Improving the Availability of Firewalls with a View to Increasing ICT Consumption Due Covid-19

Edson Luiz Ursini
Faculdade de Tecnologia
Universidade Estadual de Campinas
Limeira, Brazil
https://orcid.org/0000-0002-1597-4057

Henry de Castro Lobo dos Santos
Faculdade de Tecnologia
Universidade Estadual de Campinas
Limeira, Brazil
https://orcid.org/0000-0003-1400-3811

Marcelo Tsuguio Okano
Centro Paula Souza
Universidade Estadual de Campinas
Sao Paulo, Brazil
https://orcid.org/0000-0003-1680-7821

***Abstract*—Due to pandemic Covid-19, which suddenly forced people to change their habits and stay in their homes for several weeks, the daily routines changed, people could no longer go to work or study, physical contact should be avoided, care with personal hygiene improved and all types of crowding avoided. This causes "home office" work to skyrocket and reach significant peaks. In this way, the demand for services related to Information and Communication Technology, ICT, has grown greatly. To manage the problems caused by the lack of resources needed to transport traffic on the network, SLA (Service Level Agreement) contracts are common, which the parties involved sign (the provider and the customer). Failure to comply with these contracts may result in a fine for the party that has not fulfilled it. This work proposes an approach to improve the dimensioning of Firewalls, in terms of their availability, to establish values as close as possible to the real ones so that there is neither an underestimation nor an overestimation of commitments agreed between the actors. In addition, this work proposes a way to approach this problem in a broader way, taking into account the Dependability, that is, Availability, Reliability and Maintainability**.

Keywords— ICT, home-office, Covid-19, Firewalls, Availability, Reliability, Dependability.

I. Introduction

In unexpected epochs like the 2020 pandemic due to the Covid-19, which suddenly forced people to change their habits and stay in their homes for several weeks. Daily routines changed, people could no longer go to work or study, physical contact was to be avoided, personal hygiene was to be improved and all kinds of crowding avoided.

According to the OPAS [1], on December 31, 2019, the World Health Organization (WHO) was alerted about several cases of pneumonia in the city of Wuhan, Hubei province, in the People's Republic of China. On January 7, 2020, the Chinese authorities confirmed that they had identified a new type of coronavirus. In all, seven human coronaviruses (HCoVs) have already been identified: HCoV-229E, HCoV-OC43, HCoV-NL63, HCoV-HKU1, SARS-COV (which causes severe acute respiratory syndrome), MERS-COV (which causes respiratory syndrome in the Middle East) and the most recent new coronavirus (which in the beginning was temporarily named 2019-nCoV and on February 11, 2020 was named SARS-CoV-2). This new coronavirus is responsible for causing the disease COVID-19 [1]. On March 11, 2020, COVID-19 was characterized by the World Health Organization (WHO) as a pandemic.

In these times of limited mobility, ICTs are now playing a key role as they allow people to communicate and collaborate without having to leave home. This is all due to the possibility of computers being connected to a worldwide network, the Internet, which has given rise to various technologies, has broken physical boundaries and expanded business domains.

Teleworking, according to the SOBRATT [2], teleworking is all work done at a distance, that is, outside the workplace, with the use of ICTs, with computers, fixed and/or mobile telephony and any technology that allows working anywhere, receiving and transmitting information, files, images or sound related to the work activity. The technology was created to improve the quality of life of human beings, and with its evolution, the idea of remote work became a reality, called home office or more popularly said today, anywhere office.

Remote work in Brazil has been on the rise in recent years, according to the G1[3], a survey conducted by IBGE (Brazilian Institute of Geography and Statistics), shows that between 2012, when research on remote work in Brazil began, and 2018, this model of work grew by 44.4%.

Surveys show that remote work significantly increases employee productivity, and from the company's point of view, there is a reduction in organizational costs, such as lower consumption of energy, water, and often a reduction in the work positions of employees, and it is possible to reduce the size of physical offices, i.e., it is possible to reduce rents or the purchase of leaner locations [4, 5, 6].

Another technology widely used by organizations to connect employees to work remotely, the VPN (Virtual Private Network), in its "Client to Site" mode, creates an encrypted communication tunnel with the organization, which extends to the employee all the organizational resources, tools and applications needed to perform their activities anywhere, in addition to offering the same security of information for the employee's computer remotely [7].

The new scenario designed by the Covid-19 pandemic has required companies and organizations to adapt to this new reality and put most employees working from home by teleworking. This project has studied three large Brazilian companies, being that in other scenarios it can present different results. However, the approach can be adapted to new environments. The biggest barrier was how to enable this new ICT infrastructure in a short time for a large number of remote users. This problem brings a concern about the availability and reliability of the service, because organizations need to keep their entire production in remote work, as if their employees were working locally.

