

Estudo Técnico Preliminar 29/2025

1. Informações Básicas

Número do processo:

2. Descrição da necessidade

O presente estudo destina-se à contratação de empresa especializada para o fornecimento de solução de alta disponibilidade de Next Generation Firewall, incluindo os serviços de assistência técnica com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remoto, por 60 (sessenta) meses.

Os equipamentos e softwares contratados no contrato 029/2017 compõem a solução de segurança (firewall e IPS) do Senado Federal, sendo responsáveis pela segurança de perímetro das conexões existentes entre o Senado e a Internet, o Senado Federal e a Câmara dos Deputados, o serviço de VPN do Senado Federal e o isolamento do tráfego da rede sem fio.

Esse tipo de equipamento atua como um ponto centralizador para todo o tráfego das redes internas do Senado Federal e da Internet. Esse equipamento para segurança de redes é responsável por determinar, com base em regras pré-configuradas ou permissões de acesso de usuários, quais tipos de tráfego podem ser transmitidos entre as redes. Além disso, essa solução tem a capacidade de analisar os pacotes de dados para identificar possíveis ataques ou tráfego malicioso, utilizando assinaturas ou comportamentos suspeitos como base para essa verificação.

Nesse contexto, é importante ressaltar que o equipamento em questão desempenha um papel crucial na viabilização do acesso remoto ao ambiente do Senado Federal, permitindo o teletrabalho por meio da implementação de uma conexão VPN (Rede Virtual Privada). Além disso, ele desempenha a função de garantir a segurança da rede de dados do Senado, mantendo o firewall atualizado e operacional 24 horas por dia, 7 dias por semana. O firewall, age como uma barreira, filtrando e analisando tanto o tráfego proveniente do ambiente externo ao Senado Federal quanto o tráfego interno na rede do órgão.

A Solução de Alta Disponibilidade de Next Generation Firewall da Rede Local do Senado Federal (Solução de Firewall) é composta por equipamentos do fabricante Fortinet, e sua garantia está amparada no contrato 21/2021, do qual a NCT INFORMÁTICA LTDA é signatária, o qual possui vigência até 24/02/2026. Diante do exposto, se faz necessário renovar tal suporte e licenças através da aquisição de nova solução de Next Generation Firewall.

O objetivo desse estudo é avaliar as alternativas que viabilizem a contínua segurança de perímetro de redes, de forma a subsidiar a contratação da solução que melhor se adeque às necessidades do Senado Federal.



3. Área requisitante

Área Requisitante	Responsável
COINTI/SESIER	Rodrigo Sávio Leiros Borges, Claudio Ferreira da Silva, Roberto de Oliveira Silva

4. Necessidades de Negócio

A Solução de Alta Disponibilidade de Next Generation Firewall da Rede Local do Senado Federal (Solução de Firewall), atualmente em funcionamento, é composta por equipamentos do fabricante Fortinet, e sua garantia de funcionamento está amparada nos ITENS I, II, III e IV do Contrato 21-2021. Os referidos itens do contrato terão sua vigência encerrada em fevereiro de 2026. Para minimizar o risco de suspensão dos serviços providos pela Solução de Firewall nos casos de defeitos de funcionamento desses equipamentos, bem como eliminar os riscos devido ao encerramento dos recursos providos pelas licenças das Fortinet, os serviços de assistência técnica com garantia de funcionamento, além da solução de firewall e suas licenças e assinaturas respectivas devem ser contratadas em substituição aos serviços previstos naqueles itens do contrato 21-2021.

Desta forma, após os estudos descritos no corrente ETP, sugere-se a contratação de empresa especializada para o fornecimento de solução de alta disponibilidade de Next Generation Firewall, incluindo os serviços de assistência técnica com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remoto para atender a demanda aqui apresentada.

Portanto, entre as justificativas para manter a mesma marca e fabricante no projeto de NGFW proposta na solução escolhida, destacam-se os seguintes pontos:

Nos termos do art. 7º, §4º, da Lei nº 14.133/2021, a indicação de marca específica em licitações somente é admissível quando devidamente justificada por razões técnicas ou de padronização, visando à obtenção de maior eficiência e economicidade na contratação.

Neste contexto, a manutenção da marca cujo padrão é atualmente utilizado na solução de firewall institucional justifica-se pelos seguintes fatores:

1. Capacitação Técnica da Equipe

A equipe técnica responsável pela administração da infraestrutura de segurança da informação encontra-se amplamente capacitada na tecnologia atualmente empregada. O que garante maior autonomia, agilidade na resolução de incidentes e redução de custos com suporte terceirizado ou treinamentos adicionais.

2. Facilidade de Migração e Integração

A adoção de solução de mesmo fabricante assegura compatibilidade nativa com os ativos de rede e sistemas de monitoramento já implantados, além de permitir a reutilização de configurações, políticas de segurança e regras previamente configuradas. Isso reduz substancialmente o tempo de migração, os riscos operacionais e os custos associados à transição tecnológica.



3. **Padronização e Continuidade Operacional**

A padronização da solução de firewall com base no mesmo fabricante promove a continuidade operacional, evita a fragmentação tecnológica e facilita a gestão centralizada da segurança da informação. Tal abordagem está alinhada com as boas práticas de governança de TIC e com os princípios da economicidade e eficiência previstos na legislação vigente.

4. **Histórico de Desempenho e Confiabilidade**

A solução atualmente em uso demonstrou, ao longo dos últimos anos, desempenho satisfatório, alta disponibilidade e robustez frente às demandas institucionais. A manutenção da marca visa preservar esse histórico positivo, evitando a adoção de tecnologias não testadas no ambiente crítico da organização.

Diante do exposto, e considerando os princípios da eficiência, economicidade, continuidade do serviço público e mitigação de riscos operacionais, justifica-se tecnicamente a designação da marca Fortigate como condição essencial para a contratação da solução de firewall no presente certame. Além do exposto, é importante ressaltar que a solução da Fortinet atualmente em uso, é líder absoluta no mercado, assim posicionada no quadrante Gartner, o que indica que a Instituição está bem servida e posicionada ao manter essa solução e fabricante e, como citado anteriormente, a solução está em produção no Senado Federal desde 2017, provendo todos os recursos de segurança necessários durante o período.

Adicionalmente, é importante ressaltar que a solução pretendida irá realizar a atualização do hardware, e modernização do sistema de segurança de rede e não apenas renovar as assinaturas e o suporte. Com isso, o Senado Federal terá equipamentos modernos e ainda em produção ativa, com desempenho ainda superior ao equipamento atual, cujo suporte técnico será descontinuado em 2028. Essa atualização é fundamental para mitigar potenciais riscos no ambiente computacional, atualizando-se hardware e software e adquirindo uma licença que provê recursos de segurança de rede superiores ao que está atualmente em uso no Prodasen, como será demonstrado ao longo do documento.

Finalmente, considerando as contratações de objeto semelhante, avaliadas por ocasião deste ETP, percebeu-se que não se comprovou a vantajosidade da substituição do padrão tecnológico atual do Senado Federal.

Na solução proposta, não haverá necessidade de redesenho da infraestrutura de rede e a consequente indisponibilidade dos serviços de TI oferecidos pelo Senado Federal. Embora todas as soluções concorrentes sejam Next Generation Firewalls, cada uma delas possui suas peculiaridades e formas de atuação na rede e, mantendo-se a solução atual, pode-se reduzir significativamente as indisponibilidades durante a atualização da solução e consequentemente proporcionar um período de migração com menores intercorrências.

Dito isso, considerando o alto nível de dependência e integração da infraestrutura de rede do Senado Federal com a solução atual, tecnicamente é mais custoso realizar a migração para outro fabricante, estando mais suscetível a intercorrências. Essas intercorrências podem variar dependendo do impacto e serviço afetado, além de que, uma solução nova exigirá que a equipe técnica do Prodasen passe um extenso treinamento até dominar a solução como um todo e adquira a expertise necessária para operá-la no dia a dia.

Esses riscos não existem se a solução atual for mantida, bem como a necessidade de treinamento, uma vez que a equipe de gerenciamento já possui total domínio da ferramenta



e uma ampla experiência em todos os aspectos que a solução oferece.

Nesse contexto, o órgão técnico tem como objetivo manter a continuidade do hardware e software utilizados na solução atual durante o período de migração, e posteriormente atualizar o hardware e software da solução.

Natureza continuada

Considera-se o serviço constante do objeto como de prestação continuada, pois a contratação trata de serviço NGFW para proteção contra ameaças cibernéticas. A contratação trata de serviço essencial às atividades do Senado Federal, de caráter permanente, e sua interrupção resultaria em comprometimento da prestação do serviço público à sociedade, uma vez que a utilização do serviço de NGFW é condição imprescindível para o funcionamento de diversos sistemas vitais no Senado Federal.

Contratações Correlatas ou Interdependentes

Esta contratação substitui o contrato 21/2021, o qual será encerrado em 24/02/2026 por não ser mais possível a sua prorrogação.

