Parameterization of IPsec Framework for Security in the Smart Grid Interoperability

Latency and Throughput IPsec Overhead

Victor Neumann
UFPR – Curitiba, Brazil
Programa de Pós Graduação em Engenharia Elétrica
vneumann@ufpr.br

Christian Lyra Gomes
UFPR – Curitiba, Brazil
Ponto de Presença da RNP no Estado do Paraná
lyra@pop-pr.rnp.br

Clodomiro Unsihuay-Vila
UFPR – Curitiba, Brazil
Programa de Pós Graduação em Engenharia Elétrica
clodomiro@eletrica.ufpr.br

Keiko V. Fonseca
UTFPR - Curitiba, Brazil
Programa de Pós Graduação em Engenharia Elétrica
keiko@utfpr.edu.br

Pedro Rodrigues Torres Jr.
UFPR – Curitiba, Brazil
Ponto de Presença da RNP no Estado do Paraná
pedro@pop-pr.rnp.br

***Abstract*— The infrastructure of the Smart Grid communication will require the use of security protocols based on standards of the state-of-the-art. This work proposes a method of parameterization of the IPsec protocol framework, aimed at security of data interoperability in Smart Grid, according to the requirement levels for the security services: Integrity, Confidentiality and Availability, recommended by the SGIRM (Smart Grid Interoperability Reference Model [1]). The methodology can be used for 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. The methodology proposed for the VPN Ipsec implementation was applied as step-by-step tasks and implemented in a test bed network. Each test was repeated twenty times aimed at data analysis and statistical evaluation of the results. The field tests allowed us to measure jitter (latency variation) and data flow throughput resulting from the parameterization of IPsec to compare the results with the limits set out in SGIRM, aiming to validate the methodology.**

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

I. INTRODUCTION

Research on Cyber Security for Smart Grid recommends the adoption of comprehensive solutions and global communication architecture with a focus on security since the start of implementation, including traditional schemes such as PKI (Public Key Infrastructure) authentication mechanisms based on standards industry, and the use of security protocols based on standards of the state of the art [2]. The same survey mentions that wired networks are secure with firewalls, Virtual Private Networks (VPNs) and IPsec [3] technologies.

The power system community strives to seize the sets of existing protocols to perform secure communications, such as IPsec [4] and Transport Layer Security (TLS) [5]. The Internet-based protocols such as IPv4 and IPv6, which have been developed over many years and has its widespread use, will provide a low cost communication baseline.

Security of Smart Grid strongly depends on the Authentication, Authorization and Privacy technologies. The Federal Information Processing Standard (FIPS) approved encryption solutions Advanced Encryption Standard (AES) and Triple Data Encryption (3DES). As a specific example, NIST determined that 3DES solution will likely become unsafe by the year 2030. Considering that public service components should have a long life, AES would be the recommended solution for new components [6].

The Cyber Security in Smart Grid will be vital to the reliability of the power system operations. Applications of communications power systems are different applications of enterprise systems, and have to deal with many network security technologies [7]. Reference [7] presents an application of the IPsec tunnel between the gateway of a substation and the gateway of the power system control center, using the Encapsulating Security Payload (ESP) protocol as authenticator and DES, 3DES, AES, and others such as encryption algorithms for encrypting the data stream.

II. BACKGROUND & STATE OF THE ART

There has been much research on Internet security and information security for enterprise systems, but little in the security area networks for communication systems of power systems. Reference [8] discusses the cyber security role in an intelligent network architecture. Article [9] provides cyber security applications in networks of power systems, and proposed a functional framework for information security of utilities.

The research presented in [10] investigates the threats of attacks based on substation networks and proposed a secure

978-1-4673-6605-2/15/$31.00 ©2015 IEEE

communication protocol to combat these attacks, and the reference [11] proposes the Virtual Private Networks (VPNs) with IPsec to isolate the network of remote control rooms of the network of substations. Reference [6] highlights what is learned in years of deployment and operation of large networks communication systems is that the effort required to provide symmetric keys to thousands of devices can be very costly or unsafe. So the development of keys and trust management systems will be necessary for large network deployments; these systems can be availed from other industries based on PKI technology, and can be customized specifically for the Smart Grid operators, relieving the burden of providing the security that adheres to the standards and guidelines that are set by safety requirements in references [14] and [15].