In this article, the objective is the analysis of system availability. For this, an availability model was developed analyzing the components of a Firewall solution, as one of the main functions the availability of remote access for teleworking.

For the development of the model, two essential parameters were required, MTBF (Mean Time Between Failures) of the system components and MTTR (Mean Time to Repair). The MBTF means the Mean Time Between Failures of the components, i.e. each component of a system together with its assembly counts a time, and this forms the lifetime reliability measure of a device. MTTR means the system's average repair time, i.e. from the moment the device/component fails, what is the time it takes to fix it. Other characteristics of the system are essential and must also be considered: the quality of the supervision system that can quickly detect the occurrence of the failure, the stock of spare parts that allows the component to be quickly replaced, and the logistics of the maintenance team so that the failed component can be repaired. This article will investigate the system transient solution of differential equations showing that it is not significant, in general, because repair times are much shorter than break times (MTBF >> MTTR). However, this article proposes the analysis of other aspects related to availability. For example, when it is assumed that the time to repair follows an exponential distribution and yet it is constant, the results can be quite different. The same can occur when an exponential distribution is assumed and the correct one is a long tail. Regarding the issue of the transient solution, the continuous simulation in Matlab-Simulink elucidates the described aspects. Regarding the different probability distributions, it was necessary to program a Discrete Event Simulation model. Thus, this article intends to have a broader scope for several situations in which the correct estimate of availability is essential.

Section II deals with the Theoretical Reference, Section III addresses the simulation models, Section IV describes the methodology for a specific case, Section V shows the estimate of availability and finally Section VI with the conclusions.

II. THEORETICAL REFERENCE

A. Quality of Service - QoS

According to the ITU-T [8], QoS parameters are perceived levels of quality on the aspects of a service offered, ultimately generating customer satisfaction. The parameters represent in a subjective and abstract way numerical values (quantified), thus providing the basis for constituting the SLA (Service Level Agreement) requirements for computerized systems.

QoS deals with the perception of quality of service that the end user has of their respective applications. According to the Menasce et al. [9], the QoS attributes for systems depend on the context that the users are included. This article will deal with only two of the attributes, which are:

Reliability and availability: the reliability of a system is the probability that it will work in a satisfactory and continuous way in a determined period. Availability is more comprehensive and includes reliability and repair. As described, reliability and availability are directly related concepts, but are distinct attributes. In systems where the reliability is relatively very high (failure-free operation time), when compared to repair time. Thus, with relatively very high reliability time or relatively very low repair time, availability value is close to one.

B. Service Level Agreement - SLA

In this article, focus on the attribute of reliability and availability. Availability, as already described, is the probability that a system will work satisfactorily and for a continuous time. For this, the best way to quantify is the measurement of the "nines". According to the Chumash [10], this measure refers to the amount of time (per year) that a system is running. Still according to the author, the inverse is more useful, since it shows the amount of downtime of a system, when it is not programmed activity. As seen in Table I, a system with a service level of six "nines" has only 31.54 seconds of unavailability per year.

TABLE I. Example of system availability describes the methodology [10]

Service Level	Availability per Year	Unavailability per Year
90%	328.50 days	36.50 days
99%	361.35 days	3.65 days
99.90%	364.64 days	8.76 hours
99.99%	364.96 days	52.56 minutes
99.999%	~365 days	5.26 minutes
99.9999%	~365 days	31.54 seconds

C. Models for Availability

Systems are supposed to be repairable, that is, systems that during their lifetime go through repeated periods of failure and repair and, when they fail, are repaired and restored to look as good as if they were new. In practice it is very common that, as defects are detected, the components are replaced (for example, the exchange of boards). They operate continuously and short periods when they are out of service can be tolerated.

A common model is the RBD (Reliability Block Diagram) blocks. Each RBD block represents one component of the system and each of these blocks are associated with two parameters: the average failure rate (λ) and the repair rate (μ). For Parthasarathy and Lenin [11], availability is defined as the probability that the system is working at a given instant, this definition is in accordance with what Trivedi [12] cites in his work. It is the most appropriate metric to evaluate the efficiency of a repairable system [13]. To have an intuitive idea of the concept of availability: if a system should have an availability of four nines, or 99.99%, it means that the system can be out of operation for 0.88 hours per year (less than 53 minutes out of operation per year).

