



TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS
AV. PRUDENTE DE MORAIS, 100 - Bairro CIDADE JARDIM - CEP 30380000 - Belo Horizonte - MG

ESTUDOS TÉCNICOS PRELIMINARES

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. CARACTERIZAÇÃO DA DEMANDA

I - Software de segurança e controle de acesso parametrizável para acesso VPN (Virtual Private Network), incluindo garantia e suporte técnico, de modo a se compatibilizar com os equipamentos e serviços correlatos em produção. A solução deve se integrar ao Global Protect do Palo Alto.

1.1. ALINHAMENTO ESTRATÉGICO

I - Objetivo estratégico 08 do PETRE - Aperfeiçoamento da Governança de Tecnologia da informação - Busca garantir os meios que viabilizem a definição, o planejamento, a priorização e a implantação de soluções tecnológicas que apoiem os processos essenciais do TRE-MG, os controles efetivos dos processos de segurança e de riscos, assim como os serviços voltados para a sociedade, com utilização eficiente de recursos.

II - Objetivo Estratégico 01 do PETIC - Aprimorar a gestão do relacionamento com clientes - Indicador 1 - Índice de satisfação dos serviços aos clientes de TIC: Os investimentos em infraestrutura estão sempre correlacionados de alguma maneira à melhoria de desempenho e/ou disponibilidade da rede, que reflete direta e positivamente no índice de satisfação dos clientes de TIC com os produtos, serviços e recursos (infraestrutura) oferecidos.

III - Objetivo Estratégico 03 do PETIC - Otimizar o uso dos recursos/ativos de TIC - Estruturar a tecnologia da informação e o seu gerenciamento a fim de garantir o desenvolvimento, aperfeiçoamento e a disponibilidade dos sistemas essenciais à execução das atividades judiciais e administrativas. Conhecer e estabelecer um processo responsável por manter as informações sobre os itens de configuração necessários para a entrega de serviços de TIC, incluindo seus relacionamentos - Indicador 6 - Percentual de ativos nos estágios do fim do ciclo de vida: Verificar a necessidade de aquisições e contratações tendo em vista as tendências de diminuição do parque, seja por alienação de bens inúteis, seja por vencimento

IV - Objetivo Estratégico 04 do PETIC - Implantar as determinações estabelecidas na Política de Segurança da Informação - Indicador 12 - Índice de disponibilidade de serviços definidos como essenciais: Garantir o acesso remoto seguro, por meio da tecnologia VPN, aos serviços definidos como essenciais no ambiente computacional do TRE-MG.

1.2. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

I - Com o triste advento da Pandemia da COVID-19 no primeiro trimestre de 2020 e, por conseguinte, a necessidade de isolamento da população para reduzir os riscos de contaminação, o modelo tradicional de trabalho que todos conhecemos passou por drásticas mudanças. Em maior ou menor grau, todos os países viram a necessidade de impor medidas de isolamento social. Dentre essas medidas, estão aquelas que proíbem o trânsito de pessoas em vários locais públicos e também aquelas que determinam o fechamento de escolas, do comércio, de indústrias e diversos outros setores, abrindo-se exceção apenas para os serviços essenciais como farmácias e supermercados por exemplo.

II - Em alinhamento com as orientações dos órgãos superiores e com as recomendações dos órgãos de saúde, o TRE-MG, através da Portaria Conjunta 30/2020 PRE, adotou as devidas medidas de isolamento social e estabeleceu que "O trabalho remoto deverá ser instituído pelos gestores, consideradas as disponibilidades operacionais e tecnológicas, além da necessidade de manutenção dos serviços."

III - A STI, da noite para o dia, foi conclamada a providenciar os meios necessários para permitir que esse contingente pudesse exercer suas atividades na segurança de seus lares. O acesso remoto nos moldes que foi demandado não existia como um serviço no portfólio da STI, uma vez que, via de regra, a política adotada é a de que se evite acessos remotos.

IV - Quando foi estabelecido o distanciamento social, as primeiras ações se voltaram a dar acesso remoto às equipes de TI, pois só assim outras ações poderiam ser conduzidas de forma segura sem que a equipe se expusesse aos riscos de contaminação. Posteriormente, foram sendo concedidos acessos a áreas estratégicas do TRE-MG e, com a evolução dos trabalhos, novos grupos de servidores foram sendo incluídos.

V - Hoje temos dois perfis de acesso que podem ser utilizados conforme a demanda:

a) Perfil 1 - Estação remota se conecta à estação do próprio usuário no TRE

1. O usuário fecha uma VPN com o TRE-MG e através dessa conexão acessa a própria estação de trabalho que permanece ligada em seu respectivo setor. Uma vez conectado, o servidor tem à sua disposição todas as ferramentas que está acostumado a trabalhar. Esse foi o perfil adotado para os profissionais de TI e para algumas áreas com necessidades específicas do tribunal.

b) Perfil 2 - Estação remota acessa uma área de trabalho virtual no servidor

1. O usuário fecha uma VPN com o TRE-MG e através dessa conexão se conecta a um servidor que tem o papel de simular para

cada usuário uma área de trabalho individual. Embora as aplicações mais comuns estejam presentes, algumas outras específicas de uso de determinado usuário pode estar ausente e também é necessária a organização da área de trabalho.

