ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ESTUDOS TÉCNICOS PRELIMINARES - ETP

CÓDIGO PAC 2024: TJCESETIN_2024_031

AQSETIN2022020 - Soluções de Segurança – Firewall de grande porte

1. INTRODUÇÃO

Este documento tem como finalidade de identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

Identificação das necessidades de negócio
1. Solução alinhada com principais objetivos e padrões de referência internacional para a gestão da Segurança da informação. 2. Proteger sistemas e dados sensíveis da organização. 3. Promover a confidencialidade, integridade, disponibilidade, autenticidade e privacidade dos dados e sistemas institucionais. 4. Continuidade dos negócios com soluções robustas, performáticas e estáveis, auxiliando na manutenção da disponibilidade das atividades institucionais. 5. Defesa, controle e mitigação de ameaças digitais e reduzindo riscos que podem impactar diretamente nas estratégias do negócio. 6. Aprimoramento das políticas de segurança e ferramentas de segurança da informação. 7. Modernização da infraestrutura tecnológica, ampliação da capacidade de armazenamento e de processamento do ambiente de segurança. 8. Soluções de conexão remota segura para localidades e funcionários remotos. 9. Capaz de fornecer uma abordagem integrada e ampla para detectar, investigar e responder a ameaças externas, cibernéticas e ataques zero-day. 10. Ampliar a largura de banda da rede 11. Monitoramento para identifique possíveis ameaças, comportamentos suspeitos ou uso indevido da rede. 12. Agentes de coleta e análise de dados.

13. Orquestração e automação de tarefas de configuração.
14. Revisão de registros e eventos gerados pelos usuários, sistemas e aplicativos.
15. Capacidade de armazenar e coletar evidências para processos de investigação de incidentes de segurança.
16. Controle de acesso a determinados recursos, aplicativos ou sites da web, com base em políticas pré-definidas.
17. Reduzir riscos que podem impactar diretamente nas estratégias do negócio.

Identificação das necessidades tecnológicas

1. Utilizar estratégia de proteção em camadas de segurança. Esta estratégia consiste em criar várias camadas de proteções distintas e complementares, sendo cada camada atuando de forma especializada em algum componente de segurança.
2. Regular, analisar e determinar quais operações de transmissão ou recepção de dados podem ser executadas a partir de um conjunto de regras ou instruções, inspecionando, controlando e bloqueando o tráfego proveniente da Internet para os sistemas e serviços.
3. Aplicar políticas e restrições de acessos inter-redes.
4. Controlar os acessos dos usuários internos para a Internet.
5. Bloquear o tráfego de dados indesejado e liberar acessos impedindo a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.
6. Atuar simultaneamente na proteção do ambiente de servidores (perímetros) e na proteção borda de acesso à Internet, criando sistemas virtuais para isolar distintos segmentos da rede.
7. Manutenção e controle do tráfego de rede.
8. Filtrar o conteúdo da Web.
9. Garantir que apenas navegadores web e clientes de e-mail suportados possam ser executados na organização, idealmente utilizando apenas a versão mais recente disponibilizada pelo fabricante.
10. Desinstalar ou desabilitar plug-ins ou aplicações add-on não autorizados para navegadores web e clientes de e-mail.
11. Utilizar filtros de URL baseados em rede de forma a limitar a possibilidade de sistemas se conectarem a websites não aprovados pela organização. Tais filtros devem ser impostos a todos os sistemas da organização, quer se encontrem dentro do espaço físico da organização, quer não.
12. Subscrever serviços de categorização de URLs de forma a garantir que o filtro esteja atualizado com base nas mais recentes definições de categorias de sítios eletrônicos disponíveis. Sites não categorizados devem ser bloqueados por padrão.
13. Realizar registros de log de todas as requisições a URLs a partir de cada um dos sistemas da organização, quer nas dependências corporativas, quer em dispositivos móveis, de forma a identificar potenciais atividades maliciosas e auxiliar operadores de incidentes com a identificação de sistemas potencialmente comprometidos.
14. Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.
15. Prevenção da rede interna contra ameaças cibernéticas digitais.
16. Análise preventiva a incidentes de segurança: prevenção, detecção e resposta a incidentes baseadas nos eventos gerados pelo firewall.
17. Coleta e tratamento de dados relacionados à segurança.
18. Filtrar os dados.

19. Estabelecimento de canal de comunicação seguro através da VPN.
20. Aumento da confidencialidade, integridade e disponibilidade das informações.
21. Aumento da proteção da rede interna contra possíveis tentativas de acesso indevido.
22. Implementação de mecanismos de proteção, prevenção de intrusão.
23. Implementação de regras de segurança, além de proteção específica em nível de aplicações como correio eletrônico, servidores WEB.
24. Melhoria da qualidade dos serviços, da proteção das informações da instituição e da produtividade dos usuários.
25. Capacitação e qualificação da equipe.
26. Manter a estabilidade, confiabilidade e proteção do tráfego de perímetro e da borda de acesso à Internet, através da renovação da solução atual que está em pleno funcionado e das expansões de segurança pretendidas.
27. Introduzir o conceito de Zero Trust na arquitetura de segurança do TJCE, permitindo que o Tribunal esteja atualizado com as melhores práticas e referências do mercado no quesito segurança da informação.
28. Além disso, está contratação oferece recursos para aperfeiçoar o monitoramento, controle, penalização e bloqueio de bots (robôs) que utilizam recursos em excesso da infraestrutura de TI e aplicações do TJCE na Internet, muitas vezes até causando depreciação da performance dos sistemas e causando indisponibilidade nos serviços.
29. Prevenir, detectar e responder a incidentes baseadas nos eventos gerados pelo firewall.
30. Localizar anomalias dentro do ambiente com o uso de inteligência artificial e aprendizado de máquina
31. Aumentar o nível de resposta e detecção de incidentes
32. Bloquear ameaças desconhecidas com análises comportamentais
33. Dispor de equipamentos e soluções com novas tecnologias e recursos.
34. Prover alta disponibilidade nos equipamentos e mecanismos que são a base para proteção contra-ataques cibernéticos dentro da infraestrutura do TJCE.
35. Garantir o nível de suporte técnico necessário para atender um ambiente corporativo complexo e robusto.
36. Aperfeiçoar a detecção e respostas a ameaças cibernéticas no ambiente do TJCE.
37. Suporte a solução a ser adquirida.
38. Obter suporte adequado do fabricante quando da necessidade de aperfeiçoamento, melhores práticas, dúvidas de utilização e resolução de problemas.
39. Indicação dos resultados esperados com a contratação.
40. Continuidade ao suporte apropriado para este porte crítico de segurança da informação de hardware/software, bem como upgrade de hardware e licenciamento, além do aperfeiçoamento de proteções dos dados das aplicações do TJCE

Demais requisitos necessários e suficientes à escolha da solução de TIC

1. Todos os equipamentos, acessórios e softwares deverão possuir garantia do fabricante, do tipo 24x7x4, disponível 24 (vinte e quatro) horas por dia, durante os 07 (sete) dias na semana, pelo período de, no mínimo, 60 (sessenta) meses, contados a partir da data de assinatura do termo de recebimento definitivo, com quantitativo ilimitado de requisições de chamados, podendo o atendimento ser presencial (on-site) ou remoto, quando requisitado pelo CON-

TATANTE. Deverá compreender toda e qualquer configuração, instalação de atualizações, patches e fixes de software. A escolha do prazo de garantia 24x7x4 para todos os equipamentos, acessórios e softwares decorre da necessidade de assegurar a continuidade operacional dos sistemas essenciais ao funcionamento do contratante. Em algumas situações, intervenções físicas nos equipamentos podem ser necessárias e indispensáveis para resolver questões técnicas complexas incluindo ações e intervenções manuais por equipe técnica da empresa contratada e/ou da fabricante. Dessa forma, a abrangência do suporte, tanto presencial quanto remoto, se justifica pela natureza variada das demandas de manutenção e pela urgência em solucioná-las, garantindo a eficiência e a disponibilidade contínua dos recursos tecnológicos essenciais para as atividades do contratante.

2. Para a cobertura 24x7x4, entende-se que será substituição avançada de peças, com ou sem engenheiro de campo, onde as peças serão entregues dentro de quatro horas da determinação de que a peça a ser substituída é realmente necessária (24 horas por dia, 7 dias por semana). A exigência de entrega de peças em um prazo tão restrito como 04h (quatro horas) para a cobertura 24x7x4 se justifica pela criticidade do equipamento em questão e seu papel central no suporte às operações fundamentais do Tribunal de Justiça. Como mencionado, os equipamentos em questão sustentam outras soluções críticas do TJ, cuja disponibilidade contínua é vital para a eficiência e funcionamento adequado do ambiente de TI como um todo. Qualquer interrupção ou falha nesse equipamento pode ter um impacto significativo e imediato nas operações do tribunal, resultando em atrasos, ineficiências ou até mesmo paralisações de serviços essenciais. Portanto, a necessidade de uma reposição rápida de peças é fundamental para garantir a continuidade operacional e minimizar qualquer potencial prejuízo decorrente de falhas ou problemas técnicos.
3. A CONTRATADA será responsável pela execução da garantia contratual;
4. Os chamados referentes a problemas nos equipamentos, partes, componentes e softwares, seja reparação ou garantia, deverão ser abertos diretamente com a CONTRATADA e gerenciados pela mesma através de número telefônico 0800 ou equivalente a ligação gratuita ou por web site da CONTRATADA, fornecendo neste momento o número, data e hora de abertura do chamado. A data e a hora do registro do chamado serão consideradas o início para contagem dos prazos estabelecidos;
5. O acesso à área restrita de suporte para abertura de chamados em endereço eletrônico (web site) ou por telefone, deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
6. A CONTRATADA utilizará apenas peças e componentes novos e originais salvo nos casos fundamentados por escrito e aceitos pelo TJCE;
7. Na impossibilidade de solução definitiva do problema, obriga-se a CONTRATADA a disponibilizar para uso imediato, nas instalações do TJCE, outros equipamentos peças ou componentes e softwares de características iguais e/ou superiores ao que está sendo objeto da renovação da garantia, sem qualquer ônus ao TJCE;
8. Todo atendimento deverá ser acompanhado de relatório técnico detalhado, que explicite o diagnóstico e a solução implementada;
9. Para a correção de erros ou falhas, a CONTRATADA deverá utilizar apenas peças e componentes novos, de primeiro uso e originais do fabricante dos equipamentos, ou homologadas pelo mesmo. Caso haja a descontinuidade de fabricação dos componentes, deverá ser garan-

tida a total compatibilidade dos itens substituídos com os originalmente fornecidos.

10. O direito de posse e propriedade de todos os artefatos e produtos elaborados pela empresa fornecedora da Solução de Tecnologia da Informação em decorrência do CONTRATO é do Tribunal de Justiça do Estado do Ceará, sendo vedada sua cessão, locação ou venda a terceiros;
11. Todas as informações obtidas ou extraídas pela empresa fornecedora da Solução de Tecnologia da Informação quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo ela zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.
12. A obrigação assumida de Confidencialidade permanecerá válida durante e após o período de vigência contratual;
13. As obrigações e conhecimentos sobre os requisitos de segurança serão ratificados pelo TJCE e a empresa fornecedora da solução de TI em documentos posteriores.
14. A entrega dos equipamentos deverá ocorrer em, no máximo, 30 (trinta) dias corridos após a data de emissão da ordem de fornecimento pela Contratante.

3. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

3.1. O Poder Judiciário Cearense com o intuito de prover a segurança de rede e controlar os acessos à internet, protegendo contra possíveis tentativas de acesso indevido adquiriu através do contrato CT Nº 17/2018, celebrado com a empresa Teltec Solutiona Ltda, uma solução segurança de rede (Firewall) composta por:

3.1.1. 01 (uma)Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220 composta por 02 (dois) Firewalls de Próxima Geração;

3.1.2. 01 (uma) Garantia da Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220 com Suporte Oficial Palo Alto Networks 24x7 fornecido no Brasil em Português por ASC (Authorized Support Center) e com serviço de suporte técnico remoto por 60 meses;

3.1.3. 02 (duas Assinatura Threat prevention para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220;

3.1.4. 02 (duas) Assinatura URL filtering para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220;

3.1.5. 02 (duas) Assinatura WildFire para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220;

3.1.6. (dois) Módulos de Interface 1000BASE-T;

3.1.7. 14 (quatrorze) Módulos de interface 10GBASE-SR;

3.1.8. 01 (um) Software Panorama para Gerenciamento Palo Alto Networks Panorama para Solução de Plataforma de Segurança em cluster Palo Alto Networks PA-5220; e

3.1.9. 01 (uma) Garantia do Software para Gerenciamento Palo Alto Networks Panorama com Suporte Oficial Palo Alto Networks 24x7 fornecido no Brasil em Português por ASC (Authorized Support Center) por 60 meses.

3.2. A solução atual possui as seguintes características de desempenho e capacidades:

Taxa de transferência de firewall	15,2 Gbps
Taxa de transferência do Threat Prevention	7,7 Gbps
Taxa de transferência da VPN IPsec	9,7 Gbps
Máximo de sessões	4 M
Máximo de Sistemas virtuais	20
MTBF	9,23 anos
Fontes de alimentação	2
Armazenamento	240GB SSD

3.3. A solução atual possui a seguinte topologia lógica que interconecta diversas zonas:

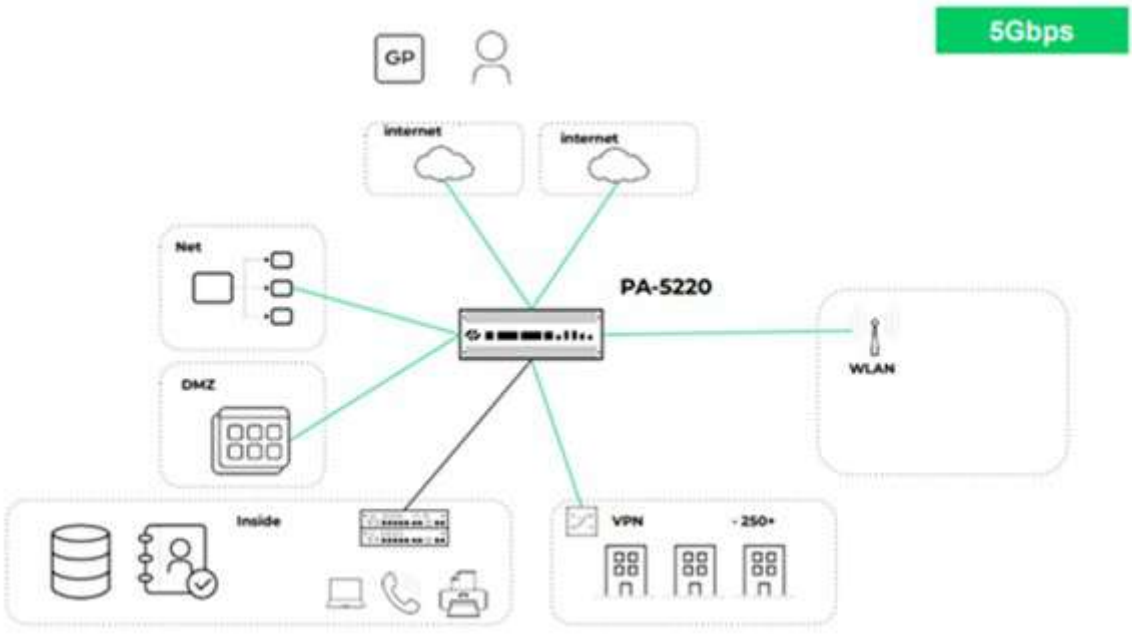


Figura 1 - Topologia Lógica Atual

3.4. A solução atual utiliza das seguintes funcionalidades do disposto:

FUNCIONALIDADES	OCUPAÇÃO ATUAL
Throughput – Tráfego total no equipamento (Valor máximo em Mbps nos últimos 30 dias)	5.000
SSL – Perfil de Tráfego total SSL no equipamento (Percentual dos últimos 90 dias)	31%
Tráfego criptografado em relação ao total SSL recebido (Percentual dos últimos 90 dias)	67%
Número de sessões/conexões simultâneas (Valor máximo em Mbps nos últimos 30 dias)	250.000
Número de novas sessões por segundo (Valor máximo nos últimos 30 dias)	5.000
VPNs Client-to-Site	5500
VPN Site-to-Site	260
Interfaces 10Gb SFP+	10
Zonas	28
Regras de NAT	238
Número de Rotas	591
Vlans	22
Regras de segurança	1042
Regras de Descriptografia	161

3.5. A infraestrutura mencionada é utilizada pelo Judiciário Cearense sendo formada por equipamentos, subscrições de softwares e software de gerência, que compõem a solução de perímetro de segurança da informação que provê, além da segurança, a integridade dos dados trafegados entre os serviços Judiciais e Administrativos, através de uma rede de dados.