As the strength of the security of an IPsec tunnel strictly depends on your encryption algorithms and their key management, it is important to evaluate encryption algorithms to IPsec tunnels in gateways substations [7]. The research underlying the preparation of this article follows the recommendations described in the preceding paragraphs, to apply the concepts and technologies of the state of the art of Network Security industry leaders, adopting scalable PKI solutions, including the selection of authentication algorithms devices, encryption algorithms and encryption keys and data, for the configuration process of Virtual Private Networks (VPNs) and parameterization of IPsec framework, adapting this process to the security requirements for the Smart Grid recommended in the SGIRM.

III. METHOLOGY

To develop a methodology for the parameterization of IPsec framework in order to cyber security interoperability in Smart Grid, is adopted the reference of the CT-IAP model architecture (Interoperability Architectural Perspective of Telecommunication Technologies) detailed in reference [1] and applied SGIRM recommendations on the application levels in security services for Integrity, Confidentiality and Availability in data flows.

III-1. The SGIRM and the Security Services

Each type of information or data flows in a communication system, or the system itself, a security category consisting of level of impact to an interface or to a particular system should be assigned. Specifically, the level of impact in each of the three security objectives: Confidentiality, Integrity, and Availability of data. A low level of impact L (Low), moderate M (Moderate), or high H (High) represent the impact on operations, assets, or individuals if there is a breach in the systems [14].

The SGIRM assigns security categories for the communication interfaces between domains, and between entities within and between domains, of the CT-IAP and established the application levels for Integrity, Confidentiality and Availability of data flows such as security objectives. As shown in Table III-1, for example, the interface CT-12 between the *Smart Meter Energy Services* entity of the *Customers* domain and the entity *Neighborhood Area Network* of the *Distribution* domain should have a high (H) *Confidentiality*, high (H) *Integrity* and High (H) *Availability.*

III-2. The IPsec compatibility with the Security Services

This paper aims to demonstrate that the IPsec framework is compatible with the requirements of the security services presented in the previous section. Among the four security services, three of them: the Confidentiality, Integrity, and Accounting (embedded in processes of identification and authentication Confidentiality service), make up the framework of the IPsec security protocol.

Thus, with the adoption of IPsec to secure data flows at the interfaces between domains and between entities, Confidentiality, Integrity and Accounting requirements will be met, as will be show in this work. Leaving only the requirement of availability to be met with the appropriate services and technologies for this purpose, such as IPS, Firewalls, Backup and Fail-over systems.

The parameters of the IPsec framework is the appropriate choice of each of the five blocks, according to the IPsec protocol type to be adopted, the complexity of encryption algorithms, the key and its exchange method, and its length (eg AH, DES, 3DES, AES, MD5, SHA, PSK, DH1, etc.) to the flow of data necessary to meet the needs of the level of security services.

IPsec is an IETF standard that defines how a VPN can be configured using the IP addressing protocol. IPsec is not tied to any specific encryption, authentication, security algorithms, or key technology. IPsec is a framework of open standards setting out the rules for secure communications. It is based on existing algorithms to implement encryption, authentication and key exchange [3]. The IPsec framework consists of five blocks:

- The first is the IPsec protocol. Options include the ESP and AH.
- The second is the type of Confidentiality implemented using an encryption algorithm such as DES, 3DES, AES (128, 192, 256) or SEAL. The choice depends on the level of security required.
- The third is the integrity that can be implemented using the MD5 or SHA hashes.
- The fourth is how the shared secret key is established. The two methods are pre-shared (PSK) or digitally signed using RSA.
- The fifth is the group DH algorithms. Four DH algorithms separate key exchange to choose from including DH Group 1 (DH1), DH Group 2 (DH2), DH Group 5 (DH5) and DH Group 7 (DH7).

