



Governo do Distrito Federal
Departamento de Estradas de Rodagem do Distrito Federal
Coordenação de Tecnologia da Informação
Gerência de Infraestrutura de Tecnologia da Informação

Nota Informativa n.º 7/2024 - DER-DF/PRESI/CTINF/GITIN

Brasília-DF, 21 de maio de 2024.

Processo: 00113-00004463/2023-87

Pregão: 90011/2024

Objeto: O Registro de preços para fornecimento de equipamento de segurança da informação, tipo firewall NGFW (Next Generation Firewall), com licenciamento para 48 meses, e treinamento.

ANÁLISE DO PEDIDO DE ESCLARECIMENTO DA GLOBAL IP

Em resposta ao E-mail (SEI/GDF 141311806), foi realizada análise do pedido de esclarecimento, a qual gerou as seguintes respostas:

DO PEDIDO DE ESCLARECIMENTO

Questionamento 1:

Referente ao item 13.37 “GERENCIAMENTO DE LOGS” (13.37 À 13.37.18) e o Item 13.38 “CONSOLE DE GERENCIAMENTO CENTRALIZADO” (13.38 à 13.38.30). No edital estes itens acima destacados versam sobre Logs. Em um contexto de Segurança da Informação, o Log é definido na ISO/IEC 27001-22 como:

“Os logs que registram atividades, exceções, falhas e outros eventos relevantes devem ser produzidos, armazenados, protegidos e analisados.”

Temos também uma definição consistente sobre Log de Firewall em um artigo de um Analista de Segurança da Informação (<https://abre.ai/o-que-eh-log>):

4. Logs de Firewalls e Dispositivos de Rede:

Firewalls e dispositivos de rede geram logs que registram tráfego de rede, bloqueios de conexões e tentativas de acesso não autorizado. Analisar esses logs ajuda a identificar padrões de tráfego incomuns e proteger a rede contra ameaças externas.

Outra análise que se faz necessário considera é o o “Marco Civil da Internet” (https://www.planalto.gov.br/ccivil_03/_ato2011-4/2014/lei/l12965.htm) em sua Subseção I “Da Guarda de Registros de Conexão” no seu Artigo 13, temos o seguinte texto:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de **1 (um) ano**, nos termos do regulamento.

Outro análise referência a Norma Governamental “DIRETRIZES PARA O REGISTRO DE EVENTOS, COLETA E PRESERVAÇÃO DE EVIDÊNCIAS DE INCIDENTES DE SEGURANÇA EM REDES” - 21/IN01/DSIC/GSIPR (<https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-21IN01DSICGSIPR.pdf>), em sua página 05, item 6.5 com o seguinte texto:

6.7 Os registros devem ser armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

Vejam, as Normas governamentais que tratam de Segurança da Informação, versam sobre um prazo de armazenamento dos registros (Logs) dos Sistemas de Informação e/ou Sistemas de Segurança da Informação. Isso se deve ao fato de que todas as análises de “Incidente de Segurança” que serão feitas posteriormente, em uma busca investigativa sobre um determinado evento, será pesquisada e efetuada através destes Registros (Logs). Neste sentido, é de extrema importância a DEFINIÇÃO da Quantidade de Espaço de Armazenamento dos registros (Logs), que é calculado com base na Quantidade de Registro Diário de Log gerado pelo Dispositivo de Segurança, neste caso do Firewall e de outros dispositivos, como indica o item 13.37.6 que informa: “13.37.6. Deve possuir API para integração com soluções de terceiros;”, ou seja, se não bem dimensionado, poderá faltar espaço de armazenamento e como consequência não terá Registro de Log armazenado por período indicado por Normas Governamentais. Temos em todo edital o Item 13.37.3 que informa sobre espaço de armazenamento:

13.37.3. Possuir capacidade de no mínimo 128 GB de armazenamento;

Esta informação é extremamente vaga, uma vez que se faz necessário a definição da Quantidade de Registro Diário (Logs) do Firewall e a Quantidade de Dias de Retenção dos Logs no Edital.

Outro fator importante é a possibilidade de realizar Pesquisa Rápida e Avançada nesta “Base de Armazenamento de Logs”, algo que não é referenciado neste Edital. Considerando o “Tempo de Pesquisa” dos eventos, se faz necessário que os dados da “Base de Armazenamento de Logs” tenha INDEXAÇÃO, técnica que agiliza de sobremaneira as buscas avançadas de informações quando é preciso saber sobre um determinado Evento de Segurança da Informação que ocorreu em uma determinada Data, Hora, Endereço IP, Equipamento etc.

