Ministério do Planejamento, Desenvolvimento e Gestão
Secretaria de Gestão - Central de Compras
Secretaria de Tecnologia da Informação - Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação

RESPOSTA ÀS SUGESTÕES DA CONSULTA PÚBLICA Nº 02/2016

OBJETO: Contratação de empresa especializada no fornecimento de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede dos órgãos e dos servidores de rede, contemplando gerência unificada com garantia de funcionamento pelo período de **60 (sessenta) meses**, incluídos todos os *softwares* e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua, suporte técnico e repasse de conhecimento de toda a solução a fim de atender às necessidades dos órgãos contratantes.

CONTRIBUIÇÕES:

1. Item 1.4.6 A amostra deve ser configurada de forma a realizar a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, e com todas as assinaturas, listas e demais métodos de controle de acesso e sistema de detecção e prevenção de intrusão habilitados.

   Manifestação: A efetividade de segurança do IPS é diretamente proporcional ao número de assinaturas suportadas pelo produto. Sabendo que esse número de assinaturas possui dimensões distintas entre cada fabricante e, visando garantir a isonomia entre os concorrentes do certame, sugerimos a seguinte redação para este item: "1.4.6. A amostra deve ser configurada de forma a realizar a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, e com todas as assinaturas solicitadas no item 2.3.2, listas e demais métodos de controle de acesso e sistema de detecção e prevenção de intrusão habilitados.

   Resposta: Sugestão parcialmente acatada. O item foi reformulado.

2. Item 2.1.10 O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.

   Manifestação: Para o caso de interfaces SFP e SFP+, considerar que tipo/modelo de módulos Gbic? E quantidades? Cada fabricante oferece uma quantidade específica de interfaces, ativas ou não, e aquelas apresentadas em modalidade SFP/SFP+ possibilitam o uso de diversos tipos de módulos. Caso não sejam definidas quantidades mínimas de interfaces e serem populadas com módulos, fabricantes que ofertarem equipamentos com quantidades de portas superiores as solicitadas serão punidas por serem obrigadas a popularem as portas adicionais.
   É recomendável indicar a quantidade mínima de interfaces a serem populadas com módulos, de forma a nivelar o fornecimento entre fornecedores concorrentes e, principalmente, reduzir os custos de aquisição inicial.

   Resposta: Sugestão acatada. Os quantitativos de interfaces mínimos vão ser definidos.

3. Item 2.1.10 O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.

   Manifestação: Afim de não limitar o caráter competitivo do certame, solicitamos que o fornecimento de transceivers seja na quantidade mínima de portas exigidas no Termo de Referência para cada tipo de equipamento, caso contrário, os fabricantes que entregarem um equipamento com quantidade de porta superior ao solicitado (o que é melhor para o Órgão) será punido, pois terá custos a mais em relação aos outros fabricantes que não possuem a mesma quantidade de portas ofertadas.

   Resposta: Sugestão acatada. Os quantitativos de interfaces mínimos vão ser definidos.

4. Item 2.1.11 Fornecido em hardware dedicado tipo appliance ou chassi, com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall multifunção.

   Manifestação: Sugerimos a alteração com relação a escrita do texto original, pois diversos fabricantes terão sua capacidade de atendimento às especificações do Termo de Referência reduzida, implicando em custos demasiados para a administração pública.

   Fornecido em hardware dedicado do tipo appliance, chassi ou equipamento homologado pelo fabricante do firewall, com sistema operacional otimizado, para o uso como firewall multifunção.

   Resposta: Sugestão não acatada, incompatível com a demanda técnica da contratação.

5. Item 2.1.11.2 O equipamento do lote 5 da solução ofertada, pode ser baseada em appliance ou chassi, deverá ter atestada, pelo fabricante, a compatibilidade entre os módulos e o chassi e deverá suportar agregação de enlaces multi-chassi (MC-LAG) segundo padrão IEEE 802.1ax.

   Manifestação: O equipamento do lote 5 da solução ofertada, pode ser baseada em appliance ou chassi, deverá ter atestada, pelo fabricante, a compatibilidade entre os módulos e o chassi

   Resposta: Sugestão não acatada

6. Item 2.1.11.2 O equipamento do lote 5 da solução ofertada, pode ser baseada em appliance ou chassi, deverá ter atestada, pelo fabricante, a compatibilidade entre os módulos e o chassi e deverá suportar agregação de enlaces multi-chassi (MC-LAG) segundo padrão IEEE 802.1ax.

   Manifestação: Entendemos que a funcionalidade de agregação de enlaces multi-chassi (MC-LAG) deverá ser entregue apenas se o fornecedor ofertar a solução em formato chassi.
   Está correto?

   Resposta: Correto, se refere somente ao chassi.

7. Item 2.1.2 Deve possuir fonte(s) de energia no próprio equipamento

   Manifestação: Solicitamos a verificação deste item, uma vez que as especificações de energia para os equipamentos do Lotes 1 e 2 (itens 3.1.1.3 e 3.8.1.3 respectivamente) permitem que a fonte de energia seja externa

   Resposta: Sugestão acatada.

8. Item 2.1.2 Deve possuir fonte(s) de energia no próprio equipamento

   Manifestação: Para o lote 1, firewall de pequeno porte, gostaríamos de solicitar que fosse aceito fonte externa ao equipamento

   Resposta: Sugestão acatada.

9. Item 2.1.13 Suportar topologias de cluster redundante de alta disponibilidade (failover) nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das conexões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das conexões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.

   Manifestação: sugerimos a complementação do item com os subitens abaixo indicando uma maior clareza:
   A configuração em alta disponibilidade deve sincronizar:
   - Sessões;
   - Configurações, incluindo, mas não limitadas às políticas de Firewall, NAT, QOS e objetos de rede;
   - Associações de Segurança das VPNs;
   - Tabelas FIB;

   Resposta: Sugestão não acatada, não faz parte da demanda técnica da contratação.

10. Item 2.1.13 Suportar topologias de cluster redundante de alta disponibilidade (failover) nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das conexões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das conexões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário

    Manifestação: Entendemos que o sistema de alta disponibilidade exigido nos modos ativo-ativo e ativo-passivo, são compostos de 2 equipamentos, e não de 3 equipamentos ou mais. Está correto?'

    Resposta: Correto. A alta disponibilidade exigida são em pares.

11. Item 2.1.14 Deve suportar a implementação tanto em modo transparente (camada 2) quanto em

modo gateway (camada 3)

Manifestação: Sugestão de novo texto:
2.1.14. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);"
2.1.14.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
2.1.14.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível
de aplicação;
2.1.14.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível
de aplicação operando como default gateway das redes protegidas;
2.1.14.4. Suporta modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

Resposta: Sugestão não acatada.

12. Item 2.1.18 Permitir a criação de, no mínimo, 500 VLANs padrão 802.1q;

Manifestação: Na consulta pública realizada no dia 21/06/2016 foi discutido tecnicamente entre todos os participantes e se chegou à conclusão que esta quantidade solicitada é bem superior à necessidade e capacidade efetiva para os equipamentos de menor porte (itens 1, 2 e 3), por este motivo e a fim de tornar possível a participação de nossos equipamentos, solicitamos que a quantidade de VLANs por tipo de equipamento seja alterada conforme abaixo:
Tipo 1: 25, Tipo 2: 50 e Tipo 3: 256

Resposta: Sugestão parcialmente acatada. Item reformulado.

13. Item 2.1.18 Permitir a criação de, no mínimo, 500 VLANs padrão 802.1q;

Manifestação: Esta quantidade de VLANs suportadas é imprescindível para equipamentos de pequeno porte?
Entendemos que esta quantidade é muito alta para requerimentos de pequeno e médio porte, o uso real de equipamentos desta natureza seguramente não demanda esta quantidade alta de VLANs e encarece desnecessariamente a oferta, pois obriga que os fornecedores ofertem equipamentos maiores apenas em função desta demanda.

Para permitir nossa participação, solicitamos que sejam especificadas as quantidades de VLANs por tipo de firewall, conforme segue:
Tipo 1: 25
Tipo 2: 50
Tipo 3: 256
Tipo 4: 512
Tipo 5: 512

Resposta: Sugestão parcialmente acatada. O item foi reformulado.

14. Item 2.1.19 Ser capaz de aceitar comandos de scripts acionados por sistemas externos como, por exemplo, correlacionadores de eventos.

    Manifestação: A plataforma de segurança deve permitir, através de API (Application Program Interface), a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução, possibilitando assim que regras e políticas de segurança possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP;"

    Resposta: Sugestão não acatada.

15. Item 2.1.2 Todos os equipamentos e seus componentes deverão ser novos, sem uso, ou recondicionados, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), patchcords, miniGbics, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310. No caso dos lotes 1 e 2, firewall multifuncionais de 100 e 250 Mbps, poderá ser fornecido os insumos como bandejas para colocação dos mesmos em racks.

    Manifestação: Há que se modificar a frase "Todos os equipamentos e seus componentes deverão ser novos, sem uso, ou recondicionados..." por "Todos os equipamentos e seus componentes deverão ser novos, sem uso...". A expressão "ou recondicionados" está permitindo a entrega de equipamentos recondicionados.

    Resposta: Sugestão acatada.

16. Item 2.1.2 Todos os equipamentos e seus componentes deverão ser novos, sem uso, ou recondicionados, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), patchcords, miniGbics, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310. No caso dos lotes 1 e 2, firewall multifuncionais de 100 e 250 Mbps, poderá ser fornecido os insumos como bandejas para colocação dos mesmos em racks.

    Manifestação: Qual o tipo de interfaces para o fornecimento dos módulos GBic? Fica a critério da CONTRATADA popular as interfaces SFP e SFP+ com os tipos de módulos que lhe parecerem adequados? Fibra? Cobre?

    Recomendamos determinar que fossem indicadas as quantidades específicas de interfaces a serem populadas, de modo a não encarecer desnecessariamente o fornecimento inicial para os órgãos considerando-se aqueles fabricantes que oferecerem appliances com mais interfaces do que o demandadas por este certame.

Resposta: Sugestão acatada

17. Itens 2.1.20 Suportar o bloqueio de tráfego em função da localização geográfica dos IPs de origem e de destino 2.1.55 Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento. 2.1.56 Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

    Manifestação: Todos os itens acima se referem a funcionalidade de GeoLocalização e ou identificação de país de origem ou destino. Sugerimos que seja aceito declaração informando que a funcionalidade está em RoadMap no fabricante e que se compromete a entregar em até 10 meses.

    Resposta: **sugestão não acatada. Não será aceito funcionalidades que estejam em RoadMap, pois as funcionalidades indicadas são necessárias na entrega imediata do equipamento.**

18. Itens 2.1.21 Suportar agregação de links, segundo padrão IEEE 802.3ad;

    Manifestação: A agregação de links é inviável para equipamento de pequeno porte devido sua limitação de desempenho, pois uma simples agregação de link para este tipo de equipamento já ultrapassaria o seu poder de processamento. Por este motivo e com o intuito de permitir o fornecimento da nossa marca, solicitamos que seja removida esta exigência para os equipamentos do tipo 01 e 02.

    Resposta: Sugestão acatada.

19. Itens 2.1.21 Suportar agregação de links, segundo padrão IEEE 802.3ad;

    Manifestação: Para os lotes 1 e 2, firewall de pequeno porte, solicitamos o recurso de agregação de link não seja obrigatório

    Resposta: Sugestão acatada.

20. Itens 2.1.21 Suportar agregação de links, segundo padrão IEEE 802.3ad;

    Manifestação: Recomendamos especificar este requerimento somente para appliances do porte adequado, pois agregação de links em equipamentos de pequeno porte encarece a oferta com uma funcionalidade que dificilmente será é utilizada por requerer infra-estrutura de rede (lan switches) mais complexos.
    Nos elementos de pequeno porte (firewall do tipo 01 e 02), a agregação de links supera até a capacidade nominal de processamento de dados da unidade, o que torna a funcionalidade inviável e totalmente dispensável.
    Recomendamos esta funcionalidade apenas para os equipamentos de Tipo 3, 4 e 5.

    Resposta: Sugestão acatada.

21. Itens 2.1.21 Suportar agregação de links, segundo padrão IEEE 802.3ad;

    Manifestação: Suportamos agregação de links, mas não segundo o padrão IEEE 802.3ad. Suportamos agregação de links de forma estática. Entendemos que o requerimento de criação dinâmicas de agregação de links não é muito comum em um cenário real de Firewall.

    Resposta: Sugestão parcialmente acatada.

22. Itens 2.1.22 Possuir ferramenta de diagnóstico do tipo tcpump

    Manifestação: Possuir ferramenta de diagnóstico do tipo tcpump ou equivalente;Também para o item para o item 2.1.22, sugerimos a adição da especificação abaixo como subitens do item 2.1.22afim de melhorar a funcionalidade solicitada, visto que vários fabricantes possuem essas funcionalidades em seus produtos:
    "Suportar efetuar a captura de pacotes no formato PCAP;"
    "Suportar e efetuar o download dos arquivos PCAP pela interface gráfica

    Resposta: Sugestão parcialmente acatada.

23. Itens 2.1.24 Suportar integração com serviços de diretório LDAP, Microsoft Active Directory, RADIUS e senha do sistema operacional no próprio firewall para identificação, autenticação e registros de logs, sem limite de número de usuários em relação ao licenciamento

    Manifestação: Deve possuir integração e suporte ao Microsoft Active Directory para os seguintes sistemas operacionais:
    Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2

    Resposta: Sugestão parcialmente acatada.

24. Itens 2.1.24 Suportar integração com serviços de diretório LDAP, Microsoft Active Directory, RADIUS e senha do sistema operacional no próprio firewall para identificação, autenticação e registros de logs, sem limite de número de usuários em relação ao licenciamento

    Manifestação: Recomendamos alterar a redação para indicar que as quantidades máximas de usuários de cada appliance deve ser liberada na sua total capacidade, sem licenciamento adicional associado a ela. Recomendamos ainda que se indiquem quantidades mínimas de usuários em operação dinâmica (SSO), conforme segue:

    Tipo 1: 250
    Tipo 2: 500
    Tipo 3: 2000

Tipo 4: 50.000
Tipo 5: 70.000

As capacidades acima recomendadas garantem que os appliances em suas diversas possibilidades atendam também a este quesito importante do dimensionamento..

Resposta: sugestão não acatada.

25. Itens 2.1.25 Deve identificar de forma transparente os usuários autenticados por single sign-on, inclusive por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server e OpenLDAP.

    Manifestação: Entendemos que para que ocorra uma autenticação transparente as ferramentas citadas deveriam suportar o envio ou registro da autenticação do usuário de forma a permitir sem instalação de software conforme item 2.1.27 a visualização do registro deste usuário de forma transparente no equipamento em questão, é suportado de forma transparente a consulta na base LDAP dos usuários via protocolo RADIUS o qual possibilita o envio e registro deste evento de forma a permitir a integração OpenLdap e FreeRadius para a autenticação transparente. Esta integração pode satisfazer a necessidade do item. Caso contrário, muitos fabricantes estariam desclassificados
    Proposta: Deve identificar de forma transparente os usuários autenticados por single sign-on, inclusive por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory e servidores RADIUS Microsoft Network Policy Server.

    Resposta: Sugestão parcialmente acatada.

26. Itens 2.1.25 Deve identificar de forma transparente os usuários autenticados por single sign-on, inclusive por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server e OpenLDAP.

    Manifestação: Proposta: Deve identificar de forma transparente os usuários autenticados por single sign-on, inclusive por meio de serviço de diretório, compatível no mínimo com duas das seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server e OpenLDAP

    Resposta: Sugestão parcialmente acatada.

27. Itens 2.1.25 Deve identificar de forma transparente os usuários autenticados por single sign-on, inclusive por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server e OpenLDAP.

    Manifestação: Solicitamos a modificação do item para a retirada do que corresponde a parte de OpenLDAP. O protocolo LDAP não gera informação se a autenticação foi previamente efetivada.

Caso ainda se decida manter o OpenLDAP, deve-se permitir o uso de Captive Portal ou "pop-up login" gerado pelo firewall.
"2.1.25 Deve identificar de forma transparente os usuários autenticados por single sign-on, por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server, sem instalação de software nos clientes ou estações de trabalho ou servidores;"

Resposta: Sugestão parcialmente acatada. O item foi reformulado.

28. Itens 2.1.26 Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory

Manifestação: sugerimos acrescentar o item abaixo, para permitir a identificação e diferenciação de usuários utilizando plataformas de VDI, Citrix Metaframe ou Terminal Server.

2.1.26.1. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

Resposta: Sugestão não acatada.

29. Item 2.1.27 Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos, e nem nos equipamentos dos usuários

Manifestação: solicitamos a alteração do item, uma vez que alguns fabricantes recomendam a instalação de um agente em servidor que faça parte do domínio para fazer a integração de autenticação de usuários entre o AD e a solução de NGFW ofertada. Recomendamos que seja mantida somente a parte onde se diz não seja permitida a utilização de agentes instalados nos equipamentos dos usuários.

Resposta: Sugestão acatada.

30. Item 2.1.29 Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP e UDP como, por exemplo, aplicações HTTP, HTTPS, FTP;

Manifestação: Do anexo B do termo de referência. Entendemos que o reconhecimento de usuários utilizando aplicações UDP atende ao item, haja vista que a autenticação dos usuários se dá através do protocolo TCP. Para melhorar o entendimento, sugerimos a seguinte redação para este item: "2.1.29. Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP como, por exemplo, aplicações HTTP, HTTPS, FTP."

Resposta: Sugestão acatada.

31. Item 2.1.3 Não serão aceitos equipamentos em modo End of Life ou End of Support durante a

vigência do contrato, estas informações deverão estar no site do fabricante

Manifestação: Proposta de novo texto: Não serão aceitos equipamentos em modo End of Life ou End of Support na data de assinatura do contrato.
Essas informações deverão estar presentes no site do fabricante ou ser comprovadas por carta ou documento oficial do fabricante quando da assinatura do contrato.

Resposta: Sugestão não acatada, incompatível com a demanda técnica.

32. Item 2.1.31 Deve suportar NAT 64.

Manifestação: As redes ipv6 e ipv4 podem existir simultaneamente no ambiente, o protocolo ipv6 foi um desenvolvido para não existir mais a necessidade de NAT, levando em consideração que a rede se comunica ipv6 e que todos os hosts podem ter um ipv4 e ipv6, sugerimos a retirada do item.