3.6. A proteção de perímetro é uma abordagem que visa, proteger por meio de medidas de segurança, os limites do ambiente externo e interno. Embora seja a proteção essencial para bloquear e filtrar o tráfego externo indesejado, ela tem suas limitações, uma vez que não aborda as ameaças internas. A abordagem que se concentra na proteção o tráfego que ocorre dentro do data center está relacionada a proteção Leste-Oeste, que garante a segurança dos sistemas, a segregação de redes e a prevenção de ataques internos. Ambas as abordagens são complementares, uma vez que a proteção de perímetro cuida do tráfego de entrada e saída, enquanto a proteção Leste-Oeste se concentra na comunicação interna, criando uma

defesa mais completa e abrangente para o ambiente de TI da organização.

3.7. Ao implementar camadas de proteção adicional, existe a necessidade de mapear todos os fluxos envolvidos na comunicação interna. O serviço de desenho da solução desempenha um papel fundamental na implementação eficiente e segura desse tipo de solução em data centers, garantindo que a infraestrutura seja projetada de forma adequada e considerando os requisitos específicos do ambiente e do cliente. Dentro desse serviço, a proteção do tráfego Leste-Oeste é de extrema importância, pois visa assegurar a segurança e a integridade dos dados sensíveis transmitidos entre servidores e recursos dentro do data center. As medidas visam assegurar segmentação de rede, controles de acesso, prevenir ameaças internas, garantir a confidencialidade dos dados e cumprir requisitos regulatórios, proporcionando um ambiente mais seguro e confiável para a organização.

3.8. A nova topologia lógica proposta engloba a proteção dos diversos tipos de comunicação interna e externa, demanda um aumento de processamento e Throughput em mais 10Gbps por meio da construção de novas zonas. Além disso, é importante ressaltar o aumento da velocidade dos links de acesso no Cinturão Digital do Ceará - CDC e o crescimento de 35% na Força Total de Trabalho de Magistrados, Servidores e auxiliares nos últimos 5 anos, possuem um impacto no planejamento, expansão da rede e projeção de tráfego futuro.

3.9. A solução proposta possui a seguinte topologia lógica que interconecta diversas zonas:

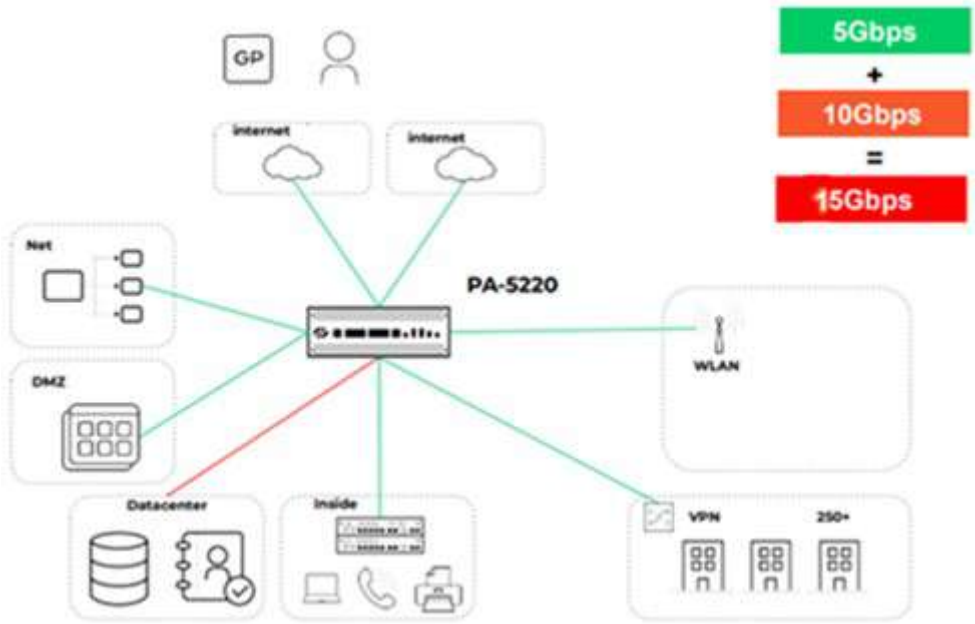


Figura 2 - Topologia Lógica Proposta criando uma zona datacenter

3.10. Com base nas medições realizadas no firewall atual, foi constatado um tráfego total de 5 Gbps. Levando em consideração as especificações do fabricante, o PA-5220 apresenta

uma capacidade de processamento de Threat Prevention limitada a 7,1 Gbps. Portanto, o tráfego atual corresponde a 70% da capacidade máxima da plataforma. É importante ressaltar que a intenção de agregar o tráfego de outras zonas indica que o hardware atingiria sua capacidade máxima, o gráfico abaixo mostra como a caixa atual impossibilita futuras expansões ou o suporte ao crescimento orgânico da infraestrutura.

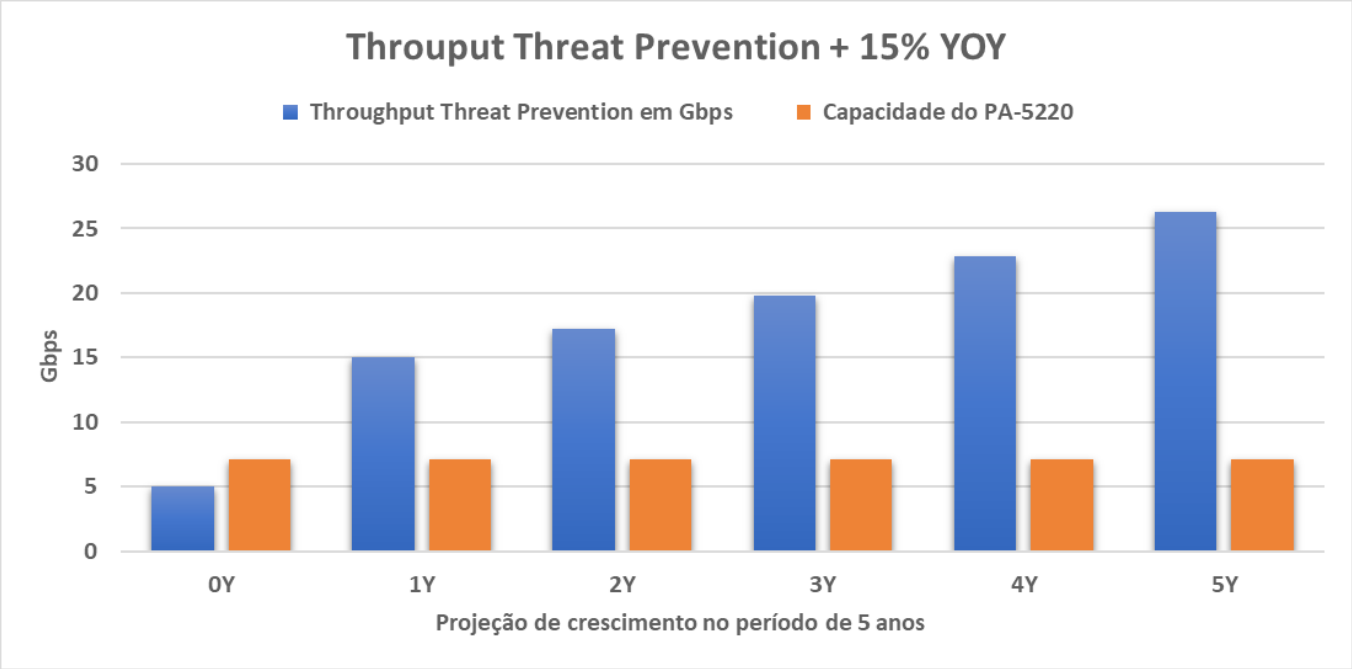
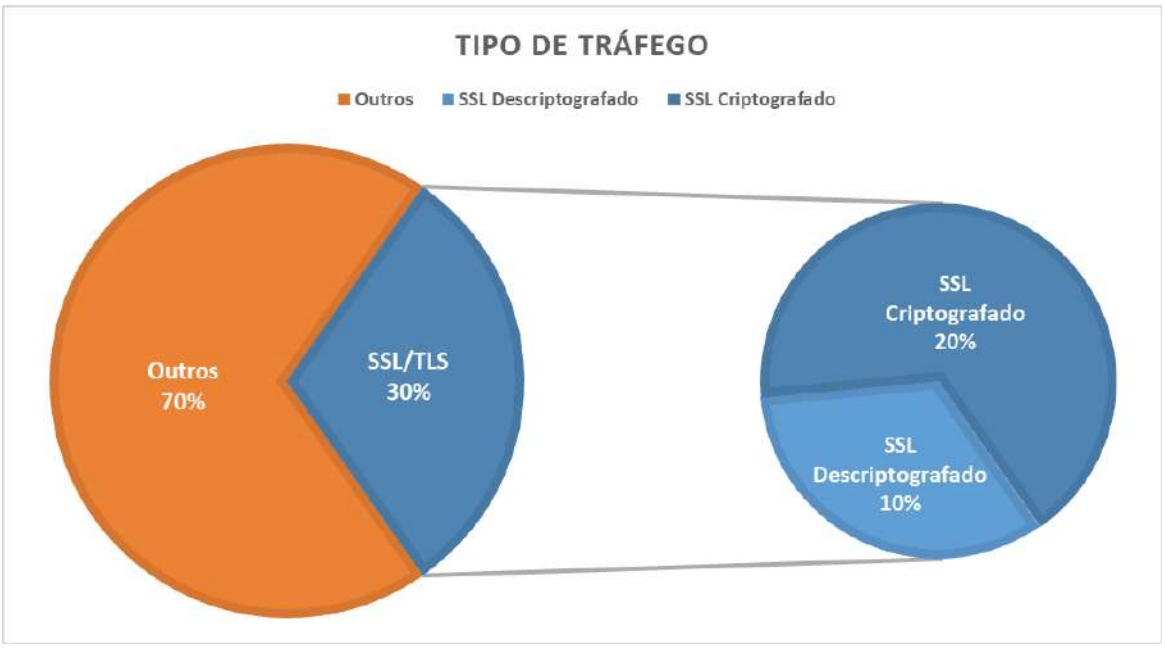


Figura 3 - Limitação do Threat Prevention com o PA-5220

3.11. O SSL decryption é uma funcionalidade crucial, desempenhando um papel de extrema importância, já que consiste em permitir a inspeção e análise do tráfego criptografado que atravessa o firewall. É válido ressaltar que o tráfego do tipo SSL representa 30% do total processado pelo equipamento, porém, apenas 33% desse valor é decodificado. Como resultado, os outros 67% não podem ser inspecionados, o que equivale a 20% do tráfego



total.

Figura 4 - Tipo de Tráfego geral e SSL no firewall

3.12. Com base nas medições realizadas no firewall atual, foi constatado um tráfego total de 5 Gbps. Levando em consideração que 30% é SSL/TLS e segundo as especificações do fabricante, o PA-5220 apresenta uma capacidade para o processamento de SSL decryption limitado em 3,5 Gbps. Portanto, adotar medidas mais seguras e tentar inspecionar todo o tráfego criptografado do equipamento, assim como agregar mais funções de inspeção ficam comprometidas com a especificação atual de capacidade máxima da plataforma

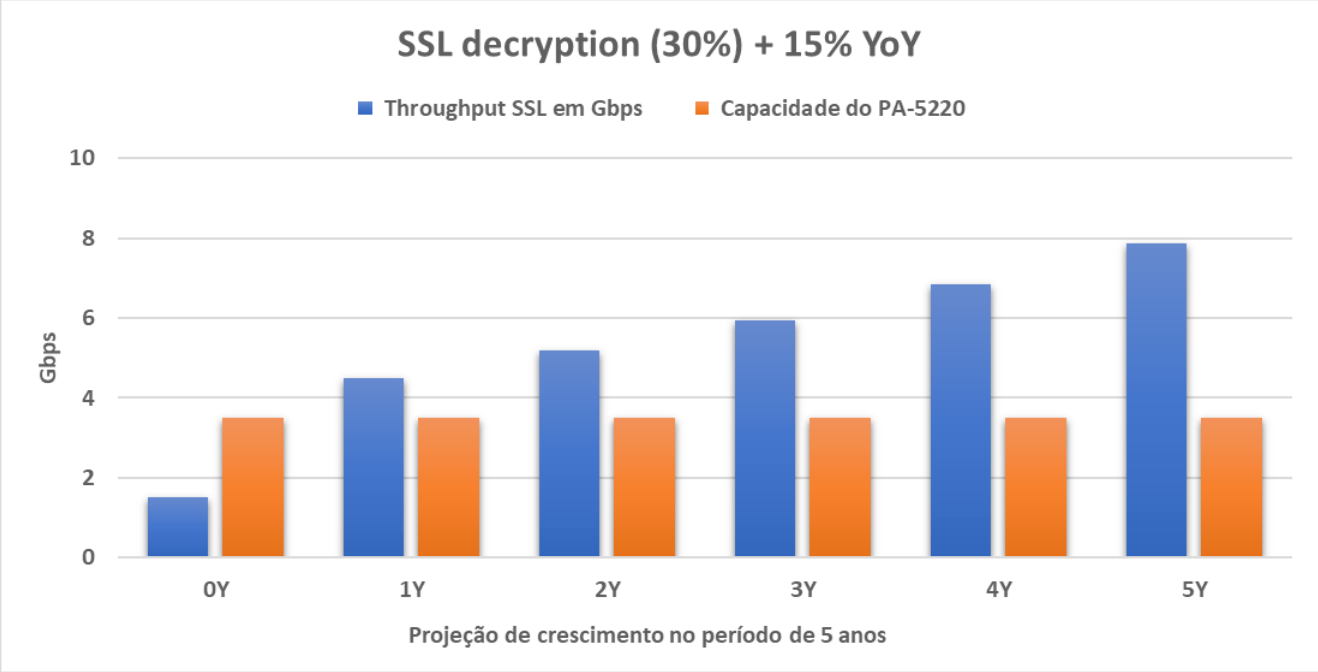


Figura 5 - Limitação do SSL decryption com o PA-5220

3.13. Com base nos números demonstrados da ocupação atual dos recursos de hardware e funcionalidades do sistema atual, na expansão da rede e projeção de tráfego futuro, a aquisição de novos equipamentos deve ter os requisitos de funcionalidades baseado nos seguintes requerimentos de especificações de acordo com a tabela abaixo, visando equilibrar o custo e o benefício de equipamentos de Firewall Next Generation:

ESPECIFICAÇÕES MÍNIMAS	
Taxa de transferência do Threat Prevention	26 Gbps
Taxa de transferência da VPN IPsec	20 Gbps

Taxa de transferência de Inspeção SSL	7 Gbps
Sessões	3,5 Milhões
Novas sessões por segundo	250 mil
Sistemas virtuais	10
Fontes de alimentação	2
Armazenamento	480GB SSD
Interfaces 1G/2.5G/5G/10G	08
Interfaces 1G/10G SFP/SFP+	12
Interfaces 40G/100G QSFP+/QSFP28	04

3.14. Ao realizar uma análise comparativa entre as especificações do estudo técnico preliminar e os principais fabricantes de equipamentos NGFW, de acordo com o quadrante de líderes do Gartner, identificamos equipamentos potenciais que atendem aos requisitos mínimos de recursos de hardware e funcionalidades.

