TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO

Estudo Técnico Preliminar de STIC (ETP)[1]

Planejamento de Contratações de STIC

PROAD 12629/2024

PAC ID 15021

1. Introdução

O Estudo Técnico Preliminar tem por objetivo 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.

Observação: Por se tratar de processo nacional, foi realizada reunião de alinhamento inicial e definição de requisitos para o processo, conforme registrado no documento 54 do presente processo.

Integram esta licitação desde o início, na forma do § 5º, do art. 12, da Resolução CNJ nº 468/2022, tendo enviado DOD e quantitativos, que estão anexados ao Proad nos documentos de marcadores 15 a 34 e 52, os seguintes órgãos:

Tribunal Superior do Trabalho (TST);
Tribunal Regional do Trabalho da 1ª Região (TRT1);
Tribunal Regional do Trabalho da 3ª Região (TRT3);
Tribunal Regional do Trabalho da 4ª Região (TRT4);
Tribunal Regional do Trabalho da 5ª Região (TRT5);
Tribunal Regional do Trabalho da 6ª Região (TRT6);
Tribunal Regional do Trabalho da 7ª Região (TRT7);
Tribunal Regional do Trabalho da 9ª Região (TRT9);
Tribunal Regional do Trabalho da 10ª Região (TRT10);
Tribunal Regional do Trabalho da 11ª Região (TRT11);

[1] Em regra, conforme art. 28, da Resolução nº 468/2022, o DOD, ETP e TR serão disponibilizados em sítio eletrônico de fácil acesso e no Connect-Jus até a data de publicação do edital da licitação. A avaliação de acesso à informação contida em ETP, com informações sensíveis ou sigilosas, será analisada a critério de cada órgão do poder judiciário, respeitando os termos da Lei no 12.527/2011, e da Resolução CNJ no 215/2015.

Tribunal Regional do Trabalho da 12ª Região (TRT12);
Tribunal Regional do Trabalho da 13ª Região (TRT13);
Tribunal Regional do Trabalho da 14ª Região (TRT14);
Tribunal Regional do Trabalho da 15ª Região (TRT15);
Tribunal Regional do Trabalho da 16ª Região (TRT16);
Tribunal Regional do Trabalho da 17ª Região (TRT17);
Tribunal Regional do Trabalho da 18ª Região (TRT18);
Tribunal Regional do Trabalho da 19ª Região (TRT19);
Tribunal Regional do Trabalho da 20ª Região (TRT20) ;
Tribunal Regional do Trabalho da 21ª Região (TRT21);
Tribunal Regional do Trabalho da 22ª Região (TRT22);
Tribunal Regional do Trabalho da 23ª Região (TRT23).

2. Definição e especificação das necessidades e requisitos

2.1. Justificativa para a contratação

A solução de Firewall é um pilar para o funcionamento e também para a garantia da segurança da informação nas redes de dados, afirma-se isso por dois motivos principais:

- Para que o Firewall inspecione todo o tráfego da rede e cumpra seu papel como barreira de segurança, a melhor posição para instalação do Firewall é fazendo o papel de roteador principal dos dados, pois assim, filtra-se todo o conteúdo que circula entre as redes da instituição, e;

- No caso específico dos Tribunais do Trabalho, a solução de Firewall ainda provê os acessos via VPN, essenciais para o teletrabalho e prestação de serviços remotos de contratos terceirizados.

Como os processos trabalhistas, utilizando o Processo Judicial Eletrônico - PJe, e expedientes administrativos desta justiça especializada, são 100% digitais, a prestação jurisdicional depende totalmente da rede de dados e do acesso à Internet.

Essa dependência existe independente dos sistemas funcionarem localmente, em centros de processamento de dados dos Tribunais, ou em nuvem.

Considerando que o término do contrato de suporte vigente para os Firewall da maior parte dos Órgãos da JT ocorre em 2025 e a atual solução de Firewall destes Tribunais data de 2018. Ademais, a garantia atual destes equipamentos encerra entre 2025 e 2026.

Considerando ainda que no TRT12 o serviço de garantia e atualização de assinaturas de proteção e suporte técnico, bem como o serviço gerenciado mensal, contendo operação assistida, está sendo prestado através do contrato PE 9665/2023, que encerra sua vigência em outubro de 2025.

Por se tratar de solução essencial para a manutenção da prestação jurisdicional e para a proteção do ambiente tecnológico da JT, é imprescindível renovar a solução para manter o funcionamento dos sistemas de TIC, especialmente com relação aos sistemas críticos que necessitam de acesso externo.

2.2 Identificação das necessidades de negócio

- Manter a prestação jurisdicional por meio do funcionamento das redes corporativas, e;

- Promover a conectividade segura aos sistemas de TIC Jurídicos e Administrativos dentro e fora das instalações dos Órgãos via solução de Firewall.

- Manter a conformidade com o ATO CSJT.GP.SG.SETIC.CGTIC Nº 132/2022 que define “Solução de Firewall e Prevenção de Ameaças (NGFW)” como item orçamentário obrigatório.

- Aprimoramento da segurança cibernética, contribuindo para a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), Resolução Nº 396 de 07/06/2021.

2.3 Identificação das necessidades tecnológicas

- Promover o correto funcionamento das redes corporativas e sistemas de TIC;

- Garantir a segurança da informação nas redes corporativas e sistemas de TIC;

- Atualizar a solução de Firewall;

- Assegurar o funcionamento da solução de Firewall via Níveis Mínimos de Serviço;

- Promover conexões dos dispositivos externos às redes corporativas mais seguras, e;

- Melhorar a disponibilidade das redes de dados.

2.4 Requisitos necessários e suficientes à escolha da solução de TIC

Além de o Firewall ser um elemento comum a todas as redes de dados, a similaridade da Infraestrutura de TIC entre os órgãos da Justiça do Trabalho torna vantajosa a contratação conjunta para esta solução. Essa abordagem, via Atas de Registro de Preço, promove economia de escala e padronização de soluções, resultando em maior eficiência e economicidade para os órgãos públicos.

A manifestação de interesse dos órgãos que compõem a JT na contratação pode ser comprovada pela participação nas reuniões dos dias 14/11/2024 e 29/5/2025, bem como da participação do chat criado para este fim no Gmail, as atas das reuniões e a lista dos participantes do chat seguem no documento de marcador 54 do presente processo.

Para atender a necessidade de proteção das redes corporativas e sistemas de TIC da Justiça do Trabalho é necessário manutenção de solução de Firewall com alta disponibilidade contendo as seguintes características mínimas.

2.4.1. Solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall

A solução proposta consiste em instalar equipamentos de Next-Generation Firewall (NGFW) nos órgãos da JT de forma que, no mínimo, contenha as mesmas funcionalidades de proteção hoje em operação nos órgãos da JT e capacidade de operar como o roteador principal da rede de dados.

Além disso, o sistema deve inspecionar todo o tráfego interno, externo e VPN, aplicar políticas de segurança em tempo real e assegurar alta disponibilidade (HA) para evitar interrupções críticas nos serviços de TIC, com os seguintes requisitos técnicos essenciais:

a) Arquitetura de Alta Disponibilidade (HA) Ativo-Ativo, que é a capacidade do sistema funcionar mesmo em situações desfavoráveis, como quando um equipamento do conjunto que a compõe estraga ou sofre manutenção por meio das seguintes funções:

   i. Ser composto por um Cluster[2] com, no mínimo, dois appliances[3] operando em modo ativo-ativo, com balanceamento de carga distribuída.

   ii. Failover automático: Em caso de falha de um equipamento, o(s) restante(s) deve(m) assumir 100% da carga operacional sem interrupção.

   iii. Monitoramento cruzado (heartbeat) entre os nós para detecção imediata de falhas.

   iv. Recuperação transparente: Retorno automático ao modo balanceado após a correção da falha.

b) Inspeção Avançada de Tráfego (até Camada 7 - Aplicação), que é a garantia de proteção no acesso aos sistemas da forma que já ocorre atualmente.

   i. Deep Packet Inspection (DPI)[4] para análise de protocolos e aplicações.

---

[2] Um cluster (ou agrupamento) é um conjunto de computadores, servidores ou dispositivos interconectados que trabalham em conjunto para desempenhar uma função como se fossem um único sistema. O objetivo principal de um cluster é melhorar o desempenho, a disponibilidade (alta disponibilidade - HA) ou a escalabilidade de serviços e aplicações.

[3] Um appliance (ou appliance de rede / appliance de hardware) é um dispositivo ou equipamento de hardware dedicado a uma função específica, geralmente pré-configurado com software otimizado para desempenhar essa tarefa de forma eficiente e segura.

[4] Os equipamentos Firewall da Checkpoint instalados nos Tribunais da JT fazem Deep Packet Inspection (DPI). Ou seja, não analisa só cabeçalho, ips e portas dos pacotes. Em tese, os equipamentos verificam assinaturas, abrindo conteúdos criptografados.

ii. Inspeção SSL/TLS (decrypt & inspect) para identificar ameaças ocultas em tráfego criptografado (HTTPS, SSH, VPN), ressalta-se que mais de 90% de sites de phishing[5] **usam HTTPS**[6].

iii. Geolocalização (identificação de países de origem/destino) para políticas de acesso segmentadas.

c) Controle de Acesso e Segurança Integrada

i. Integração com serviços de diretórios via tecnologias Microsoft Active Directory (AD) e OpenLDAP por estas duas tecnologias estarem presentes como forma de autenticação de usuários nas infraestruturas de TIC dos participantes, sendo que o órgão gerenciador, TRT12, utiliza OpenLDAP.

ii. Autenticação de usuários para políticas granulares (por departamento, grupo ou indivíduo).

iii. Filtragem de URLs e controle de aplicações (ex.: bloquear redes sociais, streaming, P2P).

d) Suporte a VPN Segura

i. VPN IPsec para conexões site-to-site (entre unidades do TRT).

ii. VPN SSL para acesso remoto seguro de servidores e usuários externos.

2.4.2. Gerência centralizada de toda a solução de Next Generation Firewall

A principal função do módulo de gerenciamento é fornecer uma interface única para gerenciamento do conjunto de equipamentos que fará parte da solução de Firewall, composta por, no mínimo, dois equipamentos que permitem a Alta Disponibilidade.

Contudo, alguns órgãos participantes também desenharam a solução de Firewall contendo três ou mais equipamentos, pois utilizarão uma rede SD-WAN

[5] Phishing é um tipo de ataque cibernético que visa obter informações pessoais de usuários. Os criminosos se passam por entidades confiáveis, como bancos, empresas de telefonia ou o governo, para induzir as vítimas a fornecer dados sigilosos.

[6] De acordo com o Anti-Phishing Working Group (APWG), mais de 90% dos sites de phishing usarão o cadeado em 2023. O relatório concluiu que a atividade de phishing, bem como o uso do protocolo HTTPS, estão em um ritmo contínuo, com quase todos os sites de phishing empregando um certificado SSL válido.

para conectar os centros de processamento de dados com as unidades descentralizadas.

Assim, para ser eficaz, a central deve permitir o gerenciamento centralizado, com monitoramento provido de sistema de alarmes (Reporting) tanto dos Firewall principais, (Cluster), quanto dos equipamentos Firewalls de menor porte (Appliances) de forma integrada, gerando alarmes e logs de todos os componentes que estejam conectados, contendo, no mínimo, as seguintes informações:

a) Console único para configuração, monitoramento e resposta a ocorrências, e;

b) Logs detalhados e relatórios para auditoria e conformidade (LGPD, PCI DSS).

A central de gerência também deve assegurar o armazenamento e backup das configurações apartadas dos aparelhos, situação fortemente recomendada para recuperação de desastres.

2.4.3. Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)

A adoção da arquitetura SASE (Secure Access Service Edge) representa uma evolução necessária para a segurança de redes corporativas, especialmente em órgãos públicos como a Justiça do Trabalho, que demandam acesso remoto seguro, proteção contra ameaças avançadas e integração com infraestruturas híbridas (nuvem e on-premises).

No cenário da Justiça do Trabalho, o SASE fornece segurança consistente entre data centers locais e provedores como AWS/Google/Azure, especialmente Acesso Remoto Seguro de servidores e ordenadores de despesa a sistemas críticos, como o SIAFI, via celular, notebooks, ou mesmo computadores normais conectados fora da rede corporativa do Tribunal, sem expor a rede e os sistemas internos a riscos.