Alinhamento entre a Contratação e o Planejamento

Tendo em vista que o PDTI 2023-2024 possuiu vigência até abril 2025, e a contratação ocorrerá em momento posterior, esta contratação estará prevista no próximo Plano Diretor de Tecnologia da Informação (PDTI). Além do citado, ela já está em consonância com diretrizes do PDTI atual, como: “Id 11 - Garantir a adequação e a segurança da infraestrutura e dos serviços de TI, necessários às novas formas de trabalho e gestão do trabalho.” “Id 14 - Promover a gestão do ciclo de vida, a segurança da informação e a qualidade das soluções de TI.”

O número da Contratação no Plano de Contratações que está no SENIC: Contratação 20260133 (Aquisição de equipamentos e serviço de suporte para Firewall).

Impactos Ambientais e medidas mitigatórias

Esta contratação não gera impactos ambientais.

Justificativa para parcelamento ou não da contratação:

Em se tratando de uma solução atrelada a um conjunto de equipamentos de comunicação e proteção de dados de propósito específico composto por elementos de hardware e software oriundos de um mesmo fabricante, para garantir o seu perfeito funcionamento, não há possibilidade de parcelamento da contratação.

Além do citado, é possível se obter economia de escala com a compra dos itens do mesmo fornecedor, bem como redução de custos de gestão de contratos.

Ademais, como citado ao longo do documento, os equipamentos, devido a critérios de desempenho, confiabilidade e padronização acima citados, são oriundos de um mesmo fabricante.



5. Necessidades Tecnológicas

A garantia de funcionamento dos equipamentos que integram a solução está amparada por um pacote de serviços oferecido pelo Fabricante Fortinet, adquirido por intermédio do Pregão 106/2016, que estabeleceu o atual padrão tecnológico usado no Senado Federal, e cuja continuidade ocorreu por meio do contrato 21/2021, operado por parceiro devidamente capacitado para realizar os procedimentos de diagnóstico e solução de problemas. O modelo escolhido se mostrou bastante adequado as necessidades do Senado Federal, sendo que o SESIER recomenda novamente a sua adoção alterando algumas funcionalidades para aumentar o nível de segurança e recursos prestados pela solução. As licenças que o Senado Federal possui junto a Fortinet são:

1. 6 licenças FC-10-03200-950-02-60
 2. 1 licença FC4-10-0ACVM-248-02-60
 3. 1 licença FC4-10-LV0VM-248-02-60
 4. 1 licença FC2-10-M3004-248-02-60
- Licença FC-10-03200-950-02-60 - Referente ao Fortigate- 3200D (Firewall do Senado Federal) - Unified Threat Protection (UTP) - (24x7 Forticare Plus Application Control, IPS, AV, Web Filtering and Antispam, Fortisandbox CLOUD). O referido pacote fornece os principais recursos de segurança de rede do Senado Federal, como IPS/IDS, Malware Protection, WEB e DNS Security. Seguem todos os serviços oferecidos pela licença:



PRODUCT OFFERINGS

For FortiGate hardware, virtual machines, and software-as-a-service (SaaS):

FORTIGUARD SECURITY SERVICES

INDIVIDUAL / BUNDLES				
Network Security	A La Carte	Enterprise	UTP	ATP
IPS	✓	✓	✓	✓
IPS	✓	✓	✓	✓
Malicious/Botnet URLs	✓	✓	✓	✓
File Content Security				
Advanced Malware Protection (AMP)	✓	✓	✓	✓
Antivirus	✓	✓	✓	✓
Botnet Domains	✓	✓	✓	✓
Mobile Malware	✓	✓	✓	✓
Virus Outbreak Protection	✓	✓	✓	✓
Content Disarm & Reconstruct*	✓	✓	✓	✓
AI-based Heuristic AV	✓	✓	✓	✓
FortiGate Cloud Sandbox	✓	✓	✓	✓
Zero-Day Threat Protection				
AI-based Inline Malware Prevention*	✓	✓		
Web & DNS Security				
URL, DNS & Video Filtering	✓	✓	✓	
URL Filtering	✓	✓	✓	
DNS Filtering	✓	✓	✓	
Video Filtering*	✓	✓	✓	
Malicious Certificate	✓	✓	✓	
Anti-spam		✓	✓	
Data & SaaS Posture				
Data Loss Prevention (DLP)	✓	✓		
Attack Surface Security	✓	✓		
IoT Device Detection	✓	✓		
IoT Vulnerability Correlation	✓	✓		
Security Rating	✓	✓		
Outbreak Check	✓	✓		
Operation Technology Security				
OT Security	✓			
OT Device Detection	✓			
OT vulnerability correlation & Virtual Patching	✓			
OT Application Control and IPS	✓			

SD-WAN AND SASE SERVICES

INDIVIDUAL / BUNDLES				
	A La Carte	Enterprise	UTP	ATP
SD-WAN Underlay Bandwidth and Quality Monitoring	✓			
SD-WAN Overlay-as-a-Service	✓			
SD-WAN Connector for FortiSASE Secure Private Access	✓			
SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth)		Desktop Models only		

NOC AND SOC SERVICES

INDIVIDUAL / BUNDLES				
	A La Carte	Enterprise	UTP	ATP
FortiConverter Service	✓	✓		
Managed FortiGate Service	✓			
FortiGate Cloud	✓			
FortiManager Cloud	✓			
FortiAnalyzer Cloud	✓			
FortiGuard SOCaaS	✓			

FORTICARE SUPPORT SERVICES AND INCLUDED SERVICES

INDIVIDUAL / BUNDLES				
	A La Carte	Enterprise	UTP	ATP
FortiCare Essentials		Desktop Models only		
FortiCare Premium	✓	✓	✓	✓
FortiCare Elite	✓			
Base Updates Services (Included with all FortiCare Support contracts)				
Application Control	✓	✓	✓	✓
Inline CASB*	✓	✓	✓	✓
Device/OS Detection	✓	✓	✓	✓
GeoIPs	✓	✓	✓	✓
Trusted CA Certificates	✓	✓	✓	✓
Internet Services & Botnet IPs	✓	✓	✓	✓
DDNS (v4/v6)	✓	✓	✓	✓
Local Protection	✓	✓	✓	✓
PSIRT Check	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Timezone	✓	✓	✓	✓

* Not available for FortiGate e/FortiWiFi 40F, 60E, 60F, 80E, 90E series, and FGR-60F series with from 7.4.4 onwards. Not available on FortiGate/FortiWiFi 30G and 50G series in any OS build.

Fonte: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiguard.pdf>

- Licença FortiAuthenticator - VM License 24x7 FortiCare Contract (1-10100 Users) - fornece serviços de gerenciamento de identidade e acesso (<https://www.fortinet.com/br/products/identity-access-management/fortiauthenticator>)
- Licença FortiAnalyzer - VM Support 24x7 FortiCare Contract (for 1-Unlimited GB /Days of Logs) - oferece análise de rede de alto desempenho e análise de riscos (<https://www.fortinet.com/br/products/management/fortianalyzer>)
- FortiManager - VM Support 24x7 FortiCare Contract (1-110 devices/ Virtual Domains) - Permite manter controle e visualização sobre a segurança e dispositivos (<https://www.fortinet.com/br/products/management/fortimanager>)



Diante do exposto, a solução escolhida como a melhor no presente estudo tem como objeto a atualização dos equipamentos, software e licenças existentes, modernizando tecnologicamente o legado, garantindo a continuidade do sistema de segurança de redes. Para que a solução possa continuar funcionando de forma eficiente, se faz necessário que o sistema seja modernizado, inclusive adotando novas tecnologias que detectam pragas e ataques virtuais, atuando na prevenção e segurança dos dados armazenados ou transmitidos pelo Senado Federal. A atualização ampliará o desempenho de serviços de Firewall e conectividade de dados.

Integração e Compatibilidade dos Sistemas:

O órgão técnico entende que a vantagem da aquisição está na padronização e alinhamento às práticas de mercado, por possibilitar o uso de equipamentos modernos, populares e amplamente utilizados por vários Órgãos e empresas públicas/privadas.

Acrescente ainda a total compatibilidade com o ambiente tecnológico atual, da facilidade de instalação e operação, não demandando qualquer “arranjo tecnológico” para o pleno funcionamento, reduzindo, assim, o risco de paralisação ou comprometimento da infraestrutura do Senado Federal.

A contratação prevê também a expansão dos serviços de manutenção e garantia do fabricante na solução Fortinet atualmente implementada, mudando a licença UTP para Enterprise. Tal medida se faz necessária para que os equipamentos atuais estejam amparados pelos serviços de atualização durante o período de aquisição, entrega e migração das funcionalidades para o parque atualizado e possua diversos recursos de segurança não integrante da licença UTP. Os equipamentos atuais serão utilizados como backup e suporte dos novos equipamentos durante o período de implantação, visando garantir que não haja parada dos serviços ofertados pelo Prodasen.

Ressalta-se os equipamentos e software a serem fornecidos deverão obrigatoriamente ser do fabricante Fortinet e ter compatibilidade com os equipamentos já existentes no Senado Federal, além de permanecer os critérios de garantia dos equipamentos atualmente instalados no parque tecnológico do Senado Federal.

Por fim, ficará a cargo da contratada a instalação e configuração dos equipamentos e softwares nas instalações da CONTRATANTE.



