Questionamentos Pregão Eletrônico Nº 12/2023 - SSP DF

Isabelle Christine Rodrigues da Silva <isabelle.silva@nordenit.com.br>

sex 29/12/2023 10:07

Para:Licitações SSPDF <licitacoes@ssp.df.gov.br>;

Cc:Denis Sousa <denis@nordenit.com.br>; Gustavo Souza <gustavo@nordenit.com.br>;

Prezado Pregoeiro, bom dia!

Afim de viabilizar nossa participação, a empresa Norden como sendo parceiro **checkpoint** para o Pregão Eletrônico Nº 12/2023, cujo objeto é aquisição Firewall, do tipo NGFW, de alta capacidade para Segurança de datacenter, firewalls de pequeno porte, gerência centralizada de logs e eventos dos firewalls e antivírus com EDR com instalação, configuração, suporte técnico, manutenção e garantia de 36 (trinta e seis) meses, solicitamos os seguintes esclarecimentos:

QUESTIONAMENTO 1

A planilha contendo o detalhamento do objeto traz a seguinte descrição para o item 1:

"Tipo I - Firewall NGFW *Licença UTP para equipamento FG-1500D, ou NGFW de outro fabricante que atue na proteção da comunicação das LANs da SSPDF, WAN e Internet"

Gostaríamos de enfatizar que o modelo da Fortinet FG-1500D entrou em período de End-of-life desde 2020. A Fortinet não prestará o serviço de suporte após a data de 10 de abril de 2025. Vale destacar que o edital prevê a garantia e suporte para 3 anos, ora, não é condizente para um órgão de segurança contratar um produto que não terá mais garantia nem suporte até o final de contrato. É um risco enorme para o órgão público e o cidadão que depende dos serviços prestados por este.

- **Product:** FortiGate-1500D
- **End of Order Date (EOO):** 2020-04-10
- **Last Service Extension Date (LSED):** 2024-04-10
- **End of Support Date (EOS):** 2025-04-10

Entendemos que por questões obvias de gestão e segurança de rede, não será aceito apenas o fornecimento da licença UTP referido modelo que está em período de end-of-life.

Está correto nosso entendimento?

QUESTIONAMENTO 2

15.2. FIREWALL TIPO 2

15.2.4. Throughput de, no mínimo, 6 (seis) Gbps de VPN IPSec;

O link de comunicação utilizado pelo SSP-DF é provido por um anel ótico do GDF e o desempenho máximo deste é de 1 Gbps. É estranho o órgão exigir no termo de referência desempenho mínimo de VPN IPSec de 6 Gbps, pois o limitador da velocidade da VPN será o link de dados, que neste caso é de 1 Gbps. Esse tipo de exigência apenas obriga os fornecedores a cotarem solução com valor mais alto para atender um desempenho que nunca será utilizado.

Entendemos que o item 15.2.4 poderá ser demonstrado seu atendimento para soluções que apresentem desempenho de VPN IPsec de 1 Gbps.

Está correto nosso entendimento?

QUESTIONAMENTO 3

15.2. FIREWALL TIPO 2

15.2.11. Possuir pelo menos 2 (duas) interfaces 1GbE SFP e seus módulos. Deverão ser fornecidos com 2 (dois) transceivers;

O termo de referência estabelece no item 15.2.11 a necessidade de equipamentos com portas de rede SFP, no entanto, gostaríamos de sugerir a avaliação da possibilidade de aceitar exclusivamente interfaces de cobre como uma alternativa viável. Temos conhecimeto a importância de atender às necessidades técnicas do órgão, porém, a utilização exclusiva de interfaces de cobre pode proporcionar vantagens consideráveis em termos de custo e simplicidade na manutenção da infraestrutura de rede.

Destacamos que a tecnologia de interfaces de cobre é amplamente utilizada e oferece desempenho satisfatório para diversas aplicações. Além disso, sua adoção poderia resultar em economias significativas, sem comprometer a qualidade e a eficiência da rede.

