PREFEITURA MUNICIPAL DE CONTAGEM - MG
QUESTIONAMENTOS

Razão Social:	**Oi S.A. (em recuperação judicial)**				
CNPJ/MF (MATRIZ):	76.535.764/0001-43				
Endereço:	Rua do Lavradio, nº 71, 2º andar - Centro				
Cidade:	Rio de Janeiro	**UF:**	RJ	**CEP:**	20230-070
CNPJ/MF (MG):	76.535.764/0007-39				
Endereço:	PC MILTON CAMPOS, 16 - ANDAR: 6 PARTE				
Cidade:	Belo Horizonte	**UF:**	MG	**CEP:**	30.130-040

OBJETO:
Registro de Preços, para contratação de empresa especializada na prestação de Serviços de links de Comunicação de Dados Simétricos filtro de conteúdo e funcionalidades SD-WAN, Serviços de Acesso à Internet dedicado com IPs fixos e Banda Larga, objetivando a interligação das redes locais de computadores das unidades da Prefeitura Municipal de Contagem com infraestrutura Datacenter Municipal, contemplando, de forma contínua, suporte à infraestrutura corporativa de comunicação de dados, voz e vídeo, com solução de segurança da informação, incluindo os serviços de operação, gerenciamento, manutenção e suporte técnico, conforme especificações constantes neste Termo de Referência.

Sr Pregoeiro.

Segue abaixo pedido de esclarecimento/sugestões ao referido TR de consulta Pública e seus anexos:

1) ***2.2.4. DA POSSIBILIDADE DE SUBCONTRATAÇÃO***

É vedada a subcontratação total dos Serviços para os lotes I e II.

Para os serviços de Internet (lote II) será permitida a subcontratação com outra operadora de telecomunicações. A subcontratação de terceiros para o para o acesso a última milha fica, desde já, limitada a 30% (trinta por cento) do total de circuitos de Link de Internet Banda Larga, exclusivamente. A subcontratação não eximirá a responsabilidade da CONTRATADA, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados.

Será permitida a subcontratação do link ou da rede de dados (lote I) com outra operadora de telecomunicações, apenas na modalidade satélite, no limite de 5% (cinco por cento) do total de circuitos de dados de toda a rede da CONTRATANTE.

Em ambos os casos, a solicitação de subcontratação deverão ser previamente e expressamente autorizados pela CONTRATANTE. A subcontratação não eximirá a responsabilidade da CONTRATADA, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados

a) Para que tenha concorrência e melhor preço para a Prefeitura de Contagem sugerimos que seja permitida a subcontratação do objeto, porem em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação. Nossa sugestão será aceita?

2) *3.1.22.1. Link Concentrador com capacidade inicial dimensionada no item 3.2;*
3.1.22.2. Equipamento CPE SD-WAN Central, permitindo cluster conforme especificação técnica definida no item xx. Este equipamento receberá os links oriundo do lote I e do lote II.

Os Links Concentradores / Central de Internet (lote I e Lote II) deverão ser instalados nos DATACENTERs da Prefeitura Municipal de Contagem, localizados nas coordenadas: -19.919987 -44.092753 (principal) e -19.919859 – 44.080152 (secundário) (ver o endereço que consta no padrão do Datacenter).

a) Entendo que o equipamento solicitado no item 6 do Encarte I é para atender aos links concentradores do Lote I, correto?
b) Para que a Contratada possa avaliar melhor técnica e financeiramente o projeto, sugerimos que a Contratante informe a velocidade do concentrador, isso será feito no ajuste do TR?
c) Onde deverá ser instado este link de 2Gbps?

3) *3.2.2. Os links simétricos deverão ser instalados nas Unidades e terão velocidades distintas de acordo com a demanda da CONTRATANTE, os quais deverão ser recepcionados por um Link Concentrador (Central), em modo ativo/standby dimensionados pela CONTRATADA. Para efeito de somatório do Link Concentrador, a largura de banda do Link simétrico, independente da velocidade, será a base para definição do Link Concentrador.*

3.4.5. Deverá ser instalado nos Datacenters da CONTRATANTE pela vencedora do lote I:
2 (dois) links concentradores, sendo um em cada DATACENTER, para o tráfego de dados entre as Unidades listadas no Encarte III e o Datacenter, transportando dados utilizando os acessos pelo Link de conectividade simétrico. A capacidade para este link será definida pela CONTRATANTE. Caso seja entregue em CPE distinto do CPE SD-WAN, este deverá possuir:

a) O Item 3.2.2 informa que a obrigação de dimensionar o link concentrador é da Contratada, mas o item 3.4.5 informa que quem irá definir a capacidade do link concentrador é a Contratante. Sugerimos que tal responsabilidade de definir a capacidade do link seja da Contratante e que tal capacidade seja informada no TR, uma vez que a Contratada terá que saber se haverá necessidade de ampliação de estação que atende o site. Nossa sugestão será aceita?