Resposta: Sugestão não acatada, incompatível com a demanda técnica.

33. Item 2.1.31 Deve suportar NAT 64.

Manifestação: Para o item 2.1.31, sugerimos a adição da especificação abaixo a fim de melhorar a funcionalidade solicitada, visto que vários fabricantes possuem essas funcionalidades em seus produtos: "2.1.31. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico. Deve suportar também NAT64 e NAT46;"

Resposta: Sugestão parcialmente acatada

34. Itens 2.1.31 Deve suportar NAT64. 2.1.33 Suportar nativamente IPv6 e tráfego de IPv6 tunelado em pacotes Ipv4

Manifestação: Esse tipo de funcionalidade é executada pelo roteador de borda, sendo uma funcionalidade de conexão e não de segurança. Solicitamos que seja retirado o item.

Resposta: Sugestão parcialmente acatada

35. Itens 2.1.33.1 Suportar, no mínimo, os protocolos de roteamento dinâmico RIP v2 e NG, OSPF v2 e v3, MPLS e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based, inclusive IPv6;

Manifestação: Entendemos que o suporte ao protocolo MPLS é desejável para fins de necessidade futura e não atual, haja vista as tendências de mercado para sua utilização. Quanto ao suporte a IPv6, entendemos que o mesmo é necessário para os protocolos que trabalham com essa versão do IP, mais especificamente o OSPF v3 e o BGP.
Para que possamos participar do certame, sugerimos a seguinte redação para este item: "2.1.33.1. Suportar, no mínimo, os protocolos de roteamento dinâmico RIP v2 e NG, OSPF v2 e v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based;"

Resposta: Sugestão parcialmente acatada

36. Itens 2.1.33.1 Suportar, no mínimo, os protocolos de roteamento dinâmico RIP v2 e NG, OSPF v2 e v3, MPLS e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based, inclusive IPv6;

    Manifestação: De acordo com a especificação extraída do site www.ietf.org, o MPLS foi descrito na RFC 3031. Em sua arquitetura, o protocolo de roteamento deve ser implementado entre os comutadores (switches) na rede fazendo essa função ser alheia às funções de um dispositivo de segurança descrito no Termo de Referência. Assim sendo, é recomendado editar o texto e suprimir o MPLS como exigência deste item, uma vez que esse protocolo deve ser utilizado apenas entre roteadores/comutadores.
    Suportar, no mínimo, os protocolos de roteamento dinâmico RIP v2 e NG, OSPF v2 e v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based, inclusive IPv6;

    Resposta: Sugestão parcialmente acatada

37. Itens 2.1.33.1 Suportar, no mínimo, os protocolos de roteamento dinâmico RIP v2 e NG, OSPF v2 e v3, MPLS e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based, inclusive IPv6;

    Manifestação: Para o item 2.1.33.1, solicitamos a modificação do item com a retirada do que se refere a MPLS, uma vez que MPLS não se trata de protocolo de roteamento.;

    Resposta: Sugestão acatada

38. Item 2.1.33.1 Suportar, no mínimo, os protocolos de roteamento dinâmico RIP v2 e NG, OSPF v2 e v3, MPLS e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based, inclusive IPv6; Item 2.1.76 Suportar os protocolos de roteamento RIPv2, RIP NG, OSPFv2 e OSPFv3 para as funcionalidades de VPN

    Manifestação: Solicitamos e exclusão do protocolo RIP NG.

    Resposta: Sugestão acatada

39. Item 2.1.34 Suportar os protocolos IGMP v2, IGMP v3 e PIM-SM; suportar no mínimo igmp v2 e v3 ou igmp v2, v3 e pim-sm.

    Manifestação: Se o texto original for mantido, ocasionará a limitação de participantes ao processo licitatório do presente Termo de Referência, uma vez que a tecnologia PIM-SM é focada para roteadores e switches, não para tecnologia de segurança como o firewall.
    Suportar os protocolos IGMP v2 e IGMP v3.

    Resposta: Sugestão parcialmente acatada. O item foi reformulado.

40. Item 2.1.35 Possuir funcionalidades de DHC client, server e relay;

    Manifestação: Acreditamos que a funcionalidade correta desejada seja a DHCP

    Resposta: Sugestão acatada.

41. Item 2.1.36 Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), RTCP, RTMP, RTSP, H323, SIP, tanto em IPv4 quanto em IPv6.

    Manifestação: Entendemos que os protocolos citados neste item estão em camada acima da camada Internet do modelo TCP/IP, tornando assim desnecessário citar versões específicas do protocolo IP. Para evitar entendimentos dúbios e para que possamos participar do certame, sugerimos a seguinte redação para este item: "2.1.36. Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), RTCP, RTMP, RTSP, H323 e SIP."

    Resposta: Sugestão parcialmente acatada.

42. Item 2.1.36 Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), RTCP, RTMP, RTSP, H323, SIP, tanto em IPv4 quanto em IPv6.

    Manifestação: O produto no qual representamos não suporta a proteção nos protocolos citados quando ocorre em tráfego IPv6. Sugerimos que seja aceito declaração informando que a funcionalidade está em RoadMap no fabricante e que se compromete a entregar em até 10 meses.

    Resposta: **sugestão não acatada. Não será aceito funcionalidades que estejam em RoadMap, pois as funcionalidades indicadas são necessárias na entrega imediata do equipamento.**

43. Item 2.1.4 O equipamento deverá atualizar firmware e softwares para novas versões durante 60 (sessenta) meses, estas informações deverão estar no site do fabricante.

    Manifestação: Nova sugestão de texto: O equipamento deverá atualizar firmware e softwares para novas versões durante a vigência do contrato;

    Resposta: **Sugestão acatada.**

44. Item 2.1.42 Deve suportar, no mínimo, a operação em modo gateway e transparente.

    Manifestação: Retirar o item 2.1.42, pois este se repete ao item 2.1.14.

    Resposta: **Sugestão acatada**

45. Item 2.1.43 Suportar, no mínimo, 1.000 regras ou políticas de firewall

    Manifestação: Para o item 2.1.43, sugerimos o aumento no número de regras ou políticas de firewall a

partir do lote 4 devido ao fato dos equipamentos serem de grande porte (10.000);

Resposta: Sugestão não acatada.

46. Item 2.1.43 Suportar, no mínimo, 1.000 regras ou políticas de firewall

Manifestação: Solicitamos que para o lote 1, firewall de pequeno porte, seja aceito o número de 250 políticas mantendo a proporcionalidade com o tamanho do ambiente que será atendido por este modelo.

Resposta: Sugestão acatada.

47. Item 2.1.5 Todas as portas de comunicação, interfaces e afins deverão estar habilitadas, operacionais e prontas para operação, sem custos adicionais.

Manifestação: Para o item 2.1.5, sugerimos que seja especificada a quantidade mínima de interfaces que serão usadas para cada equipamento de cada lote, com o intuito de tornar o certame competitivo entre todos os participantes. O fato de um licitante ofertar um equipamento que possua maior número de portas além daquelas que foram solicitadas nos itens 3.1.1.5, 3.15.1.4, 3.22.1.4, 3.29.1.4 só irá onerar o custo final do equipamento, pois terão que ser fornecidos os transceivers. Ressalte-se que para o Lote 2 não há exigência quanto ao número mínimo de portas.

Resposta: Sugestão acatada.

48. Item 2.1.5 Todas as portas de comunicação, interfaces e afins deverão estar habilitadas, operacionais e prontas para operação, sem custos adicionais.

Manifestação: O que dizer com relação às interfaces SFP e SFP+? Será definido e fornecido o módulo Gbic quando for o caso, considerando-se que todas as interfaces disponíveis no appliance estejam habilitadas conforme especificado? Recomendamos a alteração da redação de modo a adequar e clarificar este requerimento.

Resposta: Sugestão acatada.

49. Item 2.1.5 Todas as portas de comunicação, interfaces e afins deverão estar habilitadas, operacionais e prontas para operação, sem custos adicionais. Item 2.1.10 O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.

Manifestação: Solicitamos esclarecimentos quanto a este item. No caso dos nossos firewalls, as caixas são fornecidas de fábrica com todas as interfaces de rede possíveis e sem Gbics. Neste caso teremos que fornecer Gbics apenas para a quantidade de portas exigidas no edital? No caso de outros fabricantes do mercado, a caixa vem de fábrica com número inicial de interface e posteriormente podem ser adicionadas novas placas de interfaces. Neste cenário o fabricante terá que fornecer o appliance com a quantidade máxima de interfaces que o equipamento suporta ou somente a quantidade pedida no edital.
Nossa sugestão é que para ambos os casos (interfaces e gbics), seja fornecido apenas a quantidade exigida no edital. E não a capacidade total suportada pelo equipamento pronta para uso como os dois

itens pedem.

Resposta: **Sugestão acatada**

50. Item 2.1.50 Possuir suporte a, no mínimo, dois algoritmos de balanceamento de carga para novas conexões de rede a servidores internos

    Manifestação: Não suportamos balanceamento de servidores. Entendemos que o serviço de balanceamento para maior efetividade deve estar fora do firewall em equipamento exclusivo para isso. Este item impede a participação de firewalls.

    Resposta: Sugestão acatada

51. Item 2.1.58 Funcionalidades de gerência local do firewall ou do cluster (virtual ou físico) do qual o firewall faz parte

    Manifestação: Nosso gerenciamento é feito por interface gráfica centralizada o qual é responsável por configurar o cluster, nossa estrutura traz vantagens para um ambiente escalável e de fácil dimensionamento, os equipamentos funcionam como engines que são configurados via plataforma de gerencia remota. Todas as informações podem ser obtidas via interface gráfica centralizada inclusive todos os processos associados.
    Funcionalidades de gerência centralizada do firewall ou do cluster (virtual ou físico) do qual o firewall faz parte

    Resposta: **Sugestão parcialmente acatada**

52. Item 2.1.58 Funcionalidades de gerência local do firewall ou do cluster (virtual ou físico) do qual o firewall faz parte

    Manifestação: sugerimos acrescentar níveis de segurança adicionais para Radius, Microsoft AD e Certificado Digital com duplo fator para a administração da solução de segurança

    Resposta: Sugestão não acatada, improcedente com a demanda técnica.

53. Item 2.1.58.10 Deve ser capaz de testar a conectividade dos equipamentos gerenciados.

    Manifestação: Para o item 2.1.58.10, solicitamos a realocação deste item para os itens 2.2, que se referem a gerenciamento centralizado. Para os equipamentos que possuem gerência local, não há forma de testar conectividade em si mesmo;

    Resposta: **Sugestão acatada**

54. Item 2.1.58.11 Deve prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes ou regras equivalentes.

Manifestação: Para o item 2.1.58.11, solicitamos a realocação deste item para os itens 2.2, que se referem a gerenciamento centralizado. Nossa solução de gerenciamento centralizado suporta esta funcionalidade;

Resposta: **Sugestão acatada**

55. Item 2.1.58.11 Deve prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes ou regras equivalentes.

Manifestação: Recomendamos a remoção deste requerimento, e considerar que ela deve ser contemplada em item independente, pois congrega alta criticidade na escolha dos parâmetros de definição da duplicidade e prioridade das regras.
Ainda, cada fabricante utiliza metodologias diferentes de otimização de segurança que não necessariamente passem pela eliminação de regras similares ou não, o que pode inviabilizar a nossa participação e outros fabricantes que tem conceitos diferentes para este quesito.

Resposta: **Sugestão não acatada, improcedente com a demanda técnica.**

56. Item 2.1.6 Todas as licenças de hardware e software devem ser fornecidas em caráter perpétuo, atualizadas em suas últimas versões disponíveis, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares durante o contrato ou após o seu término.

Manifestação: As funcionalidades de firewall, controle de aplicações, IPS, antimalware, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante

Resposta: Sugestão parcialmente acatada quanto ao tratamento de conteúdo web.

57. Item 2.1.6 Todas as licenças de hardware e software devem ser fornecidas em caráter perpétuo, atualizadas em suas últimas versões disponíveis, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares durante o contrato ou após o seu término.

Manifestação: Serviços avançados de segurança (IPS, Anti-Malware, Sandbox/APT, NGFW) são funcionalidades do software que dependem de renovação, e não são de caráter perpétuo. A atualização de assinaturas é inerente a esta renovação e não pode ser tratada de forma separada.
O fornecimento deve considerar propriedade perpétua de hardware e sistema operacional, mas os serviços de segurança associados ao software não são perpétuos e dependentes de renovação frequente. Desta forma, é correto interpretar que é esperada a desativação dos serviços avançados de segurança, apesar da propriedade de hardware e software ser permanente?

Resposta: Sugestão parcialmente acatada.

58. Item 2.1.62 As funcionalidades de VPN não podem possuir qualquer restrição de licenciamento, inclusive em relação ao número de clientes, IPs e máquinas

Manifestação: De acordo com documentos de Datasheet, oferecidos pelos principais fabricantes de

firewall, que atuam no mercado mundial, todos os equipamentos elegíveis, possuem limitação de acessos VPN, independentemente da quantidade de licenças, por uma questão de recursos físicos de Hardware.

A especificação de throughput exigida no termo de referência, propõe um determinado valor para utilização desta funcionalidade, que deverá ser atendida pelos participantes do certame, independentemente do número de licenças que serão ou não fornecidas.

Assim sendo, entendemos ser totalmente irrelevante a necessidade de exigir-se uma quantidade ilimitada de licenças de acessos simultâneos, uma vez que a especificação técnica de termo de referência propõe o quantitativo exigido de throughput dos hardwares para cada Lote que é o fator limitador da quantidade de acessos simultâneos

As funcionalidades de VPN deverão atender à demanda, independente de licenciamento, e/ou quantidade de clientes, IPs e máquinas, respeitando a capacidade máxima de throughput exigida nas especificações técnicas dos lotes deste Termo de Referência.

Resposta: Sugestão acatada.

59. Item 2.1.62 As funcionalidades de VPN não podem possuir qualquer restrição de licenciamento, inclusive em relação ao número de clientes, IPs e máquinas

Manifestação: Sobre as capacidades de quantidades concorrentes de VPNs, recomendamos indicar que as capacidades nativas do appliances devem atender minimamente à demanda, com a possibilidade de expansão futura através de licenciamento adicional de acordo com a necessidade de cada órgão.

Recomendamos que as quantidades mínimas sejam iniciadas conforme segue:

Tipo1: 10
Tipo2: 25
Tipo3: 300
Tipo4: 2000
Tipo5: 2000

Recomendamos ainda que se determine que a instalação de clientes nas máquinas remotas (PCs, Tablets, Smartphones) seja livre de licenciamento adicional, ou seja, todo o licenciamento de VPNs esteja restrito unicamente aos appliances.

Resposta: Sugestão parcialmente acatada.

60. Item 2.1.67 Deve permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface Web do tipo portal, devendo o cliente instalável estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10), Linux, Mac OS X e para os sistemas móveis Apple iOS e Google Android. O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 7 ou superior, Firefox 3.6 ou superior;

Manifestação: A alteração do texto continua atendendo às necessidades do Órgão, mantendo a imparcialidade, princípios éticos e morais da Administração Pública Federal, pois permitirá, assim, a participação de todos os fabricantes renomados de soluções de UTM/NGFW garantindo o princípio da

livre concorrência aliada aos anseios do Ministério.

Deve permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface Web do tipo portal, devendo o cliente instalável estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10), Mac OS X podendo Linux e os sistemas móveis Apple iOS e Google Android utilizarem clientes nativos. O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 7 ou superior, Firefox 3.6 ou superior;

Resposta: Sugestão parcialmente acatada

61. Item 2.1.67 Deve permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface Web do tipo portal, devendo o cliente instalável estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10), Linux, Mac OS X e para os sistemas móveis Apple iOS e Google Android. O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 7 ou superior, Firefox 3.6 ou superior;

Manifestação: Para o item 2.1.67, solicitamos duas alterações: A primeira alteração do item é devido ao fato de navegadores como por exemplo internet explorer 7 e outros em versões inferiores, não possuírem mais suporte pelo seu fabricante. A segunda é que este item está vinculado ao 2.1.64 e portanto, deve ter a sua posição no texto modificada. 2.1.67. Deve permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do seu
equipamento ou por meio de interface Web do tipo portal, devendo o cliente instalável estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10), Linux, Mac OS X e para os sistemas móveis Apple iOS e Google Android. O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 9 ou superior, Firefox 5.6 ou superior

Resposta: Sugestão parcialmente acatada

62. Item 2.1.68 Deve suportar a customização da interface Web portal pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;

Manifestação: Solicitamos a remoção deste item, pois ele trata especificamente de serviços que não necessariamente se aplicam a firewalls de nova geração.
Para a nossa participação neste processo, solicitamos que este item, se mantido, especifique que:

1- O portal deve ser fornecido em tecnologia SSL
2- Deve possibilitar customização
3- Deve suportar pelo menos 4 serviços/protocolos distintos (SSH, Telnet, RDP, VNC).

Serviços de portal e/ou proxy reverso completos são oferecidos por appliances destinados a esta funcionalidade específica, e a integração destes serviços em firewall multifuncional torna o uso limitado e encarece a oferta desproporcionalmente.

Resposta: O item foi reformulado.

63. Item 2.1.74 Permitir alteração dos algoritmos criptográficos da VPNs permitindo a inserção de criptografia de estado.

Manifestação: Acreditamos que o objetivo a ser alcançado seja garantir que o equipamento ofertado forneça segurança para as comunicações VPN, estando livre de qualquer tipo de backdoor no tocante aos algoritmos criptográficos utilizados.
Para garantir que esse objetivo seja alcançado, sugerimos a seguinte redação para este item: "2.1.74. Permitir alteração dos algoritmos criptográficos das VPNs permitindo a inserção de criptografia de estado ou o fabricante deve apresentar carta juramentada por parte de representante legal informando que o equipamento ofertado está livre de qualquer tipo de backdoor relacionado aos algoritmos criptográficos utilizados pela solução

Resposta: O item foi removido.

64. Item 2.1.74 Permitir alteração dos algoritmos criptográficos da VPNs permitindo a inserção de criptografia de estado.

Manifestação: Solicitamos a retirada da parte do item onde diz "permitindo a inserção de criptografia de estado", uma vez que existem fabricantes que não suportam esta funcionalidade;

Resposta: Sugestão acatada.

