

Questionamentos para o Termo de Referência

Referente ao requisito 3.3.:

O item 1 refere-se ao cluster de Firewall com suporte, garantia e licenças de proteção com vigência de 60 meses. Esta solução deve funcionar em cluster do tipo ativo-ativo, com balanceamento interno.

Baseado no requisito 3.3, é claro o entendimento que os equipamentos do tipo 1 devem ser ofertados, suportando todos os requisitos técnicos do Termo de referência, assim como suportar toda capacidade de performance e características do hardware de forma individual, ou seja, no mesmo equipamento (appliance). Entendemos que não serão aceitas soluções que fazem empilhamento de appliances para somar processamento e atender o certame

PERGUNTA: Está correto o entendimento?

Referente ao ITEM 05 e requisito 3.6:

O item 05 define a contratação dos serviços de instalação para os itens 01 e 02, não abrangendo portanto a instalação do item 03.

Já no requisito 3.6 informa que o item 03 deverá ser instalado pela Contratada, contudo, não está definido um ITEM específico para a aquisição de serviço de instalação para este item 03, assim como, não estão definidas as localidades onde deverão ser realizadas as instalações das 26 unidades do tipo III.

PERGUNTA: Podemos considerar que as 26 unidades do tipo III (ITEM 03) deverão ser entregues em Brasília pela Contratada, contudo, serão instaladas e configuradas pela própria Contratante?

Referente aos requisitos 4.1.5 e 5.6.10:

Junto ao serviço de instalação, a Contratada deverá fornecer uma Operação Assistida.

PERGUNTA: O serviço de Operação Assistida deverá operar por 24x7 ou 8x5 em horário comercial ?

PERGUNTA: O serviço de Operação Assistida poderá ser executado de forma remota, através de VPN ?

PERGUNTA: Cada requisito (4.1.5 e 5.6.10) define um prazo diferente. Devemos considerar 30 dias ou 5 dias ?

PERGUNTA: O período de Operação Assistida deverá ser contabilizado a partir da instalação e operacionalização do 1º Firewall em produção ?

PERGUNTA: Além do MinC, cada partícipe da Ata deverá ter o período de Operação Assistida em separado ou podemos considerar a execução de uma única Operação Assistida abrangendo os 4 órgãos ao mesmo tempo ?

Referente ao requisito 4.4.8 - subitem IV:

No caso da abertura de chamados cuja a demanda seja "informativa" ou uma dúvida, o SLA de tempo de resposta é de 8 horas em horário comercial. Contudo, eventualmente a informação requerida no chamado pode depender de consulta ao suporte técnico do Fabricante, sendo que, este tipo de consulta tem baixa prioridade para o mesmo por não se tratar de um "incidente" e a resposta pode não vir em 8 horas.

PERGUNTA: Podemos considerar que no caso de necessidade de consulta da Contratada ao suporte do Fabricante, o tempo em que o mesmo despende para responder poderá ser expurgado da contabilização deste SLA ?

Referente ao requisito 4.11.8:

PERGUNTA: O requisito 4.11.8 define que a Contratada deverá fornecer equipamento provisório apenas nos casos em que tenha de recorrer a solicitação de prorrogação descrita no item 4.11.7. Está correto nosso entendimento?

Referente ao requisito 5.9:

Etapas 6: o projeto de instalação deverá ser entregue 10 dias úteis após a assinatura do contrato

Para confeccionar o projeto de instalação, é necessário ocorrer reuniões entre as equipes da Contratante e Contratada para detalhar a arquitetura atual, objetivos da nova arquitetura, obtenção do inventário (assessment) do ambiente atual, apreciação das especificidades da infra e da solução ofertada, discutir questões operacionais e procedimentos para mudanças no ambiente de produção e etc...

PERGUNTA: Este prazo de 10 dias úteis poderá ser contabilizado após conclusão dessa etapa de reuniões de detalhamento técnico?

Etapas 7: a instalação e configuração deverá ser concluída em até 10 dias úteis após a entrega dos equipamentos (recebimento provisório)

Neste caso sem a conclusão da etapa 6 não será possível iniciarmos a etapa 7.