Diante do exposto, entendemos que haverá a revisão dessa exigência, considerando a aceitação de interfaces de cobre como alternativa às portas SFP. Caso exista a possibilidade de flexibilização nesse ponto, acreditamos que isso contribuirá para uma maior participação de fornecedores e, consequentemente, para a obtenção de propostas mais competitivas.

Está correto nosso entendimento?

QUESTIONAMENTO 4

Todos os itens abaixo se referem ao recurso de Alta Disponibilidade. Com base os itens abaixo fazemos o seguinte questionamento:

15.2.24. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

15.2.29. A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo;

15.2.33. A solução deverá ser capaz de organizar os appliances de NG Firewall em grupos de segurança, nos quais os appliances de NG Firewall atuarão com seus recursos somados;

15.2.34.A solução deverá ser capaz de suportar, no mínimo, 4 (quatro) grupos de segurança;

15.2.61. Suportar cluster para alta-disponibilidade do tipo ativo-ativo, permitindo que um cluster possa realizar o load balance das sessões para inspeção profunda sem a necessidade de implementações ou mudanças na rede ou nos terminais já existentes;

15.2.229. A solução deve sincronizar ou aplicar as assinaturas de IPS, Anti vírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

Gostaríamos de apresentar uma consideração técnica em relação à exigência contida nos itens 15.2.24, 15.2.29, 15.2.33, 15.2.34, 15.2.61 do edital, que requer que os appliances de segurança suportem operar em cluster ativo-ativo e ativo-passivo.

Entendemos a importância da alta disponibilidade na infraestrutura de segurança, porém, gostaríamos de sugerir uma revisão na especificação para permitir a opção obrigatória somente do cluster ativo-passivo. Essa abordagem apresenta vantagens significativas em termos de eficiência e consistência operacional, especialmente em ambientes de segurança críticos.

O cluster ativo-passivo permite que um dos dispositivos no cluster atue como unidade principal (ativo) enquanto o segundo permanece em standby (passivo), pronto para assumir em caso de falha. Esta configuração oferece uma divisão clara de responsabilidades, facilitando a administração e manutenção do ambiente. Além disso, em ambientes de alta demanda, a eficiência do ativo-passivo é muitas vezes superior ao ativo-ativo, uma vez que todo o tráfego é processado por um único nó enquanto o outro permanece em standby.

Ao considerar a complexidade do gerenciamento de clusters ativo-ativo e as possíveis complicações devido à distribuição equitativa de carga entre os nós, o modelo ativo-passivo se destaca como uma escolha mais prática e eficiente para ambientes críticos de segurança.

Baseado no exposto acima, entendemos somente de soluções de cluster ativo-passivo será obrigatório, garantindo a flexibilidade necessária para atender às demandas específicas de cada ambiente. Ressaltamos que esta alteração não comprometerá a segurança, uma vez que ambos os modelos oferecem alta disponibilidade e confiabilidade.

Está correto nosso entendimento?

QUESTIONAMENTO 5

15.2.94. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia uti lizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc);

15.2.95. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

Gostaríamos de apresentar um questionamento referente ao Termo de Referência da licitação em questão, especificamente em relação aos itens 15.2.94 e 15.2.95, que exigem que a solução de Next-Generation Firewall (NGFW) possua a capacidade de criação de grupos dinâmicos de aplicações.

Entendemos a importância de garantir recursos avançados de segurança, mas gostaríamos de sugerir uma revisão nesses requisitos específicos, levando em consideração os princípios da Lei 8.666/93, que preconiza a ampla participação de fornecedores e a competitividade no processo licitatório.

A imposição da obrigação de suporte a grupos dinâmicos pode limitar a participação de potenciais fornecedores, especialmente aqueles que oferecem soluções robustas de NGFW, mas que podem não incluir esse recurso específico. Tal restrição pode resultar em um processo menos aberto e competitivo, contrariando os princípios fundamentais da legislação de licitações.

Sugerimos, portanto, que a exigência relativa aos grupos dinâmicos seja revisada para permitir a participação de uma gama mais ampla de fornecedores, desde que atendam aos demais requisitos de segurança estabelecidos. Isso permitiria a consideração de soluções inovadoras e eficazes, promovendo a concorrência e garantindo a escolha da solução mais vantajosa para a SSP-DF.

