**PREGÃO ELETRONICO PE.PPSA.003/2022**

**AQUISIÇÃO DE FIREWALL**

(**Atualizado em: 25/07/2022 – Esclarecimento nº 03, Perguntas e Respostas de 01 até 09** )

**Esclarecimento nº 03**

Gostaríamos dos seguintes esclarecimentos referentes ao EDITAL DO PREGÃO ELETRÔNICO Nº 003/2022 – AQUISIÇÃO DE FIREWALL APPLIANCE

**Pergunta nº 01:**

No item 1. Está sendo solicitado o fornecimento de *“Firewall Appliance Serão 2 (dois) equipamentos idênticos de Firewall Appliance (Firewall Next Generation – NGFW) instalados e configurados do data center da PPSA”*como os equipamentos Firewall Appliance solicitados neste edital são compostos por hardware, software e serviços de instalação e suporte, entendemos que em estrita observância à legislação vigente, denota-se que a tributação incidente nos equipamentos (hardware), ICMS, é diferente da aplicada nos serviços (garantia, serviços e softwares), ISS. À vista disso, entendemos que podemos emitir uma nota fiscal para os equipamentos (hardware), outra para os softwares e garantias e outras serviços. Nosso entendimento está correto?

**Resposta nº 01:** O entendimento está correto, os valores devem ser segregados por mercadoria e serviço.

**Pergunta nº 02:**

Não encontramos nenhuma especificação referente a fonte de alimentação dos equipamentos, como estes equipamentos são responsáveis pela segurança da PPSA e são de extrema importância para o funcionamento da empresa, entendemos que será necessário o fornecimento de equipamentos com fontes redundantes. Está correto nosso entendimento?

**Resposta nº 02:** O entendimento está incorreto, fica a critério da proponente oferecer ou não equipamento com fonte redundante.

**Pergunta nº 03:**

O item *“1.1.2 solicita Throughput para proteção de ameaças (Threat prevention) de no mínimo 1.0Gbps”*sem especificar o tipo de tráfego, visto que  muitos fabricantes divulgam diversos números inclusive tráfico do tipo UDP (User Datagram Protocol ) que não reflete a capacidade real de performance em ambiente de produção, e para que a PPSA não faça um investimento em equipamento que não atenda os requisitos mínimos  entendemos que deverá ser comprovado capacidade mínima de *Throughput para proteção de ameaças (Threat prevention) de no mínimo 1.0Gbps* com tráfego HTTP ou blend de protocolos definidos pelo fabricante como misto de aplicações. O nosso entendimento está correto?

**Resposta nº 03:** O equipamento deverá ser capaz de analisar no mínimo 1.0Gbps de dados contra ameaças de um ou mais protocolos ao mesmo tempo, respeitando os itens 3.3.3,3.5.1 e 18.1 do edital

**Pergunta nº 04:**

O item *“1.4 - Controle de Aplicações”*não específica a quantidade mínima de aplicações que devem ser reconhecidas e gerenciadas. Os dispositivos de proteção de rede atuais possuem a capacidade de reconhecer aplicações, independente de porta e protocolo, possibilitando a liberação e bloqueio somente das aplicações necessárias, e que capacidade da solução em controlar aplicações está relacionada a segurança tendo que ter um mínimo de reconhecimento e controle. Portando entendemos que a solução deverá suportar o controle e reconhecimento de pelo menos 3.500 aplicações, número esse solicitado em média em editais públicos de firewalls. Nosso entendimento está correto?

**Resposta nº 04:** Qualquer aplicação deverá ser identificada conforme o item 3.1.4 pelo equipamento, respeitando os itens 3.3.3,3.5.1 e 18.1 do edital

**Pergunta nº 05:**

Não encontramos no Termo de Referência nenhuma referência a Decriptografia SSL, TLS1.1, 1.2, 1.3 e SSH para análise do tráfego criptografado, funcionalidade essencial de de segurança, visto em médio quase 80% do tráfego de usuários para internet e o acesso de usuários externos para servidores em ambiente com WEB é https, somando a isso que se a solução de firewall não tiver essa capacidade, por mais que um ataque seja conhecido o mesmo não será evitado pois estará criptografado! Portanto entendemos que a solução deverá suportar Decriptografia inboud e outbound SSL, TLS1.1, 1.2 e TLS1.3 e SSH, está correto nosso entendimento?

**Resposta nº 05:** O equipamento deverá seguir as premissas do item 3.3.3,3.5.1 e 18.1 do edital.

**Pergunta nº 06**

No item *“1.5 - Filtro URL: “* não encontramos especificação de quantidade mínima de categorias pré-configuradas de filtro de URL. Entendemos que deve existir um número mínimo de categorias, como 60 categorias de URLs. Está correto nosso entendimento?

**Resposta nº 06:** O equipamento deverá possuir as características do item 3.1.5 do edital, respeitando as premissas do item 3.3.3,3.5.1 e 18.1 do edital.

**Pergunta nº 07:**

Não encontramos especificações mínimas para aplicações suportadas em IPV6, visto que muitos serviços da internet e serviços locais de rede já estão sendo fornecidos com esse protocolo entendemos que a solução ofertada deve ser suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação. Está correto nosso entendimento?

**Resposta nº 07:** No que diz respeito ao protocolo IPV6 o equipamento deverá suportar o máximo de sessões conforme item 3.1.1 e também deverá seguir as premissas do item 3.3.3,3.5.1 e 18.1 do edital.

**Pergunta nº 08:**

Não encontramos especificações de capacidade de análises de Malwares modernos em sandbox. Visto que os Malwares hoje em dia serem muito dinâmicos e um antivírus e outros controles comuns e reativos não serem capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta. Entendemos que a solução ofertada deverá suportar a análise de arquivos como pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP em ambiente de sandbox. Nosso entendimento está correto?

**Resposta nº 08:** O equipamento deverá fazer análise de dados de qualquer ameaça incluindo malwares, o método de análise deverá seguir as premissas do item 3.3.3,3.5.1 e 18.1 do edit

**Pergunta nº 09:**

Nos itens “1.1.6” e “1.1.7” informam que os equipamentos devem oferecer portas SFP e SFP+ mas não informa se deverá acompanhar módulos GBICs.Exemplo: Se nas portas SFP precisa ser fornecido GBICs 1000BASE-SX ou 1000BASE-LX/LH, ou então nas portas SFP+ se é preciso fornecer GBICs 10GBASE-SR ou 10GBASE-LR. Como não é solicitado entendemos que não será necessário o fornecimento de GBICs nem cordões ópticos. Nosso entendimento está correto?

**Resposta nº 09:** Os equipamentos **devem** possuir as interfaces conforme item 3.1.1, O fornecimento deverá seguir o item 3.2.4 e respeitando o item 3.3.4 para seu funcionamento adequado.