PERGUNTA: Podemos considerar que os 10 dias úteis começam a contar a partir da aprovação do projeto de instalação entregue em cumprimento à etapa 6 e adicionalmente, após atestar o atendimento dos pré-requisitos de infraestrutura e operacionais por parte da Contratante ?

Questionamentos para o ANEXO III do Termo de Referência

Referente ao ITEM 01 - Módulo de segurança (Cluster) - Tipo I:

Referente ao **item 1.2** do novo edital, percebemos a mudança da escrita onde não possui a tecnologia "Sandbox", sendo que em todo o projeto é solicitado assim como a versão anterior que já possuía. Segue abaixo modelo do item para errata:

"1.2. deve possuir throughput de, no mínimo, 10 (Dez) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware, Sandbox e log habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;"

Entendemos que o item acima é o que deve ser considerado para o processo, pois a questão de prevenção de ameaças avançadas, faz parte do ETP. Está correto o entendimento?

Referente ao ITEM 01 - Módulo de segurança (Cluster) - Tipo I:

Constam 02 especificações distintas de transceivers para as mesmas portas de 40G/100G que estão definidas nos requisitos 1.3 e 1.10. Entendemos que a especificação que consta no requisito 1.10 esteja mais detalhada e completa, portanto, esta é a que deverá ser fornecida e a definição no 1.3 deve ser desconsiderada.

PERGUNTA: Está correto nosso entendimento?

Referente ao ITEM 01 - Módulo de segurança (Cluster) - Tipo I:

Constam 02 abordagens distintas nos requisitos 1.4 e 1.13. Entendemos que a especificação original que consta no requisito do item "1.13. Deve possuir, no mínimo, 2 (duas) interface física dedicada para o recurso de alta disponibilidade não sendo permitido o uso de interface de propósito geral para essa finalidade.", é a que deverá ser considerada, não sendo considerado portanto, o requisito 1.4.

Com isso, não gera nenhum impacto na necessidade final que são as quantidades de interfaces solicitadas e também permite a participação de todos os fabricantes do mercado de segurança, além que a solução será mantida nos próximos 5 anos e deve atender qualquer mudança futura de crescimento e expansão da rede.

PERGUNTA: Está correto nosso entendimento?

Referente ao ITEM 01 - Módulo de segurança (Cluster) - Tipo I:

Item 1.7 *"Deve possuir, no mínimo, 2 (duas) interface física dedicada para o recurso de alta disponibilidade, não sendo permitido o uso de interface de propósito geral para essa finalidade."*

Entendemos que o item 1.7 publicado no documento é o que será válido para o projeto, baseado no edital publicado anteriormente, sendo que todos os fabricantes de mercado conseguem atender. Está correto o entendimento?

Referente ao ITEM 01 - Módulo de segurança (Cluster) - Tipo I:

Define o requisito 1.18: Deve suportar, no mínimo, 1.800 (mil e oitocentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;

Entendemos que as licenças oferecidas para os usuários de VPN client-to-Site, conforme exigido no item "CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO ITEM 01 - MÓDULO DE SEGURANÇA (CLUSTER) - tipo I", devem não apenas atender a todos os requisitos técnicos do Termo de Referência, mas também estar sob cobertura de suporte para correção de problemas e abertura de chamados 24/7 durante toda a vigência contratual de 60 meses, incluindo-se aqui os agentes que vão instalados nos endpoints, em atendimento às exigências do requisito 4.1.7. Conforme a gravidade ou criticidade do problema a ser resolvido, a CONTRATADA deverá possibilitar o escalonamento do incidente para a área de suporte ou engenharia do fabricante, devidamente capacitada a resolver o problema, sem custo adicional para o CONTRATANTE.

PERGUNTA: Está correto o nosso entendimento?

Referente ao ITEM 02 - Módulo de segurança - Tipo II:

Referente ao **item 2.2** do novo edital, percebemos a mudança da escrita onde não possui a tecnologia "Sandbox", sendo que em todo o projeto é solicitado assim como a versão anterior que já possuía. Segue abaixo modelo do item para errata:

"2.2. Deve possuir throughput de, no mínimo, 4.5 (quatro, cinco) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus, Anti-Spyware, Sandbox e log habilitados simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;"

Entendemos que o item acima é o que deve ser considerado para o processo, pois a questão de prevenção de ameaças avançadas, faz parte do ETP. Está correto o entendimento?