Quando consideramos que as Normas Governamentais referenciadas acima versam sobre Quantidade de Dias de Retenção dos Logs para futuras investigações, esta quantidade está entre 6(seis) a 12(doze) meses conforme Normas Governamentais, e sendo o DER um órgão Governamental, deve seguir estas recomendações; quando consideramos que se faz necessário ter uma definição de quantidade de dados armazenados diariamente, para que o DER possa ter um histórico de todo ocorrido em sua Solução de Segurança da Informação por um determinado período de tempo; e quando consideramos que o DER terá um volume de Logs significativo armazenado e que venha necessariamente fazer pesquisas através de sua Solução de Segurança da Informação, e que estas pesquisas possam ser avançadas e necessitem ser extremamente rápidas, se faz necessário que esta Base de Armazenamento de Logs seja INDEXADA. Desta forma entendemos que o DER necessita que o Sistema de Segurança da Informação que será adquirido, tenha capacidade de armazenamento de Logs com no mínimo 128GB de Armazenamento de Log diário, conforme item 13.37.3; que tenha a característica de INDEXAÇÃO dos Logs armazenados, e que possa performar pesquisa na “Base de Armazenamento de Logs” em dados gerados e armazenados com histórico de no mínimo 6(seis) meses, onde a partir deste período ocorrerá o rotacionamento dos dados de forma que os registros mais antigos sejam apagados quando não houver espaço de armazenamento disponível, e também entendemos que esta solicitação não altera de forma nenhuma os valores expressados pelas empresas em suas Propostas Comerciais. Nosso entendimento está correto?

Caso o entendimento do DER seja a não aceitação de nosso questionamento, solicitamos que seja divulgado a Quantidade Mínima de Armazenamento de Log por dia, e o tempo mínimo que estes Logs permaneçam retidos, e desta forma poderemos ser precisos no dimensionamento da solução requerida.

Resposta: Não. O volume de logs gerado diariamente pode variar significativamente de acordo com a solução de gerenciamento de logs escolhida. Essa variabilidade dificulta a determinação prévia de uma quantidade mínima de armazenamento adequada para todas as soluções.

Conforme descrito no item 13.37.2 do Edital, a solução de gerenciamento de logs pode ser implementada em appliance físico ou software. A escolha da plataforma de implementação impacta diretamente nos requisitos de armazenamento, pois appliances físicos geralmente possuem capacidade de armazenamento limitada.

No caso de appliances físicos, a necessidade de hardware com maior capacidade de armazenamento para atender à demanda por logs pode levar a um aumento nos custos do certame sem necessidade.

Para garantir a ampla competitividade entre as soluções ofertadas e evitar custos adicionais desnecessários, a equipe técnica definiu uma quantidade mínima de armazenamento de logs em 128 GB.

Portanto, questionamentos relacionados à definição de uma quantidade mínima pré-determinada de armazenamento de logs não serão aceitos.

QUESTIONAMENTO 2

Referente ao item 13.39.8 “Deverá possuir, no mínimo, 01 (uma) porta de gerenciamento out-of-band”. Caso o equipamento não possua interface dedicada de gerenciamento out-of-band, serão aceitas configurações de instâncias de firewall via software, ou uso da interface dedicada de gerenciamento para contornar a necessidade de tal interface. Está correto nosso entendimento?

Resposta: Não. A porta de gerenciamento out-of-band é crucial para separar as funções de gerenciamento do firewall das funções de processamento de dados. Essa segregação isola e protege o acesso às funções administrativas do firewall, reforçando a segurança do sistema.

A alternativa proposta pela licitante não atende ao requisito de segurança para o gerenciamento do firewall, pois, oferece um nível de proteção inferior à porta out-of-band e, portanto, não será aceita.



Documento assinado eletronicamente por **ELIZEU DE JESUS LOPES - Matr.0221525-X, Gerente de Infraestrutura de Tecnologia da Informação**, em 21/05/2024, às 19:23, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



A autenticidade do documento pode ser conferida no site:
[http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&verificador= 141446886 código CRC= 1BF04583.](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&verificador=141446886&codigo_crc=1BF04583)

"Brasília - Patrimônio Cultural da Humanidade"

SAM Bloco C - Setor Complementares - Ed. Sede do DER/DF - Bairro Asa Norte - CEP 70620.030 - DF

Telefone(s):

Sítio - www.der.df.gov.br