6. Demais requisitos necessários e suficientes à escolha da solução de TIC

No caso do Senado Federal, em função da sua infraestrutura e do grau de dependência de algumas aplicações em relação aos tipos de equipamentos a serem mantidos, o modelo da prestação de serviço deverá ser por chamado, conforme descrito neste Estudo Técnico Preliminar. Nesse modelo se caracteriza a impessoalidade, sem subordinação direta visto que, não requer a exclusividade, pois o profissional que vier a prestar o serviço poderá ser compartilhado com outros contratos que porventura a Prestadora de Serviço possua;

Não haverá controle de frequência ou de número de horas de presença mínimo nas dependências do Senado Federal;

Não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da Prestadora de Serviço e o Senado Federal.

A empresa contratada se obriga, durante o prazo do contrato, a trabalhar junto à equipe de suporte do PRODASEN com a finalidade de implementação, gerenciamento e configuração dos equipamentos objeto da prestação de serviços aqui descrita, que são de propriedade da Contratante.

A empresa contratada deverá oferecer suporte e assistência técnica na modalidade 24 (vinte e quatro) horas por 7 (sete) dias por semana através de e-mail, telefone ou pessoalmente (on-site), em português, durante o prazo do contrato, sempre que acionada pela Equipe Técnica do PRODASEN.

A empresa contratada deve possuir em seus quadros funcionais, pelo menos um técnico de nível superior, com diploma de nível superior na área de Tecnologia da Informação, ou Engenharia e certificação oficial do fabricante dos equipamentos (Fortinet), com comprovada experiência em atividades de suporte técnico. A comprovação se dará pela apresentação das certificações oficiais do fabricante Fortinet no momento da Reunião de Apresentação Inicial.

A solução a ser contratada deve ser capaz de manter operacionalmente íntegra e com as assinaturas atualizadas a solução adquirida pelo Contrato 21/2021 durante o período de migração para a nova solução de Next Generation Firewall.

Neste viés, faz-se necessária a contratação de um pacote de manutenção e atualização de licenças e assinaturas, fornecido pelo mesmo fabricante, para a instalação da solução de segurança da FORTINET, que vem atendendo as demandas do Senado Federal de modo eficiente.

7. Estimativa da demanda - quantidade de bens e serviços

O fim do ciclo de vida do Firewall FG-3200D (Firewall instalado no Senado Federal) ocorrerá, segundo documentação oficial da Fortinet, na data de 16/04/2028.





Product Life Cycle Announcement

01/16/2023

With the release of this announcement, Fortinet is notifying partners of the company's intent to discontinue the sale of the following products. Fortinet recommends the following migration path for the products being discontinued:

Current SKU	Description	Replacement SKU	Description
FG-3200D	48 SFP+ 10-Gig ports (2 SFP+ SR-type transceivers included) 2x480GB SSD internal storage, and dual AC power supplies	FG-3401E	4x 100 GE QSFP28 slots and 24x 25 GE SFP28 slots (including 22x ports, 2x HA ports), 2x GE RJ45 Management ports, SPU NP6 and CP9 hardware accelerated, 4 TB SSD onboard storage, and 2 AC power supplies

Per the terms of the Fortinet Life Cycle Policy, Fortinet will continue to provide hardware support services for a minimum of sixty (60) months from the End of Order (EOO) milestone. The EOO milestone for a given product represents the last date that Fortinet will accept new orders for fulfillment, providing there is inventory available to fulfill the order. RMA/Replacements after the EOO milestone may include "like-for-like replacements" or an "enhanced replacement". In the case of enhanced replacement, changes to the customer's network or upgrade to a currently supported software release may be required.

Product Life Cycle Milestones	
End of Orders (EOO)	16Apr2023
Last date to purchase new maintenance contract	16Apr2023
Last date to extend an existing maintenance contract	16Apr2027
Product support expires	16Apr2028

Additional information about the Fortinet life cycle policy can be found in the Fortinet Life Cycle Policy document, found in the Fortinet Support Portal at: <http://support.fortinet.com/>.

Diante do exposto, e como o contrato 21/2021 encerrará em 24/02/2026, se faz necessária a aquisição de nova solução visto que, do ponto de vista técnico e econômico, como será descrito aqui nesse estudo, não é recomendado que se mantenha a solução atual até o fim do seu ciclo de vida devido ao custo das licenças no fim do ciclo de vida de equipamento, bem como limitará os recursos a disposição do Senado Federal.

8. Levantamento de soluções

Alternativa 1

Aquisição de novo pacote de serviços semelhante ao adquirido nos itens I, II, III, IV do Contrato 21/2021, durante 24 (vinte e quatro) meses, afim de renovar o suporte do firewall até o fim do ciclo de vida do equipamento.



Alternativa 2

Aquisição de nova solução de Next Generation Firewall, mantendo o padrão atual, com garantia durante 60 (sessenta) meses, com a manutenção da solução atual durante o período de migração.

Alternativa 3

Fornecimento de nova solução (equipamentos), em licitação sem designação de marca, com garantia de 60 (sessenta) meses.

9. Análise comparativa de soluções**Da escolha do tipo de licença:**

A licença utilizada pelo Senado Federal, como citado nas necessidades tecnológicas presente neste documento, é a UTP (Unified Threat Protection (UTP)). Porém, a FORTINET possui, além da licença UTP, a licença ATP e a licença Enterprise. A ATP é inferior a UTP e possui uma menor quantidade de recursos e tecnologia, em contrapartida a Enterprise é superior a UTP e possui a maior quantidade de recursos entre as licenças oferecidas pela fabricante. Segue comparativo dos principais serviços providos por cada licença:



FORTIGUARD SECURITY SERVICES

INDIVIDUAL / BUNDLES				
Network Security	A La Carte	Enterprise	UTP	ATP
IPS	✓	✓	✓	✓
IPS	✓	✓	✓	✓
Malicious/Botnet URLs	✓	✓	✓	✓
File Content Security				
Advanced Malware Protection (AMP)	✓	✓	✓	✓
Antivirus (AV)	✓	✓	✓	✓
Botnet Domains	✓	✓	✓	✓
Mobile Malware	✓	✓	✓	✓
Virus Outbreak Protection	✓	✓	✓	✓
Content Disarm & Reconstruct*	✓	✓	✓	✓
AI-based Heuristic AV	✓	✓	✓	✓
FortiGate Cloud Sandbox	✓	✓	✓	✓
Zero-Day Threat Protection				
AI-based Inline Malware Prevention*	✓	✓		
Web & DNS Security				
URL, DNS & Video Filtering	✓	✓	✓	
URL Filtering	✓	✓	✓	
DNS Filtering	✓	✓	✓	
Video Filtering*	✓	✓	✓	
Malicious Certificate	✓	✓	✓	
Anti-spam		✓	✓	
Data & SaaS Posture				
Data Loss Prevention (DLP)	✓	✓		
Attack Surface Security	✓	✓		
IoT Device Detection	✓	✓		
IoT Vulnerability Correlation	✓	✓		
Security Rating	✓	✓		
Outbreak Check	✓	✓		
Operation Technology Security				
OT Security	✓			
OT Device Detection	✓			
OT vulnerability correlation & Virtual Patching	✓			
OT Application Control and IPS	✓			

Portanto, visando uma atualização tecnológica e aprimorar os recursos de segurança da informação, este órgão técnico adotou a licença Enterprise como o padrão para a presente contratação. Salienta-se que além de provê todos os recursos que a atual licença possui, ele acrescenta os recursos de Data Loss Prevention (DLP), Attack Surface Surface Security, e toda parte de segurança relacionada à IOT.

A licença Enterprise também acrescenta o serviço FortiConverter responsável pela migração de firewalls legados para os firewalls de próxima geração (NGFWs) do FortiGate de forma

rápida e fácil. O serviço elimina erros e redundância, empregando as melhores práticas com metodologias avançadas e processos automatizados. Além disso, pode acelerar a proteção da rede com a mais recente tecnologia FortiOS.

Salienta-se também, que as propostas presentes na alternativa 2, realizadas pela NCT Informática, estão com o serviço de FortiAI inserido na licença do FortiManager (tecnologia que não está presente na atual solução do Senado). Segue detalhe da proposta:

2.5) Para o item 5: Licença FortiCare Contrac (1 - 110 devices/Virtual Domains) (FC2-10-M3004-248-02-60), FortiAI Subscription Generative AI powered central management service, utilizing large language models (LLMs) for real-time assistance in orchestration, automation and monitoring (1 - 10 devices/Virtual Domains) (FC1-10-M3004-1118-02-60) e FortiManager AI Top Up License FortiAI Assistant upgrade license for adding 500,000 AI tokens (FC1-10-AITMG-1089-

O FortiAI protege a organização utilizando recursos de inteligência artificial, além de possuir um prompt de comandos semelhante às tecnologias mais utilizadas no mercado como chatgpt e copilot, no entanto, tal prompt está integrado a topologia da organização. Os comandos utilizados na solução são realizados e adaptados a estrutura de rede implantada, permitindo assim facilitar toda a parte de gestão e mudanças na estrutura, além de proporcionar upgrades lógicos de forma simples e reduzir a taxa de erros, visto que a IA fará todo o trabalho de "varredura" na rede e entregará a solução proposta levando em conta todos os aspectos lógicos e de configuração.