Referente ao ITEM 02 - Módulo de segurança - Tipo II:

Baseado no novo edital, o item abaixo referente a interfaces que estava publicado na primeira RFP, foi excluído.

"Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 1Gbps/2.5Gbps/5Gbps do tipo RJ-45;"

Entendemos que a solução deve possuir módulos que permitam o reconhecimento de diferentes velocidades dentro da rede, assim permitindo ajustes em determinadas redes de segurança em caso de necessidade e mudança nos próprios equipamentos de redes que serão conectados ao Firewall. Sendo assim, entendemos que o órgão irá reavaliar essa questão, pois existem outras empresas que estão participando dessa aquisição e acabaria possibilitando um grande diferencial no processo. Além disso, os fabricantes de mercado conseguem atender plenamente essa questão. Está correto o entendimento?

Referente ao ITEM 02 - Módulo de segurança - Tipo II:

Define o **requisito 2.13**: Deve suportar, no mínimo, 1.000 (mil) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;

Entendemos que as licenças oferecidas para os usuários de VPN client-to-Site, conforme exigido no item "CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO ITEM 02 - MÓDULO DE SEGURANÇA - tipo II", devem não apenas atender a todos os requisitos técnicos do Termo de Referência, mas também estar sob cobertura de suporte para correção de problemas e abertura de chamados 24/7 durante toda a vigência contratual de 60 meses, incluindo-se aqui os agentes que vão instalados nos endpoints, em atendimento às exigências do requisito 4.1.7. Conforme a gravidade ou criticidade do problema a ser resolvido, a CONTRATADA deverá possibilitar o escalonamento do incidente para a área de suporte ou engenharia do fabricante, devidamente capacitada a resolver o problema, sem custo adicional para o CONTRATANTE.

PERGUNTA: Está correto o nosso entendimento?

Referente ao ITEM 03 - Módulo de segurança - Tipo III:

Define o requisito 3.9: Deve suportar, no mínimo, 500 (quinhentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim;

Entendemos que as licenças oferecidas para os usuários de VPN client-to-Site, conforme exigido no item "CARACTERÍSTICAS FÍSICAS E DE PERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO ITEM 03 - MÓDULO DE SEGURANÇA - tipo III", devem não apenas atender a todos os requisitos técnicos do Termo de Referência, mas também estar sob cobertura de suporte para correção de problemas e abertura de chamados 24/7 durante toda a vigência contratual de 60 meses, incluindo-se aqui os agentes que vão instalados nos endpoints, em atendimento às exigências do requisito 4.1.7. Conforme a gravidade ou criticidade do problema a ser resolvido, a CONTRATADA deverá possibilitar o escalonamento do incidente para a área de suporte ou engenharia do fabricante, devidamente capacitada a resolver o problema, sem custo adicional para o CONTRATANTE.

PERGUNTA: Está correto o nosso entendimento?

Referente ao ITEM 04 - Sistema de gerência centralizada com armazenamento de logs console de gerência, monitoração e relatoria

O requisito 5.1 define: O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possui todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com Hyper-V e VMware ESXi;

Entendemos que as soluções de gerenciamento centralizados e armazenamento de logs em caso de appliance físico, deverão ser fornecidas para uso sem restrições de processamento de logs por dia, assim como capacidade de armazenamento de logs. Caso o fabricante possua licenças e hardware físico para processamento e armazenamento de logs, **deverá ser fornecido o equipamento e licenciamento de maior capacidade possível.**

PERGUNTA: Está correto o nosso entendimento?