ESPECIFICAÇÕES MÍNIMAS		**ESPECIFICAÇÕES DOS PRINCIPAIS FABRICANTES**					
Taxa de transferência do Threat Prevention	26 Gbps	**26**	**32**	**24**	**30**	**25**	**33**
Taxa de transferência da VPN IPsec	20 Gbps	21	28,7	40	49	55	105
Taxa de transferência de inspeção SSL	7 Gbps	*	*	*	*	20	29
Sessões	3,5 Milhões	3,6	5	10	10	24	70
Novas sessões por segundo	250 Mil	270	370	550	615	1000	870
Sistemas virtuais	10	10	15	125	125	10	10
Fontes de alimentação	2	2	2	2	2	2	2
Armazenamento	480GB	480	480	480	480	1Tb	1Tb
Interfaces 1G/2.5G/5G/10G - RJ45	16	8	8	10	10	16	16
Interfaces 1G/10G SFP/SFP+	12	12	12	12	12	16	16
Interfaces 40G/100G QSFP+/QSFP28	4	4	4	8	8	4	6
		5410	**5420**	**26000**	**28000**	**2600F**	**3000F**
		Palo Alto		**Check Point**		**Fortinet**	

*Informação não está disponível no datasheet do equipamento

3.15. Diante do cenário atual, a estimativa de demanda segue o seguinte quantitativo de bens e serviços necessários para a composição da solução a ser contratada:

Id	Demanda Prevista	Bem/Serviço	Unidade de Medida	Quantidade
1	Plataforma de Segurança em cluster composta por Firewalls de Próxima Geração.	Appliance de Firewall com garantia durante 60 meses	UND	02
2	Pacote de assinatura com as principais licenças para as funcionalidades de segurança do Firewall (Antivirus, Anti-Bot, Anti-Malware, IPS, Filtragem avançada de URL, DNS Security e SD-WAN).	Licença de software durante 60 meses	UND	02
3	Assinatura de licença para acesso remoto seguro de uma solução de rede virtual privada (VPN) e ZTNA.	Licença de software durante 60 meses	UND	02
4	Software para Gerenciamento centralizado do cluster de firewalls.	Software de Gerência licenciado para 2 unidades	UND	01
5	Garantia do Software para Gerenciamento centralizado do cluster de firewalls e Suporte Oficial 24x7 fornecido no Brasil em português por ASC (Authorized Support Center) com serviço de suporte técnico remoto.	Suporte durante 60 meses	UND	01
6	Garantia da Solução de Plataforma de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em português por ASC (Authorized Support Center) com serviço de suporte técnico e monitoramento.	Suporte durante 60 meses	UND	02
7	Serviço de Desenho de Alto Nível (HLD) para o cenário de implantação identificado pelo cliente.	Prestação de serviço	UND	01
8	Serviço de Instalação e configuração.	Prestação de serviço	UND	01
9	Treinamento.	Prestação de serviço	UND	01

4. ANÁLISE DE SOLUÇÕES POSSÍVEIS

4.1. Identificação das Soluções

Id	Descrição da solução (ou cenário)
1	Aquisição de novos appliances de plataforma de segurança em cluster de firewalls tipo chassi (NGFW) da Palo Alto Networks incluindo licenças equivalentes as subscrições em curso, garantia e suporte técnico para atualização dos firewalls atuais em produção.
2	Aquisição de novos firewalls compostos de clusters de firewalls tipo chassi (NGFW) de

	qualquer fabricante incluindo novas licenças, instalação, configuração, garantia, suporte técnico e treinamento de toda solução para substituir os firewalls atuais em produção.
3	Contratação de Firewall como serviço.
4	Aquisição de Firewall como dispositivos virtuais.
5	Contratação de Firewall na nuvem.
6	Renovação do Serviço de Suporte Técnico e garantia.

4.2. Análise Comparativa de Soluções

Requisito	Id da Solução	Sim	Não	Não identificado	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	**1**	**X**			
	2	**X**			
	3			**X**	
	4			**X**	
	5			**X**	
	6	**X**			
A Solução está disponível no Portal do Software Público Brasileiro?	**1**				**X**
	2				**X**
	3				**X**
	4				**X**
	5				**X**
	6				**X**
A Solução é um software livre ou software público?	**1**		**X**		
	2		**X**		
	3		**X**		
	4		**X**		
	5		**X**		
	6		**X**		
A Solução é aderente às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário?	**1**				**X**
	2				**X**
	3				**X**
	4				**X**
	5				**X**
	6				**X**
A Solução é aderente às regulamentações da ICP-	**1**				**X**

Brasil? (quando houver necessidade de certificação digital)	**2**				**X**
	3				**X**
	4				**X**
	5				**X**
	6				**X**
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)?	**1**				**X**
	2				**X**
	3				**X**
	4				**X**
	5				**X**
	6				**X**

4.3. Pesquisa de Preços de Mercado

4.3.1. A pesquisa de mercado está presente no documento acostado aos autos do processo.

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

5.1. Para atender à demanda, realizamos uma análise comparativa das opções de Tecnologia da Informação e Comunicação (TIC) disponíveis para atender às necessidades do TJCE. Foi levado em consideração a eficiência e eficácia em relação aos benefícios para alcançar os objetivos da contratação;

5.2. As soluções relacionadas ao serviço de FWNG mencionado abaixo foram obtidas por meio de pesquisas no Portal de Compras do Governo Federal e em editais de licitações da Administração Pública Estadual e Federal. É importante observar que, embora sejam semelhantes ao objeto desta contratação, cada instituição define os requisitos de acordo com suas particularidades, complexidade e capacidade, o que tem um impacto direto nos custos de cada contratação.

5.3. As soluções disponíveis no mercado para a contratação de firewalls de rede são aplicadas por meio de hardware, dispositivos virtuais e controles nativos da nuvem. Podem ser redes locais, híbridas (no local e na nuvem), nuvens públicas ou nuvens privadas. Os produtos de firewall de rede oferecem suporte a diferentes casos de implantação.

5.4. A ascensão de ambientes híbridos é o principal fator por trás da introdução dos

fornecedores de vários tipos de implantação de firewall, como FWaaS e nuvem nativa. Há uma demanda crescente para proteger ambientes locais, vários ambientes de nuvem e usuários remotos com firewalls.

5.5. O contexto aqui considerado é em relação às vantagens e desvantagens de uma mudança completa de uma solução de FWNG já implementada e solidificada em ambientes de Data Center crítico de TIC com características, especificações, particularidades e dimensões das mais variadas em cada órgão citado.

5.6. **Solução 2 - Aquisição de novos firewalls**: Decisões de substituir as tecnologias ou plataforma robustas e confiáveis que atuam diretamente na proteção de ambiente se torna complexo, não é razoável considerar uma simples análise comparativa entre os preços de soluções tecnológicas a serem substituídas. Por vezes, mudanças de tecnologia requerem antecipação de vários ciclos futuros buscando traçar a estratégia que procura reduzir a dependência de uma determinada tecnologia e as ameaças de sua substituição. Um fator de risco com a substituição da tecnologia seria a inclusão de novos elementos no ambiente de tecnologia que durante a fase de substituição poderiam conflitar com a solução já utilizada no TJCE.

Embora se possa argumentar que existam outras opções no mercado de Tecnologia da Informação e Comunicação (TIC), as informações reunidas por essa área técnica indicam que as plataformas Palo Alto têm demonstrado satisfatória eficiência em relação aos cenários de uso adotados pelo Poder Judiciário, atendendo de maneira apropriada aos requisitos técnicos estabelecidos para um sistema da categoria NGFW desde sua implementação na arquitetura de serviços de segurança atualmente em uso.

Principalmente, pode-se afirmar de forma razoável que a renovação da plataforma NGFW desejada garante a manutenção das despesas orçamentárias incorridas nas contratações anteriores.

Portanto, mesmo considerando a disponibilidade de alternativas semelhantes, a decisão de manter a solução atualmente em uso e garantir a atualização tecnológica da plataforma NGFW proporcionará os seguintes benefícios ao Poder Judiciário Cearense:

• Aproveitamento da "expertise" da equipe técnica na solução atualmente implantada.

• Amplificação da camada de proteção e disponibilidade da informação.

• Redução do tempo de implantação, tendo em vista a solução a ser adquirida é do mesmo fabricante da solução utilizada atualmente.

• Proteção, autenticidade e acessibilidade as informações.

• Implementação e operações simplificadas com rápida implementação e mínimo de

interrupção no ambiente produtivo através do gerenciamento fácil e do uso otimizado dos recursos do sistema NGFW em operação.

• Proteção de rede abrangente contra ameaças maliciosas direcionadas aos sistemas operacionais Windows e Linux em operação no parque tecnológico do Poder Judiciário empregados pela totalidade de aplicações disponibilizadas aos usuários.

Ainda assim, estima-se que uma provável migração de um ambiente complexo, dependendo do tamanho do projeto e da equipe, pode durar entre 30 a 45 dias úteis.

Também é possível relacionar possíveis impactos decorrentes da substituição completa da atual solução, que são:

- Substituição complexa e ameaça da estabilidade e interrupções de serviços críticos;
- As customizações das telas de bloqueios e alertas do filtro web deverão ser migradas e/ou refeitas;
- Zonas de bloqueios, definições de segurança, controle do tráfego de arquivos, blacklists, relatórios utilizados nas tarefas rotineiras e outras configurações provavelmente deverão ser refeitas de forma manual, podendo impactar nos prazos e gerar riscos de falhas;
- Certificados instalados nas estações para a realização do decrypt deverão ser substituídos ou nova funcionalidade deverá ser implementada;
- Todas as regras atuais deverão ser migradas. O novo fornecedor poderá não conseguir realizar a exportação /importação das regras de forma automática;
- Esforço técnico considerável para migração e reimplementação de todas as regras de segurança, perímetros, regras de NAT, VPN, IPS, customizações, integração com demais ferramentas utilizadas pela SETIN;
- Tempo para se adquirir o mesmo nível de conhecimento e experiência que a equipe possuí na solução atual;
- Interrupção e modificação de projetos desenvolvidos e customizados com a solução atual. Tais como:
    - MFA (múltiplo fator de autenticação) com a solução watchguard, para autenticação multifator, para aumentar a segurança na autenticação dos usuários com perfis de administrador nos servidores Windows;
    - Captive Portal para realizar a conexão/autenticação na rede wifi, tanto para visitantes quanto para magistrados, servidores e demais colaboradores do TJCE, monitorando os acessos dos usuários na rede

wifi;

- Global Protect atualmente utilizado para estabelecer a conexão VPN dos magistrados, servidores e colaboradores do TJCE com a rede institucional do TJCE de modo seguro;
- Projeto de implantação e utilização do IPv6 para o sistema do ESAJ, Atualmente em fase de testes.

- Substituição de todos os clientes de VPN e readequação de uso e instrução para todos os usuários de VPN. Parte dos Magistrados, servidores e demais colaboradores estão em Teletrabalho.
- Esforço técnico operacional de reconfiguração.

Há vários fabricantes que oferecem soluções de NGFW, e todas elas possuem recursos semelhantes aos da solução atual do TJCE, tais como IPS, Filtro WEB, VPN e proteção contra malware. Além da Palo Alto, outros fabricantes notáveis incluem a Checkpoint e a Fortinet. No entanto, é importante considerar os custos indiretos e os riscos associados a essa transição, que podem ser difíceis de avaliar neste momento.

Portanto, as decisões relacionadas à substituição de tecnologias não podem mais se basear apenas em uma análise comparativa dos preços entre a solução tecnológica atual e a nova opção. Às vezes, a adoção de uma nova tecnologia requer uma antecipação de vários ciclos futuros para traçar uma estratégia que visa reduzir a dependência de uma tecnologia específica e mitigar as ameaças associadas à mudança. Um fator que aumenta o risco da transição é a escassez de profissionais de segurança da informação qualificados para lidar com as demandas da mudança e com os desafios que surgirão após a implementação.

Além disso, considerando os prazos de entrega atuais e o tempo necessário para a implementação, parece inviável ficar sem a atualização da solução existente no momento.

5.7. Solução 3 - Contratação de Firewall como serviço: Nessa opção, o TJCE terceiriza a função de firewall NGFW para um provedor de serviços especializado que hospeda e gerencia os dispositivos de segurança em seus próprios datacenters. Apesar das vantagens dessa abordagem, ela também traz algumas desvantagens que devem ser consideradas.

A principal desvantagem é a dependência do provedor de serviços para garantir a disponibilidade e a eficácia do firewall. Se o provedor de serviços tiver problemas técnicos

ou for alvo de ataques, a segurança da rede do TJCE pode ser comprometida. Outra desvantagem é o risco de exposição de dados sensíveis a terceiros não autorizados, pois o provedor de serviços tem acesso aos dados que trafegam pelo firewall. Essa situação pode violar as normas e regulamentos de privacidade e segurança dos dados. Além disso, o TJCE perde o controle direto sobre a segurança da rede, pois ela está sendo gerenciada por um provedor de serviços terceirizado. Isso pode limitar a capacidade do TJCE de configurar e personalizar as políticas e regras de firewall de acordo com as suas necessidades específicas. Essa solução é inviável para o TJCE pois temos requisitos rigorosos de soberania e confidencialidade dos dados, precisamos de um controle mais granular e personalizado sobre as políticas e regras de firewall.

5.8. Solução 4 - Aquisição de Firewall como dispositivos virtuais: Nessa opção, o TJCE pode instalar o software NGFW em um servidor existente, criando um dispositivo de segurança virtual. Essa abordagem pode possibilitar que o TJCE economize espaço físico, bem como flexibilidade de configurar e atualizar os recursos de firewall sem depender de um hardware dedicado.

No entanto, essa solução também apresenta algumas desvantagens, como a necessidade de habilidades e recursos de gerenciamento de servidor. O TJCE precisará ter uma equipe técnica capacitada para instalar, configurar e monitorar o software NGFW, bem como para resolver possíveis problemas no servidor. Outra desvantagem é o risco de comprometimento da segurança e da performance se o servidor ficar sobrecarregado ou falhar. Se o servidor tiver uma alta demanda de recursos ou sofrer uma interrupção, o firewall também pode ser afetado, deixando a rede vulnerável a ataques ou indisponível para os usuários, gerando também indisponibilidades dos sistemas.

5.9. Solução 5 - Contratação de Firewall na nuvem: Essa opção oferece uma solução integrada e eficiente para proteger os dados e aplicativos hospedados em diferentes plataformas de nuvem. Pode ser que essa abordagem reduza a complexidade operacional, bem como tenha acesso a recursos de segurança avançados e atualizados fornecidos pelo provedor de nuvem.

