TRIBUNAL DE JUSTIÇA
DO RIO DE JANEIRO

2020
AQUISIÇÃO
IDPS

Sistema de Detecção e
Prevenção de Intrusão

Proceso: 2020-0617549

SUMÁRIO

O QUE É UM IDPS?

Um Sistema de Detecção e Prevenção de Intrusão (Intrusion Detection and Prevention System - IDPS) é um sistema híbrido que automatiza o processo de detecção de intrusão e tem a capacidade de impedir possíveis incidentes de segurança, bloqueando ataques maliciosos.

Existem basicamente três tipos de intrusões para um IDPS detectar: os tidos como Conhecidos, quando possuem uma estrutura rígida e seu comportamento já é devidamente catalogado; Generalizáveis, quando são parecidos com os conhecidos, no entanto apresentam modificações em seu funcionamento e Desconhecidos, isto é, intrusões não muito difundidas ou mesmo uma versão muito generalizada de uma intrusão conhecida, as quais tornam impossíveis os usos de regras predefinidas para detecção.

Para detectar as operações ilegais na rede são usadas, nos dois primeiros casos, a checagem de assinaturas, isto é, procura por padrões já pré-estabelecidos de atividades de cunho malicioso. Para invasões desconhecidas, busca-se anomalias, que são nada mais do que atividades/dados diferentes do perfil tradicional da máquina/rede em que o IDPS se encontra.

Após detectada uma intrusão, um IDPS pode apenas apresentar um comportamento passivo de resposta, isto é, ele apenas alerta o usuário do ocorrido, ou ele pode dar uma resposta ativa (uma solução) bloqueando o possível ataque.

DA NECESSIDADE DE UM IDPS.

Sistemas de detecção de intrusão são essenciais nas redes modernas. A facilidade de acesso a programas capazes de invadir tornam cada vez mais necessária a utilização de um sistema desse tipo. Ademais, não basta mais apenas alertar sobre a presença de um intruso, a tecnologia deve ser capaz de prevenir e atuar em tempo real.

Entretanto, há inúmeros problemas que ainda exigem soluções eficientes. Definir o que é normal, log e comportamento, e o que é suspeito, caracteristicamente anômalo, é complicado e muito relativo.

Para tentar diminuir o impacto das falhas do sistema IDPS, torna-se vantajosa a sua integração com diversos outros sistemas ou até mesmo entre si. Integrar diversos tipos/camadas de IDPS e introduzir IDPS aos programas conhecidos de Firewall e Antivirus, não só reduz as falhas, como também torna mais poderosos os programas de proteção já existentes.

Nesse sentido, de acordo com o Gartner, um IDPS oferece o melhor desempenho e eficácia na detecção em segurança de rede, mas os Firewalls estão absorvendo o IDPS onde o volume de tráfego não é grande (*throughput*) e nas pontas (filiiais ou sites isolados).

Trata-se de uma tendência de mercado soluções de vários fabricantes que unem diversas funções de segurança. No entanto, não se pode considerar que é uma solução definitiva para todos os problemas, havendo vantagens, desvantagens e melhores escolhas tanto na unificação, segregação ou posicionamento destas funções de segurança, de acordo com cada ambiente.

Portanto, o uso de um IDPS genuíno e dedicado ainda é mais do que uma possibilidade, mas conforme o caso, uma necessidade.

Isso se reflete nos próprios estudos do Gartner, que observou em documento publicado em janeiro de 2018, que o mercado de IDPS começaria a encolher a partir de 2017, visto que a tecnologia já se mostrava cada vez mais onipresente embutida em outras plataformas.

Esta previsão foi reafirmada em outro estudo, de julho de 2019, mas desta vez assinalou que 75% dos fornecedores relataram crescimento nos data centers, de IDPS dedicado, em um contraponto ao panorama global.

Isto porque os volumes de tráfego no data center costumam ultrapassar a capacidade de um IDPS embutido em Firewall. Ou então, os custos de um que fosse capaz, seriam proibitivos. Ademais, é importante diferenciar um IDPS dedicado de um Firewall que possa exercer esta função: o primeiro conta com diversas funções habilitadas por padrão, como visibilidade de aplicação ou inspeção profunda de pacotes, o que não é o caso dos Firewalls.

Em segundo lugar, de acordo com o Gartner, os próprios fabricantes de Firewall relatam variados níveis de degradação de desempenho quando a função de IDPS está ativada. Desta forma, deve-se projetar uma redução de 70% do throughput do Firewall com estas funções habilitadas. Isto quer dizer que dada as características do data center, um Firewall de tamanha capacidade será mais caro que um Firewall e um IDPS dedicados e devidamente dimensionados.

