Processo nº: 3001.0690.2020/DPE-RO
Interessado: Defensoria Pública do Estado de Rondônia
Assunto: Contratação de empresa especializada em locação de infraestrutura para transmissão de dados, de alta capacidade, por radiofrequência e/ou enlace óptico, e fornecimento de link de internet para atender a Defensoria Pública do Estado de Rondônia.

RESPOSTA AO PEDIDO DE ESCLARECIMENTO

Tratam-se de pedidos de esclarecimentos ao Edital do **Pregão Eletrônico nº 024/2020/CPCL/DPE/RO**, feito pelas empresas **TRUE NETWORK IT SOLUTIONS, WEBSECURE CONSULTORIA E SEGURANÇA EM TI e NBS SERVIÇOS DE COMUNICAÇÕES LTDA**, recebidos pelo Pregoeiro tempestivamente. Informamos que em consulta ao departamento técnico de Tecnologia da Informação desta DPE/RO, emitimos as seguintes respostas as perguntas realizadas:

TRUE NETWORK IT SOLUTIONS

ESCLARECIMENTO 1: Conforme subitem 2.1, do "Objeto", que requisita "O presente Termo de Referência visa a contratação de empresa especializada na prestação de serviços de locação de infraestrutura para transmissão de dados de alta capacidade por radiofrequência e/ou enlace óptico, link dedicado do tipo terrestre, para acesso à internet, e solução de controle de tráfego e segurança (firewall de próxima geração - NGFW), para atender a Defensoria Pública do Estado de Rondônia, conforme condições, quantidades e exigências estabelecidas neste instrumento, de acordo com Formulário de Intenção de Aquisição de Bens e Serviços e Estudo Técnico Preliminar, exarados pela Diretoria de Tecnologia da Informação.", entendemos que o termo Solução NGFW deva contemplar respectivamente uma unidade de: firewall NGFW, gerência e sandbox. Está correto o nosso entendimento?

Caso negativo, favor informar quais os itens e suas respectivas quantidades que devem ser contempladas na solução ofertada pela licitante.

RESPOSTA 1: O termo Solução NGFW refere-se a uma unidade de Firewall NGFW, ou seja, apenas uma caixa (box). Os recursos agregados são: gerência, analisador de logs, sandbox e ferramenta SIEM.

ESCLARECIMENTO 2: Conforme subitem 3.6 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "A gerência e registro de logs deverão ser centralizados e apartados dos equipamentos que desempenharão as funcionalidades de proteção e segurança. A gerência poderá ser virtualizada, desde que compatível com as

plataformas de virtualização da VMware ou Nutanix, ou fornecida em hardware do tipo appliance, neste último caso o dispositivo ofertado deverá possuir capacidade de armazenamento de pelo menos 02 (dois) TB e possuir redundância de disco rígido de forma que os mesmos possam ser trocados de forma ininterrupta (hot swappable)", entendemos que:

a) houve flexibilidade na oferta da solução de gerência em modo virtual ou em appliance, que visa ampliar a competitividade, que dentro do conceito de segurança, associado ao contexto de apenas um ambiente/gateway operacional a proteger, esta camada de gerenciamento torna-se um acessório desejável e não obrigatório, facultando assim a oferta de uma camada de gerenciamento dedicada para apenas um ambiente ou gateway, o qual irá contribuir com os princípios de competitividade e economicidade. Está correto o nosso entendimento?

b) houve flexibilidade na oferta da solução de gerência em modo virtual ou em appliance, que visa ampliar a competitividade que para garantia deste princípio, as soluções que funcionarem sem a obrigação de segregação de papéis, serão aceitas abstraindo assim requisitos que tornam este certame menos econômico e competitivo a DPE. Está correto o nosso entendimento?

RESPOSTA 2: a/b) Entendimento incorreto. A gerência e registro de logs são itens obrigatórios, deverão ocorrer de forma centralizada, apartados do NGFW, e poderão ser fornecidos como hardware(appliance), ou software dedicado em ambiente virtualizado, desde que compatível com as plataformas de virtualização VMware ou Nutanix.