Os principais aprimoramentos técnicos presentes em solução SASE são:

a) ZTNA (*Zero Trust Network Access*)

- Substitui modelos tradicionais de VPN por acesso granular baseado em políticas de confiança zero, garantindo que usuários e dispositivos só acessem recursos estritamente necessários.
- Reduz riscos de ataques como o ocorrido no SIAFI (2024)[7], quando credenciais comprometidas permitiram acesso indevido.

b) Proteção Contra Ameaças em Tempo Real

- Combinação de Firewall-as-a-Service (FWaaS), antimalware baseado em IA e inspeção SSL/TLS para detectar e bloquear ataques antes que alcancem a rede.
- Mitigação de riscos em redes públicas (Wi-Fi não seguras), comuns em acessos móveis.

c) Integração com Firewalls Existentes

- O SASE deve interoperar com soluções de firewall já implantadas, compartilhando inteligência sobre ameaças (como tentativas de intrusão) e logs de acesso.

d) Disponibilidade e Performance

- SLA de 99,999% (≈5 minutos de indisponibilidade/ano) para garantir continuidade no acesso de serviços críticos (ex: PJe, SIAFI, sistemas judiciais).
- Pontos de Presença (PoPs) no Brasil para baixa latência e conformidade com leis de dados (LGPD).

e) Gestão Unificada de Acesso Móvel e em Nuvem

- Controle centralizado de dispositivos BYOD (*Bring Your Own Device*), aplicando políticas de segurança diferenciadas para celulares, tablets e notebooks.

[7] Uma das reportagens acerca do ataque ao sistema SIAFI foi publicada pela revista Veja, conforme link https://veja.abril.com.br/economia/sistema-de-pagamentos-do-governo-e-invadido-pf-e-abin-investigam-o-caso/ acessado em 1/4/2025.

2.4.2. Solução de Next Generation Firewall (appliance e funcionalidades agregadas) que permita conexão via Software-Defined Wide Area Network (SD-WAN)

São equipamentos com finalidade de estabelecer conexões seguras entre as Sedes dos Tribunais e as unidades descentralizadas via Links Internet de baixo custo, via tecnologia Software Defined WAN (SD-WAN).

Muitas vezes as unidades descentralizadas encontram-se em cidades com poucos recursos de infraestrutura, que só possuem fornecedores de link com tecnologia ADSL, ou mesmo rede móvel 4G (celular).

Para estes casos e também para permitir o uso de mais de um link simultâneo nas unidades remotas, como um link via cabo e um link via celular, pode-se utilizar equipamentos Firewall capazes de proteger as unidades e ainda fornecer comunicação entre si com tecnologia SD-WAN.

São equipamentos com finalidade de estabelecer conexões seguras entre as Sedes dos Tribunais e as unidades descentralizadas via Links Internet de baixo custo, via tecnologia Software Defined WAN (SD-WAN).

Muitas vezes as unidades descentralizadas encontram-se em cidades com poucos recursos de infraestrutura, que só possuem fornecedores de link com tecnologia ADSL, ou mesmo rede móvel 4G (celular), nestes casos, a adoção de SD-WAN integrada ao Firewall pode ser estratégica.

A conexão via SD-WAN também permite o uso de mais de um link simultâneo nas unidades remotas, como um link via cabo e um link via celular, pode-se utilizar equipamentos Firewall capazes de proteger as unidades e ainda fornecer comunicação entre si com tecnologia SD-WAN.

Essa abordagem combina segurança avançada, otimização de rede e controle centralizado, garantindo que a infraestrutura de TI seja resistente a ataques, eficiente em custos e adaptável a demandas futuras.

No âmbito da JT, para permitir o funcionamento de redes SD-WAN via Firewall são necessários os seguintes requisitos mínimos.

- Compatibilidade com os equipamentos Firewall Principais das instituições;
- Capacidade de análise de protocolos de rede até a camada 7 para inspecionar aplicações;

- Conseguir inspecionar tráfego criptografado com protocolo SSL, posto que a maior parte da utilização da Internet hoje funciona com este tipo de protocolo e não inspecionar esse tráfego torna o dispositivo de segurança pouco eficaz.
- Integração com bases de usuários LDAP via OpenLDAP e Microsoft Active Directory.

Ressalta-se ainda que as conexões com unidades remotas utilizando Firewall e SD-WAN Integrados, permite, entre outras coisas, as seguintes funcionalidades de segurança:

a) Inspeção de Tráfego em Tempo Real
- O firewall aplica Deep Packet Inspection (DPI) e antivirus/IPS diretamente no tráfego SD-WAN, bloqueando ameaças antes que atinjam a rede.

b) Túneis Criptografados Automáticos
- A SD-WAN cria conexões IPSec/SSL entre unidades, enquanto o firewall gerencia políticas de acesso e autenticação.

c) Isolamento de Ameaças com Segmentação
- Se uma unidade for comprometida, o firewall bloqueia o avanço de ataques via microssegmentação integrada ao SD-WAN.

d) Failover Automático em Caso de Ataques ou Quedas
- Se um link sofrer DDoS ou interrupção, a SD-WAN alterna para 4G/5G/outro ISP sem perder segurança (firewall mantém políticas ativas).

e) Gestão de Políticas de Segurança em Um Único Painel
- Regras de firewall são aplicadas globalmente (ex: bloquear Torrent).

Por esses motivos é previsto nesta contratação adquirir licenças que permitam o uso da tecnologia SD-WAN via Firewall para os órgãos que assim desejarem.

2.4.6. Serviço de garantia e atualização de assinaturas de proteção e suporte técnico

O serviço de atualização de assinaturas das soluções de Firewall é fundamental para manter a segurança das instituições no cenário de ameaças dinâmicas.

Sem estar atualizado contra as ameaças mais atuais o Firewall fica com suas funções seriamente comprometidas, dependendo do prazo que a solução funciona com as informações obsoletas, sua função de proteção passa a ser inócua.

Além disso, o serviço de garantia assegura a troca de peças e equipamentos sempre que necessário, assegurando proteção e operação como roteador principal da rede.

2.4.7. Serviço de instalação de um cluster da solução de Next Generation Firewall

Como os órgãos participantes possuem o Firewall como roteador principal na rede de dados, a instalação com migração das configurações e regras em uso é crucial para a continuidade do negócio, ou seja, se não forem transferidas ou recriadas as configurações e regras do Firewall atual para o novo, serviços de TIC ficarão prejudicados, podendo até, em casos extremos, deixar de funcionar.

Esse serviço é de extrema importância, pois uma instalação/migração mal feita pode inviabilizar o funcionamento das redes de dados dos contratantes, interrompendo a prestação de serviços dos órgãos.

2.4.8. Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados

O serviço gerenciado é necessário para garantir a solução de problemas e aprimoramentos relacionados ao Firewall dentro de níveis mínimos de serviço, evitando que sistemas de TIC fiquem indisponíveis, ou ainda, que haja perda ou destruição de dados, por falhas da solução de Firewall.

Ademais, os Tribunais também sinalizaram interesse em suprir o eventual déficit de mão de obra técnica especializada para gerenciamento das Soluções de

Firewall via Serviço gerenciado, contendo operação assistida, em regime 24x7, com atendimento pró-ativo para casos de incidentes de segurança da Informação, ou seja, comprometimento dos aparelhos e sistemas.

O serviço gerenciado abrange atividades que não são cobertas pela garantia ou pelo suporte técnico do fabricante, visto que essas visam garantir a resolução de problemas referentes a falhas e defeitos nos equipamentos ofertados, enquanto aquele visa fundamentalmente viabilizar a administração e a operação de tais equipamentos.

Este serviço não abrange as atividades referentes à primeira instalação e configuração inicial dos equipamentos ofertados.

Em sua essência, tais serviços visam auxiliar a equipe técnica do contratante na administração e na operação dos equipamentos, no âmbito das atividades que exijam conhecimentos com maior grau de complexidade e que possam impactar negativamente no negócio caso sejam executadas com insucesso.

2.4.9. Treinamento para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall

Também foi levantada a importância de treinar as equipes de TIC dos Regionais sobre o funcionamento dos equipamentos Firewall, resultando na definição de cursos oficiais do fabricante sobre o tema.

2.5 Sustentabilidade

A presente contratação será realizada sob a modalidade de Compra Nacional por Intenção de Registro de Preço (IRP), alinhando-se às diretrizes da Resolução CNJ nº 400/2021 e do Guia Nacional de Contratações Sustentáveis da DECOR/CGU/AGU.

A adoção de compras compartilhadas, através da IRP, promove a otimização de recursos, a troca de expertise em contratações públicas sustentáveis e a obtenção de ganhos de escala, resultando em preços mais competitivos para bens e serviços com critérios de sustentabilidade.

Entre as soluções possíveis a contratação de novo suporte e garantia dos equipamentos atuais possui alinhamento significativo com os princípios da

sustentabilidade, especialmente no que tange à reutilização de bens e à extensão do ciclo de vida dos equipamentos existentes.

Manter os equipamentos hoje instalados reduz drasticamente a geração de resíduos eletrônicos, evitando o descarte prematuro de equipamentos que ainda possuem vida útil. Ainda contribui para a diminuição da demanda por novos recursos naturais e energia para a fabricação de novos hardwares. Esta solução se alinha diretamente com o item "Alternativas à Aquisição" do Capítulo III do Guia de Contratações Sustentáveis da Justiça do Trabalho, que incentiva a não aquisição quando possível.

A aquisição de novos equipamentos, embora possa trazer benefícios em termos de desempenho e recursos, apresenta um impacto ambiental potencialmente maior em comparação com a prorrogação ou a solução em nuvem. Neste caso, a EPC deverá analisar a possibilidade de adquirir equipamentos com maior eficiência energética e menor consumo de energia, o que pode reduzir o impacto a longo prazo. Haverá a geração de resíduos eletrônicos provenientes do descarte dos equipamentos antigos além do consumo de recursos naturais e energia na fabricação e transporte dos novos equipamentos.

Para mitigar esse impacto a EPC deve analisar: priorizar a aquisição de equipamentos com selos de eficiência energética e certificações ambientais; estabelecer a forma como será realizado o descarte adequado dos equipamentos antigos, garantindo a reciclagem ou descarte responsável; avaliar o ciclo de vida dos novos equipamentos, buscando aqueles com maior durabilidade e menor necessidade de substituição.

Já a contratação de Firewall em nuvem representa uma mudança de paradigma, transferindo a responsabilidade pela infraestrutura física para o provedor de serviços. Sob o ponto de vista da sustentabilidade, apresenta nuances importantes, pois a responsabilidade pela infraestrutura e seu impacto ambiental é do provedor de nuvem, que geralmente opera em escala com data centers otimizados e com maior eficiência energética. A virtualização e a consolidação de recursos em data centers de grande porte podem levar a uma menor utilização de energia e recursos totais em comparação com a manutenção de firewalls dedicados em cada organização. Caso esta solução seja escolhida é preciso estudar as políticas e certificações de sustentabilidade aplicáveis aos provedores destes serviços a fim de estabelecer critérios de sustentabilidade.

3. Estimativa da demanda – Quantidade de bens e serviços

Importante: Para esta contratação será adotada a definição de cluster como o conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

Dada a complexidade da contratação e da análise das soluções disponíveis, as diferentes necessidades, bem como a quantidade de órgãos participantes, neste ponto utilizaremos o quantitativo do TRT12, para fins de comparação entre as soluções.

Não por outros motivos, ao longo do planejamento foram realizadas consultas aos tribunais sobre as necessidades, tipos de equipamento, que embasaram a análise das soluções possíveis.

O levantamento final do quantitativo, após a escolha da solução, constará no TR.

Já os quantitativos da solução hoje em uso no TRT12, consta na tabela ETP1, abaixo.