Entendemos que os itens não serão obrigatórios seu atendimento.

Está correto nosso entendimento?

QUESTIONAMENTO 6

15.2.150. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

15.2.216. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

15.2.217. PCI – números de cartão de crédito;

Gostaríamos de apresentar uma solicitação para revisão do Termo de Referência, em específico em relação à especificação 15.2.150, que trata da necessidade do produto de Next-Generation Firewall (NGFW) ser capaz de identificar a transferência de número de cartão de crédito, esse detalhamento é característico de um produto chamado DLP - Data Loss Prevention.

Entendemos a importância da proteção de informações sensíveis, conforme descrito na especificação, no entanto, gostaríamos de sugerir a retirada da obrigatoriedade do recurso DLP do escopo do NGFW. Nossa sugestão baseia-se nos seguintes fundamentos:

1. **Especialização de Produtos de DLP:**

Produtos especializados em Data Loss Prevention (DLP) são altamente especializados e requerem uma avaliação técnica minuciosa, que pode ser mais apropriada em um processo de compra dedicado exclusivamente a soluções de DLP.

2. **Ampla Variedade de Soluções:**

Permitir que o mercado de soluções de DLP seja avaliado separadamente abrirá espaço para uma comparação mais abrangente entre os fornecedores especializados nesse campo, possibilitando a escolha da solução mais adequada às necessidades específicas do órgão.

3. **Princípios da Lei 8.666/93:**

A retirada da obrigatoriedade do DLP do Termo de Referência estará em consonância com os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, conforme preconizado pela Lei 8.666/93. Além disso, permitirá a ampliação da competitividade no processo licitatório.

Diante do exposto, sugerimos a exclusão da especificação 15.2.150 para permitir a identificação e prevenção da transferência de informações sensíveis de forma mais aberta, sem a obrigatoriedade da inclusão do recurso DLP no NGFW.

QUESTIONAMENTO 7

15.2.160. O cliente VPN deve suportar autenticação via SAML 2.0 a fim de permitir integração com plataformas Azure AD, Google Authentication ou outro provedor de identidade;

A exigência do item 15.2.160 limita a ampla participação de diversos fabricantes de solução de NGFW. Solicitamos a remoção do item, pois este somente direciona a compra pública para poucos produtos. Não é relevante tecnicamente suportar autenticação SAML 2.0 para cliente de VPN, pois os agentes que são instalados nos equipamentos remotos se autenticação primeiro no NGFW e depois permitem o uso da VPN.

Estendemos que o órgão irá manter um processo de compra aberto e irá remover o iten 15.2.160 para permitir a ampla participação.

Está correto nosso entendimento?

QUESTIONAMENTO 8

15.2.161. O cliente de VPN deve estar disponível na loja de aplicativos AppStore e PlayStore;

Este item também limita a ampla participação de fornecedores a fim de ofertar uma solução com alto padrão de qualidade, mas que por questões técnicas não possui o cliente de VPN na AppStore e PlayStore. É possível contornar a questão com agentes que são facilmente distribuídos pela rede Microsoft e instalados em dóminio.

Estendemos que o órgão irá manter um processo de compra aberto e irá remover o iten 15.2.161 para permitir a ampla participação.

Está correto nosso entendimento?

QUESTIONAMENTO 9

15.2.173. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

Entendemos que se a solução ofertada for capaz de monitorar e identificar pelo menos 2 (dois) dos testes citados no item 15.2.173, será considerado como atendido.

Está correto nosso entendimento?

QUESTIONAMENTO 10

15.2.230. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

Entendemos que os produtos que suportam o fail-open em caso de falha do hardware também serão considerados como opção de entrega para atender ao item 15.2.230.

Está correto nosso entendimento?

Governo do Distrito Federal
Secretaria de Estado de Segurança Pública do Distrito Federal
Subsecretaria de Modernização Tecnológica
Coordenação de Infraestrutura

Memorando Nº 116/2023 - SSP/SEGI/SMT/CINF

Brasília-DF, 29 de dezembro de 2023.

