DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

Processo nº: *25/1400-0004177-9*

Requerente: *Departamento de Tecnologia da Informação e Comunicação – DETIC*

Assunto: *Contratação de Proteção Anti-Ddos com Aquisição de Equipamento Dedicado*

ANEXO II

TERMO DE REFERÊNCIA – TR

1. OBJETO:

Aquisição de 2 (dois) equipamentos **Appliance Anti-DDoS** do fabricante Arbor Netscout, modelo AED-8100, contratação de serviços constituídos de 2 (dois) **Licenciamentos** do Appliance (ARBOR EDGE DEFENSE), PartNumber AE-08100-02SWA em conjunto com **suporte e garantia do fabricante**, contratação de 2 (dois) **Licenciamentos** do Arbor Atlas Intelligence Feed, PartNumber AIF-AE-08100--02SWA-ADV-3YR, contratação de 2 (dois) **Licenciamento**s de proteção Adaptativa DDoS 2G , PartNumber AED-8100-2G-ADP-3YR, contratação de 1 (um) **Serviço de Solução Software** de Sistema Centralizado de Gerenciamento, PartNumber A-9AN00 com suporte e garantia do fabricante, contratação de 1 (um) "Serviços de Configuração e Instalação", e de 1 (um) **Treinamento** para 10 usuários para manutenção de ambiente de DF-e visando garantir proteção e alta disponibilidade do ambiente. Com possibilidade de prorrogação, nos limites da lei, no que se refere a serviços de suporte, garantia e subscrição de licenças.

As especificações de hardware, software e serviços relativas aos 02 Appliances Anti-DDoS estão descritas na Tabela 1 - Relação de Equipamentos:

Item	Qnt.	GCE	Descrição	Cód. produto
1	---	---	HARDWARE	---
1.1	02	0035.0181.010115	Appliance Especializado em Proteção contra DDoS;	E-081AJ-HWBAA
2	---	---	LICENÇAS	---
2.1	02	0035.0736.010168	Licença do Appliance (ARBOR EDGE DEFENSE);	AE-08100-02SWA
2.2	02	0035.0736.010169	Licença do Arbor Atlas Intelligence Feed;	AIF-AE-08100--02SWA-ADV-3YR,
2.3	02	0035.0736.010170	Licença de proteção Adaptativa DDoS 2G;	AED-8100-2G-ADP-3YR,
2.4	01	0035.0736.010171	Solução Software de Sistema	A-9AN00

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

			Centralizado de Gerenciamento;	
3	---	---	SERVIÇOS	---
3.1	02	0035.1000.000015	Suporte e Garantia do Fabricante - 60 meses;	MNT-AE-08100-02SWA-T3-3YR
3.2	01	0035.1000.000016	Suporte e Garantia do Fabricante para Sistema Centralizado de Gerenciamento – 60 meses;	MNT-A-9ANV00-T3-3YR
3.3	01	0035.1000.000017	Serviço de Configuração e Instalação;	---
3.4	01	0035.1000.000018	Treinamento – 10 Usuários.	---

2. FUNDAMENTAÇÃO:

No ano de 2016 foi realizada a prospecção e busca de alternativas capazes de dotar a unidade de autorização de documentos fiscais (DF-e) de mecanismos para aumentar a capacidade de resistência contra a indisponibilização dos serviços internet utilizados e bloquear ataques de rede como Negação de Serviço (DoS) e Negação de Serviços Distribuídos (DDoS). O resultado deste estudo foi a realização do Pregão Eletrônico nº 567/CELIC/2016 para aquisição de um sistema especializado em proteção contra-ataques DDoS baseado em equipamento dedicado, instalado nos Datacenters da PROCERGS e da SEFAZ.

A solução atual será descontinuada EOS (End-of-Sale) e EOL (End-of-Life) pelo fabricante, e sem suporte e atualizações devido ao fim do seu contrato em 07/09/2025. Além deste fator, existe uma dificuldade na manutenção diária de políticas e ajustes de configuração, pois não há um sistema contratado que centralize estas configurações, havendo necessidade de fazê-lo um-a-um de forma independente, aumentando o tempo e o risco de erros de configuração. Com a constante evolução das técnicas dos ataques DoS/DDoS, também se faz necessário uma melhoria na proteção, com um sistema que o faça de forma adaptativa, proporcionando maior eficácia na proteção.

Foi realizado um estudo para contratação do serviço de anti-DDoS nas operadoras, porém devido o serviço de DF-e estar alocado em dois sites distintos, com múltiplos links de comunicação, seria inviável dada a necessidade de aquisição do serviço em todos os links atualmente utilizados. Futuramente este modelo de contratação pode ser implementado para complementar a solução on-premise, proporcionando segurança contra ataques do tipo DoS/DDoS volumétricos.

É necessário realizar a manutenção da proteção já implantada para manter a segurança do perímetro contra ataques DoS/DDoS. Dessa forma, existe a necessidade de atualização da solução atual, dada a criticidade do ambiente consolidado, com contratação de serviço de manutenção, suporte, assinatura de atualização dinâmica de ameaças, sistema centralizado de gerenciamento e

proteção adaptativa. Garantindo a continuidade e disponibilidade do serviço.

Esta aquisição e contratação são aderentes ao planejamento estratégico da SEFAZ RS dentro do objetivo 01 – “Assegurar continuidade e disponibilidade de serviços”, da meta 01.001 “Garantir a continuidade dos negócios e disponibilidade dos serviços de TIC” e do objetivo 01.001.0337 – “Estabilizar e aperfeiçoar ambiente de redes e conectividade”.

