BASNEY, J. Performance of Cryptographic Protocols for High-Performance, High-Bandwidth and High-Latency Grid Systems. e-Science and Grid Computing. **IEEE International Conference on**, p. 431-439. Dec. 2007. Print ISBN: 978-0-7695-3064-2.

LIU, R.; SRIVASTAVA, A. Integrated simulation to analyze the impact of cyber-attacks on the power grid. Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES). **IEEE 2015 Workshop on**, p. 1-6. April 2015. Print ISBN: 978-1-4799-7357-6.

MAIA, F. Redes Elétricas Inteligentes no Brasil – **Subsídios para um Plano Nacional,** p. 1-296. 2013, Editora: SYNERGIA EDITORA. ISBN: 9788561325947.

METKE, A. R.; EKL, R. L. Security technology for smart grid networks. **Smart Grid, IEEE Transactions on,** v. 1, n. 1. p. 99-107. June 2010. ISSN: 1949-3053.

NAEDELE, M; DZUNG, D; STANIMIROV, M. Network security for substation automation systems, in SAFECOMP ’01 **Proceedings of the 20th International Conference on Computer Safety, Reliability and Security**, p. 25–34. 2001. ISBN:3-540-42607-8.

NIST, 2009. Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI. **National Institute of Standards and Technology**, USA. Aug 2009. No. SB1341-09-CN-0031. Disponível em: http://www.nist.gov/smartgrid/upload/Report_to_NIST_August10_2.pdf

NIST, 2010. Framework and Roadmap for Smart Grid Interoperability Standards. **National Institute of Standards and Technology**, USA. Release 1.0. 2010. Disponível em: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

NIST, 2012. Recommendation for Key Management. **National Institute of Standards and Technology**, USA. Special Publication 800-57 Part 1 Rev. 3. Disponível em: http://csrc.nist.gov/groups/ST/toolkit/key_management.html

NIST, 2015. Transitioning the Use of Cryptographic Algorithms and Key Lengths. **National Institute of Standards and Technology**, USA. Special Publication 800-131A, Revision 1. DRAFT. Disponível em: http://csrc.nist.gov/publications/drafts/800-131A/sp800-131a_r1_draft.pdf

NISTIR 7628, vol. 1 - Guidelines for Smart Grid Cybersecurity: Volume 1: Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. **National Institute of Standards and Technology**, USA. Revision 1. 2014. Disponível em: http://csrc.nist.gov/publications/nistbul/itlbul2014_09.pdf

RAMOS, M. Proposta de um método de segurança da informação para sistemas de automação em redes elétricas inteligentes. **Dissertação (Mestrado),** LACTEC - Curitiba, 2012.

TANVER, A.; ALI, A.; PARACHA, M.A.; RAJA, F.R. Performance analysis of AES-finalists along with SHS in IPSEC VPN over 1Gbps link. Applied Sciences and Technology (IBCAST), **2015 12th International Bhurban Conference on**, p. 323-332. Jan 2015. INSPEC: 14984053.

WANG, D.; GUAN, X.; LIU, T ; GU, Y. A survey on bad data injection attack in smart grid. In: Power and Energy Engineering Conference (APPEEC), **2013 IEEE PES Asia-Pacific on,** p. 1-6. Dec. 2013. INSPEC: 14384094.

WEERATHUNGA, P.E.; SAMARABANDU, J.; SIDHU, T. Implementation of IPSec in substation gateways. IEEE 6th Information and Automation for Sustainability (ICIAfS), **International Conference on,** p. 327 – 331. Sept 2012. ISBN: 978-1-4673-1976-8.

WENYE, W.; ZHUO, L. Cyber security in the Smart Grid: Survey and challenges. **Computer Networks.** v. 57, n. 5. p. 1344–1371. April 2013. Disponível em: http://www.sciencedirect.com/science/article/pii/S1389128613000042

YAN, Y; QIAN, Y; SHARIF, H.; TIPPER, D. A Survey on Cyber Security for Smart Grid Communications. **IEEE Communications Surveys & Tutorials**, v. 14, n. 4. p. 998 – 1010. Oct 2012. ISSN :1553-877X.

ZADEH, L. A. Outline of a new approach to the analysis of complex systems and decision processes. Systems, Man and Cybernetics, **IEEE Transactions on,** v. SMC-3, n. 1, p. 28 – 44. Jan. 1973. ISSN : 0018-9472.

ZHANG, J.; GUNTER, C.A. Application-aware secure multicast for power grid communications. 2010 First IEEE International Conference. **Smart Grid Communications on**, p. 339 – 344, Oct 2010. Print ISBN: 978-1-4244-6510-1.