Ao Serviço de Licitações (SLIC),

Assunto: Pedido de Esclarecimento referente ao Pregão Eletrônico n° 12/2023-SSPDF.

Senhora Pregoeira,

Em atenção ao Despacho SSP/SEGI/SUAG/CLIC/SLIC (130293741) do Serviço de Licitações, encaminhando o pedido de esclarecimentos apresentado pela empresa NORDENIT (130293741) referente ao Pregão Eletrônico n° 12/2023-SSPDF, informo o seguinte:

Com relação ao questionamento 1:

"A planilha contendo o detalhamento do objeto traz a seguinte descrição para o item 1:

Tipo I - Firewall NGFW *Licença UTP para equipamento FG-1500D, ou NGFW de outro fabricante que atue na proteção da comunicação das LANs da SSPDF, WAN e Internet

Gostaríamos de enfatizar que o modelo da Fortinet FG-1500D entrou em período de End-of-life desde 2020. A Fortinet não prestará o serviço de suporte após a data de 10 de abril de 2025. Vale destacar que o edital prevê a garantia e suporte para 3 anos, ora, não é condizente para um órgão de segurança contratar um produto que não terá mais garantia nem suporte até o final de contrato. É um risco enorme para o órgão público e o cidadão que depende dos serviços prestados por este.

Product: FortiGate-1500D

End of Order Date (EOO): 2020-04-10

Last Service Extension Date (LSED): 2024-04-10

End of Support Date (EOS): 2025-04-10

Entendemos que por questões obvias de gestão e segurança de rede, não será aceito apenas o fornecimento da licença UTP referido modelo que está em período de end-of-life."

Durante a fase de Planejamento da Contratação, (Estudo Técnico Preliminar ETP), foi consultado o fabricante FORTINET, por e-mail, documento SEI (130327323), acerca dos prazos de suporte dos equipamentos existentes na SSPDF, as informações obtidas do fabricante, divergem dos prazos apresentado pelo requerente. O fabricante informou que o prazo do End of Support Date (EOS) cessa em 31/12/2026. Desta forma será aceita o fornecimento de licenças UTP, conforme especificações definidas no Termo de Referência. Visando prestigiar os princípios da transparência e da ampla concorrência foi permitido que outros fabricantes possam participar do certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Com relação ao questionamento 2:

"15.2. FIREWALL TIPO 2

15.2.4. Throughput de, no mínimo, 6 (seis) Gbps de VPN IPSec;

O link de comunicação utilizado pelo SSP-DF é provido por um anel ótico do GDF e o desempenho máximo deste é de 1Gbps. É estranho o órgão exigir no termo de referência desempenho mínimo de VPN IPSec de 6 Gbps, pois o limitador da velocidadeda VPN será o link de dados, que neste caso é de 1 Gbps. Esse tipo de exigência apenas obriga os fornecedores a cotarem solução com valor mais alto para atender um desempenho que nunca será utilizado.

Entendemos que o item 15.2.4 poderá ser demonstrado seu atendimento para soluções que apresentem desempenho deVPN IPsec de 1 Gbps."

Resposta: Atualmente a GDFNET fornece links a SSPDF de 10 Gbps, cabe ainda informar que a rede GDFNET está passando por atualizações tecnológicas e nos próximos meses outros órgãos também terão conexão a 10Gbps, portando o entendimento não está correto.

Com relação ao questionamento 3:

"15.2. FIREWALL TIPO 2 15.2.11.

