ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO Nº 0614820 / 2023 - PRESI/DG/STI/CIE/SCSEG

1 INTRODUÇÃO

1.1 Contextualização

Em informática, um firewall (em português: parede de fogo), raramente traduzido como corta-fogo ou corta-fogos, é um dispositivo de uma rede de computadores, na forma de um programa (software) ou de equipamento físico (hardware), que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP.
O firewall pode ser do tipo filtros de pacotes, proxy de aplicações, etc. A combinação de software e hardware de proteção é chamada, tecnicamente, de *appliance*. A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.
Os sistemas firewall nasceram no final dos anos 80, fruto da necessidade de criar restrição de acesso entre as redes existentes, com políticas de segurança no conjunto de protocolos TCP/IP. Nessa época, a expansão das redes acadêmicas e militares culminou com a formação da ARPANET que, posteriormente, contribuiu com a criação da Internet. A Internet e a popularização dos primeiros computadores tornaram as redes daquela época alvos fáceis para a incipiente comunidade hacker.

Casos de invasões de redes e fraudes em sistemas de telefonia começaram a surgir. Em 1988, administradores de rede identificaram o que se tornou a primeira grande infestação de vírus de computador, e que ficou conhecido como Internet Worm. O termo em inglês firewall faz alusão comparativa da função que este desempenha para evitar o alastramento de acessos nocivos dentro de uma rede de computadores, a uma parede anti-chamas que evita o alastramento de incêndios pelos cômodos de uma edificação.

1.1.1 Firewalls de Primeira Geração

Filtro de Pacotes: Tecnologia disseminada em 1988 pela DEC (Digital Equipment Corporation), o modelo consistia em um filtro de pacotes, responsável pela avaliação de pacotes do conjunto de protocolos TCP/IP. Até hoje, este tipo de tecnologia é adotado em equipamentos de rede para permitir configurações de acesso simples (as chamadas "listas de acesso"). O "ipchains" (software livre usado para fazer o papel de filtro de pacotes) é um exemplo recente de um firewall que utiliza a tecnologia desta geração. Hoje o "ipchains" foi substituído pelo "iptables" que é nativo do sistema operacional Linux e com maiores recursos.

Regras Típicas da 1ª Geração:
a) Restringir tráfego baseado no endereço IP de origem ou destino;
b) Restringir tráfego através da porta (TCP ou UDP) do serviço.

1.1.2 Firewalls de Segunda Geração

Filtros de Estado de Sessão: A tecnologia foi disseminada a partir de estudo desenvolvido no começo dos anos 90 pela Bell Labs, empresa de pesquisa industrial e desenvolvimento científico subsidiária da empresa filandesa Nokia. Pelo fato de o principal protocolo de transporte TCP orientar-se por uma tabela de estado nas conexões, os filtros de pacotes não eram suficientemente efetivos se não observassem estas características. Foram conhecidos também como firewalls de circuito.

Regras Típicas da 2ª Geração:

a) Todas as regras da 1ª Geração;

b) Restringir o tráfego para início de conexões (NEW);

c) Restringir o tráfego de pacotes que tenham sido iniciados a partir da rede protegida (ESTABLISHED);

d) Restringir o tráfego de pacotes que não tenham número de sequência corretos.

e) Firewall Statefull: Armazena o estado das conexões e filtra com base nesse estado. Existem três estados para uma conexão:

• NEW: Novas conexões;

• ESTABLISHED: Conexões já estabelecidas, e;

• RELATED: Conexões relacionadas a outras existentes.

1.1.3 Firewalls de Terceira Geração

Gateway de Aplicação: Também são conhecidos como "Firewall de Aplicação" ou "Firewall Proxy". Foi nesta geração que se lançou o primeiro produto comercial, em 13 de Junho de 1991- o SEAL da DEC. Diversos produtos comerciais surgiram e se popularizaram na década de 90, como os firewalls Raptor, Gauntlet (que tinha sua versão gratuita batizada de TIS) e Sidewinder, entre outros. Firewalls de camada de Aplicação eram conhecidos desta forma por implementarem o conceito de Proxy e de controle de acesso em um único dispositivo (o Proxy Firewall), ou seja, um sistema capaz de receber uma conexão, decodificar protocolos na camada de aplicação e interceptar a comunicação entre cliente/servidor para aplicar regras de acesso.

Regras Típicas da 3ª Geração:

a) Todas as regras das gerações anteriores;

b) Restringir acesso FTP a usuários anônimos;

c) Restringir acesso HTTP para portais de entretenimento;

d) Restringir acesso a protocolos desconhecidos na porta 443 (HTTPS).