65. Item 2.1.77 Implementar autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS.

Manifestação: Para o item 2.1.77, sugerimos a adição de suporte a duplo fator de autenticação, através de token, físico ou mobile, ou tokenless, como email ou sms, devido ao fato de alguns fabricantes conseguirem entregar uma maior capacidade de segurança para compor a solução;

Resposta: **Sugestão não acatada.**

66. Item 2.1.81 Possuir gerenciamento gráfico centralizado das funcionalidades de VPN e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface);

Manifestação: Nosso gerenciamento é feito por interface gráfica centralizada, os equipamentos funcionam como engines que são configurados via plataforma de gerencia remota. Todas as informações podem ser obtidas via interface gráfica centralizada inclusive todos os processos associados.
Possuir gerenciamento gráfico centralizado das funcionalidades de VPN e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução.

Resposta: Sugestão parcialmente acatada

67. Item 2.1.84 O equipamento deve ser apropriado para o uso em ambiente tropical com umidade

relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.

Manifestação: Entendemos que 0°C é uma temperatura que não será alcançada se os equipamentos estiverem instalados em ambientes adequados. Entendemos também que, da mesma forma, 90% é um umidade relativa que não será alcançada caso os equipamentos sejam instalados em ambientes adequados.
Levando estes pontos em consideração, pedimos para definir a faixa de temperatura de operação entre 5°C to 40°C e a umidade relativa de 10 a 85%.

Resposta: Sugestão parcialmente acatada

68. Item 2.2.1 Deverá ser fornecida solução gerenciável do mesmo fabricante externamente ao equipamento. Podendo ser um "appliance especializado" – equipamento especializado para gerência centralizada ou "appliance virtual" - solução de software baseada em máquina virtual que possa ser instalado e executado em ambientes virtuais, tais como: VMware vSphere, Xen, KVM and Hyper-V platforms.

Manifestação: Nossa solução de gerenciamento pode ser instalado em Vmware vSphere. Entendemos que, para o atendimento do item, a solução pode suportar ser instalada em um dos ambientes virtuais citados. Está correto?
Deverá ser fornecida solução gerenciável do mesmo fabricante externamente ao equipamento. Podendo ser um "appliance especializado" – equipamento especializado para gerência centralizada ou "appliance virtual" - solução de software baseada em máquina virtual que possa ser instalado e executado em ambientes virtuais, tais como: VMware vSphere, Xen, KVM OU Hyper-V platforms.

Resposta: Sugestão acatada

69. Item 2.2.1.1 Quando executado em ambientes virtuais, deverão ser fornecidas e implantadas, em caráter perpétuo, todas as licenças dos softwares e sistemas operacionais necessários ao funcionamento da solução.

Manifestação: Foi esclarecido na audiência pública que os recursos de virtualização da plataforma correm por conta dos órgãos contratantes.
Cabe apenas confirmar que as licenças adicionais de software mencionadas somente se aplicam quando a solução de gerência centralizada for instalada em sistemas operacionais que não aqueles nativos dos próprios appliances virtuais.

Resposta: O item foi reformulado.

70. Item 2.2.10 Deve automatizar o sincronismo de regras, objetos e políticas em tempo real.

Manifestação: Gostaríamos de pedir esclarecimento para este item. O que o MPOG entende como automatizar o sincronismo de regras, objetos e políticas em tempo real?

Resposta: O item foi reformulado.

71. Item 2.2.14 Deve permitir validar as regras antes e depois de aplicá-las

Manifestação: Para o item 2.2.14, solicitamos a modificação do item para esclarecer aos licitantes a real expectativa quanto ao item solicitado: 2.2.14 . Deve permitir a validação de regras, podendo isto ser feito a qualquer momento ou antes de aplicá-las;

Resposta: O item foi reformulado.

72. Item 2.2.14 Deve permitir validar as regras antes e depois de aplicá-las

    Manifestação: Que tipo de validação o MPOG espera antes de aplicar as regras?

    Resposta: O item foi reformulado.

73. Item 2.2.4 Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

    Manifestação: A fim de permitir a nossa participação, solicitamos que seja removida esta exigência.

    Resposta: O item foi reformulado.

74. Item 2.2.4 Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

    Manifestação: A plataforma de gerenciamento centralizado atualmente fornecida por nós não contempla correlação de eventos.
    Solicitamos a remoção deste item de modo a possibilitar nossa participação no certame, ou que seja aberta a possibilidade de fornecimento de plataforma adicional que entregue este requerimento de forma separada e complementar.

    Resposta: O item foi reformulado.

75. Item 2.2.7 Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.
    Manifestação: Não podemos filtrar os logs do equipamento por país de origem e destino. Pedimos a remoção dessa funcionalidade.

    Resposta: solicitação não acatada. A funcionalidade é requisito da demanda técnica.

76. Item 2.2.7 Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.

    Manifestação: Não podemos filtrar os logs do equipamento por país de origem e destino.
    Pedimos a remoção dessa funcionalidade.

    Resposta: solicitação não acatada. A funcionalidade é requisito da demanda técnica.

77. Item 2.3.17 Possuir as estratégias de bloqueio, liberar e bloquear, sendo este suportando quarentenar o IP, selecionáveis tanto por conjuntos de assinaturas quanto por cada assinatura.

Manifestação: Recomendamos a remoção do requerimento "Liberar e bloquear, quarentena", pois julgamos que cabe às equipes de segurança de cada órgão avaliar os bloqueios efetuados pelo elemento de segurança, e em função disso torná-los permanentes ou não.
O simples ato de quarentenamento oferece vulnerabilidade desnecessária ao ambiente, uma vez que os critérios de quarentena podem abrir e fechar janelas de exploração caso a política não seja adequada.
Solicitamos ainda que este requerimento seja removido para que possamos participar do certame, uma vez que em função do exposto acima não incluímos essa característica em nossos produtos.

Resposta: sugestão acatada.

78. Item 2.3.17 Possuir as estratégias de bloqueio, liberar e bloquear, sendo este suportando quarentenar o IP, selecionáveis tanto por conjuntos de assinaturas quanto por cada assinatura;

    Manifestação: Por motivo de segurança, não possuímos esta funcionalidade de quarentena de IP em seus equipamentos firewall, tendo em vista este recurso gerar riscos na rede por exigir alta gerencia devido à regra de quarentena ser um bloqueio provisório o que pode ser liberado após o prazo de quarentena. Por este motivo solicitamos que a exigência de quarentar o IP seja removido.

    Resposta: sugestão acatada.

79. Item 2.3.19 Possuir gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface).

    Manifestação: Nosso gerenciamento é feito por interface gráfica centralizada, os equipamentos funcionam como engines que são configurados via plataforma de gerencia remota. Todas as informações podem ser obtidas via interface gráfica centralizada inclusive todos os processos associados. Sugestão: "Possuir gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução;"

    Resposta: sugestão parcialmente acatada.

80. Item 2.3.2 Possuir no mínimo um conjunto de 2.000 assinaturas de detecção e prevenção de ataques, permitindo também ataques baseados em anomalias.
    Manifestação: Para o cenário atual de ameaças, recomendamos que este número seja incrementado, oferecendo assim aos órgãos uma cobertura mais ampla de proteção.
    Sugestão: 3.000.

    Resposta: sugestão não acatada, improcedente com a demanda técnica.

81. Item 2.3.21 Taxa mínima de detecção de 80% (oitenta), tendo no máximo 15% (quinze) de falso positivo.
    Manifestação: Para o item 2.3.21, solicitamos que melhore texto identificando de que forma deve ser comprovado o requerido, indicando a metodologia que será adotada durante o teste.

    Resposta: sugestão parcialmente acatada.

82. Item 2.3.6 Detectar e Proteger contra, no mínimo, os ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple MessageTransfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol), DNS (Domain Name System), FTP, SSH , Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP, CHARGEN, RDP (Remote

Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking.

Manifestação: Entendemos que o protocolo CHARGEN escuta na porta 19 TCP e UDP e o mesmo caiu em desuso, com isso, entendemos que não se faz necessário proteção específica para o mesmo, haja vista a possibilidade de bloqueio do mesmo através da porta utilizada.
Para que possamos participar do certame, sugerimos a seguinte redação para este item: "2.3.6. Detectar e Proteger contra, no mínimo, os ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol), DNS (Domain Name System), FTP, SSH , Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP ou CHARGEN, RDP (Remote Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking."

Resposta: sugestão acatada.

83. Item 2.4.2 Possuir funcionalidade de varredura contra vírus e malwares em tráfego HTTPS, HTTP, FTP, POP3, IMAP e SMTP.

Manifestação: O produto no qual representamos apenas não provê a varredura contra vírus e malware em tráfego HTTPS. Sugerimos que seja aceito declaração informando que a funcionalidade está em RoadMap no fabricante e que se compromete a entregar em até 10 meses.

Resposta: sugestão não acatada. Não será aceito funcionalidades que estejam em RoadMap, pois as funcionalidades indicadas são necessárias na entrega imediata do equipamento.

84. Item 2.4.2 Possuir funcionalidade de varredura contra vírus e malwares em tráfego HTTPS, HTTP, FTP, POP3, IMAP e SMTP.

Manifestação: Considerando que os servidores de e-mail das organizações normalmente ficam localizados em uma rede DMZ, o tráfego de e-mails enviados e recebidos através do protocolo SMTP será inspecionado e protegido pelo Firewall multifuncional, com isso a demanda por inspeção e proteção para os protocolos POP3 e IMAP é cada vez menor, haja vista que, em sua grande maioria, o tráfego destes protocolos ocorre dentro da rede interna não passando pelos Firewalls. Portanto, entendemos que a varredura contra vírus nos protocolos POP3 e IMAP deva ser efetuada por softwares anti-vírus instalados nos próprios servidores que executam esses protocolos.
Para que possamos participar do certame, sugerimos a seguinte redação para este item: "2.4.2. Possuir funcionalidade de varredura contra vírus e malwares em tráfego de pelo menos três dos seguintes protocolos: HTTPS, HTTP, FTP, POP3, IMAP e SMTP."

Resposta: sugestão parcialmente acatada.

85. Item 2.4.3 Deve ser capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, SNMP e e-mail.

Manifestação: Para o item 2.4.3, solicitamos a retirada do protocolo SNMP, uma vez que alguns fabricantes não suportam este protocolo para o tipo de alerta solicitado;

Resposta: sugestão acatada.

86. Item 2.4.6 Possuir gerenciamento gráfico centralizado das funcionalidades de antivírus e anti-malware integrado com gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface).

Manifestação: Nosso gerenciamento é feito por interface gráfica centralizada, os equipamentos funcionam como engines que são configurados via plataforma de gerencia remota. Todas as informações podem ser obtidas via interface gráfica centralizada inclusive todos os processos associados.
Possuir gerenciamento gráfico centralizado das funcionalidades de antivírus e anti-malware integrado com gerenciamento centralizado da solução.

Resposta: sugestão parcialmente acatada.

87. Item 2.4.8 Taxa mínima de detecção de 80% (oitenta), tendo no máximo 15% (quinze) de falso positivo.

    Manifestação: Para o item 2.4.8, solicitamos que melhore texto identificando de que forma deve ser comprovado o requerido, indicando a metodologia que será adotada durante o teste.

    Resposta: sugestão parcialmente acatada.

88. Item 2.5.1 Possuir base mínima contendo 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas.

    Manifestação: Para o item 2.5.1, sugerimos um melhoramento do item, visto que a maioria dos fabricantes possuem números bem maiores em suas bases de dados: "2.5.1. Possuir base mínima contendo 250 (duzentos e cinquenta) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 70 (setenta) categorias ou subcategorias pré-definidas".

    Resposta: sugestão não acatada

89. Item 2.5.10 Capacidade de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão.

    Manifestação: Não suportamos este item. Pedimos que o item seja removido para a nossa participação.

    Resposta: Sugestão não acatada. A comunicação com o usuário é um ponto importantíssimo, corroborando com a inserção da cultura da segurança da informação.

90. Item 2.5.10 Capacidade de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão.

    Manifestação: Não suportamos este item. Pedimos que o item seja removido para a nossa participação.

    Resposta: Sugestão não acatada. A comunicação com o usuário é um ponto importantíssimo, corroborando com a inserção da cultura da segurança da informação.

91. Item 2.5.11 Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;

    Manifestação: Este item é pedido dentro do filtro de URL. Pode ser atendido através da criação de aplicações em camada 7 customizadas?

Resposta: sugestão acatada.

92. Item 2.5.12 Permitir o bloqueio de URLs inválidas cujo campo CN ou DN do certificado SSL não contém um domínio válido.

    Manifestação: Não suportamos este item. Pedimos que o item seja removido para a nossa participação.

    Resposta: sugestão não acatada, tal item é requisito da demanda técnica.

93. Item 2.5.12 Permitir o bloqueio de URLs inválidas cujo campo CN ou DN do certificado SSL não contém um domínio válido.

    Manifestação: Não suportamos este item. Pedimos que o item seja removido para a nossa participação.

    Resposta: sugestão não acatada, tal item é requisito da demanda técnica.

94. Item 2.5.13 Permitir o bloqueio de páginas web por classificação, como páginas que facilitam a busca de áudio, vídeo, imagem, URLs originadas de spam e sites de proxys anônimos.

    Manifestação: Para o item 2.5.13, sugerimos a modificação do item para fins de melhor entendimento dos licitantes: "2.5.13. Permitir o bloqueio de páginas web por classificação, tais como páginas de streaming, radio e tv online, P2P, URLs originadas de spam e sites de proxys anônimos entre outros."

    Resposta: sugestão acatada.

95. Item 2.5.15 Possuir categorização de sites governamentais nacionais, mesmo não tendo domínio ".gov.br.".

    Manifestação: Para o item 2.5.15, sugerimos a modificação do item para fins de melhor entendimento dos licitantes: "2.5.15. Possuir categorização de sites governamentais, mesmo não tendo domínio ".gov" ou ".gov.br.".

    Resposta: sugestão acatada.

96. Item 2.5.16 Categorizar as URLs com taxa de acerto mínima de 85% (oitenta e cinco), tendo no máximo 20% de categorização como desconhecida.

    Manifestação: Para o item 2.5.16, solicitamos que melhore texto identificando de que forma deve ser comprovado o requerido, indicando a metodologia que será adotada durante o teste.

    Resposta: sugestão parcialmente acatada.

97. Item 2.5.17 Suportar e forçar pesquisas seguras em sistemas de buscas, contemplando no mínimo, Google, Bing e Yahoo.

    Manifestação: Para permitir o fornecimento de nossos equipamentos, solicitamos que seja aceito equipamento que contemple no mínimo duas dos três sistemas de buscas.
    Sugestão de texto: Suportar e forçar pesquisas seguras em pelo menos dois sistemas de buscas, contemplando Google e/ou Bing e/ou Yahoo.

Resposta: sugestão acatada.

98. Item 2.5.17 Suportar e forçar pesquisas seguras em sistemas de buscas, contemplando no mínimo, Google, Bing e Yahoo.

    Manifestação: Para a nossa participação neste certame, solicitamos a remoção do requerimento de Safe Search para Yahoo, uma vez que este ainda não oferece mecanismos adequados para que o controle seja efetivamente realizado, conforme já ocorre com Google e Bing.

    Resposta: sugestão acatada.

99. Item 2.5.4 Prover o funcionamento mínimo do engine de filtragem web mesmo que a comunicação com o site do fabricante esteja fora de operação.

    Manifestação: Para o item 2.5.4, solicitamos a retirada do item, uma vez que devido ao grande número de sítios criados e recategorizados diariamente, alguns fabricantes trabalham com essa categorização online a fim de ter uma assertividade bem maior, diminuindo seus índices de falsos positivos a níveis incrivelmente baixos, dessa forma.

    Resposta: sugestão acatada.

100. Item 2.5.4 Prover o funcionamento mínimo do engine de filtragem web mesmo que a comunicação com o site do fabricante esteja fora de operação.

    Manifestação: Esta funcionalidade pode ser alcançada através do uso limitado de listas locais de permissão e/ou exclusão de acessos. Ferramentas modernas e adequadas ao cenário atual de ameaças não tem capacidade de armazenar localmente as bases de dados de URLs necessárias ao cumprimento desta funcionalidade e, portanto, não operam plenamente sem o contato com suas respectivas bases de conhecimento na nuvem.
    Podemos considerar que o funcionamento mínimo requerido se baseia nas listas de permissão/exclusão limitadas inerentes às características de cada fabricante?
    Como atendemos através destas listas mencionadas, não vamos comentar este item.

    Resposta: O item será excluído.

101. Item 2.5.5 Suportar filtragem e categorização das URLs, mesmo sem conectividade com a Internet.

    Manifestação: Entendemos que se a conectividade falhar não existe a necessidade de categorização para url, pois nenhum site ou link estará disponível e nenhum usuário conseguiria acesso. Por tanto sugerimos a retirada do item.

    Resposta: sugestão parcialmente acatada.

102. Item 2.5.5 Suportar filtragem e categorização das URLs, mesmo sem conectividade com a Internet.

    Manifestação: Para o item 2.5.5, solicitamos a revisão do item devido ao fato que uma vez que o equipamento não possui conectividade com a internet, não se faz necessário a filtragem e categorização de URLs.

    Resposta: sugestão acatada.

103. Item 2.5.9 Permitir a criação de quotas de utilização por categorias.

Manifestação: Permitir a criação de agendamentos em tempos determinados de utilização por categorias.

Resposta: sugestão não acatada.

104. Item 2.5.9 Permitir a criação de quotas de utilização por categorias.

Manifestação: não suportamos a criação de quotas para usuários. A #### decidiu não desenvolver esta funcionalidade, pois ela faz com que os usuários da empresa comecem a compartilhar senhas do (AD/LDAP). Quando, por exemplo, a quota de um usuário no acesso a redes sociais acabar, ele pede a outro usuário a senha emprestada para seguir com o acesso. O problema de segurança causado por esta funcionalidade é maior do que o beneficio. Em contra partida permitimos políticas de QOS por aplicação (youtube, whatsapp. Etc), por usuário e grupo do (AD, Openldap, etc) e o agendamento do horário que o usuário pode acessar com granularidade por política.

Resposta: sugestão trata de usuários, o item trata de categorias.

105. Item 2.6.1 Possuir módulo de filtro de aplicações e de conteúdo desenvolvido e mantido pelo próprio fabricante, no mesmo equipamento do firewall.