D. RBD with Two Parallel Blocks and Single Repairman.

For a single block where a failure can occur and for a single repairman, and using the exponential distribution, we can say that the value of $E[T] = \frac{1}{\lambda}$ is called Mean Time Between Failures (MTBF). In turn, the repair rate for a block is μ. Similarly, for the failure rate, the value of $E[R] = \frac{1}{\mu}$ is called Mean Time To Repair (MTTR).

We can show that availability $D = \frac{MTBF}{MTBF+MTTR}$, in case of a single block and a repairman. We can notice that if the MTBF is too high, D tends to 1. Similarly, if MTTR is close to 0, D also tends to 1.

However, for the purpose of analyzing several situations and because our system has this type of configuration, we will analyze the system with two blocks in parallel and single repair according to Fig. 1, initially for exponential arrivals and service.

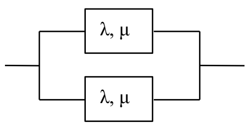

Fig. 1: System with two components in parallel and a single repairman.

We denote the system states as S_0, S_1 and S_2, which correspond to having zero, one or two defective elements, respectively. This way, the failed system state will be only S_2. Since we have only one repairman, only one of the components is repaired at a time and the repair rate will always be $\mu\Delta t$. This way, in S_0 it is possible to have a failure rate $2\lambda\Delta t$ because we have two elements working, but in S_1 the rate will be $\lambda\Delta t$. We note that the system will continue on S_1 if there is no fault or repair. In this representation we have chosen not to put the condition o(Δt), because, as we saw in the previous example, these values will not be considered as negligible (higher order values Δt). Fig. 2 illustrates the system of the diagram.

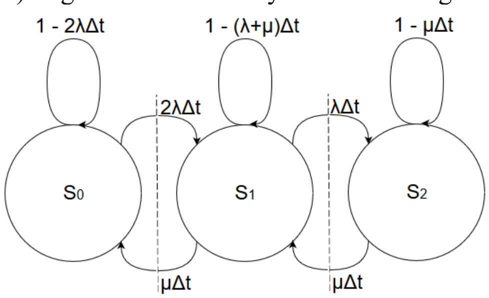

Fig. 2: System with two components in parallel and a single repairman.

Proceeding to the equation, we have (making $P(S_0) = P_0, P(S_1) = P_1, P(S_2) = P_2$):

$P_0(t + \Delta t) = P_0(t)(1 - 2\lambda\Delta t) + P_1(t)\mu\Delta t$ (1)

$P_1(t + \Delta t) = P_1(t)(1 - (\lambda + \mu)\Delta t) + P_0(t)2\lambda\Delta t + P_2(t)\mu\Delta t$ (2)

$P_2(t + \Delta t) = P_2(t)(1 - \mu\Delta t) + P_1(t)\lambda\Delta t$ (3)

Arranging, dividing by Δt and taking the limit Δt →0:

$\lim_{\Delta t\to 0} \frac{P_0(t+\Delta t)-P_0(t)}{\Delta t} = \dot{P}_0(t) = -2\lambda P_0(t) + \mu P_1(t)$ (4)

$\lim_{\Delta t\to 0} \frac{P_1(t+\Delta t)-P_1(t)}{\Delta t} = \dot{P}_1(t) = -(\lambda + \mu)P_1(t) + 2\lambda P_0(t) + \mu P_2(t)$ (5)

$\lim_{\Delta t\to 0} \frac{P_2(t+\Delta t)-P_2(t)}{\Delta t} = \dot{P}_2(t) = -\mu P_2(t) + \lambda P_1(t)$ (6)

Initially, the availability of a system in the transient state is analyzed, initial period when the probabilities of state depend significantly on time and in the steady state through the corresponding RBD [14, 15, 16, 17].

III. SIMULATION'S MODELS

To better present the various aspects of the problem, we will use Simulation, continuous and discrete. Therefore, this article expands its context and can also address Dependability, that is, Availability, Reliability and Maintainability.

A. Continuous Simulation Model

The transient state, corresponding to equations (1) to (6), is modeled in Matlab-Simulink according to Fig. 3:

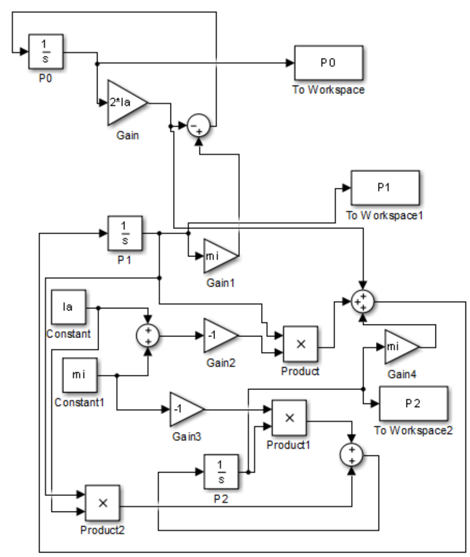

Fig. 3: Implementation of the three-state model in Matlab-Simulink.