No entanto, essa solução também apresenta algumas desvantagens, como a dependência da conectividade com a internet. Se a rede do TJCE ficar indisponível por qualquer motivo, o firewall na nuvem também ficará deixando a rede desprotegida ou inacessível. Outra desvantagem é o risco de exposição a vulnerabilidades nos provedores de nuvem, que podem afetar a segurança da rede. Se o provedor de nuvem for alvo de ataques ou tiver falhas de segurança, os dados e aplicativos do TJCE podem ser comprometidos. Além

disso, o TJCE perderá o controle direto sobre a segurança da rede, pois ela está sendo gerenciada por um provedor de nuvem terceirizado. Isso pode limitar a capacidade do TJCE de configurar e personalizar as políticas e regras de firewall de acordo com as suas necessidades específicas.

5.10. Solução 6 - Renovação do Serviço de Suporte Técnico e garantia para o firewall atual: A renovação do serviço de suporte técnico também cobre a manutenção do hardware. Isso inclui reparos e substituição de peças defeituosas, bem como a garantia de que o hardware do NGFW esteja atualizado. fornece suporte técnico quando necessário e mantém o hardware atualizado e funcionando corretamente. As desvantagens desse sistema são diversas. Primeiramente, há a questão da obsolescência do hardware, que tornar o equipamento ultrapassado em menos de 5 anos. Além disso, há um aumento significativo no risco de falhas do equipamento, o que pode comprometer sua eficiência e confiabilidade. Por fim, a capacidade atual desse sistema é insuficiente para atender à demanda atual por um período muito curto, inferior a um ano. Esses fatores combinados tornam claro que é necessário tomar medidas para lidar com esses problemas e garantir um desempenho adequado no longo prazo.

5.11. O NIST Guidelines for Media Sanitization (Diretrizes do NIST para a Sanitização de Mídia) é um documento publicado pelo National Institute of Standards and Technology (NIST), agência dos Estados Unidos responsável por desenvolver padrões técnicos e diretrizes para diversas áreas, incluindo segurança da informação. NIST SP 800-88 é atualizado periodicamente para refletir as mudanças no ambiente de segurança da informação e nas tecnologias de armazenamento de dados. As organizações podem utilizar a figura abaixo para auxiliá-las a tomar decisões de sanitização que sejam compatíveis com a categorização de segurança da confidencialidade das informações contidas em suas mídias, sendo que o processo de decisão é baseado na confidencialidade das informações, não no tipo de mídia. Dispositivos com alta categorização de segurança cuja mídia será reutilizada e deixará o controle da organização devem ser destruídos. Por esses motivos, opções como Firewall como serviço ou aluguel de equipamentos não foram consideradas.

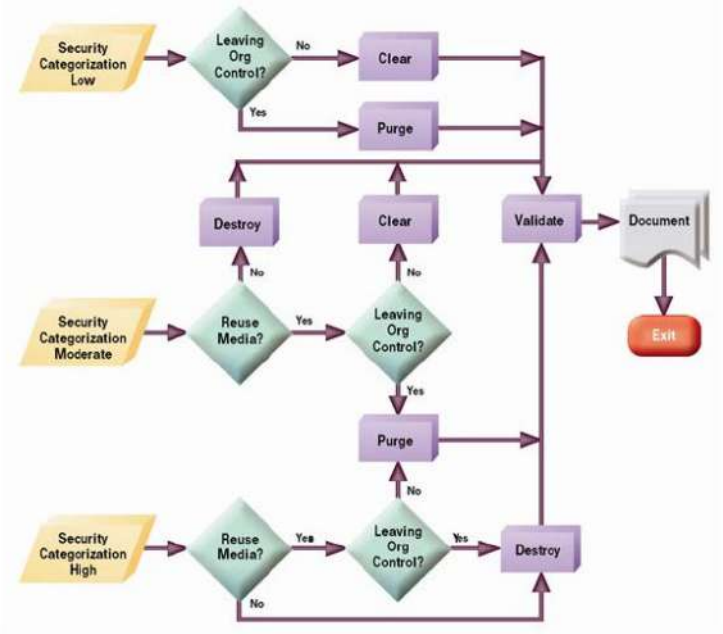


Figura 6 - Fluxo de decisão de sanitização e disposição – Fonte: NIST SP 800-88

5.12. O Quadrante Mágico para Firewalls de Rede da consultoria Gartner, publicado em 19 de dezembro de 2022 com o ID G00761497, indica como premissas do planejamento estratégico que, até 2026, mais de 30% das novas implantações de firewalls distribuídos para filiais serão de ofertas de firewall como serviço (FWaaS), em comparação com menos de 10% em 2022. No entanto, o percentual total da projeção futura e mercado atual dessa demanda, com aquisição desses serviços, não é significativo o suficiente para justificar a adoção dessas modalidades. Além disso, é importante considerar a conectividade com a estrutura do CDC (Cinturão Digital do Ceará), que atinge mais de 130 municípios cearenses. Ao adotar uma tecnologia hibrida, FWaaS ou nuvem nativa, pode haver um aumento na latência de conectividade das localidades remotas até o ponto de presença do provedor de serviço, que pode estar localizado em outro estado ou pais. Esse impacto pode afetar a qualidade do serviço, uma vez que a migração de uma conectividade local e dedicada, para uma infraestrutura pública e remota, pode interferir na qualidade da conexão dos sistemas críticos.

5.13. É importante ressaltar que há no mercado diversos modelos e soluções de firewall, resultando em uma quantidade de possíveis combinações e características relativamente amplas (capacidade de throughput, quantidade de sessões novas e simultâneas, quantidade de interfaces). Além das possíveis combinações características de hardware, existem ainda diferentes tipos de licenciamento (período de suporte/garantia, Filtro de URL, Prevenção a ameaças conhecidas ou desconhecidas, Antivírus, Segurança para DNS, etc.)

5.14. Ao analisarmos editais que abordam soluções de perímetros de segurança da informação, constatamos que, nos órgãos públicos semelhantes ao TJCE, a prática tem sido adquirir equipamentos que incluem garantia, instalação e treinamento na solução. Exemplos:

5.14.1. TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS – PREGÃO ELETRÔNICO/SRP Nº. 039/2023-TJAM: Registro de Preços para eventual renovação do suporte e das licenças do cluster de equipamentos de Next-Generation Firewall, assim como expansão da solução de firewall para as unidades descentralizadas do Tribunal de Justiça do Estado do Amazonas (TJAM), compreendendo suporte técnico e garantia pelo período de 60 meses, incluindo serviços de instalação, configuração e treinamento oficial do fabricante.

5.14.2. EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ, Ata de Registro de Preços Nº2022/12762 -

5.14.3. MINISTÉRIO PÚBLICO DO ESTADO DE ALAGOAS, Pregão Eletrônico Nº 20/2022 - Registro de preços de produtos para expansão futura de soluções de firewall, compreendendo a aquisição de equipamentos, fornecimento de suporte técnico especializado, garantia/atualização, assinaturas da solução de firewall Palo Alto Networks;

5.14.4. Universidade Federal do Amazonas, PE 7-2020;

5.14.5. Ministério Público do Estado do Pará, PE 47/2020 – Registro de Preços para a aquisição de ativos de segurança de rede, Firewalls Next Generation (NGFW) com SD-WAN integrada, contemplando os serviços de Instalação, Treinamento e Suporte Técnico;

5.14.6. Escola Nacional de Administração Pública, PE 16/2021 – contratação de empresa especializada no fornecimento de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, incluídos todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades da Enap, conforme condições, quantidades e exigências estabelecidas neste Edital e seus Anexos;

5.14.7. MINISTÉRIO DA DEFESA – COMANDO DA AERONÁUTICA – Pregão Eletrônico N. 02/2020 – Contratação de serviço de Planejamento, Instalação e

Configuração, Suporte e Treinamento de solução de segurança tipo firewall;

5.14.8. TRIBUNA REGIONAL FEDERAL DA 4a REGIÃO (TRF4) - Pregão Eletrônico N. 39/2020 - Contratação de 01 (uma) unidade de segurança de rede de dados e de 01 (uma) unidade de serviços de garantia, assistência técnica e suporte técnico pelo período de 60 (sessenta meses)".

5.14.9. TRIBUNAL REGIONAL FEDERAL DA 5ª. REGIÃO, Pregão Eletrônico N.º 19/2022 – Contratação de empresa especializada para aquisição de Solução de NGFW com licenças e garantias.

5.14.10. TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, Pregão Eletrônico N.º 73/2022 – Aquisição de firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia de 60 meses.

5.14.11. PREGÃO ELETRÔNICO Nº 37/2023/TCE-RO – Contratação de empresa para fornecimento de Solução de Segurança de Rede Palo Alto "NGFW" (Next Generation Firewall), com gerência centralizada de administração e retenção de logs, incluindo subscrições instalação, migração de configurações, suporte, garantia, repasse técnico e atualizações pelo período de 36 (trinta e seis) meses.

5.14.12. TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO – Pregão Eletrônico N.º 47/2020 - Registro de preço para aquisição de solução de proteção de rede Next Generation Firewall (NGFW);

5.14.13. MINISTÉRIO DA ECONOMIA INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA – INMETRO – Pregão Eletrônico N.º 4/2023 – Contratação de solução de tecnologia da informação e comunicação para renovação das subscrições da solução de segurança da informação Ngfw (Next Generation Firewall), composta por 04 (quatro) equipamentos, modelos PA-5220, do fabricante Palo Alto Networks, pelo período de 12 (doze) meses, incluindo serviços agregados de tratamento de incidentes, para atender às necessidades do instituto nacional de metrologia, qualidade e tecnologia (Inmetro), conforme condições, quantidades e exigências estabelecidas no edital e seus anexos.

5.14.14. TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL – Estudos Preliminares – Pregão Eletrônico N.º 1/2023 Contratação de empresa especializada no fornecimento, instalação e configuração de sistema integrado de segurança para proteção de perímetro de rede licenciado com funcionalidades de "Next-Generation Firewall" (NGFW), com gerenciamento centralizado e armazenamento de logs, incluindo serviços de migração e garantia técnica do fabricante por 60 (sessenta) meses.

5.14.15. TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO – Estudos Preliminares – PROAD: 3928/2023 – REGISTRO DE PREÇOS para aquisição de solução de para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, também contemplando atualização de assinaturas de proteção e suporte técnico em regime 24x7, pelo prazo de, no mínimo, 24 (vinte e quatro) meses, incluindo ainda serviços de instalação e treinamento.

6. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

6.1. A análise comparativa considera exclusivamente soluções técnicas e funcionalmente viáveis, conforme estabelecido na Resolução CNJ 468. A análise abrange:

6.1.1. Comparação dos custos totais de propriedade (Total Cost Ownership - TCO), que envolve a obtenção dos custos relacionados ao ciclo de vida dos bens e serviços de cada solução, como valores de aquisição dos ativos, insumos, garantia e manutenção.

6.1.2. Inclusão de uma memória de cálculo que faz referência aos preços e custos utilizados na análise, a fim de permitir a verificação da origem dos dados.

6.2. Cálculo dos Custos Totais de Propriedade

Solução Viável 1
Custo Total de Propriedade – Memória de Cálculo
Para a implementação dessa solução, o órgão adquire um conjunto de equipamentos (hardware e software), que será utilizado até o final de sua vida útil. No entanto, a lista de end-of-life do fabricante indica que esses equipamentos devem ser substituídos a partir de 2023 (https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-sale). Atualmente, o TJCE possui equipamentos deste tipo de solução com 06 anos de uso (CT Nº 17/2018). Ao calcular o custo total de propriedade (TCO) dessa solução, utilizaremos a média de preços das propostas recebidas pelos parceiros do fabricante. Consideraremos um ciclo de vida de 5 anos para essa solução, a fim de calcular o TCO. Dessa forma, o custo inicial da aquisição do equipamento, juntamente com a projeção de renovação das licenças após 60 meses, totaliza R$ 9.300.860,95.

6.3. Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

6.3.1. Uma avaliação comparativa de despesas deverá ser conduzida, levando em consideração unicamente as opções tecnicamente e funcionalmente viáveis. Isso implica:

6.3.1.1. O cálculo dos custos totais de propriedade (Total Cost of Ownership - TCO) será realizado ao identificar os custos associados ao ciclo de vida de cada alternativa, abrangendo aspectos como os valores de compra dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento.

6.3.1.2. Será mantida uma memória de cálculo que faça referência aos preços e custos empregados na análise, de forma a possibilitar a rastreabilidade da fonte dos dados.

6.3.2. A comparação de custos entre as soluções consideradas viáveis no processo visa identificar custos indiretos que podem impactar o custo total da contratação de uma solução ou serviço ao longo de seu ciclo de vida. Para isso, é essencial realizar uma análise abrangente do Custo Total de Propriedade (TCO) e verificar a fonte dos dados por meio da memória de cálculo para validação. Essa abordagem holística permite avaliar e mensurar todos os recursos necessários para adquirir e manter um bem ou serviço de TIC, abrangendo todos os custos envolvidos. Calculando o TCO, evitamos o risco comum de optar pelo "mais barato" que, a longo prazo, se revela mais oneroso.

6.3.3. Atualmente, a opção com menor risco embutido para garantir os níveis de serviço esperados e o funcionamento do Teletrabalho, bem como o acesso aos serviços de TIC oferecidos aos cidadãos, é manter a contratação das assinaturas da solução de NGFW, juntamente com suporte especializado pontual. Considerando que as outras soluções são inviáveis, e dado o contexto atual detalhado neste estudo, a escolha ideal para 2024 é manter o formato atual e aguardar o desenvolvimento das atividades de Infraestrutura de TI SI em andamento e planejadas. Além disso, não é o momento mais apropriado para aproveitar uma oportunidade trocar a atual solução de Firewall, uma vez que as limitações de pessoal são incompatíveis com a possível carga adicional de gerenciamento e supervisão, bem como as mudanças na arquitetura de rede e as necessidades de integração, que poderiam restringir a capacidade de atuação do futuro contratado.

6.3.4. Os eventuais custos indiretos, decorrentes de riscos não previstos nas na soluções consideradas inviáveis, podem ter um impacto significativo na avaliação do Custo Total de Propriedade (TCO) e potencialmente criar uma falsa expectativa de lucro

inicial. Embora seja possível analisar o TCO das referidas soluções para fins de comparação, atualmente não são viáveis devido às justificativas apresentadas.

6.4. O Gartner define o TCO (Custo Total de Propriedade) como uma análise completa dos custos associados a uma solução de tecnologia da informação ao longo de seu ciclo de vida. Isso visa revelar todos os "custos ocultos" que podem não estar evidentes no momento da aquisição. Esses custos englobam, entre outros, despesas de aquisição, gerenciamento, suporte/garantia de hardware e software, treinamento e outros. No caso desta aquisição específica, que se refere à aquisição e contratação de novas assinaturas, é apresentado uma análise de TCO na tabela a seguir. O custo foi baseado em pesquisas de preços realizadas por meio de Atas de Registro de Preços e/ou propostas de fornecedores. É importante ressaltar que esse estudo é realizado considerando o processo de centralização da compra, o que implica na adoção de premissas para aproximar ao máximo a realidade dos órgãos que apresentam a demanda.