VI - A conexão ao ambiente de trabalho remoto é realizada por meio de:

- a) Computadores particulares - Esses usuários utilizam seus computadores pessoais para fechar a VPN e ganhar acesso à rede da Justiça Eleitoral.
- b) Computadores do TRE-MG - Nesse grupo estão os servidores que levaram para as suas residências os computadores que utilizavam no ambiente de trabalho. As principais motivações que ensejam a adoção dessa medida são:

1. O servidor não tem um desktop em casa;
2. O servidor tem um desktop em casa, mas não tem recursos de hardware/software suficientes para fornecer um ambiente de trabalho produtivo;
3. O servidor tem um desktop em casa que é compatível com as necessidades para trabalho remoto, mas precisa compartilhar seu uso com outros membros da família;
4. O servidor faz uso de aplicações que dependem de software de uso exclusivo da Justiça Eleitoral. Nesse grupo recaem todos os cartórios eleitorais e setores da Secretaria que acessam sistemas eleitorais. Esses sistemas rodam sob uma plataforma de software chamada SIS – Subsistema de Instalação e Segurança, a qual foi desenvolvida por uma empresa chamada Móduloque sob a contratação do TSE. Esse subsistema faz diversas alterações no computador que resultam em várias restrições de acesso. Devido a essas modificações, não é cabível sua instalação em um computador de uso pessoal.

VII - A proteção de rede do nosso ambiente é dependente, quase em sua totalidade, dos nossos firewalls. Temos dois firewalls configurados de forma redundante no modelo ativo/passivo.

VIII - No licenciamento do firewall está incluída uma ferramenta de VPN chamada Global Protect. A implantação de VPN com essa solução se iniciou durante o projeto Solução de ampliação do serviço VPN para utilização no PAIOL. Com ela foi possível que as estações de trabalho acessassem a nossa rede para a prestação de serviços ao eleitor em localidades fora do cartório eleitoral. À época, essa solução foi considerada a mais viável levando-se em consideração principalmente os fatores: custo, segurança e recursos já disponíveis. Essa solução esta sendo utilizada para atender as necessidades de trabalho remoto dos usuários no cenário pandêmico atual.

IX - O licenciamento a que temos direito da ferramenta Global Protect é o licenciamento gratuito e contempla apenas as funcionalidades básicas de túnel VPN.

X - Entretanto, quando se avalia os potenciais riscos de permitir que o computador do usuário acesse a rede da Justiça Eleitoral, mesmo com a utilização do túnel VPN, alguns pontos importantes devem ser trazidos à tona, tais como:

- a) Licenciamento original do Windows e dos softwares no computador do usuário, uma vez que softwares piratas geralmente ampliam bastante a probabilidade de existência de múltiplos tipos de malwares naquele computador;
- b) Atualização regular dos pacotes com correções e melhorias de segurança disponibilizado pelo fornecedor do Sistema Operacional e demais aplicativos;
- c) Existência de licenciamento de antivírus com serviço de atualização automática em vigor;
- d) O compartilhamento da estação de trabalho com outros membros da família e até com amigos.

XI - Diante desses riscos adicionais, foi necessário reforçar a segurança do acesso à VPN habilitando o uso da licença paga (em regime de avaliação por 90 dias) do Global Protect em nosso Firewall. Essa licença foi disponibilizada pelo fabricante e nessa versão o software cliente de VPN Global Protect faz várias validações adicionais de segurança no computador do usuário antes de permitir a conexão e, dessa forma, alguns dos riscos são bastante reduzidos.

XII - A partir do momento que se passa a permitir que um computador remoto tenha acesso à nossa rede, é de suma importância buscar atingir o mesmo nível de configuração e controle existentes nas estações de trabalho do TRE-MG, já que as boas práticas recomendam considerar esse computador remoto como um componente hostil.

XIII - Assim, na avaliação dos potenciais riscos de permitir que o computador do usuário acesse a rede da Justiça Eleitoral, mesmo com a utilização do túnel VPN, é importante buscar alternativas para que a estação de trabalho remota se aproxime ao máximo das características de um computador da Justiça Eleitoral.

XIV - Diante do cenário apresentado acima, faz-se necessária a aquisição de licença de software cliente para a criação de túneis VPNs com recursos de validação de segurança dos computadores dos usuários de forma a possibilitar o acesso remoto seguro ao ambiente computacional do TRE-MG necessário para a prestação dos serviços administrativos e eleitorais.