Fig. 4 shows the evolution of the failure probabilities from the initial state, P(S0) = 1, P(S1) and P(S2) = 0, with λ= 0.5 (MTBF = 2 h), and μ= 1 (MTTR = 1 h). We can see that it takes about 3 hours for the system to reach steady state. However, this is not a real case. For this, we will use, relatively large MTBF and relatively small MTTR.

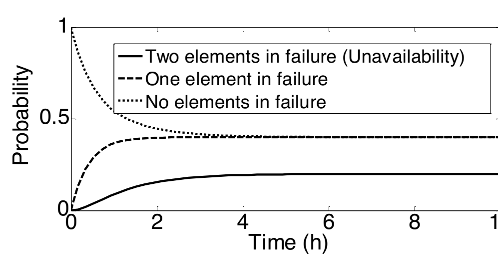

Fig. 4: Evolution in time of availability (*P*0 + *P*1 = 0.8) and unavailability (*P*2 = 0.2).

B. *Continuous Simulation Model - Stationary State*

Then we use the dynamic model to test, in Figure 5, a more realistic value, that is, $1/\lambda$ = MTBF = 500000 hours and $1/\mu$ = MTTR = 1 hour. The objective was to evaluate the system closest to the real in transient state. Fig. 5 shows that Availability is very close to 1 (one) quickly and Unavailability, also quickly, is very close to zero. To observe the system takes a long time.

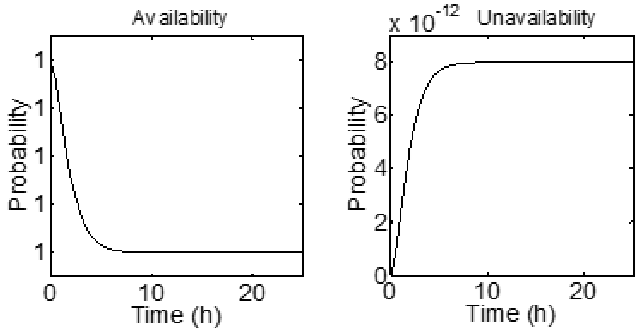

Fig. 5: Evolution in time of availability (P0 + P1) and unavailability (P2) to 1/λ= MTBF = 500000 hours.

It is clear that a significant amount of time needs to be spent in order for there to be failures so that we can observe the actual availability of the system. Note that, despite the MATLAB plot, the availability value is close to one and the unavailability value is close to zero (after only 25 minutes of operation). In this situation it is more adequate to evaluate the stationary state. In the case of electronic components, where the average time between failures is much longer than the average repair time (e.g., change of printed circuit boards), stationary state analysis is much more used. This fact is evident from the transient analysis performed.

In the steady state, with derivatives equal to zero and without dependence on time, we have:

$$2\lambda P_0 = \mu P_1 \quad (7)$$

$$P_1 = \frac{2\lambda}{\lambda+\mu} P_0 + \frac{\mu}{\lambda+\mu} P_2 \quad (8)$$

$$\mu P_2 = \lambda P_1 \quad (9)$$

Using the contour condition, $P_0 + P_1 + P_2 = 1$, and the equations (7) and (9) we can calculate the values of $P_0, P_1 e\ P_2$. The equation (8) does not need to be used but can be useful only for checking the correction of the result. For previous example, for $\lambda = 0.5$ and $\mu = 1.0$ we get $P_0 = \frac{2}{5}$, $P_1 = \frac{2}{5}$ and $P_2 = \frac{1}{5}$. We observe that unavailability is the state $P_2 = \frac{1}{5}$ and availability is the sum of $P_0 + P_1 = \frac{4}{5}$ or $1 - P_2 = \frac{4}{5}$ (Fig. 4 shows these values for the steady state).

Again, we point out that the equations (7) and (9), of steady state, can be obtained directly from Figure 2 making the input rates equal to the output rates, following the dotted lines. With the contour condition, $P_0 + P_1 + P_2 = 1$, we can also calculate the stationary states in this way.