Tabela ETP1 - Atual solução de firewall do TRT12

Atual Solução de Firewall do TRT12			
Item	**Descrição**	**QTDE**	**Contrato**
1	Solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, equipamento modelo Checkpoint 23500.	1 Cluster	PRE 11926/2017
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, por equipamento modelo Checkpoint 23500.	24 meses para 1 cluster	PE 9665/2023
3	Serviço gerenciado mensal, contendo operação assistida e resposta a incidentes de segurança, em regime 24x7 para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos modelo Checkpoint 23500.	24 meses para 1 cluster	PE 9665/2023

Conforme documentado no sítio do fabricante Checkpoint (https://www.checkpoint.com/support-services/support-life-cycle-policy/) o equipamento Checkpoint 23500 atingirá o fim da sua vida útil, que garante serviço de suporte e atualização do fabricante, em dezembro de 2025. Por essa razão necessita ser substituído, outros serviços também serão necessários, como já explicado.

No caso, além de reforçar que a solução de Firewall precisa estar disponível e atualizada para da garantia do funcionamento dos sistemas de TIC, relembra-se sobre a necessidade de evoluir com essa tecnologia por meio do produto SASE, que fornece Acesso Remoto Seguro mais seguro que VPN, essencial para ordenadores de despesa e administradores de sistemas críticos, como o SIAFI, fora da rede corporativa do Tribunal.

Portanto, para atender a demanda do TRT12 a EPC entende necessário os itens e quantidades que, no mínimo, assegurem o funcionamento da solução de NG Firewall, bem como aquisição de SASE para manter a prestação jurisdicional do TRT12 em funcionamento, considerando os seguintes itens e quantidades.

- Para viabilizar o funcionamento da Rede lógica do Tribunal e os sistemas de TIC é necessário manter uma solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada, com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7.

- Para conexão segura aos sistemas de TIC, especialmente acessos a movimentação de orçamento e contas bancárias institucionais é necessário contratar solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) para todos os usuários que acessam serviços de TIC do TRT12 remotamente, o que seriam 2.500 usuários.

- Para garantir Níveis Mínimos de Serviço na operação e funcionamento da solução de Firewall é necessário contratar serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados.

- Para manter condições de fiscalização e execução dos contratos, bem como

a operação das ferramentas de Firewall e SASE é necessário adquirir capacitações atualizadas para as soluções objetos desta contratação, para seis servidores..

Durante as reuniões de alinhamento com os demais órgãos participantes foi identificada também a necessidade de contratação de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW.

4. Análise de Soluções Possíveis

Para o atendimento dessa demanda, as opções disponíveis no momento são de compra de Serviço de Firewall em nuvem, contratação de manutenção/suporte para os equipamentos atuais e aquisição de novos equipamentos.

4.1. Identificação das soluções

A tabela ETP2 apresenta a lista das soluções julgadas possíveis para atender a demanda sobre a solução de NG Firewall.

Tabela ETP2 - Soluções possíveis para a demanda

Id	Descrição da solução (ou cenário)
4.2.1	Serviço de Firewall em nuvem
4.2.2	Aquisição de novos equipamentos Firewall
4.2.3	Contratação do serviço de suporte e manutenção para os equipamentos atuais

4.2. Análise comparativa de soluções

4.2.1 Solução 1 - Serviço de Firewall em nuvem

A solução 1 propõe a contratação de um serviço Firewall em nuvem (Firewall as a Service - FWaaS). Nesta modalidade, o Firewall é gerenciado por um provedor de serviços de nuvem, que se responsabiliza pela infraestrutura, manutenção, atualizações e segurança da solução. O tráfego de rede dos Tribunais seria

redirecionado para o firewall na nuvem, que faria a inspeção e o filtro antes de chegar aos sistemas internos.

É importante ressaltar que, atualmente, apenas os Tribunais Regionais do Trabalho da 8ª, 17ª e 24ª Regiões utilizam a infraestrutura em nuvem.

No TRT12, por exemplo, toda a infraestrutura é física, localizada em dois datacenters. Isso significa que a implementação de um Firewall em nuvem representaria uma mudança significativa na arquitetura de rede e na forma como o tráfego é gerenciado.

Contudo, mesmo no TRT8, TRT17 e TRT24 existem redes locais para atender as instalações físicas desses órgãos, o que demandaria que o roteamento e filtros de acessos para evitar ações de códigos maliciosos, como Vírus de computador acontecesse em nuvem, ou seja, o tráfego teria que ser enviado para nuvem, processado, e devolvido localmente, trazendo lentidão e dificuldades de funcionamento.

As principais vantagens deste cenário são:

a) Um Firewall em nuvem oferece escalabilidade praticamente ilimitada, permitindo ajuste dinâmico da capacidade de segurança conforme a demanda, sem a necessidade de adquirir e instalar novos equipamentos. Isso é ideal para picos de tráfego ou para acompanhar o crescimento de tráfego futuro da instituição.

b) O provedor em nuvem é responsável pela manutenção, atualização e segurança do Firewall, liberando as equipes de infraestrutura para focar em outras prioridades.

c) Atualizações de *software* e as correções de segurança são aplicadas automaticamente pelo provedor, garantindo que o Firewall esteja sempre protegido contra as vulnerabilidades e ameaças conhecidas, sem intervenção da equipe interna.

d) Soluções de Firewall em nuvem são projetadas com alta disponibilidade e redundância, distribuindo serviços por múltiplos datacenters, o que garante a

continuidade das operações mesmo em caso de falhas em uma região.

As principais desvantagens deste cenário são:

e) Como o tráfego precisa ser roteado para a nuvem para ser inspecionado e depois retornar para a infraestrutura do órgão, pode haver um aumento na latência. Isso é crítico para aplicações que exigem baixa latência, podendo impactar a performance de sistemas internos e a experiência do usuário.

f) Os Tribunais se tornarão dependentes da infraestrutura, desempenho e segurança do provedor de nuvem. Interrupções no serviço do provedor, falhas de segurança ou mudanças nas políticas de serviço, podem afetar diretamente a operação da instituição.

g) A integração de um Firewall em nuvem com a infraestrutura on-premise (presente na maioria dos Tribunais), que não possui sistemas em nuvem, pode ser complexa. Exige o redesenho de rotas de rede, configuração de túneis VPN seguros (IPsec ou MPLS) entre a rede do órgão e a nuvem, e adaptações na arquitetura de rede para garantir que todo o tráfego seja inspecionado adequadamente.

h) Uma futura troca de provedor de FWaas pode ser complexa e custosa devido a configurações específicas, integração de APIs e a necessidade de reestruturar rotas de rede.

i) Possíveis ataques ao Firewall em nuvem podem causar consumo de recursos no provedor, que, por sua vez, implicará em consumo de recursos do provedor de nuvem não programado e causar um descontrole orçamentário do contratante.

4.2.2 Solução 2 - Aquisição de nova solução para NG Firewall

No segundo cenário, há a aquisição de um novo Firewall em modo On-premise, com a compra de novos equipamentos.

Neste caso, substituir a solução de Firewall traz as seguintes vantagens.

a) Atualização do produto, com possíveis novas funcionalidades e relatórios para facilitar a operação e melhorar o funcionamento;

b) Possibilidade de reavaliar a capacidade da solução. Ao adquirir novos equipamentos, é possível redimensionar a infraestrutura de firewall para atender às necessidades atuais e futuras dos Tribunais. Isso inclui maior capacidade de processamento, maior throughput de rede, mais portas de conexão e suporte a um número crescente de usuários e dispositivos, garantindo que o firewall não se torne um gargalo à medida que a demanda por serviços digitais aumenta.

Por outro lado, implica também em desvantagens, como:

c) Riscos de migração, que inclui ameaças como parada dos sistemas ou até, em um cenário mais grave, perda de dados. A substituição de um Firewall é uma operação complexa que exige planejamento meticuloso e execução cuidadosa. Erros na configuração podem levar a interrupções prolongadas nos serviços, afetando a operação judicial e a produtividade. Há também o risco de perda de configurações ou dados de log importantes durante a transição.

d) Em caso de mudanças de fornecedor, o desconhecimento sobre operação e funcionamento da solução, reiniciando a curva de aprendizado. As equipes técnicas dos Tribunais terão que investir tempo e recursos em treinamento para aprender a operar e configurar o novo sistema. Isso pode atrasar a implementação completa e a otimização da nova solução, além de exigir um período de adaptação e familiarização.

e) A aquisição de novos equipamentos implica no descarte dos aparelhos de Firewalls atuais, o que gera lixo eletrônico e está desalinhado aos princípios de sustentabilidade ambiental. É necessário gerenciar adequadamente o

descarte desses equipamentos, seguindo as regulamentações ambientais.

f) O custo inicial de aquisição de novos equipamentos Firewall pode ser significativamente mais elevado que a contratação de suporte e garantia de equipamentos já instalados. Além do custo dos equipamentos há gastos com software de gerenciamento, instalação e treinamento.

g) A aquisição, instalação e configuração de novos equipamentos podem levar um tempo considerável, desde o processo licitatório até a sua plena operação.

4.2.3 Solução 3 - Contratação do serviço de garantia e direito de atualização para solução de NG Firewall já instalada

A Solução 3 propõe a continuidade da operação do sistema de Firewall adquirido em 2017 (PRE 11926/2017), utilizando um modelo de contrato de garantia e direito a atualização, com suporte, semelhante ao PRE 9665/2023, mas com equipamentos atualizados.

Essa alternativa só figura entre as possíveis soluções porque em dezembro de 2023, a empresa NTSEC - Soluções de Teleinformática LTDA, vencedora da ARP 1/2023, solicitou por e-mail (marcador 86 do Proad 9665/2023), a troca dos equipamentos modelo 5800 (Grupo 1, Item 4), instalados nos regionais, por novos equipamentos modelo 6700, sem custos adicionais para os órgãos participantes da referida ARP. Essa iniciativa decorreu da inclusão dos modelos 23500, 15600 e 5800 na lista de equipamentos com comercialização encerrada em 2020 pela fabricante Checkpoint, com o fim do suporte técnico e licenciamento previstos para 2025.

Como forma de prevenir problemas futuros, a empresa NTSEC também propôs a substituição preventiva dos equipamentos modelos 23500 e 15600 pelo modelo 16200.

A equipe técnica do TRT 12 manifestou-se favoravelmente a esta troca (marcador 87), e a presidência do TRT12 autorizou a aludida substituição de equipamentos para os regionais que assim desejassem.

O TRT12 foi o primeiro órgão a utilizar a ARP, em outubro de 2023, assim nossos equipamentos não seriam afetados pelo fim do suporte e garantia noticiado

pela fabricante, mesmo assim o Fabricante disponibilizou um novo aparelho para o TRT12.

Apesar do novo Cluster ter sido disponibilizado, em junho de 2025 o único Regional que ainda não realizou a troca dos equipamentos é o TRT12.

A referida substituição atualiza todos os equipamentos cuja garantia havia sido contratada em 2023 por dispositivos mais capazes e atuais, com uma vida útil prevista até 2030. Essa abordagem permite que os Tribunais mantenham a solução on-premise (instalada fisicamente nas organizações), que, até onde esta EPC tem conhecimento, ainda atende aos requisitos de desempenho.

Nesse cenário proposto, a solução mantém os equipamentos e as instalações em uso pelos Órgãos participantes, contratando-se o direito de atualização do produto e suporte técnico 24x7 para um novo período, com tempos definidos para atendimento de problemas, incluindo a troca de equipamentos.

Adicionalmente, destaca-se que a atual solução de Firewall utilizada pela maioria dos Tribunais da JT, do fabricante Checkpoint, está classificado entre os três melhores Firewalls do mundo, segundo a avaliação do Gartner Group de 2025[8].

