CIASC
CENTRO DE INFORMÁTICA
E AUTOMAÇÃO DO ESTADO DE SANTA CATARINA S.A.

ANEXO III: TERMO DE REFERÊNCIA

1 - OBJETO

Atualização do cluster de NEXT GENERATION FIREWALL (NGFW) para provimento de Internet e Data Center com capacidade de tráfego ampliada, renovação de suporte técnico e garantia das soluções de Segurança.

2 - JUSTIFICATIVA

O CIASC, como provedor de acesso à Internet da Rede de Governo de Santa Catarina e Data Center, preocupa-se em aprimorar a segurança de seus sistemas e serviços prestados ao público catarinense.

Os canais de saída da Rede de Governo para a Internet são protegidos por diversos serviços de segurança, que tornam possível a filtragem de conteúdo dos acessos internos que se dirigem à Internet, e a proteção a acessos externos indevidos com destino às redes de Data Center.

Porém, os equipamentos adquiridos em 2021, atualmente em uso, estão com as licenças de webfilter, IPS e Antivírus de Rede, com cobertura de suporte e garantia de hardware acabando em junho de 2026.

Com a renovação e ampliação, será possível dar a continuidade das funcionalidades que os equipamentos de NEXT GENERATION FIREWALL (NGFW), atualizações de software e garantia de hardware, além de ampliar a capacidade da solução de filtragem. Consequentemente haverá uma maior segurança no ambiente de Data Center e Provimento de Internet, inerente ao aumento natural do consumo de internet ao longo do tempo.

3 - ESPECIFICAÇÕES TÉCNICAS

Este projeto conta com a aquisição em LOTE ÚNICO de:

- 02 (dois) Appliances de segurança NEXT GENERATION FIREWALL (NGFW) para Data Center e Provimento de Internet com 30 VDOMs com licenças de software UTP, atualizações, suporte e garantia por 60 (sessenta) meses para software e hardware;
- Renovação de licenças da solução FortiAnalyzer VM64 (Número de série: FAZ-VMTM21009781), atualizações, suporte e garantia por 60 (sessenta) meses;

Licenciamento e suporte técnico 60 meses

Item	Descrição	Quantidade (unidades)
1	FORTINET Next Generation Firewall (NGFW) - Appliance de Segurança para Data Center e Provimento de Internet (Hardware)	02
2	Licenciamento FORTINET para suporte a 30 VDOMs. licenciamento UTP, suporte e garantia de 60 (sessenta) meses.	02
3	Renovação de licenças da solução FortiAnalyzer VM64 (FAZ-VMTM21009781) , atualizações, suporte e garantia por 60 (sessenta) meses.	01

3.1. Requisitos Mínimos da Solução de Firewall Next Generation

Os equipamentos a serem fornecidos deverão ser do tipo Next Generation Firewall (NGFW) Appliance e atender ou superar os requisitos de desempenho e funcionalidades abaixo, baseados nas especificações mínimas abaixo:

3.2. Requisitos de Performance (Mínimo Aceitável)

Característica	Mínimo Exigido
Firewall Throughput (Pacotes de 64 byte)	178.5 Gbps
IPS Throughput (Enterprise Mix)	63 Gbps
NGFW Throughput	47 Gbps
Threat Protection Throughput	45 Gbps
Concurrent Sessions (TCP)	70 Milhões
New Sessions/Sec (TCP)	800.000

IPsec VPN Throughput (512 byte)	105 Gbps
SSL Inspection Throughput	29 Gbps
Virtual Domains (V-DOMs/Contextos)	Licenciado para, no mínimo, 30 V-DOMs/Contextos

3.3. Requisitos de Hardware e Portas

- Form Factor: Rack Mount, preferencialmente 2U.
- Redundância: Fontes de alimentação redundantes e hot-swappable (1+1).
- Alta Disponibilidade (HA): Suportar configurações de HA nos modos Active-Active e/ou Active-Passive/Clustering.
- O equipamento deverá possuir uma arquitetura de alta densidade de portas e suportar os seguintes tipos e quantidades de interfaces físicas, ou um equivalente que atenda à mesma densidade e velocidade:

Tipo de Interface	Mínimo Exigido	Observações
Interfaces de Ultra-Alta Velocidade	**4 portas** (Mínimo)	Deverão suportar módulos ópticos (Transceivers) nos padrões **100 GE QSFP28 e/ou 40 GE QSFP+**. Crucial para *backbone* e *datacenter* de alta capacidade.
Interfaces de Alta Velocidade (SFP/SFP+)	**4 portas** (Mínimo)	Deverão suportar velocidades de **10 GE SFP+** para flexibilidade de conexão com *switches* de distribuição.
Interfaces HA Dedicadas	**2 portas** (Mínimo)	Interfaces dedicadas para o funcionamento de Alta Disponibilidade (HA), suportando velocidades de **10 GE SFP+**.