C. *Discrete Event Simulation Model*

To obtain values different from those in which the exponential distribution is used, that is, for other distributions than the exponential one, it is necessary to make models using simulation by discrete events. Fig. 6 illustrates the case where we have *m* machines that can fail and, when this occurs, they are repaired. The main characteristic of this simulation model is due to the fact that there is a block called *Trigger* which starts with the generations of the *m* machines in operation.

We use separate m machines because each of them may have a different repair distribution and even a different failure distribution, for example, if they come from different manufacturers.

This block is only for initialization and each one of the ***Create*** blocks, corresponding to each one of the machines in operation, has a single generation during its whole life. After that, the system goes into normal operation, which corresponds to a closed queue system, and therefore the instances (machines) are infinitely circulating through the system that is, failure-repair. Fig.6 shows the blocks of the simulation program. Remember that the times the machines are running are *Ta*, the queue time is *Tw* and the service time of the only server is *Ts.* The machine block does not have a queue, only one condition: *Delay* which means the time *Ta* of normal operation of each one of them until the failure occurs. The server block has a queue, with a *Ts* service time, waiting time *Tw*, and the three conditions: *Seize - Delay - Release*.

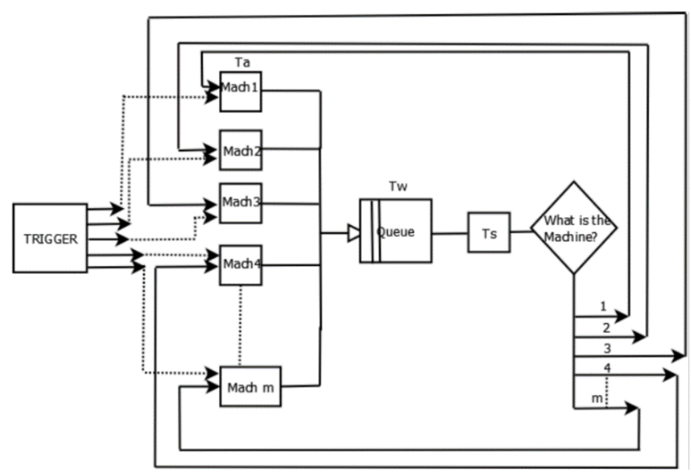

Fig. 6: Repair model as a Closed Queue System.

An essential condition is that the simulation program can be validated. Because we already have a known analytical model, this task is made easier. Once the simulation model is validated, other conditions that cannot be considered in the analytical model, which generally has simplifications, can be taken into account in the simulation model.

D. *Validation of the Discrete Event Simulation Model*

Table II below shows the values of the analytical model in steady state and the comparison with the Confidence Interval (CI) obtained by the simulation program. Both are using the exponential distribution, both for failure occurrences (λ) and for the service (μ) as in analytical model (we use m = 2 and they are exactly the same machines with the same fault and repair distribution so that it can be compared with the analytical model).

TABLE II: Analytical and Simulation Models (λ=0.5 and μ = 1.0)

Mod/prob	*P*0	*P*1	***P*2**
Analytic	0.4	0.4	**0.2**
Simulation	0.401 ± 0.003	0.399 ± 0.006	**0.200 ± 0.006**

The simulation program ran 8000 h and had six replications. The 95% confidence interval showed that the simulation program (Fig. 6) is validated and shows an excellent adherence to the analytical model.

E. Assessing Other Probability Distributions

Once the Simulation program has been validated, the goal is to evaluate how much other probability distributions may affect the availability value assignment. For this purpose, we used m = 2 in Fig. 6, and two service distributions were tested (we kept the same distribution for the failures): i) assuming that the service is performed with a constant duration equal to 1 h (μ = 1.0), and ii) using a long-tailed distribution (Lognormal) for the time of service, but with the same average duration (1 h; μ = 1.0) and greater variance. Table III, in the last two lines, shows two simulated models: i) with a constant length of service = 1h, and ii) with a length of service obeying the Lognormal distribution with an average of 1 h. We can notice the great difference in the probabilities of occurrence of each state. However, state P_2, which corresponds to Unavailability (P_2 = 0.2 for exponential service), has a significant reduction when the service is constant ($P_2 \cong 0.14$) and has a significant increase when the distribution is Lognormal ($P_2 \cong 0.29$).

TABLE III: Analytical and Simulation Models (λ=0,5 and μ = 1,0)

Mod/prob	P_0	P_1	$\boldsymbol{P_2}$
Analytic	0.4	0.4	**0.2**
Constant	0.373 ± 0.003	0.491 ± 0.004	**0.136 ± 0.002**
Lognormal	0.428 ± 0.015	0.283 ± 0.004	**0.290 ± 0.017**

Depending on the SLA value for Availability, the RBD block under consideration, and the parameters λ and μ, it is not possible to perform the calculations only with the exponential analytical model and, therefore, simulation is essential.