1.1.4 Firewalls de Quarta Geração e Subsequentes

O firewall consolida-se como uma solução comercial para redes de comunicação TCP/IP. Estes equipamentos passam a inspecionar pacotes e tráfego de dados baseado nas características de cada aplicação, nas informações associadas a todas as camadas do modelo OSI (Open Systems Interconnection), e não apenas na camada de rede ou de aplicação, e no estado das conexões e sessões ativas. Os novos equipamentos passam a adotar a prevenção de intrusão (Intrusion Prevention System - IPS) como forma de identificar o abuso do protocolo TCP/IP mesmo em conexões aparentemente legítimas. Também começam a utilizar o recurso da inspeção aprofundada de pacotes (Deep Packet Inspection - DPI) associando as funcionalidades do Statefull Inspection (inspeção de estados) com as técnicas dos dispositivos IPS. A partir dos anos 2000, a tecnologia de firewall é aperfeiçoada para ser aplicada também em estações de trabalho e computadores domésticos (o chamado Firewall Pessoal), além dos surgimento de soluções de firewall dedicado a servidores e aplicações específicas (como servidores Web e banco de dados) ou mesmo usuários.

1.1.5 Next-Generation Firewalls ou Firewalls de Próxima Geração (NGFW)

O NGFW é um novo conceito de firewall, o qual vem com recursos adicionais quando comparado ao modelo tradicional.

Diferentemente de um modelo tradicional de firewall que faz controle de IP de origem, IP de destino, porta de origem, porta de destino e flags, somente um Next Generation Firewall vai além, com análises mais profundas no pacote que é trafegado por ele. Em um NGFW é possível analisar se um download que está sendo feito contém algum tipo de ameaça, tipo um ransomware ou outro malware qualquer, conhecido (que já tenha uma assinatura) ou desconhecido (zero day). Para esse último a análise pode ser feita localmente ou na nuvem, sendo extremamente importante possuir técnicas antievasivas. O NGFW também agrega função de IPS, ou seja, enxergam dentro dos pacotes de rede se existe alguém mal intencionado tentando explorar vulnerabilidades em algum serviço que rode na sua infraestrutura. Outra funcionalidade importante é a de URL Filtering, onde é possível controlar o acesso a milhares de sites não desejados, com base nas políticas da empresa, e evitar incidentes de segurança, uso indevido dos recursos de rede da empresa e outras situações não desejadas.

Os NGFW também possuem prevenção contra vazamento de dados (DLP) sensíveis para o negócio. Em suma, suas características básicas são: conectividade de dispositivos móveis e VPN (VPN and mobile device connectivity), identificação de usuários e computadores (identity and computer awareness), filtro de URL (URL Filtering), controle de aplicação (Aplication Control), prevenção contra intrusão e ameaças (Intrusion and Threat Prevention), prevenção contra perda de dados (Data Loss Prevention) e inspeção SSL (SSL Inspection).

As ameaças modernas, como ataques de malware baseados na web, ataques direcionados, ataques de camada de aplicativos e mais, modificaram as características necessárias ao firewall. Na verdade, mais de 80% de todas as novas tentativas de malware e intrusão estão explorando pontos fracos em aplicativos, ao invés de pontos fracos em componentes e serviços de rede.
Os firewalls stateful com recursos de filtragem de pacotes simples eram o bloqueio eficiente de aplicativos indesejados, já que a maioria das aplicações atendiam as expectativas do protocolo de porta. Os administradores podiam impedir prontamente que um aplicativo inseguro fosse acessado pelos usuários ao bloquear as portas e protocolos associados.

A proteção baseada em portas, protocolos, endereços IP não é mais confiável e viável. Isso levou ao desenvolvimento de uma abordagem de segurança baseada em Identidade, que leva as organizações a um passo à frente dos dispositivos de segurança convencionais que vinculam a segurança aos endereços IP.

NGFWs oferecem aos administradores uma maior conscientização e controle sobre aplicações individuais, juntamente com capacidades de inspeção mais profundas pelo firewall. Os administradores podem criar regras muito mais amplas de "liberação / bloqueio" para controlar o uso de sites e aplicativos na rede.

Também possuem capacidade de integração com diversos produtos de segurança tais como antivírus, WAFs (Web Application Firewall) e ferramentas de verificação de ataques de dia 0 (sandbox).

Os sistemas de segurança baseados em contexto são projetados com "inteligência" incorporada para usar informações situacionais - identidade, localização, tempo, dispositivo, função comercial, etc. - para tomar decisões de segurança mais efetivas. Eles são bem adaptados aos ambientes móveis e à nuvem de hoje, pois podem responder de forma mais inteligente e rápida a situações inesperadas. Ao entender o contexto de uma solicitação do usuário, o sistema de segurança ou o firewall podem ajustar a resposta de segurança e controlar como a informação é entregue ao usuário, simplificando bastante um mundo computacional cada vez mais complexo.

1.1.6 Sistema de Gerenciamento de Logs

Um arquivo de log é um registro contínuo e com registro de data e hora de eventos e mensagens gerados automaticamente por seus sistemas de TI e aplicativos de software. Eles registram o que aconteceu, quando e por quem. Esses eventos e mensagens são gravados em um único arquivo de log ou residem em muitos arquivos localmente ou em locais remotos.
O registro em log é o ato de coletar dados não estruturados como uma trilha de auditoria para análise de causa raiz, bem como transmissão ao vivo de atividade. Eles podem ser encontrados em servidores, computadores, sistemas operacionais, redes, aplicativos, encadeamentos, estruturas de aplicativos e contêineres. Eles podem registrar falhas, exceções, ajudar a depurar erros, identificar violações de segurança e fornecer informações úteis para os desenvolvedores analisarem.