As principais vantagens da solução 3 são:

a) Inexistência dos riscos de migração: Como o Firewall geralmente é o elemento principal para o roteamento das redes das instituições, que filtra todo o tráfego de dados, sua substituição implica em uma tarefa complexa que envolve riscos de parada em sistemas, ou mesmo funcionamento inadequado destes. Muitas vezes o ajuste do funcionamento demora meses. Como os equipamentos já estão instalados e em operação, a continuidade do suporte e garantia elimina os riscos inerentes a uma substituição completa de firewall.

b) Conhecimento das equipes técnicas, as equipes técnicas dos Tribunais já possuem um conhecimento aprofundado na operação e configuração dos equipamentos em uso. Isso resulta em maior agilidade na resolução de problemas, otimização das políticas de segurança e uma curva de aprendizado inexistente, garantindo a eficiência operacional desde o primeiro

[8] Disponível no endereço: https://gartnerr.com, acessado em 4/6/2025, disponível no doc. xxx.

dia do contrato.

c) Aproveitamento máximo da vida útil dos equipamentos. A prorrogação do suporte e garantia permite maximizar o retorno do investimento já feito nesses ativos, assegurando que continuem a operar com segurança e desempenho por um período adequado, sem a necessidade de um novo ciclo de compra prematuro;

d) Contratação mais sustentável ao estender a vida útil desses equipamentos relativamente novos, os Tribunais do Trabalho contribuem para a redução do descarte de lixo eletrônico e para o consumo consciente de novos recursos, alinhando-se a práticas mais sustentáveis e ambientalmente responsáveis.

e) Historicamente, a prorrogação de contratos de suporte e garantia foi mais econômica do que a aquisição de novos equipamentos. Essa abordagem pode liberar recursos orçamentários para outras iniciativas estratégicas dentro de cada órgão. A vantagem financeira será avaliada em tópico próprio.

As principais desvantagens deste cenário são:

f) Embora tenham sido substituídos recentemente, os equipamentos atuais possuem uma vida útil projetada. Próximo ao término dessa vida útil, mesmo com o suporte e garantia, a probabilidade de falhas de componentes pode aumentar, exigindo mais intervenções do fabricante e, consequentemente, da equipe de cada tribunal para gerenciar esses incidentes.

g) Se houver um aumento significativo no volume de tráfego, no número de usuários, ou a necessidade de implementar novas funcionalidades de segurança de alta demanda que não foram previstas no projeto desses equipamentos, os modelos atuais podem se tornar um gargalo de desempenho, embora o cenário de adoção de nuvem na JT contribua para reduzir a necessidade do Firewall local.

O quadro abaixo traz um compêndio de controles previstos na Resolução CNJ

n. 468 de 15/7/2022 sobre as soluções possíveis para contratações de TIC do Judiciário nacional.

Tabela ETP3 - Controles previstos na Resolução CNJ n. 468/22

Requisito	Solução	Sim	Não	Não se aplica	Justificativa
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X			TRT17
	Solução 2	X			TRT2
	Solução 3	X			TRT12
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X	Não se trata de solução de Software
	Solução 2			X	
	Solução 3			X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X	Não se trata de solução de Software
	Solução 2			X	
	Solução 3			X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1	X			As tecnologias envolvidas em NG Firewalls atendem aos protocolos definidos no e-ping e e-mag.
	Solução 2	X			
	Solução 3	X			
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1	X			Os certificados digitais reconhecidos pelo Firewall são aderentes a ICP-Brasil
	Solução 2	X			
	Solução N	X			
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X	O objetivo da solução não é abranger documentos arquivísticos
	Solução 2			X	
	Solução N			X	

4.3. Pesquisa de Preços das Possíveis Soluções

A pesquisa de preços das soluções consta no documento apartado “Estimativa Preliminares de Preços”.

Contudo, aqui traremos o resumo da análise dos valores pesquisados que fomentaram o entendimento da EPC que a melhor solução do ponto de vista econômico seria a solução 3, aquisição de garantia para a solução já existente, conforme seção TCO, a seguir.

4.3.1. Análise Comparativa de Custos (TCO)

Se comparado com os orçamentos recebidos para solução 2, adquirir novos equipamentos, com a solução 3, adquirir garantia para a solução atual, comprova-se

economia ao adotar a solução 3, conforme comparação apresentada na tabela ETP4, abaixo, que considera apenas o orçamento mais barato da empresa Advanta.

ETP4 - Comparação de valores entre soluções - Orçamentos de março a maio de 2025

	Solução 2 - Adquirir novos produtos		Solução 3 - Adquirir garantia	Comparação de Valores	
Produto	**Preço 3 - Approach / Paloalto - Valores unitários**	**Preço 7 - Advanta / Fortinet - Valores unitários**	**Preço 12 - NTSEC / Checkpoint - Valores Unitários**	**Preço 12 em relação ao preço 3**	**Preço 12 em relação ao preço 7**
Item 1 - Firewall Tipo I	**R$ 10.042.682,87**	**R$ 8.664.815,03**	**R$ 3.996.162,01**	**+ R$ 6.046.520,86** **+ 151,31%**	**+ R$ 4.668.653,02** **+ 116,83%**
Item 2 - Firewall Tipo II	**R$ 6.462.202,22**	**R$ 4.566.938,77**	**R$ 2.740.770,49**	**+ R$ 3.721.431,73** **+ 135,78%**	**+ R$ 1.826.168,28** **+66,63%**
Item 3 - Firewall Tipo III	**R$ 5.658.077,12**	**R$ 2.355.767,21**	**R$ 2.528.895,32**	**+ R$ 3.129.181,80** **+ 123,74%**	**- R$ 173.128,11** **- 6,85%**

Comparando o cenário de aquisição de nova solução de Firewall com o cenário de aquisição de garantia para solução atual, com base nos orçamentos de maio de 2025, percebe-se que grande economia na aquisição apenas de garantia, especialmente com relação aos produtos mais caros, que atendem a maior parte dos Tribunais.

Considerando a economia financeira junto ao fato que todos os órgãos da JT que usam produto Checkpoint, exceto o TRT12, já tiveram seus equipamentos atualizados durante a execução do contrato vigente, e que o TRT12 receberá um novo e atualizado equipamento ainda em 2025.

Considerando ainda que a solução de Firewall Checkpoint é uma das três melhores do mundo segundo o Gartner, continuar com esse fabricante assegura manter a excelência na segurança dos sistemas de TIC.

Situação reforçada pelo fato de todos os fabricantes que foram acionados para fornecimento de preços solicitarem a supressão de funcionalidades em relação à solução Checkpoint.

Outra situação é que valores baixos recebidos na fase de pesquisa de preços podem representar orçamentos intencionalmente baixos para influenciar o valor do edital e forçar uma licitação mais vantajosa para as empresas.

Assim, os itens que compõem a contratação e são associados à solução de Next Generation Firewall serão estimados com base nos orçamentos solicitados a partir de junho de 2025, considerando a solução 3, aquisição de garantia para os Firewalls atualmente instalados na maioria dos órgãos da Justiça do Trabalho.

5. Registro de soluções consideradas inviáveis

A contratação de Firewall em nuvem é, neste momento, inviável pois, como explicado, a maioria dos órgãos participantes operam com infraestrutura física (on-premise), como é o caso do TRT12. Desta forma, pode haver um aumento na latência, fator crítico para aplicações que exigem baixa latência, podendo impactar a performance de sistemas internos e a experiência do usuário.

Além da latência, a dependência do provedor de serviços em nuvem é um fator crucial. Ao optar por um Firewall em nuvem, os Tribunais ficam à mercê da infraestrutura, desempenho e segurança de terceiros. Interrupções no serviço de link, falhas de segurança ou mudanças em suas políticas interrompem imediatamente as operações da instituição, sem que haja controle direto sobre esses eventos.

Por fim, a complexidade da integração com a infraestrutura on-premise para Firewall de rede em nuvem é uma desvantagem considerável. A maioria dos Tribunais não possui sistemas em nuvem, o que exigiria um redesenho complexo das rotas de rede, a configuração de túneis VPN seguros (IPsec ou MPLS) entre a rede do órgão e a nuvem, e adaptações na arquitetura de rede para garantir que todo o tráfego seja inspecionado adequadamente. Essa complexidade na implementação pode gerar custos adicionais e atrasos, tornando inviável a substituição completa dos equipamentos Firewall on-premise por Firewall em nuvem.

Além disso, os Tribunais que hoje já operam em nuvem também tem redes locais que precisam ser protegidas e também devem manter sua infraestrutura de Firewall *on-premise*.

6. Escolha e Justificativa da Solução mais Adequada

6.1 Histórico sobre a pesquisa de mercado e de preços

Os estudos técnicos para a presente contratação iniciaram em novembro de 2024, com a reunião já relatada neste documento entre os Tribunais interessados, e o posterior levantamento das necessidades iniciais de cada Tribunal. A partir destas informações e das especificações dos equipamentos hoje em uso, foram feitas as especificações técnicas iniciais.

Ao longo do planejamento da contratação, a EPC buscou analisar a possibilidade de prorrogação da garantia dos equipamentos já instalados, mas até o início de maio de 2025 não obtivemos resposta da fabricante dos equipamentos atuais. Desta forma os estudos seguiram voltados para a aquisição de nova solução de Firewall.

A solução 2 então passou a ser a solução alvo, para tanto, definiu-se as especificações técnicas baseadas nos modelos hoje em uso na JT, e, ao longo destes meses, feitas ao menos 3 rodadas de consultas ao mercado, tanto para validação das especificações técnicas, quanto para a obtenção de preços de referência.

Na primeira rodada, também foi solicitada cotação para os serviços de garantia dos produtos separadamente, pois acreditou-se que, no futuro, apenas esse serviço poderia ser prorrogado, pois estaria desvinculado do custo dos equipamentos, esta consulta foi encaminhada para os seguintes fornecedores (marcador 53):

a) Zoom Tecnologia;
b) TId;
c) Teltec Solutions;
d) Sigma Telecom;
e) Servix;
f) Safeinc;
g) Roost Soluções de Inovação e Infraestrutura de TI;
h) Petacorp;
i) IT Protect;

j) Grupo NTSEC;
k) Fasthelp;
l) Claro;
m) Aproach Tech;

Adotamos este modelo de consulta visto que as especificações técnicas de cada solução possuem parâmetros distintos, que dificultam a comparação entre serviços semelhantes.

Nenhuma empresa atendeu ao prazo solicitado para resposta, contudo, quatro Fabricantes fizeram contato via seus fornecedores solicitando reuniões, a saber:

n) Fabricante Fortinet via fornecedores TLD e OAK;
o) Fabricante Paloalto via fornecedor Approach;
p) Fabricante Cisco via fornecedor Teltec solutions, e;
q) Fabricante Huawei via fornecedor Zoomtech.

Nestas reuniões as empresas puderam salientar quais pontos da especificação técnica atendiam, quais não atendiam, puderam tirar dúvidas e fazer sugestões.

Estas reuniões também serviram para aperfeiçoar as especificações de modo a ficarem claras as necessidades dos órgãos para os futuros licitantes.

Na prática, em cada reunião eram formalizados os pontos necessários para atendimento ao Edital pelos fabricantes, além de sugestões para alteração das capacidades de Throughputs.

Aqui cabe um esclarecimento. No mercado de Firewall cada fabricante mede a capacidade de Throughput de uma forma diferente, ou seja, utiliza diferentes funcionalidades habilitadas para determinar as velocidades máximas de capacidade de processamento dos seus equipamentos, abaixo exemplificaremos o caso para os 3 fabricantes referência de mercado segundo o Gartner Group. Foram analisados dois parâmetros de medição que seriam comuns entre os fabricantes: Throughput de Next Generation Firewall e Throughput de Prevenção de ameaças. Porém, mesmo os dois parâmetros que serviriam de comparação de capacidades variam em relação às funcionalidades habilitadas, tipo tráfego utilizado na medição e nomenclatura de funcionalidades entre fabricantes.

a) Paloalto: De acordo com o datasheet PA-5400 Series, PA-3400 Series e PA-1400 Series são utilizadas as seguintes taxas principais.
Taxa de transferência (Throughput) do Threat Prevention (appmix): A taxa de transferência do Threat Prevention é medida com App-ID, IPS, antivírus, anti-spyware, WildFire, segurança DNS, bloqueio de arquivos e logs ativados, usando transações appmix.

Taxa de transferência (Throughput) de firewall (appmix): A taxa de transferência do firewall é medida com App-ID e logs ativados, usando transações appmix.

b) Checkpoint: De acordo com o datasheets dos produtos Quantum 9400, 9800 e 19200.
Throughput de Threat Prevention (Gbps): Inclui Firewall, App Control, URLF, IPS, Anti Malware (Bot, Virus & Spam), DNS Security, Zero-Phishing and SandBlast Threat Emulation & Extraction com logs habilitados.
Throughput de NGFW (Gbps): Inclui Firewall, App Control e IPS com logs habilitados.
Taxas medidas usando tráfego Enterprise.

c) Fortinet: De acordo com os datasheets dos produtos Fortigate 3200F, Fortigate 2600F e Fortigate 1800F.
Throughput de Threat Protection: A performance de Threat Protection é medida com as funcionalidades de Firewall, IPS, Application Control, Malware Protection e logs habilitadas.
Throughput de NGFW: A performance de NGFW é medida com as funcionalidades de Firewall, IPS, Application Control e logs habilitados.
Medidas feitas usando tráfego Enterprise Mix.