E ainda, além das questões de desempenho, os IDPS dedicados atingem melhores indicadores de detecção e cobertura de vulnerabilidades do que a maioria dos produtos de Firewall.

DA NECESSIDADE DA AQUISIÇÃO DE NOVA SOLUÇÃO DE IDPS.

Até maio de 2019 , o TJRJ dispunha de dois links de Internet com uma única operadora e para atender a resolução CNJ nº 211/2015 foram contratados e instalados dois circuitos de 1Gbps , providos por duas operadoras diferentes, podendo um atingir 2Gpbs de tráfego full-duplex. Até o primeiro semestre de 2019, o tráfego de internet estava dentro dos limites nominais de capacidade dos equipamentos IDPS em uso, suficientes para atender à demanda pelos serviços disponíveis na Internet.

Entretanto, uma explosão de serviços de automação para escritórios de advocacia e de integrações e automações desenvolvidas pelo Ministério Público sobre o Processo Eletrônico e o MNI, aliadas à mudança na topologia interna e reconfiguração do IDPS para implantação do sistema autônomo e divulgação do IP público do TJRJ, anteciparam a necessidade de aumento da capacidade de inspeção destes ativos, que estava prevista para o segundo semestre de 2020

No TJRJ, o IDPS está posicionado a frente do Firewall, inspecionando o tráfego oriundo e direcionado à Internet. Nesta posição, ele pode registrar informações sobre tentativas de ataques de negação de serviço, que não estariam disponíveis, caso estivesse por trás do Firewall.

Desta forma, o IDPS faz a primeira filtragem do tráfego norte-sul[1], enquanto o Firewall trabalha sobre o controle deste e de todo o tráfego leste-oeste[2] do data center.

A presente aquisição tem por objetivo a substituição da solução existente, uma vez que esta já se mostra insuficiente frente a quantidade de tráfego que deve ser analisado atualmente. A crescente informatização das rotinas judiciais e administrativas do Poder Judiciário do rio de Janeiro, aumenta de forma significativa proporcionalidade entre a oferta jurisdicional e a quantidade de tráfego que flui entre a internet e o ambiente interno do TJERJ.

A solução atual de IDPS foi dimensionada no ano de 2011, uma época em que o TJERJ possuía um link de internet de 80 Mbps. O link, entretanto, devido à crescente informatização, já citada, além de projetos como Office Online, e-mail na nuvem, processo eletrônico, dentre outros fatores como a própria popularização da internet, veio sofrendo constantes upgrades. De dois links de 100 Mbps em 2013, dois links de 300 Mbps em 2015, dois links de 500 Mbps em 2017 e atualmente TJERJ conta com dois links de 1 Gbps cada, totalizando 2 Gbps.

O gráfico abaixo mostra o incremento da quantidade de banda existente ao longo do tempo.

Figura 1 Gráfico de aumento de quantidade de tráfego

Houve um aumento de 2500% na quantidade de link desde que a atual solução de IDPS foi adquirida. Tamanho aumento, resultou na necessidade de upgrade nos ativos de segurança de rede, os quais são diretamente afetados pela quantidade de tráfego que flui da internet para o ambiente interno bem como do ambiente interno para a internet. No entanto, os equipamentos atuais (especificamente IDPS) não possuem mais capacidade de crescimento, tornando

[1] Tráfego que flui de dentro do ambiente do TJERJ para fora, e no sentido oposto. (normalmente pelo link de internet).

[2] Tráfego que flui dentro do ambiente interno do TJERJ.

necessária a aquisição de uma nova solução com capacidade proporcionalmente maior para o atendimento do link.

DAS 10 MAIS FREQUENTES AMEAÇAS.

Existem atualmente vários tipos de ataques que são detectados/prevenidos pelas ferramentas de IPS, os quais possuem os mais diversos modos de atingir o ambiente bem como os mais diversos objetivos. Com o passar do tempo, formas novas de ataques, baseados em descobertas de vulnerabilidades vão surgindo. O que obriga que as soluções de segurança se adaptem às novas descobertas em uma atualização constante a fim de manter a segurança do perímetro. Segue abaixo uma lista e descrição das dez mais frequentes ameaças detectadas e/ou prevenidas no período de 01/08/2020 a 19/08/2020:

SQL INJECTION SCANNING ATTEMPT

Este ataque consiste na varredura, feita por invasores remotos a fim de localizar vulnerabilidades potenciais para injeção de SQL[3] em um servidor, as quais poderão ser utilizadas posteriormente.