Os dados encontrados nos logs podem ser desestruturados e estruturados de várias maneiras. Na sua forma mais básica, há um timestamp, nível e mensagem. Outros detalhes podem incluir o nome do host, tipo de log, aplicativo, tags, endereço IP, endereço MAC e status do soquete TCP. Há também muitos formatos de tipos de log, como o formato de log comum, eventos do Windows, syslog, JSON, Cron e muito mais.

Os logs geralmente são criados pelos desenvolvedores para depurar a operação de um aplicativo ou para entender o comportamento do usuário. Isso significa que os dados dentro da mensagem de log podem variar entre desenvolvedores, aplicativos, fornecedores e sistemas.
O gerenciamento de logs é a abordagem usada para lidar com grandes volumes de dados de log gerados continuamente por quase todos os dispositivos de computação e aplicativos de software, e abrange o processo de coleta de dados, ingestão, agregação de logs, análise, pesquisa, relatórios e armazenamento de longo prazo e retenção.

Com os aplicativos modernos em nuvem e seus logs de infraestrutura crescendo a cada minuto na produção, é crucial ter uma visão final do que está acontecendo dentro do aplicativo, estrutura, contêiner, servidores e dispositivos de rede. Com uma solução de registro adequada, você pode pesquisar rapidamente grandes quantidades de dados, localizar problemas em tempo real com visualizações personalizadas, criar regras e alertas e oferecer suporte à análise e aos relatórios necessários.

Uma solução de gerenciamento de log escalável e centralizada deve automatizar esse processo e permitir que o monitoramento, alertas, relatórios e insights necessários permitam que suas operações de negócios prosperem com o mínimo de problemas de produção e de servidor.
O gerenciamento de log permite que os usuários criem suas próprias regras, visualizações e alertas para que os padrões possam ser facilmente reconhecidos e os dados sejam contextuais e acionáveis. Para operações de rede e operações de segurança, o gerenciamento de logs ajuda a detectar problemas e padrões proativamente, de modo que a equipe possa intervir e resolver antes que os problemas aumentem. As equipes aumentam sua eficiência operacional usando ferramentas inteligentes de gerenciamento de registros.

Ferramentas modernas de gerenciamento de logs, não apenas armazenam logs, mas são capazes de correlacioná-los a sessões de acesso de forma a detectar anomalias e remediá-las com uso de gatilhos que dispararão procedimentos pré-configurados para mitigar essas falhas.

1.2 O TRE-AC

Atualmente o TRE-AC, possui Firewall CheckPoint T160 produto este contratado em meados de 2015, já não possui mais garantia e nem suporte. Visando manter uma ferramenta que possua melhoria e recursos amplos que atendam as necessidade operacionais e de segurança desta instituição faz necessário a contratação de um Firewall Secure Web Gateway.

2. DESCRIÇÃO DO OBJETO DA CONTRATAÇÃO

2.1 A solução deverá atender aos seguintes requisitos iniciais:

a. Atender os novos requisitos da ENSEC-JUD não atendidos com o firewall existente no TRE-AC, quais sejam:

"5.4 Implantar ferramentas de gerência de configuração de sistemas que automaticamente imponham e reapliquem opções de configuração sobre os sistemas em intervalos regulares agendados;

6.3 Habilitar o log dos sistemas de forma a incluir informações detalhadas, tais como origem do evento, data, usuário, horário, endereços de origem, endereços de destino e outros elementos úteis;

6.6 Implantar Security Information and Event Management (SIEM) ou ferramenta analítica de logs para correlação e análise de logs;

6.7 Em uma base regular, revisar os logs para identificar anomalias ou eventos anormais;

6.8 Em uma base regular, ajustar as configurações do SIEM de forma a melhor identificar eventos que requeiram ações e diminuir o ruído proveniente de eventos não importantes."

b. Atender a necessidade de modernização do parque de segurança de equipamentos do TRE, diminuindo os riscos de possíveis ataques e melhorando a qualidade dos arquivos de registro (logs) das atividades realizadas na rede, facilitando a rastreabilidade e a identificação de incidentes;
c. Mitigar riscos de indisponibilidade dos sistemas com a adoção de equipamento mais atualizado;

d. Melhorar os relatórios gerados de segurança para futuras auditorias operacionais;

e. Melhorar rendimento e escala com a inclusão de novo equipamento com características de processamento e memória bem maiores que o atualmente utilizado, proporcionando uma maior durabilidade da solução na rede do TRE-AC;

f. Atender à Portaria TRE-AC n.º 163/2023, relativa ao protocolo de investigação para ilícitos cibernéticos, quanto à guarda de logs e registros.