ESCLARECIMENTO 3: Conforme subitem 3.8.3 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "Camada 3 (l3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação. Gerar roteamento virtual para pelo menos 120 roteadores virtuais e administração do tráfego entre diferentes áreas de segurança e sub-redes, suportando pelo menos 30 áreas de segurança e um mínimo de 120 sistemas virtuais", entendemos que:

a) A solução ofertada (gateway e suas respectivas funcionalidades, além da gerência segregada do subitem 3.6) deve contemplar a ativação e utilizar o mínimo de 120 sistemas virtuais. Está correto o nosso entendimento?

b) Caso negativo, entendemos que deve ser contemplada a oferta dos 120 sistemas virtuais sem a necessidade de gerenciamento deles na gerência NGFW. Está correto o nosso entendimento?

c) Caso negativo, entendemos que este item se torna desejável e não obrigatório. Está correto o nosso entendimento?

RESPOSTA 3: Correto o entendimento da alternativa “a”.

ESCLARECIMENTO 4: Conforme subitens 3.8.7 e 3.28.5 do item “Solução de controle de tráfego e segurança (NGFW)”, que requisitam respectivamente “O equipamento não deve sofrer degradação de performance de inspeção de Firewall e de controle de aplicação, quando funções de IPS, Antivírus, Anti- Spyware forem habilitadas simultaneamente” e “Suportar pelo menos 2,5 Gbps de throughput de Threat Protection (Firewall, IPS, controle de aplicação e Antivírus e Antispyware)”, entendemos que serão aceitas soluções que atenderem os requisitos de capacidade e throughput deste certame através da funcionalidade de Threat Protection. Está correto o nosso entendimento?

RESPOSTA 4: Entendimento correto.

ESCLARECIMENTO 5: Conforme subitens 3.8.8 e 3.28.5 do item "Solução de controle de tráfego e segurança (NGFW)", que requisitam respectivamente "Quando utilizadas funções de IPS e Antivírus, o equipamento deve entregar a mesma performance (não degradar) entre ter 1 única assinatura de IPS habilitada ou ter todas as assinaturas de IPS e Antivírus habilitadas simultaneamente." e "Suportar pelo menos 2,5 Gbps de throughput de Threat Protection (Firewall, IPS, controle de aplicação e Antivírus e Antispyware).", entendemos que serão aceitas soluções que atenderem os requisitos de capacidade e throughput de Threat Protection neste certame. Está correto o nosso entendimento?

RESPOSTA 5: Entendimento correto.

ESCLARECIMENTO 6: Conforme subitem 3.13.1.12 do item ""Solução de controle de tráfego e segurança (NGFW)"", que requisita ""A solução deve ser capaz de apresentar contagem e percentual de utilização das regras"", entendemos que serão aceitas soluções que permitam a contagem de utilização de regras de outras maneiras com base no volume de dados trafegados pela respectiva regra. Está correto o nosso entendimento?

Caso negativo, entendemos que serão aceitas soluções que permitam a contagem de utilização de regras. Está correto o nosso entendimento?

RESPOSTA 6: A contagem se refere à quantas vezes determinada regra foi utilizada (match) pelo firewall, seja essa regra de liberação ou bloqueio. Também refere-

se ao percentual de utilização da regra dentro do universo total de regras existentes no firewall.

ESCLARECIMENTO 7: Conforme subitem 3.15.17 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "A atualização da base de dados deve ser automática com a opção de ser feita manualmente via TFTP.", entendemos que serão aceitas soluções que permitam a atualização da base de dados de forma automática e manual podendo ser via TFTP ou via outro método. Está correto o nosso entendimento?

RESPOSTA 7: Entendimento correto. A atualização poderá ser feita de forma automática ou manual ou ainda de ambas as formas, via TFTP ou outro método.