Esta aquisição está incluída no item 1791 do plano de aquisições de 2025 da CELIC e previsto na tabela de investimentos e despesas previstas para 2025 no Anexo Único do Acordo de Cooperação técnica 01/20 atualizado pelo Acordo de Cooperação Técnica 2/24 do Confaz.

3. DESCRIÇÃO DA SOLUÇÃO:

Os aparelhos Anti-DDoS funcionam barrando pedidos maliciosos de acesso aos serviços da Fazenda, para isso contam com rotinas internas para identificar comportamentos anômalos além de atualizações constantes de endereços de onde tem partido ataques dessa natureza, por isso, é fundamental que o aparelho conte sempre com garantia, licenças e softwares atualizados. Para garantir a compatibilidade entre as licenças e o hardware e complementariedade entre os licenciamentos, a aquisição deve se dar em lote único e, por se tratar de equipamento altamente especializado, o suporte deve ser prestado pelo próprio fabricante.

A Aquisição dos novos Appliances Anti-DDoS para substituição dos Appliances Anti-DDoS APS 2600, busca manter a continuidade e proteção do ambiente, bem como evitar contratações de serviços isolados para atendimento de incidentes, o que seria impraticável e não econômico, principalmente em caso de incidente de maior porte.

Ademais, o processo de diagnóstico até a solução de determinado defeito, de forma pontual, pode oscilar de preço, afetando o orçamento previsto e aumentando o prazo de indisponibilidade do equipamento o que seria impensável em ambiente tão crítico.

4. ESPECIFICAÇÃO DO PRODUTO:

4.1. HARDWARE: Objeto Item 1.1 “Appliance Especializado em Proteção com DDoS”:

4.1.1. A solução de Proteção contra DDoS deve ser implementada em hardware dedicado, em um equipamento específico do tipo appliance, NÃO sendo aceitos: 1- PC (Personal Computer ou Servidores) adaptado para a função aqui especificada ou 2- Firewall UTM com feature de anti-DDoS;

4.1.2. Equipamentos com software e hardware especificamente projetados para atender a função de Proteção de Ataques do tipo DDoS, com sistema operacional otimizado para esse fim;

4.1.3. Os itens deverão ser fornecidos com todas as documentações, manuais, cabos,

conectores, adaptadores, acessórios, drivers e demais softwares necessários para a sua instalação e funcionamento.

4.1.4. Hardware deve ser instalável em rack 19” sem a utilização de bandeja, ocupando no máximo 2RUs;

4.1.5. Deve ser Stateless, ou seja, não deve manter o estado das conexões;

4.1.6. Cada equipamento deverá ser entregue licenciado para proteção de um throughtput de 2Gbps de dados, e deve permitir upgrade desta capacidade, via licenciamento de software, até o throughtput de proteção de 40Gbps;

4.1.7. Cada equipamento deve possuir no mínimo 2 (dois) segmentos GigabitEhernet (1GE), sendo configurados com no mínimo 4 (quatro) portas GigabitEthernet dedicadas para a finalidade de proteção, com bypass de tráfego integrado;

4.1.8. As portas devem vir populadas com 4 (quatro) transceptores 1000BASE-T (RJ45) atendendo ao padrão IEEE 802.3ab;

4.1.9. Cada equipamento deve possuir no mínimo 2 (dois) segmentos TenGigabitEhernet (10GE), sendo configurados com no mínimo 4 (quatro) portas TenGigabitEthernet dedicadas para a finalidade de proteção, com bypass de tráfego integrado;

4.1.10. As portas devem vir populadas com 4 (quatro) transceptores 10GBASE-SR, ambos com conector do tipo LC, atendendo ao padrão óptico (IEEE 802.3ae Tipo 10GBASE-SR);

4.1.11. Todas as portas devem vir licenciadas para sua capacidade máxima de tráfego, sem necessidade de licenciamento adicional;

4.1.12. Deve possuir latência menor que 80 microssegundos;

4.1.13. Deve implementar bypass do tráfego em hardware em todas as interfaces de proteção;

4.1.14. Deve implementar Link State Propagation nas interfaces de proteção, ou seja, propagar o estado de link de uma interface do segmento de proteção para a outra interface do mesmo segmento;

4.1.15. Deve possuir no mínimo duas fontes de alimentação redundantes, hot-swappable, operando entre 100 e 240Vac 60hz;

4.1.16. Deve possuir indicadores luminosos do estado de alimentação (on/off) da fonte;

4.1.17. Deve possuir indicadores luminosos do estado do equipamento, atividade de rede, status dos links;

4.1.18. Os equipamentos devem possuir um throughtput mínimo de proteção de 2 Gbps;

4.1.19. Os equipamentos devem suportar um throughtput mínimo de proteção de 12 Mpps;

4.1.20. Deve possuir dispositivo interno de alta disponibilidade em camada 2 que permita manter o funcionamento da rede (fail-open) ou bloquear o funcionamento da rede totalmente (fail-close), em caso de falha de hardware, falha de sistema, ou falta de

energia elétrica;

4.1.21. Deve possuir serviço de atualização dinâmica para novos endereços IP maliciosos a partir de centro de pesquisa do fabricante;