Alternativa 1

Aquisição de novo pacote de serviços semelhante ao adquirido nos itens I, II, III, IV do Contrato 21/2021, durante 24 (vinte e quatro) meses, afim de renovar o suporte do firewall até o fim do ciclo de vida do equipamento.

Trata-se de mercado restrito aos parceiros do fabricante FORTIGATE habilitados a fornecer equipamentos e serviços de assistência técnica com garantia de funcionamento para os equipamentos integrantes da solução de Firewall da Rede Local do Senado Federal.

Porém, tal restrição não tem o intuito de limitar a competição a um parceiro específico, visto que, há diversas empresas que possuem parceria com a Fortinet aptas a fornecer os equipamentos aqui descritos e, portanto, habilitados a competir, entre eles, pode-se citar as seguintes empresas: ISH, GlovalSec, Layer, NCT, WY, Oakmount Group, Sonda e Blueeye.

Alternativa 2

Aquisição de nova solução de Next Generation Firewall com garantia durante 60 (sessenta) meses, com a manutenção da solução atual durante o período de migração.

Trata-se de mercado restrito aos parceiros do fabricante Fortinet habilitados a fornecer equipamentos e serviços de assistência técnica com garantia de funcionamento para os equipamentos integrantes da solução de Firewall da Rede Local do Senado Federal.

Porém, tal restrição não tem o intuito de limitar a competição a um parceiro específico, visto que, há diversas empresas que possuem parceria com a Fortinet aptas a fornecer os equipamentos aqui descritos e, portanto, habilitados a competir, entre eles, pode-se citar as seguintes empresas: ISH, GlovalSec, Layer, NCT, WY, Oakmount Group, Sonda e Blueeye.

Alternativa 3



Fornecimento de nova solução (equipamentos) com garantia de 60 (sessenta) meses.

A presente alternativa implica em aquisição de nova solução, portanto, será precedida de licitação sem designação de marca. Além disso, do ponto de vista técnico, o treinamento deverá compor o contrato, visto que não há como se garantir que irá haver continuidade do fabricante dos equipamentos atuais. Diante disso, e como exposto nos capítulos 4 e 5 desse documento, tal aquisição apresenta diversos riscos, além da falta de padronização e incremento da complexidade.

10. Registro de soluções consideradas inviáveis

Prorrogação Contratual durante 60 meses.

Inviável, tendo em vista o fim do ciclo de vida do equipamento em 2028.

11. Análise comparativa de custos (TCO)

Alternativa 1

Aquisição de novo pacote de serviços semelhante ao adquirido nos itens I, II, III, IV do Contrato 21/2021, durante 24 (vinte e quatro) meses. Para efeito de comparação com o cenário anterior, foi levado em conta o valor anual do contrato, visto que as outras alternativas tratam de cenários de 60 meses. Já esse cenário possui 24 (vinte e quatro) meses, devido ao EOS (End of Support) do equipamento citado nesse documento.

Outro aspecto importante a ser considerado é que esta alternativa também restringe o mercado de empresas habilitadas a fornecerem os serviços de garantia de funcionamento àquelas habilitadas tecnicamente pelo fabricante dos equipamentos que compõem atualmente a solução (FORTINET).

Diante do exposto, segue custo estimado conforme proposta da NCT.

FG-3200D - 24 MESES UTP						
Ordem	Nome	Valor Unitário		QTD	Valor Total	
1	FC-10-03200-950-02-24 - FortiGate-3200D - Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud) - 24 meses	R\$	765.600,00	6	R\$	4.593.600,00
5	FC4-10-0ACVM-248-02 - FortiAuthenticator-VM 24x7 FortiCare Contract (1 - 10100 USERS) - 24 meses	R\$	62.700,00	2	R\$	125.400,00
6	FC5-10-LVOVM-248-02 - FortiAnalyzer-VM - Support, 24x7 FortiCare Contract (for 1-101 GB/Day of Logs) - 24 meses	R\$	61.500,00	1	R\$	61.500,00
Valor Total						R\$ 4.780.500

Com esse valor para 24 Meses, foi possível estimar o custo anual, no valor de R\$2.390.250,00 (Dois milhões trezentos e noventa mil e duzentos e cinquenta reais).

Salienta-se que, a alternativa 1 possui a licença Unified Threat Protection (UTP) 24x7 FortiCare plus (pacote de serviços semelhante ao do ITENS I, II, III e IV do Contrato 021/2021) durante o prazo de 24 meses, que é inferior a licença Enterprise presente na alternativa 2. Mesmo com tais diferenças, além de todos os ganhos técnicos proporcionados pela

atualização da solução descritos na alternativa 2, o cenário de manutenção dos Firewalls ainda assim apresenta um custo anual maior quando comparado com a alternativa abaixo.

Alternativa 2

Aquisição de nova solução de Next Generation Firewall com garantia durante 60 (sessenta) meses, com a manutenção da solução atual durante o período de migração.

Para estimar a aquisição de novos equipamentos para a substituição da solução atual foram utilizados os valores propostos pela NCT INFORMÁTICA (empresa signatária do contrato 21/2021). Salieta-se que todas as propostas enviadas contemplam o cenário de manutenção do parque atual pelo período de 3 meses, em que será possível realizar o upgrade da solução sem intercorrências.

Durante o pedido proposto, após análise do portfólio da empresa Fortinet, foram selecionados 2 equipamentos tidos pela equipe técnica como os mais adequados em requisitos de similaridade e eficiência com o atual em produção no Senado. O primeiro equipamento tido como referência foi o FortiGate 3501F, equipamento de linha semelhante ao atual presente no Senado (FortiGate 3200D), com capacidade de throughput maior, devido a ser um equipamento mais novo, de uma linha mais atual lançada pela Fortinet, porém, proporcionalmente, levando em conta o fator tempo, os equipamentos são de linhas semelhantes (O FG 3200D foi lançado em 2015, então mesmo que seja da mesma linha 3000, suas capacidades de throughput são menores). Os firewalls da empresa citada possuem a tecnologia de VDOM, que permite dividir o FortiGate em até 10 unidades virtuais por equipamento, que funcionam de forma independente, permitindo que sejam provisionadas políticas de segurança de forma separada de acordo com o tipo de conexão e a finalidade de cada VDOM, dividindo um único domínio de segurança em vários domínios lógicos. Tal tecnologia permite que se diminua o número de equipamentos a serem adquiridos no Senado Federal. Dessa forma, a estimativa de custos foi realizada utilizando 2 Firewalls FG 3501F (atualmente a solução no Senado possui 6 Firewalls 3200D), que possui 40 portas cada um, totalizando 80 portas no total e adquirindo um pacote extra de VDOMs, para que se possa fazer a segregação de domínios aqui citada, sem necessariamente adquirir um novo equipamento para isso.



Aquisição Enterprise - 2x FG-3501F 60 meses				
Ordem	Nome	Valor Unitário	Qtd	Valor total
1	Equipamento Fortigate FG-3501F	R\$ 1.360.000,00	2	R\$ 2.720.000,00
2	FC-10-F35F1-809-02-60 - FortiGate-3501F - Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) - 60 meses	R\$ 3.450.000,00	2	R\$ 6.900.000,00
3	FC4-10-0ACVM-248-02-60 - FortiAuthenticator-VM 24x7 FortiCare Contract (1 - 10100 USERS) - 60 meses	R\$ 148.000,00	1	R\$ 148.000,00
4	FC5-10-LV0VM-248-02-60 - FortiAnalyzer-VM - Support, 24x7 FortiCare Contract (for 1-101 GB/Day of Logs) - 60 meses	R\$ 146.000,00	1	R\$ 146.000,00
5	FC2-10-M3004-248-02-60 - FortiManager-VM - 24x7 FortiCare Contract (1 - 110 devices/Virtual Domains) - 60 meses	R\$ 100.000,00	1	R\$ 100.000,00
Valor Total				R\$ 10.014.000,00

O custo estimado foi de R\$ 10.014.000,00 (Dez milhões e quatorze mil reais) para 60 meses com a licença Enterprise, superior a UTP em uso no Senado Federal, como citado nesse documento. Fazendo as devidas conversões para estimar o custo e adequar a necessidade do Senado Federal (adicionado um pacote de 10 VDOMs e aumentando uma licença do FortiAuthenticator, para que o mesmo possua capacidade suficiente para integrar a solução de 802.1x do Senado), o valor resultante foi de R\$ 10.309.000,00 (Dez milhões, trezentos e nove mil reais).

Com esse valor para 60 Meses, foi possível estimar o custo anual, no valor de R\$ 2.061.800,00 (Dois milhões, sessenta e um mil e oitocentos reais).

Além de todos os ganhos citados com a aquisição da licença Enterprise, a substituição de todos os 6 equipamentos 3200D por 2 equipamentos 3500F trará, entre o principal upgrade de capacidade técnica, o aumento do throughput total de 300 Gbps para 840 Gbps. Segue tabela comparativa entre os principais indicadores do equipamento, explicitando todos os ganhos técnicos com a aquisição do Firewall 3500F.