Além disso a solução deverá possuir as seguintes características:

• Integração dos recursos de segurança de proteção contra ameaças em um único dispositivo de segurança de rede de alto desempenho;

• Possuir Unidade de processamento de segurança (SPU);

• Permitir visibilidade total dos usuários, dispositivos, aplicativos em toda a superfície de ataque e aplicação consistente da política de segurança, independentemente da localização do ativo;

• Proteger contra vulnerabilidades exploráveis da rede com IPS;

• Bloquear automaticamente ameaças no tráfego descriptografado usando inspeção SSL, incluindo o mais recente padrão TLS 1.3 com cifras obrigatórias;

• Bloquear proativamente os ataques sofisticados recém-descobertos em tempo real com IA e serviços avançados de proteção contra ameaças;

• Possuir segmentação adaptada a qualquer topologia de rede;

• Oferecer defesa em segurança profunda, com inspeção e correção L7 de alto desempenho;

• Possuir Interfaces de alta velocidade para permitir flexibilidade de implantação.

• Fornecer acesso seguro à web contra riscos internos e externos, mesmo para tráfego criptografado com alto desempenho;

• Bloquear e controlar o acesso à web com base em usuários ou grupos de usuários nos URLs e domínios;
• Bloquear solicitações de DNS contra domínios maliciosos;

• Fornecer proteção avançada em várias camadas contra ameaças de malware de dia zero entregues pela Web.

No termo de referência, os requisitos e as características da solução serão melhor detalhados e especificados.

2.1.1 Soluções Disponíveis no Mercado (Art. 14, I, a)

Há vários fabricantes de soluções de firewall disponíveis no mercado. Procuramos avaliar soluções disponíveis no principal quadrante da Gartner (Leaders), dentre elas três empresas: PALLO ALTO, FORTINET e CHECKPOINT, e também a CISCO (bem próxima do principal quadrante).

3 ROL DE NORMATIVOS QUE DISCIPLINAM A EXECUÇÃO DOS SERVIÇOS

3.1 Resolução CNJ Nº 396/2021. Que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)

3.2 Resolução CNJ Nº 182/2013. Dispõe diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ)

3.3 Estratégia Nacional de Cibersegurança da Justiça Eleitoral

3.4 Portaria TRE-AC 163/2023 – institui protocolo de investigação para ilícitos cibernéticos

4 ANÁLISE DA(S) CONTRATAÇÃO (ÇÕES) ANTERIOR (ES)

4.1 O serviço já foi contratado anteriormente?

SIM ( )

NÃO (X)

4.1.1 Se afirmativo, relatar as inconsistências porventura ocorridas nas fases do Planejamento da Contratação, Seleção do Fornecedor e Gestão do Contrato:

5 DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES

5.1 Aquisição de solução afim de deter suporte e garantia de ferramenta de serviço de Firewall SWG, já que nosso Firewall em funcionamento atual não possui mais suporte e garantia.

5.2 Fortalecer a Segurança da Informação no âmbito do Tribunal Regional Eleitoral do Acre, mantendo a integridade dos dados e das informações sensíveis; e melhorando a qualidade de serviço das aplicações internas.

5.3 Utilizar solução tecnológica afim de atender as legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet (Lei nº 12.965/2014) .

6 ALINHAMENTO DA CONTRATAÇÃO AOS PLANOS INSTITUÍDOS PELO TRIBUNAL

6.1 Segurança da informação e proteção de dados (G3 – PTE -PDTIC)

6.2 Ferramentas Automatizadas (E3- Estratégia Nacional de Cibersegurança da JE)

7 REQUISITOS DA CONTRATAÇÃO

7.1 Requisitos necessários ao atendimento da necessidade.	x
7.2 No caso de serviço, informar se possui natureza continuada	Não possui natureza continuada
7.3 Critérios e práticas de sustentabilidade que devem ser veiculados como especificação técnica do objeto ou como obrigação da contratada	• Para efeito de cumprimento dos critérios de sustentabilidade deverá ser observado que os equipamentos, preferencialmente, serão acondicionados em embalagens individuais adequadas, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento, conforme Instrução Normativa nº 01/2010 do Ministério do Planejamento, Orçamento e Gestão. • Observar que os equipamentos, do objeto, não devem conter substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados(PBBs), éteres difenil-polibromados (PBDEs) em concentração acima da recomendada pela pela Diretiva 2002/95/EC do Parlamento Europeu também conhecida como diretiva RoHS27 (Restriction of Certain Hazardous Substances), sendo que o atendimento a essa diretriz deve ser comprovado por meio de certificado ou por declaração do fabricante, nos termos do inciso IV do Art. 5º da Instrução Normativa nº 01/2010 do Ministério do Planejamento, Orçamento e Gestão.
7.4 Duração inicial do contrato de prestação de serviços de natureza continuada	Não se aplica
7.4.1 Se superior a 12 meses, apresentar justificativa	Não se aplica
7.5 Será necessário que a Contratada promova a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas	( ) Sim (X) Não
7.5.1 Em caso afirmativo, deve ser elaborado plano de transição, de modo a assegurar: • que o prazo de transição seja suficiente para não haver interrupção dos serviços; • que os riscos de sabotagem ou não cooperação por parte do contratado anterior sejam minimizados; • que as responsabilidades do novo contratado na fase de encerramento do contrato anterior sejam claramente definidas, evitando a alegação de dificuldades para implementação do novo contrato.	Não se aplica

7.1 REQUISITOS TÉCNICOS MÍNIMOS

Os requisitos técnicos mínimos estão descritos conforme segue.