Um detalhe importante das interações com os fornecedores foi que todos solicitaram a retirada de funcionalidades dos equipamentos, o que significa que todos os concorrentes que conversaram com a EPC tinham interesse de oferecer soluções menos completas que a solução Checkpoint instalada, que serviu de base

para o início da pesquisa de mercado.

No documento constante no marcador XXX são apresentadas as supressões de funcionalidades solicitadas pelos fabricantes Paloalto, Fortinet, Huawei e Cisco em relação às especificações preliminares do projeto, definidas em novembro de 2024.

Especialmente sobre as soluções de SASE, apenas o Fabricante Fortinet possui SASE integrado no seu painel de gerenciamento. Além disso, nenhum dos fabricantes de Firewall, incluindo a Checkpoint, atenderia as funcionalidades de Deception[9] que são necessárias para integrar o SASE com a solução XDR contratada na Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, que o TRT12 é participante e que já está contratada por vários dos órgãos desta justiça especializada.

Portanto, foi flexibilizado que o item SASE da contratação fosse atendido por Fabricante distinto dos demais equipamentos e licenças.

Assim foi gerada uma nova versão das especificações técnicas da contratação e encaminhada novo e-mail para estimar os valores da contratação. Neste ponto a EPC acreditava que, pelo menos, os quatro fabricantes que fizeram reuniões sobre as primeiras especificações possuíssem produtos que atendessem plenamente aos requisitos técnicos definidos pela EPC. Acreditava-se também em preços estimados mais baixos para novos equipamentos de Firewall, possivelmente melhores que de uma compra de garantia para as soluções atuais, sendo que ainda não havia proposta para o cenário de manutenção dos Firewalls já instalados.

Contrariando as expectativas, ao receberem a nova chamada de preços com especificações ajustadas, os fornecedores de Fortinet e Palo Alto responderam após o prazo estipulado, solicitando novas reduções de funcionalidades e apresentando valores acima do previsto.

Alegaram que seus equipamentos oferecem melhor desempenho mesmo com throughput nominal igual ao das soluções Checkpoint - como se 1Gbps em suas soluções fosse "mais rápido" que 1Gbps em outros fabricantes.

Registra-se que o fornecedor do fabricante Huawei não mandou preços,

[9] Deception é o nome de uma tecnologia de engano, “isca”, que cria ambientes e recursos falsos (como arquivos, servidores, contas de usuário) que imitam os ativos reais da empresa, mas que são projetados para serem "atraentes" para os invasores. Quando um invasor tenta interagir com esses recursos falsos, a tecnologia de engano detecta a atividade e notifica a equipe de segurança, permitindo que ela rastreie e analise as ações do invasor.

apenas insistiu na retirada de requisitos já presentes nas soluções de Firewall e inegociáveis para esta contratação.

Pois bem, ainda acreditando na estratégia de que a compra de novos equipamentos seria a melhor solução, fez-se nova revisão de especificação com adaptações para permitir que mais fabricantes participassem da licitação, ou ainda participassem com produtos mais competitivos.

Para isso, muitas funcionalidades hoje disponíveis e importantes, como QoS (Quality of Service) e autenticação VPN via página na Internet, foram retiradas, a fim de ampliar a concorrência e diminuir os valores estimados para a contratação. A exclusão de alguns itens foi objeto de polêmica entre os participantes do planejamento da contratação, pois são itens bastante utilizados.

Mesmo sabendo que algumas supressões de funcionalidades precisariam ser revistas, a EPC lançou um terceiro pedido de orçamentos para ver se os novos preços seriam menores ao ponto de justificar abrir mão de funcionalidades e diminuir os Throughputs especificados.

Acontece que os novos preços recebidos não tinham diminuições significativas de valor para as soluções de NG Firewall, principal item da contratação. O que demonstrou que, no cenário de contratação de nova solução, vale a pena manter os requisitos compatíveis com a solução atualmente instalada na maior parte dos Tribunais trabalhistas, e continuar com os Throughputs inicialmente definidos.

Além das dificuldades já relatadas, os orçamentos obtidos nas três solicitações de preços inviabilizariam a contratação por vários Regionais que passam por sérias restrições orçamentárias em 2025, com orçamentos na ordem de 1 milhão de Reais para solução de Firewall.

Entretanto, em maio de 2025 o fornecedor que representa a fabricante Checkpoint apresentou proposta para nova contratação de suporte e garantia dos equipamentos atuais. Essa proposta contempla a troca dos equipamentos dos modelos mais antigos por atualizados e com capacidade equivalente ou superior aos instalados, como ocorreu ao longo dos últimos dois anos, conforme já relatado.

Os valores apresentados para contratação de novas garantias ainda podem ser divididos em parcelas fixas anuais, similar ao que ocorreu na contratação de garantias para Storages via ARP 64/2023 do TRT18, que o TRT12 foi participante.

Sem esquecer que a continuidade das soluções de Firewall eliminam o risco de migrar a solução.

Desta forma a opção de prorrogação de suporte e garantia, voltou a ser analisada, em reunião com os demais órgãos participantes, realizada em 29/5/2025, foi apresentada a proposta e muito bem aceita pelo grupo, tanto pelos equipamentos estarem satisfazendo as necessidades atuais e estimadas para os próximos anos, visto que há previsão de jornada para Nuvem para todos os órgãos da JT como forma de atender o previsto na ENTIC-JUD, Resolução n.370/2021 do CNJ[10], quanto pela questão orçamentária. Alguns Tribunais já haviam sinalizado a necessidade de ampliação da solução atual, então ficou combinado que seria feito também um grupo para aquisição de equipamentos. Outra solicitação foi o pagamento anual, para alguns Tribunais que não tem orçamento disponível.

6.2 Justificativa para os serviços de contratação de suporte e garantia

Assim a Solução 3 passou a ser a mais vantajosa para os Tribunais que possuem solução de Firewall Checkpoint instalada, conforme motivos explicados no item 4.2.1 e resumidos abaixo:

a) Solução mais sustentável, aproveita os recursos existentes, evitando a produção de novos equipamentos e o descarte dos atuais;
b) Manutenção da instalação (reduzindo os custos com este item);
c) Inexistência dos riscos de migração;
d) Aproveitamento do conhecimento das equipes técnicas;
e) Aproveitamento máximo da vida útil dos equipamentos;
f) Possibilita uma economia de 49,03% em relação à aquisição de novos equipamentos do Tipo I (comparação do valor estimado para os itens 1 e 4) e de 38,5% em relação à aquisição de novos equipamentos do Tipo III (comparação do valor estimado para os itens 3 e 5), conforme Estimativa de Preliminar de Preços;
g) Utiliza despesas classificadas como GND3 (Serviços) para o pagamento e não GND4 (Investimentos) como a Solução 2 (para alguns Tribunais esta diferenciação é importante para permitir a contratação);
h) A empresa informou que é possível fazer o pagamento antecipado dos 5

[10] A ENTIC-JUD reconhece a importância da computação em nuvem como um habilitador da transformação digital. A nuvem é vista como uma forma de simplificar a infraestrutura, promover a integração entre sistemas, garantir a segurança da informação e padronizar o uso da tecnologia no Judiciário.

anos, ou pagamento anual, permitindo que o serviço seja contratado, mesmo diante das acentuadas restrições orçamentárias impostas aos órgãos do Judiciário em 2025.

Os serviços de suporte e garantia devem ser compatíveis com os equipamentos instalados e disponíveis nos Tribunais da Justiça do Trabalho, conforme tabela ETP4, abaixo.

Tabela ETP4 - Controles previstos na Resolução CNJ n. 468/22

Tribunal	Equipamento	Unidade	Quantidade
TRT1	16200 Plus	Cluster	1
TRT3	16200 Plus	Cluster	1
TRT4	9800 Plus	Cluster	1
TRT5	16200 Plus	Cluster	1
	1550	Equipamento	9
	1530	Equipamento	23
TRT6	16200 Plus	Cluster	1
TRT7	16200 Plus	Cluster	1
TRT9	9800 Plus	Cluster	1
TRT10	9700 Pluss	Cluster	1
TRT11	16200 Plus	Cluster	1
TRT12	9800 Plus (1)	Cluster	1
TRT13	16200 Plus	Cluster	1
TRT14	6700 Plus	Cluster	1
TRT15	16200 Plus	Cluster	1
TRT16	16200 Plus	Cluster	1
TRT17	6700 Plus	Cluster	1
TRT18	9800 Plus	Cluster	1
TRT19	6700 Plus	Cluster	1
TRT20	16200 Plus	Cluster	1
TRT21	16200 Plus	Cluster	1

TRT22	6700 Plus	Cluster	1
Totais	6700 Plus	Cluster	
	9700 Plus	Cluster	
	9800 Plus	Cluster	
	16200 Plus	Cluster	

(1) Equipamento disponível mas ainda não instalado

6.3 Justificativa para os itens referentes à aquisição de novos equipamentos

Sendo possível a prorrogação do suporte e garantia a **Solução 3** foi a escolhida como solução principal para a presente contratação. Ocorre que, como alguns Tribunais precisavam de equipamentos complementares, para manter a solução de firewall adequada as demandas dos TRTs 4, 7, 10 e TST, além da Solução 3, também será licitada a aquisição de novos equipamentos. Entretanto, para adequar-se à solução de Firewall já instalada na JT, os novos equipamentos e serviços a serem licitados deverão ser compatíveis com os Firewalls da fabricante Checkpoint definidos na tabela ETP4, apresentada na seção anterior, 6.2.

Como se tratam de novos equipamentos/Clusters, o serviço de instalação e configuração deverá estar incluído no preço.

6.4 Justificativa para os itens referentes à Licença de uso de solução de SASE (Secure Access Service Edge) e ZTNA ((Zero Trust Network Accesenvers)

A adoção da arquitetura SASE (Secure Access Service Edge) fornece segurança consistente para conexão entre usuários, Data Centers locais e provedores como AWS/Google/Azure, especialmente Acesso Remoto Seguro de servidores e ordenadores de despesa a sistemas críticos, como o SIAFI, via celular, notebooks, ou mesmo computadores normais conectados fora da rede corporativa do Tribunal, sem expor a rede e os sistemas internos a riscos.

A solução mitiga riscos de ataques como o ocorrido no SIAFI (2024), quando credenciais comprometidas do TSE permitiram roubo de R$ 14 milhões das contas

do governo[11]. Esse incidente demonstra que soluções de VPN simples já não atendem mais todos os perfis de usuários do Serviço Público Nacional.

O SASE deve interoperar com soluções de firewall já implantadas, compartilhando inteligência sobre ameaças (como tentativas de intrusão) e logs de acesso.

Já a respeito do quantitativo de licenças SASE o ideal era que todos os servidores e magistrados que fazem acessos remotos à infraestrutura do Egrégio tivessem licenças ativas, entretanto os custos advindos desta abordagem ainda são muito altos, desta forma, no TRT12, estabelecemos como meta a contratação de 200 licenças, o que atende, ao menos, as pessoas lotadas nas seguintes áreas tenham licenças ativas:

a) Secretaria de Orçamentos e Finanças (9 usuários);

b) Presidente;

c) Secretaria Geral da Presidência (2 usuários);

d) Secretaria de Apoio Institucional (13 usuários);

e) Gabinete da Vice Presidência (3 usuários);

f) Diretoria Geral (10 usuários);

g) Coordenadoria de Pagamento (13 usuários);

h) Secretaria de Execução de Precatórios (1 usuário);

i) Divisão de Execução Forçada e Parcelamento Trabalhista (2 usuários);

j) Coordenadoria de Execuções e Convênios (4 usuários);

[11] Matéria do Correio Braziliense, disponível no seguinte endereço eletrônico: https://www.correiobraziliense.com.br/politica/2024/04/6844678-crackers-desviaram-rs-14-milhoes-do-sistema-de-pagamentos-do-governo.html

k) Coordenadoria da Execução da Fazenda Pública (5 usuários), e;

l) Centrais de Apoio à Execução (137 usuários).