4.1.22. Não serão aceitas soluções de mitigação de ataques baseadas apenas em “Rate Limiting”;

4.1.23. Deve suportar monitoria/bloqueio de endereços IP por geolocalização, GeoIP;

4.1.24. Deve ser capaz de bloquear apenas o tráfego associado ao ataque permitindo o tráfego legítimo e não causando impacto no acesso dos usuários;

4.1.25. Deve permitir a configuração de listas de filtros contendo expressões de filtragem de pacotes para descartar ou permitir a passagem do tráfego;

4.1.26. Deve fornecer uma capacidade de moldar o tráfego que corresponde a uma expressão de filtragem especificada, e descartar o tráfego que exceda a taxa configurada. As expressões devem suportar a seleção de campos de cabeçalho IP e campos de cabeçalho da camada 4 (UDP e TCP);

4.1.27. Deve permitir a criação de perfis de monitoria/proteções independentes;

4.1.28. Deve permitir no mínimo 50 perfis de monitoria/proteção de tráfego;

4.1.29. Deve ser capaz de bloquear tentativas de negação de serviço do tipo low-and-slow;

4.1.30. Deve possuir capacidade de resistência às ferramentas de evasão;

4.1.31. Deve possuir mecanismos de prevenção de negação de serviço do tipo DNS Flood;

4.1.32. Deve possuir mecanismos de prevenção de negação de serviço do tipo DNS Amplification;

4.1.33. Deve possuir mecanismos de prevenção de negação de serviço do tipo UDP Flood;

4.1.34. Deve possuir mecanismos de prevenção de negação de serviço do tipo ICMP Flood;

4.1.35. Deve ser capaz de detectar e bloquear ICMP Flood acima de taxas configuráveis pelo usuário.

4.1.36. Deve possuir mecanismos de prevenção de negação de serviço do tipo HTTP GET Flood e HTTP POST Flood;

4.1.37. Deve ser capaz detectar e bloquear TCP SYN Flood acima de taxas configuráveis pelo usuário;

4.1.38. Deve possuir mecanismos de prevenção de negação de serviço do tipo Bandwidth Flood;

4.1.39. Deve ser capaz de bloquear pacotes inválidos (incluindo verificação para Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number).

4.1.40. Deve ser capaz de detectar e bloquear as fontes que emitem quantidades excessivas

de tráfego de acordo com parâmetros configuráveis.

4.1.41. Deve ser capaz de descartar pacotes de portas TCP especificadas com cargas correspondentes a uma expressão regular configurável.

4.1.42. Deve ser capaz de descartar pacotes de portas UDP especificadas com cargas correspondentes a uma expressão regular configurável.

4.1.43. Deve suportar Spoofed TCP SYN Flood Prevention que autentica conexões TCP a partir do host de origem;

4.1.44. A prevenção de pacotes Spoofed TCP SYN Flood deve ser capaz de especificar as portas TCP de origem e destino para serem ignoradas;

4.1.45. A prevenção de pacotes Spoofed TCP SYN Flood deve fornecer uma maneira de não impactar nas sessões HTTP dos usuários autenticados;

4.1.46. A prevenção de pacotes Spoofed TCP SYN Flood deve prover uma opção ao TCP RST enviado a clientes, de forma a evitar problemas com aplicações sensíveis a esta técnica, desta forma o método empregado para esta prevenção deverá suportar o envio de um pacote ACK fora de sequência e desta forma forçar um soft restart da conexão.

4.1.47. Deve permitir o descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período de tempo.

4.1.48. Deve ser capaz de barrar um host após consecutivos TCP inativos.

4.1.49. Deve ser capaz de bloquear pedidos de DNS na porta 53 que não estejam em conformidade com os padrões RFC.

4.1.50. Deve ser capaz de autenticar as solicitações de DNS dos hosts de origem e descartar aqueles que não podem ser autenticados dentro de um prazo especificado.

4.1.51. Deve ser capaz de limitar o número de consultas DNS por segundo através da configuração de uma taxa pelo usuário.

4.1.52. Deve ser capaz de bloquear o tráfego de qualquer máquina que gera mais pedidos consecutivos de DNS do que o limite configurado e, depois, deve barrar o host de origem.

4.1.53. Deve ser capaz de bloquear o tráfego de hosts que repetidamente interrompem solicitações HTTP.

4.1.54. Deve ser capaz de detectar e descartar pacotes HTTP que não atendam aos padrões RFC e, em seguida, barrar os hosts de origem.

4.1.55. Deve ser capaz de bloquear hosts que excedam ao número total permitido, configurado pelo usuário, de operações HTTP por segundo e por servidor de destino.

4.1.56. Deve ser capaz de ativar regularmente novas técnicas de defesa a partir de contramedidas de ataques atualizadas e mantidas pela equipe do fabricante, através

de pesquisa e monitoramento 24x7 da Internet para identificar os botnets mais significativos e recentes e suas estratégias de ataque.

4.1.57. Deve ser capaz de atualizar as contramedidas de ataque automaticamente, em tempo real ou em um intervalo de tempo configurado pelo usuário.

4.1.58. Deve ser capaz de automaticamente atualizar as contramedidas de ataque, quando solicitado manualmente pelo usuário.

4.1.59. Deve permitir a configuração de serviços de proteção que contêm configurações de prevenção pré-definidas associadas a serviços específicos, tais como Web, DNS, VoIP ou um servidor genérico.