FORTIGATE 3200D	
Interfaces and Modules	
10 GE SFP+ / GE SFP Slots	48
GE RJ45 Management Ports	2
USB Ports (Client / Server)	1 / 1
Console Port	1
Internal Storage	2x 480 GB SSD
Included Transceivers	2x SFP+ (SR 10G)
System Performance — Enterprise Traffic Mix	
IPS Throughput ²	26 Gbps
NGFW Throughput ^{2,4}	24 Gbps
Threat Protection Throughput ^{2,5}	15 Gbps
System Performance and Capacity	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 50 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 50 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	75 Mpps
Concurrent Sessions (TCP)	50 Million
New Sessions/Second (TCP)	400,000
Firewall Policies	200,000
IPsec VPN Throughput (512 byte) ¹	50 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40,000
Client-to-Gateway IPsec VPN Tunnels	200,000
SSL-VPN Throughput	8 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	17 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	11,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	3.5 Million
Application Control Throughput (HTTP 64K) ²	50 Gbps
CAPWAP Throughput (1444 byte, UDP)	22 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiSwitches Supported	256
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 2,048
Maximum Number of FortiTokens	20,000
High Availability Configurations	Active / Active, Active / Passive, Clustering

FG-3500F	
Firewall Throughput (1518/512/64 byte UDP)	595 / 590 / 420 Gbps
IPsec VPN Throughput (512 byte) ¹	165 Gbps
IPS Throughput (Enterprise Mix) ²	72 Gbps
NGFW Throughput (Enterprise Mix) ^{2,4}	65 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	63 Gbps
Firewall Latency	2.98 µs
Concurrent Sessions	140 Million / 348 Million ⁶
New Sessions/Sec	1 Million / 5 Million ⁶
Firewall Policies	200 000
Max G/W to G/W IPSEC Tunnels	40 000
Max Client to G/W IPSEC Tunnels	200 000
SSL VPN Throughput	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	63 Gbps
Application Control Throughput (HTTP 64K) ²	135 Gbps
Max FortiAPs (Total, Tunnel)	4 096 / 2 048
Max FortiSwitches	300
Max FortiTokens	20,000
Virtual Domains (Default/Max)	10 / 500
Interfaces	6x 100GE QSFP28/40GE QSFP+, 32x 25GE SFP28, 2x GE RJ45
Local Storage	4 TB (3501F)
Power Supplies	Dual PS
Form Factor	2 RU
Variants	—

Além dos ganhos técnicos citados, será economizado espaço nos racks dos Datacenters onde os Firewalls estão instalados, Passando de 6 Rack Units de ocupação, para 2 Rack Units em cada um dos Datacenters. Tal aquisição também proporciona um ganho de eficiência energética, visto que 6 Firewalls 3200D podem consumir até 3.588 Watts de potência, enquanto 2 Firewalls 3500F podem consumir até 2.348 Watts de potência.

Também foi comparado outra solução da Fortinet com o FG 3200D instalado no Prodasen, o FG-2600F, equipamento que possui capacidades de throughput maiores e recursos semelhantes, porém, como o FG 3200D foi lançado há 10 anos, proporcionalmente o equipamento 2600F é de uma linha ligeiramente inferior, além de possuir uma menor quantidade de portas (4x 100GE QSFP28/40GE QSFP+, 16x 25GE SFP28, 16x 10GE RJ45, 2x 10GESFP+ e 2x GE RJ45), visto que as 16 portas de 10 GE são RJ45, e a maioria dos servidores instalados no Datacenter possuem conexões SFP+, portanto, a grande maioria ou a totalidade dessas portas citadas não seriam utilizadas. Em comparação, o 3200D possui 18 portas SFP+. Devido a isso, mesmo com a tecnologia de VDOM, foram utilizados 6

firewalls 2600F, cenário compatível com o instalado no Senado Federal.

Também foi acrescentado uma licença do FortiAuthenticator, para que o mesmo possua capacidade suficiente para integrar a solução de 802.1x do Senado. Diante do exposto, o valor final foi de 11.423.200,00 (Onze milhões, quatrocentos e vinte três mil e duzentos reais).

FG-2600F - 60 MESES Enterprise						
Ordem	Nome	Valor Unitário		QTD	Valor Total	
1	Equipamento Fortigate -2601F	R\$	550.700,00	6	R\$	3.304.200,00
2	FC-10-02K5E-809-02 - FortiGate-2601F - Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) 60 meses	R\$	1.250.000,00	6	R\$	7.500.000,00
3	FC4-10-0ACVM-248-02 - FortiAuthenticator-VM 24x7 FortiCare Contract (1 - 10100 USERS) - 60 meses	R\$	173.000,00	2	R\$	346.000,00
4	FC5-10-LV0VM-248-02 - FortiAnalyzer-VM - Support, 24x7 FortiCare Contract (for 1-101 GB/Day of Logs) - 60 meses	R\$	173.000,00	1	R\$	173.000,00
5	FC2-10-M3004-248-02-60 - FortiManager-VM - 24x7 FortiCare Contract (1 - 110 devices/Virtual Domains) - 60 meses	R\$	100.000,00	1	R\$	100.000,00
Valor Total					R\$ 11.423.200	

Com esse valor para 60 Meses, foi possível estimar o custo anual, no valor de R\$ 2.284.640 (Dois milhões, duzentos e oitenta e quatro mil e seiscentos e quarenta reais).

Esse cenário possui um custo anual menor do que o apresentado na alternativa 1, além dos diversos ganhos expostos neste documento com a aquisição das licenças Enterprise.

Em relação a capacidade do equipamento, segue tabela comparativa explicitando todos os ganhos técnicos com a aquisição do Firewall 2600F em relação ao 3200D.



FORTIGATE 3200D	
Interfaces and Modules	
10 GE SFP+ / GE SFP Slots	48
GE RJ45 Management Ports	2
USB Ports (Client / Server)	1 / 1
Console Port	1
Internal Storage	2x 480 GB SSD
Included Transceivers	2x SFP+ (SR 10GE)
System Performance — Enterprise Traffic Mix	
IPS Throughput ²	26 Gbps
NGFW Throughput ^{2,4}	24 Gbps
Threat Protection Throughput ^{2,5}	15 Gbps
System Performance and Capacity	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 50 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 50 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	75 Mpps
Concurrent Sessions (TCP)	50 Million
New Sessions/Second (TCP)	400,000
Firewall Policies	200,000
IPsec VPN Throughput (512 byte) ¹	50 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40,000
Client-to-Gateway IPsec VPN Tunnels	200,000
SSL-VPN Throughput	8 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	17 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	11,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	3.5 Million
Application Control Throughput (HTTP 64K) ²	50 Gbps
CAPWAP Throughput (1444 byte, UDP)	22 Gbps
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiSwitches Supported	256
Maximum Number of FortiAPs (Total / Tunnel Mode)	4,096 / 2,048
Maximum Number of FortiTokens	20,000
High Availability Configurations	Active / Active, Active / Passive, Clustering

FG-2600F	
Firewall Throughput (1518/512/64 byte UDP)	198 / 196 / 140 Gbps
IPsec VPN Throughput (512 byte) ¹	55 Gbps
IPS Throughput (Enterprise Mix) ²	31 Gbps
NGFW Throughput (Enterprise Mix) ^{2,4}	27 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	25 Gbps
Firewall Latency	3.41 µs
Concurrent Sessions	24 Million / 40 Million ⁶
New Sessions/Sec	1 Million / 2 Million ⁶
Firewall Policies	100 000
Max G/W to G/W IPSEC Tunnels	20 000
Max Client to G/W IPSEC Tunnels	100 000
SSL VPN Throughput	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	20 Gbps
Application Control Throughput (HTTP 64K) ²	64 Gbps
Max FortiAPs (Total, Tunnel)	4 096 / 2 048
Max FortiSwitches	196
Max FortiTokens	20 000
Virtual Domains (Default/Max)	10 / 500
Interfaces	4x 100GE QSFP28/40GE QSFP+, 16x 25GE SFP28, 16x 10GE RJ45, 2x 10GE SFP+, 2x GE RJ45
Local Storage	2 TB (2601F)
Power Supplies	Dual PS
Form Factor	2 RU
Variants	DC

Diante do exposto, a comparação técnica e econômica dos cenários possíveis se restringirá entre o 2600F e o 3500F. Do ponto de vista econômico a aquisição do firewall 3500F apresenta um menor valor quando comparado com o 2600F. Já na parte técnica, o throughput de 6 equipamentos 2600F é idêntico ao de 2 equipamentos 3500F (840 Gbps para pacotes de 64 bytes), bem como os demais requisitos e capacidades técnicas, como o throughput, são semelhantes ou iguais, quando se compara 6 Firewalls 2600F com 2 Firewalls 3500F. Segue principais indicadores técnicos de cada equipamento:

FG-2600F		FG-3500F	
Firewall Throughput (1518/512/64 byte UDP)	198 / 196 / 140 Gbps	Firewall Throughput (1518/512/64 byte UDP)	595 / 590 / 420 Gbps
IPsec VPN Throughput (512 byte) ¹	55 Gbps	IPsec VPN Throughput (512 byte) ¹	165 Gbps
IPS Throughput (Enterprise Mix) ²	31 Gbps	IPS Throughput (Enterprise Mix) ²	72 Gbps
NGFW Throughput (Enterprise Mix) ^{3,4}	27 Gbps	NGFW Throughput (Enterprise Mix) ^{3,4}	65 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	25 Gbps	Threat Protection Throughput (Ent. Mix) ^{2,5}	63 Gbps
Firewall Latency	3.41 µs	Firewall Latency	2.98 µs
Concurrent Sessions	24 Million / 40 Million ⁶	Concurrent Sessions	140 Million / 348 Million ⁶
New Sessions/Sec	1 Million / 2 Million ⁶	New Sessions/Sec	1 Million / 5 Million ⁶
Firewall Policies	100 000	Firewall Policies	200 000
Max G/W to G/W IPSEC Tunnels	20 000	Max G/W to G/W IPSEC Tunnels	40 000
Max Client to G/W IPSEC Tunnels	100 000	Max Client to G/W IPSEC Tunnels	200 000
SSL VPN Throughput	16 Gbps	SSL VPN Throughput	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30 000	Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	20 Gbps	SSL Inspection Throughput (IPS, avg. HTTPS) ³	63 Gbps
Application Control Throughput (HTTP 64K) ²	64 Gbps	Application Control Throughput (HTTP 64K) ²	135 Gbps
Max FortiAPs (Total, Tunnel)	4 096 / 2 048	Max FortiAPs (Total, Tunnel)	4 096 / 2 048
Max FortiSwitches	196	Max FortiSwitches	300
Max FortiTokens	20 000	Max FortiTokens	20,000
Virtual Domains (Default/Max)	10 / 500	Virtual Domains (Default/Max)	10 / 500
Interfaces	4x 100GE QSFP28/40GE QSFP+, 16x 25GE SFP28, 16x 10GE RJ45, 2x 10GE SFP+, 2x GE RJ45	Interfaces	6x 100GE QSFP28/40GE QSFP+, 32x 25GE SFP28, 2x GE RJ45
Local Storage	2 TB (2601F)	Local Storage	4 TB (3501F)
Power Supplies	Dual PS	Power Supplies	Dual PS
Form Factor	2 RU	Form Factor	2 RU
Variants	DC	Variants	—

Porém, além de ser mais vantajoso do ponto de vista financeiro, com a aquisição do 3500F será economizado espaço nos racks dos Datacenters onde os Firewalls estão instalados, Passando de 6 Rack Units de ocupação, para 2 Rack Units em cada um dos Datacenters. Tal aquisição também proporciona um ganho de eficiência energética, visto que 6 Firewalls 2600F podem consumir até 3.096 Watts de potência, enquanto 2 Firewalls 3500F podem consumir até 2.348 Watts de potência.

Salienta-se que, em todos os cenários apresentados, a alternativa 2 (com a aquisição do Firewall 3500F) foi a que apresentou o menor custo estimado. Ressalta-se também que na alternativa 1, o equipamento estará no fim do seu ciclo de vida e sem possuir os diversos recursos proporcionados pela atualização tecnológica.

Por fim, cabe informar que o Senado Federal possui 2 roteadores de borda em sua topologia, responsável por fechar sessões BGP e toda parte de comunicação com as operadoras e roteamento externo ao Senado. Ambos são providos pelo contrato 22/2019. Devido ao fim do ciclo de vida dos equipamentos, foi realizado o Pregão eletrônico 90044/2025, com o valor



estimado de R\$ 750.310,61 (setecentos e cinquenta mil, trezentos e dez reais e sessenta e um centavos), visando a aquisição de 3 roteadores, adicionando um no CETEC-NORTE. A licitação restou fracassada, pois a única empresa parceira do fabricante do equipamento informou que não conseguiria chegar no preço balizado. Com isso, está sendo realizada nova pesquisa de preços, para que mais licitantes possam concorrer e o preço esteja mais adequado ao mercado. Até o momento, recebemos 2 propostas, fornecendo equipamentos Huawei e Cisco (2 líderes no segmento). Seguem valores:

Huawei:

Nome da empresa: One Linea Telecom LTDA (Nome Fantasia: OL Tecnologia)
CNPJ: 04.318.562.0001/39
Endereço: Av. Angelica 2447 – conj 43, 44 e 153 – São Paulo - SP
CEP: 01227-200
Telefone: (011) 3138-1470
E-mail: psergio@ol-tecnologia.com.br

Item	Unidade	Quant.	Especificação	Preço Unitário (R\$)	Preço Total (R\$)
I	Solução	1	Solução de alta disponibilidade de roteamento de borda	R\$ 2.005.691,78	R\$ 2.005.691,78
II	Serviço	1	Serviços de instalação da Solução	R\$ 75.620,00	R\$ 75.620,00
III	Serviço	1	Serviços de Treinamento da Solução	R\$ 95.520,00	R\$ 95.520,00
IV	Mês	60	Serviços de Garantia e Suporte de funcionamento	R\$ 3.820,00	R\$ 229.200,00
VALOR TOTAL					R\$ 2.406.031,78



Cisco:

IDENTIFICAÇÃO DO FORNECEDOR	
RAZÃO SOCIAL	TELTEC SOLUTIONS LTDA.
CNPJ	04.892.991/0001-15
INSCRIÇÃO ESTADUAL	254.353.290 (SC)
REPRESENTANTE LEGAL	Alexandre Matos da Silva Pires de Moraes
CPF	665.072.861-68
RG	1467233 SSP/DF
ENDEREÇO	Rua Miguel Daux, 100 – Coqueiros – Florianópolis-SC CEP: 88.080-220
PESSOA PARA CONTATO	Marcos Wellington Mariano Rocha
TELEFONE DE CONTATO	(61) 3771-5950 / (48) 3031-3450 / (61) 99819-1366
E-MAIL DE CONTATO	brasil@teltecsolutions.com.br / teltec@teltecsolutions.com.br marcos.rocha@teltecsolutions.com.br

Item	Descrição	Qtd	Valor Unitário (R\$)	Valor Total (R\$)
1	Roteador Cisco C8500-20X6C (3 unidades)	1	2.026.810,00	2.026.810,00
2	Serviço de Instalação da Solução	1	160.380,00	160.380,00
3	Serviço de Treinamento na Solução	1	54.950,00	54.950,00
4	Serviço de Garantia e Suporte de funcionamento da Solução	60	15.500,00	930.000,00

TOTAL	R\$ 3.172.140,00
	TRÊS MILHÕES E CENTO E SETENTA E DOIS MIL E CENTO E QUARENTA REAIS

Fazendo a média dos 2 valores, o valor final é de R\$ 2.789.085,89 (dois milhões, setecentos e oitenta e nove mil, oitenta e cinco reais e oitenta e nove centavos).

Diante do exposto, salienta-se que com a aquisição dos 2 Firewalls 3500F, como citado, os recursos de segurança e conectividade irão aumentar, bem como o throughput do Firewall irá mais que dobrar em relação a solução atual. Com isso, a função de conectividade com as operadoras, fechamento de BGP e demais funções de roteamento no geral poderão ser realizadas pelo firewall, proporcionando uma economia ao Senado Federal, tanto do ponto de vista econômico, já que não será necessário adquirir novos roteadores, como do ponto de vista técnico e de gestão processual, proporcionando menos contratos para serem fiscalizados e unificando as plataformas de segurança e conectividade, permitindo que a equipe já treinada na solução Fortinet possa operar com eficiência as funções de roteamento e segurança. Com o pregão ocorrendo para aquisição dos roteadores, além do custo econômico e de gestão, outro fabricante de roteadores (atualmente a solução em uso no Senado é Huawei) poderia ganhar a licitação, exigindo extenso treinamento para que a equipe técnica possua os conhecimentos necessários para operá-los, configurá-los e dar o devido suporte técnico.

Diante do exposto, o SESIER recomenda que a Administração opte pela alternativa 2 – aquisição do Firewall 3500F, por intermédio de processo licitatório, para a aquisição de

serviços de garantia de funcionamento na modalidade Enterprise 24x7 Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium) – durante o prazo de 60 meses.

Alternativa 3

Fornecimento de nova solução (equipamentos) com garantia de 60 (sessenta) meses.

Como já citado ao longo do documento, do ponto de vista técnico, tal alternativa traz diversos riscos e complexidades que não serão enfrentados na alternativa 2.

Já economicamente falando, em relação a custos, os preços praticados presentes na alternativa acima demonstram que as propostas enviadas, que como citado, estão compatíveis com os valores praticados no mercado e, portanto, a aquisição de nova solução de Next Generation Firewall com garantia durante 60 (sessenta) meses, com a manutenção da solução atual durante o período de migração é também viável e vantajosa do ponto de vista financeiro.

Para corroborar tal informação, seguem preços públicos, que atestam tal vantajosidade e adequação:

CLDF - Pregão Eletrônico N° 24/2023

Em relação ao pregão informado, a CLDF realizou um projeto de troca de firewall semelhante ao que trata este documento, realizando uma manutenção dos firewalls Fortinet e licenças em produção na casa e posteriormente fazendo o upgrade da solução para novos firewall também da Fortinet, fazendo uma licitação restrita aos parceiros da empresa.