The selected type of group depends on the specific needs. The linguistic variables high (H), moderate (M) and low (L) of the security objectives of SGIRM tables, and in particular in Table III-1, should have an appropriate range mapped to each of the blocks in formatting the IPsec framework.

III-3. Security Services x IPsec Blocks

On the basis of a qualitative analysis of the security level, according to the complexity of encryption algorithms, keys and their exchange method, its length and lifetime, Table III-2 presents our proposal of corresponding IPsec framework blocks assigned to meet the level requirement of the security services for interfaces or data flows.

Smart Grid Communication Interface	**Security Services Requirements**		
	Confidentiality	Integrity	Availability
CT-12	H	H	H
CT-13	L	H	M
CT-29	M	M	M
CT-52	M	M	L

Table III-1 - Security Level for Interface - Source: [1]

Although this table is a proposal of this work, may also be chosen some other IPsec blocks according to security policies

and or cost/benefit to be adopted by each company in the energy sector. The parameterization of IPsec blocks are implemented using CLI (Command Line Interface) programming in the network gateway of each domain (routers as security gateways).

IPsec Framework		Security Services					
		Confidentiality			Integrity		
Blocks	**Choice**	L	M	H	L	M	H
IPsec Protocol	AH, ESP, ESP+AH	AH	ESP	ESP+AH	AH	AH	AH
Confidentiality	DES, 3DES, AES, SEAL	DES	3DES, AES	3DES, AES, SEAL	-	-	-
Integrity	MD5, SHA	-	-	-	MD5	MD5	SHA
Autentication	PKS-RSA	PKS	PKS, RSA	PKS, RSA	PKS	PKS, RSA	PKS, RSA
Diffie-Helman	DH1, DH2, DH5, DH7	DH1	DH1 DH2	DH2 DH7	DH1	DH1 DH2	DH2 DH7

Table III-2 - Proposal IPsec blocks - Source: The Author, 2015

One basic network topology compatible with the CT-IAP [1] was designed, and used the CLI to configure the features of network devices that adopt state of art VPN and IPsec capabilities, which are closely related to the security services. These devices are routers (or firewalls) that in a basic topology serve as gateways for each one of the domains of the CT-IAP (SGIRM). Obviously, the telecommunication network is much more extensive and complex, but for the purposes of this work, we use a basic topology to provide a proof of concepts. Thus, based on CT-IAP, is drawn a topology of the telecommunications network architecture that interconnects through the main interfaces, the seven domains of SGIRM, shown in Figure III-1.

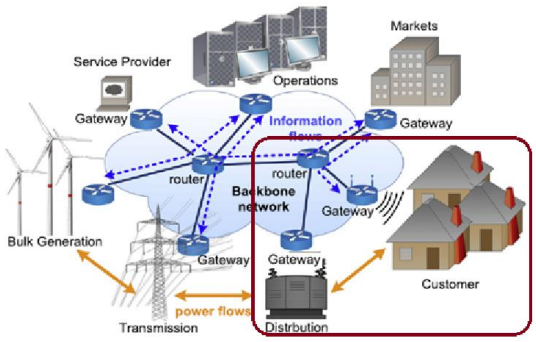

Figure III-1 - Basic Topology Network CT-IAP, Source [17]

IV. VPN IPSEC IMPLEMENTATION AND TEST

IV.1 VPN IPsec Implementation Model

The adopted VPN IPsec deployment model provides its most important benefits that are Security, Economy and Scalability. These benefits can be obtained with appropriate parameterization of key distribution methods (ISAKMP protocol), key exchange, authentication of peers, and hash algorithms and encryption (these parameters are part of the ISAKMP policy). This model can be applied between two any domains of the CT-IAP and the interfaces between such domains and the internet, which represent the pair of VPN sites where the tunnel is established, through the public Internet, and be parameterized IPsec framework.