4.1.60. Deve permitir que os parâmetros de proteção sejam alterados enquanto uma proteção está sendo executada;

4.1.61. Deve possibilitar a captura de pacotes para análise e permitir exportação dos pacotes capturados em formato de arquivo PCAP - Packet Capture.

4.1.62. O sistema deve ser fornecido com uma configuração de filtros/contra-medidas recomendados pré-configurados;

4.1.63. Deve ser fornecido com serviço de atualização permanente de filtros/contra-medidas de ataques e vulnerabilidades por 5 (cinco) anos;

4.1.64. Os equipamentos deverão ser fornecidos com seu software com licença irrestrita, em sua versão mais atual e completa. O fornecimento deverá incluir todas as licenças de software necessárias para a implementação de todas as funcionalidades disponibilizadas pelo fabricante para o equipamento fornecido;

4.1.65. Deve fornecer estatísticas e gráficos detalhados para cada proteção, mostrando o seu impacto sobre o tráfego nos últimos 5 minutos, 1 hora, 24 horas, 7 dias ou um intervalo personalizado especificado.

4.1.66. Deve exibir estatísticas em tempo real de proteção do tráfego, em bytes e pacotes, com taxas em bps e pps;

4.1.67. Deve exibir estatísticas de tráfego para, no mínimo, os top 10 IPs e/ou URLs acessados;

4.1.68. Deve exibir estatísticas de tráfego para, no mínimo, os top 10 Domínios DNS acessados;

4.1.69. Deve exibir estatísticas de tráfego geolocalizado para, no mínimo, os top 10 países de origem;

4.1.70. Deve exibir estatísticas de tráfego por protoloco IP;

4.1.71. Deve exibir estatísticas de tráfego para, no mínimo, os top 10 endereços IP bloqueados;

4.1.72. Deve permitir, no mínimo, a geração de relatórios contendo as estatísticas e gráficos

detalhados para cada perfil de proteção.

4.1.73. Deve prover um filtro relacionado a características de cabeçalho de pacote que possa ser compartilhado entre todas as regras ativas;

4.1.74. Este filtro deve poder determinar, se é permitido tráfego baseado nas características:

4.1.75. Protocolos; Portas de origem e ou destino; Flags; Tamanho de Pacote.

4.1.76. A solução deve permitir a contenção de tráfego através do uso de base de indicadores reputacionais (ex.: base de reputação de IP, lista de botnets, C&C servidores);

4.1.77. A solução deverá ser entregue com sistema de gerenciamento centralizado, com capacidade para gerenciar no mínimo 5 equipamentos, podendo ser ampliada esta capacidade com aquisição de licença adicional;

4.1.78. A solução deverá ser entregue integrada a um serviço de proteção adaptativa contra-ataques do tipo DoS e DDoS;

4.2. LICENÇAS:

4.2.1. Todos os softwares necessários deverão ser fornecidos e devidamente licenciados.

4.2.2. No caso de licenças de software, as mesmas deverão ser fornecidas em sua versão mais atual homologada pelo fabricante.

4.2.3. LICENÇA - ARBOR EDGE DEFENSE - AE-08100-02SWA (Objeto Item 2.1 – Licença do Appliance (ARBOR EDGE DEFENSE)

4.2.3.1. O item deverá ser fornecido com as seguintes características mínimas:

4.2.3.2. 60 meses de garantia e suporte do fabricante.

4.2.3.3. Os equipamentos devem possuir um throughtput mínimo de proteção de 2 gbps;

4.2.3.4. A solução deve atuar também como um tig (threat intelligence gateway), que permita sua utilização como primeira e última barreira de contenção bloqueando tráfego de/para ips que estejam inscritos em listas de indicadores de comprometimento (iocs) baseados em reputação;

4.2.3.5. Suporte a no mínimo 3.000.000 (três milhões) de indicadores de comprometimento

4.2.3.6. (ioc) que devem ser compostos por: url, ip de origem ou domínios;

4.2.3.7. O sistema deve atuar como um servidor taxii, suportando a integração com clientes de stix/taxii, para recebimento de listas de ioc de terceiros;

4.2.3.8. A solução deve permitir a mitigação de ataques criptografados de modo transparente, sem possuir endereço ip atribuído nas interfaces de proteção, como um tls proxy transparente;

4.2.3.9. Deve permitir implementar análise de tráfego através do tls proxy de tráfego ssl que use chaves assimétricas de criptografia e cifras de encriptação do tipo aes, chacha, ecdhe e rsa;

4.2.3.10. A solução deve suportar, no mínimo, 19.000 (dezenove mil) conexões por segundo

e 1,8 gbps de tráfego de entrada através do tls proxy transparente com chaves de 2048 bits;

4.2.3.11. Deve suportar tls 1.3 e pfs (perfect forward secrecy) com chaves nos formatos pkcs#1 e pkcs#8;

4.2.3.12. Deve suportar, no mínimo, as seguintes chaves:

4.2.3.13. Tls_ecdhe_ecdsa_with_aes_256_gcm_sha384;

4.2.3.14. Tls_ecdhe_rsa_with_aes_256_gcm_sha384;

4.2.3.15. Tls_ecdhe_ecdsa_ with_ chacha20_poly1305 _sha256;

4.2.3.16. Tls_ecdhe_rsa_with_chacha20_poly1305_sha256;

4.2.3.17. Tls_ecdhe_ecdsa_with_aes_256_cbc_sha;

4.2.3.18. Tls_ecdhe_rsa_with_aes_256_cbc_sha;

4.2.3.19. A solução, antes de inspecionar o tráfego criptografado, deve analisar e mitigar todo o tráfego para ataques na camada de rede (camada 3 - modelo osi) e ataques na camada de transporte (camada 4 - modelo osi);