Como até a data da realização do presente estudo ainda não é possível atingir todos os usuários do TRT no atual exercício orçamentário, e considerando que com licenças com um mínimo de licenças, pagamento antecipado para 12 meses de uso. A EPC sugere que seja estabelecido uma quantidade mínima de 200 licenças para atender aos servidores com acesso mais crítico do TRT12 em 2025 e 2026.

Estas licenças poderão sofrer mudança no quantitativo a cada 12 meses, permitindo a expansão da proteção vinculada às necessidades de proteção de usuários e às condições financeiras de cada órgão.

6.5 Justificativa para os itens referentes à Serviço gerenciado mensal

É prática comum do mercado das soluções de Next Generation Firewall não garantir a solução dos problemas em tempos determinados, apesar de garantir o tempo para início do atendimento e prazo para remessa de novos equipamentos.

Conforme página 16 do documento “Check Point Collaborative Enterprise Support Service Level Agreement”, atualizado em 27/2/2025, disponível em https://www.checkpoint.com/downloads/support-services/collaborative-enterprise-support-sla.pdf, acessado em 13/8/2025, o fabricante Checkpoint não garante a solução dos problemas em tempos determinados, apesar de garantir o tempo para início do atendimento e prazo para remessa de novos equipamentos.

Portanto, não há Nível Mínimo de Serviço definido para o Grupo I, o que aumenta a recomendação para aquisição do serviço de operação gerenciada definida no Grupo IV, conforme segue.

Ademais, os Tribunais sinalizaram interesse também em suprir o eventual déficit de mão de obra técnica especializada para gerenciamento das Soluções de Firewall via Serviço gerenciado, contendo operação assistida em regime 24x7, com atendimento pró-ativo para casos de incidentes de segurança da Informação, ou seja, comprometimento dos aparelhos e sistemas.

6.6 Justificativa para os itens referentes aos Treinamentos

Apesar de a solução de Firewall atual estar em uso desde 2018, os Tribunais participantes também demandaram treinamento oficial do fabricante para operação da solução. O treinamento deverá ocorrer para dois públicos, a saber:

a) Técnicos que irão trabalhar com a solução e que necessitam aprofundar os conhecimentos já adquiridos. A capacitação propicia compreender o equipamento específico (a ser mantido ou adquirido) e também o funcionamento geral das soluções de Firewall Next Generation.
b) Técnicos que trabalharão com a solução de SASE, nunca antes implantada na Justiça do Trabalho.

6.7 Justificativa para 60 meses de contrato

A contratação de suporte, garantia e a aquisição de clusters e equipamentos, juntamente com os serviços associados, representa um investimento estratégico na segurança da informação dos órgãos participantes. A solução Firewall Next Generation, componente essencial para a infraestrutura de rede, demanda um período extenso de configuração, migração de regras e treinamento para sua plena operação.

Um contrato de 60 meses assegura a estabilidade e o funcionamento ininterrupto da solução, protegendo o Tribunal contra ameaças cibernéticas em constante evolução. Os 60 meses de suporte e garantia, além de comuns no mercado, são vantajosos para os órgãos participantes, visto que a troca de equipamentos envolve uma série de atividades e riscos associados. Instalação, configuração e migração de regras são atividades bastante complexas, ciente disso a EPC entendeu como razoável o prazo de 90 dias da comunicação da assinatura do contrato para conclusão da instalação e configuração, constante no página 3 do Anexo I.

A manutenção da solução por mais tempo também contribui para menos risco de paralisação prolongada dos sistemas devido a problemas de implantação da solução de Firewall.

6.8 Participação dos Tribunais Regionais do Trabalho e Tribunal Superior do Trabalho

Em julho de 2025 foi encaminhado o OFÍCIO CIRCULAR TRT12/SETIC N.º 3/2025 (doc. 14), para todos os TRTs e TST, solicitando o envio do DOD contendo os quantitativos mínimos e máximos que cada órgão tem interesse em registrar.

Neste ofício salientamos o que segue:

> *Pedimos especial atenção aos itens de 1 a 6, relativos ao Serviço de garantia e atualização de assinaturas de proteção e suporte técnico: os itens de 1 a 3 são para pagamento único e antecipado, já os itens de 4 a 6 são para pagamento em 5 parcelas anuais. Os tribunais deverão optar por apenas uma forma de pagamento (único ou em cinco parcelas) - portanto, para os itens de 1 a 6, apenas um deverá ser registrado.*

Após a resposta dos Regionais (marcadores de 15 a 34 e 52), nenhum órgão apresentou interesse no Item 5 Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - Tipo II - Pagamento em 5 parcelas anuais. Por este motivo o item referente será eliminado a partir deste tópico.

A compilação final do quantitativo, após a escolha da solução, constará no Anexo II.

7. Contratações Correlatas e/ou Interdependentes.

No caso de solução de Firewall do TRT12, as contratações correlatas da SETIC são:

- SALA COFRE - Contratação de manutenção de sala cofre, que abriga o Datacenter principal, onde são armazenados todos os dados e os equipamentos de processamento de dados corporativos. (Id 15384)
- Link 1 Internet - INTERNET - Contratação de acesso corporativo à internet 2024 (Id 15013)

- Link 2 Internet - INTERNET - Contratação de acesso corporativo à internet 2024 (Id 15014)
- SWITCHES - Aquisição de equipamentos switch SAN (Id 15004)
- REDE JT - Contratação de links de alto desempenho para as conexões de dados entre as unidades do TRT (15390)

As contratações interdependentes estão todas contempladas neste estudo.

7.1. Parcelamento da Solução

A divisão da contratação em quatro grupos distintos, como apresentada na tabela ETP6, abaixo, alinha-se com o princípio do parcelamento da contratação previsto no art. 40, V da Lei n.º 14.133/2021. Essa abordagem visa aprimorar a competitividade e otimizar a contratação ao agrupar itens de natureza similar. O agrupamento dos itens que incluem serviço de suporte permite que a contratada faça avaliações mais completas das questões que envolvem o gerenciamento da solução Firewall, utilizando informações de todos os órgãos participantes, além de permitir ações preventivas para este grupo específico.

A seguir a divisão dos grupos:

a) Grupo 1: Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento;

Aqui é importante reforçar que os novos equipamentos previstos nos itens 6 e 7 precisam ser do mesmo fabricante da solução já adotada na maior parte dos órgãos da JT principalmente para que as funcionalidades de proteção referentes aos sistemas nacionais da JT, como o PJe e o SIGEP, sejam replicadas.

É muito importante também que o TST, que abriga a instalação das versões de desenvolvimento do PJe use o mesmo tipo de Firewall que os demais Regionais.

Além disso, é importantes que as garantias, as instalações e migrações previstas nos itens 1 a 7 da contratação sejam prestados pelo mesmo fornecedor, no intuito que haja uma padronização de configuração e compartilhamento de informações sobre solução de chamados entre os órgãos da JT

b) Grupo 2: Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall;

As licenças, itens 9 e 10, e equipamentos, itens 11 a 13, que compõem o Grupo 2 é o conjunto de acréscimos para a solução de Firewall que permite comunicação segura e criptografada de ponta a ponta entre a Sede dos Tribunais e suas unidades Descentralizadas.

Os equipamentos que terão o suporte e garantia prorrogados são da fabricante Checkpoint, desta forma a aquisição de itens e licenças adicionais também precisam ser deste mesmo fabricante, esta questão está amparada pela lei, que permite a restrição da competição quando as características do bem ou serviço são padronizadas e necessárias para manter a compatibilidade com a solução existente.

c) Grupo 3: Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access) na modalidade de software como serviço e Treinamento para SASE, e;

Trata-se de uma solução nova no âmbito da JT e que não depende do Fabricante Checkpoint.

Porém, é importante que o Serviço de SASE e o treinamento seja entregue pelo mesmo fornecedor para todos os órgãos participantes, assim haverá o compartilhamento de informações, especialmente no tratamento de situações que possam impedir o desvio de dinheiro pelo sistema SIAFI via rede corporativa dos Tribunais.

d) Grupo 4: Serviço gerenciado mensal.

O serviço gerenciado é importante para garantir os níveis mínimos de serviço para eventuais problemas ou situações de ajuste necessárias nas soluções de NG Firewall.

A contratação conjunta assegura a padronização das soluções entre os Tribunais, o que é fundamental para facilitar o intercâmbio de informações e o compartilhamento de melhores práticas.

Assim, a solução de um problema em um órgão pode ser rapidamente replicada em outros, garantindo mais eficiência e agilidade na resolução de eventuais desafios técnicos. No caso, ao resolver a situação para um Tribunal específico, todos os demais podem receber a sugestão para aplicar o procedimento de forma direta, via comunicação da contratada.

Por exemplo, em julho de 2025, a empresa atualmente responsável pelo serviço gerenciado identificou um volume incomum de ataques de Negação de Serviço Distribuída (DDoS) direcionados ao Tribunal Regional do Trabalho da 12ª Região (TRT12). Essa incidência foi bem maior em comparação com outros Tribunais Regionais do Trabalho que também são clientes da empresa. Essa análise só foi possível porque a solução de segurança é compartilhada por diversos tribunais, demonstrando a interdependência e a necessidade de uma abordagem integrada na gestão de segurança para todos os órgãos envolvidos.

Tabela ETP6 - Descrição dos Grupos e Itens da contratação[12]

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento		
Item	**Descrição**	**Unidade (1)**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	Cluster
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo**	Cluster

[12] A especificação completa constará no Anexo I.

	II - Pagamento em parcela única, antecipada.	
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Cluster
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Cluster
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Cluster
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	Cluster
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	Cluster
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Aluno
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede SD-WAN via Firewall		
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Licença/ Cluster
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	Licença/ Cluster
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VI**	Equip.
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VII**	Equip.
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo VIII**	Equip.
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço e Treinamento		

14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	Usuário
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	Aluno
Grupo IV - Serviço gerenciado mensal		
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) **- Tipo I e Tipo IV**	Serviço/ Cluster
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) **- Tipo II e Tipo V**	Serviço/ Cluster
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) **- Tipo III**	Serviço/ Cluster
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) **- Tipo VI, Tipo VII e Tipo VIII**	Serviço/ Equip.

(1) Para esta contratação será adotada a definição de cluster como o conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

A solução será dividida em 4 grupos que serão detalhados a seguir.

7.1.1. Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento

O Grupo I conterá os itens 1 à 8, que são apresentados na tabela ETP7.

Dentro destes oito itens, os primeiros cinco tratam de contratação de suporte e garantia para as soluções de Firewall Instaladas na JT, conforme segue:

a) Contratação de garantia e atualização para Firewalls de grande porte já instalados na JT.

i. Item 1 - Pagamento antecipado em parcela única para 60 meses;

ii. Item 4 - Pagamento antecipado em cinco parcelas fixas anuais;

b) Contratação de serviço de garantia e atualização para Firewalls de médio porte já instalados na JT.
   i. Item 2 - Pagamento antecipado em parcela única para 60 meses;

c) Contratação de serviço de garantia e atualização para Firewalls de pequeno porte já instalados na JT.
   i. Item 3 - Pagamento antecipado em parcela única para 60 meses;
   ii. Item 5 - Pagamento antecipado em cinco parcelas fixas anuais;

O padrão de mercado para pagamento do serviço de garantia e atualização é pagamento único e antecipado, para o período contratado (desta forma foram as nossas últimas contratações). Entretanto, a pedido de alguns órgãos participantes, foi prevista a possibilidade de pagamento do suporte em cinco parcelas fixas anuais, atendendo, assim, os Tribunais que não possuem orçamento suficiente para pagamento total da aquisição de garantia e atualização do seu Firewall ainda no exercício de 2025, e, como já informado, não podem ficar sem Firewall atualizado sob risco de interrupção do funcionamento dos seus sistemas de TIC.