ESCLARECIMENTO 8: Conforme subitem 3.20.5 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe, rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm;", entendemos que serão aceitas soluções que implementem o sandbox em arquivos pdf, tar, zip, rar, seven-z, exe e suite Microsoft Office. Está correto o nosso entendimento?

RESPOSTA 8: Entendimento correto.

ESCLARECIMENTO 9: Conforme subitem 3.20.6 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "Deve fazer o bloqueio efetivo do malware desconhecido (Dia Zero) oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que ele seja entregue parcialmente ao cliente.", entendemos que:

a) Entendemos que cada fabricante possui sua tecnologia e abordagem ao tema sandbox, sendo assim, serão aceitas outras tecnologias de prevenção contra malware avançado. Está correto o nosso entendimento?

b) Este requisito torna-se desejável uma vez que o ambiente de mensageria da DPE-RO hoje é hospedado e mantido na estrutura do Google. Está correto o nosso entendimento? Caso negativo, para maior assertividade no dimensionamento e formação de preço, favor informar os respectivos throughputs de tráfego HTTP/HTTPS e SMTP/TLS. (esta afirmação foi embasada na seguinte pesquisa abaixo):

RESPOSTA 9: Parcialmente correto. Cada fabricante possui sim sua abordagem sobre o ambiente “SandBox”, mesmo assim, a solução NGFW deve, obrigatoriamente, ser acompanhada de um ambiente emulado para onde os arquivos são mandados para análise e são executados em diferentes sistemas operacionais. Durante a análise, o arquivo poderá ser entregue parcialmente ao usuário.

ESCLARECIMENTO 10: Conforme subitem 3.20.9 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;", entendemos que solução ofertada deva suportar sistemas operacionais Windows e arquivos Office. Está correto o nosso entendimento? Caso negativo, para o correto dimensionamento e formação de proposta, favor informar os respectivos throughputs de inspeção para cada tipo de versão Windows e Office.

RESPOSTA 10: Entendimento correto. A solução deve suportar sistemas operacionais Windows e arquivos Office.

ESCLARECIMENTO 11: Conforme subitem 3.20.10 e 3.27.21 do item ""Solução de controle de tráfego e segurança (NGFW)"", que requisitam respectivamente ""Esse sistema automático de análise ""In Cloud"" ou local deve prover:"" e ""Permitir a integração e avaliação de todos os equipamentos de proteção de rede na gerência com os seguintes padrões regulatórios: ISO 27001, ISO 27002 e GDPR (base da norma LGPD);, entendemos que solução de Sandbox ""In Cloud"", fere o princípio da LGPD por compartilhar arquivo em ambiente de terceiros, tornando assim facultativo o requisito Sandbox neste certame. Está correto o nosso entendimento?

Caso negativo, favor os respectivos thoughputs que a solução ofertada deve contemplar.

RESPOSTA 11: De acordo com o item 3.20.2, a ferramenta “SandBox” pode ser “In Cloud” ou local. A ferramenta “SandBox” é requisito obrigatório, caso a contratada não possa fornecê-la “In Cloud” poderá fazê-lo localmente. Não há preferência por uma ou por outra, as duas formas serão aceitas. Throughput mínimo: 1Gbps.

ESCLARECIMENTO 12: Conforme subitem 3.20.10.7 do item ""Solução de controle de tráfego e segurança (NGFW)"", que requisita ""Emitir relatório com identificação de quais soluções de Antivírus existentes no mercado teriam ou não condições de bloquear o Malware"", entendemos que este requisito torna-se desejável e não obrigatório principalmente pelo fato de manusear e declarar informações de terceiros que a solução ofertada não possui direitos e nem reponsabilidade de informações

fornecida a ambiente de outros fabricantes diferente da ofertada. Está correto o nosso entendimento?

Caso negativo, favor informar o SLA mínimo permitido para consulta, suporte e garantia da veracidade de informações a serem fornecidas a soluções de fabricantes terceiros.