ITEM 1	
DESCRIÇÃO	Firewall de Borda

THROUGPUT MÍNIMO ACEITÁVEL COM THREAT PROTECTION ATIVO	2,5 GBps
THROUGPUT MÍNIMO ACEITÁVEL COM IPS ATIVO	3,5 Gbps
THROUGPUT MÍNIMO ACEITÁVEL NGFW	3,3 Gbps
STORAGE MÍNIMO	200 GB
PORTA 10 GB (Quantidade Mínima)	04 SFP+ ou 04 SFP+Opt
PORTA 1 GB (Quantidade Mínima)	12 (RJ45 ou RJ45 Opt ou SFP Opt)

ITEM 2	
DESCRIÇÃO	Firewall de Núcleo
THROUGPUT MÍNIMO ACEITÁVEL COM THREAT PROTECTION ATIVO	3,6 GBps
THROUGPUT MÍNIMO ACEITÁVEL COM IPS ATIVO	10 Gbps
THROUGPUT MÍNIMO ACEITÁVEL NGFW	6 Gbps
STORAGE MÍNIMO	128 GB
PORTA 10 GB (Quantidade Mínima)	02 SFP+
PORTA 1 GB (Quantidade Mínima)	8 RJ45

ITEM 3 – SOLUÇÃO DE GERENCIAMENTO E RELATÓRIO
1. Deve prover gestão centralizada de todos os dispositivos do lote;
2. Deve estar licenciado e suportar a gestão de, no mínimo, o quantitativo total de dispositivos presentes no lote;
3. Deve ser do tipo Appliance Físico, Appliance Virtual ou solução de software baseada em máquina virtual (VM). Caso seja baseada em Máquina Virtual (VM), a PROPONENTE deverá indicar em sua proposta qual a necessidade de hardware a ser disponibilizada para a respectiva instalação;
4. Caso seja em VM, deve ser compatível com Xen ;
5. Deve suportar operação em alta disponibilidade (há) sincronizando as mudanças na base de dados entre as estações de gerência;
6. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
7. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
8. Permitir acesso concorrente de administradores;
9. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;
10. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
11. Gerar alertas automáticos via Email;
12. Gerar alertas automáticos via SNMP;
13. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;
14. Deve ser permitido ao administrador transferir os backups para um servidor FTP;
15. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;
16. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;
17. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;

18. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;

19. Deve suportar sincronização do relógio interno via protocolo NTP;

20. Deve registrar as ações efetuadas por quaisquer usuários;

21. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;

22. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

23. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

24. A solução de gerência deve permitir criar administradores que tenham acesso à todas as instâncias de virtualização;

25. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

26. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

27. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

28. Permitir localizar quais regras um objeto está sendo utilizado;

29. Deve atribuir sequencialmente um identificador a cada regra de firewall;

30. Permitir criação de regras que fiquem ativas em horário definido;

31. Permitir backup das configurações e rollback de configuração para a última configuração salva;

32. Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras;

33. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

34. Deve permitir que todos os firewalls sejam controlados de forma centralizada utilizando apenas um servidor de gerência;

35. O servidor de gerência deve ser hospedado em um equipamento independente, não exercendo funções de firewall;

36. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;

37. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;

38. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

39. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

40. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada.

41. Deve prover console unificada e centralizada;

42. Deve auxiliar na solução e identificação de ameaças;

43. Pode ser entregue como appliance física ou virtual;

44. Deve ser do mesmo fabricante dos demais itens do lote;

45. Deve possibilitar o armazenamento e tratamento de logs de, no mínimo, 100 dispositivos.

46. Deve possibilitar o armazenamento mínimo local de logs em VM's de até 500 GB;

47. Deve estar licenciada para o total de equipamentos firewall disponíveis para o lote;

48. Deve permitir a integração com soluções de SIEM disponíveis no mercado, tais como ArcSight - Micro Focus, QRadar - IBM, Splunk visando a integração nacional dos dados coletados.

ITEM 4 – IMPLANTAÇÃO COM TREINAMENTO HANDS ON

1. Os serviços de instalação e configuração, compreendem, entre outros, os seguintes procedimentos:

1.1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;

1.2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

1.3. Regras de Firewall existentes e aplicáveis à solução ofertada dada a colocação desta na Rede deste parque;

1.4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

1.5. Apresentação do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

1.6. Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;

1.7. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será considerado entregue, quando for instalado e configurado, com todas as

atualizações, configurações e licenças. Deverão ser adicionados a este todos os firewalls contemplados na solução adquirida, e que deverão estar sendo monitorados e gerenciados por este Sistema de Gerência Centralizada;

1.8. Deve haver geração de relatório e entrega da documentação da instalação com as configurações efetuadas e as decisões tomadas, diagramas e topologias em formato legível e tecnicamente fundamentado;

1.9. A CONTRATADA deverá ministrar treinamento do tipo “Hands On” sobre a solução de Firewall adquirida, incluindo instalação, configuração básica e avançada, troubleshoot, monitoramento e gerenciamento;

1.10. A carga horária mínima será de 20 horas divididas em expedientes de 4h/dia, das 8h às 12h;

1.11. O treinamento será ministrado para um total de seis (6) participantes da CONTRATANTE;

1.12. O repasse deverá ter caráter prático e se baseará no sistema Firewall efetivamente instalado na CONTRATANTE;

1.13. O treinamento deve ser do tipo presencial e a sua realização será nas cidades indicadas no Termo de Referência.

1.14. É de responsabilidade da CONTRATADA designar um profissional certificado pelo Fabricante, fornecer todo material audiovisual, didático e, caso necessário, outros equipamentos eletrônicos para a realização dos treinamentos, além de impressos.