Quantidade de ocorrências no período: 955

SQL SERVERS SQL INJECTION OBFUSCATION TECHNIQUES

Os invasores podem usar técnicas de injeção SQL para executar comandos SQL em servidores SQL. Para evitar a detecção por dispositivos de segurança, eles podem usar várias técnicas de ofuscação para ocultar suas ações. A exploração bem-sucedida destas técnicas pode permitir que um invasor revele informações confidenciais, modifique ou desligue o banco de dados ou execute código arbitrário nos servidores afetados.

Quantidade de ocorrências no período: 923

SQLMAP AUTOMATED SQL INJECTION TOOL.

Sqlmap é uma ferramenta automatizada de injeção SQL. Os invasores remotos podem usar o Sqlmap para buscar dados do banco de dados e executar instruções SQL.

Quantidade de ocorrências no período: 834

[3] Ameaça de segurança que se aproveita de falhas em sistemas os quais interagem com base de dados por comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta (SQL query) através da entradas de dados de uma aplicação, como formulários ou URL.

MICROSOFT CAPICOM CERTIFICATES ACTIVEX CONTROL CODE EXECUTION

Certificados CAPICOM (CAPICOM.dll) é um controle ActiveX que fornece um método para criptografar dados com base na funcionalidade segura do Windows CryptoAPI. Uma vulnerabilidade de execução remota de código foi relatada em certificados CAPICOM (Cryptographic API Component Object Model). Um invasor remoto pode explorar esse problema convencendo um usuário a visitar documentos HTML especialmente criados ou abrir uma página da Web mal-intencionada. A exploração bem-sucedida pode resultar em controle remoto execução de código no sistema de destino, uma vez que a página maliciosa é carregada.

Quantidade de ocorrências no período: 507

NONECMS THINKPHP REMOTE CODE EXECUTION (CVE-2018-20062)

Existe uma vulnerabilidade de execução remota de código no framework NoneCMS ThinkPHP. A exploração bem-sucedida desta vulnerabilidade pode permitir que um invasor remoto execute código arbitrário no sistema afetado.

Quantidade de ocorrências no período: 477

COMMAND INJECTION OVER HTTP

Uma vulnerabilidade de comando de injeção sobre HTTP foi relatada. Um atacante remoto pode explorar esse problema enviando uma solicitação especialmente criada para a vítima. A exploração bem-sucedida permitiria a um invasor executar código arbitrário na máquina alvo.

Quantidade de ocorrências no período: 333

WEB SERVER EXPOSED GIT REPOSITORY INFORMATION DISCLOSURE

Uma vulnerabilidade de divulgação de informações foi relatada no Repositório Git. A exploração bem-sucedida desta vulnerabilidade pode permitir a divulgação não intencional de informações da conta.

Quantidade de ocorrências no período: 218

ADOBE READER PDF CIDFONT DICTIONARY MEMORY CORRUPTION

Existe uma vulnerabilidade de corrupção de memória no Adobe Reader. A vulnerabilidade se deve a um erro no Adobe Reader ao lidar com arquivos PDF que contêm entradas de dicionário CIDFont. Um invasor remoto pode acionar essas falhas por meio de um arquivo PDF especialmente criado. A exploração bem-sucedida causará corrupção de memória,

fazendo com que o aplicativo trave e pode permitir a execução de código arbitrário assim que um arquivo PDF malicioso for carregado em um sistema vulnerável.

Quantidade de ocorrências no período: 81

SQL SERVERS UNION QUERY-BASED SQL INJECTION

As técnicas de injeção de SQL podem permitir que invasores remotos executem comandos SQL em servidores SQL. A exploração bem-sucedida pode permitir que o invasor revele informações confidenciais, modifique ou desligue o banco de dados ou execute código arbitrário nos servidores afetados.

Quantidade de ocorrências no período: 79

NMAP SCRIPTING ENGINE SCANNER OVER HTTP REQUEST

O Nmap Scripting Engine é um produto de varredura de vulnerabilidade. Os atacantes remotos podem utilizá-lo para detectar vulnerabilidades em um servidor de destino.

Quantidade de ocorrências no período: 78

CONCLUSÕES

Pelo exposto, conclui-se que a solução de IDPS que se pretende adquirir é de fundamental importância para a manutenção, a níveis aceitáveis, da segurança dos dados e informações mantidos e trafegados pelo TJERJ.

Outrossim, opta-se pela aquisição de uma ferramenta dedicada à funcionalidade de IPS, uma vez que será alocada à inspeção do tráfego norte-sul, de modo a liberar outros ativos como o Firewall e o Proxy à inspeção do tráfego leste-oeste ou mesmo dos outros acessos com o ambiente externo, como links de parceiros, rede de longa distância com as comarcas, VPNs com as empresas colaboradoras, etc.

Não menos importantes, são os serviços atrelados à contratação, que têm por objetivo viabilizar a correta implantação e operação da solução, a fim de que se possa utilizá-la de forma eficiente e eficaz, trazendo uma maior efetividade na proteção dos dados.