Solução	Estimativa de TCO ao longo dos anos					Total
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	
Solução Viável 1 – Aquisição de novos appliances de plataforma de segurança em cluster de firewalls tipo chassi (NGFW) da Palo Alto Networks incluindo licenças equivalentes as subscrições em curso, garantia e suporte técnico para atualização dos firewalls atuais em produção.	R$ 9.055.875,76	R$ 61.246,32	R$ 61.246,32	R$ 61.246,32	R$ 61.246,32	**R$ 9.300.860,95**

7. IDENTIFICAÇÃO DA SOLUÇÃO ESCOLHIDA

7.1. Solução Escolhida: Solução 1.

7.2. Justificativa da solução escolhida

7.2.1. A solução de segurança atual é classificada como um Firewall de Próxima Geração (NGFW). Isso representa uma evolução em relação ao modelo tradicional de firewall, no qual o enfoque estava na restrição ou autorização com base em portas (protocolos) e

endereços IP. O NGFW é uma solução com funcionalidades aprimoradas e a capacidade de executar ações mais sofisticadas em resposta às crescentes ameaças cibernéticas.

7.2.2. No que se refere ao TJCE, a solução engloba diversas funcionalidades. Estas incluem:

7.2.2.1. Sistema de Prevenção de Intrusões (IPS), que detecta e impede diariamente centenas de ameaças;

7.2.2.2. Filtro de Navegação na Web, permitindo que os funcionários internos acessem a internet de maneira segura. Essa função restringe o acesso a categorias inteiras de sites com conteúdo inadequado ou inseguro;

7.2.2.3. Recursos de VPN para os usuários. Esse recurso em particular apoiou a transição da instituição para o teletrabalho durante a pandemia de Covid-19 e, logo em segui, o incêndio que ocorreu no prédio Sede do Poder Judiciário Cearense, no dia 6 de setembro. Levando a interdição do prédio e necessidade de reforma.

7.2.2.4. Inspeção de ataques e dados ocultos em tráfego criptografado SSL/TLS, mantendo a privacidade dos usuários;

7.2.2.5. Controle de aplicativos, evitando o uso indevido de recursos de tecnologia com atividades não relacionadas à empresa, além de reduzir o risco causado por aplicativos vulneráveis.

7.2.3. Todas essas funcionalidades fazem uso de recursos de inteligência de reputação, que são mantidos por meio de assinaturas fornecidas pelo fabricante da solução. Isso possibilita a automação de várias atividades, reduzindo a carga de trabalho e mitigando as possíveis falhas decorrentes da intervenção de profissionais técnicos. No entanto, a integração e consolidação de diversas funcionalidades em uma única solução aumentam a complexidade técnica do ambiente, o que torna as alterações mais propensas a erros. A implantação de um NGFW requer a realização de várias configurações e personalizações, envolvendo a participação de especialistas e a adaptação ao ambiente tecnológico.

7.2.4. A escolha da solução reforçar a proteção da rede contra ameaças e proporciona suporte a outros fatores cruciais para o sucesso do projeto. A aquisição de um dispositivo de hardware dedicado para implantação de Next Generation Firewall oferece vantagens em relação a outras formas do mesmo serviço de segurança, como serviços gerenciados, software de baseado em nuvem, soluções de firewall de software

e outras soluções.

7.2.5. O desempenho de um NGFW é otimizado, permitindo aumentar a capacidade de processar grandes volumes de tráfego, sem fornecer uma limitação da velocidade da rede atual. Além disso, sua escalabilidade garante que o firewall possa acompanhar o crescimento da infraestrutura, sem exigir substituições frequentes. Dessa forma, o dispositivo dedicado capacita a organização a atender suas necessidades futuras, adaptando-se às mudanças tecnológicas e às demandas crescentes de segurança, consolidando-se como uma solução completa e abrangente.

7.2.6. A escolha dessa solução é justificada pelas vantagens que ela oferece em comparação com outras tipos de contratação, que incluem:

7.2.6.1. Maior desempenho: Em comparação com outras soluções de segurança, os appliances NGFW são projetados especificamente para oferecer alto desempenho, alto throughput e largura de banda de rede, sem afetar o desempenho das aplicações existentes.

7.2.6.2. Adaptação às exigências do contratante: A capacidade de personalização de recursos de acordo com as necessidades da rede e segurança da infraestrutura local

7.2.6.3. Controle centralizado: A aquisição de um appliance NGFW permite que a organização tenha um controle centralizado sobre a segurança de sua rede, o que pode simplificar a implementação de políticas de segurança, a manutenção e a gerenciamento de sua infraestrutura de segurança.

7.2.6.4. Maior visibilidade: A capacidade de interceptar e inspecionar o tráfego local em detalhes agrega uma visão mais clara da rede, o que pode ajudar a detectar anomalias e ameaças mais rapidamente.

7.2.6.5. Simplificação da infraestrutura de segurança: Consolidar vários dispositivos de segurança em um único equipamento, simplificando a gerenciamento e manutenção de sua infraestrutura de segurança.

7.2.7. O interesse na confiança zero está favorecendo a seleção de fornecedores únicos de firewall que podem ajudar as empresas a obter um ZTNA (Zero trust network access), para que não precisem usar vários fornecedores. Os clientes esperam capacidades de integração maduras ao comprar tecnologias sobrepostas do mesmo fornecedor.

7.2.8. Há um grande interesse na visibilidade e controle das políticas de segmentação leste-oeste do datacenter e integrações aprimoradas de operações de segurança.

7.2.9. Os recursos avançados de segurança continuam sendo um fator importante, pois os

vetores de ameaças estão usando meios mais sofisticados de atacar forças de trabalho híbridas e redes em nuvem. A maioria dos fornecedores está tentando desenvolver ou adquirir produtos que ofereçam esses recursos, mas eles enfrentam forte concorrência dos melhores fornecedores que oferecem recursos granulares para esse caso de uso específico.

7.2.10. À medida que os firewalls de rede evoluem, selecionar o fornecedor mais adequado torna-se um desafio. Um ponto de partida para essa escolha é utilizar como fonte de comparação de soluções o Gartner, líder em consultoria de soluções de Tecnologia da Informação. Em dezembro de 2022, o Gartner avaliou 17 fornecedores para ajudar os líderes de segurança e gerenciamento de riscos a fazer a escolha certa para sua organização. Esse relatório compara as principais soluções do mercado e as posiciona em um "quadrante mágico" que representa o nível de maturidade das soluções disponíveis. Selecionamos apenas as soluções dos fabricantes que foram avaliados com os melhores resultados em suas soluções e que se enquadram no quadrante "Líderes".

7.2.11. O quadrante dos "Líderes" contém fornecedores que podem moldar o mercado sendo os primeiros a introduzir recursos adicionais e aumentar a conscientização sobre a importância desses recursos. Os líderes têm o potencial de atender aos requisitos das empresas para vários casos de uso de firewall em uma solução de plataforma única.

Figura 7 - Quadrante Mágico para Firewalls de Rede – Fonte: Gartner (dezembro 2022)

7.2.12. Com base no gráfico fornecido, e ao compará-lo com a solução atualmente empregada no TJCE, a Palo Alto Networks destaca-se dentre os líderes de mercado em seu respectivo segmento. No cenário das opções de mercado para soluções de firewall de rede, emergem alguns fabricantes proeminentes. É relevante notar que a solução atualmente em vigor no TJCE se posiciona como uma das mais eficazes nesse segmento, demonstrando um empenho contínuo em manter o padrão de efetividade no âmbito da segurança.

Vendor	4Q22 Revenue	4Q22 Market Share	4Q21 Revenue	4Q21 Market Share	4Q22/4Q21 Growth
1. Palo Alto Networks	$973.75	15.9%	$883.35	15.1%	10.2%
3. Fortinet	$966.61	15.8%	$776.23	13.3%	24.5%
2. Cisco	$921.08	15.8%	$885.79	15.2%	4.0%
4. Check Point	$473.04	7.7%	$462.55	7.9%	2.3%
5. SonicWALL	$194.16	3.2%	$183.50	3.1%	5.8%
Rest of Market	$2,582.05	42.3%	$2,645.27	45.3%	-2.4%
Total	**$6,110.69**	**100.0%**	**$5,836.70**	**100.0%**	**4.7%**

Source: IDC Worldwide Quarterly Security Appliance Tracker Q4 2022, March 9, 2023

7.2.13. A Palo Alto sendo reconhecida como 'Leader' no Quadrante Mágico para Firewalls de Rede não apenas se destaca na avaliação do Gartner, mas também comprova sua presença global no mercado. A sua participação no mercado de empresas, conforme indicado pela International Data Corporation (IDC), é um indicador de confiabilidade e sucesso, evidenciando sua solidez, confiabilidade, refletindo sua reputação, qualidade, compromisso, maturidade e estabilidade de produtos.

7.2.14. Considerando que o TJCE utiliza a plataforma de solução de segurança da fabricante Palo Alto Networks há mais de cinco anos, fica evidente a sua escolha acertada, uma vez que ela tem garantido estabilidade, pleno funcionamento e confiabilidade em um ambiente de infraestrutura complexo. Nesse contexto, o TJ busca aprimorar ainda mais as funcionalidades das soluções de segurança, com o intuito de suportar o aumento das capacidades operacionais, acompanhar as futuras demandas das cargas de trabalho provenientes dos equipamentos do datacenter, bem como possibilitar a ampliação de serviços, o acesso de usuários remotos e o gerenciamento eficiente do tráfego. Essa busca por melhorias visa assegurar que o TJCE esteja preparado para enfrentar os desafios e acompanhar o ritmo crescente das demandas tecnológicas, proporcionando um ambiente seguro e confiável para seus usuários e garantindo o bom funcionamento de suas atividades.

7.2.15. Com os recursos adquiridos, o TJCE terá a capacidade de efetuar modificações na arquitetura atual, possibilitando a modernização da tecnologia de firewall, inspeção de pacotes e para identificar possíveis ameaças para outros segmentos da rede. Essa

estratégia permitirá ao TJCE estender as medidas de segurança para além de sua infraestrutura de borda, garantindo uma proteção mais abrangente, com políticas de controle de acesso que determinam quais dispositivos e quais tipos de tráfego são permitidos entre diferentes segmentos de rede, ao mesmo tempo em que simplifica a gestão e monitoramento por meio de uma plataforma centralizada.

7.2.16. O artigo 41 da Lei nº 14.133/21 trata de situações em que a Administração pode indicar uma ou mais marcas ou modelos em licitações que envolvam o fornecimento de bens. Essa indicação deve ser justificada. As hipóteses para essa indicação incluem a necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração, quando determinada marca ou modelo forem capazes de atender às necessidades do contratante.

7.2.17. Já o Tribunal de Contas da União, no Acórdão nº 1553/2008 – Plenária, aborda sobre o seguinte:

> *"A vedação imposta por esse dispositivo é um dos mecanismos utilizados pelo legislador no sentido de conferir efetividade aos princípios informativos da licitação, entre esses o da livre concorrência, o do julgamento objetivo e o da igualdade entre os licitantes" (Acórdão 1553/2008 – Plenário.)*

7.2.18. Entretanto, é importante destacar a ressalva expressa na norma mencionada anteriormente: a possibilidade de indicação de uma marca, nos casos em que isso seja tecnicamente justificável, considerando a inexistência de produtos semelhantes. Portanto, a proibição de indicar uma marca em processos de licitação não é absoluta. E é com base nessa situação excepcional que este Estudo Preliminar se fundamenta. As opções disponíveis no mercado exigiriam a substituição completa da solução, o que não apresenta similaridade de objeto correlato, e, portanto, não há espaço para outras formas de contratação. Além disso, deve-se considerar a criticidade do projeto, que é altamente sensível por si só.

7.2.19. Existem situações em que é legítima e até mesmo recomendável a restrição por determinadas marcas, como é o caso deste projeto em questão.

7.2.20. Segundo o jurista Marçal Justen Filho, prevalece o entendimento doutrinário de que está em vigor:

> *É possível a contratação de fornecedores exclusivos ou*

> *a preferência por certas marcas desde que essa seja a solução mais adequada para satisfazer as necessidades coletivas. Não se admite a opção arbitrária, destinada a beneficiar determinado fornecedor ou fabricante. (Grifo nosso).*

7.2.21. Quanto à explicação técnica para fundamentar a necessidade estrita da indicação, em conformidade com o princípio da imparcialidade, trata-se de uma atualização da solução atual para lidar com o aumento natural do tráfego de dados.

7.2.22. É importante esclarecer que a escolha pela continuidade da solução já adotada, da marca Palo Alto, se baseia na qualidade do serviço e nos resultados obtidos até o momento. Durante o período de 2020 a 2022, a nossa solução de firewall foi fundamental na proteção do ambiente de TI do TJCE, neutralizando com sucesso **1.275.454** *(um milhão, duzentos e setenta e cinco mil e quatrocentos e cinquenta e quatro*) ataques cibernéticos.

7.2.23. O desempenho da solução já utilizada por este órgão judiciário é compatível com a realidade do mercado internacional de Firewall de Rede de Dados, no qual a fabricante Palo Alto é uma das três principais classificadas no Quadrante Mágico do Gartner, mencionado na figura 7 deste Estudo Preliminar.

7.2.24. Outro fator a ser considerado é o tipo de solução desejada, que segue o modelo já utilizado por este órgão judiciário, ou seja, uma solução de Firewall para Data Center. Entre as opções disponíveis no mercado atualmente, esse modelo ainda é o mais adequado às necessidades do TJCE.

7.2.25. Por outro lado, o TCU, em várias decisões, tem se manifestado sobre a possibilidade excepcional de indicação de uma marca em licitações, desde que haja justificativas de natureza técnica "OU" econômica devidamente fundamentadas, como ocorre neste caso. Nessas situações, não há violação do princípio da igualdade nem restrições à competitividade do processo (Decisão n. 664/2001 - Plenário; Acórdão n. 1.010/2005 - Plenário e Acórdão n. 1.685/2004 - 2ª Câmara). (TCU, Acórdão 1.122/2010, Primeira Câmara, Rel. Min. Marcos Bemquerer Costa, DOU 12/03/2010).

7.2.26. A substituição da marca resultaria na perda do conhecimento adquirido pela equipe técnica da Secretaria de Tecnologia da Informação no uso da solução da fabricante Palo Alto.

7.2.27. Além disso, a existência de várias empresas do setor que fornecem os produtos em

questão e são autorizadas a comercializá-los, torna insignificante a alegação de restrição à competitividade.

7.2.28. Além disso, a indicação recai sobre uma marca consolidada no mercado, cujas características são essenciais para atender ao interesse público.

7.2.29. Portanto, qualquer questionamento relacionado a uma possível cláusula restritiva ao caráter competitivo do processo licitatório foi esclarecido, pois, como explicado detalhadamente, há correspondência com a justificativa técnica para utilizar a indicação proposta.

7.2.30. É importante observar que não se está limitando a competitividade nem violando a igualdade. Na verdade, trata-se de uma alternativa administrativa para selecionar um objeto que atenda adequadamente às necessidades, permitindo a continuidade do uso da marca já adotada.

7.2.31. Outro ponto a ser considerado para a justificativa da solução escolhida está relacionado aos esforços necessários ao substituir a solução de FWNG Palo Alto por outra de fabricante diferente, que são:

7.2.31.1. Avaliação da nova solução: Tanto a equipe técnica do TJCE quanto da empresa de Service Desk precisará realizar uma avaliação completa da nova solução de firewall para entender suas funcionalidades, recursos e compatibilidade com a infraestrutura existente.

7.2.31.2. Planejamento e design: Será necessário planejar a implementação da nova solução, levando em consideração as necessidades específicas do TJCE. Isso inclui o dimensionamento adequado dos recursos, design da arquitetura de rede e políticas de segurança.

7.2.31.3. Testes e validação: A equipe técnica terá que realizar testes rigorosos da nova solução para garantir seu desempenho, estabilidade e segurança. Isso pode incluir testes de carga, testes de vulnerabilidade e testes de compatibilidade com outros sistemas.

