**Questionamento Prefeitura de Contagem**

**Questionamento 1:**

Conforme mencionado em Audiência Pública, por inúmeros participantes, fica complicado o ganhador do lote 1 ter a responsabilidade por gerenciar e administrar o lote 2, uma vez que são necessárias algumas informações de acesso a rede do concorrente.

A ideia de separar lote 1 e 2, e criar um 3° lote com a solução de SD-WAN + Firewall + Gerenciamento, evitaria esse tipo de conflito, o que tornaria o gerenciamento mais transparente. Ressaltando que o ganhador do lote 1 não pode ganhar o lote 2 ou lote 3 e vice versa.

 **Questionamento 2:**

**ITENS 1, 2, 3, 4, 5 e 6;**

Solicitamos a revisão dos throughputs solicitados na descrição dos appliances, pois os valores apresentados estão em divergência com os links a serem contratados para a utilização, fazendo assim com que o órgão disponibilize recursos financeiros além do necessário para cada localidade.

Além disso “todos” os throughput solicitados estão alinhados com um fabricante de firewall em específico, o que exclui qualquer tipo de competitividade no certame.

Compreendemos que o órgão pretende manter a disputa de valores aberta e com o maior número possível de participantes.

**Questionamento 3:**

**2.6.4. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;**

O fato da não oferta de uma API aberta na solução de Firewall/IPS não limita tecnicamente a qualidade de proteção ou do sistema de gerenciamento do produto.

Outro ponto importante é que o gerenciamento será feito por um “terceiro” no qual esse “terceiro” não necessita de uma API aberta para gerenciar a solução.

Compreendemos que o órgão pretende manter a disputa de valores aberta e com o maior número possível de participantes, por isso, o item de API aberta não será obrigatório.

Sugerimos o seguinte texto: **O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) ou API aberta;**

**Questionamento 4:**

**2.6.13. Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;**

Entendemos que o projeto envolve 1 (um) equipamento por localidade, não fazendo assim a necessidade de tabelas independentes de roteamento. Todas as localidades poderão ser gerenciadas centralmente de um único local, facilitando a gestão do projeto.

Sugerimos a remoção do item

**Questionamento 5:**

**2.6.27. Deve haver suporte ao protocolo ICAP, inclusive de forma segura (SSL);**

Qual a necessidade de uso do protocolo ICAP? Possuem servidores web?

**Questionamento 6:**

**2.6.33. A solução deve suportar integração nativa com Let’s Encrypt, para obtenção de certificados válidos, de forma automática;**

A solução permite a importação de qualquer certificado ou autoridade certificadora válida de modo manual. Garantindo assim um melhor controle dos acessos e segurança das informações com utilização de certificados.

Sugerimos o seguinte texto: **A solução deve suportar integração nativa com Let’s Encrypt, para obtenção de certificados válidos, de forma manual ou automática;**

**Questionamento 7:**

**2.6.36. A solução de firewall deve permitir integração com threat feeds externos.**

A solução que comercializamos, possui um laboratório especializado em vulnerabilidades, threats gerando diariamente novas assinaturas para melhorar a segurança. Também possuímos bases externas internacionais, provendo uma maior varredura no transporte das informações. Essas assinaturas são disponibilizadas atualizações automáticas diariamente.

Entendemos que se a solução possuir uma base de assinaturas internas e externas, sendo atualizadas diariamente o item se dará por atendido.

Está correto nosso entendimento?

**Questionamento 8:**

**2.6.37. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;**

A solução que representamos é focada em segurança, criasse um risco no ambiente de rede, onde um atacante pode se beneficiar deste recurso e iniciar um ataque no NGFW ao executar uma automação desconhecida que pode liberar um tráfego malicioso.

Sugerimos a remoção do item.

**Questionamento 9:**

**2.6.38. Para agilizar a gerência remota do firewall, deve ser possível carregar conteúdo estático dela a partir de objetos em cache em CDNs;**

A solução que representamos, possui armazenamento em cache do tráfego acessado, podendo este ser armazenado em disco, especificando o tamanho do armazenamento do cache.

Gostaríamos de esclarecimentos em relação ao uso de objeto em cache em CDNs.

**Questionamento 10:**

**2.8.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;**

O produto que representamos possui mais de 4.000 assinaturas em sua base de conhecimento e diariamente são disponibilizadas novas aplicações reconhecidas. Já cobrimos praticamente todas as aplicações possíveis que poderiam ser acessadas pelos usuários das empresas.

O nosso processo de customização é executado pelo próprio fabricante. Entendemos que se caso o controle de IPS baseado em assinaturas, suportar a criação de aplicações proprietária, o item se dará por atendido.