IV.2 VPN IPsec Laboratory Tests

There were applied tasks step-by-step of the methodology proposed for the implementation of VPN in the Laboratory Tests, to measure with the tools Iperf and NetPipe the jitter and data flow throughput resulting from the parameterization of IPsec to compare the results with the limits set out in SGIRM, aiming to validate the methodology proposed. Each test was repeated twenty times aimed at data analysis and statistical evaluation of the results.

A. Topologies and Test System Settings

The tests were carried out at the Laboratory of the National Network of Education and Research (RNP), UFPR Polytechnic Center, with a network topology that replicates part of the CT-IAP Basic Topology, as shown in Figure IV-1. Two domains (Consumer and Distributor) were selected and one interface that connects them. It is to test a tunnel VPN IPsec Site-to-Site to be established between these domains.

To view graphically as the Test topology would be applied to the Smart Grid devices such as smart meter (*Smart Meter Energy Services* entity) that would be installed in the *Consumer* domain infrastructure and the network components of the entity *Neighborhood Area Network* of the *Distributor* domain providing connectivity services to smart meters to obtain measurements of different electrical parameters and consumption, in Figure IV-1 overlap up Test Topology and the CT-IAP in the CT-12 interface.

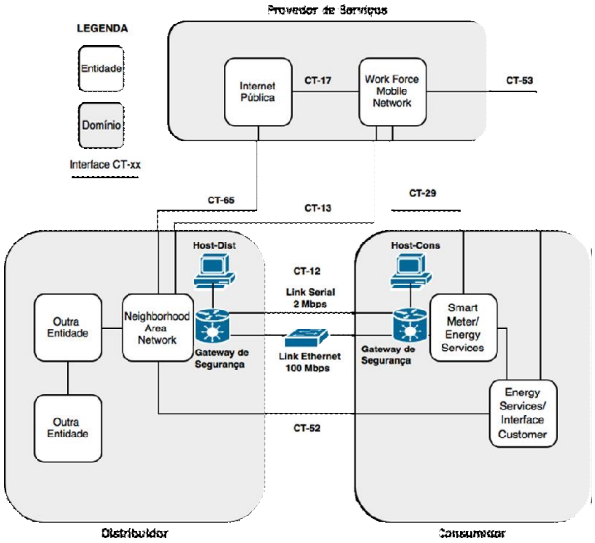

Figure IV-1 - Test Topology and CT-12 in the CT-IAP

To protect the data flow in the CT-12 interface with the IPsec, it is expected to impact the latency and bandwidth available due to the overhead generated by the protocol. To appreciate this, it was implemented with real routers test environment (represented by security gateways) and computers which were held a number of bandwidth and latency tests using different IPsec configuration parameters. All data and results of these tests are available at the following link RNP: http://www.pop-pr.rnp.br/noticias/pop-colaboracao-ppgee2/. It is noteworthy that the routers (spec details in link above) used in the tests are devices with median performance and there are others with better or worse performances, those would provide results with better or worse latency and throughput.

B. Laboratory Tests Objetives

- Set the Distributor security gateway router to support a VPN IPsec Site-to-Site with the Consumer domain router.

- Set the Consumer security gateway router to support a VPN IPsec Site-to-Site with the Distributor domain router.
- Implement several performance tests in the VPN IPsec Site-to-Site, aimed at measuring the latencies of access and reception, and data throughput due to the additional overhead introduced by the IPsec security gateways, with two scenarios network connectivity: 2 Mbps serial and 100 Mbps Ethernet links.
- Identify the most appropriate tools and more reliable tests for the desired measurements in the previous item.
- Compare the measurements with performance metrics established by SGIRM, aiming to validate the application of the methodology proposed.

C. Setting and Background

As substations (like domain entities as Distributor, Consumer, etc.) use 100 Mbps Ethernet networks and most current devices support 100 Mbps of network traffic, even if it could use gigabit links (1000 Mbps) to its external communications, in practice the communication may be limited to 2 Mbps (serial interface) or 100 Mbps (Ethernet interface). Thus, the topology used for testing, comprising two security gateways interconnected by means of a switch and its Ethernet interfaces support a maximum theoretical yield of 100 Mbps network traffic and they are also connected by serial interfaces of 2 Mbps, as shown in Figure IV-1.