4.2.3.20. A solução deve encaminhar o tráfego, limpo de ataques até a camada 4, para o proxy transparente para descriptografar o pacote e então analisar e mitigar o tráfego para ataques na camada de aplicação (camada 7 - modelo osi) e depois criptografar o tráfego limpo e encaminhar para o destino na rede;

4.2.3.21. No caso de a solução ser licenciada com a proteção adaptativa de ddos, a mesma deve realizar a análise do tráfego inspecionado e liberado para ingresso na rede visando detectar padrões de tráfego que possam ser vetores de ataque potenciais de ddos que conseguiram evadir as contramedidas configuradas, e caso detecte algum, provenha recomendações de ajustes nas contramedidas para também mitigar o ataque detectado;

4.2.3.22. Os tipos de ataque analisados pela proteção adaptativa de ddos devem ser no mínimo baseados em:

4.2.3.23. Amplificação de arms, bacnet, chargen, cldap, coap, dns, ipmi, l2tp, mdns, memcached, mssql, netbios, ntp, openvpn, quake, qotd, ripv1, rpcbind (portmap), sentinel, stun, snmp, ssdp, tcp, tcp inbound, tftp, ubiquiti, unreal tournament, valvesourceengine (vse);

4.2.3.24. Amplificação de web services discovery e web services devices profile (ws-dd);

4.2.3.25. Nonexistent domain query flood, tcp flooding, tcp ac

4.2.4. LICENÇA - ARBOR ATLAS INTELLIGENCE FEED (Objeto Item 2.2 – Licença do Arbor

Atlas Intelligence Feed)

4.2.4.1. O item deverá ser fornecido com as seguintes características mínimas:

4.2.4.2. 60 meses de garantia e suporte do fabricante.

4.2.4.3. Licença que possibilita análise e recebimento de dados contínuos de ameaças, em formato de repositório, que permitem a detecção e mitigação automática de todos os tipos de ameaças cibernéticas preventivamente.

4.2.4.4. O objeto do licenciamento deve ser disponibilizado e atualizado periodicamente nos equipamentos sem a necessidade de intervenção técnica, e sem custos adicionais ao contratante;

4.2.4.5. Hardware deve ser instalável em rack 19” sem a utilização de bandeja, ocupando no máximo 2rus;

4.2.5. LICENÇA - PROTEÇÃO ADAPTATIVA DDOS (Objeto Item 2.3 Licença de proteção Adaptativa DDoS 2G)

4.2.5.1. O item deverá ser fornecido com as seguintes características mínimas:

4.2.5.2. 60 meses de garantia e suporte do fabricante.

4.2.5.3. Licença de solução de inteligência artificial(ia) e aprendizado de máquina para detecção e mitigação de ataques ddos dinâmicos e multivetoriais.

4.2.5.4. Solução analisará continuamente o tráfego de rede, identificando ataques não bloqueados e atualiza automaticamente as configurações de contramedidas para proteger contra novos vetores de ataque.

4.2.5.5. A licença deve ser compatível com a capacidade de inspeção de 2gbps de dados.

4.2.5.6. O objeto do licenciamento deve ser disponibilizado e atualizado periodicamente nos equipamentos sem a necessidade de intervenção técnica, e sem custos adicionais ao contratante;

4.2.6. SOLUÇÃO SOFTWARE - SISTEMA CENTRALIZADO DE GERENCIAMENTO (Objeto Item 2.4 Solução Software de Sistema Centralizado de Gerenciamento)

4.2.6.1. Item deverá ser fornecido com as seguintes características mínimas:

4.2.6.2. 60 meses de garantia e suporte do fabricante.

4.2.6.3. A gerência da solução deve permitir administrar de maneira centralizada as configurações da solução de mitigação ddos on premise, a partir de agora referenciado apenas como mitigador, facilitando a manutenção das mesmas configurações e regras de proteção nos diversos appliances de uma organização;

4.2.6.4. A gerência deve permitir monitorar e responder à ataques nas redes protegidas a partir de uma única interface de usuário;

4.2.6.5. A gerência deve ser instalada como um virtual appliance no vmware vsphere

hypervisor versão 6.7 ou maior;

4.2.6.6. A gerência deve possuir licenciamento suficiente para todos os mitigadores adquiridos nesta licitação;

4.2.6.7. A gerência deve suportar simultaneamente múltiplas versões de software dos mitigadores, inclusive as versões virtualizadas do mitigador instaladas on premise ou na cloud pública/privada;

4.2.6.8. A gerência de múltiplos mitigadores a partir de uma única interface de usuário deve permitir melhoria na execução das seguintes tarefas:

4.2.6.9. Consolidar e visualizar os alertas de segurança e de sistema detectados pelos mitigadores;

4.2.6.10. Gerenciar as políticas de segurança que protegem sua rede contra possíveis ameaças e ataques;

4.2.6.11. Centralizar os modelos de proteção, grupos de proteção, filtro de ameaças de saída, lista de negações e lista de permissões para fornecer proteção consistente em toda a sua rede e um fluxo de trabalho simplificado;

4.2.6.12. Ajustar as proteções em vários dispositivos ou em um dispositivo individual;

4.2.6.13. Utilizar os mitigadores para capturar pacotes, e permitir o download desses pacotes de maneira centralizada para facilitar a análise;