A tabela abaixo, descreve os itens que compõem a solução.

Item	Descrição	Quantidade	Pagamento
1	Solução de IPS	1 (dois appliances e um dashboard)	PARCELA ÚNICA
2	SERVIÇO DE IMPLANTAÇÃO	1	PARCELA ÚNICA
3	SUPORTE TÉCNICO	48 meses	MENSAL
4	SUPORTE TÉCNICO ESPECIALIZADO	300 (trezentas) horas	SOB-DEMANDA
5	TREINAMENTO OFICIAL DA SOLUÇÃO	1 turma de 4 (quatro) alunos.	SOB-DEMANDA
6	GARANTIA DA SOLUÇÃO (item 1 e 2)	48 Meses	MENSAL

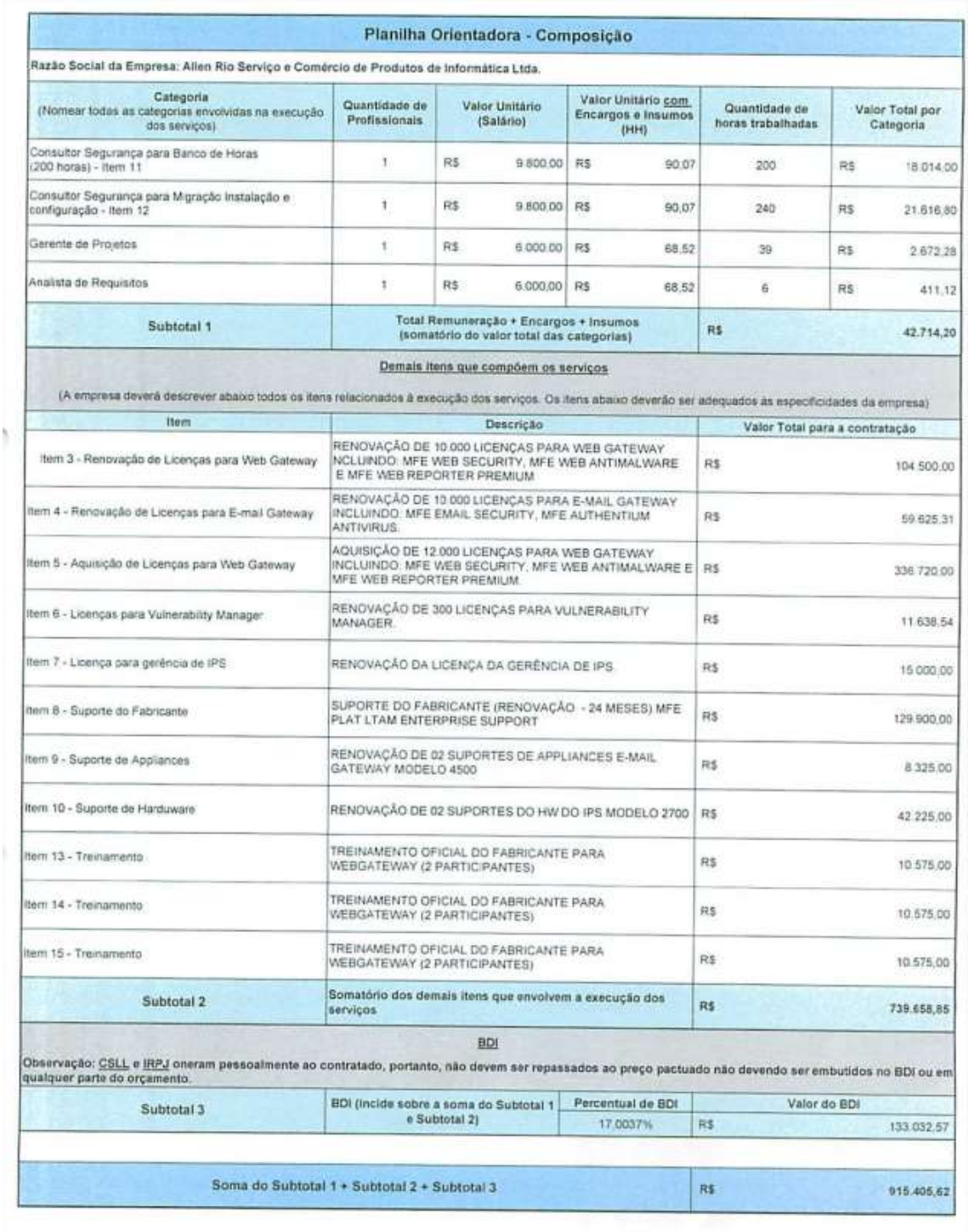
Figura 2 Tabela de itens da contratação.