D. Setting and Background

The SGIRM [1] establishes the following latency levels for the interoperability of Smart Grid services:

Protection: < 3 ms (milliseconds)
Monitoring: > 160 ms
Control: < 3 ms
Telephony: > 160 ms

And for the data flow, in certain interfaces of the CT-IAP, the permitted levels of latencies vary widely depending on the applications, but the ranges in some interfaces are:

CT-12: <1 ms to 1500 ms - 1 ms to 15 s
CT-14: <1 ms to 1500 ms
CT-15: <1500 ms
CT-52: <1 ms to 1500 ms - 4 ms to 15 s
CT-53: <10 ms to 5000 ms - 10ms to 15min·

For the payload, the range is between 10 and 1500 bytes, and the bit rate (throughput) is from 1 Kbps to 75 Mbps, in these interfaces.

E. Test Implementation

As required in the implementation of the VPN IPsec Site-to-Site, are created two sets of security associations (SAs), one for IKE SA (Phase 1 - IKE SA) and other for the IPsec SA (Phase 2 - IPsec SA), which are both implemented in security gateways. Phase 1 interchanges the attributes of the encryption and hashing algorithms to secure the exchange of the IPsec parameters Phase 2.

Thus, to perform the tests parameterization of encryption algorithms and authentication blocks, the parameter changes are made in Phase 2 for different IPsec SA settings. It is configured eleven VPN-SET representing the eleven SAs of Confidentiality and Integrity levels of IPsec framework, that are supported by the model of the routers used as security gateways. These sets of IPsec SAs are named VPN-SET0 to VPN-SET10, and the VPN-SET0 corresponding to the set SA with Plain-Text. Scripts implementations of these SAs are in the Scripts folder on link RNP: http://www.pop-pr.rnp.br/noticias/pop-colaboracao-ppgee2/.

Initially, were performed the throughput tests (TCP) by exchanging a 300 MB file (for the tests with the Ethernet link 100 Mbps) and 30 MB (for the tests with the serial link of 2 Mbps), using the Iperf tool, from the Host-Dist (connected to the security gateway Distributor) to Host-Cons (connected to Consumer security gateway) using the TCP / IP protocol for measuring throughput and latency of the data traffic with and without IPsec security, aimed at measuring the variation caused by the different IPsec framework options of Confidentiality and Integrity blocks (including Authentication).

It was then transferred the same amounts of data using the tool NetPipe, but in different payload sizes to determine the effect of the packets size in the communication (500 messages ranging from 1 to 1536 bytes). This type of test was also repeated twenty (20) times for each payload size. Were also performed various bandwidth tests using Iperf tool. The bandwidth test (UDP) was with 64/1500-byte packets, for 30 seconds. These tests were also repeated twenty (20) times for each payload size.

V. Results

The results of the tests are presented in metrics of average, minimum and maximum of RTT (Round Trip Times) in ms (milliseconds) for latency, and Mbps (Megabits per second) to test the bandwidth (throughput), accounted for twenty (20) repetitions of tests for each VPN-SET, seeking comparisons of performances and the disposal of non-systematic errors. Also, to identify significant distortions in the measurement are included the standard deviation (S) of the twenty (20) repetitions of tests by VPN-SET.

A. Latency

Table V-1 (for the tests with the Ethernet link 100 Mbps), present latencies values for Plain Text data stream (without the security of IPsec), and latency values when the different IPsec security levels of Confidentiality and integrity are applied (encryption, hashing functions and key sizes). The same tests were applied to two payload sizes (64 and 1500 bytes) due to the impact caused by the processing of data fragmentation in the performance. As reference values, are also entered Table V-1 the limits set by the latency SGIRM for the CT-12 interface. It is noted in Table V-1 for the test with 64 byte packets, the variation of the latency between the flow in plain text and the flow to the different encryptions (DES, 3DES, AES 128, AES 192 e AES 256) along with the hash function (MD5 and SHA) is more than 400%. In absolute terms the increased latency is about 1.3 ms.