RESPOSTA 12: Entendimento correto. Requisito desejável.

ESCLARECIMENTO 13: Conforme subitem 3.25.13 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "SSL VPN com suporte a proxy arp e uso de interfaces PPPoE.", entendemos que os recursos de PPOE e Proxy Arp tornam-se desejáveis uma vez que estes requisitos podem ser fornecidos por outra camada, extra SSL-VPN. Está correto o nosso entendimento?

RESPOSTA 13: Entendimento correto. Requisitos desejáveis.

ESCLARECIMENTO 14: Conforme subitem 3.27.21 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "Permitir a integração e avaliação de todos os equipamentos de proteção de rede na gerência com os seguintes padrões regulatórios: ISO 27001, ISO 27002 e GDPR (base da norma LGPD);", entendemos que estes requisitos são desejáveis uma vez que não fora explorado os domínios específicos sendo assim facultativos ou sendo atendidos por outros frameworks de segurança reconhecidos internacionalmente. Está correto o nosso entendimento?

RESPOSTA 14: Entendimento correto. A solução de controle de tráfego e segurança(NGFW) deve permitir a integração e avaliação de equipamentos como switches L2, L3, servidores físicos, roteadores e etc... Os padrões regulatórios deverão ser atendidos conforme couber cada caso.

ESCLARECIMENTO 15: Conforme subitem 3.27.1 do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "Caso a solução possua licenças relacionadas a capacidade de log e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;", fere os princípios de isonomia e economicidade, pois requisitar valores máximos sem precisar a necessidade, acarreta o decréscimo de competitividade, sendo assim, entendemos que serão aceitas soluções que armazenem pelo menos 5 GB de logs por dia. Está correto o nosso entendimento?

RESPOSTA 15: Entendimento correto. Serão aceitas soluções que armazenem, no mínimo, 5GB de logs diário.

ESCLARECIMENTO 16: Conforme subitem 3.28.2 do item “Solução de controle de tráfego e segurança (NGFW)”, que requisita "Suportar pelo menos 20 Gbps de throughput para Firewall", entendemos que soluções que possuírem o referido throughput sob a métrica de produção/empresariais, os mesmos deverão ser considerados. Está correto o nosso entendimento?

RESPOSTA 16: Não conseguimos interpretar o pedido de esclarecimento, ficando prejudicado à análise.

ESCLARECIMENTO 17: Conforme subitem 3.28.14, do item "Solução de controle de tráfego e segurança (NGFW)", que requisita "Suporte a fontes "Swappable" AC/DC", entendemos que serão aceitas soluções que possuírem fontes redundantes, garantindo assim, a continuidade do equipamento. Está correto o nosso entendimento?

RESPOSTA 17: Entendimento correto. A solução deve possuir fonte redundante.

ESCLARECIMENTO 18: Entendemos que todos os fornecedores do GARTNER em todos os quadrantes poderiam participar do certame. É correto o nosso entendimento?

RESPOSTA 18: Entendimento incorreto. Apenas os equipamentos que constarem no quadrante de líderes (leaders), de preferência, ou no quadrante de desafiantes (challengers) do GARTNER, serão aceitos.

ESCLARECIMENTO 19: Esta empresa vem, respeitosamente, em virtude dos reflexos da pandemia, solicitar a prorrogação da data de realização do pregão 024/2020 por 15 dias, tendo em vista a demora e dificuldade de prováveis fornecedores em apresentar suas propostas de custos, especificações e disponibilidade de entregáveis.

Adicionalmente, em virtude da complexidade do termo de referência, se fazem imprescindíveis os esclarecimentos de dúvidas técnicas, as quais são necessárias para possibilitar a apresentação de proposta.