IV. METHODOLOGY FOR NETWORK AVAILABILITY (FIREWALL)

A. Research Methodology and Work Plan

The methodology of this research project proposes the study of multiple cases [18] with a longitudinal perspective. The approach is exploratory in nature, through case study, which according to the [18], addresses the description of the situation. The interview is the main source of data collection.

The interviews were conducted to verify whether the concepts studied in the literature review are equivalent to the tacit knowledge of the interviewees. Once the interviews were transcribed, a codification was made.

The coding focuses on words as a basic medium and assumes that the words involved were refined from raw notes or recordings to a clear text for the reader or analyst.

The analysis was carried out by comparing the categories or standard codes of the coding with the literature review theory. Two managers of the researched company were interviewed, Table IV.

TABLE IV: Characteristics of the interviewees

Interviewed	**Company**	**Position**	**Company Time**
A1	A	Information Security Specialist	9 years
A2	A	Information Security Manager	20 years

This article was also based on the topology and descriptions provided by the organization, on which the case study was based, so as to have maximum approximation to reality.

The environment presented was analyzed from documents provided on a confidential basis and from which we will describe the essential points. Thus, this research has document analysis to describe the facts that currently occur in this infrastructure. Documental readings and visualization of the already deployed environment were made. This line of reasoning fits [19] mentions in his publication: The descriptive research observes, registers, analyzes and correlates facts or phenomena (variables), without manipulating them; it studies facts and phenomena of the physical world and, especially, of the human world, without interference of the researcher.

There is also bibliographical research in this study, which aims to provide technical background and explain all the ideas and technical terminologies used in this document to understand all the facts.

In order to develop the methodology of network availability, certain information that was granted for our research was necessary, such as the rates of MTBFs (Mean Time Between Failures) and MTTRs (Mean Time for Repair); and the RBDs (Reliability Block Diagram), the latter two being confidential.

The MTBFs were granted by the manufacturer of the equipment, approached in this study, through technical documentation. The MTTRs were informed by those responsible for supporting the technology. In a confidential way, we will describe the main points, important for the progress of this study, leaving the names of the companies anonymous.

The RBDs were modeled using the information provided in the interviews and the infrastructure documentation provided for the preparation of this survey. As far as possible, the data closest to the actual values will be used. In this way, the methodology was applied with the best data available until the conclusion of this work. On the other hand, when it is possible to obtain statistical data and distributions with more updated or more precise measures, the methodology developed will be ready to work with these new values.

B. Data Collection

Company A is a Brazilian company that operates in the Americas and has some products that are sold around the world. The company's shares are listed on some of the world's major stock exchanges.

This study focused on the technology infrastructure of Company A, which has 02 Datacenters operating in an Active and Passive mode, i.e., the Active Datacenter is responsible for all processing, data, communication, etc., which are necessary. In case the Active Datacenter is unavailable, all the work performed by this Datacenter is transferred to the Passive Datacenter, as seen in Fig. 7.

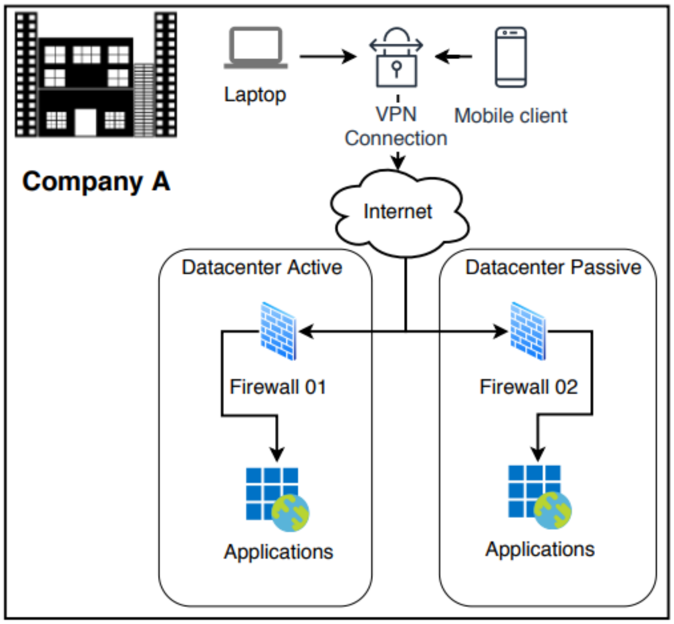

Fig. 7: Topology of the Technology Infrastructure of Company A.