4.2.6.14. A gerência deve permitir criar, configurar e gerenciar grupos de proteção, filtro de ameaças de saída, lista de filtros, denylists, allowlists e propagar tais configurações para cada mitigador gerenciado;

4.2.6.15. Na gerência deve ser possível visualizar o tráfego e as estatísticas de tráfego que passa por cada dispositivo, bem como uma visão agregada dos dados de todos os dispositivos;

4.2.6.16. A gerência deve permitir a autenticação de usuários através de serviços como radius, tacacs+ e saml além da autenticação nativa da solução;

4.2.6.17. A gerência deve permitir a notificação de eventos através do envio de e-mails, via snmp ou syslog;

4.2.6.18. A gerência deve permitir o monitoramento de seus próprios recursos através do uso de snmp polling;

4.2.6.19. A gerência deve auditar todo o sistema registrando todas as mudanças de configuração em logs de atividade;

4.2.6.20. Deve ser possível realizar backups da configuração da gerência de forma manual e programada;

4.2.6.21. A gerência deve apresentar uma lista das principais ameaças externas e internas detectadas nos mitigadores do ambiente organizada por tipo, país de origem, ip de

origem, ip de destino e grupos de proteção e permitir a filtragem dos eventos listados por tais categorias;

4.2.6.22. A gerência deve permitir a geração de relatórios sobre ataques sofridos no ambiente num determinado período, independente do mitigador que detectou e bloqueou o(s) ataque(s) com informações de alto nível sobre as tendências de tráfego da rede ao longo do tempo;

4.3. SERVIÇO.

4.3.1. SUPORTE E GARANTIA DO FABRICANTE APPLIANCE ANTI-DDOS (Objeto Item 3.1 Suporte e Garantia do Fabricante – 60 meses)

4.3.1.1. Deverá ser fornecido com as seguintes características mínimas:

4.3.1.2. Prazo de 60 meses de garantia e suporte do fabricante para todos os equipamentos, licenças e sistemas deste Edital.

4.3.1.3. Os equipamentos devem ser entregues em um prazo máximo de 60 dias a contar da data de assinatura do contrato;

4.3.1.4. Os componentes constantes desse edital deverão estar acompanhados de todas as licenças de software e hardware necessárias para sua completa operação, com prazo mínimo de validade de 60 (sessenta) meses, a contar da data de emissão do aceite técnico provisório, ou seja, após a entrega do equipamento;

4.3.1.5. Prazo de garantia para todos os componentes de 5 (cinco) ano(s) com reposição em NBD (em dias úteis e horário comercial das 08:00hs às 17:00hs 8x5xNext Business Day). Durante este período, a CONTRATADA deverá solucionar todos os chamados de assistência técnica efetuados, no local de uso do equipamento (on-site), isto é, na SEDE da PROCERGS ou em local definido pela mesma em Porto Alegre - RS, com tempo de atendimento de no máximo 08 (oito) horas para identificação do problema e tempo de solução máxima definitiva de 24 (vinte e quatro) horas

4.3.1.6. Disponibilizar as atualizações e upgrades das versões dos softwares pré-instalados nos equipamentos durante o período de garantia, sem custos adicionais, sendo que a disponibilidade destas atualizações deve ser comunicada à CONTRATANTE para planejamento das alterações necessárias.

4.3.1.7. Os equipamentos/materiais fornecidos devem ser novos e sem uso, sendo de linha normal de produção do fabricante, RMA também devem ser novos e sem uso;

4.3.1.8. Suporte técnico, no regime 24 x 7, pelo período de 60 (sessenta) meses, a contar da data de emissão do aceite técnico.

4.3.2. SERVIÇO DE SUPORTE E GARANTIA DO FABRICANTE PARA SISTEMA CENTRALIZADO DE GERENCIAMENTO (Objeto Item 3.2 Suporte e Garantia do Fabricante para Sistema Centralizado de Gerenciamento – 60 meses)

4.3.2.1. Deverá ser fornecido com as seguintes características mínimas:

4.3.2.2. Prazo de 60 meses de garantia e suporte do fabricante para todos os equipamentos, licenças e sistemas deste Edital.

4.3.2.3. O Suporte e Garantia devem atender ao Sistema Centralizado de Gerenciamento adquirido pelo prazo estipulado.

4.3.2.4. A empresa CONTRATADA deverá atuar em conjunto com o Fabricante para sanar quaisquer problemas relacionados ao Sistema Centralizado de Gerenciamento, sem ônus adicional para a CONTRATANTE.

4.3.2.5. Além de disponibilizar as atualizações e upgrades das versões do sistema durante o período contratado, sem custos adicionais, sendo que a disponibilidade destas atualizações deve ser comunicada à CONTRATANTE para planejamento das alterações necessárias.

4.3.2.6. Suporte técnico, no regime 24 x 7, pelo período de 60 (sessenta) meses, a contar da data de emissão do aceite técnico.