Referente ao ITEM 04 - Sistema de gerência centralizada com armazenamento de logs console de gerência, monitoração e relatoria

O requisito 5.2 define: Caso a solução de gerenciamento, monitoração e relatoria, possua licenciamento relacionado a armazenamento, este deve ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional

Entendemos que as soluções de gerenciamento centralizados e armazenamento de logs, deverão ser fornecidas para uso sem restrições de processamento de logs por dia, assim como capacidade de armazenamento de logs. Caso o fabricante possua licenças para processamento e armazenamento de logs, **deverá ser fornecida a licença de maior capacidade possível**

PERGUNTA: Está correto o nosso entendimento?

Referente ao ITEM 05:

Os serviços de instalação são cruciais para o sucesso do projeto e portanto, o objetivo destas questões abaixo é precificarmos os mesmos com maior acuracidade mediante as reais necessidades do MinC:

PERGUNTA: Podemos considerar a possibilidade de instalação física e setup inicial ser executado on-site e o restante da instalação + passagem de conhecimento ser efetuado de forma remota ?

PERGUNTA: Poderiam informar, em ordem de grandeza, a quantidade estimada de regras de firewall que deverão ser migradas pela Contratada para a nova solução de NGFW ?

PERGUNTA: Poderiam informar, em ordem de grandeza, a quantidade estimada de VPNs Site-to-Site que deverão ser migradas pela Contratada para a nova solução de NGFW ?

PERGUNTA: Poderiam informar, em ordem de grandeza, a quantidade estimada de Endpoints (Notebooks e Desktops) em que a Contratada deverá efetuar a instalação e configuração da VPN Client-to-Server para a nova solução de NGFW ?

Referente ao requisito 4.30.13 - PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY):

Esta funcionalidade de segurança é uma das mais importantes para na tecnologia NGFW, sendo que, a inspeção e análise de links e URLs são imprescindíveis para garantir eficiência e ampla cobertura na prevenção de ameaças avançadas (ZERO DAY).

Identificamos nesta nova versão do **Termo de Referência** que a função de "envio de links" para análise no ambiente controlado de forma automática via API para um ambiente controlado de Sandbox, foi retirada desse requisito, sendo que isso, comprometerá a eficiência de segurança da funcionalidade de PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY) na qual faz parte do ETP 3/2023, item 7.1.3 > Letra "e" que pede licenciamento de solução de "Prevenção de ameaças avançadas (Zero day)".

PERGUNTA: Podemos considerar que houve um erro de digitação neste requisito e que de fato é requerida a funcionalidade de "envio de arquivos e links para análise no ambiente controlado de forma automática via API" para ferramenta de Sandbox será considerada nesse questionamento uma vez que traz grandes benefícios de segurança que logo todos os fabricantes do mercado de segurança consegue atender plenamente o requisito. Está correto o entendimento?

Referente ao requisito 4.30.14 - PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY):

Esta funcionalidade de segurança é uma das mais importantes para na tecnologia NGFW, sendo que, a inspeção e análise de links e URLs são imprescindíveis para garantir eficiência e ampla cobertura na prevenção de ameaças avançadas (ZERO DAY).

Identificamos nesta nova versão do **Termo de Referência** que a funcionalidade de submissão "para análise automática de URLs em ambiente controlado" foi retirada desse requisito, sendo que isso, comprometerá a eficiência de segurança da funcionalidade de PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY).

PERGUNTA: Podemos considerar que houve um erro de digitação neste requisito e que de fato é requerida a funcionalidade que irá, "identificar e bloquear malwares de dia zero que trafegam pela rede e URL's contidas no corpo do e-mail dentro de ambiente controlado (Sandbox)". Pois a sua ausência difere do documento ETP 3/2023, item 7.1.3 > Letra "e" que pede licenciamento de solução de "Prevenção de ameaças avançadas (Zero day)" que logo todos os fabricantes do mercado de segurança consegue atender plenamente o requisito. Está correto o entendimento?

Referente ao requisito 4.30.19 - PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY):

Esta funcionalidade de segurança é uma das mais importantes para a tecnologia NGFW, sendo que a inspeção e análise de arquivos com uso de Machine Learning é imprescindível para garantir eficiência e ampla cobertura na prevenção de ameaças avançadas (ZERO DAY).