4) *3.4.10.2. Disponibilidade:*
• A "Disponibilidade dos Serviços", é o tempo em que os Acessos mantidos pela CONTRATADA estão aptos a serem utilizados pelas Unidades da CONTRATANTE ou no DATACENTER municipal. A disponibilidade é aferida até a interface LAN do CPE mantido pela CONTRATADA, aferida nos seguintes percentuais dispostos na tabela abaixo::

UNIDADE	DISPONIBILIDADE MÍNIMA (% do total de horas mensais)
Links / CPEs Centrais	99,80
Links / CPEs – Conectividade simétrico da Unidades	99,40
CPEs SD-WAN das Unidades	99,40
Link Internet Dedicado e Simétrico	99,80
INTERNET BANDA LARGA	100% da banda contratada

a) Entendemos que a disponibilidade dos "links/ CPEs Centrais" de 99,8% é por serviço e não por link, uma vez que os links concentradores estarão em modo ativo/standby conforme item 3.2.2. Entendimento correto?

5) *3.4.11.4. Tempo máximo total de latência para resposta à internet de 80 milissegundos.:*

a) Entendemos que tal item se refere a contratação do Lote II, correto entendimento?

6) *3.4.12.3. Treinamentos.*
• A CONTRATADA do lote I deverá oferecer treinamento com o conteúdo oficial do fabricante para cada item da solução instalada, por empresa certificada e autorizada pelo fabricante, incluindo todas as facilidades e uso equipamento fornecido, com carga horária estabelecida pelo fabricante (caso a carga horaria do fabricante seja menor, fica estabelecido o mínimo de 24 horas), contendo informações sobre as configurações dos equipamentos instalados na CONTRATANTE e do software de gerenciamento, material didático impresso ou em formato digital para todos os participantes, em português do Brasil ou em Inglês

a) Entendemos deste item que o conteúdo deverá ser oficial, mas o treinamento não, isto é, a Contratada poderia ter um parceiro para dar o treinamento com o conteúdo oficial sem ser uma certificação oficial, entendimento correto?

7) *4.1.8. Após a entrega dos links previstos no Encarte III e constante na Ordem de Serviços – Encarte IX, o prazo para instalação de novos links será de 15 (quinze) dias.*

a) Sugerimos um prazo de ativação de no mínimo 60 dias, uma vez que terá que ser feito toda infraestrutura pra ativar o link, bem como a compra de equipamentos SDWAN/Roteador, nosso prazo será aceito?

8) *4.1.12. O prazo de instalação, configuração e ativação dos links constante na Ordem de Serviço emitido pela CONTRATANTE será de, no máximo, 60 (sessenta) dias.*
4.2.9. A ativação dos Link Central, Links de conectividade simétricos, Link dedicado simétrico, Links de Internet Banda Larga, CPEs-Centrais e CPEs das Unidades deverão ser finalizadas em até 60 (sessenta) dias corridos após a assinatura do Contrato.

a) Sugerimos um prazo de ativação de no mínimo 150 dias, uma vez que terá que ser feito toda infraestrutura para ativar o link, bem como a compra de equipamentos SDWAN/Roteador, sem falar no grande quantitativo de links e concentrador que terá que ser ativado, outro ponto é em relação a equipamentos de SDWAN que são importados e não chegarão a tempo para ativação do link no prazo exigido neste item, nosso prazo será aceito?

9) *4.2.6. A CONTRATADA do Lote 1 acumulará as funções de NOC/SOC e Ativação de serviços, sendo a responsável pela articulação destas atividades, guarda das configurações e designações dos links entregues por ela e pelos links da CONTRATADA do lote 2;.*

a) Entendemos que a ativação de serviços do Lote 2 será de responsabilidade da vencedora do Lote 2 e não da vencedora do Lote 1, correto o entendimento?