RESPOSTA 19: O certame licitatório deverá continuar de acordo com a data anteriormente agendada, pois a empresa não trouxe argumentos técnicos que possibilitasse o prejuízo da sua realização. Trata-se de um objeto que é de conhecimento prévio da referida empresa, pois participou de cotações. Ainda, o edital ficou disponível aos licitantes a partir de 25/11/2020, sendo que sua abertura ocorrerá em 11/12/2020, ou seja, 17 (dezessete) dias corridos entre a disponibilização e abertura.

WEBSECURE CONSULTORIA E SEGURANÇA EM TI

ESCLARECIMENTO 1: Segundo o subitem “3.2.” da JUSTIFICATIVA

“No cenário atual, é crescente a demanda pela disponibilização online de serviços com alta disponibilidade, confiabilidade e tolerância a falhas. Nesse ambiente de missão crítica, são necessários mecanismos que melhorem a eficiência dessa infraestrutura, reduzindo custos e simplificando o gerenciamento destes ativos. Estes mecanismos aprimoram a operação da infraestrutura, reduzindo o tempo de interrupção e consequentemente melhorando os níveis de serviço", do item 3.2.”

Entendemos que a Solução NGFW deverá ser ofertada em uma “única unidade”, conforme informado no Item 3 da tabela de Especificações, mesmo a justificativa dissertando sobre alta disponibilidade. Está correto o nosso entendimento?

Caso estejamos equivocados, solicitamos informar quais as respectivas quantidades para os papéis e funcionalidades ora requisitados.

RESPOSTA 1: A solução NGFW refere-se a somente um equipamento de Firewall-NGFW, ou seja, apenas uma caixa (box).

ESCLARECIMENTO 2: Conforme subitem “3.8.3”

“Camada 3 (l3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação. Gerar roteamento virtual para pelo menos 120 roteadores virtuais e administração do tráfego entre diferentes áreas de segurança e sub-redes, suportando pelo menos 30 áreas de segurança e um mínimo de 120 sistemas virtuais;"

Do item " Solução de controle de tráfego e segurança (NGFW) ",entendemos que os roteadores virtuais não são integrados ao Firewall, e sim uma particularidade da rede do Cliente, assim o Firewall irá administrar essas redes advindas desses roteadores, sendo responsável pela segurança do tráfego das áreas de Segurança e das redes dos Sistemas Virtuais. Está correto o nosso entendimento?

Caso estejamos equivocados, solicitamos informar se a solução ofertada deva suportar para ativação em aquisição futura pelo menos 120 sistemas virtuais. Está correto o nosso 2º entendimento?

RESPOSTA 2: Entendimento correto.

ESCLARECIMENTO 3: Conforme subitens “3.20.5.””3.20.6.”

"3.20.5. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe, rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm;"

"3.20.6. Deve fazer o bloqueio efetivo do malware desconhecido (Dia Zero) oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente."

Do item “ Solução de controle de tráfego e segurança (NGFW) ”, entendemos que para o pleno atendimento deste item, existem requisitos que devem ser obrigatoriamente ser atendidos, pois os arquivos com suas respectivas extensões, serão descarregados das conexões do NGFW os quais serão totalmente enviados para o ambiente de sandbox podendo ser inloco na DPE-RO ou no site do fabricante, lembrando que caso algum arquivo seja malicioso, para haver o bloqueio sem que o mesmo seja entregue parcialmente ao cliente, todas as conexões que dependerem de inspeção sandbox, ficarão em estado de ""on hold/idle"" na tabela de estado do NGFW até que o ambiente de sandbox envie o veredito para o NGFW, onde caso contadores de sessão sejam excedidos, as respectivas conexões que originaram os respectivos, por terem que inspecionar totalmente antes de entregar ao cliente, serão finalizadas sem a passagem do arquivo retornando ao mesmos mensagens de erros comum de conectividade. Em busca de maior assertividade e oferta que atenda efetivamente em ambiente de produção, composto por diversas conexões e arquivos, para o pleno atendimento deste item, entendemos que:

Torna-se desejável e não obrigatório a inspeção total antes de entrega ao cliente, permitindo desta forma a entrega parcial ou ação similar. Está correto o nosso entendimento?