Por sua vez, os itens 6 e 7 do Grupo I servem para os Tribunais que precisam modificar a topologia da sua solução de Firewall, instalando mais de um conjunto de equipamentos e também para o Tribunal Superior do Trabalho que pretende adquirir solução de Firewall compatível com a maior parte dos Tribunais que compõem a JT, o que é recomendável posto que o desenvolvimento do PJe e dos sistemas administrativos da JT ocorrem no ambiente on-premises deste Órgão, a saber.

d) Item 6 - Aquisição de Cluster Firewall de Grande porte, compatível com o parque de equipamentos do fabricante Checkpoint instalado na JT, e;

e) Item 7 - Aquisição de Cluster Firewall de Médio porte, compatível com o parque de equipamentos do fabricante Checkpoint instalado na JT.

Ainda neste Grupo, como item 8 foi prevista a capacitação oficial do fabricante para os Clusters de Firewall Checkpoint previstos nos itens 1 a 7 da contratação.

Cabe esclarecer que a garantia de funcionamento e a atualização de assinaturas de proteção são fornecidas pela fabricante dos equipamentos, já o suporte técnico é de prestação direta da empresa contratada, estas explicações pormenorizadas constam no Anexo I.

Esta equipe entende que manter o suporte do parque já instalado com uma mesma empresa e também a expansão/modernização dos Firewall com uma mesma fabricante para todos os Tribunais propicia troca de experiências, resolução conjunta de problemas, implantação de mudanças, aprimoramentos nas configurações e suporte prestado pela empresa de forma mais ágil utilizando informações compartilhadas. A intenção desta padronização de infraestrutura entre os regionais também é demonstrada pela escolha dos tribunais em realizar uma contratação nacional.

O agrupamento dos itens 1 a 8 e sua licitação em lote único não representa restrição ou prejuízo à ampla concorrência, visto que diversas empresas são capazes de fornecer garantia para o parque instalado nos Regionais quanto aos conjuntos de equipamentos para ampliação/modernização das soluções já instaladas.

Tabela ETP7 - Descrição dos objetos do Grupo I

Grupo I - Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall, aquisição de Cluster e Treinamento	
Item	**Objeto**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada **- Tipo I - Pagamento em parcela única, antecipada.**
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada **- Tipo II - Pagamento em parcela única, antecipada.**
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada **- Tipo III - Pagamento em parcela única, antecipada.**
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada **- Tipo I - Pagamento em 5 parcelas fixas anuais.**

5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada **- Tipo III - Pagamento em 5 parcelas fixas anuais.**
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo IV**
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo V**
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall - nível básico**

7.1.2. Grupo II - Aquisição de solução para promover conexão de rede SD-WAN via Firewall

O Grupo II atende aos Tribunais que precisam manter, expandir ou melhorar a comunicação entre suas sedes e Unidades descentralizadas via canal de comunicação seguro, utilizando a Internet via solução de Software-Defined WAN (SD-WAN) integrada aos Firewalls já instalados.

Mais especificamente, os TRTs 5, 7, 9, 10 e 11 manifestaram interesse em implementar esse tipo de solução que depende de uma licença a ser implementada no Cluster central e mais equipamentos de menor porte a serem instalados nas unidades descentralizadas, conforme descrito nos itens 9 a 13, apresentados na tabela ETP8.

Explicando melhor, a solução SD-WAN integrada ao Firewall conecta os Firewalls Centrais (em configuração de Cluster) aos Firewalls menores, instalados nas unidades descentralizadas, e também permitindo ao usuário da unidade remoto acesso à Internet diretamente, sem passar pelo Firewall principal (TRT), mas com as mesmas políticas de segurança, inspeção e filtro de conteúdo, de acordo com o seu perfil.

Estas licenças e equipamentos precisam ser da fabricante Checkpoint, entretanto, considerando que a solução SD-Wan não é uma solução padrão entre os Tribunais participantes e não é a solução principal, optou-se por um grupo separado do Grupo I, com o objetivo de ampliar a competição. Já os itens foram reunidos

neste Grupo pois fazem parte de uma mesma solução e precisam ter compatibilidade entre si, além da compatibilidade com os equipamentos do Grupo I.

Tabela ETP8 - Descrição dos objetos do Grupo II

Grupo II - Aquisição de licenças e equipamentos para promover conexão de rede SD-WAN via Firewall	
Item	**Objeto**
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VI**
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VII**
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VIII**

7.1.3. Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) na modalidade Software como serviço

Já o Grupo III trata da solução de SASE e ZTNA, que é vendido no modelo serviço puro, em nuvem, do inglês Software as a Service, SAAS, e comporá como o item 14 do certame.

Como o SASE é uma tecnologia nova no âmbito da JT, também é previsto treinamento para esta solução no item 15, conforme apresentado na tabela ETP9, abaixo.

Por fim, é importante que a solução de SASE e ZTNA, item 14, e o treinamento para uso da ferramenta sejam entregues pelo mesmo fornecedor, pois a capacitação será focada no caso de implantação de SASE na JT.

Tabela ETP9 - Descrição dos objetos do Grupo III

Grupo III - Aquisição de solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) e Treinamento	
Item	**Objeto**

14	Licença de uso de solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers) por usuário pelo período de 60 meses
15	Voucher de Treinamento para solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)

7.1.4. Grupo IV - Serviço gerenciado para solução de Firewall

O Grupo IV trata do serviço gerenciado para os clusters e equipamentos Firewall desta contratação. Como há diferentes portes de solução e diferentes funcionalidades para cada porte, por esta razão há complexidades distintas para operação entre os equipamentos NG Firewall Checkpoint, dividindo, a saber:

a) Item 16 - Serviço gerenciado para Cluster 16200 Plus e 19200 Plus (porte grande ou Tipos I e IV), de capacidade mais alta entre todos os modelos instalados na JT;

b) Item 17 - Serviço gerenciado para 9700/9800 Plus (porte médio ou Tipos II e V);

c) Item 18 - Serviço gerenciado para Cluster 6700/9200 Plus (porte pequeno ou Tipo III), e;

d) Item 19 - Serviço gerenciado para os equipamentos tipo VI, VII e VIII.

Aqui, da mesma forma que no Grupo I e no Grupo II, o serviço previsto no Grupo IV, também com o propósito de manter o compartilhamento de informações entre os Tribunais a respeito do serviço gerenciado, os serviços para os diferentes equipamentos devem ser executados por uma única empresa, em lote único.

Como já dito, manter o serviço gerenciado com resposta a incidentes por meio de um único fornecedor para todos os participantes permite troca de experiências, agilidade no atendimento pela resolução conjunta de problemas e prevenção de situações utilizando o compartilhamento de informações.

O agrupamento de itens neste edital permite que a empresa faça avaliações mais completas das questões que envolvem o gerenciamento da solução Firewall.

Pois favorece o compartilhamento de experiências entre todos os órgãos participantes, além de permitir ações preventivas para o grupo de Tribunais participantes ao se compartilhar bloqueios de ataques em um dos contratantes.

O agrupamento dos itens 16 a 19 e sua licitação em único lote não representa restrição ou prejuízo à ampla concorrência, visto que diversas empresas são capazes de fornecer o conjunto de serviços.

Tabela ETP10 - Descrição dos objetos do Grupo IV

Grupo IV - Serviço gerenciado mensal	
Item	**Objeto**
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) **- Tipo I e Tipo IV**
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) **- Tipo II e Tipo V**
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) **- Tipo III**
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) **- Tipo VI, Tipo VII e Tipo VIII**

8. Estimativa de custo total da contratação

Com base nos valores levantados e apresentados no documento apartado chamado Estimativas Preliminares de Preços (marcador XXX), a estimativa dos custos da contratação, proveniente da Pesquisa de Mercado e Preços.

A tabela ETP11 traz os valores unitários estimados para os itens previstos na contratação.

Tabela ETP11 - Valores unitários estimados para Grupos e Itens da contratação

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall com aquisição de Cluster, SD-WAN e Treinamento			
Item	**Descrição**	**Unidade**	**Valor unitário**

		(1)	estimado
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	Cluster	R$ 3.996.162,02
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	Cluster	R$ 2.740.770,49
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**	Cluster	R$ 2.528.895,32
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	Cluster	Parcela fixa anual R$ 1.567.936,02 Valor para 5 anos R$ 7.839.680,10
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	Cluster	Parcela fixa anual R$ 891.193,54 Valor para 5 anos R$ 4.455.967,70
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	Cluster	R$ 6.399.252,28
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	Cluster	R$ 5.062.251,46
8	Voucher de **Treinamento** para solução de proteção de perímetro de rede lógica do tipo Next Generation **Firewall**	Aluno	R$ 13.054,41
Grupo II - Aquisição de licenciamento e equipamentos para promover conexão de rede			

SD-WAN via Firewall			
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	Licença/ Cluster	R$ 1.092.075,23
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	Licença/ Cluster	R$ 739.103,08
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VI**	Equip.	R$ 286.091,95
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VII**	Equip.	R$ 266.887,93
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VIII**	Equip.	R$ 193.879,44
Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access) na modalidade Software como serviço e Treinamento			
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)** por usuário pelo período de 60 meses	Usuário	R$ 46,97
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)**	Aluno	R$ 11.230,80
Grupo IV - Serviço gerenciado mensal			
16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) **- Tipo I e Tipo IV**	Serviço/ Cluster	R$ 14.914,41
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) **- Tipo II e Tipo V**	Serviço/ Cluster	R$ 14.914,41
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) **- Tipo III**	Serviço/ Cluster	R$ 14.914,41
19	Serviço gerenciado mensal, contendo operação assistida,	Serviço/	R$ 908,80

	monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) - **Tipo VI, Tipo VII e Tipo VIII**	Equip.	

(1) Para esta contratação será adotada a definição de cluster como o conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

Já a tabela ETP12 traz os valores estimados para os itens considerando as intenções de aquisição segundo os quantitativos formalizados pelos participantes via resposta ao Ofício Circular TRT12/SETIC n. 3/2025.

Tabela ETP12 - Preços Estimados para a contratação

Grupo 1 - Serviço de suporte e manutenção e expansão para solução de NG Firewall utilizada na JT					
Item	**Descrição**	**Qtde mín**	**Qtde máx**	**Valor Unitário**	**Valor Total**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	**10**	**11**	**R$ 3.996.162,02**	**Mínimo R$ 30.961.620,20** **Máximo R$ 43.957.782,94**
2	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo II - Pagamento em parcela única, antecipada.**	**5**	**6**	**R$ 2.740.770,49**	**Mínimo R$ 13.703.852,45** **Máximo R$ 16.444.622,94**
3	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta	**4**	**4**	**R$ 2.528.895,32**	**Mínimo R$ 10.115.581,28** **Máximo R$ 10.115.581,28**

	disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em parcela única, antecipada.**				
4	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em 5 parcelas fixas anuais.**	**1**	**1**	**R$ 7.839.680,10 (1)**	**Mínimo R$ 7.839.680,10** **Máximo R$ 7.839.680,10**
5	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses adicionais para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo III - Pagamento em 5 parcelas fixas anuais.**	**1**	**1**	**R$ 4.455.967,70 (2)**	**Mínimo R$ 4.455.967,70** **Máximo R$ 4.455.967,70**
6	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo IV - Pagamento em parcela única, antecipada.**	**1**	**1**	**R$ 6.399.252,28**	**Mínimo R$ 6.399.252,28** **Máximo R$ 6.399.252,28**
7	**Aquisição de Cluster** de solução de alta disponibilidade para roteamento principal e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de **garantia e atualização** de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses - **Tipo V - Pagamento em parcela única, antecipada.**	**3**	**4**	**R$ 5.062.251,46**	**Mínimo R$ 15.186.754,38** **Máximo R$ 20.249.005,84**
8	Voucher de **Treinamento** para solução de proteção de perímetro	**38**	**100**	**R$ 13.054,41**	**Mínimo R$ 496.067,58**

	de rede lógica do tipo Next Generation **Firewall**				**Máximo R$ 1.305.441,00**
Grupo 2 - Equipamento e licenças para conexão de SD-WAN via solução de Next Generation Firewall					
9	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 1, 4 e 6 - Firewalls **Tipo I e Tipo IV**	**3**	**3**	**R$ 1.092.075,23**	**Mínimo R$ 3.276.225,69** **Máximo R$ 3.276.225,69**
10	Licenciamento de Serviço de Software-Defined WAN (SD-WAN) compatível com os equipamentos NGFW dos itens 2 e 7 - Firewalls **Tipo II e Tipo V**	**2**	**3**	**R$ 739.103,08**	**Mínimo R$ 1.478.206,00** **Máximo R$ 2.217.309,24**
11	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VI**	**2**	**17**	**R$ 286.091,95**	**Mínimo R$ 572.183,90** **Máximo R$ 4.863.563,15**
12	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VII**	**18**	**68**	**R$ 266.887,93**	**Mínimo R$ 4.803.982,74** **Máximo R$ 18.148.379,24**
13	Equipamento Next Generation Firewall (appliance SDWAN e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses **- Tipo VIII**	**4**	**64**	**R$ 193.879,44**	**Mínimo R$ 775.517,76** **Máximo R$ 12.408.284,16**
Grupo 3 -Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)					
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)** por usuário pelo período de 60 meses	**3700**	**2820 0**	**R$ 2.818,80(3)**	**Mínimo R$ 10.429.560,00** **Máximo R$ 79.490.160,00**
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)**	**33**	**120**	**R$ 12.836,38**	**Mínimo R$ 423.600,54** **Máximo R$ 1.540.365,60**
Grupo 4 - Serviço Gerenciado Mensal					