10) *4.2.15. A mesma ordem de serviço poderá conter solicitações de "N" quantidade de Acessos conforme quadro abaixo:*

TIPO DE SOLICITAÇÃO	PRAZO
Capacidade de Acesso (reconfiguração)	10 dias corridos
Mudança de localização física do CPE dentro de um mesmo endereço	10 dias corridos
Mudança de endereço do Link (instalação no novo endereço com desativação e desinstalação no endereço anterior	15 dias corridos
Configuração simples – sem interrupção de serviços	72 horas corridas
Configuração crítica – disponibilização de serviços	24 horas corridas
Desativação de links com retirada de material	5 dias corridos

.

a) Sugerimos um prazo de ativação de no mínimo 60 dias, uma vez que terá que ser feito toda infraestrutura para ativar o link, nosso prazo será aceito?

11) *6.1.4. A contagem de tempo para a solução dos problemas se iniciará a partir do registro do incidente no sistema de chamados da CONTRATADA, sendo este registro realizado pelo CONTRATANTE ou pela própria empresa contratada. Para efeito do desconto por indisponibilidade serão observados os parâmetros abaixo:*

TIPO DE INDISPONIBILIDADE	CONCEITO	VERIFICAÇÃO DA OCORRENCIA	CATEGORIA	DESCONTO
Indisponibilidade Total	Ocorrência que deixam os serviços totalmente indisponíveis	• Indisponibilidade dos serviços do Link de Conectividade Simétrico; • Indisponibilidade dos serviços do Link de Internet Banda Larga	Emergencial	• 100% do valor do link, calculados sobre o tempo (EXCEDIDO) total de ocorrência (simétrico ou Internet); • 100% do valor dos links, calculados sobre do tempo (EXCEDIDO) total de ocorrência quando da paralização CPE-Central;

a) Sugerimos melhorar a redação deste item, pois estamos entendendo que se o link ficar indisponível, não haverá cobrança do link, mas na consulta pública foi entendido que o desconto de 100% será referente ao tempo que o link ficar indisponível, correto?

12) *6.3. DA GARANTIA CONTRATUAL*
6.3.1. Os licitantes vencedores prestarão garantia de execução do contratual nos moldes do art. 96 da lei nº 14.133/21, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (cinco por cento) do valor total do contrato;.

a) Solicitamos a Prefeitura de Contagem redução do percentual exigido neste item para 1%, uma vez que o percentual de 5% é o teto para contratações de obras, serviços e fornecimentos (Art. 98 da 14.133/21) e a Contratante tem a discricionariedade de solicitar percentual de até 5%, e lembrando que a Contratada já terá muitos custos para implantação do objeto e com mais esse desembolso de 5% do contrato de 36 meses prejudicará em muito a contratada, nossa solicitação de redução do percentual para 1% será aceita?

13) *8.1.1.2. LOTE I*
8.1.1.2.1. Atestado ou declaração de capacidade técnica de pessoa Jurídica Pública ou Privada, devidamente registrado no CREA, em nome da Licitante, que comprove a prestação de serviços de rede Corporativa SD-WAN para cliente abrangendo quantidade de circuitos previstos no Edital, velocidades e tecnologias.
8.1.1.2.2. Atestado(s) ou declaração(ões) de capacidade técnica, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, comprovando fornecimento de serviço de gestão de segurança de solução web application firewall (WAF) ou next generation firewall (NGFW), incluindo: Instalação, Licenciamento, Operação e Configuração.
8.1.1.2.3. Apresentação de profissional certificado em nível profissional em soluções de segurança do fabricante da solução de web application firewall ofertada. • Para fins deste requisito não será admitida a apresentação de certificação de nível associado, comercias, ou participação em treinamento;
8.1.1.2.4. Apresentação de outorga da ANATEL (SCM) para os Serviços de Telecomunicações.
8.1.1.2.5. Comprovar titularidade / licença de uso de software/plataforma com capacidade de orquestrar e automatizar processos de resposta a incidentes com recursos exclusivos de automação, relatórios e privacidade do ambiente;
8.1.1.2.6. APRESENTAÇÃO DATA SHEET DOS CPES VINCULANDO AOS ITENS DA CONTRATAÇÃO.
8.1.1.2.7. Comprovar que o fabricante dos equipamentos fornecidos é ser membro do tsanet (https://tsanet.ORG/MEMBERS) na categoria Basic ou Premium Membership.;.

a) Sugerimos que seja alterado a redação do item 8.1.1.2.1 para "Declaração ou Atestado de Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove que a CONTRATADA prestou ou tem prestado, pelo período mínimo de 12 (doze) meses, o serviço formação de redes Corporativa". Nossa sugestão será atendida?