DAS INFORMAÇÕES DA CONTRATAÇÃO PASSADA.

Modalidade:	Pregão Eletrônico
Tipo de licitação:	Menor preço global
Processo:	2020-0617549
Prazo:	48 meses de contrato
Valor:	R$ 4.019.446,64
Relator:	Humberto Cruz/Renato Warwar
Relação com Pje:	Toda infra de controle de acesso a internet precisa evoluir para atender a demanda prevista para o PJe.
Objetivo:	Para ciência e Deliberação
Justificativa:	A solução atualmente instalada mostra-se incapaz de atender a demanda frente ao aumento de tráfego gerado pelo aumento de serviços prestados pelo PJERJ ao público externo e a virtualização dos sistemas e rotinas judiciais e administrativas do PJERJ. Após a configuração dos dois links de 1Gbps de Operadoras distintas foi mais perceptível o esgotamento de recursos dos IPS causado em função do aumento do uso de robôs, por diversas entidades externas, em busca de informações publicadas pelo TJRJ razão esta dos problemas enfrentados nos meses de setembro e outubro de 2019, assim faz-se necessária a aquisição de nova solução de IPS.

A contratação anterior, na qual foi adquirido o equipamento que será substituído, ocorreu em 2012 e teve por objetivo a aquisição de diversos ativos/serviços entre os quais o IDPS. Ademais, existem algumas diferenças em relação à contratação que se pretende, como o tempo de contratação, que, no caso de 2012, foi de 24 meses.

Para que seja possível uma comparação, foi necessário extrair da contratação anterior os itens que são relativos ao IDPS constantes nas figuras/Tabelas abaixo.



Planilha Orientadora - Composição

Razão Social da Empresa: Allen Rio Serviço e Comércio de Produtos de Informática Ltda.

Categoria (Nomear todas as categorias envolvidas na execução dos serviços)	Quantidade de Profissionais	Valor Unitário (Salário)	Valor Unitário com Encargos e Insumos (HH)	Quantidade de horas trabalhadas	Valor Total por Categoria
Consultor Segurança para Banco de Horas (200 horas) - Item 11	1	R$ 9.800,00	R$ 90,07	200	R$ 18.014,00
Consultor Segurança para Migração Instalação e configuração - Item 12	1	R$ 9.800,00	R$ 90,07	240	R$ 21.616,80
Gerente de Projetos	1	R$ 6.000,00	R$ 68,52	39	R$ 2.672,28
Analista de Requisitos	1	R$ 6.000,00	R$ 68,52	6	R$ 411,12
Subtotal 1	**Total Remuneração + Encargos + Insumos (somatório do valor total das categorias)**			**R$**	**42.714,20**

Demais itens que compõem os serviços

(A empresa deverá descrever abaixo todos os itens relacionados à execução dos serviços. Os itens abaixo deverão ser adequados às especificidades da empresa)