**Questionamento 11:**

**2.8.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);**

**2.8.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;**

Entendemos que grupos estáticos de aplicações, mais assinaturas de IPS por risco atende integralmente a necessidade para a efetiva proteção do ambiente. A solicitação de controle de grupos dinâmicos de aplicações baseados em nível de risco e todo o texto referente a este é perfeitamente dispensável. Para o órgão público é importante permitir o máximo possível de participantes com o objetivo de existir uma disputa de preço para maior economia do ente público. Se manter esses itens acima a concorrência ficará bem limitada e por um item dispensável.

Está correto nosso entendimento?

**Questionamento 12:**

**2.8.24. Deve permitir forçar o uso de portas específicas para determinadas aplicações;**

A solução que representamos possui mais de 4.000 assinaturas em sua base de conhecimento e diariamente são disponibilizadas novas aplicações reconhecidas. Já cobrimos praticamente todas as aplicações possíveis que poderiam ser acessadas pelos usuários das empresas. O nosso processo de customização é executado pelo próprio fabricante.

Essa exigência limita o número de interessados em participar do pregão. Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos a remoção do item

**Questionamento 13:**

**2.11.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;**

O item traz a exigência de que a solução deva possuir integração a diversos métodos de autenticação. O produto que representamos permite integração com LDAP, Active Directory, RADIUS, TACACS+ e base local. Entendemos que o E-directory é um produto desenvolvido pela empresa netiq. A utilização é muito restrita e não é encontrado no facilmente sua instalação nos clientes privado e governo.

<https://www.netiq.com/documentation/edirectory-92/>

Sugerimos a remoção do recurso E-directory

**Questionamento 14:**

**2.11.10. Deve suportar SAML como método para autenticação na navegação de Internet e para VPN;**

Possuímos autenticação via servidores remotos tais como AD, LDAP, TACACS + e RADIUS, também baseado em usuários locais. Entendemos que tais recursos suprem a necessidade de uso de SAML.

Essa exigência limita o número de interessados em participar do pregão. Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos a remoção do item

**Questionamento 15:**

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

Em relação ao item acima, a descrição é de uma solução de DLP. Existe no mercado produtos específicos para essa função e que solicitar tal funcionalidade irá apenas exigir do NGFW recursos que podem causar indisponibilidade no ambiente.

Sugerimos a remoção do Item

**Questionamento 16:**

**2.14.6. Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;**

A solução que representamos, possui atribuição de DNS nos clientes de VPN forma de nativa. Faz se necessário o uso de DNS split tunnel?

**Questionamento 17:**

**2.14.12. A VPN SSL deve permitir a customização da tela em sessões RDP;**

Qual a necessidade da customização da tela em sessões RDP, tendo em vista que este tipo de acesso já criptografado, é a exibição de uma sessão em um host ou servidor (Ex: Windows AD), onde o mesmo não pode ser customizado.

Sugerimos a remoção do item.

**Questionamento 18:**

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

O recurso executado para identificar falhas na disponibilidade do link utiliza um alvo de monitoramento e alguma tecnologia de conectividade. Caso a solução não tenha sucesso na resposta, o link é marcado como inativo e o SD-WAN não utiliza esta WAN para escoamento do tráfego. Os tipos de monitoramento que estão presentes em 100% dos produtos de SD-WAN são o ping e TCP-connect.

Incluir muitas opções apenas dificulta a ampla participação de interessados em participar do pregão.

**Questionamento 19:**

**2.15.10. Deve possuir suporte ao MOS (Mean Opinion Score), para calcular a qualidade de chamadas de voz, considerando jitter, perda de pacote e codec utilizado;**

A solução que representamos possui todo o monitoramento de links baseado em sua performance, tais como jitter, latência, perda de pacotes e utilização de banda. Entendemos que se a solução possuir a escolha do melhor link na utilização de aplicações tais como VOIP. O item se dará por atendido.

Sugerimos a remoção do item.

**Questionamento 20:**

**2.15.13. Deve permitir a segmentação de várias VRFs sobre um único túnel SD-WAN;**

Entendemos que o projeto envolve 1 (um) equipamento por localidade, não fazendo assim a necessidade de uso de VRF. Todas as localidades poderão ser gerenciadas centralmente de um único local, facilitando a gestão do projeto.

**Questionamento 21:**

**2.15.55. Deve possuir suporte e estar licenciamento para uso de VRFs, em IPv4 e IPv6;**

Entendemos que o projeto envolve 1 (um) equipamento por localidade, não fazendo assim a necessidade de de uso de VRF. Todas as localidades poderão ser gerenciadas centralmente de um único local, facilitando a gestão do projeto.