14) *Item: 3.4.7.2 1 (um) CPE SD-WAN, com as seguintes características:*
• *O CPE deverá ter no mínimo 3 (três) portas de conexão WAN 100M/1G.*

a) Visto que a quantidade de link por CPE SD-WAN é de 2 por site, não faz sentido ser solicitado 3 conexões wan, desta forma sugerimos ao menos 2 interfaces WAN para ficar coerente com a quantidade de links por site, bem como da oportunidade de participação de outros fabricantes, nosso solicitação será aceita?

15) Esta sendo solicitado Equipamento NGFW/SD-Wan levando em conta agrupamento por links de Comunicação de Dados Simétricos, desta forma os equipamentos em diversos sites o equipamento pode ficar subutilizado ou mesmo deixando parte dos links disponíveis subutilizados por não atender todos os requisitos. Também esta sendo solicitado capacidades de firewall não condizentes com o link (Exemplo Tipo I)
Ex.: Site Sandra Rocha, link Dedicado Simétrico de 30Mbps e link Internet de 600 Mbps (Banda Larga), ou seja foi solicitado NGFW tipo I que não ira atender a capacidade total do link em SSL.

Desta forma sugerimos para a solução NGFW/SD-Wan o agrupamento por velocidade de link internet somado ao Dedicado, mudando assim as quantidades e capacidades por tipo de equipamentos, ou seja para unidades com 230 Mbps o equipamento deve suportar a capacidade total do link com um crescimento de 20% com todas as funcionalidades habilitadas simultaneamente sendo assim para o link de 230Mbps o equipamento deverá suportar 276Mbps em todas as funcionalidades simultaneamente.

Esta adequação em todos os itens solicitados trás maior competitividade, otimiza e preserva o investimento feito além de diminuir a quantidade.

Seguem abaixo sugestões de alteração.

Tipo I Links até 300 Mbps. (50 Sites)
1.1.1. Throughput de, no mínimo, 300 Mbps em todas as funcionalidades de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;
1.1.2. Possuir 2 Interfaces Wan (RJ45)
1.1.3. Possuir ao menos 5 interfaces RJ45;
1.1.4. Deve estar homologado na ANATEL até a data da licitação;

Tipo II Links até 700 Mbps. (189 Sites)
1.1.5. Throughput de, no mínimo, 700 Mbps em todas as funcionalidades de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;
1.1.6. Possuir 2 Interfaces Wan (RJ45 ou SFP)
1.1.7. Possuir ao menos 10 interfaces RJ45;
1.1.8. Deve estar homologado na ANATEL até a data da licitação;

Tipo III Links até 1Gbps (85 Sites)
1.1.9. Throughput de, no mínimo, 1000 Mbps em todas as funcionalidades de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;
1.1.10. Possuir 2 Interfaces Wan (+SFP ou Multigigabit em RJ45)
1.1.11. Possuir ao menos 3 interfaces SFP+;
1.1.12. Possuir ao menos 6 interfaces RJ45;
1.1.13. Deve estar homologado na ANATEL até a data da licitação;

Tipo IV Links até 1.6Gbps (2 Sites)
1.1.14. Throughput de, no mínimo, 16000 Mbps em todas as funcionalidades de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;
1.1.15. Possuir 2 Interfaces Wan (+SFP)
1.1.16. Possuir ao menos 4 interfaces SFP+;
1.1.17. Possuir ao menos 6 interfaces RJ45;
1.1.18. Deve estar homologado na ANATEL até a data da licitação;

Tipo V Links até 3Gbps (3 Sites) Datacenters
1.1.19. Throughput de, no mínimo, 3000 Mbps em todas as funcionalidades de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;
1.1.20. Possuir 2 Interfaces Wan (+SFP)
1.1.21. Possuir ao menos 6 interfaces SFP+;
1.1.22. Possuir ao menos 6 interfaces RJ45;
1.1.23. Deve estar homologado na ANATEL até a data da licitação;

Sugerimos também a retirada ou adequação dos itens abaixo, pois de alguma forma favorecem a fabricante especifico o que inviabiliza a livre concorrência e um melhor preço para a Prefeitura de Contagem.