2. ESPECIFICAÇÃO DOS REQUISITOS

2.1. REQUISITOS DE NEGÓCIO

- I - Garantir os meios necessários para que os servidores em isolamento social possam continuar a exercer suas funções a partir de suas residências;
- II - Garantir o acesso aos recursos de Tecnologia da Informação para a prestação de serviços administrativos, judiciários e de atendimento ao público em geral;
- III - Prover acesso remoto aos usuários de serviços de TIC, acesso aos sistemas administrativos e corporativos utilizados pela Justiça Eleitoral (ELO, biometria, correio eletrônico, Internet, dentre outros) para o desempenho de suas funções;
- IV - Prover acesso de boa qualidade, com o melhor índice de segurança possível entre os computadores nas residências dos usuários e o ambiente computacional do TRE-MG suportando todos os serviços atuais e com possibilidade de expansão.

2.2. REQUISITOS DE CAPACITAÇÃO

- I - Para essa contratação, não haverá necessidade de capacitação técnica.

2.3. REQUISITOS AMBIENTAIS

- I - Para essa contratação, não há requisitos ambientais.

2.4. REQUISITOS DE SUSTENTABILIDADE AMBIENTAL

- I - Não se aplicam critérios de sustentabilidade ambiental para a presente aquisição.

2.5. REQUISITOS DE MANUTENÇÃO

- I - A ferramenta deve contar com atualizações regulares de segurança e versão durante todo o período de validade da licença;
- II - Todas as novas funcionalidades da ferramenta deverão ser fornecidas na solução adquirida enquanto vigorar o período de licenciamento sem a necessidade de aquisição complementar;
- III - Deverá ser disponibilizado portal para abertura e acompanhamento de chamados técnicos, sendo que durante a abertura deverá ser possível qualificar, direta ou indiretamente, a prioridade de atendimento necessária, a qual deverá possuir pelo menos três níveis em sua escala (baixa, média e alta criticidade);
- IV - O suporte técnico deverá ser fornecido pela própria fabricante/desenvolvedora da solução e não pelas empresas intermediárias que atuam comercializando a ferramenta.
- V - O suporte aos chamados deverá ser na modalidade 24/7 com atendimento inicial nos casos de alta criticidade em até 1 (uma) hora.

2.6. REQUISITOS TEMPORAIS

- I - As licenças aplicadas do Global Protect em regime experimental nos Firewalls possuem a validade de 90 dias e expirarão em 26 de agosto de 2020. Após este prazo, o acesso por meio de VPN permanece funcional, porém, recursos importantes configurados nessa versão deixarão de funcionar fragilizando a solução. Dessa forma, recomendamos que seja dada **TRAMITAÇÃO EM CARÁTER DE URGÊNCIA**, de forma a minimizar o período em que o ambiente operacional ficará descoberto pelas funcionalidades adicionais de segurança que apenas a versão paga da licença do Global Protect possui.

2.7. REQUISITOS DE SEGURANÇA

- I - A CONTRATADA deverá observar e respeitar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do TRE-MG, assim como as suas atualizações.
- II - Observância às diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações do TRE-MG, e demais normas sobre o assunto, no que couber, dentre elas e não exaustivas.

2.8. REQUISITOS TECNOLÓGICOS

- I - A solução deverá se integrar plenamente com o firewall Palo Alto PA-3020 em uso atualmente no nosso Datacenter de forma a não depender de outra aquisição que não essa da própria ferramenta;
- II - Deve permitir levantar, no mínimo, as seguintes informações a respeito do host remoto que deseja conectar à rede do TRE-MG:
 - a) Nome e endereço IP do host;
 - b) Sistema operacional
 - 1. Fabricante;
 - 2. Versão;
 - 3. Patches de segurança instalados;
 - c) Antivírus/Anti-spyware
 - 1. Fornecedor;
 - 2. Versão do software;
 - 3. Versão da vacina (atualização);
 - 4. Status operacional (ativo ou não);
 - 5. Proteção em tempo real (ativa ou não);
 - d) Firewall local
 - 1. Fabricante;
 - 2. Status operacional (ativo ou não);
- III - As informações levantadas pelo cliente de VPN devem ser compreensíveis pelo firewall Palo Alto 3020 permitindo nesse a criação de regras e perfis de forma a permitir a continuidade da conexão VPN ou não;
- IV - Deve permitir personalizar mensagens para informar ao usuário o motivo pelo qual a conexão VPN não foi efetuada (nos casos de não atendimento aos requisitos);
- V - Deve permitir redirecionar o usuário para uma área onde possa realizar a instalação de software complementar para atender aos

requisitos de conexão da VPN;

VI - Deve permitir bloquear IPv6;

VII - Deve permitir bloquear split tunneling;

VIII - Deve possibilitar a criação de regras de split tunneling para permitir que tráfegos específicos, em especial multimídia, possam ser acessados diretamente na Internet sem passar pelo túnel de VPN;

IX - Permitir a conexão de clientes rodando, no mínimo, Windows 7/10 e Linux – ambos em 64bits;

X - Possibilitar a configuração de mais de um gateway de conexão remota e que, caso a conexão não seja estabelecida com sucesso em um gateway o cliente VPN passe a tentar, de forma automática, a conexão nos demais gateways configurados;

XI - Deve permitir a atualização do cliente de VPN na estação de trabalho remota sem a necessidade de intervenção do usuário;

XII - Desejável que o cliente de VPN tenha funcionalidades de antivírus/ antimalware, com atualização regular de assinaturas e com gerenciamento centralizado;

XIII - Desejável que o cliente de VPN tenha funcionalidade de Firewall com gerenciamento centralizado de regras.