**Questionamento 22:**

**3.2.12. O hardware instalado em qualquer localidade deverá suportar a carga de usuários e links, com até 75% dos seus recursos (CPU e memória);**

**3.2.12.1. Caso estes valores estejam entre 75% e 90%, haverá um prazo de 60 (sessenta) dias para atualização/troca, sem ônus para a CONTRATANTE, visando restabelecer o limite de 75%;**

Para um melhor diagnostico durante o uso do equipamento, pois o mesmo poderá atingir um uso de recurso acima de 75% durante um processo de atualização dos hosts da rede (Ex: Windows Update) ou através de um tentativa de ataque ( onde a solução necessitará de recursos para proteger o órgão), faz-se necessário estipular um período de tempo em que os recursos poderão estar acima do limite, sem obrigatoriedade da troca do equipamento. Ex: permanecer com valores acima por um período de 30 minutos.

Sugerimos o seguinte texto:

**Caso estes valores permaneçam entre 75% e 90% dentre um período maior de que 30 minutos, haverá um prazo de 60 (sessenta) dias para atualização/troca, sem ônus para a CONTRATANTE, visando restabelecer o limite de 75%;**

**Questionamento 23:**

**3.6.21. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;**

**3.6.38. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;**

**3.7.13. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha;**

A solução que representamos possui uma interface muito simples e amigável no qual não se faz necessário o uso de wizard ou assistente gráfico e não é necessário inserir endereço IP.

Na solução a adição de dispositivos se dá pelo número de série, tornando mais seguro o vínculo, pois mesmo o IP sendo alterado o dispositivo UTM manterá seu vínculo.

A simplificação do processo de adicionar dispositivos facilita a manutenção da solução.

Sugerimos os seguintes textos:

3.6.21. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP ou número de série, login e senha dos mesmos;

3.6.38. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço utilizando IP ou número de série, usuário e senha;

3.7.13. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP ou número de série, login e senha;

**Questionamento 24:**

**3.6.22. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;**

Este item traz certa ambiguidade de possibilidades, de um lado facilita importar os objetos e políticas, mas do outro lado irá importar objetos não utilizados, deixando a lista de objetos com itens em demasia e poderá importar políticas que não são utilizadas.

Sugerimos a remoção do item

**Questionamento 25:**

**3.6.26. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;**

**3.6.27. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;**

Suportar a execução de scripts, criasse um risco no ambiente de rede. Um atacante pode se beneficiar deste recurso e iniciar um ataque no NGFW ao executar um script que pode liberar um tráfego malicioso.

Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos a remoção dos itens acima citado

**Questionamento 25:**

**3.6.30. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;**

A solução que representamos, tais configurações são feitas diretamente nas soluções de segurança gerenciadas. Entendemos que devido a necessidade específica de cada unidade faz-se necessário a configuração local. Estas unidades de segurança podem ser acessadas diretamente da solução de gerenciamento centralizado.

Sugerimos o seguinte texto:

**Deve permitir criar regras de NAT64 e NAT46 de forma centralizada ou local, desde que as unidades de segurança possam ser acessadas diretamente através da solução de gerenciamento centralizado.**

**Questionamento 26:**

**3.6.34. Deve permitir a correlação de eventos, provendo dashboards diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;**

Compreendemos que se o produto possuir um dashboard fixo que contenha todas as informações essenciais para a coleta e visualização, ou seja, não customizável. Possuímos diversos painéis especializado, por exemplo, um painel para controle WEB outro para IPS e muitos outros baseados na análise do acesso do usuário final.

Essa exigência limita o número de interessados em participar do pregão. Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos a remoção do item

**Questionamento 27:**

**3.6.41. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;**

A solução que representamos possui diversos relatórios em tempo real, que contenham todas as informações essenciais para análise do acesso do usuário final.

Entendemos que, se a solução possuir a capacidade de exportar os logs no formato CSV, no qual, o cliente poderá importar a informação em uma ferramenta que irá permitir que seja gerado diversos gráficos, como por exemplo, barra, linha, tabela, bolha e pizza, o item será considerado como atendido

Essa exigência limita o número de interessados em participar do pregão. Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos o seguinte texto:

**Suporte a geração de relatórios de tráfego em tempo real;**

**Questionamento 28:**

**3.6.46. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;**

**3.7.16. Deve ter a capacidade de criar relatórios no formato PDF e XML;**

A solução que representamos tem a capacidade de criar relatórios no formato HTML, PDF e CSV, através destas opções é possível realizar a análise necessária, entendemos que a exportação no formato XML, não será obrigatória.

Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos os seguintes textos:

 **Deve ter a capacidade de criar relatórios no formato HTML, CSV, PDF ou XML ;**

**Deve ter a capacidade de criar relatórios no formato PDF ou XML;**

**Questionamento 28:**

**3.6.49. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;**

Visando o tamanho do projeto que hoje consta com mais de 300 caixas, observando também a LGPD que visa o armazenamento de logs por um período, faz-se necessário a especificação da quantidade de logs que o servidor de gerenciamento de logs deverá suportar, além da capacidade de armazenamento dia. (Ex: Quantidade de logs a serem armazenados 20tb, 30tb, quantidade de logs suportados por dia, 300Gb, 400GB).

Sugerimos o seguinte texto:

**A contratada deve entregar uma loção de armazenamento de log, seja físico ou virtual, nas dependências do cliente, com capacidade de receber pelo menos 500GB dia de log de todos os ativos, além de ter a capacidade de armazenar no mínimo 50tb de logs, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;**

**Questionamento 29:**

**3.6.55. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;**

Entendemos que, se a solução possuir a capacidade de exportar os logs no formato CSV, no qual, o cliente poderá importar a informação em uma ferramenta que irá permitir que seja gerado diversos gráficos, como por exemplo, barra, linha, tabela e pizza, o item será considerado como atendido.

Para o órgão público é importante permitir o máximo possível de participantes com o objetivo de existir uma disputa de preço para maior economia do ente público. Se manter esse item a concorrência ficará bem limitada e por um item dispensável.

Sugerimos a remoção do item.

**Questionamento 30:**

**3.6.59. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;**

Entendemos que, se a solução possuir a capacidade de exportar os logs no formato CSV, no qual, o cliente poderá importar a informação em uma ferramenta que irá permitir que seja gerado diversos gráficos, como por exemplo, barra, linha, tabela e pizza, o item será considerado como atendido.

Para o órgão público é importante permitir o máximo possível de participantes com o objetivo de existir uma disputa de preço para maior economia do ente público. Se manter esse item a concorrência ficará bem limitada e por um item dispensável.

Sugerimos a remoção do item.

**Questionamento 31:**

**3.6.61. Deve permitir que o relatório seja enviado por email para o destinatário específico;**

A solução possui o envio de relatório ao administrador que gerencia determinados firewalls, fazendo assim um melhor controle na divulgação das informações de segurança da corporação.

Sugerimos o seguinte texto:

**Deve permitir que o relatório seja enviado por email;**

**Questionamento 32:**

**3.6.65. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;**

Entendemos que, se a solução possuir a capacidade de exportar os logs no formato CSV, no qual, o cliente poderá importar a informação em uma ferramenta que irá permitir que seja gerado diversos gráficos, como por exemplo, barra, linha, tabela e pizza, o item será considerado como atendido.

Para o órgão público é importante permitir o máximo possível de participantes com o objetivo de existir uma disputa de preço para maior economia do ente público. Se manter esse item a concorrência ficará bem limitada e por um item dispensável.

Sugerimos a remoção do item.

**Questionamento 33:**

**3.6.70. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;**

Todas as informações solicitadas no item, é possível realizar a coleta através de monitoramento SNMP, exibindo assim de forma regular e atualizada a informação.

Sugerimos o seguinte texto

**Possibilidade de exibir nos relatórios da GUI ou através de traps de SNMP as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;**

**Questionamento 34:**

**3.6.71. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;**

Essa exigência limita o número de interessados em participar do pregão. Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos a remoção do item

**Questionamento 35:**

**3.6.72. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;**

Essa exigência limita o número de interessados em participar do pregão. Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos a remoção do item

**Questionamento 36:**

**3.7.22. Deve permitir a alteração do formato dos relatórios: fontes, cores, imagens, gráficos, tabelas e o idioma;**

Entendemos que, se a solução possuir a capacidade de exportar os logs no formato CSV, no qual, o cliente poderá importar a informação em uma ferramenta que irá permitir que seja gerado diversos gráficos, como por exemplo, barra, linha, tabela e pizza, o item será considerado como atendido.

Essa exigência limita o número de interessados em participar do pregão. Entendemos que o órgão se pauta nos princípios da transparência e economicidade e é interesse a ampla concorrência.

Sugerimos a remoção do item

**Questionamento 37:**

Na tabela que contem a descrição do item, com as quantidades, valores unitários, valores mensais, etc, existe um valor de performance para cada CPE:

“Link de Conectividade Simétrico de 30Mbps com CPE, CPE SDWAN Tipo 1 para locais até 50 usuários, mínimo de 700 Mbps de capacidade de firewall e 400 Mbps de Threat Protections de serviços de segurança e Gerência de Redes”

Ocorre que na descrição do CPE Tipo 1, página 34 do arquivo “Termo de Referência”, os valores estão completamente diferentes.

Qual valor devemos considerar?

Por fim gostaríamos de uma extensão de prazo de mais 5 dias para mitigarmos mais algumas informações a respeito do processo.