Manifestação: A exigência de que o fabricante de firewall seja desenvolvedor das soluções de filtro de aplicações de conteúdo restringe a participação de soluções líderes de mercado e é contraprodutiva, pois é notório que se um equipamento fizer uso da melhor solução de filtro de conteúdo disponível em mercado a sua eficiência será muito melhor.
A alteração de texto sugerida tem como objetivo permitir que todos os principais fabricantes de firewall possam participar do certame.
Possuir módulo de filtro de aplicações e de conteúdo desenvolvido e mantido pelo próprio fabricante ou por parceiros homologados, no mesmo equipamento do firewall.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

106. Item 2.6.11 Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory.

Manifestação: (sem texto).

Resposta: sugestão incompleta. Faltou o texto da manifestação.

107. Item 2.6.12 Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer-to-peer, streaming e download de aúdio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e e-mail.

Manifestação: Para o item 2.6.12, sugerimos o aumento mínimo para 2.200 (duas mil e duzentas) aplicações, visto que a maioria dos fabricantes possuem números bem maiores em suas bases de dados.

Resposta: sugestão não acatada

108. Item 2.6.12 Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer-to-peer, streaming e download de aúdio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.

Manifestação: Para o cenário atual de ameaças, recomendamos que este número seja incrementado, oferecendo assim aos órgãos uma cobertura mais ampla de proteção. Sugestão: 3.500.

Resposta: sugestão não acatada

109. Item 2.6.13 Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Tinder, Instagram, Twitter, Twitcam, Tweetdeck, Linkedin, Dropbox, Google Drive, Skydrive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex e Telegram.

Manifestação: A base de aplicações mantidas por cada fabricante pode variar diante a heterogeneidade dos ambientes demandados pelo Mercado. Cada fabricante possui mecanismos de demandar e/ou criar aplicações que sejam consonantes à realidade de uma determinada organização.
Foi observada que a lista de aplicações que deverão ser identificadas e tratadas pode tirar a capacidade competitiva de determinados fabricantes e/ou excluí-los do processo, criando vantagem e exclusividade para um único fabricante.
"Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Instagram, Twitter, Tweetdeck, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR e Webex."

Resposta: sugestão acatada.

110. Item 2.6.13 Identificação, bloqueio e restrinção em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Tinder, Instagram, Twitter, Twitcam, Tweetdeck, Linkedin, Dropbox, Google Drive, Skydrive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex e Telegram.

Manifestação: Para o item 2.6.13, solicitamos a substituição de aplicações SkyDrive para OneDrive e remoção de aplicações TwitCam e TweetDeck, uma vez que TwitCam utiliza protocolos de streaming e que TweetDeck é identificado como Twittter;

Resposta: sugestão acatada.

111. Item 2.6.14 Categorizar as aplicações com taxa de acerto mínima de 85% (oitenta e cinco), tendo no máximo 30% (trinta) de categorização como desconhecida.

Manifestação: solicitamos que melhore texto identificando de que forma deve ser comprovado o requerido, indicando a metodologia que será adotada durante o teste.

Resposta: O item foi reformulado.

112. Item 2.6.2 Deve ser capaz de identificar se as aplicações estão utilizando sua porta default.

Manifestação: Para o item 2.6.2, sugerimos a modificação do item para fins de melhor entendimento dos licitantes: "2.6.2. Deve ser capaz de identificar as aplicações mesmo que não estejam utilizando sua porta default;"

Resposta: sugestão acatada.

113. Item 2.6.3 Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.

Manifestação: O produto no qual representamos apenas não é capaz de identificar aplicações encapsuladas dentro de protocolos HTTPS. Sugerimos que seja aceito declaração informando que a funcionalidade está em RoadMap no fabricante e que se compromete a entregar em até 10 meses.

Resposta: Sugestão não acatada. Não será aceito funcionalidades que estejam em RoadMap, pois as funcionalidades indicadas são necessárias na entrega imediata do equipamento.

114. Item 2.6.4 Deve ser capaz de identificar aplicações criptografadas usando SSL.

Manifestação: Sugerimos que seja aceito declaração informando que a funcionalidade está em RoadMap no fabricante e que se compromete a entregar em até 10 meses.

Resposta: Sugestão não acatada. Não será aceito funcionalidades que estejam em RoadMap, pois as funcionalidades indicadas são necessárias na entrega imediata do equipamento.

115. Item 2.7.2 A carga horária mínima do treinamento não poderá ser inferior a 40 horas, a turma conterá 5 pessoas e a ementa deverá contemplar, no mínimo.

Manifestação: A carga horária de treinamentos varia de acordo com cada fabricante e o conteúdo de seus treinamentos oficiais. Desta forma seria interessante que as horas de treinamentos sejam de acordo com cada fabricante.
Sugerimos alterar a redação de forma a contemplar às 40 horas com a prestação de serviços adicionais pela contratada e/ou fabricantes das soluções, de modo que a carga horária seja atingida mediante a prestação de serviços adicionais de "Transferência de tecnologia" após a conclusão dos treinamentos oficiais.
Como alternativa, solicitamos que a carga horária mínima dos treinamentos seja reduzida para 24 horas, (ou curso de 3 dias), que é o tempo atual do treinamento entregue por nós para esta tecnologia

Resposta: sugestão parcialmente acatada.

116. Item 2.7.2 A carga horária mínima do treinamento não poderá ser inferior a 40 horas, a turma conterá 5 pessoas e a ementa deverá contemplar, no mínimo

Manifestação: Cada fabricante possui sua carga horária de treinamentos, portanto deve ser exigido que o treinamento seja oficial do fabricante respeitando a carga horária oficial do treinamento ofertado pelo fabricante.
Solicitação: Solicitamos que seja aceito também treinamento não oficial do fabricante, desde que este seja ministrado por parceiro do fabricante com instrutores certificados pelo fabricante e que entregue todo o material didático (apostilas, certificados, provas, etc).

Resposta: sugestão parcialmente acatada.

117. Item 2.7.3 Os treinamentos deverão ser realizados no Brasil, em português, em local fornecido pela CONTRATADA, em qualquer uma das capitais das Unidades da Federação a ser indicada pela CONTRATANTE. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades incluindo os recursos áudio visuais e laboratórios necessários, sem ônus algum para a CONTRATANTE.

Manifestação: Solicitamos que seja aceitos treinamentos virtual para as localidades mais remotas, caso contrário, o valor de compra do treinamento será bem superior ao valor do equipamento firewall ofertado.

Resposta: sugestão parcialmente acatada.

118. Item 2.7.3 Os treinamentos deverão ser realizados no Brasil, em português, em local fornecido pela CONTRATADA, em qualquer uma das capitais das Unidades da Federação a ser indicada pela CONTRATANTE. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades incluindo os recursos áudio visuais e laboratórios necessários, sem ônus algum para a CONTRATANTE.

Manifestação: Oferecemos treinamentos em 5 capitais. Nas demais somente com turmas fechadas e sob demanda.
Solicitamos alterar a redação de forma a concentrar os treinamentos por geografias que se adéquem a uma quantidade menor de pontos de presença, reduzindo assim os custos inerentes ao fornecimento destes treinamentos.
Aceitar que nas localidades mais remotas os treinamentos sejam executados de forma WEB.

Resposta: sugestão parcialmente acatada.

119. Item 2.7.6 Toda a documentação didática necessária aos cursos de treinamento deverá ser disponibilizada em papel impresso e mídia digital.

Manifestação: Podemos interpretar por "mídia digital" como acesso ao conteúdo dos treinamentos via web/cloud?

Resposta: interpretação correta. Sim a interpretação de "mídia digital" abrange conteúdos via web/cloud.

120. Item 2.7.9 A CONTRATANTE poderá, a seu critério, reproduzir o material didático usado e treinar multiplicadores para repetir o treinamento sem custos adicionais.

Manifestação: Atualmente o nosso treinamento oficial somente permite que cada aluno tenha acesso a uma cópia impressa do material, e é vedada a reprodução deste. Solicitamos que este requerimento seja alterado, de forma a preservar os quesitos de propriedade de direito única de cada treinamento ofertado.

Resposta: Sugestão não acatada. Conforme exposto na audiência pública, a reprodução do material não é com intuito comercial.

121. Item 3. DEFINIÇÃO DOS LOTES E ITENS
Manifestação: Equipamento do Tipo 1 (Lote 1 - Item 1):
Vazão máxima de 100 Mbps, no entanto, são exigidas 4 interfaces 10x100x1000.
1. Um equipamento com 4 interfaces 10x100 poderiam suprir a necessidade!
2. Discos SSD em equipamento deste porte?
3. Sugerimos remover capacidade de armazenamento interno;

Resposta: sugestão parcialmente acatada.

122. Item 3. DEFINIÇÃO DOS LOTES E ITENS
Manifestação: Equipamento Tipo 2 (Lote 2 - Item 1):
1. Tem vazão máxima indicada, porém, não tem definida a quantidade e tipo de interfaces de rede.
2. Discos SSD em equipamentos de pequeno porte!
3. Sugerimos remover capacidade de armazenamento interno;

Resposta: sugestão parcialmente acatada..

123. Item 3. DEFINIÇÃO DOS LOTES E ITENS

Manifestação: 3. Equipamento Tipo 3, 4 e 5 (Lotes 3,4 e 5 – Item 1):

1. Desnecessária a exigência de discos SSD para equipamentos que não possuem características de alta performance de armazenamento. Lembrando que armazenamento de Logs interno não são recomendados para soluções de segurança. O ideal é indicar armazenamento externo. Diversos fabricantes utilizam memória flash interna, somente para armazenamento de sistema operacional, configuração, assinaturas e logs temporários, em caso de falta de conexão com a gerência.

Portanto, frisamos que, para o armazenamento de logs, entendemos que não há necessidade de um disco rígido SSD. Podemos usar outros tipos de memórias para o sistema operacional, processamento e funções que necessitam de alta performance, mas para armazenamento de logs, realizamos com discos SAS (com maior capacidade e suporte a RAID).

Pedimos a alteração dos itens acima para que seja dada a oportunidade de entrega equipamentos que utilizem outras tecnologias de armazenamento e, eventualmente, de discos rígidos no formado SAS.

Resposta: Sugestão parcialmente acatada

124. Item 3.1 LOTE 1 - item 1: Firewall Multifuncional Tipo 1

Manifestação: Consideramos que logs são informações vitais para o monitoramento do appliance e das condições de segurança da rede por eles protegidas, e que por esta razão estes logs não podem estar sujeitos às falhas do próprio appliance, ou seja, não pode residir no próprio appliance."Ainda, a empresa oferece tecnologia patenteada que possibilita a inspeção de tráfego sem a necessidade de cache local, o que garante appliances muito mais eficientes e sem nenhum armazenamento local. Esta é uma característica única dos nossos appliances de Segurança e a necessidade de armazenamento local como detalhado neste item impossibilita a nossa participação no certame, uma vez que penaliza a #### por possuir tecnologia superior que não faz uso de armazenamento local (cache) para realizar sua inspeção de tráfego.

Solicitamos a remoção deste item da especificação, pois entendemos que a inexistência deste não impede nem favorece a participação de nenhum dos principais fornecedores de tecnologia do mercado, e possibilita a participação da #### com sua tecnologia única e de altíssima eficiência.

Como alternativa, sugerimos manter o requerimento, mas com a inclusão de uma ressalva que obrigue apenas àqueles fabricantes que precisam de armazenamento local para execução de suas funções e inspeção de manterem esse recurso via SSD.

Ademais desta explanação, todos os registros de logs dos appliances #### são feitos em nossa plataforma externa que faz parte da solução de gerenciamento centralizado, de forma que não há nenhum prejuízo aos órgãos quando ao quesito de logs e registros de relatórios do sistema. Pelo contrário, fazendo de forma externa é mais segura do que localmente."

Resposta: Sugestão parcialmente acatada

125. Item 3.1 LOTE 1 – item 1: Firewall multifuncional Tipo 1 3.1.1.4 3.8 LOTE 2 – item 1: Firewall multifuncional Tipo2 3.8.1.4 3.15 LOTE 3 – item 1: Firewall multifuncional Tipo3 3.15.1.5 3.22 LOTE 4 – item 1: Firewall multifuncional Tipo4 3.22.1.5 3.29 LOTE 5 – item 1: Firewall multifuncional Tipo 5 3.29.1.5

Manifestação: Para o armazenamento de logs, entendemos que não há necessidade de um disco rígido SSD. Usamos outros tipos de memórias para o sistema operacional, processamento e funções que necessitam de alta performance, mas para armazenamento de logs, realizamos com discos SAS (com capacidade nos modelos maiores de RAID).

Pediremos a alteração dos itens acima para que seja dada a oportunidade de entrega de discos rígidos no formado SAS.

Resposta: Sugestão parcialmente acatada. Item reformulado.

126. Item 3.1.1.4 Possuir disco rígido com capacidade mínima de 16 GB SSD para armazenamento de logs.

Manifestação: "A arquitetura dos Firewalls da #### foi desenvolvida primando pelo não esgotamento lógico e físico dos recursos do Firewall destinados ao armazenamento dos logs gerados pelo dispositivo. A solução foi desenvolvida nos pilares de um servidor, externo ao firewall, responsável pelo gerenciamento, correlacionamento e armazenamento; e tecnologia capaz de encaminhar os logs dos eventos gerados. A vantagem apontada pelo fabricante encontra-se no aumento sistêmico da capacidade de retenção, garantindo assim, uma forma mais econômica e viável para estocar essas informações, garantindo a conformidade com as leis vigentes no país (Ex. Marco Civil da Internet) e princípio da economia em frente aos cofres públicos – ou seja, utilização de recurso computacional já adquirido pelo Órgão.
A solicitação de que o disco do Firewall seja SSD (Solid-State Drive), exclui a nossa participação, uma vez que a arquitetura da solução, trabalha com um ambiente próprio para armazenamento dos logs, que inclusive é capaz de armazenar muito mais que 16Gb, atendendo as leis vigentes no País, já citadas acima, sem nenhuma perda de performance em relação a um disco de SSD interno."
Possuir disco rígido com capacidade mínima de 16 GB de capacidade para armazenamento de logs ou solução similar, sem que haja perda de logs.

Resposta: O item será excluído do termo de referência.

127. Item 3.1.1.4, 3.8.1.4, 3.15.1.5, 3.22.1.5 e 3.29.1.5.

Manifestação: Entendemos que por se tratar de um Firewall multifuncional onde a maior necessidade de desempenho está relacionada a CPU e memória, não se faz necessária a tecnologia SSD, desde que a capacidade de armazenamento seja atendida. Para que possamos participar do certame, sugerimos a seguinte redação para estes itens: "3.1.1.4, 3.8.1.4, 3.15.1.5, 3.22.1.5 e 3.29.1.5. Possuir disco rígido com capacidade mínima de 16, 64, 120, 120 e 240, respectivamente, GB para armazenamento de logs."

Resposta: Sugestão parcialmente acatada

128. Item 3.1.1.4 Possuir disco rígido com capacidade mínima de 16 GB SSD para armazenamento de logs.

Manifestação: Solicitamos que esta exigência seja apenas para os fabricantes que de fato necessitem de tal dispositivo para armazenamento de log, pois possuímos tecnologia patenteada de inspeção de trafego sem a necessidade de SSD.

Resposta: O item será excluído do termo de referência.

129. Item 3.1.1.7 Quantidade de sessões simultâneas 64.000.

Manifestação: Para permitir a nossa participação para este item, solicitamos que a quantidade de sessões simultâneas seja reduzida para 50.000.

Resposta: Sugestão parcialmente acatada. Item reformulado.

130. Item 3.1.1.7 Quantidade de sessões simultâneas 64.000.

Manifestação: "Consideramos a quantidade indicada como desnecessária para o porte do appliance, bem como para o universo de usuários que ele se propõe a atender.

Para a nossa participação competitiva neste certame, solicitamos reduzir para 50.000 esta quantidade, e explicitar capacidade mínima de quando operando em modo DPI para 50.000 conexões, pois é sabido que as capacidades de conexões SPI e DPI mudam drasticamente em diversos fornecedores de soluções de segurança que seguramente participarão do certame."

Resposta: Sugestão parcialmente acatada. Item reformulado.

131. Item 3.1.1.8 Quantidade de novas sessões por segundo 7.500.

Manifestação: A fim de permitir o fornecimento de nossos equipamentos, solicitamos que este item seja alterado para 5.000 sessões.

Resposta: Sugestão parcialmente acatada. Item reformulado.

132. Item 3.1.1.8 Quantidade de novas sessões por segundo 7.500.

Manifestação: entendemos que o volume de 7.500 novas sessões por segundo é proporcional, por exemplo, as maiores universidades federias do país ou empresas de processamento de dados de governos estaduais. Para o lote um sugerimos que este número seja reduzido sem prejuízo para 1000

Resposta: Sugestão parcialmente acatada. Item reformulado.

133. Item 3.1.1.8 Quantidade de novas sessões por segundo 7.500.

Manifestação: Solicitamos reduzir para 5.000 para permitir a nossa participação neste item, e também para adequar este quesito à quantidade máxima de conexões estipuladas para este modelo.

Resposta: Sugestão parcialmente acatada. Item reformulado.

134. Item 3.1.1.8 Quantidade de novas sessões por segundo 7.500

Manifestação: A fim de permitir a nossa participação neste item e também para adequar este quesito à quantidade máxima de conexões estipuladas para este modelo solicitamos reduzir para 5.000.

Resposta: Sugestão parcialmente acatada. Item reformulado.

135. Item 3.14.1.2 Possui capacidade mínima para armazenamento de logs de 500 MB.

Manifestação: "Para o item 3.14.1.2, pedimos a verificação da capacidade de armazenamento. É solicitado 64GB para o NGFW, mas somente 0.5GB para o gerenciamento, sendo que o gerenciamento centralizado deveria ter capacidade maior do que o dispositivo local, principalmente pensando em retenção a longo prazo e geração de relatórios;"

Resposta: Sugestão acatada.

136. Item 3.15 LOTE 3 - item 1: Firewall Multifuncional Tipo 3

Manifestação: "Esta especificação submete a demanda a equipamentos de categoria muito superior àquela demandada pela capacidade estipulada. Sugerimos remover este requisito para adequá-lo à real capacidade dos appliances a serem ofertados pelos diversos fabricantes.