Itens em vermelho solicitamos a retirada do mesmo e itens com marcação em negrito/destaque de amarelo solicitamos adequação do item com a retirado do item em destaque.

- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- Para telnet e ssh, deve haver opção de configurar a interface de origem ao executar o acesso remoto;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM); Não é recomendado o uso de PIM-DM em ambientes SD-Wan)
- Deve suportar BGP, OSPF, **RIP** e roteamento estático; (protocolo antigo)
- Para BGP (IPv4 e IPv6), deve suportar o anúncio apenas quando determinadas condições forem atendidas;
- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;

- Deve suportar NAT dinâmico **(Many-to-Many)**;
- Deve suportar NAT estático (1-to-1);
- Deve suportar NAT estático bidirecional 1-to-1;
- Deve suportar NAT de Origem;
- Deve suportar NAT de Destino;
- Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- Deve suportar NAT64;
- Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- Enviar log para sistemas de monitoração externos;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- Deve haver suporte ao protocolo ICAP, **inclusive de forma segura (SSL);sam**
- Suporte a configuração de alta disponibilidade Ativo/Passivo **e Ativo/Ativo; Não se faz necessário ativo/ ativo na topologia definida**.
- A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;
- Controle, inspeção e decriptografia de SSL para tráfego de Saída (Outbound);
- 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;**
- Para agilizar a gerência remota do firewall, deve ser possível carregar conteúdo estático dela a partir de objetos em cache em CDNs;
- Políticas
- Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
- Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
- Suporte a objetos e regras IPV6;
- Suporte a objetos e regras multicast;
- Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- Controle de Aplicações
- Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

- Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;
- Identificar o uso de táticas evasivas via comunicações criptografadas;
- Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 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 fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 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);
- 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;
- Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- Deve permitir forçar o uso de portas específicas para determinadas aplicações;
- Deve permitir o filtro de vídeos que podem ser visualizados no YouTube;
- Prevenção de ameaças
- Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, **Antivírus e Anti-Spyware ANTIMAwer** integrados no próprio appliance de firewall;
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
- As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- Detectar e bloquear a origem de portscans;

- Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- Possuir assinaturas para bloqueio de ataques de buffer overflow;
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- Deve permitir ao administrador adicionar um tempo mínimo para que assinaturas de IPS sejam ativadas;
- Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Identificar e bloquear comunicação com botnets;
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
- Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;
- A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;
- Filtro de URLs
- Possuir pelo menos 60 categorias de URLs;
- Permitir a customização de página de bloqueio;
- Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- Os requisitos de filtro de URL descritos acima aplicam-se apenas ao firewall das pontas remotas;
- Identificação de usuários
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve suportar o envio e recebimento de credenciais via RADIUS;
- Deve suportar SAML como método para autenticação na navegação de Internet e para VPN;
- Filtro de dados
- Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

- Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 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.
- Geolocalização
- Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

- VPN Client to Site Não é o objetivo do edital
- Suportar IPSec VPN;
- Suportar SSL VPN;
- A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;
- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- Suportar leitura e verificação de CRL (certificate revocation list);
- Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- A VPN SSL deve permitir aos usuários remotos a troca de senha no Active Directory;
- A VPN SSL deve permitir a customização da tela em sessões RDP;
- O firewall deve permitir que seja configurado como cliente VPN SSL, permitindo que tráfego de usuários locais seja tunelado por essa VPN;
- O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.14 e superior);
- Recursos Gerais de SD-WAN
- 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;
- A solução deve permitir a configuração e uso de várias interfaces SD-WAN. Cada uma com seus links;
- Deve possuir suporte ao MOS (Mean Opinion Score), para calcular a qualidade de chamadas de voz, considerando jitter, perda de pacote e codec utilizado;
- Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
- Deve permitir a segmentação de várias VRFs sobre um único túnel SD-WAN;
- Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;
- A solução deve permitir a definição do roteamento para cada aplicação;
- Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;
- Deve possibilitar a definição do link de saída para uma aplicação específica;
- Deve implementar balanceamento de link por hash do IP de origem;