1.15. Todos os demais custos, ônus, obrigações e encargos para o treinamento devem ser arcados pela CONTRATADA.

ITEM 5 – TREINAMENTO OFICIAL
1. Deve ser fornecido treinamento ou voucher de treinamento oficial do fabricante de administração e otimização do ambiente com validade de no mínimo 01 ano a ser realizada na cidade sede do Regional; 2. O treinamento deverá abarcar as configurações básicas e avançadas da solução envolvendo, no mínimo, os seguintes tópicos: 2.1 - Acesso à interface, console, etc; 2.2 - Configuração de NAT e ACL's; 2.2 - Configuração de VPN; 2.3 - Configuração de SSL-VPN; 2.4 - Otimização do ambiente; 2.5 - Gerenciamento e melhores práticas de segurança no ambiente; 2.6 - Bloqueios e liberações de portas e aplicações; 2.7 - Configurações IPS/IDS; 2.8 - DMZ; 2.9 - Zero Trust Network.

8 LEVANTAMENTO DE MERCADO – ALTERNATIVAS (SOLUÇÕES DE MERCADO) E DEFINIÇÃO

Canário 1	
Descrição	Licitação e contratação de Solução de Firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia
Fornecedor	Oi S.A. e Teledata (Fortinet) e Approach (Palo Alto). Conforme Propostas Comerciais.
Análise da Solução	Contratação da Solução através de Licitação, de fornecedores e fabricantes no mercado.

Cenário 2	
Descrição	Aderir a Ata 100/2022 do TRE-PE, para a contratação de Solução de Firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia
Fornecedor	Oi S.A. (Fortinet)

Cenário 3	
Descrição	Fornecimento em comodato da solução de Firewall com software de análise de logs, conexão 2FA para VPN e suporte/garantia
Fornecedor	Heimdallr Cybersecurity LTDA

Após estudo e avaliação da equipe de contratação, o resultado que propicia o melhor cenário é o 2 (Aderir a Ata 100/2022 do TRE-PE), conforme considerações a seguir.

- No Cenário 1 após o levantamento prévio de propostas de mercado conforme descrito no tópico 10 Estimativas de Preço, os custos mostraram-se muito superior ao Cenário 2, sendo que a menor proposta ficou 113% (cento e treze por cento) acima do valor total dos valores conferidos pela ata do TRE-PE 100/2022, portanto observa-se que o cenário 1, possivelmente resultaria uma maior despesa a administração publica. Além de questões que serão mais aprofundadas no tópico 8.1 Justificativas do Modelo de Contratação.
- Quanto ao Cenário 3, é de interesse da Administração manter domínio e propriedade do equipamento, já que se trata de algo basilar para a segurança cibernética desta instituição. Lembrando que em comodato, o bem deve ser devolvido após término do contrato, aumentando o risco desta instituição ficar sem um equipamento vital para segurança, já que de fato não é proprietário. Portanto por estas situações, já no inicio esta opção foi desconsiderada.
- Portanto o Cenário 2 que pretende a contratação de Firewall de Próxima Geração com software de análise de logs, conexão 2FA para VPN e suporte/garantia atende na totalidade os requisitos esperados pela equipe de contratação, além de possuir a principio o melhor resultado custo/benefício.

8.1 JUSTIFICATIVAS DO MODELO DE CONTRATAÇÃO

A partir disto justifica-se a adesão a ata (cenário 2) pelos motivos elencados abaixo.

- Demora na aquisição da solução: uma nova licitação pode provocar demora na aquisição da Solução e isto poderá resultar em grande prejuízo já que o Firewall que hoje esta em funcionamento no TRE-AC, não possui mais garantia e suporte da fabricante.
- Não execução do orçamento: Caso opta-se por realização de uma nova licitação há um risco maior de impossibilidade de execução do orçamento neste ano.
- Custo e limite na execução: A ARP 100/2022 do TRE-PE, foi realizada com múltiplos participes, havendo alto quantitativos de itens previstos para contratação, o que resultou em preços mais vantajosos naquele Pregão. Portanto como já falado antes, havendo adesão da ata, a despesa na aquisição desta solução é mais vantajosa. É valido frisar, que atualmente possuímos um orçamento restrito para esta contratação.
- Atendimento aos requisitos e necessidades do TRE-AC: é fato que a solução vencedora do Pregão 73/2022, em especial aos Itens 1, 2, 4, 5 e 6 do lote 1; atende as necessidades deste Tribunal; quantos outras atas de registro de preço não atendem por completo os requisitos pretendidos por este tribunal.
- Adequação ao inciso III do Art. 3º do decreto 11.462/2023.