XIV - A licitante deverá apresentar, juntamente à proposta ajustada ao seu último lance, declaração ou documento da Palo Alto Networks que comprove estar autorizada a comercializar as licenças objeto deste certame. Tal exigência baseia-se na intenção de evitar que uma empresa arrematante seja declarada vencedora do certame, por ter oferecido o menor valor para os licenciamentos especificados, não venha a concluir o fornecimento assumido, justamente por falta da anuência/autorização da fabricante dos produtos (Palo Alto Networks), que pode se negar à arrematante a fornecer produtos, fato que levaria ao fracasso da licitação e certamente acarretaria prejuízos à este Tribunal e multas e demais penalidades à arrematante.

3. AVALIAR SOLUÇÕES

3.1. USO DA SOLUÇÃO DE FIREWALL DA PALO ALTO NO TRE-MG

I - Conforme já descrito, o TRE-MG possui um par de firewalls da marca Palo Alto Networks, modelo PA-3020, operando em HA (alta disponibilidade) no modo ativo/passivo e com licenciamento básico da solução de VPN Global Protect.

II - O *datasheet* desse equipamento indica que o mesmo suporta até 1.000 conexões de VPN simultâneas. Entretanto, esse valor se baseia no uso do equipamento com foco direcionado para essa funcionalidade específica, valor que não se atinge quando o firewall exerce vários papéis no ambiente, como no nosso caso.

III - O gráfico a seguir mostra o percentual de uso da capacidade de processamento do nosso firewall desde o início da pandemia:

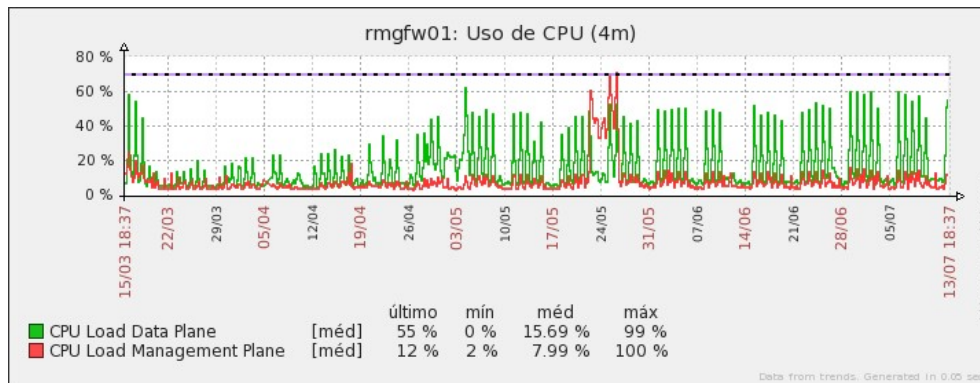


Figura 1 - Uso de processamento do firewall - 15/03/2020 a 13/07/2020

IV - Conforme se observa no gráfico da Figura 1, a utilização do nosso firewall está abaixo do limite de 80% recomendado pelo CNJ (CNJ, 2015). Embora com picos momentâneos de 99%, a média que pode ser visualizada está em torno dos 60%. Entretanto, considerando que a ferramenta de monitoramento Zabbix trabalha com médias acumuladas, estima-se que o comprometimento do firewall esteja entre 65% e 70%. A média descrita no gráfico (15,69%) não está sendo considerada, pois estão incluídos nos cálculos os períodos em que a utilização é pouco representativa.

V - Outra informação de interesse é o número de conexões simultâneas de VPNs, o qual pode ser obtido do gráfico na Figura 2, onde vemos que o número máximo de conexões simultâneas de túneis VPN é 558. Cabe observar que a coleta foi iniciada em 10/06/2020:

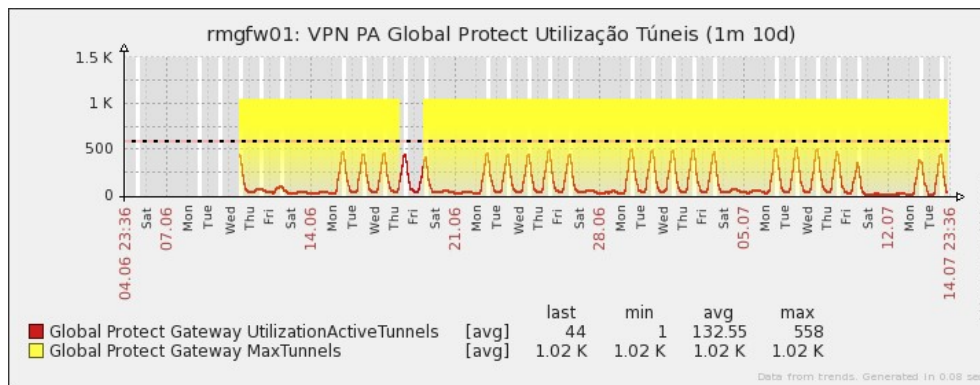


Figura 2 - Túneis ativos de VPN x Nº máximo de túneis

3.2. POSICIONAMENTO ESTRATÉGICO DA PALO ALTO

- I - Conforme pode ser visto na Figura 3, a qual traz a edição de 2019 do Quadrante Mágico do Gartner para Firewalls de Rede, a fabricante Palo Alto é a empresa melhor posicionada entre as quatro que ocupam o quadrante dos líderes.
- II - Embora todos os fabricantes estejam sujeitos a falhas, esse posicionamento da Palo Alto como líder no grupo dos líderes traz a segurança de que estamos sendo atendidos por uma empresa com tecnologia mundialmente reconhecida.



Figura 3 - Quadrante Mágico para Firewalls de Rede – Edição 2019

3.3. SOLUÇÃO DE VPN DA PALO ALTO - GLOBAL PROTECT

- I - Com a aquisição do nosso firewall Palo Alto veio o direito de uso da licença do software cliente de VPN chamado Global Protect.
- II - Entretanto, esse licenciamento não conta com algumas funcionalidades necessárias para a melhoria da segurança da conexão, como o gerenciamento de split tunneling e HIP Check.
- III - A Figura 4 abaixo faz um resumo das funcionalidades disponíveis e destaca aquelas que precisam de um contrato de subscrição para sua utilização.

FEATURE	SUBSCRIPTION REQUIRED?
Single external gateway (Windows and macOS)	—
Single or multiple internal gateways	—
Multiple external gateways	—
HIP Checks	✓
App for endpoints running Windows and macOS	—
Mobile app for endpoints running iOS, Android, Chrome OS, and Windows 10 UWP	✓
App for endpoints running Linux	✓
IPv6 for external gateways	✓
IPv6 for internal gateways (change to default behavior—starting with GlobalProtect app 4.1.3, a GlobalProtect subscription is not required for this use case)	—
Clientless VPN	✓
Split tunneling based on destination domain, client process, and video streaming application	✓

Figura 4 - Indicação de recursos ofertados apenas pela licença paga do GlobalProtect

3.4. SOLUÇÕES DE VPN DE OUTROS FABRICANTES

I - Tomando como base as quatro empresas líderes no quadrante mágico do Gartner, foi feito o levantamento das soluções de software cliente para VPN ofertadas por elas, conforme pode ser visto na Tabela 1.

EMPRESA	SOFTWARES CLIENTES VPN
Palo Alto	Global Protect
Fortinet	Forticlient
Cisco	AnyConnect VP Client
Check Point	Endpoint Security VPN, Check Point Mobile for Windows, SecuRemote

Tabela 1 - Clientes VPN das empresas líderes em firewall para rede

II - Em buscas na Internet e nos sites oficiais, foi possível apurar que todas as empresas listadas na Tabela 1 desenvolvem seus próprios softwares cliente para VPN que conversam especificamente com seus respectivos firewalls. Acredita-se que, dessa forma, conseguem extrair o máximo da integração de suas soluções, pois não há componentes de terceiros envolvidos.

3.5. DEPENDÊNCIA ENTRE AS SOLUÇÕES DE FIREWALL E CLIENTES VPN

I - Diante das informações levantadas, é possível concluir que adquirir uma solução de cliente VPN diferente do Global Protect, o qual já está em uso no nosso ambiente em sua versão completa na modalidade de avaliação, implica, necessariamente, na aquisição de novos firewalls.

3.6. AQUISIÇÃO DE NOVO FIREWALL PALO ALTO

I - Partindo do fato de que a troca da solução de VPN implica na troca do firewall, os primeiros levantamentos se voltaram à possibilidade de atualização do hardware atual por outro hardware do mesmo fabricante que suportasse um número maior que 1.000 conexões de VPN simultâneas e que já viesse com o cliente Global Protect completo.

II - Esse caminho, caso se apresentasse vantajoso, traria os benefícios de se manter o conhecimento e experiência já obtida na solução em vigor e reduzir consideravelmente os riscos de eventual troca de plataforma.

III - Há alguns anos, durante uma apresentação de estudos de caso para clientes da Palo Alto, realizada em Belo Horizonte, foi mencionada, de forma superficial, a possibilidade de troca do equipamento por outro superior com pagamento da eventual diferença.

IV - De posse dessa informação, foi solicitado à fabricante, através de sua revenda LDC SOLUÇÕES, mais detalhes dessa possível troca. Solicitamos também que fizesse a análise de qual equipamento seria necessário para o TRE-MG de forma a aumentar o número de conexões VPN e também, eventualmente, habilitarmos a funcionalidade de inspeção de tráfego criptografado, tarefa que hoje está prevista em outra solução existente no TRE-MG chamada BIG-IP, da empresa F5.