- Deve implementar balanceamento de link por hash do IP de origem e destino;
- Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);
- Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;
- A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
- Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo;
- Deve suportar balanceamento **de tráfego por sessão e pacote**;
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32
- Deve suportar o uso de DDNS, para casos em que uma ou ambas as pontas possuam IPs dinâmicos;
- O recurso de DDNS deve suportar IPv4 e IPv6;
- Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;
- Deve possuir suporte e estar licenciamento para uso de VRFs, em IPv4 e IPv6;
- Gerenciamento Centralizado
- O fornecedor deve considerar recursos de gestão centralizada para as soluções NGFW e SD-WAN;
- Sugerimos a utilização de gerência única para todo ambiente, assim facilitando a administração e solução de problemas. Preferencialmente Cloud para garantir acesso anyware da gerencia
- Deve ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados. É permitida a oferta de duas gerências, para NGFW e SD-WAN, respectivamente;
- Pode ser ofertado em VM, desde que compatível com VMware ESXI 5.5 e acima, Hyper-V 2008 e acima e KVM;
- Pode ser ofertado em hardware, desde que em appliance do próprio fabricante;
- Gerencia Centralizada de NGFW
- A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;
- A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;
- Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
- Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas elas somente sejam aplicadas após aprovação de outro administrador;
- Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;
- Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;
- Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;
- Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;
- Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

- Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;
- Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;
- Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;
- Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;
- Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;
- Permitir criar regras anti DDoS de forma centralizada;
- Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
- Deve oferecer portal personalizado para gerenciamento de dispositivos, políticas e objetos, junto com painéis, relatórios e visualizações personalizadas para atualizações de segurança abrangentes, análises em tempo real e respostas exclusivas às suas necessidades;
- 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;
- O portal deve permitir uma visão geral do tráfego de rede e da postura de segurança, incluindo widgets intuitivos com informações como principais países, principais ameaças, principais origens de tráfego, principais destinos, principais aplicativos e hits de políticas, bem como gráficos para mostrar logins de administrador, eventos do sistema, e uso de recursos;
- O portal deve suportar a sua configuração possibilite seu uso via multi-tenant, ou seja, com a possibilidade de se criarem vários portais de acesso independentes entre si para fins de administração distribuída;
- Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
- Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
- A gerência centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento/VM de gerenciamento centralizado, ou fornecido em equipamento/VM externo do mesmo fabricante;
- Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
- Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
- Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
- Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
- Deve possuir mecanismos de remoção automática para logs antigos;
- Permitir importação e exportação de relatórios
- Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;
- Deve permitir exportar os logs no formato CSV;
- Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- 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;
- A solução deve ter relatórios predefinidos;
- Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
- Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
- Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
- Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

- Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
- Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
- Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
- Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
- Permitir o envio por e-mail relatórios automaticamente;
- Deve permitir que o relatório seja enviado por email para o destinatário específico;
- Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
- Deve permitir o uso de filtros nos relatórios;
- Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- Permitir especificar o idioma dos relatórios criados;
- Gerar alertas automáticos via e-mail, SNMP **OU** Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
- Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
- Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
- Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
- Deve permitir gerar alertas de eventos a partir de logs recebidos;
- Gerência Centralizada de SD-WAN
- A console deverá ser hospedada nas dependências da contratada SD-WAN;
- As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada equipamento SD-WAN a cada 5 (cinco) minutos no mínimo;
- O gerenciamento da solução deve suportar acesso via **SSH**, WEB (HTTPS) e também via API aberta;
- A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;
- Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica **utilizando IP, login e senha dos mesmos**;
- Deve permitir especificar o destinatário de cada relatório;
- Deve permitir filtrar informações nas abas de visualização;
- Deve permitir a alteração do formato dos relatórios: fontes, cores, imagens, gráficos, tabelas e o idioma;
- Deve permitir o envio de relatórios para servidores FTP externos;

a) Nosso solicitação de adequação/retirada de itens será aceita?

Belo Horizonte - MG, 12 de maio de 2023.

GUSTAVO HENRIQUE FANTONI NAURATH
EXECUTIVO DE NEGÓCIOS
CI: M 6402858
CPF: 953.489.566-00
naurath@oi.net.br

MITSUO ORLANDO NONAKA
Gerente de Vendas Corporativo
CI: M 9.063.318
CPF: 034.455.116-40
mitsuo@oi.net.br