Identificamos nesta nova versão do **Termo de Referência** que a funcionalidade de “aplicar de forma complementar as assinaturas de antivírus a inspeção inline através de Machine learning em tempo real para arquivos tipo ELF, em tempo real para malwares desconhecidos” foi retirada deste requisito.

Como é sabido, arquivos ELF são um dos maiores vetores de malware e portanto, sua inspeção inline através de Machine learning em tempo real é fundamental para garantir a eficiência de segurança da funcionalidade de PREVENÇÃO DE AMEAÇAS AVANÇADAS (ZERO DAY).

No próprio Termo de Referência, o requerimento 4.3. define “A solução de segurança, deve possuir nativamente funcionalidade de Machine Learning capaz de bloquear grande volume dos ataques nas suas redes”, implicitamente requer a maior abrangência possível na cobertura do Machine Learning e a inspeção inline de ELF é fundamental.

No próprio Termo de Referência, o requerimento 4.30.3. define “A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio GW através de mecanismos de Machine Learning. Não serão aceitas soluções que utilizem equipamentos externos”, implicitamente requer a maior abrangência possível na cobertura do Machine Learning e a inspeção inline de ELF é fundamental.

No próprio Termo de Referência, o requerimento 4.30.15. define “As funcionalidades de sandbox tem como objetivo, analisar e bloquear em tempo real de Ameaças Avançadas Persistentes - APT. Essas funcionalidades têm o objetivo de proteger o ambiente contra a entrada de malwares não conhecidos, e para que ela seja efetiva é necessário que a inspeção e bloqueio sejam feitas em linha (inline), através de features de machine learning”, implicitamente requer a maior abrangência possível na cobertura do Machine Learning e a inspeção inline de ELF é fundamental.

PERGUNTA: Podemos considerar que houve um erro de digitação neste requisito e que de fato é requerida a funcionalidade de “aplicar de forma complementar as assinaturas de antivírus a inspeção inline através de Machine learning em tempo real para arquivos tipo ELF, em tempo real para malwares desconhecidos” ?
Lembrando que todos os fabricantes do mercado de segurança conseguem atender plenamente o requisito. Está correto o entendimento?

Questionamentos - dúvidas gerais

- A assinatura da DECLARAÇÃO DE PLENO CONHECIMENTO pode ser efetuada via Assinatura Eletrônica?
- Referente ao cadastro de lances no Portal:

O item 01 faz referência a um “Módulo de Segurança (CLUSTER)”, composto por 2 equipamentos.
Devemos considerar, para efeito de calculo do valor total, o valor unitário sendo a composição do Cluster (dois equipamentos)?
- Sendo o critério de julgamento o menor preço por Grupo, entendemos que o vencedor será o que apresentar o menor preço total do Grupo (e que esteja dentro dos valores estimados definidos no Edital), ainda que não apresente o menor valor unitário em um determinado item na etapa de lances. Está correto nosso entendimento?
- Atualmente contamos com novos recursos altamente eficazes e de alta qualidade como plataformas de treinamento online. Podemos considerar que o treinamento solicitado, seja efetuado de forma remota (formato online em tempo real, com laboratório virtual e instrutores)?
- Caso não seja aceito o treinamento de forma remota, qual a localidade que deverá ser ministrado o treinamento?
- Referente ao quantitativo do Treinamento: O total de treinamento solicitado é igual a 5, sendo:
 - 2 x Ministério Da Cultura, sendo 1 executado em 2024
 - 1 x Ministério Do Turismo
 - 1 x Ministério Do Meio Ambiente E Mudança Do Clima
 - 1 x Serviço Florestal Brasileiro

Devemos considerar que o quantitativo é uma turma com até 5 participantes em cada órgão? Ou seja, no caso do Ministério da Cultura, devemos considerar 2 turmas de 5 participantes cada?
- O prazo de vigência da contratação é de 12 (doze) meses, porém o suporte, garantia e licenças de proteção terão a vigência de 60 meses.

Ao final dos 12 meses, a responsabilidade do cumprimento do SLA termina e fica vigente apenas a condição do fabricante (Exemplo: Acionamento direto ao fabricante via 0800, atendimento em Inglês etc.)?