7.2.31.4. Configuração e integração: Uma vez que a nova solução tenha sido testada e validada, será necessário configurá-la de acordo com as necessidades específicas do TJCE. Isso inclui a definição de políticas de segurança, regras de firewall, configuração de VPN, integração com outros sistemas e dispositivos de rede, entre outros.

7.2.31.5. Migração de dados: A equipe técnica da contratada precisará planejar e

executar a migração dos dados e configurações importantes armazenadas na solução de firewall atual dados para a nova solução, garantindo a continuidade das operações e a integridade dos dados.

7.2.31.6. Treinamento e capacitação: A equipe técnica do TJCE precisará passar novamente por treinamento para adquirir o conhecimento necessário sobre a nova solução de firewall, suas características e melhores práticas de configuração e gerenciamento.

7.2.32. A substituição da atual plataforma Palo Alto em uso por outra poderá causar vários impactos no ambiente de TI do TJCE. Alguns possíveis impactos podem incluir:

7.2.32.1. Interrupção dos serviços: Durante o processo de migração, poderá haver interrupções temporárias nos serviços de rede e conectividade. Isso poderá ocorrer enquanto os firewalls estão sendo configurados, testados e integrados ao ambiente existente.

7.2.32.2. Tempo de aprendizado e adaptação: A equipe técnica do TJCE precisará se familiarizar com a nova solução de firewall, seus recursos e melhores práticas de configuração e gerenciamento. Isso pode exigir tempo de aprendizado e adaptação, o que pode impactar temporariamente a eficiência e produtividade da equipe.

7.2.32.3. Possíveis problemas de integração: Durante a substituição do firewall, podem surgir problemas de integração com outros sistemas e dispositivos de rede. Sendo necessário realizar testes abrangentes para garantir que a nova solução de firewall seja compatível e funcione corretamente em conjunto com outros componentes do ambiente de TI do TJCE.

7.2.32.4. Impactos nos processos de negócios: Dependendo da natureza dos serviços afetados pela substituição do firewall, pode haver impactos nos processos de negócios do TJCE. Por exemplo, se houver interrupções prolongadas nos serviços de rede, pode afetar a comunicação interna e externa, o acesso a aplicativos e sistemas, entre outros.

7.2.33. Estima-se que, além do prazo de entrega de novos equipamentos, um provável projeto de substituição da atual solução de NGFW poderá durar, pelo menos, entre 30/60 dias úteis, requerendo o acompanhamento priorizado de profissionais de infraestrutura de TI e da Segurança da Informação-SI da SETIN. A priorização das atividades desses profissionais neste momento para o atendimento de um projeto de

migração, acabará impactando no atendimento de outras demandas.

7.2.34. Um exemplo de fracasso e problemas na troca de solução já implantada e consolidada foi o que ocorreu no Ministério Público do Estado do Amazonas (MPAM). Conforme consta no "*Diário Oficial Eletrônico • Manaus, Terça-feira, 31 de janeiro de 2023, n.º 2540*", no qual relata a recusa do Contrato Administrativo n.º 003/2022-MP/PGJ com a empresa que arrematou o pregão devido a quatro tentativas malsucedidas de implementação do firewall. Em resposta, a Comissão Permanente de Licitação (CPL) recebeu instruções para rescindir o contrato e considerar a convocação do licitante subsequente. Após a rescisão amigável, a empresa classificada na segunda posição foi identificada como a nova escolha técnica e financeira.

7.2.34.1. Objetivando ter mais detalhes e experiência do que ocorreu no MPAM, foi feito contato com o Setor de Infraestrutura e Telecomunicações (SIET) do referido órgão para tal consulta. O retorno que tivemos foi de que tal contratação realmente exigiu bastante da equipe do MPAM, desde a produção e aprovação do termo de referência até a implantação em si. Entretanto, com relação à primeira colocada, foi necessário cancelar porque, em resumo, eles não conseguiram migrar todos os serviços de forma satisfatória, com a efetividade e estabilidade esperadas. Que tal órgão também possuía Palo Alto anteriormente e coisas simples e corriqueiras já implantadas não conseguiram passar para a nova ferramenta sem problemas, exigindo diversos rollbacks. No final das contas, cancelaram o contrato com a primeira colocada e chamados o segundo lugar que ofertou equipamentos da própria Palo Alto e a migração aconteceu de forma tranquila.

7.2.35. Após a avaliação técnica, compreende-se que existem diversos riscos que podem afetar o êxito do processo, a disponibilidade dos serviços de TIC e a eficácia da solução de segurança em si. É notável que as demandas adicionais das áreas de infraestrutura de TI e da Segurança da Informação-SI, sejam elas de natureza operacional ou não, resultantes do aumento dos ataques cibernéticos e da ênfase no teletrabalho desde março de 2020 (início da pandemia), tiveram um impacto direto nas análises necessárias para conduzir esse tipo de processo.

7.2.36. Os principais riscos associados na migração de um NGFW são: indisponibilidade ou degradação no desempenho de sistemas críticos e novas brechas de segurança no ambiente.

7.2.37. Acontece que, todos os serviços críticos do Tribunal de Justiça do Ceará (PJE, SAJ, site institucional etc.) são disponibilizados para o grande público através de publicações que passam pelo NGFW (Next-Generation Firewall) atual.

7.2.38. Basicamente, estas publicações acontecem através do redirecionamento do tráfego do endereço IP de internet, que corresponde ao endereço de acesso do sistema em questão, para um IP da rede interna do TJCE, que corresponde a um servidor onde o sistema está hospedado. Este redirecionamento é chamado de NAT (Network Address Translation).

7.2.39. Cada fabricante de NGFW utiliza um método diferente para separar estas configurações de redirecionamento. A separação das regras de NAT das regras de segurança é uma característica distintiva dos NGFWs da Palo Alto. Essa abordagem tem várias vantagens:

7.2.39.1. Fluxo Lógico do Firewall: As regras de NAT fornecem tradução de endereço e são diferentes das regras de política de segurança, que permitem ou negam pacotes. É importante entender a lógica de fluxo do firewall quando ele aplica regras de NAT e regras de política de segurança para que se possa determinar quais regras são necessárias, com base nas zonas definidas;

7.2.39.2. Flexibilidade e Controle: A separação permite maior flexibilidade e controle na configuração do firewall. É possível configurar várias regras de NAT e o firewall avalia as regras em ordem, de cima para baixo. Uma vez que um pacote corresponde aos critérios de uma única regra de NAT, o pacote não é submetido a regras de NAT adicionais.

7.2.39.3. Segurança Aprimorada: As políticas de segurança diferem das regras de NAT porque as políticas de segurança examinam as zonas pós-NAT para determinar se o pacote é permitido ou não. Como a própria natureza do NAT é modificar os endereços IP de origem ou destino, o que pode resultar na modificação da interface e zona de saída do pacote, as políticas de segurança são aplicadas na zona pós-NAT.

7.2.39.4. Redução de Erros de Configuração: A separação das regras de NAT e de segurança pode ajudar a reduzir os erros de configuração. Isso permite que se implemente rapidamente as configurações em toda a infraestrutura do firewall.

7.2.39.5. Automatização: A Palo Alto Networks permite a automatização da configuração de tudo, desde políticas de segurança (ou seja, regras de firewall) e

regras de NAT até políticas de descriptografia e todos os objetos usados dentro dessas regras e políticas.

7.2.40. Em alguns fabricantes, tais configurações são feitas juntamente com as configurações de itens de segurança (IPS, WAF, Controle de Aplicação, Antimalware, etc). Essa abordagem por si só já traz alguns riscos:

7.2.40.1. Complexidade de Configuração: A combinação de regras de NAT e de segurança aumenta a complexidade da configuração do firewall. Isso pode levar a erros de configuração e tornar mais difícil a identificação e resolução de problemas.

7.2.40.2. Riscos de Segurança: Embora o NAT possa fornecer alguma obscuridade dos endereços internos e ativos, ele não é um mecanismo de segurança. Portanto, depender do NAT para a segurança pode levar a uma falsa sensação de segurança.

7.2.40.3. Gerenciamento de Políticas: A gestão de políticas pode ser mais desafiadora quando as regras de NAT e de segurança estão combinadas. Isso pode tornar mais difícil para os administradores de rede entenderem e gerenciarem efetivamente as políticas do firewall.

7.2.40.4. Desempenho do Firewall: A combinação de regras de NAT e de segurança pode afetar o desempenho do firewall. Cada regra adicional aumenta a carga de processamento no firewall, o que pode levar a uma diminuição do desempenho.

7.2.40.5. Flexibilidade Limitada: Ter as regras de NAT e de segurança juntas pode limitar a flexibilidade na configuração do firewall. Por exemplo, pode ser mais difícil implementar políticas de segurança específicas sem afetar as regras de NAT existentes.

7.2.41. Portanto, a migração da tecnologia e abordagem atual para outro fabricante que utilize a que foi relatada acima, trás consigo os mesmos riscos listados para ela. E mesmo a migração para outro fabricante que utilize a mesma abordagem, pode trazer outros riscos, como por exemplo:

7.2.41.1. Incompatibilidade de Regras – Fabricantes diferentes podem ter abordagens únicas na implementação de regras de segurança, mesmo quando a funcionalidade é semelhante. Isso pode levar a interpretações distintas e incompatibilidades nas configurações.

7.2.41.2. Formatos e Sintaxes Variáveis – Cada fabricante utiliza formatos e sintaxes específicos para suas regras. A migração entre NGFWs pode resultar em

dificuldades na conversão, com potencial para erros que comprometem a eficácia das políticas.

7.2.41.3. Perda de desempenho – NGFWs podem implementar algoritmos distintos para inspeção de tráfego, trabalhar de forma distinta a alocação de recursos, como CPU e memória, e recursos específicos de otimização, como compressão de dados e aceleração de hardware, podem ser implementados de maneira diferente em cada NGFW. A mudança de um fabricante para outro portanto pode resultar em variações no processamento de pacotes, afetando fatores como latência e o throughput.

7.2.42. Já a migração realizada entre equipamentos do mesmo fabricante, conta com benefícios e garantias tais como:

7.2.42.1. Compatibilidade de Configuração: Equipamentos do mesmo fabricante seguem padrões de configuração iguais. Isso facilita a migração, pois as configurações existentes podem ser diretamente transferidas.

7.2.42.2. Ferramentas de Migração Específicas: Todos os fabricantes oferecem ferramentas específicas para migração entre seus próprios equipamentos, simplificando o processo e minimizando o tempo de inatividade.

7.2.42.3. Consistência de Recursos: Recursos e funcionalidades são consistentes dentro da linha de produtos de um fabricante. Ao migrar para um dispositivo semelhante, não há probabilidade de encontrar discrepâncias ou incompatibilidades.

7.2.42.4. Suporte Técnico Especializado: O suporte técnico do fabricante pode fornecer assistência especializada na migração entre seus próprios dispositivos, agilizando o processo e garantindo uma transição mais tranquila.

7.2.43. Diante disso, a migração entre equipamentos do mesmo fabricante é mais segura e menos propensa a causar indisponibilidade ou degradação no desempenho de sistemas críticos. Isso ocorre porque os fabricantes projetam seus dispositivos para trabalhar juntos de maneira integrada, o que minimiza a probabilidade de incompatibilidades ou conflitos que podem levar a interrupções. Além disso, os administradores de rede já estão familiarizados com a plataforma, o que reduz a probabilidade de erros de configuração que podem afetar o desempenho. Em termos de segurança, a migração dentro do mesmo fabricante permite que as organizações aproveitem as mesmas políticas de segurança e práticas recomendadas, minimizando a chance de novas

brechas de segurança.

7.2.44. Reforça-se o que foi citado no item **7.2.34.** referente ao exemplo de fracasso e problemas na troca de solução já implantada e consolidada que ocorreu no Ministério Público do Estado do Amazonas (MPAM).

7.2.45. Fatores agravantes, os constantes e diários ataques cibernéticos que o TJCE sofre exigem que as equipes infraestrutura de TI e de SI se concentrem nas operações de segurança.

7.2.46. Por último, mas não menos importante, a atual solução de segurança desempenha um papel fundamental ao realizar bloqueios contínuos e automáticos de ameaças que buscam explorar as vulnerabilidades dos ativos de TIC do TJCE. Essas ameaças podem resultar na indisponibilidade desses ativos, bem como em possíveis vazamentos de dados, sejam eles pessoais ou não.

7.2.47. Consideramos que outras soluções já citadas têm o potencial de afetar a eficácia dos serviços oferecidos pela solução atual de NGFW. Além disso, ao consolidar vários serviços em uma única e complexa solução, o conceito de "aprisionamento tecnológico" surge, trazendo consigo vários riscos de substituição que exigem uma análise mais abrangente para garantir precisão e a possível identificação de custos indiretos. É fundamental compreender os diferentes tipos de custos envolvidos na troca e o conceito de "aprisionamento" relacionado a esses custos, a fim de minimizar os riscos da melhor maneira possível. Portanto, parece sensato e aconselhável evitar mudanças na solução atual, uma vez que a prioridade é manter a integração com as unidades. Dessa forma, evitaremos retrabalhos e/ou adaptações que poderiam aumentar os custos a curto prazo.

7.2.48. Vale destacar da relação dos órgãos públicos que foram citados anteriormente, os que constam a seguir, que em seus estudo técnicos e avaliações, justificaram e fundamentaram os motivos que os levaram a decidir pela não troca de suas soluções de firewalls já em uso. Segue relação com os detalhes que constam nos referidos estudos técnicos:

7.2.48.1. TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL – Estudos Preliminares – Pregão Eletrônico N.º 1/2023 Contratação de empresa especializada no fornecimento, instalação e configuração de sistema integrado de segurança para proteção de perímetro de rede licenciado com funcionalidades de "Next-Generation Firewall" (NGFW), com gerenciamento centralizado e

armazenamento de logs, incluindo serviços de migração e garantia técnica do fabricante por 60 (sessenta) meses.

7.2.48.1.1. *A referida Corte em seu estudo técnico preliminar optou por licitar solução de NGFW da fabricante da atual solução em uso naquele Tribunal, a fabricante FortiNet. Justificando que: De relevância em tal cenário, faz-se importante salientar que a aquisição de sistema NGFW de outro fabricante implicaria na troca completa do sistema NFGW ora implantado no ambiente de produção de segurança de rede do Poder Judiciário. Embora possa ser alegado que possam existir alternativas no mercado de TIC, as evidências coletadas por essa área técnica sugerem que as plataformas FortiGate e FortiManager do fabricante Fortinet tem atendido de forma adequada aos casos de uso empregados pelo Poder Judiciário no que tange aos requisitos técnicos que devem ser atendidos por um sistema da categoria NGFW desde seu comissionamento na arquitetura de serviços de segurança em uso. Além disso, ao se modificar a solução, existiriam custos adicionais de capacitação do corpo técnico, uma vez que um simples treinamento em nova solução não seria suficiente para dar o mesmo embasamento na solução ao corpo técnico que foi adquirido durante praticamente 4 anos de experiência, sem falar na readequação dos procedimentos operacionais e processos de trabalho relativos à solução de segurança a ser implantada.*

7.2.48.2. TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO – Estudos Preliminares – PROAD: 3928/2023 – REGISTRO DE PREÇOS para aquisição de solução de para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, também contemplando atualização de assinaturas de proteção e suporte técnico em regime 24x7, pelo prazo de, no mínimo, 24 (vinte e quatro) meses, incluindo ainda serviços de instalação e treinamento.