Caso negativo, para formação de proposta e valores, solicitamos informar:

a. Para o ambiente HTTP:

I. Qual a quantidade de usuários que utilizarão a funcionalidade;

II. Qual o throughput de tráfego HTTP, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;

III. Tamanho máximo de arquivos a serem enviados a inspeção, iv. qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

b. Para o ambiente HTTPS:

I. Qual a quantidade de usuários que utilizarão a funcionalidade;

II. Qual o throughput de tráfego HTTPS, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;

III. tamanho máximo de arquivos a serem enviados a inspeção;

IV. Qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

c. Para o ambiente SMTP via MTA:

I. Qual a quantidade de usuários que utilizarão a funcionalidade;

II. Qual o throughput de tráfego SMTP, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;

III. tamanho máximo de arquivos a serem enviados a inspeção;

IV. Qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

d. Para o ambiente SMTPS (tls) via MTA:

I. Qual a quantidade de usuários que utilizarão a funcionalidade;

II. Qual o throughput de tráfego SMTPS, quais os sistemas operacionais devem obrigatoriamente inspecionar simultaneamente em série os respectivos arquivos;

III. Tamanho máximo de arquivos a serem enviados a inspeção;

IV. Qual a banda mínima dedicada para a comunicação do NGFW ao ambiente de sandbox para o efetivo processamento.

e. Qual o ttl de sessão máximo permitido no NGFW que fará o hold das sessões até o pleno processamento dos arquivos em sandbox.

f. Caso ocorra erros de inspeção em sandbox, para conexões oriundas de comunicações HTTP e HTTPS, será permitido o envio de mensagens de erro aos navegadores dos clientes?

g. Caso ocorra erros de inspeção em sandbox, para conexões oriundas de comunicações SMTP e SMTPS(TLS), qual o período máximo permitido para o pleno processamento em sandbox?

RESPOSTA 3: Entendimento correto. O bloqueio total do arquivo é desejável durante sua análise no ambiente “SandBox”, mas pode ser entregue parcialmente ao usuário enquanto isso ocorre.

ESCLARECIMENTO 4: Conforme subitem “3.20.9.”

“A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;”

Do item " Solução de controle de tráfego e segurança (NGFW) ", entendemos que solução ofertada deva suportar sistemas operacionais Windows e arquivos Office. Está correto o nosso entendimento?

Caso negativo, para o correto dimensionamento e formação de proposta, favor informar os respectivos throughputs de inspeção para cada tipo de versão Windows e Office.

RESPOSTA 4: Entendimento correto. A solução ofertada(NGFW) deve suportar sistemas operacionais Windows e arquivos Office.

ESCLARECIMENTO 5: Conforme subitem “3.20.10.”

“Esse sistema automático de análise "In Cloud" ou local deve prover:" do item " Solução de controle de tráfego e segurança (NGFW) ", entendemos que para a solução ofertada contemplando análise "In Cloud", todos os requisitos relacionados a sandbox tornam-se desejáveis e não obrigatórios por necessitar de comunicação direta com o ambiente de sandbox do fabricante. Está correto o nosso entendimento?

RESPOSTA 5: Entendimento incorreto. Os requisitos, do ambiente “SandBox”, são obrigatórios. Ou a análise “In Cloud” ou a análise local deve prover as informações exigidas no item 3.20.10 e em seus subitens.

ESCLARECIMENTO 6: Conforme subitem “3.20.10.9.”

"O sistema de detecção de Malware moderno deve possuir SLA de até 1 hora para finalização da análise e definição de resultado do arquivo analisado." do item " Solução de controle de tráfego e segurança (NGFW) ", entendemos que este requisito torna-se desejável e não requerido devido os diversos fatores que entram colisão com a funcionalidade de sandbox ora requisitadas neste certame. Está correto o nosso entendimento?