Caso mantido este item, solicitamos alterar a redação de modo a indicar que devem ser fornecidos os módulos SFP somente para as quantidades mínimas indicadas, além de se mencionar também o tipo destes, para que o fornecimento atenda à real demanda e não encareça e penalize os fornecedores que por ventura disponibilizem produtos com maior capacidade de interfaces do que aquela demandada."

Resposta: Sugestão parcialmente acatada.

137. Item 3.15.1.4 Possuir no mínimo 4 (quatro) portas SPF e 6 (seis) portas 10/100/100 BASE T, sendo 01 (uma) utilizada para gerência

Manifestação: Para o item 3.15.1.4, solicitamos a modificação de SPF para SFP e também a indicação se os mesmos devem ser do tipo SR ou LR;

Resposta: Sugestão acatada

138. Item 3.15.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.
Manifestação: "Consideramos que logs são informações vitais para o monitoramento do appliance e das condições de segurança da rede por eles protegidas, e que por esta razão estes logs não podem estar sujeitos às falhas do próprio appliance, ou seja, não podem residir no próprio appliance.
Ainda, a #### oferece tecnologia patenteada que possibilita a inspeção de tráfego sem a necessidade de cache local, o que garante appliances muito mais eficientes e sem nenhum armazenamento local. Esta é uma característica única dos appliances de Segurança #### e a necessidade de armazenamento local como detalhado neste item impossibilita a nossa participação no certame, uma vez que penaliza a #### por possuir tecnologia superior que não faz uso de armazenamento local (cache) para realizar sua inspeção de tráfego.
Solicitamos a remoção deste item da especificação, pois entendemos que a inexistência deste não impede nem favorece a participação de nenhum dos principais fornecedores de tecnologia do mercado, e possibilita a participação da #### com sua tecnologia única e de altíssima eficiência.
Como alternativa, sugerimos manter o requerimento mas com a inclusão de uma ressalva que obrigue apenas àqueles fabricantes que precisam de armazenamento local para execução de suas funções e inspeção de manterem esse recurso via SSD.
Ademais desta explanação, todos os registros de logs dos appliances #### são feitos em nossa plataforma externa que faz parte da solução de gerenciamento centralizado, de forma que não há nenhum prejuízo aos órgãos quando ao quesito de logs e registros de relatórios do sistema."

Resposta: Sugestão não acatada, improcedente com a demanda técnica.

139. Item 3.15.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

Manifestação: A solicitação de que o disco do Firewall seja SSD (Solid-State Drive), exclui a nossa participação, uma vez que a arquitetura da solução, trabalha com um ambiente próprio para armazenamento dos logs, que inclusive é capaz de armazenar mais que 120Gb, atendendo as leis vigentes no País, já citadas acima, sem nenhuma perda de performance em relação a um disco de SSD interno.
Possuir capacidade mínima de 120 GB para armazenamento de logs ou solução similar, sem que haja perda de logs.

Resposta: Sugestão parcialmente acatada

140. Item 3.15.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

Manifestação: Solicitamos que esta exigência seja apenas para os fabricantes que de fato necessitem de tal dispositivo para armazenamento de log, pois a #### possui tecnologia patenteada de inspeção de trafego sem a necessidade de SSD.

Resposta: Sugestão não acatada, improcedente com a demanda técnica.

141. Item 3.15.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

Manifestação: "Consideramos que logs são informações vitais para o monitoramento do appliance e das condições de segurança da rede por eles protegidas, e que por esta razão estes logs não podem estar sujeitos às falhas do próprio appliance, ou seja, não podem residir no próprio appliance.

Ainda, a #### oferece tecnologia patenteada que possibilita a inspeção de tráfego sem a necessidade de cache local, o que garante appliances muito mais eficientes e sem nenhum armazenamento local. Esta é uma característica única dos appliances de Segurança #### e a necessidade de armazenamento local como detalhado neste item impossibilita a nossa participação no certame, uma vez que penaliza a #### por possuir tecnologia superior que não faz uso de armazenamento local (cache) para realizar sua inspeção de tráfego.
Solicitamos a remoção deste item da especificação, pois entendemos que a inexistência deste não impede nem favorece a participação de nenhum dos principais fornecedores de tecnologia do mercado, e possibilita a participação da #### com sua tecnologia única e de altíssima eficiência.
Como alternativa, sugerimos manter o requerimento mas com a inclusão de uma ressalva que obrigue apenas àqueles fabricantes que precisam de armazenamento local para execução de suas funções e inspeção de manterem esse recurso via SSD.
Ademais desta explanação, todos os registros de logs dos appliances #### são feitos em nossa plataforma externa que faz parte da solução de gerenciamento centralizado, de forma que não há nenhum prejuízo aos órgãos quando ao quesito de logs e registros de relatórios do sistema."

Resposta: Sugestão não acatada, improcedente com a demanda técnica.

142. Item 3.15.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

Manifestação: Nosso gerenciamento é feito por interface gráfica centralizada, os equipamentos funcionam como engines que são configurados via plataforma de gerencia remota. Todas os logs e registros são enviados para a gerência e podem ser obtidos via interface gráfica centralizada. No caso da perca da comunicação os discos são utilizados para armazenar os logs e assim que reestabelecido a comunicação esses logs são enviados para a gerencia centralizada. Não é necessário um grande espaço para logs no equipamento local, quando esses logs são visualizados na interface de gerenciamento centralizada.
Possuir disco rígido com capacidade mínima de 16 GB SSD para armazenamento de logs.

Resposta: Sugestão parcialmente acatada.

143. Item 3.15.1.6 Virtualização mínima de 150 VDOMs.

Manifestação: "Sugerimos a reescrita para: 3.15.1.6 Virtualização mínima de 25 VDOMs."

Resposta: Sugestão parcialmente acatada. Item reformulado.

144. Item 3.15.1.6 Virtualização mínima de 150 VDOMs.

Manifestação: Entendemos que esse número de 150 VDOMs não é condizente com a capacidade do equipamento requisitado e que a capacidade de virtualização de 2 VDOMs seria mais adequado e atende ao item. Para garantir maior competitividade entre os concorrentes, sugerimos a seguinte redação para este item: "3.15.1.6. Virtualização mínima de 2 VDOMs."

Resposta: Sugestão parcialmente acatada. Item reformulado.

145. Item 3.15.1.6 Virtualização mínima de 150 VDOMs.

Manifestação: "Primando pela ampla concorrência e capacidade competitiva no processo de aquisição de firewall pelo Ministério do Planejamento, sugerimos a extinção da expressão "VDOM" adotada no Termo de Referência.
Em uma pesquisa pelo buscador do Google pela expressão acima mencionada (VDOM), os cinco primeiros resultados fazem referência direta ao site do fabricante #### fabricante concorrente às soluções por nós ofertadas, demonstrando um possível direcionamento dos itens deste Edital a fim de beneficiar diretamente um dos participantes do processo licitatório; trazendo, assim, desvantagem ao interesse público divergindo-se de um dos princípios iniciais do tal projeto – ampla concorrência e alinhado ao interesse do Estado." Possibilitar virtualização de até 5 firewalls.

Resposta: Sugestão parcialmente acatada. Item reformulado.

146. Item 3.15.1.6 Virtualização mínima de 150 VDOMs.

Manifestação: "Conforme discutidos entre todos os participantes na consulta pública realizada no dia 21/06/2016, chegou à conclusão que o número de 150 VDOMs seria inviável pelo porte do equipamento tendo em vista que os equipamentos não suportam na prática a implementação desta quantidade, pois a mesma diminuiria a performance do equipamento ou até mesmo impossibilitaria o uso do mesmo. Também foi informado que o Órgão teve dificuldade em encontrar esses números na documentação dos fabricantes, e foi solicitado que cada fabricante enviasse sugestões para este item.
Atendendo a solicitação do órgão em enviar a quantidade necessária que caberia no equipamento deste porte e a fim de permitir a participação da #### para este item, solicitamos que seja exigidas 5 instâncias virtuais já licenciadas."

Resposta: Sugestão parcialmente acatada. Item reformulado.

147. Item 3.15.1.6 Virtualização mínima de 150 VDOMs.

Manifestação: "Para o item 3.15.1.6, sugerimos a diminuição do número de VDOMs. Solicitamos a redução para pelo menos 10 instâncias virtuais;"

Resposta: Sugestão parcialmente acatada. Item reformulado.

148. Item 3.15.1.6 Virtualização mínima de 150 VDOMs.

Manifestação: "A quantidade de instâncias virtuais demandada para este porte de equipamento é incompatível com a realidade de uso deste, pois caberia considerar que teríamos a capacidade nominal do equipamento dividida entre 150 redes distintas, ou seja, a capacidade de cada uma das instâncias seria tão pequena que se tornaria inutilizável em ambiente real.
Vale ressaltar que o equipamento deste porte nem suportaria esta quantidade de VDOMs, pois esta quantidade resultaria em uma performance deficiente.
Recomendamos que esta demanda seja readequada à capacidade do modelo de appliance a ser ofertado. "
"1- Mínimo de 5 instâncias virtuais já licenciadas e disponíveis para uso no appliance

2- Passível de expansão via licenciamento adicional, com capacidade compatível com o modelo ofertado pelo fabricante."

Resposta: Sugestão parcialmente acatada. Item reformulado.

149. Item 3.15.1.6 Virtualização mínima de 150 VDOMs. Item: 3.29.1.7 Virtualização mínima de 150 VDOMs.

Manifestação: conforme apontado na consulta publica, este volume de VDOMs é adequado para operadoras com o tráfego de vários clientes passando pela mesma caixa. Entendemos que para órgão do executivo a quantidade de até 6 VDOMs é suficiente. Desta forma, o cliente poderia ter VDOMs para: perímetro, rede interna, wifi visitante, wifi corporativa e datacenter. Um volume acima de 6 VDOMs obriga que seja ofertado caixa de custo e performance muito superior pedido no lote 3

Resposta: Sugestão parcialmente acatada. Item reformulado.

150. Item 3.15.1.6;3.22.1.7; 3.29.1.7

Manifestação: "Todos os itens utilizam a nomenclatura padrão de um dado fabricante. Solicitamos que seja alterada para suporte a virtualização de Firewall, pois assim não restringe a ampla participação de diversos fabricantes que atuam no mercado.
Gostaríamos que destacar em relação a quantidade de Firewall virtuais solicitados para os lotes 3 e 5. O valor de 150 por equipamento é extremamente alto e não representa a real necessidade de qualquer órgão. Um número mais próximo da realidade é a quantidade de 5 Firewall´s virtuais por equipamento físico."

Resposta: Sugestão parcialmente acatada. Item reformulado.

151. Item 3.15.1.7 Quantidade de sessões simultâneas 500.000.

Manifestação: "Consideramos a quantidade indicada como desnecessária para o porte do appliance, bem como para o universo de usuários que ele se propõe a atender.

Para a participação competitiva da nossa empresa neste certame, solicitamos reduzir para 325.000 esta quantidade, e explicitar capacidade mínima de quando operando em modo DPI para 175.000 conexões, pois é sabido que as capacidades de conexões SPI e DPI mudam drasticamente em diversos fornecedores de soluções de segurança que seguramente participarão do certame."

Resposta: sugestão parcialmente acatada. Item reformulado.

152. Item 3.15.1.8 Quantidade de novas sessões por segundo 50.000.

Manifestação: A fim de permitir o fornecimento de equipamentos da nossa marca para este certame, solicitamos a alteração deste item para 20.000 sessões por segundo.

Resposta: sugestão parcialmente acatada. Item reformulado.

153. Item 3.15.1.8 Quantidade de novas sessões por segundo 50.000.

Manifestação: Solicitamos reduzir para 20.000 para permitir a participação da neste item, e também para adequar este quesito à quantidade máxima de conexões estipuladas para este modelo.

Resposta: sugestão parcialmente acatada. Item reformulado.

154. Item 3.22 LOTE 4- item 1: Firewall Multifuncional Tipo 4.

Manifestação: Consideramos que logs são informações vitais para o monitoramento do appliance e das condições de segurança da rede por eles protegidas, e que por esta razão estes logs não podem estar sujeitos às falhas do próprio appliance, ou seja, não podem residir no próprio appliance.
Ainda, a #### oferece tecnologia patenteada que possibilita a inspeção de tráfego sem a necessidade de cache local, o que garante appliances muito mais eficientes e sem nenhum armazenamento local. Esta é uma característica única dos appliances de Segurança #### e a necessidade de armazenamento local como detalhado neste item impossibilita a nossa participação no certame, uma vez que penaliza a #### por possuir tecnologia superior que não faz uso de armazenamento local (cache) para realizar sua inspeção de tráfego.
Solicitamos a remoção deste item da especificação, pois entendemos que a inexistência deste não impede nem favorece a participação de nenhum dos principais fornecedores de tecnologia do mercado, e possibilita a participação da #### com sua tecnologia única e de altíssima eficiência.
Como alternativa, sugerimos manter o requerimento mas com a inclusão de uma ressalva que obrigue apenas àqueles fabricantes que precisam de armazenamento local para execução de suas funções e inspeção de manterem esse recurso via SSD.
Ademais desta explanação, todos os registros de logs dos appliances #### são feitos em nossa plataforma externa que faz parte da solução de gerenciamento centralizado, de forma que não há nenhum prejuízo aos órgãos quando ao quesito de logs e registros de relatórios do sistema.

Resposta: sugestão não acatada, improcedente com a demanda técnica.

155. Item 3.15.1.8 Quantidade de novas sessões por segundo 50.000.

Manifestação: Solicitamos reduzir para 20.000 para permitir a participação da #### neste item, e também para adequar este quesito à quantidade máxima de conexões estipuladas para este modelo.

Resposta: sugestão parcialmente acatada, tem reformulado.

156. Item 3.22.1.4 Possuir no mínimo 6 (seis) portas 10/100/1000, sendo 01 (uma) utilizada para gerência, 6 (seis) portas GbE SFP e 2 (duas) portas 10 SFP+.

Manifestação: A quantidade de 6 (seis) portas GbE SFP não se faz necessária devido à baixa utilização por parte das redes desse tipo de porta, onde a tendência atual é a utilização de portas 10 Gbps SFP+. Entendemos que, no máximo, 4 (quatro) portas GbE SFP é suficiente para atender às necessidades dos clientes. Para que possamos participar do certame, sugerimos a seguinte redação para este item: "3.22.1.4. Possuir no mínimo 6 (seis) portas 10/100/1000, sendo 01 (uma) utilizada para gerência, 4 (quatro) portas GbE SFP e 2 (duas) portas 10 SFP+"

Resposta: sugestão parcialmente acatada. Item reformulado.

157. Item 3.22.1.4 Possuir no mínimo 6 (seis) portas 10/100/1000, sendo 01 (uma) utilizada para gerência, 6 (seis) portas GbE SFP e 2 (duas) portas 10 SFP+.
Manifestação: Para o item 3.22.1.4, solicitamos que seja retirado o requerimento de interfaces 10/100/1000, uma vez que equipamentos desse porte podem não suportar estas velocidades de portas solicitadas. Sugerimos interfaces do tipo 1GB Base-T ou SFP;

Resposta: sugestão parcialmente acatada. Item reformulado.

158. Item 3.22.1.4 Possuir no mínimo 6 (seis) portas 10/100/1000, sendo 01 (uma) utilizada para gerência, 6 (seis) portas GbE SFP e 2 (duas) portas 10 SFP+.

Manifestação: Quanto à quantidade de interfaces, se existe a possibilidade de porta 10GB SFP+, uma interface já supriria todo o throughput de inspeção exigida. Uma agregação com 6 portas 1GB supriria a necessidade de inspeção exigida, sugerimos a reescrita do item para possuir no mínimo 4 (quatro) portas 10/100/1000, sendo 01 (uma) utilizada para gerência, 4 (quatro) portas GbE SFP e 2 (duas) portas 10 SFP+.

Resposta: sugestão parcialmente acatada. Item reformulado.

159. Item 3.22.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

Manifestação: Nosso gerenciamento é feito por interface gráfica centralizada, os equipamentos funcionam como engines que são configurados via plataforma de gerencia remota. Todos os logs e registros são enviados para a gerência e podem ser obtidos via interface gráfica centralizada. No caso da perca da comunicação os discos são utilizados para armazenar os logs e assim que reestabelecido a comunicação esses logs são enviados para a gerência centralizada. Não é necessário um grande espaço para logs no equipamento local, quando esses logs são visualizados na interface de gerenciamento centralizada. Sugerimos possuir disco rígido com capacidade mínima de 32 GB SSD para armazenamento de logs.

Resposta: sugestão parcialmente acatada. Item reformulado.

160. Item 3.22.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

Manifestação: A solicitação de que o disco do Firewall seja SSD (Solid-State Drive), exclui a nossa participação, uma vez que a arquitetura da solução, trabalha com um ambiente próprio para armazenamento dos logs, que inclusive é capaz de armazenar mais que 120Gb, atendendo as leis vigentes no País, já citadas acima, sem nenhuma perda de performance em relação a um disco de SSD interno. Sugerimos possuir capacidade mínima de 120 GB para armazenamento de logs ou solução similar, sem que haja perda de logs.

Resposta: sugestão parcialmente acatada. Item reformulado.

161. Item 3.22.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

Manifestação: Solicitamos que esta exigência seja apenas para os fabricantes que de fato necessitem de tal dispositivo para armazenamento de log, pois possuímos tecnologia patenteada de inspeção de trafego sem a necessidade de SSD.

Resposta: sugestão não acatada.

162. Item 3.22.1.7 Virtualização mínima de 5 VDOMs.
Manifestação: Primando pela ampla concorrência e capacidade competitiva no processo de aquisição de firewall pelo Ministério do Planejamento, sugerimos a extinção da expressão "VDOM" adotada no Termo de Referência.
Em uma pesquisa pelo buscador do Google pela expressão acima mencionada (VDOM), os cinco primeiros resultados fazem referência direta ao site do fabricante #### fabricante concorrente às soluções por nós ofertadas, demonstrando um possível direcionamento dos itens deste Edital a fim de

beneficiar diretamente um dos participantes do processo licitatório; trazendo, assim, desvantagem ao interesse público divergindo-se de um dos princípios iniciais do tal projeto – ampla concorrência e alinhado ao interesse do Estado. Sugerimos possibilitar virtualização de até 2 firewalls.

Resposta: sugestão parcialmente acatada. Item reformulado.