9 ESTIMATIVAS DE QUANTIDADES

ITEM	DESCRIÇÃO	QUANT	UNID
1	Firewall de Borda	1	unidade
2	Firewall de Núcleo	2	unidade
3	Software de Gerenciamento e Relatório	3	unidade
4	Implantação com Hands ON	2	unidade
5	Treinamento Oficial	4	pessoas

9.1 Firewall de Borda (item 1)

O Produto será necessário para realizar a proteção específica da rede e infra estrutura de cópia de segurança desta instituição.

9.2 Funcionamento em HA (High Availability/Alta Disponibilidade)

O item 2 trata de duas unidades sendo que tais equipamentos em conjunto promovendo alta disponibilidade, ou seja em redundância física e lógica. E promoverão defesa de perímetro da rede do TRE-AC, em relação a outras redes.

9.3 Software de Gerenciamento

Tão importante quanto o funcionamento dos equipamento em si, é a realização do gerenciamento do ambiente, portanto é necessário que a solução possua o software de gerenciamento devidamente instalado e integrado com os equipamentos, com funcionamento pleno conforme Termo de Referência. Disso trata o item 3, sendo a quantidade de uma unidade para cada equipamento; apesar de que algumas empresas fornecedoras indicarão apenas uma unidade que atenderia o total de equipamentos necessários.

9.4 Implantação com Hands ON

Efetuar o repasse inicial da solução de firewall implantada, incluindo as configurações realizadas, senhas iniciais e apresentação ao ambiente. O serviço será executado uma única vez. São duas unidades, pois a primeira corresponde a instalação de um Firewall (item1); e a segunda unidade a instalação da dupla de Firewalls (item 2) em Alta Disponibilidade.

9.5 Treinamento

Trata-se do treinamento oficial do equipamento e software das equipes técnicas nas soluções adquiridas para os itens 1, 2 e 3. Será necessário o treinamento para 4 pessoas.

10 ESTIMATIVAS DE PREÇOS

Após recebimento de propostas encaminhadas pela fornecedoras OI S.A, Teledata e Approach Tecnologia, em conjunto com o resultado do Pregão 73/2022 do TRE-PE. Conforme observados no Procedimento SEI n. 0001214-80.2022.6.01.8000; obteve-se os valores conforme tabela abaixo.

ITEM	DESCRIÇÃO	QUANT	UNID
1	Firewall de Borda	1	unidade

Fornecedora	**Descrição (Part)**	**P. Unitário**	**P. Total**
OI S.A	FG-201F e FC-10-F201F-950-02-60	**R$ 248.640,00**	**R$ 248.640,00**
TLD TeleData	FG-201F e FC-10-F201F-950-02-60	**R$ 319.200,00**	**R$ 319.200,00**
Aprroach	PA-1410	**R$ 580.983,00**	**R$ 580.983,00**
ATA de Registro de Preços 100/2022 TRE/PE	FG-201F, FC-10-F201F-950-02-60, FN-TRAN-SFP+SR e FTM-ELIC-500	**R$ 158.152,69**	**R$ 158.152,69**

2	Firewall de Núcleo	2	unidade

Fornecedora	**Descrição (Part)**	**P. Unitário**	**P. Total**
OI S.A	FG-601F e FC-10-0601F-950-02-60	**R$ 599.170,00**	**R$ 1.198.340,00**
TLD TeleData	FG-601F e FC-10-0601F-950-02-60	**R$ 648.299,00**	**R$ 1.296.598,00**
Approach	PA-1420	**R$ 1.091.534,25**	**R$ 2.183.068,50**
ATA de Registro de Preços 100/2022 TRE/PE	FG-601E, FC-10-F6H1E-950-02-60, SP-FG300E-PS e FN-TRAN-SFP+SR	**R$ 229.509,56**	**R$ 459.019,12**

3	Software de Gerenciamento e Relatório	-	unidade

Fornecedora	**Descrição (Part)**	**quant**	**P. Unitário**	**P. Total**
OI S.A	FMG-VM-10-UG, FC1-10-M3004-248-02-60, FAZ-VM-GB25 e FC3-10-LV0VM-248-02-60	**1**	**R$ 221.960,00**	**R$ 221.960,00**
TLD TeleData	FMG-VM-10-UG, FC1-10-M3004-248-02-60, FAZ-VM-GB25 e FC3-10-LV0VM-248-02-60	**1**	**R$ 264.450,00**	**R$ 264.450,00**
Approach	PANORAMA	**1**	**R$ 171.428,74**	**R$ 171.428,74**
ATA de Registro de Preços 100/2022 TRE/PE	FMG-VM-10-UG, FC1-10-M3004-248-02-60, FAZ-VM-GB25 e FC3-10-LV0VM-248-02-60	**3**	**R$ 4.440,00**	**R$ 13.320,00**

4	Implantação com Hands ON	2	unidade

	Fornecedora		P. Unitário	P. Total
	OI S.A		**R$ 29.500,00**	**R$ 88.500,00**
	TLD TeleData		**R$ 35.000,00**	**R$ 105.000,00**
	Approach		**R$ 49.778,33**	**R$ 99.556,67**
	ATA de Registro de Preços 100/2022 TRE/PE		**R$ 64.863,25**	**R$ 129.726,50**