Possuir pelo menos 2 (duas) interfaces 1GbE SFP e seus módulos. Deverão ser fornecidos com 2 (dois)transceivers;

O termo de referência estabelece no item 15.2.11 a necessidade de equipamentos com portas de rede SFP, no entanto, gostaríamos de sugerir a avaliação da possibilidade de aceitar exclusivamente interfaces de cobre como uma alternativa viável. Temos conhecimento a importância de atender às necessidades técnicas do órgão, porém, a utilização exclusiva de interfaces de cobre pode proporcionar vantagens consideráveis em termos de custo e simplicidade na manutenção da infraestrutura de rede. Destacamos que a tecnologia de interfaces de cobre é amplamente utilizada e oferece desempenho satisfatório para diversas aplicações. Além disso, sua adoção poderia resultar em economias significativas, sem comprometer a qualidade e a eficiência da rede. Diante do exposto, entendemos que haverá a revisão dessa exigência, considerando a aceitação de interfaces de cobre como alternativa às portas SFP. Caso exista a possibilidade de flexibilização nesse ponto, acreditamos que isso contribuirá para uma maior participação de fornecedores e, consequentemente, para a obtenção de propostas mais competitivas."

Resposta: O entendimento não está correto, do ponto de vista técnico se faz necessário ao menos 2 (duas) interfaces 1GbE SFP e seus módulos.

Com relação ao questionamento 4:

"Todos os itens abaixo se referem ao recurso de Alta Disponibilidade. Com base os itens abaixo fazemos o seguinte questionamento:

15.2.24. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

15.2.29. A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo;

15.2.33. A solução deverá ser capaz de organizar os appliances de NG Firewall em grupos de segurança, nos quais os appliances de NG Firewall atuarão com seus recursos somados;

15.2.34.A solução deverá ser capaz de suportar, no mínimo, 4 (quatro) grupos de segurança;

15.2.61. Suportar cluster para alta-disponibilidade do tipo ativo-ativo, permitindo que um cluster possa realizar o load balance da ssessões para inspeção profunda sem a necessidade de implementações ou mudanças na rede ou nos terminais já existentes;

15.2.229. A solução deve sincronizar ou aplicar as assinaturas de IPS, Anti vírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo; Gostaríamos de apresentar uma consideração técnica em relação à exigência contida nos itens 15.2.24, 15.2.29, 15.2.33,15.2.34, 15.2.61 do edital, que requer que os appliances de segurança suportem operar em cluster ativo-ativo e ativo-passivo.

Entendemos a importância da alta disponibilidade na infraestrutura de segurança, porém, gostaríamos de sugerir uma revisão na especificação para permitir a opção obrigatória somente do cluster ativo-passivo. Essa abordagem apresenta vantagens significativas em termos de eficiência e consistência operacional, especialmente em ambientes de segurança críticos.

O cluster ativo-passivo permite que um dos dispositivos no cluster atue como unidade principal (ativo) enquanto o segundo permanece em standby (passivo), pronto para assumir em caso de falha. Esta configuração oferece uma divisão clara de responsabilidades, facilitando a administração e manutenção do ambiente. Além disso, em ambientes de alta demanda, a eficiência do ativo-passivo é muitas vezes superior ao ativo-ativo, uma vez que todo o tráfego é processado por um único nó enquanto o outro permanece em standby. Ao considerar a complexidade do gerenciamento de clusters ativo-ativo e as possíveis complicações devido à distribuição equitativa de carga entre os nós, o modelo ativo-passivo se destaca como uma escolha mais prática e eficiente para ambientes críticos de segurança. Baseado no exposto acima, entendemos somente de soluções de cluster ativo-passivo será obrigatório, garantindo a flexibilidade necessária para atender às demandas específicas de cada ambiente. Ressaltamos que esta alteração não comprometerá a segurança, uma vez que ambos os modelos oferecem alta disponibilidade e confiabilidade"

Resposta: Atualmente os equipamentos possuem essas funcionalidades, só serão aceitos equipamentos com especificações técnicas iguais ou superiores aos existentes. Após a conclusão dos Estudos Técnicos Preliminares, ficou comprovada a vantajosidade econômica da atualização dos equipamentos existentes, entretanto, visando prestigiar os princípios da transparência e da ampla concorrência foi permitido a participação de outros fabricantes no certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Com relação ao questionamento 5:

"15.2.94. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como :tecnologia utilizada nas aplicações (ClientServer, Browse Based, Network Protocol, etc);

15.2.95. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

Gostaríamos de apresentar um questionamento referente ao Termo de Referência da licitação em questão, especificamente em relação aos itens 15.2.94 e 15.2.95, que exigem que a solução de Next-Generation Firewall (NGFW) possua a capacidade de criação de grupos dinâmicos de aplicações.

