Amanda da Solidade Silva

De: Amanda da Solidade Silva em nome de Comissão Permanente de Licitação
Enviado em: terça-feira, 15 de dezembro de 2020 17:41
Para: 'karla.oliveira@yssy.com.br'
Assunto: ENC: [Pregão 17/2020 - FUNASA] Pedido de Esclarecimentos

Senhor licitante,

Segue resposta ao pedido de questionamento referente ao Pregão 17/2020.

Atenciosamente,
Amanda
CPL

De: Marcelo Dias de Sá **Em nome de** CGMTI
Enviada em: terça-feira, 15 de dezembro de 2020 14:10
Para: Comissão Permanente de Licitação <cpl@funasa.gov.br>; CGMTI <cgmti.assessoria@funasa.gov.br>; Darlan Henrique da Silva Venturelli <darlan.venturelli@funasa.gov.br>; Túlio César de Araújo Porto <tulio.porto@funasa.gov.br>
Assunto: RES: [Pregão 17/2020 - FUNASA] Pedido de Esclarecimentos

Boa tarde,

Prezada CPL, segue abaixo as respostas dos questionamentos da empresa Yssy.

Esclarecimento 1
4.6. **Capacidades e e quantidades**
4.6.1. Suportar no mínimo o throughput de 17 Gbps com a funcionalidade de controle de aplicação habilitada;
Questionamento: Cada fabricante utiliza as devidas métricas seguindo as boas práticas, mas a forma como é exposto no datasheet é diferente para cada vendor. A solução que será ofertada em seu datasheet faz a seguinte exposição do Throughput com base nas funcionalidades de FW (Firewall) e Controle de Aplicações habilitadas simultaneamente resultando em um valor de Throughput final de 27Gbps, sendo superior ao solicitado então acreditamos que atendemos ao item 4.6.1. Nosso entendimento está correto?
Resposta 01: O entendimento está correto.

Esclarecimento 2
4.6.2. Throughput NGFW de, no mínimo, **9 (nove) Gbps**, com as funcionalidades de firewall, controle de aplicação, filtro URL, IPS e anti-malware habilitadas e atuantes;
Questionamento: Cada fabricante utiliza as devidas métricas seguindo as boas práticas, mas a forma como é exposto no datasheet é diferente para cada vendor. A solução que será ofertada em seu datasheet faz a seguinte exposição do Throughput com base nas funcionalidades de FW (Firewall), Controle de Aplicações e IPS habilitadas simultaneamente resultando em um valor de Throughput final de 27Gbps, como pode observar a queda de desempenho da solução ofertada é mínima por isso não há uma exposição exclusiva no datasheet para o throughput especifico para URL, anti-malware por já considerar na métrica relatada acima (FW+APL+IPS) e por ser superior ao solicitado então acreditamos que atendemos ao item 4.6.2. Nosso entendimento está correto?
Resposta 02: Não está correto o entendimento. Deve ser comprovado o throughput com as funcionalidades habilitadas e atuantes simultaneamente.

Esclarecimento 3
4.6.3. Thoughput de IPS de, no mínimo, 10 (dez) Gbps;
Questionamento: Cada fabricante utiliza as devidas métricas seguindo as boas práticas, mas a forma como é exposto no datasheet é diferente para cada vendor. A solução que será ofertada em seu datasheet faz a seguinte exposição do Throughput com base nas funcionalidades de FW (Firewall), Controle de Aplicações e IPS habilitadas simultaneamente

resultando em um valor de Throughput final de 26Gbps, sendo superior ao solicitado então acreditamos que atendemos ao item 4.6.1. Nosso entendimento está correto?
Resposta 03: Deverá ser comprovado através de informações públicas do fabricante a capacidade solicitada de throughput de IPS de no mínimo 10 (dez) Gbps.

Esclarecimento 4
4.6.3.4. Quando as funcionalidades de controle de aplicação, IPS, antivírus e antispyware tiverem habilitadas de forma simultânea, o tráfego deverá ser inspecionado de modo bidirecional com inspeção em toda a sessão do pacote, sem qualquer utilização de recurso de by-pass;
Questionamento: Ao que se refere que o tráfego deverá ser inspecionado de modo bidirecional com inspeção em toda a sessão do pacote, sem qualquer utilização de recurso de by-pass, entendemos que deverá ser realizado a analise tanto da origem quanto de destino utilizando as funcionalidades citadas, com o intuito de não dar um by-pass para que a segurança não seja comprometida.
Resposta 04: A descrição do item deixa claro que todo o tráfego deverá ser inspecionado pela solução independentemente do sentido do tráfego.