The manufacturer company, through public documents on the Internet, supplies the MTBF of the equipment used in this topology. As both equipments are of the same model, due to the topology being a mirror between the Active Datacenter and the Passive Datacenter, both equipments have 10.2 years of MTBF. The equipments form a cluster, so the configuration between the two equipments are the same and the replacement of the Active Firewall by the Passive occurs instantly in case of failure (remembering that the simulation model can contemplate possible delay times for switching in case of failure, or even the possible sum of different types of distribution that are components of the repair time.).

It is necessary to present maintenance SLA data, so that the availability of the studied network (MTTR) is calculated in the most approximate way possible.

- The SLA contracted by the company studied is 99.8% per year.
- In case of equipment failure, the monitoring system opens a severity 1 call and the SLA for the start of this incident is 01 hour
- The SLA for incident resolution severity 1 is 04 hours after signing the call generated by the monitoring tool.
- If a Hardware failure is identified, the company studied has a support contract that guarantees that new equipment will be sent on the next business day. That is, the unavailability can reach up to 04 days for the new equipment to arrive at the site, in case of failure on Friday.

V. Estimate of Availability

Thus, in the case of equipment that can be repaired, the spare equipment takes over the function of what has failed, and, in this case, there will be a failure and a repairman, who will have the repair time to restore the service.

Our proposal is for a method that can be used in a broader way, but in our case study two situations occurred:

i) the time between failures is significantly longer than the time to repair. Therefore, it is not justified to make an analysis in a transient state;

ii) We have little information, mainly regarding repair distribution. Therefore, it is not worth making a simulation model to contemplate distributions other than the exponential.

For this calculation, the formulas (7), (8) and (9) will be used. Availability is given by D=1-I, where unavailability (I) is the value of the last fault in the fault state. For verification, the sum of all the states.

The calculation made for location is: when the failure occurs there are no more blocks available, i.e. when the S2 state is reached, shown in Fig. 2.

First of all, it is necessary to calculate the λ of the modules, which are the failure rates. Two maintenance scenarios will be considered: (1) the best maintenance scenario for reactivating the equipment in failure, i.e., the sum of the SLA of the signature of the incident generated by the monitoring tool (up to 01 hour) and the SLA of resolution of the incident after the signature (up to 04 hours), without the need to send a new Hardware, totaling 5 hours; (2) the worst maintenance scenario for the reactivation of the failed equipment, i.e., the sum of the incident signature SLA generated by the monitoring tool (up to 01 hour), the incident resolution SLA after the signature (up to 04 hours) and the time for sending a new Hardware by the manufacturer (up to 04 days/96 hours), i.e., a total of 101 hours. Other significant times will not be counted because we do not have an average of hours for the calculation, such as the time of equipment shipment by the teams responsible for receiving and documenting the entry of a new device in the company.

- λ.

$$\lambda = \frac{1}{MTBF}\,[horas^{-1}] = \frac{1}{10.2 \times 8760} = 0.000011191691288387 50$$

- Availability 1st scenario (05 hours);

$$P_0 = \frac{1}{1 + \left(\frac{2\lambda}{\mu}\right) + 2\left(\frac{\lambda}{\mu}\right)^2}$$

$P0 = 0.999888089349814$

$$P_2 = 2\left(\frac{\lambda}{\mu}\right)^2 \times P_0$$

$P2 = 6.2619968321575e\text{-}09$

$D_{05\ hours} = 1 - I = 1 - P2 = 0.999999993738003$

- Availability 2nd scenario (101 hours);

$P0 = 0.997741833784398$

$P2 = 2.54966057902857e\text{-}06$

$D_{101\ hours} = 1 - I = 1 - P2 = 0.999997450339421$

From the calculations obtained, it was possible to determine the unavailability time per year, assuming exponential failure distribution and repair. The analysis is made from the values of the proposed maintenance scenarios of 05 hours and 101 hours, for stationary state, as shown in Table V.

TABLE V - Hardware Availability

Maintenance	Availability (%)	Availability in days per year	Unavailability in seconds per year
05 hours	0.9999999937380	364.99999771437	0.19747833939618
101 hours	0.9999974503394	364.99906937388	80.4060960523784

As seen in Table V, with a maintenance of 05 hours, the unavailability per year would be approximately 0.2 seconds and with a maintenance of 101 hours the unavailability per year is approximately 80 seconds. It is worth noting that this analysis is not valid for a single year, but the average of a period over several years (for example MTBF of 10.2 years), where the equipment/component will fail only once.