Entendemos a importância de garantir recursos avançados de segurança, mas gostaríamos de sugerir uma revisão nesses requisitos específicos, levando em consideração os princípios da Lei 8.666/93, que preconiza a ampla participação de fornecedores e a competitividade no processo licitatório. A imposição da obrigação de suporte a grupos dinâmicos pode limitar a participação de potenciais fornecedores, especialmente aqueles que oferecem soluções robustas de NGFW, mas que podem não incluir esse recurso específico. Tal restrição pode resultar em um processo menos aberto e competitivo, contrariando os princípios fundamentais da legislação de licitações. Sugerimos, portanto, que a exigência relativa aos grupos dinâmicos seja revisada para permitir a participação de uma gama mais ampla de fornecedores, desde que atendam aos demais requisitos de segurança estabelecidos. Isso permitiria a consideração de soluções inovadoras e eficazes, promovendo a concorrência e garantindo a escolha da solução mais vantajosa para a SSP-DF. Entendemos que os itens não serão obrigatórios seu atendimento."

Resposta: Atualmente os equipamentos possuem essas funcionalidades, só serão aceitos equipamentos com especificações técnicas iguais ou superiores aos existentes. Após a conclusão dos Estudos Técnicos Preliminares, ficou comprovada a vantajosidade econômica da atualização dos equipamentos existentes, entretanto, visando prestigiar os princípios da transparência e da ampla concorrência foi permitido a participação de outros fabricantes no certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Com relação ao questionamento 6:

"15.2.150. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

15.2.216. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de dados e arquivos:

15.2.217. PCI – números de cartão de crédito; Gostaríamos de apresentar uma solicitação para revisão do Termo de Referência, em específico em relação à especificação

15.2.150, que trata da necessidade do produto de Next-Generation Firewall (NGFW) ser capaz de identificar a transferência de número de cartão de crédito, esse detalhamento é característico de um produto chamado DLP - Data Loss Prevention.

Entendemos a importância da proteção de informações sensíveis, conforme descrito na especificação, no entanto, gostaríamos de sugerir a retirada da obrigatoriedade do recurso DLP do escopo do NGFW. Nossa sugestão baseia-se nos seguintes fundamentos:

1. Especialização de Produtos de DLP: Produtos especializados em Data Loss Prevention (DLP) são altamente especializados e requerem uma avaliação técnica minuciosa, que pode ser mais apropriada em um processo de compra dedicado exclusivamente a soluções de DLP.

2. Ampla Variedade de Soluções: Permitir que o mercado de soluções de DLP seja avaliado separadamente abrirá espaço para uma comparação mais abrangente entre os fornecedores especializados nesse campo, possibilitando a escolha da solução mais adequada às necessidades específicas do órgão.

3. Princípios da Lei 8.666/93: A retirada da obrigatoriedade do DLP do Termo de Referência estará em consonância com os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, conforme preconizado pela Lei 8.666/93. Além disso, permitirá a ampliação da competitividade no processo licitatório.

Diante do exposto, sugerimos a exclusão da especificação 15.2.150 para permitir a identificação e prevenção da transferência de informações sensíveis de forma mais aberta, sem a obrigatoriedade da inclusão do recurso DLP no NGFW."

Resposta: Atualmente os equipamentos possuem essas funcionalidades, só serão aceitos equipamentos com especificações técnicas iguais ou superiores aos existentes. Após a conclusão dos Estudos Técnicos Preliminares, ficou comprovada a vantajosidade econômica da atualização dos equipamentos existentes, entretanto, visando prestigiar os princípios da transparência e da ampla concorrência foi permitido a participação de outros fabricantes no certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Com relação ao questionamento 7:

"115.2.160. O cliente VPN deve suportar autenticação via SAML 2.0 a fim de permitir integração com plataformas Azure AD, GoogleAuthentication ou outro provedor de identidade;

A exigência do item 15.2.160 limita a ampla participação de diversos fabricantes de solução de NGFW. Solicitamos a remoção do item, pois este somente direciona a compra pública para poucos produtos. Não é relevante tecnicamente suportar autenticação SAML 2.0 para cliente de VPN, pois os agentes que são instalados nos equipamentos remotos se autenticação primeiro no NGFW e depois permitem o uso da VPN.