Esclarecimento 5
4.6.6. Armazenamento de, no mínimo, 240 GB SSD em RAID 1 dedicados ao sistema operacional
e operacionalização da solução e no mínimo 240 GB para armazenamento de log.;
Questionamento: A solução atual do da FUNASA trabalha com RAID 1 utilizando 2 (dois) SSD de 240GB totalizando 480GB, existem algumas desvantagens ao utilizar RAID 1 uma delas é que a capacidade efetiva de armazenamento cairá pela metade com relação a capacidade total de cada unidade, pois os dados são gravados duas vezes resultando em 120GB para cada unidade totalizando 240GB e em alguns casos poderá dificultar a troca deste hardware estando ligado (Hot-swappable).

A solução a ser ofertada não utiliza RAID 1 e possui armazenamento de 400GB, sendo superior ao que órgão possui atualmente, portanto atendendo ao item 4.6.6. Nosso entendimento está correto?

Resposta: 05: Não está correto. A solução deve suportar RAID 1 para garantir alta disponibilidade de armazenamento.

Esclarecimento 6
4.6.7. No mínimo, 08 (oito) interfaces de rede de 1GbE;
Questionamento: No item 4.6.7 onde é requisitado 8 (oito) interfaces de rede de 1GE acreditamos que esteja sendo solicitado 8 interfaces 1GbE SFP (fibra). Nosso entendimento está correto?
Resposta 06: Não está correto. O item solicita interfaces 1GbE independentemente do meio de conexão.

Esclarecimento 7
4.7.6.11. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, WEB, alterações de política e comunicação SNMP;
Questionamento: No item 4.7.6.11 entendemos que pelo referido termo WEB seja HTTP/HTTPS. Está correto o nosso entendimento?
Resposta 07: A solução deve suportar HTTP ou HTTPS no que se refere a WEB.

Esclarecimento 8
4.7.6.13. O Firewall deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);
Questionamento: Gostaria de confirmar se nosso raciocínio está correto sobre o modo Sniffer que é solicitado seria este trecho. Uma interface "Passiva", seja no modo roteado ou transparente, tem a capacidade de monitorar os arquivos encaminhados a ela por meio de uma porta Span ou um TAP de rede, portanto, recebe uma cópia do tráfego, mesmo que o tráfego não esteja passando pelo firewall. Correto, embora possamos fornecer captura / detecção de pacotes em qualquer uma de nossas interfaces físicas, o que é algo diferente. Ao que se refere como capacidade de operar de forma simultânea mediante ao uso de interfaces físicas utilizando os modos transparente, sniffer e roteado simultaneamente se trata de funcionalidades especificas da solução atual da Funasa. A solução a ser ofertada pode ser configurada nos modos transparentes, roteados ou passivos "Sniffer" mas acreditamos que talvez não faça sentido o firewall trabalhar como transparente e ao mesmo tempo "simultaneamente"roteado. Nosso entendimento está correto?
Resposta 08: Resposta 8: Não está correto. Os três modos devem ser suportados simultaneamente.

Esclarecimento 9
4.8.16.7. Suportar a criação de categorias de URLs customizadas;
Questionamento: Essa funcionalidade é especifica da solução atual da FUNASA, a solução a ser ofertada possui inteligência própria que faz automaticamente essa função de criação de categorias de URL sem ser necessário criação manual através do administrador, com base nisso acreditamos que atendemos o item 4.8.16.7. Nosso entendimento está correto?
Resposta 09: Resposta 9: Não está correto. A equipe técnica da FUNASA deve ter a opção de criar suas categorias de URL customizadas.

Esclarecimento 10
4.9.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
Questionamentos: No item 4.6.15. é solicitado "Deve ser entregue solução em alta disponibilidade com no mínimo 02 (dois) equipamentos operando em cluster ativo/passivo ou ativo/ativo" pelo fato da alta disponibilidade ter sido flexibilizada com a condição (ou) acreditamos no item 4.9.3 que se refere a sincronização que também faz parte do (HA) high availability também deveria estar como condição (ou) "ativo/ativo ou ativo/passivo" e não (e). Nosso entendimento está correto?
Resposta 10: O entendimento está correto.