Caso contrário, favor informar qual a banda e condições de saúde de link de internet que serão garantidos até o data center do fabricante que hospedará o ambiente de sandbox para análise e definição de resultado.

RESPOSTA 6: Entendimento correto. O requisito é desejável.

ESCLARECIMENTO 7: Conforme subitem “3.25.11.”

"Deverá contar com um software cliente de VPN-SSL para os sistemas operacionais Windows SP, Vista (32 e 64 bits), Windows 7 (32 e 64 bits) e Windows 10 (32 e 64 bits).”" do item "" Solução de controle de tráfego e segurança (NGFW) ", entendemos que os requisitos de sistemas operacionais pré Windows 7 tornam-se desejáveis e não obrigatórios devido descontinuidade de suporte pela própria Microsoft. Está correto o nosso entendimento?

Caso negativo entendemos que a DPE-RO assumirá o risco do suporte conforme site da Microsoft na seguinte url https://support.microsoft.com/pt-br/windows/o-suporte-ao-windows-xp-terminou-47b944b8-f4d3-82f2-9acc-21c79ee6ef5e , assumindo assim a responsabilidade de todas as funcionalidades que se relacionarem, eximindo assim a licitante de obrigações editalícias e contratuais. Está correto o nosso entendimento?

RESPOSTA 7: Entendimento correto. O requisito é desejável.

ESCLARECIMENTO 8: Conforme subitem “3.27.21.”

“Permitir a integração e avaliação de todos os equipamentos de proteção de rede na gerência com os seguintes padrões regulatórios: ISO 27001, ISO 27002 e GDPR (base da norma LGPD);"

Do item " Solução de controle de tráfego e segurança (NGFW) " entendemos que estes requisitos podem ser atendidos por outras metodologias ou normas de segurança mundialmente reconhecidas. Está correto o nosso entendimento?

Caso negativo, sendo este um Órgão zelador das Leis, sendo uma delas até citada acima a “LGPD”, favor informar as obrigatoriedades de requisitos que devam ser atendidas segundo as respectivas normas ora requisitadas.

RESPOSTA 8: Entendimento correto. A solução de controle de tráfego e segurança(NGFW) deve permitir a integração e avaliação de equipamentos como

switches L2, L3, servidores físicos, roteadores e etc... Os padrões regulatórios deverão ser atendidos conforme couber a cada caso.

ESCLARECIMENTO 9: Conforme subitem “3.27.1.”

Caso a solução possua licenças relacionadas a capacidade de log e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;", entendemos serão aceitas soluções com capacidade do Tipo VM (VMware ou Nutanix) onde a quantidade de Log estará restrita à capacidade de Hardware que o Cliente disponibilizará para este fim. Está correto o nosso entendimento?

Caso contrário favor informar capacidade de Hardware será disponibilizará para este fim.

RESPOSTA 9: Parcialmente correto. O limite de armazenamento está atrelado à capacidade de hardware do cliente, porém a capacidade de logs diário deve ser de, no mínimo, 5GB/dia.

NBS SERVIÇOS DE COMUNICAÇÕES LTDA

ESCLARECIMENTO 1: “1.6 Todos os equipamentos da Contratada a serem instalados nas dependências do DPE-RO deverão ser protegidos por sistemas secundários de energia elétrica compostos por retificadores ligados a bancos de baterias com autonomia mínima de 8 horas, além de para-raios, cabos e sistemas de aterramento nas localidades onde não existir malha de terra ou para-raios adequados;”

Entendemos que a necessidade solicitada é de “autonomia mínima de 8 horas” sendo então aceito para esse Item Nobreak que atenda essa autonomia, ou mesmo equipamentos com fonte alternada que aceite sua conexão diretamente em bateria estacionária. Está correto nosso entendimento?

RESPOSTA 1: Entendimento correto.