7.2.48.2.1. *A referida Corte em seu estudo técnico preliminar optou por licitar solução de NGFW da fabricante da atual solução em uso naquele Tribunal, a fabricante CheckPoint. Justificando que: a aquisição de um novo Firewall, que pode ser tanto em modo On-premise, com a compra de novos equipamentos, ou o modo on-cloud, com o aluguel de Firewall como serviço. Neste caso, independente do cenário, substituir a solução de Firewall traz as seguintes vantagens. Atualização do produto, com possíveis*

novas funcionalidades e relatórios para facilitar a operação e melhorar o funcionamento. Possibilidade de reavaliar a capacidade da solução. Por outro lado, implica também em desvantagens, como: Riscos de migração, que inclui ameaças como parada dos sistemas ou até, em um cenário mais grave, perda de dados. Em caso de mudanças de fornecedor, o desconhecimento sobre operação e funcionamento da solução, reiniciando a curva de aprendizado. Assim, cientes que a solução atual ainda atende às necessidades técnicas dos Tribunais participantes, e considerando as vantagens e desvantagens de cada cenário apresentado, especialmente o risco de interrupções de sistemas ou até perda de dados por conta de problemas em migração de fornecedor Firewall e a curva de aprendizado em caso de troca de fornecedor, a equipe de planejamento recomenda a manutenção da solução de Firewall atual por mais dois anos.

7.2.48.3. TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS – PREGÃO ELETRÔNICO/SRP Nº. 039/2023-TJAM: Registro de Preços para eventual renovação do suporte e das licenças do cluster de equipamentos de Next-Generation Firewall, assim como expansão da solução de firewall para as unidades descentralizadas do Tribunal de Justiça do Estado do Amazonas (TJAM), compreendendo suporte técnico e garantia pelo período de 60 meses, incluindo serviços de instalação, configuração e treinamento oficial do fabricante.

7.2.48.3.1. *O TJAM em seu pregão manteve em uso seus dois applicanes Palo Alto 5220 e adquiriu outros 02 appliances Palo Alto 5410. Descrevendo também sobre a expansão da solução de firewall como a alternativa mais apropriada para o TJAM, permitindo que o Tribunal mantenha toda as barreiras de proteção já implementadas e proporcione um incremento nessas barreiras com a expansão desses recursos de proteção contra os ataques cibernéticos que crescem assustadoramente e que atingem diversos outros órgãos e tribunais, como por exemplo, os ataques ocorridos no Supremo Tribunal Federal (2021), Superior Tribunal de Justiça (2021), Tribunal de Justiça do Estado do Rio Grande do Sul (2021), Tribunal de Justiça do Estado do Amazonas (2021), TRT 4 Região (2021), TRF 3 Região (2022), TRT-ES (2022), Tribunal de Contas do Ceará (2022), Justiça Federal de Pernambuco (2022), entre outros. Além das razões apresentadas,*

existem as necessidades em manter a eficácia, integração e a qualidade da plataforma de segurança em um ambiente de TI complexo como o do TJAM, bem como reduzir possíveis impactos gerados pela indisponibilidade dos serviços e sistemas de TIC e também evitar a reimplementação das barreiras de seguranças já em operação do TJAM. Tal contratação tem o objetivo de aumentar a estabilidade e a confiabilidade da solução de Firewall existente no TJAM, que atua na proteção da borda de Internet, na proteção dos ativos de rede do datacenter, bem como permitir a expansão da tecnologia de firewall do TJAM, permitindo gerenciamento centralizado através do Panorama. Buscando também preservar os investimentos realizados no ambiente do TJAM, pois durante o período de vigência dos equipamentos o corpo técnico da SETIC adquiriu amplo conhecimento e experiência na solução de segurança atual, permitindo o desenvolvimento de projetos específicos para levar segurança aos usuários internos e remotos do TJAM. Relacionando como benefícios: Manter a estabilidade, confiabilidade e proteção da segurança do tráfego de perímetro e da borda de acesso à Internet, através da renovação da solução de segurança atual que se encontra em pleno funcionamento; Expandir os recursos de segurança da tecnologia de firewall do TJAM, com recursos suficientes para permitir gerenciamento centralizado através do Panorama; Introduzir o conceito de Zero Trust na arquitetura nas unidades descentralizadas do TJAM, permitindo que todo o Judiciário Amazonense esteja atualizado com as melhores práticas e referências quanto à segurança da informação; Dispor de equipamentos e soluções com tecnologias e recursos atualizados para o enfrentamento dos riscos de segurança no ambiente de TI; Prover a garantia da solução de segurança em firewall com eficaz substituição de peças dos equipamentos, para que seja mantida a alta disponibilidade das operações; Garantir o nível de suporte técnico necessário para atender um ambiente corporativo complexo e robusto como o do TJAM; Aperfeiçoar a detecção e a diminuição do tempo respostas às ameaças cibernéticas contra o ambiente do TJAM; Obter suporte adequado do fabricante quanto às necessidade de aperfeiçoamento, adoção das melhores práticas na solução de segurança e resoluções de problemas.

7.2.48.4. TRIBUNAL REGIONAL FEDERAL DA 5ª. REGIÃO, Pregão Eletrônico N.º

19/2022.

7.2.48.4.1. *ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO – Dentre os levantamentos feitos das alternativas o TRF5 elencou a "Aquisição de nova solução" com a seguinte descrição: "...existe a possibilidade de atrasos na contratação e implantação da nova solução.".*

7.2.48.4.2. *Outra solução elencada foi "Renovação da solução existente", com a seguinte descrição: "A solução atual, do fabricante Palo Alto, vem funcionando a contento e está bem adaptada às regras de negócio do Tribunal.... Pelos motivos já expostos e após análise dos possíveis cenários que atenderiam a demanda especificada, ficou estabelecido como cenário mais vantajoso para a Administração a renovação da solução de Firewall atual.".*

7.2.48.5. TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO, Pregão Eletrônico N.º 73/2022.

7.2.48.5.1. *O TRE-PE no ANEXO I - EDITAL DO PREGÃO N.º 73/2022 – ELETRÔNICO do TERMO DE REFERÊNCIA elencou os motivos de manter a atual solução em uso que em resumo disse: A decisão de padronizar a rede para a foi motivada por diversos fatores. Isso inclui a manutenção do investimento realizado, a expertise da equipe na solução em uso, gargalos e problemas de desempenho nos firewalls de outra fabricante, inadequações nos registros de log, requisitos da ENSEC-PJ, e a busca por integração e melhoria no controle de segurança da informação. A decisão visou integrar conhecimento, equipamentos, softwares e funcionalidades do fabricante, proporcionando maior eficiência e segurança à rede de dados do TRE-PE. Ou seja, o órgão optou por não trocar a solução já em uso. Também destaca as possíveis ameaças associadas à troca de marca ou fabricante, como a complexidade na substituição e ameaças à estabilidade de serviços críticos. Aponta desafios técnicos, custos indiretos, interrupções em projetos existentes e a necessidade de adquirir novo conhecimento. A análise preliminar destaca a complexidade da decisão, considerando características similares entre fabricantes líderes e alertando para custos indiretos difíceis de mensurar. Enfatiza que a substituição exige planejamento estratégico e pode introduzir conflitos com a solução atual, além de estimar que a migração de um ambiente complexo pode levar de 30 a 45 dias úteis.*

7.2.48.6. TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ, Pregão Eletrônico Nº 65/2022.

7.2.48.6.1. *O TJPR em seu pregão manteve em uso seus dois applicanes Palo Alto 5220 e adquiriu outros 02 appliances Palo Alto 5420. O órgão em seu Estudo Técnico Preliminar elencou os motivos de manter a atual solução em uso que em resumo disse: Atualmente o TJPR dispõe de uma solução de Firewall Next Generation Firewall (NGFW) de alta disponibilidade que atua simultaneamente na proteção da rede interna corporativa, proteção do ambiente de servidores (perímetros) e na proteção borda de acesso à Internet. Esta solução é fundamental para prevenção de ataques maliciosos, análise e controle de acessos aos sistemas e serviços digitais essenciais deste Tribunal. Este firewall também é responsável por exercer as funções de prevenção de intrusão na rede com IPS (Intrusion Prevention System), controle de trafficshapping e QoS (Quality of Service) do tráfego de rede e Internet, identificação de usuários e grupos, decriptografia de SSL, filtragem de conteúdo Web, análise de malware e VPN (Virtual Private Network). Este último elemento foi fundamental para política de trabalho remoto adotada pelo DTIC e TJPR e que permitiu a continuidade dos trabalhos, mesmo em tempos de pandemia da COVID-19. A solução atual é composta de hardware e software, terá o seu licenciamento de software, suporte técnico especializado e período de garantia expirado em Março de 2023, necessitando de uma renovação para manter a estrutura atual de proteção. Além de manter as funções de proteções atuais, será necessário uma expansão nas ferramentas e mecanismos de segurança para fazer frente ao considerado aumento do número de ataques cibernéticos. Outro ponto relevante a ser considerado é a necessidade de acompanhar o avanço tecnológico realizado pelo DTIC, onde as principais aplicações do TJPR, tais como Projudi, SEI e Portal, fazem uso de estrutura de contêiner, sendo necessário a amplificação de ferramentas e mecanismos de segurança específicas para proteção deste ambiente altamente crítico. O DTIC, através deste projeto, direciona os seus esforços para perseguir uma abordagem moderna de segurança, chamada de Zero Trust, ou seja, nunca confiar, sempre verificar quem realiza o acesso. Este é um novo paradigma para implementar cibersegurança. O Zero Trust consiste em substituir os*

pressupostos implícitos sobre quem é confiável com decisões explícitas tomadas cada vez que alguém ou algo tenta acessar ou usar recursos confidenciais. Para tal realização será renovado um cluster de alta disponibilidade da solução de Next Generation Firewall (NGFW), contemplando o licenciamento de software, suporte especializado e garantia. Este cluster será realocado para função de proteção da borda de Internet, inspecionando o controle acesso à Internet dos usuários internos, bem como os acessos provenientes dos usuários externos que consomem os serviços disponibilizados pelo TJPR. Nestes equipamentos, também continuarão sendo prestados os serviços de IPS (Intrusion Prevention System), NAT (Network Address Translate), VPN (Virtual Private Network), Filtro de URL, Traffic-shapping, entre outros. Destaca-se que durante o período de vigência dos equipamentos, o Departamento de Tecnologia da Informação e Comunicação adquiriu amplo Know-How sobre a solução de segurança atual, acrescentando boas práticas de uso e o desenvolvimento de projetos customizados que agregam segurança para os usuários internos e remotos do TJPR, além da integração com as ferramentas existentes deste Órgão. Avançando para o caminho do Zero Trust, este projeto contempla expansão do cluster de alta disponibilidade para incrementar a função de proteção do data center do TJPR, trazendo além das funções já mencionadas no cluster atual, a capacidade de microsegmentação [3] de rede no ambiente mencionado. Na estrutura atual temos à arquitetura de segmentação de rede que trata da divisão das redes de data center em vários segmentos ou sub-redes baseando-se na confiança do ativo. Esta abordagem permite o controle de fluxo entre sub-redes com base em políticas granulares de Firewall. No entanto, nesta arquitetura à inspeção inter-rede ou dentro do perímetro é insuficiente, possibilitando, em caso de ataques cibernéticos, um movimento lateral leste-oeste dentro do perímetro. A microsegmentação permite criar zonas seguras mais detalhadas em ambientes de data center, fornecendo mecanismos que isolam os ativos e os protegem separadamente, trazendo um controle ainda mais fino e granular. Outro ponto relevante deste projeto é a aquisição de ferramenta com capacidade de realizar microsegmetação, análise de vulnerabilidade, monitoramento, detecção de ameaças em tempo real e proteção das

aplicações Web do TJPR, através de segurança na camada de aplicação no ambiente de contêiner. Atualmente, as principais aplicações e serviços disponibilizados pelo Tribunal fazem uso de contêiner, tais como Projudi, SEI, sendo necessária a expansão para este contexto. O Tribunal de Justiça do Paraná (TJPR) utiliza a plataforma de segurança da Palo Alto Networks há mais de 5 anos, mantendo estabilidade e confiabilidade na infraestrutura. O projeto visa expandir as soluções de segurança para acompanhar os avanços tecnológicos do TJPR e suportar o aumento da capacidade dos equipamentos de rede. A contratação é considerada viável para manter a eficácia, integração e qualidade da plataforma, reduzindo impactos pela indisponibilidade de serviços e evitando retrabalhos com mudanças de solução e migrações.

7.2.48.7. PREGÃO ELETRÔNICO Nº 37/2023/TCE-RO, cujo objeto é: Contratação de empresa para fornecimento de Solução de Segurança de Rede Palo Alto "NGFW" (Next Generation Firewall), com gerência centralizada de administração e retenção de logs, incluindo subscrições instalação, migração de configurações, suporte, garantia, repasse técnico e atualizações pelo período de 36 (trinta e seis) meses.

7.2.48.7.1. *O Tribunal de Contas do Estado de Rondônia (TCE-RO) cita e seu Estudo Técnico Preliminar que: Implementou, desde 2014, a solução de firewall da fabricante Palo Alto, reconhecida repetidamente como líder no mercado de Next-Generation Firewall (NGFW) pelo Gartner. Ao longo dos quase 10 anos de uso, a solução demonstrou extrema robustez e estabilidade, sem incidentes de indisponibilidade, travamento ou falha de componentes. Além de oferecer recursos avançados de segurança, a solução evoluiu continuamente para enfrentar desafios atuais, com atualizações em 2022, que incluíram novas versões de firmware com melhorias na filtragem de URL, segurança de DNS, segurança de IoT e a introdução de recursos de inteligência artificial para tratar ameaças, além de aprimorar o recurso de Prevenção contra Perda de Dados (DLP). Segundo o Gartner, os firewalls da Palo Alto Networks são considerados a referência mais alta em recursos de segurança avançados, detecção e prevenção de ameaças. A equipe de infraestrutura da SETIC já está familiarizada com a operação e manutenção da solução. Normas e instruções técnicas da área de tecnologia orientam*

que as compras devem seguir o princípio da padronização, quando possível, desde que haja compatibilidade de especificações técnicas e de desempenho. Isso visa aproveitar treinamentos, reduzir custos de manutenção, facilitar substituições e diminuir os custos de implantação, manutenção e treinamento de mão-de-obra. O TCE-RO busca manter a padronização em seu ambiente tecnológico, garantindo eficiência e efetividade nos serviços oferecidos. A padronização também é destacada como e eficiente na manutenção da solução, contribuindo para melhor alocação de recursos públicos, melhoria nas atribuições e continuidade dos serviços de tecnologia fornecidos pela SETIC aos usuários internos e externos do TCE-RO.