Esclarecimento 11
4.9.11. Deve suportar referência cruzada com CVE;
Questionamento: Referência cruzada entendemos que seja uma relação ou vínculo semântico que se estabelece entre duas ou mais informações ou entre documentos. Pelo que analisamos com a solução atual da FUNASA essa relação/vinculo se dá em caso de vulnerabilidades por parte da solução ofertada em si, é divulgado os detalhes através do CVE, gostaríamos de saber se é essa a referência cruzada esperada pelo órgão e se nosso entendimento está correto?
Resposta 11: A solução deve conter informações do CVE disponibilizadas para os administradores da solução.
Esclarecimento 12:
4.9.13. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
Questionamento: A solução a ser ofertada faz a captura de pacote de todo o trafego que queira ser analisado, não se limita apenas assinatura de IPS e Anti-Malware então acreditamos que atendemos ao item 4.9.13. Nosso entendimento está correto?
Resposta 12: A solução deve permitir que seja realizada a captura de pacotes para as funcionalidades de IPS e Anti-Malware.
Esclarecimento 13
4.9.20.1.3 Seja possível configurar que em caso de falta de conectividade com a nuvem, a experiência do usuário não seja afetada;
Questionamentos: Poderá ser apresentado uma carta ou e-mail do fabricante comprovando o atendimento do item 4.9.20.1.3 ?
Resposta 13: Será aceito carta do fabricante.
Esclarecimento 14
4.9.24. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;
Questionamentos: Por não se tratar de uma solução de MTA **"Mail Transfer Agent"**e sim de **NGFW** é incomum a solicitação de análise de anexos de e-mail, mas a solução a ser ofertada possui a opção de submeter amostra de "Email messages extensões (.eml)" para análise de malwares de dia zero, acreditamos que com isso atendemos ao item 4.9.24. Nosso entendimento está correto?
Resposta 14: O entendimento está correto.

Esclarecimento 15
4.9.29. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;
4.9.30. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio, no mínimo, dos seguintes tipos de arquivos caso tenham malware desconhecido: analise em arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java, RAR e ZIP no ambiente de sandbox;
Questionamento: A solução a ser ofertada possui a capacidade de análise das extensões solicitadas e não se restringindo a essas, mas exatamente a extensão RAR não é suportado, mas existem outras que podem substituídas como por exemplo: 7z, gzip e ZIP então como base nisso acreditamos que atendemos ao item 4.9.30. Nosso entendimento está correto?
Resposta 15: Não está correto o entendimento. A extensão RAR é muito utilizada e precisa ser analisada para proteção de dia-zero.

Esclarecimento 16
4.11. O QoS deve possibilitar a definição de classes por:
4.11.1. Banda garantida, banda máxima e fila de prioridade;
4.11.2. Disponibilizar estatísticas RealTime para classes de QoS;
Questionamento: No item 4.11 e seus subitens ao que se refere a QoS, serão aceitas soluções que façam a análise de Qos por Limite de tráfego seja por origem, destino, aplicações, url e usuários. Esta correto o nosso entendimento?
Resposta 16: O entendimento está correto.

Esclarecimento 17
4.13.36. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;
Questionamento: Esses relatórios regulamentares seriam relatórios com a visão de detecção e bloqueio por meio de políticas de segurança em tempo real. Nosso entendimento está correto?
Resposta 17: O entendimento está incorreto.
Esclarecimento 18
4.14.1. Todos os componentes de software e/ou firmware da solução deverão ser fornecidos com licença de uso em caráter permanente, ou seja, o valor pago referente ao licenciamento deverá permitir a utilização por tempo indeterminado da última versão disponível na data do encerramento dos serviços de garantia, assistência técnica e atualização de versões, com exceção dos serviços baseados em assinatura, que por sua vez não realizará atualização após a data de encerramento da garantia;
4.14.2. Licenças com direito de atualização dos softwares envolvidos na solução quando:
4.14.3. Novas versões, revisões, distribuições (release), correções (patches) dos programas e assinaturas forem Disponibilizadas;
4.14.4. Houver lançamento de novos softwares em substituição aos fornecidos;
4.14.5. Ficar caracterizada descontinuidade dos softwares fornecidos;
Questionamentos: Entendemos que por caráter permanente se dá ao ato de fazer a aquisição de hardware e software como por exemplo NGFW que mesmo após o período de contrato de 60 meses, ainda estará funcionando mesmo que sem atualizações, sem suporte por que o contrato de suporte já expirou, já o que se refere as licenças que possuem uso especifico como Malware e URL após o tempo de licença adquirido parará de fazer os filtros para os mesmos e a sobre a funcionalidade de IPS não perderá a base de assinaturas mas não terá atualizações por não ter mais um período de licenciamento ativo. Levando em consideração todos esses pontos entendemos que atendemos aos itens 4.14.1, 4.14.2, 4.14.3, 4.14.4 e 4.14.5. Está correto nosso entendimento?
Resposta 18: O entendimento está correto.