V - Juntamente com a análise, pedimos que viessem os respectivos orçamentos do hardware, licenças e suporte, incluindo também na solicitação os custos do modelo idêntico ao que temos hoje, de forma que fosse possível realizarmos as devidas comparações para o necessário entendimento da margem de desconto que nosso equipamento representaria na negociação.

VI - Inicialmente, a LDC informou que o procedimento de troca é chamado de *refreshing* e que estaria avaliando junto ao fabricante essa possibilidade. Passados quase trinta dias desde o pedido de orçamento, recebemos uma proposta com vários valores de equipamentos e licenciamentos. Por considerar alto os valores apresentados, questioneei à empresa representante se nos valores propostos já estava incluído o desconto pelo equipamento que entraria na base de troca. A empresa informou que a fabricante Palo Alto não está

mais fazendo essa operação de refreshing diretamente e que cabe às vendas a execução dessa modalidade por conta própria. Acrescentou ainda que eles não têm interesse, pois já têm dois equipamentos do mesmo modelo que o nosso.

VII - De acordo com o dimensionamento feito pela LDC, o equipamento que atenderia nossas necessidades seria o modelo PA-3250 da Palo Alto. Os custos para aquisição desse modelo e de todos os licenciamentos necessários estão compilados na Tabela 2.

FIREWALL PALO ALTO PA-3250	R\$	515.334,46
LICENCIAMENTO GLOBAL PROTECT	R\$	140.793,41
LICENCIAMENTO URL FILTERING	R\$	140.793,41
LICENCIAMENTO THREAT PREVENTION	R\$	140.793,41
SERVIÇO DE SUPORTE 24/7	R\$	278.715,94
SERVIÇO DE IMPLANTAÇÃO/CONFIGURAÇÃO:	R\$	29.100,00
TOTAL:	R\$	1.245.530,63

Tabela 2 - Orçamento do firewall Palo Alto PA-3250 com licenciamento e suporte por 3 anos

VIII - Para facilitar o entendimento do motivo de considerarmos altos os valores, foi realizado em 2015 o investimento de R\$ 357.700,00, para aquisição do nosso atual firewall Palo Alto PA-3020 com todas as características listadas na Tabela 2, à exceção do licenciamento do Global Protect, por um período de três anos. Já em 2018 foram renovados todos os serviços de licenciamento e suporte por mais três anos, ao custo de R\$ 177.810,00. Essa renovação é válida para o período de março/2019 a março/2022.

3.7. CENÁRIO ECONÔMICO

I - Infelizmente, uma das consequências financeiras de maior destaque da pandemia foi a rápida ascensão do dólar, o qual quebrou por diversas vezes o próprio recorde de cotação, conforme pode ser visto no gráfico dos últimos seis meses mostrado na Figura 5.



Figura 5 - Histórico de cotação do dólar – Apuração em 13/07/2020
Fonte: <https://economia.uol.com.br/cotacoes/cambio/dolar-comercial-estados-unidos/>

II - No gráfico, ainda é possível acompanhar a série histórica desde 2015 para entender o tamanho da oscilação da cotação causada pela pandemia.

3.8. AVALIAÇÃO DE OUTRAS SOLUÇÕES DE FIREWALL

I - O caminho natural ao se perceber a inviabilidade financeira de se adquirir outro firewall de maior porte do mesmo fornecedor do nosso equipamento atual seria a avaliação técnica e financeira de soluções de igual porte de outras empresas.

II - Entretanto, no atual cenário, essa diretiva não é apropriada e, para isso, é necessário entender o que o nosso firewall representa no nosso ambiente:

a) Papel crítico do firewall na rede da Justiça Eleitoral Mineira

1. O firewall Palo Alto PA-3020 é o coração da rede do TRE-MG e, dentre os principais papeis por ele desempenhados podemos destacar:

- Controle de todo o tráfego de rede que é permitido sair do TRE-MG em direção a outros regionais ou para a Internet;
- Controle de todo o tráfego oriundo de outros regionais ou da Internet em direção ao nosso ambiente externo;
- Roteamento entre todos os segmentos internos de rede – VLANs, em especial entre as redes de gerenciamento, de servidores e de zona desmilitarizada (DMZ);
- Emissão e controles de validade e revogação de todos os certificados digitais utilizados para o fechamento das conexões remotas via VPN;
- Emissão e controles de validade e revogação de todos os certificados digitais utilizados nas estações de trabalho;
- Filtro de URLs com o objetivo de permitir ou bloquear acessos à Internet baseado em categorias de assuntos (bloqueio de

assuntos ligados à pedofilia e sexo, por exemplo);

- Filtros de controle de tráfego no contexto de acesso remoto pelos usuários via VPN.