7.2.48.8. TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO – Pregão Eletrônico N. 47/2020 - Registro de preço para aquisição de solução de proteção de rede Next Generation Firewall (NGFW);

7.2.48.8.1. *O TJAM em seu pregão manteve em uso seus dois applicanes Palo Alto 3050 em H/A e adquiriu outros 02 appliances Palo Alto 5220. Em sua avaliação técnica sobre as soluções possíveis destacou que "Solução 3: Atualização do atual ambiente e aquisição de equipamento de maior capacidade: ...não necessita: retreinamento da equipe (apenas atualização dos conhecimentos), retreinamento de usuários, reinstalação da VPN. Além de apresentar diversos benefícios diretos, em especial no que se refere à continuidade das soluções centralizada de segurança NGFW, não comprometendo a disponibilidade, integridade, confidencialidade e autenticidade da informação, bem como integração e gerenciamento centralizado através de software de gerência e armazenamento de logs (já adquirido e em funcionamento).". O TJAM também ressalta que a solução de Next Generation Firewall atualmente em uso pelo órgão foi adquirido e instalado no ano de 2017 e encontra-se em funcionamento. É o principal ativo de segurança sendo responsável pela inspeção do trafego da rede interna e da Internet. Com a crescente necessidade de expansão/aumento de velocidade de links de comunicação, tanto da rede MPLS quanto da Internet, cresceu também a utilização de recursos desta plataforma de segurança Firewall (NGFW), sendo necessário o crescimento deste appliance para uma solução que tenha as mesmas características, porém*

com mais poder de processamento. Necessidade do Tribunal de Justiça do Maranhão, em continuar fornecendo alta disponibilidade, integridade e confidencialidade em seus sistemas de informação, como o processo Judicial Eletrônico (PJE), e equipamentos computacionais diante da Rede Mundial de Computadores, Internet, onde novas técnicas de invasão e captura de informações por parte de pessoas e grupos mal intencionados. Assim, este Tribunal precisa estar sempre atualizado e preparado tecnicamente para enfrentar essas tentativas de captura de dados, tanto de forma ostensiva quanto preventiva. Necessidade de prover políticas de segurança da informação personalizadas para: usuários, grupos de usuários, servidores, estações de trabalho, portas, protocolos e aplicações. Permitindo uma otimização dos serviços oferecidos pelo TJMA. Necessidade de manter um ambiente para os usuários trabalharem com segurança e eficácia em locais fora da rede do TJMA, através de conexões de Rede Privada Virtual (VPN - do inglês Virtual Private Network). Continuar provendo infraestrutura de comunicação de dados segura para suporte à soluções de Vídeo Conferencia, via Internet, utilizadas na realização de audiências. O TMAM também ressaltou as JUSTIFICATIVAS PARA A PADRONIZAÇÃO E MANUTENÇÃO DA MARCA como sendo: Em 2017 o TJMA iniciou um processo de atualização dos Applainces de proteção de rede que compõem sua infraestrutura (Firewalls), juntamente com um software para gerenciamento centralizado dos mesmos. Com intuito de garantir o melhor desempenho, disponibilidade e estabilidade da Rede Corporativa que cada vez mais está sendo utilizada para tráfego sigiloso e sensível dos Sistemas de Processo Judicial Eletrônico, dos Sistemas Administrativos e Financeiros, além de todo trafego das Unidades Judiciarias do Estado(Fóruns, Comarcas e Juizados), que é centralizado na SEDE do TJMA. Assim faz-se necessário o uso de políticas, protocolos e tecnologias que visam principalmente garantir a segurança das informações e o melhor desempenho dos serviços e aplicações, e por isso estaremos adotando a prática de padronização dos equipamentos de Firewall. A criação de politicas de segurança, analise do trafego, acesso dos clientes VPN, padronizações e especificações criadas pelo TJMA, está estreitamente ligado às características próprias de cada componente e ao conjunto da

solução adotada. Diferentes fabricantes e, mesmo, diferentes modelos de equipamentos de um mesmo fabricante apresentam-se com diferentes parâmetros de configuração e de otimização. Consequentemente à aquisição de soluções de proteção de rede Next Generation Firewall(NGFW), de fabricantes diferentes (heterogeneidade), obriga uma reconfiguração dos equipamentos, reconstrução das politicas, reinstalação de todos os clientes de VPN, instruir novamente os usuários para utilização da VPN, além da curva de aprendizado da própria equipe de Administração de rede. A falta uma padronização também não garante gerenciabilidade do parque, ficando, dessa forma, comprometida a interoperabilidade e o gerenciamento integrado. Além das razões acima, justifica-se a manutenção da marca: • Investimento: com a padronização do fabricante escolhido, o TJMA garante o investimento anteriormente efetuado em : treinamento e equipamento, pois os equipamentos já adquiridos pelo TJMA são deste fabricante, o que convém com o principio da economicidade; • Gerenciamento: o software de gerenciamento já adquirido anteriormente pelo TJMA é totalmente compatível com estes equipamentos, assim todos os equipamentos podem ser configurados e administrado por uma única console proporcionando uma visão do tráfego da rede, dos acessos, tentativas de intrusão e etc, facilitando a administração e solução de eventuais incidentes/problemas; • Configuração e conhecimento: a padronização dos equipamentos auxilia e facilita a administração da rede, devido a utilização de apenas um sistema operacional em todos os equipamentos, ou seja, uma única interface de comandos a serem utilizados para configuração de toda a rede. Com isso, torna-se mais fácil o treinamento, a gestão do conhecimento, e auxilia na redução do tempo de configuração e reparo. Este convém a citar o principio da eficiência. • Desempenho: soluções de mesmo fabricante permitem a utilização de recursos proprietários, ou seja, recursos que garantem maior desempenho dos equipamentos, mas que só podemos utilizá-los com a homogeneidade da malha, como configurações de alta disponibilidade essências às necessidades desse Tribunal.

7.2.48.9. MINISTÉRIO DA ECONOMIA INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO - Pregão Eletrônico N. 4/2023 - Contratação de solução de tecnologia da informação e

comunicação para renovação das subscrições da solução de segurança da informação Ngfw (Next Generation Firewall), composta por 04 (quatro) equipamentos, modelos pa-5220, do fabricante Palo Alto Networks, pelo período de 12 (doze) meses, incluindo serviços agregados de tratamento de incidentes, para atender às necessidades do instituto nacional de metrologia, qualidade e tecnologia (Inmetro), conforme condições, quantidades e exigências estabelecidas no edital e seus anexos;

7.2.48.9.1. *O INMETRO em seu estudo técnico enfatiza que a substituição de sua atual solução de NGFW incluem possíveis reduções nos custos de aquisição e manutenção, assim como a adição de funcionalidades inexistentes na solução atual. No entanto, várias ameaças foram identificadas, como uma equipe de Segurança da Informação com recursos limitados, orçamento restrito, complexidade na substituição devido à importação de equipamentos e prazos de entrega longos, migração manual de mais de 500 regras de firewall, customizações e capacitação da equipe, potencial impacto nos prazos e riscos de falhas durante a reconfiguração de zonas de bloqueio, definições de segurança, controle de tráfego e outras configurações. A alteração na solução de VPN e a necessidade de substituir ou implementar certificados nas estações também são desafios, especialmente considerando que parte da equipe está em teletrabalho. Incluindo ameaças e riscos do tipo: Equipe de Segurança da Informação sobrecarregada, podendo exigir a contratação de serviços terceirizados. Orçamento restrito para investimentos em 2022. Complexidade na substituição devido a prazos de entrega de equipamentos, migração de regras e customizações. Necessidade de recriar mais de 500 regras de firewall manualmente. Recriação das customizações das telas de bloqueio e alerta do filtro web. Necessidade de capacitar a equipe na nova plataforma, resultando na perda de conhecimento tácito. Possível recriação manual de configurações, impactando prazos e gerando riscos. Substituição de certificados para decrypt e alterações nos softwares de VPN para profissionais em teletrabalho. Ou seja, a substituição da solução atual é considerada arriscada devido aos desafios técnicos e impactos operacionais. O estudo destaca a importância de evitar mudanças que possam resultar em retrabalhos e sugere a necessidade de avaliar adequadamente os recursos*

profissionais e reduzir riscos associados aos custos de novas ativações.

7.2.49. Como é possível notar, a equipe técnica de planejamento deste projeto não é a única em entender e decidir que no atual momento, não é ideal fazer a troca de fabricante da atual solução de Next Generation Firewall em uso no TJCE;

7.2.50. Por fim, a escolha da solução 01, com vigência das subscrições por 60 (sessenta) meses, é a mais apropriada. Também avaliando a necessidade de adequação dos recursos profissionais para atender às demandas, bem como lidar com os outros aspectos relacionados à troca do fornecedor/fabricante e reduzir os riscos associados.

8. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

8.1. Aquisição de solução de alta disponibilidade de Next Generation Firewall com gerenciamento centralizado e integrado, com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local ou remoto, no modelo 24x7, pelo prazo de 60 (sessenta) meses; incluindo serviços de instalação e treinamento.

8.2. A solução de alta disponibilidade deve ser composta por dois equipamentos (appliances) que funcionam em cluster, especificamente projetados para atuar como Next Generation Firewall, com hardware e software fornecidos pelo mesmo fabricante.

8.3. Cada equipamento (appliance) integrante da solução de alta disponibilidade deve possuir licença ativada para suportar, de maneira simultânea e integrada, as seguintes funcionalidades: firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), administração de largura de banda de serviço de Internet (QoS – Quality of Service), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL, controle de transferência de arquivos, roteamento estático e dinâmico, NAT e com garantia durante 60 (sessenta) meses. Devem ser as **ESPECIFICAÇÕES MÍNIMAS** abaixo e as **CARACTERÍSTICAS GERAIS do ANEXO I – ESPECIFICAÇÕES TÉCNICAS.**

ESPECIFICAÇÕES MÍNIMAS	
Taxa de transferência do Threat Prevention	26 Gbps
Taxa de transferência da VPN IPsec	20 Gbps
Taxa de transferência de Inspeção SSL	7 Gbps
Sessões	3,5 Milhões

Novas sessões por segundo	250 mil
Sistemas virtuais	10
Fontes de alimentação	2
Armazenamento	480GB SSD
Interfaces 1G/2.5G/5G/10G	08
Interfaces 1G/10G SFP/SFP+	12
Interfaces 40G/100G QSFP+/QSFP28	04

8.4. A solução de gerenciamento centralizado deverá ser constituída de, no mínimo, um "appliance virtual", que é uma solução de software baseada em máquina virtual, seguindo os padrões estabelecidos pelo DMTF (Distributed Management Task Force). Alternativamente, poderá ser utilizado um sistema operacional desenvolvido pelo fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual. A instalação da solução de gerenciamento ocorrerá em um ambiente de virtualização e hardware pertencente ao TJCE.

8.5. É obrigatório que todos os equipamentos e seus componentes sejam novos, sem uso prévio, entregues em perfeitas condições de funcionamento e sem quaisquer sinais de danos físicos, tais como marcas, amassados, arranhões ou outras imperfeições. Além disso, devem ser acondicionados em suas embalagens originais.

8.6. Equipamentos que estejam no fim de sua vida útil ou não recebam mais suporte não serão aceitos. Além disso, é necessário que a solução tecnológica tenha sido lançada pelo fabricante dentro de um período de 12 a 36 meses, para evitar o risco do potencial de obsolescência do hardware.

8.7. Devido à complexidade das soluções de segurança, faz-se necessário manter um suporte técnico especializado, 24x7, com o objetivo de poder acionar um suporte técnico, obter recomendações de melhores práticas e assessoramento para o funcionamento da plataforma de solução de segurança.

8.8. Além disso, a garantia é fundamental para manter contratos de substituição de peças e equipamentos durante a vigência do contrato. Com o objetivo de garantir a continuidade dos serviços e a estabilidade do ambiente, é desejável que a contratada forneça um novo hardware, que seja equivalente ou superior, para ser utilizado em situações de falha de equipamento, falha de fabricação, degradação dos serviços ou qualquer outro tipo de problema com a solução. Essa disponibilidade de hardware adicional é crucial para assegurar que o ambiente não seja interrompido ou degradado por tempo indeterminado. A

contratada deve estar preparada para lidar prontamente com qualquer eventualidade, minimizando os efeitos adversos sobre o funcionamento do equipamento. A capacidade de resposta rápida e eficiente nessas situações é essencial para manter a integridade e a confiabilidade do ambiente do tribunal, garantindo que as atividades judiciais e administrativas possam ser conduzidas sem interrupções significativas.

9. JUSTIFICATIVA PARA O PARCELAMENTO DO OBJETO

9.1. A fim de garantir uma melhor gestão, gerenciamento e manutenção da solução de TIC oferecida, é necessário centralizar a aquisição em um lote único do fornecimento de equipamentos e os serviços de garantia de manutenção de todos os ativos, uma vez que eles fazem parte de uma solução única de segurança da informação. Se o objeto fosse parcelado, diferentes empresas poderiam ser responsáveis pela prestação de serviços de manutenção nos equipamentos, o que dificultaria a aplicação de penalidades aos contratados devido à dificuldade em separar as responsabilidades de cada empresa. Isso poderia levar a uma queda na qualidade dos serviços prestados em relação à infraestrutura da rede de dados.

10. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

10.1. Aquisição AQSETIN2023009, que trata da renovação da garantia do switch de núcleo.

10.2. Aquisição AQSETIN2023004, que trata de 24 links de conectividade para as Comarcas finais e Custodias do TJCE.

10.3. Aquisição AQSETIN2022010, que trata da contratação de serviços necessários para a implantação, funcionamento e manutenção de um Security Operations Center (SOC) pelo prazo mínimo de 36 meses. O SOC será composto por: Serviço de gestão de incidentes de segurança (Blue Team); Serviço de gestão testes de invasão (Red Team) e Serviços gerenciados de monitoramento e correlação de eventos de segurança da informação.

10.4. Contrato Nº 56-2019 ETICE, que trata da Ampliação e modernização do Serviço de Transmissão de Dados/Imagens e Voz através de Links de Comunicação.

10.5. Aquisição AQSETIN2024007 – Nova contratação de Link Internet IP e Voip ETICE;

10.6. Contrato n.º 96/2023, que trata da Aquisição de Solução de segurança de perímetro de appliances para vpn, softwares de gerência, serviço de instalação, bem como fornecimento de garantia dos equipamentos pelo período de 12 (doze) meses.

11. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Id	Bem/Serviço	Qtd.	Vlr. Unit Médio	Vlr. Total Médio
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	2	R$ 652.367,61	R$ 1.304.735,22
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	2	R$ 1.561.136,02	R$ 3.122.272,04
3	GlobalProtect subscription, for device in an HA pair, PA-5410 -60 meses – Palo Alto Networks	2	R$ 482.258,32	R$ 964.516,64
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	1	R$ 2.108.798,10	R$ 2.108.798,10
5	Panorama management software, 25 devices 60 meses – Palo Alto Networks	1	R$ 67.731,11	R$ 67.731,11
6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	1	R$ 77.022,64	R$ 77.022,64
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	2	R$ 562.446,50	R$ 1.124.893,00
8	Implantação da solução de Firewall	1	R$ 17.480,33	R$ 17.480,33
9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	1	R$ 13.440,28	R$ 13.440,28
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	1	R$ 193.740,09	R$ 193.740,09
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses	1	R$ 306.231,50	R$ 306.231,50
			Valor Total Global	**R$ 9.300.860,95**

12. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Os estudos preliminares demonstram que a solução descrita é tecnicamente possível e

necessária. Limitando-se aos aspectos técnicos, afirmo que a contratação pretendida é viável, pois existem fornecedores no mercado que oferecem regularmente os produtos necessários para atender às demandas da Administração, seguindo os princípios da economicidade e eficiência da administração pública.

Além disso, destaca-se que a contratação atende adequadamente às demandas de negócio formuladas, com benefícios adequados, custos compatíveis e economicidade, e com riscos administráveis. Diante dessas informações, conclui-se que a contratação é tecnicamente viável.

13. APROVAÇÃO e ASSINATURA

Heldir Sampaio Silva – 9630 Integrante Técnico	**Fábio de Carvalho Leite – 9594** Integrante Administrativo	**Cristiano Henrique Lima de Carvalho – 5198** Área Demandante e Integrante Demandante

Denise Maria Norões Olsen – 24667
Área de Tecnologia da Informação
Fortaleza, 03 de maio de 2024