Interfaces de Gerenciamento RJ45	**1 porta** (Mínimo)	Portas de cobre (RJ45) dedicadas para gerência fora da banda (*out-of-band management*), suportando **1 GE / GE**.

3.4. Outros Requisitos de Hardware

- **Suporte de Módulos (Transceivers):** A proposta deve incluir a quantidade necessária de módulos Transceivers (SFP+, SFP28, QSFP28, etc.) para conectar o equipamento à rede existente da Contratante. São necessários **por equipamento entregue**: 4 QSFP 100G BASE-SR4 com os respectivos cordões MTP tipo B (para conexões diretas entre equipamentos) de no mínimo 3 metros, 2 transceivers 10G BASE-SR para as conexões de HA.
- **Aceleração de Hardware:** O equipamento deve possuir processadores de rede (*Network Processors*) e/ou de conteúdo (*Content Processors*) dedicados para garantir o desempenho das funções de segurança (Firewall, IPS, NGFW, etc.) e alta taxa de transferência (throughput) sem degradação.
- **IPv4 e IPv6:** As interfaces e o sistema operacional devem suportar roteamento e filtragem de tráfego (Firewall Stateful) para os protocolos **IPv4 e IPv6 simultaneamente** (Dual Stack) em todas as portas.

3.5. Requisitos de Funcionalidades NGFW (Mínimas)

- **Firewall Stateful e Next Generation:** Inspeção de pacotes em todos os níveis (L2 a L7), controle de acesso por usuários, grupos e autenticação (LDAP, AD, RADIUS).
- **Application Control:** Capacidade de identificação e controle de milhares de aplicações (incluindo redes sociais, streaming, VPNs e proxies) independente da porta ou protocolo.
- **Intrusion Prevention System (IPS/IDS):** Prevenção e detecção de intrusões com atualizações automáticas de assinaturas de ameaças (incluindo vulnerabilidades críticas).
- **Anti-Vírus/Anti-Malware:** Inspeção de tráfego (web, e-mail, arquivos) em tempo real para detecção e bloqueio de vírus e *malware*.
- **Web Filtering / Filtro de Conteúdo:** Filtragem de URL e categorização de conteúdo web com milhões de URLs e centenas de categorias.
- **SSL Inspection (Descriptografia/Inspeção/Recriptografia):** Capacidade de inspecionar tráfego criptografado (HTTPS, SMTPS, etc.) em alta performance.
- **Virtual Private Network (VPN):** Suporte a VPN IPsec (Gateway-to-Gateway e Client-to-Gateway) com suporte a múltiplos clientes simultâneos.
- **Secure SD-WAN Integrado:** O equipamento deve possuir funcionalidades nativas de SD-WAN, integradas ao *firmware* do firewall, permitindo:
    - **Monitoramento da Qualidade do Link (SLA):** Capacidade de monitorar métricas de qualidade (latência, *jitter* e perda de pacotes) de múltiplos links WAN simultaneamente.
    - **Seleção Dinâmica de Caminho:** Roteamento de tráfego (steering) baseado no desempenho do link e em políticas de Application Control (tráfego crítico deve ter prioridade sobre tráfego não essencial).
    - **Otimização e Aceleração de WAN:** Recursos para otimizar o uso da largura de banda e acelerar o tráfego de aplicações, especialmente para conexões com serviços

em nuvem (SaaS) ou datacenters remotos.
    - **Alta Disponibilidade de Link:** Capacidade de failover automático e balanceamento de carga entre diferentes links WAN (MPLS, Internet banda larga, 4G/5G, etc.).
- **Suporte a Protocolos de Roteamento:** Suporte aos principais protocolos de roteamento dinâmico (OSPF, BGP) e estático, incluindo funcionalidades de BGP complexas, necessárias em ambientes de *datacenter* e provedores.
- **Virtualização (V-DOMs/Contextos Lógicos):** Capacidade de operar múltiplos firewalls lógicos isolados (V-DOMs ou Contextos) dentro do mesmo *hardware*, conforme o mínimo estipulado.