5	Treinamento Oficial	4	unidade

Fornecedora		P. Unitário	P. Total
OI S.A		**R$ 8.000,00**	**R$ 32.000,00**
TLD TeleData		**R$ 12.000,00**	**R$ 48.000,00**
Approach		**R$ 16.759,24**	**R$ 67.036,97**
Pregão 73/2022 TRE-PE		**R$ 19.310,00**	**R$ 77.240,00**

Totais

Fornecedora	Total x Fornecedora
OI S.A	**R$ 1.789.440,00**
TLD TeleData	**R$ 2.033.248,00**
Approach	**R$ 3.102.074,03**
Pregão 73/2022 TRE-PE	**R$ 837.458,31**

11 JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DO OBJETO

Os equipamentos e licenças que constituem a solução, aqui proposta, interagem entre si de forma a convergir para um sistema unificado, de modo que o fornecimento parcelado inviabilizaria a implantação de tecnologia capaz de atender as necessidades deste órgão.

A eventual divisão do objeto em grupos diversos poderia ocasionar uma situação onde um proponente “A”, por não conhecer a solução, não teria condições de fornecer eventual licenciamento correto para tal ou mesmo propor equipamentos compatíveis. Ante ao exposto, é evidente que o agrupamento do objeto, de maneira a compor uma solução unificada, é necessário a fim de evitar eventuais problemas de compatibilidade.

Ademais, lidar com um único fornecedor diminui o custo administrativo de gerenciamento de todo o processo de contratação. O aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública.

Por fim, o agrupamento em lote, de todos os itens deste processo, visa garantir a otimização dos prazos de execução, viabilizando a sincronia nos fornecimentos e serviços de instalações, evitando assim que um fornecedor venha a prejudicar a execução de outro. Ainda, conforme disposto no inciso I, do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, todos os itens deverão ser do mesmo fabricante.

12 RESULTADOS ESPERADOS

Realizaremos pregão eletrônico aberto a todos os fabricantes de uma solução completa compreendendo um subconjunto dos seguintes itens: firewals de núcleo, e firewall de borda, e softwares de gerenciamento e de relatórios, além dos serviços de implantação com repasse hands-on e treinamentos oficiais.

Novamente, indicamos que a importância de que o lote tenha uma única solução atribuída é referendada pela Gartner, uma empresa que norteia o futuro das soluções de TIC no mundo. Em documento publicado em 2022, a Gartner indicava como boas práticas a convergência em tecnologia de segurança com o objetivo de reduzir complexidade, simplificar a administração e aumentar a eficiência.

Além disso busca-se os seguintes resultados esperados:

12.1 Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº (12.965/2014);

12.2 Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;

12.3 Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

12.4 Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.

12.5 Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.

13 NECESSIDADES DE ADEQUAÇÃO DE AMBIENTE INTERNO PARA EXECUÇÃO CONTRATUAL

A mudança no ambiente de tecnologia deverá ser efetuada de forma gradual com a substituição de funcionalidades atualmente utilizadas pelo firewall existente pelos novos firewalls adquiridos até a substituição completa e desativação/realocação do firewall atual.

As etapas do processo consistirão nas seguintes fases:

13.1 Instalação física dos novos equipamentos e conexão com a estrutura de rede existente;

13.2 Configuração dos novos equipamentos com as regras de firewall existentes;

13.3 Posicionamento do firewall na rede em momento posterior ao firewall atual para testes e ajustes;

13.4 Remoção do firewall antigo da rede.

Não será necessário maiores adequações no ambiente físico, já no ambiente lógico será necessário a realização de configurações que serão realizadas no decorrer da implantação da solução.

14 DECLARAÇÃO DA VIABILIDADE

A equipe responsável pelo planejamento da contratação, ciente das regras e diretrizes da Resolução CNJ nº 182/2013, após a conclusão de todos os estudos técnicos preliminares aqui contidos, declara ser viável a contratação pretendida, da seguinte forma:

1. Contratação por meio de adesão a Ata de Registro de Preços, por conta da previsão orçamentária e informações anunciadas no tópico 8.1.

15 EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

SILVIO FORASTIERO FRAZÃO

Técnico Judiciário - Seção de Cibersegurança

INTEGRANTE DEMANDANTE

BRUNO SAMUEL PEREIRA GOMES

Coord. de Infraestrutura - CIE

INTEGRANTE TÉCNICO

BRUNA SILVA BRASIL

Técnico Judiciário - Seção de Compras Licitações e Contratos

INTEGRANTE ADMINISTRATIVO

Documento assinado eletronicamente por **BRUNA SILVA BRASIL**, **Chefe de Seção**, em 30/09/2023, às 10:28, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRUNO SAMUEL PEREIRA GOMES SILVA**, **Coordenador(a)**, em 02/10/2023, às 09:37, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **SILVIO FORASTIERO FRAZÃO**, **Técnico Judiciário**, em 03/10/2023, às 12:20, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0614820** e o código CRC **D2E04E8C**.