Likewise, for the test with 1500 byte packets, the relative variation in latency between the flow in plain text and the flow to the different encryptions, along with the hash function, is more than 220%. In absolute terms the increase in latency is around 2.0 ms. It is also observed that the variation in average latency with the exchange of encryption between the low/high level of confidentiality (DES/AES256), is 0.037 ms when using the hash function MD5 (for 64 byte packets) and 0.064 ms (for 1500 byte packets).

The latency variations are in the same order of magnitude when using the SHA1 hashing function. This tiny variation may result from the ability of security gateways in the processing of different encryption algorithms. Thus, the appropriate choice of encryption and hashing function blocks would be the longevity of the algorithms and keys. Example: 256-bit AES would have a lifetime much more than the year

2030, however 3DES no more than 20 years [6]. The standard deviation (S) for both tests 64 and 1500 bytes remaining in the range from 0.9 to 2.4%, which indicates no significant distortion in the measurement results.

Packet Size	VPN SET	Encryption (Confidentiality Block)	Hashing function (Blocks Integrity + Authentication)								CT-12 Interface SGIRM
			Latency (ms)								
			Ave	Min	Max	S (%)	Ave	Min	Max	S (%)	
64 bytes	0	Plain Text	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	Plain Text	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

Table V-1 – Ethernet Link Latencies

In the case of the tests with the 2 Mbps serial link (data available in RNP link), with 64 byte packets the variation of the latency between the flow in plain text and the flow to the different encryptions (DES, 3DES, AES 128, AES 192 e AES 256) along with the hash function (MD5 and SHA), in absolute terms, the increased average latency is about 2.2 ms. And for 1,500 byte packets tests, the increased average is about 4.0 ms, however the average latency for 2 Mbps link is about 29 ms. This shows, as expected, that the use of links with low transfer rate such as 2 Mbps has a significant impact on latencies. Thus, the use of these links in the CT-IAP interfaces should be thoroughly evaluated when required certain restrictions on latency.

And, with the serial link, the variation in average latency to exchanges of encryption from weakest Confidentiality level (DES) to the strongest (AES 256), is 0.3 ms when using the hash function MD5 (for 64-byte packets) and 0.67 ms (for 1500 byte packets). The average latency variations are in the same order of magnitude when using the SHA1 hashing function.

In the case of tests with the 2 Mbps serial link, standard deviation (S) for both tests 64 and 1500 bytes, indicates significant distortions on the results of measurements (>> 2%). These distortions may result from overload in processing the data transfer rate over the processing of the encryption and hashing algorithms, when using the low-speed link as 2 Mbps, because a low-distortion (1.5 to 1.7%) is observed when the flow is in Plain Text.

Considerations about latency:

As the impact of IPsec security overhead in latency is a range of 1.8 a 3.6 ms for the tests with the Ethernet link, this level is close to the tolerance limit set by SGIRM for Protection and Control Communications (<3 ms). In contrast, for the tests with the serial link latency is in the range 4.0 to 29.2 ms, which extrapolates the latency tolerance for communications for Protection and Control (<3 ms).

However, for some communication interfaces of CT-IAP the impact is at the lower limit of the range of allowable latency (CT-12 < 1 to 1500 ms, and 1ms to 15s; C-T53 < 10 to 5000 ms, and 10ms to 15min). Anyway, it should always be taken into account, and shall be measured, the latency level of the link or interface propagating to be added latency caused by the IPsec security overhead.

Also, as identified in the tests with the serial link, there is a significant increase in latency when the payload size is 1500 bytes, which should be considered when some applications in Smart Grid require this size payload and low latencies in CT-IAP interfaces.

B. Throughput

Table V-2 shows throughput results, made with the Ethernet link, for Plain Text data stream (without the security of IPsec) and the results when are applied the different levels of IPsec security blocs for Confidentiality and Integrity (encryption, hashing functions and key lengths).