ESCLARECIMENTO 2: “1.3. Conectividade”
“Possuir, no mínimo, 2 portas Gigabit Ethernet 1000BaseT, com conectores SFP, suportando a instalação de GBICs para Ethernet1000Base-X.”

Verifica-se que o ponto é relativo aos CE’s das localidades remotas, sendo as mesmas solicitadas velocidade de 50mbps de Rede Privada, para o atendimento à essa velocidade um Roteador com portas de 100Mbps teria essa capacidade de

atendimento, mas temos consciência que equipamentos modernos já entregam portas Gigabit, desse modo uma porta Copper (elétrica ou RJ45) atenderia a demanda, mesmo tendo um UPGRADE de 200% da Velocidade inicial.

Desse modo entendemos que a solicitação foi superdimensionada, e entendemos que um Roteador que tenha no mínimo " 2 portas Gigabit Ethernet 1000BaseT", sendo que uma dessa portas seja compatível com conectores SFP, atende a demanda do Órgão, sendo assim atendida a necessidade do Órgão, levando desempenho, qualidade e economicidade ao Órgão. Está correto nosso entendimento?

RESPOSTA 2: Entendimento correto.

ESCLARECIMENTO 3: "1.17 Todos os roteadores da rede DPERO-WAN devem ser do mesmo fabricante e deverão disponibilizar os recursos mínimos explicitados neste termo. A determinação do mesmo fabricante para todos os roteadores visa otimizar e simplificar procedimentos de configuração, gestão, operação, monitoramento, resolução de problemas e principalmente garantir a compatibilidade entre eles;"

Verifica-se nesse ponto um vício que pode elevar o preço dos equipamentos a serem entregues, sendo que cada Fornecedor foca mais em uma linha de equipamento, na maioria das vezes as empresas têm linhas de atendimento para Grandes empresas, e não tem equipamentos para atendimento à pequenas empresas. Ex.: Cisco, Huawey.

Sendo dessa maneira viável a abertura para entrega de no máximo 02 fabricantes, para assim o atendimento no Concentrador ser um Fabricante e os CE's das localidades remotas de outros Fabricantes. Está correto nosso entendimento?

RESPOSTA 3: Entendimento incorreto. Todos os roteadores da rede DPERO-WAN devem ser do mesmo fabricante.

ESCLARECIMENTO 4: "1.11. Sistema operacional"
"O sistema operacional dos roteadores deve ser modular, com a clara separação entre plano de controle e de encaminhamento (forwarding). Deve ser fornecido com a última versão do sistema operacional disponível."

É incomum a solicitação acima ser definida para roteadores CE's instalados em localidades remotas, sendo as funcionalidades solicitadas de Softwares e Sistemas de grande porte, fazendo assim com que o custo do atendimento seja mais elevado.

Desde que a separação do Dataplane (plano de controle) e encaminhamento (forwarding), forem aceitos em roteadores que façam essas tarefas baseadas em

Software, onde a arquitetura do Hardware seja de único processador sem definição dessas tarefas por Hardware dedicado, esse custo tende à diminuir. Está correto nosso entendimento?

RESPOSTA 4: Entendimento correto.

Diante do exposto, informamos que não serão necessárias alterações no instrumento convocatório, e será mantida a data da abertura do certame para o dia 11/12/2020.

Porto Velho - RO, 10 de dezembro de 2020.

Luan Hortiz Campos
Pregoeiro da CPCL/DPE/RO

LUAN HORTIZ CAMPOS: 00435028227

Assinado digitalmente por LUAN HORTIZ CAMPOS:00435028227
DN: C=BR, O=ICP-Brasil, OU=Autoridade Certificadora Raiz Brasileira v2, OU=AC SOLUTI, OU=AC SOLUTI Multipla, OU=Certificado PF A3, CN=LUAN HORTIZ CAMPOS: 00435028227
Razão: Eu sou o autor deste documento
Localização: sua localização de assinatura aqui
Data: 2020-12-10 10:30:56
Foxit Reader Versão: 9.7.1