3.6. Licenças, Garantia e Suporte

- **Licenciamento:** A solução deverá ser fornecida com licenças de segurança unificadas (UTP ou similar, cobrindo todas as funcionalidades listadas no item 3.4) para o equipamento adquirido, com validade mínima de 60 (sessenta) meses.
- **Garantia e Suporte Técnico:**
    - Garantia *hardware* e Suporte Técnico do Fabricante por um período mínimo de 60 (sessenta) meses, cobrindo *hardware* e *software*.
    - O suporte deverá ser 24x7 (24 horas por dia, 7 dias por semana).
    - O suporte deve incluir o fornecimento de todas as atualizações de firmware, assinaturas de segurança (IPS, AV, Web Filter, Application Control, etc.) e correções durante o período de vigência.
- **Suporte em Português:** A comunicação para abertura e acompanhamento de chamados de suporte técnico deverá ser possível em Português (Brasil), preferencialmente por um Centro de Suporte Autorizado (ASC).

3.7. Considerações Finais

- A solução de Appliance Next Generation Firewall proposta deve ser compatível com a gerência existente (FortiManager) e solução de logs existente (FortiAnalyzer).
- A solução deverá ser compatível com a solução de SD-WAN (Fortinet) existente na contratante.
- As funcionalidades devem ser comprovadas por documentos de domínio público disponíveis no site do fabricante.

4 - QUALIFICAÇÃO TÉCNICA

A qualificação técnica do licitante será avaliada com base nos seguintes requisitos, que visam garantir que o fornecedor possua a capacidade técnica e operacional necessária para fornecer e manter a solução de segurança com a qualidade e a eficiência exigidas:

4.1. Qualificação Técnico-Operacional

4.1.1. Para comprovação da Qualificação Técnica Operacional, o licitante deverá apresentar documento emitido pelo fabricante do(s) equipamento(s) ou produto(s) objeto desta licitação, atestando seu **credenciamento oficial** como parceiro autorizado, revenda, distribuidor ou prestador de serviços.

4.1.2. O referido documento deverá indicar, expressamente, que o licitante está apto a comercializar e/ou prestar serviços de instalação e manutenção, com **acesso a suporte técnico e garantia de fábrica**, para o(s) item(ns) objeto da presente licitação.

4.1.3. A comprovação de credenciamento é indispensável para assegurar a originalidade do produto, a validade da garantia de fábrica e o acesso ao suporte técnico especializado, garantindo a qualidade e a segurança do fornecimento.

5 - PRAZOS

Os itens 1 e 2 deverão ser entregues em até 60 (sessenta) dias após a assinatura do contrato.

6 - LOCAL DE ENTREGA ou EXECUÇÃO

Os equipamentos deverão ser entregues na sede do CIASC em Florianópolis, na Rua Murilo Andriani, 327, bairro Itacorubi, agendando o dia de entrega junto à equipe de Segurança do CIASC pelo email cocib@ciasc.sc.gov.br.

7 - CONDIÇÕES DE ENTREGA/RECEBIMENTO OU EXECUÇÃO

As entregas estarão contempladas, após a entrega dos dois Appliances devidamente licenciados de acordo com o descritivo técnico e com a quantidade estipulada mínima de VDOMs, e também da renovação do suporte e garantia do FortiAnalyzer atual. Também deverá ser entregue a quantidade de SFPs e cordões estipulados junto com os equipamentos.

8 - CRONOGRAMA FISICO-FINANCEIRO

As entregas/execução deverão respeitar os prazos estabelecidos no item 5, sendo que o pagamento ocorrerá no dia 25 do mês subsequente à entrega do objeto e condicionada ao pleno aceitação dos gestores e fiscais responsáveis. O pagamento do item 01 será realizado em 03 parcelas iguais, mensais e consecutivas. E o pagamento do item 2 ocorrerá em 60 parcelas, iguais mensais e consecutivas.

9 - RESULTADOS ESPERADOS/ENTREGÁVEIS

Entrega dos appliances devidamente licenciados, SFPs, cordões e certificado de garantia e suporte para 60 meses.
Renovação do suporte e garantia de 60 (sessenta) meses da solução FortiAnalyzer.
Suporte técnico 24/7 para atendimento técnico, e sem limites de abertura de chamados das soluções.

10 - GARANTIA, ASSISTÊNCIA TÉCNICA, SUPORTE TÉCNICO E NÍVEIS DE SERVIÇO

Suporte técnico e garantia de software e hardware dos appliances durante a vigência do contrato de 60 (sessenta) meses.

11 - OBRIGAÇÕES DA CONTRATADA

Entrega dos appliances devidamente licenciados, SFPs, cordões e certificado de garantia e suporte para 60 meses.
Renovação do suporte e garantia de 60 (sessenta) meses da solução FortiAnalyzer.
Suporte técnico 24/7 para atendimento técnico, e sem limites de abertura de chamados das soluções.

12 - MATRIZ DE RISCO - Anexo IV