163. Item 3.22.1.7 Virtualização mínima de 5 VDOMs.

Manifestação: Os quantitativos mencionados no item 3.22.1.7 infringe a capacidade competitiva dos participantes uma vez que para atender tal demanda, o valor do projeto deverá, proporcionalmente, aumentar. Vale ater-se ao contexto político/econômico ao qual o Brasil encontra-se fazendo necessária a otimização dos recursos (tecnológicos e financeiros) que o Estado dispõe.
Outro fato a ser considerado é a capacidade de processamento do dispositivo do lote 4, item 1, comparado à demanda de virtualização, é incompatível uma vez que os recursos passam a ser compartilhados entre cada contexto virtual.
Em outras palavras, a necessidade de 'VDOMs' descrita no Termo de Referência poderá ser suprida com firewalls virtuais, bem como, a contextualização de firewalls (utilizando o mesmo recurso físico).

Resposta: Sugestão parcialmente acatada. Item reformulado.

164. Item 3.22.1.7 Virtualização mínima de 5 VDOMs.

Manifestação: Conforme discutidos entre todos os participantes na consulta pública realizada no dia 21/06/2016, chegou à conclusão que o número de 150 VDOMs seria inviável pelo porte do equipamento tendo em vista que os equipamentos não suportam na prática a implementação desta quantidade, pois a mesma diminuiria a performance do equipamento ou até mesmo impossibilitaria o uso do mesmo. Também foi informado que o Órgão teve dificuldade em encontrar esses números na documentação dos fabricantes, e foi solicitado que cada fabricante enviasse sugestões para este item.
Atendendo a solicitação do órgão em enviar a quantidade necessária que caberia no equipamento deste porte e a fim de permitir a nossa participação para este item, solicitamos que sejam exigidas 10 instâncias virtuais já licenciadas.

Resposta: sugestão parcialmente acatada. Item reformulado.

165. Item 3.22.1.7 Virtualização mínima de 5 VDOMs.

Manifestação: Recomendamos que esta demanda seja readequada à capacidade do modelo de appliance a ser ofertado. Recomendação:
1- Mínimo de 10 instâncias virtuais já licenciadas e disponíveis para uso no appliance.
2- Passível de expansão via licenciamento adicional, com capacidade compatível com o modelo ofertado pelo fabricante.
A quantidade de instâncias virtuais demandada para este porte de equipamento é incompatível com a realidade de uso deste, pois caberia considerar que teríamos a capacidade nominal do equipamento dividida entre 150 redes distintas, ou seja, a capacidade de cada uma das instâncias seria tão pequena que se tornaria inutilizável em ambiente real.

Resposta: sugestão parcialmente acatada. Item reformulado.

166. Item 3.22.1.7 Virtualização mínima de 5 VDOMs.

Manifestação: Para o item 3.22.1.7, sugerimos a alteração do número de VDOMs. Solicitamos a mudança para pelo menos 10 instâncias virtuais;

Resposta: sugestão parcialmente acatada. O item foi reformulado.

167. Item 3.22.1.7 Virtualização mínima de 5 VDOMs.

Manifestação: Entendemos que esse número de 5 VDOMs não contempla a necessidade da grande maioria dos ambientes de rede que trabalham com segmentação de redes, onde cada segmento de rede deva possuir um Firewall específico e independente dos demais e que a capacidade de virtualização de, no mínimo, 6 VDOMs seria mais adequado e atende ao item.

Para garantir que as necessidades diversas de segmentação de rede que utilizam equipamento deste porte, sugerimos a seguinte redação para este item: "3.22.1.7. Virtualização mínima de 6 VDOMs."

Resposta: sugestão não acatada

168. Item 3.22.1.8 Quantidade de sessões simultâneas 2.000.000.

Manifestação: Consideramos a quantidade indicada como desnecessária para o porte do appliance, bem como para o universo de usuários que ele se propõe a atender.

Para a participação competitiva da nossa empresa neste certame, solicitamos reduzir para 1.250.000 esta quantidade, e explicitar capacidade mínima de quando operando em modo DPI para 1.000.000 conexões, pois é sabido que as capacidades de conexões SPI e DPI mudam drasticamente em diversos fornecedores de soluções de segurança que seguramente participarão do certame.

Resposta: sugestão parcialmente acatada. Item reformulado.

169. Item 3.22.1.9 Quantidade de novas sessões por segundo 120.000.

Manifestação: A fim de permitir a participação desta empresa com equipamentos da nossa solicitamos que este item seja alterado para 100.000 sessões por segundos.

Resposta: sugestão parcialmente acatada. Item reformulado.

170. Item 3.22.1.9 Quantidade de novas sessões por segundo 120.000.

Manifestação: Solicitamos reduzir para 100.000 para que possamos participar de maneira competitiva neste item, e também para adequar este quesito à quantidade máxima de conexões estipuladas para este modelo.

Resposta: sugestão parcialmente acatada. Item reformulado.

171. Item 3.29 LOTE 5 - item 1: Firewall Multifuncional Tipo 5

Manifestação: Possuir disco rígido com capacidade mínima de 240 GB SSD para armazenamento de logs.

Consideramos que logs são informações vitais para o monitoramento do appliance e das condições de segurança da rede por eles protegidas, e que por esta razão estes logs não podem estar sujeitos às falhas do próprio appliance, ou seja, não podem residir no próprio appliance

Ainda, a #### oferece tecnologia patenteada que possibilita a inspeção de tráfego sem a necessidade de cache local, o que garante appliances muito mais eficientes e sem nenhum armazenamento local. Esta é uma característica única dos appliances de Segurança #### e a necessidade de armazenamento local como detalhado neste item impossibilita a nossa participação no certame, uma vez que penaliza a #### por possuir tecnologia superior que não faz uso de armazenamento local (cache) para realizar sua inspeção de tráfego.

Solicitamos a remoção deste item da especificação, pois entendemos que a inexistência deste não impede nem favorece a participação de nenhum dos principais fornecedores de tecnologia do mercado, e possibilita a participação da #### com sua tecnologia única e de altíssima eficiência.

Como alternativa, sugerimos manter o requerimento, mas com a inclusão de uma ressalva que obrigue apenas àqueles fabricantes que precisam de armazenamento local para execução de suas funções e inspeção de manterem esse recurso via SSD.
Ademais desta explanação, todos os registros de logs dos appliances #### são feitos em nossa plataforma externa que faz parte da solução de gerenciamento centralizado, de forma que não há nenhum prejuízo aos órgãos quando ao quesito de logs e registros de relatórios do sistema.

Resposta: sugestão não acatada, improcedente com a demanda técnica.

172. Item 3.29.1.2 Possuir no mínimo o throughput de 10 Gps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 e 2.8 ligadas simultaneamente com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo levando-se em consideração o perfil de tráfego descrito no ANEXO E.

Manifestação: Para esta categoria de appliances nos posicionamos com equipamentos multiblade, de altíssima capacidade nominal de processamento de pacotes, entretanto para que seja possível a participação, solicitamos que seja reduzida para 9 Gpbs de throughput.

Resposta: sugestão não acatada, improcedente com a demanda técnica.

173. Item 3.29.1.4 Possuir no mínimo 4 (quatro) portas de 10 Gbps SPF+, 6 (seis) portas SPF e 6 (seis) portas 10/100/1000 Mbps BASE T, sendo 01 (uma) utilizada para gerência.

Manifestação: A quantidade de 6 (seis) portas GbE SFP não se faz necessária devido à baixa utilização por parte das redes desse tipo de porta, onde a tendência atual é a utilização de portas 10 Gbps SFP+ e para equipamentos do porte do solicitado no lote 5, a tendência futura é a utilização de portas 40 Gbps. Entendemos que, no máximo, 4 (quatro) portas GbE SFP é suficiente para atender às necessidades dos clientes, bem como o suporte à portas 40 Gbps.
Para que possamos participar do certame e para garantir suporte futuro para à interfaces 40 Gbps sem a necessidade de troca do equipamento, sugerimos a seguinte redação para este item: "3.29.1.4. Possuir no mínimo 4 (quatro) portas de 10 Gbps SPF+, 4 (quatro) portas SPF, suporte a, no mínimo, 2 (duas) portas 40 GBase-F QSFP e 6 (seis) portas 10/100/1000 Mbps BASE T, sendo 01 (uma) utilizada para gerência."

Resposta: sugestão parcialmente acatada. Item reformulado.

174. Item 3.29.1.5 Possuir disco rígido com capacidade mínima de 240 GB SSD para armazenamento de logs.

Manifestação: A solicitação de que o disco do Firewall seja SSD (Solid-State Drive), exclui a nossa participação, uma vez que a arquitetura da solução, trabalha com um ambiente próprio para armazenamento dos logs, que inclusive é capaz de armazenar mais que 240 GB, atendendo as leis vigentes no País, já citadas acima, sem nenhuma perda de performance em relação a um disco de SSD interno.
Solicitamos possuir capacidade mínima de 240 GB para armazenamento de logs ou solução similar, sem que haja perda de logs.

Resposta: sugestão parcialmente acatada. Item reformulado.

175. Item 3.29.1.5 Possuir disco rígido com capacidade mínima de 240 GB SSD para armazenamento de logs.

Manifestação: Solicitamos que esta exigência seja apenas para os fabricantes que de fato necessitem de tal dispositivo para armazenamento de log, pois a #### possui tecnologia patenteada de inspeção de trafego sem a necessidade de SSD.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

176. Item 3.29.1.7 Virtualização mínima de 150 VDOMs.

Manifestação: Os quantitativos mencionados no item 3.29.1.7 infringe a capacidade competitiva dos participantes uma vez que para atender tal demanda, o valor do projeto deverá, proporcionalmente, aumentar. Vale ater-se ao contexto político/econômico ao qual o Brasil encontra-se fazendo necessária a otimização dos recursos (tecnológicos e financeiros) que o Estado dispõe.
Outro fato a ser considerado é a capacidade de processamento do dispositivo do lote 3, item 1, comparado à demanda de virtualização, é incompatível uma vez que os recursos passam a ser compartilhados entre cada contexto virtual.
Se um firewall com capacidade de throughput de 1 Gbps, compartilha com 150 contextos virtuais, conforme exige o item 3.15.1.6, tendo cada firewall virtual recursos de processamento similares, há um coeficiente de aproximadamente 70Mbps por contexto virtual.
Ao refazermos os cálculos para 3 contextos virtualizados, é possível observar que a necessidade de virtualização pode ser suprida por meio firewalls virtuais com configurações mínimas para atendimento da finalidade justificada pelo Ministério do Planejamento.
Em outras palavras, a necessidade de 'VDOMs' descrita no Termo de Referência poderá ser suprida com firewalls virtuais, bem como, a contextualização de firewalls (utilizando o mesmo recurso físico).

Resposta: sugestão parcialmente acatada. Item reformulado.

177. Item 3.29.1.7 Virtualização mínima de 150 VDOMs.

Manifestação: Primando pela ampla concorrência e capacidade competitiva no processo de aquisição de firewall pelo Ministério do Planejamento, sugerimos a extinção da expressão "VDOM" adotada no Termo de Referência.
Em uma pesquisa pelo buscador do Google pela expressão acima mencionada (VDOM), os cinco primeiros resultados fazem referência direta ao site do fabricante #### fabricante concorrente às soluções por nós ofertadas, demonstrando um possível direcionamento dos itens deste Edital a fim de beneficiar diretamente um dos participantes do processo licitatório; trazendo, assim, desvantagem ao interesse público divergindo-se de um dos princípios iniciais do tal projeto – ampla concorrência e alinhado ao interesse do Estado. Solicitamos possibilitar virtualização de até 5 firewalls.

Resposta: sugestão parcialmente acatada. Item reformulado.

178. Item 3.29.1.7 Virtualização mínima de 150 VDOMs.

Manifestação: Os quantitativos mencionados no item 3.29.1.7 infringe a capacidade competitiva dos participantes uma vez que para atender tal demanda, o valor do projeto deverá, proporcionalmente, aumentar. Vale ater-se ao contexto político/econômico ao qual o Brasil encontra-se fazendo necessária a otimização dos recursos (tecnológicos e financeiros) que o Estado dispõe.
Outro fato a ser considerado é a capacidade de processamento do dispositivo do lote 5, item 1, comparado à demanda de virtualização, é incompatível uma vez que os recursos passam a ser compartilhados entre cada contexto virtual.
Se um firewall com capacidade de throughput de 1Gbps, compartilha com 150 contextos virtuais, conforme exige o item 3.15.1.6, tendo cada firewall virtual recursos de processamento similares, há um coeficiente de aproximadamente 70Mbps por contexto virtual.
Ao refazermos os cálculos para 3 contextos virtualizados, é possível observar que a necessidade de virtualização pode ser suprida por meio firewalls virtuais com configurações mínimas para atendimento da finalidade justificada pelo Ministério do Planejamento.

Em outras palavras, a necessidade de 'VDOMs' descrita no Termo de Referência poderá ser suprida com firewalls virtuais, bem como, a contextualização de firewalls (utilizando o mesmo recurso físico).

Resposta: sugestão parcialmente acatada. Item reformulado.

179. Item 3.29.1.7 Virtualização mínima de 150 VDOMs.

Manifestação: Conforme discutidos entre todos os participantes na consulta pública realizada no dia 21/06/2016, chegou à conclusão que o número de 150 VDOMs seria inviável pelo porte do equipamento tendo em vista que os equipamentos não suportam na prática a implementação desta quantidade, pois a mesma diminuiria a performance do equipamento ou até mesmo impossibilitaria o uso do mesmo. Também foi informado que o Órgão teve dificuldade em encontrar esses números na documentação dos fabricantes, e foi solicitado que cada fabricante enviasse sugestões para este item.
Atendendo a solicitação do órgão em enviar a quantidade necessária que caberia no equipamento deste porte e a fim de permitir a nossa participação para este item, solicitamos que sejam exigidas 10 instâncias virtuais já licenciadas.

Resposta: sugestão parcialmente acatada. Item reformulado.

180. Item 3.29.1.7 Virtualização mínima de 150 VDOMs.

Manifestação: A quantidade de instâncias virtuais demandada para este porte de equipamento é incompatível com a realidade de uso deste, pois caberia considerar que teríamos a capacidade nominal do equipamento dividida entre 150 redes distintas, ou seja, a capacidade de cada uma das instâncias seria tão pequena que se tornaria inutilizável em ambiente real.
Recomendamos que esta demanda seja readequada à capacidade do modelo de appliance a ser ofertado.
Recomendação:
1- Mínimo de 10 instâncias virtuais já licenciadas e disponíveis para uso no appliance
2- passível de expansão via licenciamento adicional, com capacidade compatível com o modelo ofertado pelo fabricante.

Resposta: sugestão parcialmente acatada Item reformulado.

181. Item 3.29.1.7 Virtualização mínima de 150 VDOMs.

Manifestação: Para garantir maior competitividade entre os concorrentes, sugerimos a seguinte redação para este item: "3.29.1.7. Virtualização mínima de 6 VDOMs."
Entendemos que esse número de 150 VDOMs não é condizente com a capacidade do equipamento requisitado e que a capacidade de virtualização de, no mínimo, 6 VDOMs seria mais adequado e atende ao item.

Resposta: sugestão parcialmente acatada. Item reformulado.

182. Item 3.29.1.8 Quantidade de sessões simultâneas 4.000.000.

Manifestação: A fim de permitir que esta empresa forneça equipamentos da marca #### solicitamos que este item seja alterado para 3.000.000 de sessões.

Resposta: sugestão parcialmente acatada. Item reformulado.

183. Item 3.29.1.8 Quantidade de sessões simultâneas 4.000.000.

Manifestação: Consideramos a quantidade indicada como desnecessária para o porte do appliance, bem como para o universo de usuários que ele se propõe a atender.

Para a participação competitiva da #### neste certame, solicitamos reduzir para 3.000.000 esta quantidade, e explicitar capacidade mínima de quando operando em modo DPI para 2.500.000 conexões, pois é sabido que as capacidades de conexões SPI e DPI mudam drasticamente em diversos fornecedores de soluções de segurança que seguramente participarão do certame.

Resposta: sugestão parcialmente acatada. Item reformulado.

184. Item 3.29.1.9 Quantidade de novas sessões por segundo 120.000.

Manifestação: Recomendamos readequar este requerimento referenciado ao item anterior: 200.000.

Resposta: sugestão parcialmente acatada. Item reformulado.

185. Item 3.29.1.4 Possuir no mínimo 4 (quatro) portas de 10 Gbps SPF+, 6 (seis) portas SPF e 6 (seis) portas 10/100/1000 Mbps BASE T, sendo 01 (uma) utilizada para gerência.

Manifestação: Para o item 3.29.4, solicitamos que seja retirado o requerimento de interfaces 10/100/1000, uma vez que equipamentos desse porte podem não suportar estas velocidades de portas solicitadas. Sugerimos interfaces do tipo 1GB Base-T ou SFP;

Resposta: sugestão parcialmente acatada

186. Item 3.31.1.2 Possuir suporte nativo para a funcionalidade de APT (Advanced Persistent Threat) e Zero Day através de ativação de licenciamento.

Manifestação: Possuímos ferramenta de sandbox, no entanto é um serviço separado para essa determinada função. Uma vez que essa funcionalidade virtualiza sistemas operacionais a quantidade de memória e processamento pode prejudicar o desempenho local do equipamento.
Solicitamos possuir suporte para integração com equipamentos ou serviços com a funcionalidade de APT (Advanced Persistent Threat) e Zero Day.

Resposta: sugestão acatada.

187. Itens 3.31.1.2 Possuir suporte nativo para a funcionalidade de APT (Advanced Persistent Threat) e Zero Day através de ativação de licenciamento.
3.31.1.3 Entende-se por funcionalidade de APT (Advanced Persistent Threat) e Zero Day. Deve possuir capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, tais como: Windows XP e Windows 7 assim como Office 2003, 2010 e 2013. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

Manifestação: APT´s externos ao sistema, não deveria estar junto com o sistema de Firewall. Integração com externo.
Sugerimos que seja aceito declaração informando que a funcionalidade está em RoadMap no fabricante e que se compromete a entregar em até 10 meses.

Resposta: sugestão não acatada. Não será aceito funcionalidades que estejam em RoadMap, pois as funcionalidades indicadas são necessárias na entrega imediata do equipamento.