III - Para operar corretamente, foram configuradas várias regras que descrevem o que, quem, quando, de onde e para onde os tráfegos são permitidos. Além dessas regras, há inúmeras outras configurações realizadas e evoluídas ao longo do tempo no nosso ambiente.

IV - Dentre os controles de segurança efetuados pelo nosso firewall estão aqueles que dão acesso ao público externo aos sistemas SEI e Moodle.

V - A implantação do firewall levou aproximadamente seis meses para entrar em produção e somente quase dois anos depois é que foi possível capacitarmos dois profissionais ao custo total de R\$ 13.912,68. Hoje um deles está na SEGER e o outro na SEMOS. Cabe destacar que à época da implantação, estavam também sendo configurados nossos acessos à Internet de forma direta e independente do TSE. Além disso, ainda não havíamos realizado a segmentação da nossa rede em VLANs.

VI - Hoje, a complexidade do nosso ambiente é inúmeras vezes maior. Os profissionais estão frequentemente consultando a documentação técnica do fabricante para aprimoramento das configurações ou quando da necessidade de realizar uma atividade que ainda não tenham conhecimento.

VII - Uma simples configuração/alteração de regra feita incorretamente pode ocasionar a interrupção do acesso a todos os serviços de TIC ofertados pelo nosso regional e, dependendo da natureza da configuração, pode ser necessário se deslocar à sala-cofre do TRE-MG de posse de um notebook para acessar diretamente o firewall e realizar as ações para correção do problema.

3.9. RISCOS DA TROCA DE PLATAFORMA DE FIREWALL NESTE MOMENTO

I - A substituição de um firewall por outro de fornecedor diferente implica em nova capacitação, nova e demorada curva de aprendizado para solução de problemas, total reconfiguração da nossa rede dentro do novo dispositivo e, mesmo com o apoio de uma consultoria para implantação, colocaria em risco toda a arquitetura implantada de conectividade e acesso remoto, pois toda a configuração para trabalho remoto, tanto do lado do firewall quanto do lado do cliente (usuários remotos) teria que ser refeita.

II - Há ainda de se considerar o risco de que, por inexperiência na solução, uma configuração necessária deixe de ser feita e por esse motivo o TRE-MG venha sofrer um incidente de segurança da informação. Note que esse risco não deixa de existir na plataforma atual, entretanto, face ao longo período que o equipamento está em produção e com os devidos ajustes, a probabilidade é consideravelmente menor.

III - Considerando todos os aspectos críticos que uma eventual substituição de firewall envolve, há ainda outro fator de extrema importância que é o próprio processo de levantamento de requisitos e realização de POC – provas de conceito – para apoiar o respectivo ETP de forma a entender quais soluções atendem às demandas de segurança e disponibilidade necessária aos serviços essenciais do nosso regional. Estima-se que serão necessários pelo menos seis meses para que a equipe possa elaborar o ETP e o respectivo TR no momento em que houver indicadores de que precisamos efetivamente ampliar a capacidade do atual equipamento.

IV - Entendemos que, em algum momento no futuro, provavelmente será necessário trocarmos de solução, mas o objetivo é tentarmos conduzir os trabalhos de forma que isso aconteça em ambiente e situação mais favoráveis, estando presencialmente próximo a infraestrutura física e não sendo um ano eleitoral.

V - Assim, após a análise dos pontos discutidos, como o alto custo neste momento para troca de equipamento dentro do mesmo fabricante, a diretiva da nova gestão de se trabalhar o retorno gradual ao modelo presencial, os riscos envolvidos na troca de plataforma e a necessidade de manutenção do investimento já realizado, foi definido em reunião com a STI que não haveria a aquisição de firewall neste ano.

4. ESCOLHA DA SOLUÇÃO

4.1. DEFINIÇÃO PELA AQUISIÇÃO DA SOLUÇÃO GLOBAL PROTECT

I - Chegado o momento em que já haviam sido coletadas informações e dados suficientes durante os trabalhos no atual ETP, decidiu-se levar tais informações e considerações dos riscos envolvidos ao conhecimento da STI. A apresentação se deu em reunião havida em 26/06/2020 via plataforma de videoconferência Teams. A ata da reunião está presente no documento nº 0781666 do SEI.

II - Nessa reunião, foram apresentados os pontos levantados - alto custo neste momento para troca de equipamento dentro do mesmo fabricante, os riscos envolvidos na troca de plataforma e a necessidade de manutenção do investimento já realizado em tecnologia e pessoas.

III - A STI trouxe também a diretiva da nova gestão de se preparar para o retorno gradual ao modelo presencial e a intenção de não crescer o número de servidores em trabalho remoto que temos atualmente.

IV - Tendo os participantes deliberado, houve o entendimento comum quanto à inviabilidade técnica e financeira de trocarmos o firewall atual. Considerando que o uso da versão completa de avaliação da ferramenta Global Protect foi uma requisição do Núcleo de Segurança da Informação, os presentes também desconsideraram a possibilidade de que a mesma não fosse adquirida.