Na ocasião, a vencedora foi a mesma empresa signatária do contrato 21/2021 do Prodasen (NCT Informática LTDA), realizando a manutenção do firewall FortiGate-500E com a licença UTM (inferior a Enterprise e a UTP, como citado ao longo do documento) e posterior substituição para o firewall Fortigate-1000F UTP (inferior a licença Enterprise). Seguem valores e descrição abaixo:

ITEM	UNID.	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO CONSIDERADO PARA 36 MESES (R\$)	VALOR TOTAL CONSIDERADO PARA 36 MESES (R\$)
1	Unidade	Licenciamento e atualização, com possibilidade de evolução, de 2 (dois) equipamentos FortiGate-500E FC-10-0500E-900-02-60 Unified Threat Management - UTM 8x5 FortiCare plus Application Control, IPS, AV, BotnetIP / Domain, Web Filtering and Antispam Services, contemplando suporte do fabricante e garantia da solução pelo prazo 36 (trinta e seis) meses	2	R\$ 805.000,00	R\$ 1.610.000,00



1.1. A proposta contempla:

- 1.1.1. Para o item 1, em atendimento ao item 1.1.2, FortiGate-1000F (2x FG-1000F) com licenciamento Unified Threat Protection UTP IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium (2x FC-10-F1K0F-950-02) para 36 meses com 02 cabos DAC de 100 GE QSFP28 (4x FN-CABLE-QSFP28-3) por equipamento;

Segue comparação dos requisitos técnicos entre o Firewall 1000F e o 3500F citado na alternativa 2:

FG-1000F		FG-3500F	
Firewall Throughput (1518/512/64 byte UDP)	198 / 196 / 134 Gbps	Firewall Throughput (1518/512/64 byte UDP)	595 / 590 / 420 Gbps
IPsec VPN Throughput (512 byte) ¹	55 Gbps	IPsec VPN Throughput (512 byte) ¹	165 Gbps
IPS Throughput (Enterprise Mix) ²	19 Gbps	IPS Throughput (Enterprise Mix) ²	72 Gbps
NGFW Throughput (Enterprise Mix) ^{3,4}	15 Gbps	NGFW Throughput (Enterprise Mix) ^{3,4}	65 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	13 Gbps	Threat Protection Throughput (Ent. Mix) ^{2,5}	63 Gbps
Firewall Latency	3.45 µs	Firewall Latency	2.98 µs
Concurrent Sessions	7.5 Million	Concurrent Sessions	140 Million / 348 Million ⁶
New Sessions/Sec	650 000	New Sessions/Sec	1 Million / 5 Million ⁶
Firewall Policies	100 000	Firewall Policies	200 000
Max G/W to G/W IPSEC Tunnels	20 000	Max G/W to G/W IPSEC Tunnels	40 000
Max Client to G/W IPSEC Tunnels	100 000	Max Client to G/W IPSEC Tunnels	200 000
SSL VPN Throughput	5.3 Gbps	SSL VPN Throughput	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10 000	Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	10 Gbps	SSL Inspection Throughput (IPS, avg. HTTPS) ³	63 Gbps
Application Control Throughput (HTTP 64K) ²	44 Gbps	Application Control Throughput (HTTP 64K) ²	135 Gbps
Max FortiAPs (Total, Tunnel)	4 096 / 2 048	Max FortiAPs (Total, Tunnel)	4 096 / 2 048
Max FortiSwitches	196	Max FortiSwitches	300
Max FortiTokens	20 000	Max FortiTokens	20,000
Virtual Domains (Default/Max)	10 / 250	Virtual Domains (Default/Max)	10 / 500
Interfaces	2x 100 GE QSFP28, 8x 25 GE SFP28, 16x10 GE SFP+, 8x 10GE RJ45, 1x 2.5GE RJ45, 1 GE RJ45	Interfaces	6x 100GE QSFP28/40GE QSFP+, 32x 25GE SFP28, 2x GE RJ45
Local Storage	960 GB (1001F)	Local Storage	4 TB (3501F)
Power Supplies	Dual PS	Power Supplies	Dual PS
Form Factor	2 RU	Form Factor	2 RU
Variants	—	Variants	—

Para que as soluções sejam semelhantes em termos de capacidade técnica, visto que está sendo proposta a aquisição de 2 firewalls 3500F, será necessário utilizar 8 Firewalls 1000F, visto que, apesar do throughput maior com 8 caixas 1000F, outros throughputs específicos como Threat Protection Throughput, NGFW, SSL Inspection Throughput e Local Storage ficariam inferiores, além de ser um equipamento inferior ao 2600F, em que foram utilizados 6 equipamentos para fins de comparação na alternativa 2.

Diante do exposto, o valor R\$ 1.610.000,00 (um milhão, seiscentos e dez mil reais) será multiplicado por 4, já que ele é equivalente a 2 firewalls e posteriormente majorado para 60 meses, de forma a se adequar os tempos de contrato.

Dessa forma, o valor ficará em: R\$ 10.733.333,33 (dez milhões, setecentos e trinta e três mil, rezentos e trinta e três reais e trinta três centavos). Comparando o valor dos 2 Firewalls 3500F com as licenças Enterprise informados na proposta da NCT, o valor será de 9.620.000



(Nove milhões, seiscentos e vinte mil), portanto, ainda inferior quando se compara com um preço público que do pregão 24/2023. Salienta-se que é uma prática de mercado que os preços de pregões sejam menores do que os praticados em propostas, devido a competitividade do certame, e acrescenta-se o fato que a licença do equipamento da proposta do pregão é inferior à Enterprise presente na proposta recebida pelo Prodasen. Portanto, tal valor tem o teor de corroborar a informação não só da vantajosidade técnica, mas também econômica da aquisição citada na alternativa 2.

Banco do Nordeste – Pregão Eletrônico 90088/2024

Pregão realizado pelo Banco do Nordeste, restrito a parceiros do fabricante Palo Alto (solução de firewall implantada no banco), que corrobora também a informação que é um padrão de mercado, no caso de firewall, devido a criticidade, padronização e as diversas justificativas já citadas nesse documento, que os órgãos contratem fabricantes que já estejam em produção e atendem com eficiência suas necessidades. Segue item 4 do edital do banco do nordeste:

4. JUSTIFICATIVA DA CONTRATAÇÃO

O Banco do Nordeste do Brasil, visando a continuidade de serviços de segurança e observando a necessidade de garantir a disponibilidade, integridade, confidencialidade e segurança das informações e dos serviços providos pelo banco a seus clientes e ao negócio, pretende renovar o licenciamento e serviços de suporte (fornecedor e fabricante) da solução de defesa provida pelo Next Generation Firewall (NGFW) da fabricante Palo Alto, existente no parque computacional e tecnológico da Instituição.

Para intuito de consulta e comprovação dessa prática, bem como as suas vantagens já citadas nesse documento, seguem mais 2 pregões de Firewall licitados com um fabricante específico:

PE - Nº 90001/2025 – Ministérios das Relações Exteriores - Fortinet

PE - Nº017/2023 – TCE GO – Fortinet

Diante do exposto, foram adjudicadas licenças e garantias para 4 (quatro) equipamentos PA 5220, 1 appliance M200 além dos serviços de suporte e garantia. Esses itens compõem a solução de segurança do banco do nordeste fornecida pela Palo Alto. A solução foi adjudicada no valor de R\$ 3.237.896,33 (três milhões, duzentos e trinta e sete mil, oitocentos e noventa e seis reais e trinta e três centavos), para 18 meses.

11.061153/0001-65

Adjudicada

TRUST CONTROL - SE...

CE

Valor ofertado (unitário)

R\$ 5.000.000,0000

Valor negociado (unitário)

R\$ 3.237.896,3300

Majorando esse valor para 60 meses, o valor será proporcionalmente de R\$ 11.792.987,76 (onze milhões, noventa e dois mil, novecentos e oitenta e sete reais e setenta e seis centavos), acima do valor oferecido pela proposta da NCT informática ao Prodasen no equipamento 3500F. Salienta-se também que, quatro equipamentos 5220 da palo alto não são equivalentes 2 equipamentos 3500F, em que algumas taxas de throughput com 2 firewalls 3500F instalados são maiores que 8 equipamentos 5220, como a proposta contém o valor para 4

equipamentos, com 8 essa diferença econômica será ainda maior. Segue comparação das principais taxas de cada um:

PAN-PA-5220 Specification	
Model	PA-5220
Performance and Capacities Specifications	
Firewall throughput (App-ID enabled)	18.5 Gbps
Threat prevention throughput	9.2 Gbps
IPsec VPN throughput	5 Gbps
Max sessions	4,000,000
New sessions per second	169,000
Virtual systems (base/max)	10/20

FG-3500F	
Firewall Throughput (1518/512/64 byte UDP)	595 / 590 / 420 Gbps
IPsec VPN Throughput (512 byte) ¹	165 Gbps
IPS Throughput (Enterprise Mix) ²	72 Gbps
NGFW Throughput (Enterprise Mix) ^{3,4}	65 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	63 Gbps

Diante do exposto, tal informação corrobora a informação indicada pelo órgão técnico, que a alternativa 2 está adequada ao preço de mercado e também apresenta diversos ganhos técnicos.