4.3.3. SERVIÇO DE CONFIGURAÇÃO E INSTALAÇÃO (Objeto Item 3.3 – Serviço de Configuração e Instalação)

4.3.3.1. A empresa CONTRATADA deverá acompanhar a configuração, migração e implantação de 1 (um) equipamento adquirido no prédio SEDE da PROCERGS em Porto Alegre/RS;

4.3.3.2. A PROCERGS se encarregará de instalar o outro equipamento posteriormente quando o local de instalação estiver disponível;

4.3.3.3. A empresa CONTRATADA deverá providenciar a instalação do sistema de gerenciamento centralizado e incluir todos os equipamentos do fabricante neste;

4.3.3.4. A empresa CONTRATADA deverá integrar a solução adquirida ao ADP (Advanced DDoS Protection), bem como certificar seu funcionamento;

4.3.3.5. Suporte técnico: 24 horas/dia de segunda a domingo pela duração do contrato.

4.3.4. SERVIÇO DE TREINAMENTO DE 10 USUÁRIOS (Objeto Item 3.4 Treinamento – 10 Usuários)

4.3.4.1. O fornecedor deverá prover treinamento reconhecido pelo fabricante com emissão de certificado aos participantes, com carga horária mínima de 24 h, para até 10 pessoas, abrangendo as funcionalidades de configuração e administração/operação no formato hands on.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

4.4. REQUISITOS DA CONTRATAÇÃO:

4.4.1. A aquisição e contratação deve contemplar no mínimo os itens da Tabela 1 – Relação de equipamentos do item OBJETO, bem como sua instalação física e ativação com o suporte remoto e presencial do fabricante.

4.4.2. Todos os itens deste Termo de Referência não podem constar na situação de "final de produção" ("end of life") devendo estar em linha de produção, ou seja, sendo produzidos pelo fabricante no momento da entrega do equipamento.

4.4.3. Todos os itens deste Termo de Referência não podem constar na situação de “solicitação de venda encerrada” (“end of sale”) ou “solicitação de pedido suspensa” (“end of order”) pelo fabricante no momento da entrega do equipamento.

4.4.4. Caso algum item deste Termo de Referência não esteja disponível no momento do fornecimento, o licitante vencedor deve comprovar as mesmas características técnicas mínimas obrigatórias para o item que o substitui.

4.4.5. Os equipamentos deverão ser fornecidos com software com licença irrestrita, em sua versão mais atual e completa. O fornecimento deverá incluir todas as licenças de software necessárias para a implementação de todas as funcionalidades disponibilizadas pelo fabricante para os equipamentos fornecidos.

4.4.6. Caso necessário, o fornecimento deverá incluir todas as licenças de software necessárias para a implementação da solução nos novos equipamentos e os existentes.

4.4.7. Todos os itens deste Termo de Referência devem ser do mesmo fabricante.

4.4.8. O proponente deve apresentar proposta para todos os itens deste Termo de Referência.

4.4.9. Os equipamentos devem ser novos, sem uso, e estar na linha atual de produção do fabricante.

4.4.10. O licitante vencedor deverá estar aderente aos critérios de sustentabilidade constantes na IN CELIC/SPGG Nº 001/2025, publicada no DOE em 2 de janeiro de 2025.

5. GARANTIA:

Conforme itens **“SUPORTE E GARANTIA DO FABRICANTE APPLIANCE ANTI-DDOS”** e “**SERVIÇO DE SUPORTE E GARANTIA DO FABRICANTE PARA SISTEMA CENTRALIZADO DE GERENCIAMENTO**”, constantes das especificações técnicas acima.

O prazo de garantia começa a contar da data de emissão do aceite técnico definitivo.

O Termo de Recebimento Definitivo somente será emitido após a apresentação da comprovação da contratação do serviço de garantia junto ao fabricante dos equipamentos.

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

6. LOCAL DE ENTREGA:

A entrega de todo material deve ser direcionada à Supervisão do Departamento de Operações da PROCERGS, no Setor de Patrimônio, Arquivo e Almoxarifado (SPA) da PROCERGS, localizado na Rua Dona Margarida, nº 64, bairro Navegantes, Porto Alegre, RS, CEP 90240-610 ou em Datacenter na cidade de Porto Alegre/RS a ser determinado pelo CONTRATANTE após assinatura do contrato, em horário entre as 08:30 h e 12:00 h e das 13:30 h às 17:00 h.

O Treinamento deverá ser fornecido em local definido pela PROCERGS em Porto Alegre/RS ou, no formato EAD (Ensino à Distância) ou, ainda, em Centro de Treinamento oficial em Porto Alegre, a critério da CONTRATANTE.

O prazo para a entrega dos equipamentos será de até 60 **(sessenta) dias** após a publicação da ordem de fornecimento.

Contatos com a PROCERGS devem ser realizados através do endereço de e-mail procergs@procergs.rs.gov.br ou telefone: **(51) 3210-3100** sendo necessário o encaminhamento aos fiscais de contrato das datas e prazos para entrega.

Caso não seja possível o fornecimento no prazo assinalado, a CONTRATADA deverá comunicar as razões respectivas, com pelo menos 2 dias úteis de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

7. MODELO DE EXECUÇÃO DO OBJETO:

A partir da assinatura do contrato e da emissão, pela CONTRATANTE, da Ordem de Fornecimento, as etapas se seguirão:

7.1. A Contratada deve encaminhar os equipamentos para o endereço designado no item LOCAL DA ENTREGA;

7.2. A Contratada deve enviar e-mail para os fiscais do contrato (endereços de e-mail informados no item MODELO DE GESTÃO DO CONTRATO) com cópia para a PROCERGS (endereço de e-mail no item LOCAL ENTREGA):

7.2.1. Comunicando a remeça dos equipamentos;

7.2.2. Mencionando a expressão “envio de 02 appliances Anti-DDoS AED 8100”;

7.2.3. Informando a data de envio, a data prevista de entrega, o nome da transportadora e os números de série dos equipamentos

7.3. Em até de 5 (cinco) dias úteis após a chegada dos equipamentos no LOCAL DE ENTREGA, a CONTRATANTE encaminhará, em resposta ao e-mail de comunicação de envio dos equipamentos, o Termo de Recebimento Provisório à CONTRATADA.