Esclarecimento 19
4.15.3. Caberá à CONTRATADA prover todos os recursos didáticos necessários à realização do treinamento, incluindo (mas não se restringindo a) sala de aula, data show, apostilas, bloco de anotações e caneta para cada treinando;
4.19.1. A solução deverá ser implantada, em sua totalidade, em até 90 (noventa) dias após a emissão da Ordem de Serviço, com vistas a não ocasionar a descontinuidade dos serviços em produção na Funasa, conforme tabela abaixo
Questionamento: 90 dias uteis ou corridos ?
Resposta 19: 90 dias corrido.
Esclarecimento 20
4.15. REQUISITOS DE CAPACITAÇÃO - Treinamento Técnico
Questionamento: É solicitado quantidade 5 para treinamento o órgão se refere a treinamento para uma turma de 5 pessoas, está correto nosso entendimento?
Resposta 20: O entendimento está correto.

Esclarecimento 21
4.19.2.1. FASE 1 – Planejamento da instalação:
Questionamento: Poderá ser remoto e/ou presencial.
Resposta 21: Entendimento correto. Devido a atual situação de pandemia, o planejamento poderá ser remoto e/ou presencial.
Esclarecimento 22
4.19.2.11. FASE 3 – Instalação e configuração da Solução
Questionamento: Poderá ser feita remota e/ou presencial.
Resposta 22: A instalação e configuração deverá ser realizar in loco.

Esclarecimento 23
4.19.2.12. FASE 4 – Entrega da documentação:
Questionamento: Poderá ser feita remota e/ou presencial.
Resposta 23: entendimento correto.
Esclarecimento 24
7.1. O objeto licitado deverá ser entregue e instalado pelo próprio fornecedor ou por técnico (s) da empresa fornecedora;
Questionamento: Ao que é referenciado como técnico da empresa fornecedora, subentendemos que se trata de técnicos da própria contrata, o nosso entendimento está correto?
Resposta 24: Entendimento correto.

Esclarecimento 25
Questionamento: Qual a quantidade de sessões simultâneos, usuários e endpoints que passarão pelas políticas de acesso com base no usuário?
Resposta 24: 3.560 Endpoint e em média 4.000 usuários.
Resposta 25:
Esclarecimento 26
Questionamento: Qual a quantidade de usuários que utilizarão a solução de VPN Remote Acess (Client-to-site)?
Resposta 26: 1.000 (mil) usuários.

Atenciosamente,

Marcelo Sá
Coordenador de Infraestrutura de TI
Contato: 3314 6417
À Serviço da COINT
COINT/CGMTI/DEADM

De: Adalberto Caetano Lopes **Em nome de** Comissão Permanente de Licitação
Enviada em: terça-feira, 15 de dezembro de 2020 07:06
Para: CGMTI <cgmti.assessoria@funasa.gov.br>; Darlan Henrique da Silva Venturelli <darlan.venturelli@funasa.gov.br>; Marcelo Dias de Sá <marcelo.d.sa@funasa.gov.br>; Túlio César de Araújo Porto <tulio.porto@funasa.gov.br>
Assunto: ENC: [Pregão 17/2020 - FUNASA] Pedido de Esclarecimentos

Bom dia Senhores,
Segue pedido de esclarecimento.

Adalberto Caetano Lopes
CPL

De: Karla Oliveira [mailto:karla.oliveira@yssy.com.br]
Enviada em: segunda-feira, 14 de dezembro de 2020 21:32
Para: Comissão Permanente de Licitação <cpl@funasa.gov.br>
Cc: Hiroshi Liberal Ferreira Kanegae <hiroshi.kanegae@yssy.com.br>
Assunto: [Pregão 17/2020 - FUNASA] Pedido de Esclarecimentos

Prezado Pregoeiro,

Seguem nossos pedidos de esclarecimentos referente ao Pregão 17/2020.

Muito obrigada,

Karla Oliveira
Account Manager
+55 (61) 2196-7784
+55 (61) 9 9845-3235/
+55 (61) 9 8144-2354
karla.oliveira@yssy.com.br

Regional Brasília
SCS Quadra 09, Toore C, Ed. Parque Cidade Corporate, REGUS
70308-200 Brasília DF

yssy.com.br