VI. Conclusions

It was verified that the variation in the estimated value of the Availability, in relation to the correct value of the System, can be wrong if i) the probability distributions involved are different from the exponential one, or ii) if the repair times are not small when compared to the times between failures. In both cases simulation is essential. In the case i) it is necessary to use the Discrete Event Simulation model and in the case ii) it is important to check the transient, that is, to use the Continuous Simulation. Although the estimate for the values obtained for the Firewall was made for the steady state, considering time distribution between failures and exponential repair time, the values must be reestimated by the simulation model if the contracted QoS requirements are critical (SLA is QoS in practice). In the example for 101 hours of maintenance, an inadequate calculation could oversize the actual Availability (imagine if Availability is made for five nines and there is a fine if this does not occur). Although the results were considered adequate, other approaches such as Petri Nets, Markov Chains and Monte Carlo Method could be tested in the future.

Therefore, as already stated, this article expands its context and can also address Dependability, that is, Availability, Reliability and Maintainability.

Acknowledgment

This study was funded in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) - Finance Code 001.

References

[1] OPAS Brasil, 2020.

[2] SOBRATT - SOciedade BRAsileira de Teletrabalho e Televendas, “Aprovada resolução que regulamenta o teletrabalho no Poder Judiciário.”, 2016.

[3] G1, “Home office bateu recorde no Brasil em 2018, diz IBGE,” G1, 2019.

[4] N. Bloom, “To raise productivity, let more employees work from home,” Harvard business review, *92*(1/2), 28-29, 2014.

[5] E. Baker, G. C. Avery, J. D. Crawford, “Satisfaction and perceived productivity when professionals work from home,” Research & Practice in Human Resource Management, 2007.

[6] C. J. Fitzgerald, K. M. Danner, “Evolution in the office: How evolutionary psychology can increase employee health, happiness, and productivity,” Evolutionary Psychology, *10*(5), 147470491201000502, 2012.

[7] W. Baomin, L. Ning, J. Hongqiang, “VPNs authentication scheme based Trusted Computing Platform,” In 2010 International Conference on Computer Application and System Modeling (ICCASM 2010), (Vol. 11, pp. V11-362), IEEE, 2010.

[8] ITU-T. “Quality of Service and Network Performance: Handbook,” Handbooks on Standardization, ITU, Geneva, http://handle.itu.int/11.1002/pub/80696004-en, 2012.

[9] D. A. Menasce, V. A. Almeida, L. W. Dowdy, L. Dowdy, “Performance by design: computer capacity planning by example,” Prentice Hall Professional, 2004.

[10] T. Chumash, “Obtaining Five ‘Nines’ of Availability for Internet Services,” Rutgers University, 2005-2019.

[11] P. R. Parthasarathy, R. B. Lenin, “Birth and Death Processes (BDP) Models with Applications – Queueing, Communication Systems, Chemical Models, Biological Models: The State-of-the-Art with a Time-Dependent Perspective,” Syracuse, New York: American Sciences Press, Inc., 2004.

[12] K. S. Trivedi, “Probability & Statistics with Reliability, Queueing, and Computer Science Applications,” New Jersey: Prentice Hall, Inc., 1982.

[13] A. Goyal, S. S. Lavenberg, K. S. Trivedi, “Probabilistic Modeling of Computer System Availability,” Annals of Operations Research, Vol. 8, pp. 285 - 306. http://www.ee.duke.edu/~kst, 1987.

[14] B. V. Gnedenko, Yu. K. Belyayev, A. D. Solovyev, “Mathematical Methods of Reliability Theory,” New York: Academic Press, Translated by Scripta Technica, Inc., Translation edited by Richard E. Barlow, 1969.

[15] W. Feller, “Introduction to Probability Theory and its Applications,” Vol. I, Third edition, Revised printing, New York: John Wiley & Sons, 1970.

[16] I. Bazovsky, “Reliability Theory and Practice,” New Jersey: Prentice-Hall, Inc., 1961.

[17] M. L. Shooman, “Reliability of Computer Systems and Networks – Fault Tolerance, Analysis, and Design,” New York: John Wiley & Sons, Inc., 2002.

[18] R. K. Yin, “Estudo de caso: planejamento e métodos,” Porto Alegre, RS, 2005.

[19] L. Rampazzo, “Metodologia Científica: Para Alunos dos Cursos de Graduação e Pós-graduação,” 3. São Paulo. Ed. Loyola, 136p, 2005.