188. Item 3.31.1.3 Entende-se por funcionalidade de APT (Advanced Persistent Threat) e Zero Day. Deve possuir capacidade de emular (sandbox) ataques em diferetnse sistemas operacionais, tais como: Windows XP e Windows 7 assim como Office 2003, 2010 e 2013. A tecnologia de máquina

virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

Manifestação: (faltou o texto por parte do participante).

Resposta: sugestão incompleta.

189. Item 3.31.1.3 Entende-se por funcionalidade de APT (Advanced Persistent Threat) e Zero Day. Deve possuir capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, tais como: Windows XP e Windows 7 assim como Office 2003, 2010 e 2013. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

Manifestação: para o item 3.31.1.3, solicitamos a modificação de Office 2003, 2010 e 2013, para documentos Windows Office;

Resposta: sugestão acatada.

190. Item 3.7.1.2 Possui capacidade mínima para armazenamento de logs de 200 MB.

Manifestação: Para o item 3.7.1.2, pedimos verificação da capacidade de armazenamento. É solicitado 16GB para o NGFW, mas somente 0.2GB para o gerenciamento, sendo que o gerenciamento centralizado deveria ter capacidade maior do que o dispositivo local, principalmente pensando em retenção a longo prazo e geração de relatórios.

Resposta: sugestão acatada.

191. Item 3.8 LOTE 2 – item 1: Firewall multifuncional Tipo2.
Manifestação: para o item 3.8, faltou indicação da quantidade de interfaces requeridas.

Resposta: sugestão acatada. Item incluído.

192. Item 3.8 LOTE 2 - item 1: Firewall Multifuncional Tipo 2.

Manifestação: Consideramos que logs são informações vitais para o monitoramento do appliance e das condições de segurança da rede por eles protegidas, e que por esta razão estes logs não podem estar sujeitos às falhas do próprio appliance, ou seja, não podem residir no próprio appliance.
Ainda, a #### oferece tecnologia patenteada que possibilita a inspeção de tráfego sem a necessidade de cache local, o que garante appliances muito mais eficientes e sem nenhum armazenamento local. Esta é uma característica única dos appliances de Segurança #### e a necessidade de armazenamento local como detalhado neste item impossibilita a nossa participação no certame, uma vez que penaliza a #### por possuir tecnologia superior que não faz uso de armazenamento local (cache) para realizar sua inspeção de tráfego.
Solicitamos a remoção deste item da especificação, pois entendemos que a inexistência deste não impede nem favorece a participação de nenhum dos principais fornecedores de tecnologia do mercado, e possibilita a participação da #### com sua tecnologia única e de altíssima eficiência.
Como alternativa, sugerimos manter o requerimento, mas com a inclusão de uma ressalva que obrigue apenas àqueles fabricantes que precisam de armazenamento local para execução de suas funções e inspeção de manterem esse recurso via SSD.
Ademais desta explanação, todos os registros de logs dos appliances #### são feitos em nossa plataforma externa que faz parte da solução de gerenciamento centralizado, de forma que não há nenhum prejuízo aos órgãos quando ao quesito de logs e registros de relatórios do sistema.

Resposta: sugestão não acatada, improcedente com a demanda técnica.

193. Item 3.8.1.4 Possuir disco rígido com capacidade mínima de 64 GB SSD para armazenamento de logs.

Manifestação: A solicitação de que o disco do Firewall seja SSD (Solid-State Drive), exclui a nossa participação, uma vez que a arquitetura da solução, trabalha com um ambiente próprio para armazenamento dos logs, que inclusive é capaz de armazenar mais que 64Gb, atendendo as leis vigentes no País, já citadas acima, sem nenhuma perda de performance em relação a um disco de SSD interno.
Solicitamos possuir capacidade mínima de 64 GB para armazenamento de logs ou solução similar, sem que haja perda de logs.

Resposta: Sugestão parcialmente acatada. Item reformulado.

194. Item 3.8.1.4 Possuir disco rígido com capacidade mínima de 64 GB SSD para armazenamento de logs.

Manifestação: solicitamos que esta exigência seja apenas para os fabricantes que de fato necessitem de tal dispositivo para armazenamento de log, pois possuímos tecnologia patenteada de inspeção de trafego sem a necessidade de SSD.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

195. Item 3.8.1.4 Possuir disco rígido com capacidade mínima de 64 GB SSD para armazenamento de logs.

Manifestação: Nosso gerenciamento é feito por interface gráfica centralizada, os equipamentos funcionam como engines que são configurados via plataforma de gerencia remota. Todos os logs e registros são enviados para a gerência e podem ser obtidos via interface gráfica centralizada. No caso da perca da comunicação os discos são utilizados para armazenar os logs e assim que reestabelecido a comunicação esses logs são enviados para a gerência centralizada. Não é necessário um grande espaço para logs no equipamento local, quando esses logs são visualizados na interface de gerenciamento centralizada.
Solicitamos possuir disco rígido com capacidade mínima de 16 GB SSD para armazenamento de logs.

Resposta: sugestão parcialmente acatada

196. Item 3.8.1.5 Quantidade de sessões simultâneas 250.000.

Manifestação: Entendemos que o volume de 250.00 sessões simultâneas é proporcional a empresas de médio porte como o tráfego da sede de ministérios do governo federal . Para o lote 2 sugerimos que este número seja reduzido sem prejuízo para 64.000

Resposta: sugestão parcialmente acatada. Item reformulado.

197. Item 3.8.1.5 Quantidade de sessões simultâneas 250.000.

Manifestação: Consideramos a quantidade indicada como desnecessária para o porte do appliance, bem como para o universo de usuários que ele se propõe a atender.
Para a nossa participação competitiva neste certame, solicitamos reduzir para 100.000 esta quantidade, e explicitar capacidade mínima de quando operando em modo DPI para 90.000 conexões, pois é sabido que as capacidades de conexões SPI e DPI mudam drasticamente em diversos fornecedores de soluções de segurança que seguramente participarão do certame.

Resposta: sugestão parcialmente acatada. Item reformulado.

198. Item 3.8.1.6 Quantidade de novas sessões por segundo 50.000.

Manifestação: A fim de adequar este item ao porte de equipamentos solicitado, solicitamos que seja alterado para 6.000 sessões.

Resposta: sugestão parcialmente acatada. Item reformulado.

199. Item 3.8.1.6 Quantidade de novas sessões por segundo 50.000.

Manifestação: Entendemos que o volume de 50.000 novas sessões por segundo é proporcional, por exemplo, a grandes instituições financeiras e operadoras fora do Brasil e com este volume de tráfego dividido entre várias paredes de firewall. Para o lote dois sugerimos que este número seja reduzido sem prejuízo para 7.500.

Resposta: sugestão parcialmente acatada. Item reformulado.

200. Item 3.8.1.6 Quantidade de novas sessões por segundo 50.000.

Manifestação: 50.000 sessões por segundo é um número incompatível pelo tipo e configurações do firewall, solicitamos reduzir para 6.000 para que possamos participar de maneira competitiva neste item, e também para adequar este quesito à quantidade máxima de conexões estipuladas para este modelo.

Resposta: O item foi reformulado.

201. Item 3.8.1.7 Vazão de 50 Mbps para IPSec VPN throughput.

Manifestação: Para o item 3.8.1.7, o throughput requerido é do mesmo valor que o requerido para os equipamentos do LOTE1.
Sugerimos o aumento deste valor de throughput por se tratar de equipamento de maior capacidade;

Resposta: sugestão não acatada, incompatível com a demanda técnica.

202. Item 1.1.7.(ANEXO E) No caso de dispensa da avaliação de amostra, a equipe técnica apresentará a motivação para referida dispensa.

Manifestação: Para Isonomia:
1. Sugerimos a remoção do subitem 1.1.7, onde deve ser vedado a dispensa da avaliação da amostra, ou se for o caso sugerimos a seguinte alternativa:
1.1 Em caso do equipamento ofertado ter sido testado pelo NSS LABS e recebido o SELO DE APROVAÇÃO, o mesmo poderá ser dispensado dos testes caso tenha atingido a performance suficiente para atender ao exigido no respectivo item ao qual esteja sendo ofertado.

Resposta: O item foi reformulado.

203. Item 1.1.3.(ANEXO E) Os testes serão feitos com base no Caderno de Testes aprovado pelo grupo técnico de apoio ao DESIN/STI. Nesse caderno deverão ser incluídos, minimamente os testes descritos no item 1.1.11 deste anexo.

Manifestação: Sobre caderno de teste (1.1.3), entendemos que deveria ser especificado antes do processo competitivo, deixando todos os fabricantes no mesmo nível de conhecimento e assegurando o menor risco de "inconformidades".
1. Sabemos que não haverá capacidade técnica e/ou tempo hábil para se auditar o ambiente em caso de dúvidas sobre alguma funcionalidade / configuração / customizações indevidas;
2. Acredito que se o ambiente disponibilizado para testes for do próprio MPOG ou até mesmo da UNB, seria mais transparente e isonômico.

<u>Resposta</u>: sugestão não acatada, improcedente com a demanda técnica.

204. Item 1.1.2. (ANEXO E) Após aceite da documentação comprobatória, a licitante deverá disponibilizar para realização dos testes de homologação, no prazo de 15 (quinze) dias corridos, contados a partir da solicitação do pregoeiro, uma amostra dos itens escolhidos do lote da mesma marca e modelo ofertado na proposta, a fim de apurar o atendimento da especificação técnica. Destacando-se que a referida solicitação do pregoeiro para a licitante só poderá ocorrer após validação dos Cadernos de Testes.

<u>Manifestação:</u> Do prazo (item 1.1.2) 15 dias corridos é muito pouco tempo para se disponibilizar equipamento. Sei que o equipamento escolhido para o item 5 tem um porte enterprise, podendo ser um Chassi.
1. O tempo e o custo para se importar um equipamento do porte esperado para este subitem é de até 45 dias corridos.
2. É quase impossível um licitante possuir equipamento deste porte no país para fazer PoC.
3. Gostaria, também, de sugerir que, em caso de aprovação da amostra, em se constatando se tratar de equipamento novo, de primeiro uso, a mesma possa ser usada na entrega definitiva.

<u>Resposta</u>: sugestão parcialmente acatada. Item reformulado.

205. Item 1.1.14.(ANEXO E) A STI, em situações excepcionais e de interesse da Administração Pública, reserva o direito de suspender temporariamente a execução do Teste de Conformidade, com a respectiva suspensão dos seus prazos de completa execução.

<u>Manifestação:</u> O Subitem 1.1.14 é uma prerrogativa que pode dar margem a "dúvidas" sobre a imparcialidade deste MPOG, uma vez que a dilatação do prazo irá certamente, favorecer ao licitante que estaria sendo testado.

<u>Resposta</u>: sugestão não acatada. Serão obedecidos os princípios da Administração Pública, dentre eles, impessoalidade, moralidade, legalidade, objetividade e vinculação ao instrumento convocatório.

206. Item 1.1.16. (ANEXO E) A Licitante Convocada deverá prover, integralmente às suas custas, toda a infraestrutura necessária (equipamentos e cabos de conectividade de rede, equipamentos de geração de tráfego e ameaças, appliances, servidores de virtualização, desktops, todos os softwares e licenças de utilização, etc.) para a completa instalação e execução do Teste de Conformidade.
<u>Manifestação:</u> O Subitem 1.1.16 que exige que o fornecedor contrate o executor do teste dá margem para manipulações de configurações o que poderá acarretar a aquisição (aprovação) de equipamentos de baixa qualidade / performance / confiabilidade.
1. Sugerimos a contratação por parte do ministério do equipamento ou de um laboratório para execução de testes de performance durante um período. Uma vez que, se o escopo de contratação for por testes, poderá haver interesse em desclassificar o máximo de empresas.

<u>Resposta</u>: sugestão não acatada. Serão obedecidos os princípios da Administração Pública, dentre eles, impessoalidade, moralidade, legalidade, eficiência, objetividade e vinculação ao instrumento convocatório.

207. Item (não se aplica).

<u>Manifestação:</u> Sugeriria a vocês incluir um tipo de equipamento entre a terceira e a quarta faixa, visto que eles têm como número mínimo de sessões, respectivamente, 500 mil e 2 milhões. Pensamos que esse intervalo está muito alto, causando maior preocupação se a marca do equipamento vencedor tiver grande variação de preço (provocando salto de categoria de equipamento, por exemplo).

Resposta: Sugestão não acatada, incompatível com a demanda técnica.

208. Item 3.8.1 Firewall multifuncional Tipo2

Manifestação: Falta de especificação do tipo/quantitativo de portas no item 3.8.1 do Lote 2.

Resposta: sugestão acatada.

209. Item 2.1.12 Deve possuir fonte(s) de energia atendendo aos itens 3.1.1.3, 3.8.1.3, 3.15.1.3, 3.22.1.3 e 3.29.1.3.

Manifestação: O subitem 2.1.12 do item 2.1 (Requisitos Gerais) consta que o firewall deve possuir fonte de energia no próprio equipamento, no entanto os subitens 3.1.1.3, 3.8.1.3 (Requisitos Específicos) permitem o fornecimento de fonte interna ou externa.

Resposta: sugestão acatada.

210. Itens 3.15.1.6, 3.22.1.7 e 3.29.1.7

Manifestação: divergência na quantidade mínima de virtualização (”VDOMs”) exigidas nos lotes 03, 04 e 05, respectivamente nos subitens 3.15.1.6, 3.22.1.7 e 3.29.1.7;

Resposta: sugestão acatada

211. Item (não se aplica).

Manifestação: A exigência da tecnologia SSD para os discos de armazenamento de logs pode restringir número de participantes no certame.

Resposta: sugestão acatada.

212. Itens 3.31.1.1 Possuir todas as funcionalidades descritas no item 2.4; e 3.31.1.2 Possuir suporte nativo para a funcionalidade de APT (Advanced Persistent Threat) e Zero Day através de ativação de licenciamento.

Manifestação: Desde que não prejudique a competitividade entre os participantes da licitação, não seria viável exigir a funcionalidade APT e Zero Day (sandbox), prevista nos subitens 3.31.1.2 e 3.31.1.3 do Lote 5, no item 3 do Lote 4?

Resposta: sugestão parcialmente acatada, para o suporte ao APT.

213. Item (não se aplica).

Manifestação: O VDOM é um termo proprietário ou já é aceito/utilizado por todos fabricantes de firewall?

Resposta: sugestão acatada, termo substituído.

214. Item (não se aplica).

Manifestação: devido ao atual cenário econômico e as últimas recomendações publicadas pelo Ministério do Planejamento no que tange aos serviços de hospedagem em nuvem, gostaríamos de sugerir que ao invés do Governo comprar os equipamentos de segurança que o mesmo o faça por meio de prestação de serviços pelos motivos abaixo, não se limitando a estes:

1º) o modelo de aquisição (CAPEX) onera mais o orçamento público, gera a dependência nos equipamentos pelo seu período de depreciação, bem como um custo de suporte e manutenção extra. Como prestação de serviços todos os custos estão incluídos o que no final acaba sendo menor que o de uma aquisição e todos os insumos que compõe.
2º) como prestação de serviço (OPEX) se consegue maior flexibilidade na contratação e a mesma possibilidade de configuração e ainda a atualização de hardware e software durante a execução contratual.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

215. Item (não se aplica).

Manifestação: Sugerimos alteração no termo de referencia, prevendo o suporte de equipe de gerenciamento da solução de segurança (SOC), essa serviço trará inúmeros benefícios à administração.
Essa equipe tem alta expertise no gerenciamento de Segurança, proporcionando com maior controle de ativos e informações sensíveis, com um serviço de proteção contínua, com gerenciamento e monitoração 24 x 7 X 365;
É possível disponibilizar de relatórios mensais enviados pelo próprio SOC, além do mais, esses especialistas tem sólidos conhecimentos em diferentes tecnologias, e com isso aumenta produtividade interna, com possibilidade da administração de alocação de recursos em outros segmentos;
A administração permanecerá como o responsável por Indicadores e Políticas de Segurança, atendendo às exigências regulatórias de governança, SOX, entre outros;
Essa equipe promove redução de custos com prevenção de incidentes de segurança (atualizações e correções necessárias aos equipamentos), protegendo os dados do cliente e a integridade da marca segura.
Por todos os motivos expostos, solicitamos que seja requerido o gerenciamento dos dispositivos por uma equipe proativa SOC (Centro de gerenciamento de solução de segurança).

Resposta: sugestão não acatada, incompatível com a demanda técnica.

216. Subitem 1.1.16, 1.4.1... 1.4.4 (ANEXO E).
Manifestação: Subitem 1.1.16, 1.4.1... 1.4.4 (arquitetura do teste) Sobre o Teste de Capacidade:
1. Não vi nenhum equipamento ou solução que permita a auditoria da geração de tráfego e a garantia da sua aplicação real.
1. Em um teste efetivo, para ter certeza do funcionamento do gerador de tráfego e da sua passagem no ambiente, foi utilizado SWITCH gerenciável, que enviava dados de rede para gerência central, que reportava qual o tráfego estava passando pelo SWITCH.
2. Outro ponto é exigir que a gerência do firewall seja acionada durante o teste e que a evidência do tráfego seja mostrada em gráficos/dashboard ou similar, que mostre tudo em tempo real.

Resposta: sugestão não acatada.

217. Item 1.4.2. O conjunto de equipamentos especializados de geração de tráfego e ameaças deverá ser capaz de gerar pelo menos 5.000 (cinco mil) ameaças ou ataques de tipos variados, stateful e stateless, encapsuladas nos protocolos diversos, incluindo, HTTP, HTTPS, protocolos de e-mail, vídeo conferência, VoIP, FTP e VPN e métodos de ofuscação.
1.4.17. Será considerado prejuízo na performance do equipamento a ocorrência de quaisquer dos eventos a seguir:
1.4.17.1. Perda de pacotes superior a 3%.
1.4.17.2. Erros irrecuperáveis de transações TCP/layer-7.
1.4.17.3. Obter taxa de detecção de ameaças ou ataques menor que 80%.
1.4.17.4. Valores de latência ou de variação de latência (jitter) acima de 5x (cinco vezes) dos valores coletados no item 1.4.16 deste anexo.
1.4.17.5. Os valores de latência poderão ser comparados com os descritos nos datasheets dos equipamentos testados pelo grupo técnico de apoio ao DESIN/STI para avaliação de desempenho.