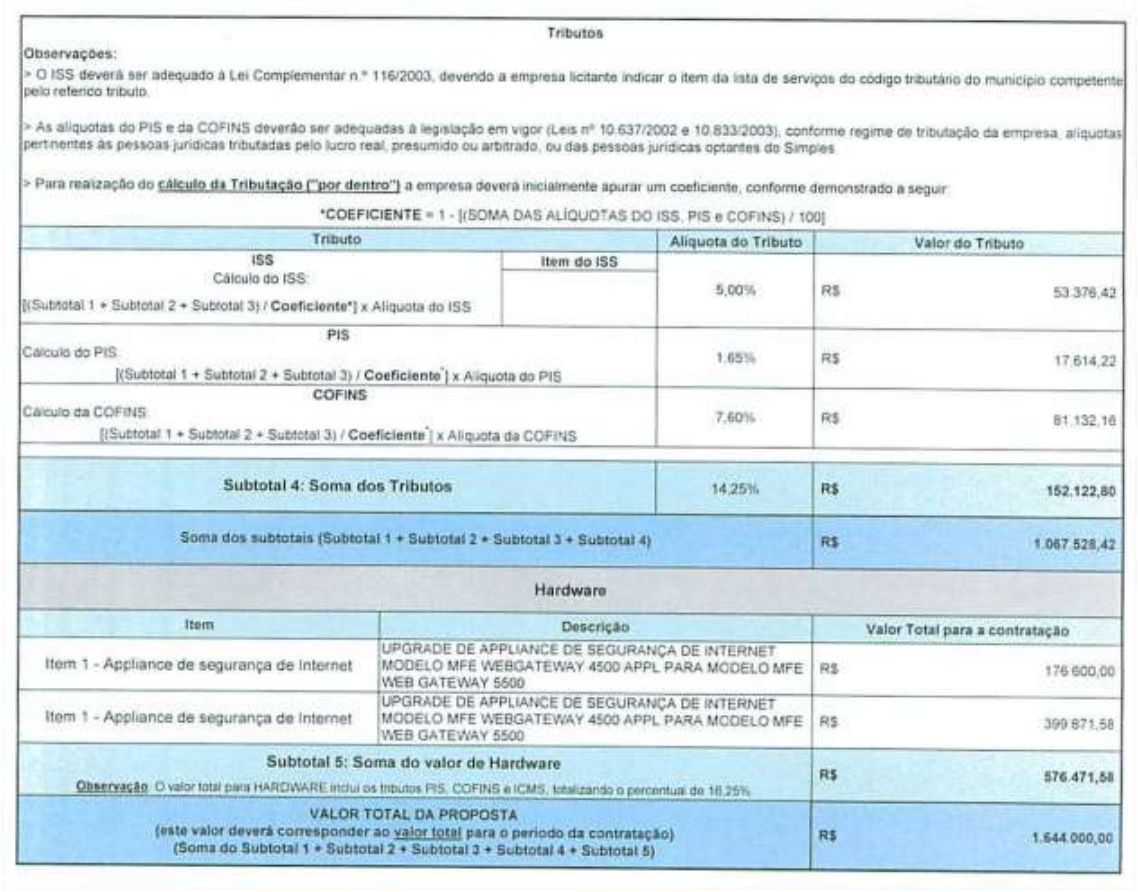
Item	Descrição	Valor Total para a contratação
Item 3 - Renovação de Licenças para Web Gateway	RENOVAÇÃO DE 10.000 LICENÇAS PARA WEB GATEWAY NCLUINDO: MFE WEB SECURITY, MFE WEB ANTIMALWARE E MFE WEB REPORTER PREMIUM	R$ 104.500,00
Item 4 - Renovação de Licenças para E-mail Gateway	RENOVAÇÃO DE 10.000 LICENÇAS PARA E-MAIL GATEWAY INCLUINDO: MFE EMAIL SECURITY, MFE AUTHENTIUM ANTIVIRUS.	R$ 59.625,31
Item 5 - Aquisição de Licenças para Web Gateway	AQUISIÇÃO DE 12.000 LICENÇAS PARA WEB GATEWAY INCLUINDO: MFE WEB SECURITY, MFE WEB ANTIMALWARE E MFE WEB REPORTER PREMIUM	R$ 336.720,00
Item 6 - Licenças para Vulnerability Manager	RENOVAÇÃO DE 300 LICENÇAS PARA VULNERABILITY MANAGER.	R$ 11.638,54
Item 7 - Licença para gerência de IPS	RENOVAÇÃO DA LICENÇA DA GERÊNCIA DE IPS	R$ 15.000,00
Item 8 - Suporte do Fabricante	SUPORTE DO FABRICANTE (RENOVAÇÃO - 24 MESES) MFE PLAT LTAM ENTERPRISE SUPPORT	R$ 129.900,00
Item 9 - Suporte de Appliances	RENOVAÇÃO DE 02 SUPORTES DE APPLIANCES E-MAIL GATEWAY MODELO 4500	R$ 8.325,00
Item 10 - Suporte de Harduware	RENOVAÇÃO DE 02 SUPORTES DO HW DO IPS MODELO 2700	R$ 42.225,00
Item 13 - Treinamento	TREINAMENTO OFICIAL DO FABRICANTE PARA WEBGATEWAY (2 PARTICIPANTES)	R$ 10.575,00
Item 14 - Treinamento	TREINAMENTO OFICIAL DO FABRICANTE PARA WEBGATEWAY (2 PARTICIPANTES)	R$ 10.575,00
Item 15 - Treinamento	TREINAMENTO OFICIAL DO FABRICANTE PARA WEBGATEWAY (2 PARTICIPANTES)	R$ 10.575,00
Subtotal 2	**Somatório dos demais itens que envolvem a execução dos serviços**	**R$ 739.658,85**

BDI

Observação: CSLL e IRPJ oneram pessoalmente ao contratado, portanto, não devem ser repassados ao preço pactuado não devendo ser embutidos no BDI ou em qualquer parte do orçamento.

Subtotal 3	**BDI (incide sobre a soma do Subtotal 1 e Subtotal 2)**	**Percentual de BDI**	**Valor do BDI**
		17,0037%	R$ 133.032,57
Soma do Subtotal 1 + Subtotal 2 + Subtotal 3			**R$ 915.405,62**

Figura 3 Composição de custos da contratação que continha o IDPS em 2012 depois da licitação.