16	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 1, 4 e 6) **- Tipo I e Tipo IV**	**9**	**10**	**R$ 894.864,60(3)**	**Mínimo R$ 8.053.781,40** **Máximo R$ 8.948.646,00**
17	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo 1 (itens 2 e 7) **- Tipo II e Tipo V**	**6**	**8**	**R$ 894.864,60(3)**	**Mínimo R$ 5.369.187,60** **Máximo R$ 7.158.916,80**
18	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade por Cluster de equipamentos do Grupo I (itens 3 e 5) **- Tipo III**	**4**	**4**	**R$ 894.864,60(3)**	**Mínimo R$ 3.579.458,40** **Máximo R$ 3.579.458,40**
19	Serviço gerenciado mensal, contendo operação assistida, monitoramento e resposta a chamados, em regime 24x7, por 60 meses, para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, sem alta disponibilidade por equipamentos do Grupo II (itens 11, 12 e 13) **- Tipo VI, Tipo VII e Tipo VIII**	**18**	**81**	**R$ 54.528,00(3)**	**Mínimo R$ 981.504,00** **Máximo R$ 4.416.768,00**

(1) Valor total para 60 meses de contrato baseado em 5 parcelas fixas anuais de R$ 1.567.936,02.
(2) Valor total para 60 meses de contrato baseado em 5 parcelas fixas anuais de R$ 891.193,54.
(3) Valores unitários para 60 meses de contrato.

9. Declaração de viabilidade da contratação

Declaramos que, de acordo com as análises do ETP, há viabilidade e adequação da contratação e, para o TRT12, há previsão de que seja realizada a

contratação ainda no presente exercício, conforme item no PAC 2025, bem como será incluído nos planejamentos orçamentários dos próximos exercícios.

10. Plano de sustentação e transição contratual

Introdução:

A etapa de elaboração da Sustentação do Contrato compreende:

a) definir Recursos Materiais e Humanos;

b) elaborar Estratégia de Continuidade;

c) definir Atividades de Transição e Encerramento do Contrato;

d) elaborar Estratégia de Independência.

10.1. Recursos necessários à continuidade do negócio durante e após a execução do contrato

10.1.1. Recursos Materiais

a) Para o Grupo I (Itens 1 a 8) - Suporte para os equipamentos dos Tribunais, novos equipamentos Cluster e Treinamento para NG Firewall

Os recursos materiais para o suporte técnico estão disponíveis nos Tribunais, itens 1 a 7. Trata-se dos equipamentos que estão em operação, softwares instalados e acessos seguros aos ambientes via caminhos físicos, redes internas ou Internet.

Já o item 8, treinamento, depende de conexões Internet, redes locais e computadores dos contratantes para permitir a participação dos alunos.

b) Para o Grupo II (itens 9 a 13) Aquisição de licenças e equipamentos para promover conexão de rede SD-WAN via Firewall

Os recursos materiais para instalação das licenças e dos equipamentos que promoverão a comunicação dos Tribunais com suas unidades descentralizadas são link Internet, energia e local físico para instalação nas unidades remotas, o que existe hoje para manter o funcionamento das unidades.

c) Grupo III (14 e 15) - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Accesenvers)

Para funcionamento do serviço SASE, que será disponibilizado em nuvem, o armazenamento, processamento e transmissão de dados é responsabilidade da prestadora do serviço, ficando este Tribunal incumbido apenas de prover os meios de acesso.

d) Grupo VI (16 a 19) - Serviço de operação gerenciado:

Os recursos materiais para os atendimentos de suporte técnico gerenciado são os mesmos da alínea a) e também já estão disponíveis nas instalações dos órgãos participantes.

10.1.2. Recursos Humanos

a) Grupo I (Itens 1 a 5) - Suporte para os equipamentos dos Tribunais, novos equipamentos Cluster e Treinamento para NG Firewall

i. Recurso 1 - Operação: No mínimo 2 servidores responsáveis pela gerência da solução ao longo do contrato.

Disponibilidade: O recurso está disponível e os servidores dos Tribunais que já fazem a gestão dos equipamentos estão alocados nas áreas de Tecnologia da Informação e Comunicação.

Alocação / Competências: Cada servidor dedicará cerca de 10 horas mensais

para operação do sistema de Firewall. Além disso, os servidores deverão ter qualificação em redes lógicas, conhecimentos de infraestrutura de TIC, segurança da informação e, especialmente, na solução de protocolos de conectividade camadas 2 a 7 do modelo OSI e cabeamento estruturado

ii. Recurso 2 - Fiscalização e Gestão do Contrato: Para esta tarefa serão necessários, no mínimo, 4 servidores responsáveis, a saber:

- Gestor titular do contrato;
- Gestor substituto do contrato;
- Fiscal técnico titular do contrato;
- Fiscal técnico substituto do contrato.

Disponibilidade: Os tribunais têm em seus quadros de TIC servidores capazes de assumir a gestão e fiscalização do contrato nos termos deste estudo.

Alocação / Competências: Do grupo de quatro servidores, ao menos 2 deles, um gestor e um fiscal, deverão despender, no mínimo, 2 horas mensais cada para atividades de conferências dos aceites mensais dos serviços. Por se tratar de contratação de TIC, especificamente solução de Firewall, é importante que os fiscais e gestores tenham competências em TIC.

b) Grupo I (Itens 6 a 7) e Grupo II (itens 11 a 13) - Aquisição de novos equipamentos para Tribunais que desejam ampliar ou integrar a solução de Firewall em uso na maior parte dos Órgãos que compõem a JT, como também licenças e equipamentos para implantação de SD-WAN via Firewall:

i. Recurso 1 - Operação: No mínimo 2 servidores responsáveis pela gerência da solução ao longo do contrato.

Disponibilidade: O recurso está disponível e são servidores de TIC que atuam com as soluções de Firewall dos Tribunais que receberão os equipamentos e depois cuidarão de mantê-los operacionais e atualizados.

Alocação / Competências: Cada servidor dedicará cerca de 10 horas mensais para operação do sistema de Firewall. Além disso, os servidores deverão ter qualificação em redes lógicas, conhecimentos de infraestrutura de TIC, segurança da informação e, especialmente, na solução de protocolos de conectividade camadas 2 a 7 do modelo OSI e cabeamento estruturado

ii. Recurso 2 - Fiscalização e Gestão do Contrato: Para esta tarefa serão necessários, no mínimo, 4 servidores responsáveis, a saber:

- Gestor titular do contrato;
- Gestor substituto do contrato;
- Fiscal técnico titular do contrato;
- Fiscal técnico substituto do contrato.

Disponibilidade: Os tribunais têm em seus quadros de TIC servidores capazes de assumir a gestão e fiscalização do contrato nos termos deste estudo.

Alocação / Competências: Do grupo de quatro servidores, ao menos 2 deles, um gestor e um fiscal, deverão despender, no mínimo, 2 horas mensais cada para atividades de conferências dos aceites mensais dos serviços. Por se tratar de contratação de TIC, especificamente solução de Firewall, é importante que os fiscais e gestores tenham competências em TIC.

c) Grupo IV (Itens 16 a 19) - Serviço de operação gerenciado:

i. Recurso 1 - Operação: No mínimo 2 servidores responsáveis por solicitar e acompanhar os chamados ao longo do contrato.

Disponibilidade: O recurso está disponível e os servidores dos Tribunais que já fazem a gestão dos equipamentos estão alocados nas áreas de Tecnologia da Informação e Comunicação.

Alocação / Competências: O tempo que cada servidor dedicará depende do número de chamados mensais. Para fazer e acompanhar chamados técnicos do serviço gerenciado. Para tanto os servidores deverão ter qualificação em

redes lógicas, conhecimentos de infraestrutura de TIC, segurança da informação e, especialmente, na solução de protocolos de conectividade camadas 2 a 7 do modelo OSI e cabeamento estruturado

ii. Recurso 2 - Fiscalização e Gestão do Contrato: Para esta tarefa, assim como na alínea a), serão necessários, no mínimo, 4 servidores responsáveis, a saber:

- Gestor titular do contrato;
- Gestor substituto do contrato;
- Fiscal técnico titular do contrato;
- Fiscal técnico substituto do contrato.

Disponibilidade: Os tribunais têm em seus quadros de TIC servidores capazes de assumir a gestão e fiscalização do contrato nos termos deste estudo.

Alocação / Competências: Do grupo de quatro servidores, estima-se que ao menos 2 deles, um gestor e um fiscal, dependerão, no mínimo, 2 horas mensais cada para atividades de conferências aceites mensais dos serviços. Por se tratar de contratação de TIC, especificamente solução de Firewall, é importante que os fiscais e gestores tenham competências em TIC.

d) Treinamentos (Grupo I, Item 8 e Grupo III, item 15)

i. Recurso 1 - Alunos: Aqui os principais recursos são os alunos que terão suas tarefas cotidianas impactadas para realizar os cursos.

Disponibilidade: Os alunos precisam ficar disponíveis, no mínimo, por 24h para cada curso, durante três dias úteis.

Alocação / Competências: Servidores que irão trabalhar com a solução firewall e SASE.

ii. Recurso 2 - Fiscalização e Gestão do Contrato: Para esta tarefa, assim como na alínea a), serão necessários, no mínimo, 4 servidores responsáveis,

a saber:

- Gestor titular do contrato;
- Gestor substituto do contrato;
- Fiscal técnico titular do contrato;
- Fiscal técnico substituto do contrato.

Disponibilidade: Os tribunais têm em seus quadros de TIC servidores capazes de assumir a gestão e fiscalização do contrato de vouchers de treinamento.

Alocação / Competências: Do grupo de quatro servidores, estima-se que ao menos 2 deles, um gestor e um fiscal, dependerão, no mínimo, 4 horas para atividades de conferências e aceites definitivos dos treinamentos, uma vez, após a realização dos cursos. Não é necessário conhecimento técnico de TIC para avaliar e fazer os recebimentos dos treinamentos.

10.2. Estratégia de continuidade contratual

10.2.1. Para o Grupo I (itens 1 a 5) - Suporte para os equipamentos dos Tribunais

Como o fim do suporte do fabricante aos produtos deste grupo está prevista para 2025, como será mantida a solução que já funciona na maior parte dos Tribunais da JT, no mínimo 60 dias antes do final da vigência do contrato deverá ser adquirida nova garantia com direito de atualização para solução de Firewall.

Nos casos de troca de equipamento, seja na instalação, como o TRT12, ou durante a vigência do contrato, caso acabe a vida útil do modelo, deverá acontecer o funcionamento concomitante dos Clusters até a transferência do Tráfego, “virada de chave”.

A EPC deve estar atenta a exequibilidade dos valores propostos e qualificação técnica das proponentes, pois trata-se de serviço com alto grau de especificidade, trata-se de suporte e garantia para equipamentos Firewall Checkpoint especificados no Anexo I.

Seguem possíveis situações de descontinuidade e ações para tratá-las.