Detran DF – Pregão Eletrônico 9004/2024

Licitação aberta para contratação de firewall next generation, aberto a todos os fabricantes do mercado, durante 36 meses. Nesse pregão, a vencedora foi a Fortinet, através da empresa BLUE EYE SOLUÇÕES DE TEMCNOLOGIA LTDA, com o Firewall, assim como na licitação da CLDF aqui presente, o 1000F.

Portanto, como já há a justificativa e comparação dos requisitos naquele cenário, será comparado apenas o preço.

Grupo	item	Descrição do Item	Métrica	Quantidade	Valor Unitário	Valor Anual
1	1	Solução de proteção de rede do tipo Next Generation Firewall (NGFW) - Appliance	Unidade	2	R\$ 1.778.990,00	R\$ 3.557.980,00
	2	Serviço de Suporte Especializado para Instalação, Migração e Suportes corretivo e preventivo da solução.	Meses	36	R\$ 16.050,00	R\$ 577.800,00
Total						R\$ 4.135.780,00



26.025.401/0001-9...	BLUE EYE SOLUCOES ...	Valor ofertado (total)	R\$ 4.135.780,0000	▼
Adjudicada	DF	Valor negociado (total)	-	

Fazendo a conversão pra 8 equipamentos e majorando o valor para 60 meses, o valor será de R\$ 13.785.933,33 (treze milhões, setecentos e oitenta e cinco mil e novecentos e trinta e três reais e trinta e três centavos). Portanto também acima do valor proposto pela NCT ao Prodasen e mais uma vez corroborando a adequação econômica da solução proposta pelo órgão técnico.

Ministério da Justiça e Segurança Pública - Pregão Eletrônico N° 90007/2024

Licitação aberta a todos os fabricantes, assim como ocorreu com a do Detran-DF na ocasião, a licitante vencedora apresentou o seguinte equipamento: CISCO Firepower 4115 NGFW, equipamento de linha e capacidade bastante inferior ao 3500F. O preço para 60 meses, de 2 equipamentos, ficou estabelecido em R\$ 3.093.000,00 (três milhões e noventa e três mil)

Item	Descrição do item	Unidade de Medida	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
1	<p>Aquisição de equipamentos de Firewalls de Próxima Geração – NGFW com proteção DNS, com suporte técnico, garantia e licenciamento por 60 meses. (CISCO Firepower 4115 NGFW - Licença TMC + CISCO Umbrella DNS Security para 600 Usuários).</p> <p>MARCA: CISCO</p> <p>MODELO: Firepower 4115 NGFW</p> <p>Cisco FirePower 8 port SFP+ Network Module FAST TRACK__10GBASE-SR SFP Module</p> <p>Cisco FirePower 8 port SFP+ Network Module FAST TRACK__10GBASE-SR SFP Module</p> <p>Licenças: Umbrella DNS Security Essentials Cisco AnyConnect Plus ISE Passive Identity Connector</p> <p>PART NUMBER: FPR4115-NGFW-K9_C3 L-FPR4115T-TMC-5Y FPR4K-PWR-AC-1100_C3 SFP-10G-SR_C3 FPR4K-NM-8X10G_C3 SFP-10G-SR_C3 UMB-DNS-ESS-K9_500-999_5Y</p>	Unidade	2	R\$ 1.546.500	R\$ 3.093.000,00

Segue capacidade de throughput do equipamento:

Features4115

Throughput: FW +33 Gbps

AVC (1024B)

Throughput: FW +33 Gbps

AVC + IPS (1024B)



Se comparado com o 3500F, o throughput é cerca de 12 a 15 vezes menor que o citado na alternativa 2, portanto, o valor, quando convertendo para capacidades semelhantes, ficará superior a dezoito milhões, bem acima da proposta recebida pelo Prodasen ao 3500F.

12. Descrição da solução de TIC a ser contratada

Contratação de empresa especializada para o fornecimento de solução de alta disponibilidade de Next Generation Firewall, incluindo os serviços de assistência técnica com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local e remoto, por 60 (sessenta) meses.

13. Estimativa de custo total da contratação

Valor (R\$): 11.000.000,00 (onze milhões)

Custo estimado conforme proposta da NCT Informática, signatária do contrato 21/2021(10.309.000,00). Porém, foi crescendo o valor de R\$ 693.000,00 (seiscentos e noventa e três mil) , devido a variação de preços e de dólar inerentes ao mercado, bem como relativo ao custo dos transceivers, que serão necessários adquirir juntamente com a solução.



14. Justificativa técnica da escolha da solução

É necessário fazer algumas ponderações sobre as necessidades do Senado Federal em virtude da criticidade dos equipamentos a serem mantidos (equipamento de segurança com funcionalidades de firewall e IPS além de equipamentos que mantêm a infraestrutura de VPN usada para acesso remoto ao parque computacional do Senado Federal para funções de teletrabalho). Considerando que os equipamentos apresentam fontes de alimentação redundantes, estão configurados em modo cluster de alta disponibilidade (equipamentos redundantes entre si), e possuem múltiplas interfaces de rede disponíveis, é improvável que uma falha venha a tornar indisponível um dos serviços prestados pelos mesmos. Portanto, o SESIER indica como adequada a reposição de peças defeituosas no próximo dia útil à abertura do chamado.

Sendo assim, os níveis de serviço OnSITE com reposição de peças defeituosas no “dia útil seguinte” deve ser o adotado para esta contratação. Diante do exposto além dos diversos recursos informados neste documento, o SESIER recomenda a contratação do pacote, Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium).

Como informado ao longo do documento, esse é o modelo que proporcionará um upgrade em relação a licença UTP atualmente em uso no Senado Federal, podendo, portanto, usufruir dos diversos recursos proporcionados pela licença Enterprise, ao qual não estão disponíveis atualmente na solução. Ademais, o Firewall 3500F possui seus requisitos de software e hardware, como throughput, memória, armazenamento bastante superiores ao 3200D que está em operação, além de proporcionar ganho de energia e espaço físico no datacenter. Além disso, em relação ao contrato 21/2021, será realizada a adoção de mais licenças do FortiAuthenticator, para que o mesmo possa ser utilizado na implementação da solução de 802.1x. Portanto, a aquisição do firewall 3500F não só manterá, como ampliará todos os recursos de software e hardware do Firewall utilizado no Senado Federal.

15. Justificativa econômica da escolha da solução

Como exposto no capítulo 11 desse estudo (Análise comparativa de custos - TCO), a alternativa 2 - Aquisição de nova solução de Next Generation Firewall com garantia durante 60 (sessenta) meses, com a manutenção da solução atual durante o período de migração é a que apresenta o menor custo anual. Portanto, tal alternativa permitirá que os equipamentos que proveem a solução de NGFW sejam renovados e estando em consonância com um melhor custo benefício ao longo do tempo. Segue planilha com o consolidado comparando o preço das alternativas (as que não contemplam equipamentos Fortinet não estão com o custo do treinamento incluso, o que irá aumentar o valor):



Alternativa 1		Alternativa 2		Alternativa 3	
Firewall (60 Meses)	Valor Anual	Firewall (60 Meses)	Valor Anual	Firewall (60 Meses)	Valor Anual
6x Fortinet 3200D	R\$2.390.250,00	2x Fortinet 3501F	R\$ 2.061.800,00	CLDF – Fortinet 8x1000F	R\$ 2.146.666,6
				Banco do Nordeste – Palo Alto 4xPA5220	R\$ 2.358.597,55
				Detran – DF – Fortinet 8x1000F	R\$ 2.757.186,6
				MJ – 12x Cisco 4115	R\$ 3.711.600

16. Benefícios a serem alcançados com a contratação

Manter e ampliar os padrões disponibilidade e desempenho atualmente em uso no Senado Federal para a comunicação de dados de sua Rede Local, com foco no serviço de alta disponibilidade de segurança da rede.



17. Providências a serem Adotadas

Não há necessidade de adequação da infraestrutura tecnológica, elétrica, espaço físico, mobiliário ou outras que se apliquem, visto que trata-se de solução já vigente e que ainda proporcionará uma economia de espaço físico e de uso energético.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pela COINTI/SESIER, considerando a análise das alternativas, o alinhamento estratégico e os potenciais benefícios, conclui pela VIABILIDADE DA CONTRATAÇÃO. Complementarmente, cabe ressaltar que os requisitos listados atendem adequadamente à demanda e o custo estimado é compatível com o mercado.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

CARLOS ALEXANDRE TAVARES LEITE

Coordenador da COINTI

GLEISON CARNEIRO GOMES

Diretor do PRODASEN



ROBERTO DE OLIVEIRA SILVA

Chefe do SESIER

RODRIGO SAVIO LEIROS BORGES

Analista de Tecnologia da Informação

CLAUDIO FERREIRA DA SILVA

Analista de Tecnologia da Informação