Tributos

Observações:

> O ISS deverá ser adequado à Lei Complementar n.º 116/2003, devendo a empresa licitante indicar o item da lista de serviços do código tributário do município competente pelo referido tributo.

> As alíquotas do PIS e da COFINS deverão ser adequadas à legislação em vigor (Leis nº 10.637/2002 e 10.833/2003), conforme regime de tributação da empresa, alíquotas pertinentes às pessoas jurídicas tributadas pelo lucro real, presumido ou arbitrado, ou das pessoas jurídicas optantes do Simples.

> Para realização do **cálculo da Tributação ("por dentro")** a empresa deverá inicialmente apurar um coeficiente, conforme demonstrado a seguir:

*COEFICIENTE = 1 - [(SOMA DAS ALÍQUOTAS DO ISS, PIS e COFINS) / 100]

Tributo	Item do ISS	Alíquota do Tributo	Valor do Tributo
ISS Cálculo do ISS: [(Subtotal 1 + Subtotal 2 + Subtotal 3) / **Coeficiente***] x Alíquota do ISS		5,00%	R$ 53.376,42
PIS Cálculo do PIS: [(Subtotal 1 + Subtotal 2 + Subtotal 3) / **Coeficiente***] x Alíquota do PIS		1,65%	R$ 17.614,22
COFINS Cálculo da COFINS: [(Subtotal 1 + Subtotal 2 + Subtotal 3) / **Coeficiente***] x Alíquota da COFINS		7,60%	R$ 81.132,16
Subtotal 4: Soma dos Tributos		14,25%	R$ 152.122,80
Soma dos subtotais (Subtotal 1 + Subtotal 2 + Subtotal 3 + Subtotal 4)			R$ 1.067.528,42

Hardware

Item	Descrição	Valor Total para a contratação
Item 1 - Appliance de segurança de Internet	UPGRADE DE APPLIANCE DE SEGURANÇA DE INTERNET MODELO MFE WEBGATEWAY 4500 APPL PARA MODELO MFE WEB GATEWAY 5500	R$ 176.600,00
Item 1 - Appliance de segurança de Internet	UPGRADE DE APPLIANCE DE SEGURANÇA DE INTERNET MODELO MFE WEBGATEWAY 4500 APPL PARA MODELO MFE WEB GATEWAY 5500	R$ 399.871,58
Subtotal 5: Soma do valor de Hardware **Observação**: O valor total para HARDWARE inclui os tributos PIS, COFINS e ICMS, totalizando o percentual de 18,25%		R$ 576.471,58
VALOR TOTAL DA PROPOSTA **(este valor deverá corresponder ao valor total para o período da contratação)** **(Soma do Subtotal 1 + Subtotal 2 + Subtotal 3 + Subtotal 4 + Subtotal 5)**		R$ 1.644.000,00

Figura 4 Continuação composição de custos da contratação que continha o IDPS em 2012 depois da licitação

Uma vez analisada a planilha com os custos da contratação em que houve a aquisição do IDPS em 2012, o próximo passo será extrair dela, os valores que possivelmente seriam obtidos com a aquisição somente do IDPS. far-se-á, então o ajuste em relação ao tempo de contrato para os itens que são sensíveis a isso. Na contratação de 2012 o tempo de contrato foi de apenas 24 meses, ao passo que nessa o tempo será de 48 meses. O banco de horas foi de 200 horas para todo o contrato, ao passo que nesta, será é de 300 horas.

Outro ajuste que precisa ser realizado, é com relação aos indicadores financeiros. Parte dos itens da contratação, têm seu valor diretamente ligado à variação do dólar, pois são produtos/serviços cotados diretamente na moeda americana e convertidos para Real no momento do fornecimento da proposta da licitante. Outros serviços, por se tratar de uma prestação realizada diretamente pelo fornecedor, terá seu reajuste pela diferença do IGP-M no período.

O valor médio do dólar em outubro de 2012 era de R$ 2,029 e em julho de 2020, R$ 5,280, o que é uma diferença de aproximadamente 160,2267%.

(Fonte: http://www.acinh.com.br/servicos/cotacao-dolar)

A diferença de IGPM no mesmo período foi de 59,8935%.