V - Assim, considerados todos os pontos levantados e riscos envolvidos entre as estratégias possíveis, ficou definido que não haveria a troca de firewall neste momento e, por conseguinte, a solução para melhoria da segurança da VPN a ser adquirida seria aquela atualmente em uso e já operacional, ou seja, o licenciamento da versão completa do Global Protect pelo período de 03 (três anos) para o nosso firewall PA-3020.

VI - O prazo de 03 (três) anos justifica-se pela obtenção da melhor relação custo-benefício quando comparado ao custo da solução por períodos inferiores e ainda, pela necessidade de dar continuidade ao acesso remoto via VPN, com maior segurança, para os Postos Itinerantes de Atendimento ao Eleitor (PAIOLs) e para os magistrados e servidores quando necessário, mesmo após estabelecida como controlada a situação Pandêmica que atravessa o País.

VII - A garantia e suporte técnico do produto, como praxe de mercado para a venda de subscrição, devem contemplar a permissão de uso, a permissão de atualizações conforme novas versões do software forem liberadas e a permissão para abertura de suporte técnico junto ao fabricante. O suporte deverá ser na modalidade 24/7 com atendimento inicial nos casos de alta criticidade em até 1 (uma) hora.

5. INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

I - Não se aplica para essa contratação.

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO**6. RECURSOS MATERIAIS E HUMANOS**

I - Os aspectos técnicos e funcionais da contratação serão fiscalizados por servidores da Seção de Infraestrutura e Redes - SEGER, não sendo necessária a contratação de serviço ou mão-de-obra adicional.

7. DEFINIR ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DO CONTRATO

I - Não se aplica para essa contratação.

8. ELABORAR ESTRATÉGIA DE INDEPENDÊNCIA

I - A Solução não cria dependência tecnológica em relação ao fornecedor, muito embora seja necessário um prazo considerável para se decidir por sua substituição. Recomenda-se iniciar o processo de recontração (nova licitação) com antecedência mínima de 6 (seis) meses antes do prazo final do contrato.

ANÁLISE DE RISCOS**9. RELAÇÃO DOS POSSÍVEIS RISCOS**

I - Apresentados conforme documento anexo Mapa de Risco - Nº 0867082.

Assinaturas da Equipe de Planejamento da Contratação	
Ricardo Resende Costa Integrante Técnico (Titular)	Gustavo Oliveira Heitmann Integrante Administrativo
Rodrigo Heringer de Salles Integrante Técnico (Suplente)	
Wellerson Rubens de Amarante Integrante Demandante	
Data: ____/____/____	

ANEXO A**LISTA DE POTENCIAIS FORNECEDORES**

	Fornecedor
1	Nome: LDC Soluções Site: www.ldc.com.br Telefone: (31) 31 3516-1998/31 998123868 / 31 991254635 E-mail: ulisses@ldc.com.br , taciana@ldc.com.br , comercial@ldc.com.br Contato(s): Ulisses, Taciana
2	Nome: TELTEC Solutions Site: www.teltecsolutions.com.br Telefone: (48) 3031-3450/(51) 99967-9839 E-mail: rsalvo@teltecsolutions.com.br / pamela@teltecsolutions.com.br Contato(s): Rodrigo Salvo, Pâmela Radunz
3	
4	

ANEXO B**CONTRATAÇÕES PÚBLICAS SIMILARES**

1. Centro integrado de Telemática do Exército, Pregão Eletrônico Nº 07/2020 - CITEEx - UASG: 160091.
2. Tribunal de Contas do Estado do Piauí, Pregão Eletrônico Nº 13/2020.
3. Tribunal de Contas do Estado do Rio de Janeiro, Pregão Eletrônico Nº 68/2018.

ANEXO C

MEMÓRIAS DE CÁLCULOS

PRODUTO	VENDEDOR	PART NUMBER	PREÇO EM REAL (R\$)	QUANTIDADE	TOTAL
Licença Global Protect (para 03 anos)	LDC Soluções	PAN-PA-3020-GP-3YR-HA2	R\$41.985,40	2	R\$83.970,80
Licença Global Protect (para 01 ano.) Obs: A empresa Teltec orçou a licença com suporte e garantia para 01 ano e ao ser questionada por email, informou que para estimativa do valor para 03 (três) anos, bastaria multiplicar por 03 (três) o valor do orçamento encaminhado.	TELTEC Solutions	PAN-PA-3020-GP-HA2	R\$25.900,00	6	R\$155.400,00
Obs 2: Consideramos o orçamento da empresa TELTEC exorbitante para apoiar no cálculo da média.					



Documento assinado eletronicamente por **ROBERTO DE CARTÉIA PRADO, Chefe de Seção**, em 27/08/2020, às 13:11, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **GUSTAVO OLIVEIRA HEITMANN, Técnico Judiciário**, em 27/08/2020, às 13:33, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade deste documento pode ser conferida no site https://sei.tre-mg.jus.br/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **0874568** e o código CRC **FD7DB976**.