Resposta a Questionamento Nº SEI 0011706/2016 **Em 21/07/2016**

PREGÃO ELETRÔNICO Nº.006/2016

PROCESSOS: SGPR Nº: 0043/2016 / SEI Nº: 00948/2016

Submetidas a questão à consideração da área técnica desta Companhia, esta manifestou-se nos seguintes termos:

1ª Pergunta: Item: 3.2.7. Possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um, N para um e um para N; Pergunta: Entendemos que, para este item, 3.2.7, a solução ofertada deverá suportar no mínimo 32.000 (trinta e dois mil) entradas de ARP e no mínimo 1.500 NATs, está correto o nosso entendimento?

Resposta à 1ª Pergunta: Não está correto, pois não definimos um número mínimo para entradas ARP ou tradução de endereços.

2ª Pergunta: Item 3.2.15. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

Pergunta: Entendemos que a solução apresentada quando composta no esquema ATIVO-PASSIVO deve atender integralmente o item 3.1.1 (Throughput de, no mínimo, 20 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote); não sendo aceito no cenário Ativo-Passivo Throughput menor do que 20 Gbps e com todas as licenças habilitadas para atendimento da solução. Está correto o entendimento?

Resposta à 2ª Pergunta: Sim, está correto o entendimento, desde que observado o atendimento ao item 3.1.2 e demais itens do edital.

3ª Pergunta: Item: 3.4.14. Permitir detecção e ação preventiva contra ataques tipo APT (Advanced Persistent Threat), como ZeroDay e novos malwares ainda sem assinatura, através do monitoramento constante do comportamento do ambiente.

Pergunta: Entendemos que, de acordo com a necessidade de proteção para APT, Dia 0 ou ameaças avançadas, a solução ofertada deverá suportar a análise de arquivos maiores que 1000KB (hum mil Kilo Bytes) para arquivos de PDF e Office, não se limitando a arquivos menores que 45 MB (quarenta e cinco Mega Bytes) para demais tipos de arquivos. Está correto o entendimento?

Resposta à 3ª Pergunta: Não está correto o entendimento, pois a detecção e prevenção de ataques do tipo APT deve ocorrer independente do tipo ou tamanho dos arquivos, através do monitoramento do ambiente.

4ª Pergunta: Item: 3.3. Funcionalidade de Prevenção de Intrusão:

Pergunta: Baseado na necessidade do cliente e performance do ambiente, entendemos que, o IPS deverá, por padrão, deverá efetuar a análise de toda a comunicação, ou seja, não se limitando a apenas a comunicação de entrada nem analisando menos que 300Kb iniciais do pacote, nosso entendimento está correto?

Resposta à 4ª Pergunta: O entendimento está parcialmente correto, pois, conforme o item 3.3.2 "O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;", entende-se que as redes possuem tráfego tanto de entrada, quanto de saída, não devendo haver nenhuma limitação de sentido do tráfego, tão pouco uma quantidade mínima de Bytes a serem analisados.

5ª Pergunta: 05 - Item: 3.10. Gerenciamento Centralizado:

Pergunta: Entendemos que para o produto de gerência e relatório devem possuir uma única interface de um mesmo fabricante, não sendo aceitas composição de terceiros e além disso, entendemos que, dentro dessa proposta, deverá possuir uma solução para os seguintes além de gerenciamento centralizado: SIEM, Relatórios "padrão" e "customizados". Está correto o entendimento?

Resposta à 5ª Pergunta: O entendimento está parcialmente correto, pois, apesar de a gerência e relatórios serem em uma única interface, deve ser observado o item 3.10.4. Não solicitamos o recurso de SIEM. Quanto aos relatórios, o licitante deverá observar o item 3.11 e seus subitens.

6ª Pergunta: Item 3.10.14. Permitir a visualização de logs de histórico dos acessos de tráfegos de rede;

Pergunta: Entendemos que para atendimento deste item a solução ofertada não se limita processar/receber a quantidade de 1(um) GB de log por dia, ou seja, a solução deverá estar licenciada para logs "ilimitados" baseado no escopo da necessidade deste edital. Está correto o entendimento?

Resposta à 6ª Pergunta: O entendimento está parcialmente correto. Os itens 3.10.10 e 3.10.18 descrevem a necessidade de suportar o envio dos logs para outro centralizador justamente para não termos limitações de log. O licenciamento não deve limitar o tamanho do log diário.

7ª Pergunta: Item 3.10.14. Permitir a visualização de logs de histórico dos acessos de tráfegos de rede; Pergunta: Entendemos que para atendimento deste item

a solução ofertada não se limita processar/receber a quantidade de 1(um) GB de log por dia, ou seja, a solução deverá estar licenciada para logs "ilimitados" baseado no escopo da necessidade deste edital. Está correto o entendimento?

Resposta à 7ª Pergunta: Questionamento respondido acima.

Documento assinado eletronicamente por **Maria de Fatima Marchi Brotto**, **Analista Administrativo Pl**, em 21/07/2016, às 17:12, conforme art. 1º, § 7º, da Lei Municipal 8.424/2015 e art. 9º, inciso I do Decreto Municipal 26.136/2015.

A autenticidade do documento pode ser conferida no site http://portalsei.cijun.sp.gov.br/autentica informando o código verificador **0011706** e o código CRC **DDB01B28**.