(Fonte: https://www3.bcb.gov.br/CALCIDADAO/publico/corrigirPorIndice.do?method=corrigirPorIndice)

Com isso, chega-se à seguinte tabela:

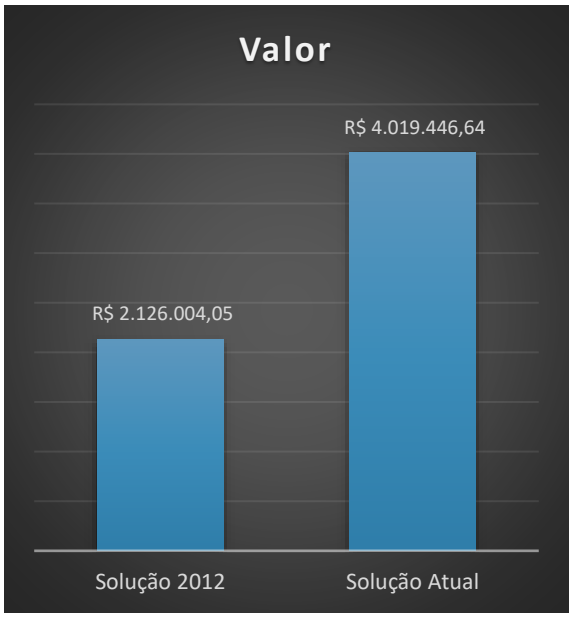
Item	Valor Encontrado	Fatores de Ajuste Financeiros	Fatores de Ajuste de Quantidade de Serviço	Resultado após ajustes
Appliances IDPS	R$ 399.871,58	Dolar (160,23%)	Não há	R$ 1.040.545,83
Licença para Gerência de IPS	R$ 15.000,00	Dolar (160,23%)	Ajuste de 24 para 48 meses.	R$ 78.066,00
Suporte Enterprise	R$ 129.900,00	Dolar (160,23%)	Ajuste de 24 para 48 meses.	R$ 676.051,56
Treinamento para 2 participantes	R$ 10.575,00	IGPM (59,8935%.)	Ajuste para 4 participantes	R$ 33.817,48
Suporte de Hardware	R$ 42.225,00	Dolar (160,23%)	Ajusde de 24 para 48 meses	R$ 219.755,79
Banco de Horas	R$ 18.014,00	IGPM (59,8935%.)	Ajuste de 200 para 300 horas.	R$ 43.204,82
Implantação	R$ 21.616,80	IGPM (59,8935%.)	Não há	R$ 34.562,58
			Total	**R$ 2.126.004,05**

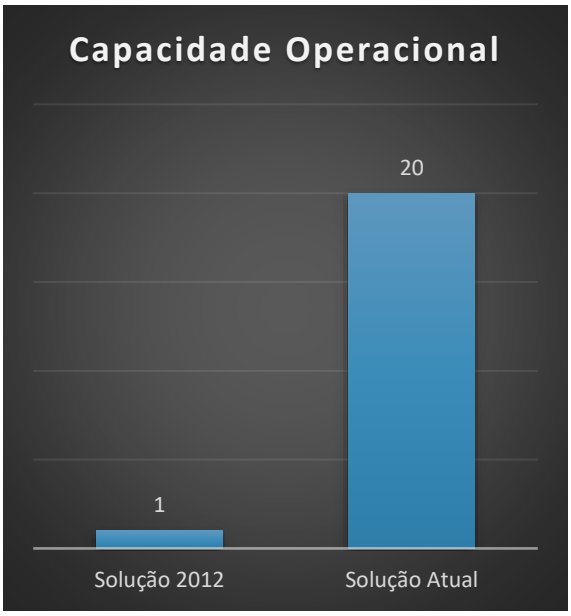
Tabela 1 Ajustes dos valores Referentes ao IDPS em 2012

Considerando os valores obtidos para a solução de IDPS, os índices de IGP-M e variação do dólar, chegou-se ao valor atualizado de R$ 2.126.004,05.

No entanto a solução que será adquirida possuirá uma capacidade de Throughput (vazão de operação) 20 vezes maior do que a solução adquirida em 2012. Possuirá uma capacidade de Análise de tráfego criptografado de 2000 Mbps contra 90 Mbps da solução da solução de 2012.

Analisando estes dados obtém-se a seguinte comparação:





REFERÊNCIAS

- https://www.checkpoint.com/advisories/ – Acesso realizado em 19 de agosto de 2020.
- Market Guide for Intrusion Detection and Prevention Systems - Published 1 July 2019 – ID G00385800 -Craig Lawson, John Watts
- Magic Quadrant for Intrusion Detection and Prevention Systems - Published: 10 January 2018 ID: G00324914 - Craig Lawson, Claudio Neiva
- https://www3.bcb.gov.br/CALCIDADAO/publico/exibirFormCorrecaoValores.do?method=exibirFormCorrecaoValores&aba=1 – Acesso realizado em 19 de agosto de 2020.
- https://www.websecurityworks.com/datasheets/ds_network_security_platform.pdf - Acesso realizado em 19 de agosto de 2020.
- Fonte: http://www.acinh.com.br/servicos/cotacao-dolar - Acesso realizado em 19 de agosto de 2020.