There is a significant impact of the IPsec security overhead reducing the average throughput of 94.15 Mbps to 29 Mbps close to around 30%. In this case, the use of computing resources to process the encryption and hashing algorithms significantly reduce the data transfer rate. As reference values, are also entered in Table V-2 throughput limits established by SGIRM for CT-12 interface.

The standard deviation (S) for the tests with an Ethernet link, present considerable distortion on the measurement results (>15% in most VPN-SET), as shown in Table V-2. These distortions may also result from overload in processing data transfer rate over the processing of encryption and hashing algorithms, but the 5.1% distortion observed when the flow is in Plain-Text is already an indication that the own processing throughput and / or TCP is an important factor in the performance of Ethernet link to the volume of the test file.

And the results of throughput testing with the TCP and 30 MB file (data available in RNP link), made with the serial

link, also for Plain-Text and different levels of Confidentiality and Integrity demonstrate a low average relative reduction of throughput due to overhead IPsec (about 6%). Also, the standard deviations (S) remained low, in the range from 0.31 to 0.67%, which indicates no significant distortion in the measurement results. These results indicate that the serial link has a uniform performance even with the change in VPN-SETs, and stable for twenty (20) repetitions of each test.

File Size	VPN SET	Encryption (Confidentiality Block)	Hashing function (Blocks Integrity + Authentication)								CT-12 Interface SGIRM
			Throughput (Mbps)								
			Ave	Min	Max	S (%)	Ave	Min	Max	S (%)	
300 MB (TCP)	**0**	**Plain Text**	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

Table V-2 - Ethernet Link Throughput

Considerations about Throughput

As the impact, in the tests with the Ethernet link, of IPsec security overhead in throughput reduces it to around 30 Mbps, and the operating range for some communication interfaces of CT-IAP according the SGIRM should be between 1 Kbps and 75 Mbps, and in particular between 30 Kbps and 1 Mbps for CT-12, should be taken into account this impact when it is needed substantial amounts of data transfer requiring Confidentiality, Integrity (also Authentication) and the use of Ethernet link of 100 Mbps. On the other hand, when it requires a low incidence of IPsec overhead on throughput and stability of the communication link performance, tests with serial link demonstrate that their use is most appropriate.

VI. Conclusions

The implementation process of VPN and IPsec Framework parameterization, along with the results of laboratory tests, demonstrate the applicability and feasibility of the proposed methodology. This methodology can be applied to any pair of domains or entities of the network architecture topology of CT-IAP according to security services levels required for Confidentiality and Integrity of data for each interface between domains and between entities.

Regarding the applicability of the different application levels of security objectives Integrity, Confidentiality and Availability, recommended by the SGIRM, was proven two of the three objectives compatibility: Integrity and Confidentiality with the parameterization of the IPsec protocol services, as demonstrated in test and analysis results.

Since the objective Availability aims to reduce the effects, or recover from DoS (denial of service attacks), it can be guaranteed by mechanisms or network protection devices such as IPSs, firewalls, fail-over and backup systems. Functionally, the service Availability lies beyond the scope of the IPsec security framework, and can be related to a potential VPN tunnel out of service resulting from attacks, but this contingency does not involve IPsec itself but devices and network protection systems.

References

[1] 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.

[2] 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.

[3] 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. ISSN: 2070-1721.

[4] 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.

[5] IEC Standard, IEC 61850, 2004. Communication Networks and Systems in Substations. 2004. https://webstore.iec.ch/p-preview/info_iec61850-9-2%7Bed1.0%7Den.pdf..

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] RFC 240 - 2412. Request for Comments, The OAKLEY Key Determination Protocol. Department of Computer Science, University of Arizona, November 1998.

[14] 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.

[15] ISO/IEC 27000 to 27011. Information technology - Security techniques Standards, ISO/IEC JTC 1/SC 27, April 2014 (Stage). ICS: 01.040.35

[16] WENYE, W.; ZHUO, L. Cyber security in the Smart Grid: Survey and challenges. Computer Networks. v. 57, n. 5. p. 1344–1371. April 2011.