Manifestação: Da quantidade de ameaças a serem testadas (5000) e da eficiência aferida.
1. O NSSLABS, principal laboratório que analisa performance e eficiência das soluções de firewall, usa uma base com 2000 assinaturas de ataques e aprova os que têm um índice de, pelo menos 98% de assertividade.
2. Sugiro que a quantidade de ameaças a serem testadas seja diminuída para 2000 ameaças e que o índice de detecção seja de, pelo menos, 97%.
3. Da mesma forma, entendemos que um firewall não pode ter nenhuma perda de pacote durante a execução dos testes (1.4.17.1). Sugerimos remover este item ou diminuir para 1%.

Resposta: sugestão parcialmente acatada.

218. Item 1.4.12. (ANEXO E) A amostra terá o tamanho dos frames variados a ser definido na ocasião dos testes.

Manifestação: sugiro que todas as definições de testes sejam definidas antes da publicação do edital para que minimizem dúvidas e riscos.

Resposta: sugestão não acatada, essas definições constarão do caderno de testes.

219. Item 1.4.17.4. Valores de latência ou de variação de latência (jitter) acima de 5x (cinco vezes) dos valores coletados no item 1.4.16 deste anexo.

Manifestação: Valores de latência ou de variação de latência (jitter) acima de 5x (cinco vezes) dos valores coletados no item 1.4.16 deste anexo.
1. Note que não há indicação de valores mínimos de jitter. Portanto, se eu tenho um equipamento que tenha um Jitter significável e ele varie para 5x, mesmo assim ele poderá ter um número máximo menor que um equipamento que tenha um Jitter Alto. Exemplo... Se tenho um equipamento com Jitter abaixo de 1 milissegundo e variar até 5 milissegundos, será muito mais baixo que um equipamento que fique sempre em 9 milissegundos. Esse número só é publicado por fabricantes de firewall que derivam de switches. Não sendo comuns em soluções de segurança que evoluíram de Software.

Resposta: sugestão não acatada.

220. Item 1.4.20. A licitante deve disponibilizar em até 5 (cinco) dias úteis contados da data da finalização dos testes, o relatório com todas as informações e resultados apurados durante os testes.

Manifestação: entendemos que deveria ser de total responsabilidade do MPOG. Que deveria tirar fotos e, eventualmente, coletar impressões e relatórios em tempo de execução do teste para gerar o relatório final, e não deixar a cargo da empresa que está sendo testada.

Resposta: Sugestão não acatada.

221. Item (não se aplica).

Manifestação: Abaixo fazemos as seguintes sugestões com o objetivo de aprimorar as funcionalidades da solução adquiridas e ampliar a participação de empresas 100% Nacionais.
• Possuir perfis de acesso hierárquicos;
• Possibilitar alterar a ordem de herança de "Pai para Filho" e de "Filho para Pai" das configurações do Perfil Hierárquico;
• O Brasil ainda produz mais matéria prima e menos produto de valor agregado, principalmente os de tecnologia. O Governo com o objetivo de incentivar a produção nacional editou o DECRETO Nº 8.186, DE 17 DE JANEIRO DE 2014 no qual é aplicado uma margem de preferência normal e adicional para aquisição de licenciamento de uso de programas de computador e serviços correlatos.

• É de se espantar que um Registro de Preço do Ministério do Planejamento não siga uma orientação do próprio Governo Federal. A CERTICS foi criada para comprovar se um software é resultado de desenvolvimento e inovação tecnológica no País. Sugerimos que o Decreto nª 8.186, de 17 de janeiro de 2014 esteja presente nesse registro de preço.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

222. Item 13 DAS SANÇÕES ADMINISTRATIVAS

Manifestação: onde são tratadas as sanções administrativas, estão sendo previstas apenas situações no momento da assinatura (recusa de assinatura, falta de documentos, etc.) do contrato e durante a sua execução (inexecução parcial, total, etc.), sendo que é importante identificarmos também os riscos em outros momentos cruciais para o bom andamento do processo em questão: a etapa de lances e a habilitação técnica por meio do Teste de Conformidade.
É muito comum enfrentarmos situações onde empresas aventureiras e imprudentes, certas da impunidade de seus atos, participam de Pregões Eletrônicos sem compromisso com o processo e acabam atrapalhando-o, seja através de lances que se mostrarão inexequíveis ou até mesmo participando sem sequer atender a especificação técnica. Visando diminuir estas práticas, alguns processos já utilizam mecanismos que fazem com que as empresas sejam responsáveis por seus atos e que, em caso de desvios, sejam penalizados administrativamente e também financeiramente. Para que isto seja possível, sugerimos a inclusão de alguns textos semelhantes aos propostos abaixo:
• Sugestão: "A participação neste Pregão implica a aceitação, plena e irrevogável, das normas constantes do presente Edital e dos seus Anexos."
• Sugestão: "A participação e o encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. A PROPONENTE declarará no sistema, antes de registrar sua proposta, que cumpre plenamente os requisitos de habilitação exigidos neste Edital, sujeitando-se às sanções legais na hipótese de declaração falsa. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará a PROPONENTE às sanções previstas neste Edital."

o Justificativa: Reforçar que qualquer empresa ao participar do certame estará se submetendo às regras estabelecidas na Lei e também no Edital;
• Sugestão: "A licitante que for desclassificada no Teste de Conformidade será multada em 0,5% (cinco décimos) por cento sobre o valor estimado da contratação do lote em questão."
o Justificativa: Garantir que empresas não irão participar do certame sem a certeza de que atendem ao especificado no Termo de Referência;
• Sugestão: "A multa deverá ser recolhida no prazo de 05 (cinco) dias úteis a contar da intimação, sob pena de cobrança judicial."
• Sugestão: "As penalidades serão registradas no SICAF."
• Sugestão: "Não serão aplicadas penalidades na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados."
• Sugestão: "As penalidades serão aplicadas com observância aos princípios da ampla defesa e do contraditório."
Justificativa: Demonstrar a severidade e seriedade com que estes aspectos serão tratados;

Resposta: sugestão parcialmente acatada.

223. Item 1.4.3. (ANEXO E) O conjunto de equipamentos especializados de geração de tráfego e ameaças deverá ser capaz de simular pelo menos 1.000 aplicações

Manifestação: Os equipamentos disponíveis no mercado possuem a capacidade de simular milhares de aplicações mediante a captura e playback, mas este procedimento requer encontrar amostras de captura e inserção das amostras no gerador, esta operação requer um tempo que torna o teste inexequível para 1000 aplicações. Por este motivo solicitamos alterar o item para: "O conjunto de

equipamentos especializados de geração de tráfego e ameaças deverá ser capaz de simular pelo menos 100 (cem) Aplicações"

Resposta: O item foi reformulado.

224. Item 1.4.13. (ANEXO E) O padrão de tráfego definido no item 1.4.10 deve ser distribuído entre todos os clientes e servidores utilizados nos testes.

Manifestação: A fim de permitir a latência média no período do teste, é importante indicar que todos os clientes e servidores emulados devem gerar tráfego, sendo que a quantidade/tipo de tráfego poderá ser diferente entre os clientes e servidores, por exemplo: os clientes e servidores que irão emular HTTP, não irão emular UDP/RTP e o volume de tráfego será diferente entre eles. Por este motivo, solicitamos alterar o item para: "O padrão de tráfego definido no item 1.4.11 deve ser distribuído entre todos os clientes e servidores utilizados nos testes, podendo o tráfego ser diferente entre os clientes e servidores."

Resposta: sugestão parcialmente acatada.

225. Item 1.4.18. (ANEXO E) A amostra deverá comprovar os itens de conexões simultâneas e novas conexões por segundo das especificações técnicas presentes no Anexo B deste termo por, pelo menos, 5 (cinco) minutos.

Manifestação: Não está claro se "Conexões Simultâneas" e "Novas Conexões" deverão ser medidos simultaneamente e com tráfego "blend", pois caso sejam simultâneos e "blended", torna-se quase impossível realizar os testes. Por este motivo, solicitamos que o texto seja modificado para: "1.4.18. A amostra deverá comprovar os itens de conexões simultâneas das especificações técnicas presentes no Anexo B deste termo por, pelo menos, 5 (cinco) minutos, com tráfego HTTP puro e objeto de 64bytes". e "1.4.18.1. A amostra deverá comprovar os itens de novas conexões por segundo das especificações técnicas presentes no Anexo B deste termo por, pelo menos, 5 (cinco) minutos, com tráfego HTTP puro e objeto de 64bytes."

Resposta: O item foi reformulado.

226. Item (ANEXO E)

Manifestação: entendemos que o teste abaixo é rigoroso e capaz de ser executado pela tecnologia disponível no Brasil (####) com apenas uma caixa.

- Deverá apresentar amostra dos seguintes requisitos mínimos:
- O appliance deverá suportar um throughput mínimo exigido em cada lote durante todo o período de teste, quando as funcionalidades de firewall de aplicação, IPS, antivírus e anti-spyware estiverem habilitadas simultaneamente. Para aferir esta performance, todas as assinaturas que o fabricante possuir para cada um destes recursos precisam estar atuantes, e a base de assinaturas atualizada na data do teste;
- Será avaliado a console de gerência no firewall, que deve continuar acessível durante os testes, sendo possível visualizar, modificar e aplicar as alterações das regras de acesso, bem como a visualização das informações constantes.
- Durante o teste de throughput deverá ser exibido os logs dos ataques e aplicações identificadas pela solução correspondente ao tráfego gerado.
- No ambiente de teste deverá ser realizado com os seguintes critérios:
- Deverá ser em modo camada 3 (L3) em todas as interfaces utilizadas nos testes;
- O Firewall sob teste deverá estar com, no mínimo, 300 regras de aplicações aplicadas e atuantes, isto é, o tráfego gerado deverá ser distribuído e ajustado de forma a passar por todas as regras e "bater" apenas na última;
- cada sentido, com pacotes do tipo TCP válido, com a seguinte proporção:

· 60% HTTP, conteúdo variável com imagens, textos, tipo e tamanho de 64 Kbytes a 128 Kbytes;
· 20% HTTPS, conteúdo variável com imagens, textos, tipo e tamanho de 64 Kbytes a 128 Kbytes;
· 10% SMTPS, com conteúdo variável, incluindo arquivos anexos, de tamanho 64 Kbytes a 128 Kbytes;
· 10% Ataques (Ataques stateful/stateless, variados, no mínimo 100 ataques diferentes, relativos aos protocolos/serviços: http, https, smtps e outros a escolher;
· Para os protocolos criptografados (HTTPS e SMTPS), a solução deve identificar, de-criptografar e inspecionar o tráfego proveniente, tanto em conexões de saída (outbound) quanto de entrada (inbound);
· Deve estar configurado o MTU (Maximum Transmission Unit) da rede do teste com tamanho entre 40 e 1500 Bytes;
· Como forma de comprovar a capacidade e visibilidade fornecida pelo Firewall sob teste, os valores deverão ser exibidos pela interface de gerência no Firewall, indicando os protocolos detectados, distribuição de tráfego por protocolo e/ou aplicação, conexões por segundo, conexões concorrentes, pacotes por segundo, bits por segundo, ataques detectados, erros, utilização da CPU e memória, estes valores devem estar próximos aos valores gerados pela ferramenta de teste;
· Deverá estar habilitado a checagem bidirecional do trafego;
· A instituição se reserva do direito de poder conferir e desabilitar recursos ou técnicas que infrinjam o edital. A conferência será feita a cada passagem de tráfego;
· Não será aceito o uso de thresholds para desabilitar funcionalidades de controle de aplicação, IPS, antivírus e anti-spyware caso a solução atinja determinado nível de uso de recurso de hardware e software.
· Durante o teste de throughput deverá ser feita a alteração de uma política e a mesma deverá ser aplicada no gateway testado. O throughput não poderá atingir valor inferior ao mínimo exigido no edital durante a aplicação da regra. Não será aceito customização do refresh de tela no gerador de carga para mascarar este resultado. O tempo máximo de refresh de tela deverá ser de até 2 segundos;
· No momento do encerramento do teste, deverá ser entregue à equipe técnica os arquivos de backup das configurações do equipamento, um arquivo com as senhas de acesso ao backup, caso esteja criptografado, além do usuário e senha de acesso a interface, os arquivos de registro de acesso (logs de acesso) e os relatórios de tráfego, em formato PDF.

Resposta: sugestão parcialmente acatada.

227. Item 1.4.11.3.1 VPN (IPSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes).

Manifestação: Para o item 1.4.11.3.1, solicitamos esclarecimento se a VPN IPSec deve ser fechada com o equipamento Device Under Test?

Resposta: Correto. Será fechado com o equipamento Device Under Test.

228. Item 1.4.11.3.4. (ANEXO E) Outros (distribuição de tamanho variável).

Manifestação: Para o item 1.4.11.3.4, solicitamos uma definição para a distribuição de "Outros".

Resposta: sugestão não acatada, essas definições constarão do caderno de testes.

229. Item 1.4.17.5 (ANEXO E) Os valores de latência poderão ser comparados com os descritos nos datasheets dos equipamentos testados pelo grupo técnico de apoio ao DESIN/STI para avaliação de desempenho.

Manifestação: Para o item 1.4.17.5, solicitamos a retirada do item uma vez que, nem todos os fabricantes divulgam informações de latência em seus datasheets e também pelo fato de as condições de testes realizados pelos fabricantes para obtenção dos valores dos datasheets são diferentes dos testes realizados pelo requerido neste termo de referência.

Resposta: sugestão acatada.

230. Item 1.4.18 A amostra deverá comprovar os itens de conexões simultâneas e novas conexões por segundo das especificações técnicas presentes no Anexo B deste termo por, pelo menos, 5 (cinco) minutos.

Manifestação: Para o item 1.4.18, solicitamos esclarecimento se os testes de conexões simultâneas e novas conexões por segundo serão realizados com somente a funcionalidade de FW ativada, ou se também serão realizados sobre as mesmas condições de funcionalidades ativas como no teste de throughput. Também gostaríamos de questionar qual a condição do teste de novas conexões por segundo, se será através de somente a quantidade de recebimentos de pacotes SYN por segundo, ou se somente com a necessidade do estabelecimento da conexão, ou se de modo que, uma vez estabelecida a conexão, deve haver passagem de tráfego pela conexão estabelecida junto com o encerramento da conexão através de envio de pacotes FYN. Caso o método a ser utilizado seja o que é necessário a passagem de tráfego pela conexão e depois o seu encerramento, favor especificar o tamanho do pacote de tráfego a ser transmitido, por exemplo, http com 1 byte;

Resposta: O item foi reformulado.

231. Item 1.4.5 (ANEXO E) A amostra deve ser configurada com as funcionalidades de firewall, tal como previstas na especificação técnica Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URL's), sistema de prevenção a intrusão (IPS, Antivírus e Anti- Malware), administração de largura de banda de serviço (QoS), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL habilitadas simultaneamente.

Manifestação: Para o item 1.4.5, solicitamos esclarecimento sobre como será feita a identificação de usuários.

Resposta: a identificação de usuários será realizada através de protocolos de rede que possibilitam autenticação.

232. Item (não se aplica).

Manifestação: Da divisão de Lotes por Sizing do Equipamento
Pontos Positivos:
Deve vencer o equipamento mais barato por categoria de performance. E a empresa que tenha maior abrangência nacional.
Pontos Negativos:
1. Se cada for vencido por fabricante distinto, e um órgão precisar de mais de um tipo de equipamento/dimensionamento, existirão duas tecnologias distintas, que poderão interoperar, mas possuirão comandos e gerências apartadas. Sabendo que a maioria dos Órgãos reclama de pouco pessoal técnico, e da alta complexidade da infraestrutura, teremos isso agravado com duas tecnologias distintas para proteção.
2. Vencerá a empresa que conseguir montar o melhor preço para uma demanda global pensando no atendimento a todas as regiões do País. Isso poderá não ser o melhor preço para atendimento a um local específico, onde poderia ter uma empresa local.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

233. Item (não se aplica).

Manifestação: A divisão de lotes por região do país (Norte, Nordeste, Sul, Sudeste, Centro-Oeste).
1. Com isso conseguiríamos menores custos para empresas localizadas em cada região.

2. Teríamos, portanto, mais lotes, mais participantes e preços mais agressivos. Então seriam 5 x 5 lotes = 25 Lotes.
3. Vantagem: Por ter mais lotes e mais participantes, teríamos mais facilidade para participação de empresas de portes variados.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

234. Item (não se aplica).

Manifestação: Dificuldades para Participação de Diversas Empresas

1. A quantidade de Equipamentos exigidos nos atestados de capacidade técnica dificulta a participação de empresas de diversos portes e especialidades.
Sugestão: Aceitar, que um atestado de firewall seja complementado por qualquer tipo de appliance e/ou equipamento de rede (roteador e/ou switches).

Resposta: sugestão não acatada. É necessidade da demanda técnica que o atestado seja de firewall.

235. Item (não se aplica).

Manifestação: Do prazo de Suporte e Garantia (60 meses)
1. Soluções de Tecnologia da Informação tem um período muito rápido de "depreciação". Acreditamos que 36 ou 48 meses seja o ideal.
2. Mesmo fazendo contrato de 12 ou 24 meses ainda existirá a possibilidade de se estender o contrato até o limite dos 60 meses.
3. Note que esse será o primeiro processo de compra compartilhada para firewall. O Registro de Preço tem duração de 12 meses, caso não seja possível a aquisição por parte de todos os Órgãos, em 12 meses o MPOG terá que desenvolver novo processo.

Contratação de empresa especializada no fornecimento de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede dos órgãos e dos servidores de rede, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, incluídos todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua, suporte técnico e repasse de conhecimento de toda a solução a fim de atender às necessidades dos órgãos contratantes.

Resposta: sugestão não acatada, incompatível com a demanda técnica.

236. Item (não se aplica)

Manifestação: Sobre o SLA e a forma como está "colocada" por Região.
1. Sabemos que a ideia é boa em separar por região, mas há de se entender que equipamentos de menor porte ou em cluster poderiam ser considerados mais "flexíveis". Sugestão do texto seria retirar equipamento e inserir "solução fornecida". Portanto o Emergencial (A) está da seguinte forma:
"São consideradas como "Emergência" todas as falhas cujas consequências tenham impactos negativos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata.
Ex: Situação de indisponibilidade total do equipamento, funcionamento intermitente ou parcial do equipamento, que possa levar à interrupção intermitente, parcial ou total de serviços ou perda de tráfego."

Resposta: sugestão não acatada, incompatível com a demanda técnica.