Estendemos que o órgão irá manter um processo de compra aberto e irá remover o iten 15.2.160 para permitir a ampla participação. Está correto nosso entendimento?"

Resposta: Atualmente os equipamentos possuem essas funcionalidades, só serão aceitos equipamentos com especificações técnicas iguais ou superiores aos existentes. Após a conclusão dos Estudos Técnicos Preliminares, ficou comprovada a vantajosidade econômica da atualização dos equipamentos existentes, entretanto, visando prestigiar os princípios da transparência e da ampla concorrência foi permitido a participação de outros fabricantes no certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Com relação ao questionamento 8:

"15.2.161. O cliente de VPN deve estar disponível na loja de aplicativos AppStore e PlayStore;

Este item também limita a ampla participação de fornecedores a fim de ofertar uma solução com alto padrão de qualidade, mas que por questões técnicas não possui o cliente de VPN na AppStore e PlayStore. É possível contornar a questão com agentes que são facilmente distribuídos pela rede Microsoft e instalados em dóminio.

Estendemos que o órgão irá manter um processo de compra aberto e irá remover o iten 15.2.161 para permitir a ampla participação."

Resposta: Atualmente os equipamentos possuem essas funcionalidades, só serão aceitos equipamentos com especificações técnicas iguais ou superiores aos existentes. Após a conclusão dos Estudos Técnicos Preliminares, ficou comprovada a vantajosidade econômica da atualização dos equipamentos existentes, entretanto, visando prestigiar os princípios da transparência e da ampla concorrência foi permitido a participação de outros fabricantes no certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Com relação ao questionamento 9:

"15.2.173. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

Entendemos que se a solução ofertada for capaz de monitorar e identificar pelo menos 2 (dois) dos testes citados no item15.2.173, será considerado como atendido."

Resposta: Atualmente os equipamentos possuem essas funcionalidades, só serão aceitos equipamentos com especificações técnicas iguais ou superiores aos existentes. Após a conclusão dos Estudos Técnicos Preliminares, ficou comprovada a vantajosidade econômica da atualização dos equipamentos existentes, entretanto, visando prestigiar os princípios da transparência e da ampla concorrência foi permitido a participação de

outros fabricantes no certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Com relação ao questionamento 10:

"15.2.230. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

Entendemos que os produtos que suportam o fail-open em caso de falha do hardware também serão considerados como opção de entrega para atender ao item 15.2.230."

Resposta: Atualmente os equipamentos possuem essas funcionalidades, só serão aceitos equipamentos com especificações técnicas iguais ou superiores aos existentes. Após a conclusão dos Estudos Técnicos Preliminares, ficou comprovada a vantajosidade econômica da atualização dos equipamentos existentes, entretanto, visando prestigiar os princípios da transparência e da ampla concorrência foi permitido a participação de outros fabricantes no certame, desde que forneça equipamento com especificações técnicas iguais ou superiores aos equipamentos Fortinet FG-1500D.

Atenciosamente,

Documento assinado eletronicamente por **GLAUCIO SILVEIRA E SILVA - Matr.1691710-3**, **Assessor(a) Técnico(a).**, em 02/01/2024, às 09:09, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **DOUGLAS WILLIAN BARBOSA MOREIRA - Matr.1699997-5**, **Diretor(a) de Suporte**, em 02/01/2024, às 09:14, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **HELIO DE FARIAS SOARES - Matr.1713991-0**, **Coordenador(a) de Infraestrutura**, em 02/01/2024, às 09:32, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **130318230** código CRC= **694C336D**.