7.4. A CONTRATADA deverá agendar uma reunião de kick-off para definição da data de configuração e instalação. (Caso haja interesse, a CONTRATADA poderá agendar uma

visita ao local da CONTRATANTE (Survey)

7.5. Os treinamentos devem ser realizados durante ou após a etapa de configuração e instalação.

7.6. Após a instalação ser concluída com sucesso, deverá ser iniciada a implantação, que consiste em colocar o ambiente em produção.

7.7. O Termo de Recebimento Definitivo será emitido conforme conclusão das etapas acima, prosseguindo-se com o devido pagamento.

8. MODELO DE GESTÃO DO CONTRATO:

Os equipamentos, licenças e serviços de suporte e garantia objeto deste Contrato serão geridos pelo DETIC, através do Chefe da Divisão de Infraestrutura e Segurança – DIS, ou quem o esteja substituindo.

A CONTRATANTE, através do gestor e dos fiscais, se reserva no direito de efetuar, a qualquer tempo, auditoria e inspeção de qualidade nos equipamentos, nas licenças e nos serviços de suporte e garantia.

Para acompanhar e fiscalizar a execução do contrato, na qualidade de FISCAL, ficam designados pela CONTRATANTE os servidores Gustavo Emilio Benitez Koppe, matrícula nº 2832631, e-mail: gustavok@sefaz.rs.gov.br; e Vinicius Keniti Yano, matrícula nº 4676173, e-mail: viniciusky@sefaz.rs.gov.br, lotados da Divisão de Infraestrutura e Segurança – DIS.

Todas as comunicações deverão ser copiadas para a caixa institucional gab.detic@sefaz.rs.gov.br.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Haverá um único Termo de Recebimento, não sendo aceito faturamento parcial destes itens.

O pagamento só será realizado após emissão de Termo de Recebimento Definitivo, conforme disposições legais e contratuais.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR:

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço global, respeitados os valores unitários de cada item.

11. ESTIMATIVA DO VALOR DA CONTRATAÇÃO:

O valor da estimativa considerando os itens catalogados no GCE está demonstrado na

DETIC
ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
DEPARTAMENTO DE TIC

tabela abaixo:

ITEM GCE	DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
0351000000016	INFORMATICA - SERVIÇOSSUPORTE GARANTIA SOFTWARE NETSCOUT ARBOR 0035.0736.010171	1	R$ 206.871,24	R$ 206.871,24
0351000000017	INFORMATICA - SERVIÇOS CONFIGURAÇÃO INSTALAÇÃO APPLIANCE DDOS ARBOR NETSCOUT	1	R$ 129.350,00	R$ 129.350,00
0351000000018	INFORMATICA - SERVIÇOS - DE TREINAMENTO APPLIANCE DDOS ARBOR NETSCOUT	1	R$ 76.840,00	R$ 76.840,00
0350181010115	APPLIANCE - PROTEÇÃO CONTRA DDOS ARBOR NETSCOUT 8100	2	R$ 422.053,51	R$ 844.107,02
0350736010168	LICENÇA - ARBOR EDGE DEFENSE - AE-08100-02SWA	2	R$ 474.221,19	R$ 948.442,38
0350736010169	LICENÇA - ARBOR ATLAS INTELLIGENCE FEED ARBOR NETSCOUT	2	R$ 223.535,34	R$ 447.070,68
0350736010170	LICENÇA - PROTEÇÃO ADAPTATIVA DDOS 2GBS NETSCOUT'S ARBOR EDGE DEFENSE (AED)	2	R$ 205.209,11	R$ 410.418,22
0350736010171	SOLUÇÃO SOFTWARE - SISTEMA CENTRALIZADO GERENCIAMENTO-NETSCOUT ARBOR PN A-9ANV00	1	R$ 321.321,17	R$ 321.321,17
0351000000015	INFORMATICA - SERVIÇO SUPORTE APPLIANCE PROTEÇÃO CONTRA DDOS ARBOR NETSCOUT	2	R$ 192.852,30	R$ 385.704,60
				R$ 3.770.125,31

12. ADEQUAÇÃO ORÇAMENTÁRIA:

A despesa deverá ser enquadrada no Recurso 2712 - CONFAZ-SEFAZ, Projeto 2080 - CONVENIO CONFAZ.

13. RESPONSÁVEL PELO TERMO DE REFERÊNCIA:

Vinicius Keniti Yano,

Divisão de Infraestrutura e Segurança – DIS/DETIC

De acordo:

NELSON RONCARATI LUZ PESSOA DE SOUZA,

Diretor Substituto do Departamento de Tecnologia da Informação e Comunicação - DETIC

Documento PROA Assinado

Nome do documento: Anexo II - 251400-0004177-9 Termo de Referencia - TR IV.pdf

Documento assinado por	Órgão/Grupo/Matrícula	Data
Vinicius Keniti Yano	SF / DETIC / 467617302	02/07/2025 13:59:20
Nelson Roncarati Luz Pessoa de Souza	SF / DETIC / 293995901	02/07/2025 14:06:41